Digital Forensic

Martin Pfeilsticker
Martin.Pfeilsticker@exodus.net

Richard Starnes
Richard.Starnes@exodus.net

THE INFRASTRUCTURE FOR THE DIGITAL ECONOMY™

EXODUS®

EXODUS®

Agenda

- **What is Digital Forensic?**
- **Definitions**
- **Case Study**
- **Q&a**

Cyber Attack Tiger Team
C.A.T.T.

THE INFRASTRUCTURE FOR THE DIGITAL ECONOMY™

EXODUS®

EXODUS®

What is Forensic?

Forensic Science is any aspect of science as it relates to the law

EXODUS

What is Digital Forensic?

Digital forensics is the application of computer investigation and analysis techniques in the interests of determining potential legal evidence

EXODUS

Definitions

- **Acquisition of Digital Evidence: Begins when information and/or physical items are collected or stored for examination purposes. The term "evidence" implies that the collector of evidence is recognized by the courts. The process of collecting is also assumed to be a legal process and appropriate for rules of evidence in that locality. A data object or physical item only becomes evidence when so deemed by a law enforcement official or designee.**
- **Data Objects: Objects or information of potential probative value that are associated with physical items. Data objects may occur in different formats without altering the original information.**
- **Digital Evidence: Information of probative value stored or transmitted in digital form.**
- **Physical Items: Items on which data objects or information may be stored and/or through which data objects are transferred.**

Definitions (cont.)

- Original Digital Evidence: Physical items and the data objects associated with such items at the time of acquisition or seizure.
- Duplicate Digital Evidence: An accurate digital reproduction of all data objects contained on an original physical item.
- Copy: An accurate reproduction of information contained on an original physical item, independent of the original physical item.

Investigations

- Intrusion
- data theft or misuse
- gathering evidence for other legal cases (warez, porn, blackmail, ..)
- intelligence

Investigation results

The investigation should answer:

- **who did**
- **what**
- **when**
- **how**

A case study

A Linux webserver shows an unusual behaviour:

- **increased network traffic**
- **file system showing more usage than expected**
- **high system load**

Stop and think!

What is the purpose of the investigation?
Ask your management!

- **Legal prosecution ?**
  Ask the police!
- **Internal investigation?**
  Ask Legal and HR!
- **Technical investigation?**
  Ask your experts/admins!

Document it!

- **Write down everything you do**
- **Write down everything you find**
- **If necessary, make photos**
- **Label everything you remove and put it in a secured place (safe, etc)**
- **document what you do with the evidence**

Legal or technical investigation?

Result of legal investigation

- evidence for a legal process
- report for police or prosecutor
- must be relevant to the case

Result of technical investigation

- input for the security process
- report for admin or management
- patches, configuration changes, etc

Secure and investigate the scene

None intrusive

- physical location
- Network topology
- IP addresses
- state of the computer or device
  (power on/off, network, etc)

stop unauthorized and uncontrolled access

- **block network connection**
  (Firewall, pull the cable)
- **security guard**

if necessary, switch the power off

- **watch out for logical bombs**
- **save the memory (core dump, crash dump)**

Document, what you have done!

Chose your investigation platform

- **must be secure and not compromised**
  - own Laptop
  - “Bouncer” computer
  - close to the victim

Gather information

information about the victim

- Name, IP addresses, OS and version
- system time!
- uptime
- file system, mount points or volumes
- hardware
- User and groups

- Port Scan from external
  compare to netstat output

- running processes

Use a bounce directory

- Not in the usual file system e.g. /tmp/CATT
- place for the gathered data and files
- place for clean binaries
- follows the file system layout
- can be easily copied and deleted

Document it!

Log files and their data

output of

- ls –al /var/adm or /var/log
- last
- who
- Kernel messages (dmesg)
- other logs like web and ftp-server logs, databases, ssh, mail, kernel, etc.

- Document and copy the logs to your bounce directory

Examine the log files

repeated entries

- errors
- logins

strange entries

- hex or binary entries
- long or entries

Document it!

Can you trust the system ?

hide the activities of a hacker

- **Altered or changed binaries (root-kit)**
- **Kernel modules**
- **backdoors and logical bombs**
- **sniffer**

quick check:

`ls –alt /usr/bin or ls –alt /usr/sbin`

(does not work with kernel module root kits)

`rpm –verify <package name>`

(use the package manager to verify the checksums)

Can you trust the system ?

Copy clean binaries into your bounce directory and add them to your command PATH
e.g.

```
mkdir /tmp/CATT/bin
scp login@bounce:/clean/cleanbin.tar.gz /tmp/CATT/bin
tar –xvof cleanbin.tar
PATH=/tmp/CATT/bin:$PATH
export PATH
```

Check the system

with the clean binaries check

- processes
- interfaces
- netstat
- strange directories e.g.

```
find / -name \.\* -xdev –ls
```

- unknown user and group id
- network connections and open files with lsof

Document it!

Investigate system files

- /etc/passwd
- inetd.conf
- services
- startup files in rc.d

Favourite places for root-kits

- /dev/ida/.*
- /usr/man
- /lib/modules
- /usr/lib

Favourite trojanized programmes

- ps, ls, find, ifconfig, netstat, du, df
- sshd
- login, passwd
- inetd, tcpd

What did the hacker do?

Examine:

- **system logs**
- **shell history (.bash_history, .history)**

- **special programmes or directories**
  - irc bouncer
  - hidden fileserver
  - DoS tools
  - sniffer

Document it!

When was the system hacked?

- **file timestamps (create and modified)**
- **logfile entries**

- **backup or other historic data**

How was the system hacked

- log files
- vulnerability scans (Nessus, ISS)
- Advisories (CERT, vendor, etc..)

Write a report

Answer to

- Who
- When
- What
- How

Write only what you can prove,
prove what you write.

T00lz

- **nmap (www.insecure.org/nmap)**
- **nessus (www.nessus.org)**
- **lsof (ftp://**vic.cc.purdue.edupub/tools/unix/lsof)
- **chkrootkit (www.chkrootkit.org)**
- **The Coroner's Toolkit (www.porcupine.org/forensics/tct.html)**

Links

- **www.cert.org**
- **http://www.washington.edu/People/dad (Dave Dittrich)**
- **www.incidents.org**
- **http://www.incident-response.org**
- **http://www.cops.org/forensic_examination_procedures.htm**
- **http://www.jura.uni-muenster.de/netlaw/default.cfm (NetLaw)**
- **www.cattir.com**

Questions?

Richard Starnes
Incident Response Team Leader
Richard.Starnes@exodus.net

+44 (0) 20-7758-4383(office)
+44 (0) 77-7167-3727(cell phone)