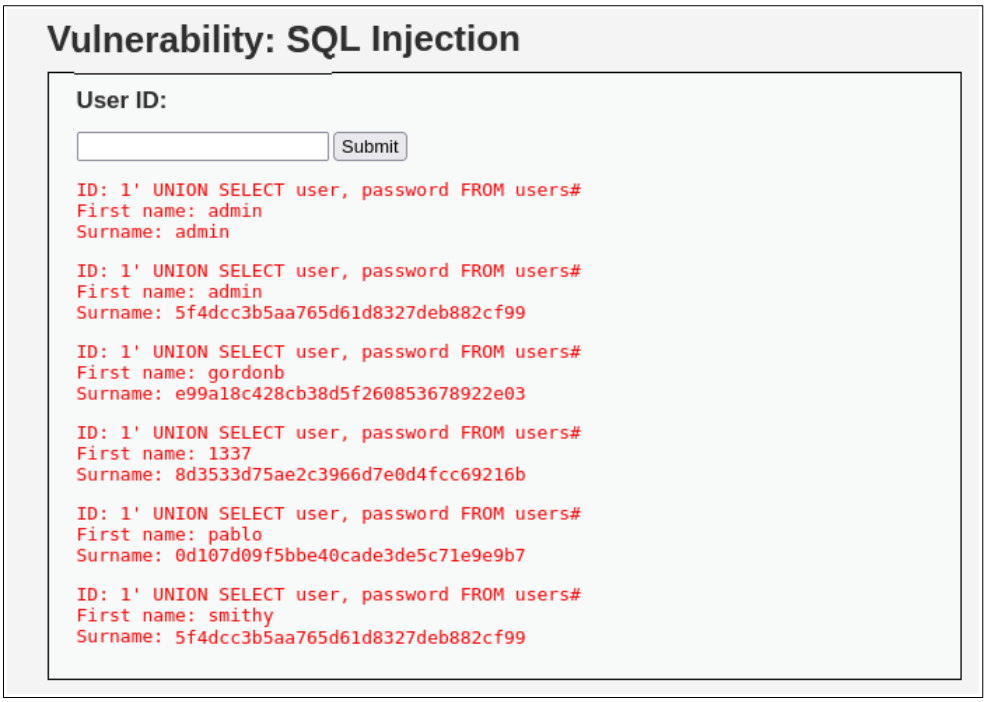
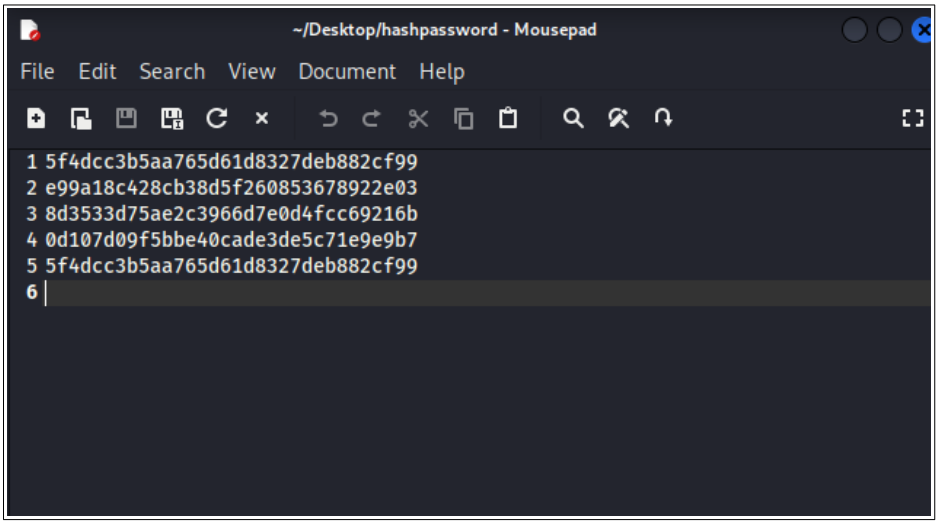
Report W14D1 Password cracking

In questo esercizio dovremo utilizzare un tool di password cracking per risolvere gli hash delle password travate tramite SQLi nel precedente esercizio.

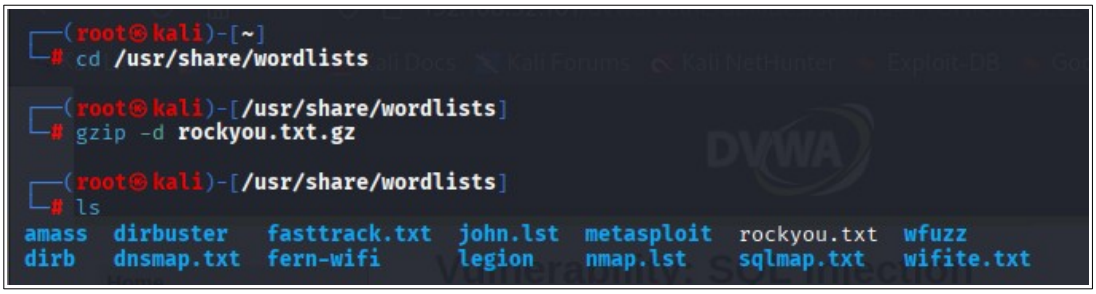
Step 1 Visualizziamo gli hash delle password da decifrare.



Step 2 Creiamo un file.txt sul Desktop contenente gli hash delle password da decifrare.

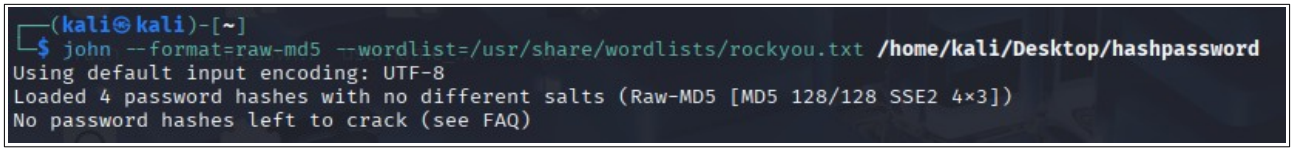


Step 3 Per eseguire il comando che ci servirà successivamente, dovremo prima estrarre il file rockyou contenuto nella cartella wordlist.
Rockyou è un file di password reali raccolte in un data-breach che John the Ripper (il tool che useremo per il cracking delle password) utilizzerà per risolvere gli hash.



Step 4 Per la funzione di password cracking utilizzeremo John the Ripper, tramite il comando john –format=raw-md5 --wordlist=/usr/share/wordlist/rockyou.txt /home/kali/Desktop/hashpassword.
La sintassi del comando è la seguente:

- --format=raw-md5: utilizza il formato di hash Raw-MD5;
- --wordlist=/usr/share/wordlist/rockyou.txt: usa la wordlist rockyou.txt come dizionario di attacco (specificato il path del file rockyou);
- /home/kali/Desktop/hashpassword: file da craccare con relativo path.



Step 5 Per avere un output pulito ed ordinato delle password utilizziamo il comando john –show –format=Raw-MD5 /home/kali/Desktop/hashpassword.

Il risultato finale saranno le password corrispondenti agli hash inseriti nel file.txt iniziale, per comodità verranno inseriti in una tabella riassuntiva.

Hash	Password in chiaro
5f4dcc3b5aa765d61d8327deb882cf99	password
e99a18c428cb38d5f260853678922e03	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	charley
0d107d09f5bbe40cade3de5c71e9e9b7	letmein
5f4dcc3b5aa765d61d8327deb882cf99	password

Facoltativo

Spiegare i passaggi di come si potrebbe mettere in sicurezza un computer aziendale affetto da WannaCry.

Azioni di contenimento pc infetto:

- Tempestiva disconnessione del computer affetto dalla rete aziendale, per limitare la diffusione del malware;
- Non spegnere o riavviare il computer per un'eventuale tentativo di recupero dati;
- Segnalare immediatamente l'incident al team IT (se l'azienda ne dispone), per una celere risposta all'infezione.
- Eseguire un backup dei dati non ancora criptati, (se possibile).

Possibili remediations post-incident:

- Scansione completa di tutti i pc aziendali per assicurarsi che il malware non si sia diffuso;
- Installazione o aggiornamento dell'antivirus;
- Formattazione del pc infetto e ripristino pulito del backup;
- Tentativo di recupero dati criptati con tool specifici (NO pagamento riscatto per decriptazione);
- Valutare se una segmentazione della rete possa aiutare contro attacchi futuri;
- Corsi di sicurezza ed educazione del personale ad un uso sicuro degli asset aziendali.

Esercizio Extra

Definire cos'è un DoS, un DDoS e uno Slowloris; successivamente lanciare il tool Slowloris contro la macchina Metasploitable 2 e controllare l'andamento del flusso con le utilities watch e tcping.

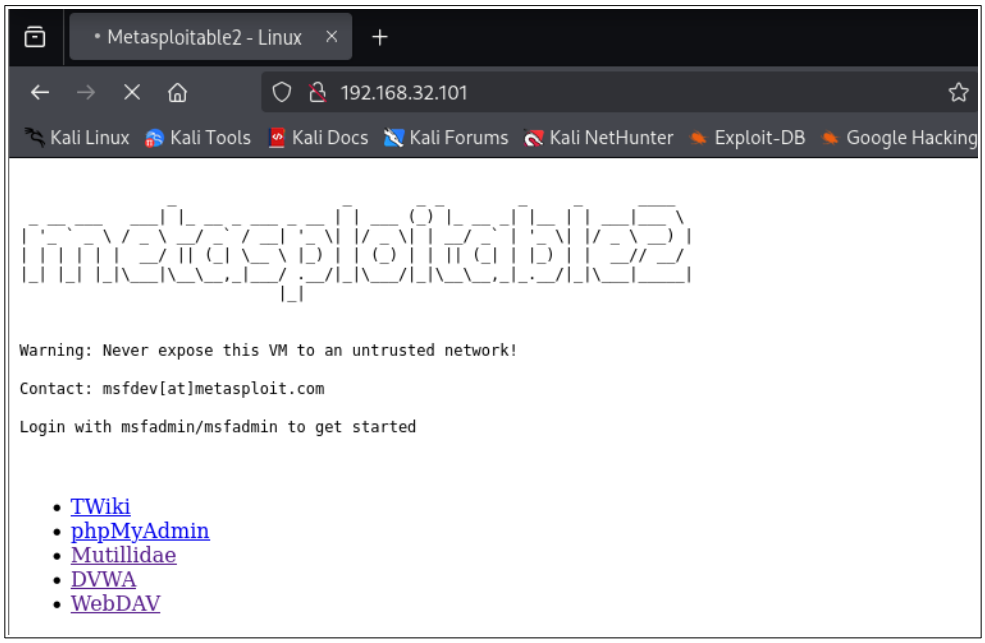
Attacco	Acronimo	Definizione
DoS	Denial of Service	Un attacco informatico che sfrutta tutte le risorse di un sistema, bloccandone il normale funzionamento e rendendolo inutilizzabile. Attacco veloce e massiccio.
DDoS	Distributed Denial of service	Simile a DoS ma eseguito da più botnet sul web.
Slowloris	/	Tipo di attacco DoS che mira a rendere un server web non disponibile, mantenendo aperte molteplici connessioni http. Attacco lento e silenzioso.

Attacco Slowloris su Metasploitable 2

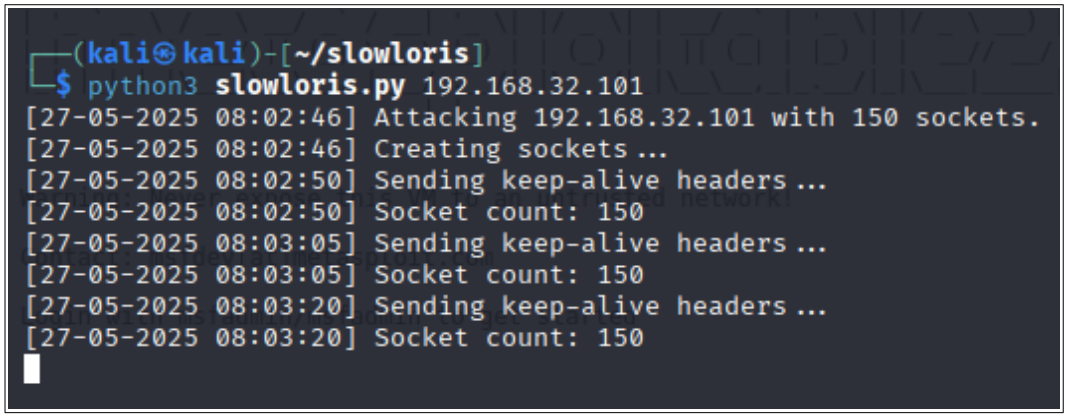
Step 1 Mentre abbiamo la macchina Kali collegata ad internet, scarichiamo il tool Slowloris tramite il comando git clone https://github.com/gkbrk/slowloris.

Step 2 Per scaricare l'utility Tcping utilizziamo il comando:
wget https://github.com/pouriyajamshidi/tcping/releases/latest/download/tcping-amd64.deb -O /tmp/tcping.deb
e successivamente il comando sudo apt install -y /tmp/tcping.deb per completare l'installazione.

Step 3 Rimettere la macchina Kali su rete interna con ip statico e testare la connessione con la macchina Metasploitable 2 tramite ping e provare a cercare l'ip di Metasploitable 2 tramite browser, verrà visualizzata la pagina nell'immagine sottostante.



Step 4 Tramite il comando python 3 slowloris.py <ip di Metasploitable 2> lanceremo l'attacco, infatti se proveremo a ricaricare la pagina della DVWA di Metasploitable 2, non saremo in grado di farlo, perché la porta 80 sarà satura.

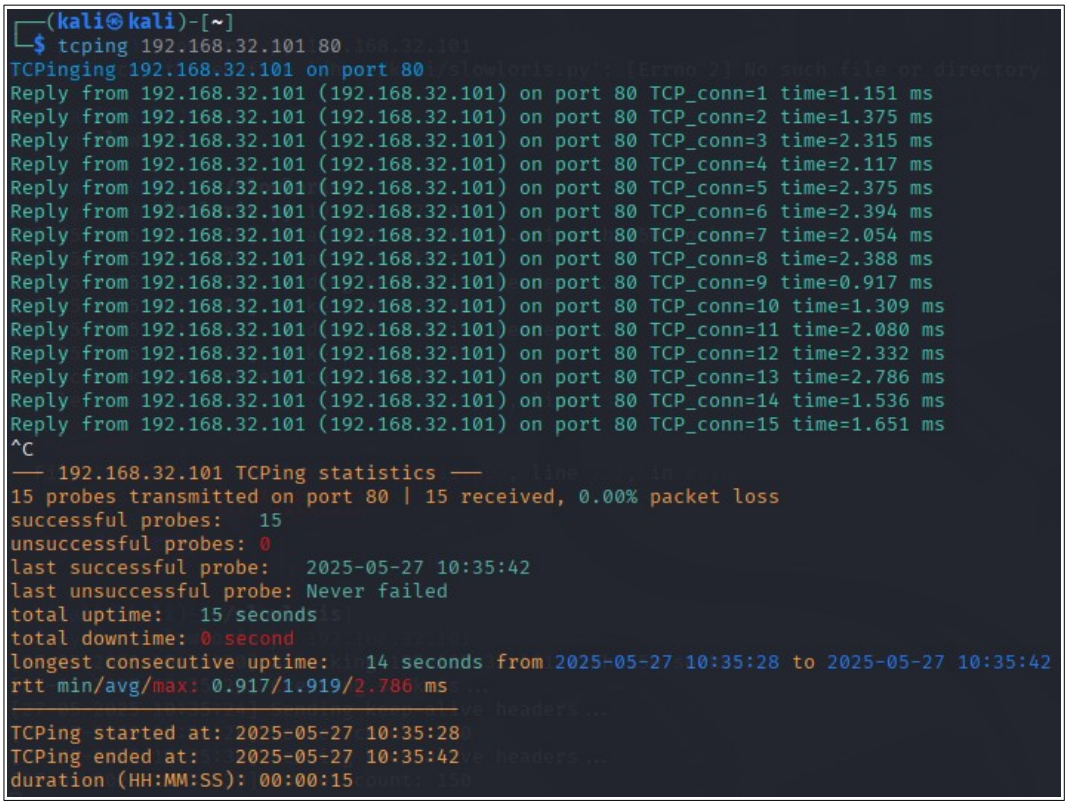


Step 5 tramite il comando watch -n 1 --differences curl -I http://192.168.32.101 --silent possiamo eseguire una richiesta HEAD per ogni secondo, in questo modo, se c'è connettività l'orologio prosegue, se la connettività è interrotta si ferma. Appena lanceremo l'attacco slowloris potremo notare che l'orologio si fermerà.
La sintassi del comando è la seguente:

- watch -n 1 –differences: esegue ripetutamente un comando e mostra le differenze tra un otuput e il successivo;

- curl -I http://192.168.32.101 --silent: effettua una richiesta HEAD (-I) all'indirizzo http di metaploitable 2 (usa la porta 80), per ottenere solo l'header della pagina, l'opzione --silent evita di mostrare progressi o messaggi di curl per avere un output pulito.

Step 6 Controllare la saturazione della porta 80 tramite l'utility Tcping.
Se i pacchetti inviati tramite l'attacco slowloris sono pari a 150, sarà comunque possibile inviare pacchetti TCP tramite Tcping ed avere una risposta positiva.



Aumentando i pacchetti inviati tramite slowloris con lo switch -s <numero pacchetti> (in questo caso 300), vedremo che la risposta non sarà sempre positiva ed alcuni pacchetti TCP inviati tramite Tcping verranno persi.