Cisco II-Routing & Switching
Lewis Joseph Feik
Week 1 Lab – Analyzing Networked Systems as Security Risks

Purpose

This lab introduces security analysis, which is the core skill of this course. Instead of configuring or fixing systems, the goal is to observe a networked environment, identify potential attack surfaces, and explain why those elements create risk. The focus is on thinking like a cybersecurity professional and building strong reasoning, not running tools or commands.

Scenario

I am reviewing a small organization’s environment that includes employee laptops/desktops, a local network with shared resources, internet connectivity, at least one externally accessible service, and a cloud-based storage/collaboration service. Since no extra technical details are provided, the analysis is based on realistic assumptions and common risks found in similar environments.

1. Identify Networked System Components

• Employee laptops and desktops

These endpoints are used by staff to access company resources such as email, internal files, cloud services, and web applications. They are a major part of the networked system because they regularly send/receive data and authenticate to internal and external services.

• Local network with shared resources (e.g., file share or internal server/printer)

This internal environment allows employees to communicate, share files, and use organizational resources. Shared resources support collaboration and productivity, but they also create central points where sensitive data may exist.

• Cloud-based service used for storage or collaboration (e.g., cloud drive, file sharing, shared documents)

This service provides remote access to organizational data and collaboration tools. It connects the organization’s users and data to an external provider, making it part of the system even though it is not physically located inside the building.

2. Identify Attack Surfaces

- **User endpoints (laptops/desktops)**

Why it is an attack surface: Endpoints interact with email, websites, downloads, USB devices, and cloud logins, creating many ways for an attacker to reach them.
Why it introduces risk: A compromised endpoint can lead to stolen credentials, malware installation, data loss, and lateral movement into shared resources on the local network.

- **Externally accessible service (public-facing system)**

Why it is an attack surface: Any service reachable from the internet is exposed to scanning, login attempts, and exploitation. It is accessible to both legitimate users and attackers.
Why it introduces risk: If the service has weak authentication, misconfigurations, unpatched vulnerabilities, or poor access control, it can become an entry point to the organization’s internal environment or sensitive data.

- **Cloud storage/collaboration access (accounts and sharing features)**

Why it is an attack surface: Cloud services often allow file sharing, external invitations, web access, and integrations. These features increase exposure beyond the local network.
Why it introduces risk: Poor sharing controls, weak passwords, lack of multi-factor authentication, or compromised accounts can allow attackers to access sensitive documents without needing to physically enter the organization’s network.

3. Connectivity vs. Security

This environment can function correctly while still being insecure because usability and connectivity do not automatically mean safe design. Systems can “work” even when they rely on risky assumptions.

- **Trust assumptions**

Organizations often assume employees are legitimate, devices are clean, and internal traffic is safe. However, if a user account or device is compromised, those trust assumptions become weaknesses that attackers can exploit.

- **Access or exposure**
The environment requires access to shared resources, internet services, and cloud platforms to support daily operations. That access increases exposure by expanding the number of reachable systems and accounts. Even if everything is operating normally, the organization may still be vulnerable to phishing, credential theft, or unauthorized access.

- **Design or configuration choices**
A network can be designed for convenience (easy sharing, broad access, minimal restrictions) and still run smoothly. For example, allowing wide access to file shares or using simple login policies may make work easier, but it increases risk because attackers have fewer barriers if they gain access.

4. Professional Security Perspective

Analyzing systems before fixing them is important because security decisions must be based on understanding, not guessing. A cybersecurity analyst needs to identify what assets exist, how they connect, what is exposed, and what threats are realistic before choosing controls.

If a team tries to "fix" security without analysis, they may:

- Focus on the wrong problem and leave major risks untouched
- Break business functions by applying controls that don't match the system's needs
- Miss root causes (like weak trust assumptions or excessive access) and only treat symptoms
- Waste time and resources on changes that do not reduce real risk

A strong analysis phase helps prioritize what matters most, reduce risk effectively, and support decisions with clear reasoning and professional justification.