Student Lab Manual

Managing Risk in Information Systems

Table of Contents

Laboratory #1

Lab 1: How to Identify Threats & Vulnerabilities in an IT Infrastructure

Learning Objectives and Outcomes

Upon completing this lab, students will be able to:

- Identify common risks, threats, and vulnerabilities found throughout the seven domains of a typical IT infrastructure.
- Align risks, threats, and vulnerabilities to one of the seven domains of a typical IT infrastructure.
- Given a scenario, prioritize risks, threats, and vulnerabilities based on their risk impact to the organization.
- Prioritize the identified critical, major, and minor software vulnerabilities.

Required Setup and Tools

This is a paper-based, hands-on lab.

The standard Instructor and Student VM workstation with Microsoft Office 2007 or higher is required for this lab. Students will need access to the Lab #1 – Assessment Worksheet Part A (a list of 21 risks, threats, and vulnerabilities commonly found in an IT infrastructure) and must identify which of the seven domains of a typical IT infrastructure the risk, threat, or vulnerability impacts.

In addition, Microsoft Word is a required tool for the student to craft an executive summary for management summarizing the findings and alignment of the identified risks, threats, and vulnerabilities that were found.

Hands-on Lab #1 – Student Steps:

Student steps needed to perform Lab #1 – Identify Threats and Vulnerabilities in an IT Infrastructure:

1. Connect your removable hard drive or USB hard drive to a classroom workstation.
2. Boot up your Student Microsoft Windows VM workstation and DHCP for an IP host address.
3. Login to your Student Microsoft Windows VM workstation.
4. Review Figure 1 – Seven Domains of a Typical IT Infrastructure.
5. Discuss how risk can impact each of the seven domains of a typical IT infrastructure: User, Workstation, LAN, LAN-to-WAN, WAN, Remote Access, Systems/Applications Domains.
6. Work on Lab #1 – Assessment Worksheet Part A. Part A is a matching exercise that requires the students to align the risk, threat, or vulnerability with one of the seven domains of a typical IT

infrastructure where there is a risk impact or risk factor to consider. Students may work in small groups of two or three.

7. Have the students perform Lab #1 – Assessment Worksheet Part A and Part B.
8. Answer Lab #1 – Assessment Worksheet questions and submit.

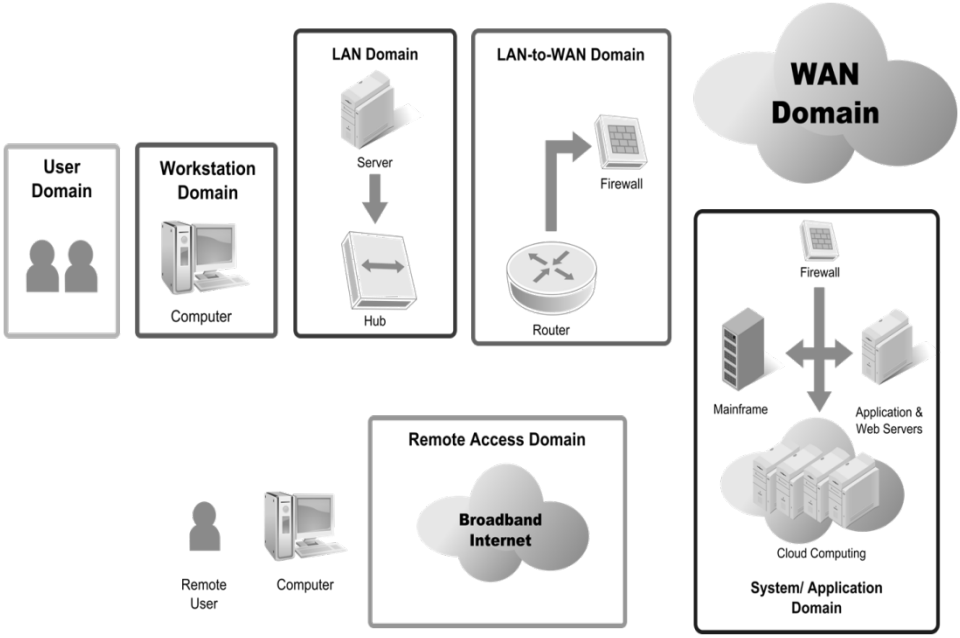

Figure 1 – Seven Domains of a Typical IT Infrastructure

Deliverables

Upon completion of Lab #1 – Identify Threats and Vulnerabilities in an IT Infrastructure, students are required to provide the following deliverables as part of this lab:

1. Lab #1 – Identification and mapping of 21 risks, threats, and vulnerabilities to the seven domains of a typical IT infrastructure.
2. Lab #1 - Assessment Worksheet with answers to the assessment questions.

Evaluation Criteria and Rubrics

The following are the evaluation criteria and rubrics for Lab #1 that the students must perform:

1. Ability to identify common risks, threats, and vulnerabilities found throughout the seven domains of a typical IT infrastructure. – [**25%**]

2. Ability to align risks, threats, and vulnerabilities to one of the seven domains of a typical IT infrastructure accurately. – [**25%**]
3. Given a scenario in Part A, ability to prioritize risks, threats, and vulnerabilities based on their risk impact to the organization. – [**25%**]
4. Ability to prioritize the identified critical, major, and minor software vulnerabilities? – [**25%**]

Lab #1: Assessment Worksheet

Part A – List of Risks, Threats, and Vulnerabilities

Commonly Found in an IT Infrastructure

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

The following risks, threats, and vulnerabilities were found in a healthcare IT infrastructure servicing patients with life-threatening situations. Given the list, select which of the seven domains of a typical IT infrastructure is primarily impacted by the risk, threat, or vulnerability.

Risk – Threat – Vulnerability	Primary Domain Impacted
Unauthorized access from public Internet	
User destroys data in application and deletes all files	
Hacker penetrates your IT infrastructure and gains access to your internal network	
Intra-office employee romance gone bad	
Fire destroys primary data center	
Communication circuit outages	
Workstation OS has a known software vulnerability	
Unauthorized access to organization owned	
Workstations	
Loss of production data	
Denial of service attack on organization e-mail Server	

Risk – Threat – Vulnerability	Primary Domain Impacted
Remote communications from home office	
LAN server OS has a known software vulnerability	
User downloads an unknown e –mail attachment	
Workstation browser has software vulnerability	
Service provider has a major network outage	
Weak ingress/egress traffic filtering degrades Performance	
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	
VPN tunneling between remote computer and ingress/egress router	
WLAN access points are needed for LAN connectivity within a warehouse	
Need to prevent rogue users from unauthorized WLAN access	

Lab #1: Assessment Worksheet

Identify Threats and Vulnerabilities in an IT Infrastructure

Course Name: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

One of the most important first steps to risk management and implementing a risk mitigation strategy is to identify known risks, threats, and vulnerabilities and organize them. The purpose of the seven domains of a typical IT infrastructure is to help organize the roles, responsibilities, and accountabilities for risk management and risk mitigation. This lab requires students to identify risks, threats, and vulnerabilities and map them to the domain that these impact from a risk management perspective.

Lab Assessment Questions & Answers

Given the scenario of a healthcare organization, answer the following Lab #1 assessment questions from a risk management perspective:

1. Healthcare organizations are under strict compliance to HIPPA privacy requirements which require that an organization have proper security controls for handling personal healthcare information (PHI) privacy data. This includes security controls for the IT infrastructure handling PHI privacy data. Which one of the listed risks, threats, or vulnerabilities can violate HIPPA privacy requirements? List one and justify your answer in one or two sentences.

2. How many threats and vulnerabilities did you find that impacted risk within each of the seven domains of a typical IT infrastructure?

   User Domain:
   Workstation Domain:
   LAN Domain:
   LAN-to-WAN Domain:

WAN Domain:

Remote Access Domain:

Systems/Application Domain:

3. Which domain(s) had the greatest number of risks, threats, and vulnerabilities?

4. What is the risk impact or risk factor (critical, major, minor) that you would qualitatively assign to the risks, threats, and vulnerabilities you identified for the LAN-to-WAN Domain for the healthcare and HIPPA compliance scenario?

5. Of the three Systems/Application Domain risks, threats, and vulnerabilities identified, which one requires a disaster recovery plan and business continuity plan to maintain continued operations during a catastrophic outage?

6. Which domain represents the greatest risk and uncertainty to an organization?

7. Which domain requires stringent access controls and encryption for connectivity to corporate resources from home?

8. Which domain requires annual security awareness training and employee background checks for sensitive positions to help mitigate risk from employee sabotage?

9. Which domains need software vulnerability assessments to mitigate risk from software vulnerabilities?

10. Which domain requires AUPs to minimize unnecessary User initiated Internet traffic and can be monitored and controlled by web content filters?