Walkthrough – Metasploitable 2

Contents

[Host Discovery 1](#_Toc148618319)

[Nmap 2](#_Toc148618320)

[Getting In 3](#_Toc148618321)

[Method 1 3](#_Toc148618322)

# Host Discovery

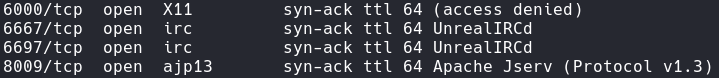


# Nmap

A screenshot of a computer program

Description automatically generated



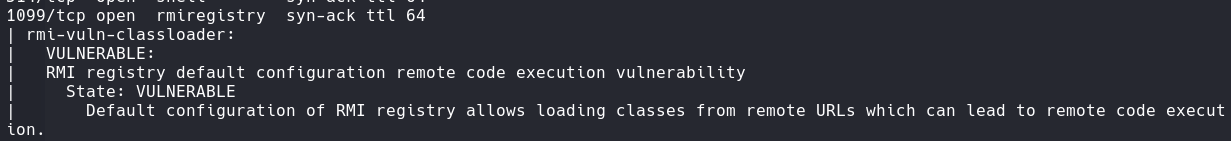
A screen shot of a computer

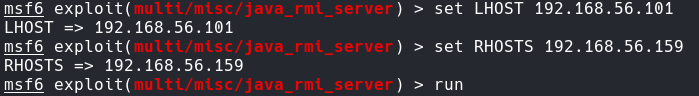
Description automatically generated

# Getting In

## Method 1

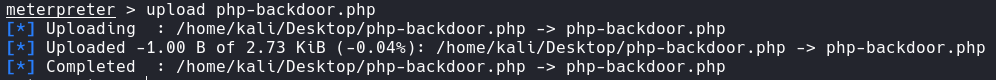
**Summary**: this method is exploiting port 1099 the rmiregistry. The process involves using nmap to discover the vulnerability, using msfconsole to create a session and exploit. The final step is setting up a php backdoor to ensure persistence.



**MsfConsole**

**Backdoor**

A screenshot of a computer

Description automatically generatedI uploaded a backdoor using a php backdoor, located in /usr/share/webshells/php/php-backdoor.php

A black background with white text

Description automatically generatedNow create a reverse shell.

## Method 2

Overview: This process of getting into the system is going onto searchsploit and finding a vulnerability associated with vsftpd 2.3.4. Then running the script to get shell access.





Now, run the shell.

Now you have root.

## Method 3

**Summary**: This process involves using netcat to connect to port 1524 (bindshell) without a password.

A close up of white text

Description automatically generated

## Method 4

Summary: This process uses the NFS service to mount to the attacker machine, then move our ssh give onto the victim share. This will allow me to ssh into the machine using my credentials.

A screenshot of a computer

Description automatically generated

The show mount command looks like it allows the root directory to be mounted. This means I can transfer my ssh key here and get root access.

I created a file in /tmp called MOUNTED.

I was able to access the NFT share, however I couldn’t get passed transfering the keys over. It didn’t work.

A computer screen shot of a computer code

Description automatically generated