

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

```
root@ip-10-10-33-61:~# nmap -T4 -A -p- --min-rate=1000 10.10.222.47

Starting Nmap 7.60 ( https://nmap.org ) at 2023-08-07 10:15 BST
Nmap scan report for ip-10-10-222-47.eu-west-1.compute.internal (10.10.222.47)
Host is up (0.00038s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
2222/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
31337/tcp open  Elite?
| fingerprint-strings:
|   DNSStatusRequest, DNSVersionBindReq, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq,
|   LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServer, X11Probe:
|_  In case I forget - user:pass
Add:  ubuntu:Dafdas!!/str0ng
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
SF-Port31337-TCP:V=7.60I=7%D=8/7%Time=64D0B66A%P=x86_64-pc-linux-gnu%r(NU
SF:LL,35,"In\x20case\x20I\x20forget\x20-\x20user:pass\nubuntu:Dafdas!!/str
SF:0ng\n\n")%r(GetRequest,35,"In\x20case\x20I\x20forget\x20-\x20user:pass\n
SF:nubuntu:Dafdas!!/str0ng\n\n")%r(SIPOptions,35,"In\x20case\x20I\x20forge
SF:t\x20-\x20user:pass\nubuntu:Dafdas!!/str0ng\n\n")%r(GenericLines,35,"In
SF:\x20case\x20I\x20forget\x20-\x20user:pass\nubuntu:Dafdas!!/str0ng\n\n")
SF:%r(HTTPOptions,35,"In\x20case\x20I\x20forget\x20-\x20user:pass\nubuntu:
SF:Dafdas!!/str0ng\n\n")%r(RTSPRequest,35,"In\x20case\x20I\x20forget\x20-\
SF:x20user:pass\nubuntu:Dafdas!!/str0ng\n\n")%r(RPCCheck,35,"In\x20case\x2
SF:0I\x20forget\x20-\x20user:pass\nubuntu:Dafdas!!/str0ng\n\n")%r(DNSVersi
SF:onBindReq,35,"In\x20case\x20I\x20forget\x20-\x20user:pass\nubuntu:Dafda
SF:s!!/str0ng\n\n")%r(DNSStatusRequest,35,"In\x20case\x20I\x20forget\x20-\
SF:x20user:pass\nubuntu:Dafdas!!/str0ng\n\n")%r(Help,35,"In\x20case\x20I\x
SF:20forget\x20-\x20user:pass\nubuntu:Dafdas!!/str0ng\n\n")%r(SSLSessionRe
SF:q,35,"In\x20case\x20I\x20forget\x20-\x20user:pass\nubuntu:Dafdas!!/stro
```

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.

```
root@ip-10-10-33-61: ~
File Edit View Search Terminal Help
root@ip-10-10-33-61:~# ssh ubuntu@10.10.222.47
ubuntu@10.10.222.47's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.13.0-1014-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ ls
```

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](#).