Ex040 - Wireshark

Simon Tobon

2020-9-29

Contents

Executive Summary

For this Exercise we were tasked to deploy several commands in order to find our active ethernet interfaces, and use Wireshark to monitor packets being received and sent during a traceroute on the plunder server and also on the f4rmc0rp domain.

Technical Report

Finding: Description of finding

Risk Rating

There is very low Risk that comes from a traceroute succeeding. All traceroute does is reveals IP address of routers involved in the routing of packets. An attacker having access to an IP address is not very significant.

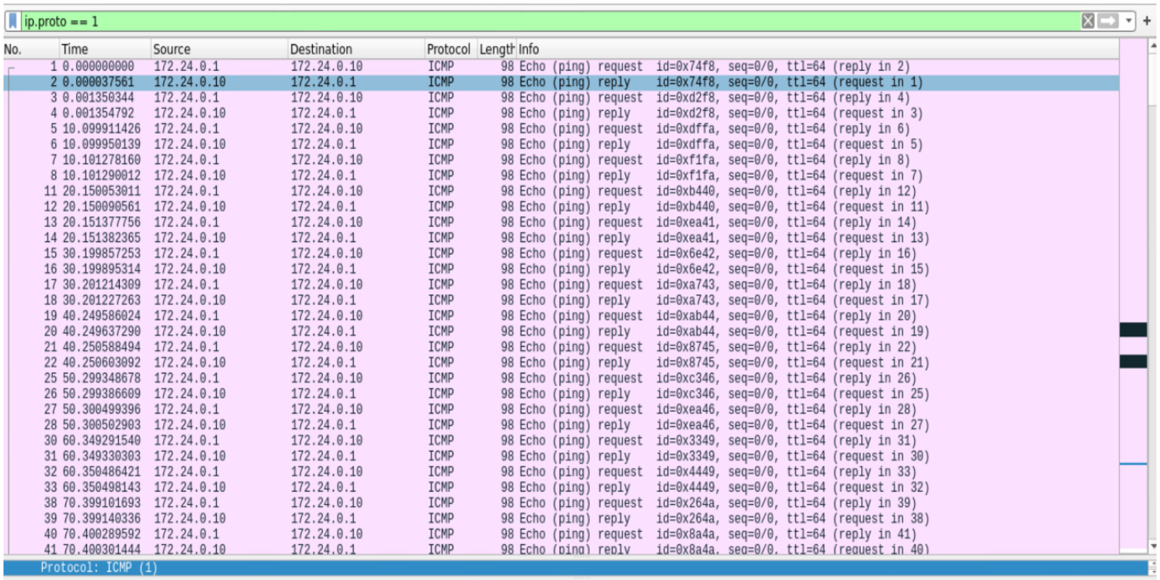
Vulnerability Description

This very small vulnerability will provide some insight on the network for attackers, and although it is not cause for major concern it can be mitigated by blocking ICMP responses. However, this may block other network fundamentals from running correctly, so you must be careful.

Attack Narrative

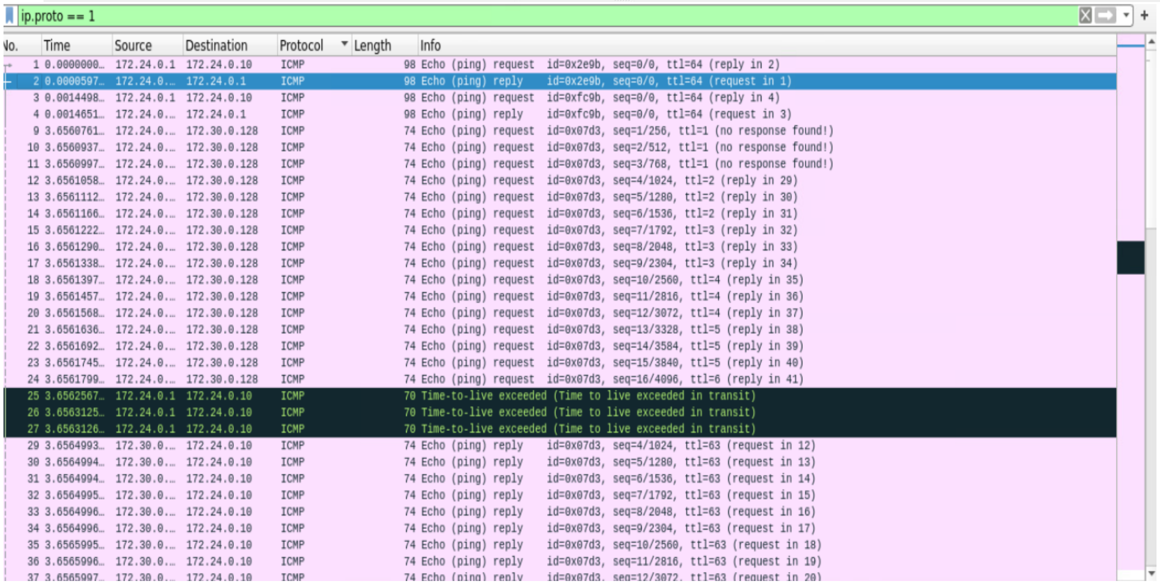
To begin I deployed the ip a command to identify my active Ethernet interfaces. I determined that the interface I would listen on with Wireshark was **eth0**. Next Wireshark was deployed and I selected eth0. Then the following commmand was run on the Terminal: **traceroute -I plunder.pr0b3.com**. This prompted traceroute to send ICMP packets to the plunder server. While Wireshark recorded all the packets I investigated the **traceroute –help 2>&1] less** command. What this command does is print the traceroute man page. 2>&1 specifies the file descriptors, 1 is the standard output (stdout) and 2 us the standard error (stderr). This command redirects stderr to stdout. Then it is piped through the less command, which displays the output one page at a time.

Wireshark found 85 total packets and 66 of those were ICMP packets. 73 pings were sent and 68 of them were ping requests. If a host did not reply to ICMP Echo requests then we could work around this by using a TCP traceroute as this bypasses the firewall. There was an ICMP packet I did not expect to find, this was the one that actually contained the key! The KEY was: **KEY006:Q6WAEkV0BzbstjreqrQQ==**. I suspect that there is a script to deliver this packet for the assignment.



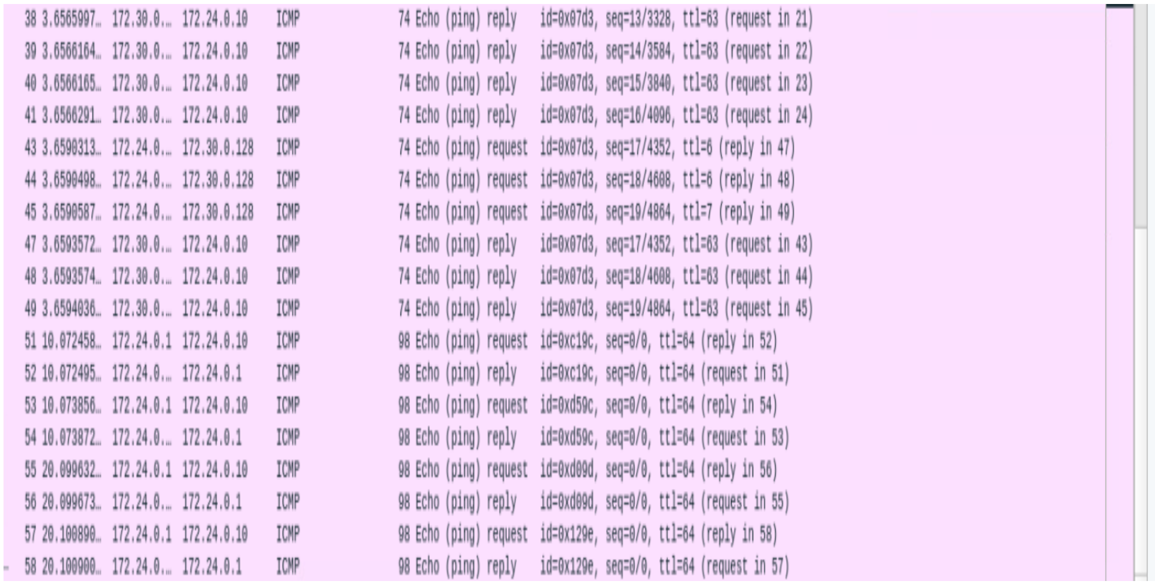
```
ip.proto == 1

No.  Time         Source       Destination  Protocol Length Info
   1 0.000000000  172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0x74f8, seq=0/0, ttl=64 (reply in 2)
   2 0.000037561  172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0x74f8, seq=0/0, ttl=64 (request in 1)
   3 0.001350344  172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0xd2f8, seq=0/0, ttl=64 (reply in 4)
   4 0.001354792  172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0xd2f8, seq=0/0, ttl=64 (request in 3)
   5 10.099911426 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0xdffa, seq=0/0, ttl=64 (reply in 6)
   6 10.099950139 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0xdffa, seq=0/0, ttl=64 (request in 5)
   7 10.101278160 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0xf1fa, seq=0/0, ttl=64 (reply in 8)
   8 10.101290012 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0xf1fa, seq=0/0, ttl=64 (request in 7)
  11 20.150053011 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0xb440, seq=0/0, ttl=64 (reply in 12)
  12 20.150090561 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0xb440, seq=0/0, ttl=64 (request in 11)
  13 20.151377756 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0xea41, seq=0/0, ttl=64 (reply in 14)
  14 20.151382365 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0xea41, seq=0/0, ttl=64 (request in 13)
  15 30.199857253 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0x6e42, seq=0/0, ttl=64 (reply in 16)
  16 30.199895314 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0x6e42, seq=0/0, ttl=64 (request in 15)
  17 30.201214309 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0xa743, seq=0/0, ttl=64 (reply in 18)
  18 30.201227263 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0xa743, seq=0/0, ttl=64 (request in 17)
  19 40.249586024 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0xab44, seq=0/0, ttl=64 (reply in 20)
  20 40.249637290 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0xab44, seq=0/0, ttl=64 (request in 19)
  21 40.250588494 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0x8745, seq=0/0, ttl=64 (reply in 22)
  22 40.250603092 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0x8745, seq=0/0, ttl=64 (request in 21)
  25 50.299348678 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0xc346, seq=0/0, ttl=64 (reply in 26)
  26 50.299386609 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0xc346, seq=0/0, ttl=64 (request in 25)
  27 50.300499396 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0xea46, seq=0/0, ttl=64 (reply in 28)
  28 50.300502903 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0xea46, seq=0/0, ttl=64 (request in 27)
  30 60.349291540 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0x3349, seq=0/0, ttl=64 (reply in 31)
  31 60.349330303 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0x3349, seq=0/0, ttl=64 (request in 30)
  32 60.350486421 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0x4449, seq=0/0, ttl=64 (reply in 33)
  33 60.350498143 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0x4449, seq=0/0, ttl=64 (request in 32)
  38 70.399101693 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0x264a, seq=0/0, ttl=64 (reply in 39)
  39 70.399140336 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0x264a, seq=0/0, ttl=64 (request in 38)
  40 70.400289592 172.24.0.1   172.24.0.10  ICMP      98 Echo (ping) request  id=0x8a4a, seq=0/0, ttl=64 (reply in 41)
  41 70.400301444 172.24.0.10  172.24.0.1   ICMP      98 Echo (ping) reply    id=0x8a4a, seq=0/0, ttl=64 (request in 40)
    Protocol: ICMP (1)
```



```
ip.proto == 1

No.  Time         Source        Destination   Protocol  Length  Info
   1 0.0000000…   172.24.0.1    172.24.0.10   ICMP      98 Echo (ping) request  id=0x2e9b, seq=0/0, ttl=64 (reply in 2)
   2 0.0000597…   172.24.0.…    172.24.0.1    ICMP      98 Echo (ping) reply    id=0x2e9b, seq=0/0, ttl=64 (request in 1)
   3 0.0014498…   172.24.0.1    172.24.0.10   ICMP      98 Echo (ping) request  id=0xfc9b, seq=0/0, ttl=64 (reply in 4)
   4 0.0014651…   172.24.0.…    172.24.0.1    ICMP      98 Echo (ping) reply    id=0xfc9b, seq=0/0, ttl=64 (request in 3)
   9 3.6560761…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=1/256, ttl=1 (no response found!)
  10 3.6560937…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=2/512, ttl=1 (no response found!)
  11 3.6560997…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=3/768, ttl=1 (no response found!)
  12 3.6561058…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=4/1024, ttl=2 (reply in 29)
  13 3.6561112…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=5/1280, ttl=2 (reply in 30)
  14 3.6561166…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=6/1536, ttl=2 (reply in 31)
  15 3.6561222…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=7/1792, ttl=3 (reply in 32)
  16 3.6561290…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=8/2048, ttl=3 (reply in 33)
  17 3.6561338…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=9/2304, ttl=3 (reply in 34)
  18 3.6561397…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=10/2560, ttl=4 (reply in 35)
  19 3.6561457…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=11/2816, ttl=4 (reply in 36)
  20 3.6561568…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=12/3072, ttl=4 (reply in 37)
  21 3.6561636…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=13/3328, ttl=5 (reply in 38)
  22 3.6561692…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=14/3584, ttl=5 (reply in 39)
  23 3.6561745…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=15/3840, ttl=5 (reply in 40)
  24 3.6561799…   172.24.0.…    172.30.0.128  ICMP      74 Echo (ping) request  id=0x07d3, seq=16/4096, ttl=6 (reply in 41)
  25 3.6562567…   172.24.0.1    172.24.0.10   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  26 3.6563125…   172.24.0.1    172.24.0.10   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  27 3.6563126…   172.24.0.1    172.24.0.10   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  29 3.6564993…   172.30.0.…    172.24.0.10   ICMP      74 Echo (ping) reply    id=0x07d3, seq=4/1024, ttl=63 (request in 12)
  30 3.6564994…   172.30.0.…    172.24.0.10   ICMP      74 Echo (ping) reply    id=0x07d3, seq=5/1280, ttl=63 (request in 13)
  31 3.6564994…   172.30.0.…    172.24.0.10   ICMP      74 Echo (ping) reply    id=0x07d3, seq=6/1536, ttl=63 (request in 14)
  32 3.6564995…   172.30.0.…    172.24.0.10   ICMP      74 Echo (ping) reply    id=0x07d3, seq=7/1792, ttl=63 (request in 15)
  33 3.6564996…   172.30.0.…    172.24.0.10   ICMP      74 Echo (ping) reply    id=0x07d3, seq=8/2048, ttl=63 (request in 16)
  34 3.6564996…   172.30.0.…    172.24.0.10   ICMP      74 Echo (ping) reply    id=0x07d3, seq=9/2304, ttl=63 (request in 17)
  35 3.6565995…   172.30.0.…    172.24.0.10   ICMP      74 Echo (ping) reply    id=0x07d3, seq=10/2560, ttl=63 (request in 18)
  36 3.6565996…   172.30.0.…    172.24.0.10   ICMP      74 Echo (ping) reply    id=0x07d3, seq=11/2816, ttl=63 (request in 19)
  37 3.6565997…   172.30.0.…    172.24.0.10   ICMP      74 Echo (ping) reply    id=0x07d3, seq=12/3072, ttl=63 (request in 20)
```



```
38 3.6565997… 172.30.0.… 172.24.0.10   ICMP   74 Echo (ping) reply    id=0x07d3, seq=13/3328, ttl=63 (request in 21)
39 3.6566164… 172.30.0.… 172.24.0.10   ICMP   74 Echo (ping) reply    id=0x07d3, seq=14/3584, ttl=63 (request in 22)
40 3.6566165… 172.30.0.… 172.24.0.10   ICMP   74 Echo (ping) reply    id=0x07d3, seq=15/3840, ttl=63 (request in 23)
41 3.6566291… 172.30.0.… 172.24.0.10   ICMP   74 Echo (ping) reply    id=0x07d3, seq=16/4096, ttl=63 (request in 24)
43 3.6590313… 172.24.0.… 172.30.0.128  ICMP   74 Echo (ping) request  id=0x07d3, seq=17/4352, ttl=6 (reply in 47)
44 3.6590498… 172.24.0.… 172.30.0.128  ICMP   74 Echo (ping) request  id=0x07d3, seq=18/4608, ttl=6 (reply in 48)
45 3.6590587… 172.24.0.… 172.30.0.128  ICMP   74 Echo (ping) request  id=0x07d3, seq=19/4864, ttl=7 (reply in 49)
47 3.6593572… 172.30.0.… 172.24.0.10   ICMP   74 Echo (ping) reply    id=0x07d3, seq=17/4352, ttl=63 (request in 43)
48 3.6593574… 172.30.0.… 172.24.0.10   ICMP   74 Echo (ping) reply    id=0x07d3, seq=18/4608, ttl=63 (request in 44)
49 3.6594036… 172.30.0.… 172.24.0.10   ICMP   74 Echo (ping) reply    id=0x07d3, seq=19/4864, ttl=63 (request in 45)
51 10.072458… 172.24.0.1 172.24.0.10   ICMP   98 Echo (ping) request  id=0xc19c, seq=0/0, ttl=64 (reply in 52)
52 10.072495… 172.24.0.… 172.24.0.1    ICMP   98 Echo (ping) reply    id=0xc19c, seq=0/0, ttl=64 (request in 51)
53 10.073856… 172.24.0.1 172.24.0.10   ICMP   98 Echo (ping) request  id=0xd59c, seq=0/0, ttl=64 (reply in 54)
54 10.073872… 172.24.0.… 172.24.0.1    ICMP   98 Echo (ping) reply    id=0xd59c, seq=0/0, ttl=64 (request in 53)
55 20.099632… 172.24.0.1 172.24.0.10   ICMP   98 Echo (ping) request  id=0xd09d, seq=0/0, ttl=64 (reply in 56)
56 20.099673… 172.24.0.… 172.24.0.1    ICMP   98 Echo (ping) reply    id=0xd09d, seq=0/0, ttl=64 (request in 55)
57 20.100890… 172.24.0.1 172.24.0.10   ICMP   98 Echo (ping) request  id=0x129e, seq=0/0, ttl=64 (reply in 58)
58 20.100900… 172.24.0.… 172.24.0.1    ICMP   98 Echo (ping) reply    id=0x129e, seq=0/0, ttl=64 (request in 57)
```