Montgomery College
Germantown Campus
Cybersecurity Program
Lab 2: Assignment + Tool

Introduction: In this assignment, you'll learn how advanced threat actors like Salt Typhoon use network scanning and other tactics to infiltrate critical systems. You'll read a real-world advisory summary, analyze attacker behavior, simulate scanning in a lab, and map your findings to the MITRE ATT&CK framework.

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

1. Explain the role of scanning in cyber-attacks.
2. Describe real attacker behavior based on a real-world threat (Salt Typhoon).
3. Perform a simple scan using Nmap or similar tools.
4. Use the MITRE ATT&CK framework to connect actions to known techniques.
5. Reflect on how defenders can protect against these threats.

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

Read the article of the August 2025 advisory on Salt Typhoon (https://medium.com/h7w/countering-chinese-state-sponsored-actors-af22ecb89371). Then write a report (2–3 pages) answering the following:

Task A: Scanning and Initial Access

1. What is network scanning, and why do attackers like Salt Typhoon use it?
2. What kinds of devices or systems do they look for when scanning?
3. What tools do they likely use to scan networks? You will select one from this list to install, configure, test, and demonstrate how it works. You will also use Nmap as listed in Part 2 below. Total of 2 as part of the hands-on.

Task B: What Happens After Scanning?

1. List 2–3 other actions Salt Typhoon takes after scanning.
2. Pick two and explain how it helps them stay hidden or steal information.
3. Why is it harder to detect attackers who "live off the land" (use built-in system tools instead of malware)?

Task C: MITRE ATT&CK Mapping

1. Choose 2 attacker techniques used by Salt Typhoon (e.g., scanning, credential access).
2. Go to https://attack.mitre.org and find:
    - The Tactic (e.g., "Reconnaissance")
    - The Technique Name
    - The Technique ID
3. Write an explanation of how each technique was used based on the article and fill in this table:

Tactic	Technique Name	Technique ID	Explanation

Part 2: Hands-On Lab – Simulated Network Scanning

You will simulate how attackers perform network scanning using tools like Nmap. Use Virtualbox to complete these tasks. 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:

1. Choose a target in your lab (e.g., another VM).
2. Run a basic Nmap scan (nmap -sV <target IP>) and a more detailed scan (nmap -A <target IP>)

3. Identify:
    - Open ports
    - Services running
    - Any potential vulnerabilities (Nmap may show version info)
4. Interpret the results by answering the prompts below.

- What services are running?
- Are any of them outdated or potentially vulnerable?
- If you were an attacker, which service might you explore first and further investigate?
- What MITRE ATT&CK technique does this scanning activity map to? Fill in this table and explain.

Tactic	Technique Name	Technique ID	Explanation

Part 3: Reflection – Defending Against Scanning and Attacks

Write a short paragraph (5–6 sentences) to answer each prompt below:

- How could a company detect or block scanning activity?
- What steps could stop attackers like Salt Typhoon after they scan the network?

Requirements:

- You must provide detailed steps and screenshots for each step for installing, configuring, and demonstrating how each of the tools work.
- 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 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 of the Salt Typhoon analysis and MITRE ATT&CK mapping	4
3. Overall clarity and effort of detailed steps and screenshots (output + explanation) for Part 1, Task A.3 and 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.