Cyber Security Tools and Technologies

Spring 2024 Semester Project Due Date: May 7, 2024

Dear Students:

You are required to work on semester project task as assigned to your group. You can find your group number in the excel file.

Task 1: Research work

Considering the topic of research assigned to your group, group convenor will submit one final report with the following details:

1. Title of the work
2. A brief abstract (100-200 words): This should be a briefly representation of your paper, you should also summarise the findings.
3. Introduction section (500-1000 words): Here you introduce the reader to the selected topic, provide brief details of the importance of your research, present the aim/objectives of your paper and describe profiles of forthcoming sections.
4. Main Body: Here you develop your argument
   - 4.1 Planning and conducting the research (i.e., list of papers investigated by each group member)
   - 4.2 Results and discussion
5. Conclusion: Here you will critically discuss your findings
6. References: You should aim for approx. 10 x group size references. All references should meet IEEE style.

Note: Your report may span from 5 to 15 pages.

Topics Covered:

1. Software security
2. Malware and Attack Technologies
3. Web and Mobile Security
4. Network / Cloud security

Topics 1 to 3 have already been discussed in detail during class.

For topic 4, the concerned groups are required to consider the following scenario while searching for research material.

Topic 4 Description: Suppose that you have applied for a job as a cloud security engineer. You have just passed the first stage of the interview. The second stage will test your research skills within the field of cloud / network security. Your employer is offering could services to Small Medium Enterprises (SMEs). There are a lot of reasons why customers are benefiting from migrating to the cloud. Your task is to investigate the current cloud infrastructure network attacks and mitigation techniques. You also need to discuss legal and ethical issues related to data privacy and security, as SMEs typically will have databases hosting sensitive data.

Common notes for all research topics:

Note 1: It is not expected that your work/paper will be at the same level of depth as the papers published in research journals. However, your investigation should not be a general overview. Your written discussion should include critical evaluation and recommendations or conclusions from your findings.

Note 2: You are required to follow the IEEE formatting style for conference proceedings:
Manuscript templates for conference proceedings can be found here:
https://www.ieee.org/conferences_events/conferences/publishing/templates.html

Note 3: Your paper must be written in your own words and must include a reference section indicating all your sources of information. Remember your sources of information should be authoritative (not Wikipedia, for example). You should also consider the use of illustrations to exemplify your discussion. You must be very careful not to plagiarise material. Plagiarism can result in a mark of 0 for the project, or even failure of the entire course. **Please do NOT copy any other student's work (or lend other students your work) or copy directly sentences and paragraphs from the Internet unless attributing the section correctly to the author in quotation marks.**

Note 4: Please also note that the content written in the report must be original in relation to your other modules, i.e. you must not copy and reuse content directly from your other modules as this will breach the rules on academic dishonesty.

Task 2: Network Security Implementation and Analysis using Packet Tracer

Description: The aim of this project is to design, implement, and analyze various cybersecurity measures within a simulated network environment using Cisco Packet Tracer. The project will cover several aspects of network security, including access control, encryption, intrusion detection, and prevention systems, as well as network monitoring and incident response.

Project objectives:

1. Design a network topology using Packet Tracer, representing a small to medium-sized enterprise network with multiple interconnected devices such as routers, switches, servers, and end-user devices.
2. Implement access control mechanisms, including firewall rules, VLAN segmentation, and access lists, to control traffic flow and restrict unauthorized access to network resources.
3. Deploy encryption protocols such as SSL/TLS or IPsec to secure data in transit between network devices and ensure confidentiality and integrity.
4. Configure and deploy intrusion detection and prevention systems (IDPS) within the network to detect and prevent malicious activities and attacks.
5. Implement network monitoring tools to monitor network traffic, identify anomalies, and generate alerts for potential security incidents.
6. Develop incident response procedures and policies to effectively respond to security breaches or incidents detected within the network.
7. Perform a comprehensive analysis of the implemented security measures, including assessing their effectiveness in protecting against common cybersecurity threats and vulnerabilities.
8. Document the entire project, including network diagrams, configurations, security policies, and analysis findings, in a detailed report.

Deliverables:

1. Network topology diagram illustrating the designed network layout.
2. Configuration files and scripts used to implement security measures within the network.
3. Documentation outlining the security policies, procedures, and configurations.
4. Analysis report summarizing the effectiveness of implemented security measures, identifying strengths, weaknesses, and recommendations for improvement.

Task 3: Web Application Security Assessment: Finding Vulnerabilities in Websites

Description: This project focuses on conducting a comprehensive security assessment of web applications to identify and exploit vulnerabilities. You will act as offensive ethical hackers, selecting random websites (at least five websites) as targets for assessment. The project will involve various stages, including reconnaissance, vulnerability scanning, exploitation, and reporting, to uncover potential security weaknesses and provide recommendations for remediation.

Objectives:

1. Select and document the target websites for the security assessment, ensuring they represent a diverse range of web applications, such as e-commerce sites, content management systems, or social media platforms.
2. Perform reconnaissance activities to gather information about the target websites, including identifying the technologies used, mapping the site structure, and identifying potential entry points for attacks.
3. Conduct automated vulnerability scans using tools like OWASP ZAP, Nikto, or Burp Suite to identify common security vulnerabilities such as SQL injection, cross-site scripting (XSS), and directory traversal.
4. Manually analyze the identified vulnerabilities to verify their existence and determine their exploitability. This may involve techniques such as manual SQL injection, XSS payload crafting, or parameter manipulation.
5. Exploit the discovered vulnerabilities to demonstrate their impact on the target websites, such as accessing sensitive data, defacing web pages, or executing arbitrary code.
6. Document the findings of the security assessment, including detailed descriptions of identified vulnerabilities, proof-of-concept exploit code, and potential impact assessments.
7. Provide recommendations for mitigating the identified vulnerabilities, including patching vulnerable software, implementing secure coding practices, and enhancing security controls.
8. Prepare a final report summarizing the results of the security assessment, including an executive summary, detailed findings, recommendations, and a conclusion.

Deliverables:

1. Target website selection and documentation, including rationale for selection.
2. Reconnaissance report detailing the findings from information gathering activities.
3. Vulnerability assessment report containing the results of automated and manual vulnerability scans.
4. Exploitation report documenting successful exploitation of identified vulnerabilities and their impact.
5. Remediation recommendations outlining steps to mitigate identified vulnerabilities and improve overall security posture.
6. Final comprehensive report summarizing the entire assessment process, findings, recommendations, and conclusions.

Task 4: Common Vulnerability Scoring System (CVSS v4.0) Calculator Development

Description: This semester project involves the development of a web-based tool for calculating Common Vulnerability Scoring System (CVSS) scores according to version 4.0 of the standard. The project will require students to understand the CVSS v4.0 metrics, develop algorithms for calculating scores, and create an intuitive user interface for the calculator tool.

Objectives:

1. Research and understand the CVSS v4.0 standard, including the base, temporal, and environmental metrics used for calculating vulnerability scores.
2. Design the architecture and data model for the CVSS calculator application, identifying the necessary inputs and outputs for calculating scores.
3. Develop algorithms and formulas for computing CVSS scores based on the provided metrics, ensuring accuracy and consistency with the CVSS v4.0 specification.
4. Implement a user-friendly web-based interface for the CVSS calculator tool, allowing users to input vulnerability details and receive calculated scores.
5. Validate the functionality of the calculator tool by testing it with a variety of real-world vulnerability scenarios and comparing the calculated scores with manual calculations.
6. Enhance the calculator tool with additional features such as score aggregation for multiple vulnerabilities, score visualization, and exporting results in various formats.
7. Document the development process, including design decisions, implementation details, and testing procedures, in a comprehensive project report.
8. Present the CVSS calculator tool to the class, demonstrating its features, usability, and accuracy in calculating vulnerability scores.

Deliverables:

1. Design documentation outlining the architecture, data model, and user interface mockups for the CVSS calculator application.
2. Algorithm documentation describing the formulas and calculations used to compute CVSS scores based on the provided metrics.
3. Web-based CVSS calculator tool with an intuitive user interface, developed using appropriate technologies such as HTML, CSS, JavaScript, and possibly backend frameworks like Django or Flask.
4. Testing documentation detailing the validation process and results of testing the calculator tool with various vulnerability scenarios.
5. User manual or guide explaining how to use the CVSS calculator tool effectively and interpret the calculated scores.
6. Final project report summarizing the entire development process, challenges faced, lessons learned, and future enhancements.

Task 5: Ethical Malware Simulation and Analysis

Description: This project focuses on simulating the creation and analysis of malware within a controlled and ethical environment. Students will explore various tools and techniques commonly used by malware researchers and analysts to understand the anatomy of malware, its behavior, and methods of defense.

Objectives:

1. Research different types of malware, including viruses, worms, trojans, ransomware, and spyware, to understand their characteristics, propagation methods, and impact on systems.
2. Explore ethical considerations and legal implications associated with creating and handling malware, emphasizing adherence to ethical guidelines and respect for applicable laws.
3. Select a malware creation tool or framework that allows for the safe generation of malware samples for educational purposes. Examples include Metasploit, Veil, or Malicious Macro Generators.
4. Use the chosen tool to create simulated malware samples, ensuring that they do not pose any real-world threat and are designed solely for educational and research purposes.
5. Document the creation process, including the techniques and features employed to simulate different types of malware, such as code obfuscation, payload delivery methods, and evasion techniques.
6. Set up a malware analysis lab environment using virtual machines or sandboxing tools to safely execute and analyze the created malware samples.
7. Perform static and dynamic analysis of the simulated malware samples to understand their behavior, functionalities, and potential impact on systems.
8. Analyze the results of the malware analysis, identifying indicators of compromise (IOCs), behavioral patterns, and mitigation strategies.
9. Develop a comprehensive report documenting the entire process, from malware creation to analysis, including findings, insights, and ethical considerations.
10. Present the findings of the malware simulation and analysis project, discussing the challenges, lessons learned, and ethical implications of engaging in such activities.

Deliverables:

1. Malware creation documentation, detailing the tools, techniques, and methodologies used to simulate different types of malware samples.
2. Malware analysis report summarizing the findings of static and dynamic analysis, including IOCs, behavioral patterns, and mitigation strategies.
3. Presenting slides highlighting key insights, ethical considerations, and lessons learned from the malware simulation and analysis project.