

**El material utilizado y el conocimiento  
presentado es solo para FINE\$  
ACADEMICOS, se espera que el espectador  
utilice estas experiencias con la esperanza  
que tengamos una mejor seguridad en el  
cibespacio**

Los hackers
NO son
ciberdelincuentes

(\\_/) ||  
(•人•) ||  
/ づ

# CLUB DE HACKING {HARDWARE}



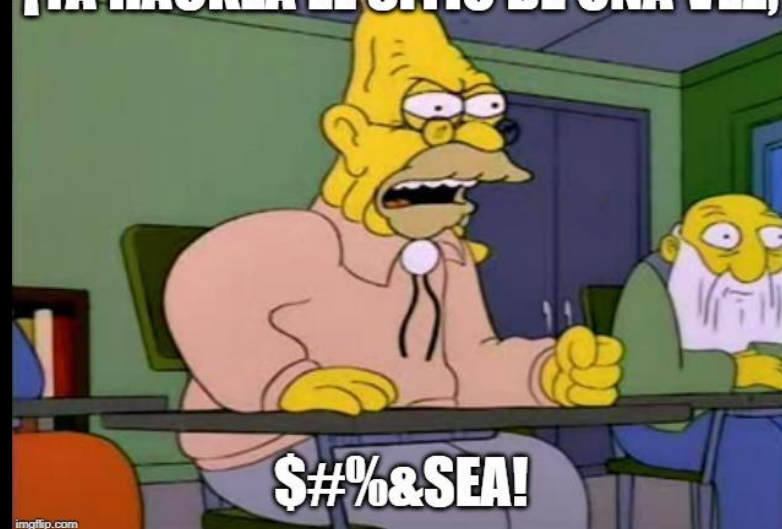
**Christian Camilo Urcuqui López**  
**Ing. Sistemas, Magister en Informática y**  
**Telecomunicaciones**  
**Big Data Scientist**

**Director de TI – Quantil S.A.S**  
**Grupo de investigación i2t – ICESI**  
**Ciberseguridad y ciencia de datos**  
**aplicada**

**BIENVENIDOS A LA CHARLA DE  
CULTURA HACKER**



**¡YA HACKEA EL SITIO DE UNA VEZ,**



**\$#%&SEA!**

HACKER  
Warning!



# Access via OpenVPN

To start hacking, you will need to connect to our network.

## OpenVPN Access Details



VPN Server Name	EU-Regular-2
Server Status	✓
Connected	✗
Internal Virtual IP Address	0.0.0.0

## Machines

## Networks

VPN Server EU-Regular-2

If you're switching for the first time, you will need to redownload your configuration file. For best performance, please use the server that's geographically closest to you.

Download My Configuration File

Regenerate

To hack machines on TryHackMe you need to connect to our network

You can connect through **OpenVPN**, or a **Kali** Linux machine controlled in your browser.

Connect using

## OpenVPN

- ✗ Setup required
- ✓ Use your machine

Connect using

## Kali Machine

- ✓ Access in-browser
- ✓ No setup required
- ✓ Other premium features

# Web Scanning

Part of the Red Primer series, intro to web scanning.

To access material, deploy machines and answer questions you need to join this room!

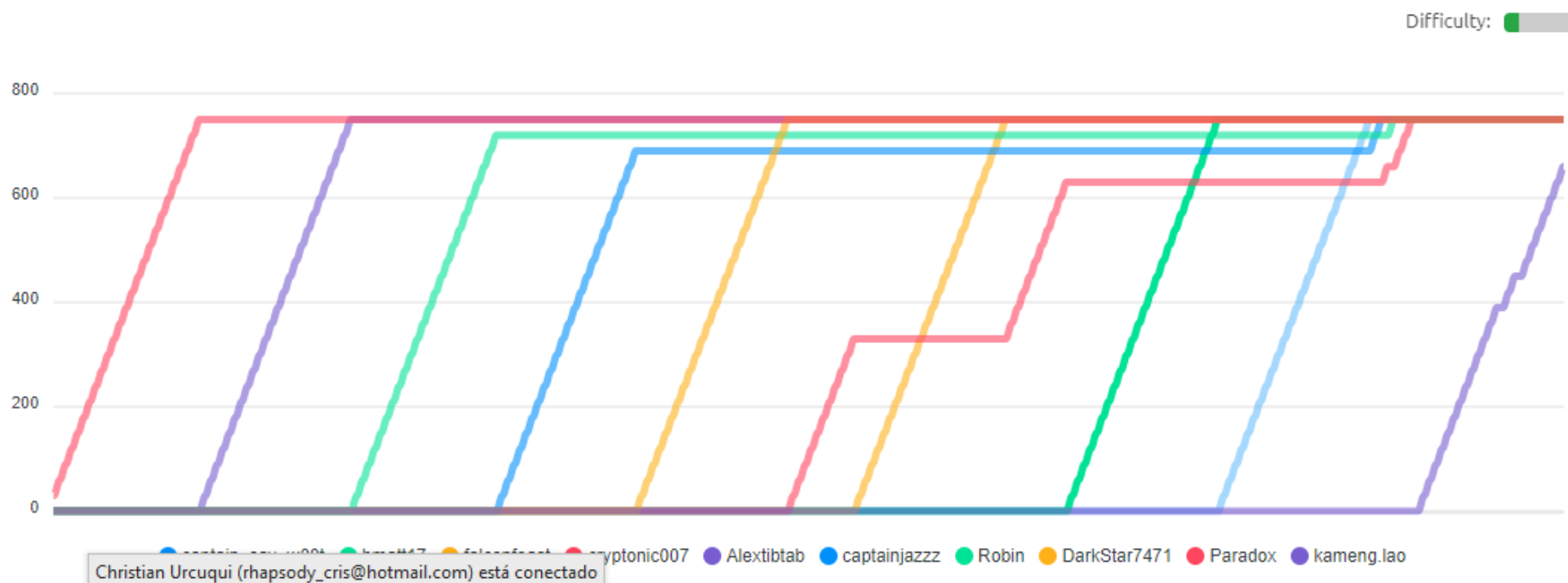
[Join Room](#)

 [Scoreboard](#)

 Discuss

 Writeups

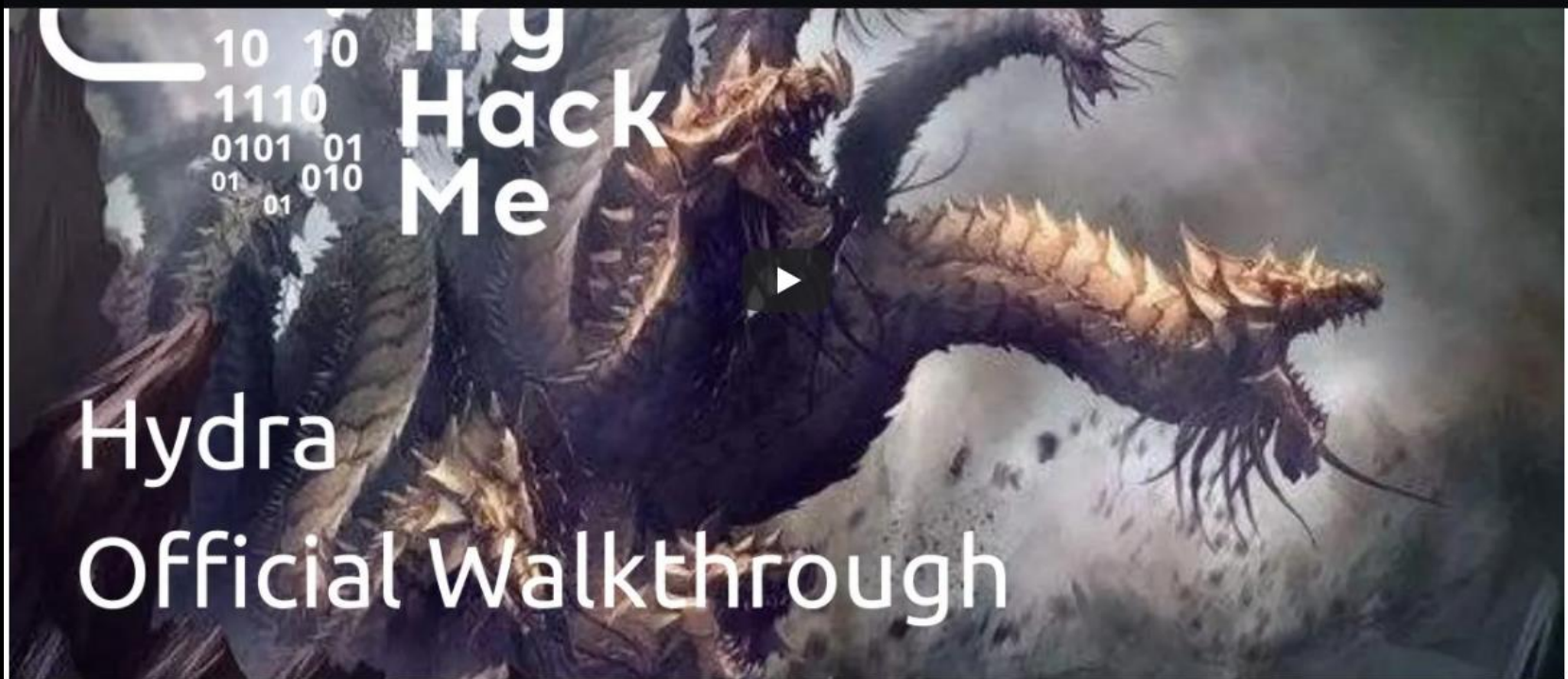
**i More**











100%

Task 1 Hydra Introduction

Task 2 Using Hydra

Deploy the machine attached to this task, then navigate to [http://MACHINE\\_IP](http://MACHINE_IP) (this machine can take up to 3 minutes to boot)

Deploy

## Hydra Commands

The options we pass into Hydra depends on which service (protocol) we're attacking. For example if we wanted to bruteforce 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
```

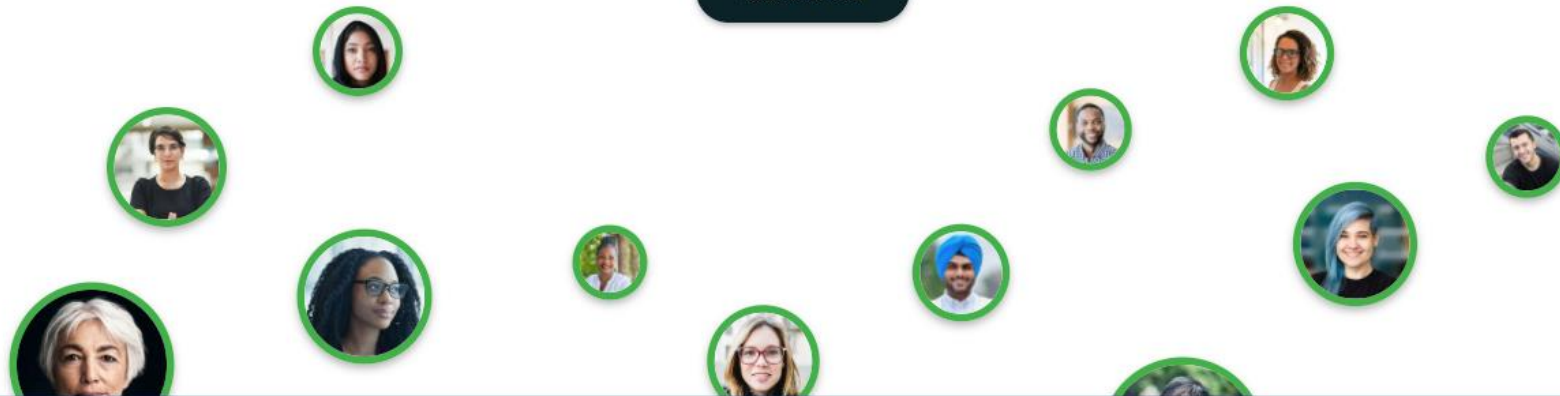
For the purpose of this deployed machine, here are the commands to use Hydra on SSH and a web form (POST method)

<https://tryhackme.com/room/hydra>

# Data science technology for a better world.

A movement that brings together millions of data science practitioners,  
data-driven enterprises, and the open source community.

Get Started



<https://www.anaconda.com/>

## SYSTEM

uname -a ==> Display linux system information  
 uname -r ==> Display kernel release information  
 uptime ==> Show how long the system has been running + load  
 hostname ==> Show system host name  
 hostname -i ==> Display the IP address of the host  
 last reboot ==> Show system reboot history  
 date ==> Show the current date and time  
 cal ==> Show this month calendar  
 w ==> Display who is online  
 whoami ==> Who you are logged in as  
 finger user ==> Display information about user

## HARDWARE

dmesg ==> Detected hardware and boot messages  
 cat /proc/cpuinfo ==> CPU model  
 cat /proc/meminfo ==> Hardware memory  
 cat /proc/interrupts ==> Lists the number of interrupts per CPU per I/O device  
 lshw ==> Displays information on hardware configuration of the system  
 lsblk ==> Displays block device related information in Linux  
 free -m ==> Used and free memory (-m for MB)  
 lspci -tv ==> Show PCI devices  
 lsusb -tv ==> Show USB devices  
 dmidecode ==> Show hardware info from the BIOS  
 hdparm -i /dev/sda ==> Show info about disk sda  
 hdparm -T /dev/sda ==> Do a read speed test on disk sda  
 badblocks -s /dev/sda ==> Test for unreadable blocks on disk sda

## USERS

id ==> Show the active user id with login and group  
 last ==> Show last logins on the system  
 who ==> Show who is logged on the system  
 groupadd admin ==> Add group "admin"  
 useradd -c "Sam Tomshi" ==> g admin -m sam #Create user "sam"  
 userdel sam ==> Delete user sam  
 adduser sam ==> Add user "sam"  
 usermod ==> Modify user information

## FILE COMMANDS

ls -al ==> Display all information about files/ directories  
 pwd ==> Show the path of current directory  
 mkdir directory-name ==> Create a directory  
 rm file-name ==> Delete file  
 rm -r directory-name ==> Delete directory recursively  
 rm -f file-name ==> Forcefully remove file  
 rm -rf directory-name ==> Forcefully remove directory recursively  
 cp file1 file2 ==> Copy file1 to file2  
 cp -r dir1 dir2 ==> Copy dir1 to dir2, create dir2 if it doesn't exist  
 mv file1 file2 ==> Rename source to dest / move source to directory  
 ln -s /path/to/file-name link-name ==> Create symbolic link to file-name  
 touch file ==> Create or update file  
 cat > file ==> Place standard input into file  
 more file ==> Output contents of file  
 head file ==> Output first 10 lines of file  
 tail file ==> Output last 10 lines of file  
 tail -f file ==> Output contents of file as it grows starting with the last 10 lines  
 gpg -c file ==> Encrypt file  
 gpg file.gpg ==> Decrypt file  
 wc ==> print the number of bytes, words, and lines in files  
 xargs ==> Execute command lines from standard input

## PROCESS RELATED

ps ==> Display your currently active processes  
 ps aux | grep 'telnet' ==> Find all process id related to telnet process  
 pmmap ==> Memory map of process  
 top ==> Display all running processes  
 kill pid ==> Kill process with mentioned pid id  
 killall proc ==> Kill all processes named proc  
 pkill process-name ==> Send signal to a process with its name  
 bg ==> Resumes suspended jobs without bringing them to foreground  
 fg ==> Brings the most recent job to foreground  
 fg n ==> Brings job n to the foreground

## FILE PERMISSION RELATED

chmod octal file-name ==> Change the permissions of file to octal  
 Example  
 chmod 777 /data/test.c ==> Set rwx permission for owner,group,world  
 chmod 755 /data/test.c ==> Set rwx permission for owner,rx for group and world  
 chown owner-user file ==> Change owner of the file  
 chown owner-user:owner-group file-name ==> Change owner and group owner of the file  
 chown owner-user:owner-group directory ==> Change owner and group owner of the directory

## NETWORK

ip addr show ==> Display all network interfaces and ip address (a iproute2 command, powerful than ifconfig)  
 ip address add 192.168.0.1 dev eth0 ==> Set ip address  
 ethtool eth0 ==> Linux tool to show ethernet status  
 mii-tool eth0 ==> Linux tool to show ethernet status  
 ping host ==> Send echo request to test connection  
 whois domain ==> Get who is information for domain  
 dig domain ==> Get DNS information for domain  
 dig -x host ==> Reverse lookup host  
 host google.com ==> Lookup DNS ip address for the name  
 hostname -i ==> Lookup local ip address  
 wget file ==> Download file  
 netstat -tupl ==> Listing all active listening ports

## COMPRESSION / ARCHIVES

tar of home.tar home ==> Create tar named home.tar containing home/  
 tar xf file.tar ==> Extract the files from file.tar  
 tar czf file.tar.gz files ==> Create a tar with gzip compression  
 gzip file ==> Compress file and renames it to file.gz

## INSTALL PACKAGE

rpm -i pkgname.rpm ==> Install rpm based package  
 rpm -e pkgname ==> Remove package

## INSTALL FROM SOURCE

./configure  
 make  
 make install

## SEARCH

grep pattern files ==> Search for pattern in files  
 grep -r pattern dir ==> Search recursively for pattern in dir  
 locate file ==> Find all instances of file  
 find /home/tom -name "index" ==> Find files names that start with "index"  
 find /home -size +10000k ==> Find files larger than 10000k in /home

## LOGIN (SSH AND TELNET)

ssh user@host ==> Connect to host as user  
 ssh -p port user@host ==> Connect to host using specific port  
 telnet host ==> Connect to the system using telnet port

## FILE TRANSFER

scp ==> Secure copy file to remote host  
 scp file.txt server2/tmp ==> Secure copy file.txt to remote host /tmp folder  
 rsync -a /home/apps /backup/ ==> Synchronize source to destination

## DISK USAGE

df -h ==> Show free space on mounted filesystems  
 df -i ==> Show free inodes on mounted filesystems  
 fdisk -l ==> Show disks partitions sizes and types  
 du -ah ==> Display disk usage in human readable form  
 du -sh ==> Display total disk usage on the current directory  
 findmnt ==> Displays target mount point for all filesystem  
 mount device-path mount-point ==> Mount a device

## DIRECTORY TRAVERSE

cd .. ==> To go up one level of the directory tree  
 cd ==> Go to \$HOME directory  
 cd /test ==> Change to /test directory



