Covert IP Allocation

By Ramece Cave

Introduction

The purpose of this document is to outline a method for gaining access to a network without DHCP, host enumeration tools, or a stealthy method is needed to go gain access.

Network Discovery

First we establish an interface with no IP address assigned or routes specified, and an empty ARP cache. The host used for this example will be refereed to as ‘oddjob’

```
root@oddjob:~# ifconfig eth0 up
root@oddjob:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0B:DB:01:69:36
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:1 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:100
          RX bytes:314 (314.0 b)  TX bytes:60 (60.0 b)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

root@oddjob:~#

root@oddjob:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
root@oddjob:~# arp -an
root@oddjob:~#
```

Use a packet sniffer to monitor the broadcast packets coming across the wire. Look for broadcasts originating from perimeter devices. Sniffers will also be used to examine response packets later in the document. Below are Tcpdump packet captures collected on the target network at different times.

```
00:07:18.654251 192.168.10.100.1030 > 192.168.10.255.162:  Trap(33)  .1.3.6.1.4.1.3955.2.2.1 192.168.10.100
enterpriseSpecific[specific-trap(1)!=0] 39810[|snmp]
02:49:12.587335 192.168.10.100.1900 > 239.255.255.250.1900: udp 280 (DF)
02:49:12.588597 192.168.10.100.1900 > 239.255.255.250.1900: udp 275 (DF)
02:49:12.590943 192.168.10.100.1900 > 239.255.255.250.1900: udp 352 (DF)
03:36:24.791734 192.168.10.100 > 224.0.0.1: igmp query v2 (DF) [ttl 1]
03:36:27.337345 192.168.10.89 > 239.255.255.253: igmp v2 report 239.255.255.253 [ttl 1]
03:36:27.464322 192.168.10.100 > 224.0.0.2: igmp v2 report 224.0.0.2 (DF) [ttl 1]
03:36:31.338558 192.168.10.89 > 224.0.0.251: igmp v2 report 224.0.0.251 [ttl 1]
03:36:31.956641 192.168.10.100 > 239.255.255.250: igmp v2 report 239.255.255.250 (DF) [ttl 1]
03:36:40.049422 192.168.10.89.50131 > 239.255.255.253.427: udp 36 [ttl 1]
03:36:40.050987 192.168.10.89.50134 > 239.255.255.253.427: udp 36 [ttl 1]
03:36:40.299378 192.168.10.89.50135 > 192.168.10.255.137: NBT UDP PACKET(137): QUERY; REQUEST;
BROADCAST
03:36:40.570326 192.168.10.89.50135 > 192.168.10.255.137: NBT UDP PACKET(137): QUERY; REQUEST;
BROADCAST
```

In the packet dump above, IGMP, SNMP and SSDP broadcast packets are observed originating from 192.168.10.100. NetBIOS and IGMP broadcasts are also originating from 192.168.10.89, this source is possibly a workstation on the network. Based on these findings 192.168.10.100 is probably a router or network device.

The following network parameters were determined based the examination of the packets.

```
network: 192.168.10.0
netmask: 192.168.10.255
broadcast: 255.255.255.0
gateway: 192.168.10.100
```

Host Discovery

In order to begin finding available IP addresses we must first configure our adapters to make a pseudo connection to the network. Any attempts to ping or connect to hosts on the network prior to this will subsequently fail. The pings below outline attempts to ping the network address and an online host.

```
root@oddjob:~# ping 192.168.10.0
PING 192.168.10.0 (192.168.10.0): 56 octets data
sendto: Network is unreachable
ping: sent 64 octets to 192.168.10.0, ret=-1
sendto: Network is unreachable
ping: sent 64 octets to 192.168.10.0, ret=-1
sendto: Network is unreachable

--- 192.168.10.0 ping statistics ---
12 packets transmitted, 0 packets received, 100% packet loss
root@oddjob:~# ping 192.168.10.46
PING 192.168.10.46 (192.168.10.46): 56 octets data
sendto: Network is unreachable
ping: sent 64 octets to 192.168.10.46, ret=-1
sendto: Network is unreachable
ping: sent 64 octets to 192.168.10.46, ret=-1
sendto: Network is unreachable

--- 192.168.10.46 ping statistics ---
9 packets transmitted, 0 packets received, 100% packet loss
root@oddjob:~#
```

An un-numbered interface is configured along with the determined routes to allow the host to pseudo-communicate on the network. Configure an un-numbered interface and add the network route to the system.

```
root@oddjob:~# ifconfig eth0 0.0.0.0 up
root@oddjob:~# route add -net 192.168.10.0 netmask 255.255.255.0 eth0
root@oddjob:# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0B:DB:01:69:36
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2281 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2903 errors:0 dropped:0 overruns:0 carrier:0
          collisions:95 txqueuelen:1000
          RX bytes:1403286 (1.3 Mb)  TX bytes:311099 (303.8 Kb)
          Interrupt:10 Base address:0x3000

root@oddjob:# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
root@oddjob:#
```

Hosts that are offline or available ☺ will receive an ICMP type 3 [Host Unreachable] message from the loopback address.

Hosts that are online or unavailable will receive the ICMP packet and respond to the original request. Currently Oddjob does not have an IP address the responses are never received.

[192.168.10.57] – Available (offline or unallocated)

```
root@oddjob:~# ping 192.168.10.57
PING 192.168.10.48 (192.168.10.47) 56(84) bytes of data.
From 127.0.0.1 icmp_seq=2 Destination Host Unreachable
From 127.0.0.1 icmp_seq=3 Destination Host Unreachable
From 127.0.0.1 icmp_seq=4 Destination Host Unreachable
From 127.0.0.1 icmp_seq=6 Destination Host Unreachable
From 127.0.0.1 icmp_seq=7 Destination Host Unreachable
From 127.0.0.1 icmp_seq=8 Destination Host Unreachable
```

Available – Packet Dump

```
03:09:29.355223 arp who-has 192.168.10.57 tell 0.0.0.0
03:09:30.355076 arp who-has 192.168.10.57 tell 0.0.0.0
03:09:31.354916 arp who-has 192.168.10.57 tell 0.0.0.0
03:09:33.355613 arp who-has 192.168.10.57 tell 0.0.0.0
03:09:34.355460 arp who-has 192.168.10.57 tell 0.0.0.0
03:09:35.355307 arp who-has 192.168.10.57 tell 0.0.0.0
```

[192.168.10.46] – Unavailable (online)

```
root@oddjob:~# ping 192.168.10.46
PING 192.168.10.46 (192.168.10.46): 56 octets data

--- 192.168.10.46 ping statistics ---
9 packets transmitted, 0 packets received, 100% packet loss
root@oddjob:~#
```

Unavailable – Packet Dump

```
00:49:48.574565 arp who-has 192.168.10.46 tell 0.0.0.0
00:49:48.574972 arp reply 192.168.10.46 is-at 0:20:78:18:11:87
00:49:48.574989 0.0.0.0 > 192.168.10.46: icmp: echo request (DF)
00:49:49.566051 0.0.0.0 > 192.168.10.46: icmp: echo request (DF)
00:49:50.566048 0.0.0.0 > 192.168.10.46: icmp: echo request (DF)
```

The ARP cache contains a listing for all of the available and unavailable hosts on the network

```
root@oddjob:# arp -an
? (192.168.10.57) at <incomplete> on eth0                    Available
? (192.168.10.200) at <incomplete> on eth0                   Available
? (192.168.10.99) at <incomplete> on eth0                    Available
? (192.168.10.100) at 00:12:17:03:DE:D1 [ether] on eth0      Unavailable
? (192.168.10.46) at 00:07:95:54:DA:CD [ether] on eth0       Unavailable
? (192.168.10.89) at 00:11:24:8D:9A:6A [ether] on eth0       Unavailable
root@oddjob:#
```

Joining The Network

To join the network, delete the previously created route (once the interface is numbered the route will automatically be re-added.) Set the interface information for the network and add the default route. To test the connectivity ping another host on the network.

```
root@oddjob:# route del -net 192.168.10.0 netmask 255.255.255.0 eth0
root@oddjob:# ifconfig eth0 192.168.10.57 broadcast 192.168.10.255 netmask 255.255.255.0 up
root@oddjob:# route add default gw 192.168.10.100
root@oddjob:# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:03:25:10:6A:5B
          inet addr:192.168.10.57  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2331 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2947 errors:0 dropped:0 overruns:0 carrier:0
          collisions:95 txqueuelen:1000
          RX bytes:1409611 (1.3 Mb)  TX bytes:314689 (307.3 Kb)
          Interrupt:10 Base address:0x3000

root@oddjob:# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags   Metric Ref Use Iface
192.168.10.0    0.0.0.0         255.255.255.0   U       0      0    0    eth0
127.0.0.0       0.0.0.0         255.0.0.0       U       0      0    0    lo
0.0.0.0         192.168.10.100  0.0.0.0         UG      0      0    0    eth0
root@oddjob:#

root@oddjob:#ping -c1 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp_seq=1 ttl=64 time=2.91 ms

--- 192.168.10.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.917/2.917/2.917/0.000 ms
root@oddjob:#
```

Conclusion

After connecting to the network now what? The choice is yours, the objective of this paper is to inform the reader on a covert method of accessing a network that is not using DHCP. There are applications and devices available that can simply this method, but they tend to be very noisy, besides you may need to use this on a pen-test. Using this tactic I have successfully accessed three networks not using DHCP during penetration tests. Remember to exercise caution; if an IP address is offline it might be used for another purpose, check with the network administrators to confirm the use prior to allocation.

old school rules
stay low keep moving

Appendix

[192.168.10.82] – Unavailable Host (online)

```
root@oddjob:~# ping 192.168.10.82
PING 192.168.10.82 (192.168.10.82): 56 octets data

--- 192.168.10.82 ping statistics ---
9 packets transmitted, 0 packets received, 100% packet loss
root@oddjob:~#

00:53:47.853078 arp who-has 192.168.10.82 tell 0.0.0.0
00:53:47.855315 arp reply 192.168.10.82 is-at 0:50:56:40:0:49

00:53:47.855335 0.0.0.0 > 192.168.10.82: icmp: echo request (DF)
00:53:48.846051 0.0.0.0 > 192.168.10.82: icmp: echo request (DF)

root@oddjob:~# arp -an
? (192.168.10.11) at 00:20:78:18:11:87 [ether] on eth0
? (192.168.10.82) at 00:50:56:40:00:49 [ether] on eth0
root@oddjob:~#
```

[192.168.10.30] – Available Host (offline or unallocated)

```
root@oddjob:~# ping 192.168.10.30
PING 192.168.10.30 (192.168.10.30): 56 octets data

--- 192.168.10.30 ping statistics ---
9 packets transmitted, 0 packets received, 100% packet loss
root@oddjob:~#
```

Available – Packet Dump

```
00:46:57.845155 arp who-has 192.168.10.30 tell 0.0.0.0
00:46:58.836049 arp who-has 192.168.10.30 tell 0.0.0.0
00:46:59.836035 arp who-has 192.168.10.30 tell 0.0.0.0
00:47:00.836042 127.0.0.1 > 127.0.0.1: icmp: host 192.168.10.30 unreachable [tos 0xc0]
00:47:00.836054 127.0.0.1 > 127.0.0.1: icmp: host 192.168.10.30 unreachable [tos 0xc0]
00:47:00.836057 127.0.0.1 > 127.0.0.1: icmp: host 192.168.10.30 unreachable [tos 0xc0]
```

Online Hosts During Testing

```
root@oddjob:# nmap -sP 192.168.10.0/24

Starting nmap 3.45 ( http://www.insecure.org/nmap/ ) at 2005-02-25 02:54 EST
Host 192.168.10.0 seems to be a subnet broadcast address (returned 2 extra pings).
Host 192.168.10.32 appears to be up.
Host 192.168.10.46 appears to be up.
Host 192.168.10.89 appears to be up.
Host 192.168.10.100 appears to be up.
Host 192.168.10.255 seems to be a subnet broadcast address (returned 3 extra pings).
Nmap run completed -- 256 IP addresses (4 hosts up) scanned in 143.030 seconds
root@oddjob:#
```