Introduction: In this assignment, you'll deepen your understanding of the evolving threat landscape, with a focus on vulnerabilities actively exploited in H1 2025, and gain practical experience in analyzing and prioritizing vulnerabilities.

Learning Objectives: By the end of this assignment, you will be able to:

1. Understand current malware and vulnerability trends as described in the H1 2025 report and their implications on cybersecurity.
2. Identify and research critical vulnerabilities (CVEs) actively exploited in the wild.
3. Prioritize vulnerabilities based on risk factors including exploitability, impact, and exposure.
4. Apply practical vulnerability management skills, including scanning and detection, in a controlled environment.
5. Develop effective mitigation strategies grounded in real-world threat intelligence.
6. Communicate technical findings clearly to both technical and non-technical stakeholders.

Part 1: Reading & Written Report (2–3 pages, single space. Use the tasks and questions as your headings.)

Read the H1 2025 Malware and Vulnerability Trends report thoroughly (https://www.recordedfuture.com/research/h1-2025-malware-and-vulnerability-trends). Then write a report (2–3 pages) addressing the following:

Task A:

1. Summarize key trends in vulnerability disclosures and exploitation.
2. Identify the top 5 most impactful vulnerabilities or malware tactics highlighted in the report.
3. Ensure that your report focuses on how these trends influence enterprise security posture.
4. At the end of your report, use this table to summarize your work:

Section	Your Response
1. Summary of Key Trends in Vulnerability Disclosures and Exploitation	*Summarize the main trends discussed in the report (e.g., types of vulnerabilities most exploited, methods of exploitation, sectors targeted, notable shifts from previous years.*
2. Top 5 Most Impactful Vulnerabilities or Malware Tactics	*List the top 5 vulnerabilities with CVEs or TTPs like "EDR evasion via BYOI"* **1.** **2.** **3.** **4.** **5.**
3. Enterprise Security Impact	*For each of the top 5, explain how they influence enterprise security posture. Consider impacts on patching, detection/response, policy changes, user awareness, and architectural shifts.* **1.** **2.** **3.** **4.** **5.**

Part 2: Hands-On Lab – Vulnerability Analysis

Tools Required:

- Access the National Vulnerability Database: https://nvd.nist.gov/
- Choose a vulnerability scanning tool: Nessus, OpenVAS, Qualys, or one of your choice
- Virtualbox with Linux or Windows

For Part 2, provide detailed steps and detailed screenshots for each step of your scan results and explain each screenshot.

Below are the high-level steps to accomplish as part of this Part 2. Additional research and troubleshooting may be needed:

Task A: Select Vulnerabilities

- From the report, select 3 CVEs actively exploited in H1 2025 (preferably ones with no authentication required and enabling remote code execution).
- For each CVE, retrieve details from NVD including:
  - CVE description and affected software
  - CVSS score and vector
  - Exploitability and mitigation measures

Task B: Vulnerability Prioritization

- Based on your research, prioritize the CVEs for remediation using the following criteria:
  - Exploitability
  - Impact on confidentiality, integrity, and availability
  - Exposure likelihood in a typical enterprise environment
- Justify your prioritization with clear reasoning.

Task C: Vulnerability Scanning and Detection

- Using Virtualbox:
  - Use a vulnerability scanner of your choice to scan a VM with the OS of your choice (Linux or Windows).
  - Identify if any of the CVEs you researched are present.
  - Report on how the scanner detects and categorizes these vulnerabilities.

Part 3: Discussion and Reflection

Write a 2-3 paragraph (5–6 sentences each) to answer each prompt below:

- Discuss how threat actors leverage these vulnerabilities as initial access vectors or to bypass defenses.
- Reflect on how organizations can better integrate threat intelligence and vulnerability management to reduce risk.
- Propose 3 mitigation strategies organizations should adopt based on your analysis.

Requirements:

- You must provide detailed steps and screenshots for each step for installing, configuring, and demonstrating how the selected tool work to include details from NVD.
- All parts of this assignment (1-3) must be submitted via a Microsoft Word file. Any other formats will not be accepted and will result in a zero grade.
- A PowerPoint slide deck (5-7 slides) summarizing your findings and recommendations for a non-technical audience
- A bibliography must accompany your submission depicting all your work for this lab. Ensure that all work is cited (MLA or APA format). Be sure to analyze your work and not just copy and paste chunks of information. Any plagiarized work will result in a zero grade and can lead to failing the course.

Evaluation: 8 points. All requirements are gradable. Use the requirements listed above as your checklist to ensure that you have completed all the requirements.

Grading Criteria	Points
1. File format requirements	-1
2. Overall clarity and effort, in depth analysis, prioritization and justification, mitigation recommendations, PowerPoint presentation and clarity	4
3. Overall clarity and effort of detailed steps and screenshots (output + explanation) for Part 2.	4
4. Overall good and consistent quality of writing, research, analysis, correct use of terminology	-1
5. Correct spelling & grammar.	-1
6. Font consistency	-0.50
7. Correct citations in MLA or APA format. All sources will also include links	-1
8. Name, course information, etc.	-1
9. Submitted the deliverables as per the due dates specified in the Course Schedule	Per syllabus

Questions:

It is up to each student to clarify any part of these guidelines, which may be unclear immediately after this lab has been assigned.