Laboratory #1

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

Course Name: IAA202

Student Name: Huynh Ngoc Quang

Instructor Name: Mai Hoang Dinh

Lab Due Date: 11/09/24

Part A – List of Risks, Threats, and Vulnerabilities

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	Remote Access
User destroys data in application and deletes all files	System/Application
Hacker penetrates your IT infrastructure and gains access to your internal network	LAN
Intra-office employee romance gone bad	User
Fire destroys primary data center	System/Application
Communication circuit outages	WAN
Workstation OS has a known software vulnerability	Workstation
Unauthorized access to organization owned Workstations	Workstation
Loss of production data	System/Application
Denial of service attack on organization e-mail Server	LAN-to-WAN
Remote communications from home office	Remote Access
LAN server OS has a known software vulnerability	LAN
User downloads an unknown e –mail attachment	Workstation
Workstation browser has software vulnerability	Workstation

Service provider has a major network outage	WAN
Weak ingress/egress traffic filtering degrades Performance	LAN-to-WAN
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	Workstation
VPN tunneling between remote computer and ingress/egress router	Remote Access
WLAN access points are needed for LAN connectivity within a warehouse	LAN
Need to prevent rogue users from unauthorized WLAN access	LAN

Identify Threats and Vulnerabilities in an IT Infrastructure

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.

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.

I think it is “User destroys data in application and deletes all files”: it can lead to severe consequences, including the loss of critical PHI. This violates HIPAA privacy requirements by failing to maintain the integrity and availability of patient data, which are crucial aspects of data protection under HIPAA regulations.

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: 01

Workstation Domain: 05

LAN Domain: 04

LAN-to-WAN Domain: 02

WAN Domain: 02

Remote Access Domain: 03

Systems/Application Domain: 03

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

Workstation: directly involves end-users, who are often the most unpredictable and susceptible to social engineering, malware, and human error. Workstations are frequently targeted by attackers due to their access to sensitive data and systems, making them a critical entry point for security breaches.

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?

Risks, threats, and vulnerabilities	Risk impact or risk factor
Weak ingress/egress traffic filtering degrades Performance	**Major**
Denial of service attack on organization e-mail Server	**Critical**

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 require a catastrophic outage?

Fire destroys primary data center: requires a well-prepared DRP and BCP. These plans ensure that the organization can quickly recover critical systems and data, maintain operations, and minimize downtime. The DRP would include procedures for restoring backups, potentially at a secondary data center. The BCP will outline how the organization will continue essential functions while recovery efforts are underway.

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

User Domain: Due to unpredictable human behavior, vulnerability to social engineering attacks, and potential insider threats, this domain represents the greatest risk and uncertainty.

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

Remote Access Domain: Requires stringent access controls and encryption for secure connectivity to corporate resources from remote locations, such as home offices.

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

User Domain: This domain involves employees, who need regular training and background checks to mitigate risks such as insider threats and employee sabotage.

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

Workstation Domain, LAN Domain, Systems/Application Domain, Remote Access: These domains should undergo regular software vulnerability assessments to identify and mitigate software vulnerabilities.

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

Workstation Domain: AUPs are essential here to control unnecessary user-initiated internet traffic, which can be monitored by web content filters.

11. In which domain do you implement web content filters?

LAN Domain: Web content filters are implemented at this level to manage and control internet access across the internal network.

12. If you implement a wireless LAN (WLAN) to support connectivity for laptops in the Workstation Domain, which domain does WLAN fall within?

LAN Domain: WLAN falls within the LAN Domain as it supports connectivity for devices like laptops within a local area network.

13. A bank under Gramm-Leach-Bliley-Act (GLBA) for protecting customer privacy has just implemented their online banking solution allowing customers to access their accounts and perform transactions via their computer or PDA device. Online banking servers and their public Internet hosting would fall within which domains of security responsibility?

LAN-to-WAN Domain: Online banking servers and their public hosting environments would fall within this domain.

14. Customers that conduct online banking using their laptop or personal computer must use HTTPS, the secure and encrypted version of HTTP: browser communications. HTTPS:// encrypts webpage data inputs and data through the public Internet and decrypts that webpage and data once displayed on your browser. True or False.

True: It uses encryption for secure communication over a computer network and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security or, formerly, Secure Sockets Layer

15. Explain how a layered security strategy throughout the 7-domains of a typical IT infrastructure can help mitigate risk exposure for loss of privacy data or confidential data from the Systems/Application Domain.

A multi-layered security strategy helps mitigate risk by deploying multiple security measures (e.g., firewalls, encryption, access controls) across each of the seven domains, creating overlapping defenses to protect against potential breaches of private data or confidential information within the System/Application Domain.