Logs and Redirection



Module

2,

Lesson

8:

# 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

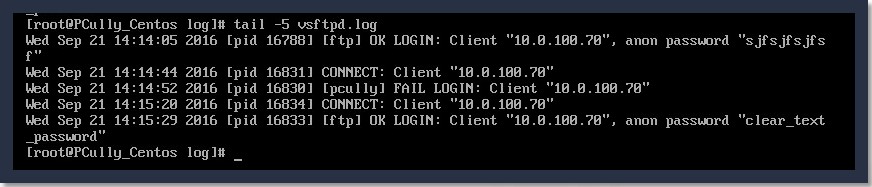
UNIX System Log Files

Logs can be modified/wiped easily

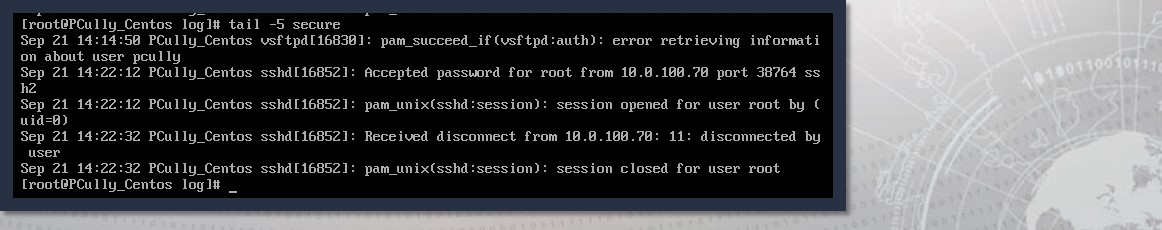
|  |  |  |
| --- | --- | --- |
| Easy to Modify/Wipe Logs |  | Syslog |
|  | Configurable logging service  Configured via /etc/rsyslog . conf  (Solaris)  Configured via / etc/ sys log . conf (Linux) |
|  | | | |
| The syslog service can be configured to first write to the local system, after logs are 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



/var/log/secure



# 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 |  | | 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 |  | Debug | |
|  | Used by developers to troubleshoot issues with programs | |

# Policy Assessment Overview

* There are three types of logs:



* Examples of event log entries:

|  |  |  |
| --- | --- | --- |
| System/Application |  |  |
|  | 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

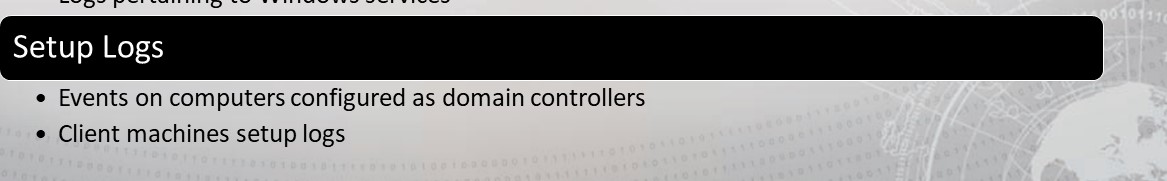
XML

|  |  |
| --- | --- |
|  |  |
| 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



### 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

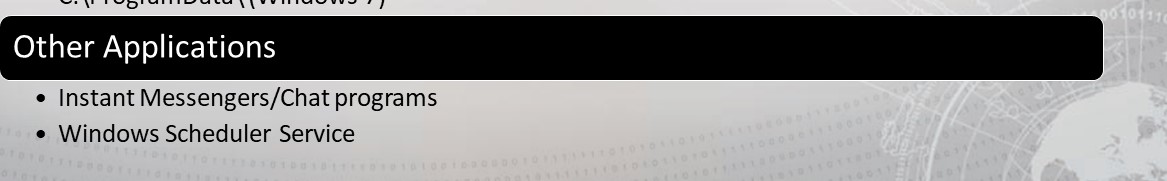
Web Servers

* /var/log/httpd/



|  |
| --- |
| 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)

## 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

# 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

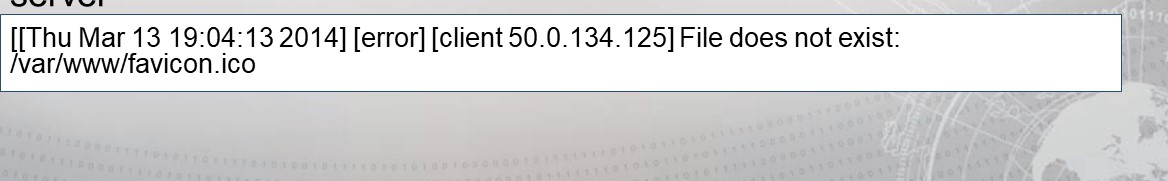
* Apache
* Web Proxy servers are used as an intermediary between a web browser and the internet
* Events are logged in local time but this is configurable
* All server log files should be reviewed

## Apache Web Server Logs

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

|  |
| --- |
| 10.185.248.71    +0000 808840 "GET  [inventoryService/inventory/purchaseItem?user d=20253471 &itemld=23434300 HTTP/I . 1 " 500 17 "Apache-HttpClient/4.2.6 (java 1.5)" |

Error logs — contains information about errors encountered by the server



### Apache Web Server logs location

Debian/Ubuntu/LinuxMint

|  |  |
| --- | --- |
| Config File | Path Value |

Directive/Setting

|  |  |  |
| --- | --- | --- |
| \*SUFFIX | /etc/apache2/envvars | (see configfile for conditional logic) |
| LOG DIR | /etc/apache2/envvars | exportAPACHE LOG DIR=/var/10g/apache2SSUFFIX |
| AccessLog | /etc/apache2/sites-available/OOO-default.conf | CustomLog S{APACHE LOG DIR}/access.log combined |

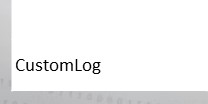
ErrorLog /etc/apache2/apache2.conf ErrorLogS{APACHE LOG DIR}/error.10g

LogLevel /etc/apache2/apache2.conf warn

LogFormat "%v:%p %h %u %t "%r" %O "%{Referer}i"

"%{User-Agent}i"" vhost\_combinedLogFormat "%h %l %u %t "%r"

LogFormat /etc/apache2/apache2.conf %O "%{Referer}i" "%{User-Agent}i"" combinedLogFormat "%h

%l %u %t "%r" %O" commonLogFormat refererL ogFormat "%{User-agent}i" agent

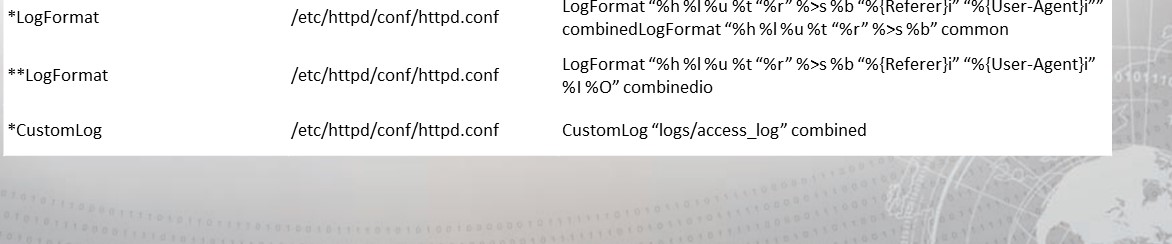
/etc/apache2/conf-available/other-vhosts-access- CustomLog S{APACHE LOG DIR}/other\_vhosts\_access.log log.conf vhost combined.

### Apache Web Server logs location

Red Hat/Fedora/CentOS

DirectiveConfig FilePath/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

"%h

"%{Referer}i"

"%{User-Agent}i""

## Apache WebServer logs location

OpenSUSE

|  |  |  |
| --- | --- | --- |
| Directive | Config File | Path/Value |

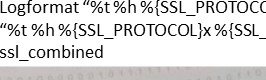
|  |  |  |
| --- | --- | --- |
| AccessLog | /etc/apache2/sysconfig.d/global.conf | /var/log/apache2/access\_log |
| ErrorLog | /etc/apache2/httpd.conf | /var/log/apache2/error\_log |
| LogLevel | /etc/apache2/sysconfig.d/global.conf | warn |

LogFormat "%h 0/01 %u %t "%r" %b" commonLogFormat "%v %h 0/01 %u %t "%r"

%b" vhost\_commonLogFormat "%{Referer}i -> %U" refererLogFormat "%{User-agent}i"

\*LogFormat /etc/apache2/mod\_log config.conf agentLogFormat "%h 0/01 %u %t "%r" %b "%{Referer}i" "%{User-Agent}i"" combinedLogFormat "%v %h 0/01 %u %t "%r" %b "%{Referer}i" "%{User-Agent}i"" vhost combined

\*\*LogFormat /etc/apache2/mod\_log config.conf LogFormat "%h 0/01 %u %t "%r" %b "%{Referer}i" "%{User-Agent}i" % I

%{SSL PROTOCOL}x%{SSL CIPHER}x "%r" %b" ssl\_commonLogformat

\*\*\*LogFormat /etc/apache2/mod\_log config.confCIPHER}x "%r"

### 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



|  |  |  |  |
| --- | --- | --- | --- |
|  |  | cs-uri-ste | sc-status |

cs-version

|  |  |  |  |
| --- | --- | --- | --- |
|  | 172.16.255 25 GE | [default.ht | 200 |

HTTP/I.O



### Windows Webserver IIS Logs

Microsoft IIS Logging Formats

#### • IIS Log File Format

|  |  |
| --- | --- |
| 192.168.114.201 , 03/20/01 ,  3223, 200, O, GET, /DeptLogo.gif, - | W3SVC2, SALESI, 172.21.13.45, 4502, 163, |

172.16.255.255, anonymous, 03/20/01 , 23:58: 1 1 , MSFTPSVC, SALES 1 ,

172.16.255.255, 60, 275, o, o, 0, PASS, /lntro.htm, -,



### Windows Webserver IIS Logs

Microsoft IIS Logging Formats

#### • NCSA Common Log File Format

|  |
| --- |
| 172.21 13.45- Microsoft\fred [08/Apr/2001 "GET  /scripts/iisadmin/ism-dll?http/serv HTTP/I -0" 200 3401 |

• ODBC Logging



# Logon Events

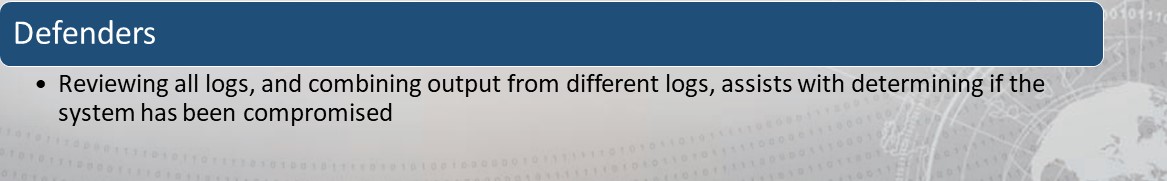
* These events are essential to establish a pattern of logon times for a user
* These events are used to flag a logon at an unusual hour or day
* Failed logon events may be evidence of brute force or password guessing attacks
* Not all accesses result in a logon event (e.g., FTP does not produce a logon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



## Log Cleaning

Look for logs that changed since your arrival:

• Antivirus, Firewall, Dr. Watson (pre-Vista), Problem Reports and Solutions



(Vista+),

and

Application

logs

Windows find Command

rbot@nick-kalil:

> run multicorm-aand —c I / c find

Running Corm-aand L isc running corm-aand / c find / 7

Output of / c find /

Searches for text string in file or files.

FIND [/OFF[LINE] ] ivæ : ] [pach] fileneme [

Displays all lines NOT containing the specified string. Displays only the count of 1 ines containing the string.

Displays 1 ine numbers with the displayed 1 ines.

Ignores the case of characters when searching for the string. / OFF [LINE] Do nac skip files with offline attribute " string" Specifies the text string Co find.

[dr ivæ:] [path] f i læname

Specifies file or files Co search.

If pach is not specified. F IND searches the text typed at c prompt or piped from another corm-aand.

rcecer:præcer > run multicorm-aand —cl "crad / c find . 1 6B . 1 . firer,rall .

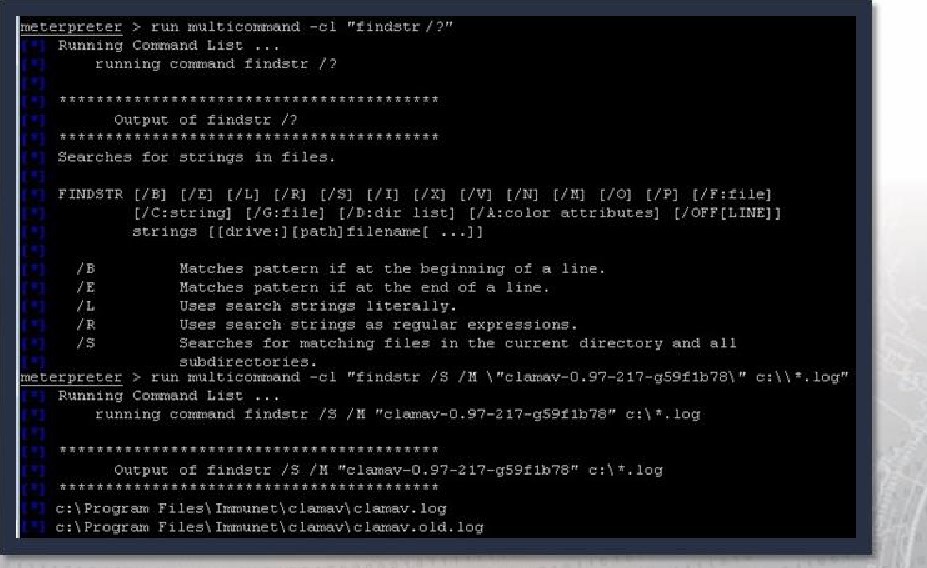
Running Corm-aand L isc running corm-aand / c find . 16B. 1. firer,rall . log

Output of / c find firer,rall . log

### Windows findstr Command

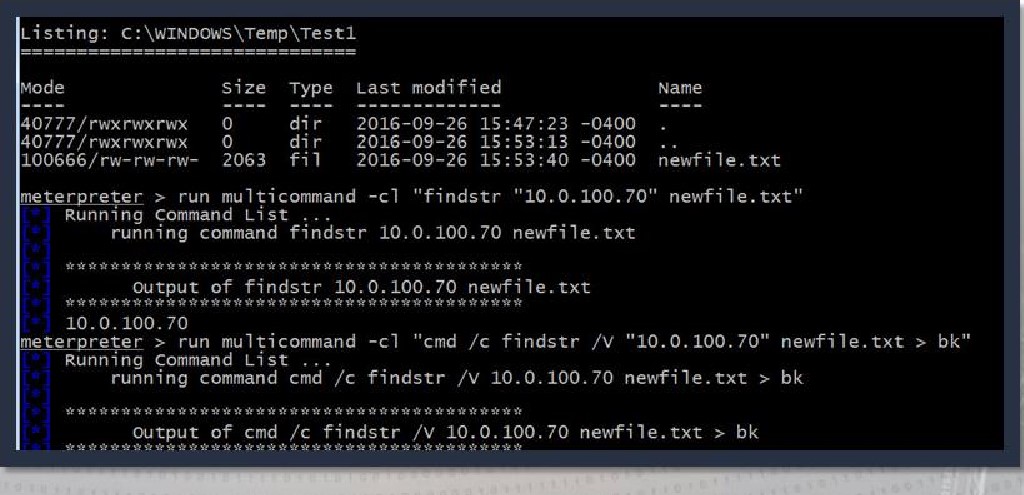
For redirection, provide a shell:

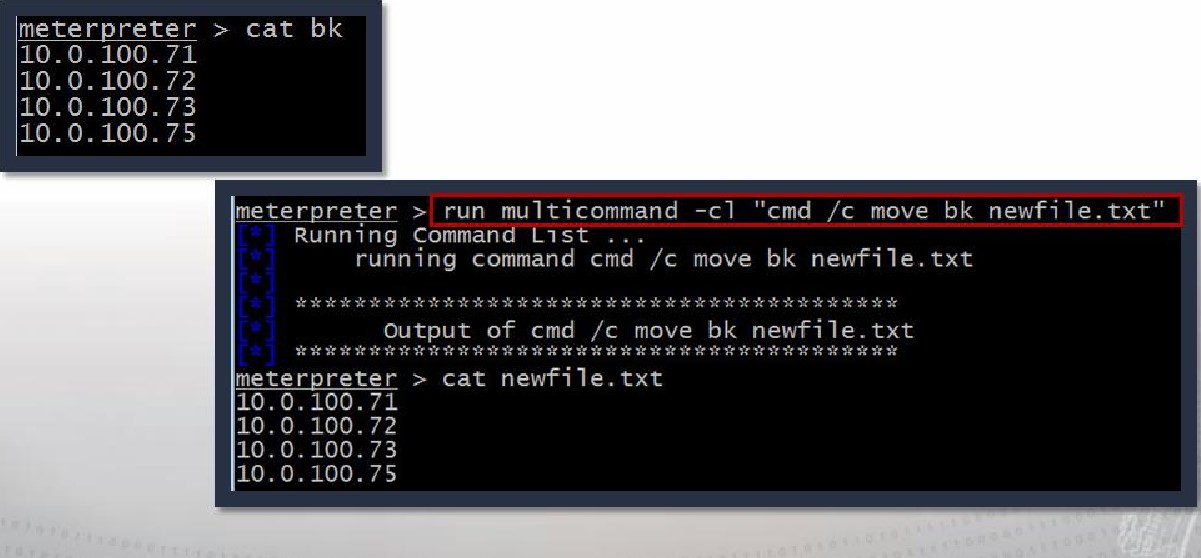
run multi command —cl 'A crnd / c findstr "string" > newfile . txt



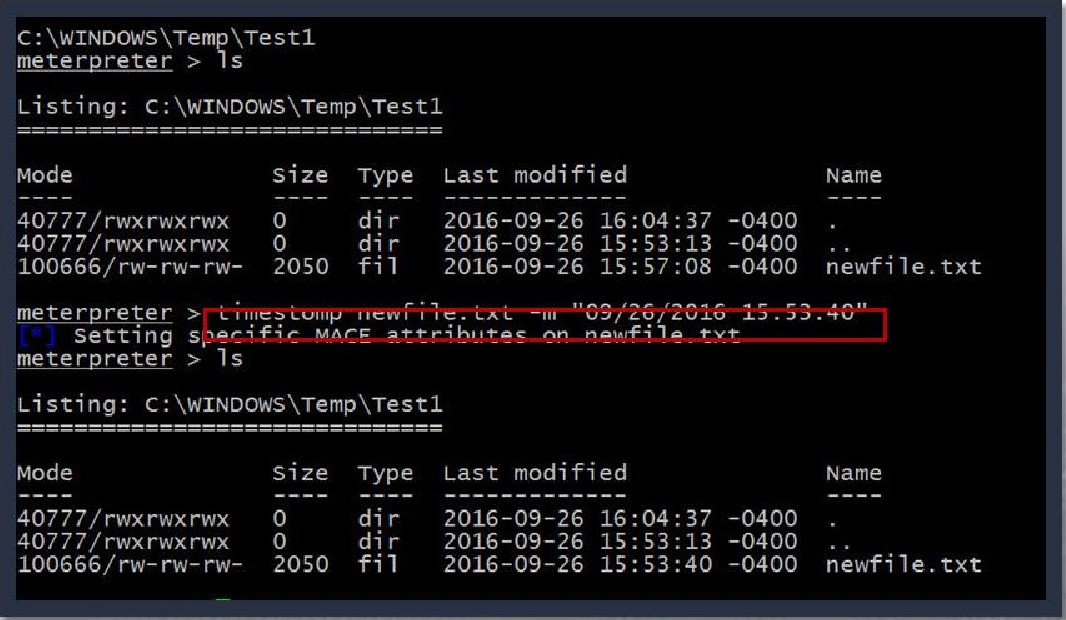
#### Windows findstr Command

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



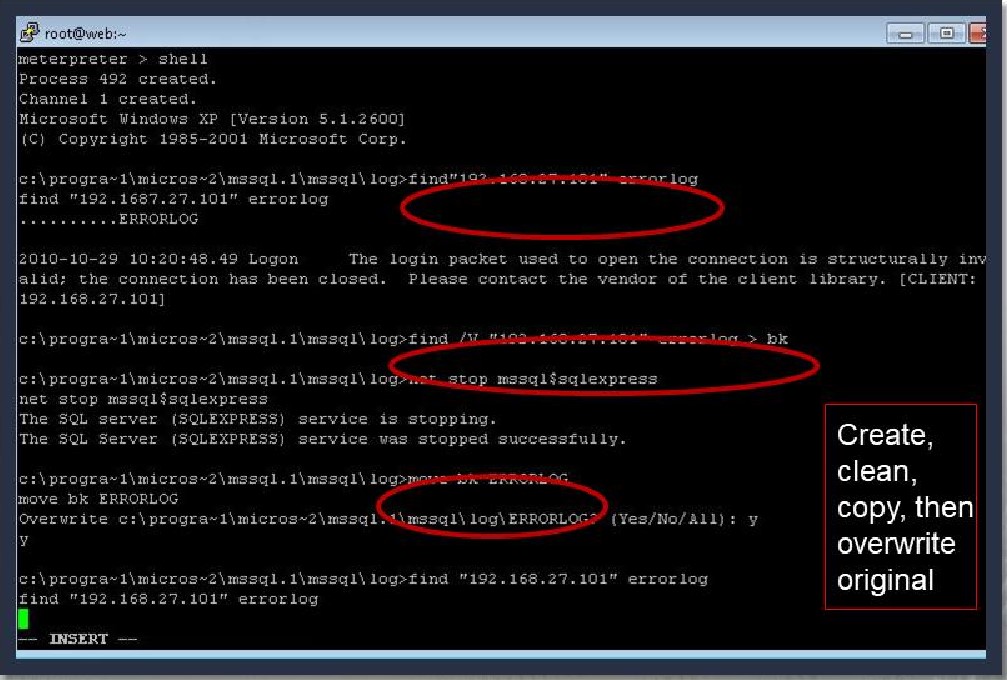
Windows findstr Command

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

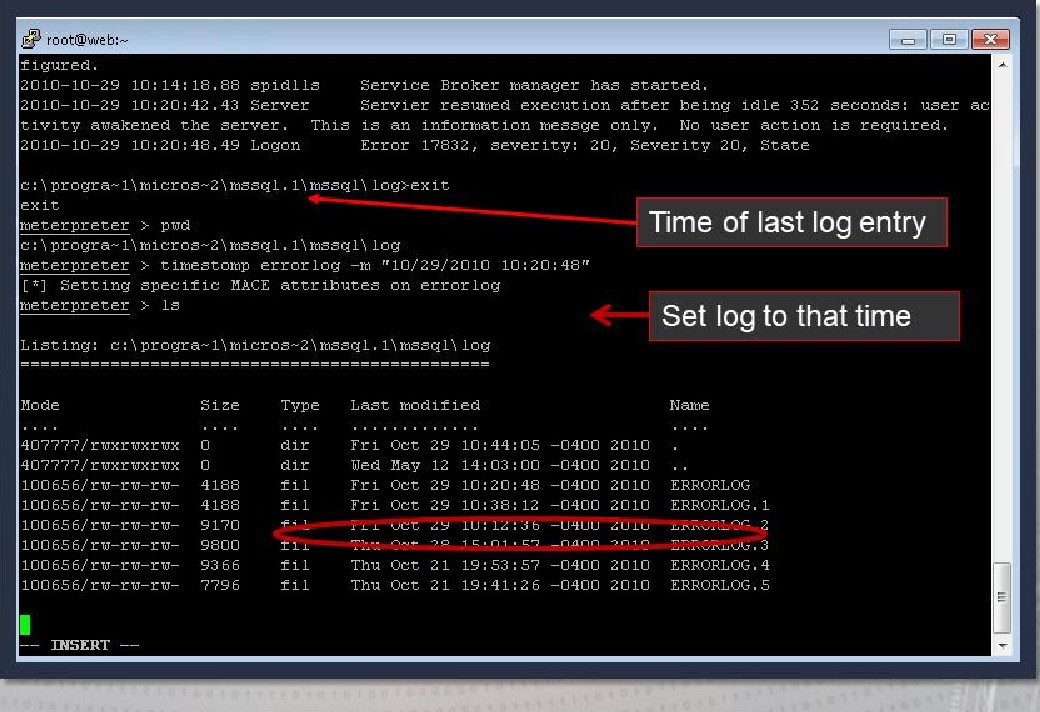
Windows timestamp Command

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

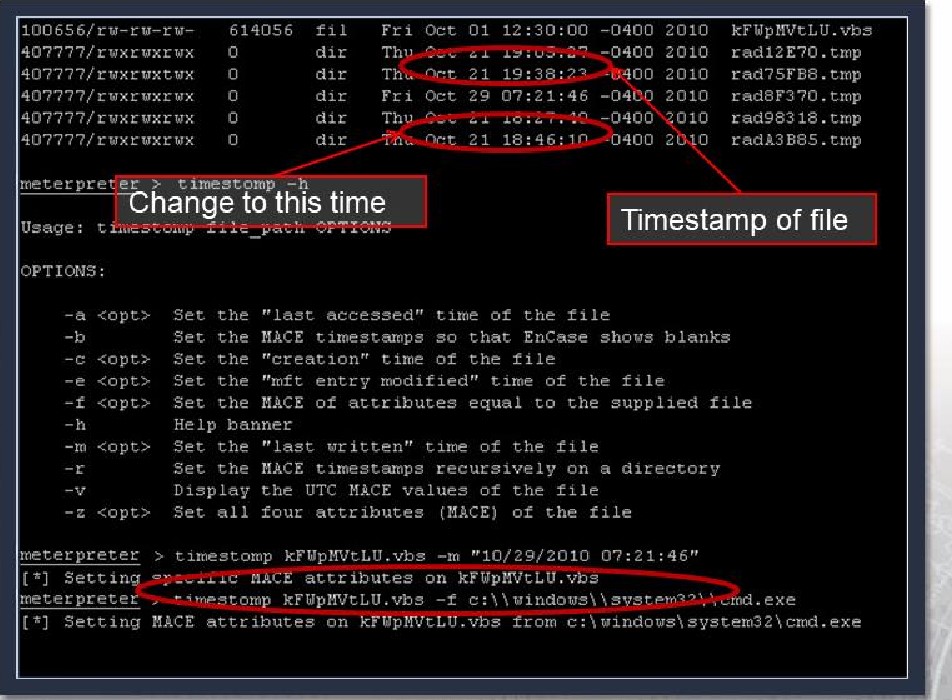
## Cleaning Logs: Always Use Multicommand Script

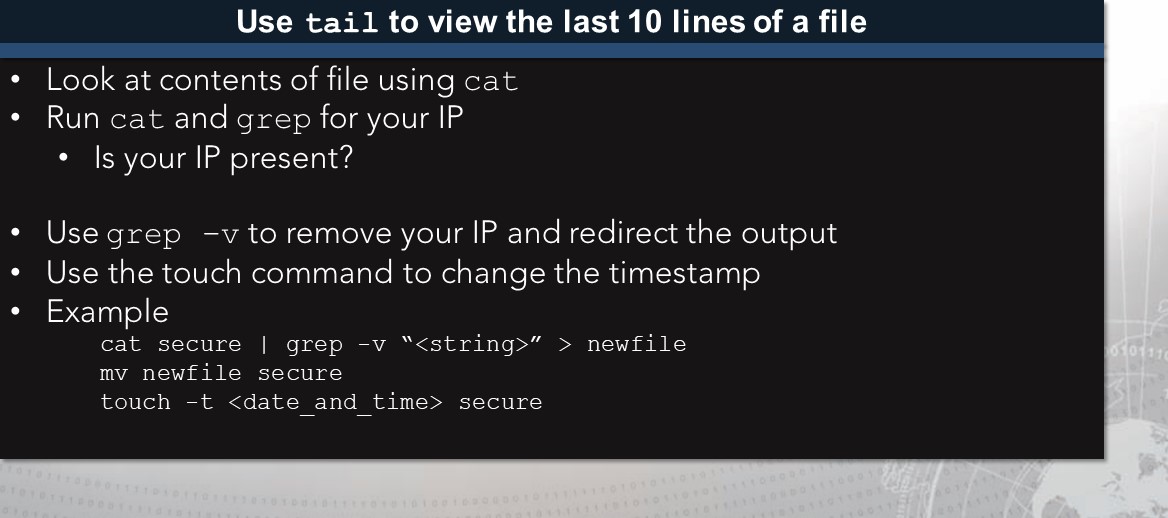


## Cleaning Logs: Always Use Multicommand Script



Windows Modify File Timestamp With timestomp



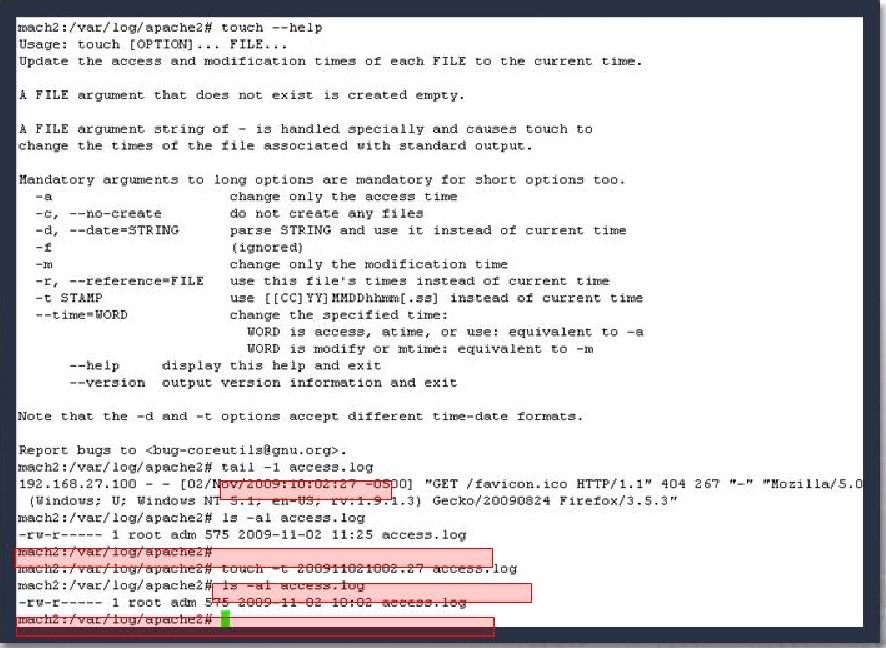


UNIX

Log

Cleaning

UNIX: Modify File Timestamp with touch Command

tetaeh ——help touch ,

Update the access and Of each FILE to the current Cire.

argument that does not ex created empty

A PILE it handled and touch to c hange the  oi the tile associated vich scandard outpuc.

"landaeory arguments to long options are mandatory for short options too.

gban•ge only

-—no—eeeaee do ereate any les parse STRING and use it instead of curcent

( ignore 4) change only the modification t

——reference•F use this Instead Of current t

[CC] current --time-WORD change the speci f fed time:

VORP —4

VORb is OK' —m this and

——verzion output version and e\*ie

Note t nat the —c accept dltferent formats.

Report bug-g co .

—i aeee•e. Log

192.16B.2Q, 100 - - 0] "GET 404 267

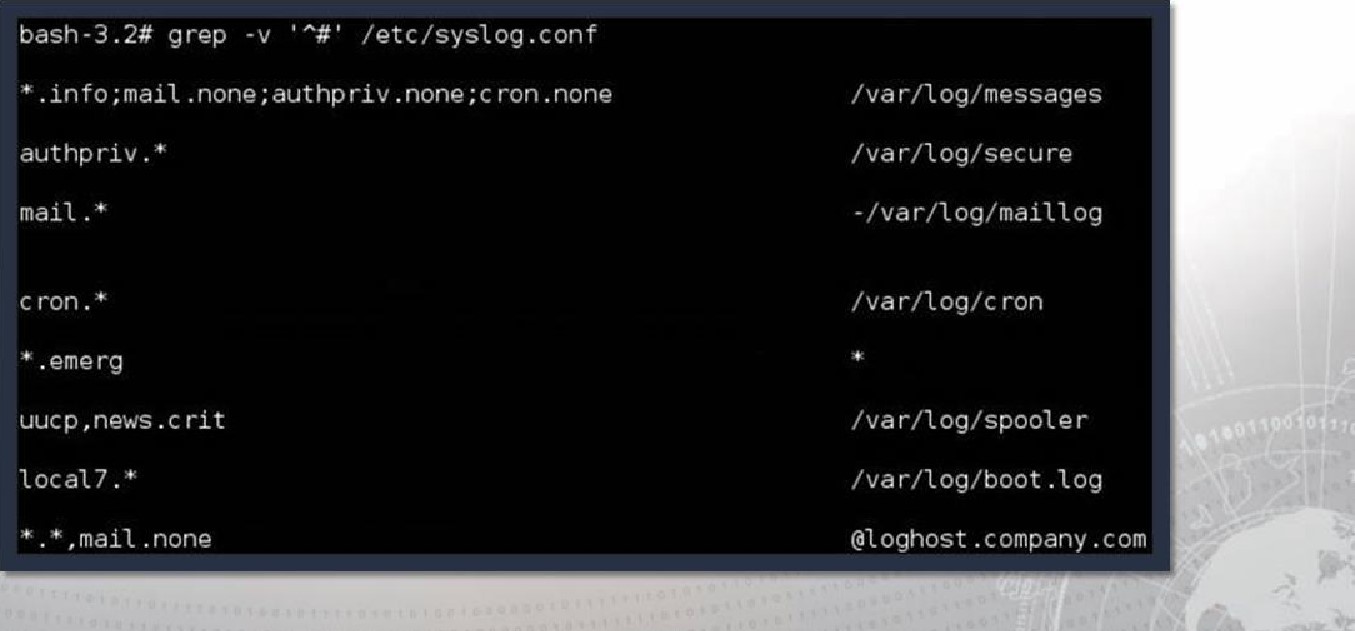
'j; gandous Gecko/20ö90624 Firefox/3 . 5.30

-rv-r———-— root 575 11:25 access. log

### Syslog

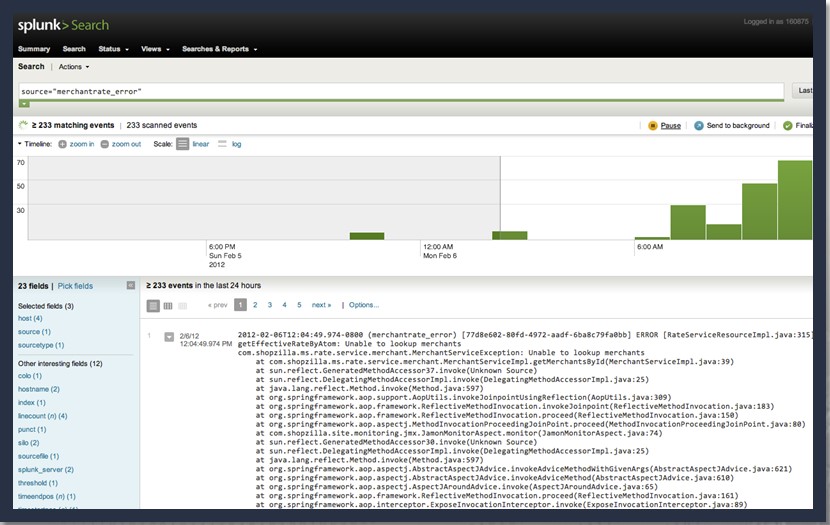
* Standard protocol for forwarding log messages to a central host
* Sent in clear text:
* Uses UDP/514 by default
* Small (less than 1 KB) text messages
* Not native in Windows
* UNIX: Setting in / etc/syslog . conf file:
* Look for /oghost setting
* Check for entry with remote IP address

### Syslog Configuration File



I

### Centralized Log Management



### Redirection

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

|  |  |
| --- | --- |
|  | Tunneling |
| A forward tunnel to deliver the exploit  • A reverse tunnel for the callback |

#### Redirection

Adds obfuscation into the

connection

• Reduces the risk of detection by

the target 

### Redirection via SSH Tunnels

root@172.16 .35.153 's password :

Linux AttackBox 3.12-kaU1-amd64 #1 SMP Debian 3.12.6-2ka1i1 (2014-01-06) x86 64

The programs included with the Kali GNU/Linux system are free software; the exact dist ribution 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 2014 from 172.16.35.153 root@AttackBox

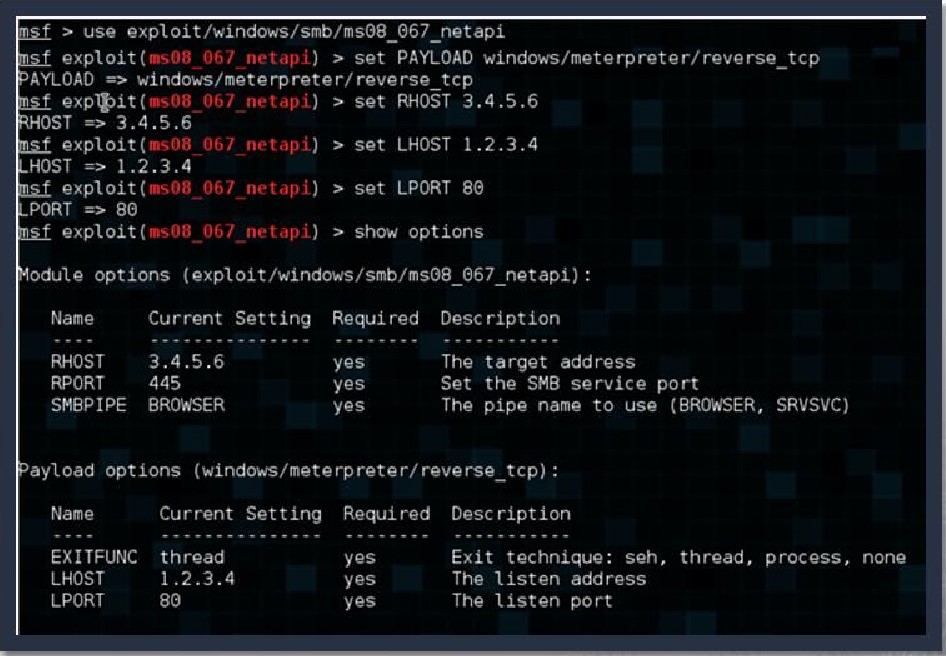
|  |
| --- |
| RHOST |

### SSH Tunnel and Meterpreter Options

|  |  |  |
| --- | --- | --- |
| |  | | --- | | SSH as root to the jump point and jump point is  LHOST | |  |
| |  |  | | --- | --- | |  |  | | ssh root @ 2.3.4.5 | | |

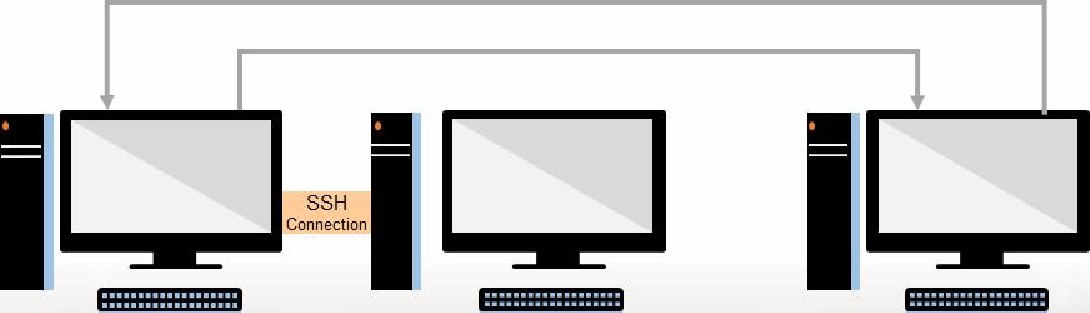


# Example 1 : Preparing the Payload



|  |  |  |
| --- | --- | --- |
|  | DP: 445  SP: 4444 | Data |

## Example 1 : Bad Tradecraft



Attacker Jump Point Target

1 .2.3.4 2.3.4.5 3.4.5.6

IP Header TCP Header

## Redirection Tunnel Example

root@172.16.35.1531s password :

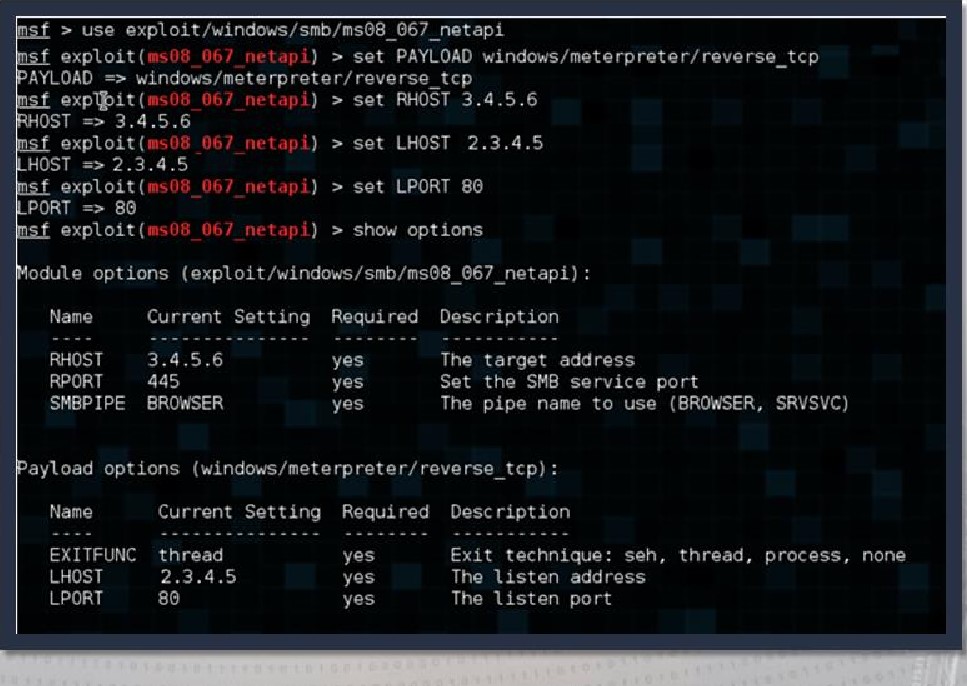
Linux AttackBox 3.12-ka1i1-amd64 SMP Debian 3.12.6-2ka1i1 (2014-01-06) x86 64

The programs included with the Kali GNU/Linux system are free software; .the exact dist ribution terms for each program are desc ribed 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 2014 from 172, 16.35.153 root@AttackBox :

### Bad Tradecraft Example 2



|  |  |  |
| --- | --- | --- |
| s: 1 .2.3.4  D: 3.4.5.6 |  | Data |

Bad Tradecraft Example 2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  | | | | | | |  | |  | | SSH  Connection |  |  |  |  |  | | |  | | |

Attacker Jump Point Target

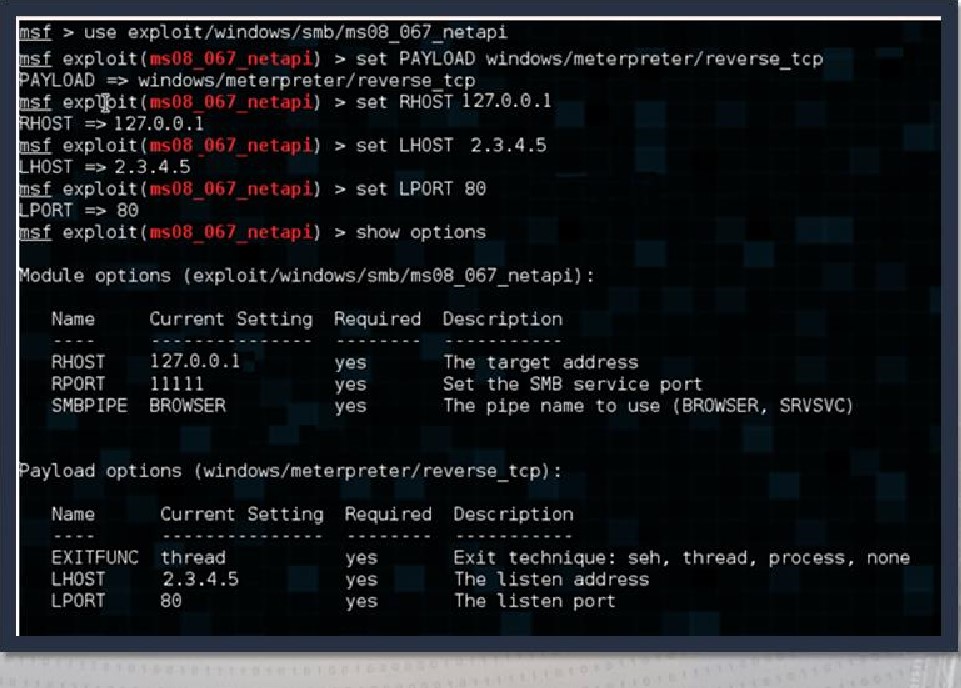
1 .2.3.4 2.3.4.5 3.4.5.6

IP Header TCP Header

## Redirection Tunnel Example



### Good Tradecraft Example



Good Tradecraft Example



Attacker Jump Point Target

1 .2.3.4 2.3.4.5 3.4 5-6

IP Header TCP Header

### Initial SSH Tunnel With Jump Point

Meterpreter Jump Point

1.2.3.4 10.20.30.40



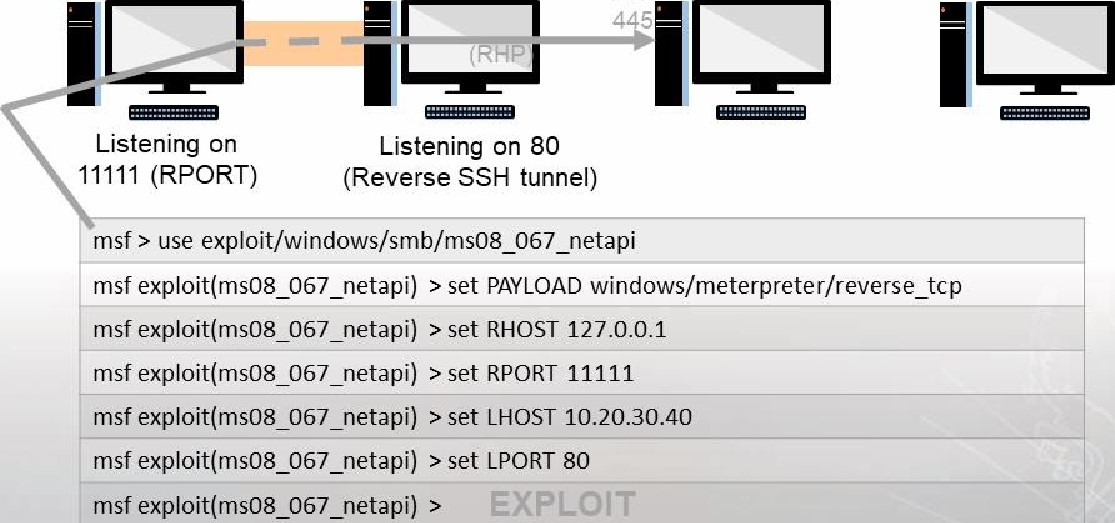
Listening on Listening on

Target 1 Target 2

20.30.40.50 30.40.50.60



### Outbound Trigger: Target 1



port

1.2.3.4

10.20.30.40

20.30.40.50

30.40.50.60

Meterpreter

Jump

Point

Target

1

Target

2



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



## Connection and Callback

Meterpreter Jump Point Target 1 Target 2

1.2.3.4 1 0.20.30.40 20.30.40.50 30.40.50.60

|  |  |  |
| --- | --- | --- |
| meterpreter> |  | 10.20.30.40 on 80 |
| Listening on 80 | Connection | (LPORT) |

Triggered to call back to



Callback

CONNECTED on 80



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



Sec. 4.4

## 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

|  |  |
| --- | --- |
| Server |  |

Note:

|  |  |
| --- | --- |
| Kali | 10.10. l.se |
| CentOS7 | 10.10.1.40 |
| Windows 12 | 10.10.1.1€ |

### 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:

|  |  |
| --- | --- |
| 1. Callback 2. Listener | 1. Payload 2. Exploit |

* List the benefits and drawbacks of:

a. listeners b callback implants

* 1. non-persistent implants
  2. 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: destination   * SO lNCe * ephemeral  local | And their possible states: open  • closed  . mode  established |

* To exploit a vulnerable service, themust 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 |