Chapter 5

Live Data Collection Windows Systems

Ed Crowley

Spring 10

Topics

- Live Investigation Goals
- Creating a Response Toolkit
- Common Tools and Toolkits
- Preparing the Toolkit
- Storing Information Obtained During the Initial Response
- Transferring Data with Netcat
- Integrity with md5sum
- Encrypting Data with Cryptcat
- Volatile Data for Live Response
- Investigation Organizing and Documenting
- Collecting Volatile Data, 10 Steps
- In Depth Live Response
- Obtaining Event Logs during Live Response
- System Passwords

Live Investigation Goals

- Obtain enough information to determine appropriate response.
- Considerations include totality of the circumstances
  - Learn before responding
- Two goals:
  1. Confirm there is an incident
  2. Retrieve volatile system data
     - Won’t be there after system powered off

Creating a Response Toolkit

- Without affecting any potential evidence, plan to obtain all relevant information.
- By collecting trusted files on a CD, you are better equipped to respond:
  - Quickly
  - Professionally
  - Successfully

Some Common Tools and Sources

- Cmd.exe
- PsLoggedOn *SysInt*
- rasusers *NTRK*
- netstat
- fport *FS*
- PsList *SysInt*
- ListDLLs *FS*
- nbstat
- arp
- kill *NTRK*
- md5sum *etree.org*
- rmtshare *NTRK*
- netcat *atstake*
- cryptcat *sourceforge*
- PsLogList *FS*
- ipconfig
- PsInfo *SysInt*
- PsFile *SysInt*
- PsService *SysInt*
- auditpol *NTRK*
- doskey

Tool Interface Categories

- Graphical or command line
  - GUI or CLI
- Since GUI programs create windows, have pull down menus, and generally do “behind the scenes” interaction, the text authors advise against using them during an investigation.

Preparing the Toolkit

- Label response toolkit media with:
  - Case number
  - Time and date
  - Name of investigator
  - Presence of output files?
- Check for dependencies (Filemon)
- Create toolkit checksum
- Write protect any toolkit floppies

Storing Information Obtained During the Initial Response

- Live refers to a currently powered on system.
- Environment untrusted
  - Unexpected should be anticipated.

Four options

1. Save the retrieved data to a hard dive
2. Record data in a notebook by hand
3. Save data onto the response floppy disk
   - Or other removable storage medium
4. Save data on a remote system using net or cryptcat

Transferring Data with Netcat

- Netcat can create a connection between the target system and the forensic workstation
  - Allows you to review information offline
- After the data transfer is complete, you will need to break the connection.
  - On the forensic workstation, press CTRL-C.

Integrity with md5sum

- Protect the integrity of retrieved files.
  - Among other places, you can get md5sum for windows from etree.org
- Perform the md5sum in the front of witnesses.

Process Summary

- Run trusted commands on NT Server
- Send output to forensics box with NetCat
- Md5sum files
- Perform off-line review

Encrypting Data with Cryptcat

- Cryptcat has the same syntax and functions as netcat
  - Encrypted data transfer.

Encrypting files means that:

- Attacker's sniffer cannot compromise your information (Unless your passphrase is compromised.)
- Encryption nearly eliminates risk of data contamination or injection

Volatile Data for Live Response

Only available prior to system power off.

Possible data items include:

- System date and time
- Currently logged on users
- Time/date stamps for entire file system
- Currently running processes
- Currently open sockets
- Applications listening on open sockets
- Systems that have current or recent connections to the system

Investigation Organization and Documentation

Two reasons to document

1. Gather information that may become evidence
2. Protect organization

Notes

- Before starting, create tool hashes
- Use a form to plan and document response.
- Good policy to have a witness sign the form and verify each MD5 sum.

Collecting Volatile Data

1. Execute trusted cmd.exe
2. Record system time and date
3. Determine logged users
4. For all files, record modification, creation, and access times.
5. Determine open ports.
6. List applications associated with open ports
7. List all running processes
8. List current and recent connections
9. Document commands used during initial response.

Gathering Data One

- For all files, record modification, creation, and access times
    - Dir
- Determine open ports
    - Fport
- Enumerate all running processes on the target system
    - PsList

Note, to identify abnormal processes, you first need to have identified normal processes i.e. done a baseline.

Gathering Data Two

- List current and recent connections
  - Netstat can determine current connections as well as the remote IP address of those connections
- Arp cache contains IP addresses mapped to MAC addresses
- Use nbtstat to access the remote NetBIOS name cache

Gathering Data Three

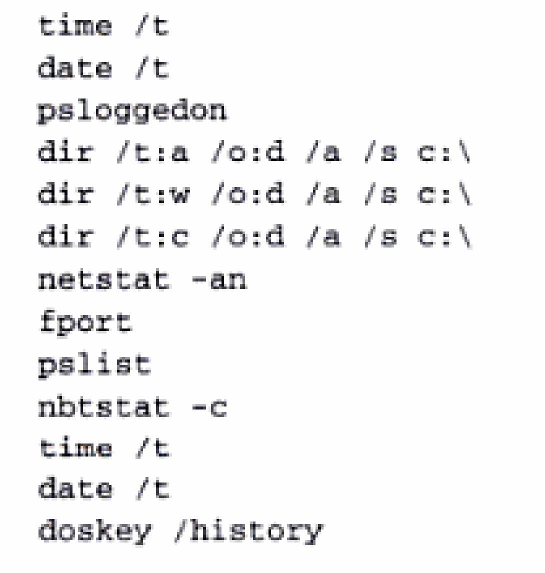
Use:

```
doskey /history
```

to display the command history of the current command shell

Scripting Initial Response

- Many technical steps performed during the initial response can be incorporated into a batch script.
- For example, ir.bat from Mandia, page 114.



```
time /t
date /t
psloggedon
dir /t:a /o:d /a /s c:\
dir /t:w /o:d /a /s c:\
dir /t:c /o:d /a /s c:\
netstat -an
fport
pslist
nbtstat -c
time /t
date /t
doskey /history
```

In Depth Live Response

- Date and time commands
- PsLoggedOn
- Netstat
- PsList
- Fport
- Safeback or EnCase.

In Depth Response Tools

- Auditpol *NTRK*
- Reg *NTRK*
- Regdump *NTRK*
- Pwdump3e
- NTLast *FS*
- Sfind *FS*
- Afind *FS*
- Dumpel *NTRK*

Collecting Live Response Data

- Review
  - Event logs
  - Registry
- Obtain system passwords
- Dump system RAM

Obtaining Event Logs during Live Response

- Auditpol discovers which audit policies exist
- NTLast allows you to monitor successful and failed system logons
- Dumpel can retrieve remote logs

Live Response: Reviewing the Registry

- Regdump creates an enormous text file from a registry.

- Reg query extracts just the Registry key values of interest

System Passwords

- Use pwdump3e to dump the passwords from the SAM file
- Crack them with John or similar tool or
- Use Rainbow tables
- You may also want to dump system RAM

Decide

- Forensic duplication necessary?

Questions?

Chapter 6

Live Data Collection from Unix Systems

Ed Crowley

Spring 10

Topics

- Creating a Response Toolkit
- Storing Obtained Information
- Obtaining Volatile Data Prior to Forensic Duplication
- Data to Collect
- Unix File Deletion
- Executing a Trusted Shell
- Gathering Info

Intro

- Unix allows the deletion of a program after it executes.
- Many Unix variants are neither backwards nor forwards compatible.

Creating a Response Toolkit

- Many Unix distributions requires their own unique toolkit.
- Prior to incident, create response toolkits.
- Only use trusted commands.

Storing Information Obtained During the Initial Response

- Options include:
  - Local hard drive
  - Remote media
  - Record information by hand
  - For digital transport, use netcat or cryptcat

Best Time

- After selecting how you will retrieve data from the target system, you must consider the optimum time to respond

Obtaining Volatile Data Prior to Forensic Duplication

- Volatile data includes:
  - Currently open sockets
  - Running processes
  - Contents of system RAM
  - Location of unlinked files.
- Unlinked files are files marked for deletion when the processes that access them terminate.

Data to Collect

- System date and time
- Users currently logged on
- Time/date stamps for the entire files system
- Currently running processes
- Currently open sockets
- Applications listening on open sockets
- Systems that have current or recent system connections

Sample Data Collection Process

1. Execute trusted shell
2. Record system time and date
3. Determine who is logged on
4. Record modification, creation, and access times of all files
5. Determine open ports
6. List applications associated with open ports
7. Determine running processes
8. List current and recent connections
9. Record the system time
10. Record the steps taken
11. Record cryptographic checksums

Unix File Deletion

- Unix tracks a file’s link count
  - Positive integer represents the number of processes currently using the file
- When link count equals zero, it means that no process is using or needs the file. So it will be deleted.
- When an attacker deletes his rogue program:
  1. Program on the hard drive is removed from the directory chain,
  2. Link count is decremented by one, and
  3. File’s deletion time is set.
- Note, link count does not equal zero until process terminates.

Executing a Trusted Shell

Two Unix modes

1. Console mode
2. Windows (GUI)

- Exit XWindows before you initiate response.
- Log on locally at the victim console to avoid generating network traffic
  - Be sure to log on with root level privileges

Mount trusted device e.g. for a floppy

```
mount /dev/fd0 /mnt/floppy
```

Gathering Info

- Record System Date and Time
  - Date command
- Determine who is logged on
  - Who command

Gather File Info

- Record file modification, access, and Inode change times. For example:

```
ls –alRu / > /floppy/atime
ls –alRc /> /floppy/ctime
ls –alR / > /floppy/mtime
```

Ports and Processes

- Ports

```
netstat –an
```

- Processes

```
netstat –anp
```

- Note, average Unix system has many more processes running than Windows system.
- Processes

```
ps command
```

Checksums

- Record checksums of all recorded files
- Consider scripting initial response

Live Response In Depth

- Use dd, cat, netcat, and des, or crypt cat to obtain log files, configuration files and any other relevant files.
- Rootkits freely available.
  - Most advanced rootkits are loadable kernel modules (LKMs)
- Unix kernel is a single program
- LKMs are programs that can be dynamically linked into the kernel after the system has booted up
  - Rogue LKMs installed by attackers can intercept system commands such as netstat, ifconfig, ps, and ls and create false results
  - Can also hide files and/or process as well as create back doors

Obtaining the System Logs During Live Response

- Most Unix flavors keep their log files in /var/adm or /var/logsubdirectories
- Log files can be obtained with a combination of netcat, cryptcat, dd, and des
- Interesting logs
  - Utmp
  - Wtmp
  - Last log
- Process accounting logs
  - /etc/syslog.comf

Sample Configuration Files

```
/etc/passwd
/etc/shadow
/etc/groups
/etc/hosts
/etc/hosts.equiv
```

More cited in text(see Mandia p.141)

Discovering Illicit Sniffers

- A sniffer can increase an attack’s severity.
- Also indicates attacker had root privileges

Reviewing the /Proc File System

- On many Unix distros, the /proc file system is a pseudo-file system used as an interface to kernel data structures.
  - By changing in to /proc, you are really accessing kernel data structures, rather than a conventional directory.
  - Each process has a subdirectory in /proc the corresponds to its PID.

The Exe Link in the /Proc File System

- The exe link allows investigators to recover deleted files as long as they are still running.
- By examining the fd (file descriptor) subdirectory, you can identify all of the files a process has open.

Dumping System RAM

- Traditionally a challenging process.
- Usually transfer the /proc/kmem file from the target system
- File contains the contents of system RAM in a non-contiguous arrangement.

Questions?