Analiza 6.tcpd

1. Przesłano 1 bajt „00001010” za pomocą protokołu UDP na IP 150.254.76.1 port 40. Została złapana ramka Ethernet II pomiędzy Klientem , o IP w sieci lokalnej 192.168.1.100 i adresie MAC 00:17:31:88:28:d2 (wytwórca ASUSTek) przesłana do urządzenia o adresie MAC 00:c0:49:69:2c:12 (Wytwórca US Robotics).

2. Wykorzystano protokoły:
UDP:
Wysłano z portu 32905 na port 40 adresu IP 150.254.76.1 (należy do UAM). To klasa B.
IPv4:
Z komputera o IP 192.168.1.100 (sieć lokalna) na IP 150.254.76.1
Ethernet II:
Z adresu MAC 00:17:31:88:28:d2 na adres MAC 00:c0:49:69:2c:12

3. Pakiet został prawdopodobnie wysłany z systemu Linux. (TTL = 64 na to wskazuje)

4. Nie można określić odległości w routerach.

5. Skaner był uruchomiony na kliencie

6. Zrzut został wykonany „Dec 1, 2007 21:54:18.334228000 CET 1”

8. Przykład programu. (Przykładowy zrzut w pliku 6_example.pcapng a program w 6_program.c)

Analiza 2.tcpd

1. Została złapana ramka Ethernet II pomiędzy Klientem , o IP w sieci lokalnej 192.168.1.100 i adresie MAC
00:17:31:88:28:d2 (wytwórca ASUSTek) przesłana do urządzenia o adresie MAC
00:c0:49:69:2c:12 (Wytwórca US Robotics).
Była to próba nawiązania połączenia TCP z serwerem 150.254.78.2 na porcie 40.

2. Wykorzystano protokoły:
TCP:
Z Flagą SYN z portu o numerze 47043 na port 40 adresu IP
IPv4:
Z 192.168.1.100 do 150.254.78.2
Ethernet II:
Z adresu MAC 00:17:31:88:28:d2 na adres MAC 00:c0:49:69:2c:12

3. Pakiet został prawdopodobnie wysłany z systemu Linux. (TTL = 64 na to wskazuje)

4. Nie można określić odległości w routerach.

5. Skaner był uruchomiony na kliencie

6. Zrzut został wykonany „Dec 1, 2007 21:46:45.315570000 CET”

8. Przykładowy program (zrzut w pliku 2_example.pcapng, a program w 2_program.c)

Tracepath

Wynik polecenia:
tracepath 150.254.78.3

```
 1?: [LOCALHOST]                 pmtu 1500
 1:  _gateway                              1.131ms
 1:  _gateway                              0.916ms
 2:  no reply
 3:  no reply
 4:  no reply
 5:  no reply
 6:  no reply
 7:  185.89.184.2                         85.181ms asymm  8
 8:  no reply
 9:  mx-pcss-1-XE0-1-0-100.man.poznan.pl          43.088ms asymm 13
10:  z-pozman.amu.edu.pl                   73.412ms asymm 14
11:  amur.amu.edu.pl                      78.174ms asymm 15
12:  nat.wmid.amu.edu.pl                   80.483ms asymm 16
13:  nat.wmid.amu.edu.pl                   88.261ms reached
     Resume: pmtu 1500 hops 13 back 16
```

Zrzut w pliku tracepath_wmi-amu-edu-pl.pcapng (wireshark capture filter: host 150.254.78.3 or icmp)

Traceroute

Wynik polecenia:
traceroute 150.254.78.3

```
traceroute to 150.254.78.3 (150.254.78.3), 30 hops max, 60 byte packets
 1  _gateway (192.168.2.1)  0.813 ms  0.967 ms  1.619 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  185.89.184.2 (185.89.184.2)  33.113 ms  25.584 ms  29.927 ms
 8  * * *
 9  mx-pcss-1-XE0-1-0-100.man.poznan.pl (150.254.162.155)  47.130 ms  46.532 ms  46.281 ms
10  z-pozman.amu.edu.pl (150.254.115.10)  46.742 ms  47.266 ms  46.357 ms
11  amur.amu.edu.pl (150.254.116.1)  47.229 ms  47.209 ms  46.879 ms
12  nat.wmid.amu.edu.pl (150.254.115.58)  46.543 ms  46.539 ms  43.461 ms
13  nat.wmid.amu.edu.pl (150.254.115.58)  43.665 ms  33.447 ms  33.666 ms
```

Zrzut w pliku traceroute_wmi-amu-edu-pl.pcapng (wireshark capture filter: host 150.254.78.3 or icmp)

Zrzut zapytania o DNS

Zapytanie zostało wykonane za pomocą polecenia „nslookup uam.edu.pl 8.8.8.8”.
Zrzut w pliku dns_query.pcapng