**Lab #1: Assessment Worksheet**

**Part A – List of Risks, Threats, and Vulnerabilities**

**Commonly Found in an IT Infrastructure**

**Course Name: IAA202**

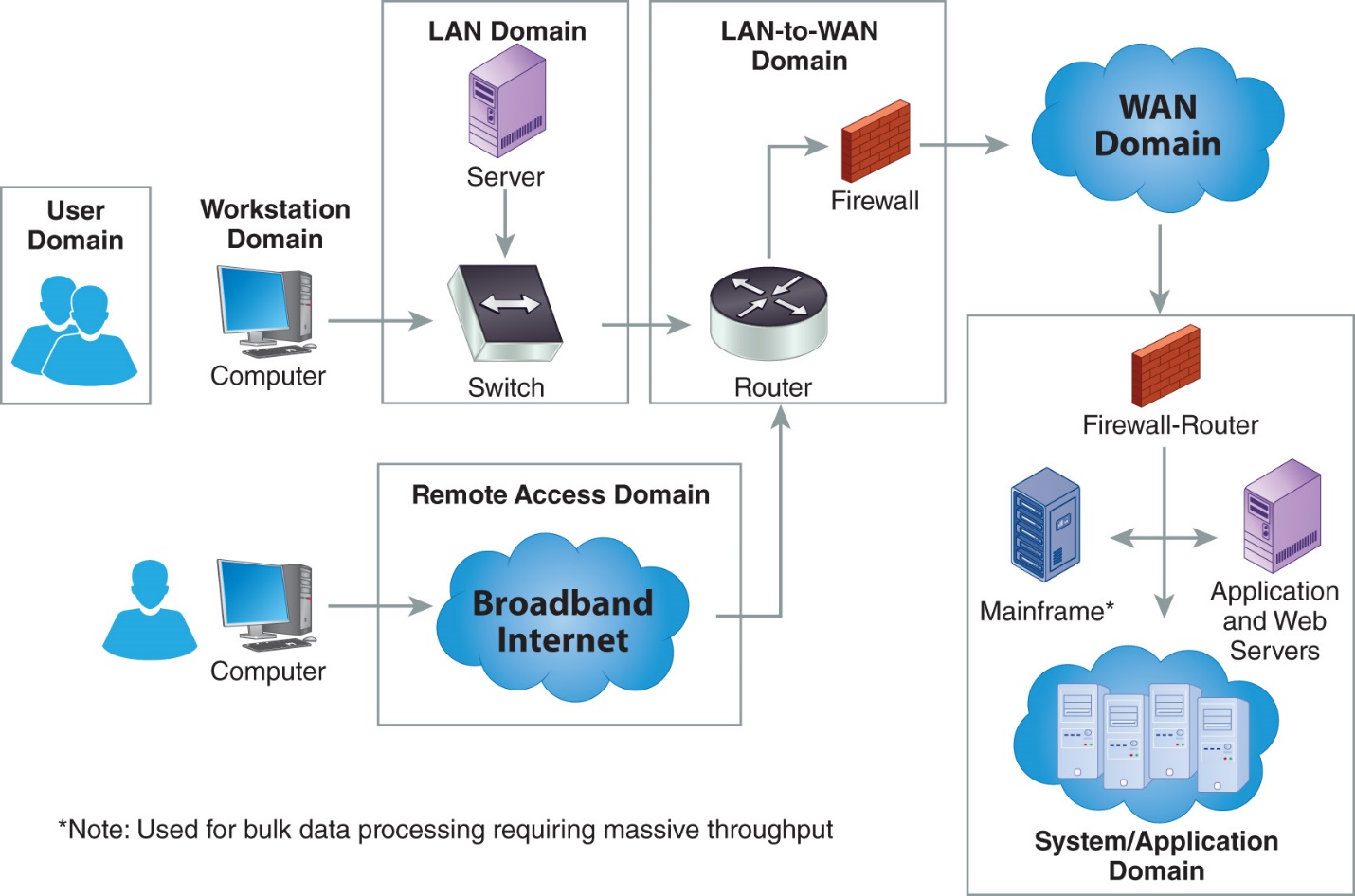
**Student Name: Phạm Thành Long**

**Instructor Name: Mai Hoàng Đỉnh**

**Lab Due Date: 09/11/2024**

**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 Domain |
| User destroys data in application and deletes all files | System/Application Domain |
| Hacker penetrates your IT infrastructure and gains access to your internal network | LAN-to-WAN Domain |
| Intra-office employee romance gone bad | User Domain |
| Fire destroys primary data center | System/Application Domain |
| Communication circuit outages | WAN Domain |
| Workstation OS has a known software vulnerability | Workstation Domain |
| Unauthorized access to organization owned Workstations | Workstation Domain |
| Loss of production data | System/Application Domain |
| Denial of service attack on organization e-mail Server | LAN-to-WAN Domain |
| Remote communications from home office | Remote Access Domain |
| LAN server OS has a known software vulnerability | LAN Domain |
| User downloads an unknown e –mail attachment | User Domain |
| Workstation browser has software vulnerability | Workstation Domain |
| Service provider has a major network outage | WAN Domain |
| Weak ingress/egress traffic filtering degrades Performance | LAN-to-WAN Domain |
| User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers | User Domain |
| VPN tunneling between remote computer and ingress/egress router | LAN-to-WAN Domain |
| WLAN access points are needed for LAN connectivity within a warehouse | LAN Domain |
| Need to prevent rogue users from unauthorized WLAN access | LAN Domain |

**Lab #1: Assessment Worksheet**

**Identify Threats and Vulnerabilities in an IT Infrastructure**

**Course Name: IAA202**

**Student Name: Phạm Thành Long**

**Instructor Name: Mai Hoàng Đỉnh**

**Lab Due Date: 09/11/2024**

**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**

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.

**Risk/Threat/Vulnerability: Unauthorized access from public Internet**

**Justification: Unauthorized access from the public Internet could expose personal healthcare information (PHI), which would directly violate HIPAA privacy requirements. This is a significant risk because attackers might gain access to sensitive patient data, leading to potential data breaches and compromising patient confidentiality.**

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

User Domain: **3**

Workstation Domain: **3**

LAN Domain: **3**

LAN-to-WAN Domain: **4**

WAN Domain: **2**

Remote Access Domain: **2**

System/Application Domain: **3**

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

**LAN-to-WAN Domain**

1. 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?

|  |  |
| --- | --- |
| **Risk – Threat – Vulnerability** | **Risk Impact/Risk Factor** |
| Hacker penetrates your IT infrastructure and gains access to your internal network | Critical |
| Denial of service attack on organization e-mail Server | Major |
| Weak ingress/egress traffic filtering degrades Performance | Major |
| VPN tunneling between remote computer and ingress/egress router | Critical |
| Intra-office employee romance gone bad | Minor |

1. 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?

**Fire destroys the primary data center because as the primary there is no other backup.**

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

**User Domain**

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

**User Domain**

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

**User Domain, Workstation Domain**

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

**Workstation Domain, LAN Domain, System/Application Domain, LAN-to-WAN Domain**

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

**Workstation Domain, WAN Domain**

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

**LAN-to-WAN Domain**

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

**LAN Domain**

1. 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?

**WAN Domain**

1. 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**

**HTTPS (Hypertext Transfer Protocol Secure) encrypts data transmitted between a user's browser and the website, ensuring that any data inputs, like login credentials or financial information, are securely encrypted over the public Internet. This encryption is decrypted once the data reaches its destination, protecting it from being intercepted by unauthorized parties.**

1. 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.

**Each domain checks and balances other domains. There are coverage overlaps that ensure that there is going to be no gaps. Software upgrades would help out workstation, LAN, and System/Application domain.**