Relazione Progetto Gestione di Rete

Riccardo Caviglia

Corso A, 507462

1 Introduzione

Il progetto ha come scopo la realizzazione di una dashboard nella quale vengono mostrate e monitorate varie metriche. Quest'ultime hanno lo scopo di facilitare l'identificazione di un possibile attacco informatico sulla rete.

2 Strumenti utilizzati

Gli strumenti ed i tool utilizzati per il progetto sono essenzialmente tre: ntopng, InfluxDB e Chronograf. ntopng (versione 4.1) è stato utilizzato per catturare il traffico e i dati della rete. I dati sono stati successivamente importati in InfluxDB (versione 1.8.1). Infine, grazie alla GUI di InfluxDB 1.8, Chronograf, è stata realizzata la dashboard.

3 Guida all'installazione degli strumenti utilizzati e all'uso

3.1 ntopng

E' possibile scaricare ntopng dal sito http://packages.ntop.org/. Successivamente è necessario scegliere il proprio sistema operativo ed eseguire le seguenti operazioni (Ubuntu 18.04):

```
apt-get clean all
apt-get update
apt-get install pfring-dkms nprobe ntopng n2disk cento
apt-get install software-properties-common wget
add-apt-repository universe
wget http://apt.ntop.org/18.04/all/apt-ntop.deb
apt install ./apt-ntop.deb
```

Una volta installato ntopng, quest'ultimo può essere lanciato da terminale eseguendo:

```
sudo ntopng -i <nome dell'interfaccia da monitorare>
```

La GUI di ntopng è reperibile su localhost, porta 3000. A questo punto è necessario selezionare InfluxDB per esportare i dati da ntopng, opzione configurabile da Settings > Preferences > Timeseries.

3.2 InfluxDB

E'possibile scaricare InfluxDB versione 1.8.1 dal sito https://portal.influxdata.com/downloads/ ed eseguire le operazioni di installazione corrispondenti al proprio sistema operativo: (Ubuntu)

```
wget https://dl.influxdata.com/influxdb/releases/influxdb_1.8.1_amd64.deb
sudo dpkg -i influxdb_1.8.1_amd64.deb
```

3.3 Chronograf

Così come InfluxDB, anche Chronograf (versione 1.8.5) è reperibile all'indirizzo https://portal.influxdata.com/downloads/. E' necessario, anche in questo caso selezionare il proprio sistema operativo, e installare il software eseguendo i seguenti comandi (per Ubuntu):

```
wget https://dl.influxdata.com/chronograf/releases/chronograf_1.8.5_amd64.deb
sudo dpkg -i chronograf_1.8.5_amd64.deb
```

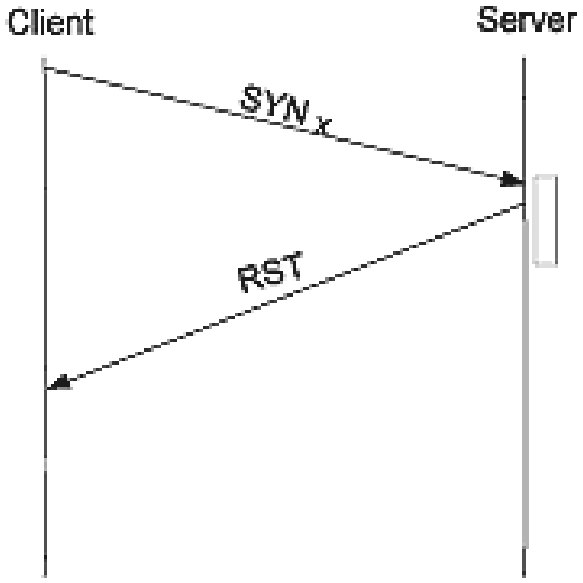
A questo punto l'installazione è completata. La GUI di Chronograf è reperibile su localhost, porta 8888. Infine per visualizzare la dashboard è necessario spostarsi sulla sezione "Dashboard" e importare il file "GR.json".

4 Metriche monitorate

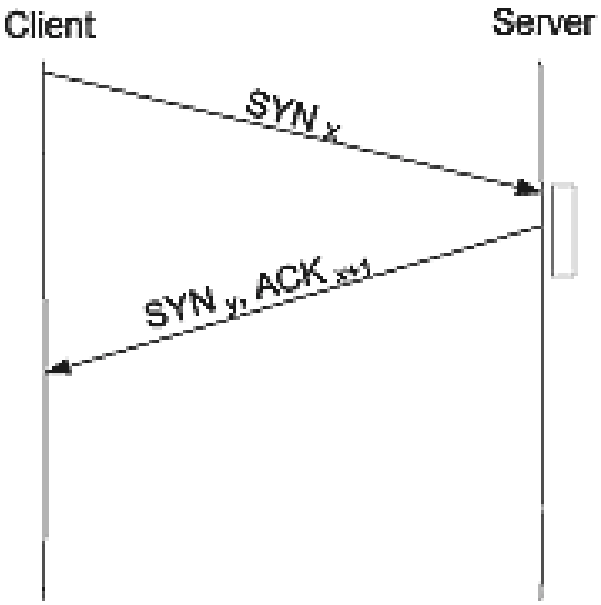
Le metriche monitorate e mostrate nella dashboard sono 8:

- Unreachable flows
- TCP packets sent/received
- SYN vs RST
- DNS Queries/ Replies OK/ Replies
- Bytes sent/received
- Misbehaving Flows
- SYN vs SYNACK
- Alerted Flows

Di seguito è possibile trovare una motivazione che giustifichi la scelta di alcune metriche prese in esame. Ad esempio l'analisi di SYN vs RST (situazione mostrata nella figura sottostante)



potrebbe essere indice di un possibile attacco DoS al server, in quanto quest'ultimo non è più in grado di rispondere al client, completando così il 3-way handshake. Un altro esempio di flusso sospetto è quello rappresentato di seguito:

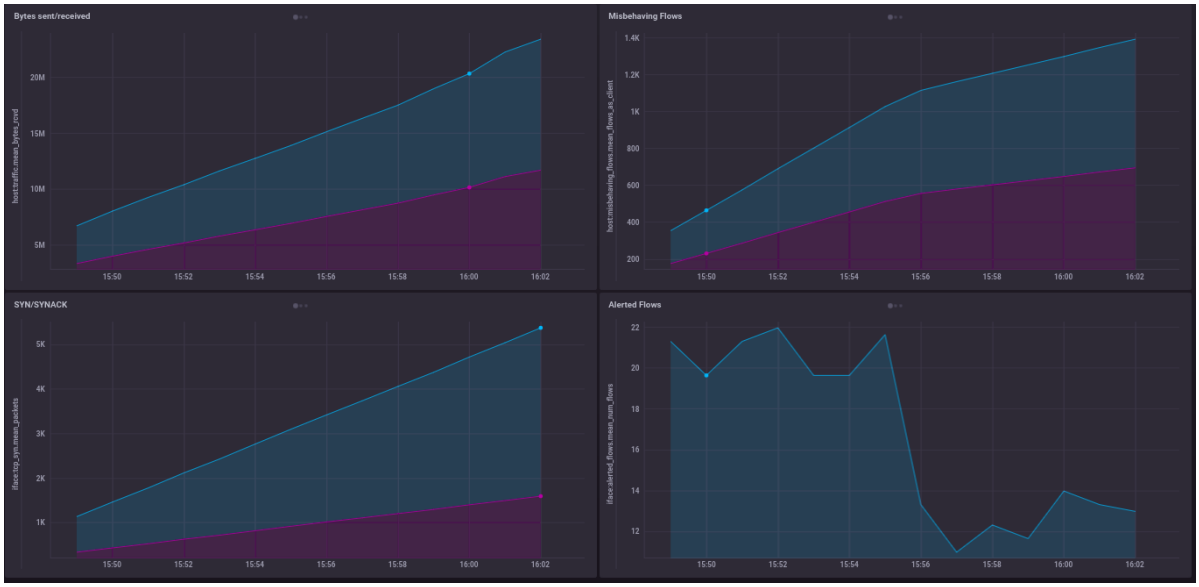


A questo punto, in condizioni normali, il client dovrebbe inviare un ultimo ACK per completare l'handshaking. Anche in questa circostanza, se il client non invia l'ultimo ACK, potrebbe essere in corso un attacco DoS e che l'indirizzo IP sorgente sia vittima di spoofing. Esiste però anche la possibilità che il client non riesca ad inviare l'ACK in quanto la rete sia congestionata e non sia effettivamente in corso un attacco. In entrambi i casi la connessione verrà chiusa allo scadere del timeout del server.

5 Dashboard

In questa sezione è possibile trovare delle immagini della dashboard e dei grafici che monitorano le varie metriche. In InfluxDB è possibile selezionare l'arco temporale dei dati da inserire nei vari grafici. Di seguito sono riportati due esempi della dashboard; il primo analizza i dati degli ultimi 15 minuti, mentre il secondo prende in esame 24 ore.

5.1 Dashboard (15 minuti)



5.1.1 Dashboard (24 ore)