Unit 8: Networks and Communications and their Inherent Weaknesses

Learning Objective

- Analyze the importance of network principles and architecture to security operations.

Key Concepts

- OSI network model and its security lapses
- Physical and logical network topologies
- Characteristics of a secure network
- 802.11 WLAN technology weaknesses, vulnerabilities, and mitigation strategies
- Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) and their use in IT infrastructures for secure communications

Reading

- Kim and Solomon, Chapter 10: Networks & Communications.

Keywords

Use the following keywords to search for additional materials to support your work:

- DoS
- Encapsulation
- Flooding
- Hijacking
- Sniffing
- Spoofing
- Service Set Identifier (SSID)
- OSI Reference Model
- WLAN

Homework

Unit 8 Assignment 1: Network Hardening

Learning Objectives and Outcomes

- You will learn the essentials of network hardening for a given network layout.

Assignment Requirements

In this assignment, you are given a handout which contains four different network layouts. Choose any ***one*** of the layouts: you do not need to do all of them.

For your layout, you are required to devise at least three strategies for hardening the network environment throughout the seven domains of a typical IT infrastructure. Support your decisions with your justification.

Required Resources

- Worksheet: Network Hardening

Submission Requirements

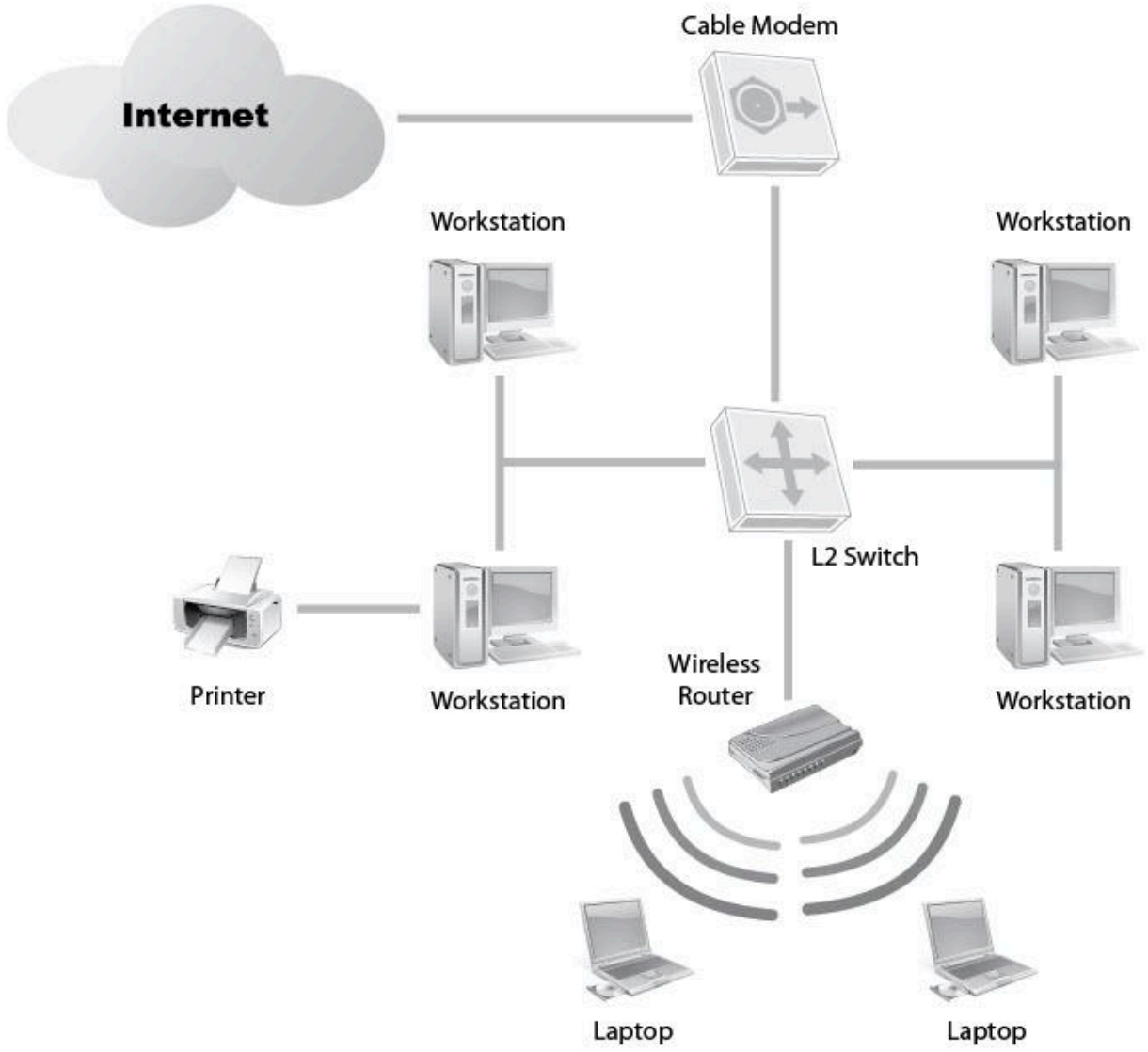
- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Length: 1–2 pages

Self-Assessment Checklist

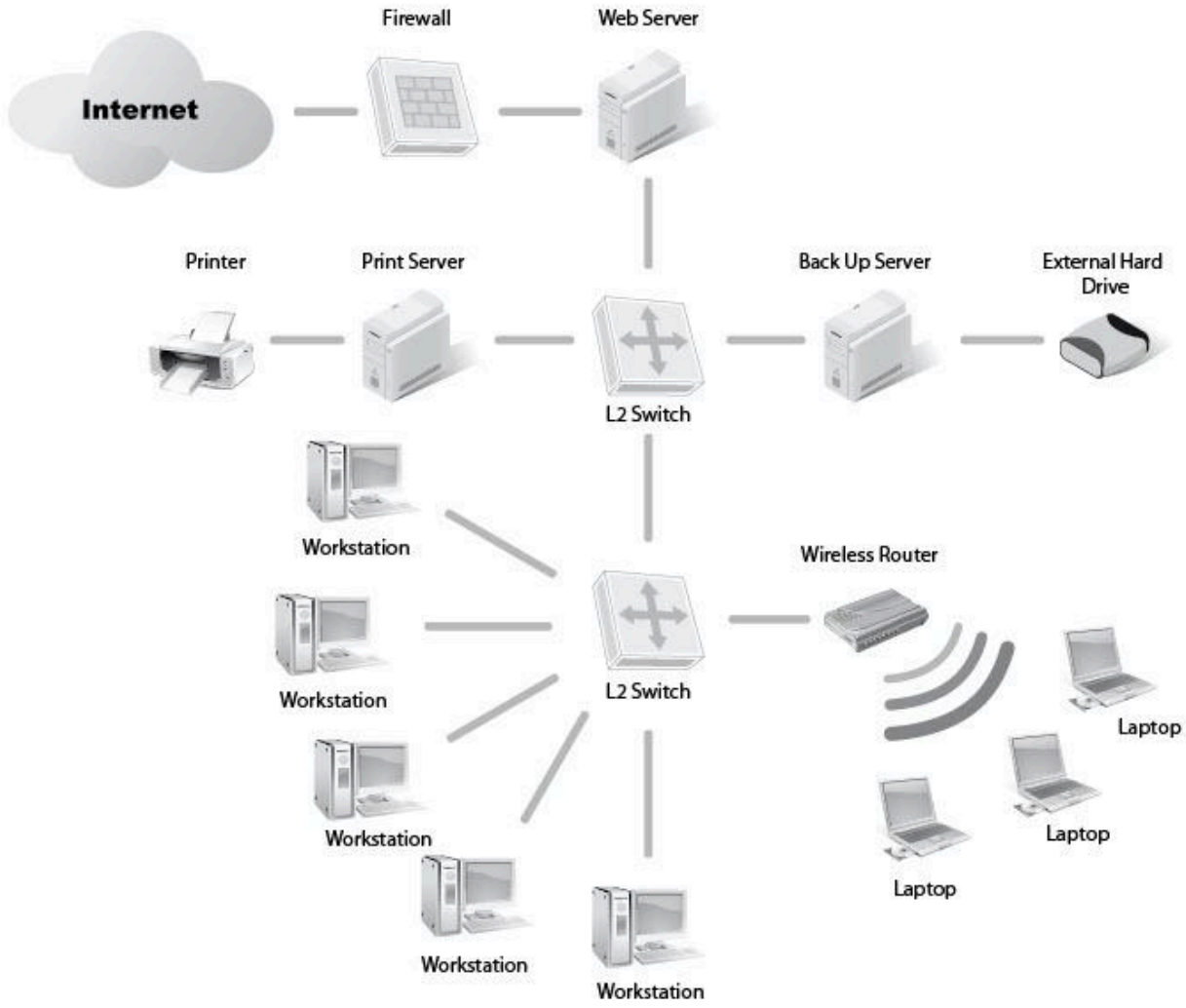
- I have identified at least three network hardening strategies for the given network layout.
- I have given the justification for my decisions.

NT2580: Unit 8 Network Hardening

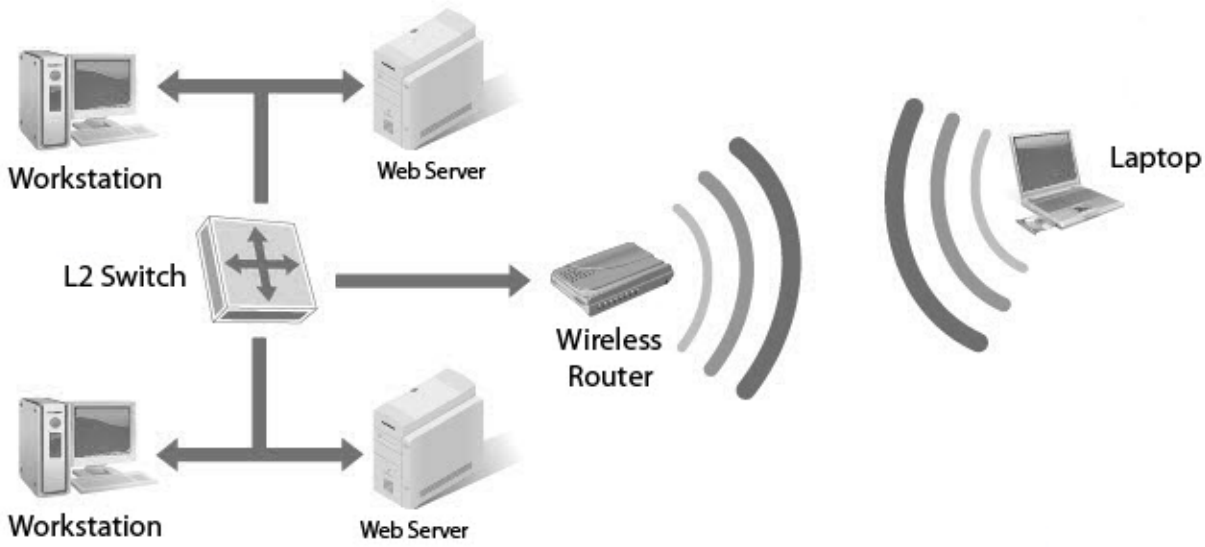
Network Layout 1: Workgroup



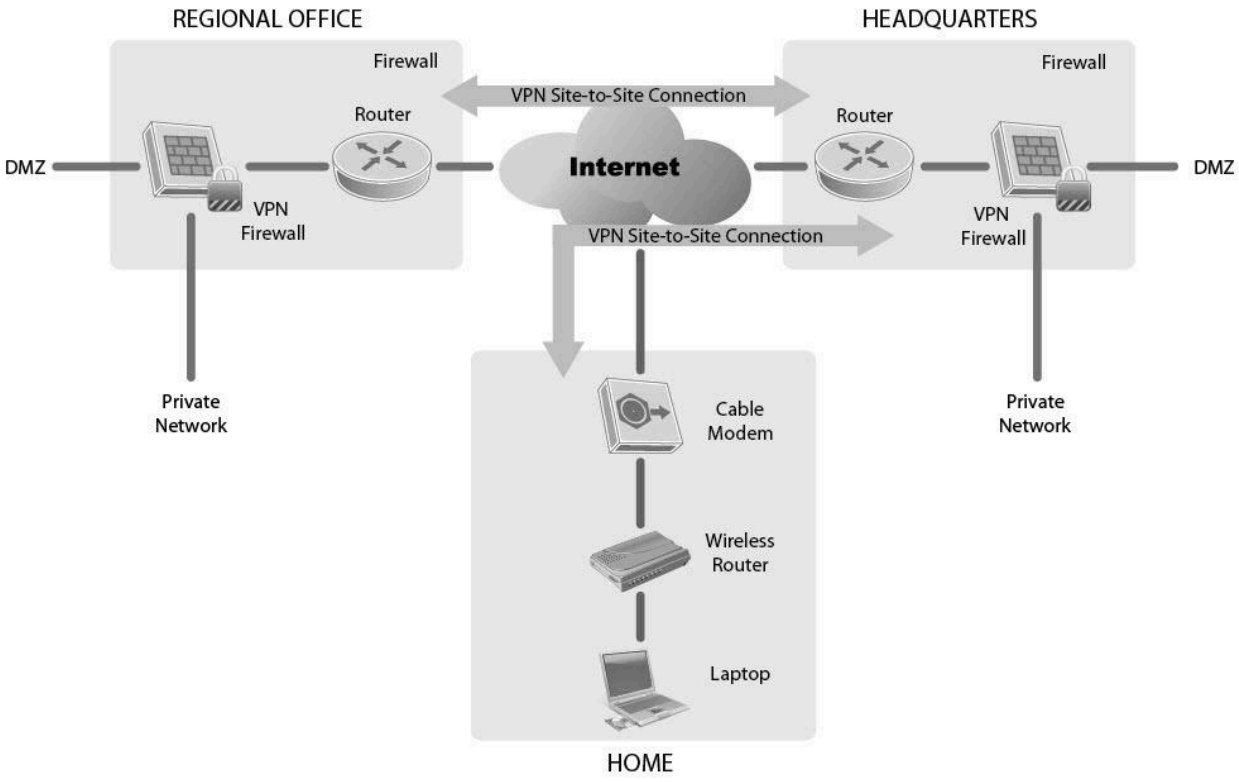
Network Layout 2: Client/server



Network Layout 3: WLAN



Network Layout 4: VPN



Unit 8 Assignment 2: Network Security Applications and Countermeasures

Learning Objectives and Outcomes

- You will learn how to determine where certain security countermeasures apply across the seven domains of a typical IT infrastructure.

Assignment Requirements

In this assignment, you are given a worksheet that contains a list of network security applications and countermeasures. You need to identify where they belong, within the seven domains of a typical IT infrastructure and what confidentiality, integrity, and availability (CIA) function they provide. Complete the worksheet and submit to your instructor for evaluation.

Required Resources

- Worksheet: Network Security Applications and Security Countermeasures

Submission Requirements

- Format: Microsoft Word
- Font: Arial, Size 12, Double-Space
- Length: 1–2 pages

Self-Assessment Checklist

- I have accurately placed security countermeasures within the seven domains of an IT infrastructure.
- I have identified the portions of the CIA triad affected by specific security countermeasures.

NT2580: Unit 8 Network Security Applications and Countermeasures

Instructions:

Given the network security applications and countermeasures in the first column of the table below, explore answers to the following questions:

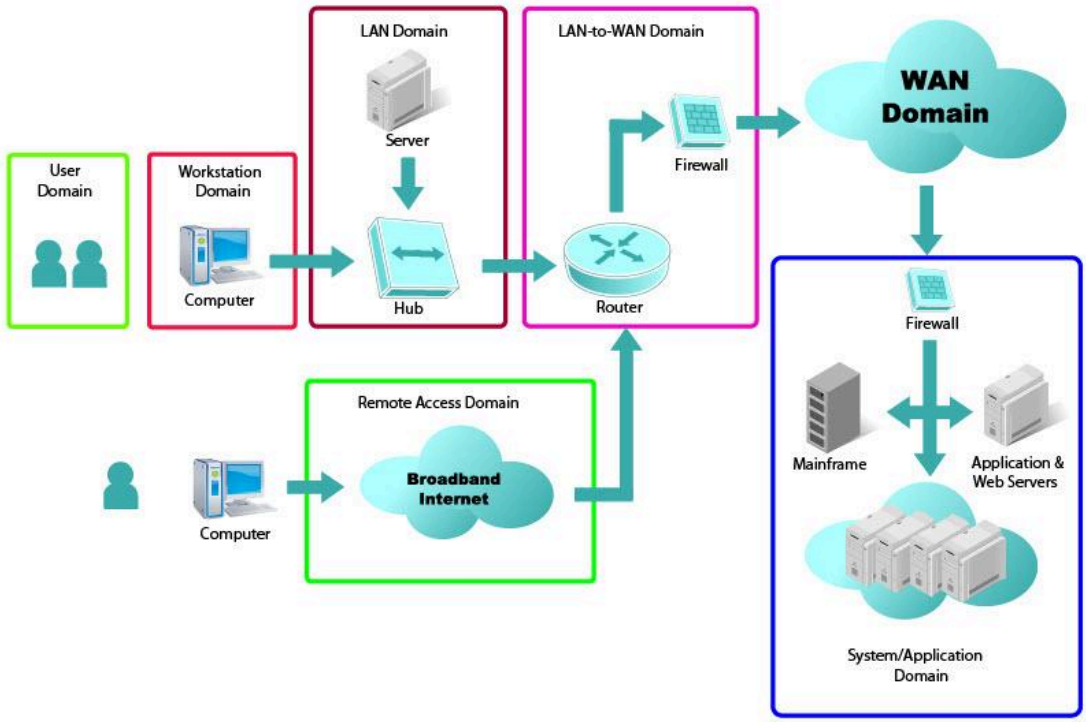
- Where does the countermeasure belong in the seven domains of a typical IT infrastructure?
- What CIA functions does the countermeasure provide?

Provide your answers in the table below.

Network Security Applications and Countermeasures	Domains	CIA Function
Ethical hacker		
Intrusion detection system/intrusion prevention system (IDS/IPS)		
Access controls		
Failover server		
Automatic updates		
Cryptography		
Data backups		
Logon rights		
Computer cluster		
Firewalls		
Proxies		
Antivirus scanners		

As a reminder, the seven domains of a typical IT infrastructure include the following domains:

- **User domain**: Actual users
- **Workstation domain**: Workstations, laptops, and end-point devices, such as smartphones and printers
- **LAN domain**: Physical and logical LAN technologies—100 Mbps/1000 Mbps switched Ethernet, 802.11-family of wireless LAN technologies—used to support workstation connectivity to the organization's network infrastructure
- **LAN-to-WAN domain**: Routers, firewalls, demilitarized zones (DMZs), and IDS/IPS
- **WAN domain**: Routers, circuits, switches, firewalls, gateways, and equivalent gear at remote locations, sometimes under a managed service offering by the service provider
- **Remote access domain**: Virtual private networks (VPNs), laptops with VPN software, and secured socket layer/VPN (SSL/VPN) tunnels
- **System/Application domain**: Hardware, operating system software, database software, client/server applications, and data that are typically housed in the organization's data center and computer rooms



Representation of the Seven Domains of a typical IT Infrastructure

Labs

Unit 8. Lab 8. Perform a Website & Database Attack by Exploiting Identified Vulnerabilities

Assignment Requirements

- Perform Laboratory #8 on Page 83 of the *Laboratory Manual*.

Special Notes

- Throughout the lab, there may be instructions for the instructor. These instructions were included in error and may be ignored.

- **Required Setup and Tools**.
    - You may ignore this section.
    - You will only need the following virtual machine for this lab:
        - **`TargetUbuntu01`**
    - The VM may also be called **`TargetUbuntu01rev2`**.

- **Student Steps**.
    - You may ignore *Steps 1 through 3*.
    - Instead, power up the **`TargetUbuntu01`** VM and begin at *Step 4*.
    - *Step 4* should return the IP address of TargetUbuntu01. If it does, you may skip *Steps 6 and 7*.
        - If *Step 4* does not return an IP address, please see the instructor *before* performing *Steps 6 and 7*.
    - *Step 5* should be performed from a Web browser on your *physical computer*, not from a virtual machine.

- **To Exploit an SQL Injection Vulberability**
    - *Steps 1 through 3* are duplicates that you would have already done in the XSS Vulnerability portion of the lab. You may ignore them.

- In *Step 6*, the correct syntax is:

  ```
  a' OR 'x' = 'x' #
  ```

- *Step 7* is confusingly-worded. Simply enter:

  ```
  a' OR '1' & '1' #
  ```

- You may skip *Steps 9 through 18*. If you wish to try some of the SQL statements, you may, but not all of them work as advertised.

- To shut down your **`TargetUbuntu01`** VM, enter the following command:

  ```
  sudo shutdown -h now
  ```

Reminders

- Readings for the next unit:
    - Kim and Solomon, Chapter 11: Malicious Code and Activity.

- The following assignments are due in the next class session:
    - Unit 8 Assignment 1: Network Hardening
    - Unit 8 Assignment 2: Network Security Applications and Countermeasures
    - Unit 8. Lab 8. Perform a Website & Database Attack by Exploiting Identified Vulnerabilities

- The following assignments are due in Unit 11:
    - Project Part 2 Student SSCP® Domain Research Paper