Cyber Security Internship

Dear Intern,

Congratulations on joining our team as a Cyber Security Intern at **The Red Users**! We are thrilled to have you on board and eager to see your contributions to our projects.

Below are your assigned tasks along with guidelines and terms for successful completion:

Task Assignment & Guidelines

Cyber Security Intern

Task 1: Introduction to Network Security Basics

Objective:

Understand the basics of network security by learning about different types of network threats and how to implement basic security measures. This task will introduce you to the foundational concepts of securing a small network.

Skills:

Basic Network Security, Threat Identification, Security Best Practices

Tools:

Firewall (Windows Defender Firewall or a basic hardware firewall), Wireshark

Guidelines:

1. **Learn Network Security Concepts:**
    - Research and summarize different types of network threats, including viruses, worms, trojans, and phishing attacks.
    - Understand basic security concepts like firewalls, encryption, and secure network configurations.
2. **Implement Basic Security Measures:**
    - Set up a simple network environment, such as your home network or a virtual lab with a router and one or two connected devices.

- Enable and configure a basic firewall (e.g., Windows Defender Firewall) to block unauthorized access.
- Set up basic security configurations, such as changing default passwords and enabling network encryption (WPA2 or WPA3).

3. **Monitor Network Traffic:**
   - Use Wireshark to capture and analyze network traffic.
   - Identify different types of traffic, such as HTTP, DNS, and others, and understand what they mean.
   - Learn how to spot unusual or suspicious traffic that might indicate a security threat.
4. **Document Findings:**
   - Create a simple report that includes:
     - A summary of the network threats you researched.
     - The security measures you implemented and why.
     - Screenshots or descriptions of the traffic you captured with Wireshark.
     - A discussion on how these basic security measures help protect the network.
5. **Reflect on Security Best Practices:**
   - Consider what additional security measures could be implemented in a larger, more complex network.
   - Write a short paragraph on how you would educate others about the importance of network security in everyday use.

Task 2: Introduction to Web Application Security

Objective:

Learn about common web application vulnerabilities by analyzing a simple web application. This task will help you understand how attackers can exploit weaknesses in web applications.

Skills:

Basic Web Security, Vulnerability Identification

Tools:

OWASP ZAP, WebGoat (or another vulnerable web application)

Guidelines:

1. **Setup:**
    - Install and set up WebGoat or another intentionally vulnerable web application on your local machine.
    - Ensure you understand how the application works and how to access it.
2. **Perform Basic Vulnerability Analysis:**
    - Use OWASP ZAP to scan the web application for vulnerabilities.
    - Focus on identifying at least one instance each of SQL Injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF).
3. **Explore Vulnerabilities:**
    - Understand how each vulnerability works by reading the descriptions provided by OWASP ZAP.
    - Attempt to manually exploit these vulnerabilities using basic techniques (e.g., inserting SQL code in a login form).
4. **Report:**
    - Document each vulnerability found, including how you discovered it and why it is dangerous.
    - Provide screenshots and a brief explanation of the exploitation process.
    - Suggest simple steps that could mitigate these vulnerabilities.

Task 3: LinkedIn Profile Engagement

Enhance your professional presence on LinkedIn by engaging with content related to cybersecurity. Follow **The Red Users** LinkedIn page, share the company's posts, and create your own posts mentioning the company.

Link: - https://www.linkedin.com/company/the-red-users/

Skills: Profile Optimization, Networking, Content Creation

Guidelines:

1. Follow The Red Users on LinkedIn.
2. Share a post about the internship with a personalized message.
3. Mention The Red Users in a post discussing the importance of cybersecurity.
4. Provide screenshots as proof of your engagement.

Guidelines:

1. Timeline: Complete all tasks within the internship period.
2. Communication: Regular check-ins will be held to review progress and address any challenges.
3. Documentation: Maintain detailed documentation of your work, including reports and project updates.
4. Quality Assurance: Ensure all deliverables meet quality standards and undergo testing before submission.
5. Completion: All tasks must be completed to endorse the completion of the internship.

Terms:

Confidentiality: All project details and company information are confidential and should not be shared outside the organization.
Ownership: Any intellectual property developed during the internship belongs to **The Red Users**.
Performance Evaluation: Your performance will be evaluated based on project outcomes, teamwork, and adherence to deadlines.

Best Regards,
The Red Users Team