Esercitazione S11/L4

L'obiettivo dell'esercitazione è acquisire familiarità con l'analisi del traffico DNS utilizzando Wireshark. Attraverso questa attività, si esplora il funzionamento delle query e delle risposte DNS, l'identificazione degli indirizzi MAC e IP associati e l'interpretazione delle informazioni catturate nei pacchetti.

Procedimento

Avviamo di Wireshark: Selezioniamo un'interfaccia di rete attiva per catturare i pacchetti.
Svuotiamo la cache DNS con il comando ipconfig /flushdns
Eseguiamo quindi una query DNS aprendo il prompt dei comandi e utilizzando il comando nslookup per inviare una query DNS a www.cisco.com

Arrestiamo la cattura su wireshark dopo aver eseguito la query.

A questo punto andiamo a filtrare i pacchetti DNS catturati utilizzando il filtro

udp.port == 53 per isolare i pacchetti DNS in transito sulla porta 53

Osservando i dettagli dei pacchetti, possiamo vedere:

- Indirizzi MAC
- Indirizzi IP
- Porte UDP

Possiamo Confrontare gli indirizzi IP e MAC: Confrontare gli indirizzi acquisiti in Wireshark con quelli ottenuti utilizzando il comando ipconfig /all

Si possono inoltre effettuare varie azioni in wireshark:

Analisi dei dettagli DNS:

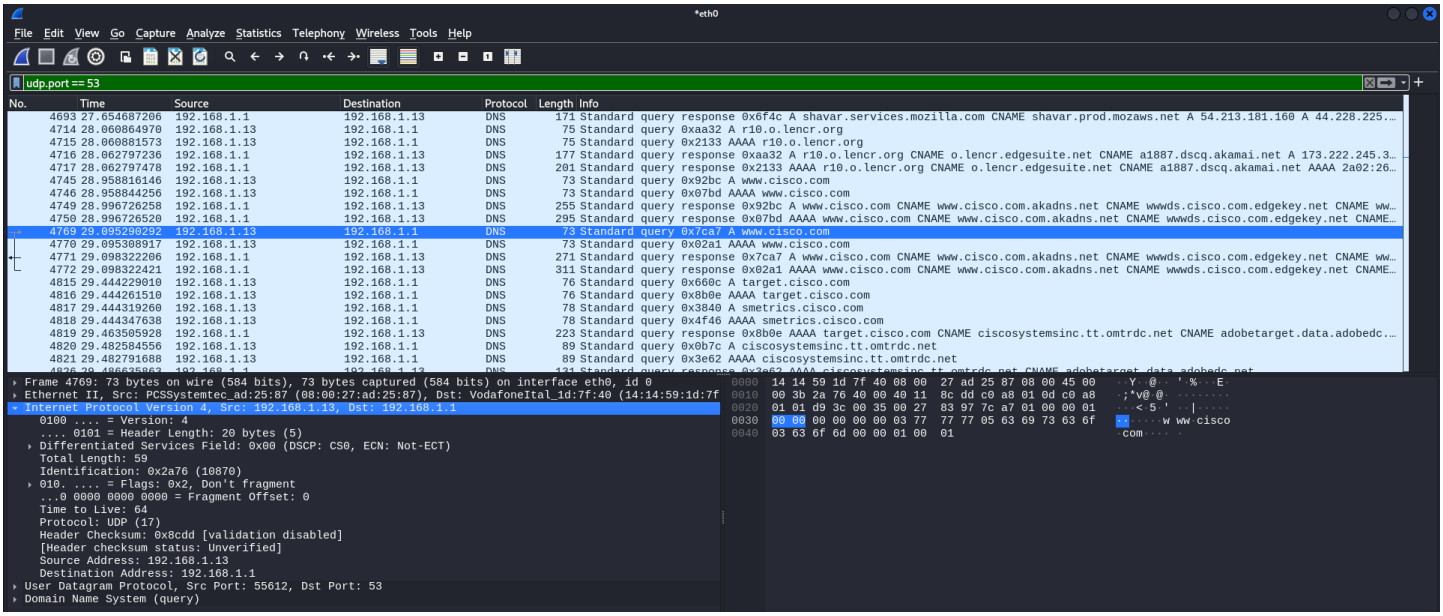
- Espandere la sezione DNS per esaminare i flag e le query. Osservare che il flag indica una query ricorsiva per risolvere www.cisco.com.

Osservare il pacchetto di risposta:

- Identificare il pacchetto DNS di risposta corrispondente alla query.
- Confrontare gli indirizzi MAC, IP e le porte con quelli del pacchetto di query.
- Gli indirizzi sorgente e destinazione sono invertiti rispetto alla query.

Analisi dei dettagli DNS nella risposta:

- Espandere le sezioni Flags, Queries e Answers per verificare la presenza di risposte ricorsive.
- Controllare i record CNAME e A nella sezione Answers. I risultati corrispondono a quelli ottenuti con nslookup.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port == 53
No. Time Source Destination Protocol Length Info
4693 27.654687206 192.168.1.1 192.168.1.13 DNS 171 Standard query response 0x6f4c A shavar.services.mozilla.com CNAME shavar.prod.mozaws.net A 54.213.181.160 A 44.228.225.
4714 28.060864970 192.168.1.13 192.168.1.1 DNS 75 Standard query 0xaa32 A r10.o.lencr.org
4715 28.060881573 192.168.1.13 192.168.1.1 DNS 75 Standard query 0x2133 AAAA r10.o.lencr.org
4716 28.062797236 192.168.1.1 192.168.1.13 DNS 177 Standard query response 0xaa32 A r10.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai.net A 173.222.245.3
4717 28.062797478 192.168.1.1 192.168.1.13 DNS 201 Standard query response 0x2133 AAAA r10.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai.net AAAA 2a02:26
4745 28.958816146 192.168.1.13 192.168.1.1 DNS 73 Standard query 0x92bc A www.cisco.com
4746 28.958844256 192.168.1.13 192.168.1.1 DNS 73 Standard query 0x07bd AAAA www.cisco.com
4749 28.996726258 192.168.1.1 192.168.1.13 DNS 255 Standard query response 0x92bc A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME ww
4750 28.996726520 192.168.1.1 192.168.1.13 DNS 295 Standard query response 0x07bd AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME
4769 29.095290292 192.168.1.13 192.168.1.1 DNS 73 Standard query 0x7ca7 A www.cisco.com
4770 29.095308917 192.168.1.13 192.168.1.1 DNS 73 Standard query 0x02a1 AAAA www.cisco.com
4771 29.098322206 192.168.1.1 192.168.1.13 DNS 271 Standard query response 0x7ca7 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME ww
4772 29.098322421 192.168.1.1 192.168.1.13 DNS 311 Standard query response 0x02a1 AAAA www.cisco.com CNAME www.cisco.com.akadns.net CNAME wwwds.cisco.com.edgekey.net CNAME
4815 29.444229010 192.168.1.13 192.168.1.1 DNS 76 Standard query 0x660c A target.cisco.com
4816 29.444261510 192.168.1.13 192.168.1.1 DNS 76 Standard query 0x8b0e AAAA target.cisco.com
4817 29.444319260 192.168.1.13 192.168.1.1 DNS 78 Standard query 0x3840 A smetrics.cisco.com
4818 29.444347638 192.168.1.13 192.168.1.1 DNS 78 Standard query 0x4f46 AAAA smetrics.cisco.com
4819 29.463505928 192.168.1.1 192.168.1.13 DNS 223 Standard query response 0x8b0e AAAA target.cisco.com CNAME ciscosystemsinc.tt.omtrdc.net CNAME adobetarget.data.adobedc.
4820 29.482584556 192.168.1.13 192.168.1.1 DNS 89 Standard query 0x0b7c A ciscosystemsinc.tt.omtrdc.net
4821 29.482791688 192.168.1.13 192.168.1.1 DNS 89 Standard query 0x3e62 AAAA ciscosystemsinc.tt.omtrdc.net
Frame 4769: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: VodafoneItal_1d:7f:40 (14:14:59:1d:7f
Internet Protocol Version 4, Src: 192.168.1.13, Dst: 192.168.1.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 59
Identification: 0x2a76 (10870)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x8cdd [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.13
Destination Address: 192.168.1.1
User Datagram Protocol, Src Port: 55612, Dst Port: 53
Domain Name System (query)
0000 14 14 59 1d 7f 40 08 00 27 ad 25 87 08 00 45 00
0010 00 3b 2a 76 40 00 40 11 8c dd c0 a8 01 0d c0 a8
0020 01 01 d9 3c 00 35 00 27 83 97 7c a7 01 00 00 01
0030 00 00 00 00 00 00 03 77 77 77 05 63 69 73 63 6f
0040 03 63 6f 6d 00 00 01 00 01