School of Computing
FACULTY OF ENGINEERING & PHYSICAL SCIENCES

UNIVERSITY OF LEEDS

COMP3911 Secure Computing

18: Intrusion Detection & Incident Response

Nick Efford

https://comp3911.info

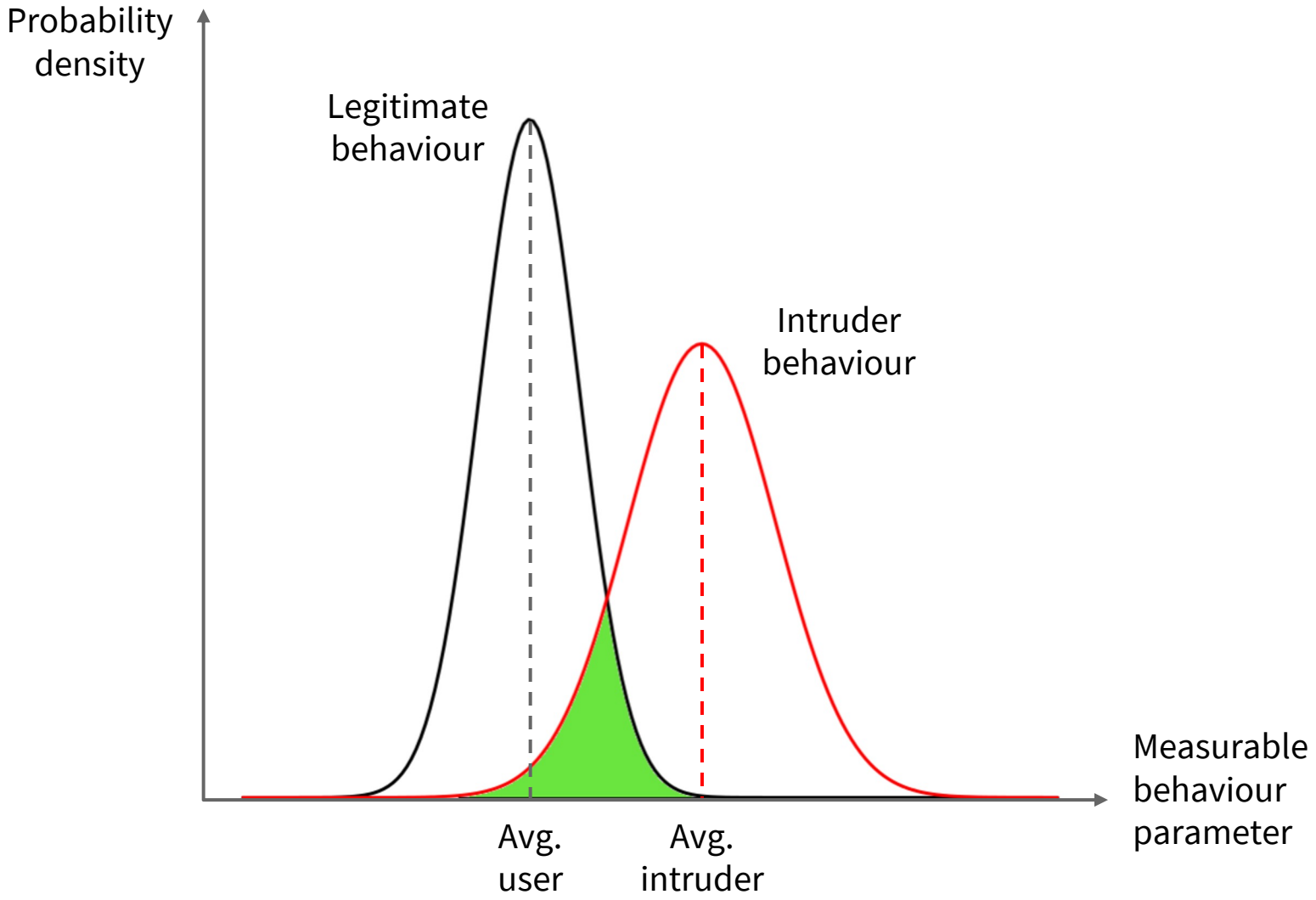
Today's Objectives

UNIVERSITY OF LEEDS

- For you to understand the basic principles of intrusion detection and see examples of how network-based intrusion detection can be done
- For you to appreciate the role of honeypots in detecting intrusion and studying attacker behaviour
- For you to learn two approaches to collecting evidence of attack from a computer system
- For you to see how we analyse a suspicious executable

The Challenge

UNIVERSITY OF LEEDS



Approaches

UNIVERSITY OF LEEDS

- Statistical anomaly detection
  - Develop profiles of each user's activity over time
  - Perform statistical tests to check whether deviation from observed profiles is significant
- Rule-based detection
  - Rules for deviation from previous usage patterns…
  - … or for explicit suspicious behaviour

Network-Based IDS

UNIVERSITY OF LEEDS

These monitor network traffic for suspicious events…

https://www.snort.org

https://zeek.org

Snort

UNIVERSITY OF LEEDS

- Signature-based, cross-platform IDS
- Can sniff packets in real time or operate on previously captured traffic
- Preprocessors for IP defragmentation, TCP stream reassembly, portscan detection…
- Supports a very wide range of rules to identify attacks by their signature
    - New rules can appear within hours of an exploit becoming public knowledge!

Rule Examples

UNIVERSITY OF LEEDS

datagrams from any IP address & any port…

… to subnet 192.168.5…

… on port used by Back Orifice RA Trojan

```
alert udp any any -> 192.168.5.0/24 31337 \
 ( msg: "Back Orifice"; )
```

```
alert tcp any any -> any any \
 ( msg: "Shellcode?"; content "|90 90 90 90|"; )
```

What problem might there be with this example?

TCP stream has four consecutive values of `0x90` (NOP on Intel CPUs)

Hiding a NOP Sled

UNIVERSITY OF LEEDS

```
00000000: 9090                    nop
00000002: 91                      xchg        ecx,eax
00000003: 91                      xchg        ecx,eax
00000004: 9090                    nop
00000006: 91                      xchg        ecx,eax
00000007: 91                      xchg        ecx,eax
00000008: 9090                    nop
0000000A: 91                      xchg        ecx,eax
0000000B: 91                      xchg        ecx,eax
0000000C: 9090                    nop
0000000E: 91                      xchg        ecx,eax
0000000F: 91                      xchg        ecx,eax
00000010: 81E086FFFAF2            and         eax,0F2FAFF86 ;'≥· å'
00000016: B964010000              mov         ecx,000000164 ;'  ☻d'
0000001B: 29CC                    sub         esp,ecx
0000001D: 33D2                    xor         edx,edx
0000001F: 87E7                    xchg        edi,esp
00000021: 89FC                    mov         esp,edi
00000023: 81E0E1A3D9A3            1and        eax,0A3D9A3E1 ;'ú┘úß'
```

Two successive register swaps have no net effect on behaviour, but break up the sequence of 0x90 values found in traditional NOP sleds…

Host-Based IDS

UNIVERSITY OF LEEDS

Example: Tripwire

- Creates and stores secure checksums of critical files (How do you think it does this?)
- Comparison with these checksums allows unexpected changes to be detected
- Only detects impact of intrusion; can't detect attacker's recon probes, for example

Honeypots

UNIVERSITY OF LEEDS

- Security resources whose value lies in being probed, attacked or compromised
- Production honeypots
  - A specialised form of IDS
  - Used for incident response (evidence collection)
- Research honeypots
  - Capture of automated threats – e.g., worms
  - Observation of new tools / techniques
  - Investigation of attacker behaviour

Interaction Level

UNIVERSITY OF LEEDS

Low interaction

- Listen on standard ports
- May give a limited, superficially believable response
- Examples: Specter, Honeyd

High interaction

- Provide or simulate full-blown OS and applications
- Good for learning about attacker behaviour
- High risk: what if attacker breaks free?

Benefits & Drawbacks

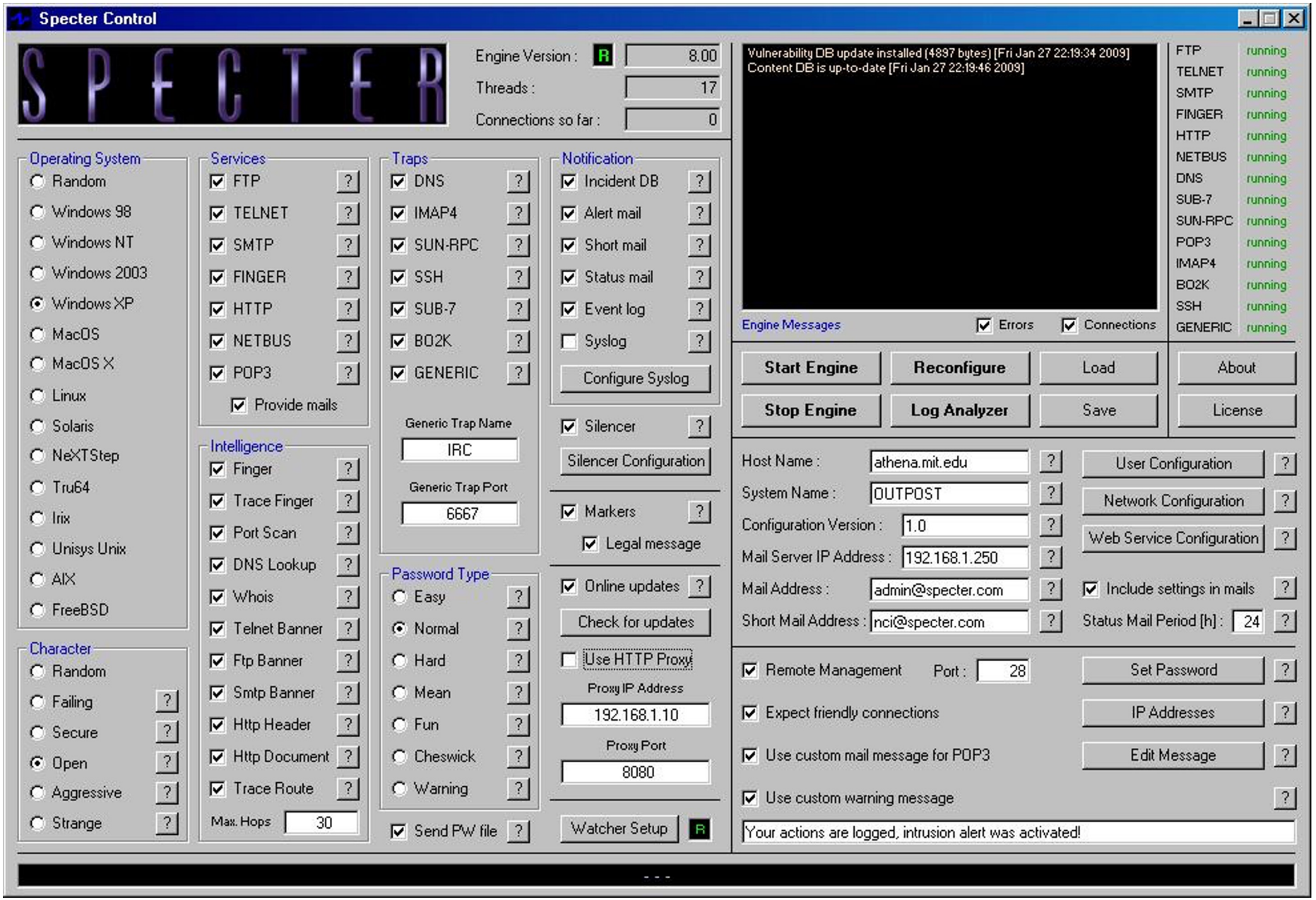
UNIVERSITY OF LEEDS

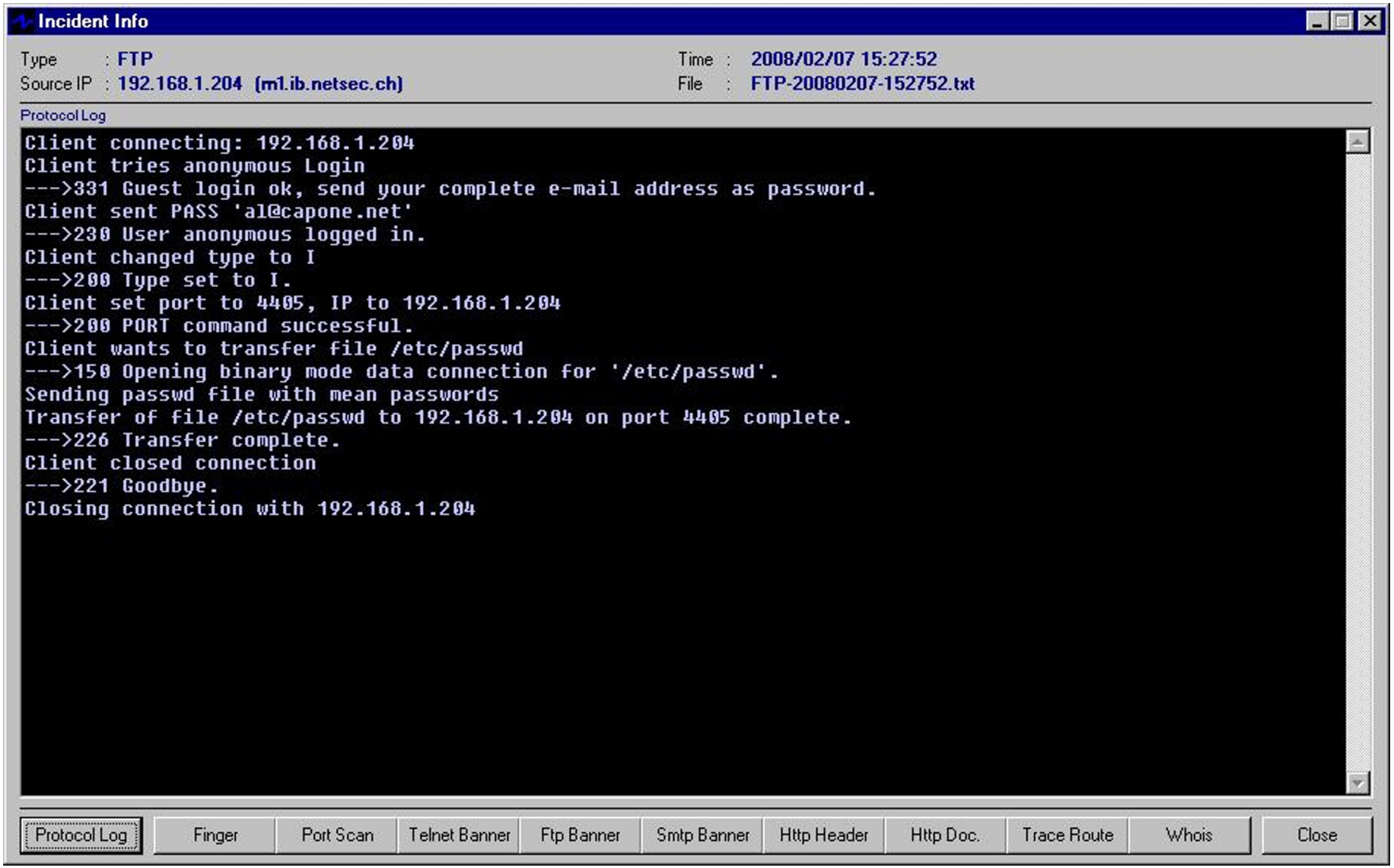
Benefits

- Smaller quantities of higher-quality data, compared with firewall logs or NIDS alerts
- Simple to set up: no special rules, no signature database to maintain, etc

Drawbacks

- Narrow field of view
- Difficulty of accurate simulation
- Risk of honeypot being used to mount attacks


Specter Control
SPECTER
Engine Version : R 8.00
Threads : 17
Connections so far : 0
Vulnerability DB update installed (4897 bytes) [Fri Jan 27 22:19:34 2009]
Content DB is up-to-date [Fri Jan 27 22:19:46 2009]
FTP running
TELNET running
SMTP running
FINGER running
HTTP running
NETBUS running
DNS running
SUB-7 running
SUN-RPC running
POP3 running
IMAP4 running
BO2K running
SSH running
GENERIC running
Engine Messages
Errors
Connections
Operating System
Random
Windows 98
Windows NT
Windows 2003
Windows XP
MacOS
MacOS X
Linux
Solaris
NeXTStep
Tru64
Irix
Unisys Unix
AIX
FreeBSD
Character
Random
Failing
Secure
Open
Aggressive
Strange
Services
FTP
TELNET
SMTP
FINGER
HTTP
NETBUS
POP3
Provide mails
Intelligence
Finger
Trace Finger
Port Scan
DNS Lookup
Whois
Telnet Banner
Ftp Banner
Smtp Banner
Http Header
Http Document
Trace Route
Max. Hops 30
Traps
DNS
IMAP4
SUN-RPC
SSH
SUB-7
BO2K
GENERIC
Generic Trap Name
IRC
Generic Trap Port
6667
Password Type
Easy
Normal
Hard
Mean
Fun
Cheswick
Warning
Send PW file
Notification
Incident DB
Alert mail
Short mail
Status mail
Event log
Syslog
Configure Syslog
Silencer
Silencer Configuration
Markers
Legal message
Online updates
Check for updates
Use HTTP Proxy
Proxy IP Address
192.168.1.10
Proxy Port
8080
Watcher Setup R
Start Engine
Reconfigure
Load
About
Stop Engine
Log Analyzer
Save
License
Host Name : athena.mit.edu
System Name : OUTPOST
Configuration Version : 1.0
Mail Server IP Address : 192.168.1.250
Mail Address : admin@specter.com
Short Mail Address : nci@specter.com
User Configuration
Network Configuration
Web Service Configuration
Include settings in mails
Status Mail Period [h] : 24
Remote Management Port : 28
Set Password
Expect friendly connections
IP Addresses
Use custom mail message for POP3
Edit Message
Use custom warning message
Your actions are logged, intrusion alert was activated!


Incident Info
Type : FTP
Source IP : 192.168.1.204 (m1.ib.netsec.ch)
Time : 2008/02/07 15:27:52
File : FTP-20080207-152752.txt
Protocol Log
Client connecting: 192.168.1.204
Client tries anonymous Login
--->331 Guest login ok, send your complete e-mail address as password.
Client sent PASS 'al@capone.net'
--->230 User anonymous logged in.
Client changed type to I
--->200 Type set to I.
Client set port to 4405, IP to 192.168.1.204
--->200 PORT command successful.
Client wants to transfer file /etc/passwd
--->150 Opening binary mode data connection for '/etc/passwd'.
Sending passwd file with mean passwords
Transfer of file /etc/passwd to 192.168.1.204 on port 4405 complete.
--->226 Transfer complete.
Client closed connection
--->221 Goodbye.
Closing connection with 192.168.1.204
Protocol Log
Finger
Port Scan
Telnet Banner
Ftp Banner
Smtp Banner
Http Header
Http Doc.
Trace Route
Whois
Close

Incident Response

UNIVERSITY OF LEEDS

- Penetrated systems are subject to **forensic analysis**
- Goals are to
  - Discover how attackers gained access
  - Deduce what they were able to do on the system
  - Possibly gather evidence of criminal activity that is solid enough to use for prosecutions

Approaches

UNIVERSITY OF LEEDS

- Post-mortem analysis
  - Non-volatile data
- Live response
  - Volatile data
  - Non-volatile data
- Network-based evidence collection

Post-Mortem Analysis Steps

UNIVERSITY OF LEEDS

1. Forensic duplication
2. Recovery of deleted files
3. Collection of MACtimes and hashes
4. Removal of known files
5. Identification of files by signature
6. Reverse engineering of unknown executables
7. Reconstruction of activity (email, browsing, etc)

Forensic Duplication

UNIVERSITY OF LEEDS

Common to remove evidence drives in order to duplicate them

Why do we use dedicated connectors when duplicating? Why not plug the evidence drives directly into the forensic PC?

Connectors allow hot-swapping and, more importantly, provide **hardware-based write blocking**

Recovery of ‘Deleted’ Data

UNIVERSITY OF LEEDS

- For most OS, deletion merely breaks link between file metadata and disk blocks holding file contents
  - … and marks those blocks as unused
- So **data persists on disk** until those blocks are reused!
  - Persistence times depend upon number of free blocks available and level of system activity
  - Farmer & Venema found that ‘data half-life’ varied between 12 and 35 days for small servers

File MACtimes

UNIVERSITY OF LEEDS

- UNIX-like filesystems define three file timestamps:
  - Last modification time (`mtime`)
  - Last access time (`atime`)
  - Time of last status change (`ctime`)
- Equivalents exist in other OS (Windows NTFS, etc)
- MACtimes provide useful evidence of system activity…
- … which can be easily lost by reboots, system backup, etc!

Computation of File Hashes

UNIVERSITY OF LEEDS

- Do it for
  - Entire duplicated disk partition
  - Individual files recovered from that partition
- UNIX-based systems offer multiple command line tools that can be used for this, e.g.:

```
shasum -a 256 foo.txt
```

- But why do we need this?

Removal of Known Files

UNIVERSITY OF LEEDS

- Typical disk may have on the order of 10^5 files, only a few of which will be interesting to us
- Hash databases for OS programs, standard system files and common apps can be used to ‘narrow the field’
  - Example: NIST National Software Reference Library

Static Analysis of Executables

UNIVERSITY OF LEEDS

- Extract text strings
- Perform a hex dump
- View symbol information
- View shared objects (DLLs)
- Examine binary file format
- Disassemble code

Dynamic Analysis of Executables

UNIVERSITY OF LEEDS

- Use VMware or similar virtualisation software to run the unknown executable in a secure sandbox
- Trace system/library calls
- Step through the code in a debugger

Live Response: Volatile Data

UNIVERSITY OF LEEDS

- System date & time
- Running processes, process memory dumps
- Running services (Windows)
- Loaded kernel modules (Linux)
- Scheduled jobs
- Network connections & open ports
- Executables that have opened ports
- Opened files
- Users currently logged on

Live Response: Approach

UNIVERSITY OF LEEDS

- Must adhere to the **Order Of Volatility Principle** – capture most volatile data first, least volatile last
- Evidence collection tools must be trustworthy and self-contained
- Typical approach is to run the tools directly from a CD containing executables & libraries
- Data can be transferred from victim to forensic workstation via the network, using `netcat`
  - Hash of any captured evidence should be computed immediately

Summary

UNIVERSITY OF LEEDS

We have

- Considered some of the principles behind automated intrusion detection
- Explored the use of network-based and host-based IDS
- Discussed how to conduct a post-mortem analysis of an attacked computer system
- Investigated an example of a suspicious executable

Follow-Up / Further Reading

UNIVERSITY OF LEEDS

- Chapters 5 & 16 of *Thinking Security*
- Provos, *Virtual Honeypots*, Addison-Wesley 2007
- Farmer & Venema, *Forensic Discovery*, Addison-Wesley, 2005