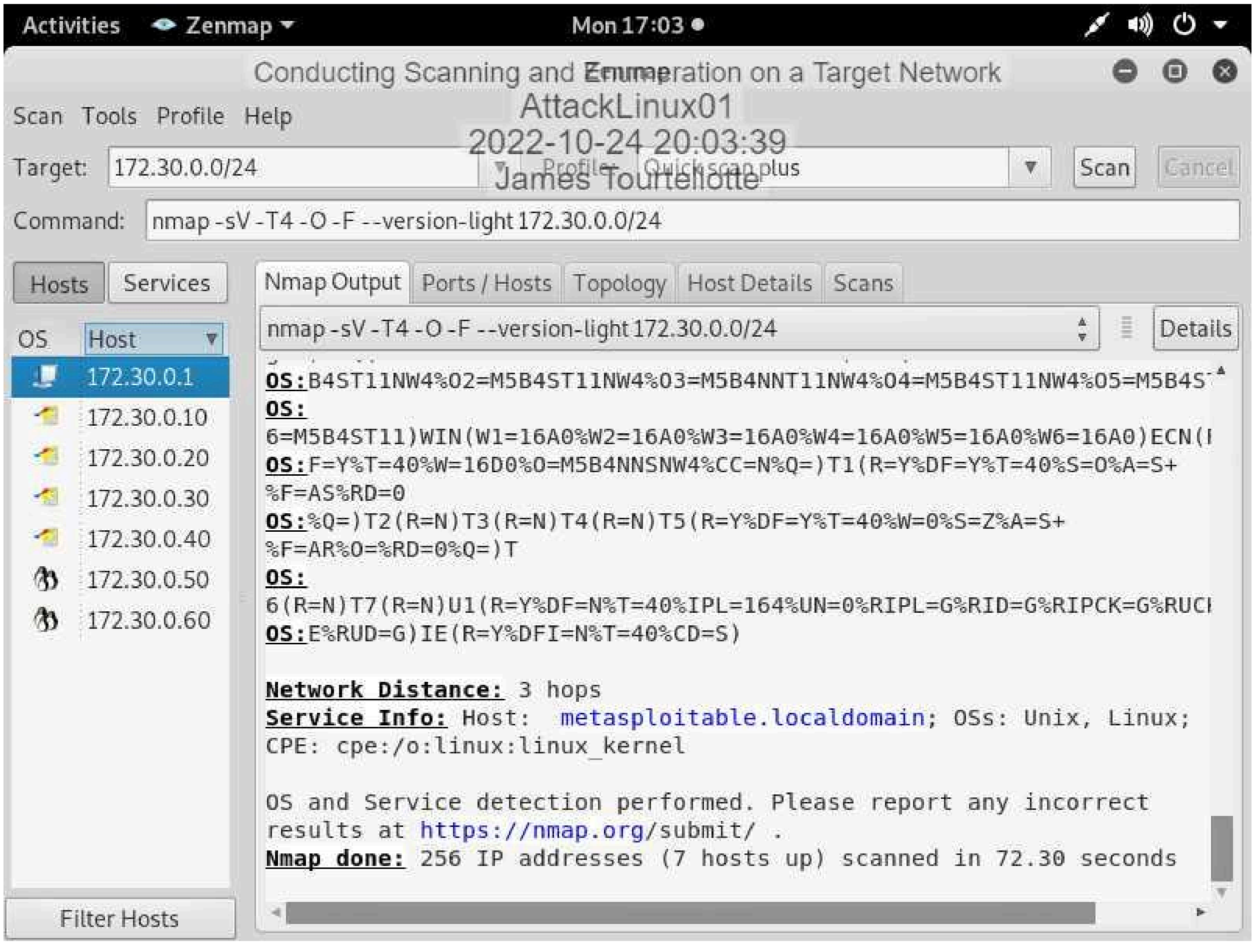
Table of Contents

SECTION 1

LAB #11 SCREEN CAPTURE 1:



Target: 172.30.0.0/24

Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 172.30.0.0/24

Hosts:

- 172.30.0.1
- 172.30.0.10
- 172.30.0.20
- 172.30.0.30
- 172.30.0.40
- 172.30.0.50
- 172.30.0.60

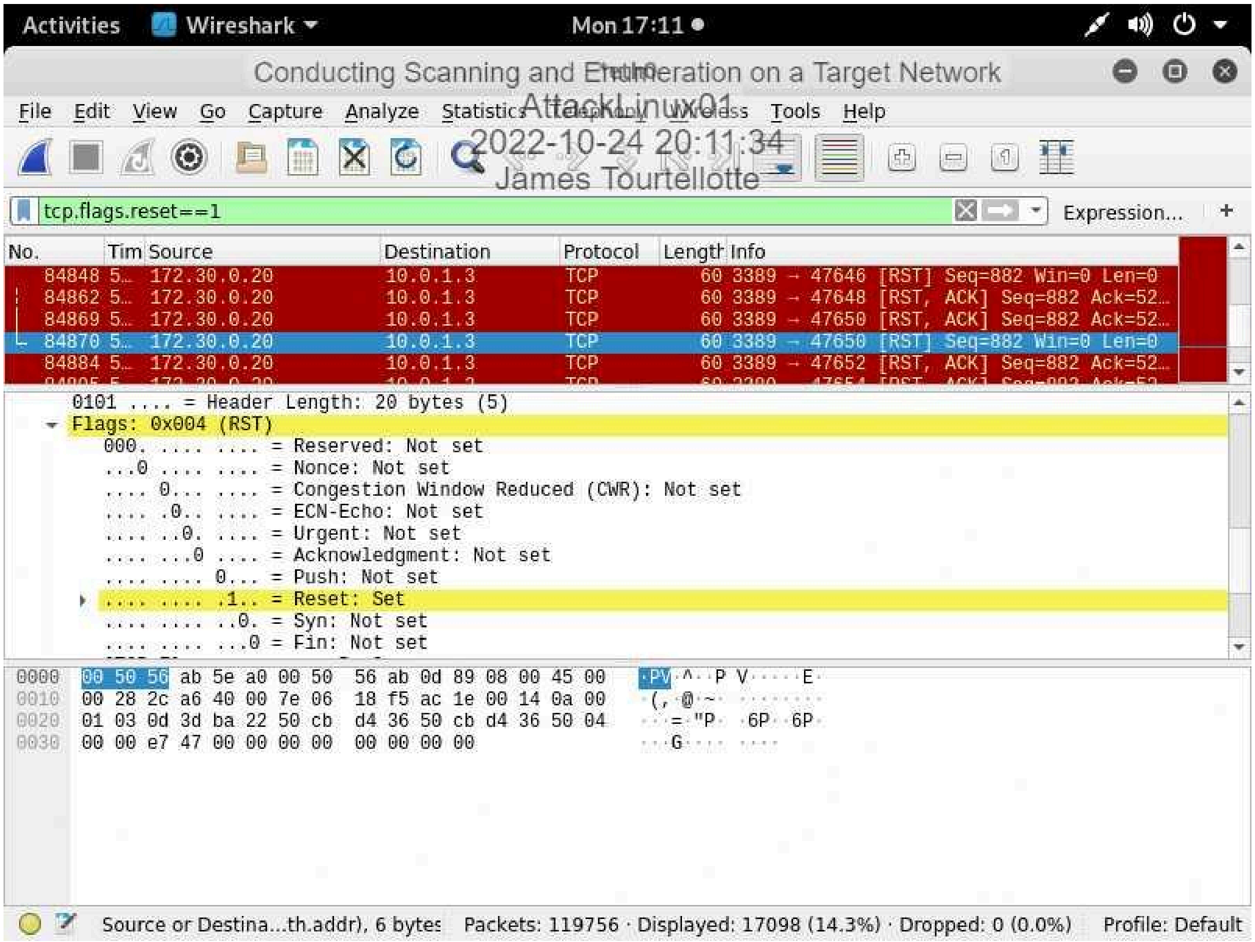
```
nmap -sV -T4 -O -F --version-light 172.30.0.0/24

OS:B4ST11NW4%O2=M5B4ST11NW4%O3=M5B4NNT11NW4%O4=M5B4ST11NW4%O5=M5B4S
OS:
6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(
OS:F=Y%T=40%W=16D0%O=M5B4NNSNW4%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)T
OS:
6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUC
OS:E%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 3 hops
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux;
CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 72.30 seconds
```

LAB #11 SCREEN CAPTURE 2:


Activities
Wireshark
Mon 17:11
Conducting Scanning and Enumeration on a Target Network
eth0
AttackLinux01
2022-10-24 20:11:34
James Tourtellotte
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
tcp.flags.reset==1
```

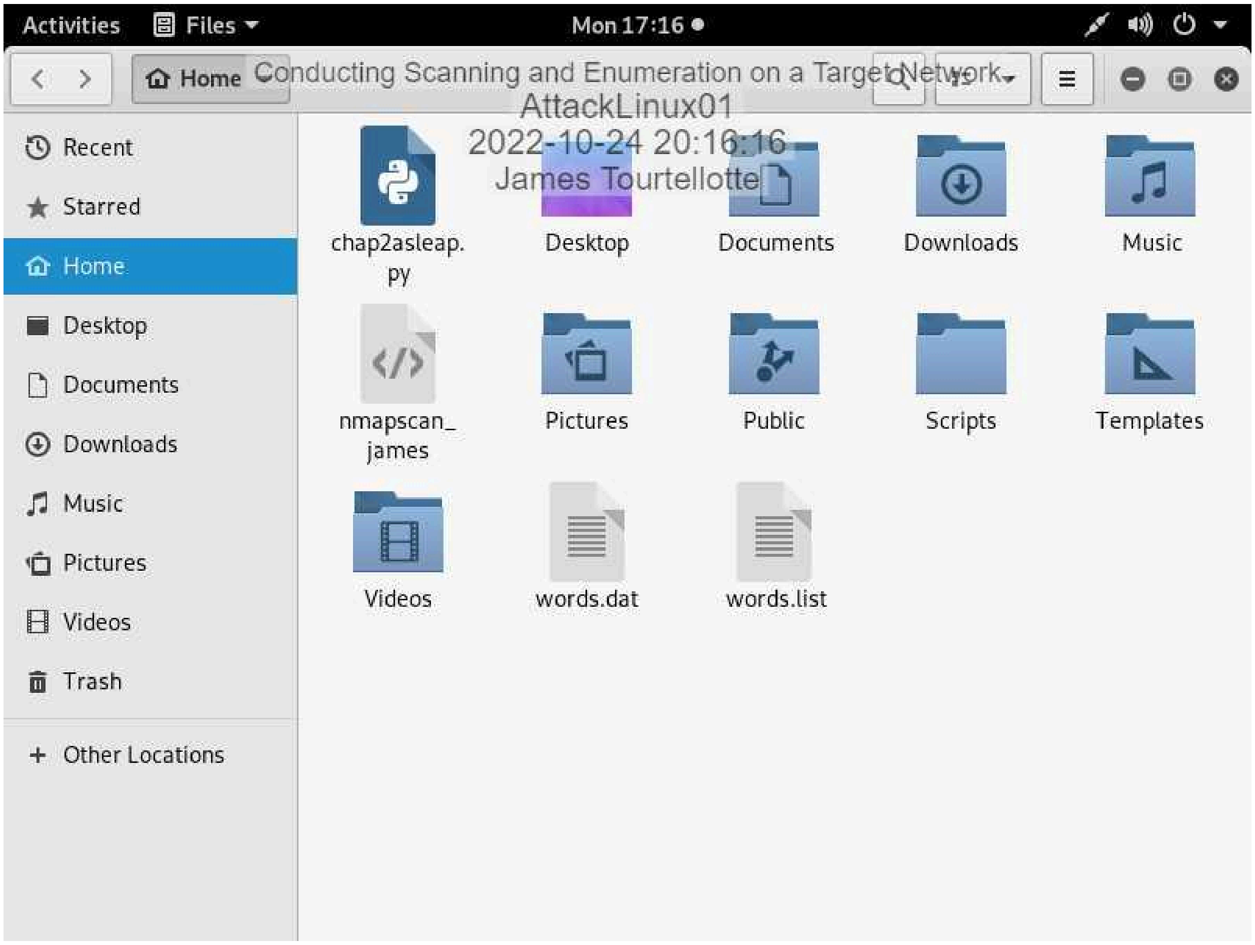
```
No.     Tim Source        Destination  Protocol  Length Info
  84848 5…  172.30.0.20   10.0.1.3     TCP       60 3389 → 47646 [RST] Seq=882 Win=0 Len=0
  84862 5…  172.30.0.20   10.0.1.3     TCP       60 3389 → 47648 [RST, ACK] Seq=882 Ack=52…
  84869 5…  172.30.0.20   10.0.1.3     TCP       60 3389 → 47650 [RST, ACK] Seq=882 Ack=52…
  84870 5…  172.30.0.20   10.0.1.3     TCP       60 3389 → 47650 [RST] Seq=882 Win=0 Len=0
  84884 5…  172.30.0.20   10.0.1.3     TCP       60 3389 → 47652 [RST, ACK] Seq=882 Ack=52…
```

```
    0101 .... = Header Length: 20 bytes (5)
  ▾ Flags: 0x004 (RST)
       000. .... .... = Reserved: Not set
       ...0 .... .... = Nonce: Not set
       .... 0... .... = Congestion Window Reduced (CWR): Not set
       .... .0.. .... = ECN-Echo: Not set
       .... ..0. .... = Urgent: Not set
       .... ...0 .... = Acknowledgment: Not set
       .... .... 0... = Push: Not set
     ▸ .... .... .1.. = Reset: Set
       .... .... ..0. = Syn: Not set
       .... .... ...0 = Fin: Not set
```

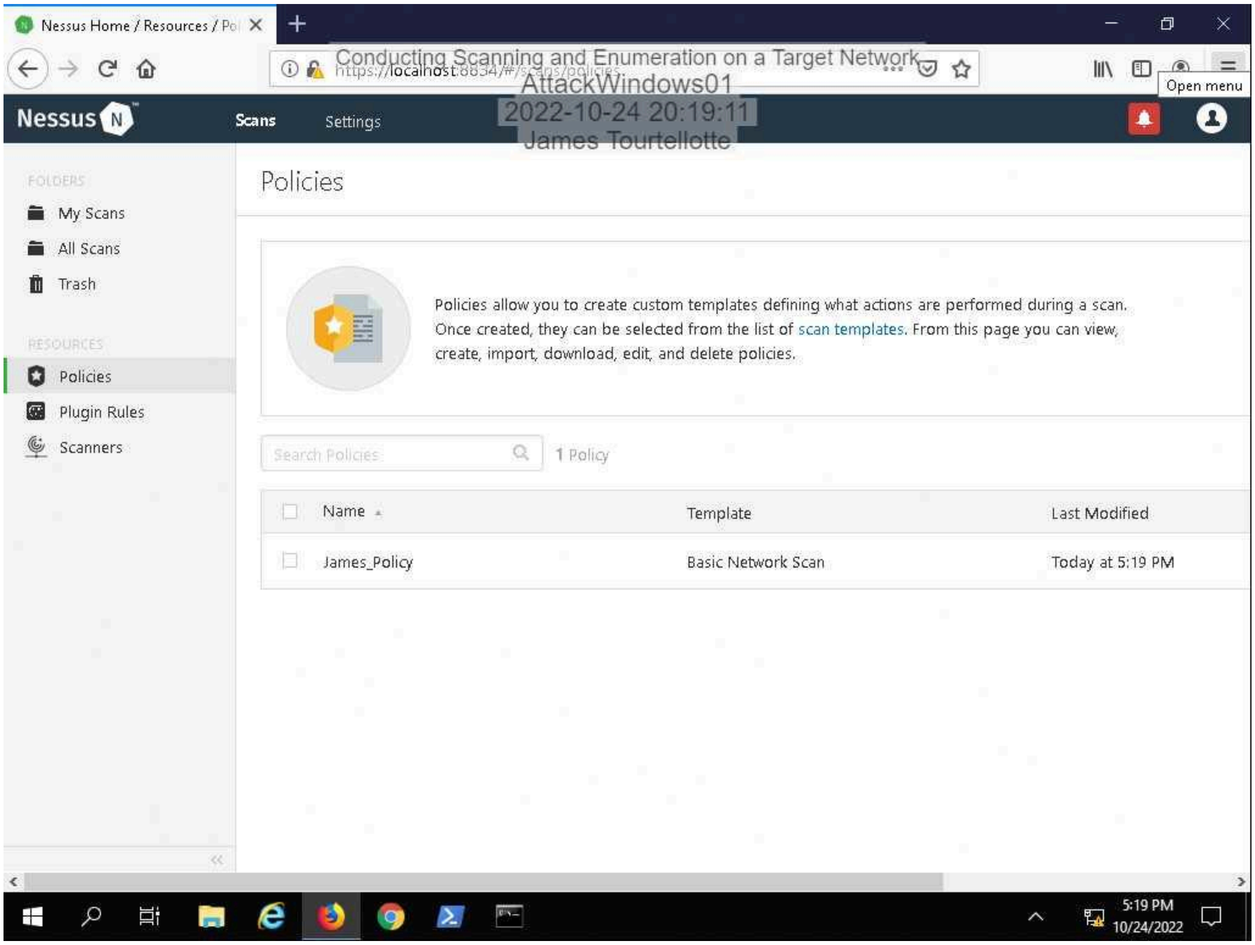
```
0000  00 50 56 ab 5e a0 00 50  56 ab 0d 89 08 00 45 00   ·PV·^··P V·····E·
0010  00 28 2c a6 40 00 7e 06  18 f5 ac 1e 00 14 0a 00   ·(,·@·~· ········
0020  01 03 0d 3d ba 22 50 cb  d4 36 50 cb d4 36 50 04   ···=·"P· ·6P··6P·
0030  00 00 e7 47 00 00 00 00  00 00 00 00               ···G···· ····
```

Source or Destina...th.addr), 6 bytes   Packets: 119756 · Displayed: 17098 (14.3%) · Dropped: 0 (0.0%)   Profile: Default

LAB #11 SCREEN CAPTURE 3:



LAB #11 SCREEN CAPTURE 4:



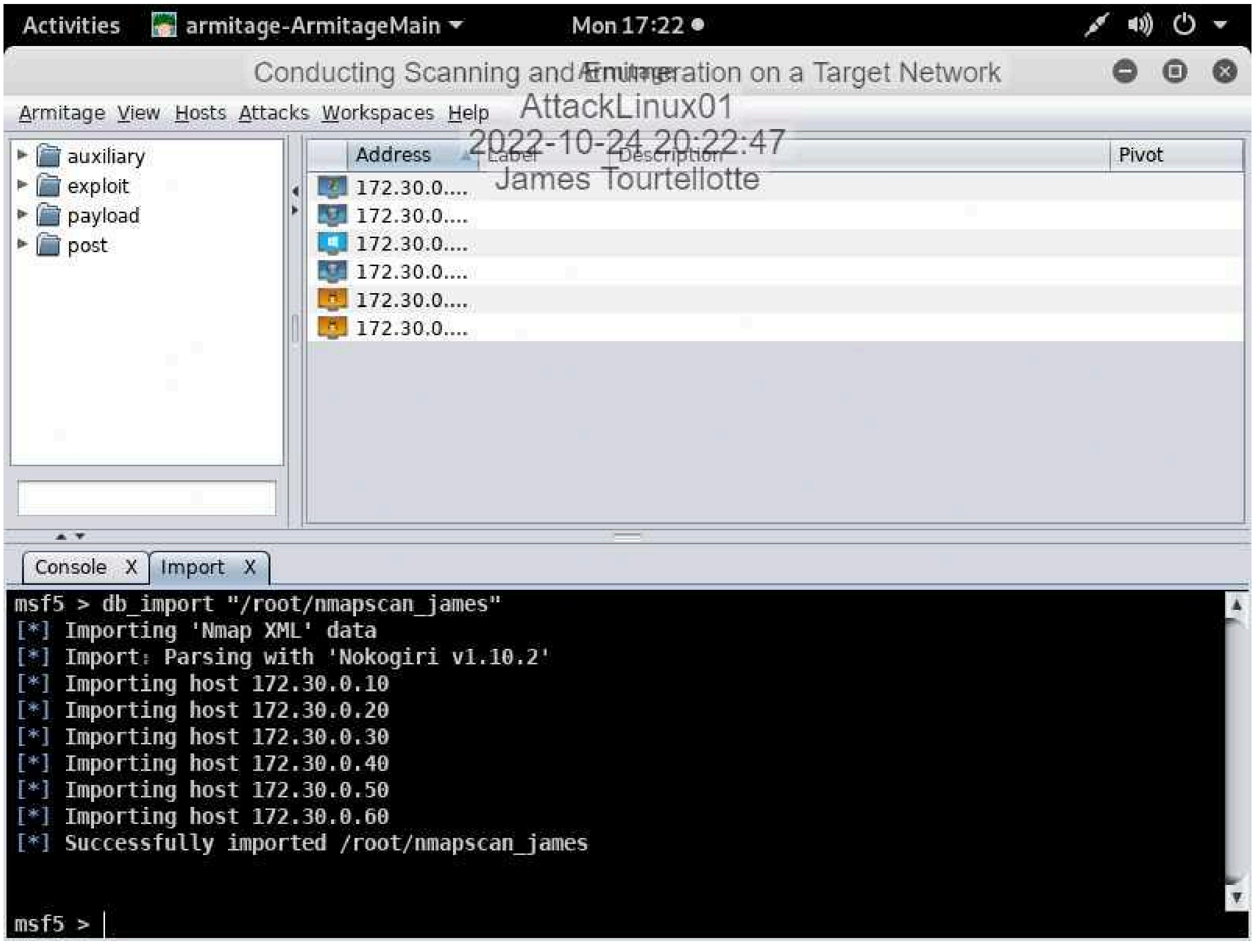
Conducting Scanning and Enumeration on a Target Network
AttackWindows01
2022-10-24 20:19:11
James Tourtellotte

Policies

Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.

□	Name	Template	Last Modified
□	James_Policy	Basic Network Scan	Today at 5:19 PM

LAB #11 SCREEN CAPTURE 5:



```
msf5 > db_import "/root/nmapscan_james"
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.10.2'
[*] Importing host 172.30.0.10
[*] Importing host 172.30.0.20
[*] Importing host 172.30.0.30
[*] Importing host 172.30.0.40
[*] Importing host 172.30.0.50
[*] Importing host 172.30.0.60
[*] Successfully imported /root/nmapscan_james

msf5 >
```