Ex040 WireShark

Gary Jones

Contents

Executive Summary

Summary of Findings

KEY006-DqyhqMKZIfctuGGA2/6rEw==

Attack Narrative

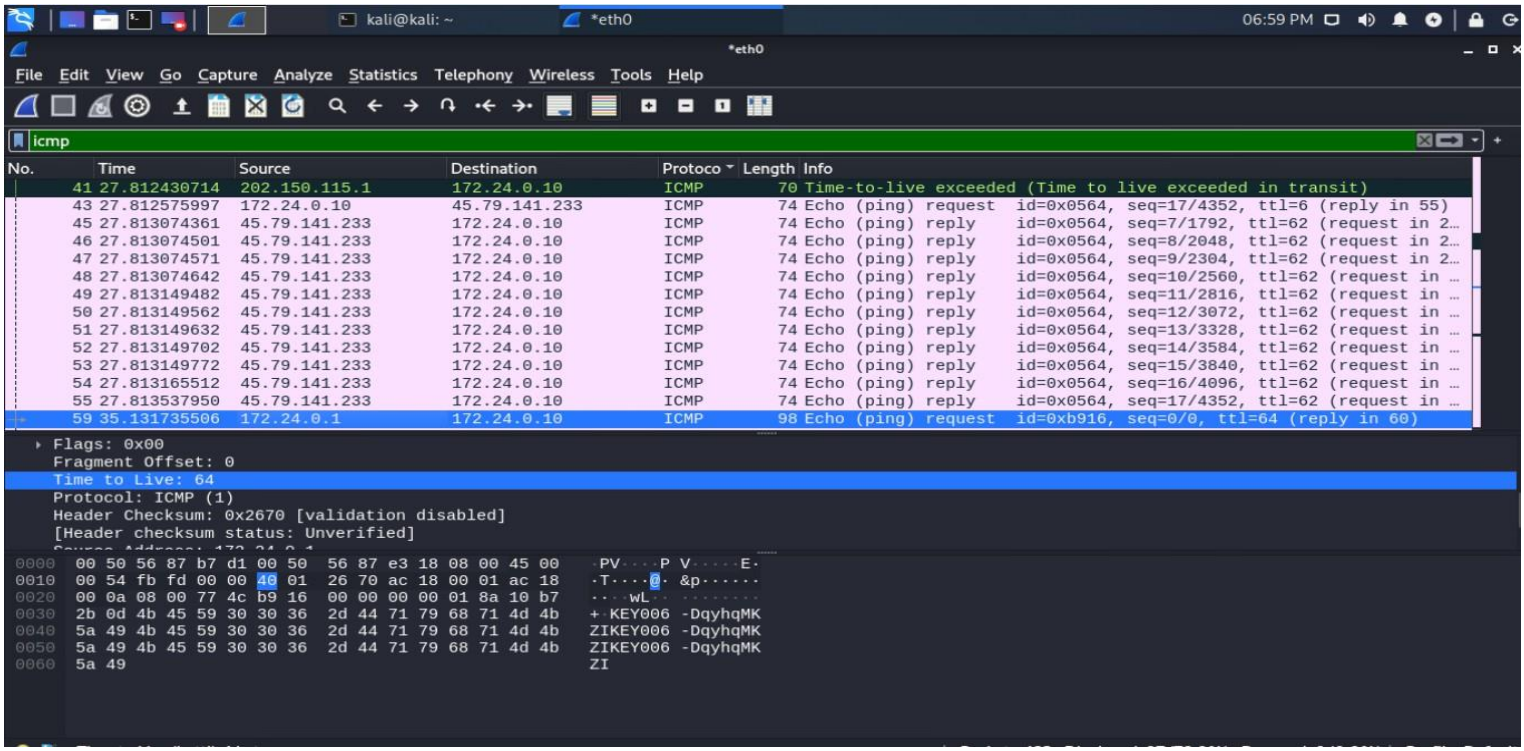
By utilizing the Wireshark traceroute (traceroute -I plunder.pr0b3.com) and traceroute -I ns.artstailor.com) functionality I traced the path using ICMP echo packets. When probing the plunder.pr0b3.com 57 ICMP packets were sent with 7 null responses. These packets came from 3 sources and had 3 different destinations. When probing ns.artstailor.com 50 IMCP packets were sent with 3 null responses. These packets come from 3 sources and go to 3 different destinations.

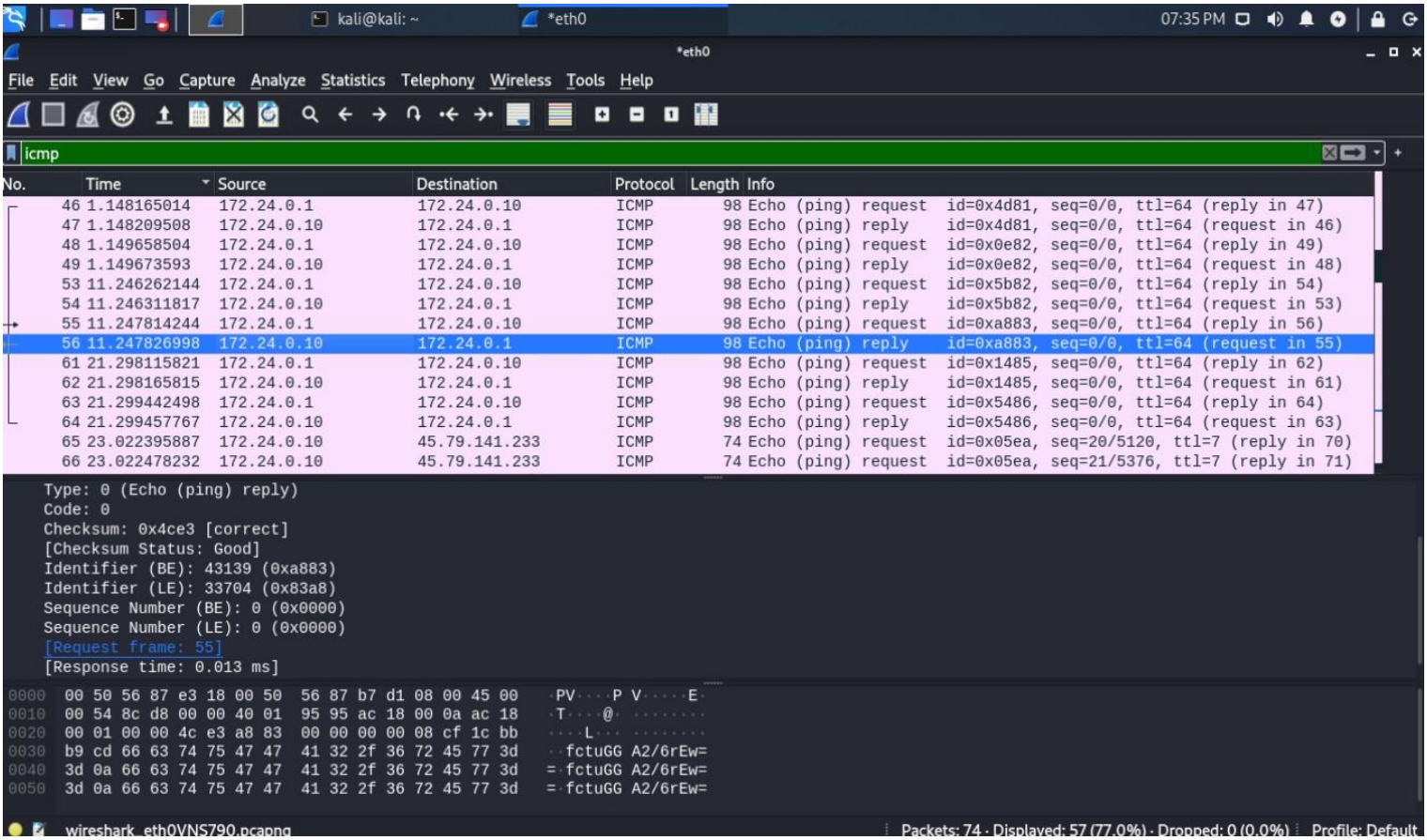
tracerout sent out 28 pings before it stopped but it didn't need to send them all.In the event that the host didn't reply to ICMP ECHO requests or requests from any other default ports I would first use UDP since those are less likely to be ignored than their ICMP counterparts and I would also try and use the -p flag for UDP and ICMP tracing to allow for incremental increasing to find port numbers.

Refer to the images below for a visual description of the steps taken to acquire KEY006.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.24.0.10  netmask 255.255.255.0  broadcast 172.24.0.255
        inet6 fe80::250:56ff:fe87:b7d1  prefixlen 64  scopeid 0×20<link>
        ether 00:50:56:87:b7:d1  txqueuelen 1000  (Ethernet)
        RX packets 261  bytes 23923 (23.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 283  bytes 25359 (24.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 32  bytes 1640 (1.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32  bytes 1640 (1.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo traceroute -I plunder.pr0b3.com
[sudo] password for kali:
traceroute to plunder.pr0b3.com (45.79.141.233), 30 hops max, 60 byte packets
 1  172.24.0.1 (172.24.0.1)  0.260 ms  0.394 ms  0.388 ms
 2  202.150.115.1 (202.150.115.1)  0.641 ms  0.639 ms  0.637 ms
 3  plunder.pr0b3.com (45.79.141.233)  1.278 ms  1.276 ms  1.273 ms

┌──(kali㉿kali)-[~]
└─$
```


kali@kali: ~
*eth0
06:59 PM
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protoco Length Info
41 27.812430714 202.150.115.1 172.24.0.10 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
43 27.812575997 172.24.0.10 45.79.141.233 ICMP 74 Echo (ping) request id=0x0564, seq=17/4352, ttl=6 (reply in 55)
45 27.813074361 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=7/1792, ttl=62 (request in 2…
46 27.813074501 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=8/2048, ttl=62 (request in 2…
47 27.813074571 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=9/2304, ttl=62 (request in 2…
48 27.813074642 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=10/2560, ttl=62 (request in …
49 27.813149482 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=11/2816, ttl=62 (request in …
50 27.813149562 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=12/3072, ttl=62 (request in …
51 27.813149632 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=13/3328, ttl=62 (request in …
52 27.813149702 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=14/3584, ttl=62 (request in …
53 27.813149772 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=15/3840, ttl=62 (request in …
54 27.813165512 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=16/4096, ttl=62 (request in …
55 27.813537950 45.79.141.233 172.24.0.10 ICMP 74 Echo (ping) reply id=0x0564, seq=17/4352, ttl=62 (request in …
59 35.131735506 172.24.0.1 172.24.0.10 ICMP 98 Echo (ping) request id=0xb916, seq=0/0, ttl=64 (reply in 60)
Flags: 0x00
Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x2670 [validation disabled]
[Header checksum status: Unverified]
0000 00 50 56 87 b7 d1 00 50 56 87 e3 18 08 00 45 00 ·PV····P V·····E·
0010 00 54 fb fd 00 00 40 01 26 70 ac 18 00 01 ac 18 ·T····@· &p·····
0020 00 0a 08 00 77 4c b9 16 00 00 00 00 01 8a 10 b7 ····wL·· ········
0030 2b 0d 4b 45 59 30 30 36 2d 44 71 79 68 71 4d 4b + KEY006 -DqyhqMK
0040 5a 49 4b 45 59 30 30 36 2d 44 71 79 68 71 4d 4b ZIKEY006 -DqyhqMK
0050 5a 49 4b 45 59 30 30 36 2d 44 71 79 68 71 4d 4b ZIKEY006 -DqyhqMK
0060 5a 49 ZI


kali@kali: ~
*eth0
07:35 PM
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
46 1.148165014 172.24.0.1 172.24.0.10 ICMP 98 Echo (ping) request id=0x4d81, seq=0/0, ttl=64 (reply in 47)
47 1.148209508 172.24.0.10 172.24.0.1 ICMP 98 Echo (ping) reply id=0x4d81, seq=0/0, ttl=64 (request in 46)
48 1.149658504 172.24.0.1 172.24.0.10 ICMP 98 Echo (ping) request id=0x0e82, seq=0/0, ttl=64 (reply in 49)
49 1.149673593 172.24.0.10 172.24.0.1 ICMP 98 Echo (ping) reply id=0x0e82, seq=0/0, ttl=64 (request in 48)
53 11.246262144 172.24.0.1 172.24.0.10 ICMP 98 Echo (ping) request id=0x5b82, seq=0/0, ttl=64 (reply in 54)
54 11.246311817 172.24.0.10 172.24.0.1 ICMP 98 Echo (ping) reply id=0x5b82, seq=0/0, ttl=64 (request in 53)
55 11.247814244 172.24.0.1 172.24.0.10 ICMP 98 Echo (ping) request id=0xa883, seq=0/0, ttl=64 (reply in 56)
56 11.247826998 172.24.0.10 172.24.0.1 ICMP 98 Echo (ping) reply id=0xa883, seq=0/0, ttl=64 (request in 55)
61 21.298115821 172.24.0.1 172.24.0.10 ICMP 98 Echo (ping) request id=0x1485, seq=0/0, ttl=64 (reply in 62)
62 21.298165815 172.24.0.10 172.24.0.1 ICMP 98 Echo (ping) reply id=0x1485, seq=0/0, ttl=64 (request in 61)
63 21.299442498 172.24.0.1 172.24.0.10 ICMP 98 Echo (ping) request id=0x5486, seq=0/0, ttl=64 (reply in 64)
64 21.299457767 172.24.0.10 172.24.0.1 ICMP 98 Echo (ping) reply id=0x5486, seq=0/0, ttl=64 (request in 63)
65 23.022395887 172.24.0.10 45.79.141.233 ICMP 74 Echo (ping) request id=0x05ea, seq=20/5120, ttl=7 (reply in 70)
66 23.022478232 172.24.0.10 45.79.141.233 ICMP 74 Echo (ping) request id=0x05ea, seq=21/5376, ttl=7 (reply in 71)
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x4ce3 [correct]
[Checksum Status: Good]
Identifier (BE): 43139 (0xa883)
Identifier (LE): 33704 (0x83a8)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Request frame: 55]
[Response time: 0.013 ms]
0000 00 50 56 87 e3 18 00 50 56 87 b7 d1 08 00 45 00 ·PV····P V·····E·
0010 00 54 8c d8 00 00 40 01 95 95 ac 18 00 0a ac 18 ·T····@· ········
0020 00 01 00 00 4c e3 a8 83 00 00 00 00 08 cf 1c bb ····L··· ········
0030 b9 cd 66 63 74 75 47 47 41 32 2f 36 72 45 77 3d ··fctuGG A2/6rEw=
0040 3d 0a 66 63 74 75 47 47 41 32 2f 36 72 45 77 3d =·fctuGG A2/6rEw=
0050 3d 0a 66 63 74 75 47 47 41 32 2f 36 72 45 77 3d =·fctuGG A2/6rEw=
wireshark_eth0VNS790.pcapng
Packets: 74 · Displayed: 57 (77.0%) · Dropped: 0 (0.0%)
Profile: Default