eJPT Lab : Network Discovery with Nmap, ARP-Scan and Netdiscover Paris Smith 7/1/25

Objective 1 1 **Tools Environment/Setup** 2 2 Methodology/Steps 2 Locate endpoints on a network Transfer files to and from target & Compile information from files on target 3 Setting up Secure Copy over SSH - Secure FIle Transfer to Host 3 **Lessons Learned/Reflection** 3 5 **Appendix** 5 Raw Output arp.txt 6 Raw Output scan2.txt Raw Output scan.txt 8 Raw Output netdiscover.txt 10

Objective

The goal of this lab is to demonstrate the ability to locate active endpoints on a local network using tools such as *arp-scan. netdiscover, and nmap*. This is aligned with eJPT's *Assessment Methodologies domain*: 'Locate endpoints on a network' and *Host and Networking Auditing*: 'Transfer files to and from target' & 'Compile information from files on target'

Tools

OS & Platforms

Win11 Desktop - Host

Proxmox Virtual Environment - via GUI @192.168.4.15

Kali Linux - Attacker VM @192.168.4.25

```
Network Discovery Tools
arp-scan
nmap
netdiscover
File Transfer / Remote Access
ssh
scp
```

Environment/Setup

The lab was executed in a Proxmox virtualized environment. The Kali Linux machine (192.168.4.25) acted as the attacker system. Multiple other devices—including routers, smart devices, and other endpoints—were present on the 192.168.4.0/24 subnet, simulating a real-world internal network.

Methodology/Steps

Locate endpoints on a network

The files and commands that produced them are listed below:

arp.txt - arp scan

```
(root@proxkali)=[~alcbec/Documents]6 ms
# arp-scan --interface=eth0 --localnet > arp.txt
```

scan.txt & scan2.txt - nmap ping sweep

```
(root® proxkali)-[~alcbec/Documents]
nmap -sn 192.168.4.0/24 > scan2.txt
```

```
root®proxkali)-[~alcbec/Documents]
nmap -sn 192.168.4.1/24 > scan.txt
```

netdiscover.txt - netdiscover passive listening

Transfer files to and from target & Compile information from files on target

Setting up Secure Copy over SSH - Secure FIle Transfer to Host

Within Kali: sudo systemetl start ssh

Within requesting machine: scp alcbec@192.168.4.25:~/Documents/'targetfile'.txt C:\Users\yourprofile\Downloads\

```
PowerShell 7 (x64)
PowerShell 7.5.2
PowerShell 7.5.2

PS C:\Users\ithin> scp alcbec@192.168.4.25:~/Documents/arp.txt

usage: scp [-346ABCOpqRrsTv] [-c cipher] [-D sftp_server_path] [-F ssh_config]

[-i identity_file] [-J destination] [-l limit] [-o ssh_option]

[-P port] [-S program] [-X sftp_option] source ... target

PS C:\Users\ithin> scp alcbec@192.168.4.25:~/Documents/arp.txt C:\Users\ithin\Downloads

The authenticity of host '192.168.4.25 (192.168.4.25)' can't be established.
ED25519 key fingerprint is SHA256:NpCuK3rnqPtt0B8BxoDsD5UQU/hpAbc+GlFmN+QMOSI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Please type 'yes', 'no' or the fingerprint:
Warning: Permanently added '192.168.4.25' (ED25519) to the list of known hosts.
alcbec@192.168.4.25's password:
                                                                                                                                  100% 1656
                                                                                                                                                  161.7KB/s
                                                                                                                                                                     00:00
PS C:\Users\ithin> scp alcbec@192.168.4.25:~/Documents/scan.txt C:\Users\ithin\Downloads
alcbec@192.168.4.25's password:
                                                                                                                                  100% 2952 240.2KB/s
                                                                                                                                                                     00:00
PS C:\Users\ithin> scp alcbec@192.168.4.25:~/Documents/scan2.txt C:\Users\ithin\Downloads
alcbec@192.168.4.25's password:
                                                                                                                                  100% 3089
                                                                                                                                                   430.9KB/s
 PS C:\Users\ithin> scp alcbec@192.168.4.25:~/Documents/netdiscover.txt C:\Users\ithin\Downloads
alcbec@192.168.4.25's password:
netdiscover.txt
                                                                                                                                 100% 5069KB 12.6MB/s
PS C:\Users\ithin>
```

Lessons Learned/Reflection

- Installing VMs takes forever (talking to you kali & parrotOS)
- Netdiscover was nice to list/discover devices by listening for arp requests on the LAN passively. Enabled with ability to have insights in volume, mac address ip and vendor.
- Arp-scan can send requests and record their responses with ip/mac info to enumerate active devices for ip address, mac address and vendor
- Nmap -sn performed host discovery using an ARP request determining who has IPs within the subnet, logging up IPs and their MAC addresses & vendor

Appendix

Raw Output arp.txt

```
Interface: eth0, type: EN10MB, MAC: bc:24:11:f4:cb:25, IPv4: 192.168.4.25
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.4.1 30:57:8e:5d:ff:12 eero inc.
                  04:d4:c4:6f:53:2d ASUSTek COMPUTER INC.
192.168.4.15
192.168.4.20
                  04:d4:c4:8f:4c:22 ASUSTek COMPUTER INC.
192.168.4.57
                  c8:34:8e:53:ca:5d Intel Corporate
                  40:a9:cf:d7:6c:d8 Amazon Technologies Inc.
192.168.4.40
192.168.4.66
                  ec:8a:c4:01:16:a4 Amazon Technologies Inc.
192.168.4.53
                  08:7c:39:02:e5:2e Amazon Technologies Inc.
192.168.4.52
                  c8:3a:6b:e5:62:f4 Roku, Inc
                  88:57:1d:7d:57:aaSeongji Industry Company
192.168.4.22
192.168.4.36
                  c8:47:8c:10:37:76 Beken Corporation
192.168.4.35
                  c8:47:8c:01:31:43 Beken Corporation
                  c8:47:8c:01:31:86 Beken Corporation
192.168.4.37
                  10:59:32:eb:1f:1b Roku, Inc
192.168.4.54
                  c8:34:8e:53:ca:5d Intel Corporate (DUP: 2)
192.168.4.57
                  cc:6a:10:28:2a:67 The Chamberlain Group, Inc
192.168.4.41
                  40:ca:63:c3:3b:7a Seongji Industry Company
192.168.4.50
192.168.4.51
                  40:ca:63:bf:f8:5e Seongji Industry Company
192.168.4.64
                  70:89:76:c7:c8:cb Tuya Smart Inc.
192.168.4.67
                  c8:47:8c:40:2b:2c Beken Corporation
192.168.4.84
                  6c:29:90:f9:b6:3c WiZ Connected Lighting Company Limited
192.168.4.91
                  2c:aa:8e:58:41:87 Wyze Labs Inc
                  2c:aa:8e:3c:c7:b9 Wyze Labs Inc
192.168.4.73
192.168.4.57
                  c8:34:8e:53:ca:5d Intel Corporate (DUP: 3)
                  c8:34:8e:53:ca:5d Intel Corporate (DUP: 4)
192.168.4.57
                  c8:34:8e:53:ca:5d Intel Corporate (DUP: 5)
192.168.4.57
192.168.4.57
                  c8:34:8e:53:ca:5d Intel Corporate (DUP: 6)
```

26 packets received by filter, 0 packets dropped by kernel Ending arp-scan 1.10.0: 256 hosts scanned in 4.331 seconds (59.11 hosts/sec). 21 responded

Raw Output scan2.txt

Starting Nmap 7.94SVN (https://nmap.org) at 2025-07-02 01:49 EDT

Nmap scan report for 192.168.4.1

Host is up $(0.023s \ latency)$.

MAC Address: 30:57:8E:5D:FF:12 (eero)

Nmap scan report for 192.168.4.15

Host is up $(0.00022s \ latency)$.

MAC Address: 04:D4:C4:6F:53:2D (ASUSTek Computer)

Nmap scan report for 192.168.4.20

Host is up $(0.0022s \ latency)$.

MAC Address: 04:D4:C4:8F:4C:22 (ASUSTek Computer)

Nmap scan report for 192.168.4.22

Host is up (0.12s latency).

MAC Address: 88:57:1D:7D:57:AA (Seongji Industry Company)

Nmap scan report for 192.168.4.35

Host is up (0.023s latency).

MAC Address: C8:47:8C:01:31:43 (Beken)

Nmap scan report for 192.168.4.36

Host is up (0.066s latency).

MAC Address: C8:47:8C:10:37:76 (Beken)

Nmap scan report for 192.168.4.37

Host is up (0.090s latency).

MAC Address: C8:47:8C:01:31:86 (Beken)

Nmap scan report for 192.168.4.40

Host is up (1.4s latency).

MAC Address: 40:A9:CF:D7:6C:D8 (Amazon Technologies)

Nmap scan report for 192.168.4.41

Host is up (0.10s latency).

MAC Address: CC:6A:10:28:2A:67 (The Chamberlain Group)

Nmap scan report for 192.168.4.50

Host is up (0.11s latency).

MAC Address: 40:CA:63:C3:3B:7A (Seongji Industry Company)

Nmap scan report for 192.168.4.51

Host is up (0.098s latency).

MAC Address: 40:CA:63:BF:F8:5E (Seongji Industry Company)

Nmap scan report for 192.168.4.53

Host is up (0.14s latency).

MAC Address: 08:7C:39:02:E5:2E (Amazon Technologies)

Nmap scan report for 192.168.4.54

Host is up $(0.047s \ latency)$.

MAC Address: 10:59:32:EB:1F:1B (Roku)

Nmap scan report for 192.168.4.57

Host is up.

MAC Address: C8:34:8E:53:CA:5D (Intel Corporate)

Nmap scan report for 192.168.4.64

Host is up (0.060s latency).

MAC Address: 70:89:76:C7:C8:CB (Tuya Smart)

Nmap scan report for 192.168.4.66

Host is up (0.0084s latency).

MAC Address: EC:8A:C4:01:16:A4 (Amazon Technologies)

Nmap scan report for 192.168.4.67

Host is up (0.056s latency).

MAC Address: C8:47:8C:40:2B:2C (Beken)

Nmap scan report for 192.168.4.73

Host is up (0.12s latency).

MAC Address: 2C:AA:8E:3C:C7:B9 (Wyze Labs)

Nmap scan report for 192.168.4.82

Host is up $(0.035s \ latency)$.

MAC Address: D8:EB:46:B1:61:1E (Google)

Nmap scan report for 192.168.4.84

Host is up (0.19s latency).

MAC Address: 6C:29:90:F9:B6:3C (WiZ Connected Lighting Company Limited)

Nmap scan report for 192.168.4.85

Host is up $(0.038s \ latency)$.

MAC Address: A8:BB:50:83:1B:11 (WiZ IoT Company Limited)

Nmap scan report for 192.168.4.86

Host is up (0.19s latency).

MAC Address: A8:BB:50:C3:D7:82 (WiZ IoT Company Limited)

Nmap scan report for 192.168.4.88

Host is up $(0.097s \ latency)$.

MAC Address: A8:BB:50:C3:AC:49 (WiZ IoT Company Limited)

Nmap scan report for 192.168.4.89

Host is up (0.18s latency).

MAC Address: A8:BB:50:E5:D6:A8 (WiZ IoT Company Limited)

Nmap scan report for 192.168.4.90

Host is up (0.19s latency).

MAC Address: A8:BB:50:C3:AC:A6 (WiZ IoT Company Limited)

Nmap scan report for 192.168.4.91

Host is up $(0.033s \ latency)$.

MAC Address: 2C:AA:8E:58:41:87 (Wyze Labs)

Nmap scan report for 192.168.4.25

Host is up.

Nmap done: 256 IP addresses (27 hosts up) scanned in 10.57 seconds

Raw Output scan.txt

Starting Nmap 7.94SVN (https://nmap.org) at 2025-07-02 01:43 EDT

Nmap scan report for 192.168.4.1

Host is up (0.0052s latency).

MAC Address: 30:57:8E:5D:FF:12 (eero)

Nmap scan report for 192.168.4.15

Host is up (0.00028s *latency*).

MAC Address: 04:D4:C4:6F:53:2D (ASUSTek Computer)

Nmap scan report for 192.168.4.20

Host is up $(0.0015s \ latency)$.

MAC Address: 04:D4:C4:8F:4C:22 (ASUSTek Computer)

Nmap scan report for 192.168.4.35

Host is up (0.078s latency).

MAC Address: C8:47:8C:01:31:43 (Beken)

Nmap scan report for 192.168.4.36

Host is up (0.098s latency).

MAC Address: C8:47:8C:10:37:76 (Beken)

Nmap scan report for 192.168.4.37

Host is up (0.084s latency).

MAC Address: C8:47:8C:01:31:86 (Beken)

Nmap scan report for 192.168.4.40

Host is up $(0.0023s \ latency)$.

MAC Address: 40:A9:CF:D7:6C:D8 (Amazon Technologies)

Nmap scan report for 192.168.4.41

Host is up (0.099s latency).

MAC Address: CC:6A:10:28:2A:67 (The Chamberlain Group)

Nmap scan report for 192.168.4.50

Host is up (0.088s latency).

MAC Address: 40:CA:63:C3:3B:7A (Seongji Industry Company)

Nmap scan report for 192.168.4.51

Host is up (0.092s latency).

MAC Address: 40:CA:63:BF:F8:5E (Seongji Industry Company)

Nmap scan report for 192.168.4.52

Host is up (0.14s latency).

MAC Address: C8:3A:6B:E5:62:F4 (Roku)

Nmap scan report for 192.168.4.53

Host is up (0.14s latency).

MAC Address: 08:7C:39:02:E5:2E (Amazon Technologies)

Nmap scan report for 192.168.4.54

Host is up (0.19s latency).

MAC Address: 10:59:32:EB:1F:1B (Roku)

Nmap scan report for 192.168.4.57

Host is up.

MAC Address: C8:34:8E:53:CA:5D (Intel Corporate)

Nmap scan report for 192.168.4.64

Host is up $(0.15s \ latency)$.

MAC Address: 70:89:76:C7:C8:CB (Tuya Smart)

Nmap scan report for 192.168.4.66

Host is up $(0.0056s \ latency)$.

MAC Address: EC:8A:C4:01:16:A4 (Amazon Technologies)

Nmap scan report for 192.168.4.67

Host is up (0.099s latency).

MAC Address: C8:47:8C:40:2B:2C (Beken)

Nmap scan report for 192.168.4.73

Host is up (0.16s latency).

MAC Address: 2C:AA:8E:3C:C7:B9 (Wyze Labs)

Nmap scan report for 192.168.4.82

Host is up (0.056s latency).

MAC Address: D8:EB:46:B1:61:1E (Google)

Nmap scan report for 192.168.4.84

Host is up (0.19s latency).

MAC Address: 6C:29:90:F9:B6:3C (WiZ Connected Lighting Company Limited)

Nmap scan report for 192.168.4.85

Host is up (0.029s latency).

MAC Address: A8:BB:50:83:1B:11 (WiZ IoT Company Limited)

Nmap scan report for 192.168.4.86

Host is up (0.19s latency).

MAC Address: A8:BB:50:C3:D7:82 (WiZ IoT Company Limited)

Nmap scan report for 192.168.4.88

Host is up $(0.071s \ latency)$.

MAC Address: A8:BB:50:C3:AC:49 (WiZ IoT Company Limited)

Nmap scan report for 192.168.4.90

Host is up (0.18s latency).

MAC Address: A8:BB:50:C3:AC:A6 (WiZ IoT Company Limited)

Nmap scan report for 192.168.4.91

Host is up (0.19s latency).

MAC Address: 2C:AA:8E:58:41:87 (Wyze Labs)

Nmap scan report for 192.168.4.25

Host is up.

Nmap done: 256 IP addresses (26 hosts up) scanned in 4.04 seconds

Raw Output netdiscover.txt

1245 Captured ARP Req/Rep packets, from 35 hosts. Total size: 90614

```
192.168.4.15
              04:d4:c4:6f:53:2d
                                       42 ASUSTek COMPUTER INC.
                                  1
192.168.4.20
              04:d4:c4:8f:4c:22
                                  5
                                      300 ASUSTek COMPUTER INC.
              40:a9:cf:d7:6c:d8
192.168.4.40
                                  23
                                      1646 Amazon Technologies Inc.
                                      1202 Amazon Technologies Inc.
192.168.4.66
              ec:8a:c4:01:16:a4
                                  17
                                       60 The Chamberlain Group, Inc
192.168.4.41
              cc:6a:10:28:2a:67
                                  1
              c8:3a:6b:e5:62:f4
192.168.4.52
                                  1
                                      60 Roku. Inc
192.168.4.53
              08:7c:39:02:e5:2e
                                  1
                                       60 Amazon Technologies Inc.
192.168.4.82
              d8:eb:46:b1:61:1e
                                  1
                                       60 Google, Inc.
              40:ca:63:bf:f8:5e
                                      60 Seongji Industry Company
192.168.4.51
                                  1
192.168.4.50
              40:ca:63:c3:3b:7a
                                   2
                                      120 Seongji Industry Company
192.168.4.22
              88:57:1d:7d:57:aa
                                  75
                                      5536 Seongji Industry Company
              c8:47:8c:10:37:76
192.168.4.36
                                   3
                                      208 Beken Corporation
              c8:47:8c:01:31:43
192.168.4.35
                                       874 Beken Corporation
                                  12
192.168.4.37
              c8:47:8c:01:31:86
                                   8
                                      578 Beken Corporation
192.168.4.54
              10:59:32:eb:1f:1b
                                  2
                                      134 Roku, Inc
192.168.4.57
              c8:34:8e:53:ca:5d
                                  1
                                       60 Intel Corporate
192.168.4.64
              70:89:76:c7:c8:ch
                                      282 Tuya Smart Inc.
                                   4
192.168.4.67
              c8:47:8c:40:2b:2c
                                   7
                                      504 Beken Corporation
              2c:aa:8e:3c:c7:b9
192.168.4.73
                                  1
                                       60 Wyze Labs Inc
              38:1f:8d:ab:0f:d6
192.168.4.34
                                 12
                                      888 Tuya Smart Inc.
9
                                      666 Unknown vendor
192.168.6.103
               7c:78:b2:ca:04:a7
                                   24
                                       1776 Wyze Labs Inc
              6c:29:90:f9:b6:3c
                                      1924 WiZ Connected Lighting Company
192.168.4.84
                                  26
Limited
                                       962 Beken Corporation
192.168.4.33
              c8:47:8c:30:29:6c
                                  13
192.168.4.68
              c8:47:8c:40:2a:02
                                  16
                                      1184 Beken Corporation
              fc:d7:49:2d:3f:6b
                                      1586 Amazon Technologies Inc.
```

22

192.168.6.70