Report on Metasploitable

Submitted by:

Uttam Kumar Rajbanshi

Submitted to:

Director of SBComputer

Date:2022/12/27

Time: 5:58 PM

1. Contents

[1 Introduction 3](#_Toc123229537)

[1. Scanning with Nmap 5](#_Toc123229538)

[1.1 Screenshot 5](#_Toc123229539)

[1.2 Port number 21 6](#_Toc123229540)

[1.3 Googling ftp service version vulnerability 6](#_Toc123229541)

[1.4 Exploitation 7](#_Toc123229542)

[1.4.1 Running Metasploit framework 7](#_Toc123229543)

[1.4.2 Attacking target 8](#_Toc123229544)

[1.5 Port number 22 9](#_Toc123229545)

[1.6 Port number 23 12](#_Toc123229546)

[1.6.1 Screenshot 12](#_Toc123229547)

[1.6.2 Bruteforcing using hydra 13](#_Toc123229548)

# Introduction

Metasploitable 2 is a vulnerable machine which serves as a server to host several vulnerable website where a person practice his/her hacking knowledge. Metasploitable 2 is a open source machine were people can download and use it for their practice.

It is a test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

# Scanning with Nmap

## Screenshot

Text

Description automatically generated

We can see that there are so many open ports in this server. Now serially we can check the version of the services running in the port there and search for exploit in the google.

## Port number 21

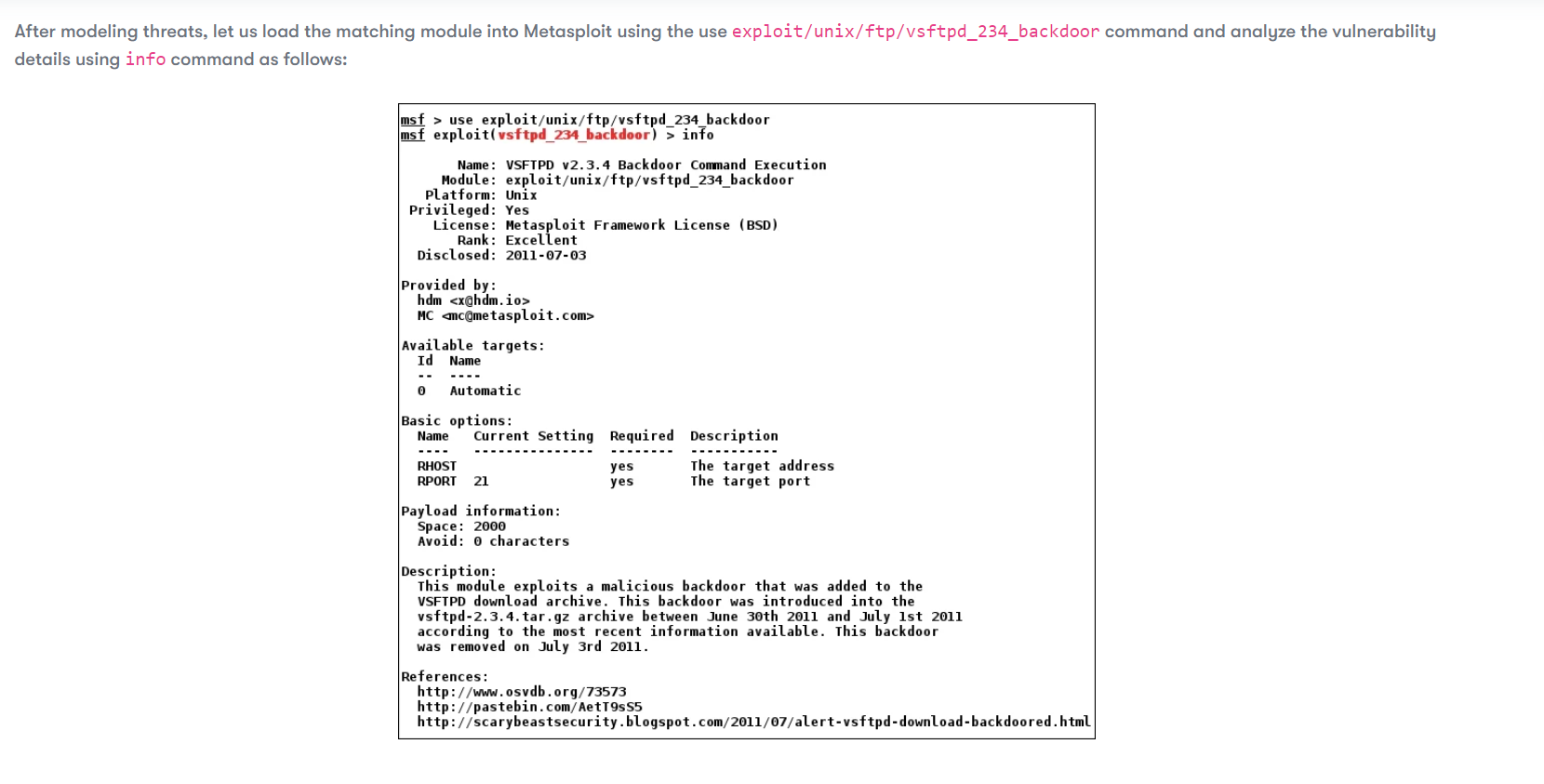
We can see port number 21 is open. We can see ftp service running in port number 21. Version of the running ftp service is vsftpd 2.3.4.

## Googling ftp service version vulnerability

Graphical user interface, text, application

Description automatically generated

I took help of google to search for the vulnerability of running version. Google gave so many result, can be looked at for exploitation.



In the above result, we can know that there is backdoor present were attacker can remotely access the server.

## Exploitation

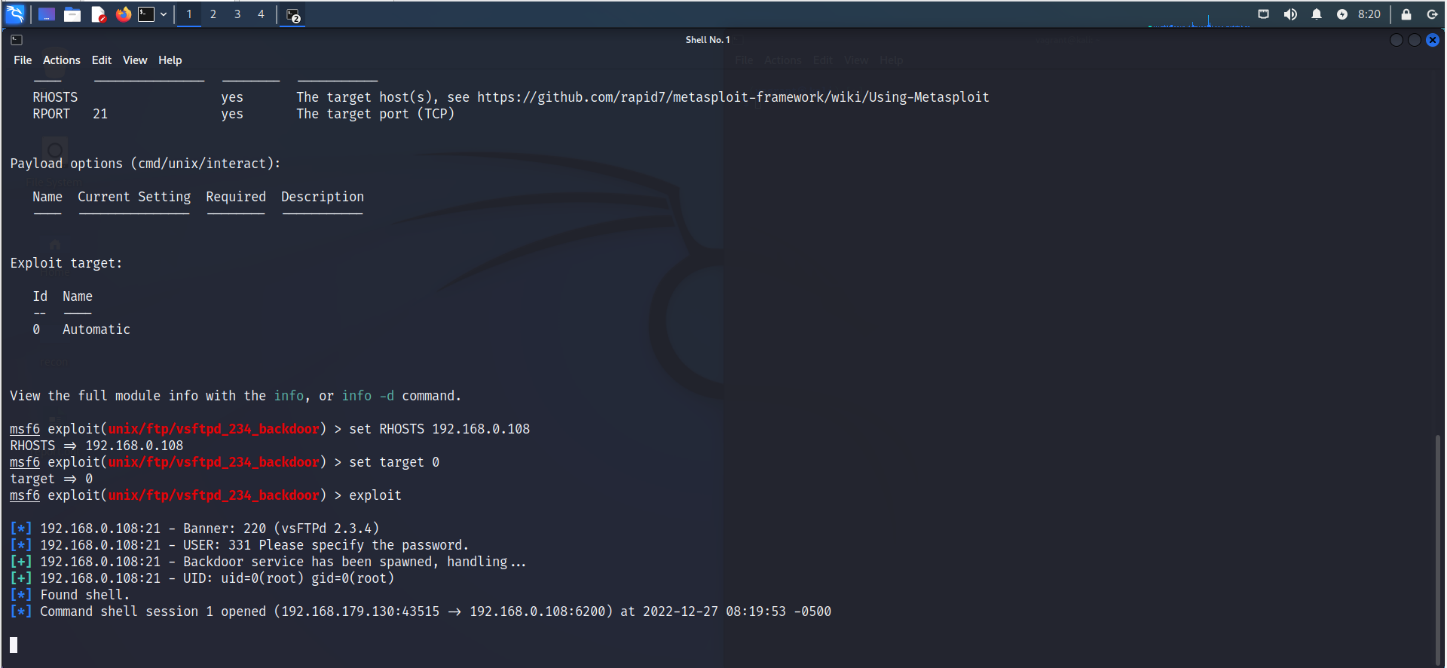
### Running Metasploit framework

Graphical user interface, text

Description automatically generated

Opening Metasploit framework in kali linux where we can search for exploitation is available or not. We can see Metasploit v6.2.26-dev is running in kali linux terminal.

### Attacking target



We set RHOSTS and target on the Metasploit framework and run the command we got the service spawned. We can see FOUND SHELL in the above pictures. After that we need to give SHELL command and use “pwd” for root access.

A screenshot of a computer

Description automatically generated with medium confidence

In the above picture we can see that we got root access in the metasploitable server on port number 21.

## Port number 22

We know that on port number 22, ssh service is running with version “openssh 4.7pi debian 8ubuntu1 (protocol 2.0) vulnerability”. After that, I searched for vulnerabilities on the google and I found following result as result. Result is shown on the screenshot

Graphical user interface, text, application, email

Description automatically generated

We knew that ssh is enabled on the ip address. So, I tried “ssh msfadmin@192.168.0.114” on the terminal and it gave me result like this:

Graphical user interface, application

Description automatically generated

As highlighted on the image, it asked me for password and I used hydra for bruteforcing the password. It is shown in the below images:

Graphical user interface, text

Description automatically generated

In hydra, it gave results as shown in the above highlighted area. We can see that login and password guessed by the hydra.

Text

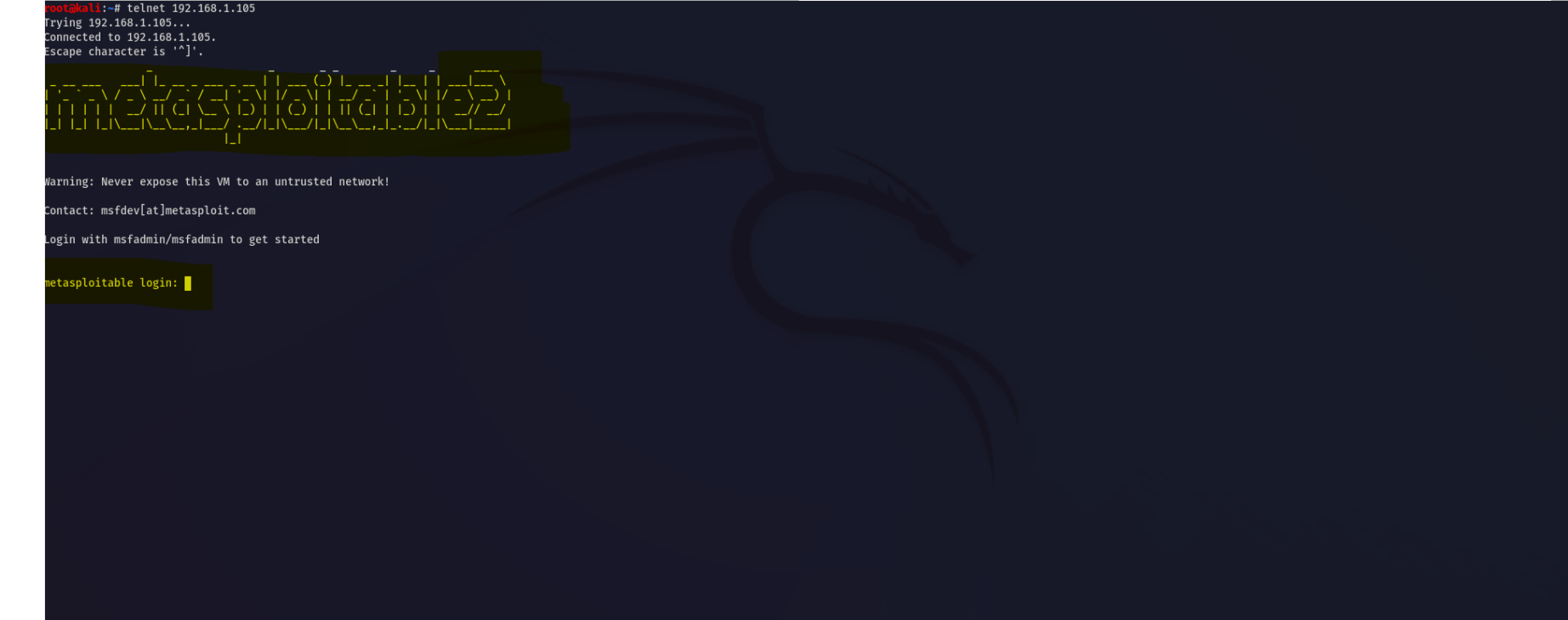
Description automatically generated

Using the above credentials, I was able to get access the server. And we can also see that directory named vulnerable is listed.

## Port number 23

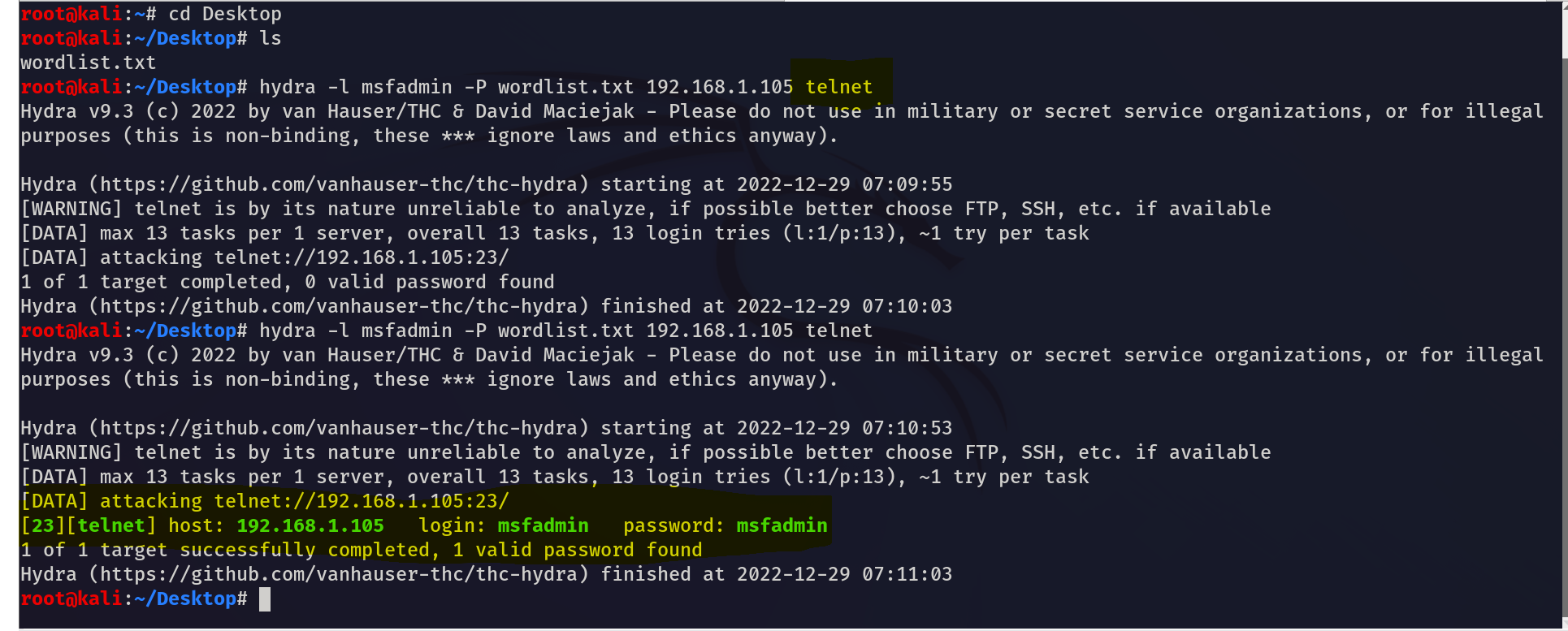
On port number 23, telnet services are running named Linux telnetd.

### Screenshot



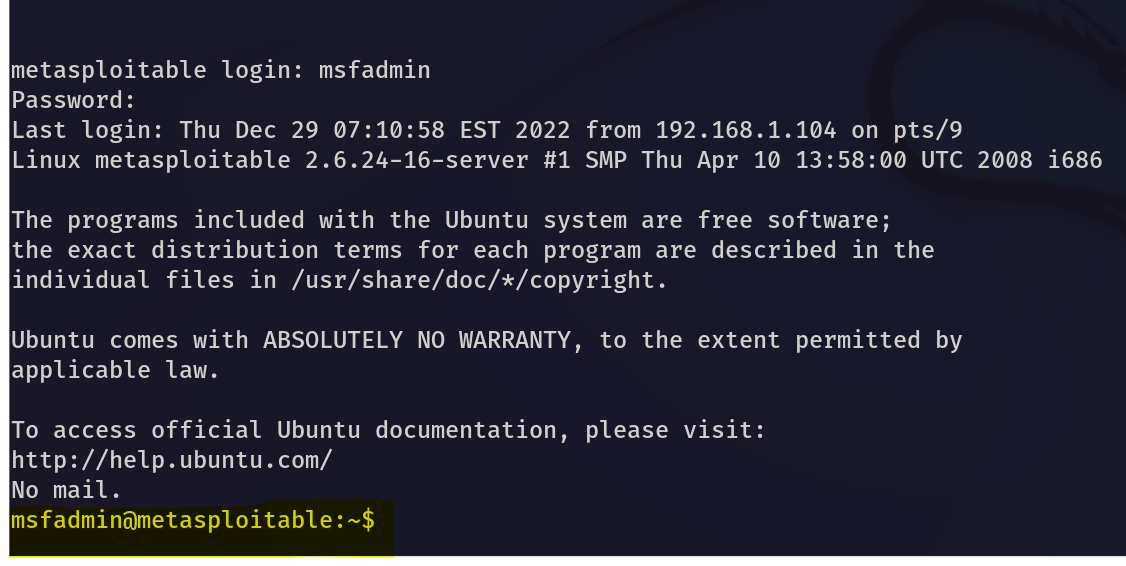
We can see that, we used “telnet ipaddress” and we can access the machine in the teminal. And we can know the password and username of the machine by bruteforcing using hydra as shown in the below image.

### Bruteforcing using hydra

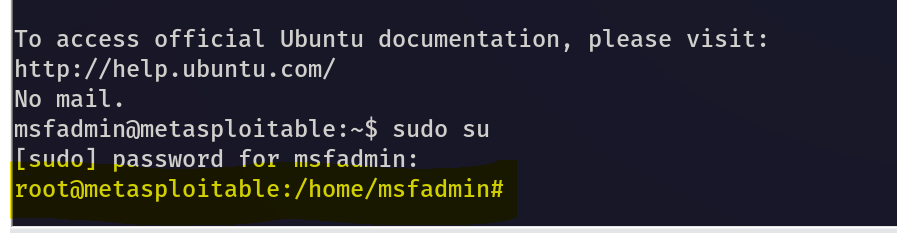


We can see that hydra got login and password from the wordlist. I have highlighted on the above occuring result.

### Got Access to Machine



By using the above credentials, I was able to login on the machine. Because I was able to login in the machine, I was also able to get root access using the same credentials as we can see in the below picture.



## Port number 25

### Introduction

In port number 25 smtp service is running with version postfix smtpd.