

Cybersecurity & Networking Basics: Foundations

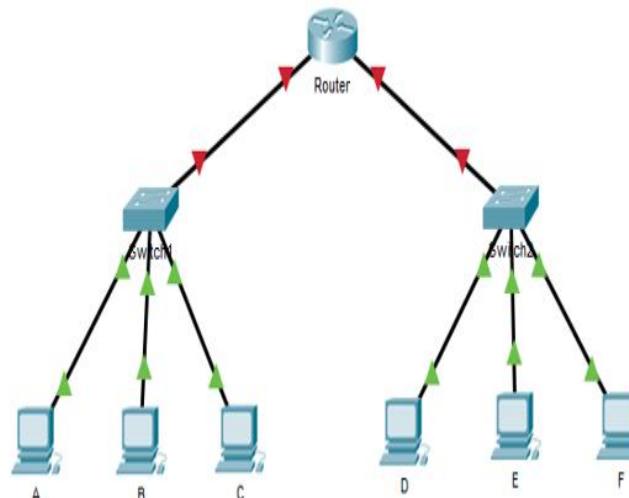
Day 3: Network Practice & Traffic Analysis

Network Simulation with Cisco Packet Tracer



Introduction to Packet Tracer

Cisco Packet Tracer is a powerful network simulation tool that allows users to design, configure, and troubleshoot network topologies. It's an invaluable educational resource for understanding networking principles without requiring expensive hardware.



Introduction to Packet Tracer

Cisco Packet Tracer is a powerful network simulation tool that allows users to design, configure, and troubleshoot network topologies. It's an invaluable educational resource for understanding networking principles without requiring expensive hardware.

Building a Basic Client-Server Network

- In this guided hands-on session, students will construct a fundamental network to understand the core components and their interaction.

1

Build Components

Assemble a basic network comprising a PC (client), a server, a network switch, and a router.

2

Connect Devices

Physically connect the PC to the switch, the server to the switch, and the switch to the router to establish the network topology.

3

Assign IP Addresses

Configure unique IP addresses for each device, enabling them to communicate on the network.

4

Configure Connectivity

Implement basic network settings to ensure all devices can communicate successfully within the simulated environment.

Key Concepts Reinforced

- ▶ This practical exercise solidifies understanding of crucial networking fundamentals, laying the groundwork for more advanced topics.



Client-Server Communication

Grasp the fundamental interaction between clients requesting services and servers providing them.



Network Devices

Familiarize with the roles of routers (inter-network communication) and switches (intra-network communication).



IP Addressing

Understand how IP addresses uniquely identify devices on a network, enabling targeted communication.



Data Flow in a Network

Visualize and understand the path data packets take as they traverse a network from source to destination. This activity directly reinforces concepts introduced on Day 2.

Understanding Ports & Protocols via Simulation

- ▶ Delve into how services operate on network devices and how different protocols enable specific types of communication.
- ▶ **Ports & Services in Packet Tracer**
 - ▶ HTTP (Port 80) and HTTPS (Port 443) for web traffic.
 - ▶ FTP (Port 21) for file transfers and DNS (Port 53) for domain name resolution.
 - ▶ Understanding how these services are hosted and run on servers.
- ▶ **Simulation Mode & Packet Flow**
 - ▶ Visualize the journey of individual packets across the network.
 - ▶ See how IP addresses pinpoint devices and ports identify specific services.
 - ▶ Observe the high-level stages of a TCP handshake, a crucial communication setup process.

Real Network Traffic with Wireshark

- ▶ Transition from controlled simulations to the raw, dynamic world of live network traffic analysis using Wireshark.
- ▶ **Simulation vs. Reality**
 - ▶ Contrast the clean, predictable nature of Packet Tracer simulations with the noisy, chaotic, and often overwhelming reality of live network traffic. Real networks are a constant stream of diverse data.
- ▶ **Wireshark Basics**
 - ▶ Learn to navigate the essential features of Wireshark, including selecting the correct network interface, initiating and stopping packet captures, and understanding the layout of the packet list and detailed views.

Dissecting a Packet: Key Identifiers

Understand the critical components that make up a network packet and how they facilitate communication.

- ▶ **Source IP & Destination IP:** These addresses identify the sending and receiving devices on the network, analogous to postal addresses.
- ▶ **Protocol:** The set of rules governing how data is formatted and transmitted, e.g., TCP, UDP, ICMP.
- ▶ **Source & Destination Ports:** These numbers identify the specific application or service on the host that sent or is intended to receive the data.

tcpdump & Live Traffic Lab

- ▶ practical experience with a powerful command-line packet capture tool, tcpdump, and apply Wireshark skills to live network data.
- ▶ **tcpdump Introduction**
 - ▶ Learn about tcpdump, a versatile command-line packet analyzer widely used by security professionals for its efficiency and scripting capabilities. Understand its role in capturing network traffic directly from the command line and saving it for later analysis.
- ▶ **Hands-On Lab**
 - ▶ Capture live traffic using Wireshark.
 - ▶ Generate various types of traffic (web browsing, ping, DNS queries).
 - ▶ Identify IPs, ports, and protocols within the captured data.
 - ▶ Compare observable differences between HTTP and encrypted HTTPS traffic.

Security Discussion: The Importance of Encryption

Reflect on the implications of network visibility and the critical role of encryption in protecting sensitive information.

Attacker Visibility

Discuss what information attackers can glean from unencrypted traffic on open networks, emphasizing the risks of data interception and unauthorized access.

Encryption's Role

Highlight the fundamental importance of encryption in securing communications, preventing eavesdropping, and ensuring data integrity and confidentiality.

SOC Teams & Packet Captures

Explore how Security Operations Center (SOC) teams utilize packet captures for incident response, forensic analysis, and proactive threat hunting to maintain network security.