

Slide 1

*Digital Audit Trails and Their Importance  
in Computer Crime Investigations*



Ottawa HTCIA Meeting  
24<sup>th</sup> Oct 2002

6/24/2003

Jamie French

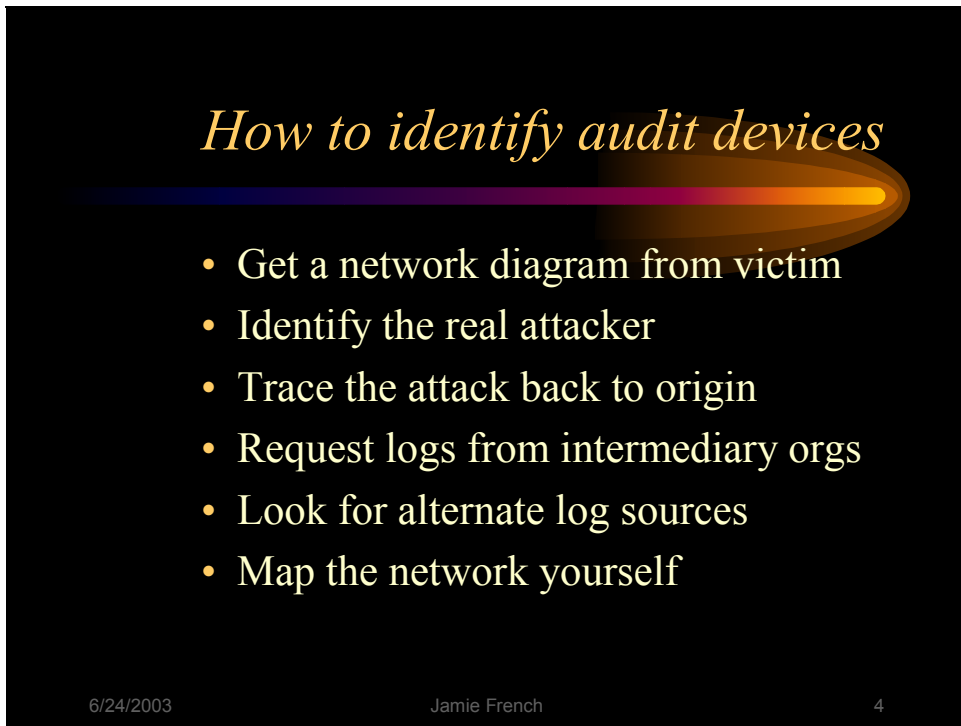
1

## *Introduction*

- Computer crime – leaves a trail
- Jamie French
  - DND CIRT Team
  - NRNS Inc. - RCMP CPIC
  - President Whitehats.ca
  - 9 years experience in packet analysis
  - SANS Intrusion Analyst Lead Grader (GCIA) and Advisory Board member

## *Topics of Discussion*

- Different log types
- Techniques used to preserve digital evidence
- What questions should be asked
- Common motives
- Overview of techniques used by cyber attackers
- Open discussion on legal issues



## *How to identify audit devices*

- Get a network diagram from victim
- Identify the real attacker
- Trace the attack back to origin
- Request logs from intermediary orgs
- Look for alternate log sources
- Map the network yourself

6/24/2003 Jamie French 4

Almost all network devices are capable of logging. Everything from printers to switches, firewalls to proxy servers. Remote attacks provide the best potential for an audit trail, however the complexity can increase dramatically.

Care must be taken to identify the real attacker. Spoofing an attack is not difficult to perform against many operating systems (OS'). Email addresses can easily be spoofed too. Additionally, an attacker may be using a "throw-away-host" that incriminates someone else, who unknowingly is a victim of the attack themselves.

Some cursory analysis should reasonably identify the true source of an attack or discount the spoofed sources. This can be done through passive OS fingerprinting, using tools such as traceroute, analyzing time stamps and graphing latency, correlation with other logs, conversation with the administrators of suspect computers etc.

Alternate log sources, once uncovered help fill in the puzzle. You have to act fast though, some of these logs are very large and their shelf-life is limited sometimes from a few days to a few hours.

Through the above mechanisms, you should be able to identify numerous potential audit devices. The next step is to try and obtain logs from them.

[http://www.eff.org/Privacy/Surveillance/Terrorism\\_militias/20011031\\_eff\\_usa\\_patriot\\_analysis.html](http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html)

<http://www.usatoday.com/life/cyber/tech/2002/05/28/net-surveillance.htm>

[http://www.internetnews.com/bus-news/article.php/3\\_1107521](http://www.internetnews.com/bus-news/article.php/3_1107521)

## *Audit device short list*

- Firewalls
  - Usually monitor ingress/egress
  - Personal FW
- Proxies
  - Log transactions and nat'ing
- System Applications
  - Win32 Eventlog
  - UNIX syslog
- Intrusion Detection Systems
  - NIDS
  - HIDS

## *Firewall - IPTables*

**IPTables:**  
<http://www.iptables.org>

**Explanation:**  
A full, stateful firewall that is found in use by both individuals and large organisations. Popular because it works well and the price is right. It is opensource and distributed with many Linux flavours.

**Example:**

```
Sep 29 15:54:15 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC= SRC=BAD.GUY0.168.107
DST=MY.NET.10.10 LEN=78 TOS=0x00 PREC=0x00 TTL=109 ID=44900 PROTO=UDP SPT=1047 DPT=137 LEN=58
Sep 29 15:55:40 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC= SRC=BAD.GUY1.132.160
DST=MY.NET.10.10 LEN=64 TOS=0x00 PREC=0x00 TTL=47 ID=48034 DF PROTO=TCP SPT=2581 DPT=1433
WINDOW=64240 RES=0x00 SYN URGP=0
Sep 29 15:58:26 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC= SRC=BAD.GUY2.232.145
DST=MY.NET.10.10 LEN=78 TOS=0x00 PREC=0x00 TTL=110 ID=24086 PROTO=UDP SPT=1064 DPT=137 LEN=58
Sep 29 16:03:53 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC= SRC=BAD.GUY3.70.197
DST=MY.NET.10.10 LEN=48 TOS=0x00 PREC=0x00 TTL=109 ID=3716 DF PROTO=TCP SPT=2696 DPT=27374
WINDOW=8760 RES=0x00 SYN URGP=0
Sep 29 16:26:22 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC= SRC=BAD.GUY4.77.82
DST=MY.NET.10.10 LEN=78 TOS=0x00 PREC=0x00 TTL=105 ID=42285 PROTO=UDP SPT=1025 DPT=137 LEN=58
```

6/24/2003 Jamie French 6

**IPTables:**

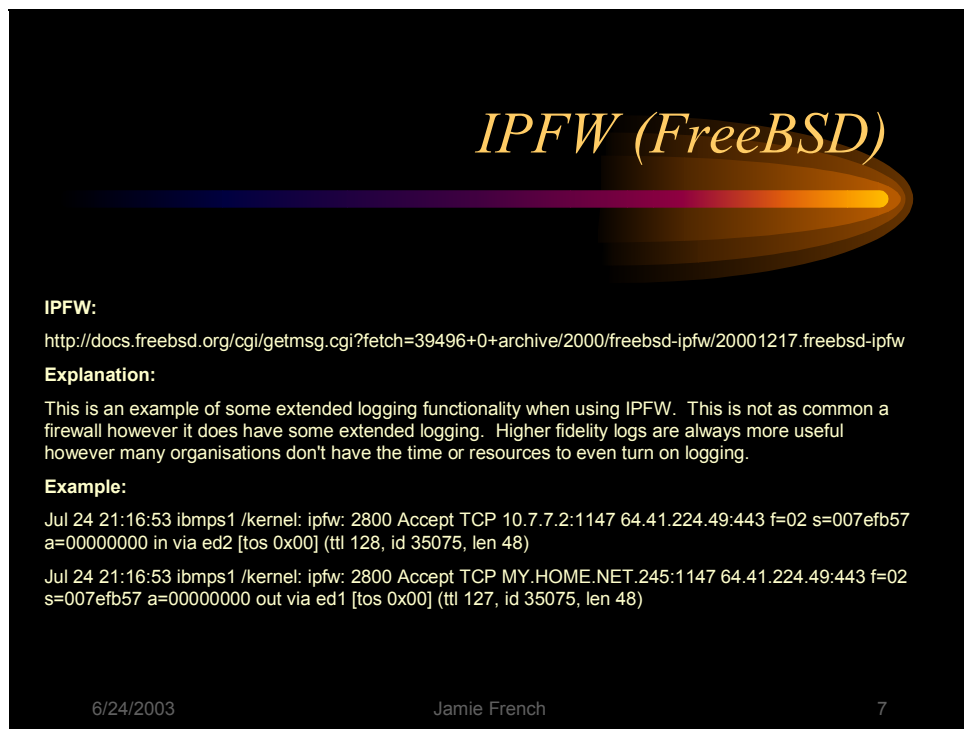
<http://www.iptables.org>

**Explanation:**

A full, stateful firewall that is found in use by both individuals and large organisations. Popular because it works well and the price is right. It is opensource and distributed with many Linux flavours.

**Example:**

```
Sep 29 15:54:15 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC=
SRC=BAD.GUY0.168.107 DST=MY.NET.10.10 LEN=78 TOS=0x00 PREC=0x00
TTL=109 ID=44900 PROTO=UDP SPT=1047 DPT=137 LEN=58
Sep 29 15:55:40 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC=
SRC=BAD.GUY1.132.160 DST=MY.NET.10.10 LEN=64 TOS=0x00 PREC=0x00 TTL=47
ID=48034 DF PROTO=TCP SPT=2581 DPT=1433 WINDOW=64240 RES=0x00 SYN
URGP=0
Sep 29 15:58:26 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC=
SRC=BAD.GUY2.232.145 DST=MY.NET.10.10 LEN=78 TOS=0x00 PREC=0x00
TTL=110 ID=24086 PROTO=UDP SPT=1064 DPT=137 LEN=58
Sep 29 16:03:53 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC=
SRC=BAD.GUY3.70.197 DST=MY.NET.10.10 LEN=48 TOS=0x00 PREC=0x00 TTL=109
ID=3716 DF PROTO=TCP SPT=2696 DPT=27374 WINDOW=8760 RES=0x00 SYN
URGP=0
Sep 29 16:26:22 firewall kernel: IPT INPUT packet killed: IN=ppp0 OUT= MAC=
SRC=BAD.GUY4.77.82 DST=MY.NET.10.10 LEN=78 TOS=0x00 PREC=0x00 TTL=105
ID=42285 PROTO=UDP SPT=1025 DPT=137 LEN=58
```

The slide features a dark background with a horizontal rainbow-colored oval graphic. The title 'IPFW (FreeBSD)' is written in a gold, serif font. Below the title, the text is organized into sections: 'IPFW:' with a URL, 'Explanation:' with a paragraph, and 'Example:' with two lines of kernel log output. At the bottom, there are three small white text elements: a date, a name, and a page number.

## IPFW (FreeBSD)

**IPFW:**  
<http://docs.freebsd.org/cgi/getmsg.cgi?fetch=39496+0+archive/2000/freebsd-ipfw/20001217.freebsd-ipfw>

**Explanation:**  
This is an example of some extended logging functionality when using IPFW. This is not as common a firewall however it does have some extended logging. Higher fidelity logs are always more useful however many organisations don't have the time or resources to even turn on logging.

**Example:**  
Jul 24 21:16:53 ibmps1 /kernel: ipfw: 2800 Accept TCP 10.7.7.2:1147 64.41.224.49:443 f=02 s=007efb57 a=00000000 in via ed2 [tos 0x00] (ttl 128, id 35075, len 48)  
Jul 24 21:16:53 ibmps1 /kernel: ipfw: 2800 Accept TCP MY.HOME.NET.245:1147 64.41.224.49:443 f=02 s=007efb57 a=00000000 out via ed1 [tos 0x00] (ttl 127, id 35075, len 48)

6/24/2003 Jamie French 7

**IPFW (FreeBSD Netfilter with extended logging by Crist J. Clark):**

<http://docs.freebsd.org/cgi/getmsg.cgi?fetch=39496+0+archive/2000/freebsd-ipfw/20001217.freebsd-ipfw>

**Explanation:**

This is an example of some extended logging functionality when using IPFW. This is not as common a firewall however it does have some extended logging. Higher fidelity logs are always more useful however many organisations don't have the time or resources to even turn on logging.

**Example:**

Jul 24 21:16:53 ibmps1 /kernel: ipfw: 2800 Accept TCP 10.7.7.2:1147 64.41.224.49:443 f=02 s=007efb57 a=00000000 in via ed2 [tos 0x00] (ttl 128, id 35075, len 48)  
Jul 24 21:16:53 ibmps1 /kernel: ipfw: 2800 Accept TCP MY.HOME.NET.245:1147 64.41.224.49:443 f=02 s=007efb57 a=00000000 out via ed1 [tos 0x00] (ttl 127, id 35075, len 48)

Slide 8



**Cisco PIX:**  
<http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/>

**Explanation:**  
This is a commonly found integrated software and hardware solution. It is likely that you will run across PIX logs while in the process of investigations at some point in time.

**Example:**  
May 15 11:22:31 [192.149.115.1] %PIX-4-500004: Invalid transport field for protocol=6, from 199.120.223.5/0 to MY.NET.197.4/0  
May 14 19:35:15 [192.149.115.1] %PIX-4-500004: Invalid transport field for protocol=6, from 144.232.173.2/0 to MY.NET.197.4/3072

6/24/2003                      Jamie French                      8

**Cisco PIX:**

<http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/>


**Explanation:**

This is a commonly found integrated software and hardware solution. It is likely that you will run across PIX logs while in the process of investigations at some point in time.

**Example:**

May 15 11:22:31 [192.149.115.1] %PIX-4-500004: Invalid transport field for protocol=6, from 199.120.223.5/0 to MY.NET.197.4/0

May 14 19:35:15 [192.149.115.1] %PIX-4-500004: Invalid transport field for protocol=6, from 144.232.173.2/0 to MY.NET.197.4/3072



**Norton Internet Security Firewall:**  
[http://www.symantec.com/sabu/nis/nis\\_pe/](http://www.symantec.com/sabu/nis/nis_pe/) (This is a newer product than the logs presented)

**Explanation:**  
Some SOHO or personal users will have personal firewalls. They can provide a lot of useful information.

**Example:**  
Date: 2002-07-22 Time: 15:27:28  
Unused port blocking has blocked communications. Details:  
Inbound TCP connection  
Remote address,local service is (216.150.220.206,ms-sql-s)

Date: 2002-07-22 Time: 15:29:47  
Unused port blocking has blocked communications. Details:  
Inbound TCP connection  
Remote address,local service is (206.246.124.41,ms-sql-s)

6/24/2003 Jamie French 9

**Norton Internet Security Firewall:**

[http://www.symantec.com/sabu/nis/nis\\_pe/](http://www.symantec.com/sabu/nis/nis_pe/) (This is a newer product than the logs presented)

**Explanation:**

Some SOHO or personal users will have personal firewalls. They can provide a lot of useful information.

**Example:**

Date: 2002-07-22 Time: 15:27:28

Unused port blocking has blocked communications. Details:

Inbound TCP connection

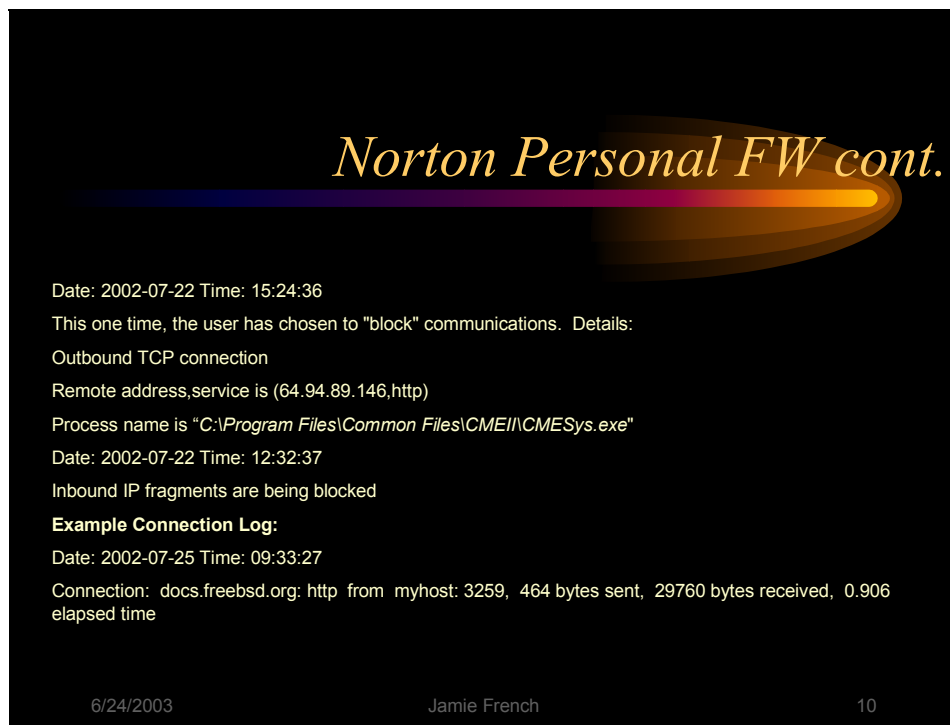
Remote address,local service is (216.150.220.206,ms-sql-s)

Date: 2002-07-22 Time: 15:29:47

Unused port blocking has blocked communications. Details:

Inbound TCP connection

Remote address,local service is (206.246.124.41,ms-sql-s)




*Norton Personal FW cont.*

Date: 2002-07-22 Time: 15:24:36  
This one time, the user has chosen to "block" communications. Details:  
Outbound TCP connection  
Remote address,service is (64.94.89.146,http)  
Process name is "C:\Program Files\Common Files\CMEII\CMESys.exe"  
Date: 2002-07-22 Time: 12:32:37  
Inbound IP fragments are being blocked  
**Example Connection Log:**  
Date: 2002-07-25 Time: 09:33:27  
Connection: docs.freebsd.org: http from myhost: 3259, 464 bytes sent, 29760 bytes received, 0.906 elapsed time

6/24/2003 Jamie French 10

Notice that personal firewalls can also monitor system processes and their attempted accesses to network resources.

Date: 2002-07-22 Time: 15:24:36  
This one time, the user has chosen to "block" communications. Details:  
Outbound TCP connection  
Remote address,service is (64.94.89.146,http)  
Process name is "C:\Program Files\Common Files\CMEII\CMESys.exe"  
Date: 2002-07-22 Time: 12:32:37  
Inbound IP fragments are being blocked  
**Example Connection Log:**  
Date: 2002-07-25 Time: 09:33:27  
Connection: docs.freebsd.org: http from myhost: 3259, 464 bytes sent, 29760 bytes received, 0.906 elapsed time



**Squid Proxy:**  
<http://www.squid-cache.org>  
<http://www.tenon.com/support/webten/papers/squidlog.shtml>

**Explanation:**  
If a proxy is used it by a suspect you will want to obtain these logs. The entries will contain information on the originating request and the destination host requested. This is very important when trying to trace traffic back to a proxied address because the address will have been modified by the proxy and all evidence once past the proxy will contain the proxy servers address vice the real attacker.

**Example:**

```
1011164724.171 1337 10.0.0.1 TCP_MISS/200 20110 GET \ http://images.google.com/images? -  
DIRECT/10.0.0.2 text/html 1011164724.965 740 10.0.0.1 TCP_MISS/200 26461 GET \  
http://www.ia.hiof.no/informatikk/forelesning/historie/historie.html \ - DIRECT/10.0.0.3 text/html  
1011164727.626 2580 10.0.0.1 TCP_MISS/200 111927 GET \  
http://www.ia.hiof.no/informatikk/forelesning/historie/transistor.jpg \ - DIRECT/10.0.0.3 image/jpeg
```

6/24/2003 Jamie French 11

**Squid Proxy:**

<http://www.squid-cache.org>

<http://www.tenon.com/support/webten/papers/squidlog.shtml>

**Explanation:**

If a proxy is used it by a suspect you will want to obtain these logs. The entries will contain information on the originating request and the destination host requested. This is very important when trying to trace traffic back to a proxied address because the address will have been modified by the proxy and all evidence once past the proxy will contain the proxy servers address vice the real attacker.

**Example:**

```
1011164724.171 1337 10.0.0.1 TCP_MISS/200 20110 GET \  
http://images.google.com/images? - DIRECT/10.0.0.2 text/html 1011164724.965 740  
10.0.0.1 TCP_MISS/200 26461 GET \  
http://www.ia.hiof.no/informatikk/forelesning/historie/historie.html \ - DIRECT/10.0.0.3  
text/html 1011164727.626 2580 10.0.0.1 TCP_MISS/200 111927 GET \  
http://www.ia.hiof.no/informatikk/forelesning/historie/transistor.jpg \ - DIRECT/10.0.0.3  
image/jpeg
```



## *Windows EventLog Cont.*

### **Example System Log:**

Type,Date,Time,Source,Category,Event,User,Computer  
Information,2002-10-22,01:08:27,Tcpip,None,4201,N/A,MYHOST  
Information,2002-10-22,01:08:07,Browser,None,8033,N/A,MYHOST  
Warning,2002-10-21,01:49:47,Dnscache,None,11050,N/A,MYHOST  
Information,2002-10-20,10:34:15,VMnetx,None,34,N/A,MYHOST  
Error,2002-10-18,07:54:09,MrxSmb,None,8003,N/A,MYHOST

### **Example Security Log:**

Type,Date,Time,Source,Category,Event,User,Computer  
Success Audit,2002-10-24,10:40:11,Security,Logon/Logoff ,528,USER,MYHOST  
Success Audit,2002-10-24,10:40:11,Security,Account Logon ,680,SYSTEM,MYHOST  
Failure Audit,2002-10-24,10:40:06,Security,Privilege Use ,578,USER,MYHOST  
Failure Audit,2002-10-24,10:39:59,Security,Privilege Use ,578,USER,MYHOST

6/24/2003

Jamie French

13

### **Example System Log:**

Type,Date,Time,Source,Category,Event,User,Computer  
Information,2002-10-22,01:08:27,Tcpip,None,4201,N/A,MYHOST  
Information,2002-10-22,01:08:07,Browser,None,8033,N/A,MYHOST  
Warning,2002-10-21,01:49:47,Dnscache,None,11050,N/A,MYHOST  
Information,2002-10-20,10:34:15,VMnetx,None,34,N/A,MYHOST  
Error,2002-10-18,07:54:09,MrxSmb,None,8003,N/A,MYHOST

### **Example Security Log:**

Type,Date,Time,Source,Category,Event,User,Computer  
Success Audit,2002-10-24,10:40:11,Security,Logon/Logoff ,528,USER,MYHOST  
Success Audit,2002-10-24,10:40:11,Security,Account Logon ,680,SYSTEM,MYHOST  
Failure Audit,2002-10-24,10:40:06,Security,Privilege Use ,578,USER,MYHOST  
Failure Audit,2002-10-24,10:39:59,Security,Privilege Use ,578,USER,MYHOST

## Syslog (Unix Logs)

### Syslog:

<http://www.balabit.hu/en/downloads/syslog-ng/>

<http://www.campin.net/newlogcheck.html>

<http://sourceforge.net/projects/syslogd-sql/>

### Explanation:

Similar to the Windows Event logs. Unix and Linux systems perform accounting on applications. Larger organisations will forward these logs to a central server for correlation and to add extra protection against the possibility of system compromise and log destruction by the attacker. Check for a central logging server when trying to find evidence. Optimally you hope to find a central server where the mark function was enabled. This will give time references at specific intervals in the log and help identify troubles with the host in question. There are lots of log naming conventions and location positions between different Unix and Linux systems. The most common place to look is in the /var directory on the local host. Important to note too is that some of these logs can be written to a database. The configuration files for syslog are usually located in /etc/syslog.conf

### Example Syslog:

```
Oct 7 11:26:01 sunshine sendmail[25467]: [ID 801593 mail.info] g97FQ06u025467:
from=<nobody@sunshine>, size=530, class=0, nrcpts=1, msgid=<200210071526.g97FQ0Sh
025461@sunshine>, proto=ESMTP, daemon=MTA-v6, relay=localhost [IPv6:::1]
Oct 7 11:26:01 sunshine sendmail[25461]: [ID 801593 mail.info] g97FQ0Sh025461:
to=user@domain.com, ctladdr=nobody (60001/60001), delay=00:00:01, xdelay=00
6/24/2003 Jamie French
```

14

### Syslog:

<http://www.balabit.hu/en/downloads/syslog-ng/>

<http://www.campin.net/newlogcheck.html>

<http://sourceforge.net/projects/syslogd-sql/>

### Explanation:

Similar to the Windows Event logs. Unix and Linux systems perform accounting on applications. Larger organisations will forward these logs to a central server for correlation and to add extra protection against the possibility of system compromise and log destruction by the attacker. Check for a central logging server when trying to find evidence. Optimally you hope to find a central server where the mark function was enabled. This will give time references at specific intervals in the log and help identify troubles with the host in question. There are lots of log naming conventions and location positions between different Unix and Linux systems. The most common place to look is in the /var directory on the local host. Important to note too is that some of these logs can be written to a database. The configuration files for syslog are usually located in /etc/syslog.conf

### Example Syslog:

```
Oct 7 11:26:01 sunshine sendmail[25467]: [ID 801593 mail.info] g97FQ06u025467:
from=<nobody@sunshine>, size=530, class=0, nrcpts=1, msgid=<200210071526.g97FQ0Sh
025461@sunshine>, proto=ESMTP, daemon=MTA-v6, relay=localhost [IPv6:::1]
Oct 7 11:26:01 sunshine sendmail[25461]: [ID 801593 mail.info] g97FQ0Sh025461:
to=user@domain.com, ctladdr=nobody (60001/60001), delay=00:00:01, xdelay=00
```

## *Syslog (Unix Logs) Cont.*

### **Example Message Log:**

```
[root@host directory]# tail -2 /var/log/messages
```

```
Oct 24 11:31:46 host su(pam_unix)[4844]: authentication failure; logname=user uid=500 euid=0 tty=
ruser= rhost= user=root
```

```
Oct 24 11:31:53 host su(pam_unix)[4845]: session opened for user root by user(uid=500)
```

### **Example Secure Log:**

```
[root@host directory]# tail -3 /var/log/secure
```

```
Oct 24 11:31:42 host sshd[4801]: Accepted password for user from 192.168.3.15 port 4003 ssh2
```

```
Oct 24 11:31:42 host sshd[4801]: Could not reverse map address 192.168.3.15.
```

```
Oct 24 11:32:16 host sshd[4701]: fatal: Timeout before authentication for 192.168.3.15.
```

6/24/2003

Jamie French

15

### **Example Message Log:**

```
[root@host directory]# tail -2 /var/log/messages
```

```
Oct 24 11:31:46 host su(pam_unix)[4844]: authentication failure; logname=user uid=500
euid=0 tty= ruser= rhost= user=root
```

```
Oct 24 11:31:53 host su(pam_unix)[4845]: session opened for user root by user(uid=500)
```


### **Example Secure Log:**

```
[root@host directory]# tail -3 /var/log/secure
```

```
Oct 24 11:31:42 host sshd[4801]: Accepted password for user from 192.168.3.15 port 4003
ssh2
```

```
Oct 24 11:31:42 host sshd[4801]: Could not reverse map address 192.168.3.15.
```

```
Oct 24 11:32:16 host sshd[4701]: fatal: Timeout before authentication for 192.168.3.15.
```



**Snort IDS:**  
<http://www.snort.org>

**Explanation:**  
Snort is an opensource Network Intrusion Detection System (NIDS) that is in wide use. It is signature based and contains numerous plugins to help it process network traffic and reduce false positives. There are numerous methods of logging configurable. Depending upon how Snort was configured, you will either have high fidelity logs or low fidelity logs or possibly no logs at all if the activity didn't trigger a predefined signature.

**Example of Full Alert:**

```
[**] [1:498:3] ATTACK RESPONSES id check returned root [**]  
[Classification: Potentially Bad Traffic] [Priority: 2]  
10/14-14:47:30.112960 205.206.231.26:60933 -> dilbert:25  
TCP TTL:48 TOS:0x0 ID:64651 IpLen:20 DgmLen:1500 DF  
***A**** Seq: 0xF594B59F Ack: 0x9F72644E Win: 0x1920 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 242243528 1462264552
```

**Example of Fast Alert:**

```
09/04-00:00:13.042590 [**] ICMP Destination Unreachable (Network Unreachable) [**] MY.NET.30.2 ->  
195.78.199.37
```

6/24/2003 Jamie French 16

**Snort IDS:**

<http://www.snort.org>

**Explanation:**


Snort is an opensource Network Intrusion Detection System (NIDS) that is in wide use. It is signature based and contains numerous plugins to help it process network traffic and reduce false positives. There are numerous methods of logging configurable. Depending upon how Snort was configured, you will either have high fidelity logs or low fidelity logs or possibly no logs at all if the activity didn't trigger a predefined signature.

**Example of Full Alert:**

```
[**] [1:498:3] ATTACK RESPONSES id check returned root [**]  
[Classification: Potentially Bad Traffic] [Priority: 2]  
10/14-14:47:30.112960 205.206.231.26:60933 -> dilbert:25  
TCP TTL:48 TOS:0x0 ID:64651 IpLen:20 DgmLen:1500 DF  
***A**** Seq: 0xF594B59F Ack: 0x9F72644E Win: 0x1920 TcpLen: 32  
TCP Options (3) => NOP NOP TS: 242243528 1462264552
```

**Example of Fast Alert:**

```
09/04-00:00:13.042590 [**] ICMP Destination Unreachable (Network Unreachable) [**]  
MY.NET.30.2 -> 195.78.199.37
```



**Tcpdump (Shadow IDS):**  
<http://www.tcpdump.org>

**Explanation:**  
 Tcpdump is a tool that can sniff traffic off of the network. Some IDS' employ tcpdump to perform their network captures. If you suspect an attacker is still online or will return, it is recommended that you run a properly configured tcpdump command on the network segment to gather more logs.

**Example:**

```
12:58:44.952664 216.136.171.197.http > 192.168.3.14.4554: S [tcp sum ok] 488899854:488899854(0)
ack 482888143 win 32476 <mss 1412,nop,nop,sackOK> (DF) (ttl 49, id 7470, len 48)

    4500 0030 1d2e 4000 3106 e495 d888 abc5
    c0a8 030e 0050 11ca 1d24 050e 1cc8 49cf
    7012 7edc 217b 0000 0204 0584 0101 0402

12:58:44.952664 64.230.5.120.4554 > 216.136.171.197.http: . [tcp sum ok] ack 488899855 win 16944
(DF) (ttl 126, id 20718, len 40)

    4500 0028 50ee 4000 7e06 e135 40e6 0578
    d888 abc5 11ca 0050 1cc8 49cf 1d24 050f
    5010 4230 0814 0000
```

6/24/2003 Jamie French 17

**Tcpdump (Shadow IDS):**

<http://www.tcpdump.org>

**Explanation:**

Tcpdump is a tool that can sniff traffic off of the network. Some IDS' employ tcpdump to perform their network captures. If you suspect an attacker is still online or will return, it is recommended that you run a properly configured tcpdump command on the network segment to gather more logs.

**Example:**

```
12:58:44.952664 216.136.171.197.http > 192.168.3.14.4554: S [tcp sum ok]
488899854:488899854(0) ack 482888143 win 32476 <mss 1412,nop,nop,sackOK> (DF) (ttl
49, id 7470, len 48)

    4500 0030 1d2e 4000 3106 e495 d888 abc5
    c0a8 030e 0050 11ca 1d24 050e 1cc8 49cf
    7012 7edc 217b 0000 0204 0584 0101 0402

12:58:44.952664 64.230.5.120.4554 > 216.136.171.197.http: . [tcp sum ok] ack 488899855
win 16944 (DF) (ttl 126, id 20718, len 40)

    4500 0028 50ee 4000 7e06 e135 40e6 0578
    d888 abc5 11ca 0050 1cc8 49cf 1d24 050f
    5010 4230 0814 0000
```

## *Techniques used to Preserve Digital Evidence*

- Disclaimer\*\*\* I have not had any formal training in the handling of digital evidence. The techniques presented here represent some methods of handling digital evidence however they may not be fit for use in a trial.

## *Techniques used to Preserve Digital Evidence*

- **Maintain Media Integrity**
  - Do not write to the media
  - Try to take a snapshot of RAM prior to shutdown or powerdown of the system
  - Take care of the evidence
- **Watch the suspect has not sabotaged evidence**
- **Use math to your advantage**

6/24/2003 Jamie French 19

**Don't write to the media:**

Once you find the evidence, it must be protected so that it does not become modified. Even rebooting a system from the operating system will have an impact on the integrity of state at the time of seizure. This will write information to the hard drive.

**Try to take a snapshot of RAM if possible:**

Easier said than done. Especially if the tools are already on the machine. Reason why we want to take a snapshot of RAM is because once power stops flowing to the RAM, it will reset itself and anything stored there will be lost.

On Solaris you can use the command gcore and direct output to another device. There are perl scripts such as dump that will also create core files. A very common utility for use in this area is lsof or list of open files. It is a hit and miss as to whether this will be installed on a system however a statically linked 32 or 64 bit sparc or x86 version should be kept on a floppy or CDROM and may be mounted and used to retrieve information on the network sockets (ports) open on a system, take a snapshot of which processes are being called by which other processes, where temp and log files are being currently written to for future reference etc.

On XP, the webpage found at [http://www.kellys-korner-xp.com/win\\_xp\\_logfiles.htm](http://www.kellys-korner-xp.com/win_xp_logfiles.htm) gives some good information. Something similar to lsof on Win32 machines would be fport from Foundstone.

<http://www.foundstone.com/knowledge/proddesc/fport.html>

**Take care of the evidence:**

Example: Don't drop a hard drive, keep in mind environmental issues and how they can affect the physical media and the evidence. Another bad idea is keeping a floppy disk left on the front dash of a car. It could damage the media if the temperature rises too high.

**Watch the suspect has not sabotaged evidence:**

Be very careful when first inspecting the crime scene. The suspect may have placed a bomb in their computer case that goes off if the case is turned on its side, which would destroy the evidence.

Create a copy or duplicate of the evidence so that you have a working copy, then secure the original evidence and make sure you follow well documented, written down procedures and policies, keeping a written journal of the activity and have proof that there is a chain of custody for the evidence to disprove any opposition that might question the authenticity of the evidence and ask for proof that it was not tampered with.

**Use Math to your advantage:**

This is an important step. This will, when done correctly, support the law enforcements evidence and chain of custody procedures and should completely put any dispute by the defense to rest regarding the validity of evidence, unless of course there was a problem with the chain of evidence and it was truly tampered with.

When duplicating digital evidence, make a cryptographic hash of the evidence. This hash is a one-way value that is computationally infeasible to generate going backwards. Examples of hash functions are Message Digest 5 (MD5) and SHA1. There is a listing of various hash functions at <http://planeta.terra.com.br/informatica/paulobarreto/hflounge.html>. Basically, SHA1 is considered to be the strongest as it uses longer hash values, is fast, and was developed by the NSA. The value computed on the digital evidence will very difficult to reproduce. If the evidence is modified, the value of the hash will be incorrect. The possibility of the evidence being modified and generating the same hash value is what is computationally infeasible.

You can also cryptographically sign digital evidence so that it is authenticated as having been worked on by you, or depending on the protocol used, at least worked on and signed by someone with your private key. Talking about the strengths and weaknesses of these protocols is well outside the scope of this discussion. Simply put, if you use a digital signature you can provide a very strong argument to support the authenticity, data integrity, and non-repudiation of data and work completed.

## *What Questions should I Ask?*

- What other logging sources are there? Where can I gather more evidence?
- Can one of your staff map the current network for me or would you allow me to do this?
- May I perform some forensics prior to the machine being shutdown?
- How was the evidence handled before I arrived on the scene?

6/24/2003Jamie French20

Generally, you want to identify as many sources of logging as you can. If the attack came in over a network, your odds have increased dramatically in being able to obtain logs from other devices. There is a finite life of logs however and they usually overwrite themselves in a cyclical fashion. Old logs usually disappear, sometimes within a few hours, sometimes not for a few months. The moral of the story is, after securing the device in question, you should be looking at securing logs from other devices, and making notes on time differentials from the victim machine or another reference time that you have chosen to apply to all logs from this point forward into your investigation.

It is important to note that it is probably not always advisable to immediately deny access to the resource being attacked. If the attacker is currently on the scene or logged in, start gathering some additional evidence of their behaviour. This will very likely save a lot of man-hours in analysis later. For example, if you can gather video footage of a crime, say an employee stealing from an employer, the case will be a lot easier to prove in court. I am confident the same would apply to a computer crime case where the more targeted the evidence, the easier the prosecution would be. Actually, if the attacker is online at the time the investigation starts, I would highly recommend keeping the attacker online as long as possible and using various methods to trace him or her back to their point of origin, and if possible, securing that point and start monitoring for all inbound/outbound connections from there to the next point and so on... This could take an investigation from being in the realm of not being prosecutable to being a very strong case and actually catching the hacker.

If possible, perform some forensics prior to shutting down the computer. This will be a luxury if you come across a suspected crime scene that is still hot.

Ask questions that create a chain of custody around the evidence prior to your arrival. The complete system should be confiscated as evidence, not just the hard drive. There are times when peripherals may be needed, such as if it is deemed necessary to boot a duplicate image of the digital evidence up to support forensic evidence etc.

What other questions would you ask?

## *Common Motives of Computer Crime*

- Feeling of lawlessness. People don't take it seriously because they compare it to the Wild West where they can't be traced or prosecuted.
- Phenomenal power of information, speed, and access to the crime scene.
- Low cost
- Shortage of Law Enforcement

6/24/2003Jamie French21

### **Access to the crime scene:**

Comparison – If a thief were to break into the Canadian Mint to steal a bag of money, they would face a lot of resistance and security. They may even have to use physical force and risk being killed while trying to take the money. Risk factor vs payoff might be considered a 9/10. Now if the same amount of money could be stolen via a computer connection, the thief has bypassed all the guards, and still got their money. More importantly, even if they are caught, the guards that catch the thief won't be able to hurt them physically because they are not physically at the scene. Risk factor vs payoff might be considered 3/10, with the added benefit that you can digitally transfer sums of money much larger than you could physically carry in a few fractions of a second! Now consider the work that would be involved in trying to break into the mint. Think of the movie "The Score" with Robert DeNiro and Edward Norton. They had to go to a lot of work to get into the crime scene. On the Internet, there are literally hundreds of thousands of them and many offer the potential intruder anonymity through poor security or developed techniques for evading detection.

### **Low Cost:**

The cost to commit computer crime can be very low. From free (a library terminal) to a few hundred dollars for a used computer and a free connection to the Internet. Remember, hackers don't necessarily require a high speed connection. It is easier to steal dial-up account password and logins than it is to forge a PPPoE Magic Cookie. Issuing commands to a compromised host only takes a few bytes where that host might have a high speed connection and therefore be used to perform high bandwidth DoS, DDoS attacks, or reconnaissance probes.

### **Shortage of Law Enforcement Qualified to Perform the job:**

I don't think this is relegated only to computer crime. I'm sure more resources would help in all areas from homicide to fraud to domestic disturbances to traffic etc. I do however think that with more resources and better preparedness by our current law enforcement we would be able to better handle cases of computer crime.

*Thank You!*



Ottawa Chapter HTCIA Meeting

Oct 24<sup>th</sup> 2002

275 Slater St

Ottawa, ON

## *Open Discussion*

- Legal issues
  - Open Kiosks in public places
  - Liability issues
  - Honeypots and entrapment
  - ???
  - ???
  - ???