COMP 8506 Assignment 2

Active and Passive Network Reconnaissance Techniques

Xinghua Wei

A00978597

Nmap ... 3

Introduction ... 3

Task 1 – Decoy ... 3

Task 2 – Decoy and RND ... 5

Defense ... 6

Conclusion ... 7

Netdiscover ... 7

Introduction ... 7

Task 1 – Active Scan ... 7

Task 2 – Passive Scan ... 8

Possible Ways to Block ... 9

Conclusion ... 10

Sparta ... 10

Introduction ... 10

Task 1 – Penetrating Network ... 10

Defense ... 13

Conclusion ... 13

Enumeration Techniques - Dumpsec ... 13

Introduction ... 13

Task – Dump information of my Windows PC ... 14

Defense ... 16

Conclusion ... 16

Maltego ... 16

Introduction ... 16

Task 1 – My Network ... 16

Defense ... 19

Conclusion ... 19

Nmap

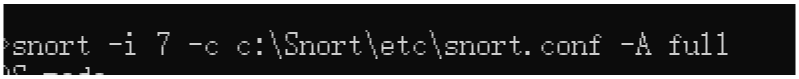
Introduction

Nmap is a free and open-source tool for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network. It is the tool to scan the network rapidly. In this exercise, I will use the Nmap decoy scan function which generates large scans with different IP addresses to confuse the target. this can be defeated through router path tracing, response-dropping, and other active mechanisms, it is generally an effective technique for hiding your IP address. Also, use RND to generate a random IP address.

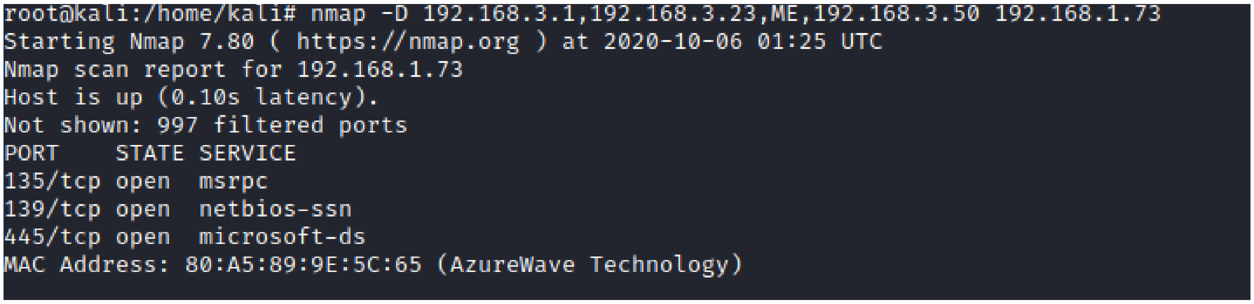
Task 1 – Decoy

A decoy scan will scan the remote target network with different unique IP addresses. Thus IDS will report different IP addresses but they won't know which IP was scanning them and which were decoys.

In this case, I use 192.168.3.1, 192.168.3.23 and 192.168.3.50 as my decoys, and 192.168.1.98(ME) will be positioned in the third position. My target network is 192.168.1.73. The IDS I use is Snort with command:

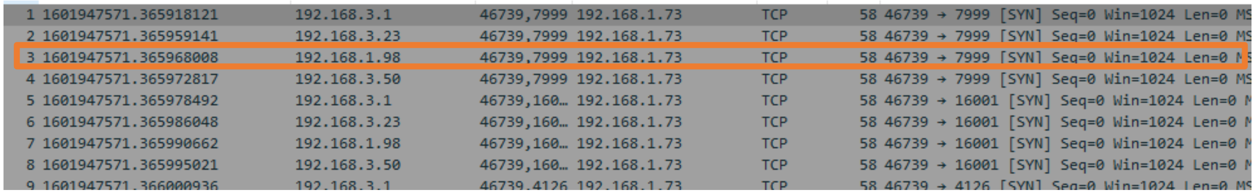


```
snort -i 7 -c c:\Snort\etc\snort.conf -A full
```



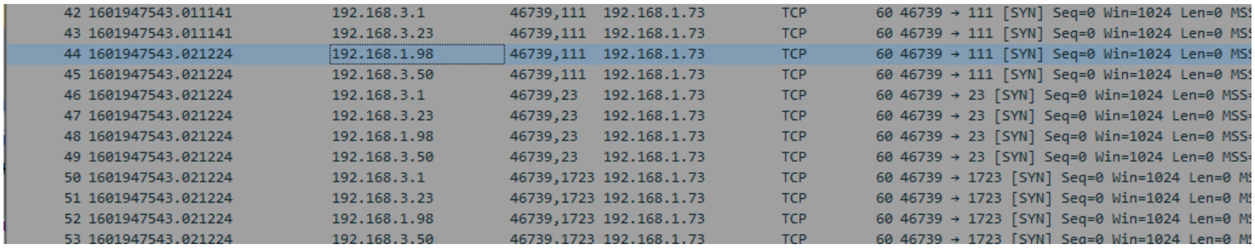
```
root@kali:/home/kali# nmap -D 192.168.3.1,192.168.3.23,ME,192.168.3.50 192.168.1.73
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-06 01:25 UTC
Nmap scan report for 192.168.1.73
Host is up (0.10s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 80:A5:89:9E:5C:65 (AzureWave Technology)
```

From the attacker machine, we can tell our IP shows up every 3rd request. And every other decoy is scanning either.



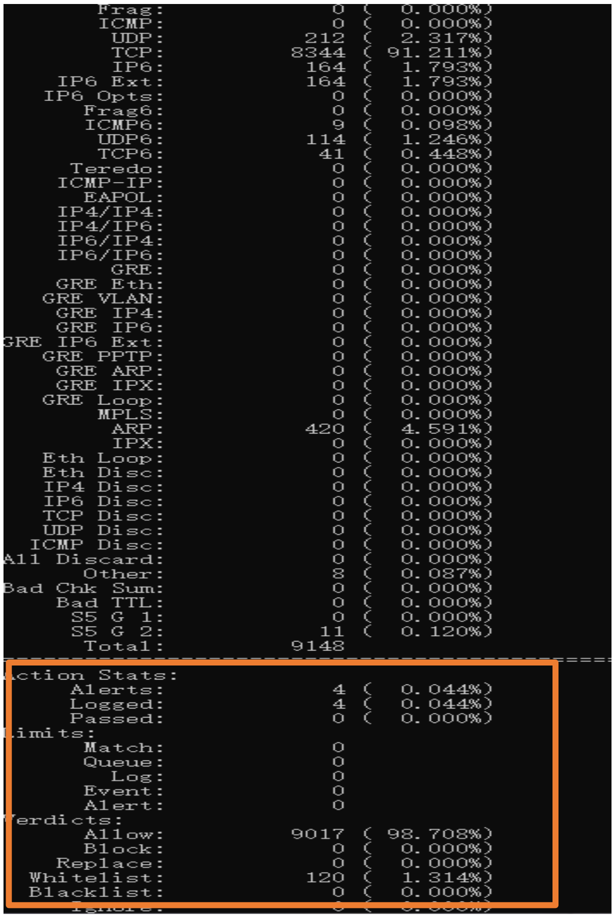
```
1 1601947571.365918121    192.168.3.1     46739,7999 192.168.1.73    TCP    58 46739 → 7999 [SYN] Seq=0 Win=1024 Len=0 MS
2 1601947571.365959141    192.168.3.23    46739,7999 192.168.1.73    TCP    58 46739 → 7999 [SYN] Seq=0 Win=1024 Len=0 MS
3 1601947571.365968008    192.168.1.98    46739,7999 192.168.1.73    TCP    58 46739 → 7999 [SYN] Seq=0 Win=1024 Len=0 MS
4 1601947571.365972817    192.168.3.50    46739,7999 192.168.1.73    TCP    58 46739 → 7999 [SYN] Seq=0 Win=1024 Len=0 MS
5 1601947571.365978492    192.168.3.1     46739,160… 192.168.1.73    TCP    58 46739 → 16001 [SYN] Seq=0 Win=1024 Len=0 M
6 1601947571.365986048    192.168.3.23    46739,160… 192.168.1.73    TCP    58 46739 → 16001 [SYN] Seq=0 Win=1024 Len=0 M
7 1601947571.365990662    192.168.1.98    46739,160… 192.168.1.73    TCP    58 46739 → 16001 [SYN] Seq=0 Win=1024 Len=0 M
8 1601947571.365995021    192.168.3.50    46739,160… 192.168.1.73    TCP    58 46739 → 16001 [SYN] Seq=0 Win=1024 Len=0 M
9 1601947571.366000936    192.168.3.1     46739,4126 192.168.1.73    TCP    58 46739 → 4126 [SYN] Seq=0 Win=1024 Len=0 MS
```

On the target machine side, it receives multiple SYN from 4 unique IP addresses where the IDS won't be able to know which IP is scanning them.



```
42 1601947543.011141    192.168.3.1     46739,111  192.168.1.73    TCP    60 46739 → 111 [SYN] Seq=0 Win=1024 Len=0 MS
43 1601947543.011141    192.168.3.23    46739,111  192.168.1.73    TCP    60 46739 → 111 [SYN] Seq=0 Win=1024 Len=0 MS
44 1601947543.021224    192.168.1.98    46739,111  192.168.1.73    TCP    60 46739 → 111 [SYN] Seq=0 Win=1024 Len=0 MS
45 1601947543.021224    192.168.3.50    46739,111  192.168.1.73    TCP    60 46739 → 111 [SYN] Seq=0 Win=1024 Len=0 MS
46 1601947543.021224    192.168.3.1     46739,23   192.168.1.73    TCP    60 46739 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS
47 1601947543.021224    192.168.3.23    46739,23   192.168.1.73    TCP    60 46739 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS
48 1601947543.021224    192.168.1.98    46739,23   192.168.1.73    TCP    60 46739 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS
49 1601947543.021224    192.168.3.50    46739,23   192.168.1.73    TCP    60 46739 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS
50 1601947543.021224    192.168.3.1     46739,1723 192.168.1.73    TCP    60 46739 → 1723 [SYN] Seq=0 Win=1024 Len=0 M
51 1601947543.021224    192.168.3.23    46739,1723 192.168.1.73    TCP    60 46739 → 1723 [SYN] Seq=0 Win=1024 Len=0 M
52 1601947543.021224    192.168.1.98    46739,1723 192.168.1.73    TCP    60 46739 → 1723 [SYN] Seq=0 Win=1024 Len=0 M
53 1601947543.021224    192.168.3.50    46739,1723 192.168.1.73    TCP    60 46739 → 1723 [SYN] Seq=0 Win=1024 Len=0 M
```

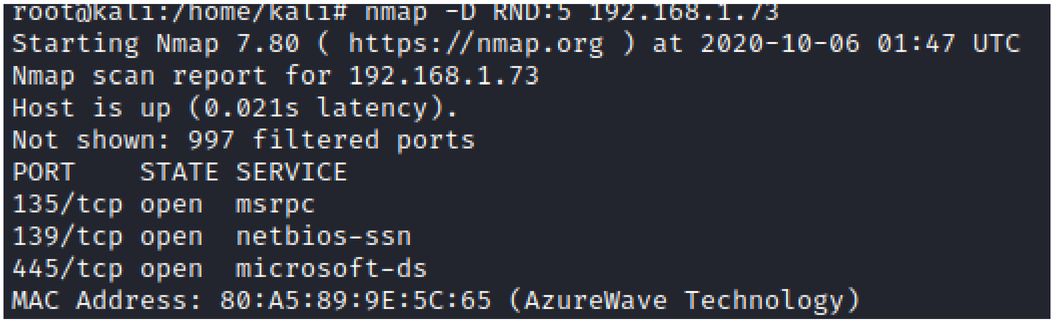
Therefore, Snort, the IDS I use, is completely missed the scans. The only 4 alerts are because there is a website running in the background where it generates alerts when bad connections happened.



```
       Frag:            0 (  0.000%)
       ICMP:            0 (  0.000%)
        UDP:          212 (  2.317%)
        TCP:         8344 ( 91.211%)
        IP6:          164 (  1.793%)
    IP6 Ext:          164 (  1.793%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            9 (  0.098%)
       UDP6:          114 (  1.246%)
       TCP6:           41 (  0.448%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
        GRE:            0 (  0.000%)
    GRE Eth:            0 (  0.000%)
   GRE VLAN:            0 (  0.000%)
    GRE IP4:            0 (  0.000%)
    GRE IP6:            0 (  0.000%)
GRE IP6 Ext:            0 (  0.000%)
   GRE PPTP:            0 (  0.000%)
    GRE ARP:            0 (  0.000%)
    GRE IPX:            0 (  0.000%)
   GRE Loop:            0 (  0.000%)
       MPLS:            0 (  0.000%)
        ARP:          420 (  4.591%)
        IPX:            0 (  0.000%)
   Eth Loop:            0 (  0.000%)
   Eth Disc:            0 (  0.000%)
   IP4 Disc:            0 (  0.000%)
   IP6 Disc:            0 (  0.000%)
   TCP Disc:            0 (  0.000%)
   UDP Disc:            0 (  0.000%)
  ICMP Disc:            0 (  0.000%)
All Discard:            0 (  0.000%)
      Other:            8 (  0.087%)
Bad Chk Sum:            0 (  0.000%)
    Bad TTL:            0 (  0.000%)
     S5 G 1:            0 (  0.000%)
     S5 G 2:           11 (  0.120%)
      Total:         9148
===================================================
Action Stats:
     Alerts:            4 (  0.044%)
     Logged:            4 (  0.044%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:         9017 ( 98.708%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:          120 (  1.314%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
```

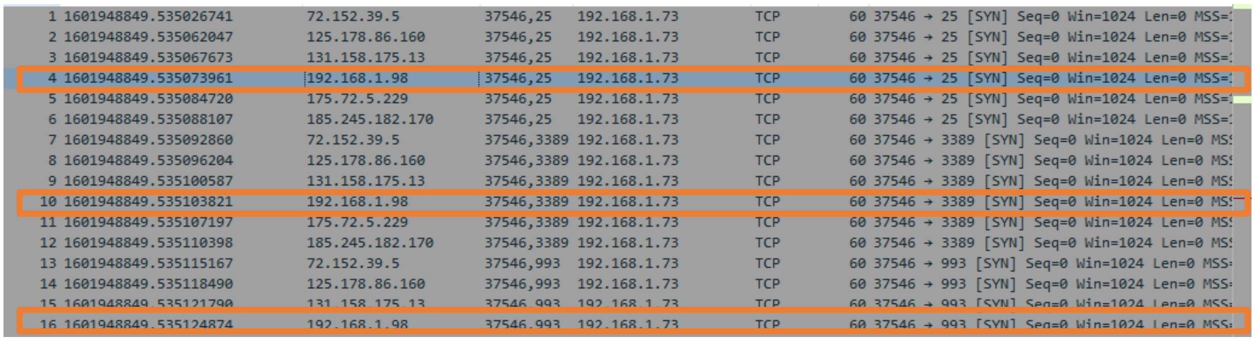
Task 2 – Decoy and RND

Except for only use decoy, Nmap also provides RND option to generate a random, non-reserved Ip address. In this case, I will randomly generate 10 IP addresses with RND and Decoy set.

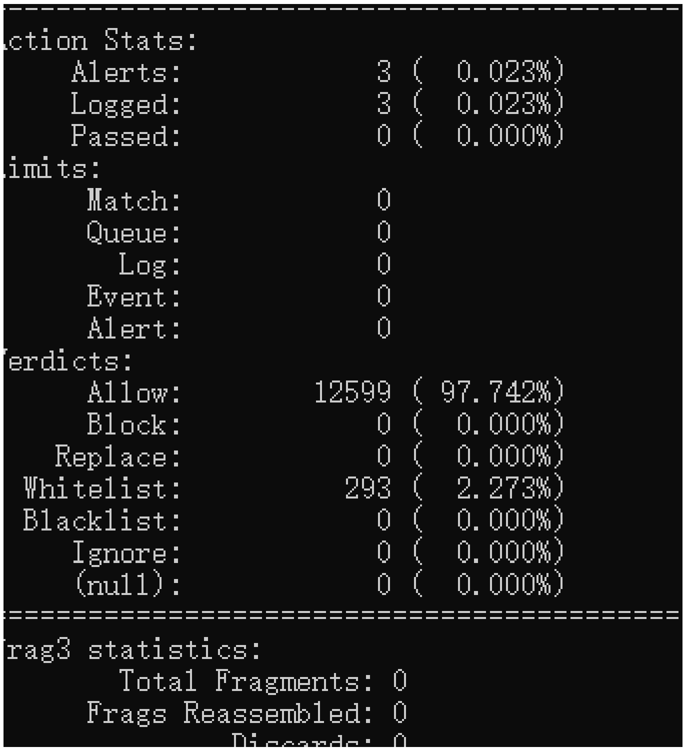


```
root@kali:/home/kali# nmap -D RND:5 192.168.1.73
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-06 01:47 UTC
Nmap scan report for 192.168.1.73
Host is up (0.021s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 80:A5:89:9E:5C:65 (AzureWave Technology)
```

My real IP is randomly showed when scanning the target network. The other IP address is just a random decoy helps me confusing the target network.



```
 1 1601948849.535026741   72.152.39.5       37546,25    192.168.1.73   TCP   60 37546 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=
 2 1601948849.535062047   125.178.86.160    37546,25    192.168.1.73   TCP   60 37546 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=
 3 1601948849.535067673   131.158.175.13    37546,25    192.168.1.73   TCP   60 37546 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=
 4 1601948849.535073961   192.168.1.98      37546,25    192.168.1.73   TCP   60 37546 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=
 5 1601948849.535084720   175.72.5.229      37546,25    192.168.1.73   TCP   60 37546 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=
 6 1601948849.535088107   185.245.182.170   37546,25    192.168.1.73   TCP   60 37546 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=
 7 1601948849.535092860   72.152.39.5       37546,3389  192.168.1.73   TCP   60 37546 → 3389 [SYN] Seq=0 Win=1024 Len=0 MS
 8 1601948849.535096204   125.178.86.160    37546,3389  192.168.1.73   TCP   60 37546 → 3389 [SYN] Seq=0 Win=1024 Len=0 MS
 9 1601948849.535100587   131.158.175.13    37546,3389  192.168.1.73   TCP   60 37546 → 3389 [SYN] Seq=0 Win=1024 Len=0 MS
10 1601948849.535103821   192.168.1.98      37546,3389  192.168.1.73   TCP   60 37546 → 3389 [SYN] Seq=0 Win=1024 Len=0 MS
11 1601948849.535107197   175.72.5.229      37546,3389  192.168.1.73   TCP   60 37546 → 3389 [SYN] Seq=0 Win=1024 Len=0 MS
12 1601948849.535110398   185.245.182.170   37546,3389  192.168.1.73   TCP   60 37546 → 3389 [SYN] Seq=0 Win=1024 Len=0 MS
13 1601948849.535115167   72.152.39.5       37546,993   192.168.1.73   TCP   60 37546 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=
14 1601948849.535118490   125.178.86.160    37546,993   192.168.1.73   TCP   60 37546 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=
15 1601948849.535121790   131.158.175.13    37546,993   192.168.1.73   TCP   60 37546 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=
16 1601948849.535124874   192.168.1.98      37546,993   192.168.1.73   TCP   60 37546 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=
```



```
-------------------------------------------
ction Stats:
     Alerts:            3 (  0.023%)
     Logged:            3 (  0.023%)
     Passed:            0 (  0.000%)
imits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
erdicts:
      Allow:        12599 ( 97.742%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:          293 (  2.273%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
     (null):            0 (  0.000%)
===========================================
rag3 statistics:
        Total Fragments: 0
      Frags Reassembled: 0
               Discards: 0
```

Also, Snort will miss all the scans. But with RND:10 set, it will generate about 10 times larger scan requests than usual. IDS may not notice but a human may notice this abnormal.

Defence

To block a Nmap scan with a decoy, we know that even with a decoy, each IP address will scan the target network more than 2 or 3 times. So, the user should set up a firewall and put the IP address who shows up more than 3 or 4 times to a block list. Block all IP will basically block the real attackers at the same time.

Even with the RND mode set, we can tell that Snort shows unusual requests at a certain time. And we can make use that abnormal to block the IPs.

Users can also set up a host with a firewall machine where only the firewall machine can see the real host. Thus Nmap won't be able to scan the host.

Conclusion

Nmap is a powerful tool when scanning the target network. It provides plenty of options to confuse or bypass the IDS. Decoy and RND are great options when attackers do not want the victim machine to discover the real attacker IP. But Nmap could be easily detected or blocked. Users with basic networking knowledge could set up rules to block all scanning IPs, which include the real IP.

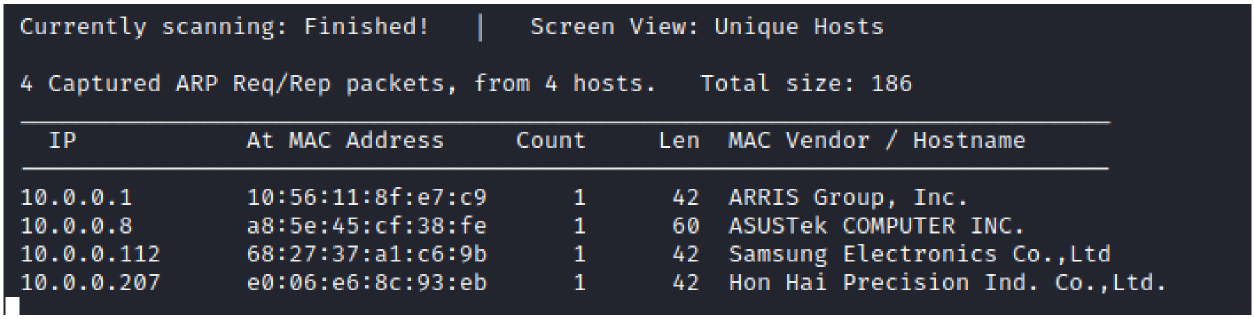
Netdiscover

Introduction

Netdiscover is an active, passive arp reconnaissance tool. ARP, the address resolution protocol, is a communication protocol used for discovering the link-layer address, such as a Mac address with associated IPv4 address. Using arp, we could know if any IP address is used and then find the live hosts. Netdiscover is the tool using arp to discover hosts actively or passively.

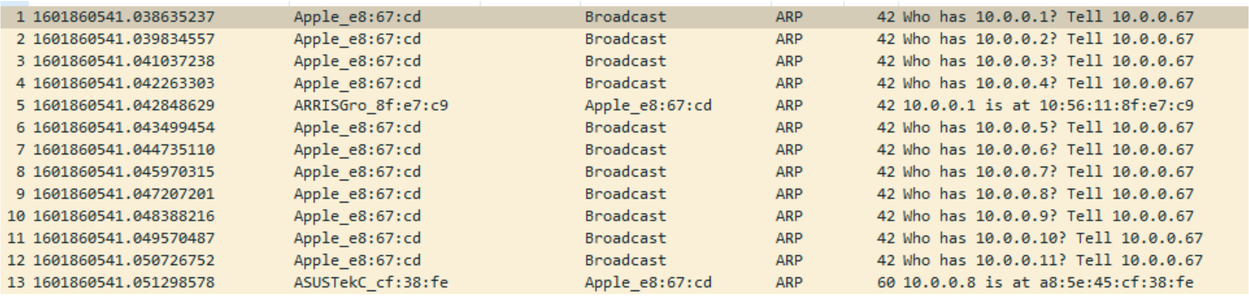
Task 1 – Active Scan

Netdiscover active scan will send out arp requests and receive an arp response to identifying the live hosts in the network. For example, if my IP in the local network is 10.0.0.174, and my target network is 10.0.0.0/24. The command I use for Netdiscover is Netdiscover -r 10.0.0.0/24. Then Netdiscover will start sending arp requests to 10.0.0.1 until 10.0.0.254 and receive arp response, identify live hosts.



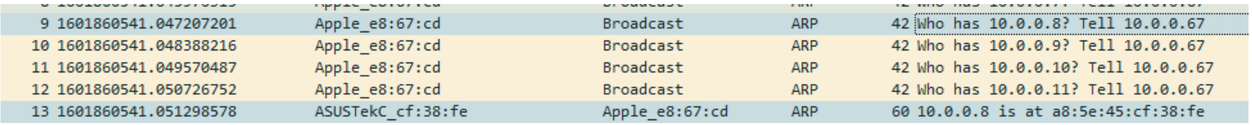
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 186
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.0.1        10:56:11:8f:e7:c9      1      42  ARRIS Group, Inc.
10.0.0.8        a8:5e:45:cf:38:fe      1      60  ASUSTek COMPUTER INC.
10.0.0.112      68:27:37:a1:c6:9b      1      42  Samsung Electronics Co.,Ltd
10.0.0.207      e0:06:e6:8c:93:eb      1      42  Hon Hai Precision Ind. Co.,Ltd.
```

Netdiscover scanned my network, 10.0.0.0/24, and gathered 4 live hosts. Where 10.0.0.1 is the router, 10.0.0.207 and 10.0.0.8 are computers and 10.0.0.112 is a smart TV. Therefore, we could know that Netdiscover can not only identify a computer operating system but also able to identify devices with assigned Mac addresses and IP addresses, such as TVs, mobile phones.



```
 1 1601860541.038635237   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.1? Tell 10.0.0.67
 2 1601860541.039834557   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.2? Tell 10.0.0.67
 3 1601860541.041037238   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.3? Tell 10.0.0.67
 4 1601860541.042263303   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.4? Tell 10.0.0.67
 5 1601860541.042848629   ARRISGro_8f:e7:c9   Apple_e8:67:cd   ARP   42 10.0.0.1 is at 10:56:11:8f:e7:c9
 6 1601860541.043499454   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.5? Tell 10.0.0.67
 7 1601860541.044735110   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.6? Tell 10.0.0.67
 8 1601860541.045970315   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.7? Tell 10.0.0.67
 9 1601860541.047207201   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.8? Tell 10.0.0.67
10 1601860541.048388216   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.9? Tell 10.0.0.67
11 1601860541.049570487   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.10? Tell 10.0.0.67
12 1601860541.050726752   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.11? Tell 10.0.0.67
13 1601860541.051298578   ASUSTekC_cf:38:fe   Apple_e8:67:cd   ARP   60 10.0.0.8 is at a8:5e:45:cf:38:fe
```

Inactive mode, Netdiscover will send requests from IP address 10.0.0.1 until 10.0.0.254. Then receive a response and identify live hosts.

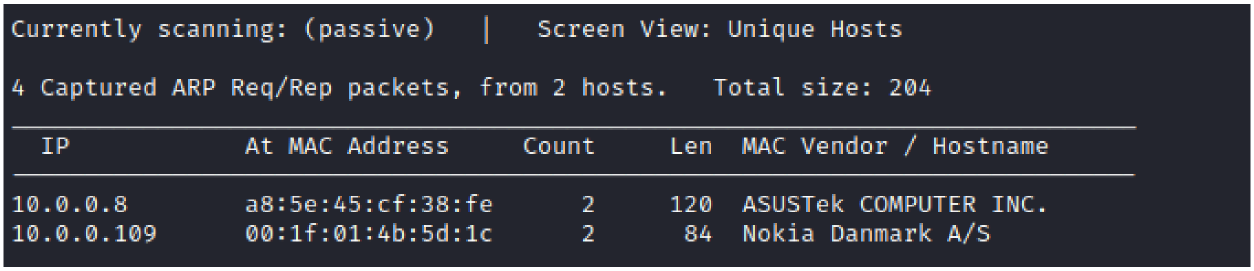


```
 9 1601860541.047207201   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.8? Tell 10.0.0.67
10 1601860541.048388216   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.9? Tell 10.0.0.67
11 1601860541.049570487   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.10? Tell 10.0.0.67
12 1601860541.050726752   Apple_e8:67:cd      Broadcast        ARP   42 Who has 10.0.0.11? Tell 10.0.0.67
13 1601860541.051298578   ASUSTekC_cf:38:fe   Apple_e8:67:cd   ARP   60 10.0.0.8 is at a8:5e:45:cf:38:fe
```

Note that the attacker machine sends requests from an Apple machine and broadcast to every machine. Then the response goes from the victim machine to the Apple machine. In passive mode, it is different.

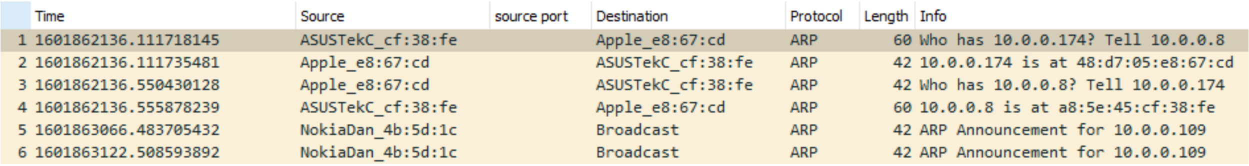
Task 2 – Passive Scan

Netdiscover active scan will easily be discovered by an IDS or IPS. So, a passive scan is a safer way, but it takes a lot of time. For example, if my IP in the local network is 10.0.0.174, and my target network is 10.0.0.0/24. The command I use for Netdiscover is Netdiscover -r 10.0.0.0/24 -p. The -p enable passive mode.



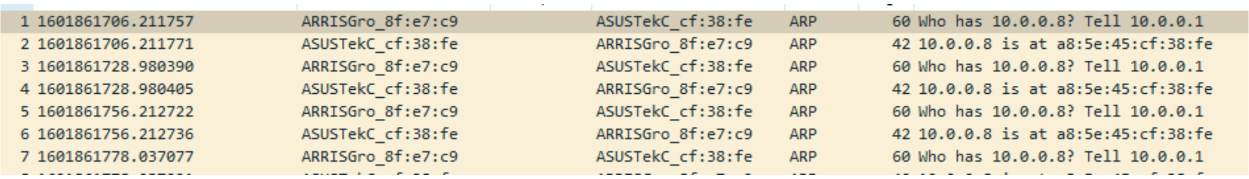
```
Currently scanning: (passive)   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 204
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
10.0.0.8        a8:5e:45:cf:38:fe      2     120  ASUSTek COMPUTER INC.
10.0.0.109      00:1f:01:4b:5d:1c      2      84  Nokia Danmark A/S
```

After about 20 minutes scan, Netdiscover finds 2 live hosts. Because passive mode is so slow, so I decide to not finish the whole scan and that is the reason why only 2 live hosts are detected. Usually, Netdiscover passive mode will take a few hours to identify a network with more than 100 live hosts.



	Time	Source	source port	Destination	Protocol	Length	Info
1	1601862136.111718145	ASUSTekC_cf:38:fe		Apple_e8:67:cd	ARP	60	Who has 10.0.0.174? Tell 10.0.0.8
2	1601862136.111735481	Apple_e8:67:cd		ASUSTekC_cf:38:fe	ARP	42	10.0.0.174 is at 48:d7:05:e8:67:cd
3	1601862136.550430128	Apple_e8:67:cd		ASUSTekC_cf:38:fe	ARP	42	Who has 10.0.0.8? Tell 10.0.0.174
4	1601862136.555878239	ASUSTekC_cf:38:fe		Apple_e8:67:cd	ARP	60	10.0.0.8 is at a8:5e:45:cf:38:fe
5	1601863066.483705432	NokiaDan_4b:5d:1c		Broadcast	ARP	42	ARP Announcement for 10.0.0.109
6	1601863122.508593892	NokiaDan_4b:5d:1c		Broadcast	ARP	42	ARP Announcement for 10.0.0.109

Note that in passive mode, Netdiscover will not send and broadcast arp requests, but only sniff.



1	1601861706.211757	ARRISGro_8f:e7:c9		ASUSTekC_cf:38:fe	ARP	60	Who has 10.0.0.8? Tell 10.0.0.1
2	1601861706.211771	ASUSTekC_cf:38:fe		ARRISGro_8f:e7:c9	ARP	42	10.0.0.8 is at a8:5e:45:cf:38:fe
3	1601861728.980390	ARRISGro_8f:e7:c9		ASUSTekC_cf:38:fe	ARP	60	Who has 10.0.0.8? Tell 10.0.0.1
4	1601861728.980405	ASUSTekC_cf:38:fe		ARRISGro_8f:e7:c9	ARP	42	10.0.0.8 is at a8:5e:45:cf:38:fe
5	1601861756.212722	ARRISGro_8f:e7:c9		ASUSTekC_cf:38:fe	ARP	60	Who has 10.0.0.8? Tell 10.0.0.1
6	1601861756.212736	ASUSTekC_cf:38:fe		ARRISGro_8f:e7:c9	ARP	42	10.0.0.8 is at a8:5e:45:cf:38:fe
7	1601861778.037077	ARRISGro_8f:e7:c9		ASUSTekC_cf:38:fe	ARP	60	Who has 10.0.0.8? Tell 10.0.0.1

Also, remember in active mode, requests are sent from an Apple machine. But in passive mode, ARRIS group did the ask, which is the router. Therefore, it hides the Apple machine, the one starts the scan.

Possible Ways to Block

To block arp scan generated by Netdiscover, the Dynamic ARP Inspection system, DAI, might be helpful. DAI is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings.

DAI prevents these attacks by intercepting all ARP requests and responses. Each of these intercepted packets is verified for valid MAC address to IP address bindings before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped. DAI also determines the validity of an ARP packet based on valid MAC address to IP address bindings stored in a trusted database.

However, the downside of this solution is that DAI could be very expensive. For individuals, maybe we should use an arp firewall, such as ARP AntiSpoofer, etc.

Conclusion

Netdiscover is a decent reconnaissance tool using ARP to identify if any IP address is used and then find the live hosts. Netdiscover can do an active scan, which is fast, but easy to detect. So, a passive scan should be the first choice to do any reconnaissance work because the passive scan is hard to detect. The downside of the passive scan is that it could be very slow.

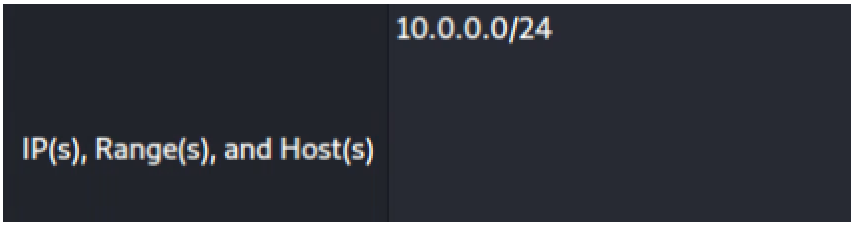
Sparta

Introduction

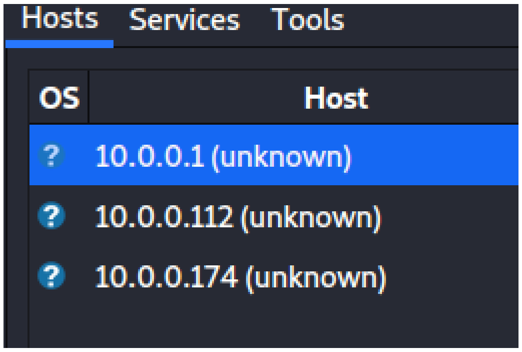
Legion is an open-source python-based GUI tool that performs network penetration testing. Legion is an upgraded version of Sparta. Legion could automatic recon and scanning with Nmap, Nikto, Hydra, etc.

Task 1 – Penetrating Network

Using Legion, the user needs to enter an IP address, website URL or local network address. For this task, I am penetrating my own network, which is 10.0.0.0/24 with timing and performance option set to insane.

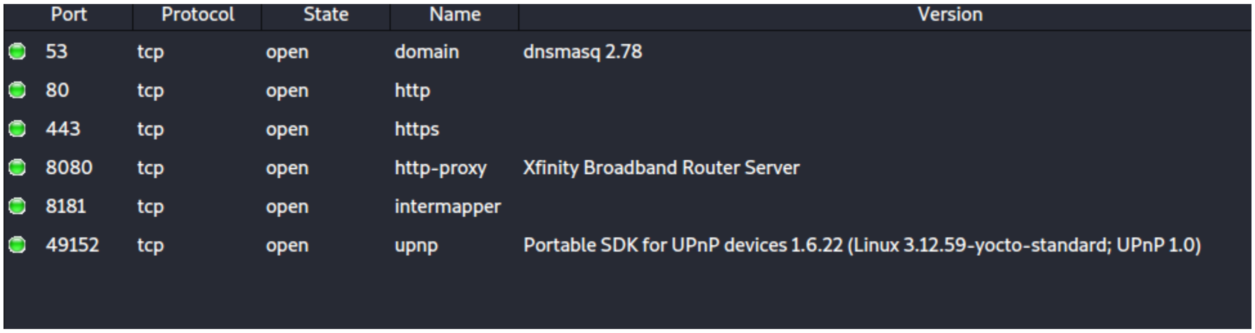


IP(s), Range(s), and Host(s)	10.0.0.0/24



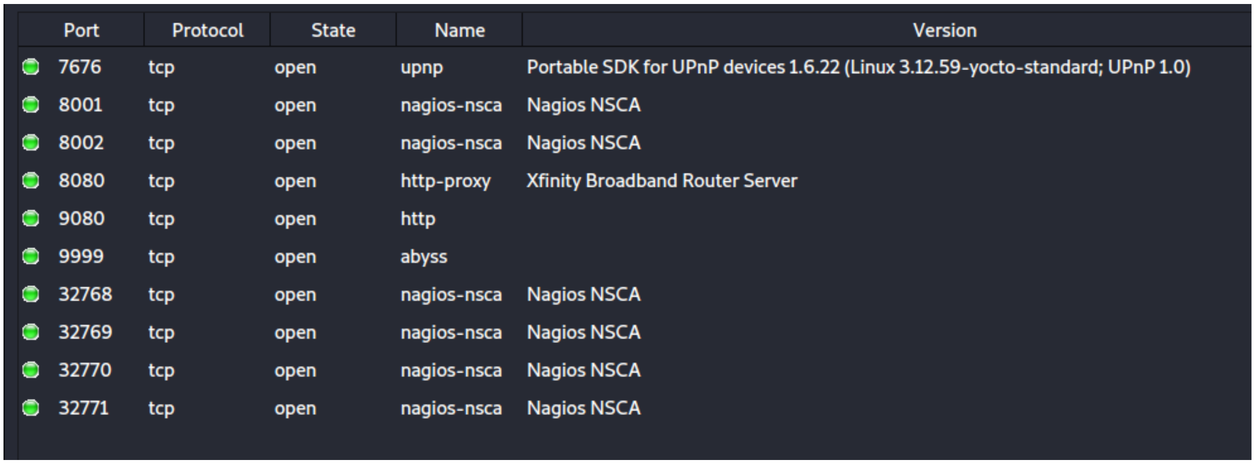
OS	Host
?	10.0.0.1 (unknown)
?	10.0.0.112 (unknown)
?	10.0.0.174 (unknown)

After few minutes scanning, Legion can find 3 hosts under my network. 10.0.0.1 is the router, 10.0.0.112 is the TV and 174 is the laptop itself.



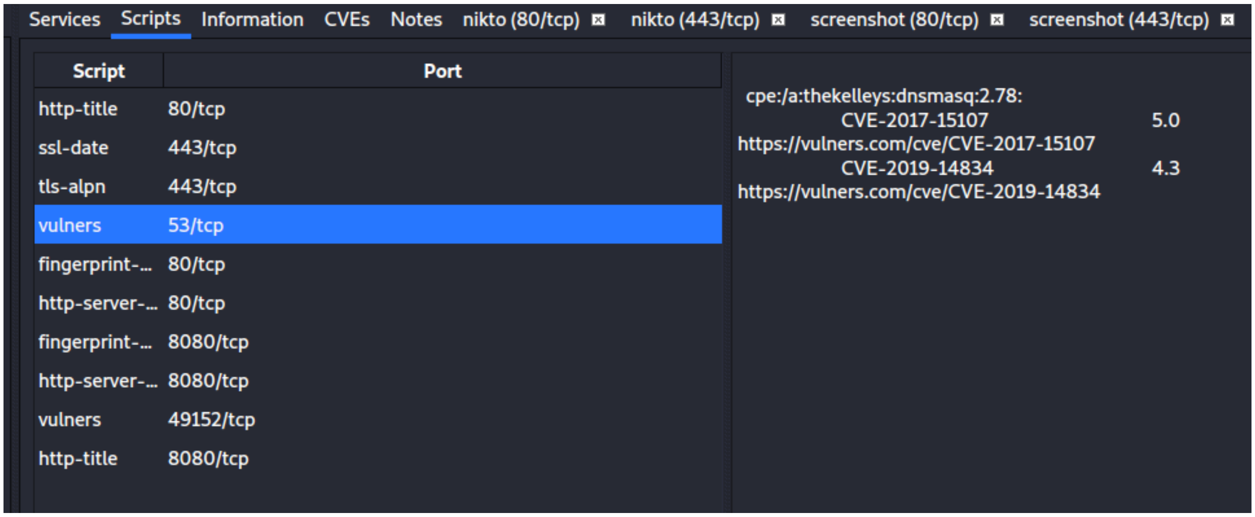
Port	Protocol	State	Name	Version
● 53	tcp	open	domain	dnsmasq 2.78
● 80	tcp	open	http	
● 443	tcp	open	https	
● 8080	tcp	open	http-proxy	Xfinity Broadband Router Server
● 8181	tcp	open	intermapper	
● 49152	tcp	open	upnp	Portable SDK for UPnP devices 1.6.22 (Linux 3.12.59-yocto-standard; UPnP 1.0)

Legion finds the open ports of my router, 10.0.0.1. Notice that no UDP port open, but only TCP ports.



	Port	Protocol	State	Name	Version
●	7676	tcp	open	upnp	Portable SDK for UPnP devices 1.6.22 (Linux 3.12.59-yocto-standard; UPnP 1.0)
●	8001	tcp	open	nagios-nsca	Nagios NSCA
●	8002	tcp	open	nagios-nsca	Nagios NSCA
●	8080	tcp	open	http-proxy	Xfinity Broadband Router Server
●	9080	tcp	open	http	
●	9999	tcp	open	abyss	
●	32768	tcp	open	nagios-nsca	Nagios NSCA
●	32769	tcp	open	nagios-nsca	Nagios NSCA
●	32770	tcp	open	nagios-nsca	Nagios NSCA
●	32771	tcp	open	nagios-nsca	Nagios NSCA

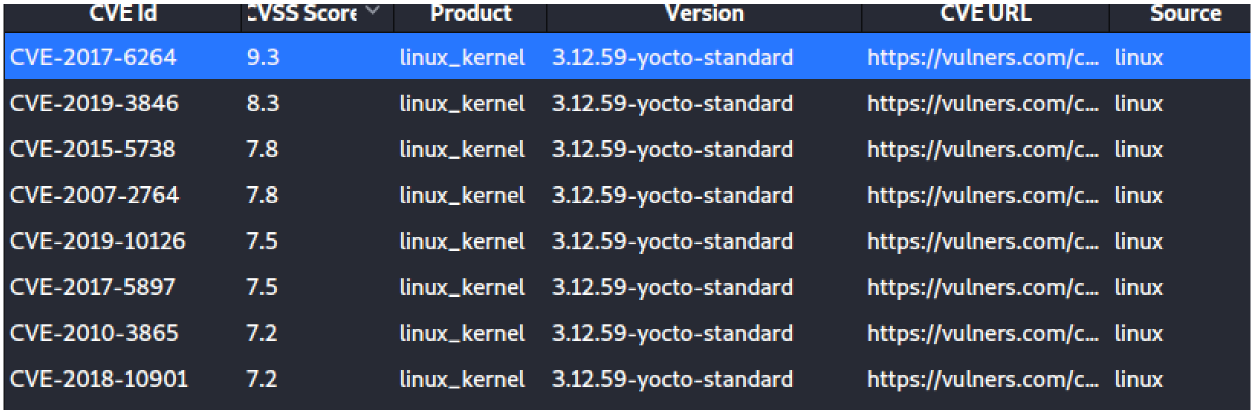
No UDP ports open for the TV either.



Script	Port
http-title	80/tcp
ssl-date	443/tcp
tls-alpn	443/tcp
vulners	53/tcp
fingerprint-...	80/tcp
http-server-...	80/tcp
fingerprint-...	8080/tcp
http-server-...	8080/tcp
vulners	49152/tcp
http-title	8080/tcp

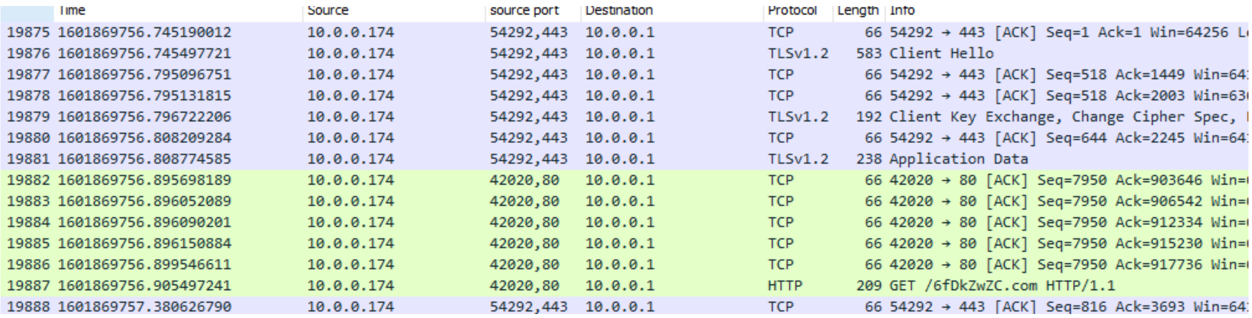
```
 cpe:/a:thekelleys:dnsmasq:2.78:
        CVE-2017-15107              5.0
https://vulners.com/cve/CVE-2017-15107
        CVE-2019-14834              4.3
https://vulners.com/cve/CVE-2019-14834
```

Legion detects some common vulnerabilities of my router. For example, CVE-2019-14834 is a vulnerability that memory leak allows remote attackers to cause a denial of service through vectors involving DHCP response creation.



CVE Id	CVSS Score	Product	Version	CVE URL	Source
CVE-2017-6264	9.3	linux_kernel	3.12.59-yocto-standard	https://vulners.com/c...	linux
CVE-2019-3846	8.3	linux_kernel	3.12.59-yocto-standard	https://vulners.com/c...	linux
CVE-2015-5738	7.8	linux_kernel	3.12.59-yocto-standard	https://vulners.com/c...	linux
CVE-2007-2764	7.8	linux_kernel	3.12.59-yocto-standard	https://vulners.com/c...	linux
CVE-2019-10126	7.5	linux_kernel	3.12.59-yocto-standard	https://vulners.com/c...	linux
CVE-2017-5897	7.5	linux_kernel	3.12.59-yocto-standard	https://vulners.com/c...	linux
CVE-2010-3865	7.2	linux_kernel	3.12.59-yocto-standard	https://vulners.com/c...	linux
CVE-2018-10901	7.2	linux_kernel	3.12.59-yocto-standard	https://vulners.com/c...	linux

Legion scores and captures every possible CVEs of the network. For user, user can update their system based on this. Also, attackers could try possible attacks based on the rating of the CVE result.



```
      Time                  Source        source port Destination  Protocol Length Info
19875 1601869756.745190012  10.0.0.174    54292,443   10.0.0.1     TCP        66 54292 → 443 [ACK] Seq=1 Ack=1 Win=64256 L
19876 1601869756.745497721  10.0.0.174    54292,443   10.0.0.1     TLSv1.2   583 Client Hello
19877 1601869756.795096751  10.0.0.174    54292,443   10.0.0.1     TCP        66 54292 → 443 [ACK] Seq=518 Ack=1449 Win=64
19878 1601869756.795131815  10.0.0.174    54292,443   10.0.0.1     TCP        66 54292 → 443 [ACK] Seq=518 Ack=2003 Win=63
19879 1601869756.796722206  10.0.0.174    54292,443   10.0.0.1     TLSv1.2   192 Client Key Exchange, Change Cipher Spec,
19880 1601869756.808209284  10.0.0.174    54292,443   10.0.0.1     TCP        66 54292 → 443 [ACK] Seq=644 Ack=2245 Win=64
19881 1601869756.808774585  10.0.0.174    54292,443   10.0.0.1     TLSv1.2   238 Application Data
19882 1601869756.895698189  10.0.0.174    42020,80    10.0.0.1     TCP        66 42020 → 80 [ACK] Seq=7950 Ack=903646 Win=
19883 1601869756.896052089  10.0.0.174    42020,80    10.0.0.1     TCP        66 42020 → 80 [ACK] Seq=7950 Ack=906542 Win=
19884 1601869756.896090201  10.0.0.174    42020,80    10.0.0.1     TCP        66 42020 → 80 [ACK] Seq=7950 Ack=912334 Win=
19885 1601869756.896150884  10.0.0.174    42020,80    10.0.0.1     TCP        66 42020 → 80 [ACK] Seq=7950 Ack=915230 Win=
19886 1601869756.899546611  10.0.0.174    42020,80    10.0.0.1     TCP        66 42020 → 80 [ACK] Seq=7950 Ack=917736 Win=
19887 1601869756.905497241  10.0.0.174    42020,80    10.0.0.1     HTTP      209 GET /6fDkZwZC.com HTTP/1.1
19888 1601869757.380626790  10.0.0.174    54292,443   10.0.0.1     TCP        66 54292 → 443 [ACK] Seq=816 Ack=3693 Win=64
```

Legion usually use Nmap to scan all the ports which can be easily detected. Users can set up a firewall to block scanning IP.

Defence

For blocking tools like legion, a user should definitely set up a proper firewall with proper rules. Blocking the IP which scanned too many ports. Because Legion will scan port 22, port 0 and all other danger ports, a user should set up firewall rules specifically for those ports and block any malicious activities.

Conclusion

Legion is a useful network penetration testing that automatic recon and scanning with Nmap, Nikto, Hydra and other tools so a user can understand possible vulnerabilities of the victim machine if the victim machine not setting up a proper firewall.

Enumeration Techniques - Dumps

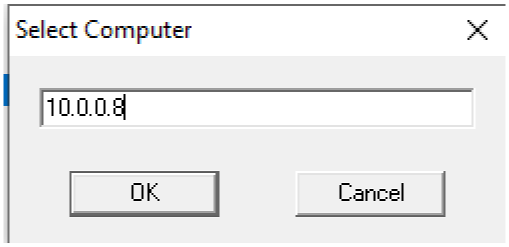
Introduction

Enumeration techniques are mainly operating system specific and identify network and systems in earlier reconnaissance. Dumpsec is a security auditing program for Microsoft Windows systems. It dumps permissions, discretionary access control list, and audit settings, system access control list, for the file system, registry, printers and shares in a readable format.

Therefore, vulnerabilities in system security are readable. Dumpsec also dumps user, group and replication information.

Task – Dump information of my Windows PC

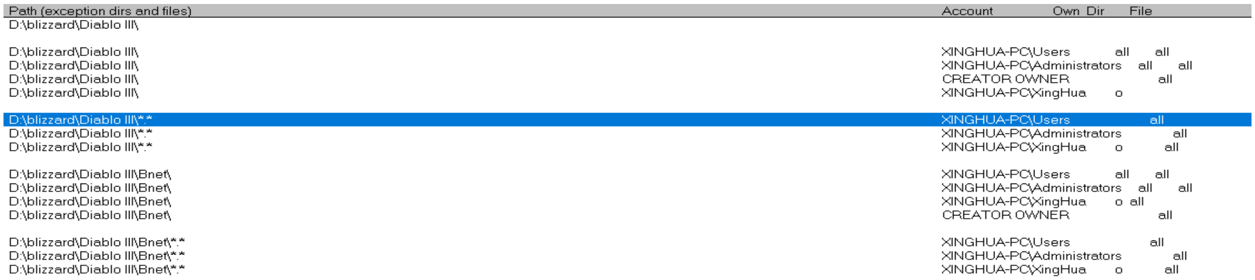
Dumpsec allows users to select a target machine by using the target machine IP. In this case, I use my machine, 10.0.0.8.



Select Computer

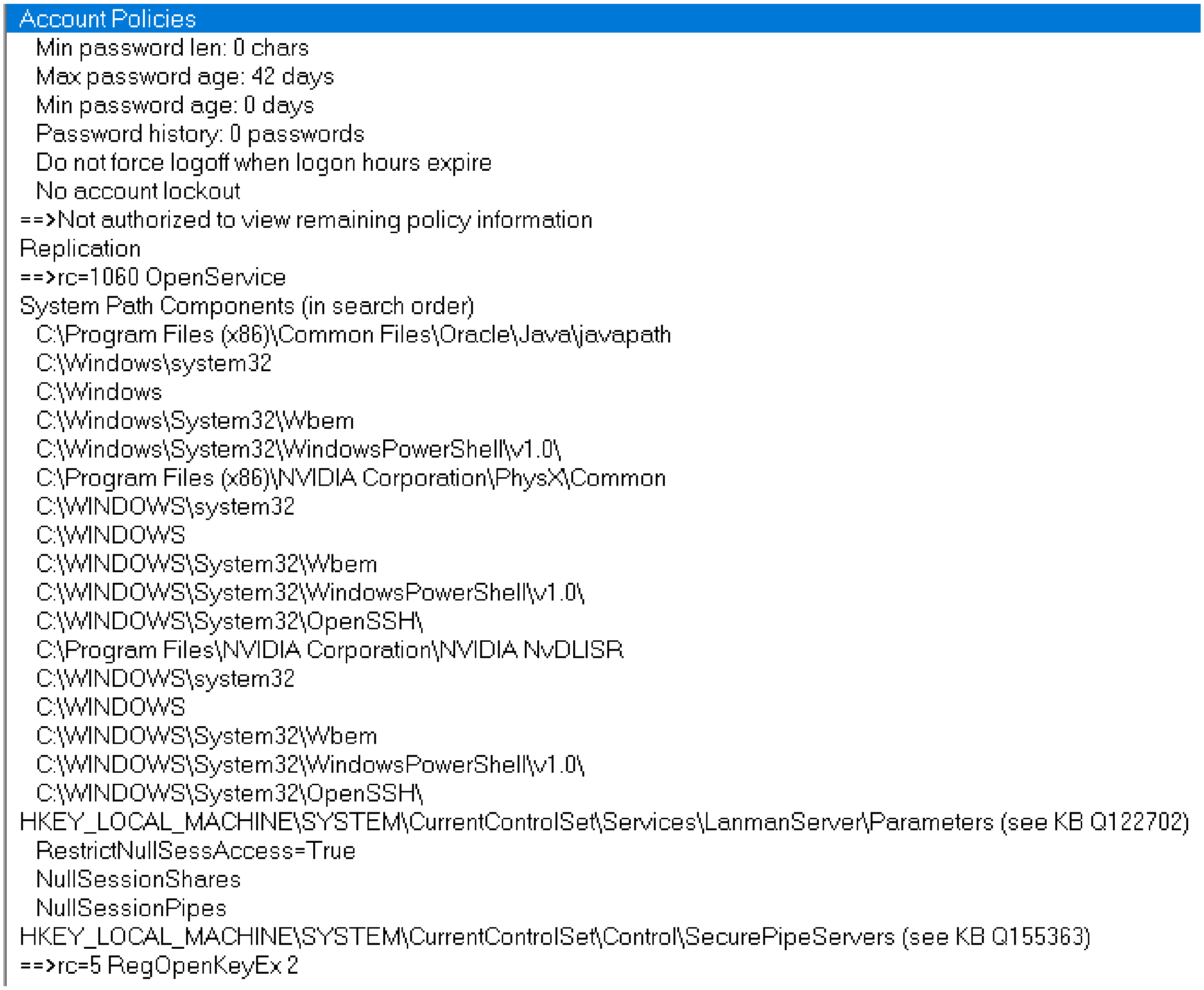
10.0.0.8

Dumpsec could generate permissions for file directories of the target machine.



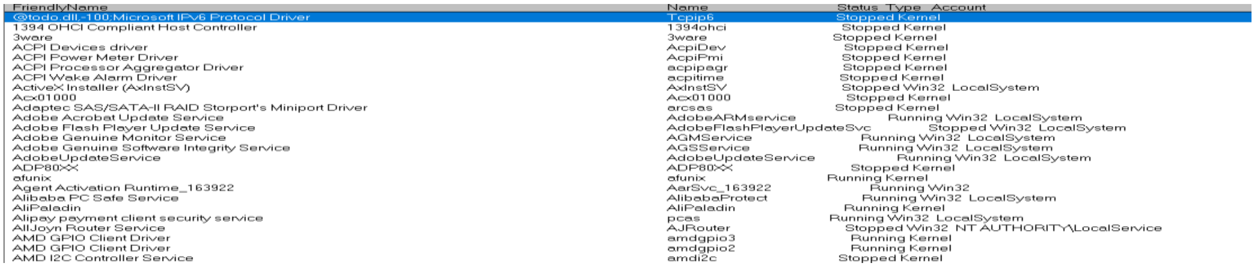
```
Path (exception dirs and files)                                                              Account                     Own  Dir     File
D:\blizzard\Diablo III\

D:\blizzard\Diablo III\                                                                      XINGHUA-PC\Users             all     all
D:\blizzard\Diablo III\                                                                      XINGHUA-PC\Administrators     all     all
D:\blizzard\Diablo III\                                                                      CREATOR OWNER                     all
D:\blizzard\Diablo III\                                                                      XINGHUA-PC\XingHua        o

D:\blizzard\Diablo III\*.*                                                                   XINGHUA-PC\Users                  all
D:\blizzard\Diablo III\*.*                                                                   XINGHUA-PC\Administrators          all
D:\blizzard\Diablo III\*.*                                                                   XINGHUA-PC\XingHua        o        all

D:\blizzard\Diablo III\Bnet\                                                                 XINGHUA-PC\Users             all     all
D:\blizzard\Diablo III\Bnet\                                                                 XINGHUA-PC\Administrators     all     all
D:\blizzard\Diablo III\Bnet\                                                                 XINGHUA-PC\XingHua        o  all
D:\blizzard\Diablo III\Bnet\                                                                 CREATOR OWNER                     all

D:\blizzard\Diablo III\Bnet\*.*                                                              XINGHUA-PC\Users                  all
D:\blizzard\Diablo III\Bnet\*.*                                                              XINGHUA-PC\Administrators          all
D:\blizzard\Diablo III\Bnet\*.*                                                              XINGHUA-PC\XingHua        o        all
```

It dumps which account holds the file, who can access the file. By checking this, attackers could gather information about which account should they attack and compromise.



```
Account Policies
  Min password len: 0 chars
  Max password age: 42 days
  Min password age: 0 days
  Password history: 0 passwords
  Do not force logoff when logon hours expire
  No account lockout
==>Not authorized to view remaining policy information
Replication
==>rc=1060 OpenService
System Path Components (in search order)
  C:\Program Files (x86)\Common Files\Oracle\Java\javapath
  C:\Windows\system32
  C:\Windows
  C:\Windows\System32\Wbem
  C:\Windows\System32\WindowsPowerShell\v1.0\
  C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common
  C:\WINDOWS\system32
  C:\WINDOWS
  C:\WINDOWS\System32\Wbem
  C:\WINDOWS\System32\WindowsPowerShell\v1.0\
  C:\WINDOWS\System32\OpenSSH\
  C:\Program Files\NVIDIA Corporation\NVIDIA NvDLISR
  C:\WINDOWS\system32
  C:\WINDOWS
  C:\WINDOWS\System32\Wbem
  C:\WINDOWS\System32\WindowsPowerShell\v1.0\
  C:\WINDOWS\System32\OpenSSH\
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters (see KB Q122702)
  RestrictNullSessAccess=True
  NullSessionShares
  NullSessionPipes
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers (see KB Q155363)
==>rc=5 RegOpenKeyEx 2
```

Dumpsec gathers the system policies of the machine. It shows minimal password length, when the user changed the password, what components in the system path, null section restriction level, etc. Attackers could use that information to do another type and passive reconnaissance or use null sessions to attack the target machine.



FriendlyName	Name	Status	Type	Account
@todo.dll,-100;Microsoft IPv6 Protocol Driver	Tcpip6	Stopped	Kernel	
1394 OHCI Compliant Host Controller	1394ohci	Stopped	Kernel	
3ware	3ware	Stopped	Kernel	
ACPI Devices driver	AcpiDev	Stopped	Kernel	
ACPI Power Meter Driver	AcpiPmi	Stopped	Kernel	
ACPI Processor Aggregator Driver	acpipagr	Stopped	Kernel	
ACPI Wake Alarm Driver	acpitime	Stopped	Kernel	
ActiveX Installer (AxInstSV)	AxInstSV	Stopped	Win32	LocalSystem
Acx01000	Acx01000	Stopped	Kernel	
Adaptec SAS/SATA-II RAID Storport's Miniport Driver	arcsas	Stopped	Kernel	
Adobe Acrobat Update Service	AdobeARMservice	Running	Win32	LocalSystem
Adobe Flash Player Update Service	AdobeFlashPlayerUpdateSvc	Stopped	Win32	LocalSystem
Adobe Genuine Monitor Service	AGMService	Running	Win32	LocalSystem
Adobe Genuine Software Integrity Service	AGSService	Running	Win32	LocalSystem
AdobeUpdateService	AdobeUpdateService	Running	Win32	LocalSystem
ADP80XX	ADP80XX	Stopped	Kernel	
afunix	afunix	Running	Kernel	
Agent Activation Runtime_163922	AarSvc_163922	Running	Win32	
Alibaba PC Safe Service	AlibabaProtect	Running	Win32	LocalSystem
AliPaladin	AliPaladin	Running	Kernel	
Alipay payment client security service	pcas	Running	Win32	LocalSystem
AllJoyn Router Service	AJRouter	Stopped	Win32	NT AUTHORITY\LocalService
AMD GPIO Client Driver	amdgpio3	Running	Kernel	
AMD GPIO Client Driver	amdgpio2	Running	Kernel	
AMD I2C Controller Service	amdi2c	Stopped	Kernel	

Dumpsec generates information about system services which installed to the system. The attacker could check and decide what attack to use. For example, maybe a Trojan to the mail service, or the target machine’s Bluetooth is open, so Bluetooth virus can be used like BlueBorne.

Defence

User should regularly check their system status. Use uncommon username and passwords, close unnecessary service, add authentication to files and backup important data to another offline machine.

Conclusion

Dumpsec is a security auditing program for Microsoft Windows systems. It exposes permissions, discretionary access control list, and audit settings, system access control list, for the file system, registry, printers and shares in a readable format. If attackers can access that detailed information, there is a high possibility that attackers could break into the target machine.

Maltego

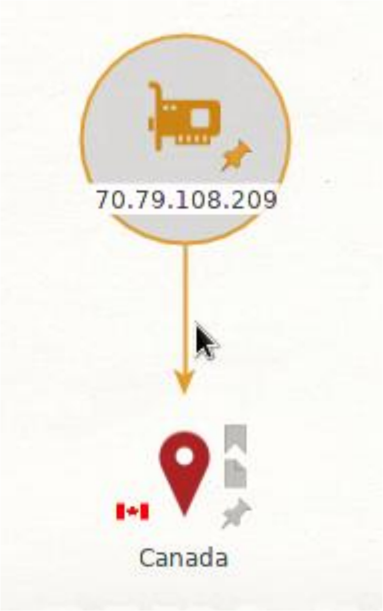
Introduction

Maltego is an open-source intelligence and graphical link analysis tool for gathering and connecting information for a specific target. Maltego permits creating custom entities, allowing it to represent any type of information in addition to the basic entity types which are part of the software. The basic focus of the application is analyzing real-world relationships between people, groups, websites, domains, networks, etc.

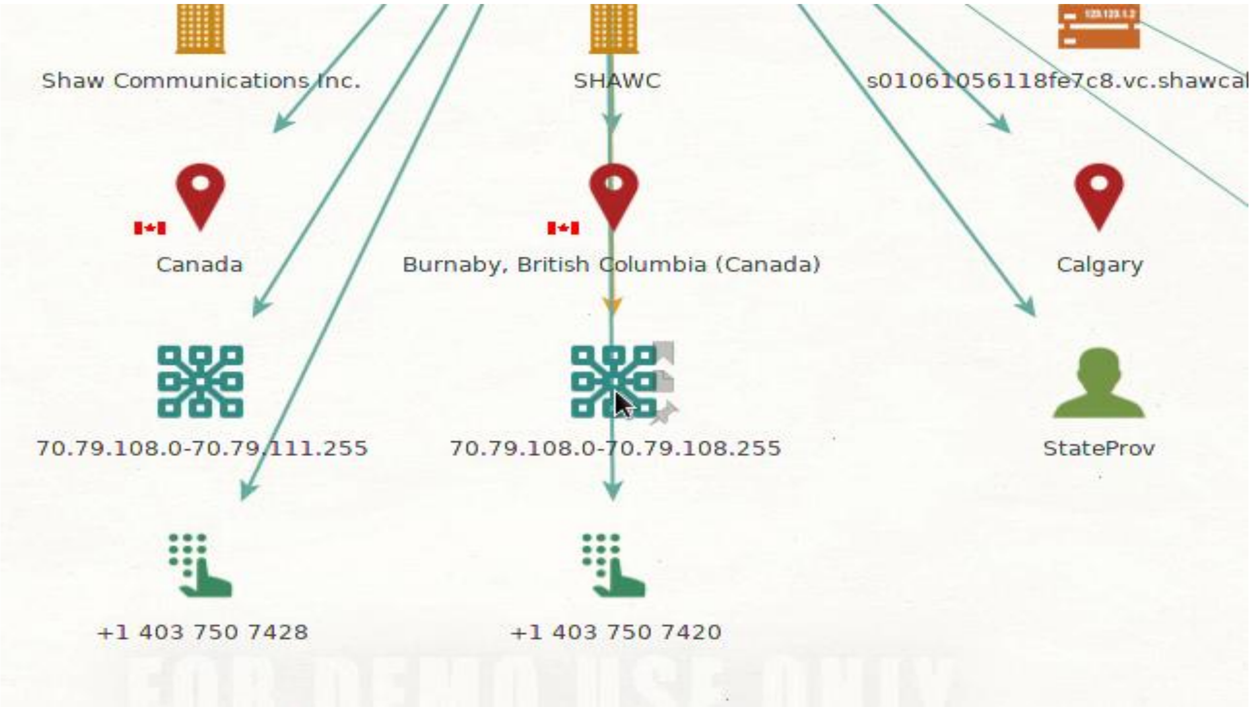
Task 1 – My Network

Since it is better to not perform OSINT on anyone else, so I will perform OSINT on my own network using my IPv4 address.

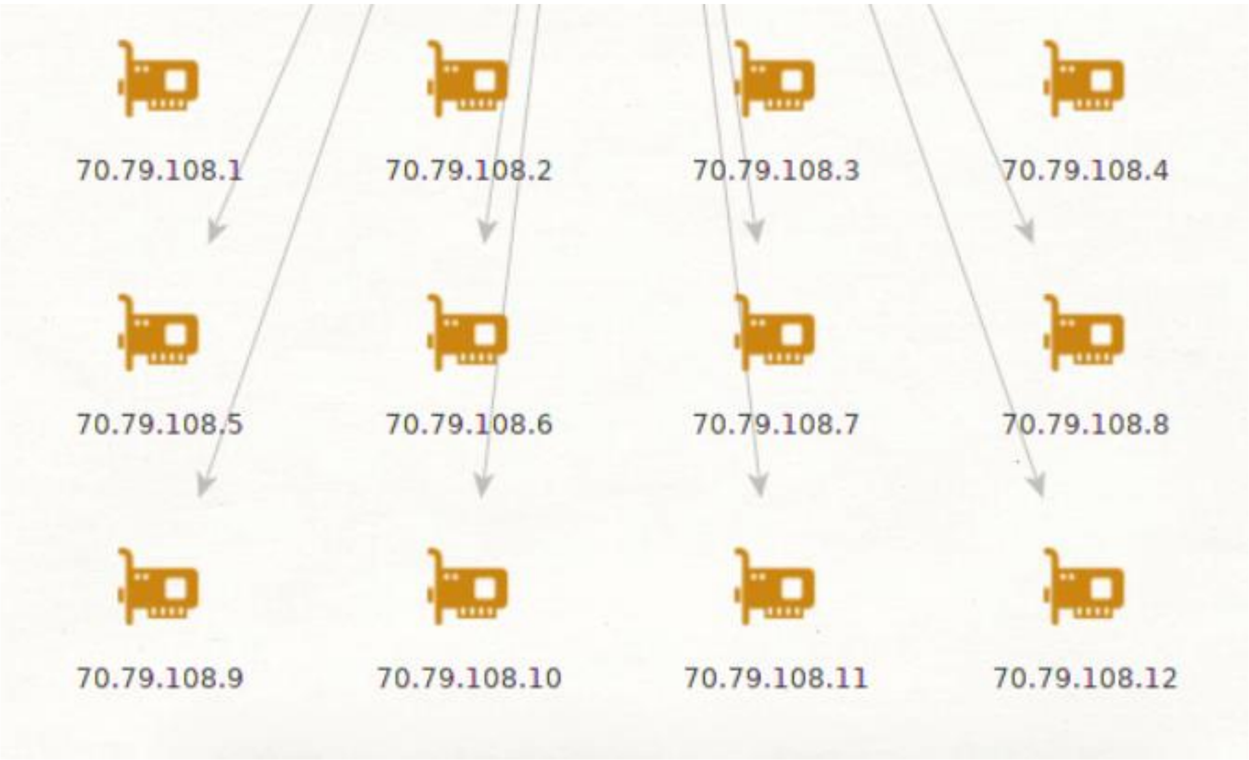
Maltego's basic functions allow users to gather some information about the IP address. Such as IP owner details. Inside that, users could gather GPS information of the target IP, contract information if the information is available.

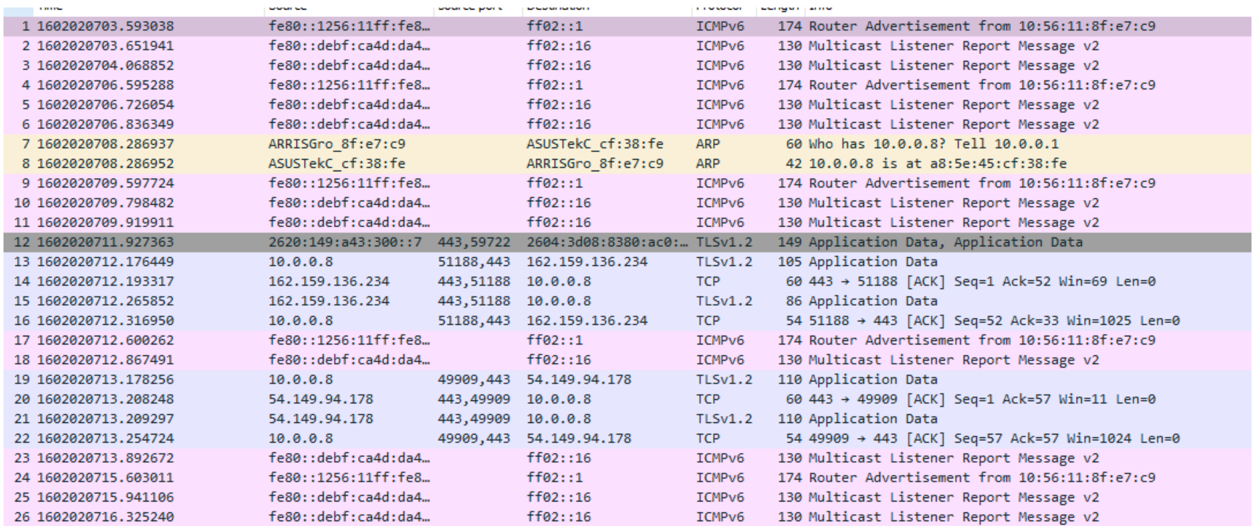


Besides that, it gathers information like alternative DNS, IP addresses in the bock, netblock information, network provider, network provider GPS information, contact information.



Also, users can know what other devices in the network.





```
 1 1602020703.593038  fe80::1256:11ff:fe8…             ff02::1              ICMPv6   174 Router Advertisement from 10:56:11:8f:e7:c9
 2 1602020703.651941  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
 3 1602020704.068852  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
 4 1602020706.595288  fe80::1256:11ff:fe8…             ff02::1              ICMPv6   174 Router Advertisement from 10:56:11:8f:e7:c9
 5 1602020706.726054  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
 6 1602020706.836349  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
 7 1602020708.286937  ARRISGro_8f:e7:c9                ASUSTekC_cf:38:fe    ARP       60 Who has 10.0.0.8? Tell 10.0.0.1
 8 1602020708.286952  ASUSTekC_cf:38:fe                ARRISGro_8f:e7:c9    ARP       42 10.0.0.8 is at a8:5e:45:cf:38:fe
 9 1602020709.597724  fe80::1256:11ff:fe8…             ff02::1              ICMPv6   174 Router Advertisement from 10:56:11:8f:e7:c9
10 1602020709.798482  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
11 1602020709.919911  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
12 1602020711.927363  2620:149:a43:300::7  443,59722   2604:3d08:8380:ac0:… TLSv1.2  149 Application Data, Application Data
13 1602020712.176449  10.0.0.8             51188,443   162.159.136.234      TLSv1.2  105 Application Data
14 1602020712.193317  162.159.136.234      443,51188   10.0.0.8             TCP       60 443 → 51188 [ACK] Seq=1 Ack=52 Win=69 Len=0
15 1602020712.265852  162.159.136.234      443,51188   10.0.0.8             TLSv1.2   86 Application Data
16 1602020712.316950  10.0.0.8             51188,443   162.159.136.234      TCP       54 51188 → 443 [ACK] Seq=52 Ack=33 Win=1025 Len=0
17 1602020712.600262  fe80::1256:11ff:fe8…             ff02::1              ICMPv6   174 Router Advertisement from 10:56:11:8f:e7:c9
18 1602020712.867491  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
19 1602020713.178256  10.0.0.8             49909,443   54.149.94.178        TLSv1.2  110 Application Data
20 1602020713.208248  54.149.94.178        443,49909   10.0.0.8             TCP       60 443 → 49909 [ACK] Seq=1 Ack=57 Win=11 Len=0
21 1602020713.209297  54.149.94.178        443,49909   10.0.0.8             TLSv1.2  110 Application Data
22 1602020713.254724  10.0.0.8             49909,443   54.149.94.178        TCP       54 49909 → 443 [ACK] Seq=57 Ack=57 Win=1024 Len=0
23 1602020713.892672  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
24 1602020715.603011  fe80::1256:11ff:fe8…             ff02::1              ICMPv6   174 Router Advertisement from 10:56:11:8f:e7:c9
25 1602020715.941106  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
26 1602020716.325240  fe80::debf:ca4d:da4…             ff02::16             ICMPv6   130 Multicast Listener Report Message v2
```

Notice that Wireshark does not capture any taffic from Maltego. It is hard for detection systems or firewalls to stop grabbing information by Maltogo.

Gathering publicly available information using search engines, like Google, and manual techniques, like visiting the target website or office, is time-consuming and exhausting. Maltego automates the information gathering process will save a lot of time for the attackers.

That information will be very helpful if the target network is a company. Attackers can directly grab email address to perform email spoofing, or understand the DNS of the company to perform DNS attack suck as Dos or DDos attacks, or social network profiles of a person or company to perform social engineering attack or pawn the victim for more information.

With Maltego it is also possible to find links into and out of any particular site. It also returns the plugins used in a blog, links to social networking sites, Facebook pages, and so on.

Defence

Individuals should not use the same email for everything, including social media account, website registration and personal use. Should create a sperate email account and only use personal email on a private network.

Conclusion

Starting out with just the IP of a machine, we obtained a network provider on which we executed transforms, which in turn led us to a netblock. We were able to establish external links within the netblock and determined the websites that the IP address was associated with. It is possible to gather emails associated with the IP. From there, we could gather any URL related to the email or any social networks to perform further pawn or malicious activities.