NAME:

HASNAIN TAHIR

ROLL NUMBER:

231-450367

COURSE:

COMP421

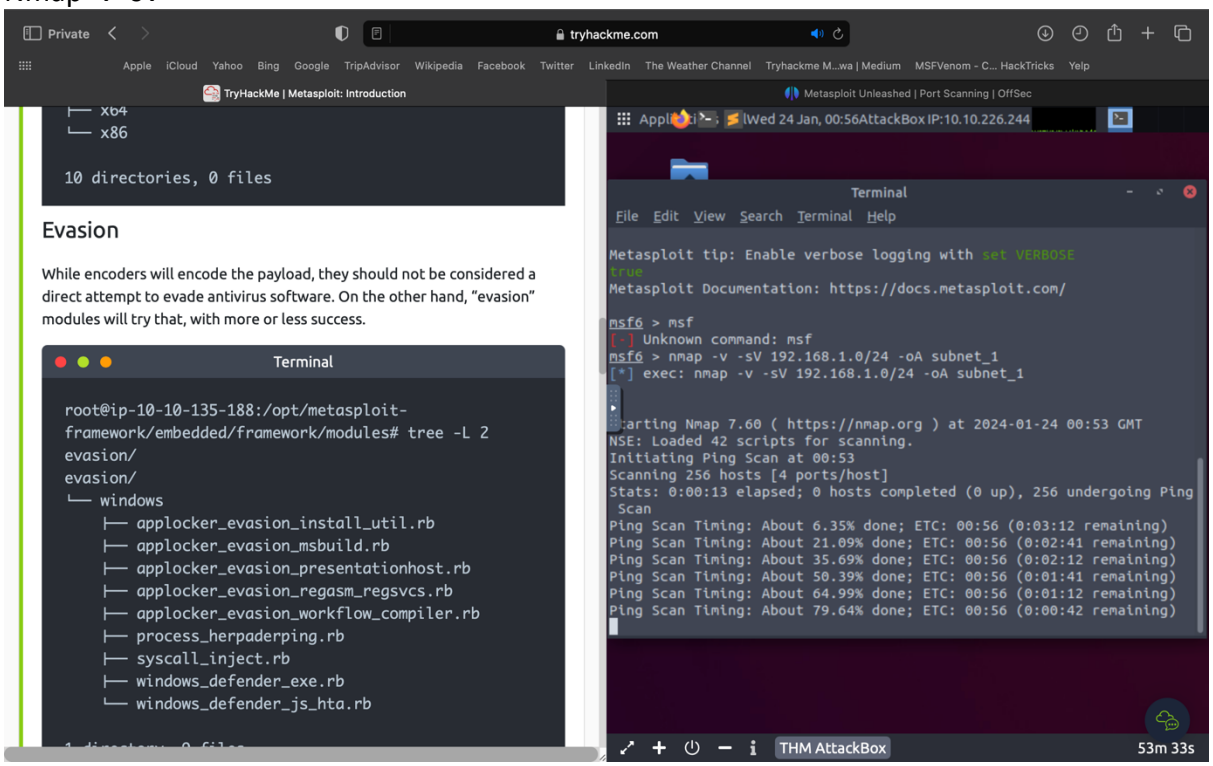
SECTION:

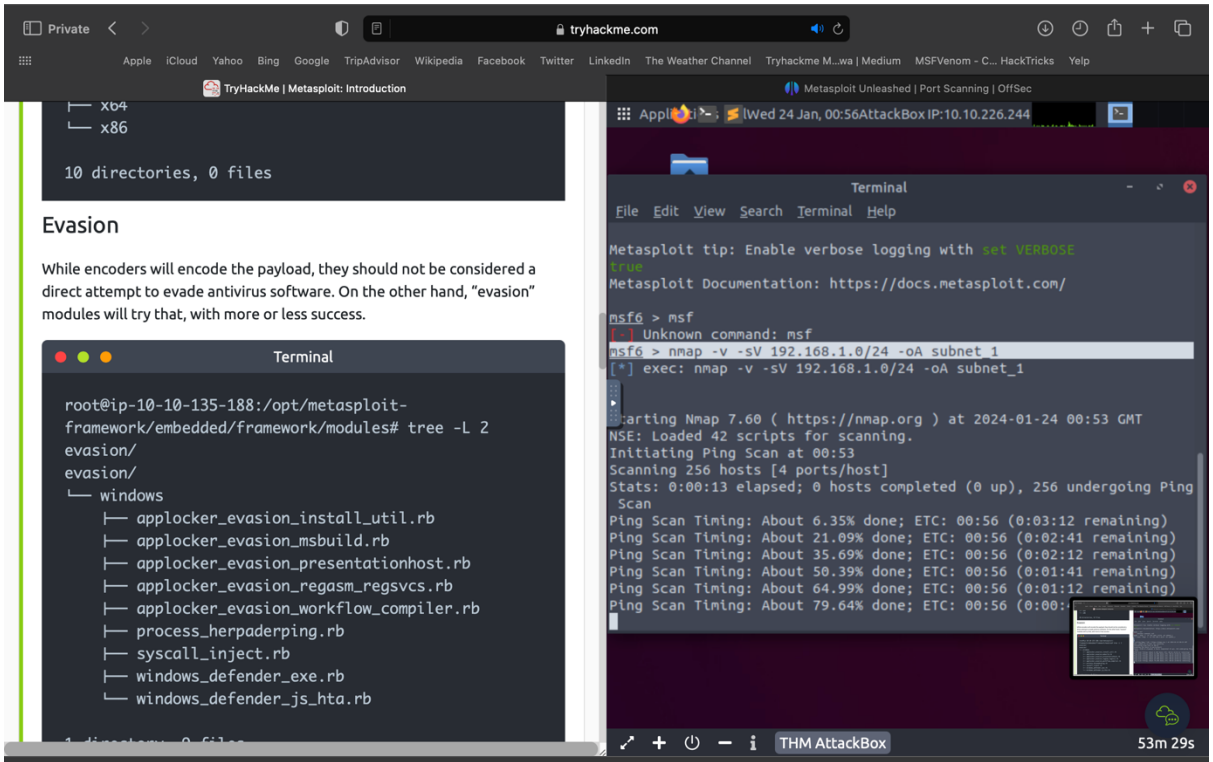
B

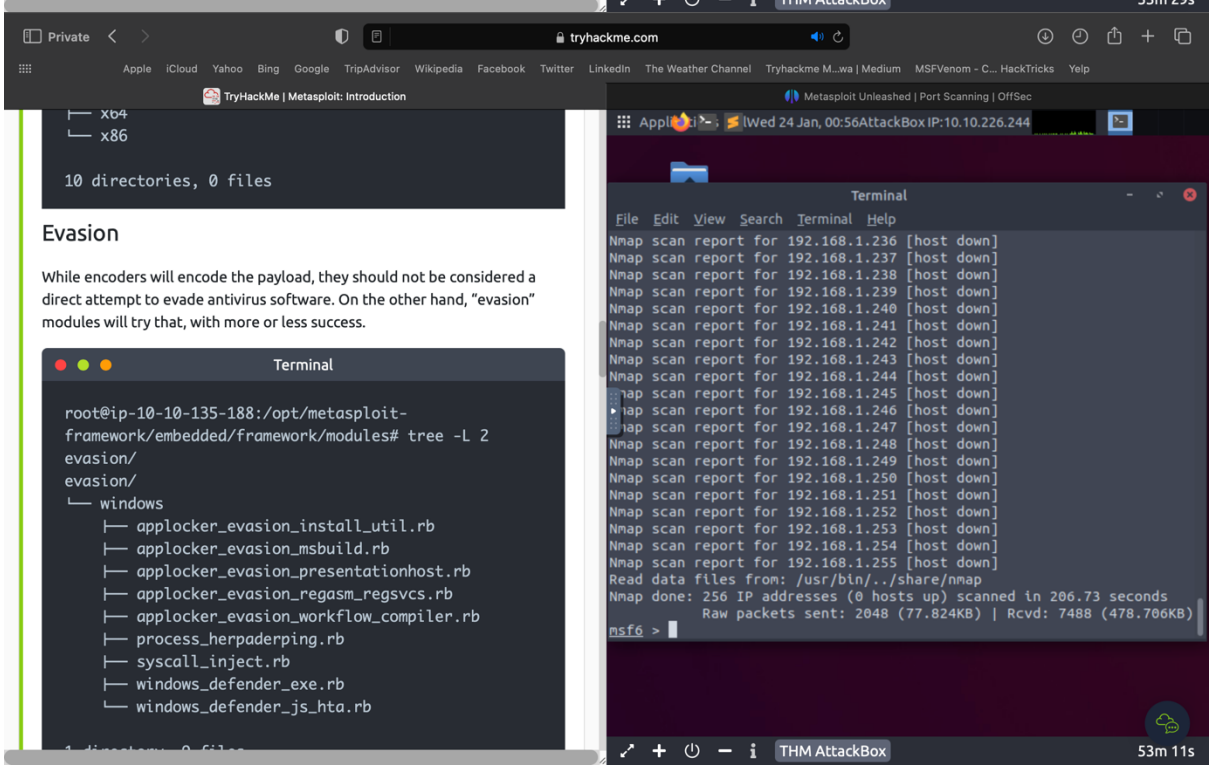
ASSIGNMENT:

1

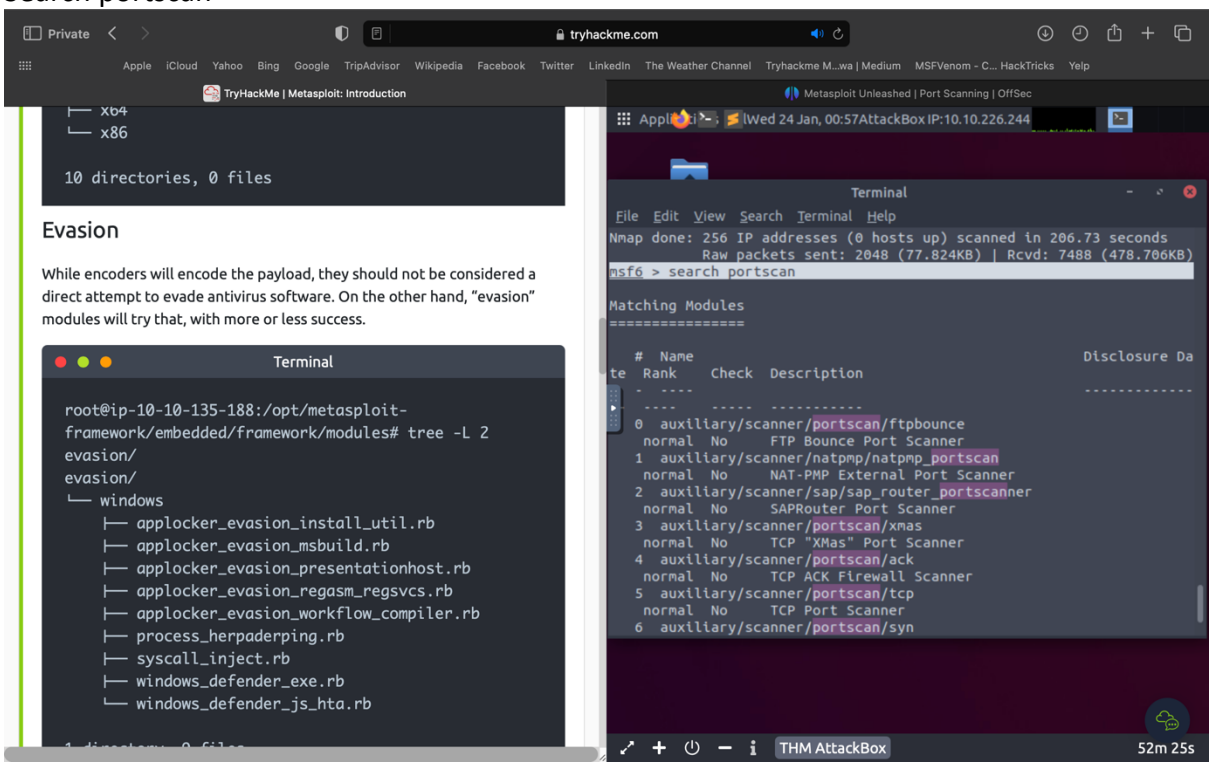
Nmap -v -sV


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
└── 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_herpaderping.rb
├── syscall_inject.rb
├── windows_defender_exe.rb
└── windows_defender_js_hta.rb
Wed 24 Jan, 00:56
AttackBox IP:10.10.226.244
Terminal
File Edit View Search Terminal Help
Metasploit tip: Enable verbose logging with set VERBOSE true
Metasploit Documentation: https://docs.metasploit.com/
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)
THM AttackBox
53m 33s


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
Wed 24 Jan, 00:56
AttackBox IP:10.10.226.244
Terminal
File Edit View Search Terminal Help
Metasploit tip: Enable verbose logging with set VERBOSE true
Metasploit Documentation: https://docs.metasploit.com/
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:
THM AttackBox
53m 29s
├── x64
└── 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_herpaderping.rb
├── syscall_inject.rb
├── windows_defender_exe.rb
└── windows_defender_js_hta.rb

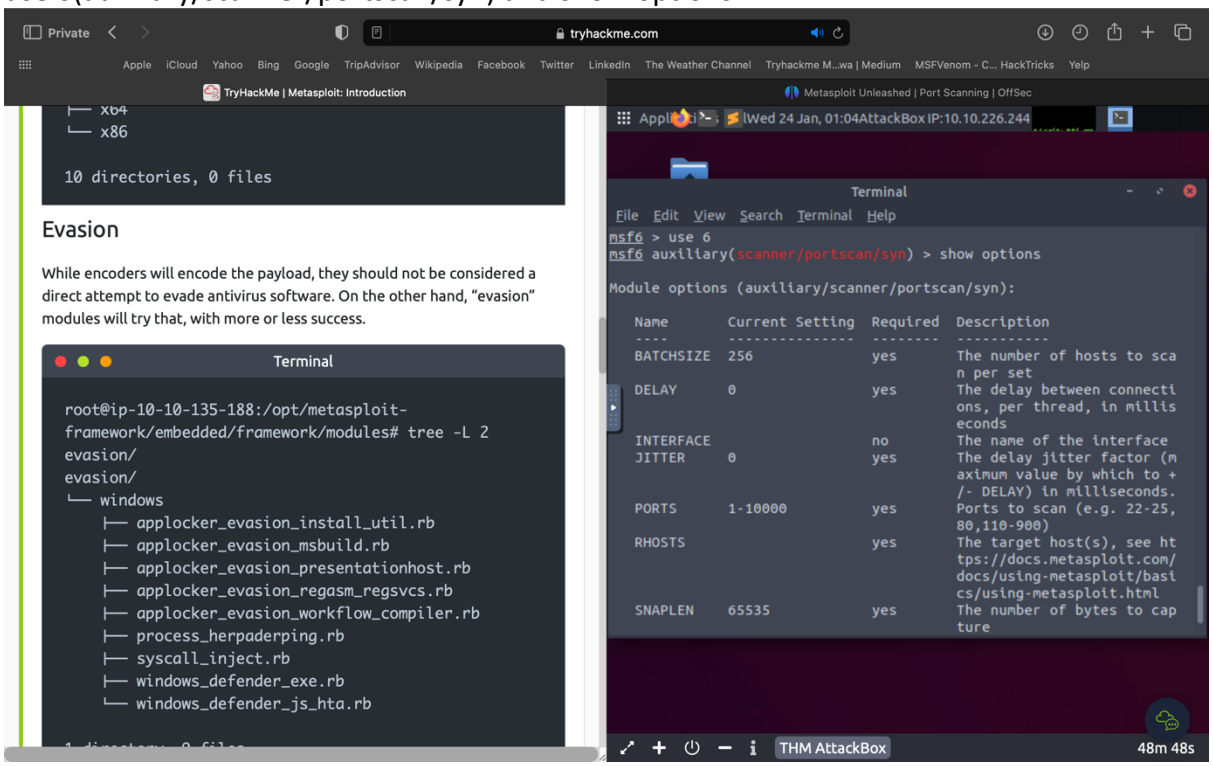

Private
tryhackme.com
Apple iCloud Yahoo Bing Google TripAdvisor Wikipedia Facebook Twitter LinkedIn The Weather Channel Tryhackme M...wa | Medium MSFVenom - C... HackTricks Yelp
TryHackMe | Metasploit: Introduction
Metasploit Unleashed | Port Scanning | OffSec
Wed 24 Jan, 00:56
AttackBox IP:10.10.226.244
Terminal
File Edit View Search Terminal Help
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)
msf6 >
THM AttackBox
53m 11s
├── x64
└── 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_herpaderping.rb
├── syscall_inject.rb
├── windows_defender_exe.rb
└── windows_defender_js_hta.rb

Search portscan

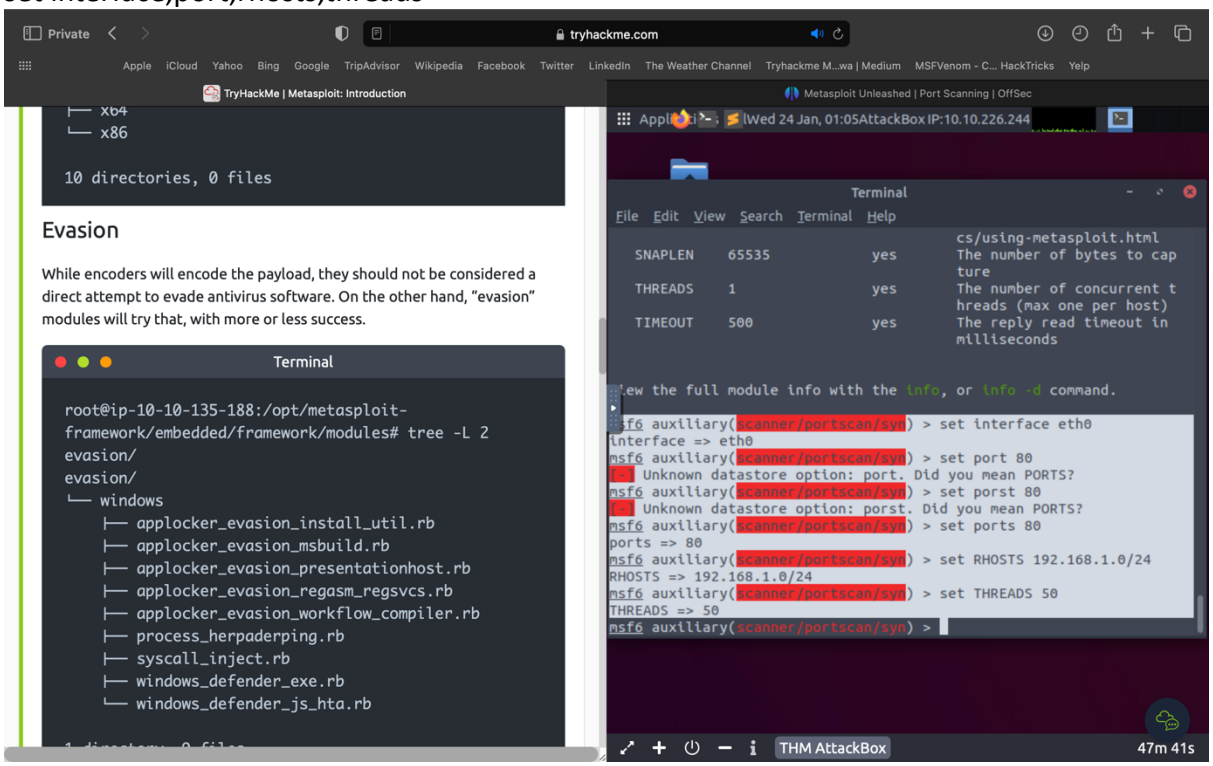


cat

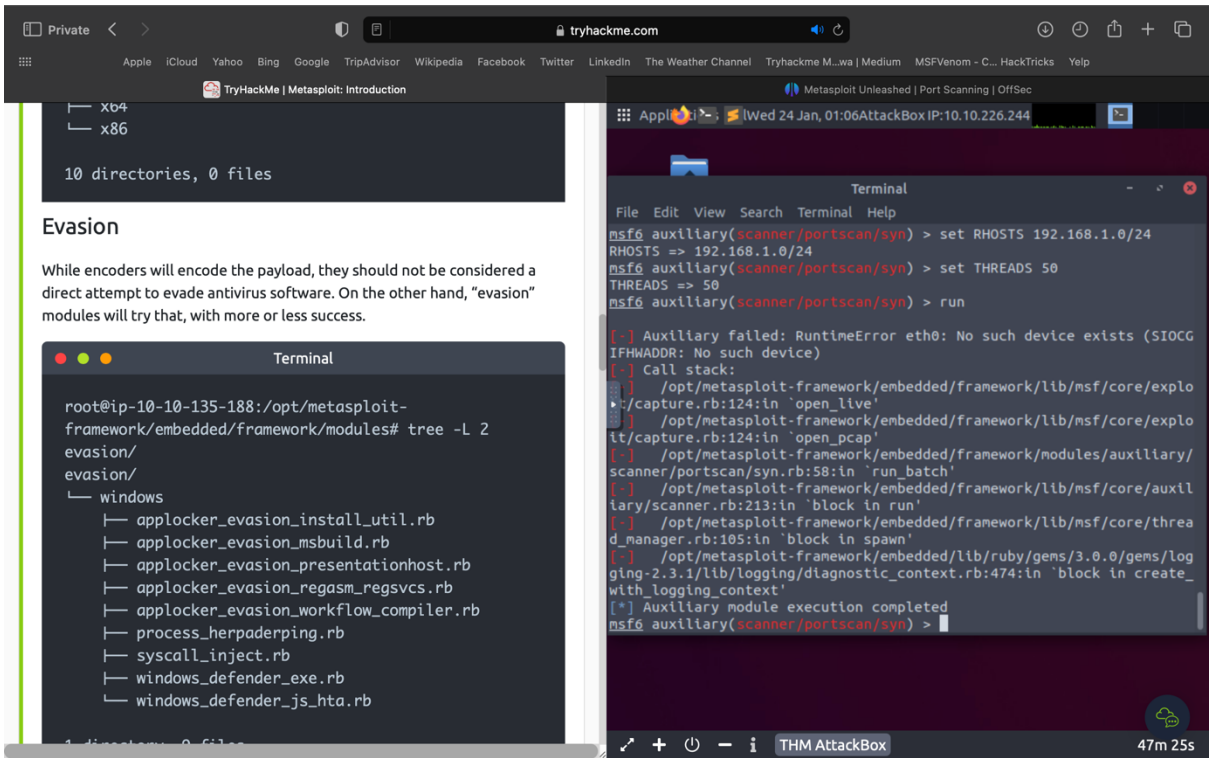
use 6(auxiliary/scanner/portscan/syn) and show options



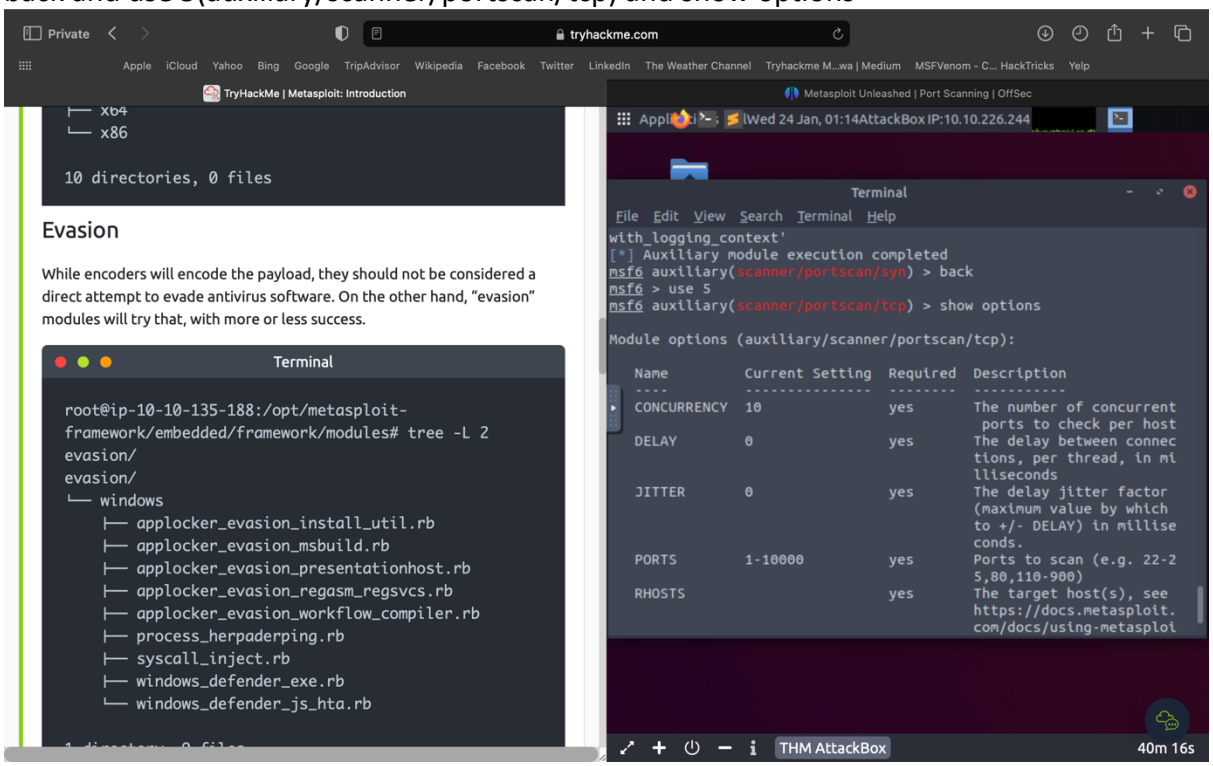
set interface,port,rhosts,threads



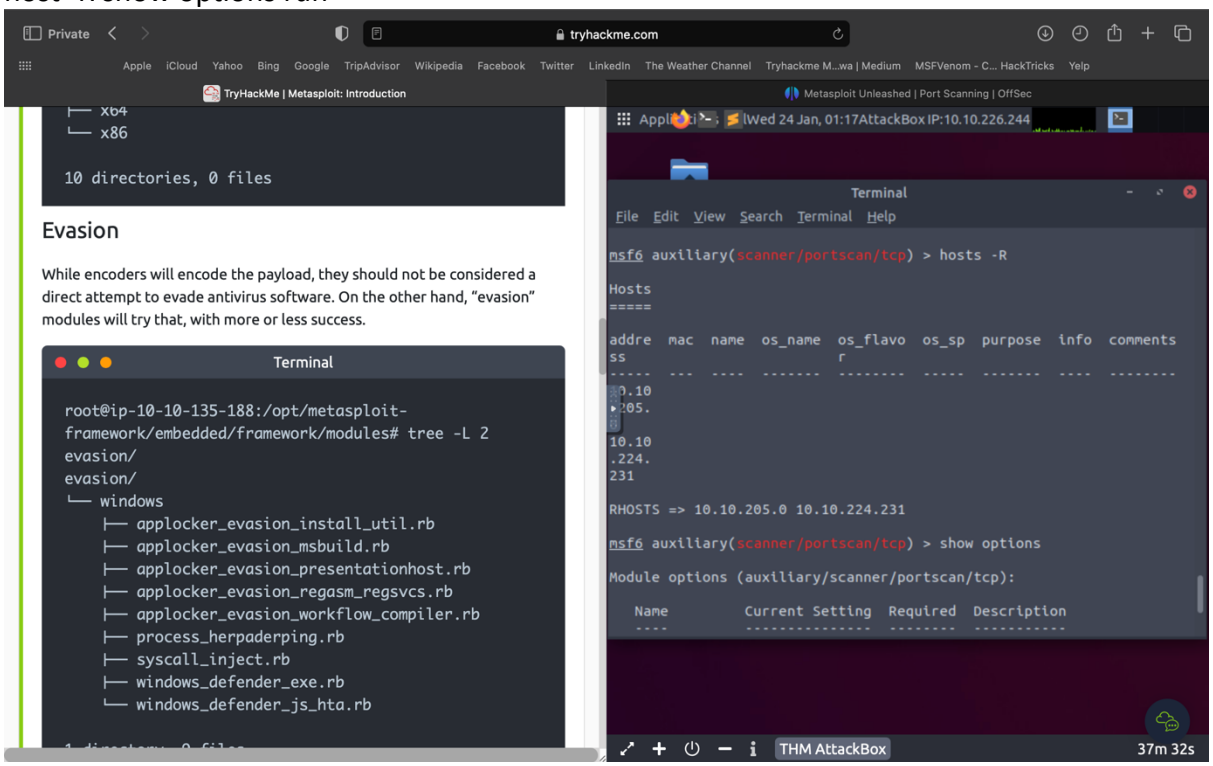
run



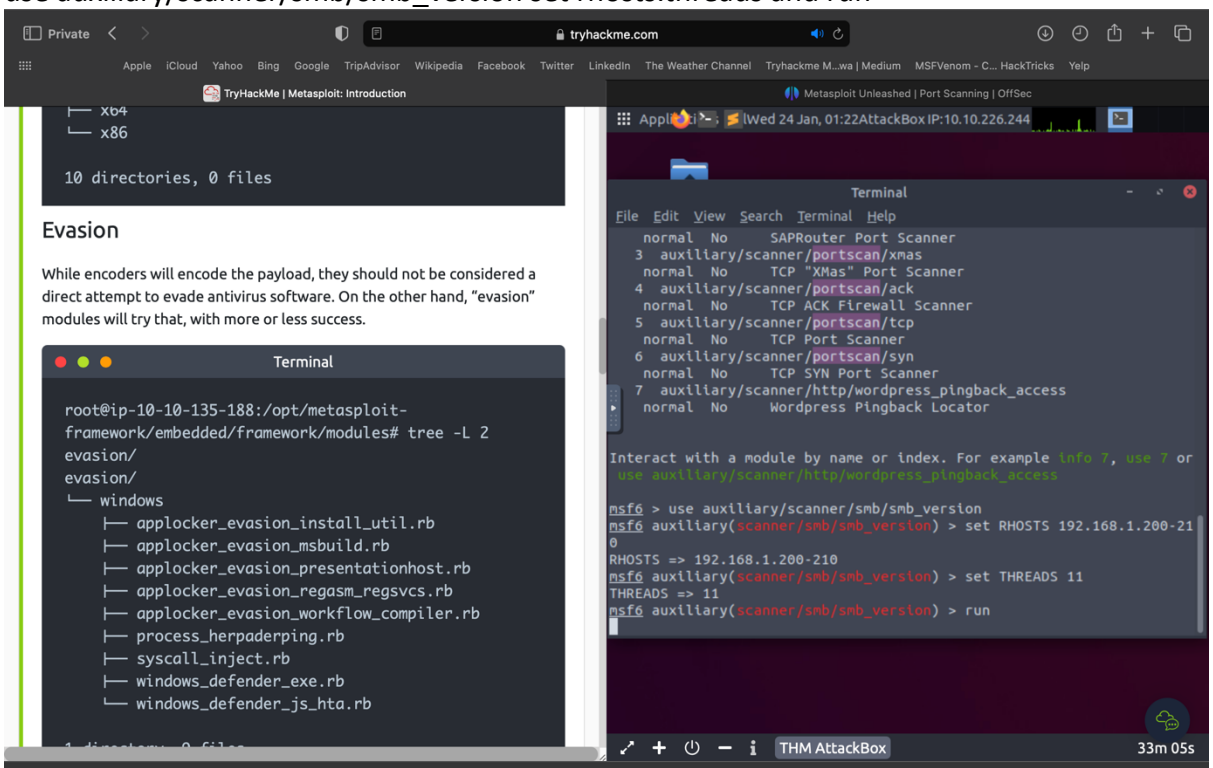
back and use 5(auxiliary/scanner/portscan/tcp) and show options

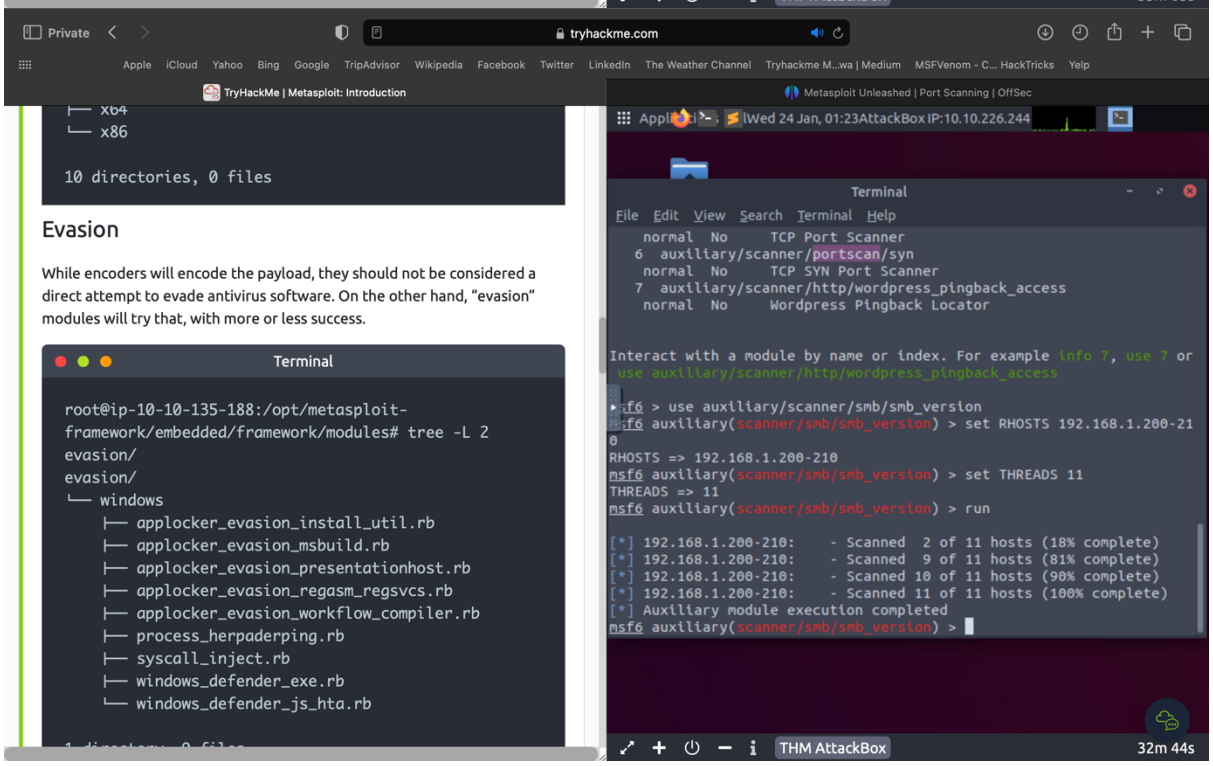


host -R show options run

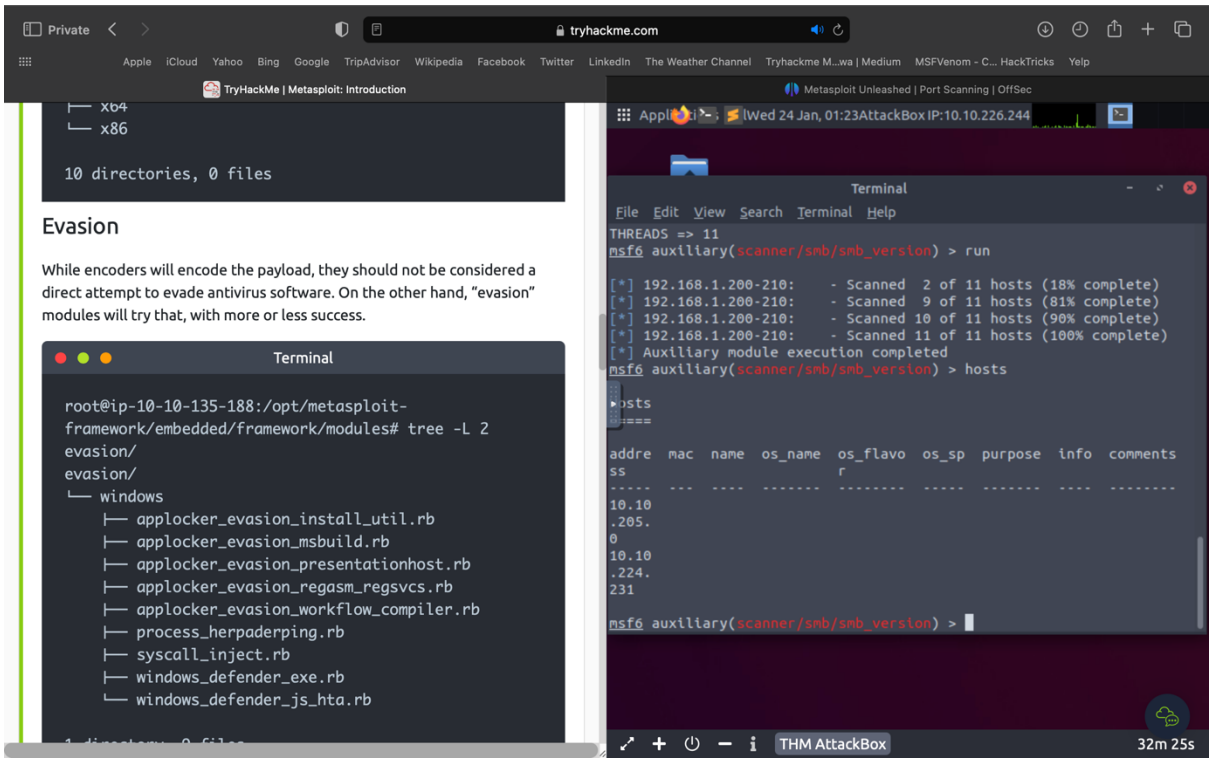


use auxiliary/scanner/smb/smb_version set rhosts.threads and run

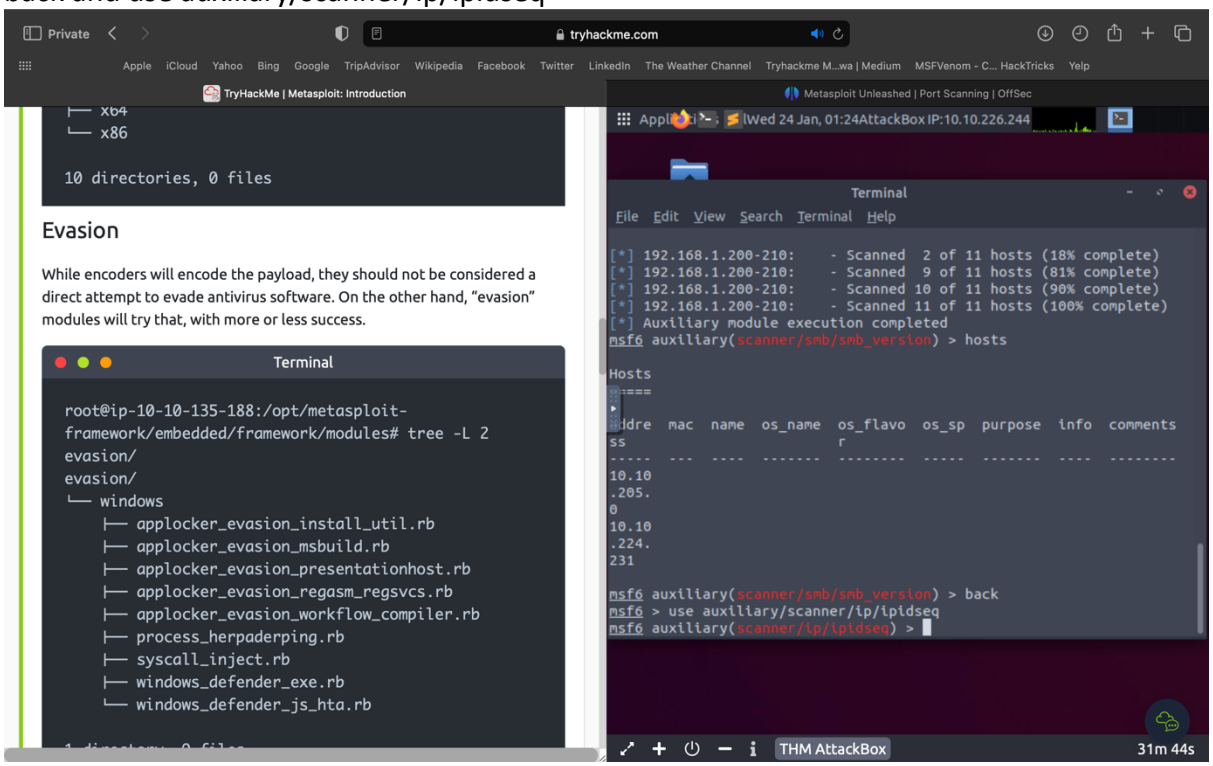




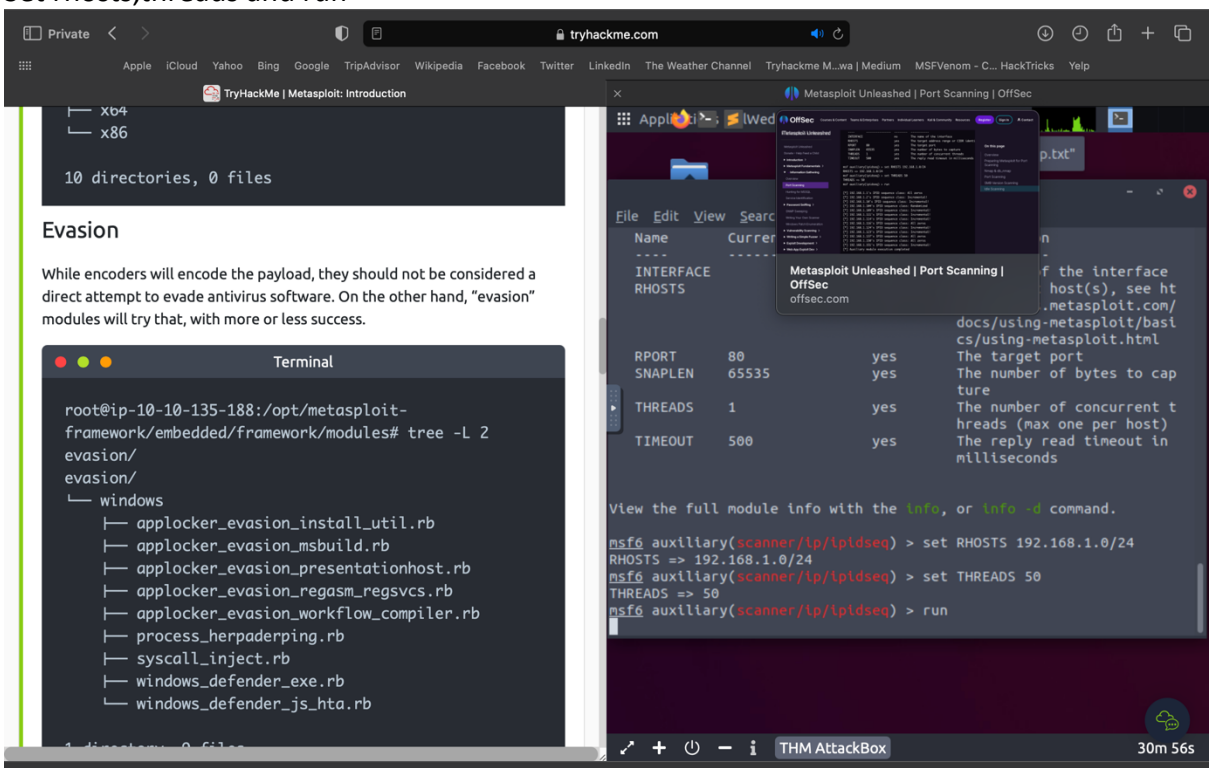
hosts

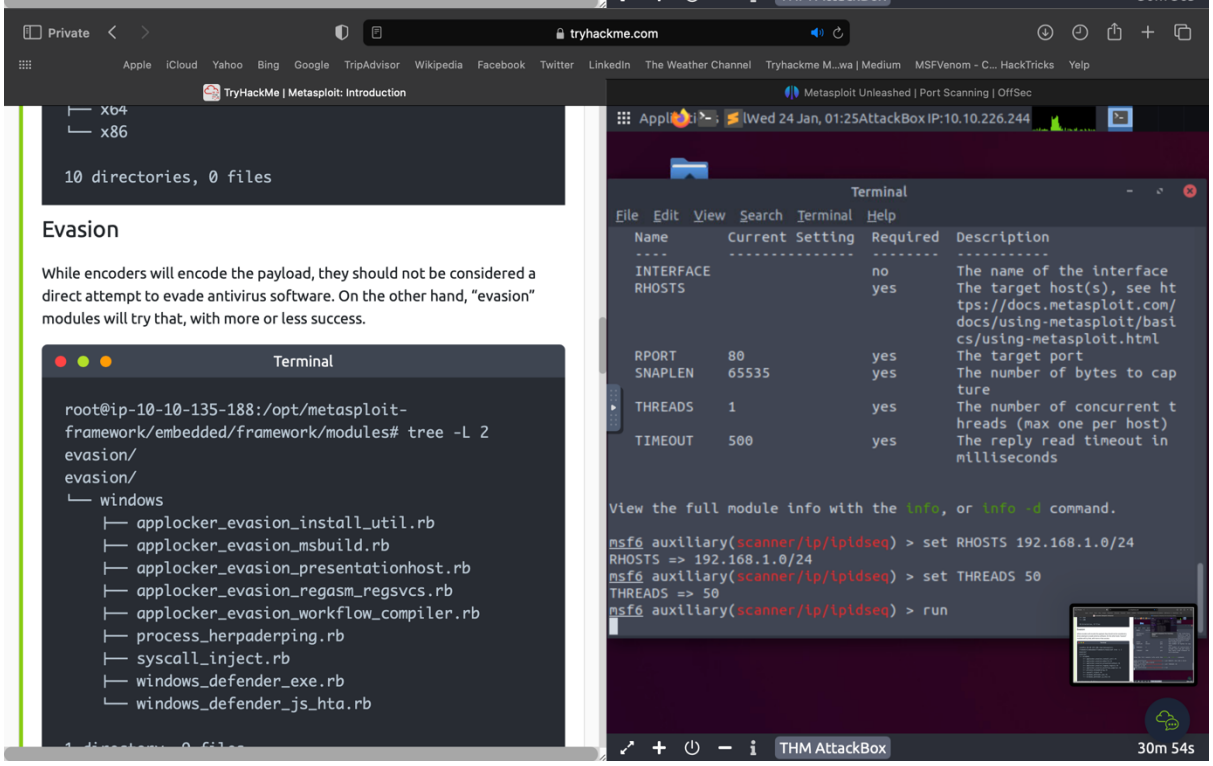


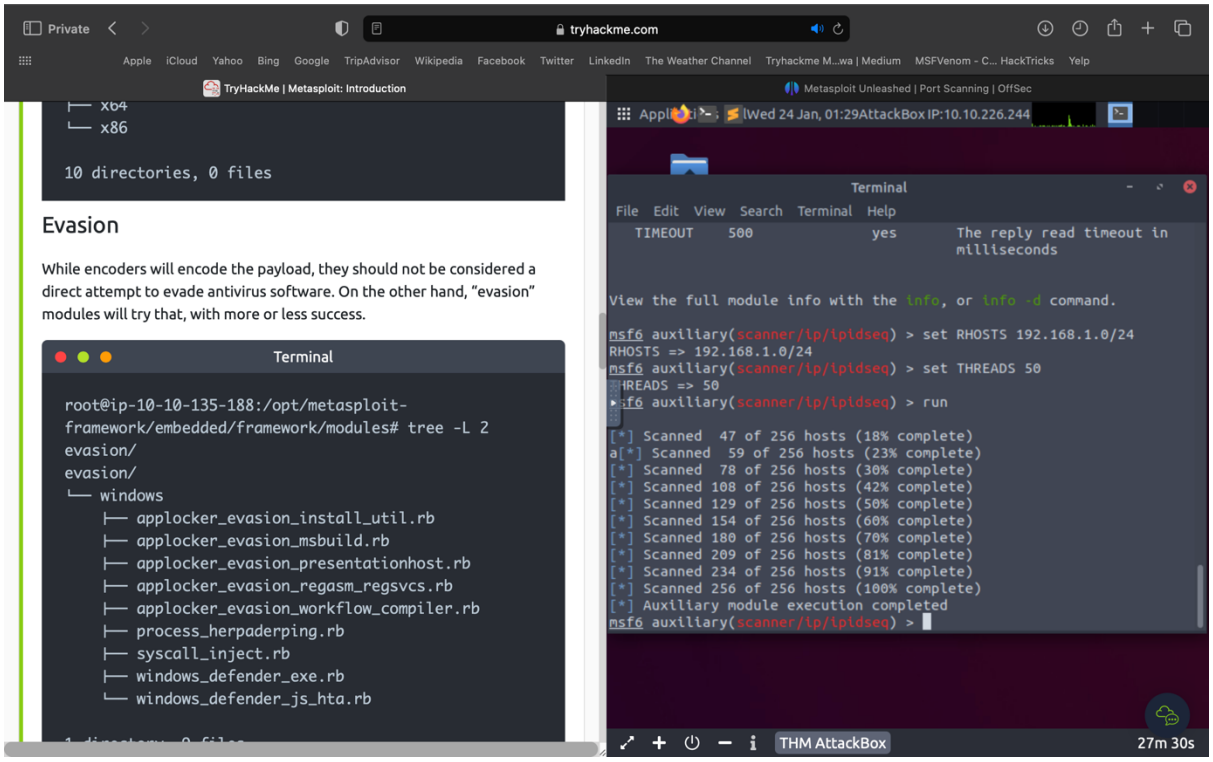
back and use auxiliary/scanner/ip/ipidseq



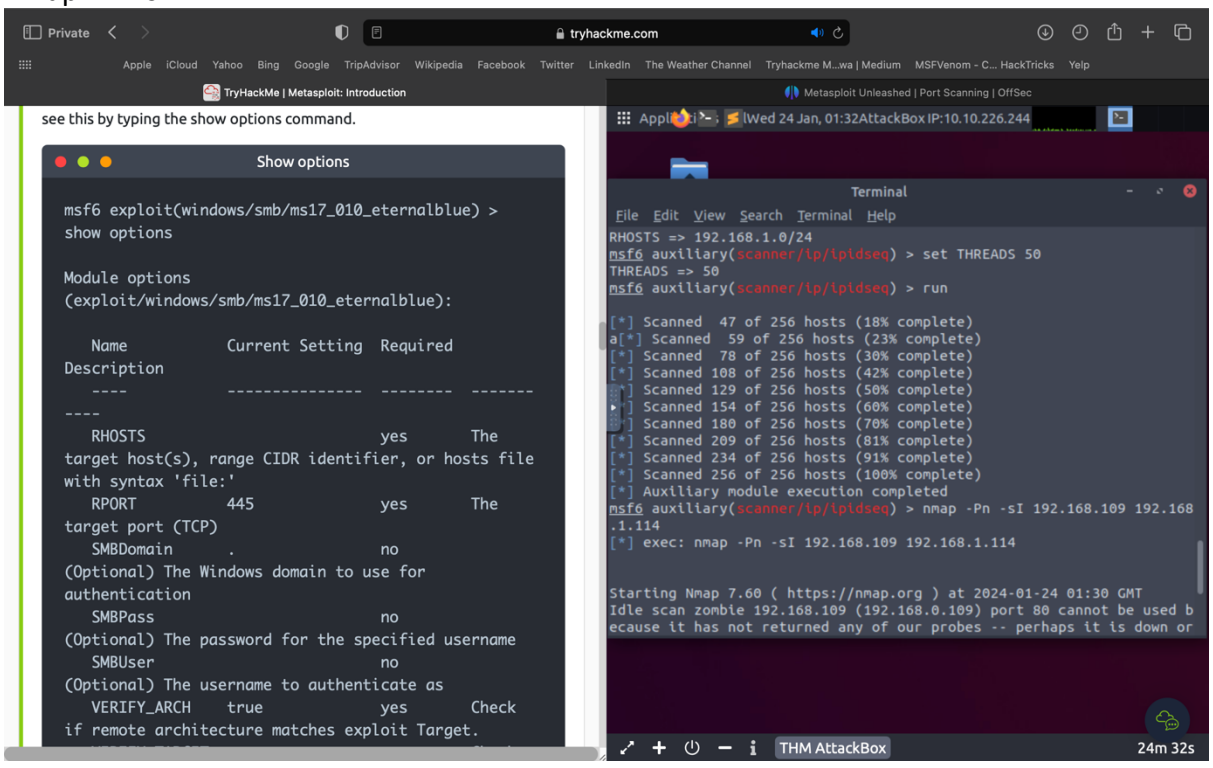
Set rhosts,threads and run



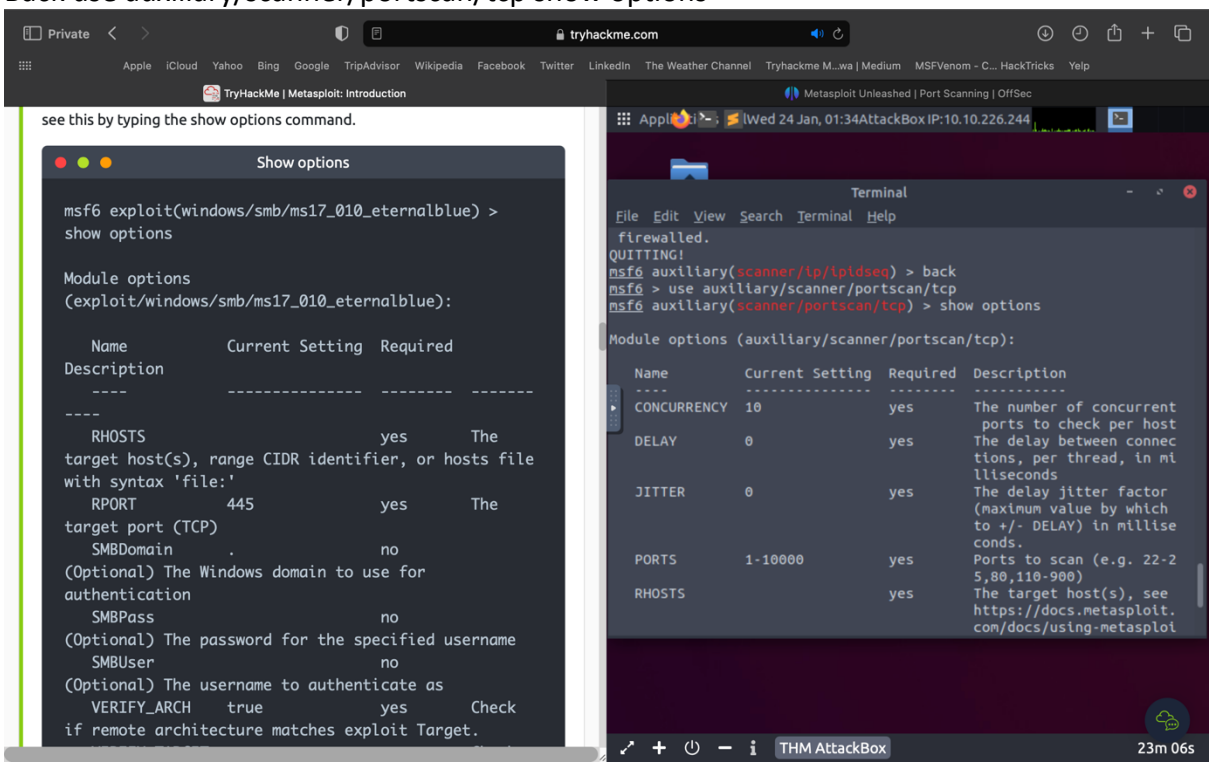



tryhackme.com
TryHackMe | Metasploit: Introduction
Metasploit Unleashed | Port Scanning | OffSec
Wed 24 Jan, 01:29
AttackBox IP:10.10.226.244
10 directories, 0 files
Evasion
While encoders will encode the payload, they should not be considered a direct attempt to evade antivirus software. On the other 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_herpaderping.rb
├── syscall_inject.rb
├── windows_defender_exe.rb
└── windows_defender_js_hta.rb
Terminal
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/ip/ipidseq) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf6 auxiliary(scanner/ip/ipidseq) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/ip/ipidseq) > 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/ip/ipidseq) >
THM AttackBox
27m 30s

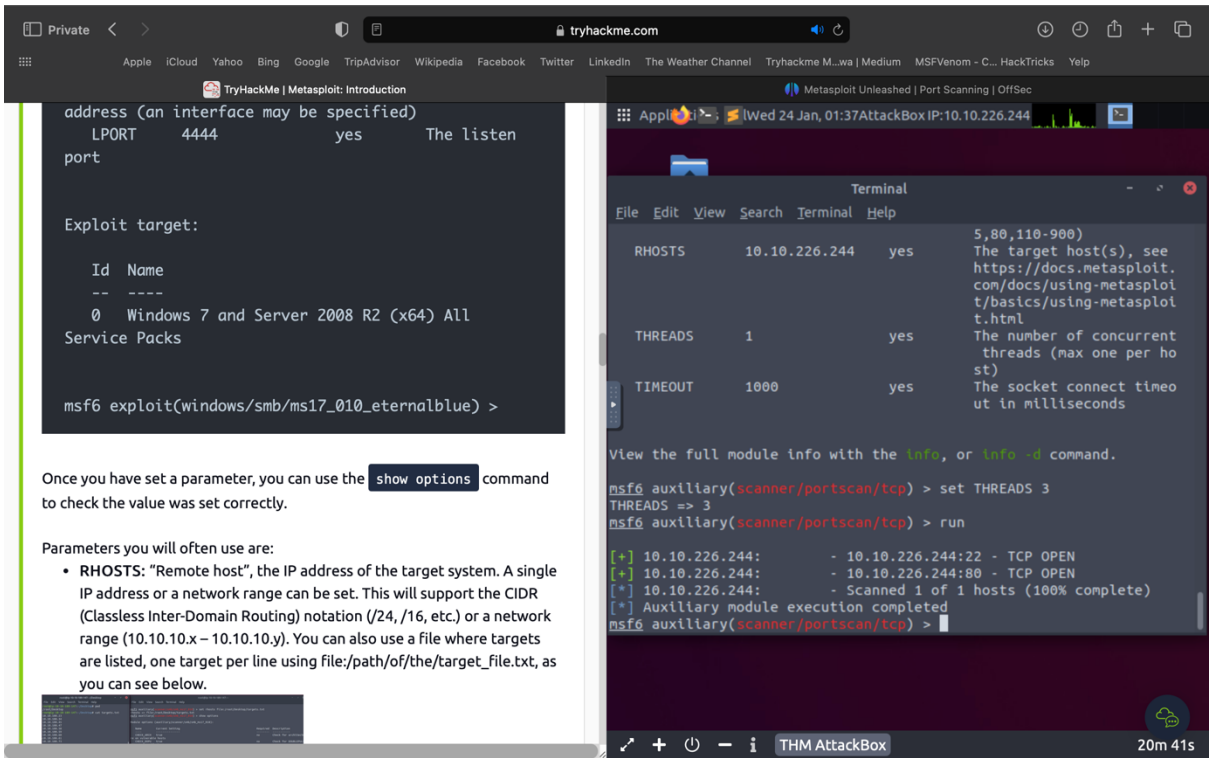
nmap -Pn -sI


tryhackme.com
TryHackMe | Metasploit: Introduction
Metasploit Unleashed | Port Scanning | OffSec
Wed 24 Jan, 01:32
AttackBox IP:10.10.226.244
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:'
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.
Terminal
File Edit View Search Terminal Help
RHOSTS => 192.168.1.0/24
msf6 auxiliary(scanner/ip/ipidseq) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/ip/ipidseq) > 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/ip/ipidseq) > 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 because it has not returned any of our probes -- perhaps it is down or
THM AttackBox
24m 32s

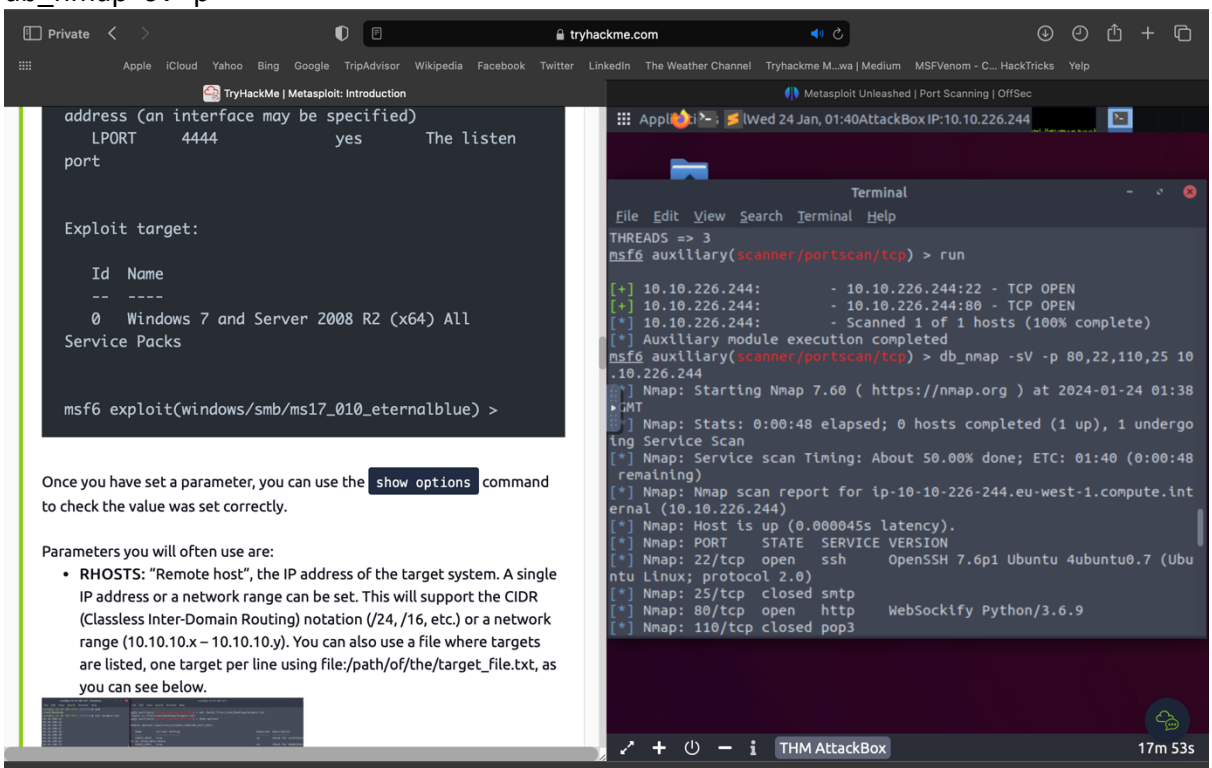
Back use auxiliary/scanner/portscan/tcp show options

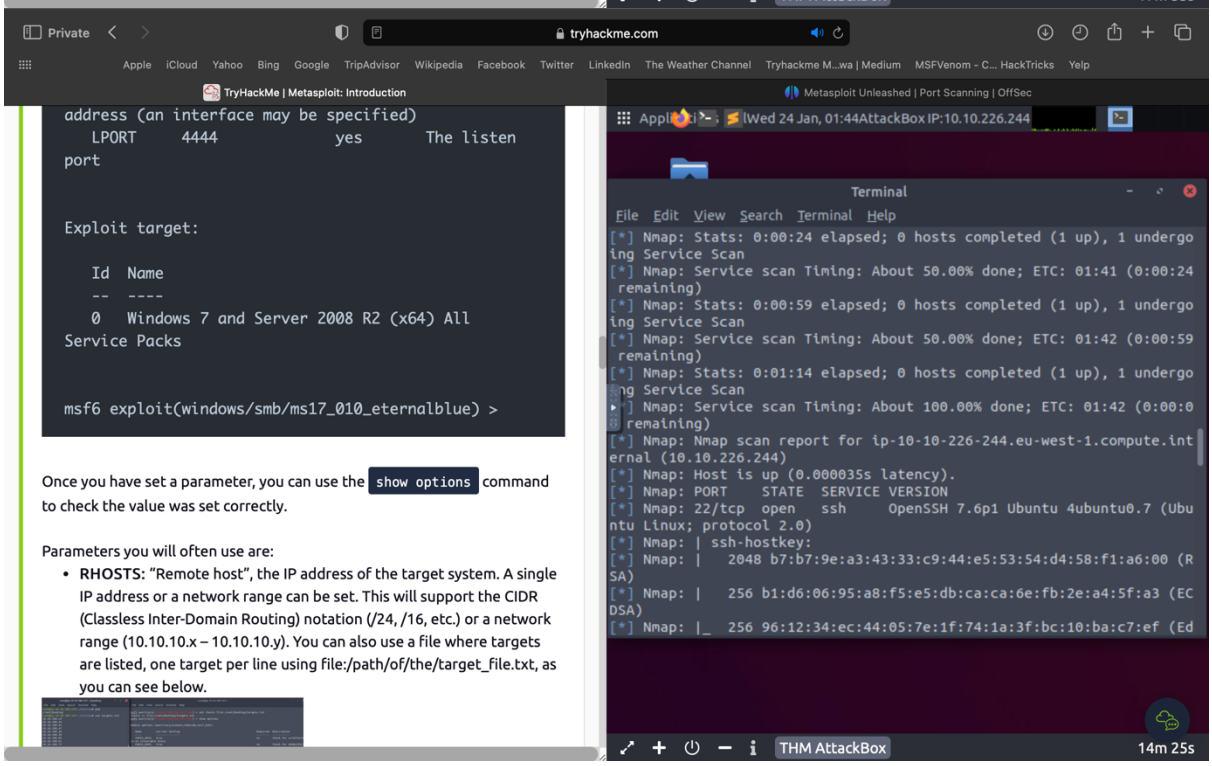


set threads and run

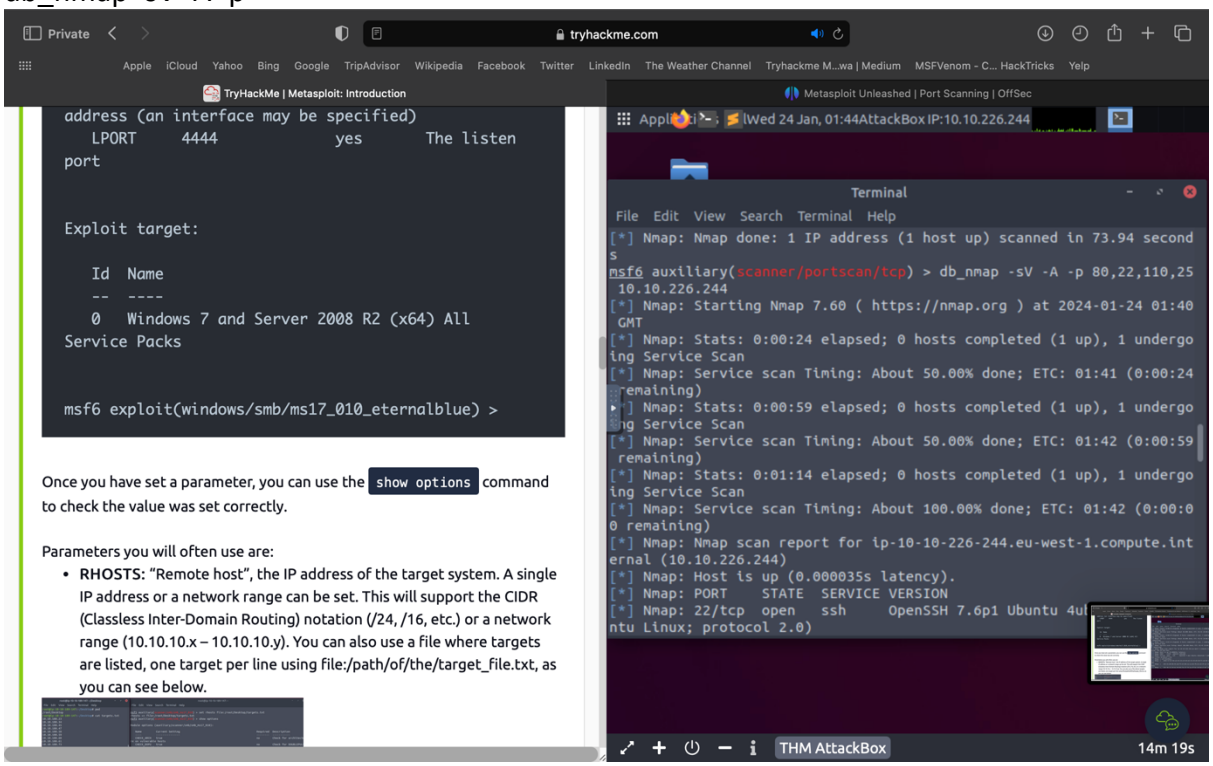


db_nmap -sV -p


Private
tryhackme.com
TryHackMe | Metasploit: Introduction
address (an 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
Wed 24 Jan, 01:40AttackBox IP:10.10.226.244
Terminal
File Edit View Search Terminal Help
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 80,22,110,25 10
.10.226.244
[*] Nmap: Starting Nmap 7.60 (https://nmap.org) at 2024-01-24 01:38
GMT
[*] Nmap: Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergo
ing Service Scan
[*] Nmap: Service scan Timing: About 50.00% done; ETC: 01:40 (0:00:48
remaining)
[*] Nmap: Nmap scan report for ip-10-10-226-244.eu-west-1.compute.int
ernal (10.10.226.244)
[*] Nmap: Host is up (0.000045s latency).
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubu
ntu Linux; protocol 2.0)
[*] Nmap: 25/tcp closed smtp
[*] Nmap: 80/tcp open http WebSockify Python/3.6.9
[*] Nmap: 110/tcp closed pop3
THM AttackBox
17m 53s


Private
tryhackme.com
TryHackMe | Metasploit: Introduction
address (an 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
Wed 24 Jan, 01:44AttackBox IP:10.10.226.244
Terminal
File Edit View Search Terminal Help
[*] Nmap: Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergo
ing Service Scan
[*] Nmap: Service scan Timing: About 50.00% done; ETC: 01:41 (0:00:24
remaining)
[*] Nmap: Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergo
ing Service Scan
[*] Nmap: Service scan Timing: About 50.00% done; ETC: 01:42 (0:00:59
remaining)
[*] Nmap: Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergo
ng Service Scan
[*] Nmap: Service scan Timing: About 100.00% done; ETC: 01:42 (0:00:0
remaining)
[*] Nmap: Nmap scan report for ip-10-10-226-244.eu-west-1.compute.int
ernal (10.10.226.244)
[*] Nmap: Host is up (0.000035s latency).
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubu
ntu Linux; protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: | 2048 b7:b7:9e:a3:43:33:c9:44:e5:53:54:d4:58:f1:a6:00 (R
SA)
[*] Nmap: | 256 b1:d6:06:95:a8:f5:e5:db:ca:ca:6e:fb:2e:a4:5f:a3 (EC
DSA)
[*] Nmap: |_ 256 96:12:34:ec:44:05:7e:1f:74:1a:3f:bc:10:ba:c7:ef (Ed
THM AttackBox
14m 25s

db_nmap -sV -A -p


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
address (an 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
Wed 24 Jan, 01:44AttackBox IP:10.10.226.244
Terminal
File Edit View Search Terminal Help
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 73.94 seconds
msf6 auxiliary(scanner/portscan/tcp) > db_nmap -sV -A -p 80,22,110,25 10.10.226.244
[*] Nmap: Starting Nmap 7.60 (https://nmap.org) at 2024-01-24 01:40 GMT
[*] Nmap: Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 50.00% done; ETC: 01:41 (0:00:24 remaining)
[*] Nmap: Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 50.00% done; ETC: 01:42 (0:00:59 remaining)
[*] Nmap: Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
[*] Nmap: Service scan Timing: About 100.00% done; ETC: 01:42 (0:00:00 remaining)
[*] Nmap: Nmap scan report for ip-10-10-226-244.eu-west-1.compute.internal (10.10.226.244)
[*] Nmap: Host is up (0.000035s latency).
[*] Nmap: PORT STATE SERVICE VERSION
[*] Nmap: 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4u
ntu Linux; protocol 2.0)
THM AttackBox
14m 19s