Universidad del Valle de Guatemala
Cifrado de Información
Diego Andrés Morales Aquino
21762

Ejercicio CTF introducción

Desafío 1

```
nobody@3d2533ce9269:/$ cd etc
nobody@3d2533ce9269:/etc$ ls
adduser.conf            e2scrub.conf      issue.net           networks       rc6.d              sudoers
alternatives            environment       kernel              nsswitch.conf  rcS.d              sudoers.d
apt                     fstab             ld.so.cache         opt            resolv.conf        sysctl.conf
bash.bashrc             gai.conf          ld.so.conf          os-release     rmt                sysctl.d
bindresvport.blacklist  group             ld.so.conf.d        pam.conf       security           systemd
binfmt.d                group-            legal               pam.d          selinux            terminfo
ca-certificates         gshadow           libaudit.conf       passwd         shadow             tmpfiles.d
ca-certificates.conf    gshadow-          login.defs          passwd-        shadow-            ucf.conf
cloud                   gss               logrotate.d         profile        shells             ufw
cron.d                  hidden_config.txt lsb-release         profile.d      skel               update-motd.d
cron.daily              host.conf         machine-id          python3        ssh                vim
dbus-1                  hostname          mime.types          python3.10     ssl                wgetrc
debconf.conf            hosts             mke2fs.conf         rc0.d          subgid             xattr.conf
debian_version          hosts.allow       modules-load.d      rc1.d          subgid-            xdg
default                 hosts.deny        motd                rc2.d          subuid
deluser.conf            init.d            mtab                rc3.d          subuid-
dhcp                    inputrc           netconfig           rc4.d          sudo.conf
dpkg                    issue             networkd-dispatcher rc5.d          sudo_logsrvd.conf
nobody@3d2533ce9269:/etc$ cat /etc/hidden_config.txt
Contraseña: LinuxForHackers
```

```
nobody@3d2533ce9269:/etc$ su hacker
Password:
hacker@3d2533ce9269:/etc$ sudo ls -la /home/hacker
[sudo] password for hacker:
sudo: a password is required
hacker@3d2533ce9269:/etc$ ls -la /home/hacker
total 24
drwxr-x--- 1 hacker hacker 4096 Feb 13 23:51 .
drwxr-xr-x 1 root   root   4096 Feb 13 23:51 ..
-rw-r--r-- 1 hacker hacker  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 hacker hacker 3771 Jan  6  2022 .bashrc
-r-------- 1 hacker hacker   58 Feb 13 23:51 .flag.txt
-rw-r--r-- 1 hacker hacker  807 Jan  6  2022 .profile
```

```
hacker@3d2533ce9269:~$ cd /home/hacker
hacker@3d2533ce9269:~$ ls
hacker@3d2533ce9269:~$ ls -a
.  ..  .bash_logout  .bashrc  .flag.txt  .profile
hacker@3d2533ce9269:~$ cat .flag.txt
¡Felicidades! Encontraste la bandera: FLAG{LINUX_BASICS}
```

Flag: FLAG{LINUX_BASICS}

Desafío 2:

```
PS C:\Users\diego\OneDrive\Documents\uvg\semestre 9\cifrados\repositorio\ejercicios\ctf_intro_ciphers> docker exec -it c
hallenge2_ctf bash
nobody@d1e67a2a418a:/$ su hacker
Password:
hacker@d1e67a2a418a:/$
```

```
hacker@d1e67a2a418a:/etc$ cd
hacker@d1e67a2a418a:~$ ls
flag_base64.txt  instrucciones.txt
hacker@d1e67a2a418a:~$ cat instrucciones.txt
Este archivo está cifrado en base64. Descifra la flag utilizando base64 -d.
hacker@d1e67a2a418a:~$ cat flag_base64.txt | base64 -d
FLAG{BASE64_DESCIFRADO}
hacker@d1e67a2a418a:~$
```

Flag: FLAG{BASE64_DESCIFRADO}

Desafío 3:

```
PS C:\Users\diego> docker exec -it challenge3_ctf bash
nobody@550996b636b4:/$ su hacker
Password:
hacker@550996b636b4:/$
```

```
hacker@550996b636b4:/$ ls -la /home
total 16
drwxr-xr-x 1 root   root   4096 Feb 13 19:44 .
drwxr-xr-x 1 root   root   4096 Feb 28 00:10 ..
drwxr-x--- 1 hacker hacker 4096 Mar  2 03:49 hacker
hacker@550996b636b4:/$ ls -la /home/hacker
total 40
drwxr-x--- 1 hacker hacker 4096 Mar  2 03:49 .
drwxr-xr-x 1 root   root   4096 Feb 13 19:44 ..
-rw------- 1 hacker hacker  547 Mar  2 03:49 .bash_history
-rw-r--r-- 1 hacker hacker  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 hacker hacker 3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 hacker hacker  807 Jan  6  2022 .profile
-r-------- 1 hacker hacker   20 Feb 13 19:44 cifrado_cesar.txt
-r-------- 1 hacker hacker   25 Feb 13 19:44 cifrado_rot13.txt
-r-------- 1 hacker hacker  138 Feb 13 19:46 instrucciones.txt
hacker@550996b636b4:/$
```

```
hacker@550996b636b4:/$ cd /home/hacker
hacker@550996b636b4:~$ cat instrucciones.txt
Utiliza Cifrado César (desplazamiento de 3) y ROT13 para descifrar los mensajes (utilizando el abecedario ingles en lowe
r y upper case).
hacker@550996b636b4:~$ ls
cifrado_cesar.txt  cifrado_rot13.txt  instrucciones.txt
hacker@550996b636b4:~$ cat cifrado_cesar.txt
IODJ{FHVDU_FLIUDGR}
hacker@550996b636b4:~$ cat cifrado_cesar.txt | tr 'D-ZA-Cd-za-c' 'A-Za-z'
FLAG{CESAR_CIFRADO}
```

Flag: FLAG{CESAR_CIFRADO}

```
hacker@550996b636b4:~$ cat cifrado_rot13.txt
FLAG{SECRET_FLAG_ROOT13}
```

Flag: FLAG{SECRET_FLAG_ROOT13}

Desafío 4:

```
PS C:\Users\diego> docker exec -it challenge4_ctf bash
nobody@1ac9f83af98f:/$ ls
bin  boot  challenge4  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
nobody@1ac9f83af98f:/$ ls -la /home
total 12
drwxr-xr-x 1 root   root   4096 Feb 13 23:24 .
drwxr-xr-x 1 root   root   4096 Feb 28 00:10 ..
drwxr-x--- 1 hacker hacker 4096 Feb 13 23:25 hacker
nobody@1ac9f83af98f:/$ su hacker
Password:
hacker@1ac9f83af98f:/$
```

```
hacker@1ac9f83af98f:/$ ls -la /home/hacker
total 28
drwxr-x--- 1 hacker hacker 4096 Feb 13 23:25 .
drwxr-xr-x 1 root   root   4096 Feb 13 23:24 ..
-rw-r--r-- 1 hacker hacker  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 hacker hacker 3771 Jan  6  2022 .bashrc
-rw-r--r-- 1 hacker hacker  807 Jan  6  2022 .profile
-r-------- 1 hacker hacker  323 Feb 13 23:24 cifrado_frecuencia.zip
-r-------- 1 hacker hacker  129 Feb 13 23:25 instrucciones.txt
hacker@1ac9f83af98f:/$ cd /hom/hacker
bash: cd: /hom/hacker: No such file or directory
hacker@1ac9f83af98f:/$ cd /home/hacker
hacker@1ac9f83af98f:~$ ls
cifrado_frecuencia.zip  instrucciones.txt
hacker@1ac9f83af98f:~$ cat instrucciones.txt
Utiliza el Análisis de Frecuencia para descifrar el archivo cifrado al parecer el usuario ha guardado en un zip con cont
raseña
hacker@1ac9f83af98f:~$
```

```
hacker@1ac9f83af98f:~$ unzip cifrado_frecuencia.zip
Archive:  cifrado_frecuencia.zip
[cifrado_frecuencia.zip] home/hacker/cifrado_frecuencia.txt password:
  inflating: home/hacker/cifrado_frecuencia.txt
hacker@1ac9f83af98f:~$ ls
cifrado_frecuencia.zip  home  instrucciones.txt
hacker@1ac9f83af98f:~$ cd home
hacker@1ac9f83af98f:~/home$
hacker@1ac9f83af98f:~/home$ ls
hacker
hacker@1ac9f83af98f:~/home$ cat hacker
cat: hacker: Is a directory
hacker@1ac9f83af98f:~/home$ cd hacker
hacker@1ac9f83af98f:~/home/hacker$ ls
cifrado_frecuencia.txt
hacker@1ac9f83af98f:~/home/hacker$ cat cifrado_frecuencia.txt
SV OHU JVUZLNBPKV, OHU LUJVUAYHKV BUH MSHN WHYH LS ZPNBPLUAL KLZHMPV MSHN{JYFWAV_HUHSFZPZ}
```

Utilizando el script de Python bruteforce_frequency.py se encontró lo siguiente:

```
PS C:\Users\diego\OneDrive\Documents\uvg\semestre 9\cifrados\repositorio> & "C:/Program Files/Python313/python.exe" "c:/Users/diego/OneDrive/Documents/uvg/semest
re 9/cifrados/repositorio/ejercicios/ctf_intro_ciphers/bruteforce_frequency.py"
Shift: 7, Métrica: 0.25566870386376866, Texto descifrado: LO HAN CONSEGUIDO, HAN ENCONTRADO UNA FLAG PARA EL SIGUIENTE DESAFIO FLAG{CRYPTO_ANALYSIS}
Shift: 20, Métrica: 0.42712055911175456, Texto descifrado: YB UNA PBAFRTHVQB, UNA RAPBAGENQB HAN SYNT CNEN RY FVTHVRAGR QRFNSVB SYNT{PELCGB_NANYLFVF}
Shift: 18, Métrica: 0.4630961914693006, Texto descifrado: AD WPC RDCHTVJXSD, WPC TCRDCIGPSD JCP UAPV EPGP TA HXVJXTCIT STHPUXD UAPV{RGNEID_PCPANHXH}
Shift: 21, Métrica: 0.46780526252999416, Texto descifrado: XA TMZ OAZEQSGUPA, TMZ QZOAZFDMPA GZM RXMS BMDM QX EUSGUQZFQ PQEMRUA RXMS{ODKBFA_MZMXKEUE}
Shift: 22, Métrica: 0.4704547644266113, Texto descifrado: WZ SLY NZYDPRFTOZ, SLY PYNZYECLOZ FYL QWLR ALCL PW DTRFTPYEP OPDLQTZ QWLR{NCJAEZ_LYLWJDTD}
Shift: 9, Métrica: 0.4752235893946278, Texto descifrado: JM FYL AMLQCESGBM, FYL CLAMLRPYBM SLY DJYE NYPY CJ QGESGCLRC BCQYDGM DJYE{APWNRM_YLYJWQGQ}
Shift: 3, Métrica: 0.48749338749143745, Texto descifrado: PS LER GSRWIKYMHS, LER IRGSRXVEHS YRE JPEK TEVE IP WMKYMIRXI HIWEJMS JPEK{GVCTXS_EREPCWMW}
Shift: 1, Métrica: 0.48812153583824663, Texto descifrado: RU NGT IUTYKMAOJU, NGT KTIUTZXGJU ATG LRGM VGXG KR YOMAOKTZK JKYGLOU LRGM{IXEVZU_GTGREYOY}
Shift: 19, Métrica: 0.4950600749693626, Texto descifrado: ZC VOB QCBGSUIWRC, VOB SBQCBHFORC IBO TZOU DOFO SZ GWUIWSBHS RSGOTWC TZOU{QFMDHC_OBOZMGWG}
Shift: 6, Métrica: 0.4992305883052905, Texto descifrado: MP IBO DPOTFHVJEP, IBO FODPOUSBEP VOB GMBH QBSB FM TJHVJFOUF EFTBGJP GMBH{DSZQUP_BOBMZTJT}
Shift: 11, Métrica: 0.5299678058760207, Texto descifrado: HK DWJ YKJOACQEZK, DWJ AJYKJPNWZK QJW BHWC LWNW AH OECQEAJPA ZAOWBEK BHWC{YNULPK_WJWHUOEO}
Shift: 14, Métrica: 0.5348627221284667, Texto descifrado: EH ATG VHGLXZNBWH, ATG XGVHGMKTWH NGT YETZ ITKT XE LBZNBXGMX WXLTYBH YETZ{VKRIMH_TGTERLBL}
Shift: 17, Métrica: 0.5419749138264827, Texto descifrado: BE XQD SEDIUWKYTE, XQD UDSEDJHQTE KDQ VBQW FQHQ UB IYWKYUDJU TUIQVYE VBQW{SHOFJE_QDQBOIYI}
Shift: 16, Métrica: 0.5444857248156094, Texto descifrado: CF YRE TFEJVXLZUF, YRE VETFEKIRUF LER WCRX GRIR VC JZXLZVEKV UVJRWZF WCRX{TIPGKF_RERCPJZJ}
Shift: 4, Métrica: 0.5478335285126323, Texto descifrado: OR KDQ FRQVHJXLGR, KDQ HQFRQWUDGR XQD IODJ SDUD HO VLJXLHQWH GHVDILR IODJ{FUBSWR_DQDOBVLV}
Shift: 0, Métrica: 0.5524107689344603, Texto descifrado: SV OHU JVUZLNBPKV, OHU LUJVUAYHKV BUH MSHN WHYH LS ZPNBPLUAL KLZHMPV MSHN{JYFWAV_HUHSFZPZ}
Shift: 2, Métrica: 0.5760694178188763, Texto descifrado: QT MFS HTSXJLZNIT, MFS JSHTSYWFIT ZSF KQFL UFWF JQ XNLZNJSYJ IJXFKNT KQFL{HWDUYT_FSFQDXNX}
Shift: 15, Métrica: 0.5814363456910706, Texto descifrado: DG ZSF UGFKWYMAVG, ZSF WFUGFLJSVG MFS XDSY HSJS WD KAYMAWFLW VWKSXAG XDSY{UJQHLG_SFSDQKAK}
PS C:\Users\diego\OneDrive\Documents\uvg\semestre 9\cifrados\repositorio>
```

Flag: FLAG{CRYPTO_ANALYSIS}