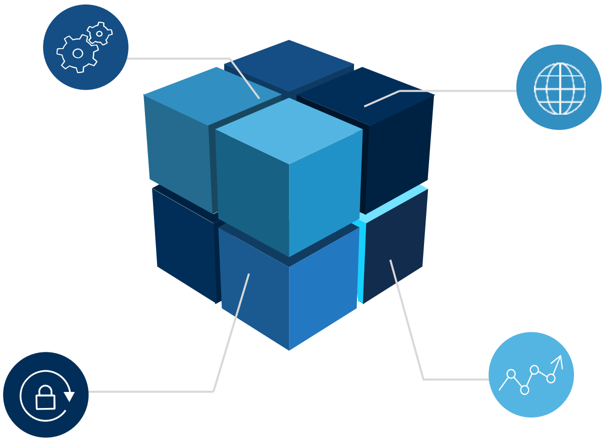
Penetration Testing

Program Code: ZX301

OPERATION ORDER

Most security checks and penetration testing should be automated to stay up-to-date and protect our assets.



1. VISION

To create a self-running system that automatically finds security holes in our networks, keeping our data safe from hackers with minimal human intervention.

2. MISSION

To swiftly and automatically scan networks, identifying and fortifying weak spots against unauthorized access, ensuring our data remains protected.

3. STRATEGY

Creating automation to map services and vulnerabilities on the entire local network.

4. OBJECTIVES

- Scan the network for ports and services.
- Map vulnerabilities.
- Look for login weak passwords.

Project Structure

1. Getting the User Input

1.1 Get from the user a network to scan.

1.2 Get from the user a name for the output directory.

1.3 Allow the user to choose **'Basic'** or **'Full'**.

1.3.1 **Basic:** scans the network for TCP and UDP, including the service version and weak passwords.

1.3.2 **Full:** include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.

1.4 Make sure the input is valid.

2. Weak Credentials

2.1 Look for weak passwords used in the network for login services.

2.1.1 Have a built-in password.lst to check for weak passwords.

2.1.2 Allow the user to supply their own password list.

2.2 Login services to check include: SSH, RDP, FTP, and TELNET.

3. Mapping Vulnerabilities

3.1 Mapping vulnerabilities should only take place if **Full** was chosen.

3.2 Display potential vulnerabilities via NSE and Searchsploit.

4. Log Results

4.1 During each stage, display the stage in the terminal.

4.2 At the end, show the user the found information.

4.3 Allow the user to search inside the results.

4.4 Allow to save all results into a Zip file.

5. Creativity

General

- Suggested tools: Nmap, Hydra, Medusa, Searchsploit.
- 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.

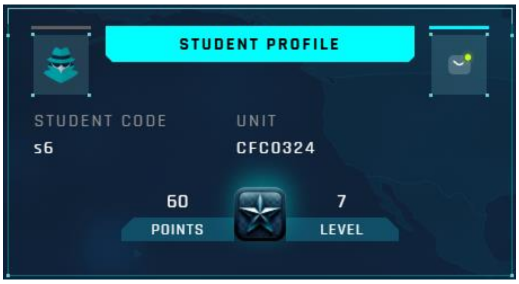
1. **What to Submit**

   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



STUDENT PROFILE

STUDENT CODE: s6

UNIT: CFC0324

60 POINTS

7 LEVEL

   For example, if your unit is CFC0324, your student ID is s6, and your program code is zx301, the correct filenames should be:

   CFC0324.s6.zx301.sh
   CFC0324.s6.zx301.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: VULNER <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).

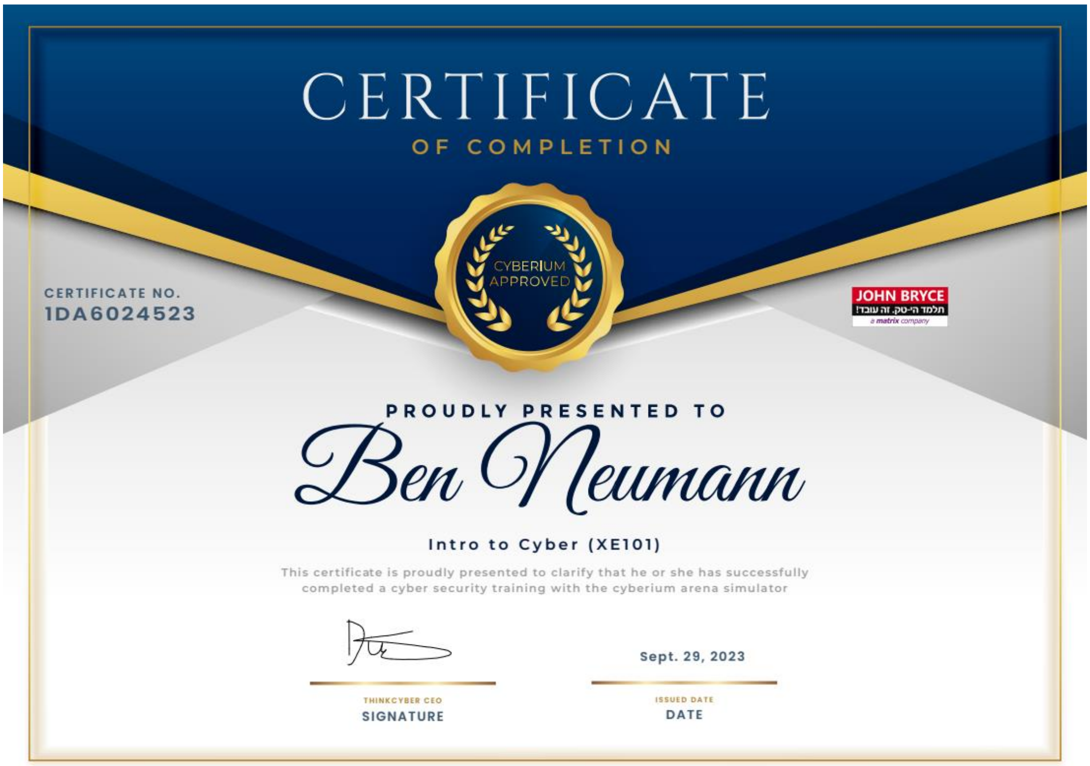
Example Intro:

"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."



CERTIFICATE
OF COMPLETION

CYBERIUM APPROVED

CERTIFICATE NO.
1DA6024523

JOHN BRYCE
תלמד הי-טק. זה עובד!
a matrix company

PROUDLY PRESENTED TO

Ben Neumann

Intro to Cyber (XE101)

This certificate is proudly presented to clarify that he or she has successfully completed a cyber security training with the cyberium arena simulator

Sept. 29, 2023

THINKCYBER CEO
SIGNATURE

ISSUED DATE
DATE

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.