Cybersecurity Website Hardening Project: A Comprehensive Overview

Team #3, Course section 01-W01, D2L group #3

Date: 09/01/2024

Project Overview

Background Information

The **Cybersecurity Website Hardening Project** is a rigorous, hands-on initiative aimed at enhancing the cybersecurity posture of a small business website hosted on a **Red Hat Linux server**. This project is being conducted by **Team #3** of course section 01-W01, D2L group #3, under the guidance of **Professor Donald Privitera**, and it spans from **September 1, 2024, to November 15, 2024**. The project's goal is to simulate real-world scenarios by addressing cybersecurity challenges faced by small businesses, which often lack the resources for dedicated IT security teams but are increasingly vulnerable to evolving cyber threats. By leveraging industry best practices, the team will assess, mitigate, and prevent security risks, ensuring the website's resilience to potential cyberattacks.

Small businesses have become prime targets for cybercriminals due to the perception that they are less secure, which makes this project especially relevant in today's digital landscape. As part of this initiative, the project will focus on assessing vulnerabilities, designing mitigation strategies, drafting a robust information security policy, and engaging in an offensive and defensive cybersecurity exercise. The hands-on nature of this project ensures that Team #3 gains practical experience in protecting digital assets while enhancing their cybersecurity knowledge and technical skills.

Objectives:

The primary goal of the Cybersecurity Website Hardening Project is to **evaluate and secure a small business website** from a wide array of cyber threats. The project is broken down into three key phases, each of which is designed to build upon the last, ensuring that all aspects of the website's security are carefully analyzed, addressed, and tested.

- **Phase One** involves conducting a **comprehensive risk assessment** to identify the website's vulnerabilities and threats.
- **Phase Two** focuses on creating and implementing a **detailed information security policy** based on the risk assessment, which will include authentication protocols, encryption practices, and employee access controls. The team will also mitigate any identified vulnerabilities in this phase.

- **Phase Three** is a **Red/Blue Team exercise**, where Team #3 will take on both the roles of attackers (Red Team) and defenders (Blue Team) in a simulated cybersecurity battle. This phase tests the effectiveness of the measures put in place during the earlier phases.

At the end of the project, the team will produce a **comprehensive research report** that outlines the entire process, evaluates the effectiveness of the website hardening efforts, and provides recommendations for further improvements.

Scope of the Project:

This project is designed to tackle a wide range of cybersecurity challenges, from vulnerability identification to the creation of mitigation strategies and security policies. The focus will be on protecting a theoretical small business's **Red Hat Linux-based website infrastructure** by implementing state-of-the-art cybersecurity techniques and measures. The following tasks and deliverables are part of the project scope:

1. **Risk Assessment & Threat Analysis:**
    a. Identify and categorize all critical assets of the website, such as databases, web applications, and servers.
    b. Conduct a thorough assessment of the website's infrastructure to identify vulnerabilities, potential entry points for cyberattacks, and external threats.
    c. Analyze various forms of cyber threats, such as malware, SQL injection, cross-site scripting (XSS), and phishing attacks, and determine their potential impact on the business.
    d. Draft a detailed risk assessment report that outlines the website's vulnerabilities, security gaps, and the threats it faces. This report will form the basis for the subsequent phases of the project.
2. **Development and Implementation of a Security Policy:**
    a. Draft a **comprehensive information security policy** that will be tailored to the small business environment. This policy will cover essential areas such as:
        i. **Authentication and Authorization**: Ensuring that only authorized personnel have access to sensitive areas of the website and associated systems.
        ii. **Encryption Protocols**: Protecting data both in transit and at rest by using industry-standard encryption techniques.
        iii. **Password Management**: Implementing strong password policies that require complex passwords and mandate regular updates.
        iv. **Access Control**: Developing role-based access control (RBAC) to ensure that employees only have access to the information and tools they need for their specific roles.
        v. **Incident Response**: Creating an incident response plan that outlines the steps to be taken in the event of a security breach or attack.

   b. This phase will also involve the **mitigation of risks** identified during the risk assessment phase. This could include patching software vulnerabilities, hardening server configurations, or implementing additional layers of security such as firewalls or intrusion detection systems (IDS).

3. **Red/Blue Team Exercise:**
   a. The final phase of the project is the **Red/Blue Team exercise**, which simulates real-world cyberattacks and defenses.
   b. **Red Team Role**: Team #3 will act as the **offensive team** (Red Team), attempting to exploit vulnerabilities in the opposing team's website infrastructure. The focus will be on penetration testing, where various attack vectors (e.g., phishing attacks, SQL injections, password cracking) will be employed to breach the opposing team's defenses.
   c. **Blue Team Role**: In parallel, Team #3 will also serve as the **defensive team** (Blue Team) for their own website, protecting it from similar attacks initiated by the opposing team. The Blue Team will be responsible for monitoring the website for indicators of compromise (IOCs), patching vulnerabilities in real-time, and implementing countermeasures to prevent attacks.
   d. **Outcome**: The Red/Blue Team exercise will provide valuable insights into the effectiveness of the security measures implemented during the project. The results of this phase will also highlight any weaknesses that need further attention.

Detailed Timeline & Milestones:

To ensure that the project is completed within the set timeframe, the following milestones have been established for each phase:

- **Phase One (Risk Assessment Phase)** – September 1, 2024, to October 1, 2024
  - Conduct a website and server infrastructure analysis.
  - Identify and document potential threats and vulnerabilities.
  - Draft the initial risk assessment report.
  - Present findings to Professor Privitera for feedback.
- **Phase Two (Security Policy & Risk Mitigation)** – October 1, 2024, to October 30, 2024
  - Create a detailed information security policy.
  - Implement risk mitigation strategies.
  - Conduct a final review of the website's security configurations.
  - Prepare for the Red/Blue Team exercise.
- **Phase Three (Red/Blue Team Exercise)** – November 1, 2024, to November 15, 2024
  - Conduct penetration tests (Red Team).
  - Defend against attacks (Blue Team).
  - Monitor website logs for indicators of compromise.

- Complete the final research report, summarizing the project’s successes, challenges, and areas for improvement.

Final Deliverables:

At the conclusion of the project, Team #3 will submit several deliverables, including:

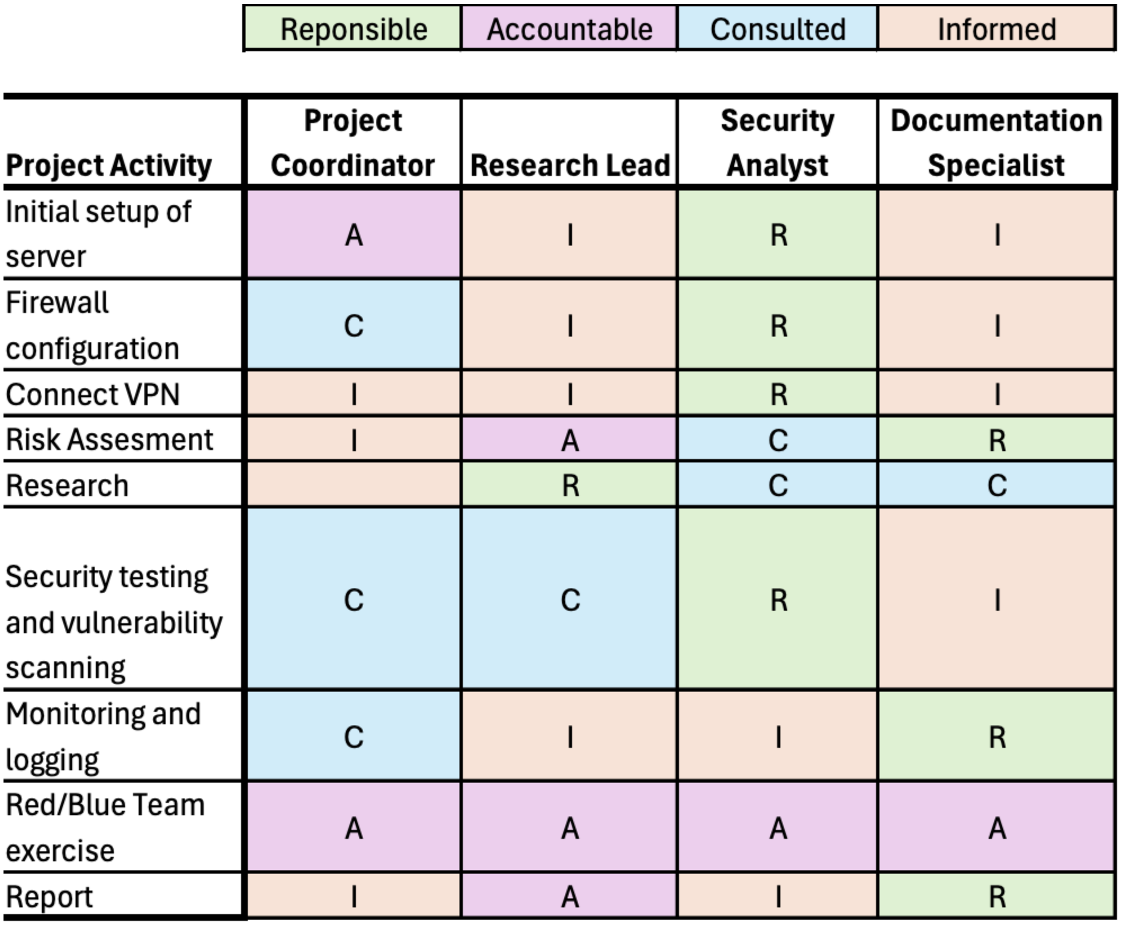
- A **detailed risk assessment report** that highlights vulnerabilities and their potential impacts.
- A **comprehensive information security policy** tailored to the small business's website infrastructure.
- A **final research paper**, which will summarize the Red/Blue Team exercise, analyze the effectiveness of the implemented security measures, and provide recommendations for future improvements. This paper will also include **logs and evidence of potential compromise**, as well as steps taken to resolve security breaches during the Red/Blue Team phase.

Project Participants

Roles	**Name**	**Major responsibilities**	**Contact (Email and/or Phone)**
Project owner sponsor	Professor Privitera	Determine the Projects goals and receive the deliverables throughout the project.	dprivit2@kennesaw.edu
Team leader	Robin Tandongfor	Technical Writing, meeting note taker/recorder, creating and maintaining the team site, cybersecurity research and some web server testing. I also help to facilitate group progress by scheduling and running the team meetings, creating outlines for presentations, being available as much as possible to help clarify any issues or questions regarding the project and its expectations. I also act as liaison between the Project Owner/Professor and the team.	Rtandong@students.kennesaw.edu /470-461-9759

Team members	Kylah Wilson	Research, network defense planning, security policy drafting & implementation.	Kwils261@students.kennesaw.edu /678-386-3466
	Elijah Vandorn	Research risk assessment on import assets, list common threats, analysis on threats that could happen	evandorn@students.kennesawedu /678-852-9309
	Jack Pursley	Server infrastructure management, research security. hardening tactics, penetration testing within the server.	jpursle8@students.kennesaw.edu /404-376-8154
	Valentine Wairimu	Help to research and implement the in accordance with the various tasks that need to be done to successfully complete this project.	vwairim1@students.kennesaw.edu
Advisor / Instructor	Donald Privitera	Facilitate project progress; advise on project planning and management.	dprivit2@kennesaw.edu

RACI Chart



Reponsible	Accountable	Consulted	Informed

Project Activity	Project Coordinator	Research Lead	Security Analyst	Documentation Specialist
Initial setup of server	A	I	R	I
Firewall configuration	C	I	R	I
Connect VPN	I	I	R	I
Risk Assesment	I	A	C	R
Research		R	C	C
Security testing and vulnerability scanning	C	C	R	I
Monitoring and logging	C	I	I	R
Red/Blue Team exercise	A	A	A	A
Report	I	A	I	R

Final Deliverables

<u>Risk Assessment Phase (Milestone 1):</u>

- A detailed assessment of the server infrastructure, highlighting its strengths and vulnerabilities.
- Identification and documentation of the critical digital assets that require protection.
- Analysis of potential threats and vulnerabilities for each asset. This will include the probability of major attacks and the potential damage if these attacks were to occur.
- Recommendations for mitigating identified risks, including a prioritization strategy based on the severity of each risk.

<u>Information Security Policy and Risk Mitigation Phase (Milestone 2):</u>

- A well-researched information security policy tailored to the needs of the small business, covering areas such as internet access, email usage, authentication, encryption, password management, and BYOD (Bring Your Own Device) policies. (Including but not limited to)

- An access management policy that defines roles and permissions for employees, ensuring that access is restricted based on necessity.
- A risk mitigation plan that addresses all identified risks from the risk assessment phase, with a clear timeline and strategy for implementing security measures.

Red/Blue Team Exercise (Milestone 3):

- A comprehensive log of the Red Team activities, including detailed documentation of penetration attempts, vulnerabilities exploited, and any data exfiltration.
- A log of Team 3's defensive actions, including monitoring activities, detection and response to penetration attempts, and efforts to maintain server integrity.

Conclusion: Research Report

- A final analysis of the Red/Blue Team exercise, summarizing the effectiveness of both the offensive and defensive strategies, along with lessons learned.
- Screenshots and documentation of any indicators of compromise and downtime events.

Milestones

- Milestone #1 completed by 9/20/2024
- Milestone #2 completed by 10/18/2024
- Milestone #3 completed by 11/15/2024

Deliverable Expectations

Risk Assessment:

The risk assessment should provide a detailed evaluation of the server infrastructure. It should clearly identify digital assets and categorize them based on their importance. The analysis of threats and vulnerabilities must be well-researched and documented using resources such as KSU Library and The KSU Writing Center.

Information Security Policy and Risk Mitigation Plan

The policies must be based on the best practices in information security, and only include research from the past three years. The security policies should cover critical areas, including internet usage, email security, authentication processes, encryption standards, password management, and BYOD policies. The risk mitigation plan should identify each risk from the assessment and include specific steps and timelines for implementing security measures.

Red/Blue Team Exercise/Report:

The report should include detailed logs of all activities conducted during the Red/Blue Team exercise. This includes descriptions of penetration attempts, defensive actions, and any indicators of compromise detected. The final report should assess the effectiveness of both offensive and defensive strategies, providing insights into what worked well and what could be improved.

Future meetings date/time

- Weekly Team 3 meetings will be held once a week on Tuesday, Wednesday, and Thursday at 1pm. The team members expected to attend meetings are Robin Tandongfor, Jack Pursley, Kylah Wilson, Elijah Vandorn, and Valentine Wairimu. Robin Tandongfor is expected to record weekly meetings, take notes, and distribute meeting notes.
- Future general weekly meetings with Professor Privitera will be held on Microsoft Teams every Thursday at 8pm.

Collaboration Plan

- We will be using Microsoft Teams as our main communication channel. Therefore, we will use Teams to distribute files concerning the project among each other, updating each other on our individual progress, ask questions, and hold meetings.
- Team members will be expected to respond in Teams within three hours and will be expected to commit to 12 hours per week of work time individually. In an event where a team member is not actively participating in the group, emails and messages will be used to communicate and if this fails, the last resort will be involving the professor for the next cause of action.
-

Communication Plan & Policy

The communication methods used by team members are Microsoft Teams, KSU emails (Outlook and D2l), and phone. Group members are expected to stay in communication with each other throughout the week. We will have weekly meetings through Microsoft Teams. If any members cannot attend a meeting, they are expected to tell the rest of the team through any method of communication in advance. In addition, to catch up, they are expected to watch meeting recordings and read meeting notes.

Project Schedule, WBS, and Tasks Plan

See the .MPP file and Gantt chart - file attached.

Project Change Management

If the scope of the project changes, the team leader will contact the client with updates and changes to the timeline of the project per the client's approval.

If the project owner ever changes the requirements of the project later, a new team meeting will be held ASAP to determine how the changes will affect our workload.

If it is determined the scope of the project is made too great for the team, our contact with the owner will mention needing to shrink the scope back. This will only happen if we are confident that the changes cannot be satisfied within the remaining time.

Quality Assurance Plan

To ensure Quality Assurance (QA) in the project, Team #3 wil follow these steps:

1. **Define Quality Standards Early**
   Set clear benchmarks like 100% uptime, 90% accuracy in vulnerability detection, and compliance with frameworks (NIST, OWASP). Assign QA roles to team members for continuous oversight.
2. **Detailed Project Plan with QA**
   Break the project into milestones with clear deliverables. Incorporate QA checkpoints at each stage to review and ensure progress meets set standards.
3. **Peer Reviews and Audits**
   Have team members review each other's work for thoroughness. Perform audits to ensure alignment with established security standards and assess risk findings.
4. **Document Every Process**
   Track all actions, updates, and changes with consistent documentation to ensure accuracy and up-to-date information.
5. **Automated Testing and Tools**
   Use tools like Nmap, Nessus, and Snort for automated security checks. Continuous monitoring will alert the team to any suspicious activities.
6. **Feedback Loop**
   Regular team meetings and feedback from Professor Privitera will address issues early and keep the project on track.
7. **Testing and Validation**
   Perform penetration testing at key points to confirm vulnerabilities are mitigated. Validate security policies by testing them against real-world scenarios.
8. **Milestone-Specific QA Checks**
   At each milestone, review completeness and ensure all identified risks are addressed. Validate results during the Red/Blue Team exercise.
9. **Risk Management and Contingency Plans**
   Proactively update the risk register and test backup solutions like VM recovery to handle potential failures.
10. **Final QA Review**
    Before submission, review all documentation and deliverables to confirm that all quality standards have been met. Perform a final review of the project report to ensure accuracy and completeness.

Risk Management Plan

- If a team member misses a deliverable and is not responding within 2-3 hours, we will send them an email. If there is still no response we will contact the professor.
- If the team leader cannot attend a meeting, an alternative will be announced in advance before the meeting is held. If any team member is not able to attend the meeting, the meeting will be scheduled to a later date and time per the team's convivence and schedules.

- If Microsoft Teams goes down, team members will move to the second line of communication by phone text or email. If D2L goes down, the team leader will contact to prepare for any changes to the project.
- If a team member drops the course the team leader will update the professor/client and proceed with the project per the other team members and professors' approval.

Signed by:

Jack Pursley, Robin Tandongfor, Kylah Wilson, Elijah Vandorn, Valentine Wairimu