Nordio Filippo
nordio.filippo715@gmail.com

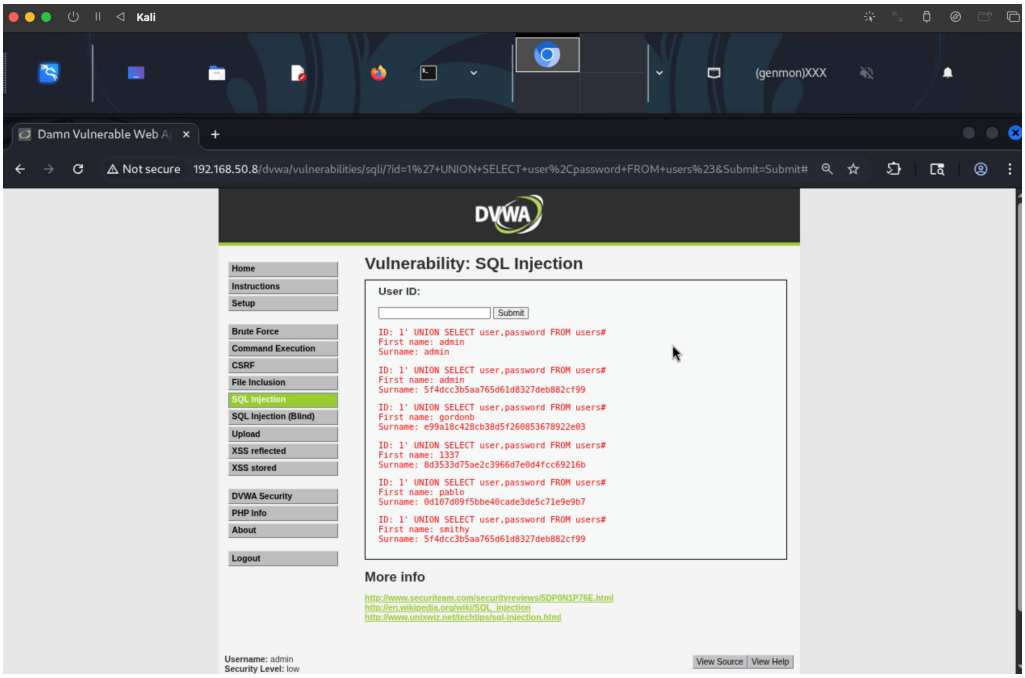
Cyber Security

Indice:

0)

-In questo esercizio dobbiamo craccare le password trovate nella nostra DVWA in SQL injection
-Nell'esercizio facoltativo dobbiamo simulare un attacco DoS usando Slowloris sulla nostra Metasploitable.

1)



-Come prima cosa troviamo gli hash da craccare, andiamo nella nostra DVWA e su SQL injection (ovviamente prima di fare questo andiamo su DVWA security e cambiamo il livello di sicurezza da high a low) e usiamo il comando: 1' UNION SELECT user, password FROM users# ,ci darà gli hash da craccare.

2)

-Successivamente creiamo una cartella nel nostro desktop con gli hash trovati e andiamo a visualizzarla nel nostro terminale come nella foto qui sopra.

3)

-Una volta creata la cartella andiamo ad usare il nostro JohnTheRipper con il comando : "john --format=raw-md5 --wordlist=/home/kali/Desktop/rockyou.txt /home/kali/Desktop/hash.txt ".
Ci restituirà le varie password dei vari hash in ordine in base a come li abbiamo scritti nel nostro documento creato.

4)

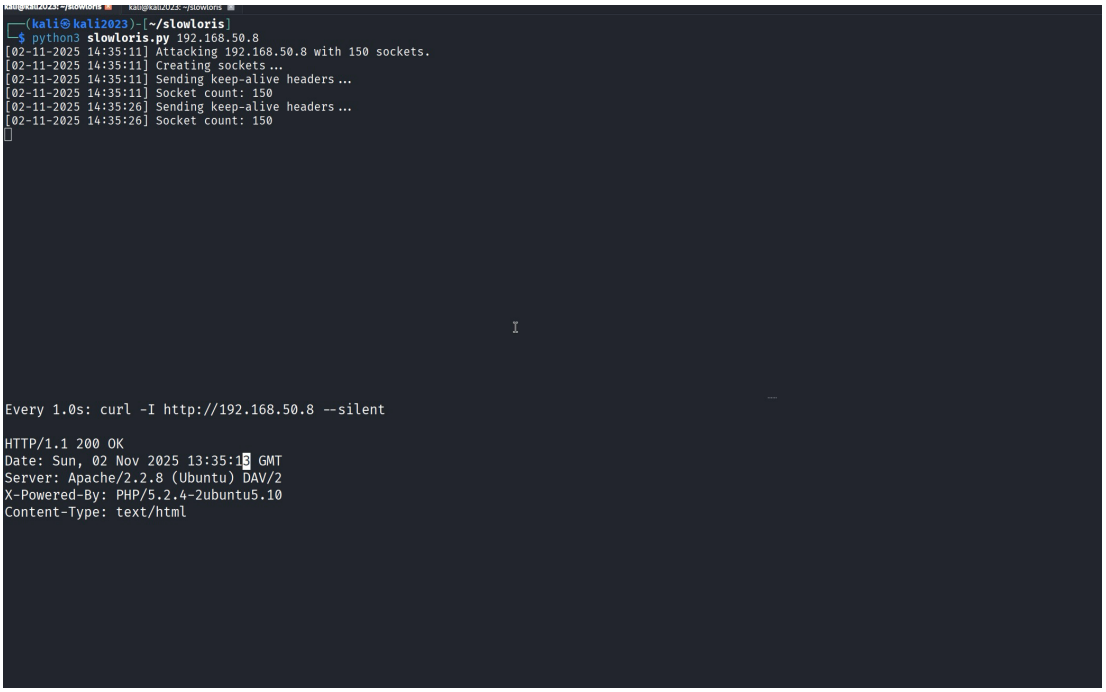
Interveniamo immediatamente sul sistema compromesso
Azioni da eseguire:
• Disconnettere immediatamente il sistema infetto dalla rete per prevenire la propagazione del malware verso altri dispositivi o server.
• Isolare fisicamente la macchina compromessa, rimuovendo eventuali connessioni cablate o wireless.
• Se le condizioni lo permettono, eseguire un backup offline dei dati critici al fine di preservarli da ulteriori compromissioni.
• Segnalare tempestivamente l'incidente al team IT e ai responsabili della sicurezza informatica per l'attivazione delle procedure di risposta all'incidente.

Procedure di messa in sicurezza
• Eseguire una formattazione completa e procedere con la reinstallazione pulita del sistema operativo.
• Ripristinare il sistema da un backup verificato e precedente all'infezione, per garantire l'integrità dei dati.
• Impiegare strumenti di rimozione malware professionali per l'individuazione e l'eliminazione di eventuali residui dell'infezione.
• Aggiornare il sistema operativo e le applicazioni a versioni recenti e supportate, in modo da ridurre le vulnerabilità e migliorare la sicurezza complessiva.

5)

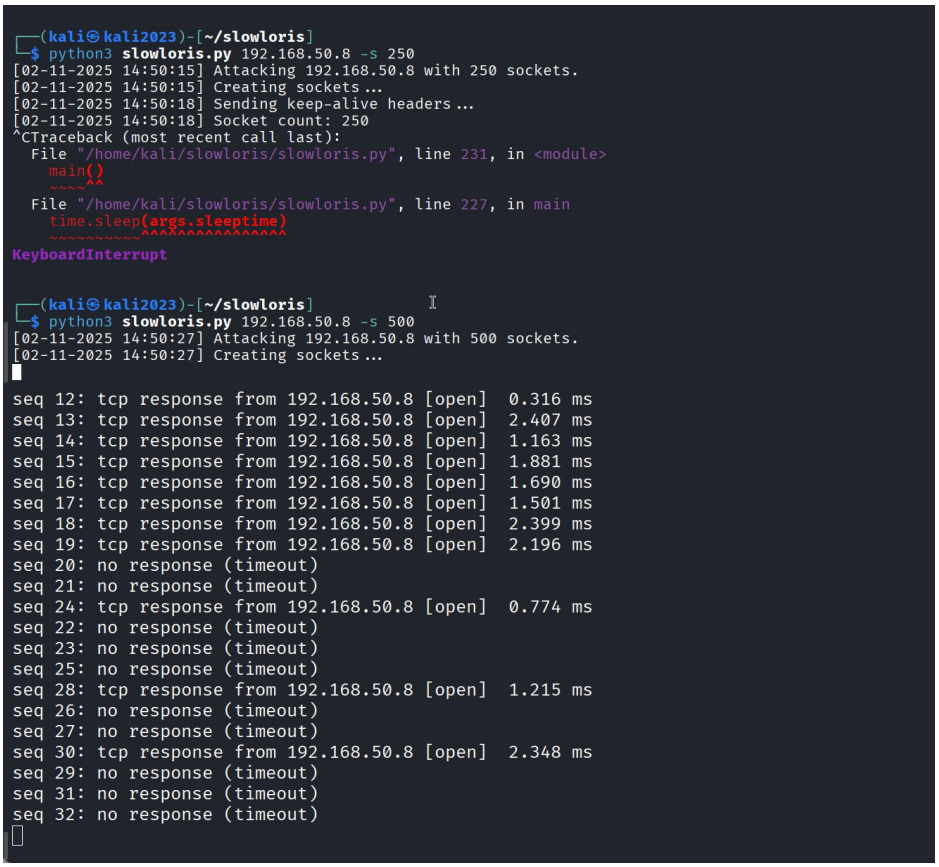
```
┌──(kali㉿kali2023)-[~]
└─$ git clone https://github.com/gkbrk/slowloris
fatal: destination path 'slowloris' already exists and is not an empty directory.

┌──(kali㉿kali2023)-[~]
└─$ cd scd slowloris

┌──(kali㉿kali2023)-[~/slowloris]
└─$
```

-Cloniamo Slowloris con il comando "git clone" e successivamente il link fornitoci : https://github.com/gkbrk/slowloris
-Andiamo nella directory con "cd"



-Successivamente avviamo slowloris con il comando "python3 slowloris.py 192.168.50.8" e si avvieranno i vari socket.
-Contemporaneamente monitoriamo il tutto con il comando "watch -n 1 --differences curl I http://192.168.50.200 --silent" per verificare la risposta del web server.

6)



-Avviamo slowloris aggiungendo al comando il "-s 500",significa che aumentiamo il numero di socket a 500
-Con il comando "tcping 192.168.50.8" monitorio la risposta del web server in tcp
-Come si vede dallo screen il server inizia a non rispondere più avendo aumentato i socket.

FINE