Week 7

Day 31

Firewall & Web Application Firewall (WAF)

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between a trusted internal network and untrusted external networks such as the internet. A Web Application Firewall (WAF) is a specialized type of firewall designed to protect web applications from common web-based attacks.

In cybersecurity, firewalls and WAFs are essential for preventing unauthorized access, reducing attack surfaces, and ensuring secure communication.

Types of Firewalls

i. **Packet Filtering Firewall** – Filters traffic based on IP address, port number, and protocol.
ii. **Stateful Inspection Firewall** – Monitors the state of active connections.
iii. **Proxy Firewall** – Acts as an intermediary between users and the internet.
iv. **Web Application Firewall (WAF)** – Protects web applications by filtering HTTP/HTTPS traffic.

Tools Used

1. Windows Firewall

Windows Firewall is a host-based firewall integrated into the Windows operating system that provides network protection by controlling traffic at the system level.

Key Features:

- Filters inbound and outbound traffic
- Uses rule-based access control
- Protects against unauthorized connections
- Integrates with Windows Defender

Practical Usage:

i. Created inbound and outbound rules
ii. Allowed or blocked specific ports and applications
iii. Tested firewall behavior using network traffic
iv. Observed how unauthorized access attempts are blocked

2. iptables

iptables is a powerful command-line firewall utility used in Linux systems to configure packet filtering rules in the kernel.

Key Features:

- Controls network traffic using chains and tables
- Supports NAT, packet filtering, and traffic mangling
- Highly customizable and efficient
- Commonly used in servers and cybersecurity labs

Basic Components:

- **Tables:** filter, nat, mangle
- **Chains:** INPUT, OUTPUT, FORWARD
- **Rules:** Define actions such as ACCEPT, DROP, or REJECT

Practical Usage:

i. Configured firewall rules to allow or deny traffic
ii. Blocked unused ports to reduce attack surface
iii. Implemented IP-based filtering
iv. Tested rule effectiveness using network tools

Web Application Firewall (WAF)

A Web Application Firewall protects web applications by filtering and monitoring HTTP/HTTPS traffic between a client and a web server.

Functions of WAF:

- Prevents SQL Injection

- Blocks Cross-Site Scripting (XSS)
- Protects against CSRF attacks
- Monitors application-layer traffic

Unlike traditional firewalls that operate at the network layer, WAF operates at the application layer (Layer 7) of the OSI model.

Practical Work Performed

As part of the cybersecurity lab:

- Windows Firewall rules were configured and tested
- iptables rules were implemented in a Linux environment
- Traffic behavior before and after firewall configuration was analyzed
- Security impact of firewall policies was observed
- All activities were performed in a controlled lab environment following ethical guidelines

Importance in Cybersecurity

Firewalls and WAFs are critical for:

- Preventing unauthorized network access
- Protecting systems from network-based attacks
- Securing web applications
- Enforcing security policies
- Reducing the risk of data breaches

Conclusion

Firewalls and Web Application Firewalls play a vital role in protecting systems and applications from cyber threats. Through hands-on practice using Windows Firewall and iptables, a practical understanding of traffic filtering, rule creation, and security enforcement was achieved. This study enhanced knowledge of both network-level and application-level security mechanisms.

Day 32

Career Guidance in Cybersecurity

Career guidance plays an important role in helping students understand industry requirements, career paths, and skill expectations in the field of cybersecurity. With the rapid growth of digital technologies, organizations require skilled cybersecurity professionals to protect systems, networks, and data from cyber threats. This practical focused on exploring career opportunities, building professional profiles, and understanding job readiness using industry platforms and resume tools.

Tools Used

1. LinkedIn

LinkedIn is a professional networking platform widely used by recruiters, industry experts, and job seekers.

Key Features:

- Professional profile creation
- Networking with cybersecurity professionals
- Job search and career insights
- Skill endorsements and certifications display

Practical Usage:

- Created or updated a professional LinkedIn profile
- Added cybersecurity-related skills and certifications
- Followed cybersecurity companies and experts
- Explored job roles such as Security Analyst, SOC Analyst, Ethical Hacker, and Cybersecurity Engineer
- Analyzed job descriptions and required skills

2. Resume Tools

Resume tools help in creating well-structured, professional resumes tailored to specific job roles.

Key Features:

- ATS (Applicant Tracking System) friendly templates
- Skill-based and role-specific formatting
- Keyword optimization
- Easy editing and exporting

Practical Usage:

- Created a cybersecurity-focused resume
- Highlighted technical skills such as networking, Linux, firewalls, and security tools
- Added academic projects and lab work
- Customized resumes for entry-level cybersecurity roles

Career Paths in Cybersecurity

During the study, various cybersecurity career options were explored, including:

- Cybersecurity Analyst
- SOC Analyst
- Ethical Hacker / Penetration Tester
- Network Security Engineer
- Digital Forensics Analyst
- Cloud Security Engineer

Each role requires a combination of technical knowledge, practical experience, and continuous learning.

Practical Work Performed

As part of the controlled lab environment:

- Researched cybersecurity career roles and skill requirements
- Built a professional online presence using LinkedIn
- Prepared a job-ready resume using resume tools
- Analyzed current industry trends and certifications
- Understood the importance of internships, projects, and continuous skill development

All activities were conducted ethically and aligned with the cybersecurity syllabus.

Importance of Career Guidance

Career guidance helps students:

- Identify suitable cybersecurity career paths
- Understand industry expectations
- Improve employability skills
- Build professional networks
- Prepare for interviews and job applications

Conclusion

Career guidance is an essential component of cybersecurity education. By using LinkedIn and resume tools, practical knowledge was gained on professional branding, job readiness, and career planning. This practical enhanced awareness of cybersecurity career opportunities and provided a clear roadmap for future professional growth

Day 33

Networking Fundamentals

Networking fundamentals form the foundation of cybersecurity. A strong understanding of how computers communicate over networks is essential for identifying vulnerabilities, securing data, and preventing cyber attacks. This practical focused on understanding basic networking concepts, network components, protocols, and command-line networking tools in both Windows and Linux environments.

Basic Networking Concepts

- **Network:** A collection of interconnected devices that share data and resources.
- **IP Address:** A unique numerical identifier assigned to each device on a network.
- **MAC Address:** A hardware address used for device identification.
- **Subnet Mask:** Defines the network and host portions of an IP address.
- **Default Gateway:** The device that connects a local network to external networks.

Types of Networks

- **LAN (Local Area Network)** – Small geographical area like an office or campus.
- **WAN (Wide Area Network)** – Large geographical area such as the internet.
- **MAN (Metropolitan Area Network)** – Covers a city or region.
- **PAN (Personal Area Network)** – Short-range personal devices.

Tools Used

1. Windows OS & Command Prompt

Command Prompt is used to view and troubleshoot network configurations.

Common Commands Used:

- ipconfig – Displays IP configuration
- ping – Tests network connectivity
- tracert – Tracks packet path
- netstat – Displays network connections

2. Linux OS

Linux provides powerful networking tools commonly used in cybersecurity.

Common Commands Used:

- ifconfig / ip a – Displays network interfaces
- ping – Tests connectivity
- traceroute – Traces route of packets
- netstat / ss – Displays active connections

3. Network Diagrams

Network diagrams visually represent network structure and communication flow.

Usage:

- Designed basic network topologies
- Understood client-server communication
- Identified network devices such as routers, switches, and firewalls
- Analyzed data flow paths for security planning

Practical Work Performed

As part of the cybersecurity lab:

- Configured and verified IP addresses in Windows and Linux
- Tested connectivity between systems using command-line tools
- Analyzed routing paths and network behavior
- Created basic network diagrams to represent logical and physical layouts
- Observed how data flows across different network layers

All tasks were performed in a **controlled lab environment** following cybersecurity best practices.

Importance in Cybersecurity

Networking fundamentals are essential for:

- Understanding attack vectors and threats
- Configuring secure networks
- Troubleshooting network issues

- Implementing firewalls and intrusion detection systems
- Supporting ethical hacking and incident response

Conclusion

This practical provided a strong foundation in networking fundamentals using Windows OS, Linux OS, command-line tools, and network diagrams. The hands-on experience enhanced understanding of network communication, configuration, and troubleshooting, which are critical skills for cybersecurity professionals.

Day 34

IP Addressing and Subnetting

IP addressing and subnetting are fundamental concepts in computer networking and cybersecurity. Every device connected to a network requires a unique IP address for identification and communication. Subnetting is the process of dividing a large network into smaller, manageable sub-networks to improve performance, security, and efficient use of IP addresses. This practical focused on understanding IP address formats, subnet calculation, and network configuration in a controlled lab environment.

IP Addressing

Types of IP Addresses

- **IPv4:** Uses 32-bit addresses (e.g., 192.168.1.1)
- **IPv6:** Uses 128-bit addresses for larger address space

Address Categories

- **Public IP:** Accessible over the internet
- **Private IP:** Used within local networks (e.g., 10.0.0.0/8, 192.168.0.0/16)

Components of an IP Address

- **Network Portion:** Identifies the network
- **Host Portion:** Identifies the device within the network
- **Subnet Mask:** Determines network and host boundaries

Subnetting

Subnetting divides a network into smaller sub-networks (subnets) by borrowing bits from the host portion.

Benefits of Subnetting

- Efficient IP address utilization
- Improved network performance
- Enhanced security and isolation
- Easier network management

Key Terms

- **CIDR Notation:** Represents subnet mask (e.g., /24)
- **Network Address:** First address of a subnet
- **Broadcast Address:** Last address of a subnet
- **Usable Hosts:** Addresses available for devices

Tools Used

1. Kali Linux & Terminal

Kali Linux provides a Linux-based environment for networking and cybersecurity analysis.

2. ipconfig (Windows)

- Displays IP address, subnet mask, and gateway

- Used to verify network configuration

3. ifconfig (Linux)

- Displays network interface configuration
- Used for checking assigned IP addresses

4. ip addr

- Modern Linux command for network configuration
- Provides detailed interface and IP information

5. Subnet Calculator

- Used to calculate subnet masks, network IDs, and usable hosts
- Verified manual subnet calculations
- Helped understand CIDR-based subnetting

Practical Work Performed

As part of the cybersecurity lab:

- Identified IP addresses on Windows and Linux systems
- Analyzed subnet masks and CIDR notation
- Performed subnet calculations manually and using tools
- Configured and verified network interfaces
- Observed how subnetting affects network segmentation

All tasks were conducted in a **controlled lab environment** as per cybersecurity syllabus guidelines.

Importance in Cybersecurity

IP addressing and subnetting are crucial for:

- Designing secure and efficient networks
- Implementing network segmentation
- Reducing attack surfaces
- Supporting firewall and routing configurations
- Enhancing monitoring and access control

Conclusion

This practical provided hands-on experience with IP addressing and subnetting using Kali Linux, terminal commands, and subnet calculators. The study enhanced understanding of network identification, address allocation, and subnet design, which are essential skills for cybersecurity professionals.

Day 35

OSI & TCP/IP Models

The OSI (Open Systems Interconnection) and TCP/IP models are conceptual frameworks used to understand how data is transmitted across networks. These models divide network communication into layers, where each layer has specific functions. Understanding these models is essential in cybersecurity for analyzing network traffic, identifying vulnerabilities, and implementing security controls at different layers.

OSI Model

The OSI model consists of 7 layers, each with a defined role in network communication.

Layers of OSI Model

1. **Physical Layer** – Transmits raw bits over physical media (cables, signals)
2. **Data Link Layer** – Handles framing, MAC addressing, and error detection
3. **Network Layer** – Manages IP addressing and routing (e.g., IP, ICMP)
4. **Transport Layer** – Ensures reliable data transfer (TCP, UDP)
5. **Session Layer** – Manages sessions between applications
6. **Presentation Layer** – Data formatting, encryption, compression
7. **Application Layer** – Provides network services to end users (HTTP, FTP, SMTP)

TCP/IP Model

The TCP/IP model is a practical and widely used networking model with **4 layers**.

Layers of TCP/IP Model

1. **Network Interface Layer** – Physical and data link functions
2. **Internet Layer** – Logical addressing and routing (IP)
3. **Transport Layer** – End-to-end communication (TCP, UDP)
4. **Application Layer** – Network services (HTTP, HTTPS, FTP, DNS)

Comparison Between OSI & TCP/IP Models

OSI Model	TCP/IP Model
7 layers	4 layers
Theoretical model	Practical model
Clear separation of functions	Some layers combined
Used for learning and troubleshooting	Used in real-world networking

Tools Used

1. Presentation Slides

- Used to study layer-wise functions
- Explained protocols and data flow
- Helped visualize communication process

2. Network Diagrams

- Illustrated data movement across layers
- Mapped protocols to specific layers
- Helped understand encapsulation and decapsulation

Practical Work Performed

As part of the cybersecurity lab:

- Studied OSI and TCP/IP models in detail
- Created diagrams representing layered communication
- Mapped common protocols to each layer
- Analyzed how attacks occur at different layers
- Understood security controls such as firewalls, IDS, and encryption at various layers

All activities were performed in a controlled lab environment according to cybersecurity syllabus guidelines.

Importance in Cybersecurity

Understanding OSI and TCP/IP models helps in:

- Network troubleshooting
- Identifying attack points
- Designing layered security (defense in depth)
- Implementing firewalls and intrusion detection systems

Conclusion

This practical provided a comprehensive understanding of OSI and TCP/IP models using presentation slides and network diagrams. The study enhanced conceptual clarity of layered network communication, which is crucial for effective cybersecurity analysis and defense .