Carolina Ferrari
Simone Stanganini

NetMan Project

NetWork Management Project è un tool per cercare dei possibile Black Holes in una rete e tenere traccia degli host con cui questi comunicano.

———————————————- **Funzionamento**:

Il programma utilizza la libreria pcap, prende i pacchetti dalla scheda di rete data in input. Analizzando solo i pacchetti TCP, tramite una hashmap teniamo traccia di tutti gli host che hanno traffico rx o tx.

Ad ogni indirizzo nella hashmap associamo una struttura dati (struct DATA) per tenere le informazioni di:

- Tempo dell'ultimo pacchetto rx.
- Tempo dell'ultimo pacchetto tx.
- Patrcia Tree per tenere le porte e l'indirizzo ip usato dal possibile host attaccante che ha mandato pacchetti al blackhole.
- dst e src se l'host ha avuto traffico in entrata o uscita.
- Il numero totale di pacchetti scambiati nel secondo precedente.

Usiamo una Bitmap compressa (bitmap_BH) per tenere traccia di possibili blackhole. Ogni secondo stampiamo a schermo le varie informazioni contenute nell'hashmap. Se un host per 5 secondi non ha traffico in tx, sebbene avendolo in rx, viene segnalato come Black Hole, in modo da tenere aggiornato il suo stato nella tabella. Se un BlackHole torna a funzionare il suo stato viene notificato e le strutture dati aggiornate.

Per ogni elemento contenuto nella bitmap viene creato un file rrd contenente 60 elementi, chiamato con il nome dell'inirizzo ip. Ogni secondo prenderà valori compresi tra 0 e 1000000 tenendo aggiornati i dati ogni minuto. Per fare l'aggiornamento dei dati utilizzeremo la differenza tra il numero dei pacchetti e il valore al secondo precedente per rendere la serie stazionaria. Ogni 5 secondi aggiorneremo un grafico con la media dei valori contenuti nell'archivio.

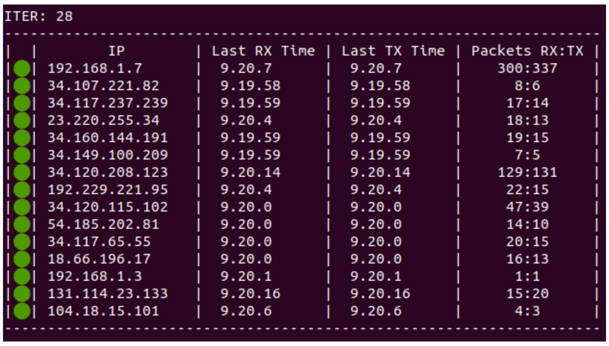
Il programma ogni 10 minuti fa un ciclo di ottimizzazione delle compressed bitmap, e elimina gli host che non sono più attivi da 1 ora.

In caso di uscita, viene avviata la procedura per la free di tutte gli elementi nella hashmap, comprese le Bitmap.

——————————————- **Test**:

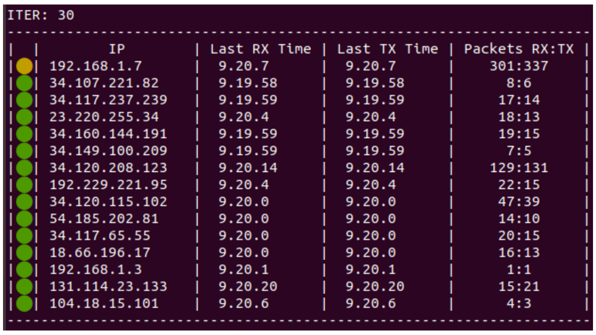
Per testare l'applicazione abbiamo creato uno script in python che consente di bloccare i pacchetti in uscita dal proprio device creando così un blackhole locale.

Quando arriverà un pacchetto viene creato il file rrd, aggiunto alla bitmap_BH l'indirizzo IP associato e creato un grafico che si aggiornerà ogni 5 secondi.



ITER: 28

IP	Last RX Time	Last TX Time	Packets RX:TX
192.168.1.7	9.20.7	9.20.7	300:337
34.107.221.82	9.19.58	9.19.58	8:6
34.117.237.239	9.19.59	9.19.59	17:14
23.220.255.34	9.20.4	9.20.4	18:13
34.160.144.191	9.19.59	9.19.59	19:15
34.149.100.209	9.19.59	9.19.59	7:5
34.120.208.123	9.20.14	9.20.14	129:131
192.229.221.95	9.20.4	9.20.4	22:15
34.120.115.102	9.20.0	9.20.0	47:39
54.185.202.81	9.20.0	9.20.0	14:10
34.117.65.55	9.20.0	9.20.0	20:15
18.66.196.17	9.20.0	9.20.0	16:13
192.168.1.3	9.20.1	9.20.1	1:1
131.114.23.133	9.20.16	9.20.16	15:20
104.18.15.101	9.20.6	9.20.6	4:3

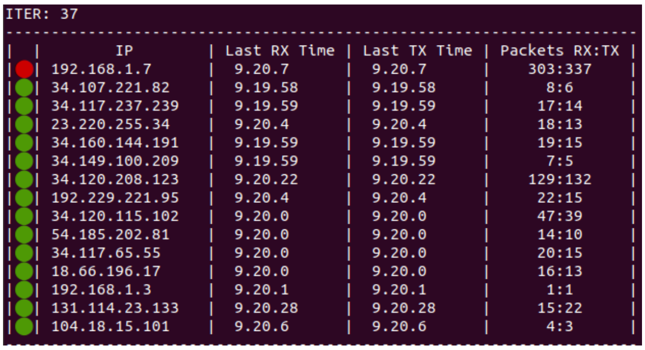


ITER: 30

IP	Last RX Time	Last TX Time	Packets RX:TX
192.168.1.7	9.20.7	9.20.7	301:337
34.107.221.82	9.19.58	9.19.58	8:6
34.117.237.239	9.19.59	9.19.59	17:14
23.220.255.34	9.20.4	9.20.4	18:13
34.160.144.191	9.19.59	9.19.59	19:15
34.149.100.209	9.19.59	9.19.59	7:5
34.120.208.123	9.20.14	9.20.14	129:131
192.229.221.95	9.20.4	9.20.4	22:15
34.120.115.102	9.20.0	9.20.0	47:39
54.185.202.81	9.20.0	9.20.0	14:10
34.117.65.55	9.20.0	9.20.0	20:15
18.66.196.17	9.20.0	9.20.0	16:13
192.168.1.3	9.20.1	9.20.1	1:1
131.114.23.133	9.20.20	9.20.20	15:21
104.18.15.101	9.20.6	9.20.6	4:3

Se riceve il primo pacchetto nei primi 20 secondi in cui ne manda all'inizio viene segnalato visualizzando a schermo il colore giallo.

se continua a ricevere pacchetti allora verrà visualizzato il colore rosso.



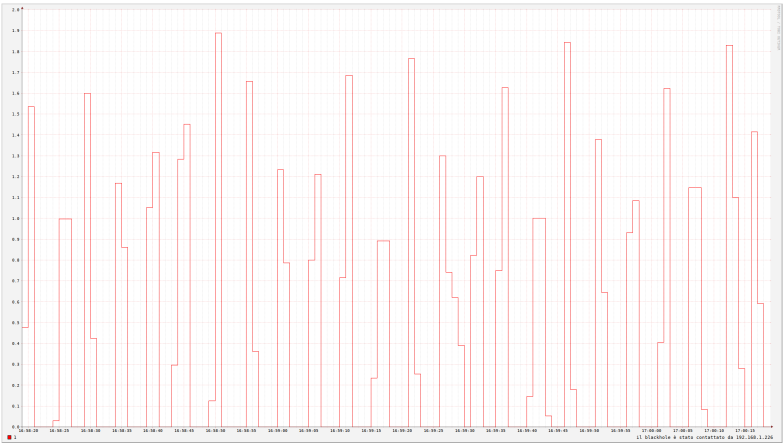
ITER: 37

IP	Last RX Time	Last TX Time	Packets RX:TX
192.168.1.7	9.20.7	9.20.7	303:337
34.107.221.82	9.19.58	9.19.58	8:6
34.117.237.239	9.19.59	9.19.59	17:14
23.220.255.34	9.20.4	9.20.4	18:13
34.160.144.191	9.19.59	9.19.59	19:15
34.149.100.209	9.19.59	9.19.59	7:5
34.120.208.123	9.20.22	9.20.22	129:132
192.229.221.95	9.20.4	9.20.4	22:15
34.120.115.102	9.20.0	9.20.0	47:39
54.185.202.81	9.20.0	9.20.0	14:10
34.117.65.55	9.20.0	9.20.0	20:15
18.66.196.17	9.20.0	9.20.0	16:13
192.168.1.3	9.20.1	9.20.1	1:1
131.114.23.133	9.20.28	9.20.28	15:22
104.18.15.101	9.20.6	9.20.6	4:3

Se riprende a funzionare verrà aggiornato lo stato in verde e sarà rimosso dalla bitmap_BH.

Esempio di un Grafico:

Notare in basso a destra del grafico c'è la lista degli host che hanno provato a mandargli pacchetti.



———————————————- **Conclusioni**:

Il tool funziona bene nei test, purtroppo prendendo in considerazione solamente i pacchetti TCP è molto limitato in una situazione reale.

In caso venisse esteso con più protocolli potrebbe essere utile come modo per scovare possibili attaccanti, facendo eseguire nmp su un server che vede passare tutto il traffico north-south di una rete, e segnalare gli host che per qualche motivi sono andati down oppure eventuali attaccanti.