In21-S4-CS3460

Mini Project Topics

Prepared By:

Kasun Chathuranga

Principal Security Engineer – TechCERT

Guidelines for Topic Selection and Project Submission

- **Topic Selection:** There are 9 topics available for the mini projects. Although multiple students may select the same topic, each topic has a limit of five students.
- **Report Format:** Submit reports in PDF format.
- **Incorporating Language Learning Models:** While students are allowed to utilize Language Learning Models like ChatGPT or Gemini for assistance with report writing, it is crucial to note that completion of the assignment will not be possible solely through these means. The reports must include screenshots, empirical results, and other direct evidence of practical engagement with the project topic.
- **Multiple Projects:** Students who are *keen to challenge themselves* are encouraged to undertake more than one topic. It is recommended that submissions for additional projects be sent directly via email to kasun@techcert.lk. These submissions will be for feedback purposes only and will not be included in the formal marking.
- **Blogging and Career Development:** Students are also encouraged to start a blog related to information security. Documenting the process and findings of your mini projects can serve as a valuable resource for others and enhance your online professional presence. Sharing your work publicly can significantly benefit your future career, showcasing your practical skills and knowledge to potential employers or collaborators.

Target Practicing Guidelines

- Do not target any public/enterprise network unless explicit authorization is given.
- Set up a Controlled Environment using a Virtualization Platform such as VMware, VirtualBox, or KVM.
- Utilize intentionally vulnerable software applications, for example:
  - Metasploitable
  - OWASP WebGoat
  - OWASP Juice Shop
- Understand the tool's purpose and functionality before use.
- Analyze and interpret results accurately to derive meaningful insights.
- Always adhere to ethical and responsible use guidelines during practice

1. Reconnaissance and IP Discovery using Nmap

The aim of this assignment is to highlight the significance of reconnaissance in security assessments and showcase the practical application of Nmap, a widely used security assessment tool. Your task is to carry out reconnaissance activities using Nmap, such as open port detection, script utilization, and fine-tuning of options, in order to gather information from multiple IP addresses. Subsequently, you are required to compile a detailed report spanning 3–4 pages, complete with relevant screenshots. The report should encompass the following sections:

a) **Introduction:** Provide an overview of reconnaissance & Nmap.

b) **Preparation:** Describe the necessary preparations undertaken prior to conducting the reconnaissance activities with Nmap.

c) **Activities Performed:** Present actual command and options used for open port detection, script utilization, and options fine-tuning.

d) **Results and Observations:** Document the findings obtained from the reconnaissance activities, highlighting any noteworthy discoveries or observations. Include relevant screenshots to support your analysis.

e) **Interpretation of the Findings:** Analyze and interpret the results obtained, offering insights into the implications of the identified details and their potential impact on security.

f) **Summary and Conclusion:** Summarize the key findings and conclusions drawn from the reconnaissance activities using Nmap, emphasizing the importance of reconnaissance in security assessments and its role in mitigating potential vulnerabilities.

Note: Make sure to adhere to target practicing guidelines.

Please contact kasun@techcert.lk if you need any clarifications.

2. Vulnerability Scan with Nessus Essential

The objective of this assignment is to demonstrate the process of conducting a sample vulnerability scan using Nessus Essential, a popular vulnerability assessment tool. Your task is to perform a vulnerability scan using Nessus Essential, identify potential vulnerabilities within a given system, and generate a comprehensive 3–4-page report with accompanying screenshots. The report should include the following sections:

a) **Introduction:** Provide an overview of vulnerability scanning and the role of Nessus in identifying potential security weaknesses.
b) **Preparation:** Describe the necessary preparations undertaken before initiating the vulnerability scan with Nessus Essential. This may include installing and configuring Nessus Essential, setting up scan policies, and ensuring connectivity to the target system.
c) **Activities Performed:** Explain the process of configuring and running the vulnerability scan using Nessus Essential. Describe the scan policies selected, target systems scanned, and any specific requirements or considerations during the scan. Discuss any notable actions taken during the scan, such as pausing or resuming the scan, adjusting scan settings, or excluding specific hosts.
d) **Results and Observations:** Present the findings obtained from the vulnerability scan using Nessus Essential. This section should include a detailed report of identified vulnerabilities, their severity levels, and accompanying descriptions. Include relevant screenshots or excerpts from the Nessus Essential interface displaying the scan results.
e) **Interpretation of the Findings:** Analyze and interpret the scan results, discussing the potential impact and implications of the identified vulnerabilities on the security of the target system. Identify any common trends or patterns in the vulnerabilities discovered and provide insights into their potential exploitation.
f) **Summary and Conclusion:** Summarize the key findings and conclusions drawn from the vulnerability scan conducted using Nessus Essential. Emphasize the importance of vulnerability assessments and the role of Nessus Essential in identifying and mitigating potential security weaknesses.

Notes: Make sure to adhere to target practicing guidelines. It is better to use readily available intentionally built vulnerable systems such as metasploitable VM as the target.

Please contact kasun@techcert.lk if you need any clarifications.

3. Intercepting HTTP Requests with a Proxy (ZAP/Burp)

The objective of this assignment is to demonstrate the utilization of an intercepting proxy tool, such as ZAP (Zed Attack Proxy) or Burp Suite, for HTTP request analysis. Your task is to employ an intercepting proxy tool to capture and analyze HTTP requests, gain insights into request parameters, headers, cookies, and other relevant information, and generate a comprehensive report (spanning 3–4 pages) documenting your findings. The report should consist of the following sections:

a) **Introduction:** Provide an overview of the significance of intercepting proxy tools in HTTP request analysis and their role in identifying potential security vulnerabilities.

b) **Preparation:** Describe the necessary preparations undertaken before initiating the HTTP request analysis using the intercepting proxy tool. This may include configuring the proxy tool, setting up the testing environment, and ensuring proper connectivity to the target application.

c) **Activities Performed:** Explain the process of capturing and analyzing HTTP requests using the intercepting proxy tool (e.g., ZAP or Burp Suite). Detail the steps taken to intercept requests, examine request parameters, headers, cookies, and other relevant information. Discuss any specific actions performed during the analysis, such as modifying requests, injecting payloads, or manipulating parameters.

d) **Results and Observations:** Present the findings obtained from the HTTP request analysis using the intercepting proxy tool. This section should include relevant screenshots showcasing intercepted requests, highlighted parameters, modified payloads, and any noteworthy observations or findings.

e) **Interpretation of the Findings:** Analyze and interpret the information gathered from the HTTP request analysis. Discuss potential security vulnerabilities or misconfigurations identified, such as cross-site scripting (XSS), SQL injection, insecure direct object references, or insecure communication. Explain the implications of these findings and their potential impact on the security of the application.

f) **Summary and Conclusion:** Summarize the key findings and conclusions drawn from the HTTP request analysis performed using the intercepting proxy tool. Emphasize the importance of intercepting proxies in understanding the structure and security of HTTP requests and their role in identifying and mitigating potential vulnerabilities.

Notes: Make sure to adhere to target practicing guidelines. It is better to use readily available intentionally built vulnerable web app as the target.

Please contact kasun@techcert.lk if you need any clarifications.

4. Packet Sniffing with Wireshark

The objective of this assignment is to demonstrate the process of sniffing packets using Wireshark and identifying sensitive data within network traffic. Your task is to utilize Wireshark, a popular packet sniffing tool, to capture and analyze network packets, identify potential instances of sensitive data transmission, and generate a comprehensive report (spanning 3–4 pages) consisting of the following sections:

a) **Introduction:** Provide an overview of the importance of packet sniffing and the significance of identifying sensitive data within network traffic.

b) **Preparation:** Describe the necessary preparations undertaken before initiating the packet sniffing activities with Wireshark. This may include installing Wireshark, setting up the capture environment, configuring network interfaces, and ensuring proper connectivity.

c) **Activities Performed:** Explain the process of capturing network packets using Wireshark, including the selection of appropriate network interfaces and filters. Describe any specific actions taken during the packet capture process and highlight the focus on capturing sensitive data.

d) **Results and Observations:** Present the findings obtained from the packet sniffing activities using Wireshark. This section should include screenshots of captured packets, highlighting instances of potential sensitive data, such as login credentials, personally identifiable information (PII), or confidential information.

e) **Interpretation of the Findings:** Analyze and interpret the identified instances of sensitive data within the captured packets. Discuss the potential risks associated with the exposure of this data and its potential impact on the security of the network and its users.

f) **Summary and Conclusion:** Summarize the key findings and conclusions drawn from the packet sniffing activities conducted with Wireshark. Emphasize the importance of packet sniffing in identifying potential security vulnerabilities and the need for implementing appropriate measures to protect sensitive data.

Notes: Make sure to adhere to target practicing guidelines. It is better to use readily available intentionally built vulnerable web app as the target which does not have SSL/TLS.

Please contact kasun@techcert.lk if you need any clarifications.

5. Analysis of Disk Image of USB drive with using FTK Imager and Finding Deleted Files

The objective of this assignment is to demonstrate the process of creating a sample disk image of a USB drive using FTK Imager, a forensic imaging tool, and finding deleted files within the disk image. Your task is to utilize FTK Imager to create a forensic disk image of the USB drive, analyze the image to identify any deleted files, and generate a comprehensive report documenting (spanning 3–4 pages) your findings. The report should consist of the following sections:

a) **Introduction:** Provide an overview of disk imaging in forensic investigations.

b) **Preparation:** Describe the necessary preparations undertaken before initiating the disk imaging process using FTK Imager. This may include installing and configuring FTK Imager, connecting the USB drive, and ensuring proper hardware and software compatibility.

c) **Activities Performed**

   i. Disk Image Creation: Explain the process of creating a forensic disk image of the USB drive using FTK Imager. Describe the steps taken to acquire a bit-by-bit copy of the USB drive, ensuring the integrity and preservation of the original data. Discuss any specific settings or options utilized during the imaging process.

   ii. Deleted File Analysis: Detail the steps taken to analyze the disk image and identify any deleted files within it. Explain the techniques and tools used within FTK Imager to search for deleted files, including file carving and signature-based analysis. Discuss any notable findings or observations during the analysis.

d) **Results and Observations**: Present the findings obtained from the deleted file analysis using FTK Imager. This section should include information on the identified deleted files, their locations within the disk image, and any associated metadata. Include relevant screenshots or excerpts from FTK Imager showcasing the deleted files discovered.

e) **Interpretation of the Findings**: Analyze and interpret the significance of the deleted files found within the disk image. Discuss the potential implications and relevance of the deleted files to the forensic investigation. Consider the potential evidentiary value and any insights they may provide into the activities or history of the USB drive's user.

f) **Summary and Conclusion**: Summarize the key findings and conclusions drawn from the disk imaging and deleted file analysis conducted using FTK Imager. Emphasize the importance of disk imaging in forensic investigations and the role of FTK Imager in preserving and analyzing digital evidence.

Notes: Please contact kalana@techcert.lk if you need any clarifications.

6. Conducting Wi-Fi reconnaissance with using Aircrack-ng or Similar

The objective of this assignment is to demonstrate the process of conducting Wi-Fi reconnaissance using Aircrack or a similar tool. Your task is to utilize Aircrack or a comparable tool to perform Wi-Fi reconnaissance, gather information about nearby wireless networks, and generate a comprehensive report documenting your findings (spanning 3–4 pages). The report should consist of the following sections:

1. **Introduction**: Provide an overview Wi-Fi reconnaissance and the role of Aircrack or similar tools in gathering information about wireless networks.
2. **Preparation**: Describe the necessary preparations undertaken before initiating the Wi-Fi reconnaissance activities using Aircrack or a comparable tool. This may include installing and configuring the tool, ensuring compatibility with the wireless adapter, and ensuring a working knowledge of the tool's capabilities.
3. **Activities Performed**: Explain the process of conducting Wi-Fi reconnaissance using Aircrack or a similar tool. Describe the steps taken to scan for nearby wireless networks, gather information about their SSIDs (network names), security protocols, signal strengths, and MAC addresses. Discuss any specific actions performed during the reconnaissance process, such as deauthentication attacks to capture handshake packets.
4. **Results and Observations**: Present the findings obtained from the Wi-Fi reconnaissance activities using Aircrack or a comparable tool. This section should include a detailed report of the identified wireless networks, their characteristics, and any notable observations. Include relevant screenshots or excerpts from the tool's interface displaying the gathered information.
5. **Interpretation of the Findings**: Analyze and interpret the Wi-Fi reconnaissance findings, discussing the potential security implications of the identified wireless networks. Highlight any vulnerable networks with weak security protocols or misconfigurations that may expose them to potential attacks. Discuss the potential risks associated with the gathered information, such as unauthorized access or eavesdropping.
6. **Summary and Conclusion**: Summarize the key findings and conclusions drawn from the Wi-Fi reconnaissance activities conducted using Aircrack or a similar tool. Emphasize the importance of Wi-Fi security and the significance of reconnaissance in identifying potential vulnerabilities. Provide recommendations for improving the security of the identified wireless networks.

Notes: You can do recon on public wi-fi networks without sending deauth type intrusive requests.

Please contact kasun@techcert.lk if you need any clarifications.

7. Cracking password hashes using John the Ripper

The objective of this assignment is to demonstrate the process of cracking password hashes using John the Ripper or a similar password cracking tool. Your task is to utilize John the Ripper or a comparable tool to crack password hashes, recover plaintext passwords from the hashes, and generate a comprehensive report documenting your findings (spanning 3–4 pages). The report should consist of the following sections:

a) **Introduction:** Provide an overview of password cracking and the role of John the Ripper or similar tools in recovering plaintext passwords from password hashes.

b) **Preparation**: Describe the necessary preparations undertaken before initiating the password cracking process using John the Ripper or a comparable tool. This may include installing and configuring the tool, obtaining the password hashes, and ensuring the availability of relevant dictionaries or wordlists.

c) **Activities Performed**: Explain the process of cracking password hashes using John the Ripper or a similar password cracking tool. Describe the steps taken to load the password hashes into the tool, select the appropriate cracking mode (e.g., dictionary-based, brute-force, or hybrid), and configure any additional options or rules. Discuss any specific actions performed during the cracking process, such as customizing the attack parameters or applying specific password cracking techniques.

d) **Results and Observations**: Present the findings obtained from the password cracking activities using John the Ripper or a comparable tool. This section should include a detailed report of the recovered plaintext passwords from the cracked hashes. Include relevant screenshots or excerpts from the tool's interface showcasing the cracked passwords and the associated hashes.

e) **Interpretation of the Findings**: Analyze and interpret the cracked passwords, discussing the significance of the recovered plaintext passwords. Assess the strength or weakness of the cracked passwords, highlight any patterns or commonalities among the passwords, and discuss their potential implications for password security.

f) **Summary and Conclusion:** Summarize the key findings and conclusions drawn from the password cracking process conducted using John the Ripper or a similar tool. Emphasize the importance of strong password policies, password complexity, and password hashing algorithms to enhance password security. Provide recommendations for improving password security based on the findings of the password cracking exercise.

Notes: Please contact kasun@techcert.lk if you need any clarifications.

8. Security analysis of a WordPress website using WPScan

The objective of this assignment is to demonstrate the process of conducting web security analysis of a WordPress website using WPScan Your task is to utilize WPScan or a comparable tool to perform a web security analysis, identify potential vulnerabilities within the WordPress website, and generate a comprehensive report documenting your findings (spanning 3–4 pages). The report should consist of the following sections:

a) **Introduction:** Provide an overview of the assignment's objectives, emphasizing the importance of web security analysis and the role of WPScan in identifying potential vulnerabilities within WordPress websites.
b) **Preparation**: Describe the necessary preparations undertaken before initiating the web security analysis using WPScan . This may include installing and configuring WPScan, ensuring connectivity to the WordPress website, and ensuring the availability of relevant plugins or themes for testing.
c) **Activities Performed**: Explain the process of conducting web security analysis using WPScan Describe the steps taken to scan the WordPress website for known vulnerabilities, insecure configurations, outdated plugins or themes, and other security issues. Discuss any specific actions performed during the analysis, such as specifying custom scan options or targeting specific areas of the website.
d) **Results and Observations**: Present the findings obtained from the web security analysis using WPScan or a comparable tool. This section should include a detailed report of identified vulnerabilities, their severity levels, and accompanying descriptions. Include relevant screenshots or excerpts from the WPScan interface showcasing the scan results.
e) **Interpretation of the Findings**: Analyze and interpret the scan results, discussing the potential impact and implications of the identified vulnerabilities on the security of the WordPress website. Highlight any vulnerabilities that may lead to unauthorized access, data breaches, or other security risks. Discuss the importance of addressing the identified vulnerabilities and the potential consequences of leaving them unpatched.
f) **Summary and Conclusion**: Summarize the key findings and conclusions drawn from the web security analysis conducted using WPScan Emphasize the importance of regular security assessments for WordPress websites and the role of WPScan in identifying and mitigating potential vulnerabilities. Provide recommendations for improving the security of the WordPress website based on the identified vulnerabilities.

Note: Make sure to adhere to target practicing guidelines. You can set vulnerable WordPress installation using old WP versions & plugins.

Please contact kasun@techcert.lk if you need any clarifications.

9. Security Analysis of Android Mobile Application InsecureBankv2

The objective of this assignment is to provide practical experience in identifying and exploiting vulnerabilities in Android applications through the analysis of InsecureBankv2, a purposely vulnerable app. Your task is to explore the InsecureBankv2 application and identifying and exploiting vulnerabilities. Begin by reviewing the list of known issues provided, including hardcoded secrets, weak authorization mechanisms, and more, and generate a comprehensive report documenting your findings (spanning 3–4 pages). The report should consist of the following sections:

a) **Introduction:** Provide a comprehensive overview of the importance of mobile application security and common Android vulnerabilities.
b) **Preparation:** Detail the steps you have taken to prepare for your analysis, such as setting up the InsecureBankv2 application on an Android emulator or device, configuring the necessary analysis tools, and ensuring a secure environment for testing.
c) **Activities Performed:** Outline the activities you performed while exploring the application. This should include the methodologies you employed to identify vulnerabilities such as hardcoded secrets, weak authorization mechanisms, etc., and any tools or techniques you used to exploit these vulnerabilities.
d) **Results and Observations:** Present the findings from your analysis. This should involve a detailed account of each vulnerability identified, how you discovered it, and the potential or actual exploitation. Include screenshots or other evidence to illustrate the vulnerabilities.
e) **Interpretation of the Findings:** Analyze and interpret the implications of the vulnerabilities you discovered. Discuss the potential impact on users and the application itself, and reflect on how these vulnerabilities could be addressed or mitigated.
f) **Summary and Conclusion:** Conclude with a summary of your findings. Provide recommendations for improving the security of the mobile application based on the identified vulnerabilities.

Notes: Please contact chalana@techcert.lk if you need any clarifications.