Week 20

Day 96

DNS, DHCP, and Protocols

DNS (Domain Name System) is a hierarchical system that translates human-readable domain names (e.g., www.example.com) into IP addresses, allowing devices to locate and communicate with each other over the internet.

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to automatically assign IP addresses and other network configuration details to devices on a network. It simplifies network administration and ensures that each device has a unique IP address.

Protocols are standardized rules that govern how data is transmitted and received across networks. Examples include TCP/IP, HTTP, FTP, and ICMP. Understanding protocols is essential for network communication and cybersecurity monitoring.

Tools Used

- **Kali Linux:** A Linux distribution used for cybersecurity testing and network analysis.
- **nslookup:** A command-line tool to query DNS servers and obtain domain information.
- **dig:** A command-line tool used for detailed DNS lookup and troubleshooting.
- **traceroute:** A tool that tracks the path packets take to reach a target IP address or domain, helping identify network hops and delays.

Practical Work Performed

- Studied the working and importance of DNS and DHCP in network communication.
- Used nslookup and dig to:
    - Query DNS records (A, MX, CNAME, NS)
    - Analyze domain configurations
    - Troubleshoot DNS resolution issues
- Used traceroute to:
    - Trace packet routes from source to destination
    - Identify network latency and intermediate devices
- Explored how DHCP assigns IP addresses and how misconfigurations can lead to network issues.
- Studied network protocols and observed how data is exchanged between devices on a network.

Work Description

The topic of DNS, DHCP, and Protocols was studied in detail according to the cybersecurity syllabus. All practical exercises were performed in a controlled lab environment on authorized systems, ensuring ethical and legal compliance. The exercises helped in understanding network configurations, DNS behavior, and the role of protocols in secure communication.

Conclusion

Understanding DNS, DHCP, and network protocols is fundamental for network security and administration. Through hands-on practice using Kali Linux, nslookup, dig, and traceroute, practical knowledge of domain resolution, IP allocation, and packet routing was gained. This study emphasized the importance of proper network configuration and monitoring to prevent misconfigurations, attacks, and communication failures.

Day 97

Wireshark Packet Analysis

Wireshark is a widely used network protocol analyzer that captures and inspects data packets traveling across a network in real time. Packet analysis is a critical skill in cybersecurity, allowing professionals to monitor network traffic, troubleshoot issues, and detect malicious activity. Understanding packet structures and protocols is essential for securing networks and investigating cyber incidents.

Tools Used

- **Wireshark:** A network analysis tool used to capture, filter, and inspect network packets. It supports multiple protocols and provides detailed insights into network communication.

Practical Work Performed

- Studied the fundamentals of network packets, including headers, payload, and protocol types.
- Captured live network traffic using Wireshark in a controlled lab environment.
- Analyzed different protocol packets, such as TCP, UDP, ICMP, HTTP, and DNS.
- Applied filters to isolate specific traffic (e.g., IP address, protocol type, port number).
- Observed packet flow to understand communication between devices.
- Detected anomalies, such as unusual traffic patterns or potential attack indicators.
- Learned to reconstruct sessions and analyze payloads for deeper insights.

Work Description

The topic of Wireshark Packet Analysis was studied in detail as per the cybersecurity syllabus. All practical exercises were conducted on authorized systems within a controlled lab environment, ensuring ethical and legal compliance. The exercises provided hands-on experience in capturing, filtering, and analyzing network packets to understand both normal and suspicious network activity**.**

Conclusion

Wireshark packet analysis is an essential skill for network monitoring, troubleshooting, and cybersecurity investigation. Through practical exercises, knowledge was gained in capturing and analyzing network traffic, interpreting protocol details, and identifying anomalies. This study emphasized the importance of packet-level inspection for maintaining secure and reliable networks.

Day 98

Kali Linux Installation & Setup

Kali Linux is a Debian-based Linux distribution widely used for penetration testing, ethical hacking, and cybersecurity research. Proper installation and setup are crucial to ensure a secure and functional environment for conducting cybersecurity experiments and lab exercises.

Tools Used

- **VirtualBox:** A virtualization platform used to create virtual machines for running Kali Linux without affecting the host system.
- **Kali Linux ISO:** The official installation image of Kali Linux, containing all necessary tools and packages for cybersecurity tasks.

Practical Work Performed

i. Studied system requirements for Kali Linux and VirtualBox.

ii. Installed VirtualBox and configured a new virtual machine with appropriate CPU, RAM, and storage settings.

iii. Mounted the Kali Linux ISO to install the operating system on the virtual machine. iv. Performed the Kali Linux installation, including partitioning, user creation, and network configuration.

v. Installed Guest Additions for better integration and display performance. vi. Verified network connectivity and updated the system with the latest packages and security patches.

vii. Explored the default toolset in Kali Linux for penetration testing, network analysis, and ethical hacking.

Work Description

The topic of Kali Linux Installation & Setup was studied in detail as per the cybersecurity syllabus. All practical exercises were performed in a controlled lab environment on authorized systems. The process provided hands-on experience in installing, configuring, and preparing a secure Linux environment for cybersecurity tasks.

Conclusion

Installing and configuring Kali Linux is a foundational skill for any cybersecurity professional. Through practical exercises using VirtualBox and the Kali Linux ISO, knowledge was gained in setting up a virtual lab environment, configuring system resources, and preparing a secure platform for penetration testing and ethical hacking. This study emphasized the importance of a well-configured and updated lab setup for safe and effective cybersecurity practice.

Day 99

Linux Commands Practical

Linux Commands Practical focuses on learning and executing essential commands in a Linux environment, which is a critical skill for cybersecurity professionals. Linux provides powerful command-line tools for system administration, file management, networking, and security testing. Mastery of these commands is essential for performing tasks efficiently in penetration testing, network monitoring, and ethical hacking.

Tools Used

- **Kali Linux Terminal:** The command-line interface in Kali Linux used to execute Linux commands, run scripts, and manage system operations.

Practical Work Performed

i. Studied and executed basic Linux commands for file and directory management, such as:
   - ls, cd, pwd, mkdir, rm, cp, mv

ii. Explored file permissions and ownership using: o chmod, chown, chgrp

iii. Monitored system performance and processes with:
   - top, ps, df, free

iv. Performed network-related tasks using commands like:
   - ifconfig, ping, netstat, traceroute

v. Learned to search and filter data using:
   - grep, find, locate

vi. Practiced package management and system updates using:

- apt-get, apt-cache

Work Description

The topic of Linux Commands Practical was studied in detail as per the cybersecurity syllabus. All exercises were performed in a controlled lab environment on authorized systems. The practical sessions enhanced understanding of Linux file systems, process management, and networking commands, which are foundational for cybersecurity tasks.

Conclusion

Mastering Linux commands is essential for cybersecurity professionals, as it enables efficient system navigation, network monitoring, and administration. Through practical exercises in the Kali Linux terminal, hands-on experience was gained in executing commands, managing files and directories, monitoring system resources, and performing network diagnostics. This study highlighted the importance of Linux command-line skills in cybersecurity investigations, penetration testing, and ethical hacking.

Day 100

Ethical Hacking Concepts

Ethical Hacking is the authorized practice of identifying vulnerabilities in systems, networks, and applications to improve security. Ethical hackers use the same techniques as malicious hackers but operate with legal permission and within defined boundaries. The main objective is to discover weaknesses before attackers can exploit them and to recommend appropriate security controls.

Tools Used

- **Documentation:** Industry standards, frameworks, and learning resources used to understand ethical hacking methodologies and best practices.
- **Case Studies:** Real-world examples of cyber attacks and security breaches used to analyze attack techniques, impacts, and mitigation strategies.

Practical Work Performed

i. Studied real-world case studies of cyber attacks to understand attacker techniques and system weaknesses.

ii. Analyzed how ethical hackers identify vulnerabilities and suggest remediation steps. iii. Reviewed cybersecurity documentation and standards related to ethical hacking practices.

iv. Learned the importance of scope definition, consent, and reporting in ethical hacking activities.

Work Description

The topic of Ethical Hacking Concepts was studied in detail as per the cybersecurity syllabus. Learning activities were conducted in a controlled lab environment and through authorized study material, ensuring adherence to ethical and legal guidelines. This helped in building a strong conceptual foundation for practical cybersecurity tasks.

Conclusion

Ethical hacking plays a vital role in strengthening cybersecurity defenses by proactively identifying and mitigating security risks. Through the study of documentation and real-world case studies, a clear understanding of ethical hacking methodologies, legal considerations, and responsible practices was developed. This topic emphasized the importance of ethical conduct, authorization, and systematic approaches in protecting digital systems from cyber threats.