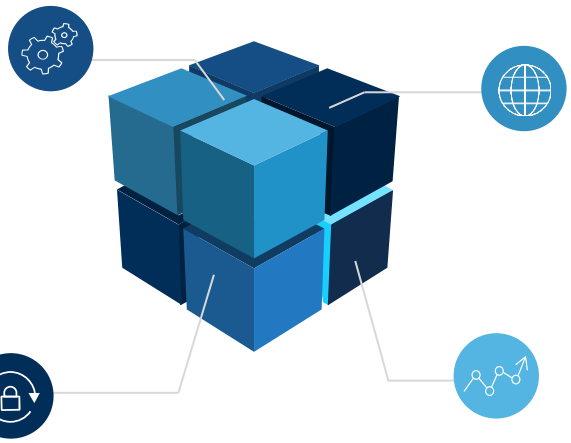
OPERATION ORDER

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

1. VISION

Cyber units can automate finding vulnerabilities in local networks.



2. MISSION

Maps network devices for ports, services, and vulnerabilities.

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

Submit the source code (.sh) and a pdf file with screenshots proving the functions work.
Send the project to the trainer's email.
In the email subject type **project: Vulner <student name>**.