Progetto gestione di rete

Dns sniffer

AA 2018-2019

Studente: Carlo Leo

Matricola: 546155

1. INTRODUZIONE

Il programma ***dns_sniffer*** anilizza il traffico DNS al fine di calcolare i nomi con maggiori richieste di risoluzione ed il volume di tale traffico. Il software è stato sviluppato nel linguaggio di programmazione python, utilizzando la libreria ***pyshark*** per la cattura del traffico. E' stata definita una classe per la memorizzazione delle informazioni necessarie al calcolo delle statistiche ***storage.py***, la quale, in pratica, incapsula un dizionario e un contatore. Il primo è necessario per il calcolo delle top request, mentre il secondo serve per calcolare il volume totale del traffico.

2. FUNZIONAMENTO

Con l'opzione ***-h*** è possibile visualizzare un messaggio di ***help***.

Appena avviato controlla la validità dei parametri, i quali sono:

- [-i] nome dell'interfaccia;
- [-m] tempo in minuti della durata della cattura;
- [-n] numero di top request da calcolare;

Se i controlli hanno avuto esito positivo viene istanziato un oggetto per la cattura, utilizzando un filtro che riesce a far arrivare al processo pacchetti DNS. Viene utilizzato il metodo ***applay_on_packets***, che permette di gestire ogni pacchetto recapitato al processo tramite una funzione, ***handler_pkt*** *(definita nel programma)*, la quale verifica se si tratta di una query dns e in quel caso memorizza le informazioni per il calcolo delle top request in una instanza di storage precedentemente allocata e stampa una stringa che identifica la query corrente. I byte invece vengono accumulati per ogni pacchetto.

Quando il tempo si è esaurito, le statistiche vengono clacolate e stampate a video.

NOTA: Se tra le n top request richieste vi sono piu' nomi con lo stesso numero di richieste vengno stampati tutti.

3. INDICAZIONI

Il software è stato sviluppato e testato su ***ubuntu-14.04.02 LTS*** utilizzando la ***versione di python 3.6***, necessita che sull' host vi siano installati:

- Pyshark
- Tshark > v2
- Versione di python > v3.5

Per avviare il programma:

sudo python3.6 dns_sniffer.py -i [interfaccia] -m [minuti] -n[numero top]

Il programma è stato testato generando traffico DNS utilizzando il comando ***host*** [es. host unipi.it].

Per testare il programma eseguire lo script ***test.sh***:

bash test.sh -i [interfaccia]

Il file ***lista.txt*** contiene una lista di nomi che vengono utilizzati dallo script per generare traffico DNS.

NOTA: nello script si utilizza il comando python3.6 per eseguire il programma.