AUGUST 21, 2024

VULNERABILITY ASSESSMENT REPORT

SUMMER 2024

PREPARED BY: RAMON LOPEZ & CHRISTOPHER ALSAY
UAT CYBER PROJECT

Table of Contents

Executive Summary:

The UAT Cyber Project is a resolute team tasked with conducting a comprehensive vulnerability assessment on the University of Advancing Technology's network. The team's primary goal is to meticulously identify any potential flaws within the school's network infrastructure. By doing so, we aim to uncover vulnerabilities that could be exploited by unauthorized entities.

Objectives:

- **Identify Vulnerabilities:** Conduct thorough scans and tests to pinpoint weaknesses in the network.
- **Prevent Unauthorized Access:** Implement recommendations to mitigate the risks of break-ins and unauthorized access.
- **Enhance Security Posture:** Provide recommendations and solutions to fortify the network against future threats.

By identifying and addressing these vulnerabilities, we strive to create a safer and more secure environment for the entire UAT community. Our efforts will help protect sensitive information and ensure the integrity and reliability of the university's network systems.

Members:

Below is the list of members who have participated in the 2024 UAT Vulnerability Assessment.

Semester Members

Christopher Alsay	Penetration Testing Team Lead
Ramon Lopez	SCRUM Master Team Lead
Braden Greenwall	Website Tester
Shjon Oelke	Website Tester
Sarah Dahm	Researcher/Documenter
Adam Warren	General Penetration Tester
Curran Rose	General Penetration Tester
Keven Baquerizo	General Penetration Tester
Mahmoud Hamadah	General Penetration Tester

Milestone Members

Tecumseh McMullin	General Penetration Tester	Milestone 1
Brian Whitlow	Documenter	Milestone 1
Mariam Ahandy	Documenter	Milestone 2

Introduction:

In conducting a risk assessment for the school's IT infrastructure, our focus centered on performing penetration testing of both the web application and network enumeration. Through this process, we identified significant vulnerabilities within the web application, such as inadequate session management and potential information leakage via error messages. Out of the 12 IP Addresses that we have attacked, a total of 5 vulnerabilities were found within the school's network:

Vulnerability Risk Level	***Unique Count***
High Severity Vulnerabilities	1
Medium Severity Vulnerabilities	2
Low Severity Vulnerabilities	2

These findings underscored the importance of continuously updating and refining security measures to protect sensitive data and ensure compliance with regulatory standards. Additionally, our network enumeration highlighted weaknesses in network segmentation and identified open ports susceptible to exploitation. Addressing these issues promptly is essential to fortifying the school's IT defenses, ensuring data security, and maintaining a safe digital environment for students, faculty, and staff. The most critical vulnerabilities identified include the use of unencrypted protocols on ports 21 (FTP) and 80 (HTTP). Both ports expose the network to significant risks, including data breaches and man-in-the-middle attacks. The presence of services on these ports without encryption or strong authentication represents a serious security flaw that must be addressed immediately. Additionally, improper configurations on port 22 (SSH) and the unidentified service on port 1119 pose potential risks that require attention to prevent unauthorized access and ensure secure communication.

Assessment Scope:

The project focuses on performing a comprehensive vulnerability assessment of the school's network infrastructure. This assessment will encompass the following key activities:

1. **Network Scanning and Testing:** Conduct a series of thorough scans and penetration tests to identify potential weaknesses and vulnerabilities within the network systems. This includes evaluating network devices, servers, applications, and other critical components for security gaps.
2. **Risk Analysis:** Analyze the identified vulnerabilities to determine their potential impact and the likelihood of exploitation by unauthorized entities. This will involve assessing the severity of each vulnerability and its implications for network security.
3. **Recommendation and Mitigation:** Develop and propose actionable recommendations to address the discovered vulnerabilities. This will include specific measures and best practices to prevent unauthorized access and enhance the overall security posture of the network.
4. **Reporting and Documentation:** Compile a detailed report outlining the findings of the assessment, including identified vulnerabilities, their potential risks, and recommended remediation strategies. The report will serve as a guide for implementing improvements and fortifying the network against future threats.

The project aims to ensure a secure and reliable network environment for the UAT community by proactively identifying and addressing potential security risks.

Objectives:

The main objective of the vulnerability assessment is to rigorously identify and evaluate potential weaknesses within the school's network infrastructure. This process involves conducting comprehensive scans and tests to uncover any vulnerabilities that could be exploited by unauthorized entities. By pinpointing these weaknesses, the assessment aims to provide a detailed understanding of where and how the network may be susceptible to security breaches. Furthermore, the assessment seeks to enhance the overall security posture of the network by offering targeted recommendations and solutions to address the identified vulnerabilities. The goal is to mitigate the risks of unauthorized access, thereby safeguarding sensitive information and maintaining the integrity and reliability of the university’s network systems. Through these efforts, the assessment contributes to creating a safer and more secure environment for the entire UAT community.

Vulnerability Assessment:

The UAT Cyber Project team employed a systematic and comprehensive approach to conduct the vulnerability assessment of the university's network. The goal was to identify potential security weaknesses that could be exploited by unauthorized entities. Our methodology consisted of the following key steps:

1. Initial Scoping and Planning
2. Researching Tools and New Exploits
3. Reconnaissance
4. Practice Assessment
5. Main Vulnerability Assessment

This methodology reflects a thorough and structured approach to vulnerability assessment, ensuring that all critical areas were examined and that the recommendations provided are based on a solid understanding of the network's security needs. If there are specific tools or techniques that were used that you want to highlight, I can incorporate those details as well.

Tools:

Tool	*Description of Tool*
Nmap	NMap (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It identifies hosts, services, and vulnerabilities on a network by sending specially crafted raw packets and analyzing the responses. NMap can perform tasks like host discovery, port scanning, service version detection, and operating system detection. Its ability to scan large networks efficiently and its flexibility make it a critical tool for understanding the security posture of a network.
Kali Linux	Kali Linux is an advanced, open-source operating system specifically designed for penetration testing, ethical hacking, and digital forensics. It comes preloaded with hundreds of security tools and utilities that target both online and physical systems, applications, and networks. Kali Linux supports a wide range of wireless devices and is equipped to perform tasks such as vulnerability assessments, security research, and penetration testing, making it an essential platform for cybersecurity professionals.
Metasploit	Metasploit is an open-source framework that provides security professionals with the tools to evaluate and exploit security vulnerabilities in computer systems. It contains a vast library of exploits and payloads, allowing users to simulate real-world attacks to uncover weaknesses in their systems. Metasploit is also used for developing and testing custom exploits, performing security assessments, and conducting penetration testing, making it a versatile and indispensable tool in the cybersecurity field.
Greenbone	Greenbone is an open-source vulnerability management tool that helps identify, assess, and mitigate security vulnerabilities in IT systems before attackers can exploit them. It provides a comprehensive solution for vulnerability scanning, management, and reporting. Greenbone integrates with the OpenVAS (Open Vulnerability Assessment System) scanner to perform in-depth security assessments, identifying misconfigurations, outdated

software, and other potential security risks, making it a valuable tool for initiative-taking security management.

The assessment identified several open ports, including port 21 (FTP), port 22 (SSH/SFTP), port 80 (HTTP), port 443 (HTTPS), and port 1119. These open ports present various risks such as unauthorized access, data breaches, and potential exploitation of web services.

Assessment:

The assessment identified several open ports, including port 21 (FTP), port 22 (SSH/SFTP), port 80 (HTTP), port 443 (HTTPS), and port 1119. These open ports present various risks such as unauthorized access, data breaches, and potential exploitation of web services.

Port	*Description*	*Impact*	*Risk Level*	*Affected Systems*
21	FTP (File Transfer Protocol) - Used for transferring files between systems, typically without encryption, which means data can be intercepted or tampered with.	Potential unauthorized uploading of malicious files, downloading of sensitive data, and gaining system access, leading to data breaches or system compromise.	High	Web servers, file servers
22	SSH/SFTP (Secure Shell/Secure File Transfer Protocol) - Used for secure remote access to systems, networks, and devices.	Allows for remote admin access, file transfers, and access to cloud services. If exploited, it can grant unauthorized admin-level access and lead to a full system takeover.	Medium	Web servers, file servers, network devices, cloud servers
80	HTTP (Hypertext Transfer Protocol) - The default port for web browsers to access websites and web services.	Allows access to websites and services, potentially leading to SQL injections, cross-site scripting, malware distribution, and other web-based attacks.	Medium	Web servers, web applications
443	HTTPS (Hypertext Transfer Protocol Secure) - Like HTTP but with encryption to ensure secure communication over the network.	Enables secure data transfer but can be exploited for eavesdropping, tampering, and man-in-the-middle attacks if not effectively managed, particularly in certificate handling and updates.	Low- Medium	Web servers, web applications

1119	Custom/Network File Systems/Testing and Development Port - Not a well-known port and usage can vary, making it a potential target for custom applications.	Requires monitoring as it is uncommon, but if exploited, it could indicate malicious activity related to custom applications or testing environments, potentially leading to unauthorized access.	Low-Medium	Custom applications, testing environments

Recommendations:

Port	*Remediation Steps*	*[#]*	*Mitigation Strategies*
21	**Disable or Replace**: FTP is an insecure protocol as it transmits data in plaintext. Consider disabling it and using SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure) instead. **Restrict Access**: If FTP is essential, restrict access to only trusted IP addresses and implement strong authentication mechanisms. **Encrypt Data**: Ensure that all data transfers are encrypted to prevent data interception.	1	**Short-Term Mitigation:** Restrict access to FTP by allowing only trusted IPs. Implement strong passwords and monitor FTP traffic closely until SFTP or FTPS is fully implemented.
22	**Use Strong Authentication**: Implement key-based authentication instead of password-based to reduce the risk of brute-force attacks. **Limit Access**: Restrict access to port 22 using IP authorization or VPNs to allow only trusted users. **Disable Root Login**: Prevent direct root login and use sudo for privilege escalation. **Monitor and Log**: Regularly monitor and log all SSH connections to detect unauthorized access attempts.	2	**Short-Term Mitigation:** Immediately disable root login and enforce key-based authentication. Use IP authorization or VPNs to limit access to trusted users until more permanent solutions are in place.
80	**Migrate to HTTPS**: All HTTP traffic should be migrated to HTTPS to ensure encrypted communication and data integrity. **Redirect HTTP to HTTPS**: Implement redirection from HTTP to HTTPS to enforce secure connections. **Harden Web Server**: Ensure the web server is configured securely by disabling unnecessary modules, setting secure headers, and keeping software up to date.	3	**Short-Term Mitigation:** Enable HTTP to HTTPS redirection immediately to ensure all traffic is encrypted, even if the full migration isn't complete yet.
443	**Use Strong Encryption**: Ensure that SSL/TLS configurations are strong by using up-to-date protocols and ciphers.	4	**Short-Term Mitigation:** Review and update SSL/TLS configurations to ensure they are strong. Begin

	Regularly Update Certificates: Regularly update SSL certificates and ensure they are from a trusted Certificate Authority (CA). **Implement Web Application Firewall (WAF)**: Use a WAF to protect web applications from common vulnerabilities like SQL injection, XSS, etc. **Monitor and Log**: Continuously monitor SSL/TLS traffic and log suspicious activities for analysis.		implementing a WAF to protect web applications and start logging SSL/TLS traffic for suspicious activity.
1119	**Identify the Service**: Determine the specific service running on this port. If it's not essential, consider disabling it. **Harden the Service**: If the service is necessary, ensure it is properly secured with the latest patches, strong authentication, and encryption. **Restrict Access**: Limit access to the service to only necessary users or systems, using firewalls or access control lists (ACLs).	5	**Short-Term Mitigation:** Limit access to the service running on this port using firewalls or ACLs. Apply any available patches and ensure the service is up to date.

Conclusions:

In this vulnerability assessment, we identified several critical vulnerabilities that pose significant risks to the network. The most urgent issues involve the use of unencrypted protocols on ports 21 and 80, which could lead to data breaches and other security incidents. We also identified potential risks associated with SSH configurations on port 22 and an unidentified service on port 1119. To mitigate these risks, we recommend immediately replacing FTP with a secure protocol, migrating all HTTP traffic to HTTPS, and implementing stronger authentication and access controls on SSH. Additionally, securing or disabling the service on port 1119 is crucial. These steps will significantly enhance the network's security posture, protecting it from unauthorized access and potential attacks.

Final Thoughts:

The penetration test identified several critical and high-risk vulnerabilities associated with open ports, weak configurations, and potential security gaps. While some of these issues are common in many networks, their presence in your environment underscores the need for a more robust security strategy. In conclusion, this penetration test serves as a crucial step in identifying and mitigating risks. The key to enhancing security lies in prompt action, continuous vigilance, and a commitment to fostering an initiative-taking security mindset across the organization.