R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contentsof this informationisstrictlyprohibited.

22CS930 ENTERPRISE CYBER SECURITY

Department:	CSE(CS)
Batch/Year:	2022-2026/IV
Created by:	Dr. Udhaya Sankar S M Professor & Head/CSE(CS)
Date:	15.5.2025

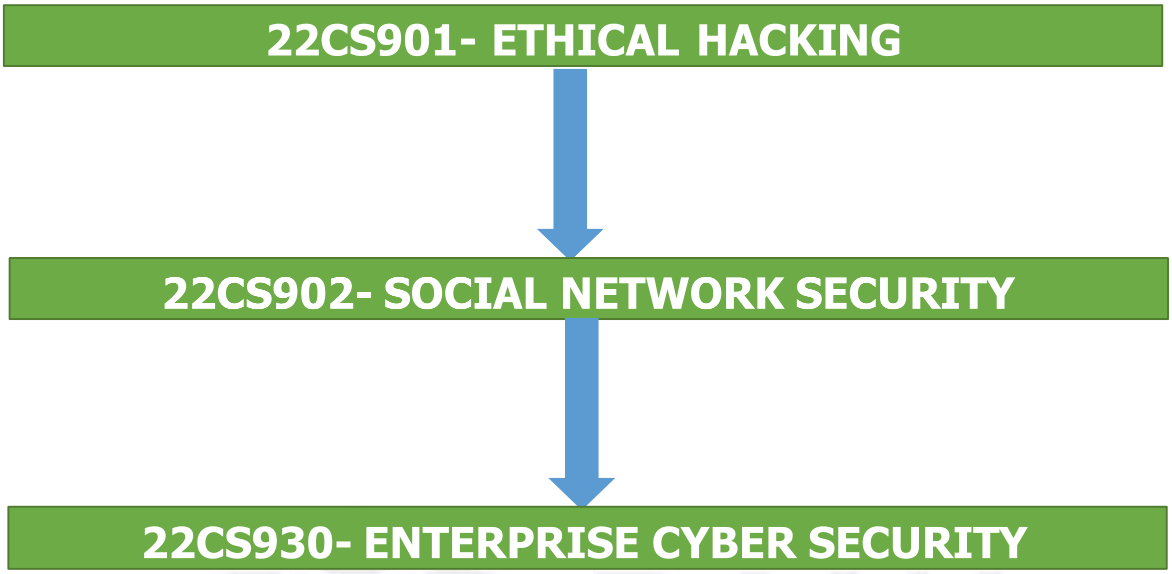
1.TABLE OF CONTENTS

2. COURSE OBJECTIVES

- Learn the fundamentals of cryptography.
- Learn the key management techniques and authentication approaches.
- Explore the network and transport layer security techniques.
- Understand the application layer security standards.
- Learn the real time security practices.

3. PRE REQUISITES

PRE-REQUISITE CHART



22CS901- ETHICAL HACKING

22CS902- SOCIAL NETWORK SECURITY

22CS930- ENTERPRISE CYBER SECURITY

4.SYLLABUS

22CS930- ENTERPRISE CYBER SECURITY

L T P C
3 0 0 3

Unit-I INTRODUCTIONTOCYBERSECURITY 9

Cyber Security – Need of Cybersecurity in Organizations – CIA Triad- Confidentiality, Integrity, Availability; Reason for Cyber Crime –Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes– A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.

Unit II : NETWORK SECURITY BASICS 9

Network Security Concepts- Basics of Networks- Common Types of Network Attacks- Introduction to Firewalls- Types of Firewalls- IDS/IPS- Virtual Private Networks (VPN's)- Secure configuration and management of network devices. Case Study: Install Kali Linux on Virtual box.

Unit III : SECURE COMMUNICATION PROTOCOLS 9

Encryption Principles- Cryptography, Cryptanalysis, Feistel Cipher Structure. Block Encryption algorithms: DES, triple DES, and AES. Transport-Level Security: Secure Sockets Layer (SSL), Transport Layer Security TLS). Electronic Mail Security- Pretty Good Privacy (PGP), S/MIME. Securing wireless networks: WPA, WPA2, WPA3.

Unit IV : INTRUSION DETECTION AND PREVENTION SYSTEMS 9

IDPS- Need of Intrusion Detection Systems in Cyber Security- Types of IDPS: Network-based and Host-based. Configuring and Managing IDPS for threat detection using Honeypots. Case Study: Setup a honey pot and monitor the honey pot on network.

Unit V : WEB APPLICATION SECURITY 9

Introduction to Web Application Vulnerabilities – Cross Site Scripting (XSS) – SQL injection- Denial of Service (DoS)- Web Application Testing - Types of Penetration Tests- OWASP and OWASP Top.

5.COURSE OUTCOME

Course Code	Course Outcome Statement	Cognitive / Affective Level of the Course Outcome	Course Outcome
Course Outcome Statements in Cognitive Domain			
22CS930	Understanding the core concepts and importance of cybersecurity in organizational settings.	Apply K3	CO1
22CS930	Acquire the knowledge common network attacks and deploy appropriate security measures.	Apply K3	CO2
22CS930	Implement encryption and secure communication protocols for data integrity and confidentiality.	Apply K3	CO3
22CS930	Deploy and manage Intrusion Detection and Prevention Systems for threat detection.	Apply K4	CO4
22CS930	Identify and mitigate common web application vulnerabilities	Apply K4	CO5
22CS930	Conduct penetration tests to evaluate the security posture of web applications.	Apply K5	CO6

6.CO-PO/PSO MAPPING

Correlation Matrix of the Course Outcomes to Programme Outcomes and Programme Specific Outcomes.

Course Outcomes (Cos)		Programme Outcomes (POs), Programme Specific Outcomes (PSOs)														
		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
22CS930.1	K2	3	2	3	-	2	-	-	1	-	-	-	2	3	2	1
22CS930.2	K3	3	3	3	-	3	-	-	-	-	-	-	2	3	3	2
22CS930.3	K3	2	3	3	-	3	-	-	-	1	1	-	2	3	3	2
22CS930.4	K3	2	3	3	-	3	-	-	2	-	-	-	2	3	3	2
22CS930.5	K2	3	2	3	-	2	-	-	-	-	-	-	3	3	3	3
22CS930.6	K3	3	3	3	-	3	-	-	-	-	2	1	3	3	3	3

UNIT II
NETWORK SECURITY BASICS

9. LECTURE NOTES : UNIT – II

NETWORK SECURITY BASICS

Syllabus:

Network Security Concepts- Basics of Networks- Common Types of Network Attacks- Introduction to Firewalls- Types of Firewalls- IDS/IPS- Virtual Private Networks (VPN's)- Secure configuration and management of network devices. Case Study: Install Kali Linux on Virtual box.

1. Network Security Concepts

Basics of networks

- A group of interconnected (via cable and/or wireless) computers and peripherals that is capable of sharing software and hardware resources between many users.
- Telecommunication network is a electronic system of links and switches, and the controls that govern their operation, that allows for data transfer and exchange among multiple users.
- Example: The Internet is a global network of networks.

Node

A node in a network refers to any active, physical or logical device that is capable of sending, receiving, or forwarding data across a network. Nodes are the building blocks of both computer networks and telecommunications systems.

Types of Nodes:

Computer Nodes

Devices like desktops, laptops, smartphones, or servers connected to the network.

Networking Devices

Routers, switches, modems, firewalls, and hubs that help manage traffic and direct data packets.

Peripheral Nodes

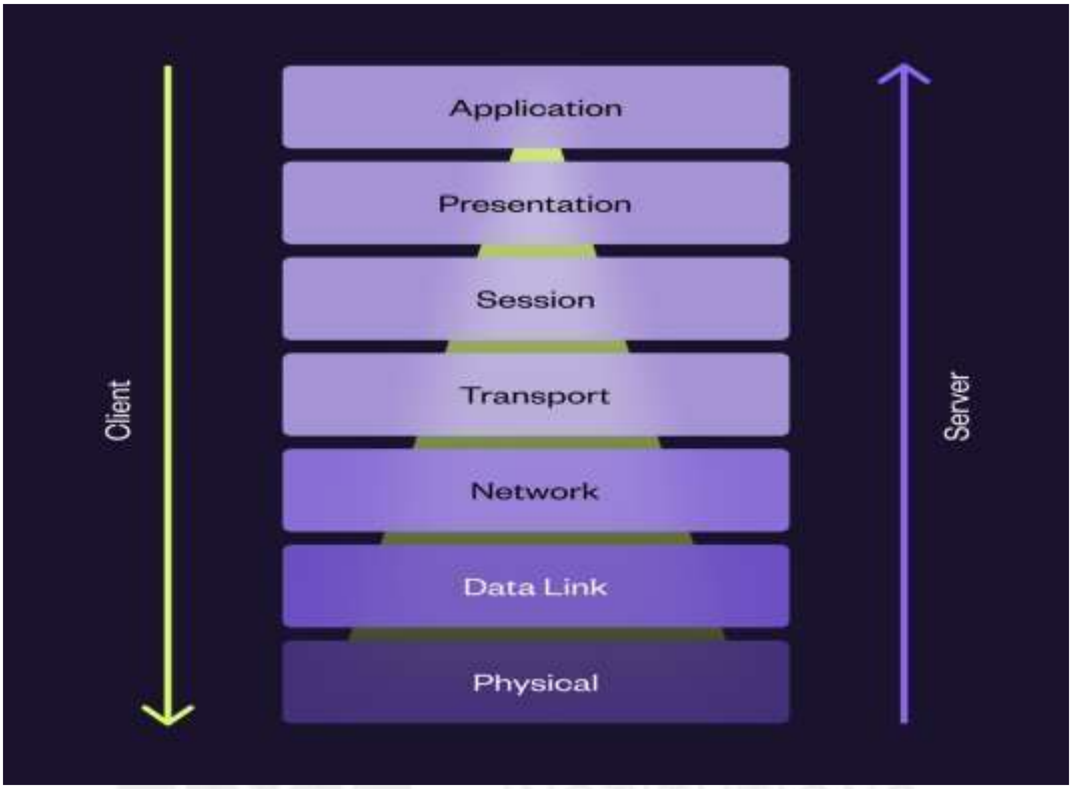
Devices like printers or IP cameras connected to the network that can communicate data.

Virtual Nodes

Software-based entities like virtual machines or containers operating within a cloud or virtualized environment.

2.1 Basic Network Concepts

OSI LAYER AND FUNCTIONS



1. Physical: Bit transmission

2. Data Link: MAC addressing

3. Network: IP routing

4. Transport: TCP/UDP

5. Session: Communication control

6. Presentation: Encryption/translation

7. Application: End-user interface

Advantages of Computer Networks

Computer networks offer a wide range of benefits, whether in homes, businesses, or educational settings. Here are the key advantages:

1. Resource Sharing

Devices such as printers, scanners, and storage drives can be shared across multiple computers.

Reduces cost and improves utilization of hardware.

2. Data and File Sharing

Users can easily share files, documents, and media across devices and locations.

Promotes collaboration and fast information exchange.

3. Increased Reliability

A well-designed network increases system reliability, ensuring users have continuous access to data and services with minimal disruption.

4. Expandablity and scalablity

Expandability refers to the ease with which a network can accommodate additional devices, users, or services without major changes to its existing infrastructure.

Network Vulnerablities

❑ Anonymity

❑ Points of attack

❑ Resource and workload sharing

❑ System complexity

❑ Unknown boundary

2.3 Network Vulnerablities

Concept	Description
Anonymity	Hides user identity; can protect privacy or enable cybercrime
Points of Attack	Vulnerable spots that attackers exploit (e.g., apps, endpoints, servers)
Resource and Workload Sharing	Efficient use of network devices and services
System Complexity	Increases risk due to size, integration, and variety of components
Unknown Boundary Vulnerabilities	Risks from undefined network edges (remote users, cloud, personal devices)

Anonymity

Anonymity in networking refers to the ability of a user to conceal their identity or actions on the internet or a private network. Attacker does need to be in physical contact with the information system in attack.

Points of Attack

These are the specific locations or vulnerabilities in a network or system where cyber attackers can attempt unauthorized access or data manipulation.

Resource and Workload Sharing

More users can have access computational assets exposing assets to be at risk

System Complexity

As networks grow in size and functionality, they often become more complex, which introduces challenges in management, maintenance, and security.

Unknown Boundary Network Vulnerabilities

Modern networks often extend beyond clearly defined borders due to mobile access, cloud computing, and remote users. This results in unknown or dynamic boundaries, which makes securing the network more difficult.

2.4 Network Attacks

Network attacks present significant risks to an organization’s data security, operational stability, and reputation. These attacks focus on compromising the organization's IT infrastructure to access confidential information, interrupt business processes, or exploit security weaknesses for financial or strategic advantage.

TYPES OF ATTACKS

Active Attacks

- ❑ Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- ❑ Man-in-the-Middle (MitM)
- ❑ SQL Injection
- ❑ Privilege Escalation
- ❑ Malware
- ❑ Phishing
- ❑ Ransomware
- ❑ Botnets

Passive Attacks:

- ❑ Eavesdropping
- ❑ Packet Sniffing
- ❑ Traffic Analysis

Emerging Attack Trends

- ❑ Cryptojacking
- ❑ Zero-day exploits

2.4.1 Types of Network Attacks

Active Attacks

Active attacks involve altering the data stream or generating fake data transmissions. These attacks are typically classified into four main types: masquerade, replay, message modification, and denial of service (DoS).

Attack Type	Purpose	Example
DoS	Overload system to deny access	Flooding a website with fake traffic
DDoS	Large-scale DoS using multiple devices	Botnet sending mass requests to crash a site
Man-in-the-Middle	Intercept/modify communication	Stealing login info on public Wi-Fi
SQL Injection	Modify database through web input	Bypassing login with SQL commands
Privilege Escalation	Gain higher access without permission	Normal user becomes system admin
Malware	Damage or hijack systems	Trojan horse disguised as a file or app
Phishing	Trick users into giving data	Fake bank email asking for login details
Ransomware	Encrypt data, demand ransom	Files locked with ransom note
Botnets	Remote control of many infected devices	Used to launch DDoS or spam attacks

Man-in-the-middle MITM

Man-in-the-middle (MitM) attacks are cyberattacks where an attacker intercepts communication between two parties

DNS Spoofing

ARP Poisoning

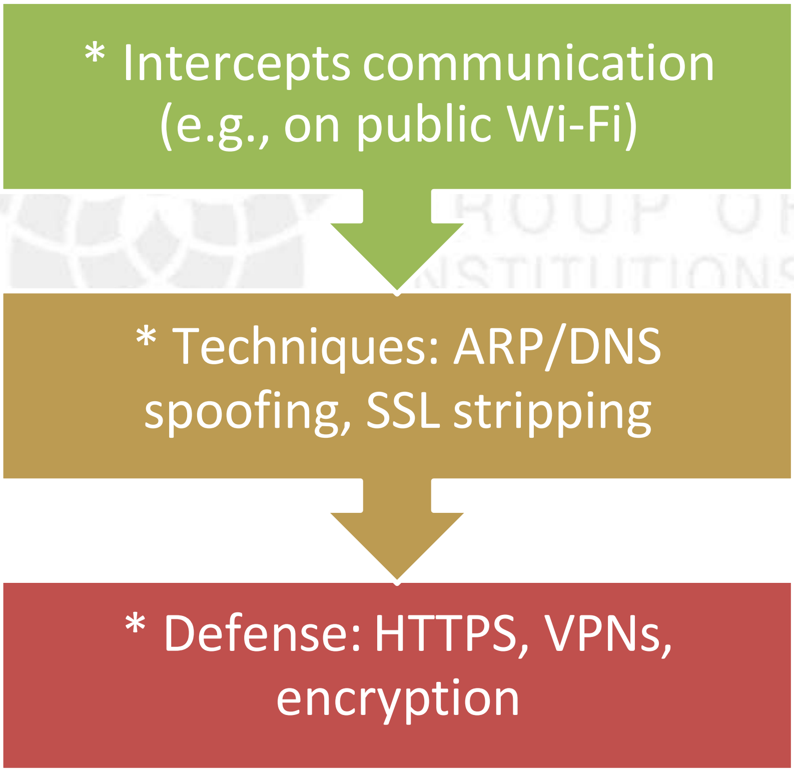
Wi-Fi Eavesdropping

Session Hijacking

SSL/TLS Stripping

Email Hijacking

IP Spoofing



* Intercepts communication (e.g., on public Wi-Fi)

* Techniques: ARP/DNS spoofing, SSL stripping

* Defense: HTTPS, VPNs, encryption

Network Attacks: DoS & DDoS

A DDoS (Distributed Denial of Service) attack involves multiple compromised systems working together to overwhelm a target with excessive traffic, resulting in service disruptions or shutdowns.

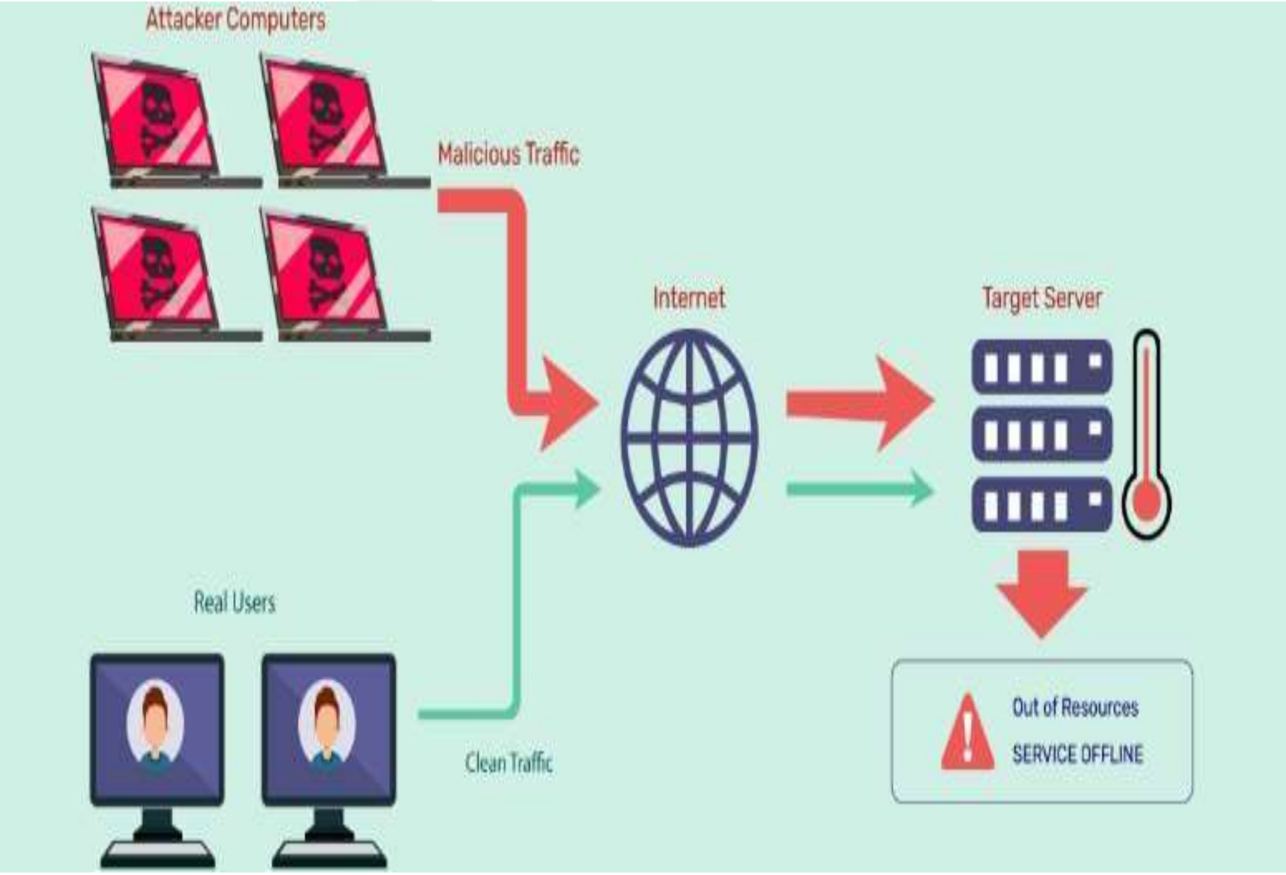
Unlike a DoS (Denial of Service) attack, which typically comes from a single source, the distributed nature of a DDoS attack makes it significantly more difficult to counter and can cause widespread disruption.

Denial of Service (DoS): Overloads a target with traffic

Distributed DoS (DDoS): Multiple sources (botnet) attack target

Example: SYN Flood

Defenses: Rate-limiting, firewalls, anti-DDoS services



Passive Attacks

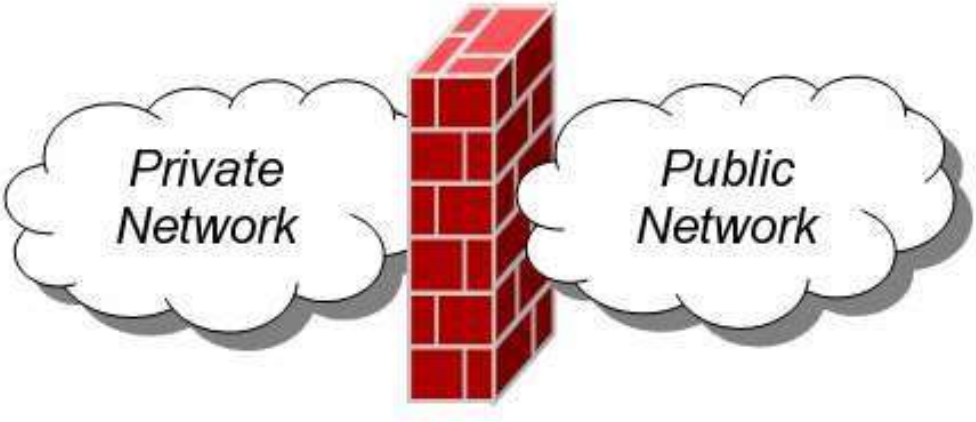
Passive attacks are types of network attacks where the attacker monitors or intercepts data without altering the communication or affecting system operations. The main goal of passive attacks is to collect sensitive information or analyze traffic patterns without the victim's knowledge. These attacks are often difficult to detect because they don't involve any change in the data being transmitted.

Attack Type	Description	Purpose	Detection Difficulty	Prevention Methods
Eavesdropping	Unauthorized interception of private communications (voice, text, etc.).	To steal sensitive information.	Very hard to detect	Encryption (e.g., TLS, VPN)
Packet Sniffing	Capturing data packets moving through a network using special software tools.	To monitor or collect network traffic data.	Hard to detect	Use secure protocols; network segmentation
Traffic Analysis	Observing patterns of communication (e.g., frequency, size, timing) without reading contents.	To infer information like sender/receiver identities or behavior.	Extremely hard to detect	Use of tunneling, encryption, dummy traffic

2.5 Firewall

A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.

A network firewall is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another. Firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet, to block malicious traffic like viruses and hackers.



Hardware firewall vs Software firewall

Feature	Hardware Firewall	Software Firewall
Definition	A physical device placed between a network and gateway	A program installed on a device (PC, server, etc.)
Deployment	Protects entire networks	Protects individual devices
Performance	High throughput, optimized for network traffic	May slow down the device it's installed on
Configuration	Centralized, managed from a single interface	Must be configured on each device separately
Maintenance	Requires knowledge to install and manage	Easier to install and update (auto-updates possible)
Security Level	More robust for external threats	Useful for blocking internal threats or outgoing connections
Scalability	Better suited for larger networks or businesses	Best for personal or small office use
Cost	Typically more expensive (hardware + support)	Usually free or low-cost (built-in or downloadable)
Example Products	Cisco ASA, Fortinet FortiGate, SonicWall	Windows Defender Firewall, ZoneAlarm, Comodo

Generation of firewall

Generation	Key Technology	OSI Layer	Key Features
1st	Packet Filtering	Layer 3 (Network)	Basic traffic filtering
2nd	Stateful Inspection	Layers 3–4	Connection state awareness
3rd	Application Firewall / Proxy	Layer 7 (App)	Protocol-aware filtering
4th	Next-Gen Firewall (NGFW)	Layers 3–7	DPI, IPS, App control, user identity
5th	UTM	Layers 3–7	Multi-function security appliance
6th	Cloud & AI-based Firewalls	All layers	Cloud-native, AI/ML analytics, Zero Trust support

Types of firewall

Firewalls can be classified based on how they filter traffic and where they are deployed. The main types include:

1. Packet-Filtering Firewall

How it works: Examines packets (small chunks of data) and allows or blocks them based on source/destination IP addresses, ports, and protocols.

Pros: Fast and low resource usage.

Cons: Doesn't inspect payload (data inside packets), so it may miss complex attacks.

2. Stateful Inspection Firewall (Dynamic Packet Filtering)

How it works: Tracks the state of active connections and makes decisions based on the context of the traffic.

Pros: More secure than simple packet filters.

Cons: More resource-intensive.

3. Proxy Firewall (Application-Level Gateway)

How it works: Acts as an intermediary between users and the services they access; inspects application-level data.

Pros: Strong security at the application level.

Cons: Slower due to deep inspection; may not support all protocols.

4. Next-Generation Firewall (NGFW)

How it works: Combines traditional firewall with advanced features like intrusion prevention systems (IPS), deep packet inspection, and application awareness.

Pros: Very effective at detecting modern threats.

Cons: Expensive and resource-heavy.

5. Software Firewall

Where it runs: Installed on individual devices (e.g., Windows Firewall).

Pros: Customizable per device.

Cons: Must be installed and managed on each device.

6. Hardware Firewall

Where it runs: Physical devices placed between your network and gateway.

Pros: Centralized protection for entire network.

Cons: Requires maintenance and expertise.

2.6 Virtual Private Network (VPN)

A Virtual Private Network (VPN) creates a secure, encrypted connection over a public network (usually the internet). It allows users to send and receive data as if their devices were directly connected to a private network.

Key Features:

Encryption: Protects data from eavesdropping.

Tunneling: Encapsulates data packets for secure transmission.

Remote Access: Allows users to access internal resources from outside.

Anonymity: Hides IP addresses and masks online activity.

Common VPN Protocols:

Protocol	**Features**
PPTP	Fast but less secure (obsolete for sensitive data)
L2TP/IPsec	More secure; uses double encapsulation
OpenVPN	Highly secure; open source; uses SSL/TLS
IKEv2/IPsec	Stable and secure, especially on mobile
WireGuard	Newer, faster, modern encryption

VPN protocols are the underlying rules that define how data is transmitted between a device and a VPN server, ensuring a secure and private connection. They dictate encryption, authentication, and data routing within the VPN tunnel. Different protocols offer varying levels of speed, security, and compatibility, making it important to choose the right one for your needs.

Common VPN Protocols:

OpenVPN:

A widely used open-source protocol known for its strong security and flexibility, but potentially slower speeds compared to other protocols. It uses SSL/TLS encryption, providing a high level of security.

IKEv2/IPsec:

A popular choice, especially for mobile users, offering good speed, security, and compatibility with various operating systems. It uses a combination of Internet Key Exchange version 2 (IKEv2) for key exchange and Internet Protocol Security (IPsec) for encryption.

WireGuard:

A relatively new, lightweight, and fast protocol with excellent security and compatibility, often considered a strong contender against OpenVPN. It's designed for speed and efficiency.

L2TP/IPsec:

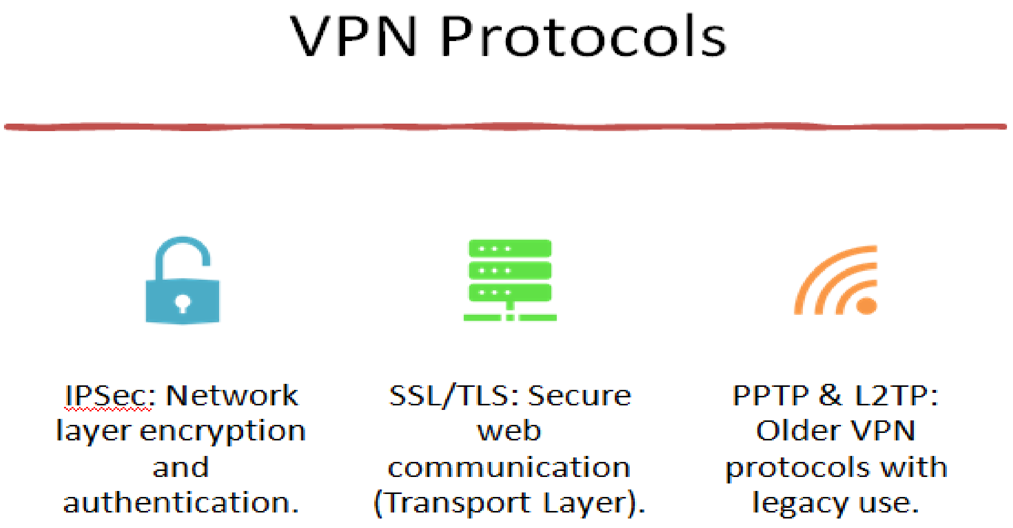
A protocol that combines Layer 2 Tunneling Protocol (L2TP) with IPsec for enhanced security, but it may be slower than IKEv2/IPsec and has limited compatibility.

SSTP:

A Microsoft-developed protocol designed for secure remote access, offering a good balance of security and speed.

PPTP:

An older protocol that is considered less secure than other options due to its vulnerabilities.



VPN Protocols

IPSec: Network layer encryption and authentication.

SSL/TLS: Secure web communication (Transport Layer).

PPTP & L2TP: Older VPN protocols with legacy use.

Benefits of VPN

1. Enhanced Privacy

A VPN hides your IP address, which is your unique identifier on the internet. By routing your traffic through an encrypted tunnel and masking your real location, VPNs prevent websites, advertisers, and even your Internet Service Provider (ISP) from tracking your online activity.

2. Secure Data Transmission

VPNs encrypt all the data you send and receive, protecting sensitive information such as login credentials, emails, banking transactions, or company data from hackers—especially when using public Wi-Fi networks (e.g., in airports, cafés, or hotels).

3. Bypass Restrictions

VPNs allow you to access content that may be blocked or restricted in your location. By changing your virtual location to another country, you can access streaming services, websites, or applications that are otherwise unavailable (e.g., Netflix libraries, BBC iPlayer, or blocked news sites).

4. Avoid Censorship

In countries with internet restrictions or censorship, VPNs help users access free and open internet by bypassing government firewalls. This is especially valuable for journalists, researchers, and citizens in authoritarian regimes.

5. Remote Access for Businesses

VPNs enable employees to securely connect to a company's internal network from remote locations. This supports remote work while keeping company data safe from interception or breach, especially over unsecured networks.

6. Prevention of Bandwidth Throttling

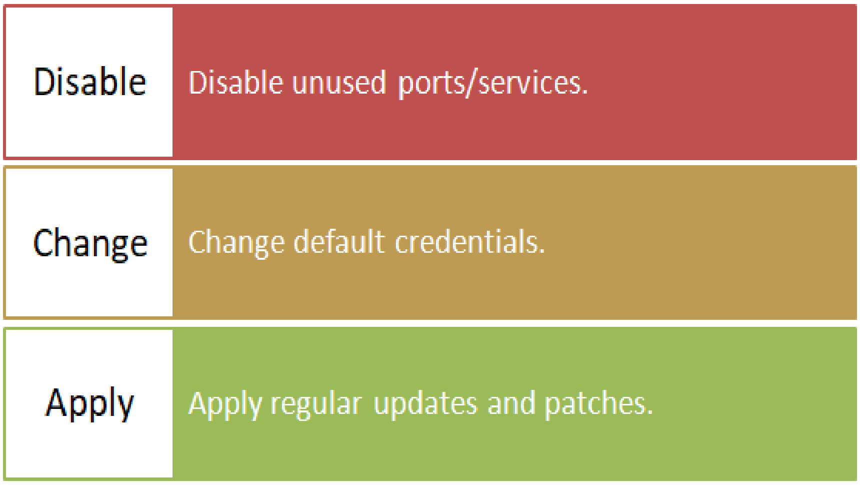
ISPs sometimes slow down your internet speed if they detect high-bandwidth activities like streaming or gaming. A VPN masks your traffic, making it harder for your ISP to throttle specific types of data usage.

7. Safe Online Transactions

VPNs add an extra layer of security when performing online banking or shopping, reducing the risk of data theft, phishing, or fraudulent activity during these sensitive operations.

2.7 Secure Configuration of Network Devices

Practice	Description
Change Default Credentials	Always set strong, unique passwords.
Disable Unused Services/Ports	Reduce attack surface by turning off unnecessary services (e.g., Telnet).
Use SSH Instead of Telnet	SSH encrypts administrative access.
Implement Access Control Lists (ACLs)	Limit who can access or configure the device.
Update Firmware and OS Regularly	Patch known vulnerabilities.
Backup Configurations	Regularly back up device settings in case of failure or attack.
Use Centralized Management	Tools like Cisco Prime, SolarWinds, or cloud-based dashboards help monitor and control devices.
Enable Logging and Monitoring	Record configuration changes and login attempts.
Use Network Segmentation	Isolate critical systems from general traffic.



Disable — Disable unused ports/services.

Change — Change default credentials.

Apply — Apply regular updates and patches.

2.8 Case Study: Install Kali Linux on Virtual box.

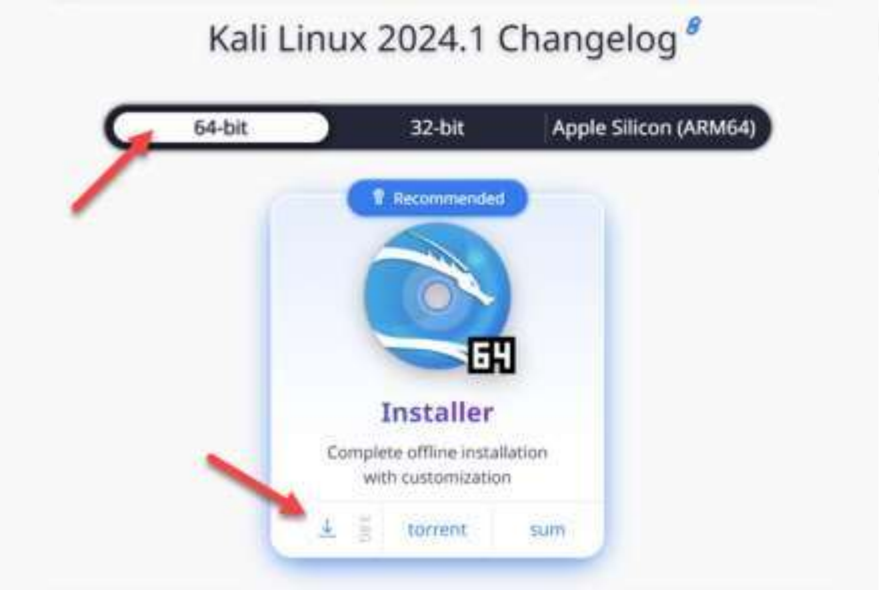
Preparing to Install Kali Linux on VirtualBox

To create and prepare a virtual machine for Kali Linux, you must load an ISO file and configure virtual hardware, such as memory, CPU cores, and hard disks. Follow the steps below to complete these actions.

Step 1: Download Kali Linux ISO Image

Kali Linux offers ISO images for 32-bit, 64-bit, and ARM64 architectures. To download an ISO file:

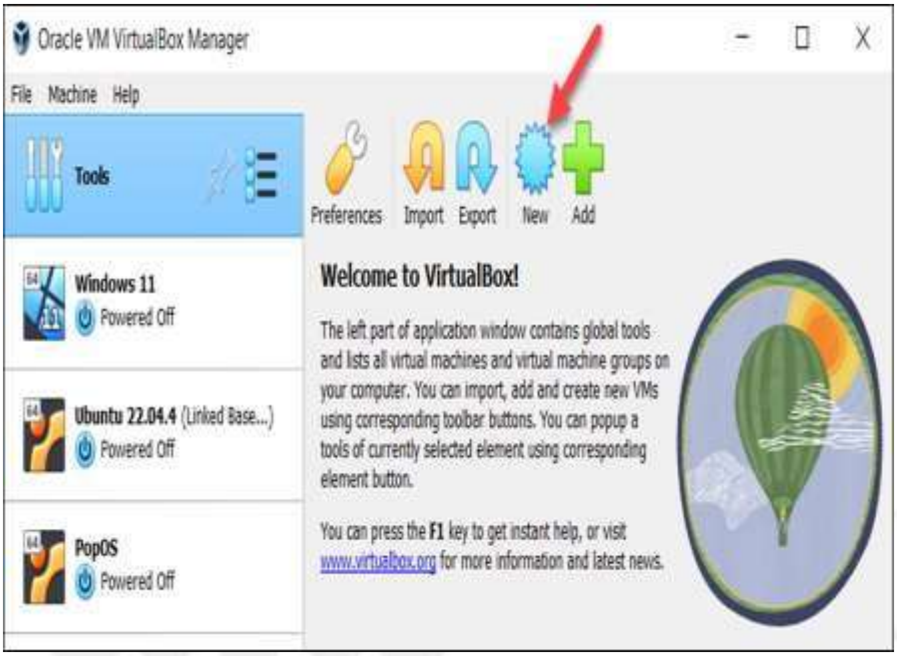
1. Visit the installer section of the Kali Linux official website.
2. Select the system architecture of the host OS and download the ISO file by clicking the button in the bottom-left corner of the installer card.


Kali Linux 2024.1 Changelog
64-bit
32-bit
Apple Silicon (ARM64)
Recommended
64
Installer
Complete offline installation with customization
torrent
sum

Step 2: Create Kali Linux VirtualBox Instance

Create a new virtual machine and configure it to run Kali Linux. Proceed with the steps below to correctly set up a Kali Linux VM in VirtualBox:

1. Launch VirtualBox Manager and click the New icon.

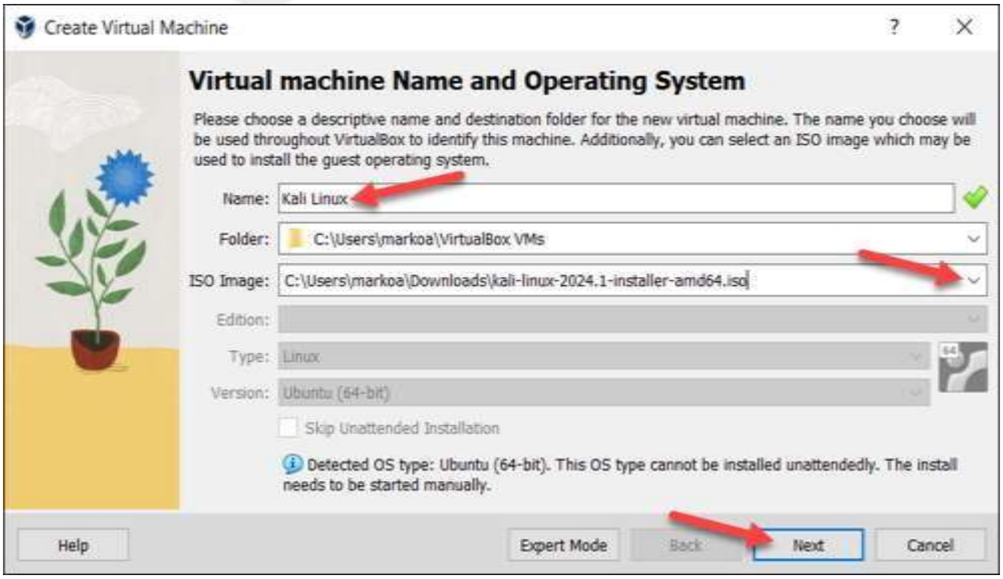


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the F1 key to get instant help, or visit www.virtualbox.org for more information and latest news.

Specify a name for the VM and provide the path to the ISO image. Select Next.



Virtual machine Name and Operating System

Please choose a descriptive name and destination folder for the new virtual machine. The name you choose will be used throughout VirtualBox to identify this machine. Additionally, you can select an ISO image which may be used to install the guest operating system.

Name: Kali Linux

Folder: C:\Users\markoa\VirtualBox VMs

ISO Image: C:\Users\markoa\Downloads\kali-linux-2024.1-installer-amd64.iso

Edition:

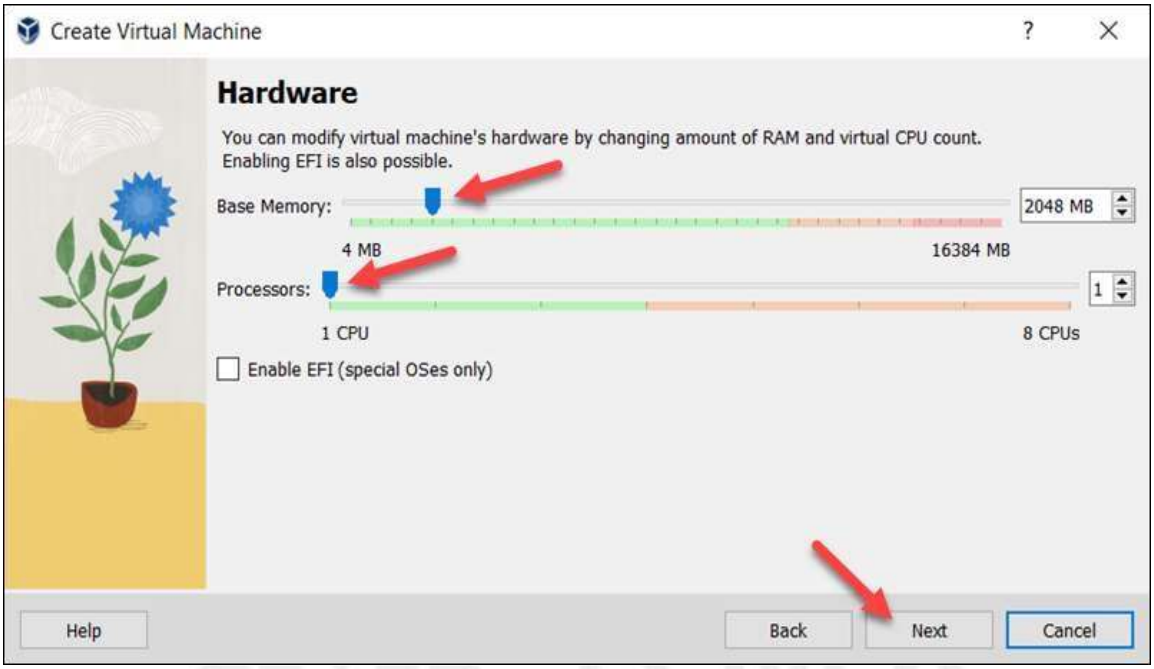
Type: Linux

Version: Ubuntu (64-bit)

□ Skip Unattended Installation

Detected OS type: Ubuntu (64-bit). This OS type cannot be installed unattendedly. The install needs to be started manually.

3. Select the amount of memory and the number of virtual CPUs to allocate to the VM. The minimum recommended values for Kali Linux are 2 GB of RAM and 1 CPU. Select Next when you finish setting up the VM hardware.



Create Virtual Machine

Hardware

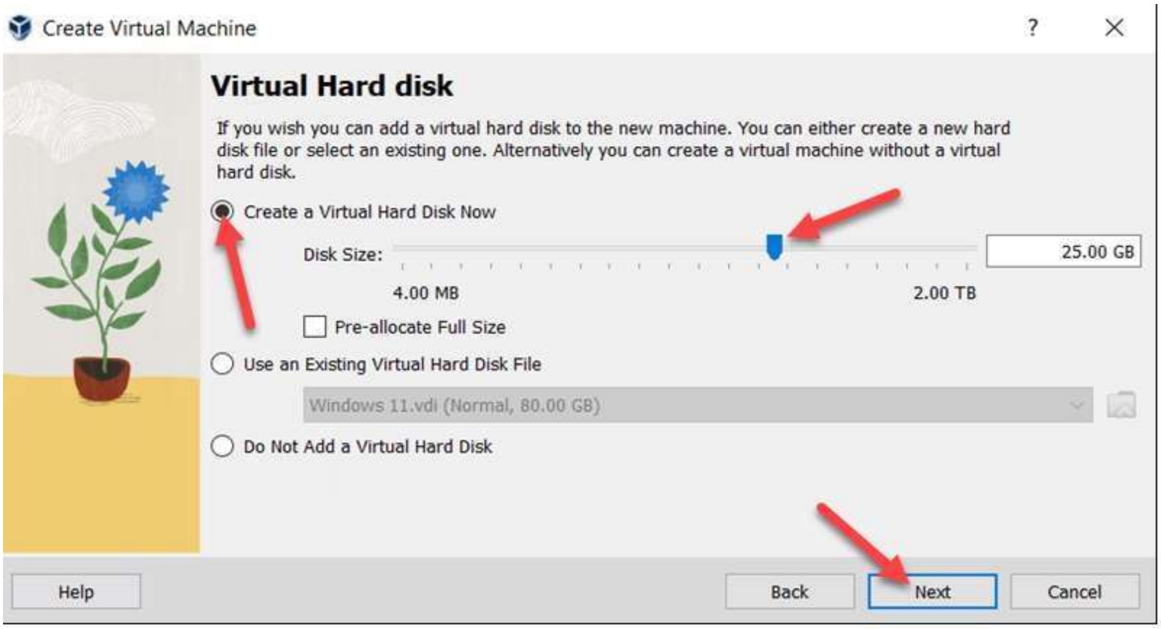
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 2048 MB

Processors: 1

□ Enable EFI (special OSes only)

4.Create a virtual hard disk for the new VM. The recommended hard disk size is at least 25 GB. Alternatively, you can use an existing virtual hard disk file or decide not to add one. Click Next to proceed to the next step.



Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 25.00 GB

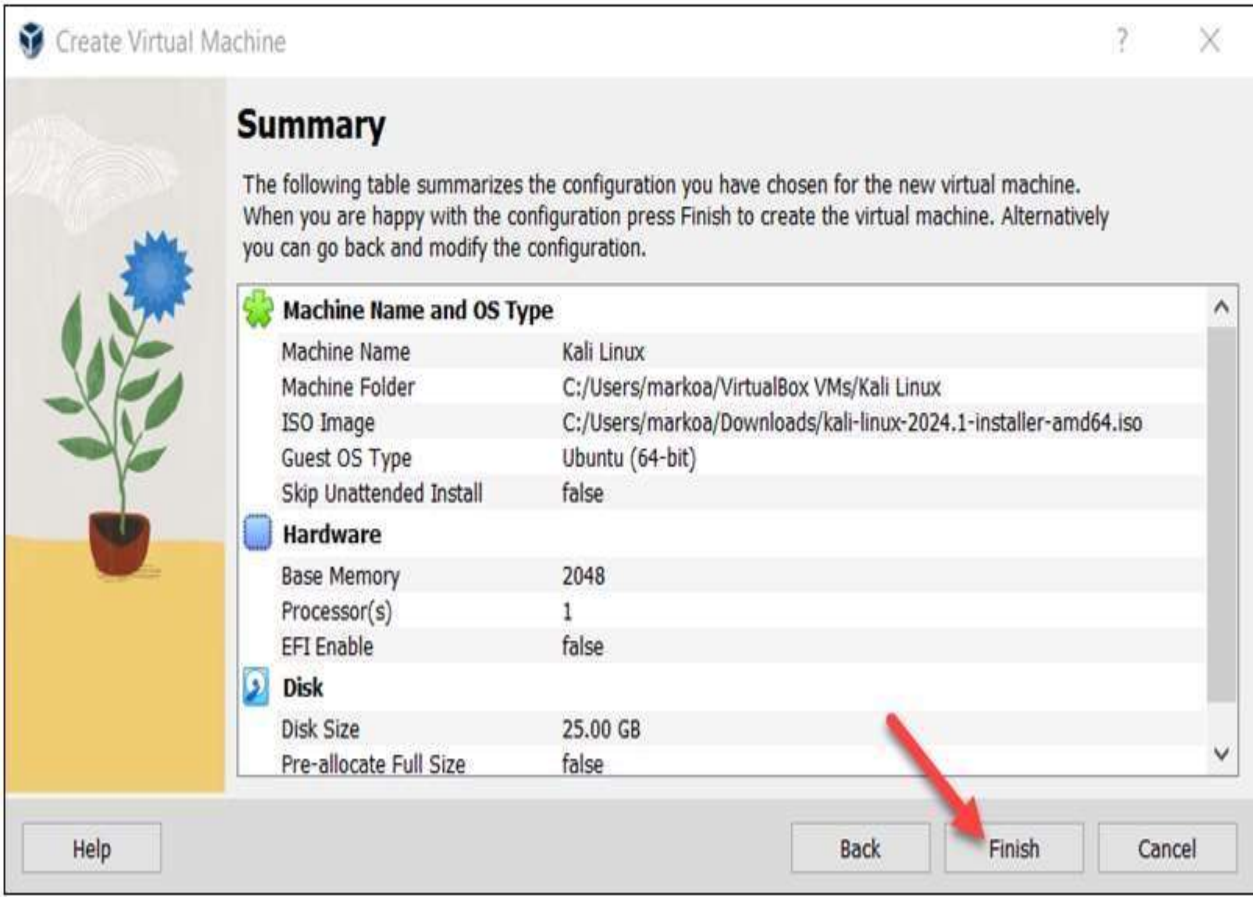
□ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

Windows 11.vdi (Normal, 80.00 GB)

○ Do Not Add a Virtual Hard Disk

5. Review the new VM setup on the Summary page. Select Finish to create the virtual machine.



Create Virtual Machine

Summary

The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.

Machine Name and OS Type	
Machine Name	Kali Linux
Machine Folder	C:/Users/markoa/VirtualBox VMs/Kali Linux
ISO Image	C:/Users/markoa/Downloads/kali-linux-2024.1-installer-amd64.iso
Guest OS Type	Ubuntu (64-bit)
Skip Unattended Install	false
Hardware	
Base Memory	2048
Processor(s)	1
EFI Enable	false
Disk	
Disk Size	25.00 GB
Pre-allocate Full Size	false

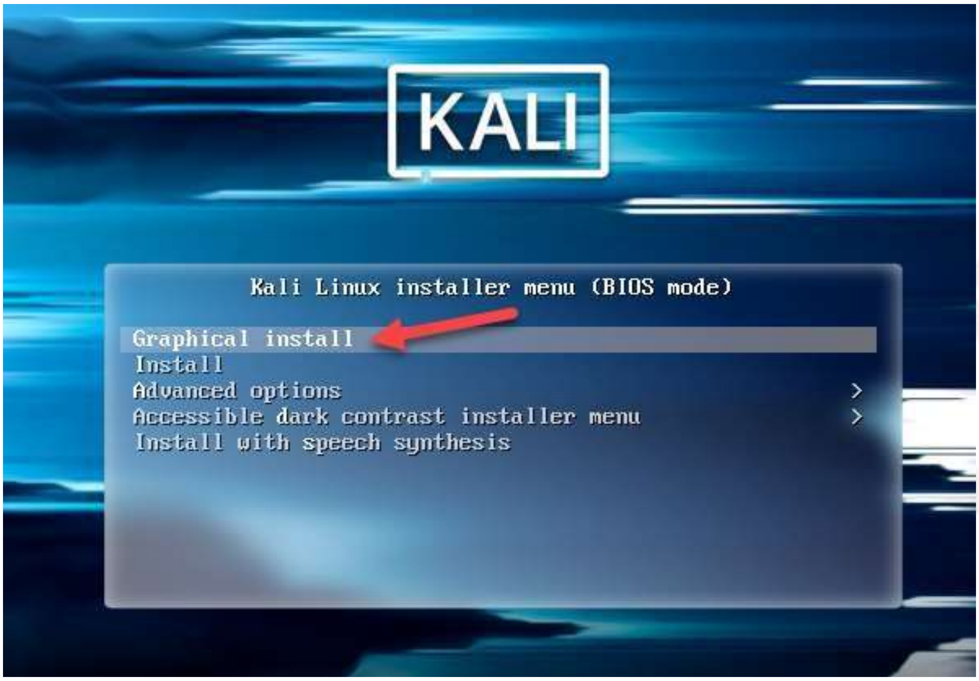
How to Install Kali Linux on VirtualBox

Kali Linux uses the Debian installer to set up the operating system. The sections below provide a detailed walkthrough of the installer and offer advice on configuring Kali Linux.

Step 1: Perform Initial Configuration

When the new VM is started, the Kali Linux installer menu appears. Start the installation procedure by following the steps below:

1. Select the Graphical install option.

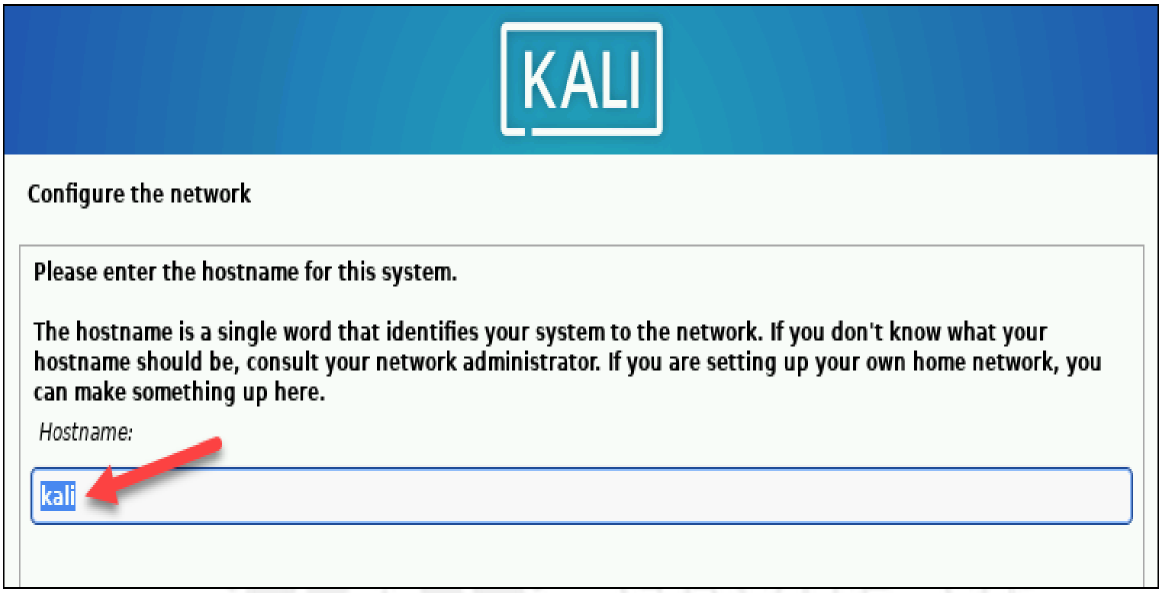

KALI
Kali Linux installer menu (BIOS mode)
Graphical install
Install
Advanced options >
Accessible dark contrast installer menu >
Install with speech synthesis

2. Choose the system's default language, which will also be used during installation.
3. Find and select your country from the list, or choose other.
4. Decide which keyboard mapping to use.

Step 2: Configure Host, User, and Time Zone

The following installer steps set up the hostname and domain of the system and configure the user:

1. In the Configure the network section, enter a system hostname.
2. Type a domain name that the OS will use to identify the VM within a network.
3. Specifying a domain name is not necessary if the VM is not part of an extensive local network
4. Create a user account by providing the user's full name and username.



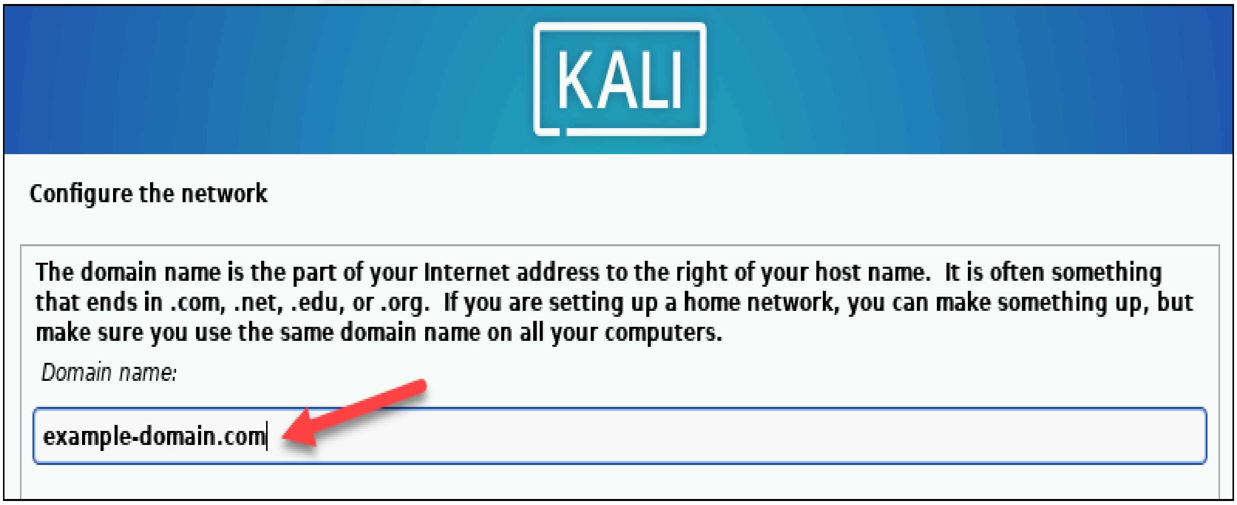
Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

kali



Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

Domain name:

example-domain.com

Step 3:Choosing guided partitioning for the disk.

2. Select the disk you want to use for partitioning. The only available option is the disk created during the VM creation.

3. Select the partitioning scheme. The default option is All files in one partition.

4. The wizard provides an overview of the configured partitions. Ensure that the Finish partitioning and write changes to disk option is selected.

5. Confirm the choice by selecting Yes on the next screen.

Confirming disk partitioning.

The wizard starts installing Kali.

Step 4: Customize Kali Linux Installation

After installing the system's core, Kali enables users to customize the OS further.

Choose the components to install by executing the following steps:

1. Select the desktop environment and the tools you want, or click Continue to proceed with the default options.

Choosing a desktop environment and tool collections.

2. Select whether you want to use a network mirror.

3. If you use an HTTP proxy, enter the necessary information. Otherwise, leave the field blank.

4. Install the GRUB bootloader on the hard disk. Select Yes and Continue.

5. Select a bootloader device to ensure the newly installed system is bootable.

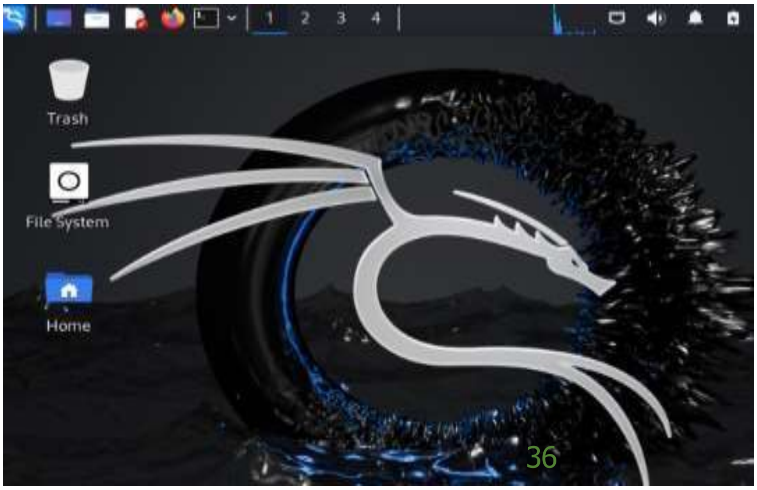
Installing the GRUB bootloader.

When Kali finishes installing, the Installation is complete message appears.

6. Click Continue to reboot your VM. After rebooting, the Kali login screen appears.

7. Enter the username and password created in the previous steps.

The Kali Linux desktop appears on the screen.



7.LECTURE PLAN – UNIT I

	UNIT I INTRODUCTION						
Sl. No	TOPIC	NO OF PERIODS	PROPOSED LECTURE	ACTUAL LECTURE	PERTAINING CO(s)	TAXONOMY LEVEL	MODE OF DELIVERY
			PEROID	PERIOD			
1	Network Security Concepts- Basics of Networks	2			CO1	K2	MD1, MD5
2	Common Types of Network Attacks	1			CO1	K1	MD1, MD5
3	Introduction to Firewalls- Types of Firewalls	1			CO1	K2	MD1, MD5
4	IDS/IPS- Virtual Private Networks (VPN's)	2			CO1	K2	MD1, MD5
5	Secure configuration and management of network devices.	2			CO1	K2	MD1, MD5
6	Case Study: Install Kali Linux on Virtual box.	1			CO1	K2	MD1, MD5

LECTURE PLAN – UNIT I

ASSESSMENT COMPONENTS

- AC 1. Unit Test
- AC 2. Assignment
- AC 3. Course Seminar
- AC 4. Course Quiz
- AC 5. Case Study
- AC 6. Record Work
- AC 7. Lab / Mini Project
- AC 8. Lab Model Exam
- AC 9. Project Review

MODE OF DELEIVERY

MD 1. Oral presentation

MD 2. Tutorial

MD 3. Seminar

MD 4 Hands On

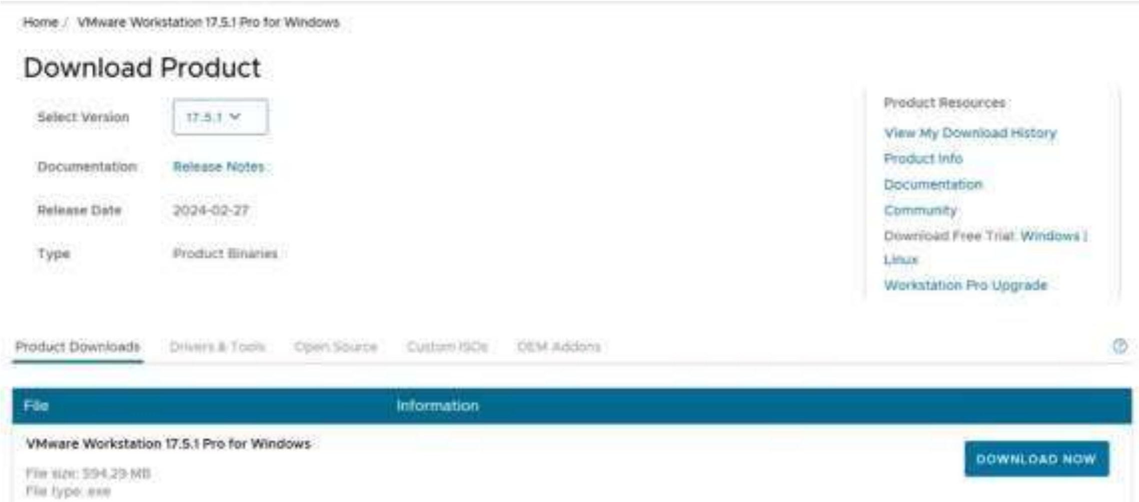
MD 5. Videos

MD 6. Field Visit

8. ACTIVITY BASED LEARNING : UNIT – I

ACTIVITY 1:

Step1: Download and install VMware Workstation Pro



Home / VMware Workstation 17.5.1 Pro for Windows

Download Product

Select Version: 17.5.1

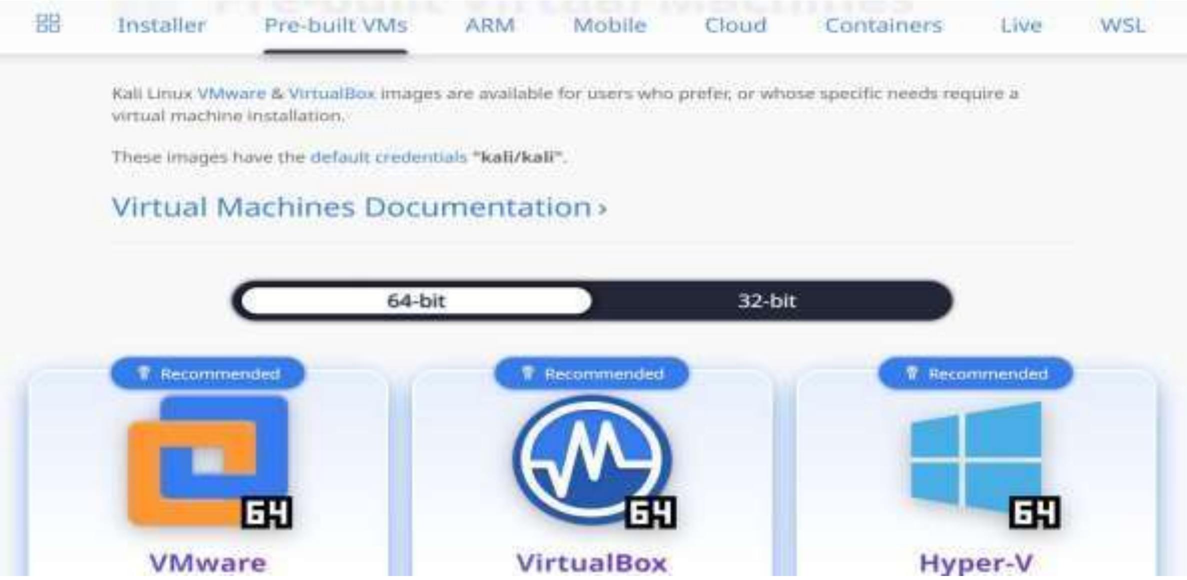
Documentation: Release Notes

Release Date: 2024-02-27

Type: Product Binaries

File	Information
VMware Workstation 17.5.1 Pro for Windows File size: 594.29 MB File type: exe	DOWNLOAD NOW

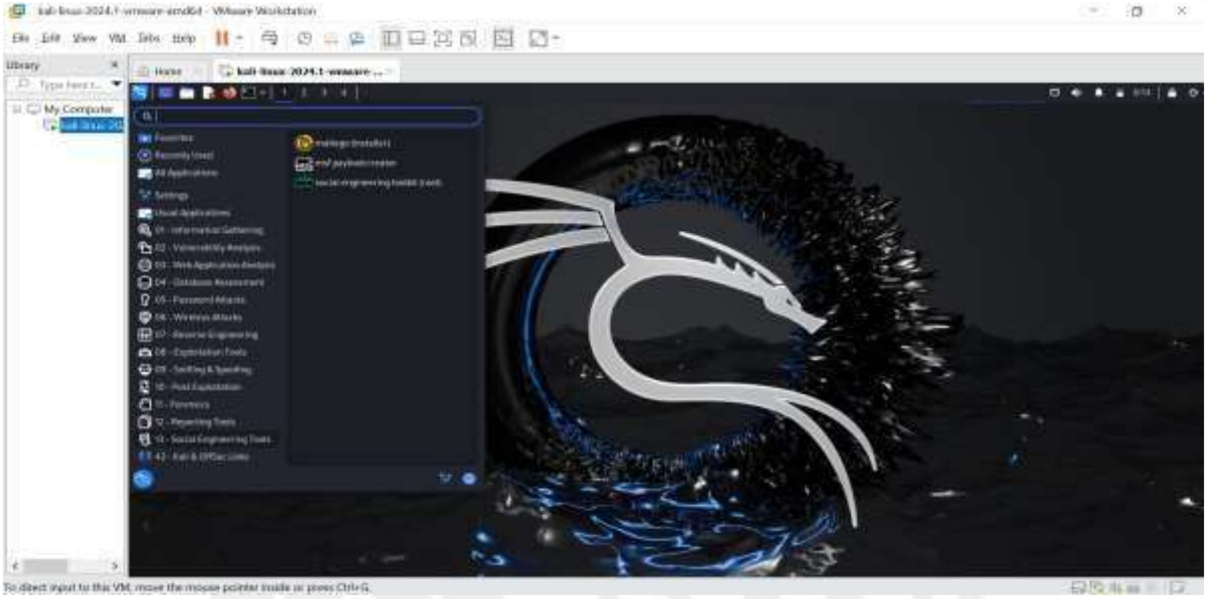
Step2: Download and Install Kali Linux VMware for operating VMware Workstation



Kali Linux VMware & VirtualBox images are available for users who prefer, or whose specific needs require a virtual machine installation.

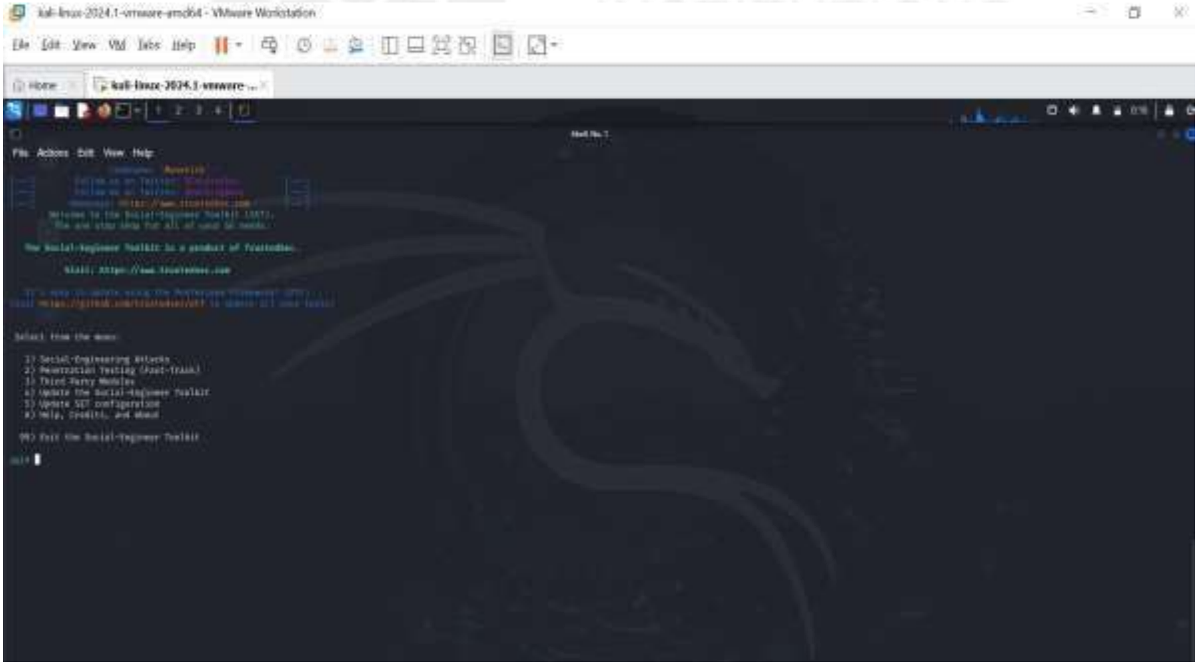
These images have the default credentials "kali/kali".

Step3: Select Social Engineering Toolkit application from Social Engineering Tool



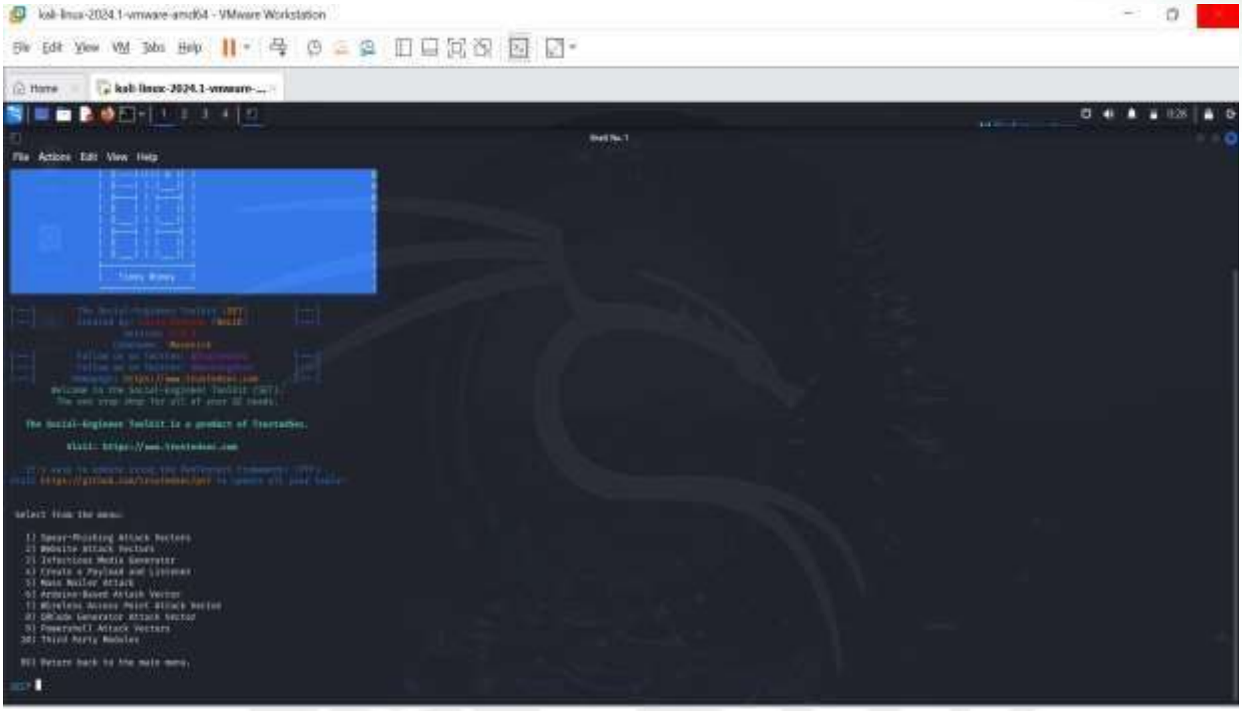
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 4: Select Social Engineering Attacks from Menu


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-...
File Actions Edit View Help

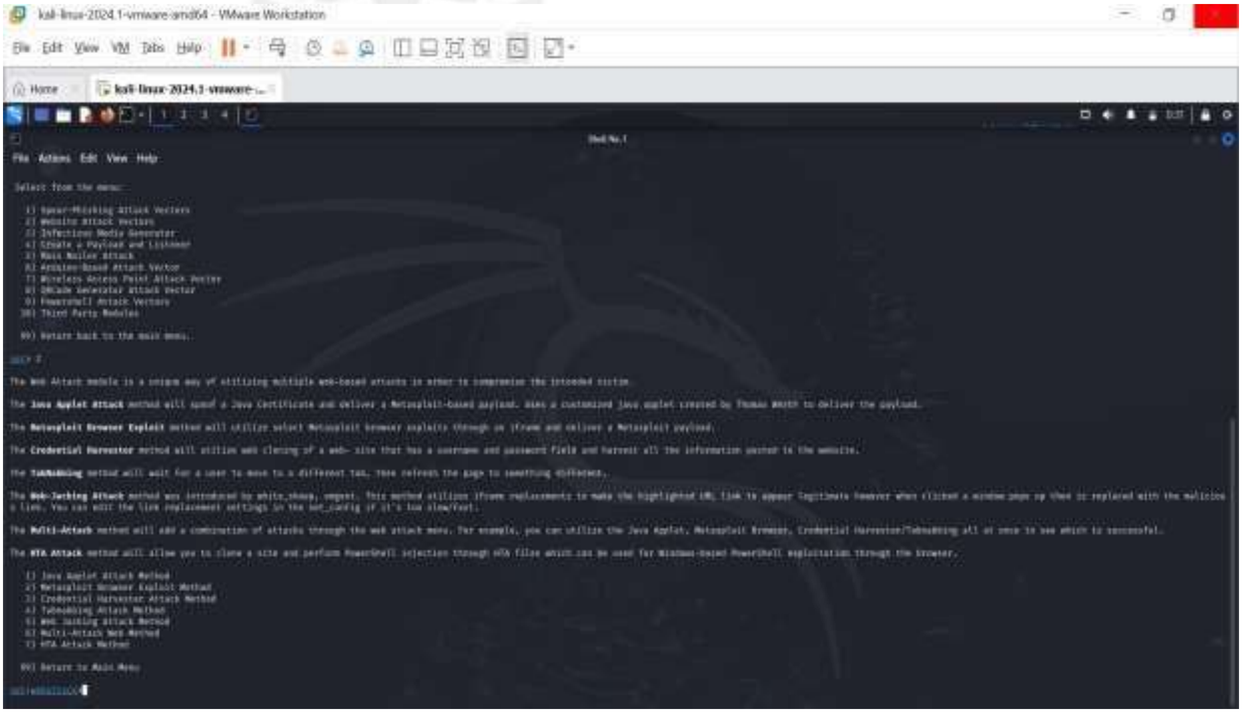
```
            Codename: 'Maverick'
          Follow us on Twitter: @TrustedSec
          Follow me on Twitter: @HackingDave
        Homepage: https://www.trustedsec.com
    Welcome to the Social-Engineer Toolkit (SET).
     The one stop shop for all of your SE needs.

 The Social-Engineer Toolkit is a product of TrustedSec.

        Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

Step 5: Select Website Attack Vectors from Menu


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-...
Shell No. 1
File Actions Edit View Help

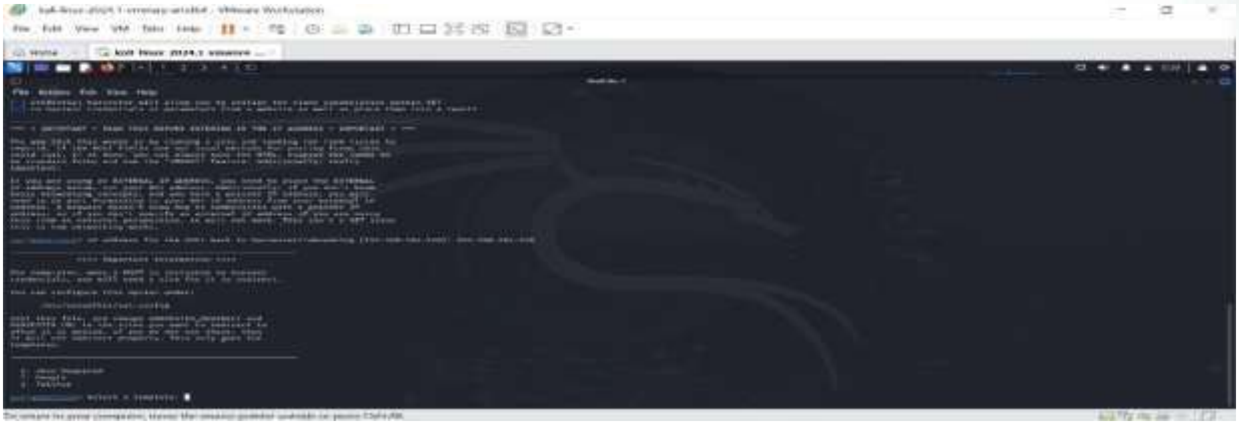
```
             The Social-Engineer Toolkit (SET)
             Created by: David Kennedy (ReL1K)
                      Version: 8.0.3
                    Codename: 'Maverick'
             Follow us on Twitter: @TrustedSec
             Follow me on Twitter: @HackingDave
            Homepage: https://www.trustedsec.com
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set>
```

Step 6: Select Credential Harvester Attack Method from Menu


kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2024.1-vmware-...
Shell No. 1
File Actions Edit View Help

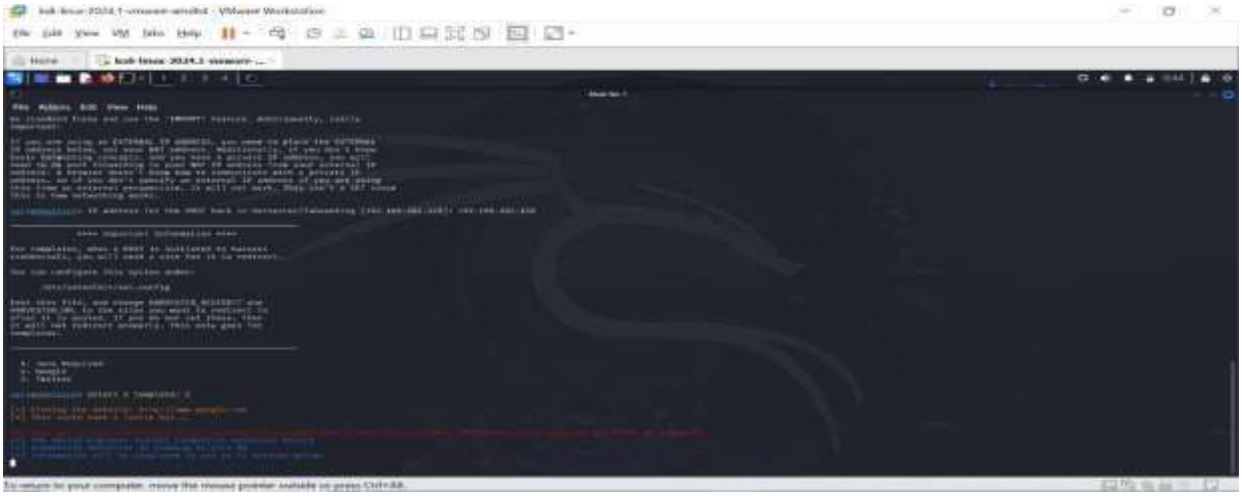
```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicio
s link. You can edit the link replacement settings in the set_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```

Step 7:Select Template of the website from Menu

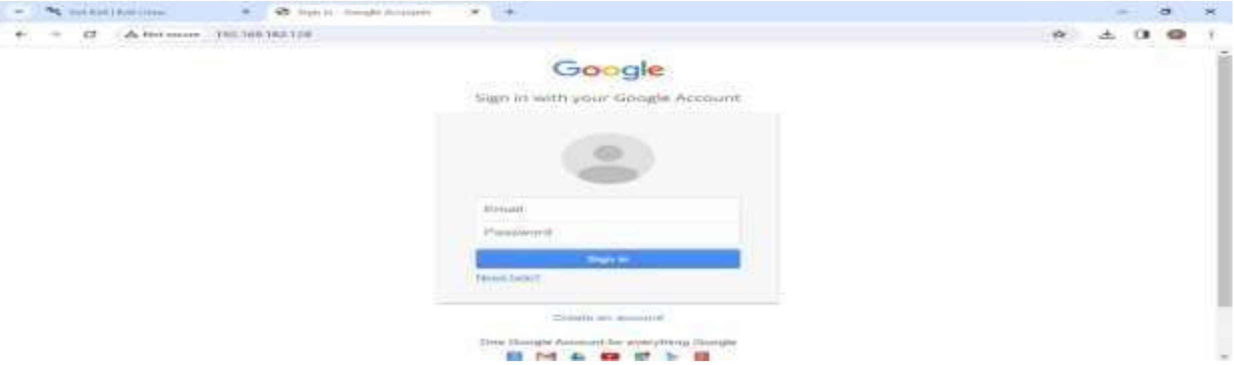


```
**** Important Information ****

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:
```

Step 8: Connect to the website login page through the IP address and sniff the website credentials



```
**** Important Information ****

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 2
```



Google

Sign in with your Google Account

Email

Password

Sign in

Need help?

Create an account

One Google Account for everything Google

Thus, a social networking website login page is created using phishing techniques.

9. LECTURE NOTES : UNIT – II

NETWORK SECURITY BASICS

Syllabus:

Network Security Concepts- Basics of Networks- Common Types of Network Attacks- Introduction to Firewalls- Types of Firewalls- IDS/IPS- Virtual Private Networks (VPN's)- Secure configuration and management of network devices. Case Study: Install Kali Linux on Virtual box.

10. ASSIGNMENTS- UNIT II

SET 1. Explain the various types of network attacks and their impact on network security. Provide real-world examples for at least three types of attacks.

SET 2. Compare and contrast the different types of firewalls. Discuss scenarios in which each type would be most effective.

SET 3: Describe the functioning of IDS and IPS in network defense. How do they differ, and how are they integrated into modern networks?

SET4: Write a report on the installation of Kali Linux on VirtualBox, including all steps, configurations, and screenshots. Discuss how Kali Linux can be used for network security testing.

SET5: Discuss best practices for securing and managing network devices such as routers, switches, and firewalls. Why is it important to follow these practices in enterprise environments?

11.PART A Q & A (WITH K LEVEL AND CO) UNIT 1

1. What is the primary goal of network security?

The primary goal of network security is to ensure the confidentiality, integrity, and availability (CIA) of data transmitted across or stored within networked systems and infrastructure.

2. Explain the CIA triad in network security.K1,CO1

- The CIA triad stands for Confidentiality, Integrity, and Availability, which are the three core principles used to guide and evaluate network security strategies and controls.

3. Differentiate between LAN and WAN. K2,CO1

- A LAN (Local Area Network) connects devices in a limited area like a home or office, while a WAN (Wide Area Network) covers a broader geographical area.

4. What is a network protocol? Give examples. K2,CO1

A network protocol is a set of rules that govern data transmission. Common examples include TCP/IP, HTTP, FTP, and DNS, each serving specific purposes.

5. What is the OSI model and why is it important? K3,CO1

The OSI model is a 7-layer framework that standardizes communication functions, helping troubleshoot, design, and implement interoperable network systems and protocols.

6. What is a Denial of Service (DoS) attack? K3,CO1

A DoS attack overwhelms a system or network with traffic or requests, making it unavailable to legitimate users, often disrupting services significantly.

7. Explain phishing in the context of network attacks.K4,CO1

Phishing is a social engineering attack where attackers deceive users into revealing sensitive data, often via fake emails or websites posing as legitimate entities.

8. What is a Man-in-the-Middle (MitM) attack? K4,CO1

A MitM attack occurs when an attacker secretly intercepts and possibly alters communication between two parties without their knowledge.

9. How does a malware attack compromise network security? K5,CO1

Malware, such as viruses or worms, can infiltrate network devices, steal sensitive information, disrupt services, or provide attackers with unauthorized access.

10. What is packet sniffing and why is it dangerous? K5,CO1 (GATE)

Packet sniffing involves capturing and analyzing data packets transmitted over a network. Attackers use it to steal sensitive information like passwords and private messages.

11. What is the purpose of a firewall in network security? K1,CO1

A firewall monitors and controls incoming and outgoing network traffic based on predetermined security rules, acting as a barrier between trusted and untrusted networks.

12. How does a firewall differ from an antivirus? K1,CO1

A firewall filters network traffic, while antivirus software detects and removes malware. Both are crucial but operate on different aspects of cybersecurity.

13. Describe a packet-filtering firewall. K2,CO1

Packet-filtering firewalls inspect individual data packets and allow or block them based on IP addresses, ports, and protocols without tracking the state of connections.

14. What is a stateful inspection firewall? K2,CO1

A stateful firewall monitors active connections and determines whether a packet is part of an established session, providing more robust security than packet filtering.

15. Explain application-layer firewalls. K3,CO1

Application-layer firewalls operate at the application level of the OSI model, inspecting traffic for specific applications like HTTP or FTP to prevent protocol-based attacks.

16. What is a proxy firewall and how does it work? K3,CO1

A proxy firewall acts as an intermediary between a client and a server, forwarding requests on behalf of the client and filtering content for security.

17. Differentiate between IDS and IPS. K4,CO1

An IDS (Intrusion Detection System) monitors network traffic for suspicious activity, while an IPS (Intrusion Prevention System) can take action to block the threats in real time.

18. What are the types of IDS? K4,CO1

IDS can be classified as Host-based (HIDS) or Network-based (NIDS). HIDS monitors activities on a single host, while NIDS scans network traffic for threats.

19. What is the function of a VPN? K5,CO1 (GATE)

A VPN creates a secure, encrypted tunnel over public networks, allowing users to access private networks remotely and securely, protecting data from eavesdroppers.

20. Explain tunneling in VPNs. K5,CO1

Tunneling is the process of encapsulating one network protocol within another, enabling secure data transmission over an insecure network like the internet.

21. How does encryption secure a VPN connection? (K1,CO1)

Encryption scrambles data during transmission, ensuring that only authorized recipients with the correct decryption keys can access the original information.

22. Why is secure configuration important for network devices? (K2.CO1) (GATE)

Secure configuration eliminates unnecessary services, applies patches, and strengthens passwords to reduce vulnerabilities that attackers can exploit in routers, switches, and firewalls.

23. What are some best practices for managing network devices securely? (K3)

Best practices include disabling unused ports, changing default credentials, applying firmware updates, logging activities, and using secure management protocols like SSH.

24. What are the steps to install Kali Linux on VirtualBox? (K4)

Steps include downloading VirtualBox and the Kali ISO file, creating a new VM, allocating memory and disk space, mounting the ISO, and following the installation wizard.

25. Why use Kali Linux in a virtual environment? (K2)

Running Kali Linux in a virtual environment allows safe testing of penetration tools without affecting the host system or network, ideal for ethical hacking practice.

12.PART B Q s (WITH K LEVEL AND CO) UNIT 1

1. Explain the CIA triad and how it forms the foundation of network security. Illustrate with examples how violations of each aspect (Confidentiality, Integrity, and Availability) can affect an organization.(13) **K2,CO1**

2. Describe the OSI model and discuss its relevance to understanding network communication and security. How does each layer contribute to building a secure network infrastructure?(13) **K2,CO1**

3. List and explain at least five common types of network attacks. For each, describe how the attack works, potential damage, and methods used to mitigate the risk.(13) **K4,CO1**

4. What are firewalls, and how do they function to protect networks? Compare different types of firewalls (packet-filtering, stateful, proxy, application-layer) and explain with appropriate use-cases. (15) **K3,CO1**

5. Discuss Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). Explain the key differences, types of IDS/IPS, and their role in enhancing network security. Include examples where possible.(8) **K3,CO1**

6. Define and explain the concept of a Virtual Private Network (VPN). Describe how VPNs ensure secure communication over public networks and discuss the protocols involved (e.g., IPsec, PPTP, L2TP).(15) **K2,CO1**

13. Supportive online Certification courses

1. Udacity: **ENTERPRISE CYBER SECURITY**

   https://www.udacity.com/course/enterprise-security-nanodegree--nd0035

2. NPTEL: **ENTERPRISE CYBER SECURITY**

   https://onlinecourses.nptel.ac.in/noc23_cs127/preview

14. Real time applications in day to day life and to Industry

❖ Burp Suite

Companies that want to run security tests on web apps should use this service. It includes various hacker applications that operate together to support the entire pen-testing procedure. It has everything from the initial mapping to analyzing an app's attack surface.

➢ Burp Suite has the following features:

✓ A prominent ethical hacking software that discovers over 3000 online application flaws.

✓ Examines custom apps as well as open-source software and code.

✓ It comes with an easy-to-use Login Sequence Recorder that enables automated scanning.

✓ Its built-in vulnerability management examines data safety.

✓ It detects key network vulnerabilities with 100 percent precision.

✓ Easily generates a wide range of compliance and technical data.

✓ Scanning and crawling capabilities are automated.

❖ Metasploit

Metasploit is a hacking framework that focuses on ethical hacking. It's an open-source ethical hacking app. The framework is built with Ruby, and ethical hackers use it to find flaws and write code to fix them.

➢ Metasploit's key features include:

✓ How to get past detecting systems.

✓ Attacks that are launched from afar.

✓ There is a list of all networks and hosts.

✓ Scanning for vulnerabilities using various methods.

15. ASSESSMENT SCHEDULE

Tentative schedule for the Assessment During 2021-2022 ODD semester

S.NO	Name of the Assessment	Start Date	End Date	Portion
1	Unit Test 1			UNIT 1
2	IAT 1			UNIT 1 & 2
3	Unit Test 2			UNIT 3
4	IAT 2			UNIT 3 & 4
5	Revision 1			UNIT 5 , 1 & 2
6	Revision 2			UNIT 3 & 4
7	Model			ALL 5 UNITS

16. PRESCRIBED TEXT BOOKS & REFERENCE BOOKS

TEXT BOOKS:

1. Anand Shinde, “Introduction to Cyber Security Guide to the World of Cyber Security”, Notion Press, 2021.
2. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education, 2018.

REFERENCES:

1. William Stallings, "Cryptography and Network Security - Principles and Practice", Seventh Edition, Pearson Education, 2017.
2. Ravi Das and Greg Johnson, “Testing and Securing Web Applications”, 2021.
3. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O’Reilly Media, Inc, 2020.

17. MINI PROJECT SUGGESTION

SET 1: Simulate and Analyze Common Network Attacks Using Kali Linux

SET2: Configure and Demonstrate a Firewall Setup for a Secure Network

SET3: Create a Virtual Private Network (VPN) and Test Secure Remote Access

SET4: Install and Evaluate IDS/IPS Tools (Snort/Suricata) in a Virtual Network

SET5: Design and Secure a Small Office Network Architecture

18. GATEQUESTIONS

1. Which of the following best represents the Availability aspect of the CIA triad?
A. Preventing unauthorized access to data
B. Ensuring that data is not altered without authorization
C. Ensuring systems and data are accessible when needed
D. Encrypting data during transmission
Answer: C

2. A firewall operates at which OSI layer(s)?
A. Physical and Data Link
B. Network and Transport
C. Transport and Application
D. Varies depending on the type of firewall
Answer: D

3. Which of the following attacks can be mitigated using a properly configured IDS/IPS system?
A. Insider data theft
B. Physical theft of hardware
C. SQL injection and port scans
D. Natural disasters
Answer: C

4. Which one of the following protocols is commonly used in VPNs for encryption and tunneling?
A. HTTP
B. FTP
C. Ipsec
D. DNS
Answer: C

5. Which statement is TRUE about a Man-in-the-Middle (MitM) attack?
A. It encrypts data at rest in a server
B. It is a type of phishing attack
C. The attacker intercepts communication between two parties
D. It is a form of physical attack
Answer: C

6. In a packet-filtering firewall, which of the following information is NOT used to make decisions?
A. Source IP address
B. Destination port number
C. Packet payload content
D. Transport layer protocol
Answer: C

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in relianceon the contentsof this informationis strictlyprohibited.