



EPICODE

Cyber Security & Ethical Hacking
Laboratorio giorno 3 – Cisco
CyberOps



Esplorazione del Traffico DNS



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

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.

Risorse Richieste

1 PC con accesso a internet e Wireshark installato



Istruzioni

Parte 1: Catturare il Traffico DNS

Passo 1: Scaricare e installare Wireshark.

- a. Scaricare l'ultima versione stabile di Wireshark da www.wireshark.org. Scegliere la versione software necessaria in base all'architettura e al sistema operativo del PC. In alternativa potete usare kali.
- b. Seguire le istruzioni a schermo per installare Wireshark. Se viene richiesto di installare USBPcap, **NON** installare USBPcap per la normale cattura del traffico. USBPcap è sperimentale e potrebbe causare problemi USB sul PC. Questo passaggio non è necessario se avete optato per kali.



Passo 2: Catturare il traffico DNS.

a. Avviare Wireshark. Selezionare un'interfaccia attiva con traffico per la cattura dei pacchetti.

b. Pulire la cache DNS (non necessario se avete optato per kali).

1) In Windows, inserire ipconfig /flushdns nel Prompt dei Comandi.

2) Per la maggior parte delle distribuzioni Linux, una delle seguenti utility viene utilizzata per la cache DNS: Systemd-Resolved, DNSMasq e NSCD. Se la tua distribuzione Linux non utilizza una delle utility elencate, esegui una ricerca su internet per l'utility di caching DNS della tua distribuzione Linux.

(i) Identificare l'utility utilizzata nella tua distribuzione Linux controllando lo stato:
Systemd-Resolved: `systemctl status systemd-resolved.service`
DNSMasq: `systemctl status dnsmasq.service`
NSCD: `systemctl status nscd.service`

(ii) Se stai usando systemd-resolved, inserisci `systemd-resolve --flush-caches` per pulire la cache per Systemd-Resolved prima di riavviare il servizio. I seguenti comandi riavviano il servizio associato usando privilegi elevati:

Systemd-Resolved: `sudo systemctl restart systemd-resolved.service`
DNSMasq: `sudo systemctl restart dnsmasq.service`
NSCD: `sudo systemctl restart nscd.service`

3) Per macOS, inserire `sudo killall -HUP mDNSResponder` per pulire la cache DNS nel Terminale. Eseguire una ricerca su internet per i comandi per pulire la cache DNS per un OS più vecchio

c. A un prompt dei comandi o terminale, digitare nslookup per entrare in modalità interattiva.

d. Inserire il nome di dominio di un sito web. Il nome di dominio **www.cisco.com** è usato in questo esempio.

e. Digitare exit quando finito. Chiudere il prompt dei comandi.

f. Fare clic su Stop capturing packets (Interrompi cattura pacchetti) per fermare la cattura di Wireshark.



Parte 2: Esplorare il Traffico delle Query DNS

a. Osservare il traffico catturato nel riquadro Elenco Pacchetti (Packet List) di Wireshark. Inserire `udp.port == 53` nella casella del filtro e fare clic sulla freccia (o premere invio) per visualizzare solo i pacchetti DNS.

Nota: Gli screenshot forniti sono solo esempi. Il tuo output potrebbe essere leggermente diverso.

The screenshot shows the Wireshark interface with the filter `udp.port == 53` applied. The packet list displays several DNS packets. Packet 33 is selected, and its details are shown in the packet details pane.

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...

Details of Frame 33:

- > 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
- > Domain Name System (query)

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



b. Selezionare il pacchetto DNS che contiene Standard query e A www.cisco.com nella colonna Info.

c. Nel riquadro Dettagli Pacchetto (Packet Details), notare che questo pacchetto ha Ethernet II, Internet Protocol Version 4, User Datagram Protocol e Domain Name System (query).

d. Espandere Ethernet II per visualizzare i dettagli. Osservare i campi di origine e destinazione.

Quali sono gli indirizzi MAC di origine e destinazione?

A quali interfacce di rete sono associati questi indirizzi MAC?

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port == 53 Expression...

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



e. Espandere Internet Protocol Version 4.
Osservare gli indirizzi IPv4 di origine e destinazione.

Quali sono gli indirizzi IP di origine e destinazione?

A quali interfacce di rete sono associati questi indirizzi IP?

***Ethernet**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: `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 (p), 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

f. Espandere User Datagram Protocol (UDP). Osservare le porte di origine e destinazione.

Quali sono le porte di origine e destinazione?

Qual è il numero di porta DNS predefinito?

g. Determinare l'indirizzo IP e MAC del PC.

1. In un prompt dei comandi di Windows, inserire `arp -a` e `ipconfig /all` per registrare gli indirizzi MAC e IP del PC.
2. Per PC Linux e macOS, inserire `ifconfig` o `ip address` in un terminale.

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



h. Espandere Domain Name System (query) nel riquadro Dettagli Pacchetto. Quindi espandere Flags e Queries.

i. Osservare i risultati. Il flag è impostato per eseguire la query ricorsivamente per interrogare l'indirizzo IP di 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

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

▼ Domain Name System (query)

[Response In: 34]

Transaction ID: 0x0002

▼ Flags: 0x0100 Standard query

- 0... .. = Response: Message is a query
- .000 0... .. = Opcode: Standard query (0)
-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.cisco.com: type A, class IN
 - Name: www.cisco.com
 - [Name Length: 13]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

Domain Name System (dns), 31 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 34: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0

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

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

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

> Domain Name System (response)

Frame (frame), 254 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default

Parte 3: Esplorare il Traffico delle Risposte DNS

a. Selezionare il corrispondente pacchetto DNS di risposta che ha Standard query response e A www.cisco.com nella colonna Info

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

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

b. Espandere Domain Name System (response). Quindi espandere Flags, Queries, e Answers.

c. Osservare i risultati.

Il server DNS può fare query ricorsive?



d. Osservare i record CNAME e A nei dettagli delle Risposte (Answers).

Come si confrontano i risultati con quelli di nslookup?

Riflessione

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

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

The screenshot shows the Wireshark interface with a packet capture filter of `udp.port == 53`. The packet list shows several DNS packets. Packet 34 is selected, showing a DNS query response for `www.cisco.com` with a CNAME record pointing to `www.cisco.com.akadns.net`.

Domain Name System (response)
 [Request In: 33]
 [Time: 0.010817000 seconds]
 Transaction ID: 0x0002

▼ Flags: 0x8180 Standard query response, No error

- 1... .. = Response: Message is a response
- .000 0... .. = Opcode: Standard query (0)
-0... .. = Authoritative: Server is not an authority for domain
-0... .. = Truncated: Message is not truncated
-1... .. = Recursion desired: Do query recursively
-1... .. = Recursion available: Server can do recursive queries
-0... .. = Z: reserved (0)
-0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
-0... .. = Non-authenticated data: Unacceptable
-0000 = Reply code: No error (0)

Questions: 1
 Answer RRs: 5
 Authority RRs: 0
 Additional RRs: 0

▼ Queries

- ▼ www.cisco.com: type A, class IN
 - Name: www.cisco.com
 - [Name Length: 13]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

▼ Answers

- > www.cisco.com: type CNAME, class IN, cname www.cisco.com.akadns.net
- > www.cisco.com.akadns.net: type CNAME, class IN, cname wwds.cisco.com.edgekey.net
- > wwds.cisco.com.edgekey.net: type CNAME, class IN, cname wwds.cisco.com.edgekey.net.globalredir.akadns.net
- > wwds.cisco.com.edgekey.net.globalredir.akadns.net: type CNAME, class IN, cname e144.dscb.akamaiedge.net
- > e144.dscb.akamaiedge.net: type A, class IN, addr 23.52.234.158

Frame (frame), 254 bytes | Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) | Profile: Default



EPICODE

Roma | Milano | Berlino

business@epicode.com

