

NAME:

HASNAIN TAHIR

ROLL NUMBER:

231-450367

COURSE:

COMP421

SECTION:

B

ASSIGNMENT:

1

Nmap -v -sV

The screenshot shows a web browser window titled "TryHackMe | Metasploit: Introduction". The browser's address bar shows "tryhackme.com". The main content of the browser is a terminal window titled "Metasploit Unleashed | Port Scanning | OffSec". The terminal window has two tabs: "AppSpider" and "Metasploit Unleashed | Port Scanning | OffSec". The tab title is "Metasploit Unleashed | Port Scanning | OffSec". The terminal window displays the following text:

```
msf6 > msf
[!] Unknown command: msf
msf6 > nmap -v -sV 192.168.1.0/24 -oA subnet_1
[*] exec: nmap -v -sV 192.168.1.0/24 -oA subnet_1

Starting Nmap 7.60 ( https://nmap.org ) at 2024-01-24 00:53 GMT
NSE: Loaded 42 scripts for scanning.
Initiating Ping Scan at 00:53
Scanning 256 hosts [4 ports/host]
Stats: 0:00:13 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 6.35% done; ETC: 00:56 (0:03:12 remaining)
Ping Scan Timing: About 21.09% done; ETC: 00:56 (0:02:41 remaining)
Ping Scan Timing: About 35.69% done; ETC: 00:56 (0:02:12 remaining)
Ping Scan Timing: About 50.39% done; ETC: 00:56 (0:01:41 remaining)
Ping Scan Timing: About 64.99% done; ETC: 00:56 (0:01:12 remaining)
Ping Scan Timing: About 79.64% done; ETC: 00:56 (0:00:42 remaining)
```

Below the terminal window, the status bar shows "THM AttackBox" and "53m 33s".

On the left side of the browser window, there is a sidebar with a tree view showing directory structures for "xb4" and "x86". The "x86" section shows "10 directories, 0 files".

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

Terminal window content:

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2
evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_Regasm_Regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpaderpinglevel.rb
    ├── syscall_inject.rb
    └── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2
evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_Regasm_Regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpadeping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2
evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_Regasm_Regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpadeping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

```
msf6 > msf
[-] Unknown command: msf
msf6 > nmap -v -sV 192.168.1.0/24 -oA subnet_1
[*] exec: nmap -v -sV 192.168.1.0/24 -oA subnet_1

Starting Nmap 7.60 ( https://nmap.org ) at 2024-01-24 00:53 GMT
NSE: Loaded 42 scripts for scanning.
Initiating Ping Scan at 00:53
Scanning 256 hosts [4 ports/host]
Stats: 0:00:13 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 6.35% done; ETC: 00:56 (0:03:12 remaining)
Ping Scan Timing: About 21.09% done; ETC: 00:56 (0:02:41 remaining)
Ping Scan Timing: About 35.69% done; ETC: 00:56 (0:02:12 remaining)
Ping Scan Timing: About 50.39% done; ETC: 00:56 (0:01:41 remaining)
Ping Scan Timing: About 64.99% done; ETC: 00:56 (0:01:12 remaining)
Ping Scan Timing: About 79.64% done; ETC: 00:56 (0:00:31 remaining)

msf6 >
```

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2
evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_Regasm_Regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpadeping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2
evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_Regasm_Regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpadeping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

```
msf6 > msf
[-] Unknown command: msf
msf6 > nmap -v -sV 192.168.1.0/24 -oA subnet_1
[*] exec: nmap -v -sV 192.168.1.0/24 -oA subnet_1

Nmap scan report for 192.168.1.236 [host down]
Nmap scan report for 192.168.1.237 [host down]
Nmap scan report for 192.168.1.238 [host down]
Nmap scan report for 192.168.1.239 [host down]
Nmap scan report for 192.168.1.240 [host down]
Nmap scan report for 192.168.1.241 [host down]
Nmap scan report for 192.168.1.242 [host down]
Nmap scan report for 192.168.1.243 [host down]
Nmap scan report for 192.168.1.244 [host down]
Nmap scan report for 192.168.1.245 [host down]
Nmap scan report for 192.168.1.246 [host down]
Nmap scan report for 192.168.1.247 [host down]
Nmap scan report for 192.168.1.248 [host down]
Nmap scan report for 192.168.1.249 [host down]
Nmap scan report for 192.168.1.250 [host down]
Nmap scan report for 192.168.1.251 [host down]
Nmap scan report for 192.168.1.252 [host down]
Nmap scan report for 192.168.1.253 [host down]
Nmap scan report for 192.168.1.254 [host down]
Nmap scan report for 192.168.1.255 [host down]
Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (0 hosts up) scanned in 206.73 seconds
    Raw packets sent: 2048 (77.824KB) | Rcvd: 7488 (478.706KB)
```

Search portscan

The screenshot shows a browser window with the URL tryhackme.com. The search results for "portscan" are displayed under the "Metasploit: Introduction" section. The results show two main categories: "x86" and "x64". Under "x86", there are 10 directories and 0 files. The "Evasion" category is expanded, showing various evasion modules for Windows.

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

Terminal

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_regas_m_regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpadeping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

10 directories, 0 files

Terminal

```
msf6 > search portscan
Matching Modules
=====
#  Name          Rank   Check  Description
----- 
0  auxiliary/scanner/portscan/ftpbounce      normal  No   FTP Bounce Port Scanner
1  auxiliary/scanner/natpmp/natpmp_portscan  normal  No   NAT-PMP External Port Scanner
2  auxiliary/scanner/sap/sap_router_portscanner  normal  No   SAPRouter Port Scanner
3  auxiliary/scanner/portscan/xmas            normal  No   TCP "XMas" Port Scanner
4  auxiliary/scanner/portscan/ack             normal  No   TCP ACK Firewall Scanner
5  auxiliary/scanner/portscan/tcp            normal  No   TCP Port Scanner
6  auxiliary/scanner/portscan/syn           normal  No   SYN Port Scanner
```

File Edit View Search Terminal Help

Nmap done: 256 IP addresses (0 hosts up) scanned in 206.73 seconds
Raw packets sent: 2048 (77.824KB) | Rcvd: 7488 (478.706KB)

msf6 >

THM AttackBox 52m 25s

cat

use 6(auxiliary/scanner/portscan/syn) and show options

The screenshot shows a browser window with the URL tryhackme.com. The "Evasion" category is expanded, showing various evasion modules for Windows.

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

Terminal

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_regas_m_regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpadeping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

10 directories, 0 files

Terminal

```
msf6 > use 6
msf6 auxiliary(scanner/portscan/syn) > show options
Module options (auxiliary/scanner/portscan/syn):
Name      Current Setting  Required  Description
----      -----        ----       -----
BATCHSIZE  256           yes        The number of hosts to scan per set
DELAY      0              yes        The delay between connections, per thread, in milliseconds
INTERFACE   eth0         no         The name of the interface
JITTER     0              yes        The jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS      1-10000        yes        Ports to scan (e.g. 22-25, 80,110-900)
RHOSTS     10.10.10.188  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic-using-metasploit.html
SNAPLEN    65535          yes        The number of bytes to capture
```

File Edit View Search Terminal Help

msf6 >

THM AttackBox 48m 48s

set interface, port, rhosts, threads

The screenshot shows a browser window with the URL tryhackme.com open. The page title is "TryHackMe | Metasploit: Introduction". On the left, there's a sidebar with "Private" and "tryhackme.com" buttons, and a navigation bar with links like Apple, iCloud, Yahoo, Bing, Google, TripAdvisor, Wikipedia, Facebook, Twitter, LinkedIn, The Weather Channel, TryHackMe M...wa | Medium, MSFVenom - C... HackTricks, and Yelp. Below the sidebar, it says "TryHackMe Metasploit: Introduction" and shows a file tree: "└── x86". Under "x86", there are "10 directories, 0 files". To the right, there's a terminal window titled "Metasploit Unleashed | Port Scanning | OffSec" with the command "Wed 24 Jan, 01:05 AttackBox IP:10.10.226.244". The terminal shows configuration settings:

```
File Edit View Search Terminal Help
SNAPLEN 65535 yes cs/using-metasploit.html
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 500 yes The reply read timeout in milliseconds
```

It also shows the command to view module info: "msf6 auxiliary(scanner/portscan/syn) > set info or info -d". The terminal then attempts to set the interface to eth0, but fails with "Unknown datastore option: port. Did you mean PORTS?". It then sets ports to 80, RHOSTS to 192.168.1.0/24, and THREADS to 50. Finally, it runs the scanner.

run

The screenshot shows a browser window with the URL tryhackme.com open. The page title is "TryHackMe | Metasploit: Introduction". On the left, there's a sidebar with "Private" and "tryhackme.com" buttons, and a navigation bar with links like Apple, iCloud, Yahoo, Bing, Google, TripAdvisor, Wikipedia, Facebook, Twitter, LinkedIn, The Weather Channel, TryHackMe M...wa | Medium, MSFVenom - C... HackTricks, and Yelp. Below the sidebar, it says "TryHackMe Metasploit: Introduction" and shows a file tree: "└── x86". Under "x86", there are "10 directories, 0 files". To the right, there's a terminal window titled "Metasploit Unleashed | Port Scanning | OffSec" with the command "Wed 24 Jan, 01:06 AttackBox IP:10.10.226.244". The terminal shows the configuration and execution of the port scan module:

```
File Edit View Search Terminal Help
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf6 auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/portscan/syn) > run
```

It fails with "Auxiliary failed: RuntimeError eth0: No such device exists (SIOCGIFHWADDR: No such device)". The stack trace shows multiple frames from the Metasploit framework, including "capture.rb:124:in 'open_live'", "capture.rb:124:in 'open_pcap'", "scanner/portscan/syn.rb:58:in 'run_batch'", "scanner/framework/embedded/framework/lib/msf/core/auxiliary/scanner.rb:213:in 'block in run'", "opt/metasploit-framework/embedded/framework/lib/msf/core/thread_manager.rb:105:in 'block in spawn'", and "opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/logging-2.3.1/lib/logging/diagnostic_context.rb:474:in 'block in create_with_logging_context'". Finally, it says "Auxiliary module execution completed".

back and use 5(auxiliary/scanner/portscan/tcp) and show options

The screenshot shows a browser window with the URL tryhackme.com and a terminal window. The terminal window is titled 'Terminal' and shows the following command history:

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_regasasm_regsrvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_heraderping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

The terminal then displays module options for 'auxiliary/scanner/portscan/tcp':

Name	Current Setting	Required	Description
CONCURRENCY	10	yes	The number of concurrent ports to check per host
DELAY	0	yes	The delay between connections, per thread, in milliseconds
JITTER	0	yes	The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS	1-10000	yes	Ports to scan (e.g. 22-25,80,110-900)
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit

host -R show options run

The screenshot shows a browser window with the URL tryhackme.com and a terminal window. The terminal window is titled 'Terminal' and shows the following command history:

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_regasasm_regsrvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_heraderping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

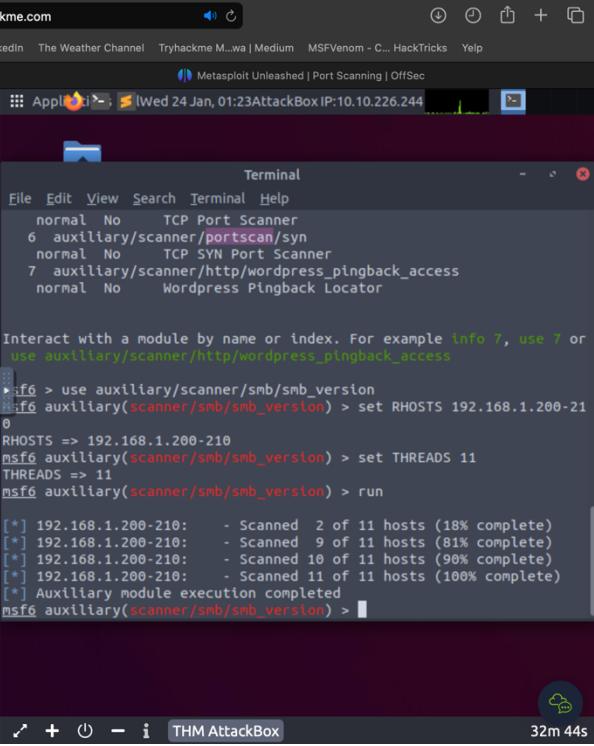
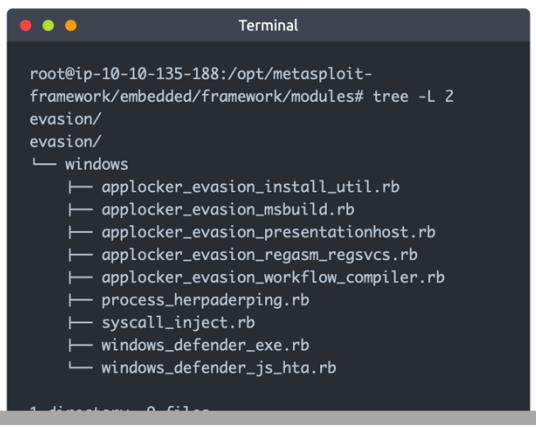
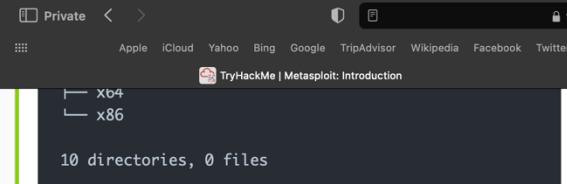
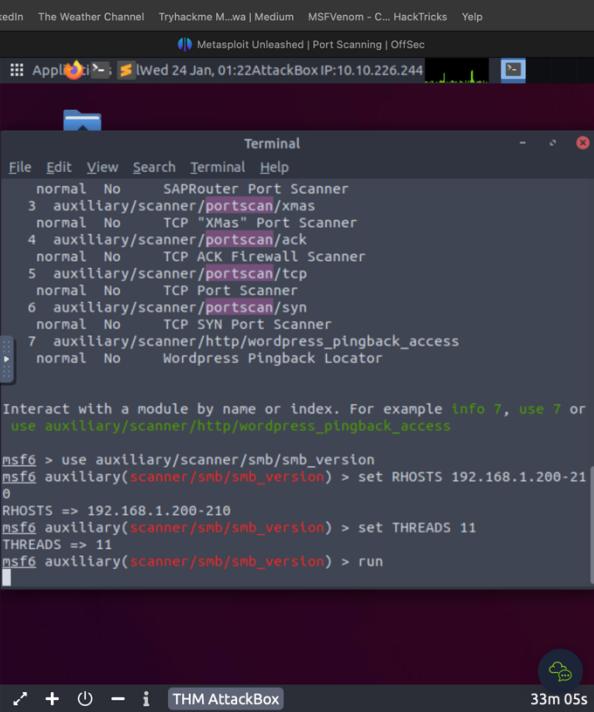
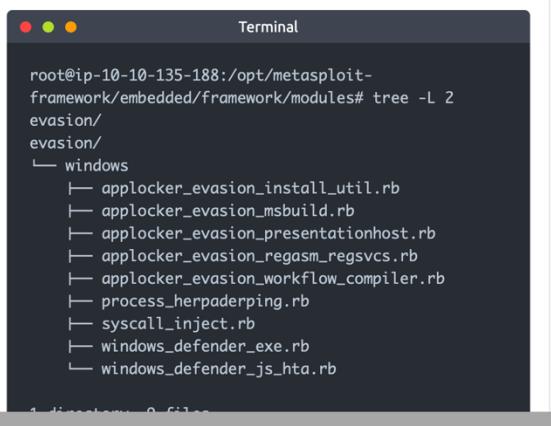
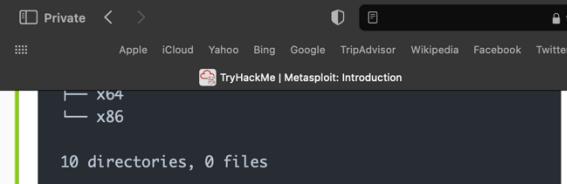
The terminal then runs 'hosts -R' and shows the results:

addr	mac	name	os_name	os_flavo	os_sp	purpose	info	comments
10.10								
>205.								
10.10								
.224.								
231								

It then runs 'show options' for the 'auxiliary/scanner/portscan/tcp' module:

Name	Current Setting	Required	Description
CONCURRENCY	10	yes	The number of concurrent ports to check per host
DELAY	0	yes	The delay between connections, per thread, in milliseconds
JITTER	0	yes	The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS	1-10000	yes	Ports to scan (e.g. 22-25,80,110-900)
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit

use auxiliary/scanner/smb/smb_version set rhosts.threads and run



hosts

Private < > tryhackme.com

Apple iCloud Yahoo Bing Google TripAdvisor Wikipedia Facebook Twitter LinkedIn The Weather Channel Tryhackme M...wa | Medium MSFVenom - C... HackTricks Yelp

TryHackMe | Metasploit: Introduction

Metasploit Unleashed | Port Scanning | OffSec

Appl... (Wed 24 Jan, 01:23) AttackBox IP: 10.10.226.244

Terminal

File Edit View Search Terminal Help

THREADS => 11

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.1.200-210: - Scanned 2 of 11 hosts (18% complete)

[*] 192.168.1.200-210: - Scanned 9 of 11 hosts (81% complete)

[*] 192.168.1.200-210: - Scanned 10 of 11 hosts (90% complete)

[*] 192.168.1.200-210: - Scanned 11 of 11 hosts (100% complete)

[*] Auxiliary module execution completed

msf6 auxiliary(scanner/smb/smb_version) > hosts

Hosts

====

addr	mac	name	os_name	os_flavo	os_sp	purpose	info	comments
10.10				r				
.205.								
0								
10.10								
.224.								
231								

msf6 auxiliary(scanner/smb/smb_version) >

THM AttackBox 32m 25s

back and use auxiliary/scanner/ip/iphidseq

Private < > tryhackme.com

Apple iCloud Yahoo Bing Google TripAdvisor Wikipedia Facebook Twitter LinkedIn The Weather Channel Tryhackme M...wa | Medium MSFVenom - C... HackTricks Yelp

TryHackMe | Metasploit: Introduction

Metasploit Unleashed | Port Scanning | OffSec

Appl... (Wed 24 Jan, 01:24) AttackBox IP: 10.10.226.244

Terminal

File Edit View Search Terminal Help

THREADS => 11

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.1.200-210: - Scanned 2 of 11 hosts (18% complete)

[*] 192.168.1.200-210: - Scanned 9 of 11 hosts (81% complete)

[*] 192.168.1.200-210: - Scanned 10 of 11 hosts (90% complete)

[*] 192.168.1.200-210: - Scanned 11 of 11 hosts (100% complete)

[*] Auxiliary module execution completed

msf6 auxiliary(scanner/smb/smb_version) > hosts

Hosts

====

addr	mac	name	os_name	os_flavo	os_sp	purpose	info	comments
10.10				r				
.205.								
0								
10.10								
.224.								
231								

msf6 auxiliary(scanner/smb/smb_version) > back

msf6 > use auxiliary/scanner/ip/iphidseq

msf6 auxiliary(scanner/ip/iphidseq) >

THM AttackBox 31m 44s

Set rhosts,threads and run

The screenshot shows a macOS desktop environment with two terminal windows and a Metasploit interface window.

Top Terminal Window:

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_reasm_regsrvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_heraderping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

Bottom Terminal Window:

```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_reasm_regsrvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_heraderping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

Metasploit Interface Window:

The Metasploit interface shows the following configuration:

Name	Current	Setting	Required	Description
INTERFACE			no	The name of the interface
RHOSTS			yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic-using-metasploit.html
RPORT	80		yes	The target port
SNAPLEN	65535		yes	The number of bytes to capture
THREADS	1		yes	The number of concurrent threads (max one per host)
TIMEOUT	500		yes	The reply read timeout in milliseconds

Below the configuration, the terminal shows the command history:

```
msf6 auxiliary(scanner/lp/lpldseq) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf6 auxiliary(scanner/lp/lpldseq) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/lp/lpldseq) > run
```

tryhackme.com

TryHackMe | Metasploit: Introduction

```

Xb4
└── x86
    10 directories, 0 files

```

Evasion

While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other hand, "evasion" modules will try that, with more or less success.

Terminal

```

root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2
evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_Regasm_Regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpadeping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb

```

File Edit View Search Terminal Help

TIMEOUT 500 yes The reply read timeout in milliseconds

View the full module info with the `info`, or `info -d` command.

```

msf6 auxiliary(scanner/lo/ipldseq) > set RHOSTS 192.168.1.0/24
msf6 auxiliary(scanner/lo/ipldseq) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/lo/ipldseq) > run
[*] Scanned 47 of 256 hosts (18% complete)
[*] Scanned 59 of 256 hosts (23% complete)
[*] Scanned 78 of 256 hosts (30% complete)
[*] Scanned 108 of 256 hosts (42% complete)
[*] Scanned 129 of 256 hosts (50% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 180 of 256 hosts (70% complete)
[*] Scanned 209 of 256 hosts (81% complete)
[*] Scanned 234 of 256 hosts (91% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/lo/ipldseq) >

```

THM AttackBox 27m 30s

nmap -Pn -sl

tryhackme.com

TryHackMe | Metasploit: Introduction

see this by typing the `show options` command.

Show options

```

msf6 exploit(windows/smb/ms17_010_eternalblue) >
show options

Module options
(exploit/windows/smb/ms17_010_eternalblue):

  Name      Current Setting  Required
Description
  ----      -----          -----
  RHOSTS           yes        The
target host(s), range CIDR identifier, or hosts file
with syntax 'file:'
  RPRT          445         yes        The
target port (TCP)
  SMBDomain       .          no
(Optional) The Windows domain to use for
authentication
  SMBPass         no
(Optional) The password for the specified username
  SMBUser         no
(Optional) The username to authenticate as
  VERIFY_ARCH     true       yes      Check
if remote architecture matches exploit Target.

```

File Edit View Search Terminal Help

RHOSTS => 192.168.1.0/24

```

msf6 auxiliary(scanner/lo/ipldseq) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/lo/ipldseq) > run
[*] Scanned 47 of 256 hosts (18% complete)
[*] Scanned 59 of 256 hosts (23% complete)
[*] Scanned 78 of 256 hosts (30% complete)
[*] Scanned 108 of 256 hosts (42% complete)
[*] Scanned 129 of 256 hosts (50% complete)
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 180 of 256 hosts (70% complete)
[*] Scanned 209 of 256 hosts (81% complete)
[*] Scanned 234 of 256 hosts (91% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/lo/ipldseq) > nmap -Pn -sI 192.168.109 192.168.1.114
[*] exec: nmap -Pn -sI 192.168.109 192.168.1.114

Starting Nmap 7.60 ( https://nmap.org ) at 2024-01-24 01:30 GMT
Idle scan zombie 192.168.109 (192.168.0.109) port 80 cannot be used b
ecause it has not returned any of our probes -- perhaps it is down or

```

THM AttackBox 24m 32s

Back use auxiliary/scanner/portscan/tcp show options

see this by typing the show options command.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options
(exploit/windows/smb/ms17_010_eternalblue):

Name          Current Setting  Required
Description
-----  -----  -----
RHOSTS          yes      The
target host(s), range CIDR identifier, or hosts file
with syntax 'file:'
RPORT           445       yes      The
target port (TCP)
SMBDomain        .         no
(Optional) The Windows domain to use for
authentication
SMBPass          no
(Optional) The password for the specified username
SMBUser          no
(Optional) The username to authenticate as
VERIFY_ARCH     true      yes      Check
if remote architecture matches exploit Target.
```

```
Metasploit Unleashed | Port Scanning | OffSec
Terminal
File Edit View Search Terminal Help
firewalled.
QUITTING!
msf6 auxiliary(scanner/tcp/pidseq) > back
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

Name          Current Setting  Required
Description
-----  -----  -----
CONCURRENCY    10        yes      The number of concurrent
ports to check per host
DELAY           0         yes      The delay between connec-
tions, per thread, in mi-
lliseconds
JITTER          0         yes      The delay jitter factor
(maximum value by which
to +/- DELAY) in milli-
conds.
PORTS          1-10000    yes      Ports to scan (e.g. 22-2
5,80,110-900)
RHOSTS          yes      The target host(s), see
https://docs.metasploit.
com/docs/using-metasploit
```

set threads and run

```
address (can interface may be specified)
LPORT      4444       yes      The listen
port

Exploit target:

Id  Name
--  --
0   Windows 7 and Server 2008 R2 (x64) All
Service Packs

msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Once you have set a parameter, you can use the `show options` command to check the value was set correctly.

Parameters you will often use are:

- RHOSTS: "Remote host", the IP address of the target system. A single IP address or a network range can be set. This will support the CIDR (Classless Inter-Domain Routing) notation (/24, /16, etc.) or a network range (10.10.10.x – 10.10.10.y). You can also use a file where targets are listed, one target per line using file:/path/of/the/target_file.txt, as you can see below.

```
Metasploit Unleashed | Port Scanning | OffSec
Terminal
File Edit View Search Terminal Help
RHOSTS      10.10.226.244  yes      5,80,110-900)
THREADS     1             yes      The target host(s), see
                                https://docs.metasploit.
                                com/docs/using-metasploit
                                t/basics/using-metasploit
                                t.html
TIMEOUT     1000         yes      The number of concurrent
                                threads (max one per ho-
                                st)
                                The socket connect timeo-
                                ut in milliseconds

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/portscan/tcp) > set THREADS 3
THREADS => 3
msf6 auxiliary(scanner/portscan/tcp) > run

[*] 10.10.226.244:          - 10.10.226.244:22 - TCP OPEN
[*] 10.10.226.244:          - 10.10.226.244:80 - TCP OPEN
[*] 10.10.226.244:          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > 
```

db_nmap -sV -p

The screenshot shows a web browser window with the URL tryhackme.com. The page displays the Metasploit interface for running a port scan. The command entered is `db_nmap -sV -p`. The output shows the target configuration (LPORT 4444) and the exploit target (Windows 7 and Server 2008 R2 (x64) All Service Packs). Below this, the msf6 exploit command is shown.

Once you have set a parameter, you can use the `show options` command to check the value was set correctly.

Parameters you will often use are:

- RHOSTS: "Remote host", the IP address of the target system. A single IP address or a network range can be set. This will support the CIDR (Classless Inter-Domain Routing) notation (/24, /16, etc.) or a network range (10.10.10.x – 10.10.10.y). You can also use a file where targets are listed, one target per line using file:/path/of/the/target_file.txt, as you can see below.

The screenshot also includes a terminal window showing the Nmap scan results for the target IP 10.10.226.244, which identifies the host as Ubuntu 4ubuntu0.7 (OpenSSH 7.6p1).

The terminal window shows the Nmap scan results for the target IP 10.10.226.244. The output indicates that port 22/tcp is open (ssh, OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)). Other ports like 25/tcp, 80/tcp, and 110/tcp are closed. The scan took approximately 17 minutes and 53 seconds.

The terminal window shows the Nmap scan results for the target IP 10.10.226.244. The output indicates that port 22/tcp is open (ssh, OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)). Other ports like 25/tcp, 80/tcp, and 110/tcp are closed. The scan took approximately 14 minutes and 25 seconds.

```
db_nmap -sV -A -p
```

The screenshot shows a web browser window with the URL tryhackme.com. The page content is a Metasploit introduction guide. It includes configuration settings for the exploit (LPRT port 4444), a target selection table, and a command prompt showing the msf6 exploit(windows/smb/ms17_010_eternalblue) > prompt.

Once you have set a parameter, you can use the `show options` command to check the value was set correctly.

Parameters you will often use are:

- RHOSTS: "Remote host", the IP address of the target system. A single IP address or a network range can be set. This will support the CIDR (Classless Inter-Domain Routing) notation (/24, /16, etc.) or a network range (10.10.10.x – 10.10.10.y). You can also use a file where targets are listed, one target per line using file:/path/of/the/target_file.txt, as you can see below.

The terminal window on the right shows the output of the command `db_nmap -sV -A -p 80,22,110,25 10.10.226.244`. The output details the Nmap scan process, including service detection for SSH (OpenSSH 7.6p1 Ubuntu 4ubuntu1.11) and port 22/tcp.