Capstone Project Report

Jack Pursley, Robin Tandonfor, Elijah VanDorn, Valentine Wairimu, and Kylah Wilson

College of Computing and Software Engineering, Kennesaw State University

IT4983: IT Capstone Project

Professor Donald Privitera

November 17th, 2024

Table of Contents:

Executive Summary

During this project, we leveraged Microsoft Project to manage our tasks, assignments, and progress, using Gantt charts for effective scheduling and tracking. Our primary responsibility was to conduct a comprehensive risk assessment on a designated IP address to fortify a web server against potential penetration attempts by an opponent. The key objective was to ensure the security of the server infrastructure and mitigate vulnerabilities to prevent unauthorized access.

Our risk assessment involved evaluating the server's infrastructure and identifying critical digital assets requiring protection. These included databases, application code, user credentials, and sensitive company information. We also assessed potential threats such as malware, brute force attacks, and other known vulnerabilities that could compromise these assets. For each identified threat, we evaluated the potential damage that could occur if an attack were successful, which helped us prioritize the risks accordingly.

In addition to the technical risk assessment, we were tasked with developing a general security policy for the organization. This policy encompassed key areas such as internet access, email usage, authentication mechanisms, encryption standards, password management, and guidelines for employees using their own devices (BYOD). We also implemented an access management policy to regulate employee access to sensitive data, ensuring that permissions were aligned with job roles and responsibilities.

Our work also included a prioritized a list of risks from the assessment, each requiring tailored mitigation strategies to enhance the server's security posture. These efforts will be concluded at Milestones 2, marking the completion of the risk management phase, and laying the foundation for a robust, secure infrastructure.

This comprehensive approach ensures that both technical vulnerabilities and organizational security policies are addressed, safeguarding the company's digital assets from internal and external threats.

Background

Business Information and Context:

This project is designed for small businesses that rely heavily on its digital infrastructure to store sensitive information, facilitate communication, and run critical business operations. As digital threats evolve and become more sophisticated, the business recognizes the need to protect its server from potential cyberattacks that could compromise sensitive data or disrupt its services. This project aims to assess the business's cybersecurity posture and implement effective policies and defenses.

Some problems the business faces would be ensuring that its server infrastructure is secure from common cyber threats such as unauthorized access, malware, ransomware, and data breaches. Also, without an effective risk assessment and mitigation strategy, the business is vulnerable to operational downtime, data loss, financial losses, and reputational damage.

Goals:

The goal of this project is to:

- Evaluate the security of the server infrastructure.
- Identify critical assets and associated threats.
- Implement a comprehensive information security policy to mitigate risks.
- Prepare the server for real-time attacks and defenses in a simulated cybersecurity exercise.

Specific Project Scope, Objectives, and Deliverables:

- Assess the server's infrastructure to identify weaknesses.
- Create an information security policy that addresses the business's needs, focusing on areas like access management, password policies, encryption, and BYOD.
- Engage in a Red/Blue Team cybersecurity exercise, where teams will alternately attack and defend their servers in a controlled environment.

Objectives:

- Conduct a risk assessment of the business's server
- Identify critical digital assets that require protection.
- Evaluate potential threats and vulnerabilities that could affect these assets.
- Develop risk mitigation strategies to protect the server.
- Establish and document a security policy tailored to the business.
- Engage in a cybersecurity exercise to test the effectiveness of the servers' defenses.

Deliverables:

- A detailed risk Assessment Report Assuagement Report (Milestone 1), including the evaluation of the server's infrastructure, assets, threats, and risk mitigation strategies.
- A comprehensive Information Security Policy for the business.
- Logs and reports of Red/Blue Team Exercise results, including offensive and defensive actions taken, as well as screenshots of vulnerabilities and exploits.

Technical Background:

The business operates a server that hosts critical applications, databases, and sensitive data. This server forms the backbone of the company's digital infrastructure, handling everything from web hosting to email and database management. The server may run on common operating systems like Linux or Windows Server, with numerous services supporting the company's day-to-today operations. Ensuring the security of this server is paramount to maintain business continuity and safeguarding sensitive information.

In this project, key technical concepts and practices are integral to securing the server. Risk assessment plays a significant role, involving the evaluation of potential threats, understanding their likelihood, and prioritizing them based on the severity of their impact. This assessment informs the creation of robust information security policy, which will outline best practices for securing the organization's IT environment. Such policies for securing the organizations IT environment. Such policies cover areas including password protocols, encryption standards, authentication methods, and access control measures, all designed to mitigate the risk of unauthorized access or breaches.

Access control is another critical component, ensuring that only authorized personnel can reach sensitive data and systems. This is enforced through techniques like role-based access controls and multifactor authentication. Vulnerability management also plays a key role in identifying and addressing security flaws in the server's software and hardware. Keeping the server updated with the latest patch is essential to minimize its exposure to attacks.

Various technologies will be employed through the project. Firewalls will help prevent unauthorized access to the network, while intrusion detection and prevention systems monitor for suspicious activity. Antivirus and antimalware tools will protect against malicious software, and encryption technologies will ensure that sensitive data is secured both at rest and in transit. During the Red/Blue Team exercise, penetration testing tools such as Metasploit and Nmap will be utilized to simulate attacks and test the effectiveness of the defenses. These tools and practices form the foundation of the technical environment in which the project is carried out, ensuring that the server is protected from evolving cybersecurity threats.

Project Outcomes and Achievements Summary

The Cybersecurity Website Hardening Project successfully enhanced the security of a small business's website, hosted on a Red Hat Linux server (*The World's Open-Source Leader*, n.d.). This initiative involved a comprehensive risk assessment, development of an information security policy, and a Red/Blue Team exercise simulating real-world attacks and defense mechanisms. Our project met its objectives by creating a robust security framework that significantly reduced potential vulnerabilities while strengthening the team's practical cybersecurity skills.

Key Outcomes

Milestone 1

1. Risk Assessment - Team #3 conducted a thorough risk assessment of the website's server infrastructure. The analysis identified key vulnerabilities in authentication, access management, and outdated software versions. Critical digital assets, such as customer databases and financial records, were prioritized for protection. A mix of various tool websites were utilized, along with ChatGPT for explanations of their common uses (OpenAI, 2024).

Results:

- Identified 79 vulnerabilities from our Lynis scan ranging from suggested changes to priority changes (*Lynis - Security Auditing and Hardening Tool for Linux/Unix*, n.d.).
- Assessed the probability and potential impact of each threat, including DDoS attacks and data breaches.
- Developed a prioritized mitigation plan focusing on high-severity vulnerabilities, Real Time monitoring, Web Application Firewall and using Modsecurity to identify attacks (*OWASP ModSecurity Project*, n.d.).
- Risk Mitigations that helped with overall project success included Penetration testing and vulnerability assessment to identify and address potential security risks in systems.

The Red Hat server we were given had many issues that needed addressing. The following is a technical summary of our different findings and fixes:

- We first looked around at how the systems worked. After learning how to download some audit tools (Lynis and Nmap), we ran them to see what we were dealing with (*Nmap: The Network Mapper - Free Security Scanner*, n.d.). Some of the most obvious issues included Red Hat being out of date, no malware scanner being installed, and the Kernal keys not matching.

Milestone 2

1. Risk Mitigation - Our next step was to figure out how to patch these most important issues. We first updated the Red Hat OS by installing the package update. Next, we installed a malware scanner called ClamAV (*ClamAVNet*, n.d.). Afterwards, we enabled the server’s default firewall to help prevent automatic system responses to malicious scans or pings.

Unfortunately, additional risks were also spotted in this milestone as well, such as the server admin password needing to be changed, Apache headers needing additional security, and backups needing to be created. Here is how we dealt with these new risks along with the others:

- We changed the administrator password and increased it from 12 characters to 24.
- We added various headers for Apache, including MIME Sniffing protection, Cross Site Scripting Attack protection, and Clickjacking protection.

- HSTS was also enabled for Apache. It tells browsers that they should only communicate with the server using HTTPS, not HTTP, and it also prevents users from bypassing SSL/TLS warnings by clicking through.
- Downloaded and enabled Modsecurity for Apache, which enables real-time monitoring, logging, and access control for traffic to protect web applications from various attacks/vulnerabilities.
- Downloaded a DNS server software called BIND, which ensured that DNSSEC would be turned on to prevent DNS spoofing.
- Installed rng-tools, a package that helps bridge the HW RNG and the kernel's entropy pool.
- Updated GRUB2 to ensure the bootloader was working correctly.
- Kernel Hardening Key Pairs were updated to match their expected values

2. Security Policy - Internet Usage/Acceptable Use Policy

It is important to note that internet access is provided for business purposes only. Therefore, the internet should not be used for violation of any law or for social media purposes. Personal use is discouraged and should not interfere with work duties. Access to inappropriate sites, such as those containing illegal content or related to gambling, is strictly prohibited. Please be aware that all internet activity will be monitored. It is essential for employees to refrain from engaging in activities that pose cybersecurity risks, such as connecting to unsecured Wi-Fi networks, downloading unauthorized software, or visiting suspicious websites. Additionally, it is crucial to adhere to the following guidelines: refraining from attempting to disrupt the information security of any computer network, refraining from posting commercial messages without prior permission, refraining from sending junk email messages or spam, refraining from attempting to mail bomb a site in order to flood the server, refraining from attempting to steal intellectual property, and reporting any attempt to break into your account. (Kirvan, 2022)

Email Usage:

To ensure the security of our business communications, all email accounts are to be used exclusively for business purposes. Employees are required to exercise caution and refrain from opening suspicious attachments or clicking on links from unknown sources. It is imperative that all staff members undergo training in email security best practices, including creating strong passwords that incorporate a combination of letters, numbers, and special characters to bolster email protection. Furthermore, employees are advised to refrain from using easily guessable information such as birthdays and names in their passwords. Email encryption must be utilized for all confidential communications. In addition, passwords should be changed every three months, and employees must be educated on the risks associated with reusing passwords. Multi-factor authentication will be implemented to enhance security, and employees will be provided with training on identifying and responding to cyber security threats such as phishing attacks. To promote awareness and vigilance, employees should be taught to recognize common red flags for phishing emails, such as requests for sensitive information, misspellings, and unfamiliar sender addresses. It is essential for employees to verify the authenticity of requests before taking any action, especially in cases where urgent action or sensitive data is demanded. Adoption of email security features, such as spam filters and email authentication protocols, can aid in identifying potential phishing attempts. Moreover, we encourage all employees to promptly report any suspicious emails to our IT or security team. (ShareFile, 2024)

Authentication and Access Control Policy:

To ensure a secure environment, users are required to adopt strong, unique passwords and implement multi-factor authentication (MFA) where applicable. Passwords must be at least sixteen characters long, incorporating a mix of uppercase and lowercase letters, numbers, and special characters. These passwords should be updated every 90 days to enhance security (ShareFile, 2024). Furthermore, default accounts will be disabled, and default passwords will be replaced to reduce the risk of unauthorized access. Appropriate file permissions will be enforced, restricting access to web server configuration files to only authorized personnel, ensuring the integrity of critical directories and files.

Access control will be managed using various models to enhance security. Discretionary Access Control (DAC) allows resource owners to dictate who can access the data and the level of access granted. Mandatory Access Control (MAC) enforces strict access based on organizational policies and data sensitivity, suitable for environments where data confidentiality is paramount. Role-Based Access Control (RBAC) limits access based on the user's job functions, streamlining access management in larger organizations.

In addition, regular software and system updates, including security patches, are essential to addressing known vulnerabilities. Employee training on security best practices should be conducted regularly to ensure that users are aware of how to maintain a secure environment and recognize potential threats. To detect unauthorized activity, continuous monitoring and logging of network and system activities should be implemented. Conducting routine security audits and vulnerability assessments will identify and mitigate potential risks, ensuring the organization maintains a robust security posture.

Network Security:

Access to the internal network requires secure authentication methods, including biometrics (such as fingerprint and facial recognition), strong passwords, multi-factor authentication (MFA), and ID tokens. These layers of security provide a defense against unauthorized access by ensuring that only verified users can gain entry to systems.

To safeguard against potential breaches, all systems must log and monitor login attempts. This logging will track successful and failed authentication attempts, providing an essential layer of oversight for detecting unauthorized access and responding swiftly to suspicious activity. (CIS,2023)

Firewall Configuration:

The firewall must be configured to block all unnecessary ports, allowing only the traffic essential for the web server’s operation. This approach minimizes the exposure of the server to external threats.

Network segmentation should be implemented to isolate the web server from other critical internal systems. This measure reduces the risk of a compromised server leading to wider access within the network. (CIS, 2023)

Intrusion Detection and Prevention:

Akwabaa will deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to continuously monitor network traffic for suspicious behavior. IDS will alert administrators to potential security breaches, while IPS can actively block malicious traffic in real-time. These systems are crucial for identifying and mitigating threats before they cause significant harm.

Encryption Policy:

Advanced Encryption Standard (AES) is a widely adopted encryption algorithm used to secure sensitive data in both software and hardware implementations. AES-256, the most secure variant, provides robust protection for data at rest and in transit, making it ideal for cybersecurity applications in protecting IT infrastructures such as databases, communications, and sensitive files. AES encryption is critical for ensuring confidentiality in modern cybersecurity frameworks.

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that ensure secure communication over networks, providing data encryption, privacy, and integrity. TLS, the successor to SSL, is widely implemented to protect information exchanged between computers over the internet, ensuring authentication of both parties and preventing data interception (CISA, 2021). SSL/TLS is essential for encrypting web traffic, safeguarding online transactions, and securing email communications.

Incident Response:

In the event of a security breach, it is imperative that all incidents are reported immediately to the IT department. Prompt reporting enables a swift response immediately to the IT department. Prompt reporting enables a swift response to contain and mitigate the potential damage caused by the breach. Upon receiving the report, the organization will conduct a thorough investigation to determine the nature and extent of the threat, take immediate action to contain the incident, and implement any necessary remediation steps to protect the systems and data. Following the incident, a post incident analysis will be conducted to identify the root cause, evaluate the effectiveness of the response, and implement improvements to enhance future security measures and prevent similar occurrences. This process ensures continuous improvement in the organization’s security posture. (Jones, 2024)

Security Awareness and Training:

All staff members are required to undergo regular security training to understand organizational security procedures, best practices for data handling, and incident response protocols. This training equips employees with the knowledge to protect sensitive information, recognize potential security threats, and respond appropriately in the event of a security incident, thereby contributing to the overall security of the organization. (Katz, 2023)

Roles and Responsibilities:

Key personnel play a critical role in maintaining the security of the organization. The IT department is responsible for overseeing the implementation of all security measures and promptly responding to any security incidents that may arise. They ensure that the system is protected, and any vulnerabilities are addressed. The HR department manages the onboarding and offboarding processes, which include creating and deactivating employee accounts to prevent unauthorized access when an employee leaves the organization. Employees on their part are expected to adhere to all security policies and actively report any suspicious activity they observe, contributing to the overall security posture of the organization. (OpenAI, 2024)

Policy Review and Enforcement:

The policy will undergo an annual review to ensure it remains aligned with evolving security requirements and industry best practices. During this review, any necessary updates will be made to address emerging threats, modern technologies, or changes in the organization's infrastructure. This proactive approach ensures that the policy stays relevant and effective in safeguarding the organization's assets. Employees are expected to fully comply with the policy, as adherence is critical to maintaining the security and integrity of the webserver and other systems. Failure to comply with the policy may result in disciplinary actions, which could range from warnings to more severe consequences, such as suspension or termination of employment, depending on the severity of the non-compliance. The organization takes security seriously, and these measures are in place to protect both the employees and the company from potential security breaches or vulnerabilities. (Indeed, Editorial Team, n.d)

Monitoring and Logging:

To enhance web server security, it is crucial to enable logging for all activities, such as login attempts, access requests, and configuration changes, and to store these logs securely in a centralized location to prevent tampering. Monitoring tools should be employed to detect unusual activities or potential threats, like excessive login failures or abnormal traffic patterns.

Regular backups of web server configurations and content are essential, and the restoration process should be tested periodically to ensure quick recovery in the event of a failure or security incident. Additionally, storing copies of data helps protect it in case of a system failure, while maintaining a strong Data Security Posture (DSPSM) ensures comprehensive protection against potential risk. (Aharon,2023)

Access Management Policy:

The Access Management Policy ensures that access to company systems, applications, and data is controlled, monitored, and restricted based on the principle of least privilege. This policy is based on guidelines set by NIST and ISO standards to protect the organization from unauthorized access, data breaches, and ensure compliance with regulatory requirements (NIST, 2020; ISO/IEC 27001, 2022).

User Identification and Authentication:

- All users are uniquely identified by a username, and passwords must meet complex requirements and be changed every 90 days.

- multi-factor authentication (MFA) is required for accessing critical systems (NIST, 2020).

User Access Provisioning:

- Access is granted based on job roles and responsibilities through a formal request and approval process (ISO/IEC 27001, 2022).
- Access must be approved by department managers and IT security.

Role-Based Access Control (RBAC):

- Access permissions are defined based on roles within the company, adhering to the principle of least privilege (NIST, 2020).
- Regular reviews ensure that roles remain appropriate for each user.

Access Reviews and Audits:

- Periodic access reviews are conducted quarterly to maintain appropriate access levels.
- Any unauthorized access or discrepancies are reported and corrected immediately (ISO/IEC 27001, 2022).

Termination of Access:

- When an employee or contractor leaves, access is immediately revoked. Role changes or department transfers trigger a review and update of access privileges (NIST, 2020).

Privileged Access Management:

- Privileged accounts undergo additional scrutiny and monitoring, and all activities performed using these accounts are logged and reviewed periodically.
- Privileged accounts are used only when necessary for specific tasks (ISO/IEC 27001, 2022).

Third-Party and Vendor Access:

- Third-party access is limited to the required scope of work and is time-bound with regular reviews.
- All external parties must sign confidentiality agreements and comply with the company’s access management policies (NIST, 2020).

Incident Reporting:

- Any unauthorized access or suspicious activity is reported to IT security immediately, and incidents are thoroughly investigated (ISO/IEC 27001, 2022).

Milestone 3

Red/Blue Team Exercise:

Red Team Findings

Conducting a stealth scan, a popular technique used in pen testing to gather information about a target system in a way that minimizes the chances of detection by intrusion detection systems or firewalls, we found open ports.

The system has several open ports, each corresponding to a specific service. Port 22/tcp is running the Secure Shell (SSH) service, which enables secure remote login and command execution. SSH is a critical tool for system administrators but can pose a security risk if improperly configured or if weak authentication methods are used, potentially allowing unauthorized access. Port 25/tcp is associated with the Simple Mail Transfer Protocol (SMTP) service, which is primarily used for sending email.

While essential for email communication, an open SMTP port can sometimes be misconfigured, leading to vulnerabilities such as open relays. Open relays allow attackers to use the server to send spam or malicious emails, which could lead to security issues. Finally, port 443/tcp is running Hypertext Transfer Protocol Secure (HTTPS), the secure version of HTTP. HTTPS ensures encrypted communication between a web browser and the server, protecting sensitive data, such as login credentials and personal information, during transmission. The presence of HTTPS indicates that the server is configured to handle secure web traffic and protect user data from eavesdropping or tampering.

After downloading and setting up Medusa, we created the necessary userlist.txt and passlist.txt files to be used for the attack. However, during the first attempt, Medusa was unable to load the required SSH module (ssh.mod), which prevented the tool from executing the brute-force attack against the target server. This issue was related to either a misconfiguration in the Medusa installation or a compatibility issue with the SSH module. In the second attempt, despite resolving the module issue, Medusa faced difficulties establishing an SSH session with the target server at IP address 10.96.33.60. This failure could have been caused by network issues, incorrect SSH configurations on the target server, or security measures like firewalls or rate-limiting that blocked or throttled the connection attempts.

The results of the SSH server scan reveal several important security configurations. First, the scan shows "NULL" for compression, indicating that compression is disabled on the server. While compression can improve performance, it has historically been associated with certain vulnerabilities, such as the "CRIME" attack, so disabling it is a prudent security measure. The server is set to control the choice of encryption method (cipher) during the SSH handshake, rather than letting the client decide. This is a safer setup because it allows the server to enforce the use of stronger encryption, reducing the risk of weaker or outdated methods being used. Additionally, the weakest cipher available on the server is rated "A," which means all supported ciphers are strong and secure. This setup ensures that the server is well-protected with strong encryption, making it harder for attackers to exploit any weaknesses in the encryption process.

Blue Team Findings:

Brief Preparations

We Pen-tested with Nmap on our IP address. We received level 250 “good luck” with TCP sequence prediction. This means the chance of a cyberattack involving predicting the sequence numbers used in our TCP connection to inject malicious data or take over the connection is incredibly low. The scan couldn’t determine the operating system. We did find our open ports, though. We then Installed hunter to scan for potential rootkit malware. Afterwards, we updated found an update for RHEL 8 and updated again. Finally, we correctly enabled fail2ban jails to block someone once just in case before turning it off as instructed.

Initial Brute Force Attack

A user tried to get in using Administrator and root names. They didn’t get in, but they were able to take advantage of Visudo and disabled the firewall briefly. If our password was not as strong as it is, this could have been disastrous.

We fixed this by requiring a password when the user wants to use the “sudo” command. We also made it so any user without a password wanting to generate an SSH public key to copy onto our server to bypass password inputs would not be allowed. It’s possible that they used SSH key generation to run certain commands without a password. As far as we can tell through various logs tracking the IP address’s actions, they did not find or do anything else.

Second Brute Force Attack

Another IP address tried to get in on November 4 but couldn’t find the correct administrator name.

System Log Monitoring

Conducted a Logwatch scan to monitor system logs for unusual activities or potential threats. This step was critical in maintaining visibility over login attempts and identifying suspicious patterns that could indicate a security breach.

Sudo Command Monitoring

Monitored sudo command usage to track administrative actions on the system. Observed frequent use of commands related to file management, system updates, and security configurations. This tracking of privileged command usage aids in detecting potential misuse or unauthorized changes.

Disk Space Verification and Logwatch Configuration

Verified disk space availability to ensure adequate resources for logging activities. Encountered and resolved a permission error during initial Logwatch setup, which improved our logging configuration and confirmed that system resources were managed efficiently.

Logwatch Report Analysis (Extended Period)

Generated and analyzed Logwatch reports covering the entire red/blue team exercise period. Key findings included multiple authentication failures, unmatched entries indicating system cache errors, and repeated failed login attempts from specific IP addresses. This proactive monitoring helped identify potential security threats and refine our response strategies.

Project Planning and Management Summary

Overview:

We managed the project effectively by distributing the workload based on our project plan and assigned roles. Initially, we faced challenges with meeting consistency; our schedules varied for the first milestone. However, we addressed this by improving our communication and aligning our availability.

To enhance our collaboration, we shifted from weekly meetings on Wednesdays to holding them every Tuesday, Wednesday, and Thursday. This change significantly increased our communication, leading to improved productivity and clarity about individual contributions.

For project management, we utilized several tools: Microsoft Project, Microsoft Teams, and Microsoft PowerPoint. We created our Gantt chart and Resource Overview in Microsoft Project, while Teams facilitated communication and hosted our Milestone Presentations and weekly meetings. PowerPoint was used to develop our presentation materials. This streamlined approach has helped us stay organized and focused throughout the project.

Project process:

Milestone 1: Risk Assessment Phase

Objective: Identify digital assets and categorize their importance. Analyze threats and vulnerabilities and research ways to mitigate them.

Deliverables:

- Detailed Assessment of the Server
- Identification of Critical Assets
- Analysis of Potential Threats
- Recommendations to mitigate risks

Challenges:

Setting up the server and getting the E-commerce site live.

The first Milestone report meeting was too close to due dates for presentations. Going forward, the team needs to plan better to allow more time for decision making and planning.

Meetings need to be clear and systematic with clear expectations/goals that need to be met by the end of the meeting to ensure high collaboration.

Lack of background/experience in technicalities in the cyber space – more time required to do research and acquire knowledge and overall team support

The lack of consistent Teams Channel communication due to the nature of Teams Channel organization – the solution was to create a separate Team's channel which improved fluidity of communication and for quick responses.

Milestone 2: Information Security and Risk Mitigation Phase

Objective: A comprehensive information security policy for a small business should address key areas like internet access, email usage, authentication, encryption, password management, and BYOD (Bring Your Own Device) policies. It should include an access management policy that defines employee roles and permissions to restrict access based on necessity. Additionally, a risk mitigation plan is essential, outlining identified risks from the assessment phase along with a clear timeline and strategy for implementing security measures.

Deliverables:

- Creation of information security policy.
- Risk Mitigation Plan that addresses all identifies risk mentioned in risk assessment phase.

Milestone 3: Red/Blue Team Phase

Objective: To penetrate the opposing team's website while keeping the integrity of our own. We will then conclude the project by producing a final research paper/report that will show our website's integrity and indicators of compromise over time.

Deliverables:

- Detailed log of penetration attempts
- Log of our Team’s defensive action.

Team contribution summary:

1. Robin Tandongfor (Team Leader)

- Tasks: Technical writing, meeting note-taker/recorder, creating and maintaining the team site, cybersecurity research, and web server testing.
- Responsibilities: Facilitating group progress by scheduling and running meetings, creating outlines for presentations, and acting as a liaison between the project owner/professor and the team.

2. Kylah Wilson

- Tasks: Research, network defense planning, security policy drafting, and implementation.
- Responsibilities: Drafting and implementing security policies related to the website hardening project.

3. Elijah VanDorn

- Tasks: Research risk assessment on important assets, list common threats, and analyze potential threats.
- Responsibilities: Conducting risk assessments, identifying threats, and analyzing their potential impact on the website.

4. Jack Pursley
- Tasks: Server infrastructure management, research on security hardening tactics, and penetration testing.

Responsibilities: Managing the server infrastructure and conducting penetration tests to identify vulnerabilities.

5. Valentine Wairimu
- Tasks: Assist in researching and implementing various project tasks.
- Responsibilities: Supporting team members by conducting research and contributing to various implementation tasks.

Workload summary:

1. Robin Tandongfor (Team Leader)
   - Responsibilities:
     - Led the Kickoff Meeting on 8/23/24 to initiate project planning.
     - Coordinated Team 3 Weekly Meetings from 8/28/24 to 9/18/24 to ensure progress towards Milestone 1.
     - Recorded meeting notes and kept the team on track with the project timeline.
     - Acted as the liaison between the team and Professor Privitera, ensuring clarity on project goals and deliverables.
     - Time Commitment: Weekly meetings and additional hours facilitating communication and project management.
2. Kylah Wilson
   - Responsibilities:
     - Conducted research on network defense planning, contributing to the identification of potential vulnerabilities and creating a strategy for mitigating threats.
     - Assisted in drafting sections of the security policy that will be further refined in later phases (Milestone 2).
     - Provided input during weekly meetings to support the completion of the risk assessment.
     - Time Commitment: Focused on research and policy drafting in collaboration with other team members.
3. Elijah VanDorn
   - Responsibilities:
     - Focused on risk assessment of important assets for the website infrastructure, identifying common threats and analyzing potential security risks.
     - Compiled the findings into a report outlining vulnerabilities and prioritizing risks based on their severity.
     - Collaborated with Jack Pursley on understanding the server infrastructure to ensure a thorough assessment of both physical and digital threats.

        - Time Commitment: Significant time spent on research, threat analysis, and report writing.

4. Jack Pursley
    - Responsibilities:
        - Managed the server infrastructure and conducted research on security hardening tactics to prepare for the later phases of the project.
        - Supported Team members in understanding the server’s potential vulnerabilities for the risk assessment.
        - Provided technical insight during weekly meetings to ensure the accuracy of the assessment.
        - Time Commitment: Server management and technical research leading up to Milestone 1.
5. Valentine Wairimu
    - Responsibilities:
        - Assisted in researching various aspects of cybersecurity risks and helped compile information for the risk assessment report.
        - Supported other team members in gathering data on network defense and server infrastructure vulnerabilities.
        - Time Commitment: General support for research and documentation.

This summary outlines each team member’s workload for Milestone 1, detailing their contributions to the project’s first major deliverable, the Risk Assessment.

Team Reflection

Project success:

- The team worked well together and followed a clear, organized plan.
- Each team member had specific skills, such as risk assessment, network defense, server management, and penetration testing, which helped us secure the Red Hat Linux server hosting the small business website.
- We followed the project steps carefully, starting with a detailed vulnerability assessment, creating and applying a strong security policy, and finally doing a Red/Blue Team exercise.
- By finding and fixing weaknesses, we made sure the website could resist cyber threats.

Collaboration and communication experiences

- Good communication, teamwork, and strong leadership by Robin Tandongfor helped us complete the project on time and meet all our goals.
- We all held each other accountable for time and strong communication skills to ensure that work was done effectively and efficiently.
- In the beginning we had challenges with organization and finding out what the meeting objectives are, but the team was able to outline expectations to meet at the end of each meeting which helped the team to remain focused.

Appendix

Project files list:

- Weekly Log Template.docx: Where all are submitted, and future logs are located
- Vulnerability tools.docx: Where are vulnerabilities tools that we run on the server are located
- Updates to Project Plan.docx: Where the updated Project Plan is located
- RACI Chart.xlsx: Where the RACI chart and RACI chart example is located
- Project Plan.docx: Where the original project Plan is located

Bibliography

ClamAVNet. (n.d.). https://www.clamav.net/

Lynis - Security auditing and hardening tool for Linux/Unix. (n.d.). https://cisofy.com/lynis/

Nmap: The Network Mapper - Free Security Scanner. (n.d.). https://nmap.org/

OpenAI. (2024). *ChatGPT (October 2024)*. https://chat.openai.com

OWASP ModSecurity Project. (n.d.). https://modsecurity.org/

The world's open-source leader. (n.d.). https://www.redhat.com/en

Indeed Editorial Team. (n.d.). *IT security policies: What they are and what to include*. Indeed. https://www.indeed.com/hire/c/info/security-policies

Splunk. (n.d.). *Audit logs*. Splunk. https://www.splunk.com/en_us/blog/learn/audit-logs.html

Jones, H. (2024, April 8). *Cybersecurity best practices: Incident reporting*. Collaboris. https://www.collaboris.com/cybersecurity-best-practices-incident-reporting/

Katz, S. (2023, August 1). *7 reasons why security awareness training is important*. CybSafe. https://www.cybsafe.com/blog/7-reasons-why-security-awareness-training-is-important/

Aharon, A. (2023, October 10). *What is log monitoring? A detailed guide*. Middleware. https://middleware.io/blog/what-is-log-monitoring/

Kirvan, P. (2022). What is acceptable use policy (AUP)? - definition from whatis.com. Retrieved fromhttps://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP#:~:text=An%20acceptable%20use%20policy%20(AUP)%20is%20a%20document%20stipulating%20constraints,being%20granted%20a%20network%20ID.

Top 16 email security best practices 2024 - A Comprehensive Guide. (2024). Retrieved from https://www.sharefile.com/resource/blog/email-security-best-practices-guide

Center for Internet Security. (2023). *Logging and Monitoring Control: CIS Controls v8*. Retrieved from https://www.cisecurity.org/controls/log-monitoring-and-management/

Cybersecurity & Infrastructure Security Agency. (2021). *Securing Web Applications with SSL/TLS*. Retrieved from https://www.cisa.gov/publication/securing-web-apps-ssl-tls

National Institute of Standards and Technology (NIST). (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5).

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity, and Privacy Protection.

https://www.iso.org/standard/82875.html