



Road to Battle of Hackers 2020: Introduction to CTF

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

#H4CKFROMHOM3 #SAFEMODE





\$ whoami



FSEC-SS 2020

S Y S T E M A N A L Y S T I N T E R N @ T O P N O T C H C O M P U T E R S

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

C O M M I T T E E @ F S E C - S S 2 0 2 0

basically the reason why im here

V I C E P R E S I D E N T @ I N D O N E S I A N S T U D E N T S O C I E T Y

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)

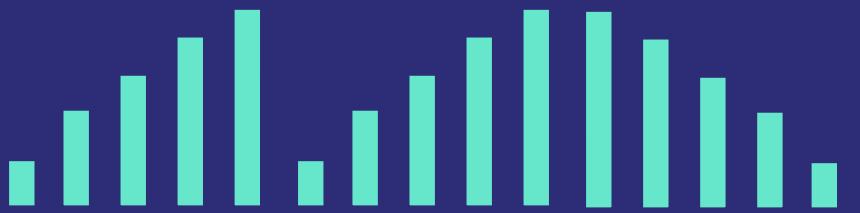
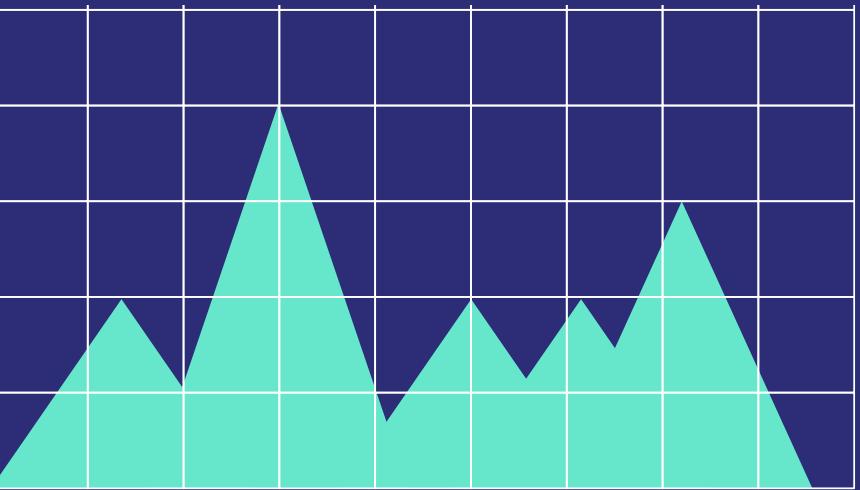
- Setting up your hacking box
- Linux 101
- Solving Some Challenges



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 defend 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.





Jeopardy CTF Challenges



Forensics

Data recovery,
Steganography,
Network Analysis

R E C A P →



Binary Exploitation

Buffer Overflow,
Format String

R E C A P →



Reverse Engineer

Reverse Engineering
Binary/Executables

R E C A P →



Web

XSS, SQLi, Cookies,
JWT

R E C A P →



Crypto

ROT13 to RSA

R E C A P →



Miscellaneous

Fun Stuff, General
Knowledge,
Programming

R E C A P →



Challenge Problems

Score: 13650

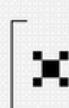
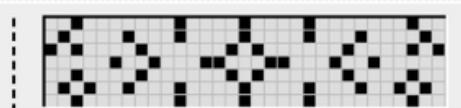
Progress Tracker

Search

name category score

Categories

Only Binary Exploitation

ins3cure
Logout Team

ANNOUNCEMENTS (17)

1011.23
302.03T-0h
16/09/2020

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

Scoreboard

My Team



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.

The image is a collage of screenshots from several cybersecurity-related websites:

- HackTheBox:** Shows a user profile for "Ncaps" with a rank of "Pro Hacker". It includes sections for Dashboard, Rules, Support, Education, Careers, Rankings, and Labs.
- TryHackMe:** Shows a challenge titled "Configuring neural network" with a streak of 0 and 2517 users online.
- VulnHub:** Shows a "Dashboard" for "Virtual Machines". It lists four challenges: "Chili: 1", "Tomato: 1", "Potato (SunCSR): 1", and "Monitoring: 1". Each challenge card includes a thumbnail image, difficulty level, test environment, and a "more..." link.
- Nagios XI:** Shows a "Welcome" screen for the Nagios XI platform.



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?

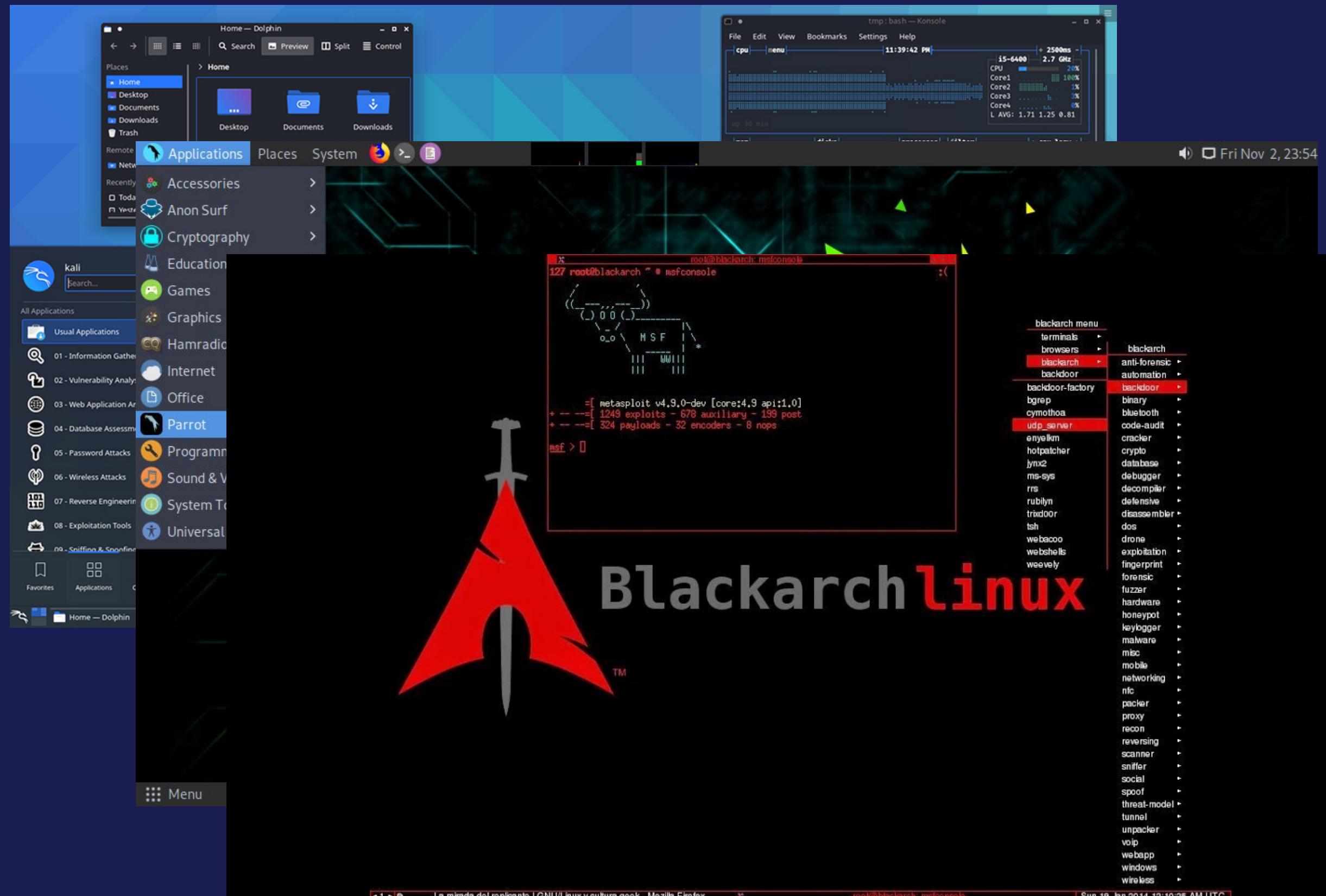
1. Highly Costumizable
2. Arguably more secure
3. A lot of hacking tools
designed for linux
4. There are distros
specifically designed for
hacking/pentest

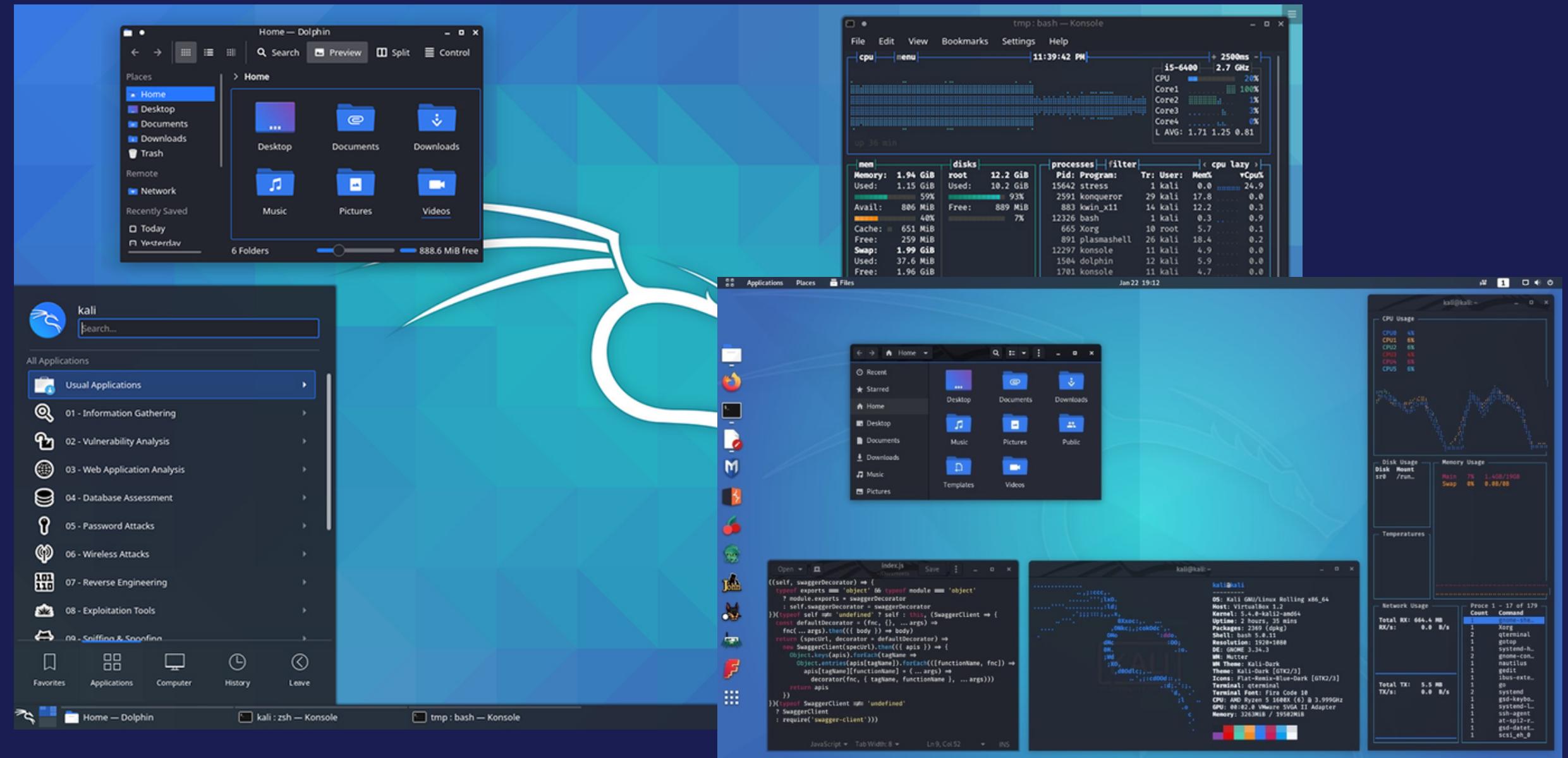


Hacking Distros

- 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.



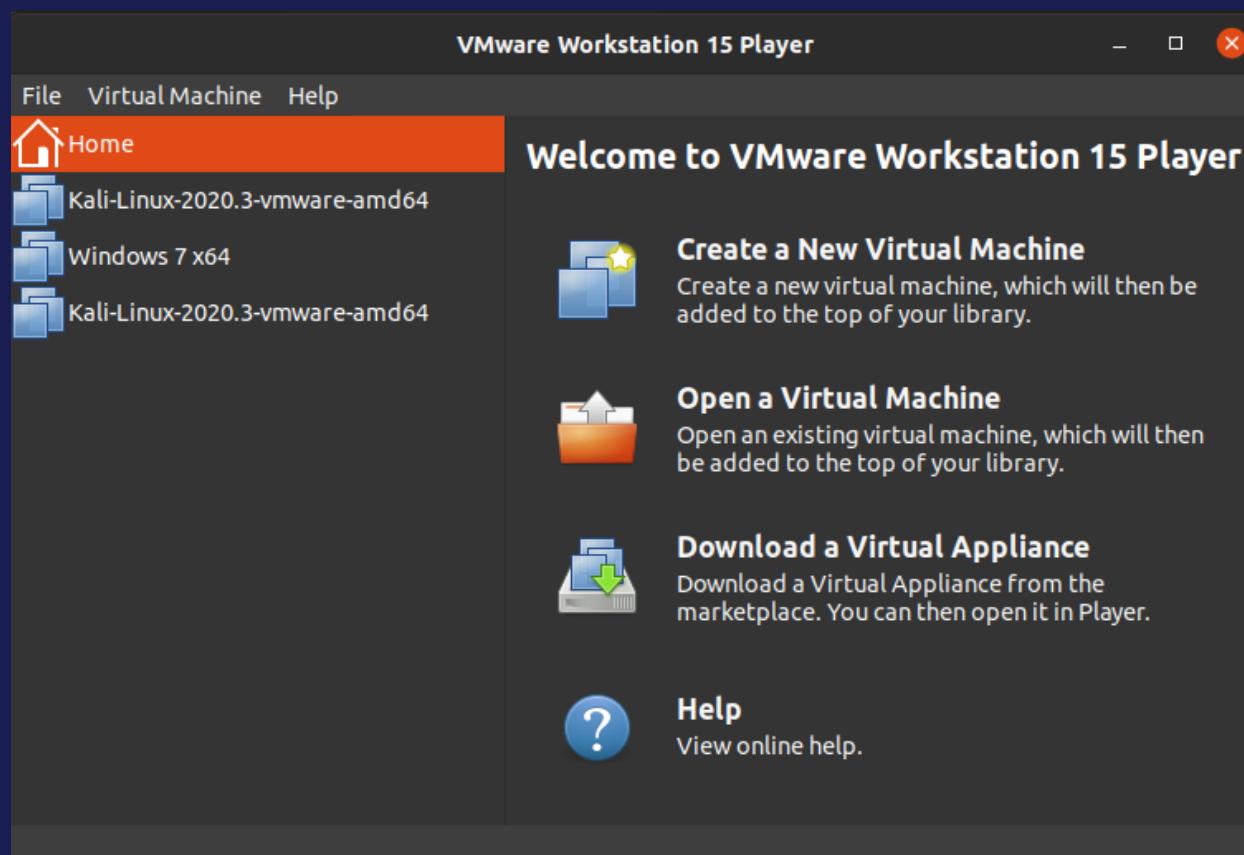
Why?

- 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.



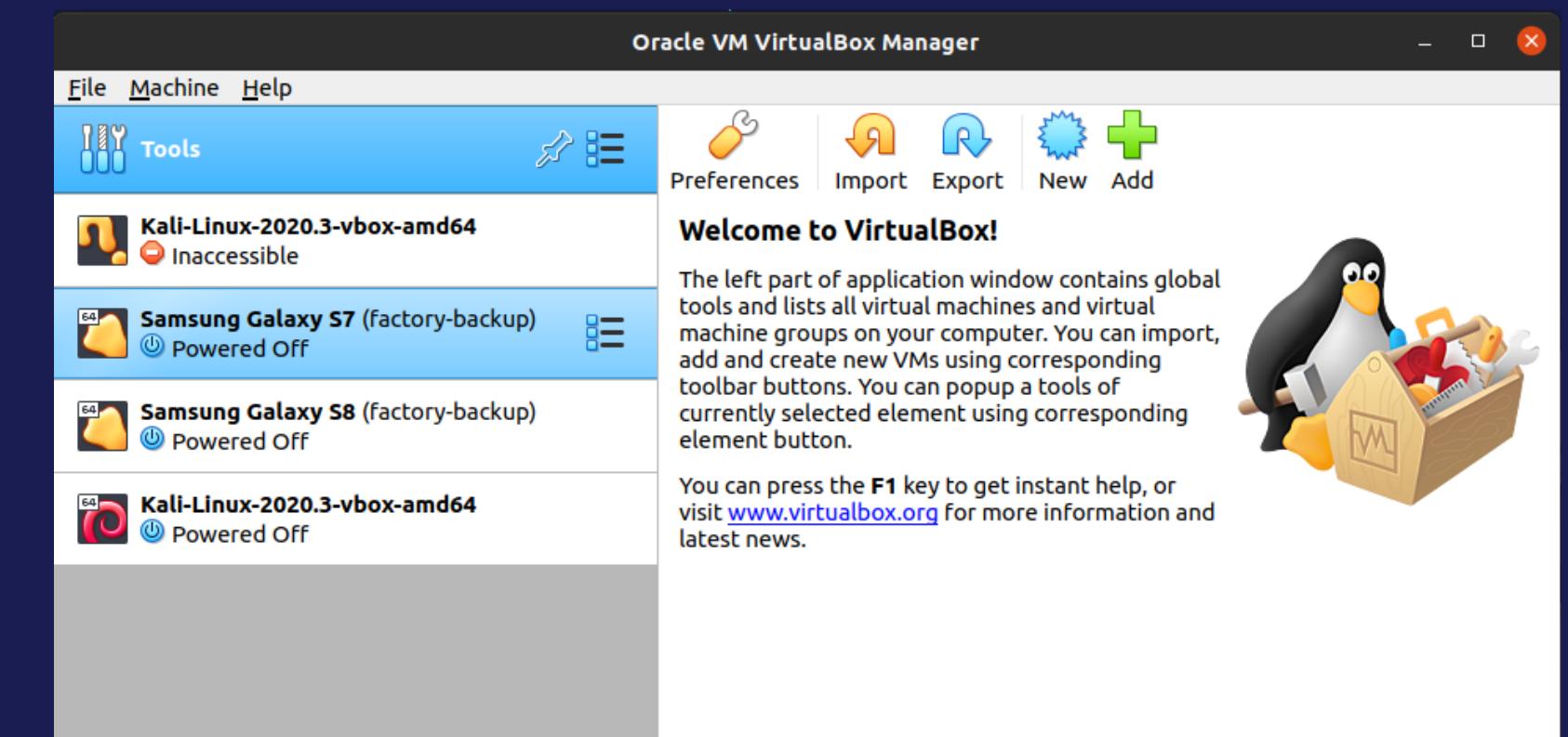
For Windows

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

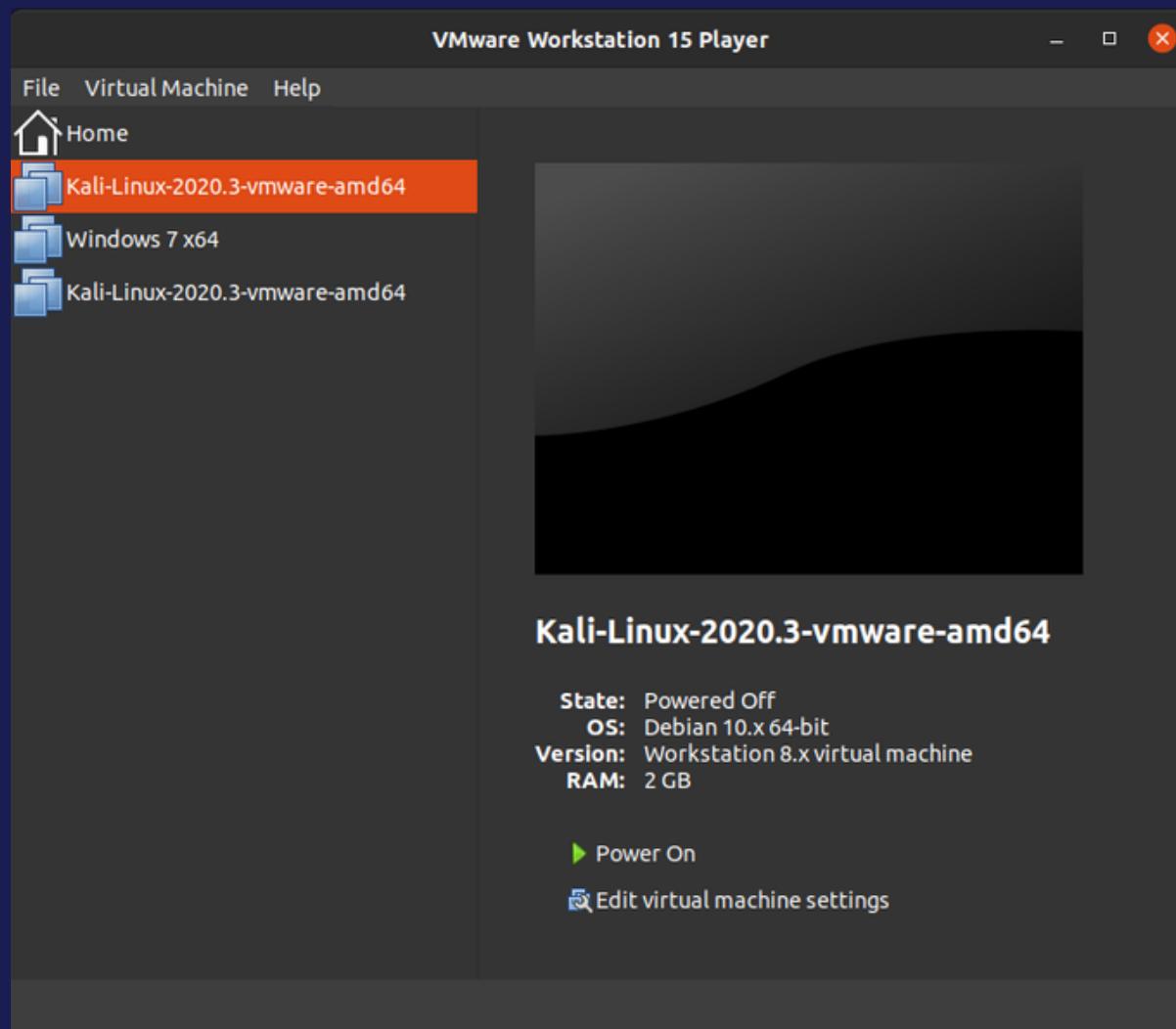
1. **Unzip everything**
2. **Install the VirtualBox by double clicking the .dmg file**
3. **Go to 'Tools' and Click 'Import' and load the .ova file**





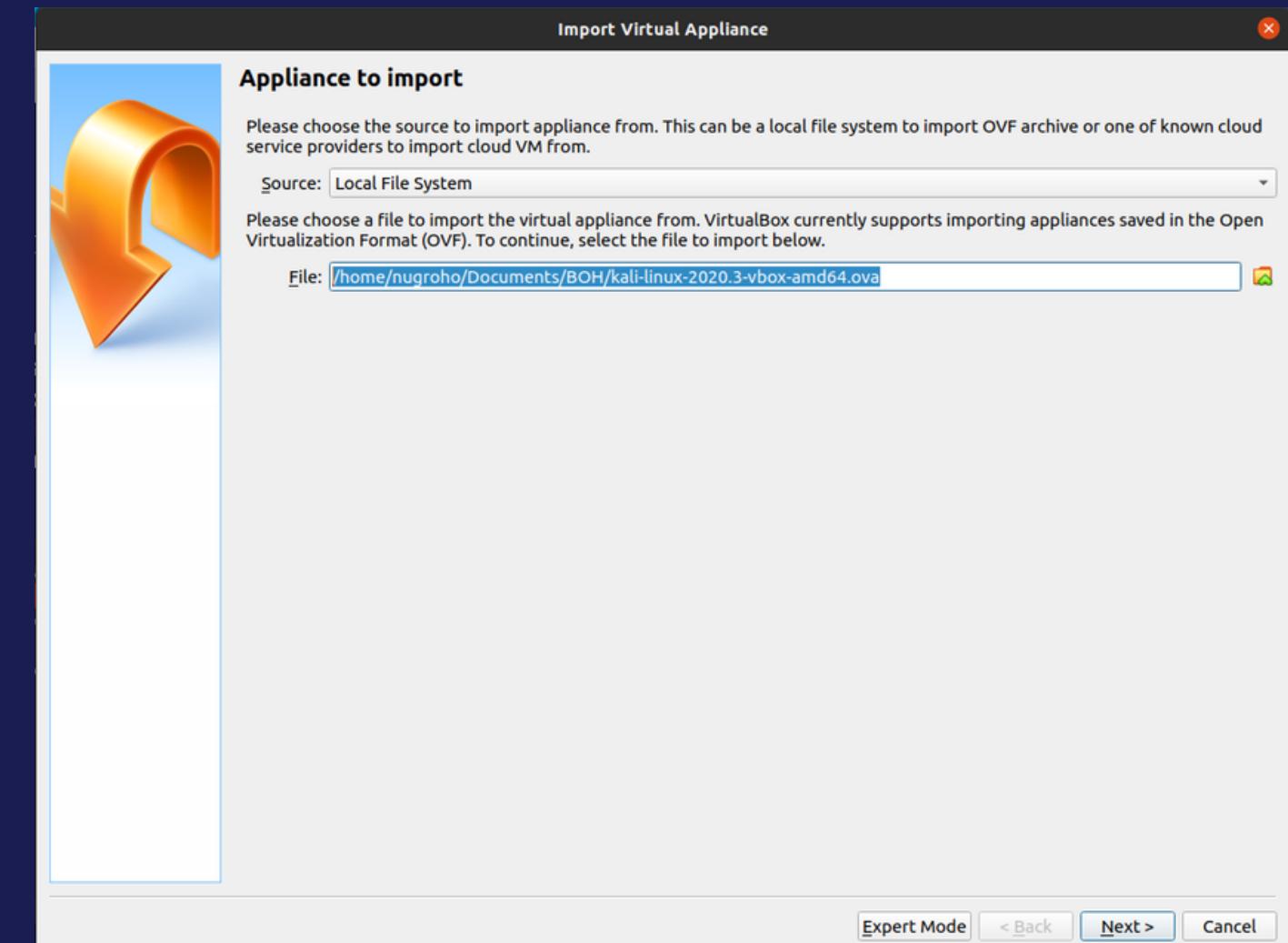
For Windows

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**



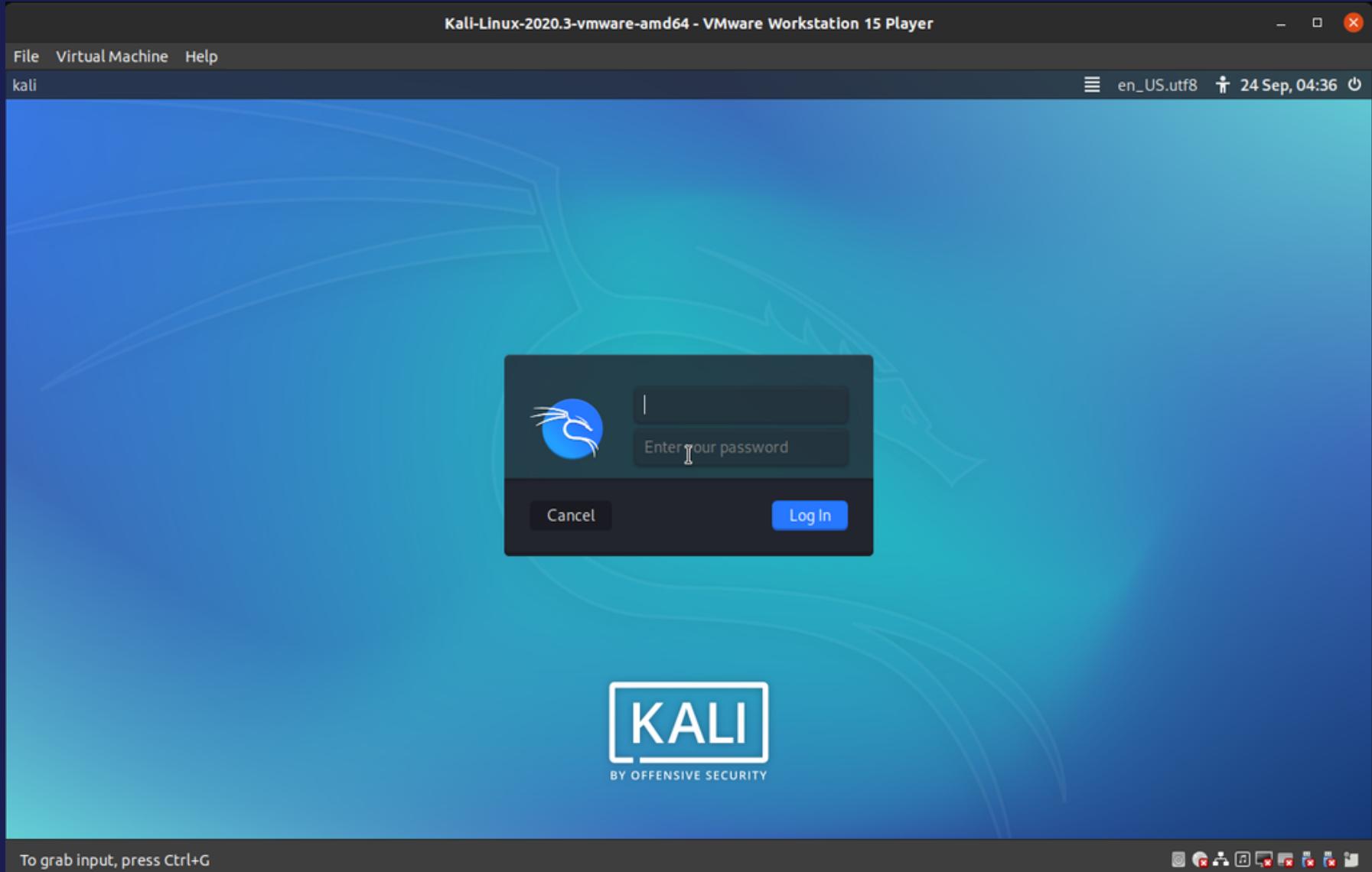


Keep clicking
next till it's done

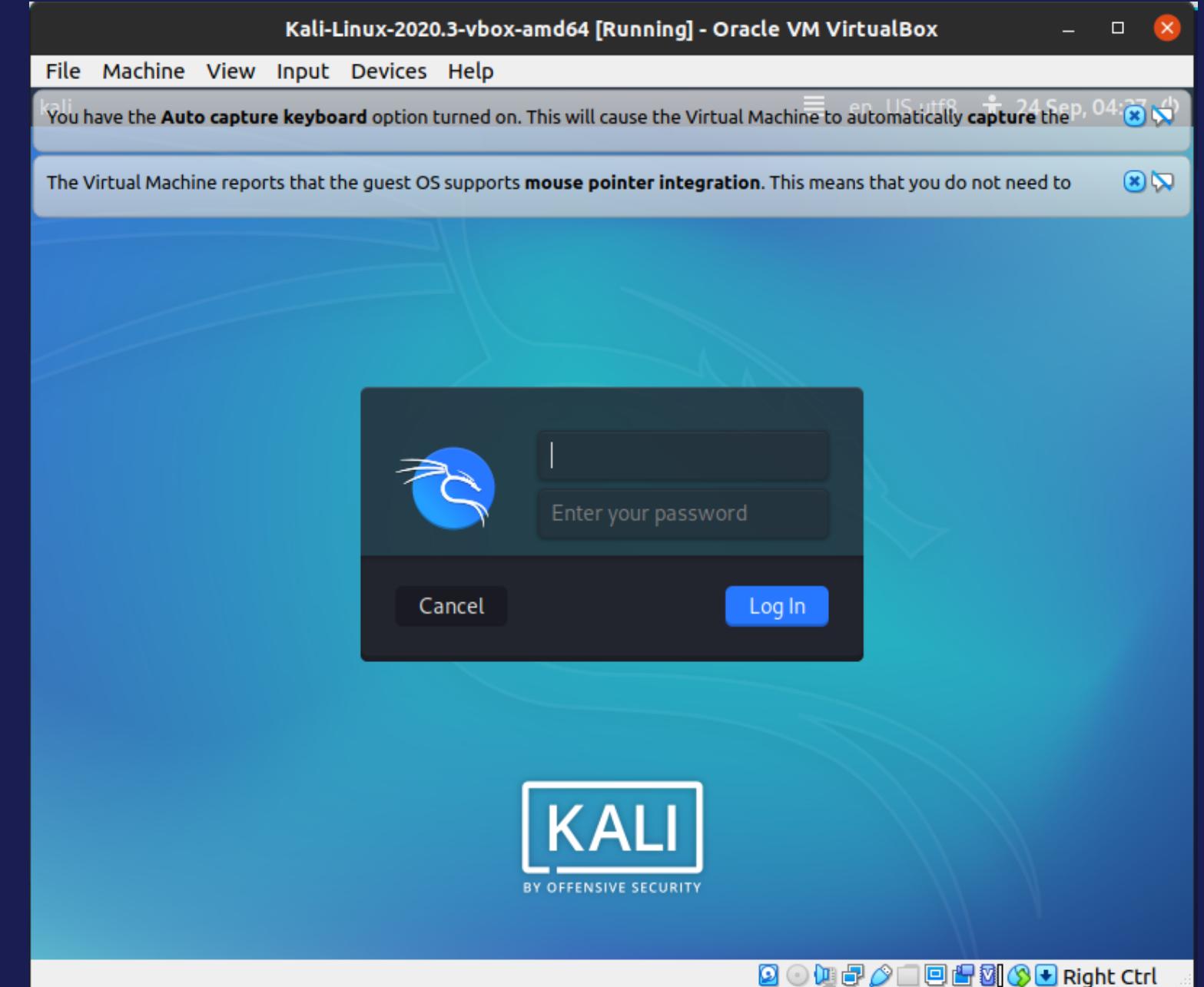




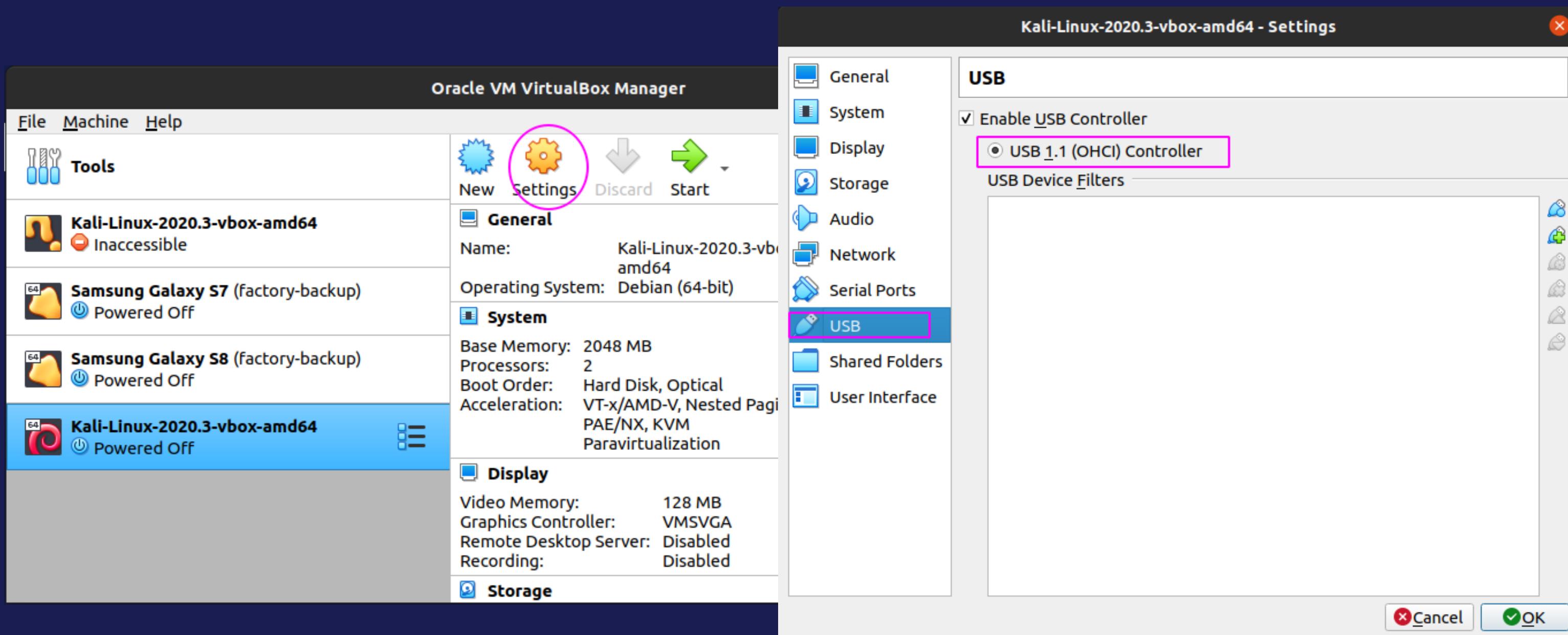
For Windows



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



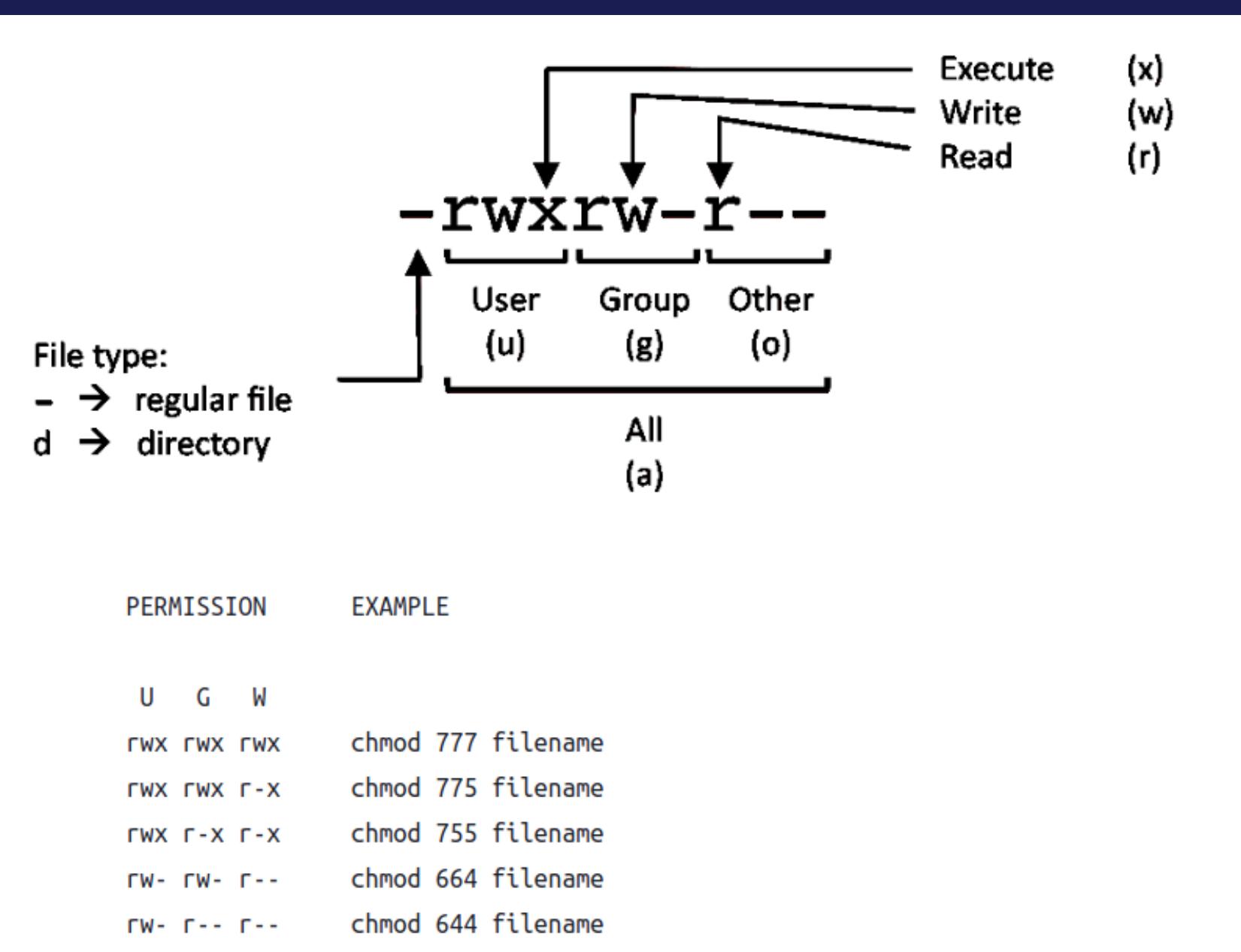
Root Privilege

Admin privilege named 'root'



\$File Permission

What you can do
with the files





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

```
kali㉿kali:~$ mkdir yourname
kali㉿kali:~$ ls
Desktop      Downloads    Pictures    Templates   yourname
Documents    Music        Public      Videos     youtube
kali㉿kali:~$ mv yourname/ Documents/
kali㉿kali:~$ cd Documents/
kali㉿kali:~/Documents$ ls
qc  yourname
kali㉿kali:~/Documents$ █
```

Datacenter.-
ovpn





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$ █
```

Terminal & Command

cd, ls, pwd and all kind of thing

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

This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use. [Learn more](#)

Visual Studio Code Docs Updates Blog API Extensions FAQ

Search Docs Download

Version 1.49 is now available! Read about the new features and fixes from August.

Download Visual Studio Code

Free and built on open source. Integrated Git, debugging and extensions.

 [Windows](#)
Windows 7, 8, 10

 [.deb](#)
Debian, Ubuntu

 [.rpm](#)
Red Hat, Fedora, SUSE

[.zip](#)
User Installer
System Installer
.tar.gz

[.deb](#)
64 bit 32 bit ARM

[.rpm](#)
64 bit

[.tar.gz](#)
64 bit

[Snap Store](#)



Let's install an IDE

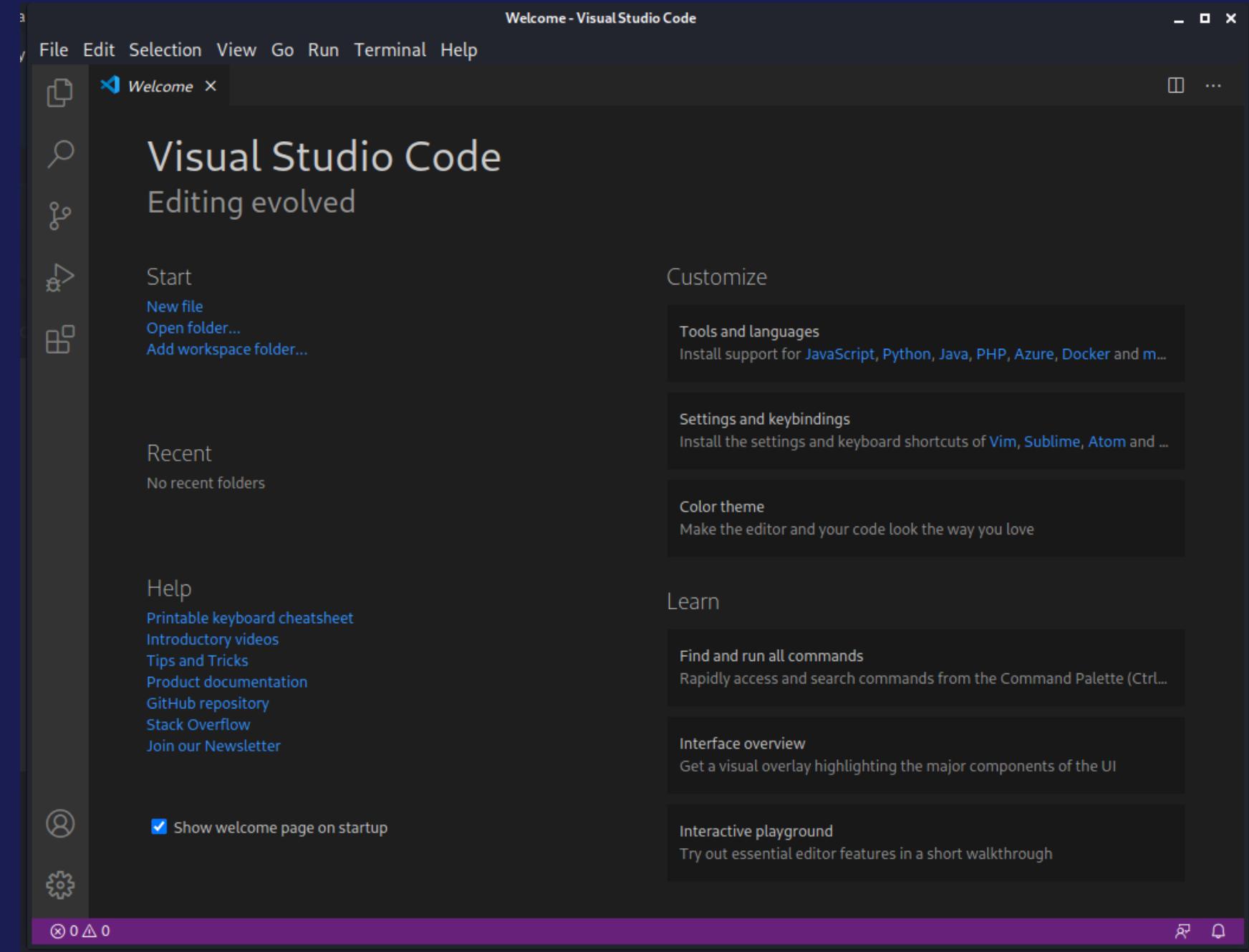
1. INSTALL FROM TERMINAL WITH THE COMMAND:
`sudo dpkg -i <file name>`

```
kali@kali:~/Downloads$ ls
burpsuite_community_linux_v2020_9_1.sh  code_1.49.2-1600965325_amd64.d
kali@kali:~/Downloads$ sudo dpkg -i code_1.49.2-1600965325_amd64.deb
Selecting previously unselected package code.
(Reading database ... 267333 files and directories currently installed)
Preparing to unpack code_1.49.2-1600965325_amd64.deb ...
Unpacking code (1.49.2-1600965325) ...
Setting up code (1.49.2-1600965325) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for mime-support (3.64) ...
kali@kali:~/Downloads$
```



Let's install an IDE

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





OK

LET'S HAVE A BREAK



LET'S
Jump into it!



A screenshot of a web browser window titled "Awesome!" showing the URL "http://128.199.155.55:8000/". The browser has orange-themed UI elements. The page itself is white and features the "CTFd" logo, which consists of the letters "CTFd" in a large, bold, black font. The letter "d" is stylized to look like a flag with a red base and a white top, featuring a small keyhole icon. Below the logo, the text "A cool CTF platform from ctfd.io" is displayed. Underneath that, there is a section titled "Follow us on social media:" with icons for Twitter, Facebook, and GitHub. At the bottom of the page, a blue link reads "Click here to login and setup your CTF".

Road to BOH Users Scoreboard Challenges [+ Register](#) [Login](#)

CTFd

A cool CTF platform from [ctfd.io](#)

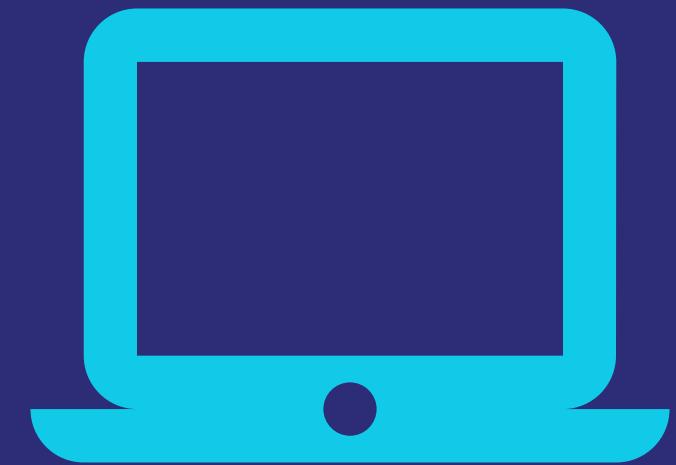
Follow us on social media:

[Click here to login and setup your CTF](#)

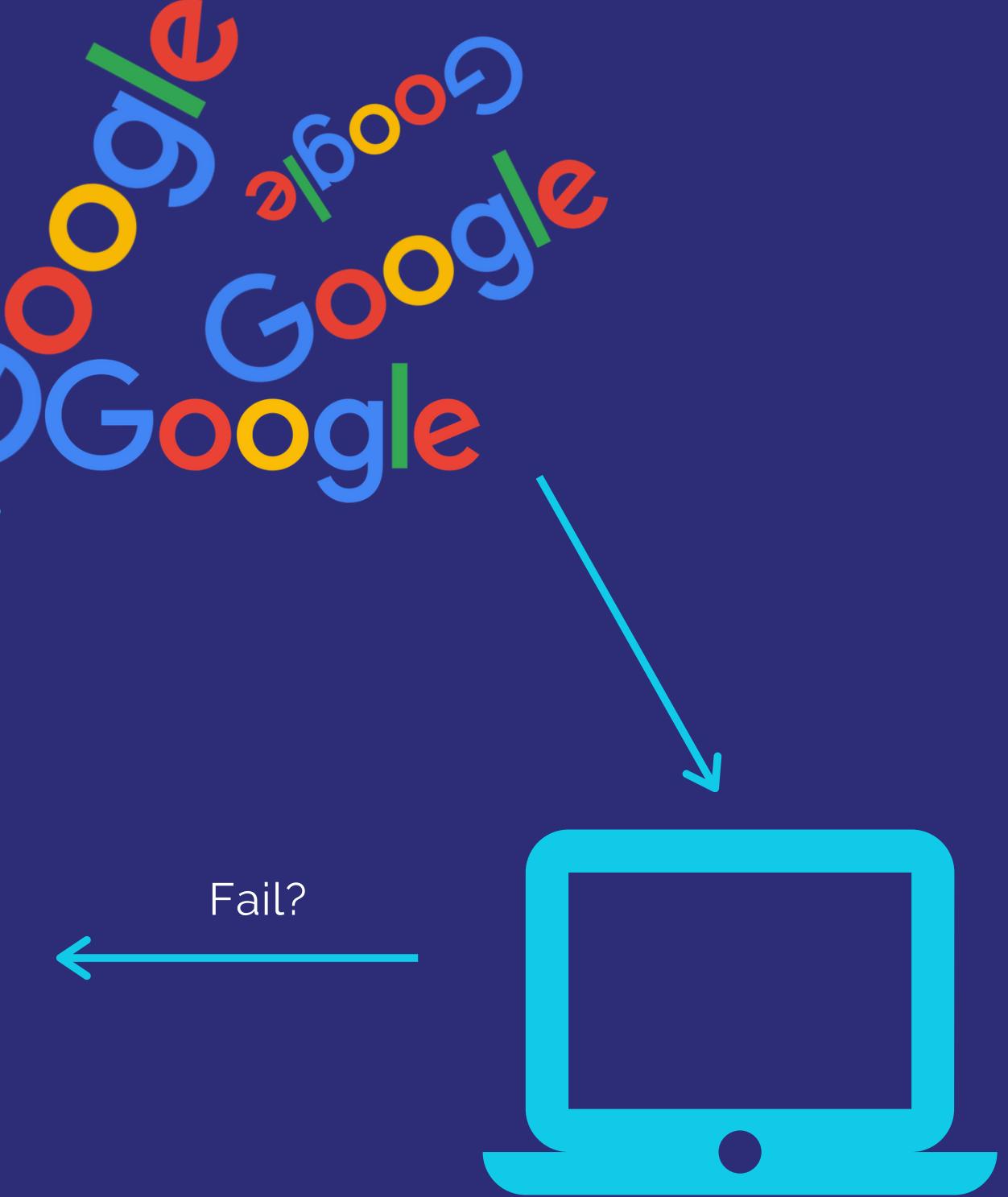


How to solve challenges in CTF?

Short answer. Research!



Analyze and read the challenge



Try whatever you've found on google



Learning source

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

<https://ctf101.org/> - CTF 101

The screenshot shows a Google Chrome browser window with several tabs open. The active tab is github.com/JohnHammond/ctf-katana. The page displays the README.md file for the CTF-Katana project, which is described as a "Capture The Flag 101" guide. The page includes sections for Welcome, Forensics, Cryptography, Web Exploitation, Reverse Engineering, and Binary Exploitation, each with corresponding icons. A navigation bar at the top of the page includes links for CTF 101, Forensics, Cryptography, Web Exploitation, Reverse Engineering, and Binary Exploitation. The CTF 101 logo is visible in the top left corner of the page content.

JohnHammond/ctf-katana: This repository aims to hold suggestions (and hopefully/eventually code) for CTF challenges. The "project" is nicknamed Katana. - Google Chrome

github.com/JohnHammond/ctf-katana

README.md

CTF-Katana

John Hammond | February 1st, 2018

CTF > 101 Forensics Cryptography Web Exploitation Reverse Engineering Binary Exploitation

Capture The Flag 101

Welcome

Capture The Flags, or CTFs, are a kind of computer security competition. Teams of competitors (or just individuals) are pitted against each other in a test of computer security skill. Very often CTFs are the beginning of one's cyber security career due to their team building nature and competitive aspect. In addition, there isn't a lot of commitment required beyond a weekend. In this guide/wiki/handbook you'll learn the techniques, thought processes, and methodologies you need to succeed in Capture the Flag competitions.

 Forensics
 Cryptography
 Web Exploitation
 Reverse Engineering
 Binary Exploitation

A project by the OSIRIS Lab at The NYU Tandon School of Engineering and CTFd LLC



Learning source

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

<https://www.youtube.com/channel/UClxE-kVhqiHCcjYwcpfjgw> - LiveOverflow

The screenshot shows the YouTube channel page for "JOHN HAMMOND". The channel banner features a dark background with a circuit board pattern and the text "JOHN HAMMOND" in large white letters, with "cybersecurity", "ctfs", "pentesting", and "howtohack" below it. The channel has 120K subscribers. The main video thumbnail is from a cartoon showing a character working on a computer with the word "pwn" displayed on the screen. Below the video, there's a thumbnail for a video titled "XSS on Google Search - Sanitizing HTML in The Client?" by "LiveOverflow". The thumbnail shows a Google search interface with a exploit message. The "LiveOverflow" channel has 519K subscribers. The page also includes sections for featured channels like "LiveOverflow2", "GynvaelEN", "Murmus CTF", and "John Hammond".

Try it out!

<https://bsidesbos.ctf.games/>

BsidesBOS CTF Rules Prizes Deployments Users Scoreboard Challenges [Register](#) [Login](#)



WELCOME
EST. BSIDES 2009
BOSTON

BsidesBOS CTF

September 26th, 9:00 AM EST - 5:00 PM EST
8-Hour Competition



And we're done
for the day!

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