تمرین چهارم

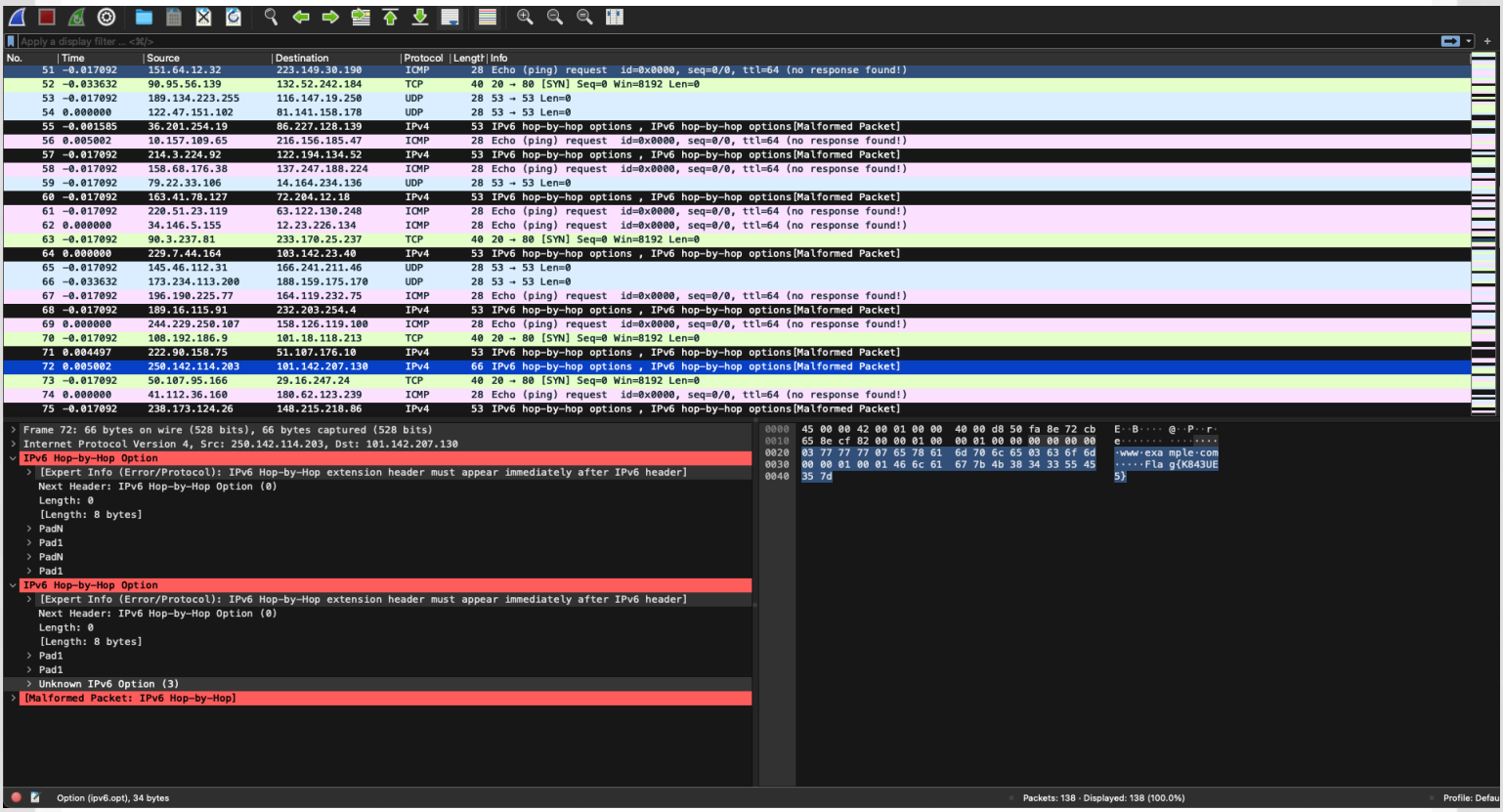
پرنیا اسماعیل پور - ۹۹۰۲۹۲۳

۱. فایل رو با Wiresharkباز کردم بعد دونه دونه پکت هارو نگاه کردم توی شماره پکت ۷۲ میشه فلگ رو دید فلگ رو کپی کردم

۲. بیشتر پکت ها از پروتکل های TCP (۳۶پکت) و UDP به تعداد (۳۱ پکت) هستن که برای برنامه ها و سرویس های شبکه رایج هستند.
در کنار این دو پروتکل (۲۱ پکت)ICMP با فلگ IPv4 وجود دارد.
توی این پکت ها بنظر میرسه که مبدا بیشترشون:
۲۶.۲۱۳.۲۳۲.۹۹
۴۶.۱۹۳.۱۰۱.۲۳۹
۲۱۴.۱۳۱.۲۲۹.۳۱
۱۶۰.۱۶۹.۱۵۵.۱۳
۱۹۳.۲۰۱.۵.۲۱۷
و مقصد بیشترشون:
۱۰۴.۱۴۱.۲۰۸.۱۱۰
۲۵.۹۴.۲۲۵.۱۰۲
۸۴.۲۴.۱۵۱.۷۳
۱۳۴.۲۴۲.۹۸.۲۰
۱۸۱.۲۴۶.۲۴۲.۱۳۸
هستند.

وجود ریکوئست های متعدد ICMP echo و پکت های IPv6 اشتباه
و پکت های TCP با مجموعه فلگ SYN
باعث آسیب پذیری های امنیتی احتمالی میشود .

همچنین قسمت زیادی از ترافیک UDP مربوط به DNS (پورت ۵۳) هست که عادی هست.


Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
51 -0.017092 151.64.12.32 223.149.30.190 ICMP 28 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
52 -0.033632 90.95.56.139 132.52.242.184 TCP 40 20 → 80 [SYN] Seq=0 Win=8192 Len=0
53 -0.017092 189.134.223.255 116.147.19.250 UDP 28 53 → 53 Len=0
54 0.000000 122.47.151.102 81.141.158.178 UDP 28 53 → 53 Len=0
55 -0.001585 36.201.254.19 86.227.128.139 IPv4 53 IPv6 hop-by-hop options , IPv6 hop-by-hop options[Malformed Packet]
56 0.005002 10.157.109.65 216.156.185.47 ICMP 28 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
57 -0.017092 214.3.224.92 122.194.134.52 IPv4 53 IPv6 hop-by-hop options , IPv6 hop-by-hop options[Malformed Packet]
58 -0.017092 158.68.176.38 137.247.188.224 ICMP 28 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
59 -0.017092 79.22.33.106 14.164.234.136 UDP 28 53 → 53 Len=0
60 -0.017092 163.41.78.127 72.204.12.18 IPv4 53 IPv6 hop-by-hop options , IPv6 hop-by-hop options[Malformed Packet]
61 -0.017092 220.51.23.119 63.122.130.248 ICMP 28 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
62 0.000000 34.146.5.155 12.23.226.134 ICMP 28 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
63 -0.017092 90.3.237.81 233.170.25.237 TCP 40 20 → 80 [SYN] Seq=0 Win=8192 Len=0
64 0.000000 229.7.44.164 103.142.23.40 IPv4 53 IPv6 hop-by-hop options , IPv6 hop-by-hop options[Malformed Packet]
65 -0.017092 145.46.112.31 166.241.211.46 UDP 28 53 → 53 Len=0
66 -0.033632 173.234.113.200 188.159.175.170 UDP 28 53 → 53 Len=0
67 -0.017092 196.190.225.77 164.119.232.75 ICMP 28 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
68 -0.017092 189.16.115.91 232.203.254.4 IPv4 53 IPv6 hop-by-hop options , IPv6 hop-by-hop options[Malformed Packet]
69 0.000000 244.229.250.107 158.126.119.100 ICMP 28 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
70 -0.017092 108.192.186.9 101.18.118.213 TCP 40 20 → 80 [SYN] Seq=0 Win=8192 Len=0
71 0.004497 222.90.158.75 51.107.176.10 IPv4 53 IPv6 hop-by-hop options , IPv6 hop-by-hop options[Malformed Packet]
72 0.005002 250.142.114.203 101.142.207.130 IPv4 66 IPv6 hop-by-hop options , IPv6 hop-by-hop options[Malformed Packet]
73 -0.017092 50.107.95.166 29.16.247.24 TCP 40 20 → 80 [SYN] Seq=0 Win=8192 Len=0
74 0.000000 41.112.36.160 180.62.123.239 ICMP 28 Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
75 -0.017092 238.173.124.26 148.215.218.86 IPv4 53 IPv6 hop-by-hop options , IPv6 hop-by-hop options[Malformed Packet]
Frame 72: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Internet Protocol Version 4, Src: 250.142.114.203, Dst: 101.142.207.130
IPv6 Hop-by-Hop Option
[Expert Info (Error/Protocol): IPv6 Hop-by-Hop extension header must appear immediately after IPv6 header]
Next Header: IPv6 Hop-by-Hop Option (0)
Length: 0
[Length: 8 bytes]
PadN
Pad1
PadN
Pad1
IPv6 Hop-by-Hop Option
[Expert Info (Error/Protocol): IPv6 Hop-by-Hop extension header must appear immediately after IPv6 header]
Next Header: IPv6 Hop-by-Hop Option (0)
Length: 0
[Length: 8 bytes]
Pad1
Pad1
Unknown IPv6 Option (3)
[Malformed Packet: IPv6 Hop-by-Hop]
0000 45 00 00 42 00 01 00 00 40 00 d8 50 fa 8e 72 cb E··B···· @··P··r·
0010 65 8e cf 82 00 00 01 00 00 01 00 00 00 00 00 00 e··· ····
0020 03 77 77 77 07 65 78 61 6d 70 6c 65 03 63 6f 6d ·www·exa mple·com
0030 00 00 01 00 01 46 6c 61 67 7b 4b 38 34 33 55 45 ····Fla g{K843UE
0040 35 7d 5}
Option (ipv6.opt), 34 bytes
Packets: 138 · Displayed: 138 (100.0%)
Profile: Defau