Web Browsing (DNS, TCP, HTTP, SMTP)

Obiettivo

In questo esercizio analizziamo che cosa succede sui livelli trasporto e applicazione durante una transazione HTTP e una SMTP.

Esercizio 1.

1. Fate partire Wireshark (da terminale: `sudo wireshark`).
2. Aprite un browser web e puntatelo su un indirizzo non usato recentemente (per evitare che il valore DNS possa trovarsi in cache) ma non premete ENTER.
3. Fate partire una sessione di cattura frame con Wireshark.
4. Premete ENTER nel browser e attendete che la pagina sia **completamente** caricata.
5. *Determinate l'indirizzo IP del vostro compagno di banco ed effettuate un comando ping <indirizzoIPdelvostrocollega>. Per sapere l'indirizzo IP di una macchina, digitate ipconfig (Windows) oppure ifconfig (Linux).*
6. Fermate la cattura e salvate i frame registrati su file.
7. Salvate la pagina web come riferimento.

Protocol Analysis Questions

Analizzando l'elenco dei frame catturati, rispondete alle seguenti domande.

1. ***Protocolli catturati***
   - Esaminate la colonna dei protocolli catturati nella finestra di Wireshark, stendete un elenco di tutti i protocolli catturati, che dovrebbero contenere DNS, TCP, HTTP, ICMP.
   - Ci sono tra i frame catturati, dati di cui **non siete** destinatari?

2. ***Frame IP e UDP***
   - Cercate il primo frame DNS inviato da voi.
     a. Identificate l'indirizzo IP del mittente. Dovrebbe trovarsi nell'intestazione IP (che studieremo in dettaglio in seguito).
   - Guardate l'intestazione UDP del primo frame DNS
     a. Identificate il numero di porta sorgente e destinazione. Qual è la porta destinazione?

3. ***DNS***
   - Esaminate il payload (I dati) del primo frame DNS inviato.
     a. Dove sta l'informazione che dice se il messaggio è una query o una risposta?
     b. Il corpo della query cosa dice?
     c. Quant'è il codice (ID) della query?
     d. Qual'è il TIPO della query? In che campo viene codificato?

- Ora cercate la risposta alla query DNS fatta.
    a. Quali dovrebbero essere gli indirizzi IP di mittente e destinatario di questo frame? Verificate che corrispondano a ciò che vi aspettate.
    b. Quanti byte occupa il datagramma di risposta? E' più piccolo o più grande del datagramma di query?
    c. Verificate che l'ID della risposta corrisponda con l'ID della query.
    d. Quante risposte ci sono in totale nel messaggio di risposta? Hanno tutte lo stesso TTL? Cos'è il TTL nelle risposte DNS?

4. HTTP GET

- Trovate quei frame che trasportano dei comandi "HTTP GET". Identificate quante connessioni sono state usate. Riuscite a ritrovare le stesse connessioni nell'output del comando netstat?
    a. Confermate che i numeri di sequenza e acknowledgement sono quelli che vi aspettavate.
    b. Guardate i flag? Sapete spiegare perché i valori sono tali?
    c. Quant'è lungo il segmento TCP? Quanti byte sono invece i dati effettivi?
- Guardate ora il contenuto del comando GET.
    a. Confrontate i valori grezzi nel terzo riquadro in basso con i valori decodificati presentati nel secondo riquadro.
    b. Contate il numero di byte nel messaggio e verificate che questo numero corrisponda al campo lunghezza nell'intestazione TCP.
    c. Quali cookie sono stati inviati dal client? Quali cookie sono stati settati dal server?
    d. Qual è la lingua preferenziale che è stata specificata dal client?
    e. Che numero di sequenza vi aspettate nel prossimo frame in arrivo dal server? Che numero di acknowledgement?

Esercizio 2.

1. Fate partire una sessione di cattura con Wireshark.
2. Recuperate il client SMTP da voi scritto per la precedente esercitazione oppure scaricate e compilate il sorgente presente a questo URL https://www.mat.unical.it/informatica/Reti%20di%20Calcolatori?action=AttachFile&do=view&target=smtpcpp.zip, da usare al punto 3.
3. Invocate da terminale il programma smtpclient, *opportunamente cambiando la voce VOSTROINDIRIZZOMAIL e FILEAPIACERE.txt* nel seguente modo:

    ```
    smtpclient ml.mat.unical.it VOSTROINDIRIZZOMAIL
    ianni@mat.unical.it < FILEAPIACERE.txt
    ```

4. Verificate che i messaggi a video riportino che il messaggio è stato correttamente messo in coda.
5. Fermate la cattura.
6. Individuate in Wireshark i frame relativi alla conversazione SMTP appena svolta. Qual l'IP del mail server SMTP che viene contattato? E qual è l'IP del client che vi si connette?

7. Provate ora a usare smtpclient, cambiando l'indirizzo mittente in sorcio@sorcino.it e lanciate di nuovo il programma. Questa volta dovreste leggere un errore da console. Perché? Usate Wireshark per capire cosa c'è che non va nella conversazione SMTP.

Esercizio 3.

1. Fate partire una sessione di cattura con Wireshark.
2. Recuperate e annotate gli indirizzi IP degli host www.amazon.co.uk, www.google.it, www.google.com
3. Qual è (nome e IP) il server DNS autoritativo per il dominio .tv?
4. Qual è il mail exchanger per il dominio hotmail.com? e gmail.com?
5. Fermate la cattura: individuate il frame che contiene la richiesta DNS al punto 3 e la corrispondente risposta. Quanti sono i record addizionali in questa risposta?