Subject code and name

Assessment number

Report title: Worthy college IT infrastructure Vulnerability Analysis

Assessment due date

Word count: 1724

Student names

Student IDs

Torrens’s email addresses

Learning facilitator

Subject coordinator

Table of Contents

[Executives Summary 3](#_Toc108245500)

[Introduction 3](#_Toc108245501)

[Vulnerabilities in worthy college IT infrastructure 3](#_Toc108245502)

[Moodle XSS Attack - Lack of user input validation vulnerability 3](#_Toc108245503)

[Denial of Service Attack (DoS Attack) 4](#_Toc108245504)

[Lack of Communications Encryption 4](#_Toc108245505)

[Lack of Logging and Monitoring 5](#_Toc108245506)

[Broken Access Control 5](#_Toc108245507)

[Lack of Internal Network Segmentation 6](#_Toc108245508)

[Ransomware Attack 7](#_Toc108245509)

[Summary Table 7](#_Toc108245510)

[Lack of Logging and Monitoring 7](#_Toc108245511)

[Broken Access Control 7](#_Toc108245512)

[Conclusion 7](#_Toc108245513)

[References 8](#_Toc108245514)

Executives Summary

This business report details the findings of an examination of vulnerabilities in the IT infrastructure at Worthy College. The research included both white box and grey box testing. Upon investigating the IT infrastructure, which included end devices such as PCs and servers, as well as the network and network architecture, several security flaws were discovered. The company lacked a password policy, communication encryption resulting in sniffing attacks, logging and network monitoring to uncover attacks such as malware and backdoors, access control where sensitive data can be accessed by anyone, denial of service attack, cross-site scripting, and network segmentation resulting in pivoting attack threats.

Introduction

The scope and complexity of information technology have expanded tremendously over time. As a result, the value of internet targets has expanded dramatically, drawing numerous malevolent agents motivated by financial or other motives. They have created a range of attack tactics and strategies, abandoning some that were ineffectual owing to improved protection measures and embracing different approaches when flaws and openings are identified. The objective to be achieved in this report is to bring to attention the cyber security state of Worthy College IT infrastructure and the risk it poses to the business aspect of this organization. This report will analyze current vulnerabilities and issues impacting the IT systems at Worthy College, including those relating to software, hardware, human elements, and data storage.

Vulnerabilities in worthy college IT infrastructure

Moodle XSS Attack - Lack of user input validation vulnerability

Essentially, Moodle platforms are used to store any organization's primary and secondary data. This may include email addresses, messages, and credential information about students and staff in the case of Worthy College. XSS arises when the system does not validate user input. Therefore, an attacker can utilize this vulnerability to inject malicious code into the system, mostly web pages, to alter backend data. XSS attacks are self or store XSS.

This is ultimately a trap because the said person's browser and webpages will execute the script without knowing and having faith in the script. Volition on the part of the user would hardly matter at this point. Because of not being able to distinguish between a trusted and malicious source, all the relevant and sensitive information and cookies are also accessible. These scripts can even rewrite the content of the HTML page. This can lead to an unethical leak of highly confidential information about the organization (Hackerone, n.d.).

Denial of Service Attack (DoS Attack)

A denial of Service (DoS) attack is an attack in which the entire system is shut down, making it inaccessible for the intended users to use the program. This attack is usually accomplished by flooding the website or webpage of the target with unregulated traffic or sending unauthorized information that facilitates the crash of the entire system due to misconfigured firewall, IDS of complete lack of firewall leading to attacks like ICMP flood attacks, ping of death attacks, etc.

In the case of Worthy College, a DoS attack might lead to a lack of access to essential files and documents about the information on grants from governments and data on scholarship money.

Lack of Communications Encryption

All staff and student passwords at Worthy College are transmitted and stored as plain text in their databases. This technique dramatically enhances the likelihood that your information system will be penetrated by external attackers (who have gained network access) and malevolent employees.

If a network node is compromised, an attacker can capture all broadcast information using eavesdropping software, such as Wireshark. This method is referred to as "sniffing."

To maximize the effectiveness of the sniffer, the attacker assumes a "Man in the Middle" position. MitM attacks, often known as spying attacks, involve an attacker employing tools such as Ettercap to intercept communication between two devices or servers (Xu et al., 2017). Once in the position of the Man in the Middle, the attacker starts Wireshark to listen to the traffic in order to exfiltrate important information and data.

FTP servers and Databases need to be protected from such threats. A successful attack would lead to a data breach where in turn attacker can solicit funds from the Worthy College so that not to leak the data.

Lack of Logging and Monitoring

The absence of monitoring and logging is a technological and organizational vulnerability that enables attackers to retain their position in a network for as long as feasible.

As with network segmentation, robust Logging and Monitoring procedures can not guarantee 100% security against attacks, but they can detect unexpected events and incursions and reduce their impact (Stankov & Tsochev, 2020).

The majority of network communication elements (information sharing, data exchange, etc.) maintain information about the network. Indeed, all operating systems and apps "log" all occurrences. Similar to access points, routers, proxies, and firewalls also maintain track of each packet. The design of the machines to which each of these things belongs then manages this data.

It is stored, for a given amount of time, in files referred to as "logs."

In a white box penetration testing of the Worthy College network, its noted that the organizations don't have a dedicated team to monitor network traffic or to

perform periodic maintenance to IT systems. Threats such as backdoor attacks can persist in the network without being noticed. In the long run, this might lead to attacks such as cyber espionage where competitors still business secretes.

Logs should be centralized on the internal server for easy maintenance and use. Then, agents must monitor and synchronize all log file occurrences on other workstations.

If a system is hacked, the attacker will likely delete the logs. Centralizing, syncing, and duplicating records ensures backups.

Broken Access Control

Broken access control vulnerabilities arise when a user can access a resource or execute an activity that they should not be able to access or accomplish, posing threats such as indirect, direct object references, IDOR, and privilege escalation attacks (Yadav et al., 2020).

While testing Worthy College IT infrastructure, it's noted that the system is vulnerable to broken access control resulting from platform configurations. Staff may install any software on their computer at work, which should only be done by admins. All files, sensitive or otherwise, are hosted on an FTP server and can be accessed by all staff through an FTP application of their choice. This is risky as it can breach the confidentiality and integrity of the organization when sensitive documents meant for management are accessed by all staff.

Lack of Internal Network Segmentation

All end devices at Worthy College operate on the same LAN, allowing all network applications and systems to communicate and directly connect with each other.

This technique should be avoided from a security standpoint, as the majority of these systems do not need interaction. In addition, if a network is flat and a single system is compromised, the entire IT system is at risk. In reality, several attacks involve "pivoting," which comprises leveraging a hacked entity to gain access to other network components and freely move around (Lu et al., 2021).

Even if network segmentation cannot prevent attacks, it remains one of the most effective techniques for reducing their repercussions. The principle is straightforward. It involves dividing a computer network into smaller network segments that are separated by VLANs. This permits the grouping of end devices into network sub-partitions depending on security concerns and priorities, as well as the significance of these systems. IP filtering and firewalls assist in the partitioning of regions.

Grey box penetration testing on Worthy College's internal network included segmentation tests. As the audit was a grey box, the pen tester was granted access to Wi-Fi to evaluate network segmentation. During tests, the network wasn't partitioned. Thus, critical services were on the same subnet as other departments. An attack in this network would lead to compromise to all resources since they are on the same VLAN. Therefore, the organization would lose trust from stakeholders learning that the whole school network was compromised.

Therefore, the network design segmentation confines the impacts of an intrusion on a bounded portion of the IT system. In the event of a cyberattack, the intruder would be incapable of lateral movement, preventing its propagation.

Ransomware Attack

Ransomware is primarily a form of malware assault. In this, the data like that of a victim and their important feelings are somehow made inaccessible by the attacker. They then encrypt it and make it impossible to access unless a specific condition is met, mostly monetary (Bruce Lynch 2022).

Notably, thousands of ransomware viruses can cause widespread damage to the organization, namely, 'WannaCry,' 'Cryptolocker,' 'NotPetya,' and 'Petya.' This attack arises primarily due to a lack of user education vulnerability in an organization.

Summary Table

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Threats** |  **Vulnerability** |  **Attacks** |
| 1 | Denial of Service | **Firewall/IDS Mis-configuration(lack)** | Ping of death, ICMP flood |
| 2 | XSS Attack  | **Lack of user input validation** | Self XSS, Stored XSS |
| 3 | Man in the middle attack | **Lack of Communications Encryption** | Mitm, Sniffing, Data breach |
| 4 | Pivoting Attack | **Lack of Internal Network Segmentation** | Malware, VLAN hopping |
| 5 | BackDoor Attack | Lack of Logging and Monitoring | Cyber Espionage |
| 6 | IDOR attacks | Broken Access Control  | Vertical Privilege Escalation |
| 7 | Ransomeware Attacks | Lack of User Training | Wannacry |

Conclusion

Based on the initial testing efforts, the average risk level is extremely high. Complete system penetration is easily attained on vital security and file servers, which hold a plethora of sensitive and secret information and, if broken, expose the customer to a high risk of hefty fines and considerable commercial effect. Therefore, CFO Jerry Seinfield should not restrict the budget for security.

The purpose of this study is to draw attention to the cyber security status of the IT system at Worthy College and the danger it presents to the organization's commercial operations.

Software (Moodle platform, OS), hardware (FTP Servers, routers), human factors (User training), and data storage were among the most critical factors evaluated for IT infrastructure vulnerabilities and difficulties at Worthy College (Database).

References

Bruce Lynch (2022),  *Ransomware.* Imperva. Retrieved from https://www.imperva.com/learn/application-security/ransomware/#:~:text=Ransomware%20is%20a%20type%20of,unlock%20and%20decrypt%20the%20data.

Titus (2022), How Secure is Moodle? *Moodle Security.* Retrieved from https://www.tituslearning.com/moodle-security/

N.D. (2021), Cross-Site Scripting (XSS)/ Moodle XSS. Hackerone. Retrieved from

<https://hackerone.com/reports/1165540>

Yadav, S., Crasto, C., Syed, S., & Syed, S. (2020, June). Validation and Optimization of Vulnerability Detection on Web Application. In *Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT)*.

Lu, Q. C., Xu, P. C., & Zhang, J. (2021). Infrastructure-based transportation network vulnerability modeling and analysis. *Physica A: Statistical Mechanics and its Applications*, *584*, 126350.

Stankov, I., & Tsochev, G. (2020). Vulnerability and protection of business management systems: threats and challenges. *Problems of Engineering Cybernetics and Robotics*, *72*, 29-40.

Xu, Y., Yang, Y., Li, T., Ju, J., & Wang, Q. (2017, November). Review on cyber vulnerabilities of communication protocols in industrial control systems. In *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)* (pp. 1-6). IEEE.