VOLUMETRIC ATTACK DETECTION

Progetto di Gestione di Reti
Andrea Luchetti
2024/2025

1. Introduzione:

Il tool nasce dall'esigenza di capire se una rete è sotto attacco volumetrico, come attacco DoS (Denial of Service) o DDoS (Distributed Denial of Service). Questi attacchi mirano a sovraccaricare la rete, rendendo i servizi inutilizzabili agli utenti legittimi. L'analisi viene eseguita su file di tipo "pcap". Il file pcap viene catturato dal firewall e analizzato dal tool, che gestisce il processo in modo automatico: scarica il file, lo elabora, lo rimuove dalla memoria del firewall e avvia una nuova scansione dopo un intervallo di tempo predefinito.
Il progetto è pensato per interfacciarsi con un firewall Mikrotik, che permette di utilizzare il tool "Packet Sniffer" che cattura i pacchetti transitati.
Grazie anche all'uso di chiavi pubbliche, è possibile effettuare l'accesso remoto senza la necessità di inserire credenziali.
I passaggi principali del processo sono:

- Collegamento al firewall
- Configurazione dello sniffer
- Avvio dello sniffing
- Interruzione dello sniffing
- Cattura del file pcap
- Analisi del file
- Rimozione del file dal firewall
- Riavvio dello sniffing

2. Descrizione tool:

Il tool si compone di tre modalità:

1. **Modalità analisi di un file**: Questa modalità legge e analizza un file "pcap" presente nella stessa directory specificata. Il tool apre il file, legge e analizza ogni pacchetto catturato.
2. **Modalità analisi dei limiti**: Questa modalità avvia un'analisi temporizzata per determinare il traffico medio di pacchetti sulla rete durante un intervallo predefinito. Viene calcolato un limite medio di pacchetti/sec. Viene aggiunto scarto di 100 pacchetti/sec per gestire picchi di traffico legittimi. Al termine dell'analisi, il tool passa automaticamente alla modalità ascolto.
3. **Modalità ascolto**: In questa modalità, il tool si collega al firewall e avvia un ciclo infinito. Ogni intervallo di tempo predefinito, interrompe la scansione, scarica il file pcap, lo analizza e riavvia la scansione.

L'analisi del file catturato avviene suddividendo i pacchetti in blocchi di 30 secondi, durante i quali viene conteggiato il numero di pacchetti e di byte transitati. I pacchetti vengono inseriti in una struttura dati RRD (Round Robin Database) in base all'indirizzo IP di destinazione e alla porta. Alla fine di ogni intervallo di 30 secondi, il tool genera un report con le statistiche dell'intervallo e, alla conclusione dell'intero processo, produce un report finale dell'analisi.

Per calcolare il numero medio di pacchetti al secondo, il tool utilizza il “timestamp” di ogni pacchetto del file. Una volta letto il primo pacchetto viene salvato il “timestamp” e confrontato con i pacchetti successivi. La variabile “deltaSec” calcola il tempo trascorso tra l'inizio dell'intervallo e il pacchetto corrente. Quando “deltaSec” raggiunge 30 secondi, vengono calcolate e stampate le statistiche relative a quell'intervallo. Al termine dell'analisi di tutti i pacchetti, il “timestamp” dell'ultimo pacchetto viene utilizzato per calcolare il tempo totale di osservazione del traffico.

3. Configurazione del tool

Per far funzionare correttamente il tool, è necessario che sia già stato effettuato lo scambio delle chiavi pubbliche per l'autenticazione SSH senza password con il firewall MikroTik. Di seguito sono riportati i passaggi per generare e scambiare le chiavi pubbliche:

I. Create a new public key:
```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/mikrotik_rsa -N ""
```
II. Condividere la chiave pubblica con miktorik:
```
scp ~/.ssh/mikrotik_rsa.pub admin@ip:/
```

III. Aggiungere la chiave pubblica all'account:
```
ssh admin@ip
/user ssh-keys import public-key-file=mikrotik_rsa.pub
user="MIKROTIK_USER"
```

IV. Testare la connessione con:
```
ssh -i mikrotik_rsa MIKROTIK_USER@ip
```

Il tool per essere efficiente deve essere adattato alle proprie esigenze, queste sono le variabili che devono essere modificate all’interno del codice:

- **PACKET_THRESHOLD**: Definisce la soglia di pacchetti al secondo oltre la quale il traffico è considerato sospetto. Il valore predefinito è 3000 pacchetti/sec, ma viene dinamicamente calcolato durante la modalità "analisi dei limiti".

- **FILE_TO_CHECK**: Il nome del file “.pcap” da recuperare dalla memoria del firewall. Predefinito: "./sniffer.pcap".

- **SLEEP_INTERVAL**: Intervallo di tempo (in secondi) tra una scansione e la successiva. Un valore più basso produce statistiche meno accurate ma più rapide, mentre un valore più alto migliora l'accuratezza, aumentando però la dimensione del file di cattura. Predefinito: 120 secondi (2 minuti).

- **REMOTE_FILE**: Percorso del file di cattura remoto sul firewall MikroTik. Predefinito: "./sniffer.pcap".

- **LOCAL_FILE**: Directory locale in cui verranno salvati i file catturati dal firewall. Predefinito: "." (la cartella corrente).

- **MIKROTIK_USER**: Nome utente utilizzato per accedere al firewall MikroTik. Predefinito: "admin".

- **MIKROTIK_IP**: Indirizzo IP del firewall MikroTik.
- **SSH_KEY_PATH**: Percorso della chiave privata SSH utilizzata per connettersi al firewall. Predefinito: "./mtik_rsa".
- **RRD_SIZE**: Numero massimo di indirizzi IP di destinazione da tracciare e monitorare nella struttura RRD (Round Robin Database). Predefinito: 100.

4. Esempio

Modalità analisi di un file


```
1
Elenco dei file disponibili con estensione .pcap:
    1: TrafficoLegittimo.pcap
    2: TrafficoMalevolo.pcap
Inserisci il numero corrispondente al file da analizzare: 2
Modalità analisi avviata con soglia 3000 Packets/sec.
        che pacchetti vuoi analizzare?
         premi:
         1: TCP
         2: UDP
         3: TUTTI
        3



        Analyzing file: TrafficoMalevolo.pcap

…
…

Interval duration: 30.06 seconds
Packets in interval: 233660, Bytes in interval: 12427273
Packets/sec: 7773.2, Bytes/sec: 413.42 KB/sec

                        WARNING: Possible DDoS detected! 7773.2
packets/sec or 413419.36 bytes/sec

Interval duration: 30.00 seconds
Packets in interval: 647, Bytes in interval: 79792
Packets/sec: 21.6, Bytes/sec: 2.66 KB/sec
No DDOS attack detected! 21.6 packets/sec or 2659.67 bytes/sec
…
```

…

Final interval duration: 29.04 seconds
No DDOS attack detected! 18.5 packets/sec or 2386.87 bytes/sec

Total capture time: 299.33 seconds
Total Packets: 346910, Total Bytes: 18631496
Overall Packets/sec: 1159.0, Overall Bytes/sec: 62.24 KB/sec

Statistiche traffico:
…
…
P: 192.168.100.255:
        Porta: 9956, Pacchetti: 12
        Porta: 138, Pacchetti: 3
        Porta: 137, Pacchetti: 1
…
…

Vuoi analizzare un nuovo file?
y:yes oppure n:no n

Modalità analisi dei limiti e modalità ascolto

2
modalità analisi dei limiti avviata
Cercando di connettermi al firewall...
File configurato correttamente...
Ho avviato l'iterazione numero: 1 di 2
sniffer.pcap   100%   10MB 16.8MB/s   00:00
File remoto eliminato con successo!
Attesa di 60 secondi prima del prossimo controllo...
Ho avviato l'iterazione numero: 2 di 2
sniffer.pcap   100%   10MB 16.8MB/s   00:00
File remoto eliminato con successo!
Attesa di 60 secondi prima del prossimo controllo...
Raggiunto il numero massimo di 2 iterazioni, uscita dal ciclo
L'analisi del traffico ha portato ad una soglia della rete a 1656 Packets/sec, continuo l'analisi con tale soglia+100
Modalità ascolto avviata con soglia 1756 Packets/sec. Controllo ogni 60 secondi se esiste './sniffer.pcap'.
File configurato correttamente...
Sniffer avviato con successo!
Ho avviato la cattura dei pacchetti numero: 1 e attendo 60 secondi per l'analisi numero 2
Tentativo di scaricare il file dal firewall...
sniffer.pcap   100%   10MB 16.9MB/s   00:00
File scaricato con successo!
Analisi in corso...

```
Interval duration: 30.10 seconds
Packets in interval: 9814, Bytes in interval: 6746603
Packets/sec: 326.1, Bytes/sec: 224.17 KB/sec
No DDOS attack detected! 326.1 packets/sec or 224173.01 bytes/sec

Final interval duration: 11.79 seconds
No DDOS attack detected! 425.5 packets/sec or 276054.99 bytes/sec

Total capture time: 41.88 seconds
Total Packets: 14829, Total Bytes: 10000332
Overall Packets/sec: 354.1, Overall Bytes/sec: 238.77 KB/sec

Statistiche traffico:
…
…
IP: 192.168.100.152:
        Porta: 7437, Pacchetti: 1
        Porta: 10001, Pacchetti: 5
        Porta: 6667, Pacchetti: 5
        Porta: 5678, Pacchetti: 8
        Porta: 443, Pacchetti: 24
IP: 8.8.8.8:
        Porta: 53, Pacchetti: 9
…
…
File remoto eliminato con successo!
Attesa di 60 secondi prima del prossimo controllo...
Sniffer avviato con successo!
Ho avviato la cattura dei pacchetti numero: 2 e attendo 60 secondi
per l'analisi numero 3
^C
Ho catturato l'interruzione e ho interrotto la cattura
```

5. Note finali

Inizialmente il tool era pensato per riconoscere un attacco DDOS, che comporterebbe il riconoscimento anche di un attacco DOS. Per questioni di tempo non sono riuscito a capire come distinguere un traffico legittimo da un traffico malevolo, ho quindi optato per una opzione più semplice nella quale analizzo un frangente di traffico lecito per determinare una media di pacchetti al secondo, capendo quindi quando nella rete sta trafficando una quantità anomala di pacchetti. Grazie alla struttura rrd è possibile intuire quale servizio è sotto attacco.