# ETHICAL HACKING

**INTRODUCTION TO ETHICAL HACKING**

. Basics of linux

. virtual box

.Kali linux> 64 bit installer iso file

.virtual box installer

virtual image > 64 bit

In chrome> type kali linux open the file download kali linux 64 bit kali linux installer. Then download virtual box / virtual box images. Then download virtual box seperate

Then open virtual box > Then click new option in that name , type , version:debian 64 ,click next ,then choose ur ram what u wanted , then next , create virtual hard disk, click finish.

Then in virtual box click settings then click storage in that thery will be an empty option then click virtual hard disk .Then select the iso file were u downloaded and click ok button.

Then click start button . Then click install option thenthe kali linux will be installed

1 what is hacking?

it is the use of a security weakness or vulnerability to gain the unwanted access to a system and to steal the personal data inside the system

2 what is vulnerability ?

vulnerability is acyber security term that refer flaw in a system that can leave it open to attack

There are five phases of methodology

. information gathering: it mean gathering information but non-technical information just to knowing about it

.network scanning:The collected non-technical information and findout technical information and capture more technical information .Then they combine both technical and non-technical information and findout is there any security weakness in the app or website......etc.... that is called security weakness

.vulnerability analysis:To find the entry point.If we find the entry point then we exploit into the website by using some codes

**SOCIAL ENGINEERING**

Social engineering is the art of hacking into human's mind

**KALI LINUX INSTALLATION**

Go to chrome then type virtual box download then go in to it . In that there will be downloading options(in windows:windows hosts,in linux: there will be linux options) then downlod it in windows host.After this we need an OVA file.Then type kali linux then go in to it.Then u can see an virtual machines option click in to it then u can see virtual box OVA file (virtual box 64bit,32bit).You can choose an option what ur computer support (virtual box 64bit). Then install virtual box

then double click an OVA file then u automatically go inside the virtual box .Then there adjust the RAM (minimum 4gb RAM) then import it and it will make some time to import the file. Then click the start button then it will automaticallly start.Then they will ask the username and password u can enter username and password kali then click enter u will go into kali linux.Then ur kali linux installation is complete.

NETWORKING BASICS

NETWORKING-ELECTRICITY IN COMPUTING

NETWORKING REFRESHER

1 What is a network?

.A computer is a digital telecommunications network for sharing resorces between computers.It is the connection between two or more devices.

2 What is the internet?

.A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

DIFFERENT TYPE OF NETWORKS

.LAN (Local Area Network): LAN connects group of computers together across short distance (within a building or between a group of two or three buildings in close proximitty to each other)to share information and resources

.WLAN (Wireless LAN): WLAN's functionality is same as the LAN difference is that WLAN make use of wireless communication technology.

.MAN (Metropolitan Area Network): MAN's span an entire geographic area (typically a town or city, but sometimes a campus.

.WAN (Wide Area Network): WAN connects computers together across longer physical distance. The internet is the most basic example of a WAN

.VPN (Virtual Private Network): VPN lets its users send and recieve data as if their devices were connected to the private network-even if they are not.

IP ADDRESS( Internet Protocol Address)

.IP Address: An internet protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the internet protocol for communication.

.There are two versions available in IP which are;

.IPV4

.IPV6

.IPV4 is introduced in 1981.

.Eg: 192.168.1.1 ex:(1-->ON--> high voltage

0-->OFF--> low voltage)

.An IPV4 address have two parts;

.Host portion

.Network portion

.These parts are determined using the subnet mask

**NUMBERING SYSTEM**

.A numbering system is asystematic method for representing numbers using a particular set of symbols

.Computer use binary numbering system (0,1) eg:(radics or base)

.In our day to day communication we use decimal numbering system(0,1,2,3,4,,5,6,7,8,9)

.Computers can't understand the decimal numbering so we need to convert them into binary.

**IP Address Coversation**

.As there are lot of method available for conversation you can choose one as per ur easiness. I will be using the subtraction method.

128 64 32 16 8 4 2 1

.First let's find out how this table is calculated.

.As we are converting from decimal to binary we will be calculated the power of 2 starting from 0. The 2 is used because it is the radix of binary numbering system.

**SUBNETTING**

.A subnetwork or subnet is a logical subdivision of an IP network . The practice of dividing a network into two or more network is called subnetting.

.Subnetting also allowws us to calculate the network ID and host ID

In IPV4 There are five classes: class A,B,C,D,E

**MAC Address**

.MAC address or Media Access Control address is the physical address of NIC(Network Interface Controller ) card. Using the MAC address we can identify a device in our local area network because MAC address are always unique.

**OSI Model**

. OSI --> Open Systen Interconnection model

. OSI is a great tool to learn about network

. OSI is introduced by ISO

OSI layers (there sre 7 types of layers)

.Application layer

. Browser , Email

. HTTP , SMPT , POP3 , etc.....

.Presentation layer

. Encryption & decription

. WMV, MP4, JPEG

.Session layer

Initiate, Manage, Terminate sessions

.Transport

.Deals with the transportation of the data.

.TCP and UDP

.Network

.IP addressing

.Routing

.Data Link

.Switching, MAC address

.Physical

.Data cables

TCP (Transmission Control Protocol)

. TCP(Tranmission Control Protocol) is a standard that defines how to establish and maintain a network conversation through which programs can exchange data

.TCP flags

.In TCP connection, flags are used to indicate a particular state of connection of a particular connection.

UDP (User Datagram Protocol)

.UDP (User Datagram Protocol) is a communication protocol that is primarily used for establishing low-latency and loss-tolerating connections between applications onthe internet

**LINUX BASICS**

**DEEP DRIVE INTO LINUX**

**LINUX**

.Do you like time travel?Then roll back to 1969. in 1969 Ken Thompson and Dennis Ritchie of Bell Laboratories created UNIX OS. It was writtern assembly language and later rewritten in C to make it protable and eventually it became a widely used OS

.After UNIX some reserchers created UNIX like-system such as BSD, MINIX. But they were lacking one important thing... kernel.

.The kernel is a computer prgm at the core of a computer's operating system with complete control over everything in the system. It is an integral part of any operating system

.In 1991 one of the brightest young fellow started devolping Linux Kernel.

.In 1991 he released the first version.

.The latest version of Linux is released was very recent,24 april 2020

.On the top of Linux Kernel developers around the global have created a lot of other distribution like Debian, Redhat, Fedora, Gentoo, Mint, Android etc...

**DEBIAN**

.Throughout the course we use kali linux, which is based on debian for the practical session.

.Debian is an operating system composed entirely of free and open-source software. It's widely known and has been in development for over 20 years. There are three branches that ypu can use, stable, Testing and Unstable.

.Kali Linux is Debian-derived Linux distribution designed for digital forensics and pentration testing. This OS maintained and funded by offensive security.

THE SHELL

.The shell is basically a prgm that takes your commands from the keybord and sends them to the operating system to perform

.In this course we will use the shell prgm bash (Bourne Again Shell)

.Thre are other shells available such as KSH,ZSH,TSCH

**FILESYSTEM OF LINUX**

./- The root directory of the entire filesystem hierachy,everything is nestled under this directory.

./bin- Essential rerady-to-run prgms(binaries), includes the most basic commands such as ls and cp.

./boot-Contains kernel boot loader files.

./dev-Devices files.

./etc- core system configuration directory, should hold only configuration files and not any binaries.

./home-Personal directories for user, holds your documents,files,settings etc.

./lib-Holds library files that binaries can use.

./media-Used as an attachment point for removable media like USB drives.

./mnt-Temporarily mounted filesystems.

./opt-Optional application software packages.

./proc-Information about currently running processes.

./root-The root user's home directory.

./run-Information about the running system since the last boot.

./sbin-Contains essential system binaries, usually can only be ran by root.

./tmp-Storage for temporary files

./usr-This is unfortunately named, most often it does not contain user file in the sense of a home folder. This is meant for user installed software and utilities

./var-Variable directory, it's used for system logging, user tracking, caches, etc. Basically anything that is subject to change all the time.

**DEEP DRIVE INTO LINUX-PART-2**

**Ethical Hacking Methodology**

**. INFORMATION..**

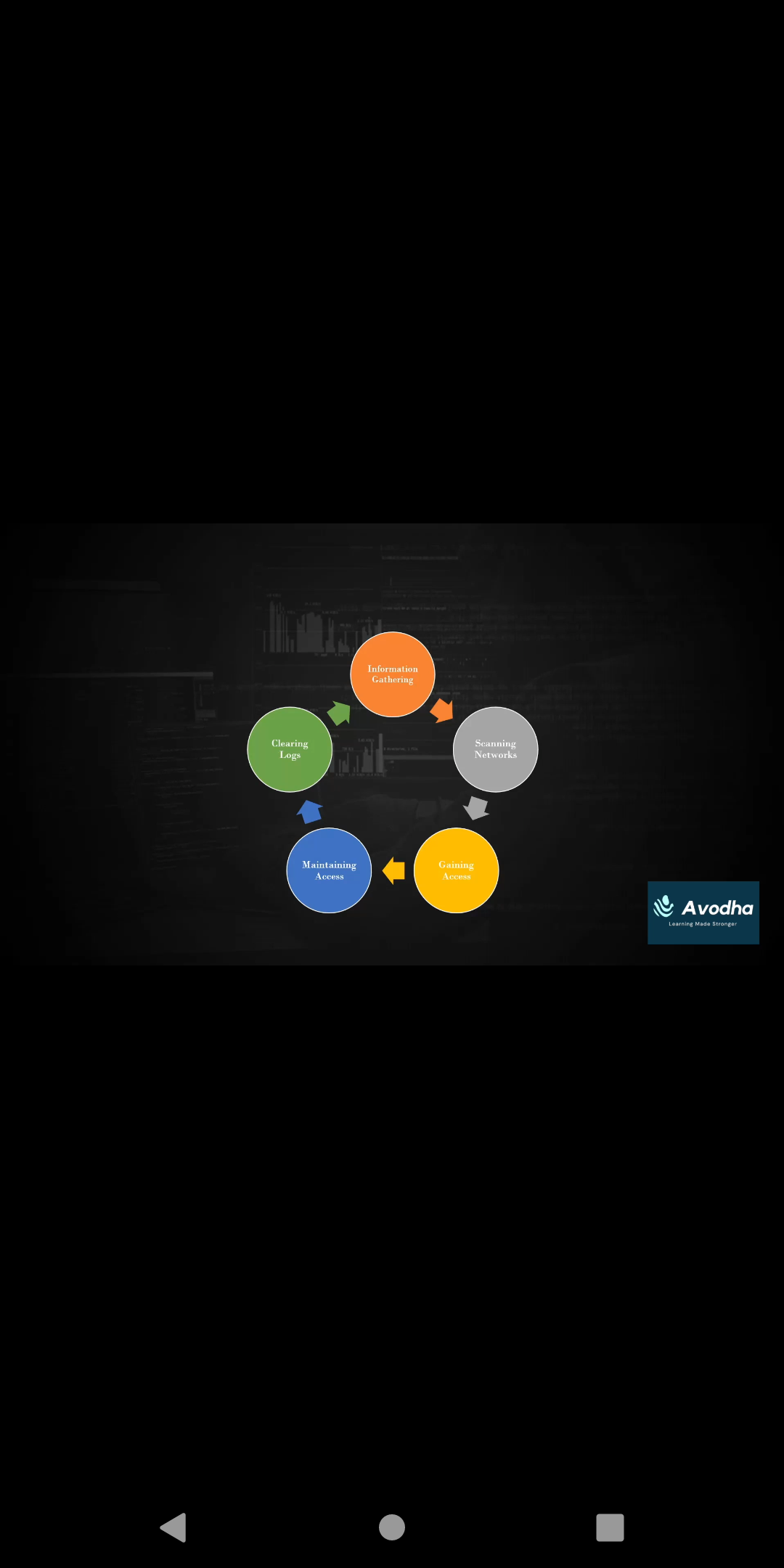
. Information is the money for our scenario..

. What we need?? MONEY

. Consider a tresure box, our money is hidden inside the tressure box so we need to gather it from the tresure box

. HOW? We will use a methodology to open our tressure box

.let's explore it.......



**INFORMATION GATHERING**

* We have seen our tressure box to open it first we need to find out the structure of that tressure box and its surrounding..;-)
* So we will look deeply into the environment so that we can get an idea about the box and we can reduce the focus area..
* We need to collect as much as possible information about our target.
* HOW? Using the public sources itself, we don’t have any secret places and we call this procedure OSINT (Open Source Intelligence).

**SCANNING NETWORKS**

* Now we have the outer structure of the tressure box but we are missing the important thing.. ”KEY”
* In ethical hacking our KEY is the “VULNERABILITY”, but from where we can get this??
* To get the KEY we need to find what are the services provided by our tressure box, what is the base of our tressure box.
* HOW? We will use some special communication using some famous tool..

**GAINING ACCESS**

* Yes!!!! We got the structure and key of the tressure box now we can open our tressure box and we can take our great tressure…
* In ethical hacking the OPEN means getting into the system as a normal user or admin.
* HOW? Here can use some specially crafted snippets of code or “exploits” to get into the machine..

**MAINTAINING ACCESS**

What will happen if I lost my KEY?:-(…

* Here the importance maintaining access comes. We need to maintain our access to the system
* HOW? Hackers use malicious software to maintain the access. We call the Trojan, Backdoors, Etc..

**CLEARING LOGS**

* Accessing a tressure box which is not yours is completely illegal so the hackers will clear the evidence from tressure box.

**DATA INTELLIGENCE(Information Gathering)**

What is data?

* **D**ata is distinct pieces of information, usually formatted in a special way.
* Eg : students names in a class are Data

**W**hat is information

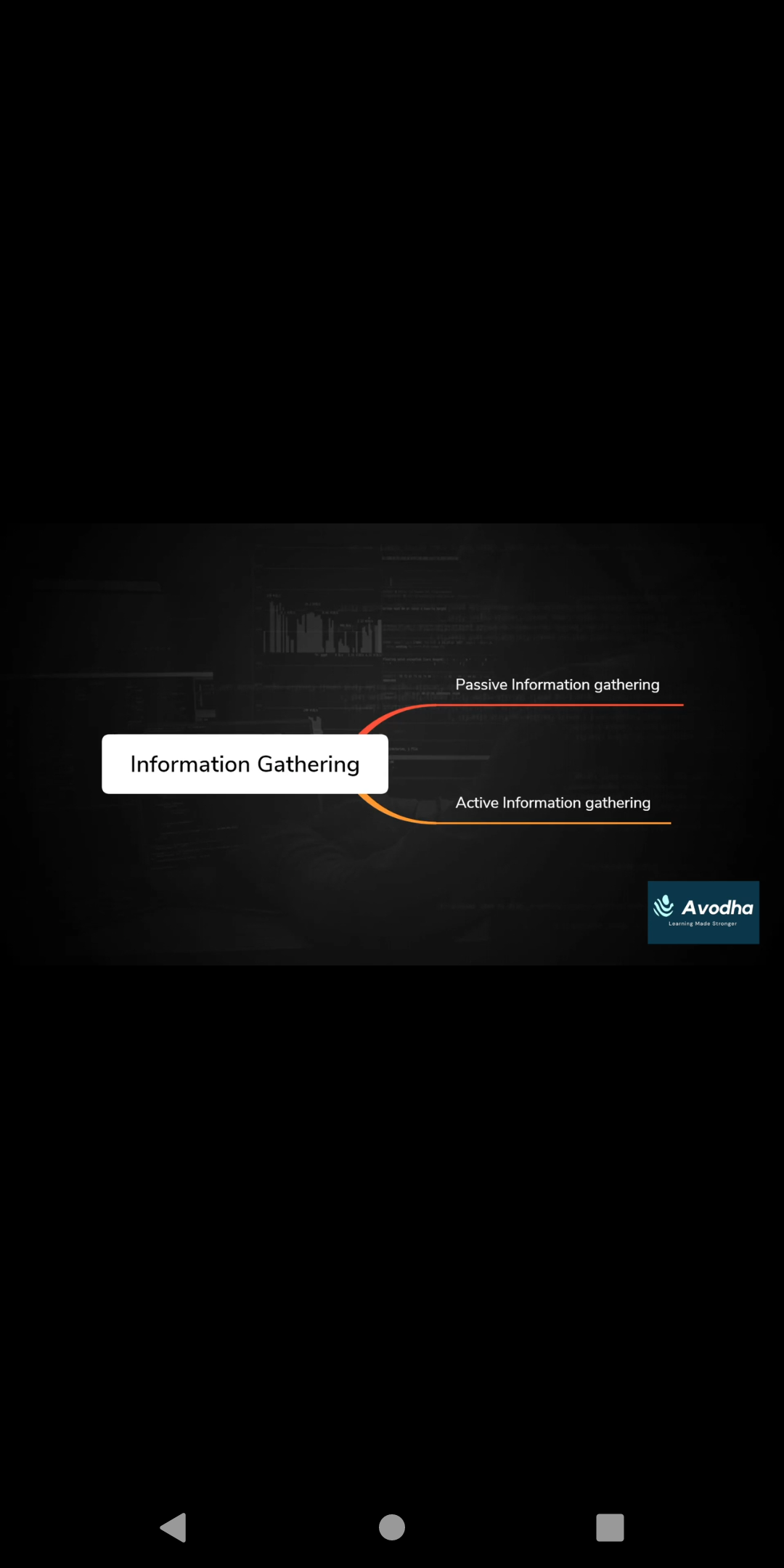
* Information is something obtained by comparing the data other data. These other data

may be part of the same collection of data or part of another collection

* Eg : names of students in alphabetic order are information.

What is data intelligence?

* Intelligence can be defined as the collection of information.
* So the data intelligence means nothing bity collection of information in other words gathered information.



**PASSIVE INFORMATION GATHERING**

* Passive information gathering refers to gathering as much as possible without establishing contact between the attacker and the target about which we are collecting information.
* We need to collect same important information about the target so that we will use the following methods to gather information.
* Website footprinting.
* DNS(Domain Name Server/System) Reconnaissance.
* E-Mail Collection

**DNS RECONNAISSANCE**

* DNS stands for Domain System/Server. The main function of DNS is to translate domain name into IP Address, which computers can understand
* DNS Record;

A Record

An A record is what points your domain to an IP Address. It stands for address record and is the purest form of DNS. It allows user to type in an easily recognizable and still get pointed to the IP Address**.**

CNAME

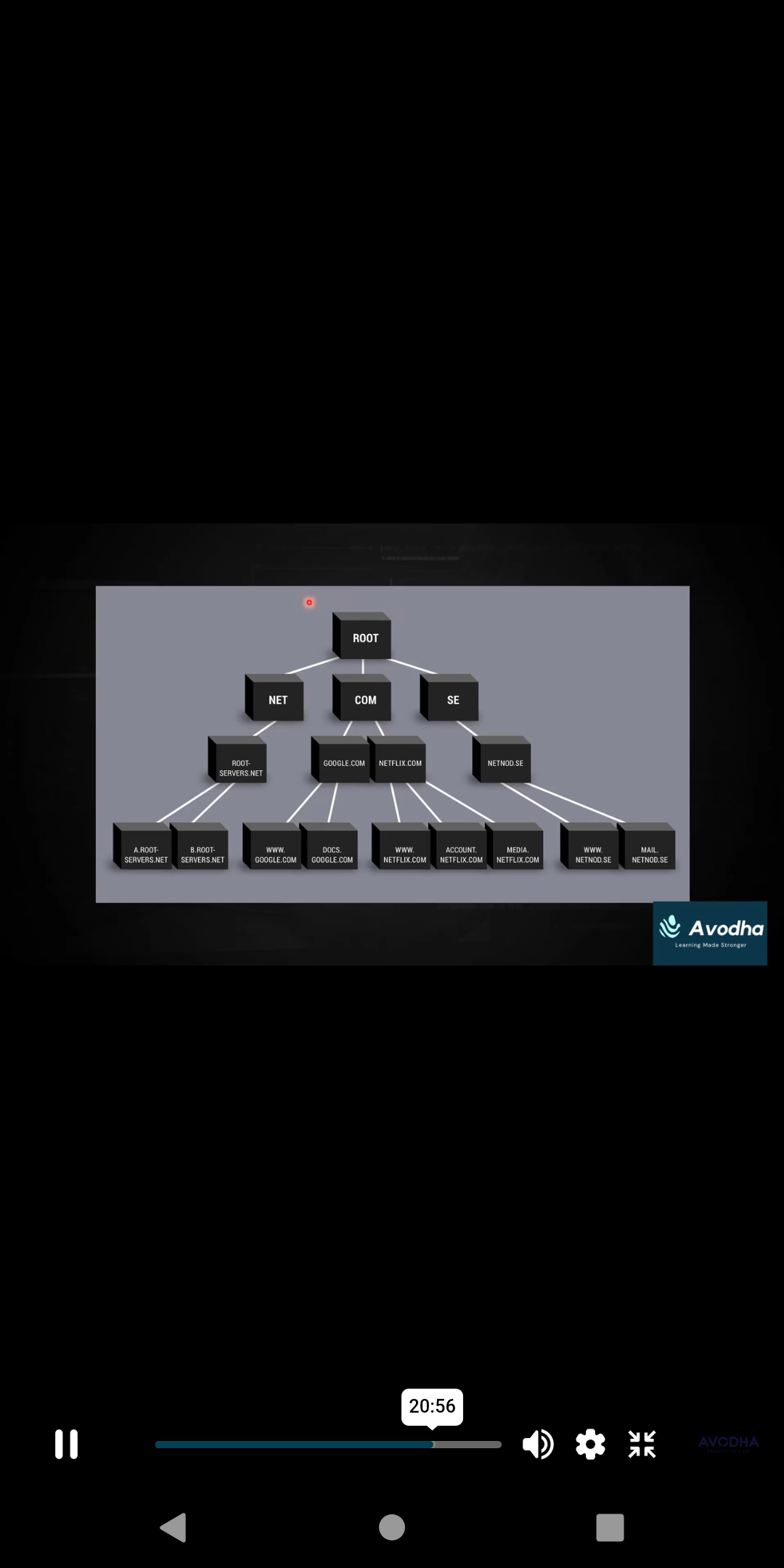
CNAME, or canonical name, redirects one domain to another to another, allowing you to only update one A record each time you make a change. For example, the CNAME record allows ”cloudwards.net” to fetch up ”www.cloudward.net” with the “www” in front.

* MX Entry
* A mail exchanger entry directs email to a different server despite being a subdomain. Essentially, it specifies how email should be routed when sent to an address at your domain.
* TXT Record
* This is a bit of catch all record, not intended to direct any traffic , but instead to provide information to external sources. It serves several different purpose depending on your needs.
* AAAA record
* This record is the same as an A record, but allows you to point a domain to an IPV4 address instead of an IPV4 one.
* ROOT SERVER

A root server is a name server for the root zone of the domain name system (DNS) of the internet. It directly answer request for records in the root zone and answers other request by returning a list of the authoritative name servers for the appropriate top-level domain(TLD).

TOP LEVEL DOMAIN

Top-level domain (TLD) refers to the last segment of a domain name, or the part that follows immediately after the “dot” symbol. For example, in the internet address: <http://www.google.com>, the “.com” portion is the TLD





What is network scanning?

* Network scanning refers to a set of procedures for identifying host,ports,and services
* Objectives
  + To discover live host, IP address and open ports of live host
  + To discover operating system
  + To discover service running on host
  + (MAC address)

**Address Resolution Protocol (ARP)**

* Most of the computer program/application use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address) This is were ARP (Address Resolution Protocol) comes into the picture, its functionality is to translate IP address to physical address.