

**PROJECT: PENETRATION TESTING**

**NAME: BAREL COHEN**

**CLASS: UNIT - Tmagen773624**

**S8**

**JHONBRYCE**

**BC\_PT [Version: s.8]**

**.2024 Barel Cohen ©**



**MY PT PROJECT: BC\_PT**

**Penetration Testing Project Report - Summary**

**Information…………………….1-2**

**Manual.. .....................................3**

**Summery and Introduction……………….4**

**Advanced Manual……………..…...5-8**

**Details of the tool………………………..9-10**

**See the tool in action…………………..…10-18**

**Link to video…………………………….19**

**Logo Credits…………………………….22**



**MANUAL:**

**1)**

**HOW TO RUN THE TOOL - (SCRIPT)**

**Checking your Permissions have to get root Permissions to activate. run as sudo ./BC\_PT.sh or as root in order to allow you using this tool.**

**2)**

**Let's ensure your toolkit is primed and ready for action. We'll check if you have all the essential apps onboard: Chafa for displaying base64-encoded logo, geoiplookup for geolocation, and tor with nipe for anonymous. If any are missing, — we'll handle the installation seamlessly.**

**Now, let's take stock of what's already in your arsenal by default:**

**For Basic and Full Scans:**

**Nmap for comprehensive network scanning**

**Masscan for fast udp open port scanning and then to Nmap -sV**

**Hydra for potent password cracking on weak credentials**

**For passive reconnaissance, we'll rely on:**

**whois for domain ownership information**

**ipinfo.io for detailed IP data**

**And for web scanning, we'll harness the power of:**

**dirb for directory brute-forcing**

**nikto for web server vulnerability assessment**



**Project Summary: BC\_PT**

**Introduction**

The BC\_PT project focuses on Penetration Testing of computer networks and websites. The project's goal is to develop an automated tool for penetration testing that includes basic and full scans of TCP and UDP protocol's networks, passive scans for non-intrusive information gathering, and web scans. The tool utilizes open-source utilities like nmap, masscan, hydra, dirb, nikto, and others. The results are stored in designated folders and displayed to the user for analysis and risk assessment.

**Project Objectives Summary**

**1.** Create a directory on the desktop named BC\_PT-DB for storing all information.

**2.** Develop options for basic scans (basic scan), full scans (full scan), passive scans (passive scan), and web scans (web scan)

Save scan results in separate files for each IP address or URL**.3**

**4.** Test weak credentials using hydra and save the results in designated files

**5.** Use searchsploit to identify potential exploits and display the results

Option to save all scan results in a ZIP file based on user preference**.6**

**7.**  Allow the user to search through saved scan results from previous scans

****

**Advanced Manual:**

**Workflow**

**Create Working Directory**

**Data Management**

- At the beginning of the script execution, the user is prompted to define a name for the folder where all information will be stored

The directory is created on the desktop under a fixed name, BC\_PT-DB-

**Activate Anonymous**

‏The tool include the ability to enable anonymity by selecting option A from the script menu. Using geoiplookup, tor, and nipe software automatic install them if they dont installed , the user will be able to set anonymously. The public IP address and geographic location of the ip user will be displayed to them, and they can choose to disable anonymity using flag A -S. The option to enable or disable anonymity. part of the user-friendly interface and operation of the tool.

**Network Scanning**

**Basic Scan**

- TCP scanning with nmap using the command `nmap -sV -p- to display the actual service running on each port, preventing errors where a port number might be used for a non-standard service. Results are saved in the file tcp\_$ip

****

- UDP scanning with masscan fast scan for all open ports,and then followed by to nmap -sV -sU -p to the open ports from massscan scan for the open ports and real services with nmap, and saving the results in the file udp\_$ip

**Basic Scan && Full Scan Include: Weak Credentials Testing**

file Using hydra to test weak credentials with default usernames

(user, admin, administrator, root)

Using a default password file (John pass list)

or a custom file defined by the user for password file or users file

Services: SSH, RDP, FTP, Telnet, SMB

Option to reselect the default file if the user changes their mind after choosing a custom file for users or passwords

Saving the test results if found weak credentials in the file: Found-BF\_$IP` for each IP address

****

**Full Scan**

- Performed Basic Scan + vulnerability scan

Additional scans with nmap -sV -p- all ports --script=vuln NSE Scripting engine for TCP and UDP services

Saving the results in the files vuln\_tcp\_$ip and vuln\_udp\_$ip

Using searchsploit to identify potential exploits and saving the results in the files searchsploit\_tcp\_$ip and searchsploit\_udp\_$ip

**Passive Scan**

- Performing a passive scan to collect information without the target knowing they are being scanned.

- Using Whois and the website [ipinfo](https://ipinfo.io) to gather information

Displaying the collected information to the user and saving it in the file `Passive\_$ip` within a subdirectory named by the user in the BC\_PT-DB folder.

.

- ****

**Web Scan**

- Scanning websites via http or https using the dirb tool.

- Saving the scan results in the file `dirb\_scan.txt` and displaying the information to the user.

- Additional scanning with the nikto tool and saving the results in the file `nikto\_scan.txt`.

- ****

**Saving Scan Results**

After each scan type, the tool asks the user if they want to save the results in a ZIP file.

- If the user agrees, the results are compressed and saved in a ZIP file in the appropriate directory.

- There is an option to search through saved scan results from previous scans according to user preference.

**Project Results**

- An automated penetration testing tool was successfully developed, capable of performing complex network scans, passive scans, and web scans.

- Scan results are stored in designated directories and clearly displayed to the user.

- Tests identified several weak passwords and vulnerabilities, which are presented to the user for immediate remediation.

- ****

Passive scanning provides additional information about the network and addresses without detection by the target.

- Web scans provide critical information on website vulnerabilities and exploitable points.

- Option to save all scan results in a ZIP file based on user preference, facilitating convenient information management.

- Option to search through saved scan results from previous scans according to user preference, allowing quick access to important information.

**Conclusions and Recommendations**

- The developed tool offers an efficient solution for penetration testing, passive scans, and web scans.

****

**Help Menu**

**[\*] DB FILE IS: BC\_PT-DB (Located at: Desktop)**

**[\*] Input Format for Scanning:**

**- Enter an IP address to scan a single host.**

**Example: 10.10.10.10**

**- Enter an IP address with CIDR notation to specify a range for scanning.**

**Example: 10.10.10.0/24**

**- Enter a range of IP addresses in the format start-end to specify multiple hosts.**

**Example: 192.168.1.100-150**

**[\*] Input Format for Web Scan:**

**- Enter the target URL or IP address in the format [HTTP/HTTPS]://[TARGET].**

**Example: http://10.10.10.10 or https://example.com**

**[\*] Anonymous IP Activation:**

**- Check if necessary dependencies (geoip-bin, tor, nipe) are installed.**

**- If not, install them.**

**- Check if the user is anonymous. If not, activate the anonymous IP using nipe.**

**+ A will activate Anonymous ip**

**- -S Will stop your Anonymous ip**

**Example: A -S**

**[\*] Additional Scanning Options:**

**[\*] Basic Scan:**

**Scans the network for TCP using Nmap and UDP using Masscan, including the service version and weak passwords.**

**- Utilizing HYDRA for weak credentials. The default password file is located at: /usr/share/commix/src/txt/passwords\_john.txt**

**- Default user list includes: administrator, kali, root, user, admin**

**- Services: SSH, RDP, FTP, Telnet, SMB**

**- -V VERBOSE MODE**

**Example: B -V**

**[\*] Full Scan:**

**- Includes all functionalities of BASIC SCAN, plus vulnerability analysis using Nmap Scripting Engine (NSE)**

**and search for exploits using searchsploit.**

**- -V VERBOSE MODE**

**Example: F -V**

**[\*] Passive Scan:**

**- Execute a passive scan to gather information without directly interacting with the target.**

**Example: Passive scan (P) using whois and ipinfo.com tools.**

**[\*] Web Scan:**

**- Initiate a web scan to analyze web-based services and vulnerabilities.**

**using dirb and nikto tools.**

**CREDITS :**

**LOGO CREDIT**: <https://smashinglogo.com>

****

****

****

****

****

****

****

****

****

****

****

****

****

****