Intermediate Nmap

TryHackMe CTF Walkthrough: Intermediate Nmap

Introduction

In this walkthrough, we will explore how to leverage Nmap alongside netcat and other protocols to gain access to a vulnerable machine and locate the flag. The challenge involves scanning a target machine with Nmap, analyzing the results, utilizing the provided information to log in, and ultimately discovering the flag.

Prerequisites

- Access to the TryHackMe platform.
- Familiarity with basic Linux command-line usage.
- Understanding of Nmap scanning and netcat utilities.

Challenge Description

You've honed your `nmap` skills, and now it's time to integrate them with `netcat` and other protocols. Your goal is to connect to a target machine, which is listening on a high port. By connecting to this port, you may receive information that can help you establish a connection to a lower port commonly used for remote access.

Walkthrough

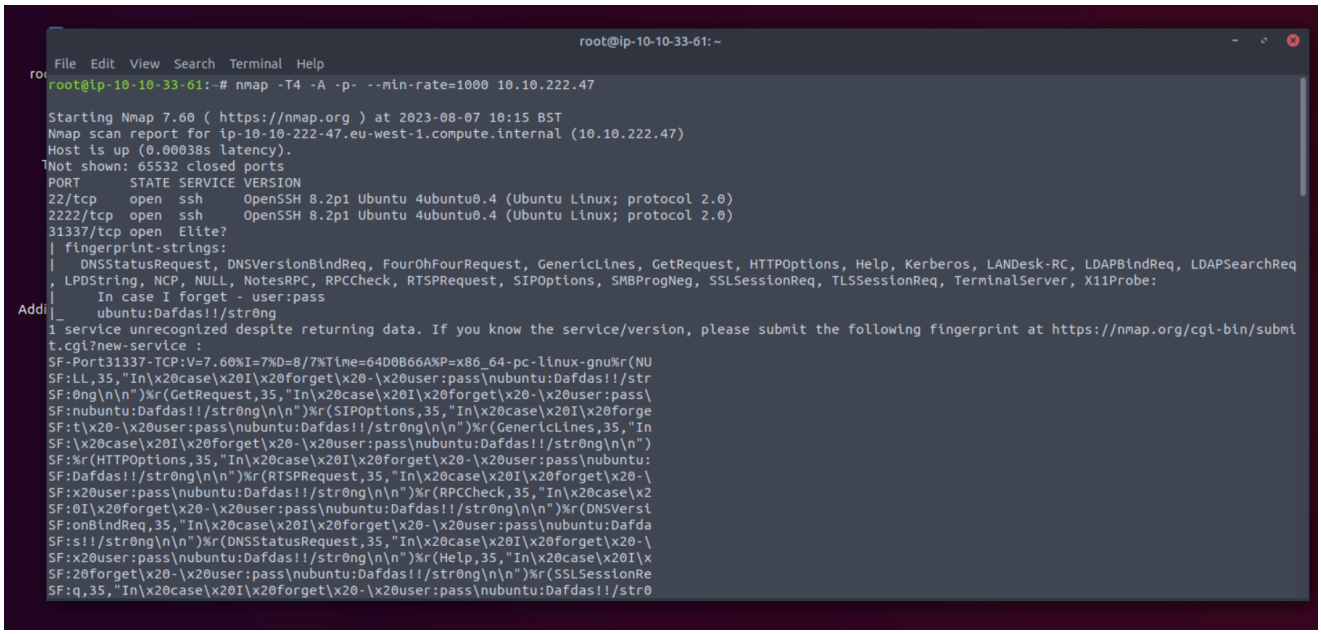
Step 1: Nmap Scanning

To start, let's perform a thorough Nmap scan on the target machine to identify open ports and services. Run the following command:

```
nmap -T4 -A -p- --min-rate=1000 MACHINE_IP
```

This command performs a comprehensive scan with aggressive timing and service detection. It scans all ports using a minimum rate of 1000 packets per second. Replace `MACHINE_IP` with the actual IP address of the target machine.

The output



Step 2: Analyzing Nmap Results

After the scan completes, carefully examine the scan results. You should notice a line that contains the following information:

```
|     In case I forget - user:pass
|_    ubuntu:Dafdas!!/str0ng
```

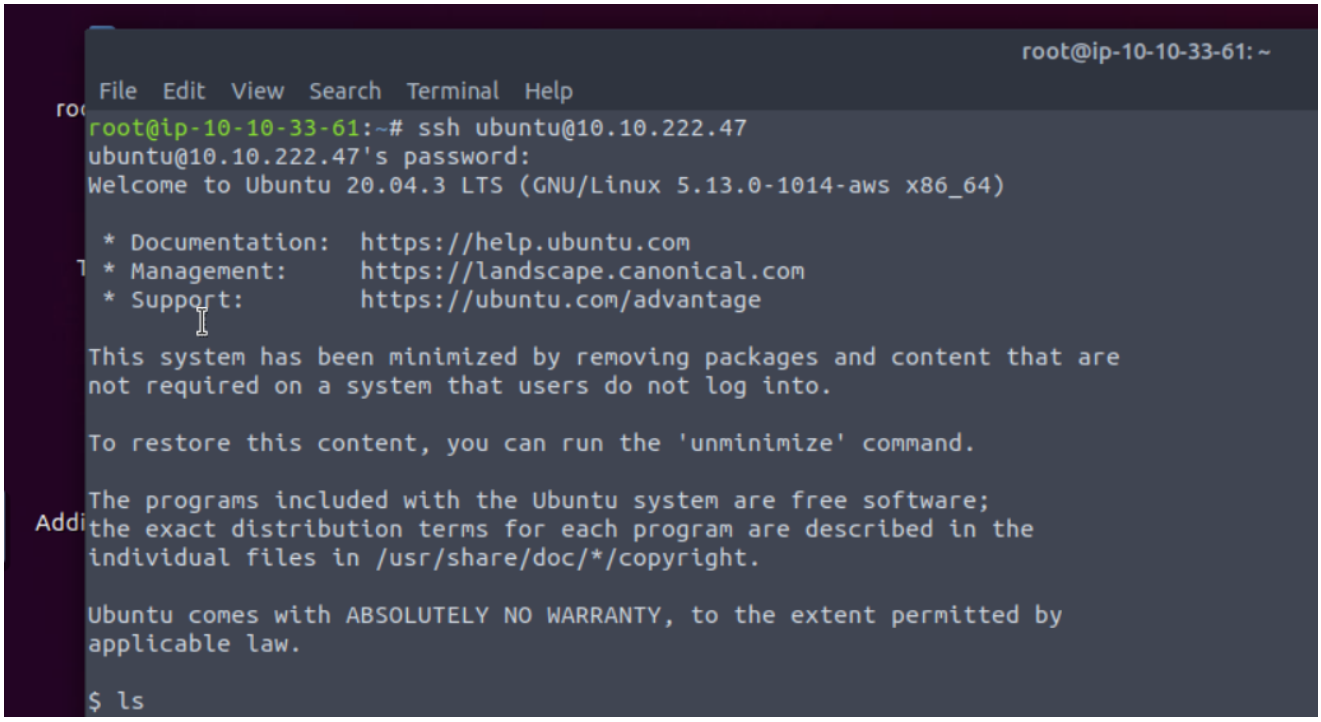
This line provides valuable credentials that can be used for authentication.

Step 3: Establishing SSH Connection

Now that we have the username and password, let's use them to establish an SSH connection to the target machine. Use the following command:

```
ssh ubuntu@MACHINE_IP
```

When prompted for a password, enter: `Dafdas!!/str0ng`.



Step 4: Exploring the Filesystem

Once logged in, explore the filesystem to locate the flag. Use the following commands:

```
ls
pwd
cd Desktop
ls -l
cd ..
ls
cd user
ls
cat flag.txt
```

You should find the flag in the `flag.txt` file within the `/home/user` directory.

Conclusion

Congratulations! You've successfully completed the Intermediate Nmap challenge on TryHackMe. By combining Nmap scanning with netcat and SSH protocols, you were able to discover the required credentials, establish a secure connection, and locate the flag. This walkthrough demonstrates how effective scanning and protocol analysis can be in uncovering vulnerabilities and accessing hidden information.

Remember to practice responsible hacking and ethical behavior when participating in CTF challenges. Happy hacking!

For further resources and learning opportunities, check out the Nmap Module on TryHackMe.