**Riferimenti:**

* ss: un'altra utility per analizzare le socket (<https://manpages.ubuntu.com/manpages/focal/en/man8/ss.8.html>)
* lsof: elenca i file aperti (<https://manpages.ubuntu.com/manpages/jammy/en/man8/lsof.8.html>)
* Wireshark: analizzatore di protocolli di rete (<https://www.wireshark.org/>)

**Comando** ss**:**

ss

Elenca tutte le “open non-listening sockets (e.g. TCP/UNIX/UDP) that have established connection”. Quindi, per TCP le connessioni in stato ESTABLISHED mentre per UDP le socket (ancora aperte) connesse (cioè, quelle per cui è stata chiamata la bind per associarle a un indirizzo remoto).

L’opzione -n evita che ss tenti di risolvere i nomi dei servizi, mostrandoli in formato numerico.

Le varie opzioni possono essere combinate. Pertanto, di seguito descriviamo il vincolo imposto da ciascuna opzione, da combinarsi con i vincoli di altre opzioni o i vincoli predefiniti (se non sovrascritti da un’opzione).

ss -u

Solo socket UDP.

Per esempio, avendo in esecuzione udpserver e avendo fatto una richiesta con udpclient.

ss -un

Recv-Q Send-Q Local Address:Port Peer Address:Port Process

Non ottengo nessun risultato perché sia la socket del client sia la socket del server non sono associate a un indirizzo remoto.

Lanciando invece udpclient2 vedo la socket del client (se eseguo il comando prima che il client abbia ricevuto la risposta e quindi chiuda la socket).

ss -un

Recv-Q Send-Q Local Address:Port Peer Address:Port Process

0 0 127.0.0.1:34725 127.0.0.1:7000

ss -t

Elenca solo le socket TCP.

ss -l

Elenca solo le open *listening socket* che sono escluse per default.

Per esempio, avendo in esecuzione udpserver e avendo fatto una richiesta con udpclient.

ss -uln

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

UNCONN 0 0 0.0.0.0:7000 0.0.0.0:\*

UNCONN 0 0 0.0.0.0:39955 0.0.0.0:\*

UNCONN 0 0 127.0.0.53%lo:53 0.0.0.0:\*

UNCONN 0 0 127.0.0.1:323 0.0.0.0:\*

UNCONN 0 0 [::1]:323 [::]:\*

La prima e la seconda socket corrispondono rispettivamente al server e al client. Ma come facciamo essere sicuri che la seconda sia del client?

ss -p

Mostra il processo che usa le socket.

Per esempio, avendo in esecuzione udpserver e avendo fatto una richiesta con udpclient.

ss -ulpn

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

UNCONN 0 0 0.0.0.0:39603 0.0.0.0:\* users:(("udpclient",pid=50731,fd=3))

UNCONN 0 0 0.0.0.0:7000 0.0.0.0:\* users:(("udpserver",pid=37804,fd=3))

UNCONN 0 0 127.0.0.53%lo:53 0.0.0.0:\*

UNCONN 0 0 127.0.0.1:323 0.0.0.0:\*

UNCONN 0 0 [::1]:323 [::]:\*

ss -a

Mostra le socket in tutti gli stati. Si noti che questo comando può fornire più risultati della somma dell’esecuzione senza opzioni e della esecuzione con -l. Infatti, nel caso di TCP -a può restituire anche socket in stati come TIME-WAIT.

curl http://example.org/ > /dev/null

ss -ta

Ci mostrerà delle socket in stato TIME-WAIT

**Comando** lsof**:**

Permette di sapere chi ha una socket sulla porta 7000. Le opzioni -n e -P (combinate nell’esempio dui sotto), inibiscono rispettivamente la traduzione degli indirizzi di rete in hostname e la traduzione dei numeri di porta in nomi di servizi.

lsof -i :7000 -nP

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

udpserver 4080 terra 3u IPv4 66652 0t0 UDP \*:7000

Possiamo anche specificare il protocollo (es. UDP o TCP):

lsof -i UDP:7000 -nP

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

udpserver 4080 terra 3u IPv4 66652 0t0 UDP \*:7000

O l’indirizzo di rete:

lsof -i @0.0.0.0:7000

-nP

COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME

udpserver 4080 terra 3u IPv4 66652 0t0 UDP \*:7000

In realtà, possiamo combinare i selettori di protocollo, indirizzo e porta.

Usando l’opzione -t, viene stampato solo il pid. Se non c’è il comando non stampa nulla a termina con un valore non zero.

**Wireshark**

**Attenzione**: prestate la massima attenzione alle questioni di sicurezza quando installate questo software. Si consiglia di installarlo all’interno di una macchina virtuale, compreso Windows Subsystem for Linux (WSL).

Nota: se state usando WSL, dovete installare Wireshark dentro a WSL.

Nella prima schermata, fate doppio click sulla interfaccia dove volete avviare la cattura dei pacchetti.

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

Premete sul pulsante di stop (quadrato rosso) in alto a sinistra per interrompere la cattura. Premendo la pinna accanto si ricomincia la cattura.

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

Nota: i pacchetti catturati possono essere salvati in un file, che può essere successivamente riaperto con Wireshark, per analizzare il traffico successivamente alla sua cattura.

Immagine che contiene testo, elettronica, schermata, schermo

Descrizione generata automaticamente

La schermata è composta approssimativamente da 3 parti:

* La lista dei pacchetti catturati
* Un albero che illustra la struttura del pacchetto selezionato (si noti l’incapsulamento delle varie PDU), ottenuta da Wireshark analizzando i byte ottenuti dalla cattura
* Visualizzazione dei byte del pacchetto (il menu contestuale permette di copiare e fare altre operazioni e cambiare la visualizzazione). Si noti che se viene selezionato qualcosa nell’albero al centro, viene selezionata in questa vista la porzione corrispondente del pacchetto

Nell’area di testo in cima possiamo inserire dei filtri.

Usare il nome di un protocollo (es. udp o tcp) per filtrare i pacchetti contenenti quel tipo di protocollo.

Possiamo scrivere un filtro usando qualsiasi proprietà che si trova nell’albero sottostante, anche aiutandoci col menu contestuale.

Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente

Immagine che contiene testo, schermata, software, Icona del computer

Descrizione generata automaticamente

Si possono usare operatori logici.

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

Negli esempi di sopra abbiamo usato udp.srcport e udp.dstport. Esiste anche il campo “virtuale” udp.port che sussume entrambi.

Possiamo anche verificare l’appartenenza a un insieme.

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

Possiamo anche indicare degli intervalli.

Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamente

Possiamo seguire “flussi” UDP. Nell’esempio ho invocato due volte udpserver, per calcolare 256 + 1 = 257 e 1 + 255 = 256.

Immagine che contiene testo, schermata, software, Pagina Web

Descrizione generata automaticamente

Nella finestra che si apre usare il selettore (evidenziato in rosso) per scorre tra i vari flussi. Se scegliamo il formato Hex Dump (o raw) possiamo vedere i numeri da sommare nel primo pacchetto e la somma nel secondo:

Immagine che contiene testo, schermata, schermo, software

Descrizione generata automaticamente Immagine che contiene testo, elettronica, schermata, schermo

Descrizione generata automaticamente

Quando premiamo “Close”, ci troviamo un filtro che seleziona solo i pacchetti dentro il flusso corrente.

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

Aprendo nell’albero (al centro) i dettagli del pacchetto di richiesta, abbiamo avuto modo di vedere che:

* Nell’intestazione IP ci sono:
  + Indirizzo IP di origine e di destinazione
  + Lunghezza totale: 36 byte
* Nell’intestazione UDP ci sono:
  + i numeri di porta di origine e di destinazione
  + Lunghezza totale: 16 byte
* Poi abbiamo visto gli 8 byte del payload. Ricordate che 2 x 32 bit = 2 x 4 byte = 8 byte

La somma “torna”, perché la intestazione di UDP è di 8 byte + gli 8 byte di payload fanno i 16 byte riportati nella intestazione. La intestazione di questo pacchetto IP è 20 byte (perché non usa opzioni), quindi la lunghezza totale è 36 come riportato.

Notate che selezionando il nodo corrispondente a IPv4 nell’albero ci viene selezionata la intestazione e detta la sua lunghezza.

Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamente

Potete trovare l’elenco di tutti i filtri nel menu come segue:

Immagine che contiene testo, schermata, software, schermo

Descrizione generata automaticamente

Guida ai filtri: <https://www.wireshark.org/docs/wsug_html_chunked/ChWorkBuildDisplayFilterSection.html>