



PROJECT: PENETRATION TESTING

NAME: BAREL COHEN

JohnBryce&ThinkCyber

© Barel Cohen 2024 BC PT [Version: s.8]

MY PT PROJECT: BC PT

Framework

Penetration Testing Project Report - Summary

Information.....	1-2
Manual.....	3
Summery and Introduction.....	4
Advanced Manual.....	5-8
Details of the tool.....	9-13
See the tool in action.....	14-35
Conclusions.....	36
Link to video.....	37
Logo Credit.....	38

MANUAL:

1)

HOW TO RUN THE TOOL - (FrameWork 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 look 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

Nmap scan with NSE script engine vulnerability

-sV(Real Service if was a manipulation on a fixed port) for tcp and udp if found by Masscan Nmap results searching in searchsploit

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

Enumerating Scan Using the enum4linux tool

Project Summary: BC PT

Introduction

The BC_PT project is a framework that focuses on Penetration Testing of computer networks and websites. The project's goal is to develop an automated framework tool for penetration testing that includes basic and full scans of TCP and UDP protocol's networks, passive scans for non-intrusive information gathering, web scan, and enumerating scan . The tool utilizes open-source utilities like nmap, masscan ,searchsploit, hydra, dirb, nikto, enum4linux 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+ Log file BC_PT.log on /var/log/
- 2.** Develop options for basic scans (basic scan), full scans (full scan), passive scans (passive scan), web scans (web scan), enumerating scan
- 3.** Save scan results in separate files for each IP address or URL
- 4.** Test weak credentials using hydra and save the results in designated files
- 5.** Use searchsploit to identify potential exploits and display the results
- 6.** Option to save all scan results in a ZIP file based on user preference
- 7.** Allow the user to search through saved scan results from previous scans



Advanced Manual:

Workflow

The screenshot shows two terminal windows. The top window displays the initial setup of the BC_PT framework on a Kali Linux system, showing the command `./BC_PT.sh` being run with root privileges. The bottom window shows the main menu of the BC_PT framework, listing various scanning options and credits to Barel Cohen and Natalie Erez.

```
kali@192: ~/Desktop
File Actions Edit View Help
[~] kali@192:~/Desktop
↳ sudo ./BC_PT.sh
[sudo] password for kali:
[*]Checking your permissions...
[★] You Are With root Permissions
[*] Starting the BC_PT Framework console..-
```



```
File Actions Edit View Help
kali@192: ~/Desktop
[~] kali@192:~/Desktop
[!] P[RE]SCAN
[!] F[ULL]SCAN
[!] P[ASSIVE]SCAN
[!] W[EB]SCAN
[!] E[NUMERATING]SCAN
[!] V[IEW]LOGFILE
[!] S[earch]RESULTS
[-h] H[elp]
C[lear]

Documentation: https://github.com/Barel-cohen/BC_PT
[NAME: BAREL COHEN] [s8] [TEACHER: NATALIE EREZ]
Penetration_Testing 🔒
BC_PT [Version: s.8]
© 2024 Barel Cohen.

[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive Scan
W) Web Scan
E) Enumerating Scan
V) View Log File
S) Search Results
-h) Help
C) Clear
EX) Exit BC_PT Penetration Testing
bc_pt> |
```

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

Logging and Auditing for BC_PT

The BC_PT framework now incorporates robust logging and auditing capabilities to provide security managers with detailed records of penetration testing activities. This enhancement is facilitated through the integration of a dedicated log file, located at /var/log/BC_PT.log

Log File Details

The log file meticulously records essential information for each scan executed within the framework, including:

Timestamp: The precise date and time at which the scan was finished

Scan Type: The specific type of scan performed (Basic Scan, Full Scan+ [Fast, Verbose], Web Scan, Passive Scan, Enumeration Scan)

Target Information

For network scans: The IP address or range of IP addresses targeted in the scan

For web scans: The URL of the scanned web application

For passive scans: The target address/range for information gathering

Anonymity Status: If anonymity is activated or disabled, the log records the country associated with the anonymous IP address and the anonymous IP itself, or the real IP and country if choose disabled

Directory: The name of the directory where the scan results are stored



Benefits of Enhanced Logging

The inclusion of detailed logging offers several key advantages for security managers/penetration testers:

Activity Tracking: Maintain a chronological record of all penetration tests conducted, aiding in identifying trends and patterns in security assessments

Post-Scan Analysis: Facilitate in-depth analysis of scan results over time, enabling comparisons between different assessments and tracking the progress of remediation efforts

By incorporating this enhanced logging functionality, BC_PT ensures that security managers/penetration testers have a comprehensive and auditable record of all penetration testing performed, bolstering their ability to make informed security decisions and maintain a robust security posture

Activate Anonymous

The tool include the ability to enable anonymity by selecting option A from the script menu. Using geolookup, tor, and nipe software automatic install them if they don't 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.

Extra explanation of the anonymous process: The Ip address of your private device receives 3 different Ip addresses using the TOR && Nipe tool, and it will look like this for example: 80.80.80.80 Your real ip -> 55.55.55.55 TOR ip changed -> 70.70.70.70 TOR ip changed -> 100.100.100.100 TOR Ip last that visible

***NOTE:** These services, such as TOR and NIPE, are designed to conceal the user's true IP address and provide a level of privacy and anonymity. However, it's important to understand that no anonymous IP address can provide absolute anonymity.

These services can provide a high level of privacy during their use, as they offer encrypted connections and data traffic in an encrypted and protected manner. However, there is still a small possibility that attacks could compromise anonymity and identify the user, especially when using the services to engage in illegal activities or harm others.

TIP: (You can use VPN, Proxy, Agents for More layers of Anonymous)

Network Scanning

Basic Scan

- TCP scanning with nmap using the command `nmap -sV -p-` to display the actual service running on each port, preventing manipulation errors where a fixed 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 `nmap -sV -sU -p <open_ports>` to the open ports from masscan 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

Using hydra to test weak credentials with default usernames file

(user, admin, administrator, root)

Using a default passwords file (John Pass list -
`/usr/share/commix/src/txt/passwords_john.txt`)

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

Services: SSH, RDP, FTP, 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

Searchsploit is a critical tool in cybersecurity, used for vulnerability assessment and exploitation. It searches the Exploit-DB database for attack codes, exploits, and payloads, providing detailed information on potential vulnerabilities. It's essential for security researchers and professionals to identify and mitigate security risks effectively.

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'.

Enumerating Scan

Scanning with Enum4linux. is a tool used to gather information from Windows and Samba systems via the SMB (Server Message Block) protocol. collect details about users, shared resources, groups, password policies, operating systems, and more.

Key Features:

Gathering information about users and groups

Identifying network shares and resources

Retrieving password policy details

Detecting operating system and security identifiers (SIDs)

Supported Systems:

Windows systems

Samba systems (on Linux and UNIX)

Saved the collected data as Enum_ \$IP

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

Search: 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, web scans and enumerating scan.

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

Basic & Full Scan Scanning TCP and UDP ports and Tests services - identified weak credentials

Full Scan+ Scanning vulnerabilities & Exploits 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

Enumerating Scan provide Information of the target that can be useful specially to the Brute force you can fit the Users and passwords to the policies if found

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

Tool in Action: Demonstration with Images

Activate Anonymous

The screenshot shows a terminal window titled 'kali@192: ~/Desktop'. The title bar includes 'File Actions Edit View Help'. The main area displays the BC_PT tool interface with the following text:

Documentation: https://github.com/Barel-cohen/BC_PT
[NAME: BAREL COHEN] [s8] [TEACHER: NATALIE EREZ]
Penetration Testing 🔒 ⓘ
BC_PT [Version: s.8]
© 2024 Barel Cohen.

[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive Scan
W) Web Scan
E) Enumerating Scan
V) View Log File
S) Search Results
-h) Help
C) Clear
EX) Exit BC_PT Penetration Testing

bc_pt> A
[*]geoip-bin:[✓]
[*]tor:[✓]

bc_pt> A
[*]geoip-bin:[✓]
[*]tor:[✓]
[*]nipe:[✓]

Checking Anonymos ...

% Total % Received % Xferd Average Speed Time Time Current
 Dload Upload Total Spent Left Speed
100 13 100 13 0 0 44 0 --::-- --::-- --::-- 44
[*]IP: 77.137.69.249
% Total % Received % Xferd Average Speed Time Time Current
 Dload Upload Total Spent Left Speed
100 13 100 13 0 0 59 0 --::-- --::-- --::-- 59
[*]You are not anonymous!
[*]start activated nipe anonymous ...
[+] Status: true
[+] Ip: 107.189.28.199
[*]YOU GET ANONYMOS
[*]your anonymos country: Luxembourg
[2024-06-07 14:38:48] [Anonymity Activated] [IP: 107.189.28.199] [Country: Luxembourg]
[*]Select Your Choice From The Menu:

Stop Anonymous

```
bc_pt> A -S
[*]geoip-bin:[ ✓ ]
[*]tor:[ ✓ ]
[*]nipe:[ ✓ ]

Checking Anonymos ...
*****
% Total    % Received % Xferd  Average Speed   Time   Time     Time Current
          Dload  Upload   Total Spent  Left Speed
100  14  100  14    0     0  11      0 0:00:01 0:00:01 --:--:-- 11
[*]IP: 192.42.116.199
% Total    % Received % Xferd  Average Speed   Time   Time     Time Current
          Dload  Upload   Total Spent  Left Speed
100  14  100  14    0     0    9      0 0:00:01 0:00:01 --:--:-- 9
You are anonymous
[*]stop nipe anonymos ...

[+] Status: false
[+] Ip: 77.137.69.249

Success stoped anonymous
[*]your country: Israel
[ 2024-06-07 14:45:45 ] [ Anonymity Disabled ] [ IP: 77.137.69.249 ] [ Country: Israel ]

[*]Select Your Choice From The Menu:
```

```
bc_pt> A -S
[*]geoip-bin:[ ✓ ]
[*]tor:[ ✓ ]
[*]nipe:[ ✓ ]

Checking Anonymos ...
*****
% Total    % Received % Xferd  Average Speed   Time   Time     Time Current
          Dload  Upload   Total Spent  Left Speed
100  13  100  13    0     0   26      0 --:--:-- --:--:-- --:--:-- 26
[*]IP: 77.137.69.249
% Total    % Received % Xferd  Average Speed   Time   Time     Time Current
          Dload  Upload   Total Spent  Left Speed
100  13  100  13    0     0    59      0 --:--:-- --:--:-- --:--:-- 60
[*]You are not anonymous
[*]your country: Israel
[ 2024-06-07 14:46:39 ] [ Anonymity Disabled ] [ IP: 77.137.69.249 ] [ Country: Israel ]

[*]Select Your Choice From The Menu:
```

Help Manual Anonymous

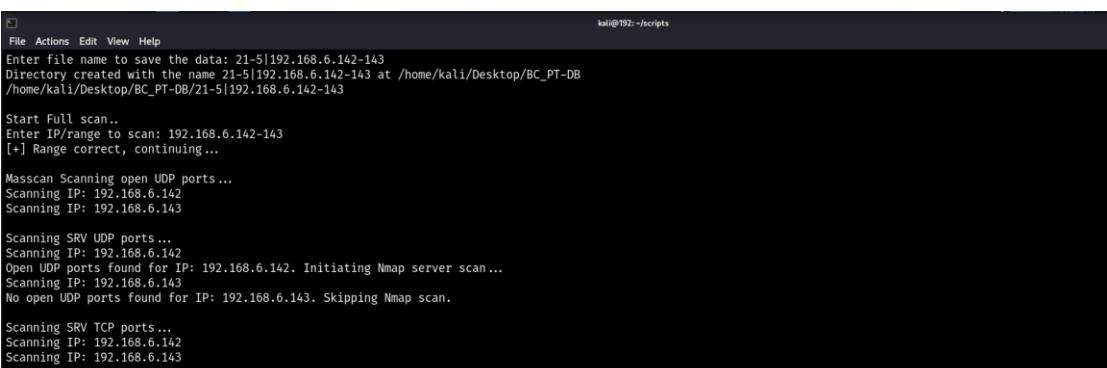
```
[*] Anonymous IP Activation:
- Check if necessary dependencies (geoip-bin, tor, nipe) are installed.
- If not, install them.
- Check if the user is anonymous. If not, activate the anonymous IP using nipe.
+ A will activate Anonymous ip
- -S Will stop your Anonymous ip
Example: A -S
```

Basic & Full Scan



Documentation:https://link-to-video
[NAME: BAREL COHEN] [s8] [TEACHER: NATALIE EREZ]
Penetration Testing 🔒🌐
BC_PT [Version: s.8]
© 2024 Barel Cohen.

[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive Scan
W) Web Scan
S) Search Results
-h) Help
C) Clear
E) Exit BC_PT Penetration Testing
bc_pt> F
DB file is: /home/kali/Desktop/BC_PT-DB
Enter file name to save the data: 21-5|192.168.6.142-143
Directory created with the name 21-5|192.168.6.142-143 at /home/kali/Desktop/BC_PT-DB



File Actions Edit View Help
kali@192: ~/scripts
Enter file name to save the data: 21-5|192.168.6.142-143
Directory created with the name 21-5|192.168.6.142-143 at /home/kali/Desktop/BC_PT-DB
/home/kali/Desktop/BC_PT-DB/21-5|192.168.6.142-143

Start Full scan..
Enter IP/range to scan: 192.168.6.142-143
[:+] Range correct, continuing...
Masscan Scanning open UDP ports ...
Scanning IP: 192.168.6.142
Scanning IP: 192.168.6.143

Scanning SRV UDP ports ...
Scanning IP: 192.168.6.142
Open UDP ports found for IP: 192.168.6.142. Initiating Nmap server scan...
Scanning IP: 192.168.6.143
No open UDP ports found for IP: 192.168.6.143. Skipping Nmap scan.

Scanning SRV TCP ports ...
Scanning IP: 192.168.6.142
Scanning IP: 192.168.6.143

If Open udp ports found with masscan will move to scan with nmap if not skip nmap

User-Friendly Customization: Choosing User and Password Files

you can choose your own users file or passwords file

If you cant find them / or regret and want to use the default you still can after you choose your own instead start from the begin of the scan

```
Starting Brute Force on Services tried weak credentials
Do you want to use your own users file? (y/n): Y
Please enter 'y' or 'n': y
Enter the path to your users file: bdd
Enter the path to your users file [or press D for default users file]: D
Do you want to use your own password file? (y/n): y
Enter the path to your password file: gfs
File not found. Please enter a valid path to your password file.
Enter the path to your password file [you can use the /usr/share/commix/src/txt/passwords_john.txt]: /usr/share/commix/src/txt/passwords_john.txt

Starting Brute Force on Services [smb-rdp-ftp-telnet-ssh]
Hydra trying weak credentials for smb on 192.168.6.142. It's crucial to have strong passwords for security.
Hydra trying weak credentials for rdp on 192.168.6.142. It's crucial to have strong passwords for security.
```

Brute Force checking weak credentials

```
File Actions Edit View Help                               kali@192: ~/scripts
Scanning IP: 192.168.6.142
Open UDP ports found for IP: 192.168.6.142. Initiating Nmap server scan...
Scanning IP: 192.168.6.143
No open UDP ports found for IP: 192.168.6.143. Skipping Nmap scan.

Scanning SRV TCP ports...
Scanning IP: 192.168.6.142
Scanning IP: 192.168.6.143

Starting Brute Force on Services tried weak credentials
Do you want to use your own users file? (y/n): n
Do you want to use your own password file? (y/n): n

Starting Brute Force on Services [smb-rdp-ftp-ssh]
Hydra trying weak credentials for smb on 192.168.6.142. It's crucial to have strong passwords for security.
Hydra trying weak credentials for rdp on 192.168.6.142. It's crucial to have strong passwords for security.
Hydra trying weak credentials for ftp on 192.168.6.142. It's crucial to have strong passwords for security.
Hydra trying weak credentials for ssh on 192.168.6.142. It's crucial to have strong passwords for security.

Found weak credentials, saves at FOUND-BF_192.168.6.142.txt
+-----+
| Service | Host | Login |
+-----+
[445][smb] host: 192.168.6.142    login: msfadmin    password: msfadmin
[21][ftp] host: 192.168.6.142    login: msfadmin    password: msfadmin

Hydra trying weak credentials for smb on 192.168.6.143. It's crucial to have strong passwords for security.
Hydra trying weak credentials for rdp on 192.168.6.143. It's crucial to have strong passwords for security.
Hydra trying weak credentials for ftp on 192.168.6.143. It's crucial to have strong passwords for security.
Hydra trying weak credentials for ssh on 192.168.6.143. It's crucial to have strong passwords for security.

Not found weak credentials for 192.168.6.143
```

Move the mouse pointer inside or press Ctrl+G

Help Manual Basic & Full Scan

```
[*] 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, SMB
- -V VERBOSE MODE
  Example: B -V
- -F FAST SCAN
- B -FV / -VF Fast & Verbose

[*] 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
- -F FAST SCAN
- F -FV / -VF Fast & Verbose
```

-V Will show also the results of the tcp and udp nmap scan on the screen

(Verbose)

```
kali@192: ~/scripts
File Actions Edit View Help
bc_pt> B -VF
DB file is: /home/kali/Desktop/BC_PT-DB

Enter file name to save the data: 31-5:Basic-VF
Directory created with the name 31-5:Basic-VF at /home/kali/Desktop/BC_PT-DB
/home/kali/Desktop/BC_PT-DB/31-5:Basic-VF

Start Fast & Verbose Basic Scan..
Enter IP/range to scan: 192.168.6.142-143
[+] Range correct, continuing ...

Masscan Scanning open UDP ports ...
Scanning IP: 192.168.6.142
Scanning IP: 192.168.6.143

Scanning SRV UDP ports ...
Scanning IP: 192.168.6.142
Open UDP ports found for IP: 192.168.6.142. Initiating Nmap server scan ...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 13:54 IDT
Nmap scan report for 192.168.6.142
Host is up (0.0021s latency).

PORT      STATE SERVICE      VERSION
53/udp    open  domain      ISC BIND 9.4.2
137/udp   open  netbios-ns  Microsoft Windows netbios-ns (workgroup: WORKGROUP)
MAC Address: 00:0C:29:1E:C1:D2 (VMware)
Service Info: Host: METASPOITABLE; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.94 seconds
Scanning IP: 192.168.6.143
No open UDP ports found for IP: 192.168.6.143. Skipping Nmap scan.

Move the mouse pointer inside or press Ctrl+G.
```

```
kali@192: ~/scripts
File Actions Edit View Help

Scanning SRV TCP ports ...
Scanning IP: 192.168.6.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 13:54 IDT
Nmap scan report for 192.168.6.142
Host is up (0.0055s latency).
Not shown: 65504 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp       vsftpd 2.3.4
22/tcp    open  ssh       OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet    Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain    ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind  2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login    OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql    MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc      VNC (protocol 3.3)
6000/tcp  open  X11      (access denied)
6200/tcp  open  lm-x?

Scanning IP: 192.168.6.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 13:57 IDT
Nmap done: 1 IP address (0 hosts up) scanned in 1.71 seconds

Starting Brute Force on Services tried weak credentials
Do you want to use your own users file? (y/n): n
Do you want to use your own password file? (y/n): n

Starting Brute Force on Services [smb-rdp-ftp-ssh]
Hydra trying weak credentials for smb on 192.168.6.142. It's crucial to have strong passwords for security.
```

End Basic Scan

Zip the result?

```
kali@192: ~/scripts
File Actions Edit View Help
Scanning SRV TCP ports ...
Scanning IP: 192.168.6.142
Scanning IP: 192.168.6.143

Starting Brute Force on Services tried weak credentials
Do you want to use your own users file? (y/n): n
Do you want to use your own password file? (y/n): n

Starting Brute Force on Services [smb-rdp-ftp-ssh]
Hydra trying weak credentials for smb on 192.168.6.142. It's crucial to have strong passwords for security.
Hydra trying weak credentials for rdp on 192.168.6.142. It's crucial to have strong passwords for security.
Hydra trying weak credentials for ftp on 192.168.6.142. It's crucial to have strong passwords for security.
Hydra trying weak credentials for ssh on 192.168.6.142. It's crucial to have strong passwords for security.

Found weak credentials, saves at FOUND-BF_192.168.6.142.txt
+-----+
| Service | Host | Login |
+-----+
[445][smb] host: 192.168.6.142 login: msfadmin password: msfadmin
[21][ftp] host: 192.168.6.142 login: msfadmin password: msfadmin

Hydra trying weak credentials for smb on 192.168.6.143. It's crucial to have strong passwords for security.
Hydra trying weak credentials for rdp on 192.168.6.143. It's crucial to have strong passwords for security.
Hydra trying weak credentials for ftp on 192.168.6.143. It's crucial to have strong passwords for security.
Hydra trying weak credentials for ssh on 192.168.6.143. It's crucial to have strong passwords for security.

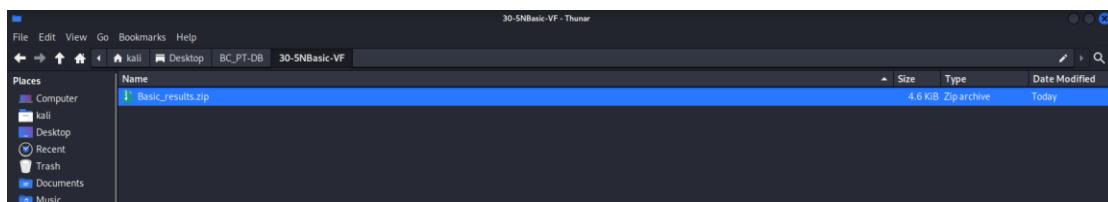
Not found weak credentials for 192.168.6.143

Do you want to zip the scan results? (y/n): y
*inside or press Ctrl+G.
```

*Note:

The Files Called BF_ \$IP.txt Are for the user can see the progress of BF

The Files FOUND-BF_ \$IP.txt Are Saving The Weak Credentials if Found



```
(kali㉿192) [~/Desktop/BC_PT-DB/30-SNBasic-VF]
$ sudo unzip Basic_results.zip
[sudo] password for kali:
1
Sorry, try again.
[sudo] password for kali:
Archive:  Basic_results.zip
  inflating: BF_192.168.6.142.txt
  inflating: BF_192.168.6.143.txt
  inflating: FOUND-BF_192.168.6.142.txt
  extracting: FOUND-BF_192.168.6.143.txt
  inflating: sv-udp_192.168.6.142.txt
  inflating: tcp_192.168.6.142.txt
  inflating: tcp_192.168.6.143.txt
```

Full Scan (+ Vulnerabilities)

Start Vulnerability's Scan UDP Ports If found open

```
Scanning for vulnerabilities for 192.168.6.142 services udp ports...
Scanning IP: 192.168.6.142
Open UDP ports found for IP: 192.168.6.142. Initiating Nmap server scan...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 19:29 IDT
Nmap scan report for 192.168.6.142
Host is up (0.0066s latency).

PORT      STATE SERVICE      VERSION
53/udp    open  domain      ISC BIND 9.4.2
| vulners:
|_ cpe:/a:isc:bind:9.4.2:
|   SSV:2853      10.0  https://vulners.com/seebug/SSV:2853      *EXPLOIT*
|   PRION:CVE-2008-0122  10.0  https://vulners.com/prion/PRION:CVE-2008-0122
|   SSV:60184      8.5   https://vulners.com/seebug/SSV:60184      *EXPLOIT*
|   PRION:CVE-2012-1667  8.5   https://vulners.com/prion/PRION:CVE-2012-1667
|   CVE-2012-1667  8.5   https://vulners.com/cve/CVE-2012-1667
|   SSV:60292      7.8   https://vulners.com/seebug/SSV:60292      *EXPLOIT*
|   PRION:CVE-2014-8500  7.8   https://vulners.com/prion/PRION:CVE-2014-8500
|   PRION:CVE-2012-5166  7.8   https://vulners.com/prion/PRION:CVE-2012-5166
|   PRION:CVE-2012-4244  7.8   https://vulners.com/prion/PRION:CVE-2012-4244
|   PRION:CVE-2012-3817  7.8   https://vulners.com/prion/PRION:CVE-2012-3817
|   CVE-2014-8500      7.8   https://vulners.com/cve/CVE-2014-8500
|   CVE-2012-5166      7.8   https://vulners.com/cve/CVE-2012-5166
|   CVE-2012-4244      7.8   https://vulners.com/cve/CVE-2012-4244
|   CVE-2012-3817      7.8   https://vulners.com/cve/CVE-2012-3817
|   CVE-2008-4163      7.8   https://vulners.com/cve/CVE-2008-4163
|   PRION:CVE-2010-0382  7.6   https://vulners.com/prion/PRION:CVE-2010-0382
|   CVE-2010-0382      7.6   https://vulners.com/cve/CVE-2010-0382
|   EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2  7.2   https://vulners.com/exploitpack/EXPLOITPACK:D6DDF5E24DE171DAAD71FD95FC1B67F2
*EXPLOIT*
|   EDB-ID:42121      7.2   https://vulners.com/exploitdb/EDB-ID:42121      *EXPLOIT*
|   CVE-2017-3141      7.2   https://vulners.com/cve/CVE-2017-3141
|   PRION:CVE-2015-8461  7.1   https://vulners.com/prion/PRION:CVE-2015-8461
```

Nmap scanning NSE script engine- vuln, then to Searchsploit

```
kali@kali:~/Desktop$ nmap -p- --script vuln 192.168.6.142
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-30 19:30 IDT
Nmap done: 1 IP address (1 host up) scanned in 12.65 seconds
[+] Searchsploit's XML mode (without verbose enabled). To enable: searchsploit -v --xml...
[+] Reading: 'nmap_udp_vuln_scan_192.168.6.142.xml'

[+] /usr/bin/searchsploit -t --json domain
[-] Skipping output: domain (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t --json domain)

[i] /usr/bin/searchsploit -t --json isc_bind
[i] /usr/bin/searchsploit -t --json isc_bind 9.4.2
[i] /usr/bin/searchsploit -t --json netbios_ns
[i] /usr/bin/searchsploit -t --json microsoft_windows_netbios_ns
Vulnerabilities Saved at searchsploit_udp_results_192.168.6.142.txt :
{
  "SEARCH": "isc bind",
  "DB_PATH_EXPLOIT": "/usr/share/exploitdb",
  "RESULTS_EXPLOIT": [
    {
      "NAME": "isc_bind_9.4.2_exploit",
      "DESCRIPTION": "Exploit for ISC BIND 9.4.2 vulnerability (CVE-2008-0122).",
      "URL": "https://www.exploit-db.com/wp-content/themes/exploit/exploits/1224/isc_bind_9.4.2_exploit.py"
    }
  ]
}

the mouse pointer is idle or press Ctrl+C
```

```

kali@192:~/scripts
File Actions Edit View Help
MAC Address: 00:0C:29:1E:C1:D2 (VMware)
Service Info: Host: METASPLOITABLE; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.57 seconds
[i] SearchSploit's XML mode (without verbose enabled). To enable: searchsploit -v --xml ...
[i] Reading: 'nmap_udp_vuln_scan_192.168.6.142.xml'

[i] /usr/bin/searchsploit -t --json domain
[-] Skipping output: domain (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t --json domain)

[i] /usr/bin/searchsploit -t --json isc bind
[i] /usr/bin/searchsploit -t --json isc bind 9.4.2
[i] /usr/bin/searchsploit -t --json netbios ns
[i] /usr/bin/searchsploit -t --json microsoft windows netbios ns
Vulnerabilities Saved at searchsploit_udp_results_192.168.6.142.txt :
{
    "SEARCH": "isc bind",
    "DB_PATH_EXPLOIT": "/usr/share/exploitdb",
    "RESULTS_EXPLOIT": [
        {
            "Title": "ISC BIND (Linux/BSD) - Remote Buffer Overflow (1)",
            "EDB-ID": "19111",
            "Date_Published": "1998-04-08",
            "Date_Added": "1998-04-08",
            "Date_Updated": "2017-09-08",
            "Author": "ROTHB",
            "Type": "remote",
            "Platform": "linux",
            "Port": "",
            "Verified": "1",
            "Codes": "OSVDB-913;CVE-1999-0009",
            "Tags": "",
            "Aliases": "",
            "Screenshot": ""
        }
    ]
}

```

Move the mouse pointer inside or press Ctrl+G.

If not found open UDP ports Skipping

```

Scanning for vulnerabilities for 192.168.6.143 services udp ports ...
Scanning IP: 192.168.6.143
No open UDP ports found for IP: 192.168.6.143. Skipping Nmap scan.

```

Scan TCP ports Vulnerability's

```

kali@192:~/scripts
File Actions Edit View Help
Scanning for vulnerabilities for 192.168.6.142 services tcp ports...
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-30 19:30 IDT
Nmap scan report for 192.168.6.142
Host is up (0.0048s latency).
Not shown: 65504 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| vulners:
|   cpe:/a:vsftpd:vsftpd:2.3.4:
|     PRION:CVE-2011-2523 10.0  https://vulners.com/prion/PRION:CVE-2011-2523
|     EDB-ID:49757 10.0  https://vulners.com/exploitdb/EDB-ID:49757 *EXPLOIT*
|     1337DAY-ID-36095 10.0  https://vulners.com/zdt/1337DAY-ID-36095 *EXPLOIT*
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|     SSV:78173 7.8  https://vulners.com/seebug/SSV:78173 *EXPLOIT*
|     SSV:69983 7.8  https://vulners.com/seebug/SSV:69983 *EXPLOIT*
|     EDB-ID:24450 7.8  https://vulners.com/exploitdb/EDB-ID:24450 *EXPLOIT*
|     EDB-ID:15215 7.8  https://vulners.com/exploitdb/EDB-ID:15215 *EXPLOIT*
|     SECURITYVULNS:VULN:8166 7.5  https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|     PRION:CVE-2010-4478 7.5  https://vulners.com/prion/PRION:CVE-2010-4478
|     CVE-2010-4478 7.5  https://vulners.com/cve/CVE-2010-4478
|     SSV:20512 7.2  https://vulners.com/seebug/SSV:20512 *EXPLOIT*
|     PRION:CVE-2011-1013 7.2  https://vulners.com/prion/PRION:CVE-2011-1013
|     PRION:CVE-2008-1657 6.5  https://vulners.com/prion/PRION:CVE-2008-1657
|     CVE-2008-1657 6.5  https://vulners.com/cve/CVE-2008-1657
|     SSV:60656 5.0  https://vulners.com/seebug/SSV:60656 *EXPLOIT*
|     PRION:CVE-2011-2168 5.0  https://vulners.com/prion/PRION:CVE-2011-2168
|     PRION:CVE-2010-5107 5.0  https://vulners.com/prion/PRION:CVE-2010-5107
|     CVE-2010-5107 5.0  https://vulners.com/cve/CVE-2010-5107

```

Nmap results to Searchsploit

```
kali@192:~/scripts
File Actions Edit View Help
|     Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|     References:
|     https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
53834/tcp open  status      1 (RPC #100024)
56526/tcp open  mountd    1-3 (RPC #100005)
MAC Address: 00:0C:29:1E:C1:D2 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
[_]_smb-vuln-ms10-054: false
[_]_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)
[_]_smb-vuln-ms10-061: false

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 512.71 seconds
[i] SearchSploit's XML mode (without verbose enabled). To enable: searchsploit -v --xml...
[i] Reading: ['nmap_vuln_scan_192.168.6.142.xml']

[-] Skipping term: ftp  (Term is too general. Please re-search manually: /usr/bin/searchsploit -t --json ftp)

[i] /usr/bin/searchsploit -t --json vsftpd
[i] /usr/bin/searchsploit -t --json vsftpd 2.3.4
[-] Skipping term: ssh  (Term is too general. Please re-search manually: /usr/bin/searchsploit -t --json ssh)

[i] /usr/bin/searchsploit -t --json openssh
[i] /usr/bin/searchsploit -t --json openssh 4.7p1 debian 8ubuntu1
[i] /usr/bin/searchsploit -t --json telnet
[i] /usr/bin/searchsploit -t --json linux telnetd
[i] /usr/bin/searchsploit -t --json smtp
[-] Skipping output: smtp  (Too many results, 100+. You'll need to force a search: /usr/bin/searchsploit -t --json smtp)

[i] /usr/bin/searchsploit -t --json postfix smtpd
[i] /usr/bin/searchsploit -t --json domain
[

we the mouse pointer inside or press Ctrl+G.
```

```
kali@192:~/scripts
File Actions Edit View Help
[i] /usr/bin/searchsploit -t --json status 1
[i] /usr/bin/searchsploit -t --json mountd 1 3
Vulnerabilities Saved at searchsploit_results_192.168.6.142.txt :
{
  "SEARCH": "vsftpd",
  "DB_PATH_EXPLOIT": "/usr/share/exploitdb",
  "RESULTS_EXPLOIT": [
    {
      "Title": "vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption",
      "EDB-ID": "5814",
      "Date_Published": "2008-06-14",
      "Date_Added": "2008-06-13",
      "Date_Updated": "2016-12-07",
      "Author": "Praveen Darshanam",
      "Type": "dos",
      "Platform": "linux",
      "Port": "",
      "Verified": "1",
      "Codes": "CVE-2007-5962",
      "Tags": "",
      "Aliases": "",
      "Screenshot": "",
      "Application": "http://www.exploit-db.comvsftpd-2.0.5.tar.gz",
      "Source": "",
      "Path": "/usr/share/exploitdb/exploits/linux/dos/5814.pl"
    },
    {
      "Title": "vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)",
      "EDB-ID": "31818",
      "Date_Published": "2008-05-21",
      "Date_Added": "2008-05-21",
      "Date_Updated": "2016-12-07",
      "Author": "Martin Nagy",
      "Type": "dos",
      "Platform": "windows",
      "Port": ""
    }
  ]
}

we the mouse pointer inside or press Ctrl+G.
```

```
kali@192: ~/scripts
File Actions Edit View Help

XPath set is empty
No vulnerabilities found for 192.168.6.143

Do you want to zip the scan results? (y/n): y
adding: nmap_udp_vuln_scan_192.168.6.142.txt (deflated 78%)
adding: nmap_udp_vuln_scan_192.168.6.142.xml (deflated 88%)
adding: nmap_vuln_scan_192.168.6.142.txt (deflated 85%)
adding: nmap_vuln_scan_192.168.6.142.xml (deflated 90%)
adding: nmap_vuln_scan_192.168.6.143.txt (deflated 10%)
adding: nmap_vuln_scan_192.168.6.143.xml (deflated 46%)
adding: searchsploit_results_192.168.6.142.txt (deflated 87%)
adding: searchsploit_results_192.168.6.143.txt (stored 0%)
adding: searchsploit_udp_results_192.168.6.142.txt (deflated 85%)
adding: sv-udp_192.168.6.142.txt (deflated 31%)
adding: tcp_192.168.6.142.txt (deflated 50%)
adding: tcp_192.168.6.143.txt (deflated 10%)
Scan results zipped to Full-Verbose_results.zip

[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive Scan
W) Web Scan
E) Enumerating Scan
S) Search Results
-h) Help
C) Clear

EX) Exit BC_PT Penetration Testing
bc_pt> █
```

Log File

```
kali@192:~/scripts

[ 2024-06-07 00:46:18 ] [ Scan Type: Fast & Verbose Basic Scan ] [ Scanned Addresses: 192.168.6.142-143 ] [ Directory: Basic_Scan::142-143 ]
[ 2024-06-07 01:09:28 ] [ Scan Type: Fast Full Scan ] [ Scanned Addresses: 192.168.6.142-143 ] [ Directory: Full_Fast::142-143 ]
[ 2024-06-07 01:11:44 ] [ Scan Type: Passive Scan ] [ Target Address: 8.8.8.8 ] [ Directory: Passive::8.8.8.8 ]
[ 2024-06-07 01:16:37 ] [ Scan Type: Web Scan ] [ Web Address: http://192.168.6.142 ] [ Directory: Web_Scan::142 ]
[ 2024-06-07 01:19:13 ] [ Scan Type: Enumeration Scan ] [ Scanned Addresses: 192.168.6.142-143 ] [ Directory: Enum-142-143 ]
[ 2024-06-07 14:38:48 ] [ Anonymity Activated ] [ IP: 107.189.28.199 ] [ Country: Luxembourg ]
[ 2024-06-07 14:39:17 ] [ Anonymity Disabled ] [ IP: 77.137.69.249 ] [ Country: Israel ]

[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive Scan
W) Web Scan
E) Enumerating Scan
V) View Log File
S) Search Results
-h) Help
C) Clear

EX) Exit BC_PT Penetration Testing

bc_pt> V
mouse pointer inside or press Ctrl+G

bc_pt> V
The Log File is: /var/log/BC_PT.log

[ 2024-06-07 00:46:18 ] [ Scan Type: Fast & Verbose Basic Scan ] [ Scanned Addresses: 192.168.6.142-143 ] [ Directory: Basic_Scan::142-143 ]
[ 2024-06-07 01:09:28 ] [ Scan Type: Fast Full Scan ] [ Scanned Addresses: 192.168.6.142-143 ] [ Directory: Full_Fast::142-143 ]
[ 2024-06-07 01:11:44 ] [ Scan Type: Passive Scan ] [ Target Address: 8.8.8.8 ] [ Directory: Passive::8.8.8.8 ]
[ 2024-06-07 01:16:37 ] [ Scan Type: Web Scan ] [ Web Address: http://192.168.6.142 ] [ Directory: Web_Scan::142 ]
[ 2024-06-07 01:19:13 ] [ Scan Type: Enumeration Scan ] [ Scanned Addresses: 192.168.6.142-143 ] [ Directory: Enum-142-143 ]
[ 2024-06-07 14:38:48 ] [ Anonymity Activated ] [ IP: 107.189.28.199 ] [ Country: Luxembourg ]
[ 2024-06-07 14:39:17 ] [ Anonymity Disabled ] [ IP: 77.137.69.249 ] [ Country: Israel ]

[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive Scan
W) Web Scan
E) Enumerating Scan
V) View Log File

bc_pt> -h
Help_Menu
[*] DB FILE IS: BC_PT-DB (Located at: Desktop)
[*] Log FILE IS: BC_PT.log (Located at: /var/log)
```

Help Manual

```
kali@192: ~/scripts

File Actions Edit View Help
[Documentation: https://github.com/Barel-cohen/BC_PT
[NAME: BAREL COHEN] [s8] [TEACHER: NATALIE EREZ]
[Penetration Testing 🔒]
BC_PT [Version: s.8]
© 2024 Barel Cohen.

[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive Scan
W) Web Scan
E) Enumerating Scan
V) View Log File
S) Search Results
-h) Help
C) Clear

EX) Exit BC_PT Penetration Testing
bc_pt> -h
mouse pointer inside or press Ctrl+G.

File Actions Edit View Help
kali@192: ~/scripts
bc_pt> -h
Help Menu
[*] DB FILE IS: BC_PT-DB (Located at: Desktop)
[*] Log FILE IS: BC_PT.log (Located at: /var/log)

[*] 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, SMB

File Actions Edit View Help
kali@192: ~/scripts
[*] 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, SMB
- -V VERBOSE MODE
  Example: B -V
- -F FAST SCAN
- B -FV / -VF Fast & Verbose

[*] 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
- -F FAST SCAN
- F -FV / -VF Fast & Verbose

[*] 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.

[*] Enumerating Scan:
- Scanning with Enum4linuX. is a tool used to gather information from Windows and Samba systems via the SMB (Server Message Block) protocol.
  collect details about users, shared resources, groups, password policies, operating systems, and more.
- Tips: fit the Users and Passwords of Brute Force To the Password Policy and User names if found.
  Notice the target time zone.

[*] Help Menu:
  To display this help menu, use the following options:
  -h | --h | -help | ? | --help
```

Passive Scan

```
kali@192: ~/scripts
File Actions Edit View Help
[ P ] [ S ] [ E ] [ A ] [ N ]
Documentation: https://github.com/Barel-cohen/BC_PT
[NAME: BAREL COHEN] [s8] [TEACHER: NATALIE EREZ]
Penetration_Testing 🔒
BC_PT [Version: s.8]
© 2024 Barel Cohen.

[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive Scan
W) Web Scan
E) Enumerating Scan
V) View Log File
S) Search Results
-h) Help
C) Clear
EX) Exit BC_PT Penetration Testing
bc_pt> P
DB file is: /home/kali/Desktop/BC_PT-DB
Enter file name to save the data: Passive::Google
```

```
kali@192: ~/scripts
File Actions Edit View Help
bc_pt> P
DB file is: /home/kali/Desktop/BC_PT-DB

Enter file name to save the data: Passive::Google
Directory created with the name Passive::Google at /home/kali/Desktop/BC_PT-DB
/home/kali/Desktop/BC_PT-DB/Passive::Google

Start Passive scan..
Enter IP/range to scan: 8.8.8.8
[+] Range correct, continuing...
{
  "ip": "8.8.8.8",
  "hostname": "dns.google",
  "anycast": true,
  "city": "Mountain View",
  "region": "California",
  "country": "US",
  "loc": "37.4056,-122.0775",
  "org": "AS15169 Google LLC",
  "postal": "94043",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}
{
  "ip": "8.8.8.8",
  "hostname": "dns.google",
  "anycast": true,
  "city": "Mountain View",
  "region": "California",
  "country": "US",
  "loc": "37.4056,-122.0775",
  "org": "AS15169 Google LLC",
  "postal": "94043",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}
```

```

kali@192: ~/scripts
File Actions Edit View Help
{
    "anycast": true,
    "city": "Mountain View",
    "region": "California",
    "country": "US",
    "loc": "37.4056,-122.0775",
    "org": "AS15169 Google LLC",
    "postal": "94043",
    "timezone": "America/Los_Angeles",
    "readme": "https://ipinfo.io/missingauth"
}
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

NetRange:      8.8.8.0 - 8.8.8.255
CIDR:         8.8.8.0/24
NetName:       GOGL
NetHandle:     NET-8-8-8-0-2
Parent:        NET8 (NET-8-0-0-0-0)
NetType:       Direct Allocation
OriginAS:
Organization: Google LLC (GOGL)
RegDate:      2023-12-28
Updated:      2023-12-28
Ref:          https://rdap.arin.net/registry/ip/8.8.8.0

kali@192: ~/scripts
File Actions Edit View Help
Comment:      Regards,
Comment:      The Google Team
Ref:          https://rdap.arin.net/registry/entity/GOGL

OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:  Abuse
OrgAbusePhone: +1-650-253-0000
OrgAbuseEmail: network-abuse@google.com
OrgAbuseRef:   https://rdap.arin.net/registry/entity/ABUSE5250-ARIN

OrgTechHandle: ZG39-ARIN
OrgTechName:  Google LLC
OrgTechPhone: +1-650-253-0000
OrgTechEmail: arin-contact@google.com
OrgTechRef:   https://rdap.arin.net/registry/entity/ZG39-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
[ 2024-06-06 14:32:38 ] [ Scan Type: Passive Scan ] [ Target Address: 8.8.8.8 ] [ Directory: Passive::Google ]
[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
mouse pointer inside or press Ctrl+G.

```

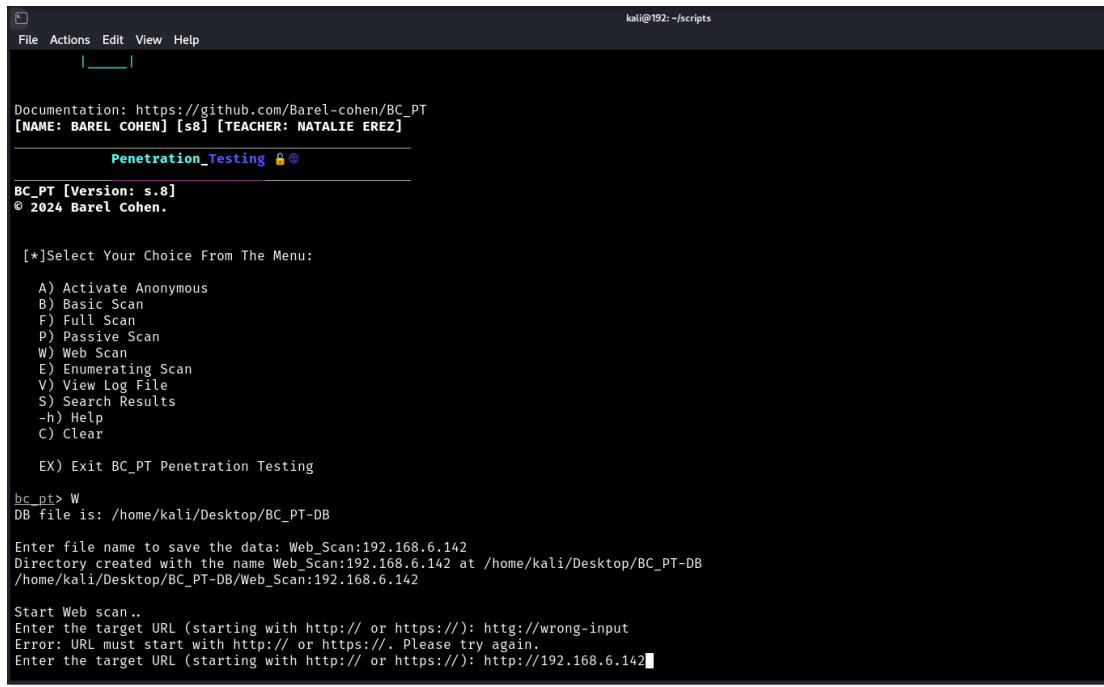
```

File Edit View Go Bookmarks Help
← → ⌘ Desktop BC_PT-DB Passive:24-5
Places Name Size Type
Computer PASSIVE_8.8.8.8 2.3 KiB Manual page
-i/Desktop/BC_PT-DB/Passive:24-5/PASSIVE_8.8.8.8 [Read Only] - Mousepad
File Edit Search View Document Help
File Edit View Document Help
1 | "ip": "8.8.8.8",
2 | "hostname": "dns.google",
3 | "city": "Mountain View",
4 | "region": "California",
5 | "country": "US",
6 | "loc": "37.4956,-122.4715",
7 | "org": "Google LLC",
8 | "postal": "94035",
9 | "state": "CA",
10 | "timezone": "America/Los_Angeles",
11 | "readme": "https://ipinfo.io/missingpath"
12 |
13 # ARIN WHOIS data and services are subject to the Terms of Use
14 # available at: https://www.arin.net/resources/registry/whois/tou/
15 #
16 # If you see inaccuracies in the results, please report at
17 # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
18 #
19 # Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
20 #
21 #
22 #
23 #
24 Netrange: 8.0.0.0 - 8.8.8.255
25 Network: 8.0.0.0/24
26 Netname: 600XL
27 Netmangle: 8.0.0.0-8.8.8.4
28 Netmangle: 8.0.0.0-8.8.8.8-8-4
29 NetType: DIRECT Allocation
30 Organization: Google LLC (GOOL)
31 Updated: 2023-10-28
32 Ref: https://rdap.arin.net/registry/ip/8.8.8.8
33
34
35
36 Organization: Google LLC
37 OrgID: GOOL
38 Address: 1600 Amphitheatre Parkway
39 Address: Mountain View
40 StateProv: CA
41 Postcode: 94035
42 Country: US
43 Updated: 2019-02-28
44 Updated: 2019-02-28
45 Updated: 2019-02-28
46 Comment: Please note that the recommended way to file abuse complaints are located in the following links.
47 Comment: To report abuse and illegal activity: https://www.google.com/contact/
48 Comment: For legal requests: http://support.google.com/legal
49 Comment: Regards,
50 Comment: Regards,
```

Passive Scan Help Menu

[*] **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



kali@192: ~/scripts

File Actions Edit View Help

Documentation: https://github.com/Barel-cohen/BC_PT
[NAME: BAREL COHEN] [s8] [TEACHER: NATALIE EREZ]

Penetration Testing 🔒 ⓘ

BC_PT [Version: s.8]
© 2024 Barel Cohen.

[*]Select Your Choice From The Menu:

- A) Activate Anonymous
- B) Basic Scan
- F) Full Scan
- P) Passive Scan
- W) Web Scan
- E) Enumerating Scan
- V) View Log File
- S) Search Results
- h) Help
- C) Clear

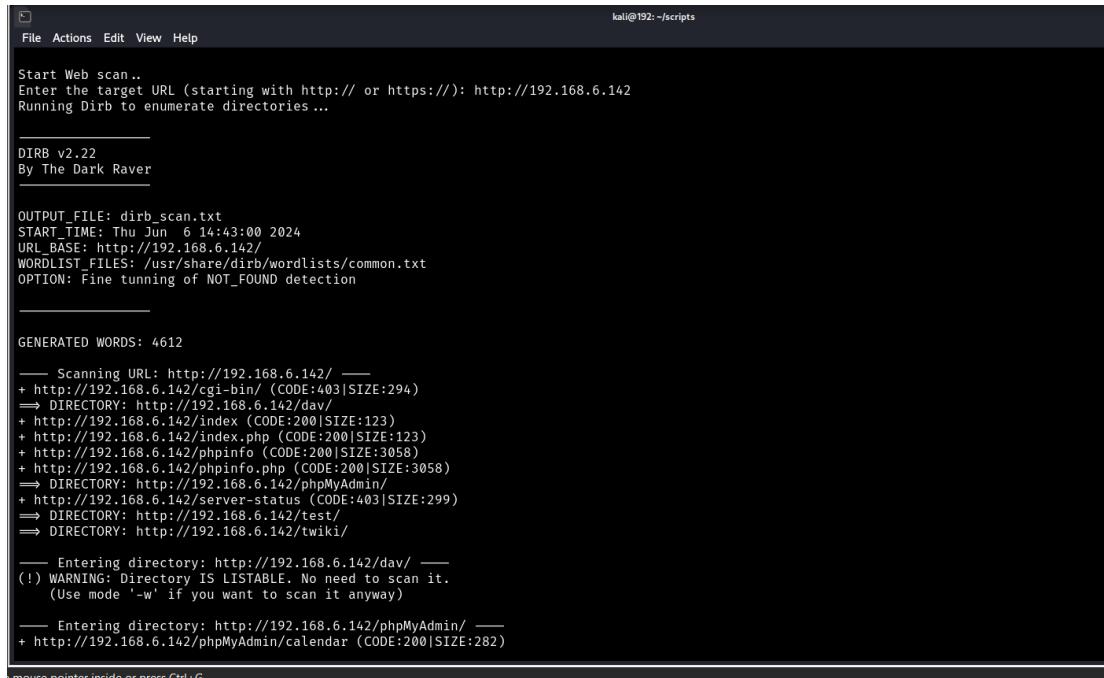
EX) Exit BC_PT Penetration Testing

bc_pt> W
DB file is: /home/kali/Desktop/BC_PT-DB

Enter file name to save the data: Web_Scan:192.168.6.142
Directory created with the name Web_Scan:192.168.6.142 at /home/kali/Desktop/BC_PT-DB
/home/kali/Desktop/BC_PT-DB/Web_Scan:192.168.6.142

Start Web scan..
Enter the target URL (starting with http:// or https://): http://wrong-input
Error: URL must start with http:// or https://. Please try again.
Enter the target URL (starting with http:// or https://): http://192.168.6.142

dirb



kali@192: ~/scripts

File Actions Edit View Help

Start Web scan..
Enter the target URL (starting with http:// or https://): http://192.168.6.142
Running Dirb to enumerate directories ...

DIRB v2.22
By The Dark Raver

OUTPUT_FILE: dirb_scan.txt
START_TIME: Thu Jun 6 14:43:00 2024
URL_BASE: http://192.168.6.142/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Fine tuning of NOT_FOUND detection

GENERATED WORDS: 4612

— Scanning URL: http://192.168.6.142/ —
+ http://192.168.6.142/cgi-bin/ (CODE:403|SIZE:294)
⇒ DIRECTORY: http://192.168.6.142/dav/
+ http://192.168.6.142/index (CODE:200|SIZE:123)
+ http://192.168.6.142/index.php (CODE:200|SIZE:123)
+ http://192.168.6.142/phpinfo (CODE:200|SIZE:3058)
+ http://192.168.6.142/phpinfo.php (CODE:200|SIZE:3058)
⇒ DIRECTORY: http://192.168.6.142/phpMyAdmin/
+ http://192.168.6.142/server-status (CODE:403|SIZE:299)
⇒ DIRECTORY: http://192.168.6.142/test/
⇒ DIRECTORY: http://192.168.6.142/twiki/

— Entering directory: http://192.168.6.142/dav/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://192.168.6.142/phpMyAdmin/ —
+ http://192.168.6.142/phpMyAdmin/calendar (CODE:200|SIZE:282)

mouse pointer inside or press Ctrl+G.

Nikto

```
kali@192:~/scripts
File Actions Edit View Help
DOWNLOADED: 32284 - FOUND: 56
Running Nikto to scan for vulnerabilities ...
- Nikto v2.5.0

+ Target IP: 192.168.6.142
+ Target Hostname: 192.168.6.142
+ Target Port: 80
+ Start Time: 2024-06-06 14:44:12 (GMT3)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ : Retrieved x-powered-by header: PHP/5.2.4-zubuntu5.10.
+ : The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ : The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: https://www.wireshark.org/sections/doc_id_696ebdd59d15.https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?PHP885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F34-0428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F35-0428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/Changelog: Server may leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 19:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/Changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
```

```
mouse pointer inside or press Ctrl+G
kali@192:~/scripts
File Actions Edit View Help
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?PHP885F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F34-0428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F35-0428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?PHP9568F35-0428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/Changelog: Server may leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 92462, size: 40540, mtime: Tue Dec 9 19:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/Changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/.phpMyAdmin directory found.
+ /phpMyAdmin/Documentation: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
End Time: 2024-06-06 14:44:50 (GMT3) (38 seconds)

+ 1 host(s) tested
Dirb scan results saved to dirb_scan.txt
Nikto scan results saved to nikto_scan.txt
Do you want to zip the scan results? (y/n): y
  adding: dirb_scan.txt (deflated 84%)
  adding: nikto_scan.txt (deflated 60%)
Scan results zipped to web_scan_results.zip
[ 2024-06-06 14:44:57 ] [ Scan Type: Web Scan ] [ Web Address: http://192.168.6.142 ] [ Directory: Web_Scan::192.168.6.142 ]

[*]Select Your Choice From The Menu:
 A) Activate Anonymous
```

mouse pointer inside or press Ctrl+G.

if choose y:

Name	Size	Type	Date Modified
web_scan_results.zip	2.8 KB	Zip archive	Today

if choose n:

Name	Size	Type	Date Modified
dirb_scan.txt	7.0 KB	plain text document	Today
nikto_scan.txt	3.4 KB	plain text document	Today

both under the name file you gave at the start

Web Scan Help Menu

- ```
[*] Web Scan:
- Initiate a web scan to analyze web-based services and vulnerabilities.
 using dirb and nikto tools.
```

## Enumerating Scan

```
kali@192: ~/scripts

File Actions Edit View Help

Documentation: https://github.com/Barel-cohen/BC_PT
[NAME: BAREL COHEN] [s8] [TEACHER: NATALIE EREZ]
Penetration_Testing 🔒

BC_PT [Version: s.8]
© 2024 Barel Cohen.

[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive Scan
W) Web Scan
E) Enumerating Scan
V) View Log File
S) Search Results
-h) Help
C) Clear

EX) Exit BC_PT Penetration Testing

bc_pt> E
DB file is: /home/kali/Desktop/BC_PT-DB

Enter file name to save the data: Enum-192.168.6.142-143

mouse pointer inside or press Ctrl+G.
File Actions Edit View Help

bc_pt> E
DB file is: /home/kali/Desktop/BC_PT-DB

Enter file name to save the data: Enum-192.168.6.142-143
Directory created with the name Enum-192.168.6.142-143 at /home/kali/Desktop/BC_PT-DB
/home/kali/Desktop/BC_PT-DB/Enum-192.168.6.142-143

Start Enumerating
Enter IP/range to scan: 192.168.6.142-143
[+] Range correct, continuing ...
Enumerating IP: 192.168.6.142
Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Thu Jun 6 14:51:36 2024
 =(Target Information)=

Target 192.168.6.142
RID Range 500-550,1000-1050
Username ''
Password ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 =(Enumerating Workgroup/Domain on 192.168.6.142)=

[+] Got domain/workgroup name: WORKGROUP

 =(Nbtstat Information for 192.168.6.142)=

Looking up status of 192.168.6.142
 METASPLOITABLE <00> - B <ACTIVE> Workstation Service
 METASPLOITABLE <03> - B <ACTIVE> Messenger Service
 METASPLOITABLE <20> - B <ACTIVE> File Server Service
 __MSBROWSE__. <01> - <GROUP> B <ACTIVE> Master Browser
 WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
 WORKGROUP <1d> - B <ACTIVE> Master Browser
```

```

kali@192: ~/scripts
File Actions Edit View Help
_____(Nbtstat Information for 192.168.6.142)_____
Looking up status of 192.168.6.142
 METASPLOITABLE <00> - B <ACTIVE> Workstation Service
 METASPLOITABLE <03> - B <ACTIVE> Messenger Service
 METASPLOITABLE <20> - B <ACTIVE> File Server Service
.. _MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
MAC Address = 00-00-00-00-00-00
_____(Session Check on 192.168.6.142)_____
[+] Server 192.168.6.142 allows sessions using username '', password ''
_____(Getting domain SID for 192.168.6.142)_____
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
_____(OS information on 192.168.6.142)_____
[E] Can't get OS info with smbclient

```

## Domain name

```

kali@192: ~/scripts
File Actions Edit View Help
_____(OS information on 192.168.6.142)_____
[E] Can't get OS info with smbclient
[+] Got OS info for 192.168.6.142 from srvinfo:
 METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
 platform_id : 500
 os version : 4.9
 server type : 0x9a03
_____(Users on 192.168.6.142)_____
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user,lli,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4d8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)

```

## Users and rids

```

File Actions Edit View Help
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xb8 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name: ,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x404]
user:[user] rid:[0x bba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]

[ie the mouse pointer inside or press Ctrl+G]

```

## Shared Folders

```

File Actions Edit View Help
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]

(Share Enumeration on 192.168.6.142)

Sharename	Type	Comment
print\$	Disk	Printer Drivers
tmp	Disk	oh noes!
opt	Disk	
IPC\$	IPC	IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN\$	IPC	IPC Service (metasploitable server (Samba 3.0.20-Debian))

Reconnecting with SMB1 for workgroup listing.

Server	Comment

Workgroup	Master
WORKGROUP	METASPLOITABLE

[+] Attempting to map shares on 192.168.6.142
//192.168.6.142/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.6.142/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.6.142/opt Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing *
//192.168.6.142/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.6.142/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A

(Password Policy Information for 192.168.6.142)

[ie the mouse pointer inside or press Ctrl+G]

```

## Password Policy

Tip: (Password Policy and Users can use at Brute Force (Basic&Full Scan) if found)

```
kali@192:~/scripts
File Actions Edit View Help
===== (Password Policy Information for 192.168.6.142) =====

[+] Attaching to 192.168.6.142 using a NULL share
[+] Trying protocol 139/SMB...
[+] Found domain(s):
 [+] METASPOITABLE
 [+] Builtin
[+] Password Info for Domain: METASPOITABLE
 [+] Minimum password length: 5
 [+] Password history length: None
 [+] Maximum password age: Not Set
 [+] Password Complexity Flags: 000000
 [+] Domain Refuse Password Change: 0
 [+] Domain Password Store Cleartext: 0
 [+] Domain Password Lockout Admins: 0
 [+] Domain Password No Clear Change: 0
 [+] Domain Password No Anon Change: 0
 [+] Domain Password Complex: 0
 [+] Minimum password age: None
 [+] Reset Account Lockout Counter: 30 minutes
 [+] Locked Account Duration: 30 minutes
 [+] Account Lockout Threshold: None
 [+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0

e the mouse pointer inside or press Ctrl+G
```

## Groups and Sids

```
kali@192:~/scripts
File Actions Edit View Help
Password Complexity: Disabled
Minimum Password Length: 0
===== (Groups on 192.168.6.142) =====

[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
===== (Users on 192.168.6.142 via RID cycling (RIDS: 500-550,1000-1050)) =====

[!] Found new SID:
S-1-5-21-1042354039-2475377354-766472396
[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username "", password ""

S-1-5-21-1042354039-2475377354-766472396-500 METASPOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPOITABLE\root (Local User)

e the mouse pointer inside or press Ctrl+G
```

```
kali@192: ~/scripts
File Actions Edit View Help
enum4linux complete on Thu Jun 6 14:51:54 2024
Enumerating IP: 192.168.6.143
Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Thu Jun 6 14:51:55 2024
===== (Target Information) =====
Target 192.168.6.143
RID Range 500-550,1000-1050
Username ''
Password ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== (Enumerating Workgroup/Domain on 192.168.6.143) =====

[E] Can't find workgroup/domain

===== (Nbtstat Information for 192.168.6.143) =====
Looking up status of 192.168.6.143
No reply from 192.168.6.143

===== (Session Check on 192.168.6.143) =====

[E] Server doesn't allow session using username '', password ''.
Aborting remainder of tests.

[2024-06-06 14:52:18] [Scan Type: Enumeration Scan] [Scanned Addresses: 192.168.6.142-143] [Directory: Enum-192.168.6.142-143]
[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
mouse pointer inside or press Ctrl+G.
```

## Enumeration Scan Help Menu

```
[*] Enumerating Scan:
- Scanning with Enum4linux. is a tool used to gather information from Windows and Samba systems via the SMB (Server Message Block) protocol.
 collect details about users, shared resources, groups, password policies, operating systems, and more.
- Tips:fit the Users and Passwords of Brute Force To the Password Policy and User names if found.
 Notice the target time zone.
```

## **Conclusions**

The BC\_PT framework represents a sophisticated and structured approach to penetration testing, effectively leveraging automation and the integration of multiple tools to achieve thorough and comprehensive security assessments. By utilizing this framework, penetration testers and users can significantly enhance their ability to identify and mitigate potential security risks within their networks and web applications.

The key advantages of the BC\_PT framework include:

- 1. Efficiency:** Automation streamlines the testing process, allowing for rapid and consistent identification of vulnerabilities.
- 2. Comprehensive Coverage:** The integration of diverse tools ensures a wide range of vulnerabilities are detected, from weak credentials to network misconfigurations and web application flaws.
- 3. User-Friendly:** The organized structure of the framework simplifies the testing process, making it accessible even to those with limited penetration testing experience.
- 4. Scalability:** The framework can easily adapt to different environments and scales of operation, from small networks to large enterprise systems.
- 5. Detailed Reporting:** The framework provides detailed and organized reports, aiding in the clear communication of findings and recommended remediation actions.

By following the BC\_PT framework, penetration testers and security professionals can improve their operational efficiency and effectiveness, ultimately enhancing the overall security posture of the organizations they serve.



### Link To Video of The BC PT Framework Tool:

<https://drive.google.com/file/d/1BKPeTrU0B7JjzzwQpRdPwEccmnwrEbKD/view>

**GitHub:** [https://github.com/Barel-cohen/BC\\_PT](https://github.com/Barel-cohen/BC_PT)

**Linkdin:** [www.linkedin.com/in/barel-cohen-7699b3281](http://www.linkedin.com/in/barel-cohen-7699b3281)



## **CREDITS:**

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



## Ethical Penetration Testing

