

Cisco CyberOps 3

Cattura del traffico DNS

1. Avvio di Wireshark

- Avviare Wireshark e selezionare un'interfaccia di rete attiva per la cattura dei pacchetti.

2. Svuotare la cache DNS

- **Windows:** Aprire il prompt dei comandi ed eseguire:
 - cmd
 - Copia codice
 - ipconfig /flushdns

3. Generare traffico DNS

- Aprire un prompt dei comandi o terminale ed eseguire:
 - cmd
 - Copia codice
 - nslookup www.cisco.com
 - Uscire dalla modalità interattiva di nslookup digitando exit.

4. Interrompere la cattura dei pacchetti

- In Wireshark, fare clic su "Stop" per interrompere la cattura.

Parte 2: Esplora il traffico delle query DNS

Filtraggio dei pacchetti DNS

1. Inserire il filtro:
2. plaintext
3. Copia codice
4. udp.port == 53
5. Questo mostrerà solo i pacchetti DNS.

*Ethernet						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
<div> <div>udp.port == 53</div> <div>Expression...</div> </div>						
No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1_
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN_
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com_
<div> <div>> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0</div> <div>> Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)</div> <div>> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1</div> <div>> User Datagram Protocol, Src Port: 57729, Dst Port: 53</div> <div>> Domain Name System (query)</div> </div>						
<div> <div>Frame (frame), 73 bytes</div> <div>Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)</div> <div>Profile: Default</div> </div>						

Analisi del pacchetto di query DNS

1. Espansione dei dettagli:

- **Ethernet II:** Identificare gli indirizzi MAC di origine (NIC del PC) e di destinazione (gateway o server DNS locale).
- **IPv4:** Osservare gli indirizzi IP di origine (PC) e di destinazione (gateway o server DNS).
- **UDP:** Analizzare le porte di origine e destinazione. La porta 53 è quella predefinita per DNS.

2. Confronto con la configurazione locale:

- Utilizzare i comandi:
- cmd
- Copia codice
- arp -a
- ipconfig /all
- Confrontare gli indirizzi MAC e IP trovati in Wireshark con quelli registrati dal PC.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1_
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN_
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com_

> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

▼ Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)

▼ Destination: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)

Address: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)

.... ..0. = LG bit: Globally unique address (factory default)

.... ...0 = IG bit: Individual address (unicast)

▼ Source: PcsSyste_09:14:c4 (08:00:27:09:14:c4)

Address: PcsSyste_09:14:c4 (08:00:27:09:14:c4)

.... ..0. = LG bit: Globally unique address (factory default)

.... ...0 = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 57729, Dst Port: 53

> Domain Name System (query)

Frame (frame), 73 bytes || Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) || Profile: Default

Dettagli della query DNS

- Espandere "Domain Name System (query)" per analizzare flag, domande e opzioni.
- Confermare che la query è ricorsiva e richiede l'indirizzo IP per www.cisco.com.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1_
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN_
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com_

Internet Protocol Version 4, Src: 192.168.1.16, 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: 0x24fb (9467)
- > Flags: 0x00
- Fragment offset: 0
- Time to live: 128
- Protocol: UDP (17)
- Header checksum: 0x0000 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.1.16
- Destination: 192.168.1.1
- [Source GeoIP: Unknown]
- [Destination GeoIP: Unknown]

Internet Protocol Version 4 (ip), 20 bytes

Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)

Profile: Default

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 53

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1_
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN_
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com_

> Frame 33: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0

> Ethernet II, Src: PcsSyste_09:14:c4 (08:00:27:09:14:c4), Dst: Netgear_ea:b1:7a (80:37:73:ea:b1:7a)

> Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.1

> User Datagram Protocol, Src Port: 57729, Dst Port: 53

- Source Port: 57729
- Destination Port: 53
- Length: 39
- Checksum: 0x839a [unverified]
- [Checksum Status: Unverified]
- [Stream index: 2]

> Domain Name System (query)

User Datagram Protocol (udp), 8 bytes

Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%)

Profile: Default

Parte 3: Esplora il traffico di risposta DNS

Analisi del pacchetto di risposta

1. **Confronto indirizzi:**

- Gli indirizzi MAC e IP di origine/destinazione sono invertiti rispetto al pacchetto di query.
- Verificare che il numero di porta DNS (53) sia utilizzato nella risposta.

2. **Espansione dei dettagli DNS:**

- Analizzare i flag e i record (CNAME e A).
- Verificare che i risultati coincidano con quelli di nslookup.

Riflessione

1. **Osservazione senza filtri:**

- La rimozione del filtro consente di vedere altri tipi di traffico (es. ARP, DHCP), che possono rivelare informazioni su dispositivi e configurazioni di rete.

2. **Potenziale pericolo:**

- Un attaccante potrebbe utilizzare Wireshark per intercettare traffico non crittografato e ottenere informazioni sensibili come credenziali o dati personali.

Conclusione

L'utilizzo di strumenti come Wireshark è essenziale per comprendere il funzionamento del traffico di rete, ma è fondamentale garantire che il traffico sensibile sia protetto con crittografia per prevenire intercettazioni da parte di terzi.