

S11L3

Esplorazione del Traffico DNS

Obiettivi

- Parte 1: Catturare il Traffico DNS
- Parte 2: Esplorare il Traffico delle Query DNS
- Parte 3: Esplorare il Traffico delle Risposte DNS

Risorse Richieste

1 PC con accesso a internet e Wireshark installato

Contesto / Scenario

Wireshark è uno strumento open source per la cattura e l'analisi dei pacchetti. Wireshark fornisce una scomposizione dettagliata dello stack dei protocolli di rete. Wireshark permette di filtrare il traffico per la risoluzione dei problemi di rete, investigare problemi di sicurezza e analizzare i protocolli di rete. Poiché Wireshark permette di visualizzare i dettagli dei pacchetti, può essere usato come strumento di ricognizione da un attaccante.

In questo laboratorio, installerai Wireshark e lo userai per filtrare i pacchetti DNS e visualizzare i dettagli sia dei pacchetti di query DNS che di quelli di risposta.

Osservare i campi di origine e destinazione.

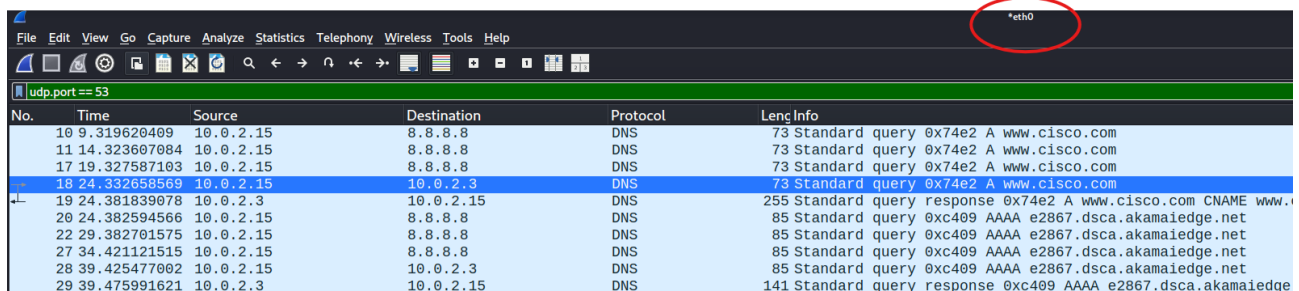
Quali sono gli indirizzi MAC di origine e destinazione?

52:55:0a:00:02:03 destinazione, 08:00:27:06:15:77 source

```
- Ethernet II, Src: PCSSystemtec_08:00:27:06:15:77 (08:00:27:06:15:77), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
  Destination: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0 .... = IG bit: Individual address (unicast)
  Source: PCSSystemtec_08:00:27:06:15:77 (08:00:27:06:15:77)
    ....0 .... = LG bit: Globally unique address (factory default)
    ....0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 4]
```

A quali interfacce di rete sono associati questi indirizzi MAC?

Gli indirizzi MAC sono associati all'interfaccia di rete utilizzata per la cattura dei pacchetti. Avendo catturato i pacchetti tramite una connessione internet, l'interfaccia di rete è eth0.



No.	Time	Source	Destination	Protocol	Length	Info
10	9.319620409	10.0.2.15	8.8.8.8	DNS	73	Standard query 0x74e2 A www.cisco.com
11	14.323607084	10.0.2.15	8.8.8.8	DNS	73	Standard query 0x74e2 A www.cisco.com
17	19.327587103	10.0.2.15	8.8.8.8	DNS	73	Standard query 0x74e2 A www.cisco.com
18	24.332658569	10.0.2.15	10.0.2.3	DNS	73	Standard query 0x74e2 A www.cisco.com
19	24.381839078	10.0.2.3	10.0.2.15	DNS	255	Standard query response 0x74e2 A www.cisco.com CNAME www.
20	24.382594566	10.0.2.15	8.8.8.8	DNS	85	Standard query 0xc409 AAAA e2867.dsca.akamaiedge.net
22	29.382701575	10.0.2.15	8.8.8.8	DNS	85	Standard query 0xc409 AAAA e2867.dsca.akamaiedge.net
27	34.421121515	10.0.2.15	8.8.8.8	DNS	85	Standard query 0xc409 AAAA e2867.dsca.akamaiedge.net
28	39.425477002	10.0.2.15	10.0.2.3	DNS	85	Standard query 0xc409 AAAA e2867.dsca.akamaiedge.net
29	39.475991621	10.0.2.3	10.0.2.15	DNS	141	Standard query response 0xc409 AAAA e2867.dsca.akamaiedge

Osservare gli indirizzi IPv4 di origine e destinazione

Quali sono gli indirizzi IP di origine e destinazione?

L'indirizzo IP di origine è 10.0.2.15, mentre l'indirizzo IP di destinazione è 10.0.2.3

```
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 59
  Identification: 0x8359 (33625)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xdf47 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.2.15
  Destination Address: 10.0.2.3
```

A quali interfacce di rete sono associati questi indirizzi IP?

Gli indirizzi IP sono associati all'interfaccia di rete eth0

```
Frame 18: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_08:00:27:06:15:77 (08:00:27:06:15:77), Dst: 52:55:0a:00:02:03 (52:55:0a:00:02:03)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.3
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 59
  Identification: 0x8359 (33625)
  000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0xdf47 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.0.2.15
  Destination Address: 10.0.2.3
```

Osservare le porte di origine e destinazione

Quali sono le porte di origine e destinazione?

La porta di origine è 41758. La porta di destinazione è 53

```
User Datagram Protocol, Src Port: 41758, Dst Port: 53
  Source Port: 41758
  Destination Port: 53
```

Qual è il numero di porta DNS predefinito?

Il numero predefinito di porta DNS è 53

Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?

L'indirizzo IP e MAC che abbiamo trovato su Wireshark combacia perfettamente a quelli del mio PC.

Abbiamo catturato il traffico del nostro PC tramite Wireshark

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:06:15:77 brd ff:ff:ff:ff:ff:ff
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
```

Esplorare il Traffico delle Risposte DNS

Quali sono gli indirizzi MAC e IP e i numeri di porta di origine e destinazione?

L'indirizzo MAC di origine è 52:55:0a:00:02:02 mentre quello di destinazione è 08:00:27:06:15:77

L'indirizzo IP di origine è 10.0.2.3, mentre quello di destinazione è 10.0.2.15

La porta di origine è 53, mentre quella di destinazione è 41758

```
Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_06:15:77 (08:00:27:06:15:77)
Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
User Datagram Protocol, Src Port: 53, Dst Port: 41758
```

Come si confrontano con gli indirizzi nei pacchetti di query DNS?

Confrontato la query dns e la query response, ci accorgiamo che gli indirizzi di destinazione e origine si invertono

Il server DNS può fare query ricorsive?

Sì, il server DNS può fare query ricorsive

```
= Response: Message is a response
= Opcode: Standard query (0)
= Authoritative: Server is not an authority for domain
= Truncated: Message is not truncated
= Recursion desired: Do query recursively
= Recursion available: Server can do recursive queries
= Z: reserved (0)
= Answer authenticated: Answer/authority portion was n
= Non-authenticated data: Unacceptable
= Reply code: No error (0)
```

Come si confrontano i risultati con quelli di nslookup?

Confrontando i risultati di Wireshark e nslookup, possiamo notare che Wireshark fornisce una visione dettagliata di tutto il traffico di rete e permette di ispezionare ogni singolo pacchetto, anche di altri protocolli.

Nslookup si limita a risolvere i nomi di dominio in indirizzi IP, restituendo solo l'esito della query DNS

Riflessione

Dai risultati di Wireshark, cos'altro puoi imparare sulla rete quando rimuovi il filtro?

Togliendo il filtro possiamo notare molte cose interessanti, come ad esempio numerosi pacchetti ARP che chiedono "Who has 10.0.2.4? Tell 10.0.2.15" Queste richieste indicano che i dispositivi stanno cercando di mappare gli IP ai MAC corrispondenti. I pacchetti ARP sono tutti broadcast, il che significa che le richieste vengono inviate a tutti i dispositivi sulla rete per scoprire chi possiede l'IP in questione.

Alcuni pacchetti ARP contengono risposte, che rivelano gli indirizzi MAC associati agli indirizzi IP. Ciò significa che i dispositivi sulla rete stanno aggiornando la loro tabella ARP con le informazioni corrette sugli indirizzi MAC.

Tramite queste informazioni possiamo imparare alcune cose della rete, come ad esempio:

Topologia di rete, attività sulla rete e/o presenza di dispositivi

Come può un attaccante usare Wireshark per compromettere la sicurezza della tua rete?

Un attaccante può usare Wireshark principalmente per intercettare e analizzare il traffico di rete al fine di ottenere informazioni sensibili. Wireshark è uno sniffer, il che significa che cattura i dati che passano attraverso una rete. Per compromettere una rete, un attaccante non usa Wireshark per l'attacco stesso, ma come strumento di ricognizione e analisi.

Un attaccante può utilizzare Wireshark in diverse fasi di un attacco:

Ricognizione e acquisizione di informazioni: un attaccante può usare Wireshark per analizzare il traffico di rete e individuare i sistemi attivi, i servizi in esecuzione, gli indirizzi IP e i protocolli utilizzati. Questa fase è cruciale per pianificare attacchi mirati.

Cattura di dati sensibili: può usare Wireshark per catturare pacchetti di dati non crittografati. Questo include password, nomi utente, cookie di sessione, e-mail e altri dati che viaggiano in chiaro.

Analisi di vulnerabilità: analizzando il traffico, può identificare protocolli insicuri, come HTTP o FTP, e sfruttare queste debolezze per ottenere accesso non autorizzato o per eseguire attacchi Man-in-the-Middle.

Decodifica e analisi post-attacco: dopo aver catturato i pacchetti, l'attaccante può usare le funzionalità di decodifica di Wireshark per interpretare i dati grezzi e estrarre informazioni utili. Questo può includere la ricostruzione di file trasferiti o la lettura di messaggi di chat.