CS3002- Information Security

Assignment 1

Information Security Primer

Objective

The objective of this assignment is to get students acquainted with real-world scenarios where ethical hackers are hired by organizations to asses vulnerabilities in their IT infrastructure, act like hackers, and penetrate the system or network exploiting vulnerabilities and suggesting appropriate remediations so that identified vulnerabilities are not exploited in the future. Attempting this assignment will enable students to exploit vulnerabilities in the systems, analyse suspicious files, perform reconnaissance to find vulnerabilities in websites, and draft a professional report laying down step-by-step instructions on how these tasks are to be performed.

PLEASE READ THE BELOW MENTIONED GUIDELINES VERY CAREFULLY

Submission Guidelines

- Compile your research and analysis into a well-structured report.
- Your report should be approximately 1500-2000 words in length (References and citations are not included in the word count)
- Ensure proper citations and references for all sources used in your research. Use https://www.mybib.com for referencing and citation
- Submit your report in a digital format
- You can use CHATGPT or any other AI tools for ideas or research but refrain from using the exact content. Include screenshots of the prompts you give to CHATGPT while doing research as part of Appendix.
- You are required to submit a Turnitin report of the written document along with the assignment.
- No Assignments will be accepted after the deadline.

- **Cases of plagiarism and copying will be taken very seriously and could lead to severe consequences as per the university policy**

Submission Deadline

11:55PM Thursday 19th September, 2024.

Task 1:

Scenario

You have been hired by a company as an **Ethical hacker** to conduct a **vulnerability assessment**. During the assessment, you came across a vulnerability in the Windows 7 Operating System one of the organization's critical systems. The vulnerability is identified as Eternal Blue (**MS17-010 Eternal Blue SMB Remote Windows Kernel Pool Corruption**).

Requirement

As an **Ethical hacker**, you need to inform the relevant information security department and the higher management about this vulnerability in the form of a report. The report will most likely serve as a walkthrough of the steps involved in the exploitation of the vulnerability. Your aim is to list down step-by-step instructions along with screenshots on how this vulnerability can be exploited in a controlled environment (Your virtualized environment) and lastly communicate very clearly how the organization can prevent further exploitation (Adopting particular countermeasures or remediation steps).

You must achieve persistence and perform actions post exploitation to deepen your understanding of red team tactics.

Research on the vulnerability "**Eternal Blue**" and exploit it using the described tools below

Tools Required

- Kali Linux Virtual machine / ISO (Download Link Attached)
- Nmap
- Metasploit / msfconsole
- Windows 7 OS ISO Image (Download Link Attached)

Task 2

Some samples have been provided in this assignment which contain both malicious and benign files. You are required to complete the following tasks.

- Determine the file type of the file.
- Determine whether the file is malicious or not?
- If the file is malicious, specify its category, the URLs it contacted, and any files it dropped.

- Hidden in one of these files is your roll number. You must find out which file is yours. CERCA TROVA.
- If the file is an executable, specify 5 APIs that it uses.

Perform your analysis on a virtual machine so as not to infect your primary system with malwares.

Task 3

You are required to perform recon on the following website.
https://cms.comsats.edu.pk:8083.

The report on this section should contain the following details.

- At least 5 CVEs in the current tech stack the website uses.
- 5 ways to exploit this website and the mitigation for each exploit as well.
- Results of an Nmap scan of the website.

Report Format

- Title Page
- Table of Contents
- Task 1 details including introduction, background of the vulnerability, step by step procedure on how the vulnerability is to be exploited, mitigation strategies, references and conclusion.
- Task 2 report containing all the information required as described above.
- Task 3 report containing all the information required as described above.
- Every task should contain references to the resources you have used to research the task.
- The tools used in every task must be mentioned in the report.

Evaluation Criteria

Category	**Excellent (90-100%)**	**Good (75-89%)**	**Fair (50-74%)**	**Poor (0-49%)**
Report Structure & Format	Exceptionally organized with clear sections; follows all guidelines perfectly.	Well-structured with minor formatting issues; mostly follows guidelines.	Some organization issues; missing sections or notable formatting problems.	Disorganized; missing critical sections; formatting errors.
Task 1: Vulnerability Research & Exploitation	Detailed research on Eternal Blue; all steps clearly outlined with screenshots; strong mitigation strategies.	Good research; most steps and screenshots present; appropriate but not fully detailed	Basic research; missing or unclear steps; sparse screenshots; superficial mitigation strategies.	Little to no research; missing or unclear steps; no screenshots; incomplete or missing

		mitigation strategies.		mitigation strategies.
Task 2: Malware Analysis	Comprehensive analysis; accurate identification of files; full details on malicious activity; correct roll number found.	Good analysis; accurate identification; sufficient details; correct roll number found.	Basic analysis; some errors in identification; limited details; roll number found with effort.	Minimal or incorrect analysis; inaccurate identification; few details; roll number not found.
Task 3: Website Reconnaissance	Exhaustive recon; accurate CVEs and exploits; thorough Nmap scan analysis.	Solid recon; most CVEs and exploits identified; good Nmap scan analysis with minor details lacking.	Basic recon; some CVEs and exploits identified; vague mitigation; incomplete Nmap analysis.	Insufficient recon; few or incorrect CVEs/exploits; missing or incorrect mitigation; little to no Nmap analysis.
Clarity & Depth of Explanation	Exceptionally clear explanations; well-explained technical concepts; strong understanding.	Clear explanations; minor gaps in technical details; good understanding.	Somewhat clear; lacks depth; moderate understanding of technical concepts.	Unclear explanations; missing or inaccurate concepts; poor understanding.
References & Citations	All sources cited properly with no errors; follows guidelines perfectly; credible and relevant.	Most sources cited with minor errors; follows guidelines well; generally credible and relevant.	Some sources cited; several errors or inconsistencies; sources not always credible or relevant.	Few or no sources cited; improper citation; sources not credible or relevant.
Tools Used	All relevant tools mentioned and applied correctly; screenshots provided.	Most tools mentioned and applied; screenshots provided for most tools.	Some tools mentioned; not all applied correctly; few screenshots.	Few or no tools mentioned or applied correctly; missing screenshots.
Demo Viva	Exceptional understanding; clear explanations; answers all questions confidently and accurately.	Good understanding; clear explanations; answers most questions accurately.	Moderate understanding; struggles with some concepts; answers basic questions but may miss complex ones.	Little to no understanding; unable to explain concepts or answer questions accurately.