Vulnerability Assessment and Exploitation Write-Up

Machine: Stapler: 1 – VulnHub

Prepared by: Melisa Sarıtaş

Table of Contents

1. Introduction

Misconfigurations occur when a service or system is set up incorrectly, leading to unintended behavior or security weaknesses.[1] In the context of FTP (File Transfer Protocol) servers[2], one common misconfiguration is enabling anonymous access without proper restrictions. Anonymous FTP allows users to connect without authentication, often intended for public file sharing. However, if not properly managed, it can expose sensitive files or user information to unauthorized users.

In this machine, anonymous FTP access is misconfigured, allowing users to log in without authentication. This insecure setup exposes files that would normally require proper credentials. Accessing these files through the misconfigured FTP server is the first step in the process, allowing for further enumeration and exploitation within the target system.

The machine used to solve the target machine[3] is Kali Linux[4] as it includes most of the necessary tools. To solve the machine, download the zip file from the source[3], extract it and import the machine into VirtualBox[5].

2. Solution Overview

The solution consists of four steps: reconnaissance, information gathering, brute force, and privilege escalation. Each of these steps will be explained in detail in the following sections.

2.1. Reconnaissance

Scan the network to find the target ip using Command 1.

```
netdiscover
```

Command 1

Scan the target with using Command 2. Notice that port 21 is open, which is the default port for ftp service.

```
nmap <target-ip>
```

Command 2

2.2. Information Gathering

Try connecting the ftp service using Command 3. It can be seen from the output that there is potentially a user named Harry. Note the user.

```
ftp <target-ip>
```

Command 3

Enter *anonymous* as user and enter blank password when prompted. Check and get the files that the user has access using Command 4. Press *y* when required.

```
ls
mget note
```

Command 4

Exit from ftp service and check the inside of the retrieved file using Command 5.

```
exit
cat note
```

Command 5

It can be seen from the output of Command 5 that there are potentially users named Elly and John. Note the users.

2.3. Brute Force

Put the noted users inside of a file using Command 6.

```
vim <users-file>
```

Command 6

Use Command 7 to find the passwords of the gathered users for ftp service. The command checks whether the passwords are null, same with the username or the reverse of the username.

```
hydra -L users -e nsr ftp://<target-ip>
```

Command 7

The output of Command 7 gives that the password for the user *Elly* is the reverse of the username, which is *ylle*. Use Command 3 to connect to ftp service and enter the user with its credentials when prompted. There are lots of folders and files for this user. Get the *passwd* file, which contains a copy of the */etc/passwd* file, with Command 8.

```
mget passwd
```

Command 8

Append the users that access bash terminal upon login to the *<users-file>* using Command 9.

```
awk -F':' '/\/bin\/bash/{print $1}' passwd > <users-file>
```

Command 9

Use Command 10 to find the passwords of the gathered users for ssh service.

```
hydra -L users -e nsr ssh://<target-ip>
```

Command 10

The output of Command 10 gives that the password for the user *SHayslett* is the same with the username. Use Command 11 to connect to the ssh service and enter the password when prompted.

```
ssh <username>@<target-ip>
```

Command 11

At the current directory, home directory, there is a file named *.bash_history*. Get the contents of the file for each user using Command 12, and take note of any usernames and passwords found in the output.

```
cat /home/*/.bash_history
```

Command 12

2.4. Privilege Escalation

Attempt to connect to the SSH service using the newly found users with Command 11, and gain root access using Command 13.

```
sudo su
```

Command 13

Get the flag using Command 14.

```
ls -l
cat flag.txt
```

Command 14

3. References

[1] https://csrc.nist.gov/glossary/term/misconfiguration
[2] https://en.wikipedia.org/wiki/FTP_server
[3] https://www.vulnhub.com/entry/stapler-1,150/
[4] https://www.kali.org/
[5] https://www.virtualbox.org/