Day 1: STTP on Ethical Hacking and Cyber Forensics @IIITK

Dr. Jobin Jose & Dr. Fasila K.A

June 9, 2025

1. Introduction to Ethical Hacking

1.1. Passive Reconnaissance

Passive reconnaissance, as introduced by Jobin Jose, is a key step in information gathering for ethical hacking. It involves collecting information without directly interacting with the target system. This method utilizes publicly available sources like websites and search engines.

1.2. Phases of Penetration Testing

Ethical hacking follows a structured approach, typically involving several phases.

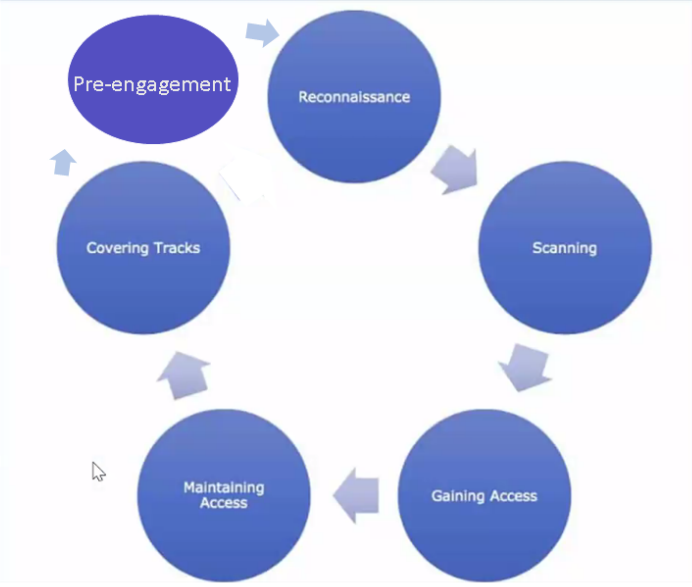

Figure 1: Phases of Penetration Testing

The phases include:

1. **Pre-Engagement**: This is a phrase where the tester communicates with the client and determines the scope of test and other valid details.
2. **Reconnaissance**: The initial phase of information gathering.
3. **Scanning and Enumeration**: Identifying live hosts, open ports, services, and system information.
4. **Gaining Access**: Exploiting vulnerabilities to gain unauthorized entry.
5. **Escalation of Privileges**: Increasing access rights within the compromised system.
6. **Maintaining Access**: Ensuring persistent connection to the system.
7. **Covering Tracks**: Removing evidence of the intrusion.

1.3. Reconnaissance: Information Gathering

Reconnaissance is the crucial first phase of hacking. It is broadly split into three parts:

1. **Footprinting**: Passive collection of information about an organization.
2. **Scanning**: Active reconnaissance methods, such as Nmap scanning, to extract information about networks and systems.
3. **Enumeration**: Using gathered information to identify attack areas after footprinting and scanning.

1.3.1 Types of Reconnaissance

There are two primary types of reconnaissance:

- **Passive Reconnaissance**: Gathering information without direct interaction with the target system, using publicly available sources.
  - **Tools/Methods**: Exiftool (geolocation extraction), Sherlock (social media search), Image search (Google, Yandex), Location identification (Google Maps, Google Earth).
- **Active Reconnaissance**: Directly interacting with the target system, which carries a higher risk of detection.(Not covered in the session)
  - **Techniques**: Network scans, vulnerability scans.

2. Introduction to Cybersecurity

Dr. Fasila K.A introduces cybersecurity as the process of securing sensitive data and critical systems from cyber attacks. [Intro to Cybersecurity slides, page 1]

2.1. Objective of Cybersecurity

The main goal of cybersecurity is to preserve the confidentiality, integrity, and availability (CIA Triad) of an organization's critical assets from attack, damage, or unauthorized access.

Key ways to lower the risk of cyber attacks include:

- Reduce data transfers
- Update software regularly
- Download carefully and verify sources
- Monitor for data leaks
- Improve passwords
- Develop a breach response plan

2.2. Cybersecurity Terminologies

Important terms in cybersecurity:

- **Threat**: A potential danger that could exploit a vulnerability.
- **Assets**: Anything that adds value to an organization (physical, hardware, software, information, personnel).
- **Risk**: The likelihood of a threat exploiting a vulnerability and the impact it would have.
- **Vulnerability**: A weakness or flaw in a system that can be exploited by a threat.
- **Exploit**: A piece of software, data, or sequence of commands that takes advantage of a bug or vulnerability.
- **Payload**: The part of malware that performs the malicious action.
- **0-day**: A newly discovered software vulnerability for which no patch has been released.

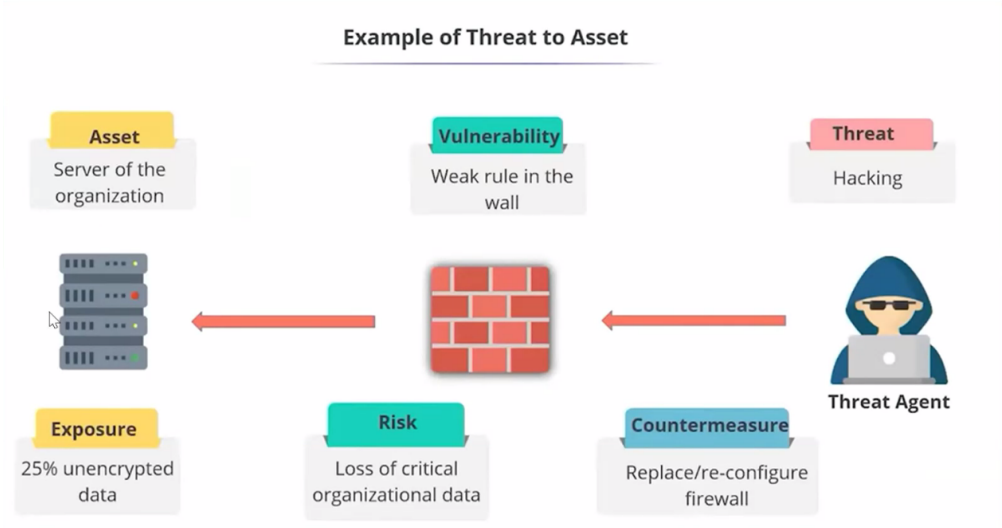

Figure 2: Example of Threat to Asset

An asset (e.g., server) can have a vulnerability (e.g., weak firewall rule) that a threat (e.g., hacking) can exploit, leading to a risk (e.g., loss of data). Countermeasures (e.g., reconfiguring the firewall) can reduce this risk.

2.3. Asset Classification and Protection

2.3.1 Asset Classification

1. Prepare an inventory of assets and allocate to owners.
2. Classify assets by business value.
3. Assign business value based on criticality, operations, or sensitivity.
4. Determine overall risk to asset.
5. Determine classification level by potential impact.
6. Allocate protection resources based on business value.

2.3.2 Asset Protection

Asset protection involves security management practices that align with business and compliance requirements. These practices are known as security controls.

Types of security controls:

- Physical entry controls (e.g., to office buildings).
- Monitoring controls (e.g., CCTV).
- Hardware protection controls (e.g., locks).
- Tamper proofing (e.g., hashing, encryption for software and data).

- Intellectual property protection (e.g., copyrights, patents).
- Identity management systems.

2.4. Types of Cyber Attacks

Cyber attacks vary in their methods and objectives:

- **Malware**: Includes viruses, worms, trojans, and spyware that damage or steal data. The number of malware incidents slightly decreased in 2024.
- **Phishing**: Deceptive emails, websites, or SMS messages tricking users into revealing information.
- **Ransomware**: Encrypts data and demands payment. One of the most costly cyber attacks for businesses.
- **DDoS (Distributed Denial of Service)**: Overwhelms systems with excessive traffic to cause downtime. DDoS attacks increased by 13% in Q1 and Q2 2024, with over 8 million incidents.
- **Man-in-the-Middle**: Intercepts communications to steal or alter data unnoticed.

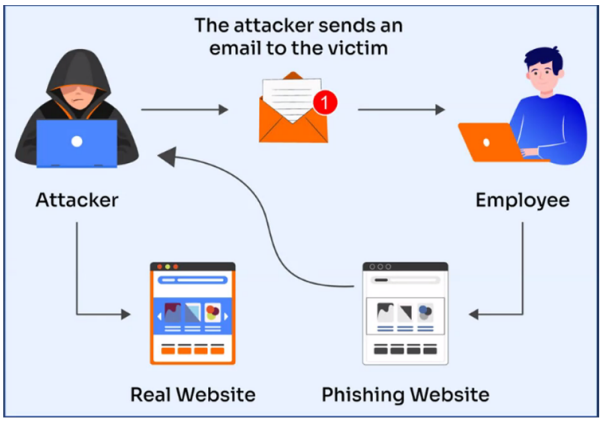

Figure 3: Phishing Attack Flow

A phishing attack often involves an attacker sending a deceptive email to a victim, leading them to a fake website that mimics a real one to steal credentials.

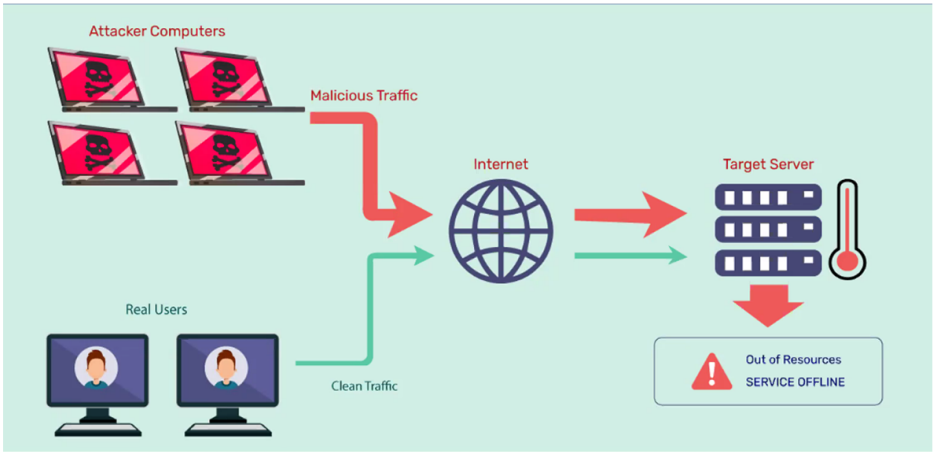

Figure 4: DDoS Attack Diagram

In a DDoS attack, multiple attacker computers generate malicious traffic, overwhelming a target server and rendering its service offline.

2.5. CIA Triad: Confidentiality, Integrity, Availability

The CIA Triad is a fundamental model in cybersecurity, representing three primary features for securing information and systems.

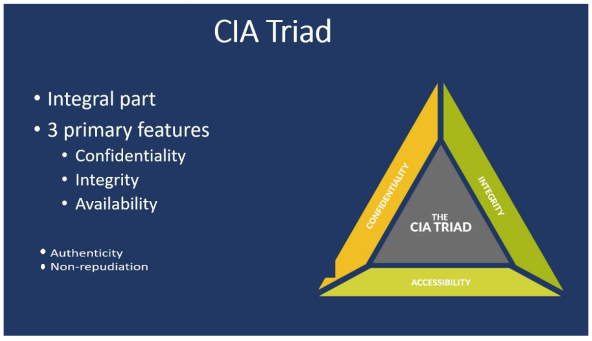

Figure 5: The CIA Triad

2.5.1 Confidentiality

Confidentiality means private or confidential information should not be disclosed to unauthorized individuals.

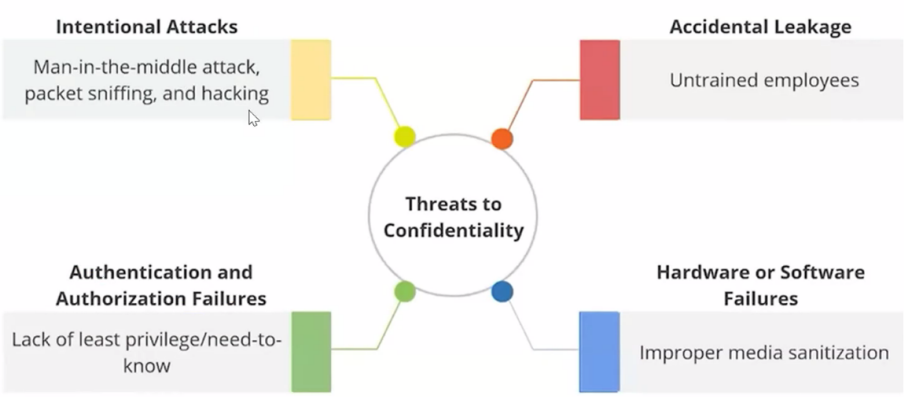

Figure 6: Threats to Confidentiality

Countermeasures to ensure confidentiality:

- **Encryption**: Converts information to an unreadable format.
- **Access Control**: Prevents unauthorized access to confidential information.
- **Administrative**: Confidentiality policies and Non-Disclosure Agreements (NDAs).

2.5.2 Integrity

Integrity means information or systems should be protected from intentional, unauthorized, or accidental changes.

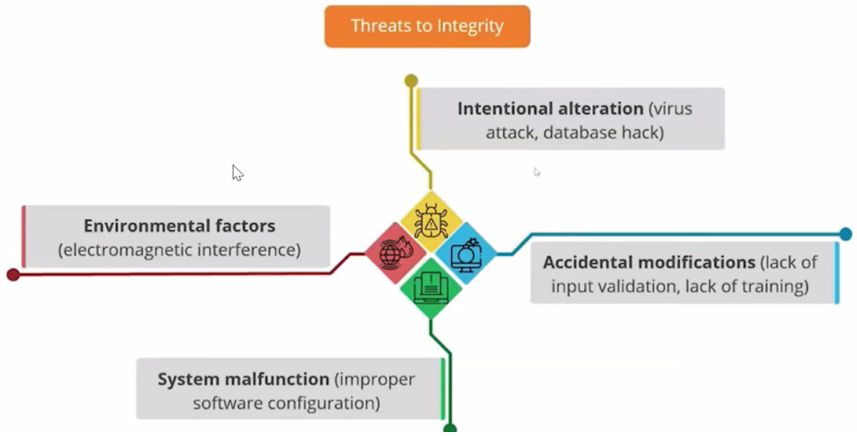

Figure 7: Threats to Integrity

Countermeasures to ensure integrity:

- **Cryptographic Hash**: Hash value of a file can be used to detect modifications.
- **Checksums**: Detect errors and reconstruct missing data.
- **Database Integrity**: Referential and entity integrity ensure logical integrity.

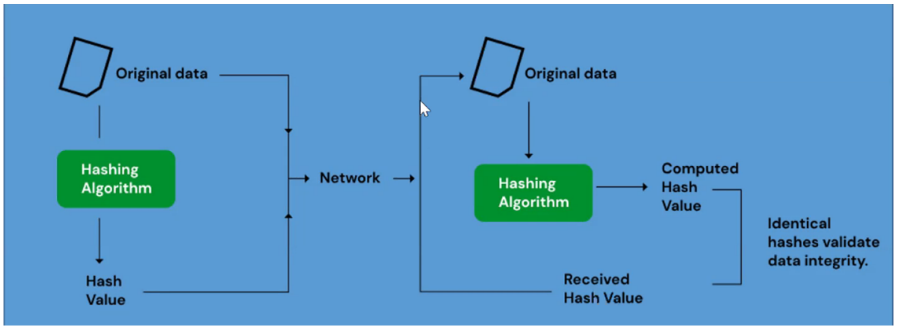

Figure 8: Online Hash Calculator - Data Integrity Validation

Hashing validates data integrity by comparing the computed hash of received data with the original hash. An online hash calculator like `https://www.tools4noobs.com/online_tools/hash/` can be used for this purpose.

2.5.3 Availability

Availability refers to ensuring that authorized users have timely and uninterrupted access to information and resources.

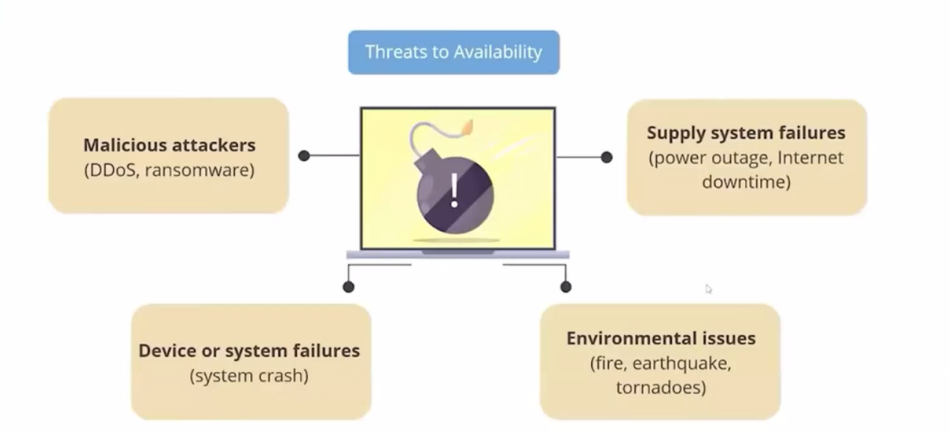

Figure 9: Threats to Availability

Threats to Availability: **Countermeasures to ensure availability**:

- **High Availability**: Ensure system availability at all times.
- **Backup Procedures**: Ensure data restoration after a disaster.
- **Security Devices**: Prevent DoS/DDoS attacks using IPS (Intrusion Prevention System) and WAF (Web Application Firewall).

3. Cybersecurity Teams: Red Team vs. Blue Team

To defend against cyber threats, it's crucial to understand the attacker's perspective and the defender's role. This is often conceptualized as Red Team vs. Blue Team.

Figure 10: Red Team vs. Blue Team Roles

- **Red Team**:
  - Focuses on Offensive Security, Ethical Hacking, Exploiting Vulnerabilities.
  - Conducts Penetration Tests, Black Box Testing, Social Engineering, Web App Scanning.
  - Simulates attacks to test the organization's security posture and identify weaknesses.
- **Blue Team**:
  - Focuses on Defensive Security, Infrastructure Protection, Damage Control.
  - Handles Incident Response, Operational Security, Threat Hunting, Digital Forensics.
  - Performs vulnerability assessments and security audits to identify vulnerabilities and test control effectiveness.
  - Primary objective is to defend against and predict/prevent attacks.

4. Cyber Kill Chain (CKC)

The Cyber Kill Chain is a framework that helps to understand and respond to cyber threats. It outlines the stages of a typical cyber attack, from initial planning to data exfiltration or system disruption.

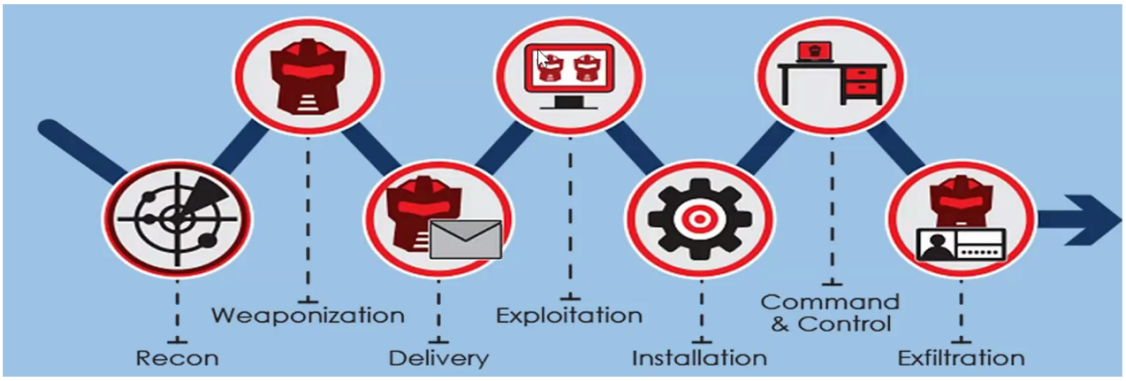

Figure 11: Stages of a Typical Cyber Attack (Cyber Kill Chain)

4.1. 7 Stages of the Cyber Kill Chain

1. **Reconnaissance**: Attackers gather information about their target (e.g., network architecture, vulnerabilities, entry points).

2. **Weaponization**: Attackers develop or obtain malicious tools and payloads (e.g., malware, exploit kits).

3. **Delivery**: Attackers transmit their weapons to the target (e.g., phishing emails, compromised websites).

4. **Exploitation**: Attackers leverage vulnerabilities to gain unauthorized access to systems.

5. **Installation**: Attackers establish a foothold on compromised systems, often by deploying backdoors or creating user accounts.

6. **Command and Control (C2)**: Attackers establish communication channels to remotely control and manipulate compromised systems.

7. **Actions on Objectives**: Attackers execute their goals (e.g., data exfiltration, system disruption, other malicious activities).

4.2. MITRE ATT&CK Framework

While CKC provides a bird's-eye view, the MITRE ATT&CK Framework offers a more granular knowledge base of real-world adversary behaviors, detailing Tactics, Techniques, and Procedures (TTPs).

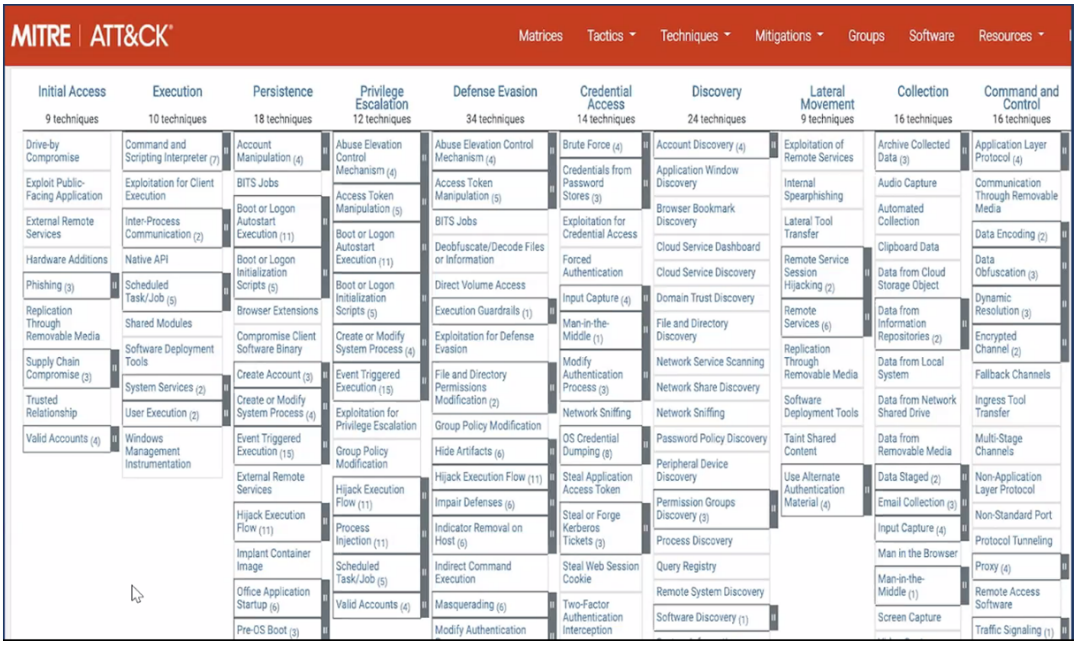

Figure 12: MITRE ATT&CK Framework Matrix

The MITRE ATT&CK framework is a comprehensive matrix categorizing various adversarial tactics and techniques used in cyber attacks.

5. Ethical Hacking and Penetration Testing

5.1. Ethical Hacking Overview

Ethical hacking is the authorized practice of testing and evaluating the security of systems, networks, or applications to identify exploitable vulnerabilities. It involves using the same tools, techniques, and processes as malicious hackers, but with permission, to find and fix security flaws.

5.1.1 Prerequisites: Skills and Knowledge

- **Networking**: Strong grasp of TCP/IP, OSI model, and protocols.
- **Operating Systems**: Proficiency in Windows and Linux environments.
- **Programming**: Knowledge of Python, C++, Bash scripting essentials.
- **Security Basics**: Understanding cryptography and core security principles.

5.1.2 Types of hackers

Black Hat Hackers

Black Hat hackers are criminals who break into computer networks with malicious intent. They may release malware that destroys files, holds computers hostage, or steals sensitive information like passwords, credit card numbers, and personal data. Their actions are illegal and driven by personal or financial gain.

- **Primary Goal:** Malicious activities such as data theft, financial fraud, espionage, or cyber vandalism.
- **Legality:** Strictly illegal.
- **Analogy:** A digital burglar or vandal.

White Hat Hackers

Often referred to as "ethical hackers," White Hat hackers are cybersecurity experts who use their skills for good. They are typically hired by organizations to test the security of their systems. They use the same techniques as Black Hats but with the owner's permission and the goal of finding and fixing vulnerabilities before they can be exploited.

- **Primary Goal:** To identify and remediate security vulnerabilities with proper authorization.
- **Legality:** Completely legal and ethical.
- **Analogy:** A security guard or a digital locksmith hired to test the locks.

Grey Hat Hackers

Grey Hat hackers operate in the ambiguous space between White and Black Hats. They may search for vulnerabilities in a system without the owner's permission. If they find one, they might report it to the owner, sometimes requesting a fee to fix it. While their intentions may not be malicious, their unauthorized methods are legally and ethically questionable.

- **Primary Goal:** To find vulnerabilities, often for public recognition or a potential bounty, without prior consent.
- **Legality:** Operates in a legal grey area; their actions can be considered a crime.
- **Analogy:** A citizen who picks the lock on a stranger's house to show them it's insecure.

Red Hat Hackers

Red Hat hackers aim to stop malicious attackers (Black Hats), but their methods are far more aggressive than White Hats. A Red Hat hacker will actively go on the offensive to dismantle a Black Hat's infrastructure. Their approach can be ruthless and may involve launching counter-attacks to destroy the attacker's machine.

- **Primary Goal:** To neutralize and stop Black Hat hackers using offensive tactics.
- **Methodology:** Proactive and often destructive counter-attacks.
- **Analogy:** A digital vigilante who fights fire with fire.

Green Hat Hackers

Green Hat hackers are the novices or "newbies" of the hacking world. They are characterized by their enthusiasm and a strong desire to learn the skills of the trade. While not yet experts, they are on the path to becoming more proficient and are often found on forums asking questions to learn from experienced hackers.

- **Primary Goal:** To learn and grow into a more skilled hacker.
- **Key Characteristic:** A strong sense of curiosity and a willingness to learn.
- **Analogy:** An apprentice in the field of cybersecurity.

Blue Hat Hackers

Blue Hat hackers are external security professionals hired by a company to perform rigorous vulnerability testing on a new system *before* it is launched. They are brought in for a specific project to find and report flaws so they can be fixed pre-release. The term is famously associated with Microsoft's security events.

- **Primary Goal:** To conduct bug testing and find security loopholes in pre-launch software.
- **Nature of Work:** Contract-based, focused on a specific system or software.
- **Distinction:** Differs from a White Hat as they are external and focus on pre-deployment systems.

5.2. Ethical Hacking vs. Penetration Testing

- **Ethical Hacking**:

- Broad term for legally hacking systems to find and fix vulnerabilities.
- Identifies all possible vulnerabilities across multiple layers and improves security posture.
- Broader toolset: reconnaissance, exploitation, social engineering, etc.

- **Penetration Testing**:
  - A focused, simulated cyber attack on a system to test its defenses.
  - Assesses specific entry points and determines how far an attacker can go.
  - Uses specific tools for scanning and exploitation (e.g., Nmap, Metasploit).

5.3. What is Penetration Testing?

Penetration testing is the process of simulating an attack on a network or system to evaluate its security posture and identify exploitable vulnerabilities. It is achieved by simulating various types of attacks on the target network or host, with documented results. It requires written permission and authorization, including scope and timeline, from management.

5.3.1 Penetration Testing Methodologies

Both proprietary and open-source methodologies exist. **Open source methodologies**:

1. **OSSTMM** - Open Source Security Testing Methodology Manual (`https://www.isecom.org/OSSTMM.3.pdf`)
2. **OWASP** - Open Web Application Security Project (`https://owasp.org/www-project-web-securi assets/archive/OWASP_Testing_Guide_v4.pdf`)

5.3.2 Penetration Testing Approaches

- **Black-Box**: No prior knowledge of the target system. Simulates an external attacker.
- **Grey-Box**: Partial knowledge of the target system. Simulates an internal threat (e.g., disgruntled employee).
- **White-Box**: Full knowledge of the target system. Simulates an attacker with privileged access.

5.4. Phases of Penetration Testing

Penetration testing follows distinct phases:

1. **Pre-Engagement Phase**:
   - Define rules of engagement and goals.
   - Identify scope, timeline, target systems.
   - Define testing approach (black box, white box, grey box).

- Obtain written authorization.
- Discuss legal and compliance boundaries.

2. **Reconnaissance**:
   - Information Gathering (Passive and Active).
   - Tools (e.g., mentioned earlier in reconnaissance section like Exiftool, Sherlock, Nmap).
3. **Scanning & Enumeration**:
   - Vulnerability Identification: Spot weaknesses to exploit in target systems.
   - Port Scanning: Discover open ports and running services.
   - Scanning Tools: Nessus, OpenVAS.
4. **Gaining Access (Exploitation Techniques)**:
   - Buffer overflows.
   - SQL injection.
   - Other common attack vectors.
5. **Maintaining Access & Covering Tracks**:
   - Persistent Access: Keep connection without alerting system defenders.
   - Covering Tracks: Alter logs and traces to avoid detection.
6. **Reporting**:
   - Documentation: Record process, findings, and vulnerabilities.
   - Detailed Reporting: Create comprehensive reports for clients.
   - Remediation Suggestions: Offer actionable strategies to fix issues.

6. Lab Setup: Virtualization Basics

6.1. Requirements for Lab Setup

- VirtualBox or VMware.
- Virtual machines (VMs).

6.2. Virtualization Explained

Virtualization allows you to run multiple operating systems (OS) on a single physical machine using Virtual Machines (VMs).

- **Host Machine**: Your physical computer.
- **Virtual Machine (VM)**: A simulated computer running inside the host machine.
- **Hypervisor**: Software that manages VMs.

Two common virtualization tools are Oracle VirtualBox and VMware Workstation.

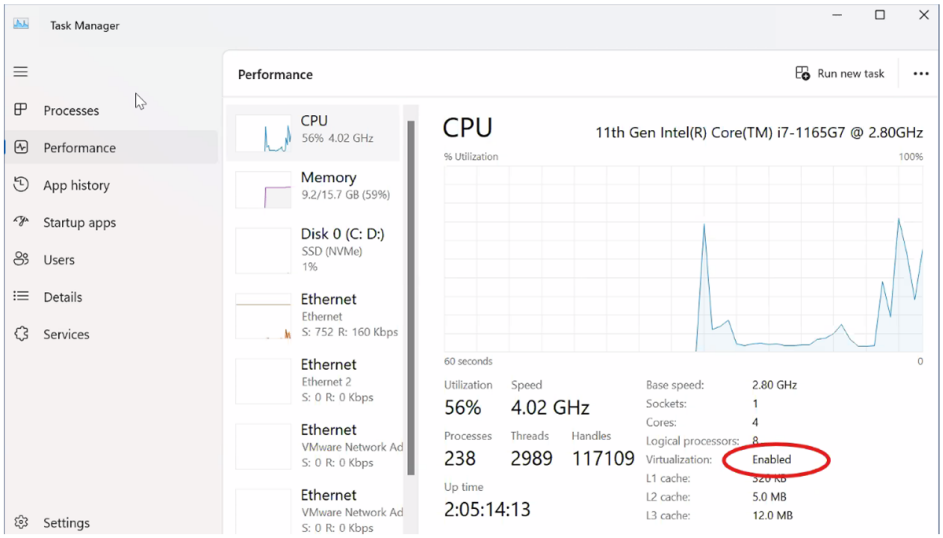

Figure 13: Task Manager showing Virtualization Enabled

To check if virtualization is enabled on Windows, you can open Task Manager and look under the 'Performance' tab, then 'CPU' to see if 'Virtualization' is enabled.

6.3. Oracle VirtualBox

VirtualBox is a free, open-source virtualization tool developed by Oracle.

6.3.1 Key Features

:

- Cross-platform (Windows, Linux, macOS).
- Supports snapshots, shared folders, USB device access.
- Lightweight and user-friendly.
- Good for beginners and students.

6.3.2 VirtualBox Installation Steps (Visual Walkthrough)

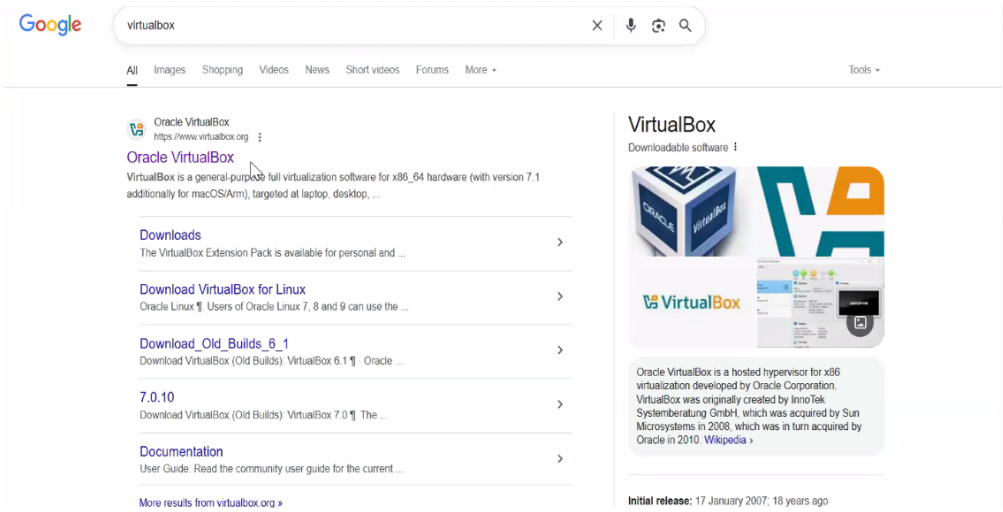

Figure 14: Google Search for VirtualBox

Step 1: Search for "virtualbox" on Google and navigate to `https://www.virtualbox.org`.

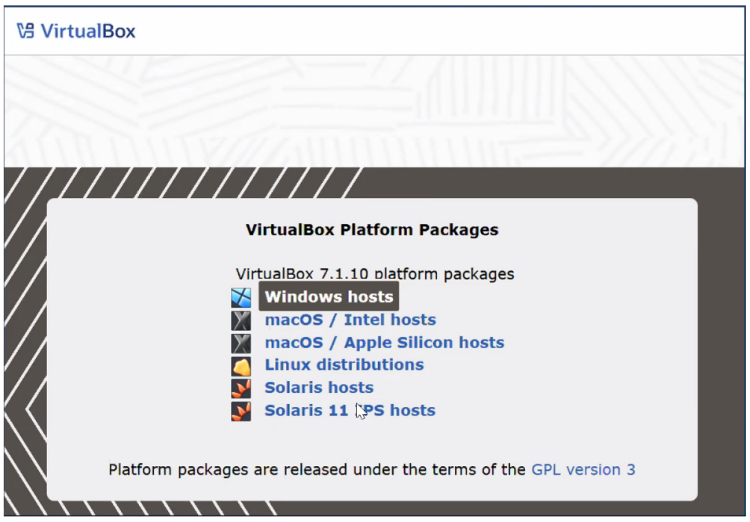

Figure 15: VirtualBox Platform Packages Selection

Step 2: Choose the appropriate platform package (e.g., Windows hosts, macOS, Linux distributions) for your host operating system.

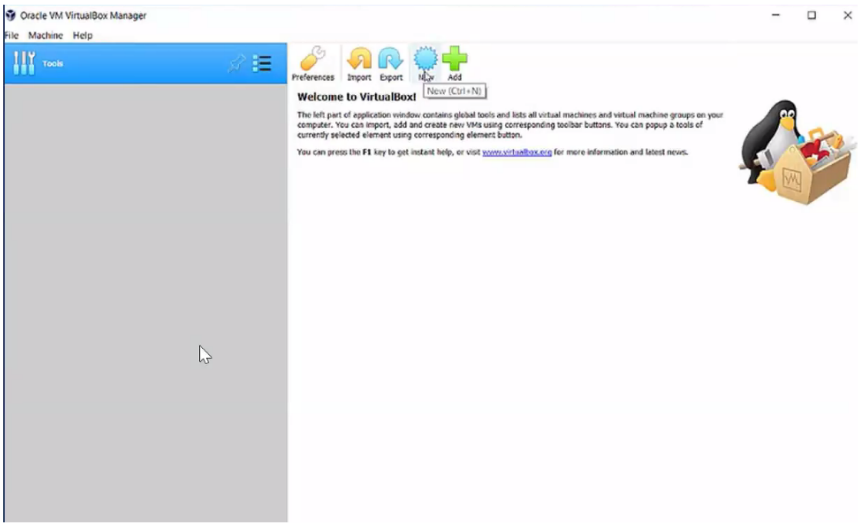

Figure 16: Oracle VM VirtualBox Manager Interface

Step 3: After installation, open the Oracle VM VirtualBox Manager.

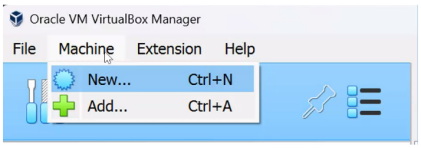

Figure 17: Creating a New Virtual Machine

Step 4: Go to "Machine" and select "New..." (Ctrl+N) to create a new virtual machine.

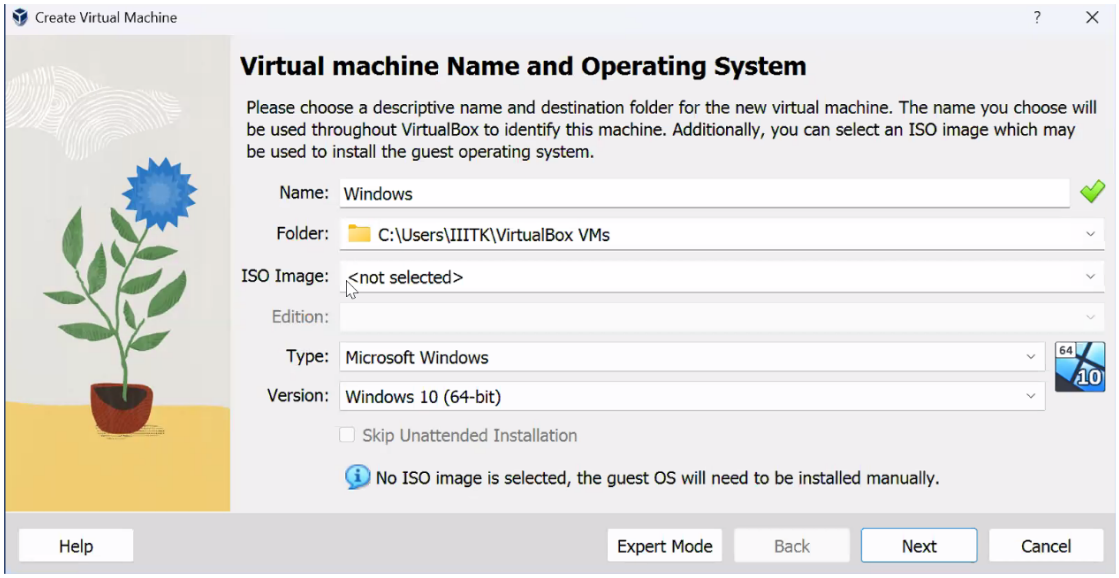

Figure 18: Virtual Machine Name and Operating System Setup

Step 5: In the "Create Virtual Machine" wizard, specify a name for your VM, choose the destination folder, select the ISO Image (if you have one), and verify the Type and Version of the OS.

6.3.3 Installing Ubuntu VM in VirtualBox

Reference: For detailed steps, refer to `https://ubuntu.com/tutorials/how-to-run-ubuntu-desktop-or 1-overview`.

6.3.4 Installing Kali Linux VM on VirtualBox

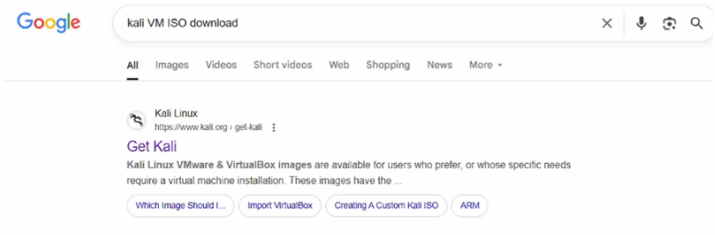

Figure 19: Google Search for Kali Linux VM Download

Step 1: Search for "kali VM ISO download" and go to the official Kali Linux website `https://www.kali.org/get-kali/`.

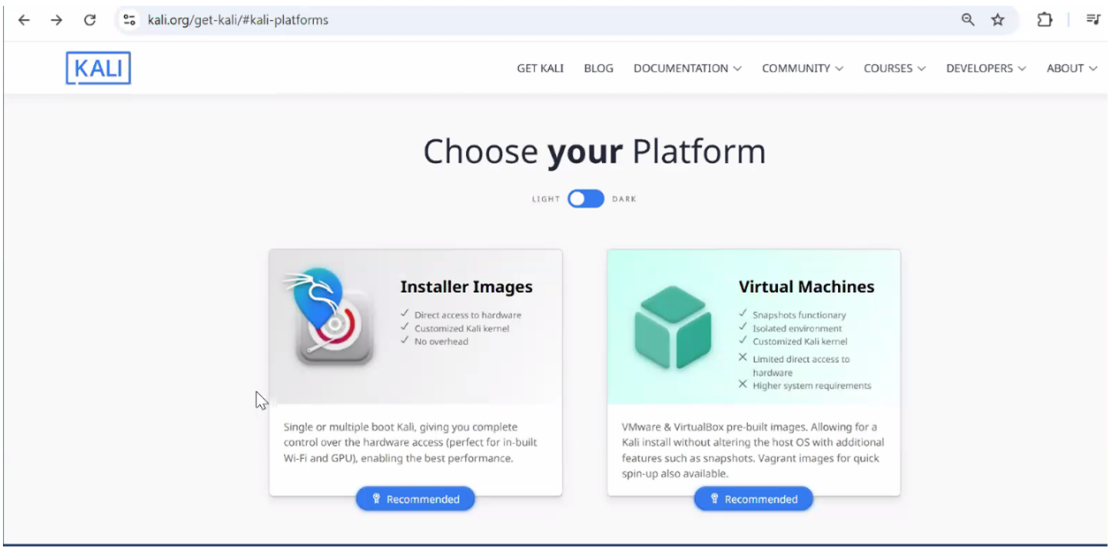

Figure 20: Kali Linux Platform Choice: Installer vs. Virtual Machines

Step 2: Choose "Virtual Machines" to download pre-built images for VMware & VirtualBox.

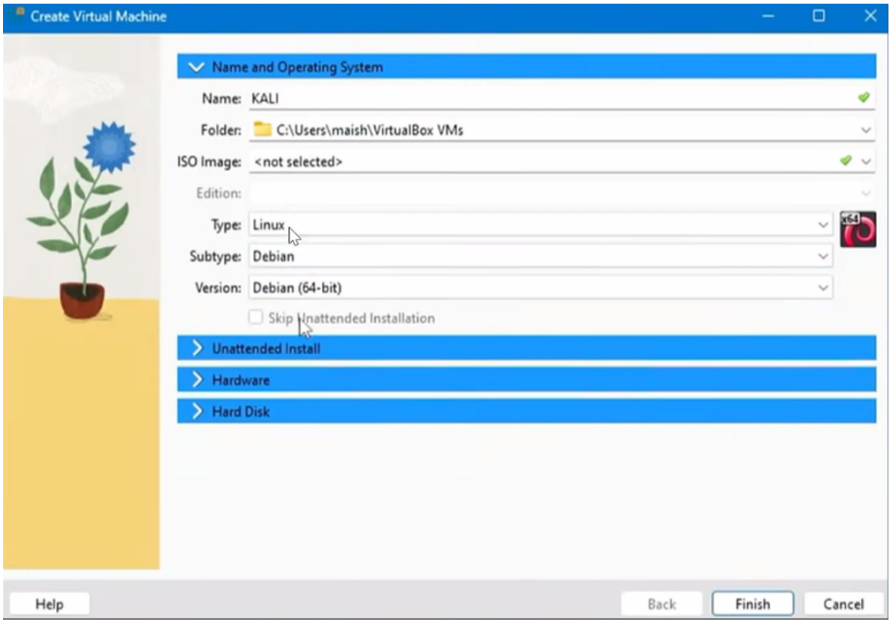

Figure 21: VirtualBox Setup for Kali Linux VM

Step 3: Follow the VirtualBox new VM creation wizard, ensuring to select 'Linux' as Type and 'Debian (64-bit)' as Subtype.

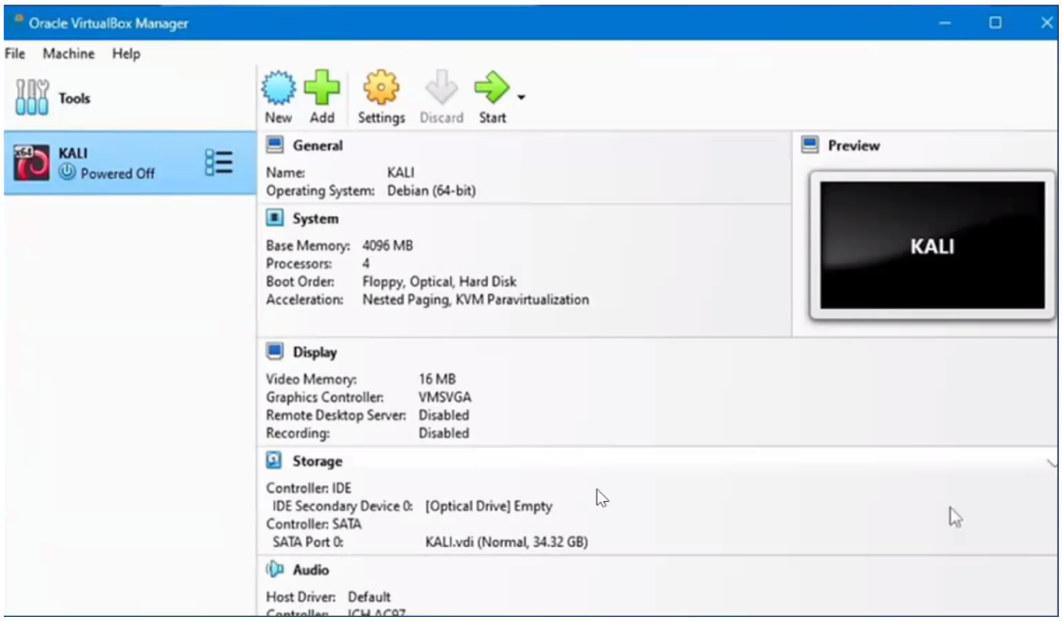

Figure 22: Kali Linux VM Settings Summary in VirtualBox

Step 4: Review the VM settings, such as Base Memory, Processors, Boot Order, and Display settings, before starting the VM.

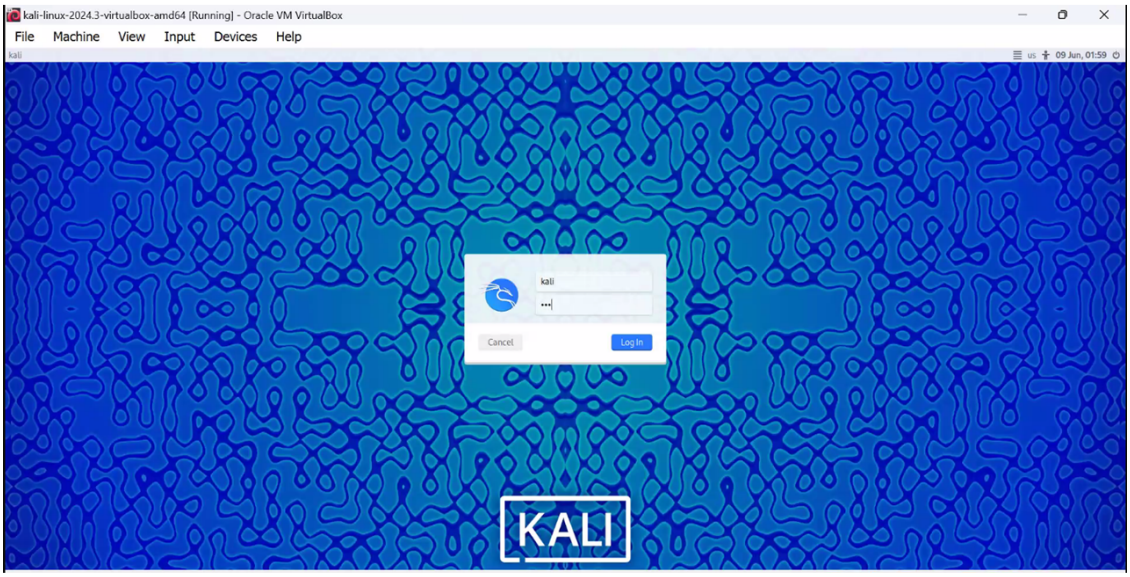

Figure 23: Kali Linux Login Screen

Step 5: Boot the Kali Linux VM and log in.

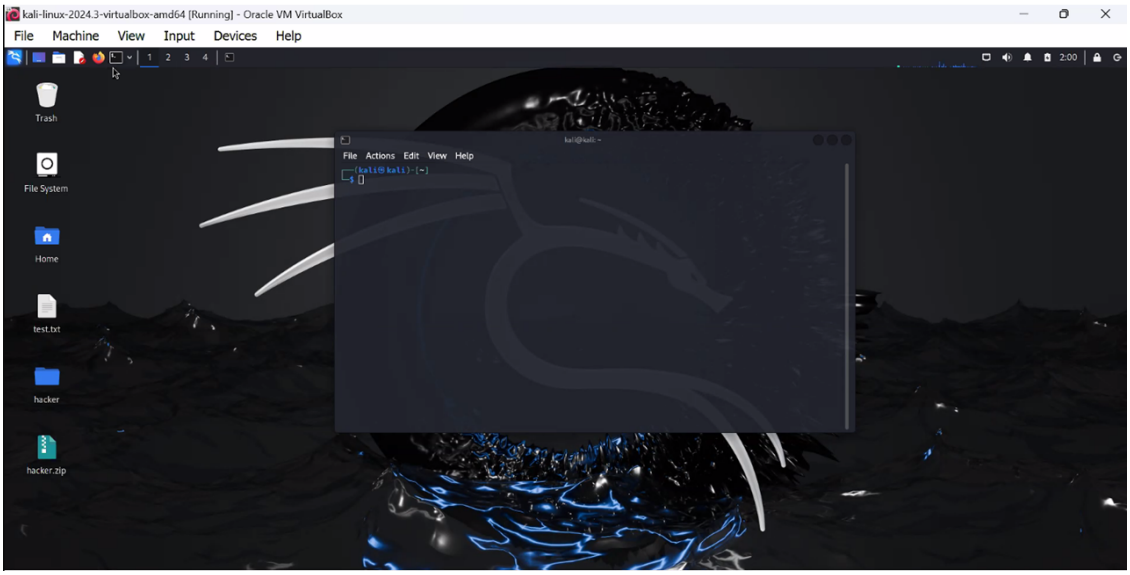

Figure 24: Kali Linux Desktop with Terminal Window

Step 6: Explore the Kali Linux desktop environment. The terminal is a key tool.

6.4. Basic Linux Commands (Kali Linux)

Navigating and managing files in Kali Linux:

- ‘pwd‘: Print the current working directory.
- ‘ls‘: List directory contents.
- ‘cd Desktop‘: Change to another directory location (e.g., ”Desktop”).
- ‘mkdir‘: Make a new directory (e.g., ‘mkdir new‘).
- ‘touch filename‘: Create a new empty file (e.g., ‘touch test.txt‘).
- ‘cat filename‘: Displays the contents of a file.
- ‘echo ”hi” ¿ filename‘: Write ”hi” to a file, overwriting existing content.
- ‘echo ”world” ¿¿ filename‘: Append ”world” to a file.
- ‘cp [source] [destination]‘: Copy a file or directory to another location.
- ‘info‘: The GNU alternative to ‘man‘ for documentation.
- ‘man‘: The standard Unix documentation system.
- ‘mv [source] [destination]‘: Move or rename a file or directory.
- ‘rmdir [directory]‘: Delete an empty directory (e.g., ‘rmdir new‘).
- ‘rm [file/directory]‘: Delete a file or directory tree (use ‘rm -r‘ for directories).
- ‘which [command]‘: Locate a command.
- ‘chmod‘: Change file permissions. For example, ‘chmod +x shell.sh‘ makes ‘shell.sh‘ executable. ‘chmod 000 /var/log/auth.log‘ prevents log updates (dangerous).

6.5. File Permissions in Pen Testing

Understanding and changing file permissions is crucial in penetration testing for several reasons:

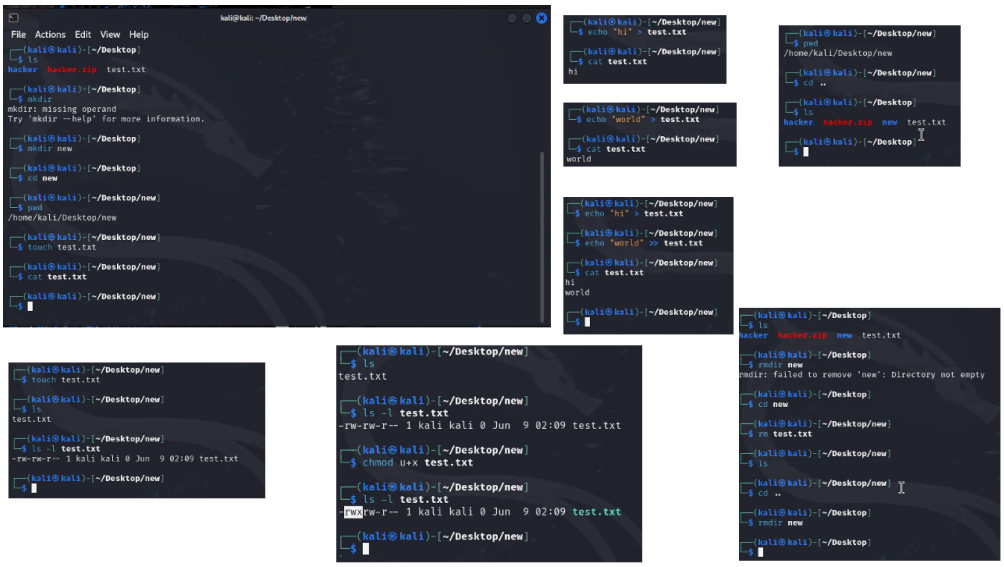

Figure 25: File Permissions in Pen Testing Context

- **Gaining or Escalating Privileges (Privilege Escalation)**:
  - Attackers might change permissions to gain more control over a file or script.
  - Example: ‘chmod -rwxrwxrwx update.sh‘ might be used to give full read/write/execute permissions to all users on a script.
- **Clearing Logs or Hiding Evidence**:
  - Attackers might modify log file permissions to prevent further logging or hide their activities.
  - Example: ‘chmod 000 /var/log/auth.log‘ would remove all permissions, preventing log updates (though this is easily detectable and dangerous for an attacker).
- **Maintaining Access (Persistence)**:
  - Changing a file’s permission to executable (‘chmod +x‘) allows an attacker to run their backdoor or malicious script.
  - Example: ‘chmod +x shell.sh‘ makes the ‘shell.sh‘ script executable.

Users, groups, and others have read (r), write (w), and execute (x) permissions.