Network Security

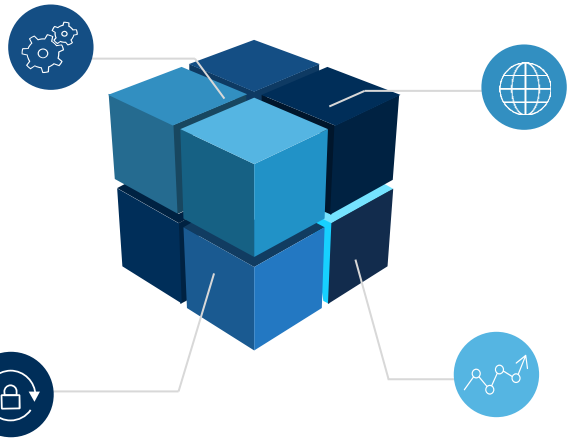
Program Code: ZX305

OPERATION ORDER

Operation **Domain Mapper** is set to commence, targeting the intricate landscapes of network security. This mission will deploy cutting-edge reconnaissance, infiltration, and fortification techniques to safeguard digital territories.

1. VISION

This operation aims to build a strong digital defense by training a new group of cyber protectors. These skilled individuals will use powerful network analysis tools to find and stop threats before they can do harm, making our digital spaces safer.



2. MISSION

The goal is to teach upcoming network security experts how to thoroughly check networks for weak spots and defend against attacks.

3. STRATEGY

Scanning, information gathering, and strategic attacks.

4. OBJECTIVES

- To Educate: Build a team of skilled cyber security workers who know how to use advanced tools to keep networks safe.
- To Protect: Improve digital safety by practicing finding and fixing security weak spots.
- To Encourage Creativity: Promote innovative thinking and the creation of new methods to fight off the constantly changing threats in cybersecurity.
- To Enable: Give participants the skills they need to do their own security checks and take action to make their networks stronger against attacks.

Project Structure

1. Getting the User Input

1.1. Prompt the user to enter the target network range for scanning.
1.2. Ask for the Domain name and Active Directory (AD) credentials.
1.3. Prompt the user to choose a password list, defaulting to Rockyou if none is specified.
1.4. Require the user to select a desired operation level (Basic, Intermediate, Advanced or None) for each mode: Scanning, Enumeration, Exploitation. **Note:** Selection of a higher level automatically encompasses the capabilities of the preceding levels.

2. Scanning Mode

2.1. **Basic:** Use the **-Pn** option in Nmap to assume all hosts are online, bypassing the discovery phase.
2.2. **Intermediate:** Scan all 65535 ports using the **-p-** flag.
2.3. **Advanced:** Include UDP scanning for a thorough analysis.

3. Enumeration Mode

3.1. **Basic:**
- 3.1.1. Identify services (-sV) running on open ports.
- 3.1.2. Identify the IP Address of the Domain Controller.
- 3.1.3. Identify the IP Address of the DHCP server.

3.2. **Intermediate:**
- 3.2.1. Enumerate IPs for key services: FTP, SSH, SMB, WinRM, LDAP, RDP.
- 3.2.2. Enumerate shared folders.
- 3.2.3. Add three (3) NSE scripts you think can be relevant for enumerating domain networks.

3.3. **Advanced (Only if AD credentials were entered):**
- 3.3.1. Extract all users.
- 3.3.2. Extract all groups.
- 3.3.3. Extract all shares.
- 3.3.4. Display password policy.
- 3.3.5. Find disabled accounts.
- 3.3.6. Find never-expired accounts.
- 3.3.7. Display accounts that are members of the Domain Admins group.

4. Exploitation Mode

4.1. **Basic:** Deploy the NSE vulnerability scanning script.
4.2. **Intermediate:** Execute domain-wide password spraying to identify weak credentials.
4.3. **Advanced:** Extract and attempt to crack Kerberos tickets using pre-supplied passwords.

5. Results

5.1. For every execution, save the output in a PDF file.

6. Creativity (Optional)

6.1. Display the current stage, to give the user progress feeling.
6.2. Allow Wizard mode, to help students choose.
6.3. Include a help menu to help users understand how to use this tool effectively.

General

- Suggested tools: Nmap, Hydra, CrackMapExec, Enum4Linux, Impacket, Rpcclient, Sipcalc.
- Everything other than the user input should be automated.
- Use functions.

Comments

Use comments in your code to explain what you did.
If you are using code from the internet, add credit and links.
In the script, write the student's name and code, the class code, and the lecturer's name.

Submitting Your Project

To ensure a successful submission of your project, please adhere to the instructions provided below. Following these guidelines will facilitate a smooth evaluation process and allow you to receive feedback on your work promptly.

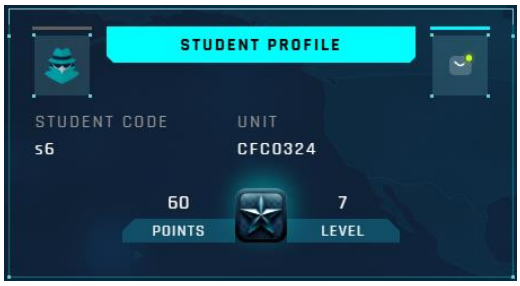
1. What to Submit

Only .sh and .pdf files will be accepted. **No other file types** (e.g., .docx, .txt) will be accepted. Ensure your files are in the correct format before submission.

You must submit both the script (.sh) and the corresponding PDF. The PDF should prove that you completed all the tasks and that the project works as expected. If you miss the script file or the PDF, you will be asked to resend your submission.

2. File Naming

Ensure your project files follow the correct naming convention:
UNIT.STUDENT.PROGRAM



For example, if your unit is CFC0324, your student ID is s6, and your program code is zx305, the correct filenames should be:

CFC0324.s6.zx305.sh
CFC0324.s6.zx305.pdf

3. Submission Process

Email Address: Forward your project materials to **projects@thinkcybergroup.com** and to your trainer.

Email Subject: Format your email subject as follows: **Project: DOMAIN MAPPER <Student Name:Unit Name>**. Make sure to replace **<Student Name>** with your actual name and **<Unit Name>** with the precise name of the unit as shown in the simulator.

4. **Unique Work**
   Your work **must** be unique. If the system detects that your project has been copied from another student, **both** the student who copied the work **and** the student who allowed their work to be copied will be **banned**. After being banned, the server will no longer check your future submissions.

   Important: You are encouraged to help each other with ideas and techniques, but each student **must submit their own, original project**. If you submit a project that is flagged as identical or too similar to another student's, both of you will be banned from submitting future work to the system.

5. **Use of AI Tools**
   You are allowed to use tools like ChatGPT or other AI bots for assistance, but your program must work and be clear. If your AI code is simply copied, doesn't work, or is unclear, you will be banned from future submissions.

Response Time: After submitting, you can track the status of your submission (pass or fail) through the ***Progress Tracker*** inside your student account. Allow up to one week for your project to be reviewed.

How to Showcase Your Cybersecurity Projects on LinkedIn

1. **Write a Compelling Post**:
   When you share your project on LinkedIn, make sure to write a post that highlights the importance of the project and your key takeaways from it. Use engaging language and explain:
   - **The challenge** you solved.
   - **Tools** and technologies you used (mention relevant tools like Python, Shell Scripting, Scapy, etc.).
   - **Skills** you developed (problem-solving, incident response, penetration testing, etc.).
   - **Real-world relevance** of your project. Explain how it can be applied to secure networks, detect vulnerabilities, or analyze threats in a professional setting.

Example:

"Excited to share my latest project in Network Security (ZX305) where I built a script to detect network anomalies. This project helped me understand intrusion detection and how to safeguard systems against real-world threats. Using Python and Shell scripting, I developed a tool that can assist security teams in monitoring and reacting to suspicious network activities."

2. **Attach Your PDF**:
   Upload the PDF file of your project as an attachment to your post. This will allow recruiters, potential employers, or other professionals in the cybersecurity field to directly review your work.
   - Ensure your **PDF is professional**, free of errors, and clearly explains each section of the project.
   - **Highlight results**: If you were able to detect or simulate cyber threats, mention how your tool worked and the outcomes of your project.

3. **Record a Video Demo**:
   Videos are powerful on LinkedIn. Record a quick demo of your project where you:
   - Explain the problem.
   - Walk through your code.
   - Show your script in action (for example, showing how your network security tool detects a threat).

Example Intro:

"Here's a quick demo of my project where I developed a Python-based tool to monitor network traffic and detect potential cyber threats. Watch how it scans real-time traffic and flags suspicious activity."

4. **Mention the Certificate**:
   Once you complete the project, your simulator generates an official **ThinkCyber certificate**. Share this alongside your post to demonstrate your verified completion of the project.

Example:

"Proud to have completed my Network Security (ZX305) program with ThinkCyber! This certificate is proof of the skills I've acquired in identifying and mitigating cybersecurity threats."

Make sure to upload the certificate as an image. Use relevant hashtags like **#cybersecurity**, **#networksecurity**, and **#Python** to increase your visibility.

5. **Encourage Networking**:
   Mention that you are open to connecting with cybersecurity professionals and recruiters who might find your skills and projects relevant to their needs.