Greenhorn writeup - Hack The Box

Escrito por : tellmefred

Dificultad : fácil

Introducción:

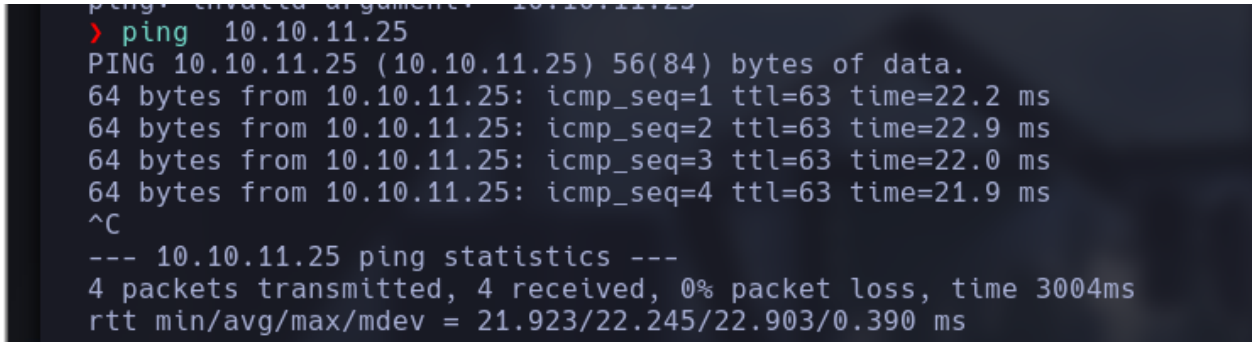
En este writeup, exploraremos "Greenhorn", una máquina de Hack The Box que ofrece una experiencia orientada a aprender y aplicar técnicas específicas de reconocimiento y explotación.

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,

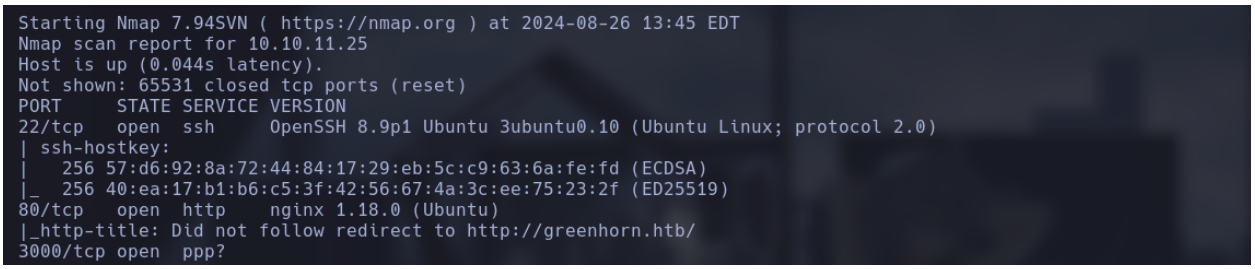
procederemos a la explotación de fallos de seguridad que nos permitirán acceder al sistema y obtener privilegios adicionales.

Reconocimiento:

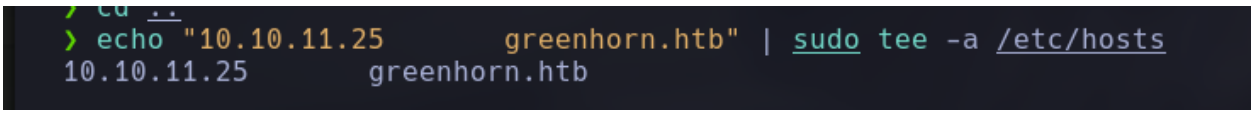
Aquí empezamos con un Ping para confirmar la conectividad con la máquina.



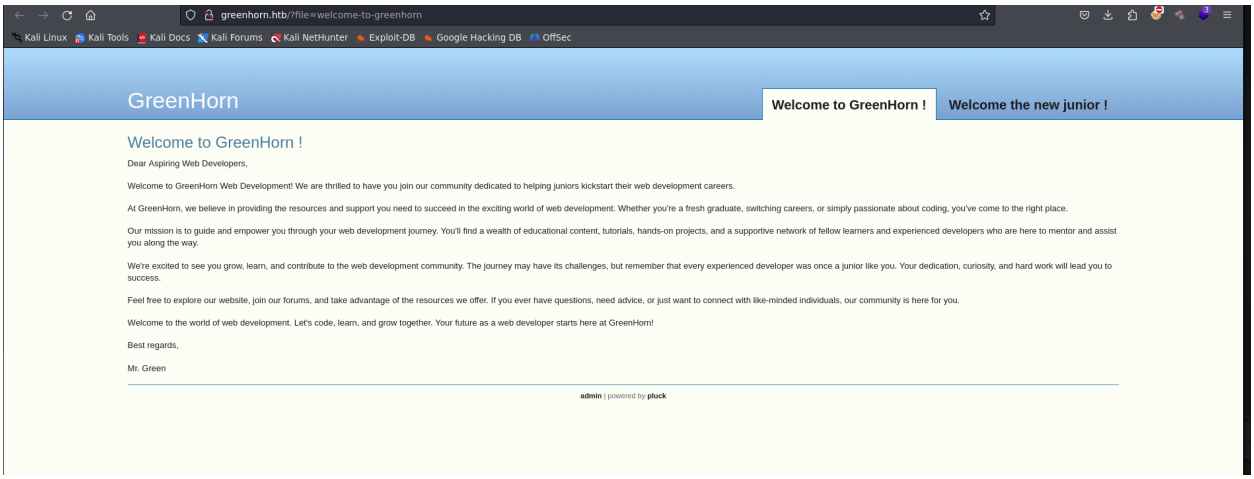
Aquí el resultado de el escaneo de nmap que verificando bien tiene una redireccion en el puerto 80 a http://greenhorn.htb/.



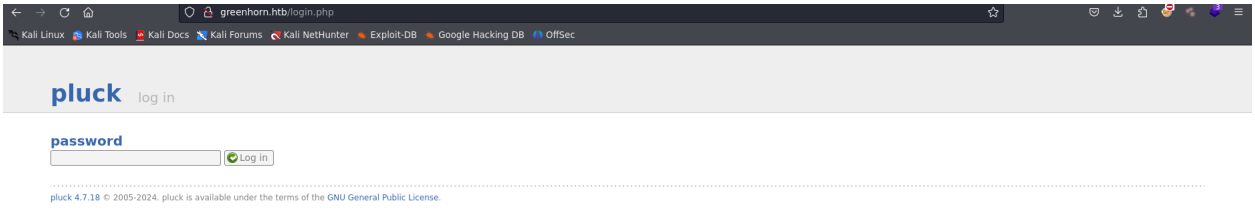
Así que agregamos a nuestro archivo /etc/hosts.



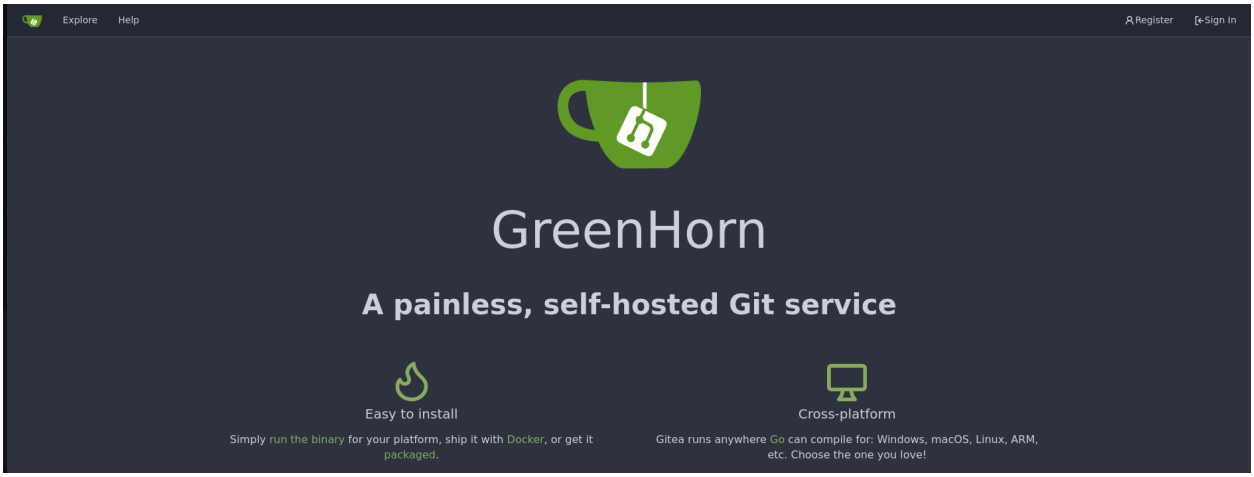
Y ya podemos acceder a la página web. Si se fijan abajo tenemos la parte de admin.



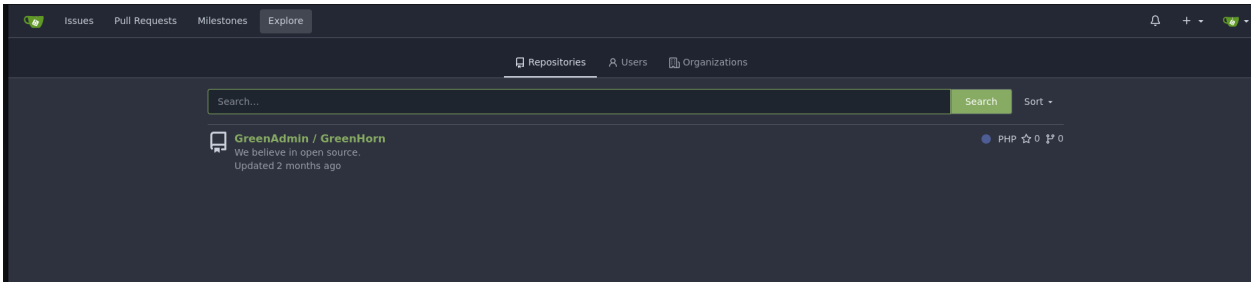
Y nos encontramos con un pluck 4.7.18 así que investigue y hay una forma de acceder al servidor con una vulnerabilidad, pero es requerido la contraseña.



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.

Explotación:

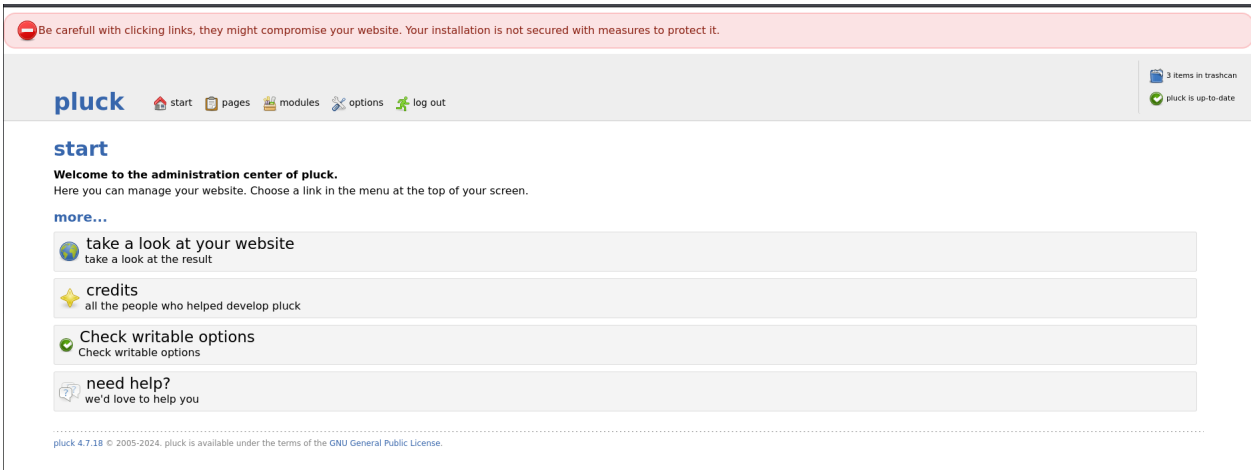
Aquí en el código vemos el tipo de encriptado que tiene la contraseña.

```
//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);
```

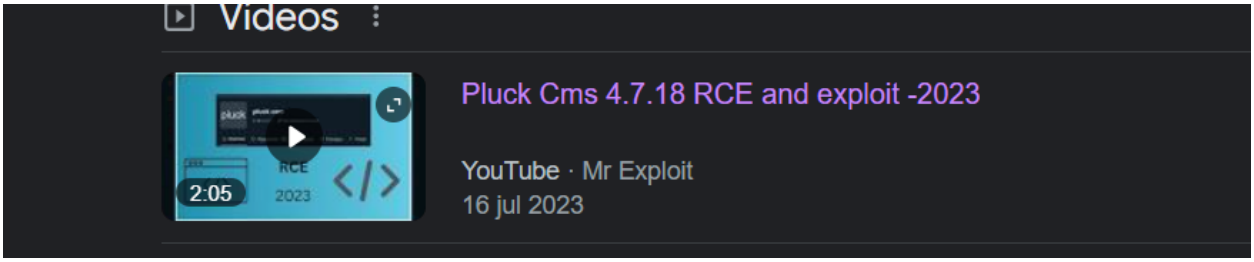
Hacemos el decrypt con este comando y obtenemos la contraseña iloveyou1.

```
❯ 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        (?)
```

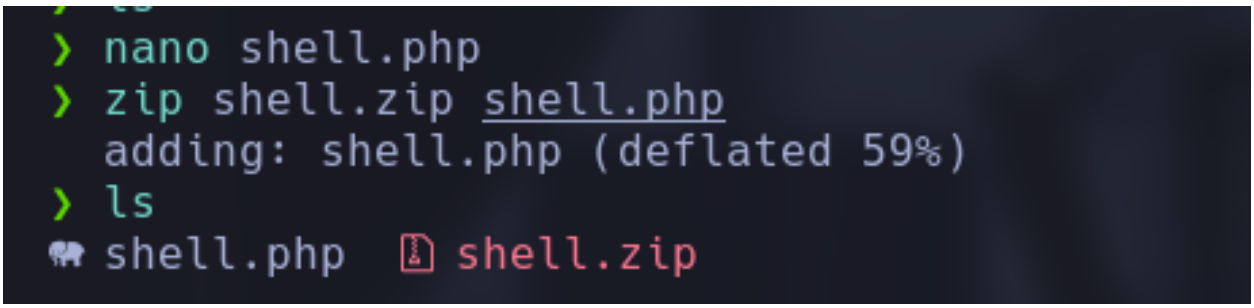
Luego ya entramos a la interfaz.



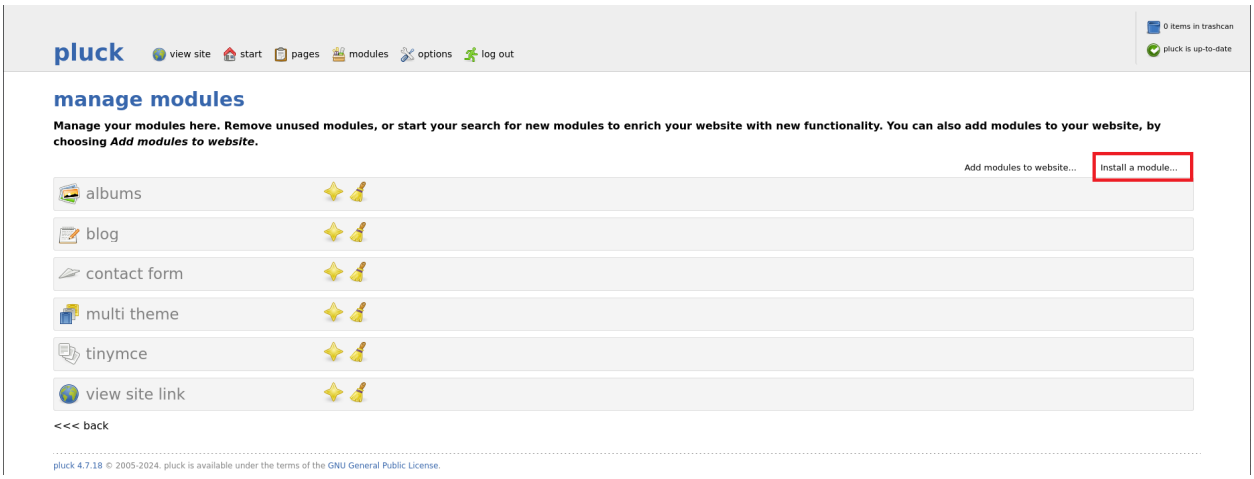
Y pues pude encontrar este video para explotar esta versión.



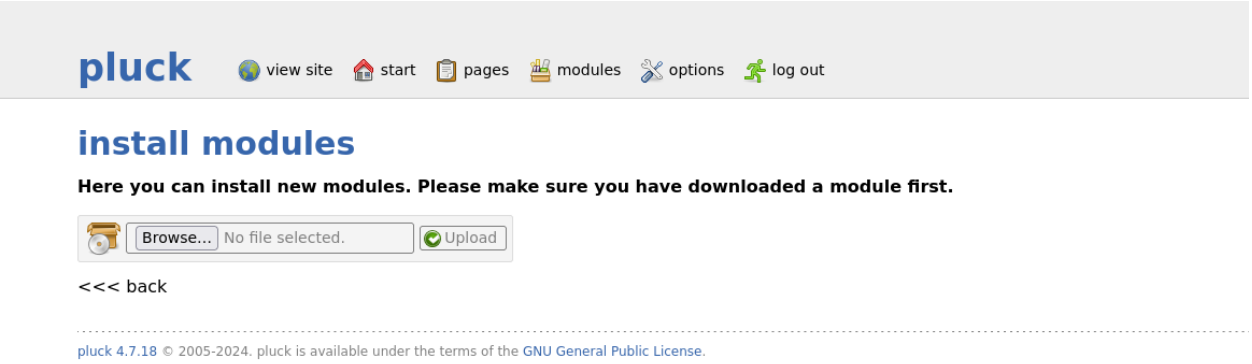
Creo una shell.php y la comprimo en un .zip.



Buscamos install a module.

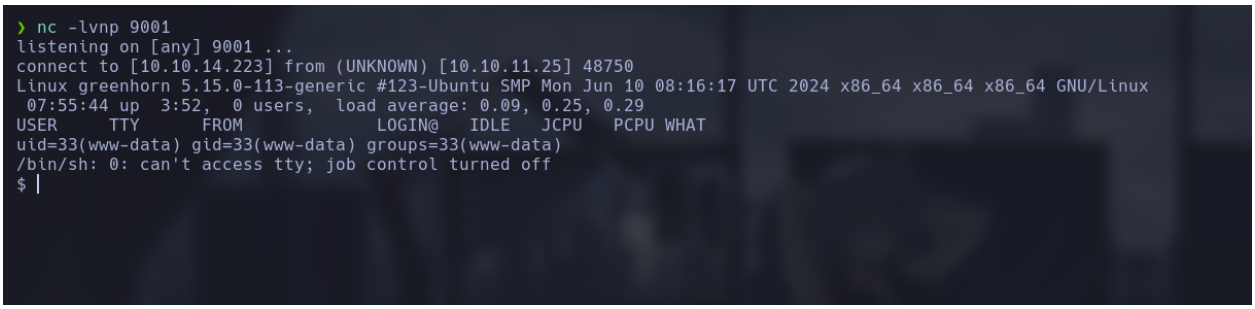


Y aquí subimos el archivo. Antes de subir el archivo ponte en escucha y obtendrás la shell.

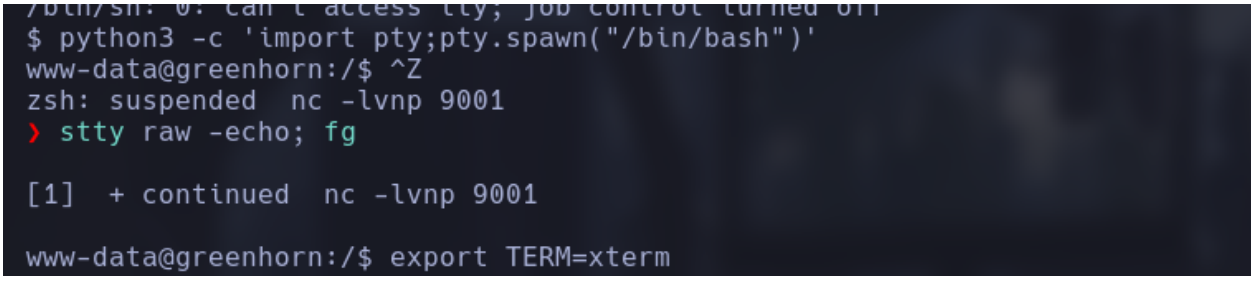


Escalada de privilegios:

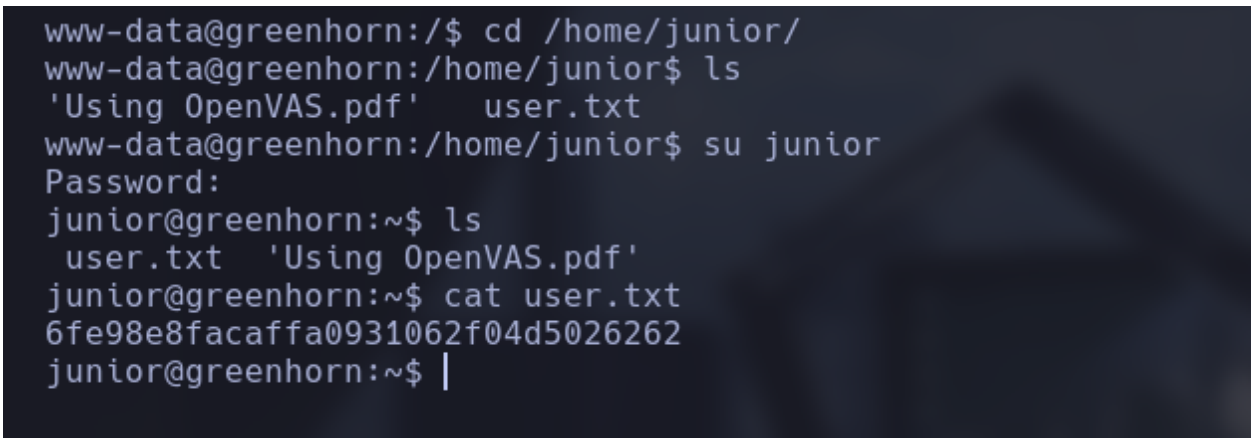
Aquí ya con la shell interactiva.



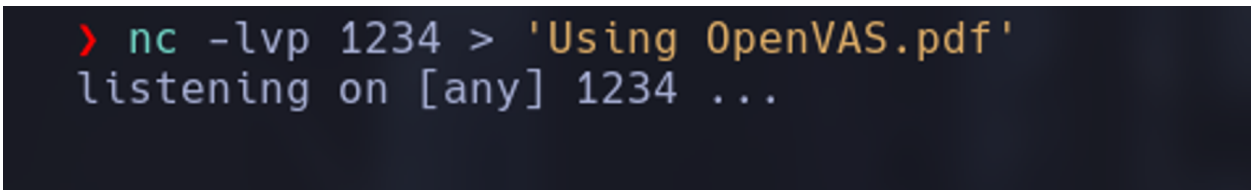
Paso a darle un tratamiento a la tty.



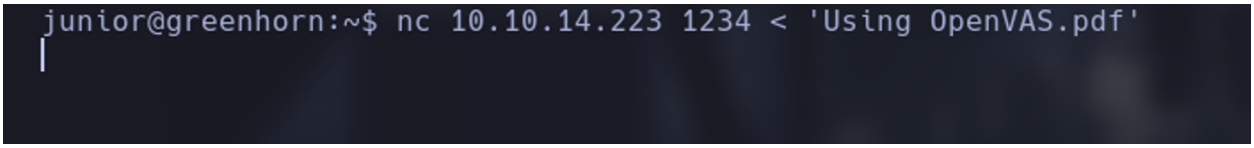
Luego lo primero fue verificar y reutilizar la contraseña para el usuario junior y perfecto accedemos a la user.txt.



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



Mi pc atacante.



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: [redacted]

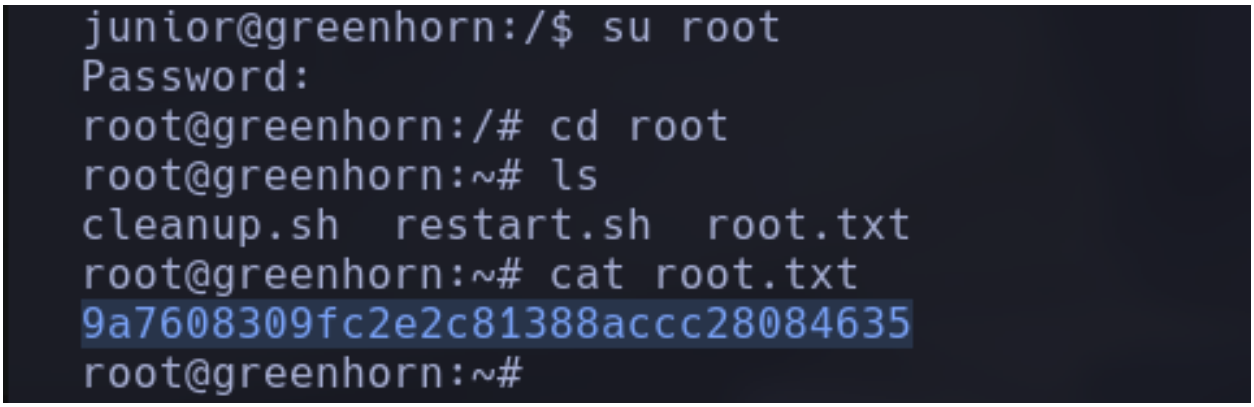
As part of your familiarization with this tool, we encourage you to learn how to use OpenVAS effectively. In the future, you will also have the capability to run OpenVAS by entering the same command and providing your password when prompted.

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:~#