LAPORAN

UTS – TryHackMe Hydra Official Walkthrough

Disusun untuk memenuhi tugas mata kuliah keamanan sistem dan jaringan komputer

Nama : Zaqiatus Sholihah

Kelas : 3B

NIM : 2231740044

TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

PSDKU LUMAJANG

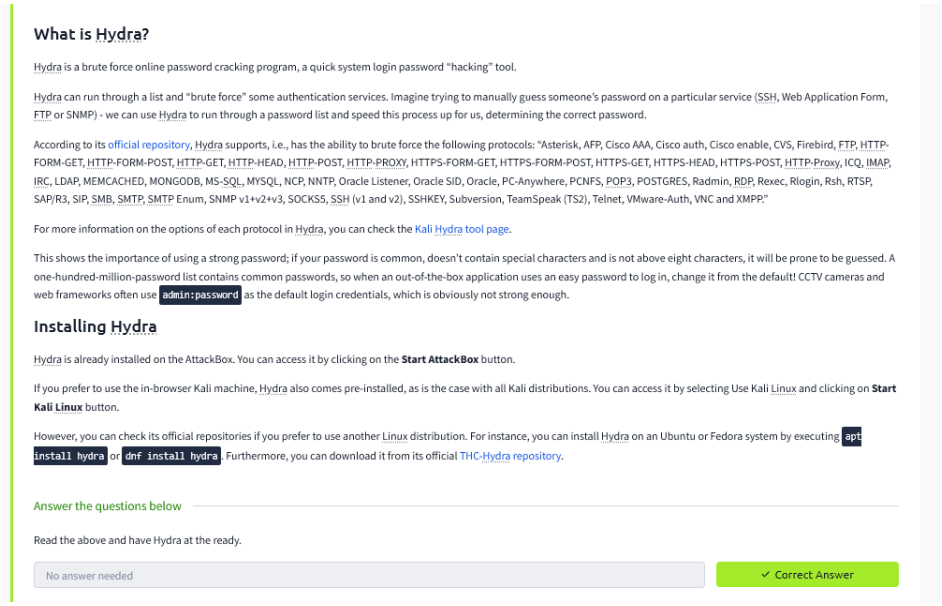
2025

Task 1. Hydra Introduction

What is hydra?

Hydra adalah program peretasan kata sandi online dengan brute force, alat peretasan kata sandi login sistem yang cepat. Pentingnya menggunakan kata sandi yang kuat, jika kata sandi umum tidak mengandung karakter khusus dan atau tidak lebih dari delapan karakter, itu akan rentan ditebak. 10 juta kata sandi atau 100 juta daftar kata sandi ada yang berisi kata sandi umum jadi, ketika aplikasi out of the box menggunakan kata sandi yang mudah untuk log on pastikan untuk mengubahnya dari default.

Setelah membaca task 1 klik “completed” sebagai tanda selesai dan lanjut ke task 2.



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, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, 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.

Answer the questions below

Read the above and have Hydra at the ready.

No answer needed

✓ Correct Answer

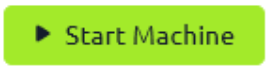
Task 2. Using Hydra

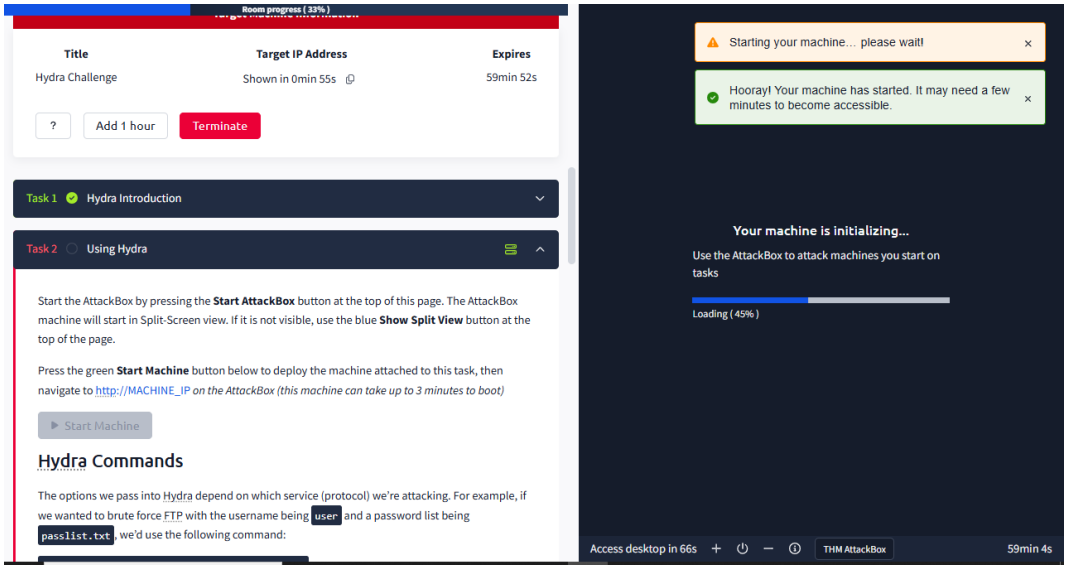
Task 2 menggunakan hydra untuk memainkan mesin dalam kasus ini yaitu alamat IP yang dibuat secara dinamis.

Perintah dibawah ini adalah struktur dasar dari seperti apa penggunaan hydra

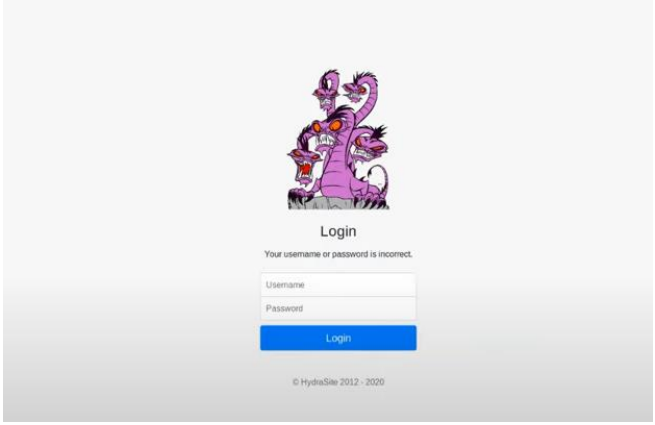
```
hydra -l user -P passlist.txt ftp://MACHINE_IP
```

Selanjutnya kita masuk ke terminal. Klik tombol hijau “start machine” dan akan muncul tampilan seperti dibawah ini.

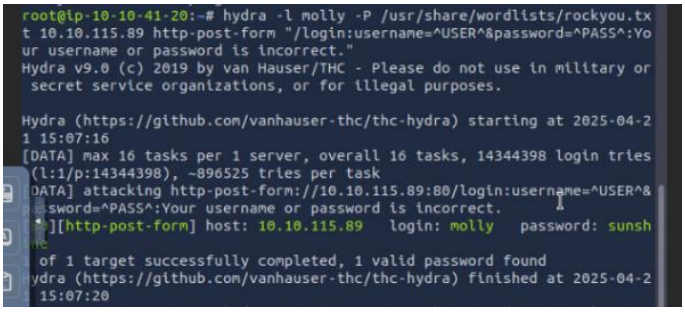




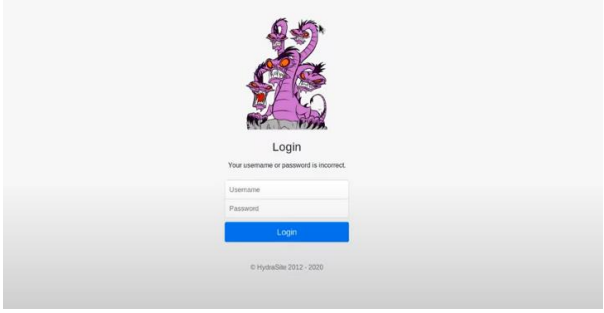
Kemudian kita masuk ke situs website sederhana seperti dibawah ini



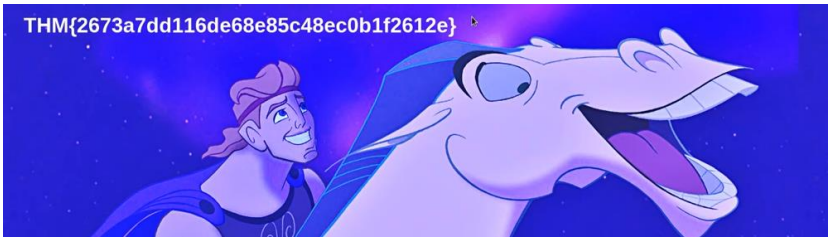
Selanjutnya ketik perintah `hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.115.89 http-post-form "/login:username=^USER^&password=^PASS^:Your username or password is incorrect."` dibawah ini pada terminal dan jalankan. Kemudian dapat dilihat kita memiliki username: molly dan password: sunshine



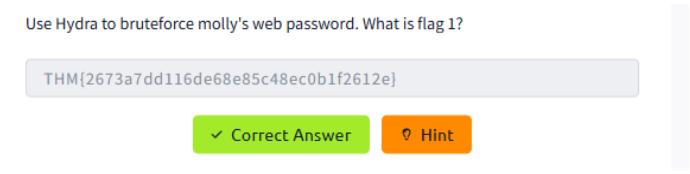
Ketik username dan password diatas pada website dibawah ini



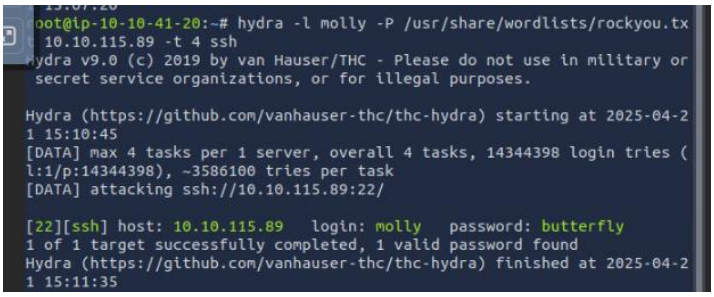
Dan klik login kemudian muncul halaman dibawah ini



Dan dapat ditemukan flag 1 nya yaitu



Selanjutnya kita beralih ke terminal untuk mencoba flag ssh, ketik perintah `hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.115.89 -t 4 ssh`



Dapat ditemukan flag 2 nya yaitu, kemudian klik “submit” dan selesai.