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

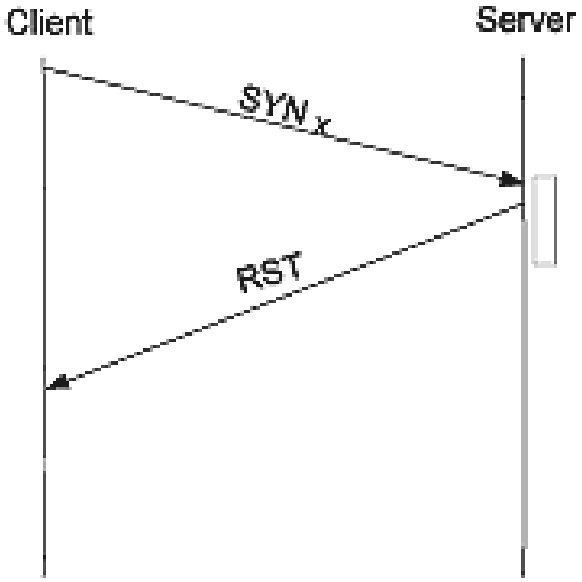
Gli strumenti ed i tool utilizzati per il progetto sono essenzialmente due: ntopng e InfluxDB. ntopng (versione 4.1) è stato utilizzato per catturare il traffico e i dati della rete. I dati sono stati successivamente importati in InfluxDB (versione 1.8.1) e, grazie alla GUI di quest'ultimo, è stata realizzata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

3 Metriche monitorate

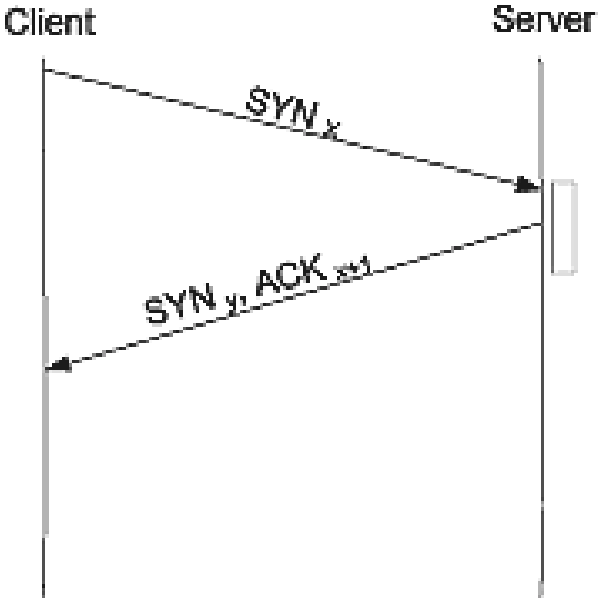
Le metriche monitorate e mostrate nella dashboard sono 8:

- 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:



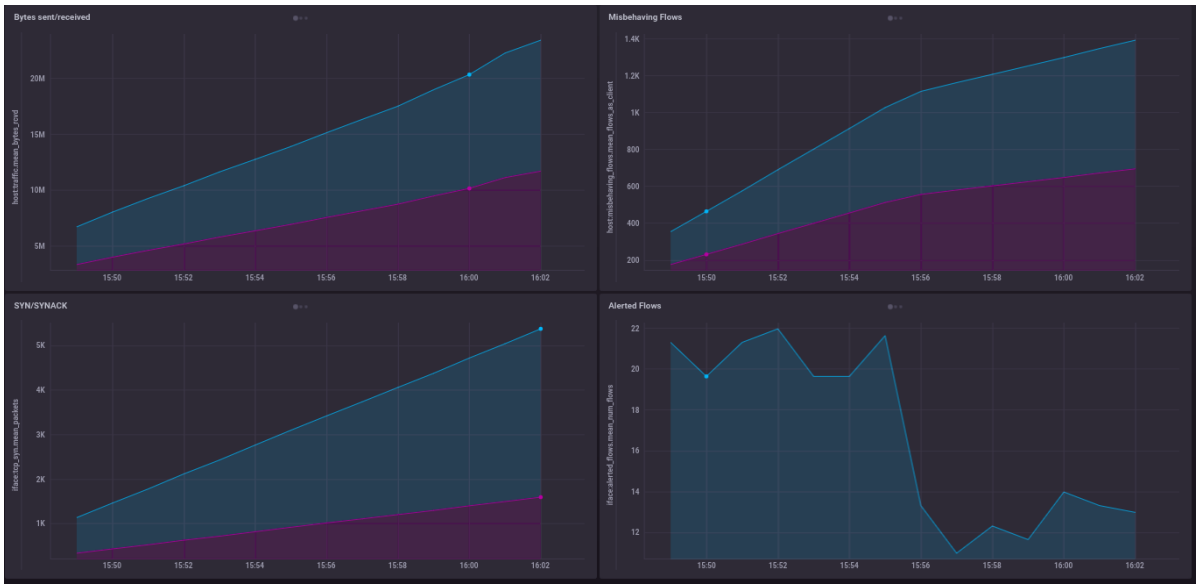
A questo punto, in condizioni normali, il client dovrebbe inviare un ultimo ACK

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.

4 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.

4.1 Dashboard (15 minuti)



4.1.1 Dashboard (24 ore)


Bytes sent/received
300M
250M
200M
150M
100M
50M
0
host:traffic.mean_bytes_sent
18 Aug
06:00
12:00
18:00
Misbehaving Flows
20K
15K
10K
5K
0
host:misbehaving_flows.mean_flows_as_client
18 Aug
06:00
12:00
18:00
SYN/SYNACK
90K
80K
70K
60K
50K
40K
30K
20K
10K
0
iface:tcp_syn.mean_packets
18 Aug
06:00
12:00
18:00
Alerted Flows
20
15
10
5
0
iface:alerted_flows.mean_num_flows
18 Aug
06:00
12:00
18:00