

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:

```
File Actions Edit View Help
L$ nslookup
> www.instagram.com
Server:      10.128.128.128
Address:     10.128.128.128#53

Non-authoritative answer:
www.instagram.com canonical name = z-p42-instagram.c10r.instagram.com.
Name:   z-p42-instagram.c10r.instagram.com
Address: 157.240.203.174
Name:   z-p42-instagram.c10r.instagram.com
Address: 2a03:2880:f26d:e9:face:b00c:0:4420
> www.facebook.com
Server:      10.128.128.128
Address:     10.128.128.128#53

Non-authoritative answer:
www.facebook.com canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 157.240.203.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f16d:81:face:b00c:0:25de
> www.cisco.com
Server:      10.128.128.128
Address:     10.128.128.128#53

Non-authoritative answer:
www.cisco.com canonical name = www.cisco.com.akadns.net.
www.cisco.com.akadns.net canonical name = wwds.cisco.com.edgekey.net.
wwds.cisco.com.edgekey.net canonical name = wwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwds.cisco.com.edgekey.net.globalredir.akadns.net canonical name = e2867.dsca.akamaiedge.net.
Name:   e2867.dsca.akamaiedge.net
Address: 2.22.33.46
Name:   e2867.dsca.akamaiedge.net
Address: 2a02:29f0:8d00:c9e::b33
Name:   e2867.dsca.akamaiedge.net
```

Esplorare il traffico delle query DNS

Ho filtrato la porta 53 (DNS) per UDP:

No.	Time	Source	Destination	Protocol	Length	Info
9	21.315014210	10.142.219.49	10.128.128.128	DNS	77	Standard query 0x72fb A www.instagram.com
10	21.342794942	10.128.128.128	10.142.219.49	DNS	128	Standard query response 0x72fb A www.instagram.com CNAME z-p42-
11	21.344994102	10.142.219.49	10.128.128.128	DNS	94	Standard query 0xbfce AAAA z-p42-instagram.c10r.instagram.com
12	21.366453187	10.128.128.128	10.142.219.49	DNS	122	Standard query response 0xbfce AAAA z-p42-instagram.c10r.inst.
15	37.221361344	10.142.219.49	10.128.128.128	DNS	76	Standard query 0xb2c3 A www.facebook.com
16	37.253941151	10.128.128.128	10.142.219.49	DNS	121	Standard query response 0xb2c3 A www.facebook.com CNAME star-
17	37.255693257	10.142.219.49	10.128.128.128	DNS	87	Standard query 0x072b AAAA star-mini.c10r.facebook.com
18	37.277917855	10.128.128.128	10.142.219.49	DNS	115	Standard query response 0x072b AAAA star-mini.c10r.facebook.c.
19	41.323809577	10.142.219.49	10.128.128.128	DNS	73	Standard query 0xf537 A www.cisco.com
20	41.378727251	10.128.128.128	10.142.219.49	DNS	255	Standard query response 0xf537 A www.cisco.com CNAME www.cisc.
21	41.372950982	10.142.219.49	10.128.128.128	DNS	85	Standard query 0x4d60 AAAA e2867.dsca.akamaiedge.net
22	41.406652315	10.128.128.128	10.142.219.49	DNS	141	Standard query response 0x4d60 AAAA e2867.dsca.akamaiedge.net.

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)
      ...0... = LG bit: Globally unique address (factory default)
      ...0... = IG bit: Individual address (unicast)
    Source: 32:97:05:d9:84:95 (32:97:05:d9:84:95)
      ...1... = LG bit: Locally administered address (this is NOT the factory default)
      ...0... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
  Internet Protocol Version 4, Src: 10.142.219.49, Dst: 10.128.128.128
  User Datagram Protocol, Src Port: 41806, Dst Port: 53
  Domain Name System (query)
```

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)
  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)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x01c3 [validation disabled]
    [Header checksum status: Unverified]
    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: 32:97:05:d9:84:95 (32:97:05: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: 0x70fc [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
  [Timestamps]
    [Time since first frame: 0.000000000 seconds]
    [Time since previous frame: 0.000000000 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`:

```
(rinatrastamov@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.142.219.49 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::e8db:4aa8:1d38:d0ef prefixlen 64 scopeid 0x20<link>
    ether 32:97:05:d9:84:95 txqueuelen 1000 (Ethernet)
    RX packets 154 bytes 19143 (18.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 66 bytes 6153 (6.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 10 bytes 580 (580.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 580 (580.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(rinatrastamov@kali)-[~]
$ arp -a
?([10.128.128.128] at e0:cb:bc:b7:c6:bd [ether] on eth0)
```

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:

```
Domain Name System (query)
Transaction ID: 0x72fb
Flags: 0x0100 Standard query
 0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
... .. = Truncated: Message is not truncated
... ..1 ... = Recursion desired: Do query recursively
... ..0 ... = Z: reserved (0)
... ..0 ... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  www.instagram.com: type A, class IN
    Name: www.instagram.com
    [Name Length: 17]
    [Label Count: 3]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
[Response in: 10]
0000 e0 cb bc b7 c6 bd 32 9
0010 00 3f 08 2c 00 00 40 1
0020 80 80 a3 4e 00 35 00 2
0030 00 00 00 00 00 00 03 7
0040 67 72 61 6d 03 63 6f 6
```

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:

```
udp.port==53
No. Time Source Destination Protocol Length Info
10 21.310014210 10.142.219.49 10.128.128.128 DNS 77 Standard query 0x72fb A www.instagram.com
11 21.342794942 10.128.128.128 10.142.219.49 DNS 128 Standard query response 0x72fb A www.instagram.com CNAME
11 21.344994102 10.142.219.49 10.128.128.128 DNS 94 Standard query 0xbfce AAAA z-p42-instagram.c10r.instagram.com

Frame 10: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface eth0, id 0
Ethernet II, Src: CiscoMeraki_b7:c6:bd (e0:cb:bc:b7:c6:bd), Dst: 32:97:05:d9:84:95 (32:97:05:d9:84:95)
Internet Protocol Version 4, Src: 10.128.128.128, Dst: 10.142.219.49
User Datagram Protocol, Src Port: 53, Dst Port: 41806
Domain Name System (response)
Transaction ID: 0x72fb
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
  www.instagram.com: type A, class IN
    Name: www.instagram.com
    [Name Length: 17]
    [Label Count: 3]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
Answers
  www.instagram.com: type CNAME, class IN, cname z-p42-instagram.c10r.instagram.com
    Name: www.instagram.com
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 2179 (36 minutes, 19 seconds)
    Data length: 23
    CNAME: z-p42-instagram.c10r.instagram.com
  z-p42-instagram.c10r.instagram.com: type A, class IN, addr 157.240.203.174
    Name: z-p42-instagram.c10r.instagram.com
    Type: A (1) (Host Address)
    Class: IN (0x0001)
0000 32 97 05 d9 84 95 e0 c
0010 00 72 69 5e 40 00 40 1
0020 db 31 08 35 a3 4e 00 5
0030 00 02 00 00 00 00 03 7
0040 67 72 61 6d 03 63 6f 6
0050 05 00 01 00 00 08 83 0
0060 69 6e 73 74 61 67 72 6
0070 c0 2f 00 01 00 01 00 0
```