Road to Battle of Hackers 2020: Introduction to CTF

Reza Ahmad Nugroho
Cyber Security Student,
Committee of Battle of Hackers 2020

#H4CKFROMHOM3 #SAFEMODE

$ whoami

SYSTEM ANALYST INTERN @ TOP NOTCH COMPUTERS

It's an intern position, you know how it is . . .

COMMITTEE @ FSEC-SS 2020

basically the reason why im here

VICE PRESIDENT @ INDONESIAN STUDENT SOCIETY

Yes im busy, thx

Reza Nugroho

@jmp2rsp

About Today

Topics and What to Expect

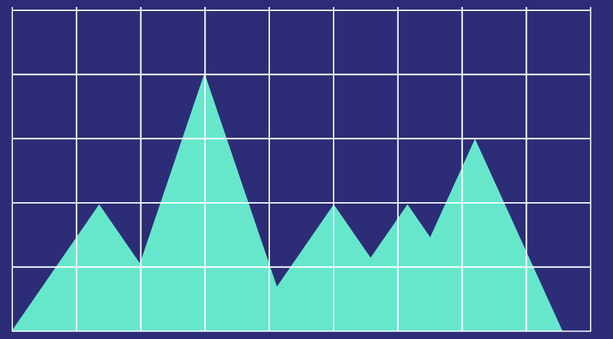
Introduction to CTF

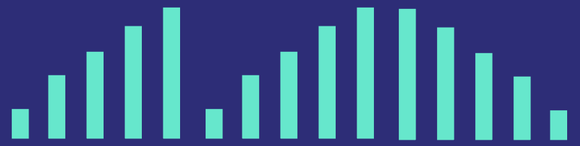
- What is CTF
- Types of CTF
- How CTF can help you learn
- Pros and cons
- Platform to Learn

How to Get Started (Hands On)

- Setting up your hacking box
- Linux 101
- Solving Some Challenges

What is Security CTF?





A cyber security CTF is a competition between security professionals and/or students learning about cyber security. This competition is used as a learning tool for everyone that is interested in cyber security and it can help sharpen the tools they have learned during their training.

*TL;DR: It's a game to learn and demonstrate security skills

CTF Types

Several types of security CTF around the world

ATTACK & DEFENSE

Defending our machine and attacking other team's machine

JEOPARDY

Solving numerous type of challenges

BOOT2ROOT

Compromise a machine and get access to user and root flag

Attack & Defense CTF

FORMAT

in Attack & Defense CTF each team will be given a vulnerable box/machine. We will have to defense our own machine and attack other team's machines. Successfully defending your machine will grant you defense point. Compromising enemy's machine will grant you attack point

HISTORY

The very first cyber security CTF developed and hosted was in 1996 at DEFCON in Las Vegas, Nevada. DEFCON is the largest cyber security conference in the United States and it was officially started in 1993 by Jeff Moss.

DEF CON CTF 2015 - Game Replay

25,004 views • 29 Aug 2015

58 25 SHARE SAVE

Jeopardy CTF Challenges

Forensics

Data recovery,
Steganography,
Network Analysis

RECAP →

Binary Exploitation

Buffer Overflow,
Format String

RECAP →

Reverse Engineer

Reverse Engineering
Binary/Executables

RECAP →

Web

XSS, SQLi, Cookies,
JWT

RECAP →

Crypto

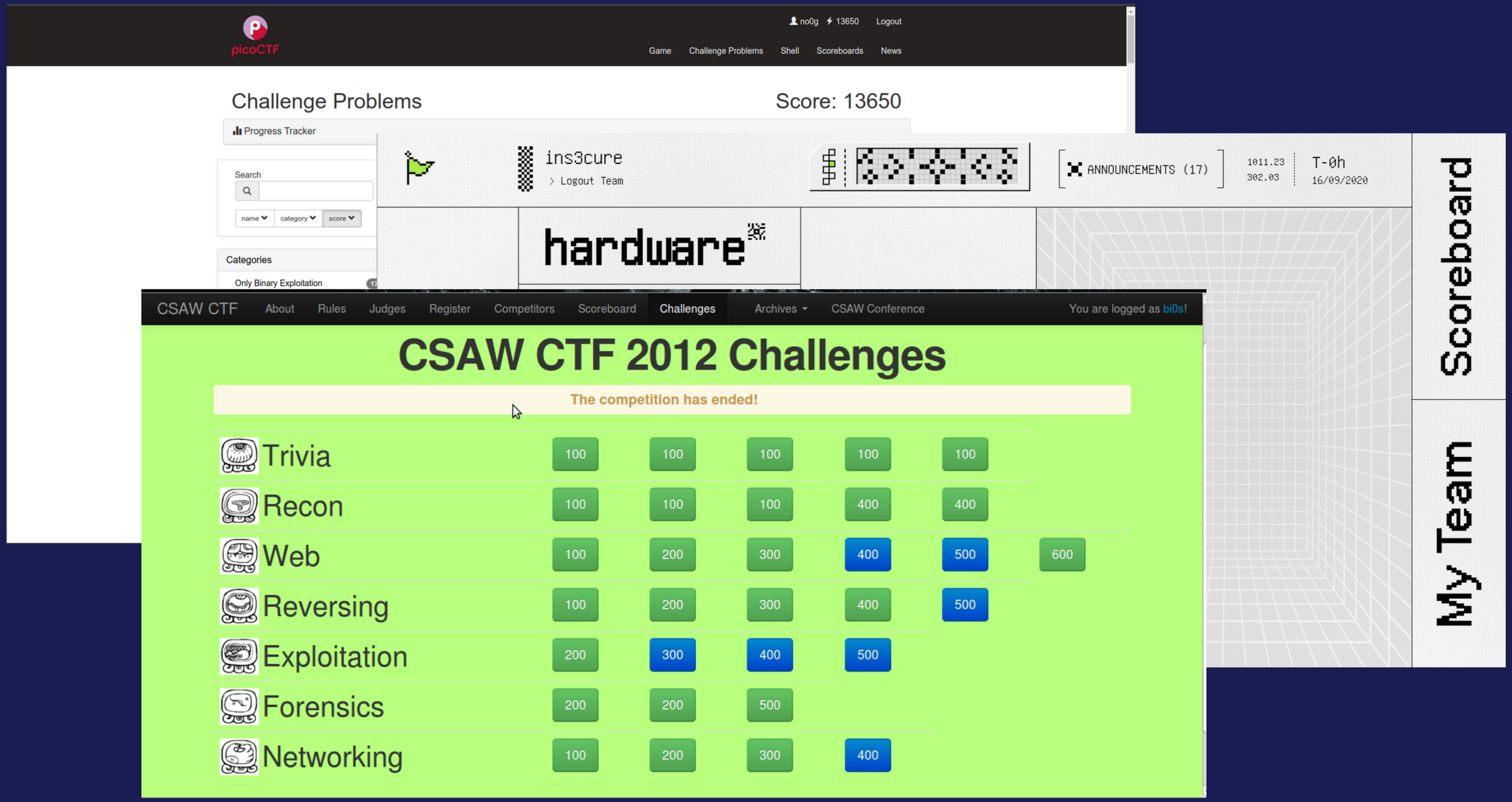
ROT13 to RSA

RECAP →

Miscellaneous

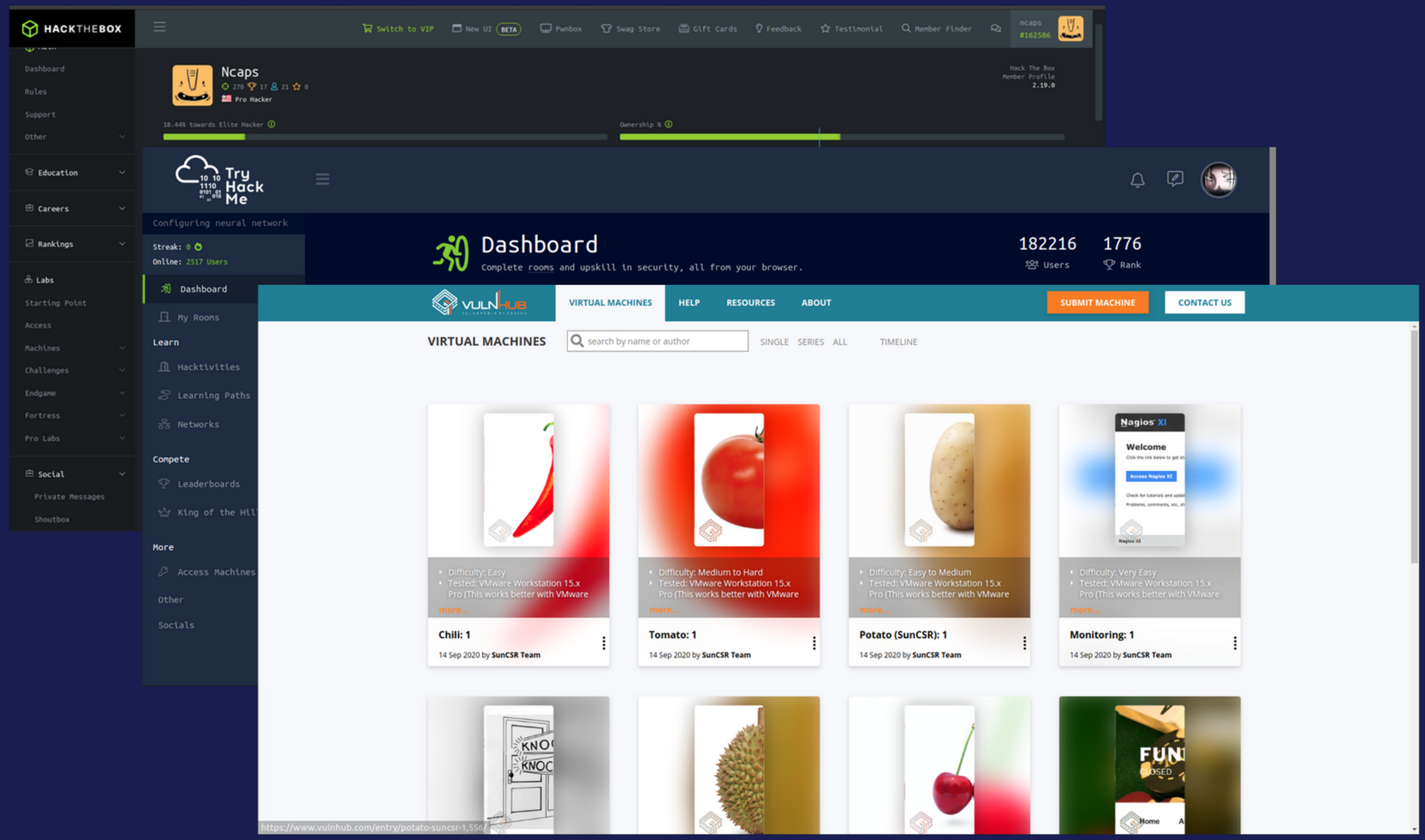
Fun Stuff, General
Knowledge,
Programming

RECAP →


picoCTF
no0g 13650 Logout
Game Challenge Problems Shell Scoreboards News
Challenge Problems
Score: 13650
Progress Tracker
Search
name category score
Categories
Only Binary Exploitation
ins3cure
> Logout Team
ANNOUNCEMENTS (17)
1011.23
302.03
T-0h
16/09/2020
hardware
Scoreboard
My Team
CSAW CTF
About Rules Judges Register Competitors Scoreboard Challenges Archives CSAW Conference
You are logged as bi0s!
CSAW CTF 2012 Challenges
The competition has ended!
Trivia 100 100 100 100 100
Recon 100 100 100 400 400
Web 100 200 300 400 500 600
Reversing 100 200 300 400 500
Exploitation 200 300 400 500
Forensics 200 200 500
Networking 100 200 300 400

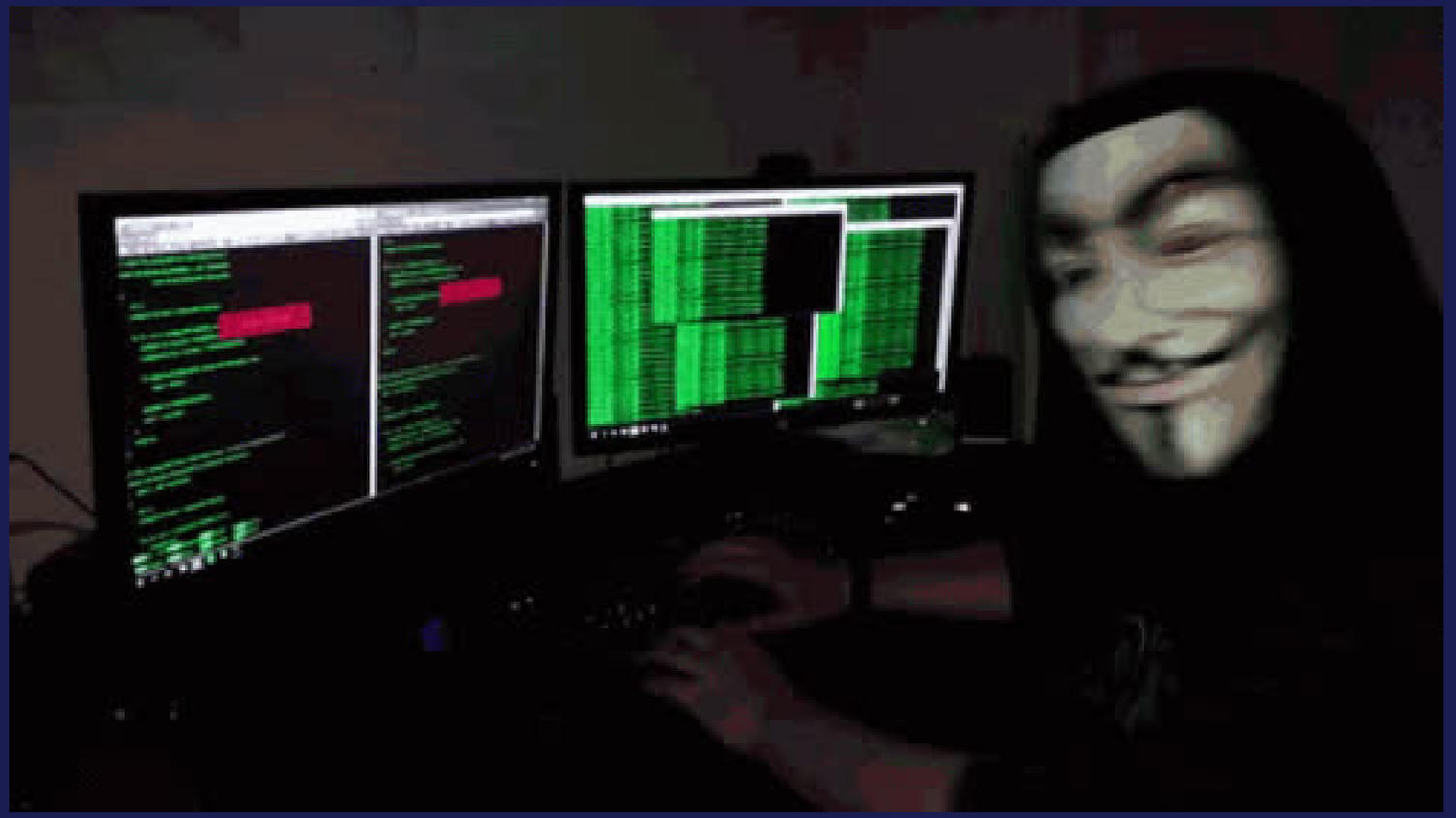
Boot2Root

In this CTF participant will have to compromise a machine. Usually there will be 2 flags to be collected. the first one will be accessible with low level privilege user and the second one is accessible with root level privilege user.



Getting Started

By the end of this session
you will NOT look like this



Linux and Why

This is going to be short i promise

What is Linux?

GNU/Linux or Linux OS is open-source Operating System

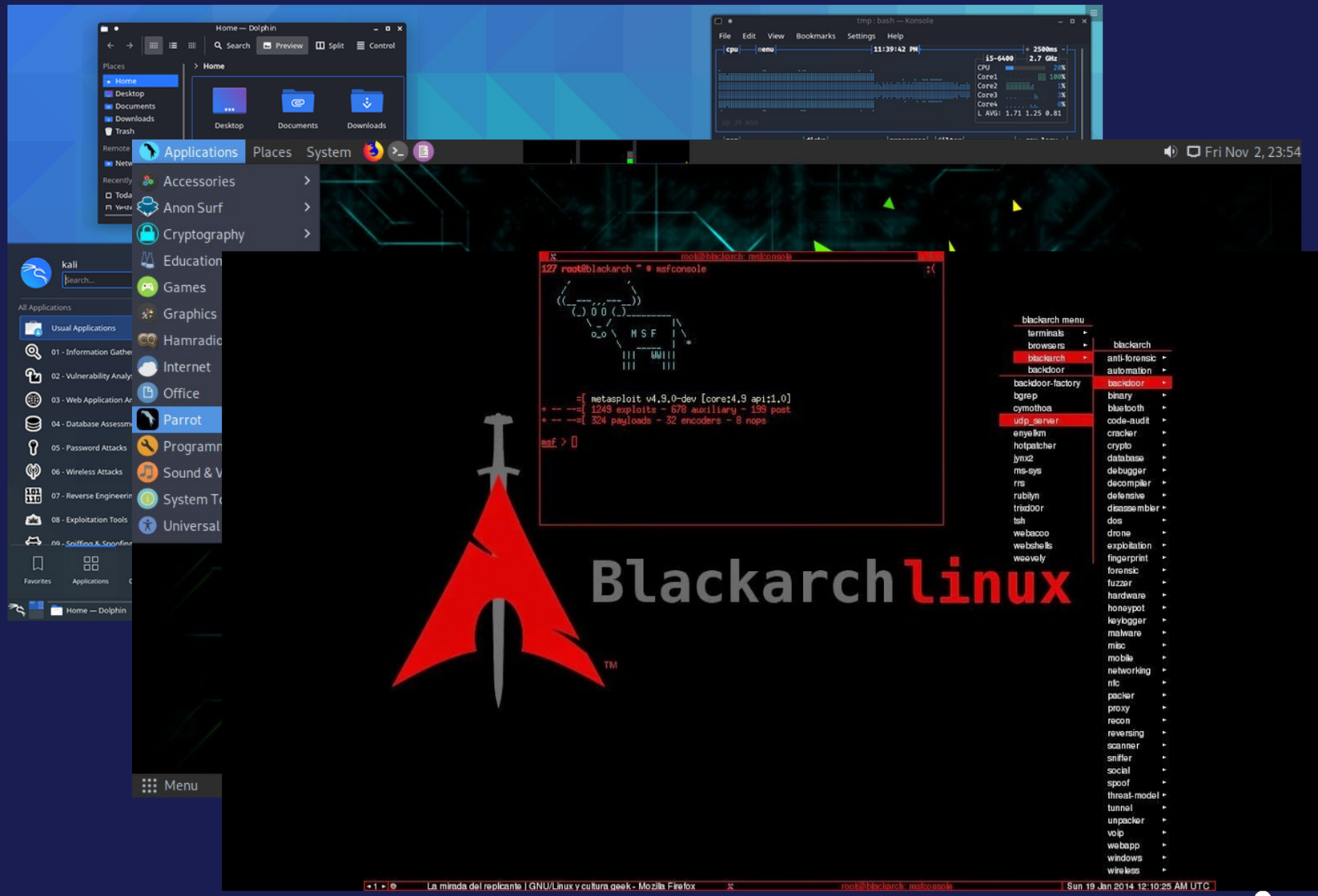
Why?

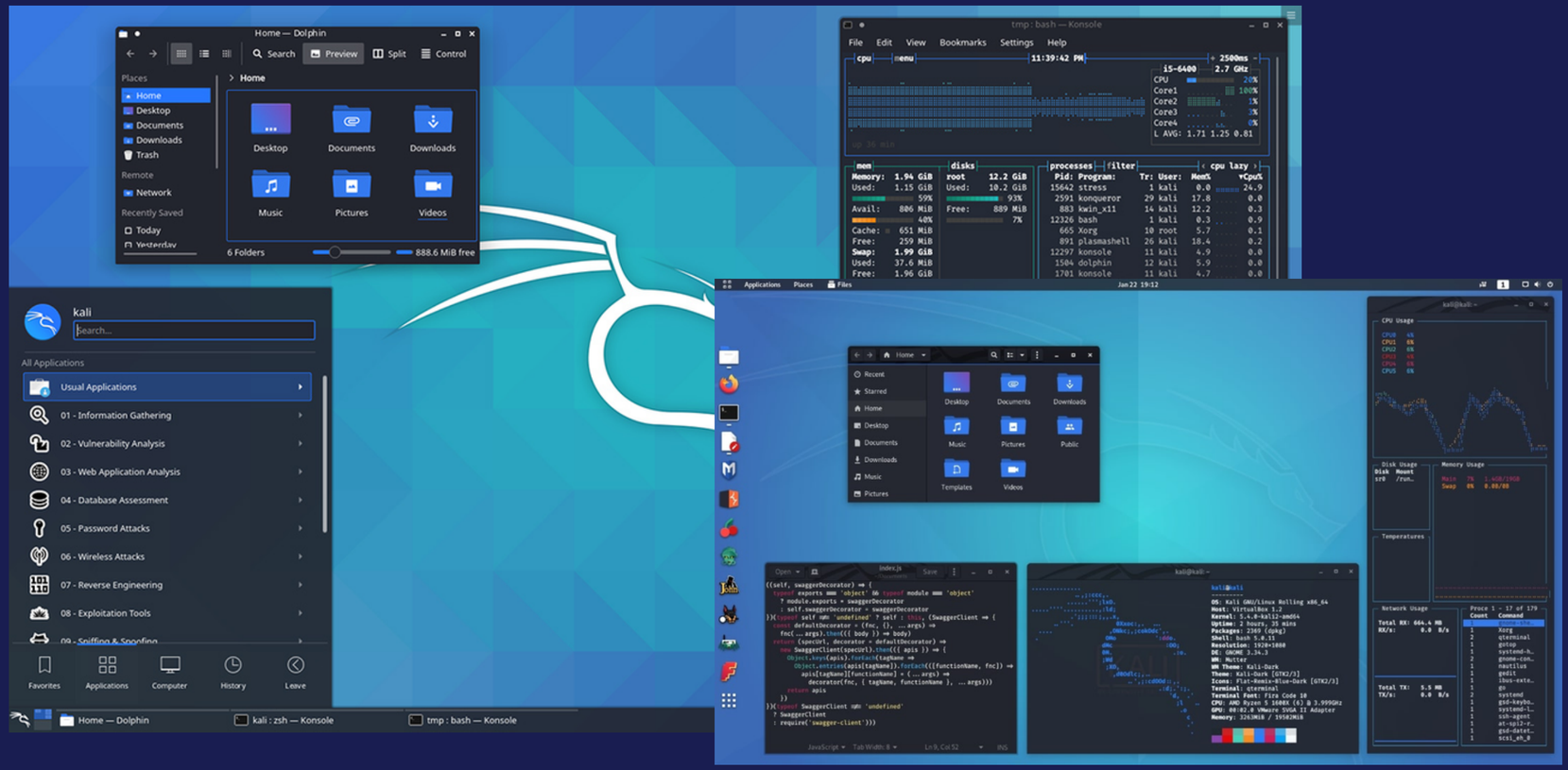
1. Highly Costumizable
2. Arguably more secure
3. A lot of hacking tools designed for linux
4. There are distros specifically designed for hacking/pentest

Hacking Distros

- Kali Linux
- Parrot OS
- Black Arch
- etc

These Distros have pre-installed hacking tools inside





Kali linux

Hacking distros developed and maintained by Offensive-Security

How to install?

Dual Boot

Installing Kali alongside Windows/Mac

RECAP →

WSL

Installing Kali with Windows Subsystem Linux in Windows

RECAP →

Virtual Machine

Install Kali as a virtual machine with VMware or VirtualBox

RECAP →

Virtual Machine and Why

Just to give you an overview

What is Virtual Machine?

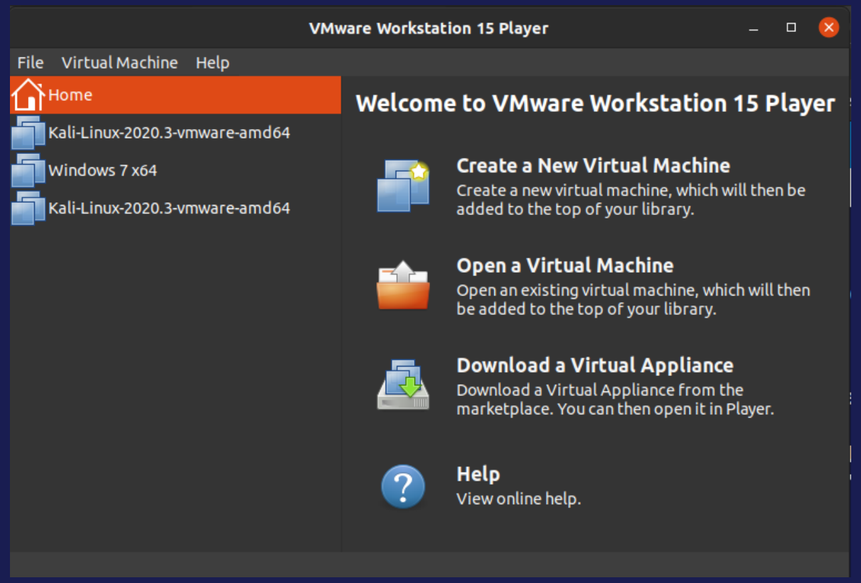
a virtual machine is an emulation of a computer system.

Why?

- VMs allow for reduced overhead, with multiple systems operating from the same console at the same time
- VMs also provide a safety net for your data, as they can be used to enable rapid disaster recovery and automatic backups.

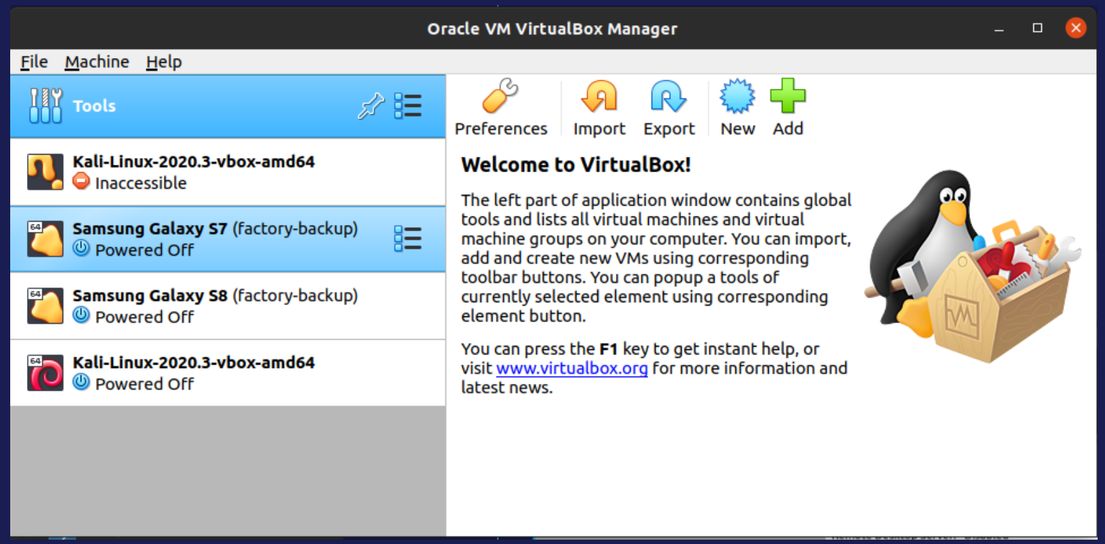
For Windows

1. **Unzip everything**
2. **Install the VMware by double clicking the .exe file**
3. **Click 'Open Virtual Machine' and load the .vmx file from Kali's Folder**



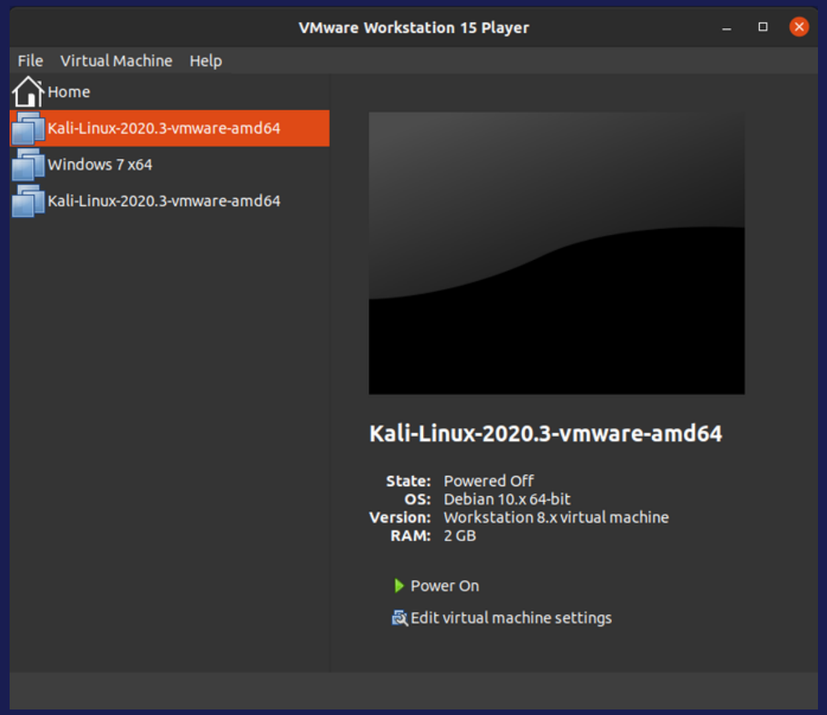
For Mac

1. **Unzip everything**
2. **Install the VirtualBox by double clicking the .dmg file**
3. **Go to 'Tools' and Click 'Import' and load the .ova file**



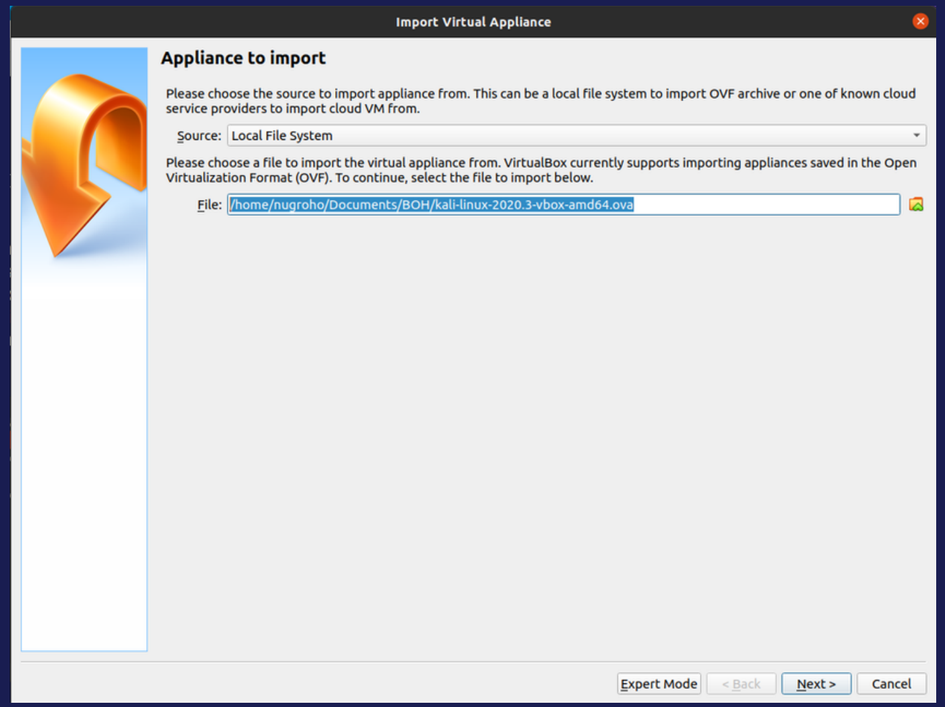
For Windows

1. **Unzip everything**
2. **Install the VMware by double clicking the .exe file**
3. **Click 'Open Virtual Machine' and load the .vmx file from Kali's Folder**



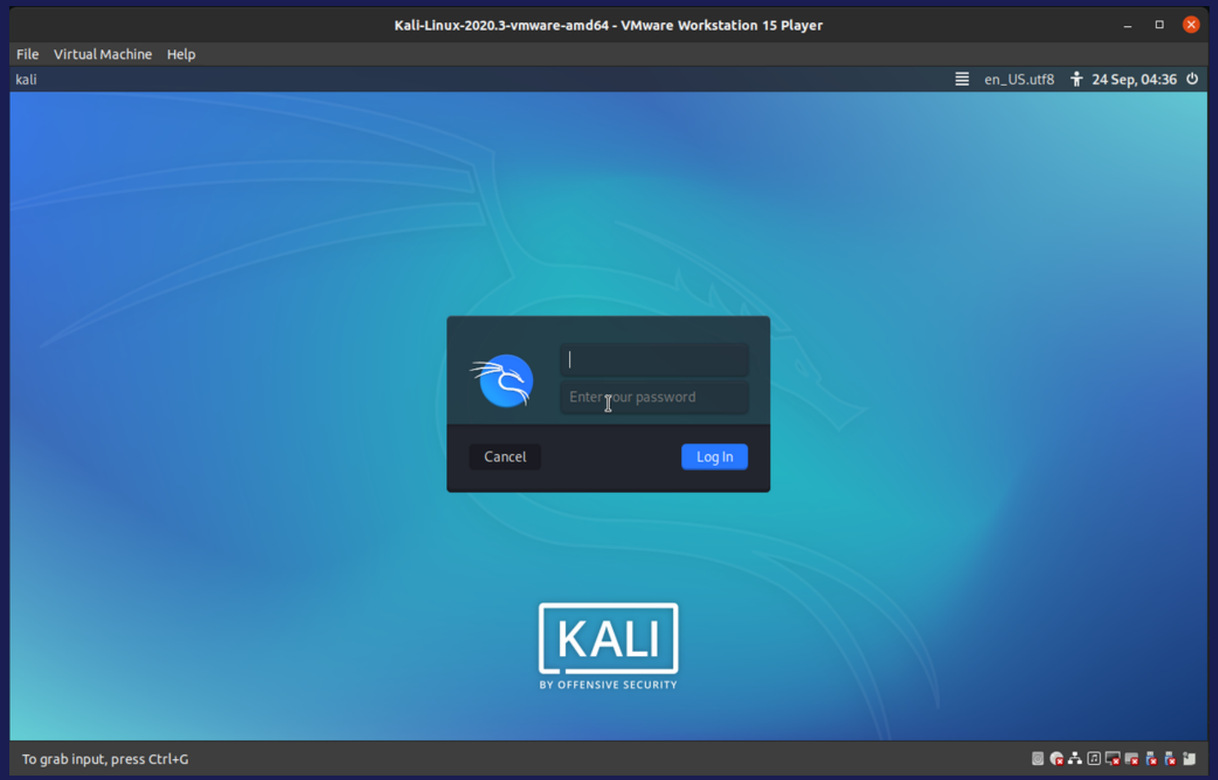
For Mac

1. **Unzip everything**
2. **Install the VirtualBox by double clicking the .dmg file**
3. **Go to 'Tools' and Click 'Import' and load the .ova file**

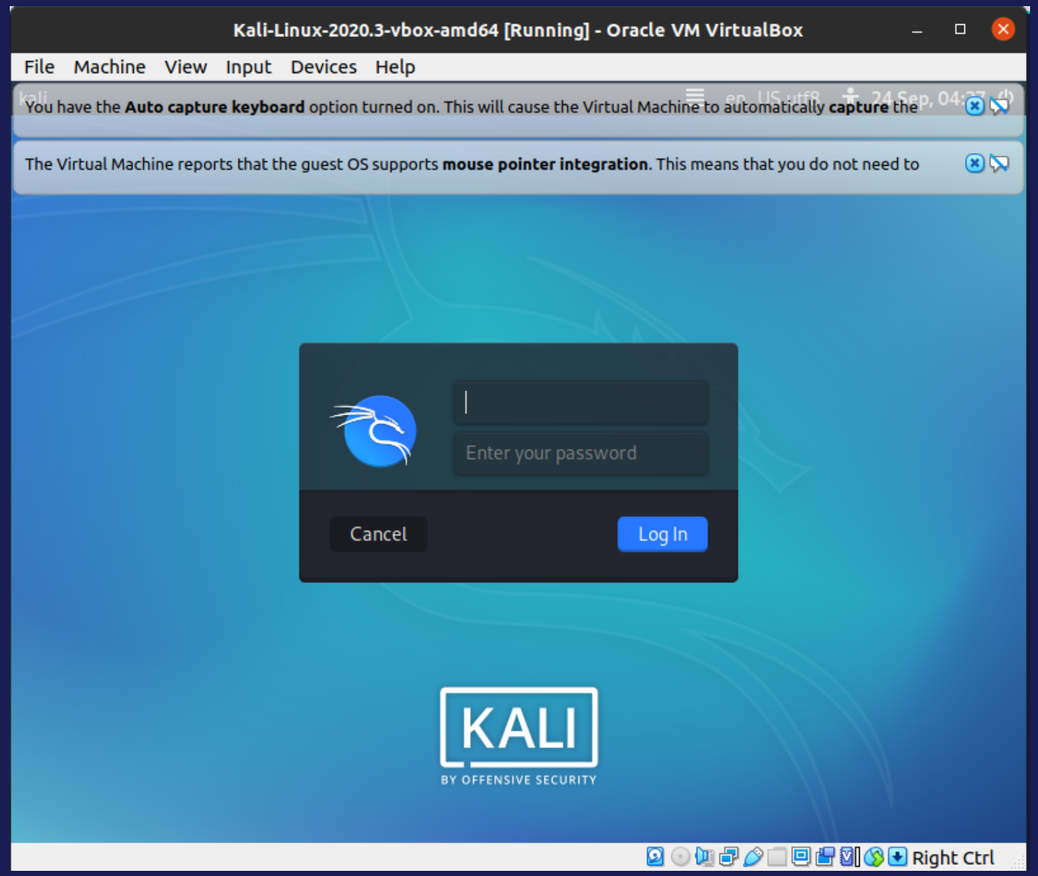


Keep clicking next till it's done

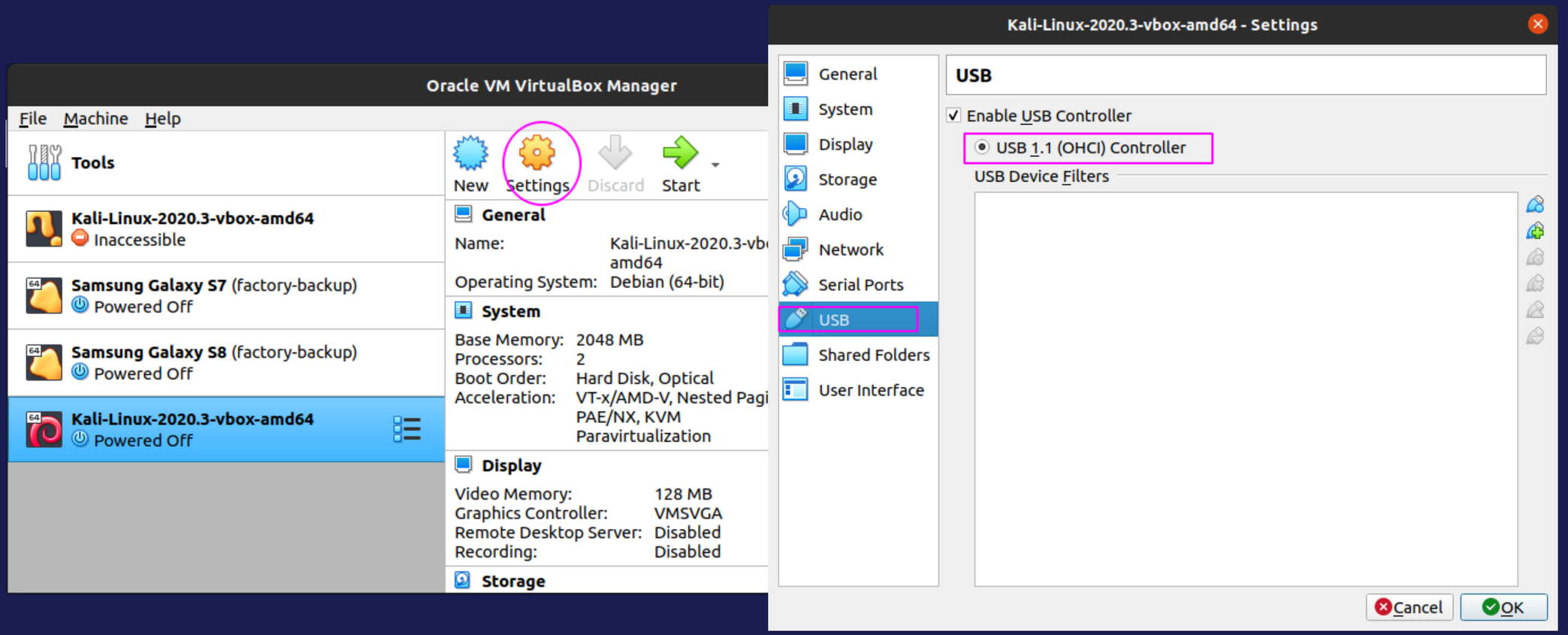
For Windows



For Mac



Common Problem for Virtual Box



Congrats!

YOU HAVE INSTALLED YOUR HACKING MACHINE

Now **START LEARNING!!!**

$Users

Types of users in linux

Whenever you need root access you need 'SUDO'

User Privilege

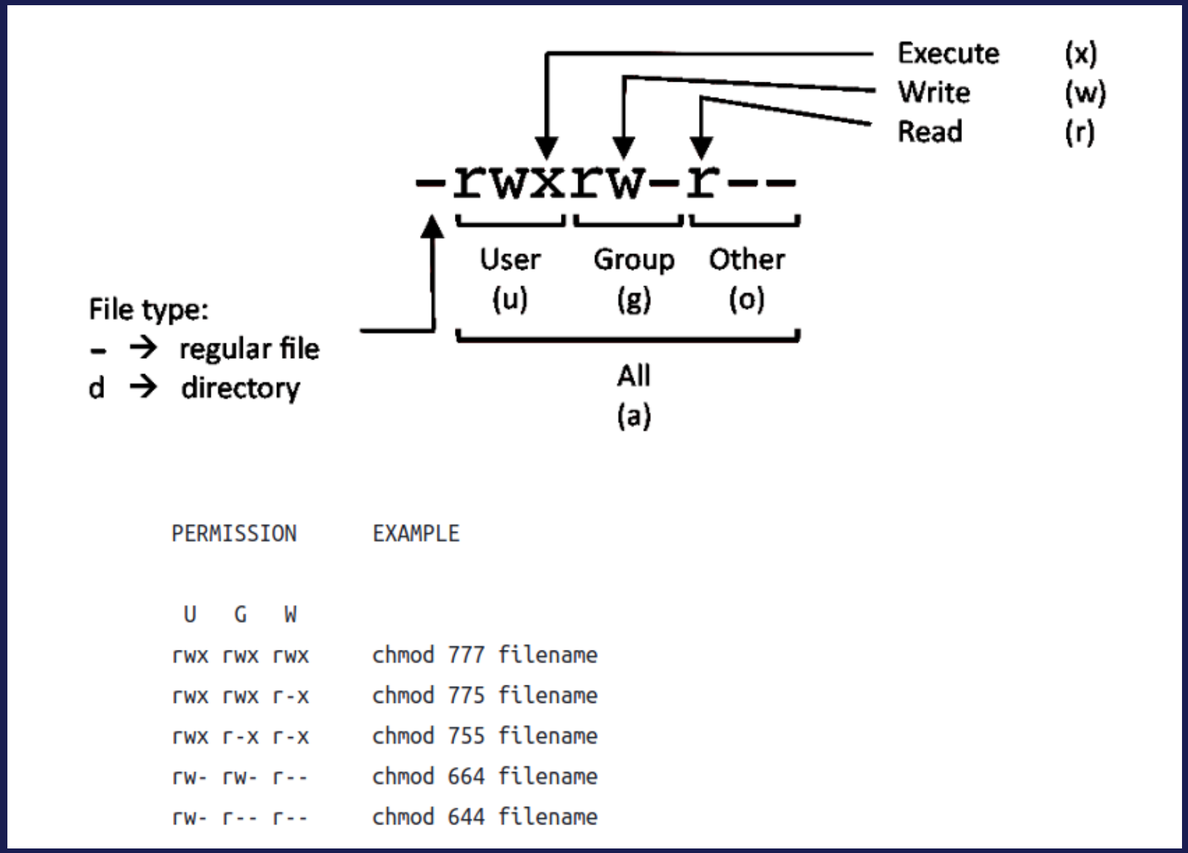
Limited privilege named anything

Root Privilege

Admin privilege named 'root'

$File Permission

What you can do with the files



PERMISSION			EXAMPLE
U	G	W	
rwx	rwx	rwx	chmod 777 filename
rwx	rwx	r-x	chmod 775 filename
rwx	r-x	r-x	chmod 755 filename
rw-	rw-	r--	chmod 664 filename
rw-	r--	r--	chmod 644 filename

Terminal & Command

cd, ls, pwd and all kind of thing

Directory Lisiting

```
kali@kali:~$ ls
Desktop    Downloads  Pictures  Templates  youtube
Documents  Music      Public    Videos
kali@kali:~$
```

Current Directory

```
kali@kali:~$ pwd
/home/kali
kali@kali:~$
```

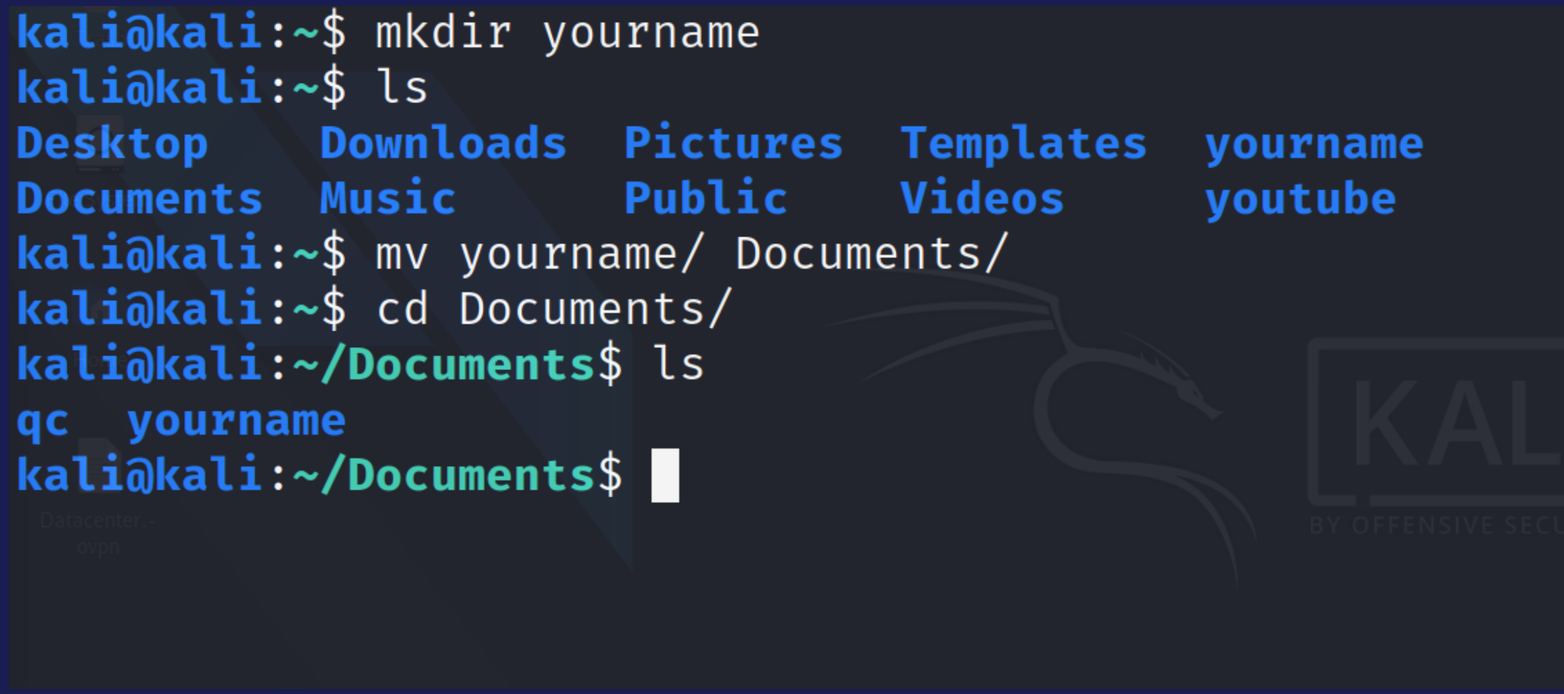
Jump to Directory

```
kali@kali:~$ cd Documents/
kali@kali:~/Documents$
```

Terminal & Command

cd, ls, pwd and all kind of thing

Make and move directory



Terminal & Command

cd, ls, pwd and all kind of thing

Read file and copy file

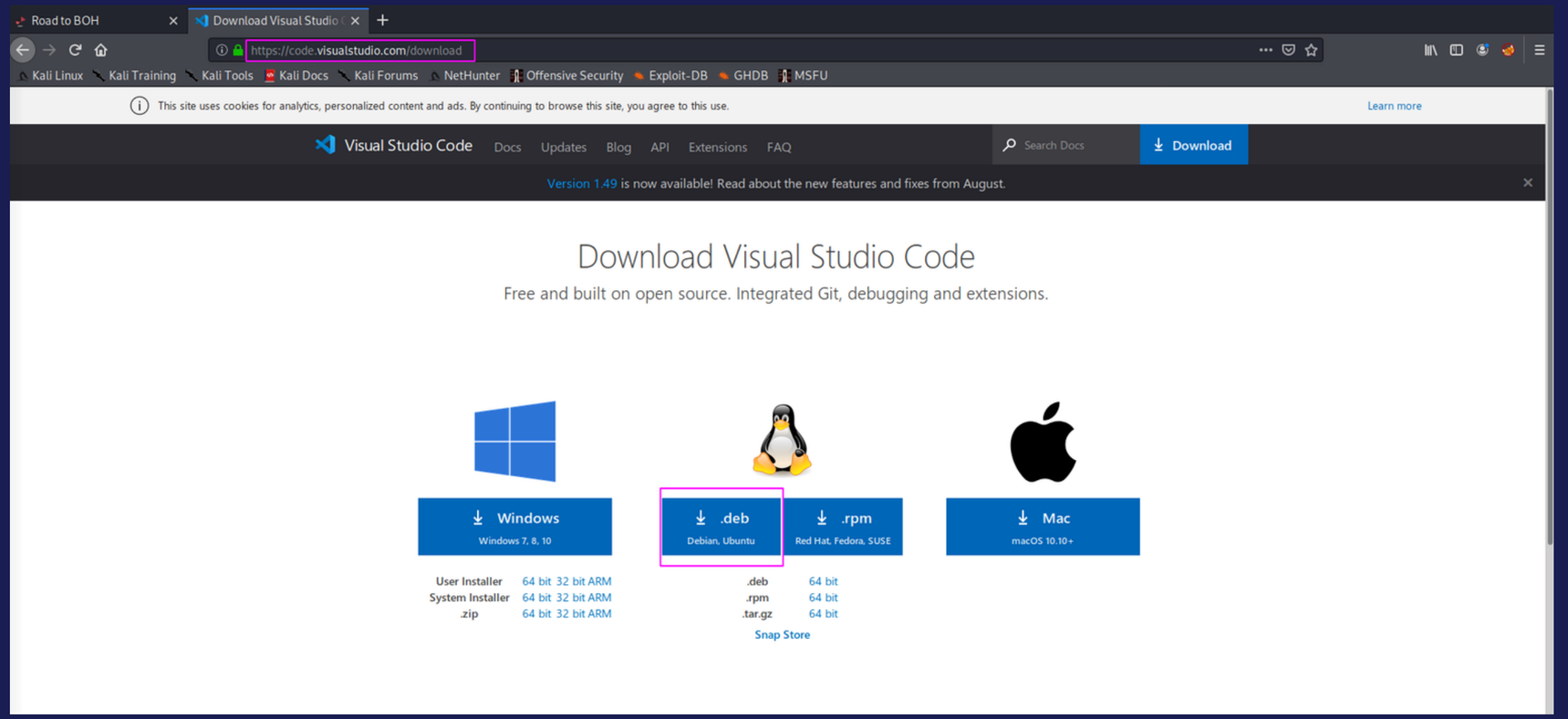
```
kali@kali:~/Documents/yourname$ cat flag.txt
FLAG{asdfadsf}
kali@kali:~/Documents/yourname$ cp flag.txt ../
kali@kali:~/Documents/yourname$
```

Update Command

```
kali@kali:~/Downloads$ sudo apt update
Get:1 http://packages.microsoft.com/repos/vscode stable InRelease [3,959 B]
Get:2 http://packages.microsoft.com/repos/vscode stable/main amd64 Packages [201 kB]
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.5 kB]
Get:4 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Packages [16.6 MB]
Get:5 http://kali.cs.nctu.edu.tw/kali kali-rolling/contrib amd64 Packages [100 kB]
Get:6 http://kali.cs.nctu.edu.tw/kali kali-rolling/non-free amd64 Packages [199 kB]
Fetched 17.1 MB in 13s (1,298 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
79 packages can be upgraded. Run 'apt list --upgradable' to see them.
kali@kali:~/Downloads$
```

Let's install an IDE

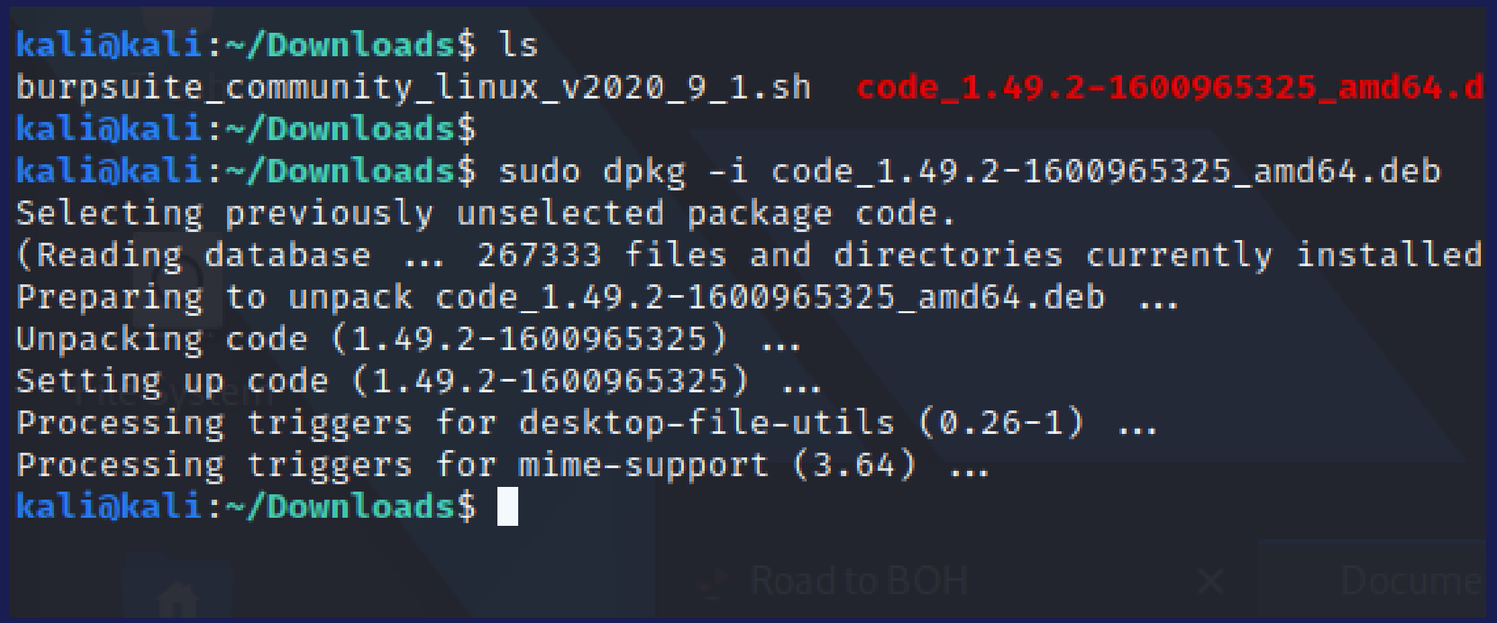
1. GO TO VISUAL CODE PAGE
2. DOWNLOAD THE .DEB PACKAGE



Let's install an IDE

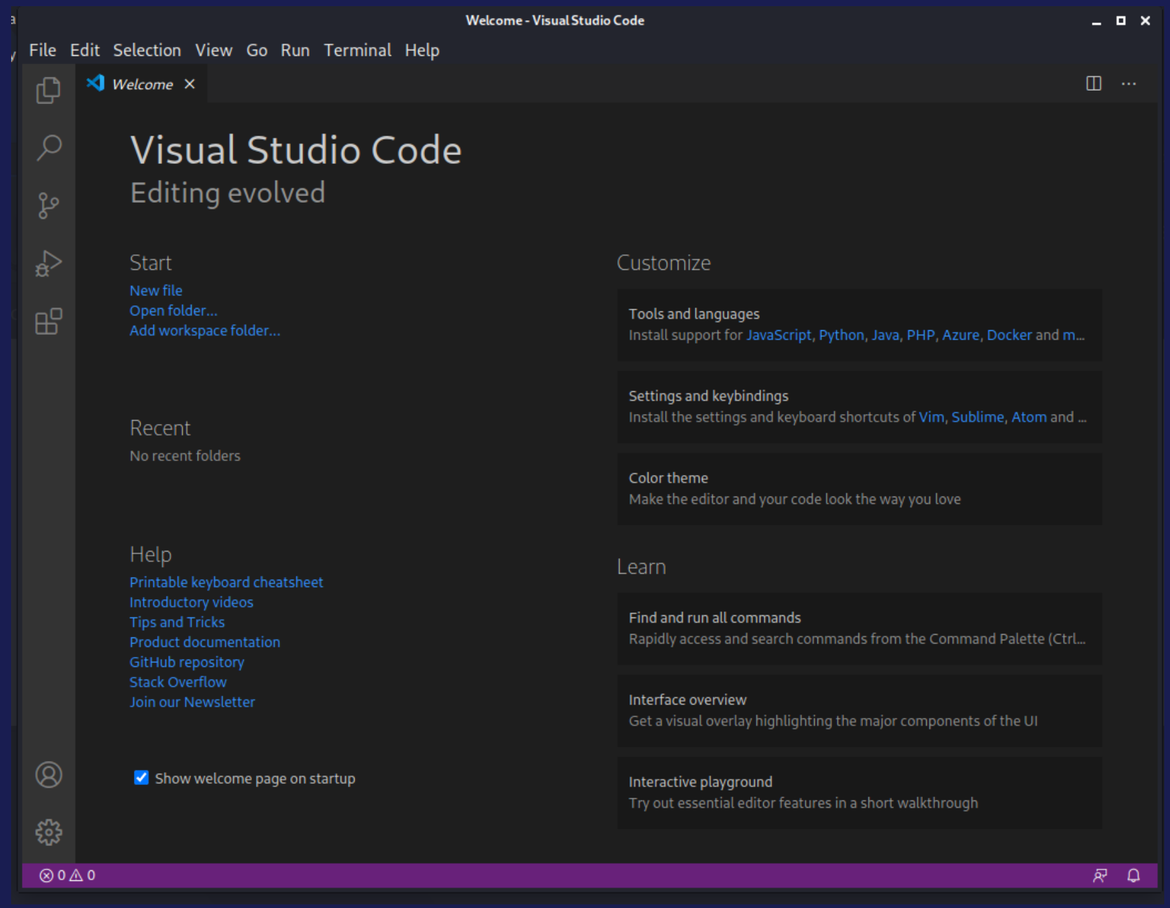
1. INSTALL FROM TERMINAL WITH THE COMMAND :

   `sudo dpkg -i <file name>`



Let's install an IDE

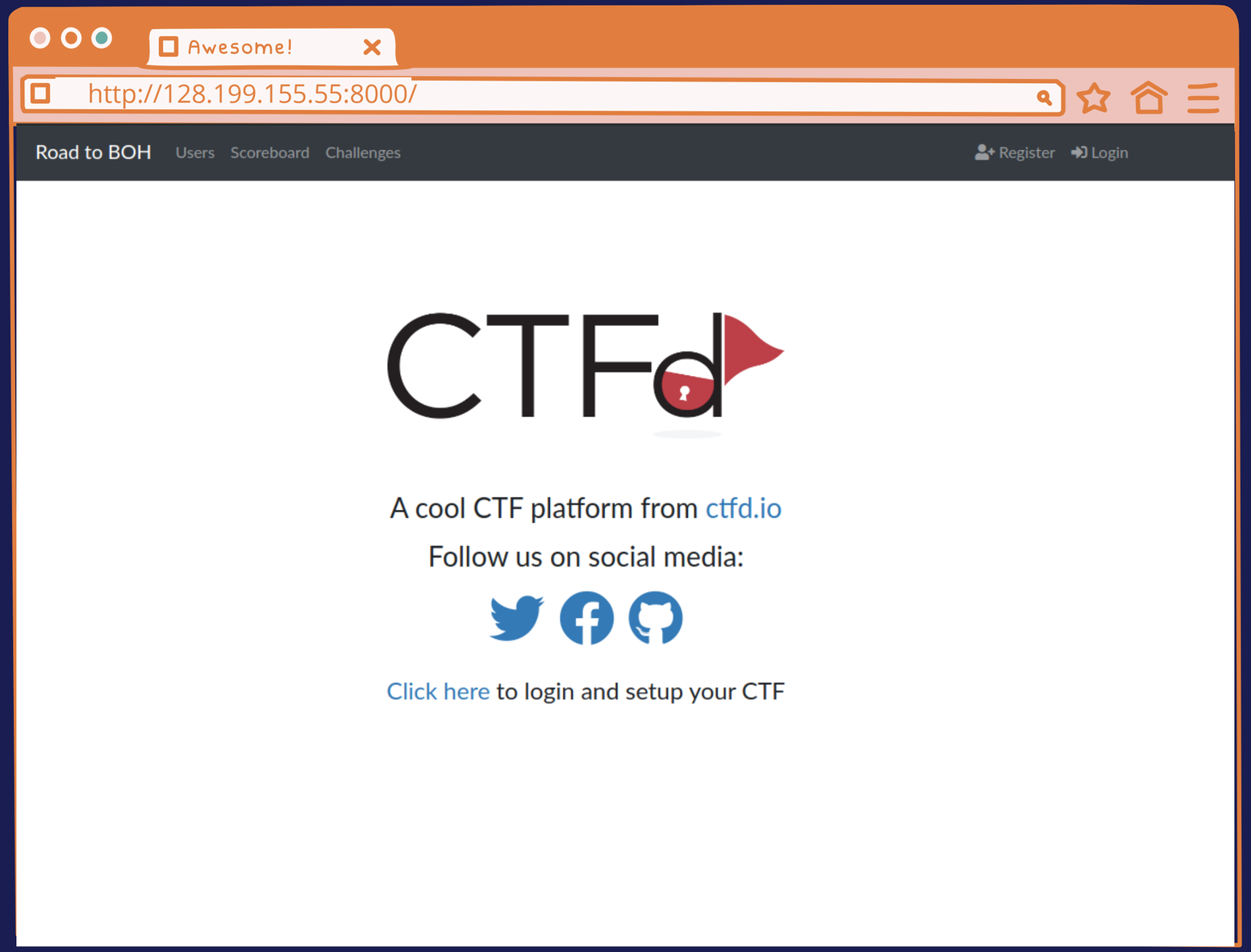
1. RUN FROM TERMINAL WITH THE COMMAND :
   `code`



Ok

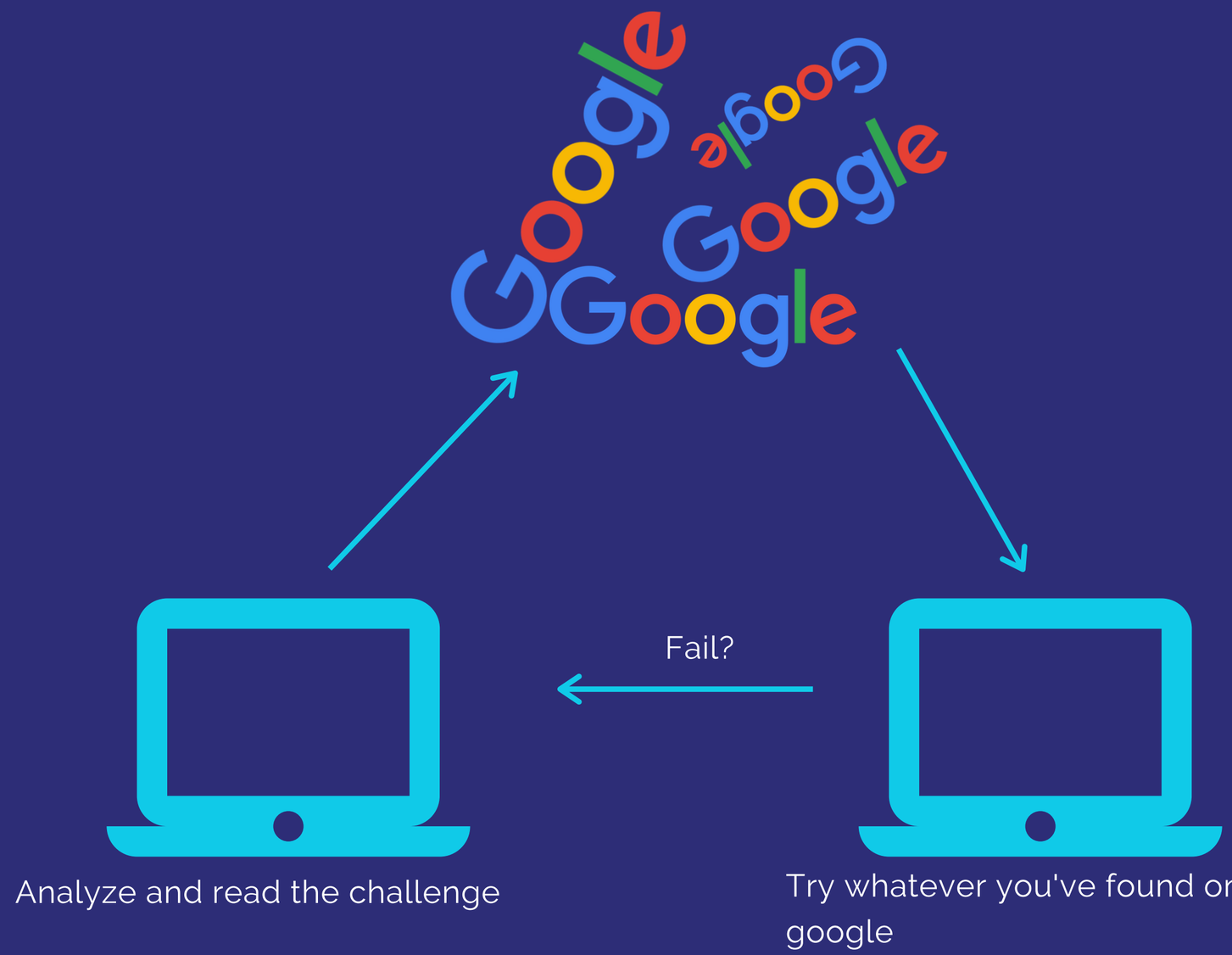
LET'S HAVE A BREAK

LET'S
Jump into it!


Awesome!
http://128.199.155.55:8000/
Road to BOH
Users
Scoreboard
Challenges
Register
Login
CTFd
A cool CTF platform from ctfd.io
Follow us on social media:
Click here to login and setup your CTF

How to solve challenges in CTF?

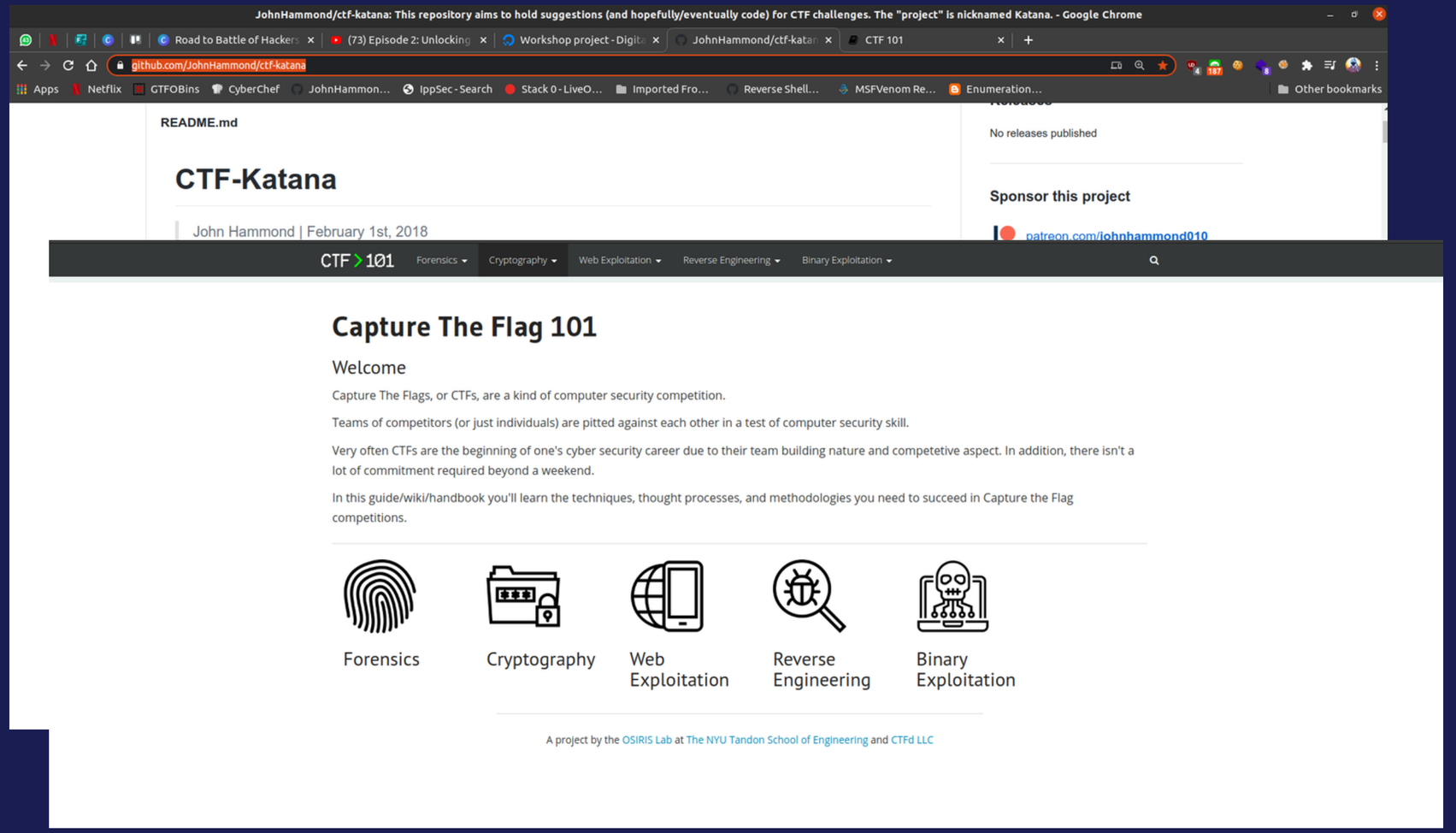
Short answer. Research!



Learning source

https://github.com/JohnHammond/ctf-katana - KATANA

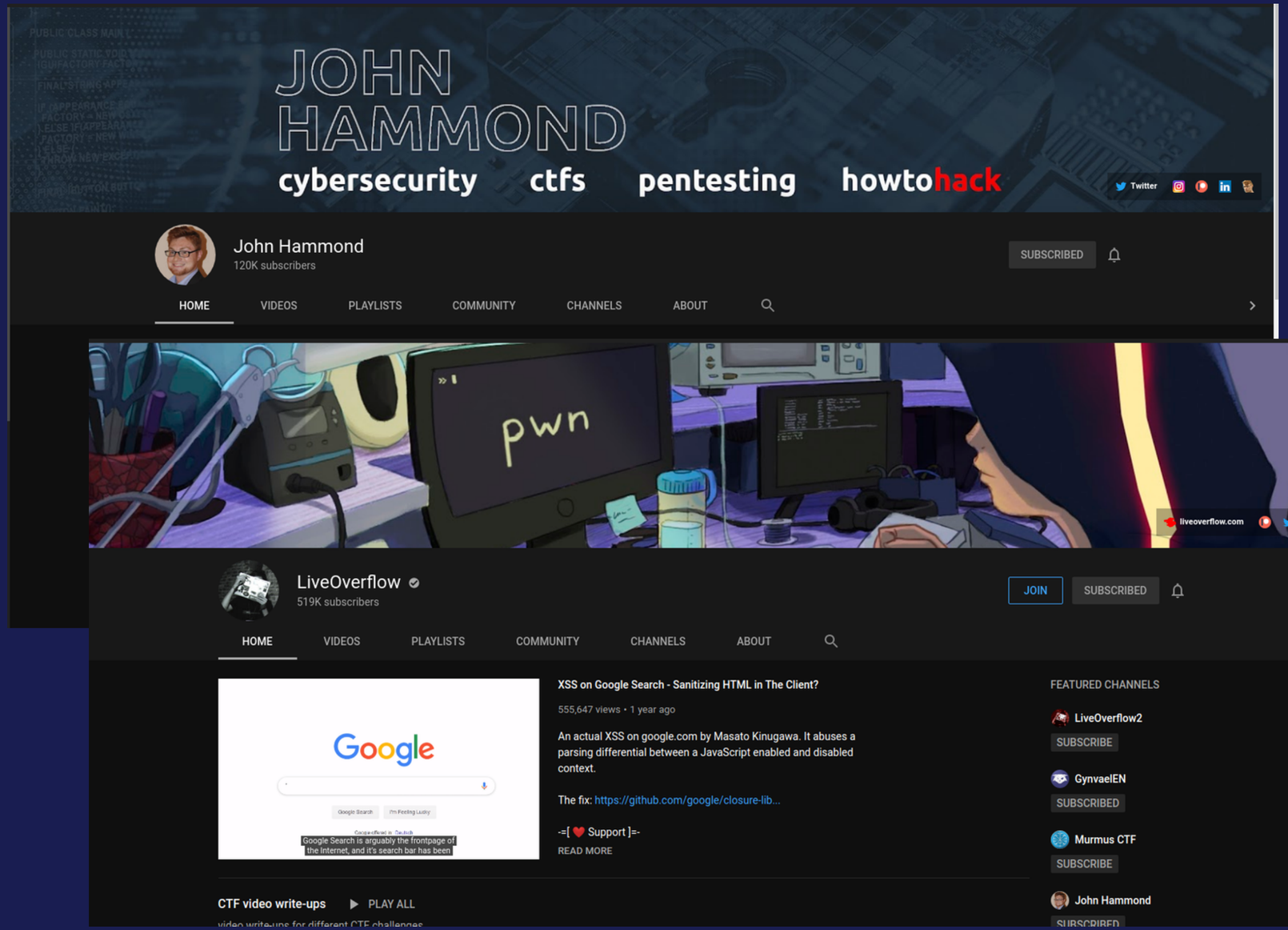
https://ctf101.org/ - CTF 101



Learning source

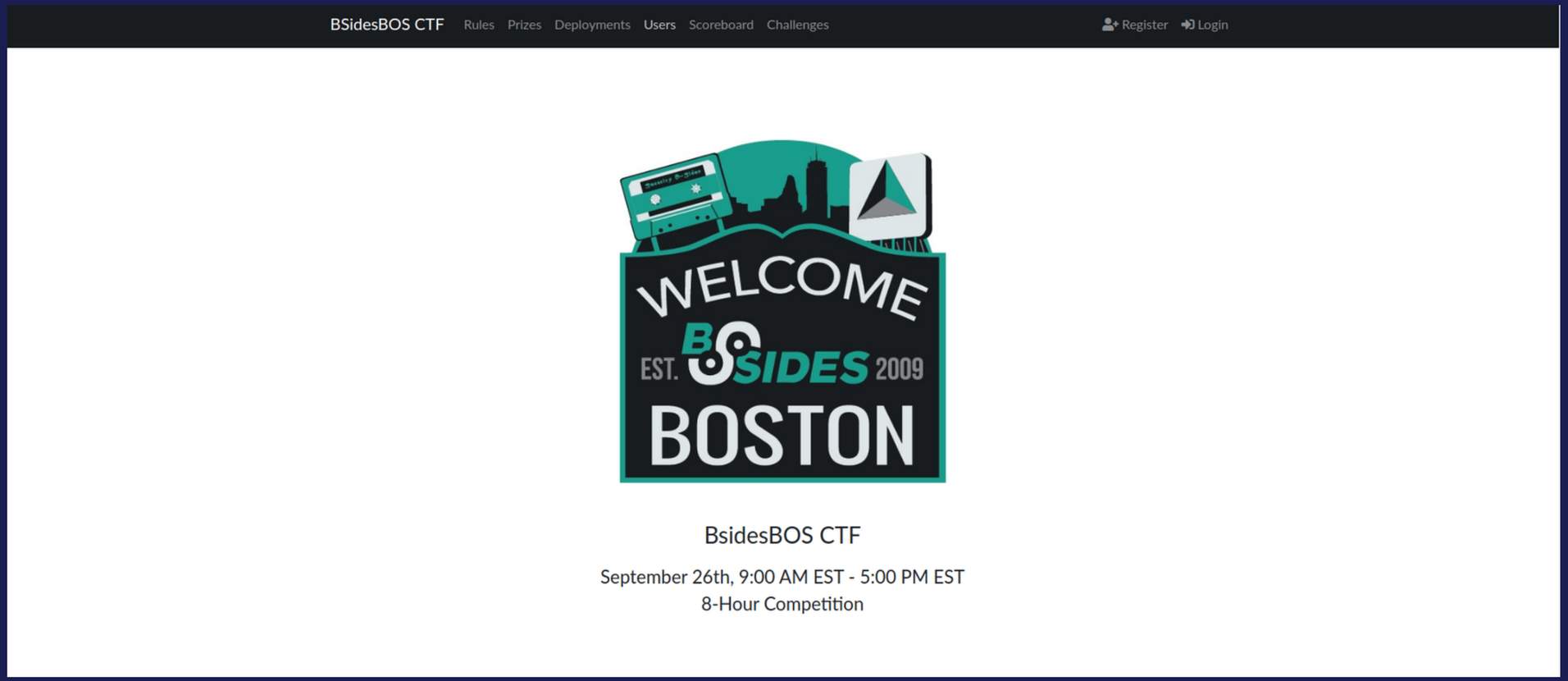
https://www.youtube.com/user/RootOfTheNull - John Hammond

https://www.youtube.com/channel/UClcE-kVhqyiHCcjYwcpfj9w - LiveOverflow



Try it out!

https://bsidesbos.ctf.games/



And we're done for the day!

See you in another episode of Road to Battle of Hackers!!