**PENETRATION TESTING PROJECT**

**Project Explanation:**

This project involves creating a script for comprehensive network device mapping, identifying ports, services, and vulnerabilities.

The user defines the network range, after which the program deploys tools like Nmap and masscan for scanning and mapping purposes, storing the data in a newly created directory.

The script also probes for network vulnerabilities, employing Nmap, Searchsploit, hydra, and medusa to identify security gaps, such as weak passwords.

the scan summary and findings are presented to the user.

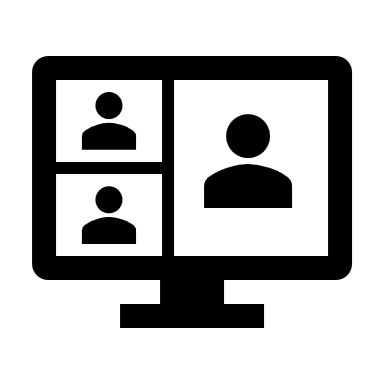
Finally the user can saved to script output into a zip file.

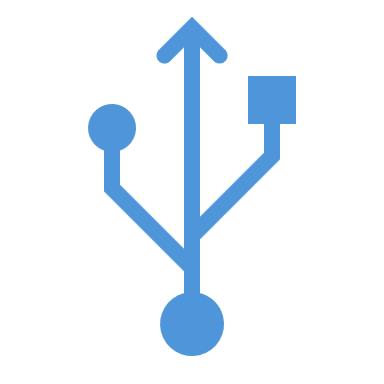
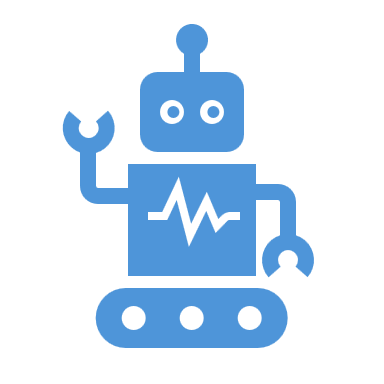
In the following pages, I'll delve into the script's functions, detailing how each one impacts its overall performance.

**Peleg odi**

**S24**

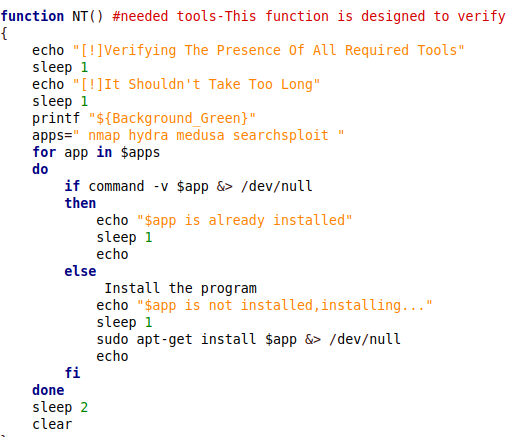
**lecturer's name : Natali erez**



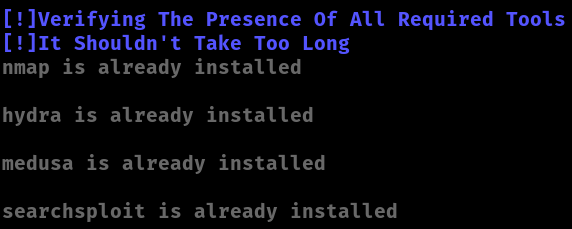
**Function detail's**

**Our first function called "NT" -this function stands for "needed tools"-** **Her role involves verifying whether the script user possesses all the necessary tools for its execution; if not, she ensures to download them on their behalf.**

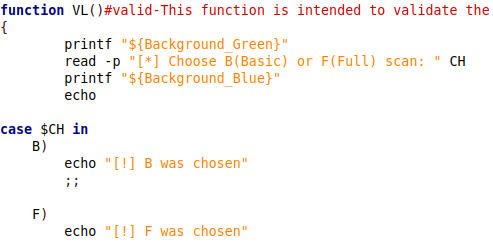


**In the command "apps" -I placed all the tools that needed for this script like: Nmap ,hydra ,medusa and searchsploit.**

**In the second part it says "if the command I type above in the "apps" is not installed then make "Sudo apt-get install" and installed the apps".**



**Our Second function called "** **VL" -this function stands for "Valid"-** **Her role is to ask the script user if he want a Basic scan Or a Full scan than he will answer B for Basic Or F for full scan.**



**The command "read -p stands for reading input from the user with a prompt. The -p option is used to specify a prompt that is displayed to the user before they input their response.**

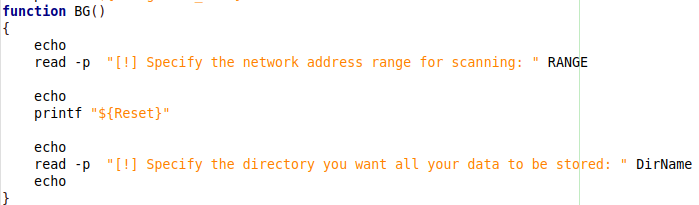


**In the second part it says "in case that B was chosen say "B was chosen"**

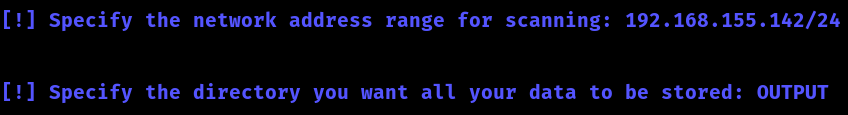
**In case "F" was chosen say F was chosen.**



**Our Third function called "** **BG" -** **This function, designated as "Begins," involves her task of prompting the script user to specify both the directory name where they wish to store all the script output and the range they want to scan.**



**Asking for an IP range to scan and then for a directory name to save all the output in.**



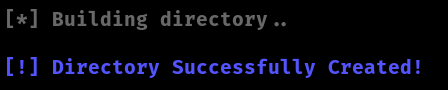
**ראש הטופס**

**Our Fourth function called "** **MK" -** **This function, named "mkdir," essentially establishes the directory where the user intends to store all output.**

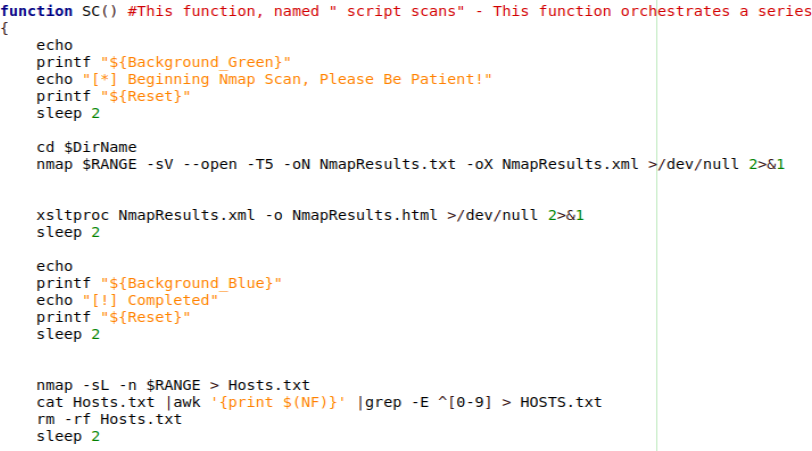
תמונה שמכילה טקסט, צילום מסך, גופן

התיאור נוצר באופן אוטומטי

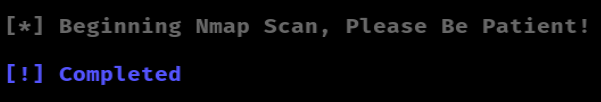
**The "mkdir" command is generating the directory under the username chosen in the previous function.**



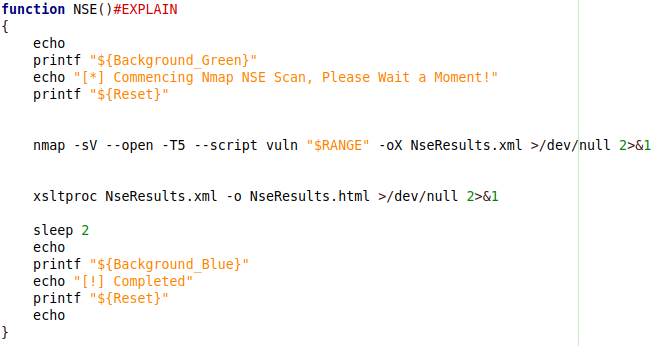
**Our Fifth function called "** **SC" -** **This function, named "** **script scans" -** **This function orchestrates a series of network scans using Nmap, saving results in various formats while maintaining user interface aesthetic.**



**In this function, I included the "cd $DirName" command to ensure that all subsequent data is saved within the directory created earlier.**



**Our Sixth function called "** **NSE" -** **This function executes an Nmap NSE (Nmap Scripting Engine) scan to identify vulnerabilities within the specified range, converting results into XML and HTML formats.**

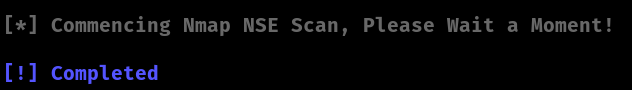


**In This command "** **nmap -sV --open -T5 --script vuln "$RANGE" -oX NseResults.xml"**

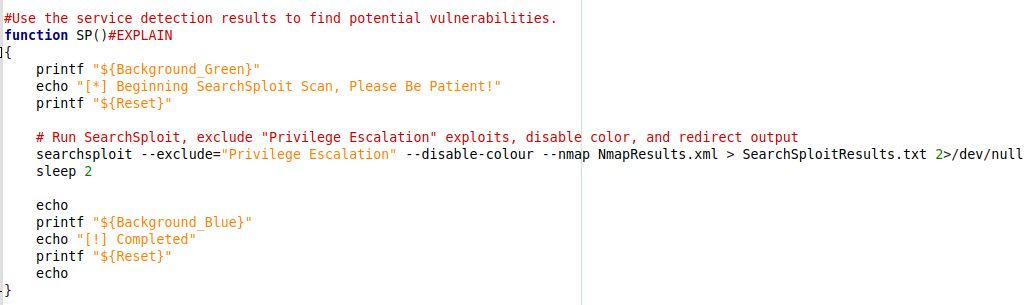
**sV: Enables version detection.**

**open: Only displays open ports.**

**RANGE: Specifies the IP range to scan.**



**Our seventh function called "** **SP" -** **This function executes a SearchSploit scan, excluding "Privilege Escalation" exploits, disabling color output, and saving results to a text file.**

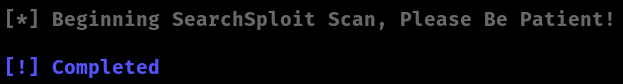


**In This command searchsploit --exclude="Privilege Escalation" --disable-color --Nmap NmapResults.xml > SearchSploitResults.txt"**

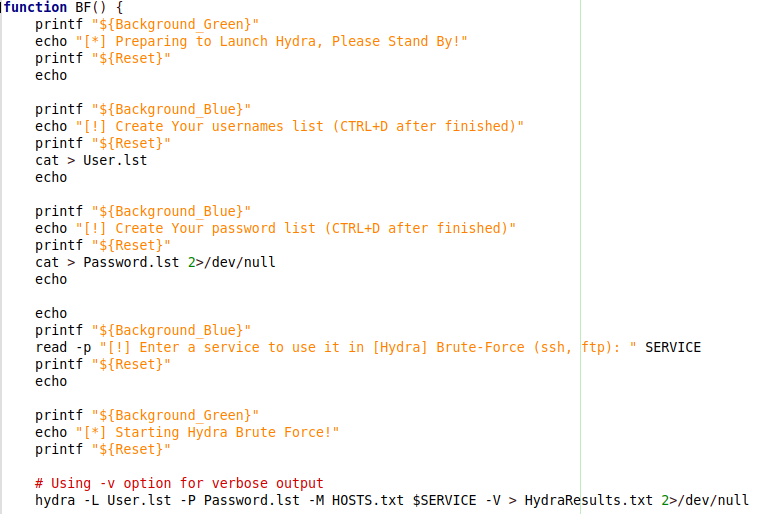
**exclude="Privilege Escalation": This option excludes exploits related to "Privilege Escalation" from the search results.**

**disable-color: This option disables color output, making the results more suitable for parsing or redirecting.**

**Nmap NmapResults.xml: This specifies that the search should be based on the Nmap scan results provided in the file "NmapResults.xml".**



**Our eighth function called "** **BF" -** **This function executes a SearchSploit scan, excluding "Privilege Escalation" exploits, disabling color output, and saving results to a text file.**

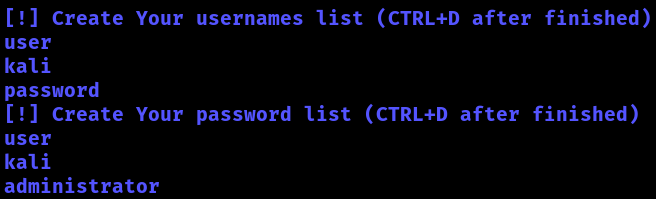


**This command "** **hydra -L User.lst -P Password.lst -M HOSTS.txt $SERVICE -V > HydraResults.txt"**

**--L User.lst: Specifies a list of usernames to try during the attack, sourced from the file" User.lst."**

**-p passwords.lst Specifies a list of passwords to try for each username, sourced from the file Password.lst.**

**--M HOSTS.txt: Specifies a list of target hosts to attack, sourced from the file HOSTS.txt.**



**In this function, I allow the user to input their chosen username and password lists for scanning. Once they're done, they can press Ctrl+D to signal completion and proceed.**

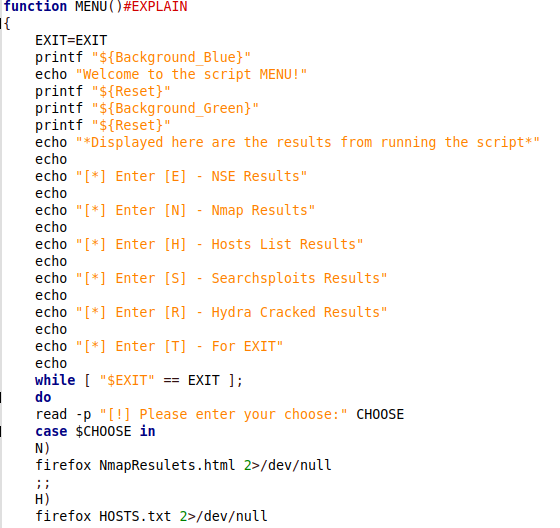
**Our ninth function called "** **LOG " -** **This function compiles various statistics and findings from different scan results into a single log file named "LOG.txt". It includes counts of open ports from Nmap and Masscan scans, numbers of vulnerabilities found by Searchsploit for various services, and counts of cracked logins from Hydra.**

תמונה שמכילה טקסט, צילום מסך, גופן, מספר

התיאור נוצר באופן אוטומטי

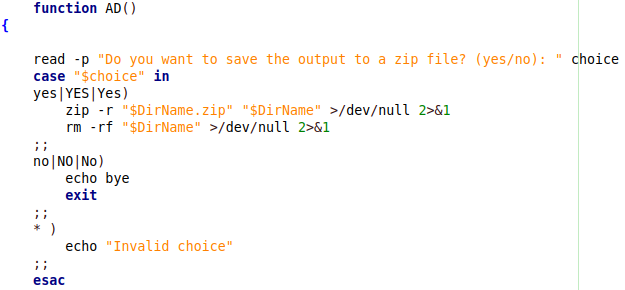
**The function consolidates all outputs into a log.txt file for the user's quick reference.**

**Our tenth function called "** **MENU" -** **This function presents a menu interface to the user, allowing them to access various results generated by the script. Users can choose to view Nmap results, host lists, NSE (Nmap Scripting Engine) results, Hydra cracked results, or Searchsploit results. The function also includes options to exit the menu. Additionally, it opens the selected results in Firefox browser for user convenience.**



**In this function, I offer the user the choice to visualize all the script's output in an engaging manner.**

**Our eleventh function called "** **AD" This function prompts the user, upon selecting the exit option, to decide whether they wish to archive all output into a zip file or not.**





**Upon affirmative confirmation, it will generate a compressed file containing all the output data.**

**OVERVIEW OF THE TOOLS EMPLOYED IN THIS PROJECT**

**Searchsploit is a command-line utility used for searching and retrieving exploits from the Exploit Database (Exploit DB). It helps security professionals quickly find and analyze known vulnerabilities and corresponding exploits for various software and systems.**

**Nmap is a versatile network scanning tool used for discovering hosts and services on a computer network. It's widely used by network administrators and security professionals for network inventory, monitoring, and vulnerability assessment.**

**Hydra is a powerful and fast network login cracker which supports numerous protocols to attack, including HTTP, HTTPS, FTP, Telnet, and more. It's commonly used in penetration testing and security assessments to brute-force login credentials and identify weak passwords on various services and applications.**

**NSE (Nmap Scripting Engine) is a flexible and extensible framework within Nmap that allows users to write and execute scripts to automate a wide variety of tasks during network scanning. These scripts can perform tasks such as vulnerability detection, service enumeration, and network discovery, greatly enhancing Nmap's capabilities for security assessments and network exploration.**

**WEB SOURCES INCORPORATED IN THIS SCRIPT**

**ChatGPT-- Helped me with accuracy and correct spelling and knowledge question.**

**GitHub- Great website for script codes.**

**Stack overflow-- website for questions and answers around the world.**

**THIS SCRIPT Written by Peleg Odi**