RAPPORTO

Catturare il traffico DNS

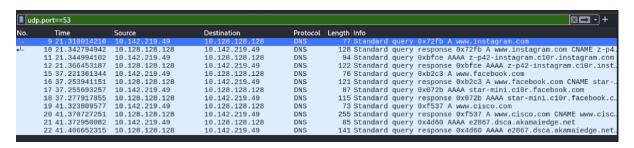
Ho deciso di riavviare il sistema per cancellare tutte le cache, incluso il DNS, poiché Kali Linux ha risposto negativamente a ciascuno dei seguenti comandi:

- sudo systemctl restart systemd-resolved.service
- sudo systemctl restart dnsmasq.service
- sudo systemctl restart nscd.service

Dopo il riavvio, ho prima abilitato Wireshark e poi ho comandato nslookup nel terminale Linux e ho cercato www.instagram.com e altri siti web. Poi ho chiuso nslookup e sono tornato a Wireshark per analizzare il traffico catturato:

Esplorare il traffico delle query DNS

Ho filtrato la porta 53 (DNS) per UDP:



Ho scelto la prima cattura da analizzare. Ethernet II mostra gli indirizzi MAC sia del dispositivo sorgente (in questo caso Linux VM) sia del dispositivo di destinazione (il router):

```
| Frame 9: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0, id 0
| Ethernet II, Src: 32:97:05:d9:84:95 (32:97:05:d9:84:95), Dst: CiscoMeraki_b7:c6:bd (e0:cb:bc:b7:c6:bd)
| Destination: CiscoMeraki_b7:c6:bd (e0:cb:bc:b7:c6:bd) (e0:cb:bc:b7:c6:bd)
| Destination: CiscoMeraki_b7:c6:bd (e0:cb:bc:b7:c6:bd) (e0:cb:bc:b7:c6:
```

Il protocollo Internet versione 4 mostra gli indirizzi IP di origine e destinazione. L'indirizzo IP di destinazione è il gateway in questo caso:

```
Frame 9: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0, id 0

Ethernet II, Src: 32:97:05:d9:84:95 (32:97:05:d9:84:95), Dst: CiscoMeraki_b7:c6:bd (e0:cb:bc:b7:c6:bd)

1 Internet Protocol Version 4, Src: 10.142.219.49, Dst: 10.128.128.128

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 63

Identification: 0x082c (2092)

0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: UDP (17)

Header Checksum: 0x01c3 [validation disabled]
[Header Checksum status: Univerified]

Source Address: 10.142.219.49

Destination Address: 10.128.128.128
[Stream index: 0]

User Datagram Protocol, Src Port: 41806, Dst Port: 53

Domain Name System (query)
```

In User Datagram Protocol (UDP), possiamo vedere le porte di origine e di destinazione. La porta di origine è 41806, mentre quella di destinazione è 53:

```
Frame 9: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0, id 0

Ethernet II, Src: 32:97:95:d9:84:95 (32:97:95:d9:84:95), Dst: CiscoMeraki_b7:c6:bd (e0:cb:bc:b7:c6:bd)

Internet Protocol Version 4, Src: 10.142.219.49, Dst: 10.128.128.128

User Datagram Protocol, Src Port: 41806, Dst Port: 53

Source Port: 41806

Destination Port: 53

Length: 43

Checksum: 9x79fc [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

[Stream Packet Number: 1]

- [Times since first frame: 0.0000000000 seconds]

[Time since previous frame: 0.0000000000 seconds]

UDP payload (35 bytes)

Domain Name System (query)
```

Possiamo verificare se le informazioni fornite in Wireshark corrispondono a quelle effettive scrivendo nel terminale arp -a e ifconfig:

E sì, corrispondono.

Nella sezione DNS del traffico catturato, possiamo vedere i flag. Tutti i flag sono stati impostati su 0, eccetto la ricorsione. Esegue query ricorsivamente:

Esplorare il traffico delle risposte DNS

Ora scelgo il pacchetto di risposta corrispondente al primo caso che abbiamo analizzato. Tutti gli IP di destinazione e di origine, le porte, gli indirizzi MAC sono stati sostituiti rispetto al caso precedente. Inoltre, anche la query ricorsiva del server è impostata su 1. Ora vengono visualizzate le sezioni delle risposte in DNS, che sono identiche a quelle visualizzate sul terminale quando è stato richiesto nslookup:

