Week 2

Day 6

Kali Linux Installation & Setup

Kali Linux Installation and Setup is an important practical topic in the cybersecurity syllabus. Kali Linux is a special Linux operating system that is mainly used for ethical hacking, penetration testing, and security testing. It contains many built-in tools that help in finding security weaknesses in systems and networks. To practice safely, Kali Linux was installed in a virtual environment instead of directly on the main computer.

For this practical work, VirtualBox was used. VirtualBox is a software that allows us to run another operating system inside our existing system. It creates a virtual machine that works like a separate computer. Using VirtualBox helps in creating a safe and controlled lab environment where cybersecurity tools can be practiced without harming the host system.

Installation Process

The installation was performed step by step to ensure proper setup of the system.

- First, the official Kali Linux ISO file was downloaded from the Kali Linux website.
- A new virtual machine was created in VirtualBox and the operating system type was selected as Linux (Debian 64-bit).
- Required system resources such as RAM, processor, and virtual hard disk space were allocated.
- The Kali Linux ISO file was attached to the virtual machine as a boot disk.
- The virtual machine was started and the Graphical Install option was selected.

- Basic settings like language, location, keyboard layout, username, and password were configured.
- Network settings were set automatically to allow internet access.
- Disk partitioning was done using the guided option by using the entire virtual disk.
- Kali Linux system files and tools were installed, and the bootloader was set up.

Post-Installation Tasks

After installation, some important tasks were performed to make the system ready for use.

- The system was logged in using the created user account.
- Updates were installed to keep the system and tools up to date.
- Network connection was checked.
- Screen resolution and basic system settings were adjusted.
- Pre-installed Kali Linux tools were explored to understand their use.

Learning Outcome

This practical helped in understanding both theory and practical concepts of cybersecurity.

i. Learned how to install Kali Linux using VirtualBox
ii. Understood the basics of virtualization
iii. Gained experience in setting up a secure lab environment
iv. Became familiar with Kali Linux interface and tools

Conclusion

The Kali Linux Installation and Setup practical was completed successfully in a controlled lab environment. This setup provides a safe platform for performing future cybersecurity experiments such as vulnerability scanning and penetration testing. The practical improved technical skills and helped in building a strong foundation for advanced cybersecurity learning.

Day 7

Linux Commands Practical

Linux Commands Practical is an important part of the cybersecurity syllabus because most security tools and tasks in Kali Linux are performed using the terminal. The terminal allows users to interact directly with the operating system by typing commands. Learning basic Linux commands helps in understanding how files, folders, processes, and system resources are managed in a Linux environment.

In this practical, the Kali Linux Terminal was used to practice commonly used Linux commands in a safe and controlled lab environment. These commands are essential for ethical hacking, penetration testing, and system administration tasks. Practicing them helps build confidence in working with Linux-based systems, which are widely used in cybersecurity.

Practical Tasks Performed

The following basic Linux commands were studied and practiced to understand their purpose and usage:

- **pwd** – Used to display the current working directory.
- **ls** – Used to list files and folders in a directory.
- **cd** – Used to change from one directory to another.
- **mkdir** – Used to create a new directory.
- **rmdir** – Used to delete an empty directory.
- **touch** – Used to create a new empty file.

- **cp** – Used to copy files or directories.
- **mv** – Used to move or rename files and directories.
- **rm** – Used to delete files or directories.
- **cat** – Used to view the content of a file.
- **nano / vi** – Used to create and edit text files.
- **clear** – Used to clear the terminal screen.
- **whoami** – Used to display the current logged-in user.

Each command was executed multiple times to understand how it works and how it affects files and directories in the system.

Learning Outcome

By performing this practical, the following learning outcomes were achieved:

i. Understood the importance of the Linux terminal in cybersecurity
ii. Learned how to navigate the Linux file system
iii. Gained hands-on experience with basic Linux commands
iv. Learned file and directory management using the terminal
v. Built a strong foundation for using advanced Kali Linux tools

Conclusion

The Linux Commands Practical was successfully completed using the Kali Linux terminal in a controlled lab environment. This practical improved understanding of the Linux operating system and command-line usage, which is essential for performing cybersecurity tasks. Mastery of basic Linux commands is very important for ethical hacking and penetration testing, as it helps in efficiently using security tools and managing system resources.

Day 8

Ethical Hacking Concepts

Ethical hacking is an important concept in cybersecurity. It means testing computer systems, networks, or applications to find security problems with proper permission. The main aim of ethical hacking is to improve security and protect systems from cyber-attacks. Ethical hackers work legally and follow rules and ethical guidelines while identifying weaknesses in systems.

In this practical, ethical hacking concepts were studied in detail using documentation such as books, notes, and online learning materials. Case studies were also used to understand real cyber-attacks and security breaches. Studying case studies helped in understanding how attacks happen in real life and how ethical hackers help organizations prevent such attacks.

Concepts Studied

The following important ethical hacking concepts were learned:

Types of Hackers

a) White Hat Hackers – legal and ethical hackers

b) Black Hat Hackers – illegal and harmful hackers

c) Grey Hat Hackers – work between legal and illegal boundaries

Phases of Ethical Hacking

- Information gathering (footprinting)
- Scanning and enumeration
- Gaining access to the system
- Maintaining access

Common Types of Attacks

I. **Phishing Attacks:** Phishing attacks are fake messages or emails sent by attackers to trick users into giving personal information such as passwords, bank details, or OTPs. These messages usually look real and pretend to be from trusted companies or people.

II. **Password Cracking:** Password cracking is the process of trying to find a user's password using different methods like guessing, using common passwords, or automated tools. Attackers do this to gain unauthorized access to systems or accounts.

III. **Malware Attacks:** Malware attacks involve harmful software such as viruses, worms, trojans, or ransomware. Malware is designed to damage systems, steal data, or control devices without the user's knowledge.

IV. **Network Attacks:** Network attacks target computer networks to steal data, disrupt services, or gain unauthorized access. Common examples include denial-of-service (DoS) attacks, man-in-the-middle attacks, and packet sniffing.

V. **Web Application Attacks:** Web application attacks target websites and online applications to exploit security weaknesses. Examples include SQL injection, cross-site scripting (XSS), and file upload attacks, which can lead to data theft or website defacement.

Learning Outcome

This practical helped in gaining basic knowledge and understanding of ethical hacking.

- Learned the meaning and purpose of ethical hacking
- Understood different hacker types and attack methods
- Gained awareness of cybersecurity laws and ethics

- Understood how theory is applied in real-life cases
- Built a strong foundation for advanced cybersecurity topics

Conclusion

The Ethical Hacking Concepts practical was completed successfully using documentation and case studies in a controlled lab environment. This activity helped in understanding how ethical hackers protect systems by finding and fixing security weaknesses. It also emphasized the importance of ethical behavior and legal boundaries in cybersecurity.

Day 9

Footprinting & Reconnaissance

Footprinting and Reconnaissance is the first and one of the most important stages of ethical hacking and penetration testing. In this stage, information about a target system, website, or organization is collected before performing any security testing. The main aim of footprinting and reconnaissance is to understand the target environment, identify possible security weaknesses, and plan further security assessment activities. This process is carried out legally and ethically, with proper authorization, in a controlled lab environment as per the cybersecurity syllabus.

In this practical, the topic of footprinting and reconnaissance was studied in detail through theoretical learning and hands-on practice. Emphasis was given to passive reconnaissance, which involves collecting information without directly interacting with the target system. This helps in avoiding detection and reduces the risk of harming the target. Various online tools and techniques were used to gather publicly available information that could be useful for cybersecurity analysis.

Tools Used and Practical Tasks Performed

To perform footprinting and reconnaissance, the following tools were used:

- **GoogleDorks**

  Google Dorks are advanced search queries used to find sensitive or hidden information on the internet that is indexed by search engines. In this practical, Google Dorks were used to locate publicly available documents, login pages, directories, error messages,

and exposed files. This helped in understanding how misconfigured websites can unintentionally expose important information.

- **Netcraft**

  Netcraft was used to collect information related to website infrastructure. Using this tool, details such as domain registration, hosting provider, server type, operating system, and website history were identified. This information helps ethical hackers understand the backend setup of a website and identify potential vulnerabilities related to servers or hosting environments.

- **Wappalyzer**

  Wappalyzer was used to analyze the technologies used by websites. It helped in identifying content management systems (CMS), programming languages, frameworks, databases, web servers, and analytics tools. Knowing the technologies used by a website is important because certain technologies may have known security issues if not properly updated.

Learning Outcome

By completing this practical, the following learning outcomes were achieved:

i. Gained a clear understanding of footprinting and reconnaissance concepts
ii. Learned the difference between passive and active information gathering
iii. Understood how attackers collect information before launching attacks
iv. Gained hands-on experience using reconnaissance tools
v. Learned how publicly available information can become a security risk
vi. Developed awareness about ethical and legal boundaries in cybersecurity

Conclusion

The Footprinting and Reconnaissance practical was successfully completed using Google Dorks, Netcraft, and Wappalyzer in a controlled lab environment. This activity helped in understanding how ethical hackers gather useful information during the initial phase of security testing. It also highlighted the importance of protecting publicly accessible information to reduce the risk of cyber-attacks. This practical forms a strong foundation for advanced ethical hacking and penetration testing activities.

Day 10

Network Scanning using Nmap

Network scanning is an important topic in cybersecurity. It is used to find devices connected to a network and to check which ports and services are open on those devices. This helps in understanding how secure a network is. Network scanning is usually done before testing security so that possible weak points can be identified.

In this practical, network scanning was studied and performed using Nmap and Zenmap in a controlled lab environment. Nmap is a powerful command-line tool that helps in scanning networks, while Zenmap is the graphical version of Nmap that makes scanning easier and more user-friendly. Both tools were used only on authorized systems as per ethical and legal rules.

Practical Tasks Performed

The following tasks were performed during the practical:

i. Scanned the network to find active devices connected to it.

ii. Checked open ports on target systems to see which services were running.

iii. Identified basic information about services and operating systems.

iv. Used Zenmap to perform scans using a graphical interface and view results easily.

v. Analyzed scan results to understand network exposure and security status.

Learning Outcome

From this practical, the following things were learned:

i. Basic understanding of network scanning

ii. How to use Nmap and Zenmap tools

iii. Meaning of open ports and running services

iv. Importance of network scanning in cybersecurity

v. Ethical and safe use of scanning tools

Conclusion

The Network Scanning using Nmap practical was completed successfully in a controlled lab environment. This practical helped in understanding how networks are scanned to find active devices and open services. Learning Nmap and Zenmap is very important for cybersecurity, as these tools help in identifying security weaknesses and improving network protection.