

Keamanan Sistem Dan Jaringan Komputer

NAMA :

1. Fajar Sapto Mukti Raharjo (2231740018)



**D3
TEKNOLOGI INFORMASI
POLITEKNIK NEGERI MALANG
PSDKU LUMAJANG
JALAN LINTAS TIMUR, LUMAJANG**

1. Pengenalan Hydra sebagai alat untuk brute force

The screenshot shows the 'Hydra Introduction' page in the TryHackMe web interface. The page title is 'Task 1 - Hydra Introduction'. The main heading is 'What is Hydra?'. The text explains that Hydra is a brute force online password cracking program. It lists various protocols supported by Hydra, including Asterisk, AFP, Cisco AAA, Cisco auth, CVS, Firebird, FTP, HTTP, HTTP-GET, HTTP-FORM-POST, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, 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. It also mentions that Hydra can be installed on Kali Linux or Ubuntu/Fedora. The page includes a 'Start AttackBox' button and a 'Start Kali Linux' button. The bottom of the page shows a Windows taskbar with various application icons and the system clock.

Room progress (0%)

Task 1 - Hydra Introduction

What is Hydra?

Hydra is a brute force online password cracking program, a quick system login password "hacking" tool.

Hydra can run through a list and "brute force" some authentication services. Imagine trying to manually guess someone's password on a particular service (SSH, Web Application Form, FTP or SNMP) - we can use Hydra to run through a password list and speed this process up for us, determining the correct password.

According to its [official repository](#), Hydra supports, i.e., has the ability to brute force the following protocols: "Asterisk, AFP, Cisco AAA, Cisco auth, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, HTTP-Proxy, ICQ, IMAP, 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](#).

76° Search 07:03 22/04/2025

2. Munculkan Virtual Machine untuk diserang

The screenshot shows the 'Using Hydra' page in the TryHackMe web interface. The page title is 'Task 2 - Using Hydra'. The main heading is 'Hydra Commands'. The text explains that the options we pass into Hydra depend on which service (protocol) we're attacking. It provides an example command for brute forcing FTP with the username 'user' and a password list 'passlist.txt'. It also mentions that for this deployed machine, there are commands to use Hydra on SSH and a web form (POST method). The page includes a 'Start Machine' button. The bottom of the page shows a Windows taskbar with various application icons and the system clock.

Room progress (33%)

Task 2 - Using Hydra

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://10.10.204.208> 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://10.10.204.208
```

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

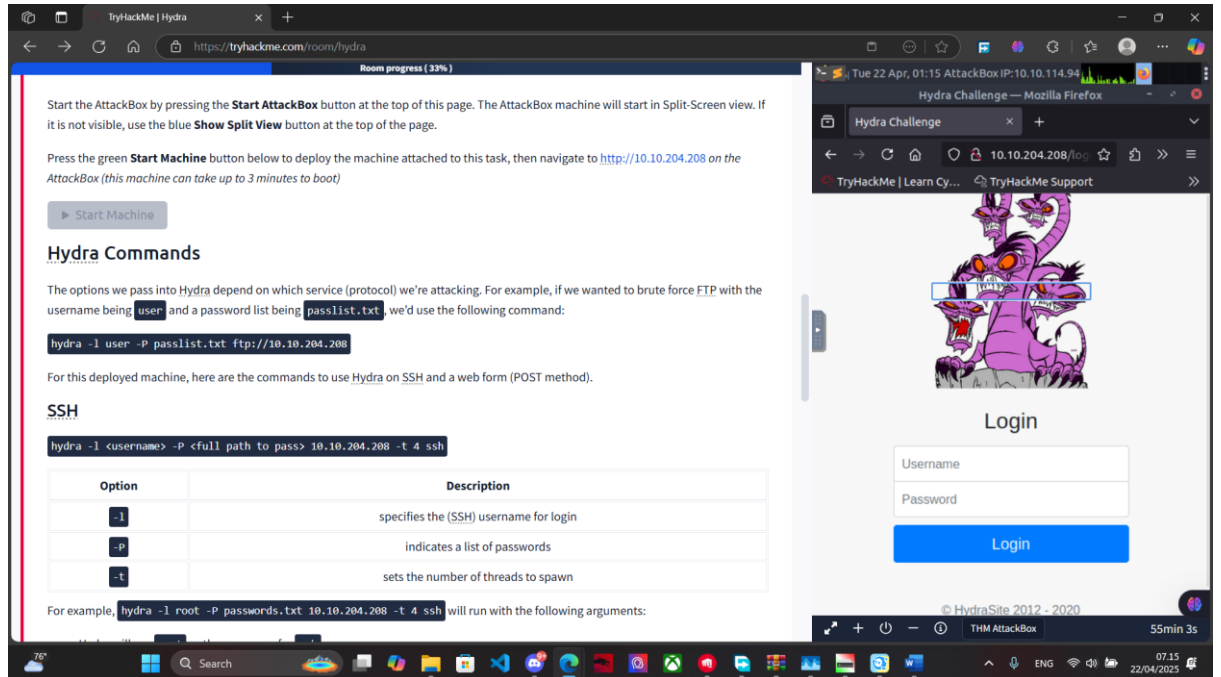
SSH

```
hydra -l <username> -P <full path to pass> 10.10.204.208 -t 4 ssh
```

Option	Description
<code>-l</code>	specifies the (SSH) username for login
<code>-P</code>	indicates a list of passwords
<code>-t</code>	sets the number of threads to spawn

76° Search 07:06 22/04/2025

3. Buka Ip machine dengan Virtual Machine di browser



The screenshot shows the TryHackMe Hydra room page on the left and a virtual machine login screen on the right. The TryHackMe page includes instructions on how to start the machine and lists Hydra commands for different protocols. The virtual machine screen shows a login form with fields for Username and Password, and a Login button.

Room progress (33%)

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://10.10.204.208> 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://10.10.204.208
```

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> 10.10.204.208 -t 4 ssh
```

Option	Description
<code>-l</code>	specifies the (SSH) username for login
<code>-P</code>	indicates a list of passwords
<code>-t</code>	sets the number of threads to spawn

For example, `hydra -l root -P passwords.txt 10.10.204.208 -t 4 ssh` will run with the following arguments:

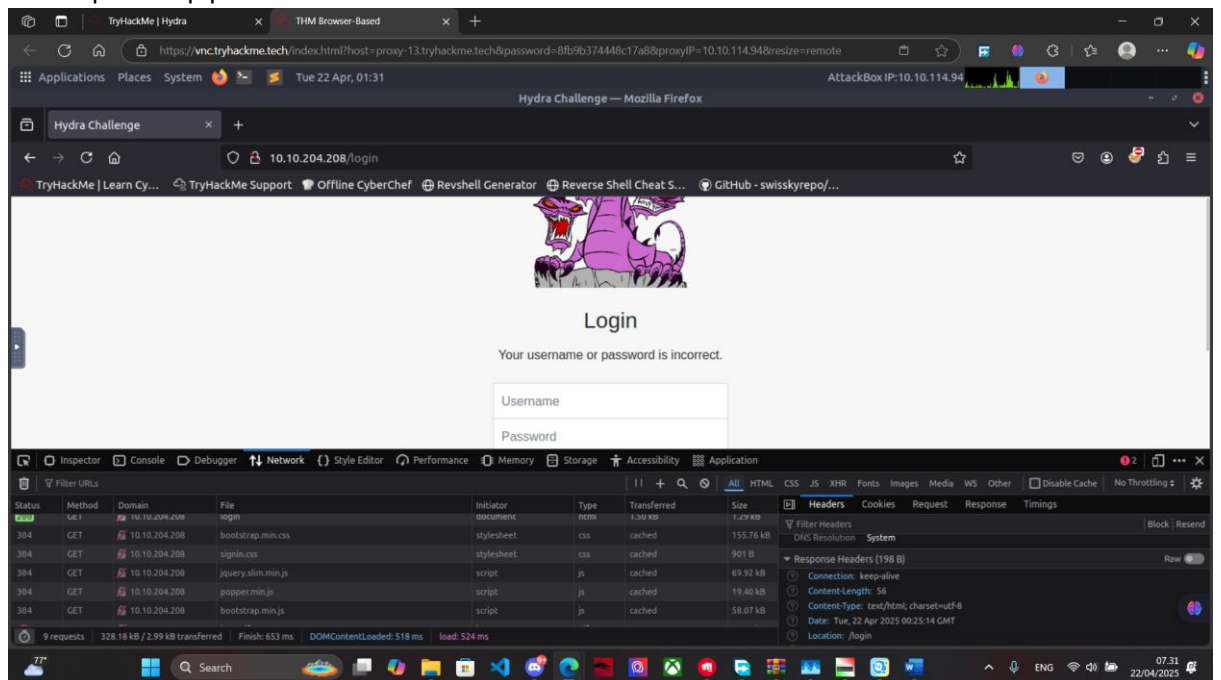
Hydra Challenge — Mozilla Firefox

AttackBox IP: 10.10.114.94

HydraSite 2012 - 2020

THM AttackBox 55min 3s

4. Lalu buka inspect element ke network dan isikan random username password untuk mendapatkan ip post



The screenshot shows the Hydra Challenge login page in a browser. The Network tab is open in the developer tools, showing a list of requests. The first request is a GET request to the login page, which has a status of 200. The second request is a POST request to the login page, which has a status of 400. The third request is a GET request to the login page, which has a status of 200. The fourth request is a POST request to the login page, which has a status of 400. The fifth request is a GET request to the login page, which has a status of 200. The sixth request is a POST request to the login page, which has a status of 400. The seventh request is a GET request to the login page, which has a status of 200. The eighth request is a POST request to the login page, which has a status of 400. The ninth request is a GET request to the login page, which has a status of 200. The tenth request is a POST request to the login page, which has a status of 400. The eleventh request is a GET request to the login page, which has a status of 200. The twelfth request is a POST request to the login page, which has a status of 400. The thirteenth request is a GET request to the login page, which has a status of 200. The fourteenth request is a POST request to the login page, which has a status of 400. The fifteenth request is a GET request to the login page, which has a status of 200. The sixteenth request is a POST request to the login page, which has a status of 400. The seventeenth request is a GET request to the login page, which has a status of 200. The eighteenth request is a POST request to the login page, which has a status of 400. The nineteenth request is a GET request to the login page, which has a status of 200. The twentieth request is a POST request to the login page, which has a status of 400. The twenty-first request is a GET request to the login page, which has a status of 200. The twenty-second request is a POST request to the login page, which has a status of 400. The twenty-third request is a GET request to the login page, which has a status of 200. The twenty-fourth request is a POST request to the login page, which has a status of 400. The twenty-fifth request is a GET request to the login page, which has a status of 200. The twenty-sixth request is a POST request to the login page, which has a status of 400. The twenty-seventh request is a GET request to the login page, which has a status of 200. The twenty-eighth request is a POST request to the login page, which has a status of 400. The twenty-ninth request is a GET request to the login page, which has a status of 200. The thirtieth request is a POST request to the login page, which has a status of 400. The thirty-first request is a GET request to the login page, which has a status of 200. The thirty-second request is a POST request to the login page, which has a status of 400. The thirty-third request is a GET request to the login page, which has a status of 200. The thirty-fourth request is a POST request to the login page, which has a status of 400. The thirty-fifth request is a GET request to the login page, which has a status of 200. The thirty-sixth request is a POST request to the login page, which has a status of 400. The thirty-seventh request is a GET request to the login page, which has a status of 200. The thirty-eighth request is a POST request to the login page, which has a status of 400. The thirty-ninth request is a GET request to the login page, which has a status of 200. The fortieth request is a POST request to the login page, which has a status of 400. The forty-first request is a GET request to the login page, which has a status of 200. The forty-second request is a POST request to the login page, which has a status of 400. The forty-third request is a GET request to the login page, which has a status of 200. The forty-fourth request is a POST request to the login page, which has a status of 400. The forty-fifth request is a GET request to the login page, which has a status of 200. The forty-sixth request is a POST request to the login page, which has a status of 400. The forty-seventh request is a GET request to the login page, which has a status of 200. The forty-eighth request is a POST request to the login page, which has a status of 400. The forty-ninth request is a GET request to the login page, which has a status of 200. The fiftieth request is a POST request to the login page, which has a status of 400. The fifty-first request is a GET request to the login page, which has a status of 200. The fifty-second request is a POST request to the login page, which has a status of 400. The fifty-third request is a GET request to the login page, which has a status of 200. The fifty-fourth request is a POST request to the login page, which has a status of 400. The fifty-fifth request is a GET request to the login page, which has a status of 200. The fifty-sixth request is a POST request to the login page, which has a status of 400. The fifty-seventh request is a GET request to the login page, which has a status of 200. The fifty-eighth request is a POST request to the login page, which has a status of 400. The fifty-ninth request is a GET request to the login page, which has a status of 200. The sixtieth request is a POST request to the login page, which has a status of 400. The sixty-first request is a GET request to the login page, which has a status of 200. The sixty-second request is a POST request to the login page, which has a status of 400. The sixty-third request is a GET request to the login page, which has a status of 200. The sixty-fourth request is a POST request to the login page, which has a status of 400. The sixty-fifth request is a GET request to the login page, which has a status of 200. The sixty-sixth request is a POST request to the login page, which has a status of 400. The sixty-seventh request is a GET request to the login page, which has a status of 200. The sixty-eighth request is a POST request to the login page, which has a status of 400. The sixty-ninth request is a GET request to the login page, which has a status of 200. The seventieth request is a POST request to the login page, which has a status of 400. The seventy-first request is a GET request to the login page, which has a status of 200. The seventy-second request is a POST request to the login page, which has a status of 400. The seventy-third request is a GET request to the login page, which has a status of 200. The seventy-fourth request is a POST request to the login page, which has a status of 400. The seventy-fifth request is a GET request to the login page, which has a status of 200. The seventy-sixth request is a POST request to the login page, which has a status of 400. The seventy-seventh request is a GET request to the login page, which has a status of 200. The seventy-eighth request is a POST request to the login page, which has a status of 400. The seventy-ninth request is a GET request to the login page, which has a status of 200. The eightieth request is a POST request to the login page, which has a status of 400. The eighty-first request is a GET request to the login page, which has a status of 200. The eighty-second request is a POST request to the login page, which has a status of 400. The eighty-third request is a GET request to the login page, which has a status of 200. The eighty-fourth request is a POST request to the login page, which has a status of 400. The eighty-fifth request is a GET request to the login page, which has a status of 200. The eighty-sixth request is a POST request to the login page, which has a status of 400. The eighty-seventh request is a GET request to the login page, which has a status of 200. The eighty-eighth request is a POST request to the login page, which has a status of 400. The eighty-ninth request is a GET request to the login page, which has a status of 200. The ninetieth request is a POST request to the login page, which has a status of 400. The ninety-first request is a GET request to the login page, which has a status of 200. The ninety-second request is a POST request to the login page, which has a status of 400. The ninety-third request is a GET request to the login page, which has a status of 200. The ninety-fourth request is a POST request to the login page, which has a status of 400. The ninety-fifth request is a GET request to the login page, which has a status of 200. The ninety-sixth request is a POST request to the login page, which has a status of 400. The ninety-seventh request is a GET request to the login page, which has a status of 200. The ninety-eighth request is a POST request to the login page, which has a status of 400. The ninety-ninth request is a GET request to the login page, which has a status of 200. The hundredth request is a POST request to the login page, which has a status of 400.

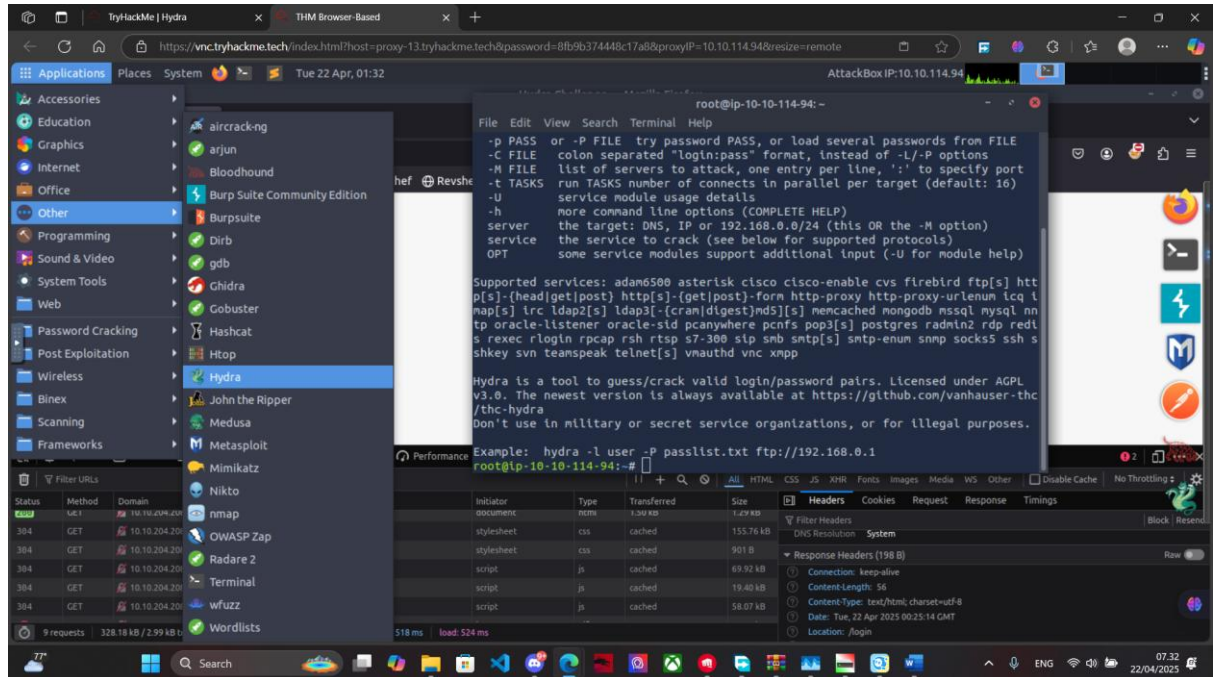
Hydra Challenge — Mozilla Firefox

AttackBox IP: 10.10.114.94

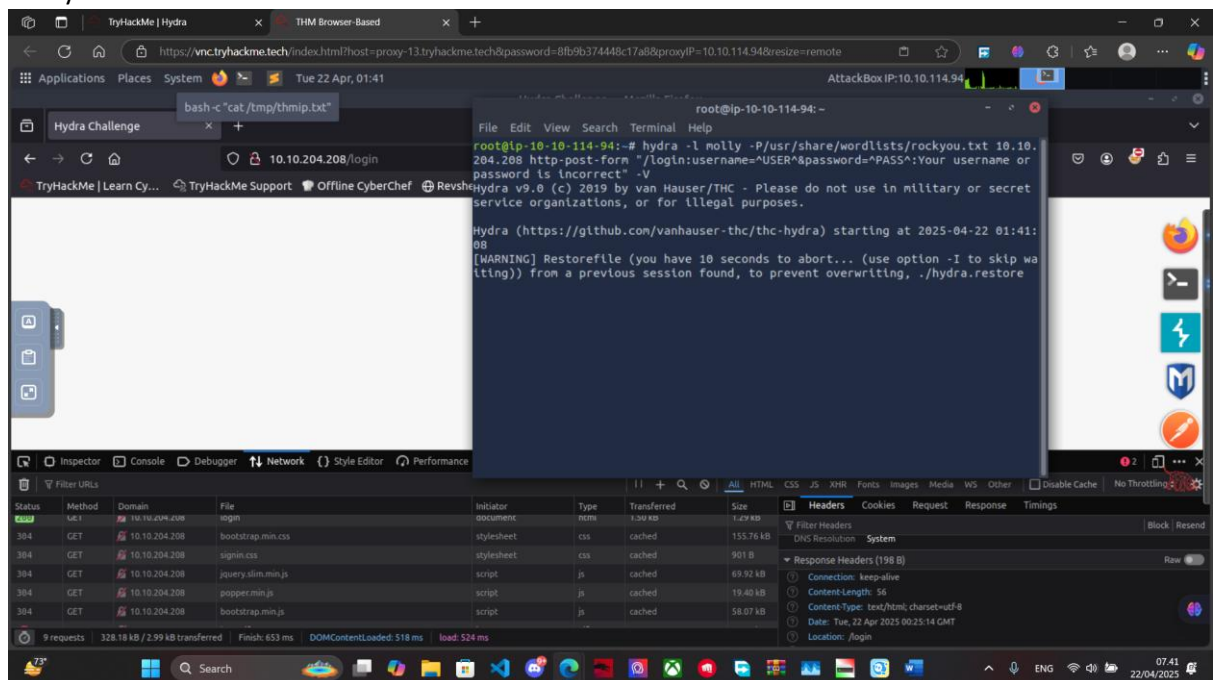
HydraSite 2012 - 2020

THM AttackBox 55min 3s

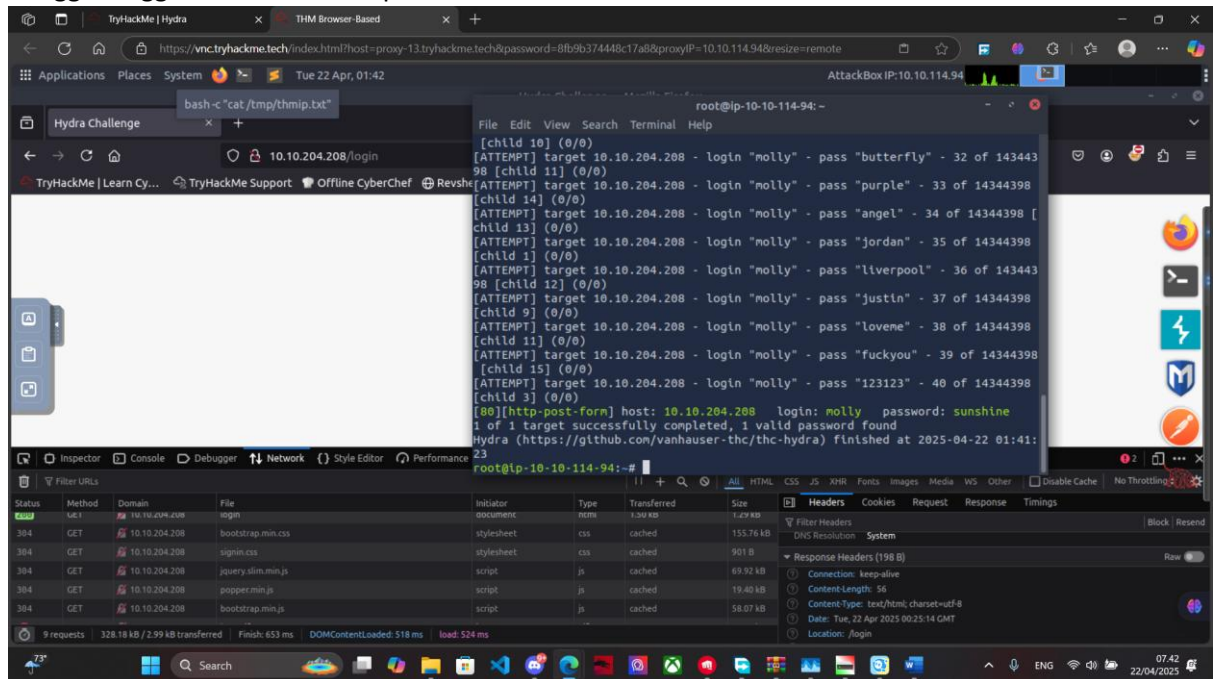
5. Lalu buka terminal hydra dengan mengikuti gambar ini



6. Lalu ketik "hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.204.208 http-post-form \"/login:username=^USER^&password=^PASS^:Your username or password is incorrect" -V"
Molly username contoh



7. Tunggu hingga selesai keluar seperti ini



8. Lalu login dengan hasil paling bawah ke website yang bisa diakses di virtual machine dan hasilnya akan seperti ini

