

Anonforce



Anonforce

boot2root machine for FIT and bsides guatemala CTF

[Task 1] Anonforce Machine

Read user.txt and root.txt

#1
user.txt

606083fd33beb1284fc51f411a706af8

#1
root.txt

f706456440c7af4187810c31c6cebdce

nmap-scan

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 Aug 06 13:41 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 106 0     0      0 Aug 06 13:41 proc
| drwx-----  3 0      0      4096 Aug 11 2019 root
| drwxr-xr-x 18 0      0      540 Aug 06 13:41 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 Aug 06 13:41 sys
```

Only 20 shown. Use --script-args ftp-anon.maxlist=-1 to see all.

ftp-syst:

STAT:

FTP server status:

Connected to ::ffff:10.2.27.69

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 1

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

creds

xbox360

root:-

\$6\$07nYFaYf\$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1yclm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM

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:::

uuid*:18120:0:99999:7:::

melodias:\$1\$xDhc6S6G\$IQH5ZtMkBQ5pUMjEQtL1:18120:0:99999:7:::

sshd*:18120:0:99999:7:::

ftp*:18120:0:99999:7:::

root:hikari

writeup

-----user-flag-----

--ran **nmap -sC -sV <IP>** and found open ports on **21** and **22**, and also found **ftp anonymous login allowed**
--went to **ftp://anonymous@<IP>** and went to **/home/melodias** directory
--ran **cat user.txt** to get user flag:
606083fd33beb1284fc51f411a706af8

-----root-flag-----

--in my ftp web browser session I saw a directory **/notread**
--that directory contains a **backup.pgp** file and **private.asc**
--downloaded files and tried **gpg --import private.asc** but a password is required
--converted the hash using **gpg2john** with command **gpg2john private.asc > hash**, then cracked it with **john** to get password **xbox360**
--then ran **gpg --import private.asc** again with given password **xbox360** and then **gpg --decrypt backup.pgp** with **xbox360**, and got a shadow file with 2 hashes:
root:-
\$6\$07nYFaYf\$F4VMAegmz7dKjsTukBLh6cP01iMmL7CiQDt1yclm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:18120
melodias:\$1\$xDhc6S6G\$IQHUUW5ZtMkBO5pUMjEQtL1:18120:0:99999:7:::

--I then inserted them into a file called hashes, and cracked them with **john** to get **root** password **hikari**
--logged in with **ssh root@<IP>** and the password **hikari** with success
--then ran **cat /root/root.txt** to get root flag:
f706456440c7af4187810c31c6cebdce