Session's main points:

- Attack and defence. (what does my enemy have?)
- Ethics is number one. (don't fall in haram; you can just be the leader and teach others these ethics)
- Network analysis: Devices that are working on the same network. (IP address - penetration testing)
- The philosophy of computers is you! (input and output)
- Rule number 1 to being an expert is to build a strong base
- It is all about social engineering (it could be physically through a flash memory) to fall in a hack.
- You have to be the WHITE hacker.
- In the beginning, we have to be VERY simple in the basics to process all the info in an exemplary manner.
- You are free when we go to the top. (penetration web-attack || network security)
- Everything in our life is involved in duality (0, 1) {why that and what will happen if that happens} like the compiler (assembly → assembler → Hexa → language).
- Disk partitions of the Linux → homedir - root user - swap area.

Introduction to CyberS

Information Warfare: It refers to using information and communication technologies (ICT) to acquire competitive advantages over an opponent.

We have 2 types of information warfare:

1- **Defensive information warfare**: It refers to all the strategies and actions designed to defend against attacks on ICT assets.

{e.g., Prevention – Deterrence – Alerts – Detection – Emergency Preparedness – Response.}

2- **Offensive information warfare**: It refers to the attacks against the ICT assets of an opponent.

{e.g., Web applications attacks – Web server attacks – Malware attacks – MITM attacks – system hacking.}

- We will delve deeper into each of these examples in the upcoming sessions after learning the Linux commands.

Hacker Classes:

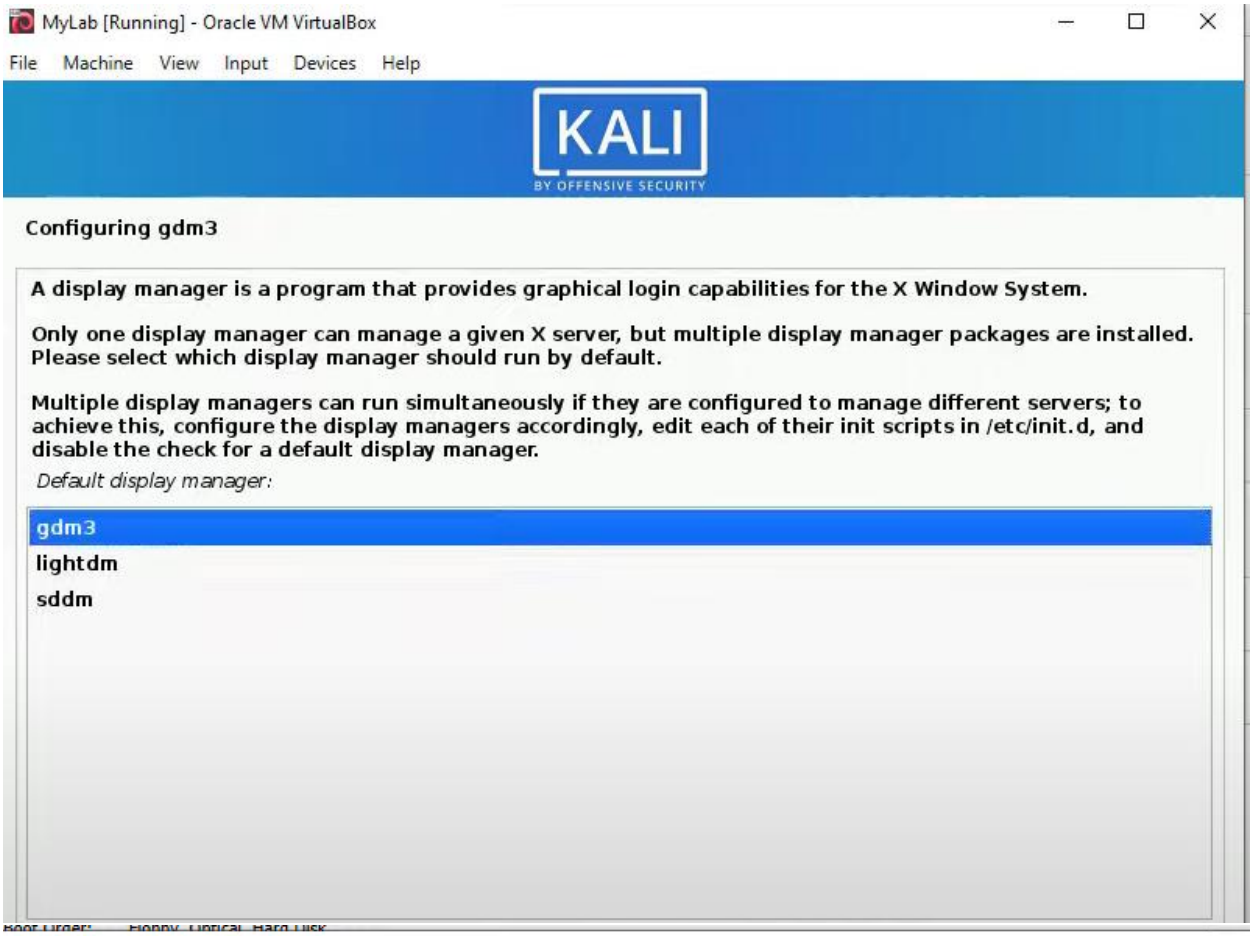
1- **Black Hats:** Individuals with advanced skills; they resort to destructive activities (**Crackers)**
2- **White Hats:** Individuals who use their advanced skills for defensive purposes (**System analysts)**; they have permission from their boss.
3- **Gray Hats:** Individuals who both work both offensively and defensively.
4- **Suicide Hackers:** Individuals who focus on bringing down the critical infrastructure for a cause and are not worried about-facing jail terms.
5- **Script Kiddies:** Individuals who do not have skills; they copy the scripts that real hackers developed to run it on their software.
6- **Cyber Terrorists:** Individuals with advanced skills who are motivated by political beliefs to create fear through the computer networks of their target.
7- **State-Sponsored Hackers:** Individuals employed by the government to penetrate and acquire top-secret information from and harm the information systems of other governments.
8- **Hacktivists:** Individuals who promote social change by hacking. (e.g., disabling websites)

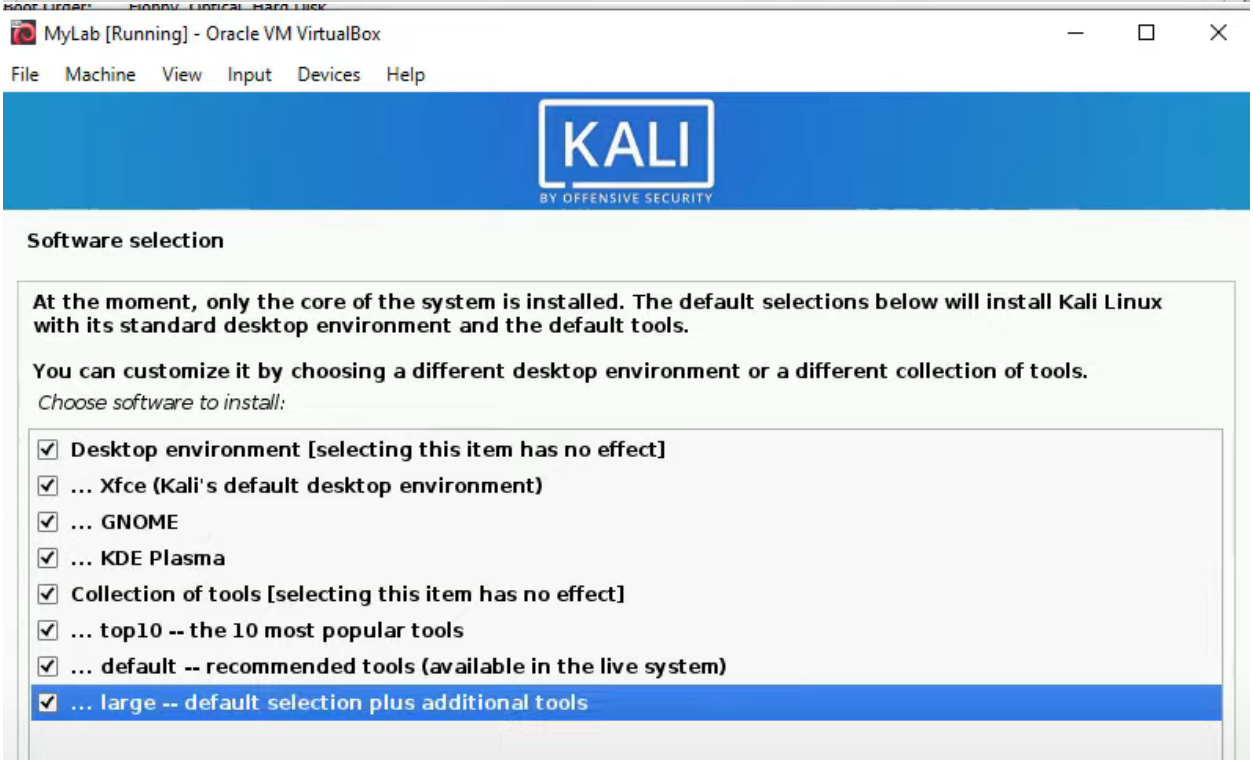
Defense-in-depth layers:

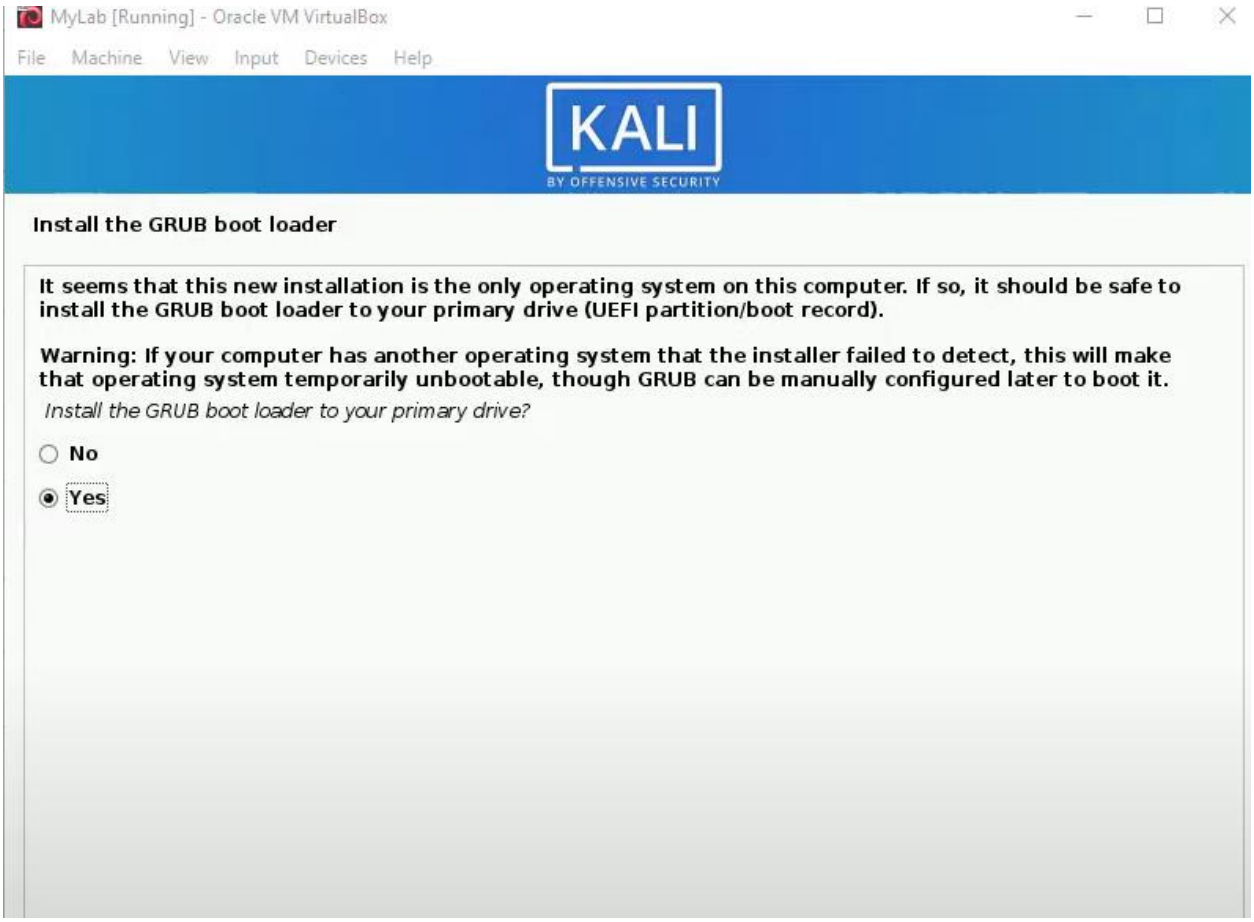
Policies < Physical < Perimeter < internal network < host < application < **DATA**

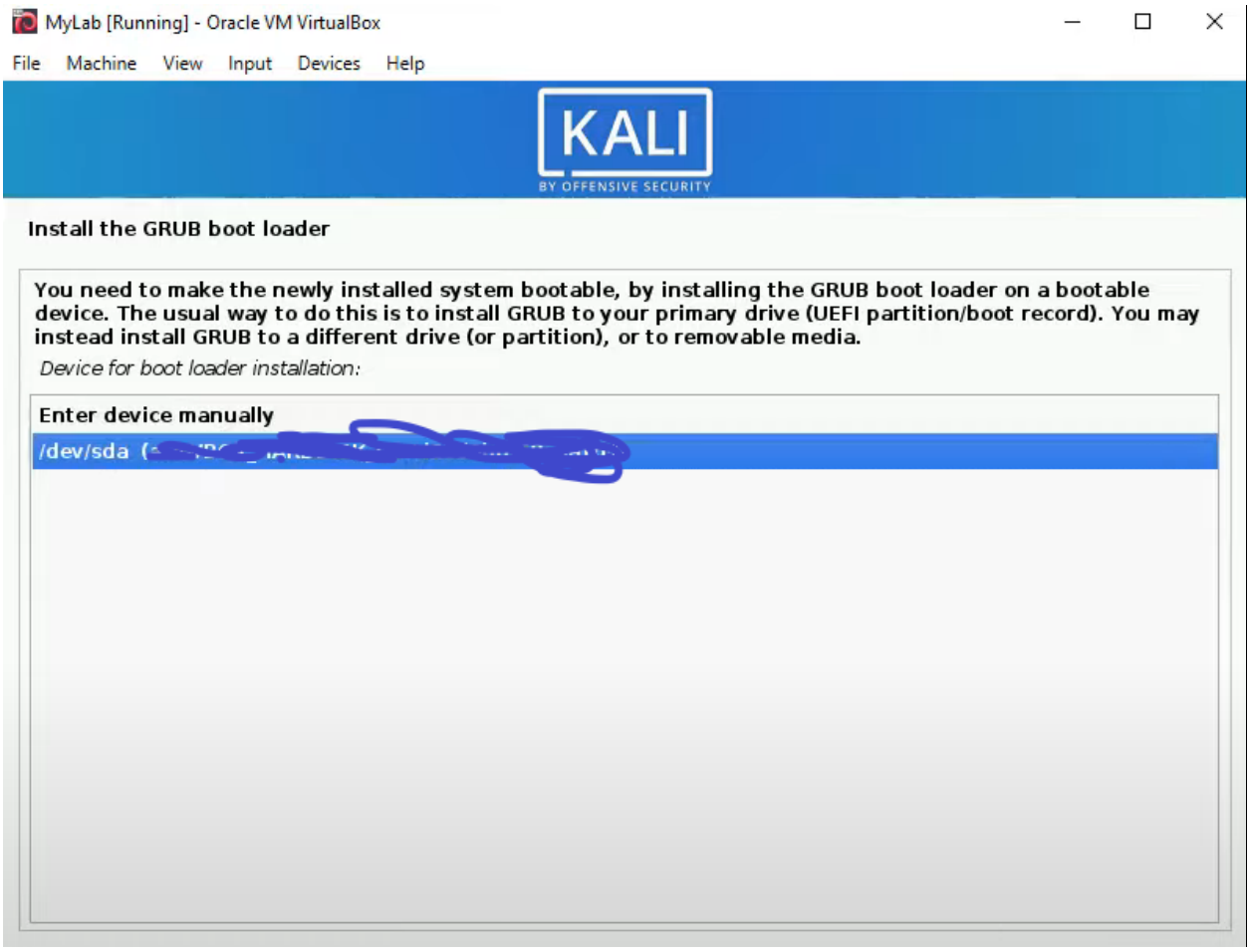
Now it is time to install our Linux softwares

Download the following files: http://old.kali.org/kali-images/kali-2020.4/kali-linux-2020.4-installer-amd64.iso
https://www.virtualbox.org/wiki/Downloads


MyLab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
BY OFFENSIVE SECURITY
Configuring gdm3
A display manager is a program that provides graphical login capabilities for the X Window System.
Only one display manager can manage a given X server, but multiple display manager packages are installed. Please select which display manager should run by default.
Multiple display managers can run simultaneously if they are configured to manage different servers; to achieve this, configure the display managers accordingly, edit each of their init scripts in /etc/init.d, and disable the check for a default display manager.
Default display manager:
gdm3
lightdm
sddm


MyLab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
BY OFFENSIVE SECURITY
Software selection
At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.
You can customize it by choosing a different desktop environment or a different collection of tools.
Choose software to install:
Desktop environment [selecting this item has no effect]
... Xfce (Kali's default desktop environment)
... GNOME
... KDE Plasma
Collection of tools [selecting this item has no effect]
... top10 -- the 10 most popular tools
... default -- recommended tools (available in the live system)
... large -- default selection plus additional tools


MyLab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
BY OFFENSIVE SECURITY
Install the GRUB boot loader
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).
Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to your primary drive?
No
Yes


MyLab [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
KALI
BY OFFENSIVE SECURITY
Install the GRUB boot loader
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.
Device for boot loader installation:
Enter device manually
/dev/sda