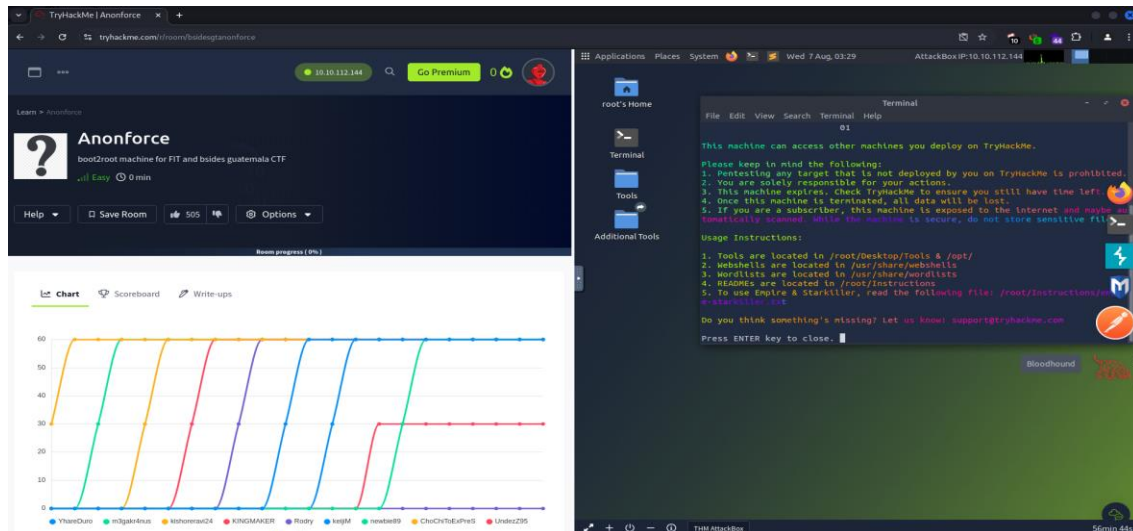


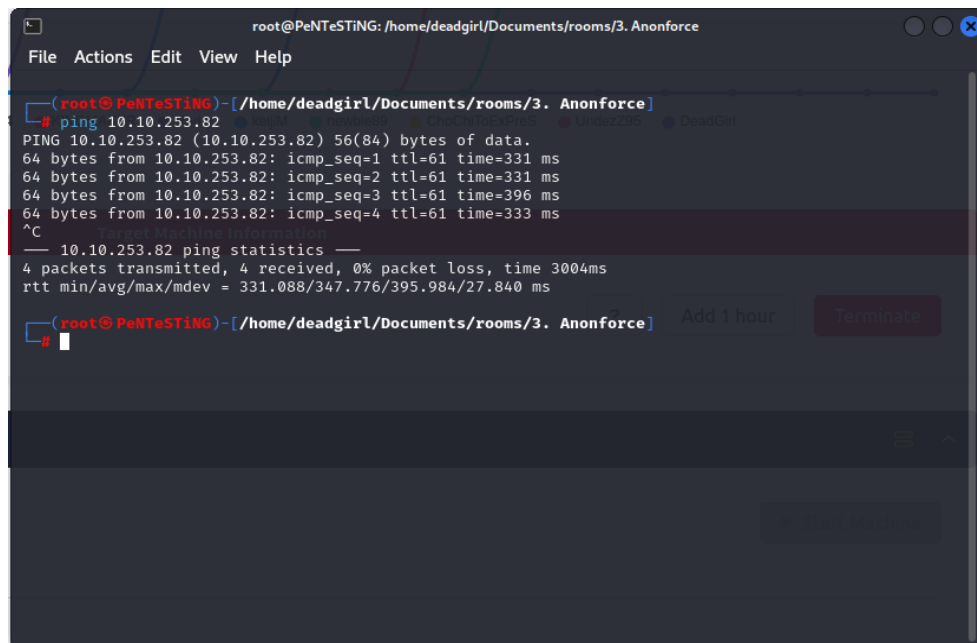


Anonforce

Anonforce es una maquina bastante sencilla que no toma entre 5 - 10 minutos el poder resolverla y el proposito es poder obtener información de claves privadas.



Lo primero es realizar ping hacia la máquina para corroborar que tenemos respuesta ICMP, con el comando **ping 10.10.253.82** (más adelante esta IP cambia... XD se me había acabado el tiempo XD)





Luego con el comando ***nmap -T4 -sVC 10.10.253.82*** veras los puertos abierto. Hay 2 servicios en ejecución: FTP y SSH.

```
root@PeNteStiNG: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help
(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# nmap -T4 -sVC 10.10.253.82
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 23:05 -04
Nmap scan report for 10.10.253.82
Host is up (0.34s 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:10.2.37.202
|_   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 Aug 06 20:03 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-g
|_ eneric
```

```
root@PeNteStiNG: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help
|_ lrwxrwxrwx  1 0      0           33 Aug 11 2019 initrd.img → boot/initrd.img-4.4.0-157-g
|_ eneric
|_ lrwxrwxrwx  1 0      0           33 Aug 11 2019 initrd.img.old → boot/initrd.img-4.4.0-1
|_ 42-generic
|_ drwxr-xr-x 19 0      0          4096 Aug 11 2019 lib
|_ drwxr-xr-x  2 0      0          4096 Aug 11 2019 lib64
|_ drwxr-xr-x  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
|_ lrwxrwxrwx  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 103 0      0           0 Aug 06 20:03 proc
|_ drwxr-xr-x  3 0      0          4096 Aug 11 2019 root
|_ drwxr-xr-x 18 0      0          540 Aug 06 20:03 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 20:03 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:
|_   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: 1 IP address (1 host up) scanned in 17.01 seconds
(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
#
```



Como se logra observar, no tan solo ha detectado el puerto 21 FTP abierto, sino que también ha descubierto un usuario **Anonymous**

```
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 20:03 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-g
eneric
```

Primero, iniciar sesión en FTP como Anonymous, aquí solicitara una Password, en mi caso solo presioné enter y pude ingresar vía Telnet.



Luego de un rato, comencé a moverme por los directorios para encontrar archivos valiosos. Después de un rato, encontré la primera bandera: **user.txt**

```
root@PeNteSTING: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help
ftp> ls
229 Entering Extended Passive Mode (|||7955|)
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 Aug 06 20:03 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-gen
eric
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 Aug 06 20:03 proc
drwx----- 3 0      0      4096 Aug 11 2019 root
drwxr-xr-x 18 0      0      540 Aug 06 20:03 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 20:03 sys
drwxrwxrwt  9 0      0      4096 Aug 06 20:03 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-gener
root.txt
```

```
root@PeNteSTING: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help
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-gener
ic
226 Directory send OK.
ftp> cd home
250 Directory successfully changed.
ftp> pwd
Remote directory: /home
ftp> ls
229 Entering Extended Passive Mode (|||28799|)
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
229 Entering Extended Passive Mode (|||34866|)
150 Here comes the directory listing.
-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
229 Entering Extended Passive Mode (|||44138|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% |*****| 33 429.68 KiB/s 00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.09 KiB/s)
ftp>
```



El archivo `user.txt` lo he copiado a mi directorio (he creado una carpeta que contiene lo archivos que iré descargando conforme vaya avanzando en la resolución de la máquina) y con el comando **`cat user.txt`** se obtiene la primera bandera.

```
root@PeNteStiNG: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help

(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# ls
user.txt
# cat user.txt
606083fd33beb1284fc51f411a706af8
#
```

Primera bandera

user.txt

606083fd33beb1284fc51f411a706af8

✓ Correct Answer



Regreso al directorio raíz y aquí observo otro directorio con el nombre **notread**.

```
root@PeNteSTING: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help
ftp> pwd
Remote directory: /home/melodias
ftp> cd ..
250 Directory successfully changed.
ftp> cd ..
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||46528|)
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 Aug 06 20:03 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-gen
eric
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 Aug 06 20:03 proc
drwx----- 3 0 0 4096 Aug 11 2019 root
drwxr-xr-x 18 0 0 540 Aug 06 20:03 run
drwxr-xr-x 2 0 0 12288 Aug 11 2019 sbin
drwxr-xr-x 3 0 0 4096 Aug 11 2019 srv
```

Con el comando **cd notread** ingresar a dicho directorio y posterior con el comando **ls** se observa 2 archivos:

- **backup.pgp**
- **private.asc**

```
root@PeNteSTING: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help
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-gen
ic
226 Directory send OK.
ftp> cd notread
250 Directory successfully changed.
ftp> pwd
Remote directory: /notread
ftp> ls
229 Entering Extended Passive Mode (|||59684|)
150 Here comes the directory listing.
-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 backup.pgp
local: backup.pgp remote: backup.pgp
229 Entering Extended Passive Mode (|||61792|)
150 Opening BINARY mode data connection for backup.pgp (524 bytes).
100% [*****] 524 446.91 KiB/s 00:00 ETA
226 Transfer complete.
524 bytes received in 00:00 (1.52 KiB/s)
ftp> get private.asc
local: private.asc remote: private.asc
229 Entering Extended Passive Mode (|||59579|)
150 Opening BINARY mode data connection for private.asc (3762 bytes).
100% [*****] 3762 143.50 MiB/s 00:00 ETA
226 Transfer complete.
3762 bytes received in 00:00 (10.94 KiB/s)
ftp>
```



Con el comando **get** descargar ambos archivos al directorio de preferencia (en mi caso he creado un directorio exclusivo para la resolución de la máquina)

Luego con el comando **cat private.asc** y el comando **cat backup.gpg** se observa el bloque de claves cifrados, al igual que con el comando **strings** se intenta observar para el archivo backup.gpg la clave cifrada, pero sigue siendo ilegible.

```
root@PeNtEStiNG: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help

(root@PeNtEStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# cat private.asc
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: BCPG v1.56

lQOBBF1Q5b0RCACMPpWfiiRRNpQxK0kAhv2w69+5fSmbS4+4QxgoDSBIIITWNkAF
GTVoPBz3My0NzF4IN5GTspwgZtwF0eQixsuM41CiGQzqRMPHIuxwJeqjWfSaaVRP
6IXFMaLa0nOg9CNmhljzIUdu2yLRCLWBrmCFptFmhL60NeP4tOCX9Vbok2TvFSdT
cbeXyOFraia9bAKtf9Ioky7Jyja06HF9XZ8o2k+LKVyaAkj/Vmxoo6DISHZZbMuJ
HcwR86Dw7+agpqpX4hLvGoZASMrX/qpmWZrePtHw1wHuN9/vhu0QFFQRmTrxRrgz
73iazo3s6QDtdEWNakJf0FWw3YAqmZWbZxvdAQDCsrET6ESqWRweYj45mQimgGYq
snIw5fskEE4M1xQ5ywf/SXgpGC50Ffo27EEdtpnCZKjKicv53+6LXL8pV1zVs4r
3PCY0oI0xyYQzTvcfCLGzBmCuUx6KdNXswlrqprTWT4K/NT54UbJ4QUjtr9unA2v
SjL/+T+e8IAdq+cifpONsbJ/PprDW+SYeB04sKZJ4FQ34N7E6NsdgONQehQNn5tm
x1Zq6bqfsJ+GdE0RLjugRbNEtnRCf6pm573kWNqrZa38EuQtVxV8NmOyomFA0q5Z
FDZilngg9kSwcQLfvwWtbNdrPLe8p0iafEL70fYvUXDY03LBFx6wG/H8fIJYs0JA
JpX8xVpFngEtinZjIB3iqVAootZhs3fM9Bo0Z9IpAf+L3ILQU1xULjB1qB6LA9a
4RM3rJWeCqFuLAHGrzJ9sKhNP35IQ084x+Pyx9KFbKgzDjeA3v3RL27Iec887hMW
z8ZmvEu5+UBUysSR84rrtaF7KB3EM0fZCettwukUasj0BsdAU9TcSEXF5++jkC
Fg2p8RGyDvVvIZMmI4kpyJwsKinZiNEWHbcpOWWkJOH7AOjuXiqUE+DU7YueYVpi
cnqPsdZAnzbh18U5AapzSev4S/qQXDeGve5L4twUfseZKB5JqHThpct2rH+hTXL
YRawy2DG+C8y/7sBX+kfybeKL5nY4e8Z1hoD+gGmSPwDS0APAzU/Y5DfIokvXwF
uv4JAwLX0R2b9tCJaGBdBE2CV47MYrqfCg88c/d58mscV7VUZcSL9Cskd4MiZt
uDtjo/DRa39fs9srk6apLQE7seev9pfngtUFiR7iY0LXE2V3tCJhbm9uZm9yY2Ug
PG1lbG9kaWZzQGfub25mb3JjZS5uc2E+IF4EEeEIAAYFAL1Q5b0ACgkQuZSR8oCt
gsLYAD+MnWnZUPILmIdWvDHmq8bk49t0jVfqu0e//LuaBI2joA/juindQ78DzX
bQ6FQg8KKIQCNo6cukKUQ6LLAfrVozlnQE/BF1Q5b0QAgCULP7Alf04XuKGVCS4
NvyBp0KA0m0wjndOHRNSIz44x24vLFT00GrueWjPMqRRLLH08zLJS/BXO/BHo6yp
jN87AfoVPV1hcq20MEW2iujh3hBwthNwBWhKdPXOndJGZaB7LshLJuWv9z6WyDN
```

```
root@PeNtEStiNG: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help

(root@PeNtEStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# cat backup.gpg
***bheaa)g+l=++++^+QA[x+~+NZI+p+J++Q++R`n<!7P["u[m9+++4
++++.$++G[+e+hW+aQ++3i+[+e+>+J/
=8B+++++F>+At+c+eN+8+!+Y+++++^+e+e+p+e+h+|.v+eOagb+e,+++2++3+6+.QkuX++=X3+e++=2+}w+|K+NR(h+
:qy+G+I+e+(W+Y!S+e+cE+h=8I+5.9+eW+++++v+{Kq+++++[^{L(+++++4!
+++++C~+G+e+rP5+z+tm`V+++++PX9++
+a+++i+etx+{L+!(+n+e#++7++=++++0+
+a+U0+0++++VNZ++w+an\+d60
LTS>+
VE+++h+/n|$@nvR+T:++*3+_I+z+0+$++{+0+++X+++++eXJ++f++++[M[+.
++@CS|

(root@PeNtEStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# strings backup.gpg
;R`n<
!7P["u
J=8B
|.v*
NR(h
h=8I
tm`V
U0+0
LTS>
/n|$@nvR
@CS|

(root@PeNtEStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
#
```



Como se mencionó anteriormente, con los comandos `cat` y `strings` las claves privadas son ilegibles, con el siguiente comando **`gpg2john backup.pgp`** y el comando **`gpg2john private.asc`** se extraerá y transformará las contraseñas cifradas en archivos de clave GPG legible.

NOTA: GPG por su sigla en inglés (GNU Privacy Guard) es una herramienta de cifrado y firma digital que se utiliza para asegurar la comunicación y los datos mediante criptografía de clave pública

En mi caso cree un archivo de texto con el comando **`nano room-Anonforce`** el cual he guardado la clave cifrada del usuario anonforce, ya con el comando **`cat room-Anonforce`** se observa y corrobora que dicha clave ha sido guardada.

```
root@PeNteStiNg: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help

(root@PeNteStiNg)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# gpg2john backup.pgp

File backup.pgp
Encrypted data [sym alg is specified in pub-key encrypted session key]
SYM_ALG_MODE_PUB_ENC is not supported yet!
$gpg$*0*376*f4d05e78bd0365e8fb70ea19dcd683ea7c2e762a1112c24f6167dfbd62ba022cf3b11b2207ea1a32d5c65dd
0ada936c42e516b0e0e7558050484a33d587f33c1658ab33d32c21f7d77e7c97c4bc24e52286895e16a0f4c799e3e854201
deae2fd90d3a897176c247df495eb0ca2857a6592153fb1f866345ff683d3849a4352e398b6f57fb19c7f405f6f976f51a7
b0e4b7183bcf019e5b7e95b5ee99b96156c288df4a2e8f496d83401210c08929e88b9f78be81bec437e2c08a726c7cc72d2
5035917afdf7746d605685f59fa825d09f5839f9fad61ccb89015fbca699fb97478db7b4cf62128886ea923fdec3709a19
33de28bf4c24f8e0aaa619d1855302a4fae8c1e94564e5a83f8771a1b70d1a89b6e5ca8d8643604300b4c54533eec2f0c
5645a18add68c51e2f6e7c24406e765205ad543aed9522d8d585fccbb7204917e47acc3018c124201eeb16ca7bde308ea1e
558ebf2ffff8a965584aed91662e0817b1a08715db5b1e3e084d5bcf2e838de54043537c*0*18*0*0*0000000000000000

(root@PeNteStiNg)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# gpg2john private.asc

File private.asc
anonforce:$gpg$*17*54*2048*e419ac715ed55197122fd0acc6477832266db83b63a3f0d16b7f5fb3db2b93a6a995013b
b1e7aff697e782d505891ee260e957136577*3*254*2*9*16*5d044d82578ecc62baaa15c1bcf1cfd*65536*d7d11d9bf6
d08968:::anonforce <melodias@anonforce.nsa>:private.asc

(root@PeNteStiNg)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# nano room-AnonForce

(root@PeNteStiNg)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# cat room-AnonForce
$gpg$*17*54*2048*e419ac715ed55197122fd0acc6477832266db83b63a3f0d16b7f5fb3db2b93a6a995013bb1e7aff697
e782d505891ee260e957136577*3*254*2*9*16*5d044d82578ecc62baaa15c1bcf1cfd*65536*d7d11d9bf6d08968

(root@PeNteStiNg)-[/home/deadgirl/Documents/rooms/3. Anonforce]
#
```




Primero, use `gpg2john` para cambiar la clave privada al formato que John pueda leer y luego con el comando `John room-Anonforce --wordlist=/home/deadgirl/Desktop/rockyou.txt` descifrar la contraseña cifrada.

Con el comando `John room-Anonforce --show` verificar la password descifrada.

```
root@PeTeStiNG: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help

(root@PeTeStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# john room-AnonForce --wordlist=/home/deadgirl/Desktop/rockyou.txt
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:SHA512 11:SHA224]) is 2 for all loaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Camellia128 12:Camellia192 13:Camellia256]) is 9 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
xb0x360 (?)
1g 0:00:00:00 DONE (2024-08-06 23:21) 25.00g/s 23300p/s 23300c/s 23300C/s xb0x360..madalina
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@PeTeStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# john room-AnonForce --show
?:xb0x360

1 password hash cracked, 0 left

(root@PeTeStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
#
```

Con el comando `gpg --list-secret-keys` en mi caso quise listar las claves secretas y con el comando `gpg --import private.asc` se importa la clave privada.

```
root@PeTeStiNG: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help

(root@PeTeStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# gpg --list-secret-keys
/root/.gnupg/pubring.kbx

sec   dsa2048 2019-08-12 [SCA]
      4D2E29E1DEADB9BC160BD88B92CD1F280AD82C2
uid    [ unknown] anonforce <melodias@anonforce.nsa>
ssb    elg512 2019-08-12 [ER]

(root@PeTeStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# gpg --import private.asc
gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not changed
gpg: key B92CD1F280AD82C2: secret key imported
gpg: key B92CD1F280AD82C2: "anonforce <melodias@anonforce.nsa>" not changed
gpg: Total number processed: 2
gpg:      unchanged: 2
gpg:      secret keys read: 1
gpg:      secret keys unchanged: 1
```

[illegible]

```

root@PeNtEStiNg: /home/deadgirl/Documents/rooms/3. Anonforce
File Actions Edit View Help
root@PeNtEStiNg)~[/home/deadgirl/Documents/rooms/3. Anonforce]
# 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.bs0IBp0DwXvB9XI2EtULXJzBtaMZMNd2tV4uob5
RVM0:18120:0:99999:7:::
daemon*:17953:0:99999:7::: ? Add 1 hour Terminate
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:::

```



Lo mismo que se realizó anteriormente, he creado otro archivo, pero he copiado la clave cifrada del usuario **root** y he creado un archivo de texto con el comando y nombre **nano tryhackme** y con el comando **cat tryhackme** se muestra el contenido del archivo.

Volver a repetir el mismo procedimiento de descifrar la password con el comando **john tryhackme --wordlist=/home/deadgirl/Desktop/rockyou.txt** y con el comando **john tryhackme --show** se obtiene el comando **hokari**

```
(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# 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.bs0IBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5
RVM0:18120:0:99999:7:::

(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# nano tryhackme

(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# cat tryhackme
$6$07nYFaYf$F4VMaegmz7dKjsTukBLh6cP01iMmL7CiQDt1ycIm6a.bs0IBp0DwXVb9XI2EtULXJzBtaMZMNd2tV4uob5RVM0

(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# john tryhackme --wordlist=/home/deadgirl/Desktop/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# john tryhackme --show
?:hikari

1 password hash cracked, 0 left
```

Ahora tengo la contraseña de root. Consigue la bandera final.

```
root@ubuntu: ~
File Actions Edit View Help

(root@PeNteStiNG)-[/home/deadgirl/Documents/rooms/3. Anonforce]
# ssh root@10.10.124.96
The authenticity of host '10.10.124.96 (10.10.124.96)' can't be established.
ED25519 key fingerprint is SHA256:+bhLW3R5qYI2SvPQSCWR9ewCoewWWvFTVFQUAGr+ew.
This host key is known by the following other names/addresses:
 ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.124.96' (ED25519) to the list of known hosts.
root@10.10.124.96'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:~# whoami
root
root@ubuntu:~# ls
root.txt
root@ubuntu:~# cat root.txt
f706456440c7af4187810c31c6cebdce
root@ubuntu:~#
```

root.txt

f706456440c7af4187810c31c6cebdce

✓ Correct Answer



Congratulations!

You've completed the room! Share this with your friends:

 Twitter

 Facebook

 LinkedIn

[Leave feedback](#)