Analisi del Traffico di Rete e Gestione della Cache su Kali Linux

---

1. Comportamento di nslookup con URL

Domanda: Output di nslookup con http://www.cisco.com/ e https://google.com che mostra NXDOMAIN e errori di comunicazione. **Risposta:** Il comando nslookup è utilizzato per interrogare i server DNS (Domain Name System) per la mappatura di nomi di dominio o indirizzi IP. Si aspetta un nome di dominio come argomento, non un URL completo.

Quando hai fornito http://www.cisco.com/ e https://google.com a nslookup, il server DNS ha interpretato l'intera stringa, inclusi http:// o https:// e il / finale, come il nome di dominio da risolvere. Dato che queste non sono nomi di dominio validi, il server ha restituito NXDOMAIN (Non-Existent Domain), indicando che non ha trovato un record per quel nome esatto.

Inoltre, l'errore iniziale "communications error to 8.8.8.8#53: host unreachable" suggerisce un problema di connettività di rete momentaneo verso il server DNS pubblico di Google (8.8.8.8), forse intermittente o specifico per la rotta IPv4. Tuttavia, le query successive mostrano 8.8.8.8 utilizzato con successo, il che indica che il problema si è risolto o nslookup ha commutato su un server funzionante.

L'indirizzo del server fd33:2f24:9b00:5900:ca00:6ff:fe5a:4 è un indirizzo IPv6, probabilmente un server DNS locale o interno configurato sul tuo sistema.

Per usare correttamente nslookup, dovresti fornire solo il nome del dominio, ad esempio: > www.cisco.com > google.com

2. Come cancellare la cache su Kali Linux

Domanda: Come si cancella la cache su Kali Linux? **Risposta:** Su Kali Linux (che è basato su Debian), ci sono diversi tipi di cache che potresti voler cancellare, a seconda di cosa intendi per "cache". Ecco i più comuni e come gestirli:

1. Cache della RAM (Memory Cache) Il kernel Linux usa la RAM per memorizzare i dati usati di frequente per velocizzare le operazioni. Generalmente, non c'è bisogno di pulire manualmente questa cache perché il sistema la gestisce in modo intelligente, liberando spazio quando necessario.

- **Svuotare solo la PageCache:** sudo sync && echo 1 | sudo tee /proc/sys/vm/drop_caches
- **Svuotare dentries e inodes:** sudo sync && echo 2 | sudo tee /proc/sys/vm/drop_caches
- **Svuotare PageCache, dentries e inodes (tutta la cache di sistema):** sudo sync && echo 3 | sudo tee /proc/sys/vm/drop_caches *sync: Forza la scrittura dei dati sui dischi. *echo [numero] > /proc/sys/vm/drop_caches: Scrive un valore nel file drop_caches del kernel. *sudo tee: Scrive in un file di sistema con permessi di root.

2. Cache di APT (Package Manager) Kali Linux usa apt per gestire i pacchetti software, e apt memorizza i pacchetti scaricati nella sua cache.

- **Pulire solo i pacchetti non più necessari:** sudo apt autoclean
- **Pulire tutti i pacchetti scaricati:** sudo apt clean Questo può liberare molto spazio su disco.

3. Cache DNS Se hai problemi con la risoluzione dei nomi di dominio o vuoi assicurarti che il tuo sistema utilizzi le informazioni DNS più recenti, puoi svuotare la cache DNS.

- **Per systemd-resolved (il più comune su Kali):** sudo systemd-resolve --flush-caches Oppure riavvia il servizio: sudo systemctl restart systemd-resolved
- **Per dnsmasq (se in uso):** sudo killall -USR1 dnsmasq Oppure riavvia il servizio: sudo systemctl restart dnsmasq
- **Per nscd (meno comune):** sudo systemctl restart nscd.service

4. Cache del Browser Web Ogni browser web (Firefox, Chromium, ecc.) ha la propria cache. Per cancellarla, devi farlo dalle impostazioni interne del browser:

- **Firefox:** Menu (tre linee) > Impostazioni > Privacy e sicurezza > "Cookie e dati dei siti web" > "Cancella dati...", seleziona "Contenuti web in cache" > "Cancella".
- **Chromium/Chrome:** Menu (tre puntini) > "Altri strumenti" > "Cancella dati di navigazione..." > Seleziona intervallo e "Immagini e file memorizzati nella cache" > "Cancella dati".

5. Cache dell'ARP (Address Resolution Protocol) La cache ARP memorizza le associazioni tra indirizzi IP e indirizzi MAC.

- **Per svuotare tutta la cache ARP:** sudo ip -s -s neigh flush all
- **Per eliminare una singola voce:** sudo arp -d [IP_ADDRESS]

3. Output del comando sudo

Domanda: Mi è uscito un 3 dopo aver immesso la password per il comando sudo sync && echo 3 | sudo tee /proc/sys/vm/drop_caches è giusto? **Risposta:** Sì, è **completamente normale e esattamente ciò che ci si aspetterebbe di vedere!**

Il 3 che è apparso dopo aver inserito la password è semplicemente l'output della parte echo 3 del tuo comando. Questo 3 viene quindi "pipato" (|) a sudo tee /proc/sys/vm/drop_caches, che lo scrive nel file del kernel responsabile della pulizia della cache.

In sintesi:

- [sudo] password for kali: - Il sistema che ti chiede la password.
- (Tu digiti la tua password e premi Invio)

- 3 - L'output di echo 3 che appare sul tuo terminale. Questo conferma che il valore 3 è stato inviato a tee e successivamente scritto in /proc/sys/vm/drop_caches, svuotando con successo tutte le cache di memoria del tuo sistema.

Tutto ha funzionato come previsto!

4. Analisi degli Indirizzi MAC

Domanda: Quali sono gli indirizzi MAC di origine e destinazione? A quali interfacce di rete sono associati questi indirizzi MAC? **Risposta:** Dall'immagine fornita ("MAC.png"):

- **Indirizzo MAC di Origine (Src):** PCSsystemtec_b4:a1:05 (08:00:27:b4:a1:05)
- **Indirizzo MAC di Destinazione (Dst):** SkyUk_43:d0:a1 (c8:96:5a:43:d0:a1)

Per quanto riguarda le interfacce di rete:

- La cattura è stata effettuata su **interfaccia eth0**.
- L'indirizzo MAC di origine (08:00:27:b4:a1:05) è associato all'interfaccia di rete del **dispositivo mittente** (la tua macchina Kali Linux o un'interfaccia che inoltra il traffico).
- L'indirizzo MAC di destinazione (c8:96:5a:43:d0:a1) è associato all'interfaccia di rete del **router** o del **gateway predefinito** nella rete locale del mittente, poiché il pacchetto è diretto a un IP remoto (8.8.8.8).

5. Analisi degli Indirizzi IP

Domanda: Quali sono gli indirizzi IP di origine e destinazione? A quali interfacce di rete sono associati questi indirizzi IP? **Risposta:** Dall'immagine fornita ("IPv4.png"):

- **Indirizzo IP di Origine (Source Address):** 192.168.0.123
- **Indirizzo IP di Destinazione (Destination Address):** 8.8.8.8

Per quanto riguarda le interfacce di rete:

- L'indirizzo IP di origine (192.168.0.123) è associato all'interfaccia di rete del **dispositivo locale (il mittente)** che ha generato questo pacchetto (ad es., l'interfaccia eth0 del tuo PC Kali Linux).
- L'indirizzo IP di destinazione (8.8.8.8) è associato all'interfaccia di rete di un **server DNS pubblico di Google** (un host remoto su Internet).

6. Analisi del Protocollo UDP e Confronto con Dati Locali

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

Risposta:

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?

Dall'immagine "UPD.png":

- **Porta di Origine (Src Port):** 59085
- **Porta di Destinazione (Dst Port):** 53

Il numero di porta DNS predefinito (standard) è **53**.

g. Determinare l'indirizzo IP e MAC del PC. Confrontare gli indirizzi MAC e IP nei risultati di Wireshark con gli indirizzi IP e MAC. Qual è la tua osservazione?

Dall'immagine "ip addr.png" (output del comando ip address su Kali Linux):

- **Indirizzo MAC del PC (per l'interfaccia eth0):** 08:00:27:b4:a1:05
- **Indirizzo IP del PC (per l'interfaccia eth0):** 192.168.0.123

Confronto con i risultati di Wireshark (dalle immagini precedenti):

- **Indirizzo MAC di Origine in Wireshark:** 08:00:27:b4:a1:05
- **Indirizzo IP di Origine in Wireshark:** 192.168.0.123

Osservazione: L'indirizzo MAC e l'indirizzo IP di origine mostrati nei risultati di Wireshark (cattura del pacchetto) **corrispondono esattamente** agli indirizzi MAC e IP dell'interfaccia eth0 del PC Kali Linux, come mostrato dall'output del comando ip address. Questo indica che il pacchetto catturato da Wireshark è stato effettivamente generato e inviato dal PC Kali Linux stesso, attraverso la sua interfaccia eth0.

7. Analisi del Traffico delle Risposte DNS e Implicazioni di Sicurezza

Domanda: 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? h. 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?

Risposta:

a. Selezionare il corrispondente pacchetto DNS di risposta. 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?

Dall'immagine "response.png" (pacchetto di risposta DNS):

- **Indirizzo MAC di Origine (Src MAC):** SkyUk_43:d0:a1 (c8:96:5a:43:d0:a1)
- **Indirizzo MAC di Destinazione (Dst MAC):** PCSsystemtec_b4:a1:05 (08:00:27:b4:a1:05)
- **Indirizzo IP di Origine (Src IP):** 8.8.8.8
- **Indirizzo IP di Destinazione (Dst IP):** 192.168.0.123
- **Porta di Origine (Src Port):** 53
- **Porta di Destinazione (Dst Port):** 34803

Confronto con i pacchetti di query DNS (basandoci sulle immagini precedenti):

- **Indirizzi MAC:** Origine e Destinazione sono **invertiti** rispetto alla query. Il mittente della query (PC) è il destinatario della risposta, e il destinatario della query (router/gateway) è il mittente della risposta a livello MAC.
- **Indirizzi IP:** Origine e Destinazione sono **invertiti** rispetto alla query. Il mittente della query (PC) è il destinatario della risposta, e il destinatario della query (server DNS 8.8.8.8) è il mittente della risposta.
- **Numeri di Porta:** Le porte sono **invertite**. La porta di destinazione standard del DNS (53) è la porta di origine per la risposta del server. La porta effimera (59085 dalla query originale) del client è la porta di destinazione per la risposta.

b. Espandere Domain Name System (response). Quindi espandere Flags, Queries, e Answers. L'immagine "response.png" mostra già queste sezioni espanse.

c. Osservare i risultati. Il server DNS può fare query ricorsive? Sì, osservando i "Flags" nella sezione "Domain Name System (response)", il flag Recursion available: Server can do recursive queries è impostato. Questo indica che il server DNS **8.8.8.8 può eseguire query ricorsive**.

h. Osservare i record CNAME e A nei dettagli delle Risposte (Answers). Come si confrontano i risultati con quelli di nslookup?

Dall'immagine "response.png", nella sezione "Answers":

- **Query:** cisco.com: type AAAA, class IN
- **Answer:** cisco.com: type AAAA, class IN, addr 2001:420:1101:1::185

In questo pacchetto di risposta DNS specifico, **non è presente un record CNAME**. Viene fornita una risposta per un record **AAAA** (indirizzo IPv6) per cisco.com che punta a 2001:420:1101:1::185.

Confronto con nslookup: Il risultato di Wireshark qui mostra una risoluzione DNS che restituisce un indirizzo IPv6. Un comando nslookup cisco.com o nslookup -type=AAAA cisco.com dovrebbe produrre risultati simili, includendo l'indirizzo IPv6. Le differenze potrebbero sorgere se nslookup per impostazione predefinita prioritizzasse i record IPv4 (A record) o se la specifica query fosse solo per un tipo di record. Wireshark fornisce la granularità del pacchetto grezzo, mentre nslookup è uno strumento più orientato alla risoluzione del nome.

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

Quando si rimuove il filtro in Wireshark e si cattura tutto il traffico, si ottiene una visione completa della rete:

- **Servizi e Protocolli in uso:** È possibile identificare tutti i tipi di traffico (HTTP/HTTPS, FTP, SSH, SMB, DNS, DHCP, ARP, ICMP, ecc.), ottenendo una panoramica su come i dispositivi comunicano.
- **Dispositivi Connessi:** Si possono identificare tutti i dispositivi attivi in rete tramite i loro indirizzi MAC e IP, e potenzialmente i loro sistemi operativi e i servizi che eseguono.
- **Comunicazioni Bidirezionali:** Si possono osservare non solo le richieste in uscita, ma anche le risposte e il traffico generato da altri dispositivi sulla rete.
- **Rilevamento di Anomalie/Problemi:** Si possono identificare tentativi di connessione falliti, traffico eccessivo, uso di protocolli non sicuri (dati in chiaro), scansioni di porte e traffico broadcast/multicast insolito.
- **Dipendenze e Flusso di Comunicazione:** È possibile tracciare intere conversazioni per capire come applicazioni o servizi interagiscono tra loro.
- **Performance della Rete:** Misurando i ritardi (RTT) tra richiesta e risposta, si possono valutare le prestazioni della rete e identificare colli di bottiglia.

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

Un attaccante può usare Wireshark (o strumenti simili) per compromettere la sicurezza della rete tramite:

- **Cattura di Credenziali e Dati Sensibili:** In reti con protocolli non criptati (es. HTTP, FTP, Telnet), un attaccante può intercettare nomi utente, password e altri dati sensibili trasmessi in chiaro.
- **Ricognizione della Rete (Network Mapping):** L'attaccante può identificare dispositivi attivi, servizi in esecuzione, sistemi operativi e la topologia della rete, fornendo informazioni cruciali per attacchi mirati.

- **Analisi del Traffico per Attacchi Specifici:** Permette di identificare pattern di traffico per attacchi di session hijacking (dirottamento di sessione), replay attacks, e la rilevazione di comunicazioni malware o tentativi di esfiltrazione dati.
- **Pianificazione di Attacchi Sofisticati:** La conoscenza della rete acquisita tramite sniffing può aiutare a pianificare attacchi Man-in-the-Middle (MITM) o avvelenamento ARP, che aumentano ulteriormente la capacità di intercettazione.

Wireshark è uno strumento potente sia per la difesa che per l'attacco, rendendolo essenziale per la comprensione delle vulnerabilità della rete.