UNIVERSITÀ DI PISA

Progetto Gestione di Reti

Analisi volume traffico TCP e UPD

Thomas Conti

A.A 2019/2020

Progetto

Il progetto consiste in uno script Python che tramite l'ausilio di librerie per l'analisi del traffico e analisi di dati mostra il volume trasferito da una scheda di rete, presente nel dispositivo che lancia lo script, ad un altro indirizzo IP.

Il volume è valutato sui protocolli TCP e UDP.

Fasi script:

1) inizialmente lo script andrà a creare un file **.pcap** contenente i pacchetti acquisiti in base agli argomenti passati al lancio.

2) Successivamente analizza il pcap file (metodo pkt_analysis), per ogni pacchetto verifica:

   - **IP destinazione (pkt[IP].dest)**, in questo modo si può usare l'IP come **chiave** per una struttura dati **dizionario** ed associare di volta in volta il payload dei vari pacchetti che l'host ha inviato o ricevuto verso e da quell'indirizzo IP. Il dizionario:
     {IP, (tcpIN,tcpOUT),(udpIN,udpOUT)}

     L'indirizzo IP di destinazione viene confrontato con l'indirizzo IP dell host nel quale opera lo script, essendo l'indirizzo IP utilizzato come chiave del dizionario, nel caso in cui l'indirizzo fosse se stesso allora verrebbe usato l'indirizzo IP del mittente come chiave.

     Inoltre verificare se l'indirizzo IP di destinazione è se stesso o un indirizzo esterno è utile per distinguere i pacchetti in uscita ed i pacchetti in ingresso ed aggiungere il payload **(pkt[IP].len)** nel dizionario.

3) Infine i dati verranno mostrati tramite un grafico a barre orizzontali, contenente sull'asse ***x*** la quantità di byte trasferiti e sull'asse ***y*** ogni indirizzo IP.

Prerequisiti

Per poter eseguire lo script è necessario installare Scapy e Matplotlib, le altre librerie sono già presenti in Python.

Per installare Scapy digitare da terminale:

pip install scapy

Per installare Matplotlib:

sudo apt-get install python-matplotlib

Utilizzo

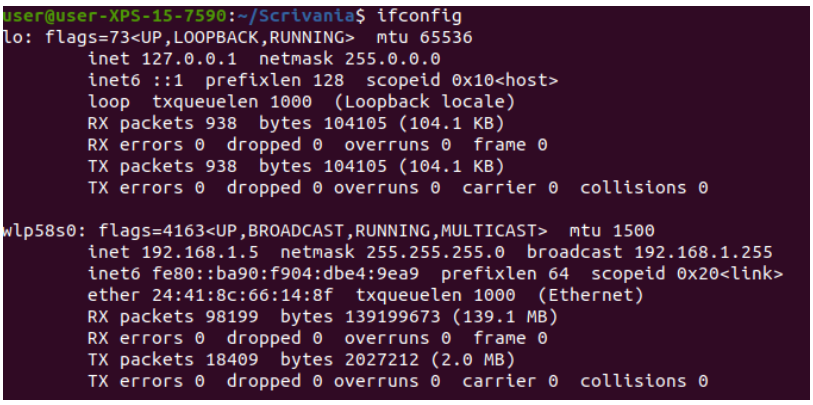
Aprire il terminale nella stessa cartella dello script ed eseguire il comando

sudo python ./packetsanalysis.py nome_scheda_rete packet_number

Parametri:

- **nome_scheda_rete:** specificare il nome della scheda sulla quale effettuare la analisi

  Per trovare il nome della scheda di rete digitare sul terminale il comando **ifconfig**



In questo caso la scheda di rete utilizzata sarà **wlp58s0**

- **packet_number:** inserire il numero di pacchetti di cui fare la analisi.

Alternativamente se si volesse misurare non un numero di pacchetti prestabilito ma un intervallo di tempo inserire 0, lo script continuerà ad acquisire pacchetti fino a quando non verrà effettuata una interruzione da terminale con CTRL+C.

Nel terminale sarà possibile visualizzare in tempo reale l'acquisizione dei pacchetti.

Terminata la acquisizione di pacchetti verrà salvato il file **mypcap.pcap** contenente i pacchetti acquisiti.

Successivamente verrà visualizzata e salvata **ima_final.png** per una visualizzazione grafica ordinata dall'indirizzo con volume maggiore all'indirizzo con volume minore.

Il risultato sarà del tipo:

comanda lanciato:
sudo python ./packetanalysis.py wlp58s0 0