VIRTUAL VIGILANTES

"CODING FUTURES & CRAFTING CAREERS"

Elevate Your Career with us

www.virtualvigilantes.com

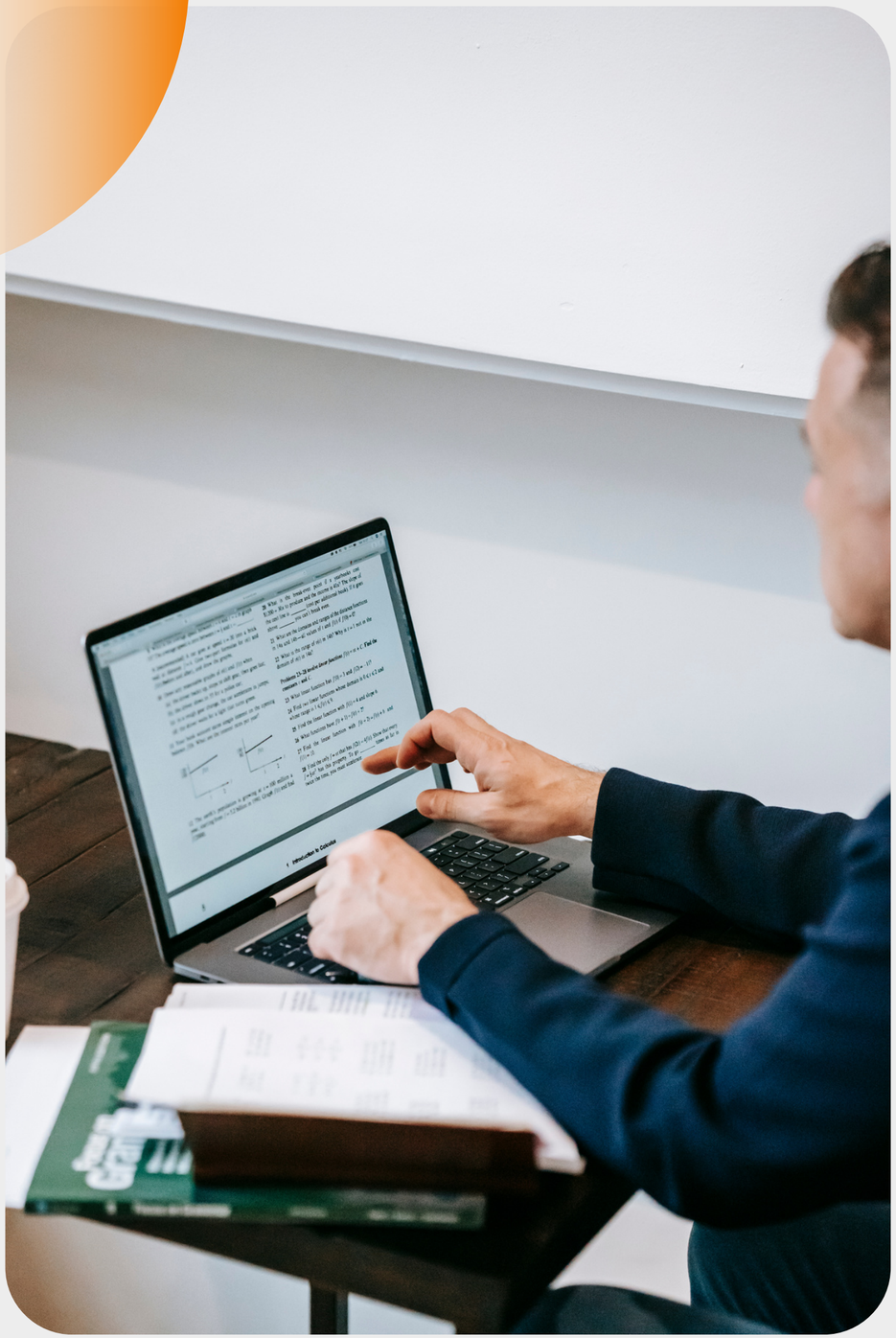
contact@virtualvigilantes.com

VIRTUAL VIGILANTES

"CODING FUTURES & CRAFTING CAREERS"

About Us

At Virtual Vigilantes, we're on a mission to impact the lives of 1 million students. Our commitment is to provide the best virtual internships, enabling students to enhance their skills and impress future employers. Join us in shaping a brighter professional future for aspiring talents worldwide!



VIRTUAL VIGILANTES
"CODING FUTURES & CRAFTING CAREERS"

Cyber Security Internship Tasks

VIRTUAL VIGILANTES
"CODING FUTURES & CRAFTING CAREERS"

Task 1 -
Web Application Vulnerability Assessment

Conduct a vulnerability assessment on a web application to identify potential security weaknesses. Use tools like OWASP ZAP or Burp Suite to scan for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and security misconfigurations. Generate a comprehensive report with recommendations for mitigation.

This task allows students to gain practical skills in web application security testing, a critical aspect of cybersecurity.

VIRTUAL VIGILANTES
"CODING FUTURES & CRAFTING CAREERS"

Task II -
Password Strength Checker

Create a simple password strength checker script in Python. The script should take a user-input password and evaluate its strength based on criteria such as length, presence of uppercase and lowercase letters, numbers, and special characters. Provide feedback to the user about the password strength.

This task is designed to be a beginner-friendly introduction to basic programming concepts and encourages students to think about cybersecurity aspects like password strength.

VIRTUAL VIGILANTES
"CODING FUTURES & CRAFTING CAREERS"

Task II - Reference
Password Strength Checker

1. **Basic Python Programming:**
   - Use basic Python programming concepts to take user input, perform string manipulations, and implement conditional statements.
2. **Password Strength Criteria:**
   - Define simple criteria for password strength, such as minimum length, inclusion of uppercase and lowercase letters, numbers, and special characters.
3. **User Feedback:**
   - Provide clear and user-friendly feedback to the user about the strength of their password.

VIRTUAL VIGILANTES
"CODING FUTURES & CRAFTING CAREERS"

Task III -
Basic File Encryption/Decryption

Perform customer segmentation using clustering techniques on a dataset containing customer information. Use algorithms such as K-means clustering to group customers based on common characteristics like purchase history, demographics, or behavior. Analyze and interpret the clusters to derive actionable insights.

This task introduces students to the concept of file encryption and the importance of key-based security.

VIRTUAL VIGILANTES
"CODING FUTURES & CRAFTING CAREERS"

Task III - Reference
Basic File Encryption/Decryption

1. File Handling in Python:
   - Learn how to read from and write to files in Python.
2. Encryption Algorithm:
   - Choose a simple encryption algorithm, such as a substitution cipher, to transform the contents of the file.
3. Key-Based Encryption:
   - Use a key-based approach where the user needs a key to both encrypt and decrypt the file.

VIRTUAL VIGILANTES
"CODING FUTURES & CRAFTING CAREERS"

Task IV - Basic Security Audit and Report

Conduct a basic security audit on your computer system to identify potential vulnerabilities. Explore settings, configurations, and habits that impact cybersecurity. Prepare a detailed report outlining the findings, potential risks, and recommended actions for enhancing security.

Note: This task encourages students to critically assess their own cybersecurity practices, providing them with a practical understanding of security principles.

Task IV - Reference Basic Security Audit and Report

VIRTUAL VIGILANTES
"CODING FUTURES & CRAFTING CAREERS"

1. System Settings Review:
   - Review operating system settings (Windows, macOS, or Linux) for security-related configurations.
   - Examine settings related to user accounts, automatic updates, and firewall configurations.
2. Antivirus and Malware Scan:
   - Run a malware scan using the installed antivirus software (e.g., Windows Defender).
   - Check for the presence of any malicious software.
3. Browser Security Settings:
   - Evaluate and document the security settings of your web browser.
   - Review privacy settings, cookie policies, and other security-related configurations.
4. Password Management:
   - Check if a password manager is installed and properly configured.
   - Evaluate the strength and uniqueness of stored passwords.
5. Network Security:
   - Examine Wi-Fi network settings, including encryption protocols and password strength.
   - Verify that the home network is secured against unauthorized access.

Task IV - Reference
Basic Security Audit and Report

VIRTUAL VIGILANTES
"CODING FUTURES & CRAFTING CAREERS"

Submission Requirement:

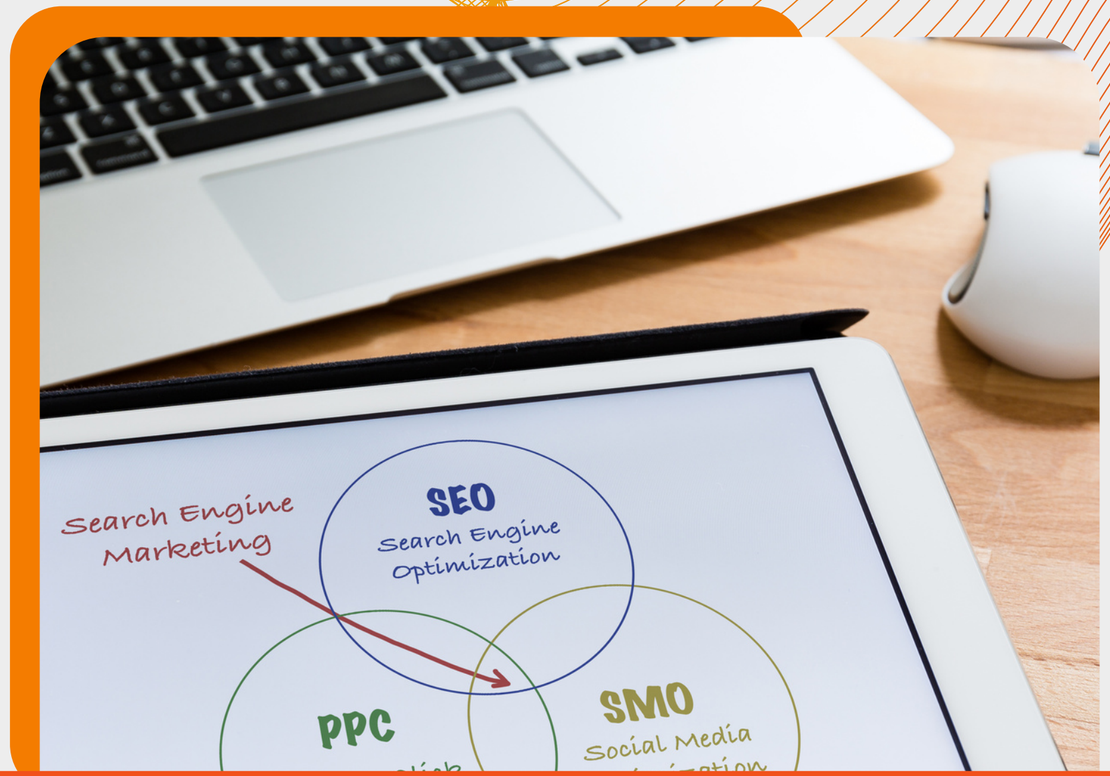
1. Prepare a comprehensive report that includes:
2. An overview of the current security settings and configurations.
3. Identified vulnerabilities or areas of concern.
4. Potential risks associated with the findings.
5. Recommendations for improving security, including step-by-step instructions if applicable.

VIRTUAL VIGILANTES

"CODING FUTURES & CRAFTING CAREERS"

Contact Us

Our Goal is to Empower 1 Million Students with Premier Virtual Internships



www.virtualvigilantes.com

contact@virtualvigilantes.com