PROJECT: PENETRATION TESTING

NAME: BAREL COHEN

JohnBryce&ThinkCyber

MY PT PROJECT: BC_PT Framework

Penetration Testing Project Report - Summary

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

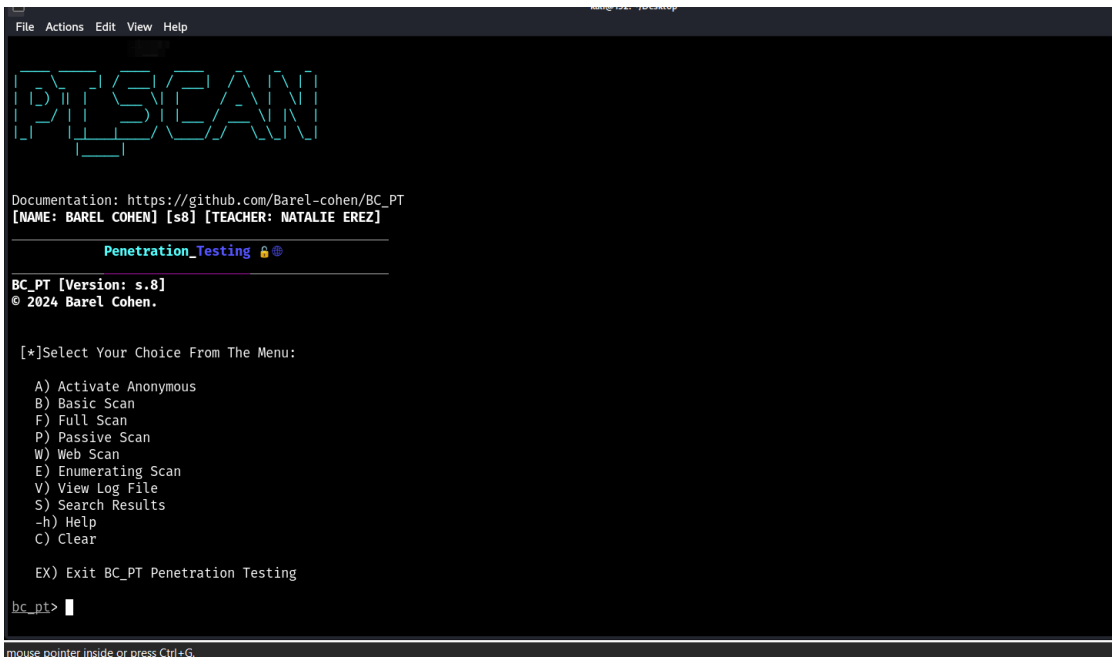
5. Use searchsploit to identify potential exploits and display the results

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



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 finish

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 geoiplookup, 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 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

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

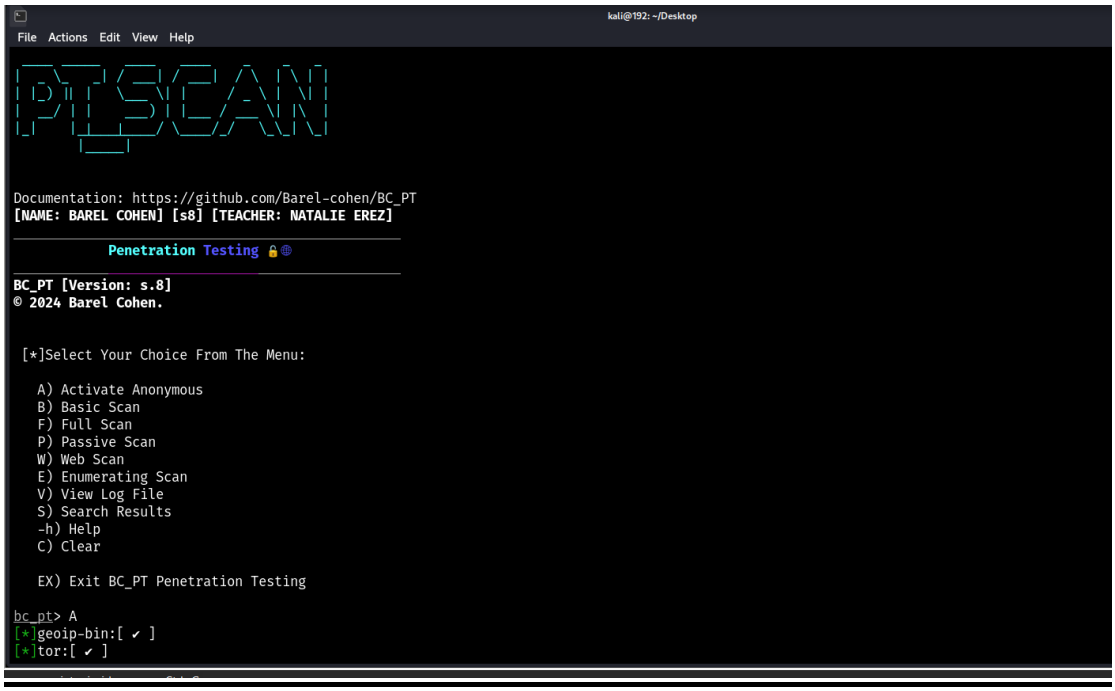
Enumerating Scan provide Information of the target that can be useful specially to the Brute force you can fit the Users and passwords to the policies if found

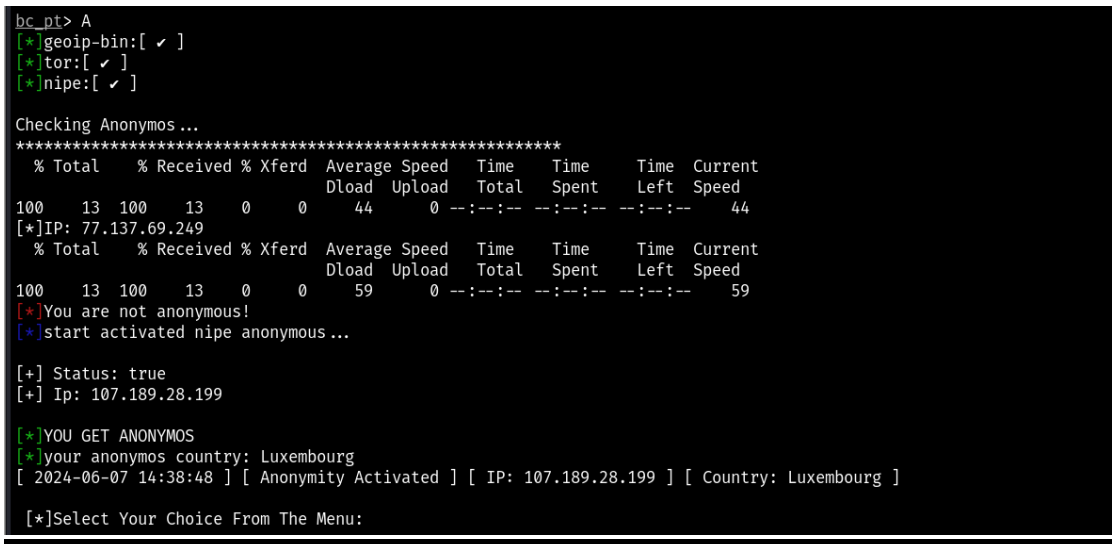
Option to save all scan results in a ZIP file based on user preference, facilitating convenient information management

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





Stop Anonymous

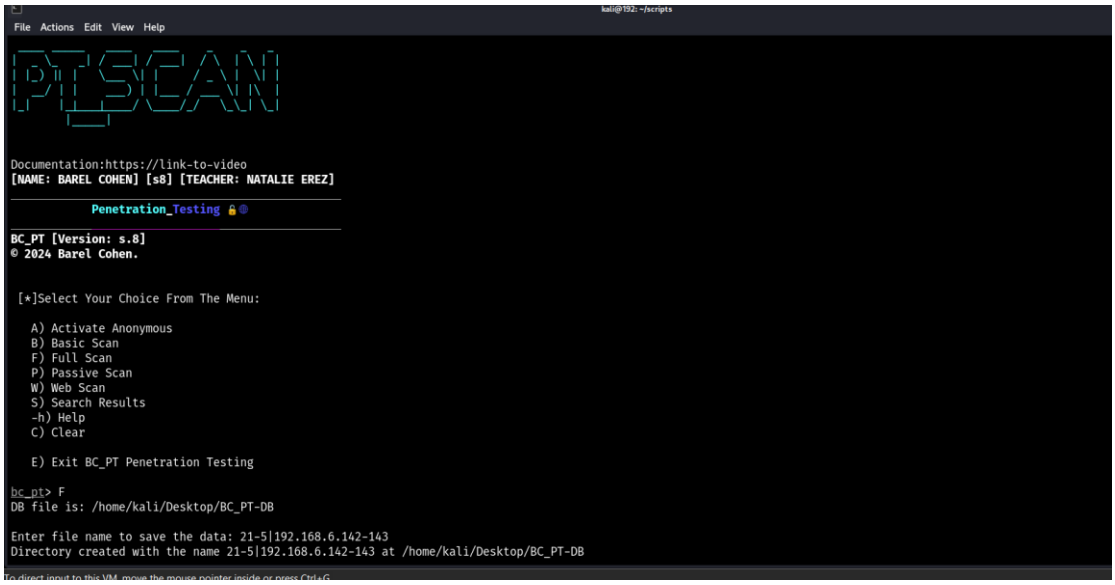
```
bc_pt> A -S
[*]geoip-bin:[ ✔ ]
[*]tor:[ ✔ ]
[*]nipe:[ ✔ ]

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:
```

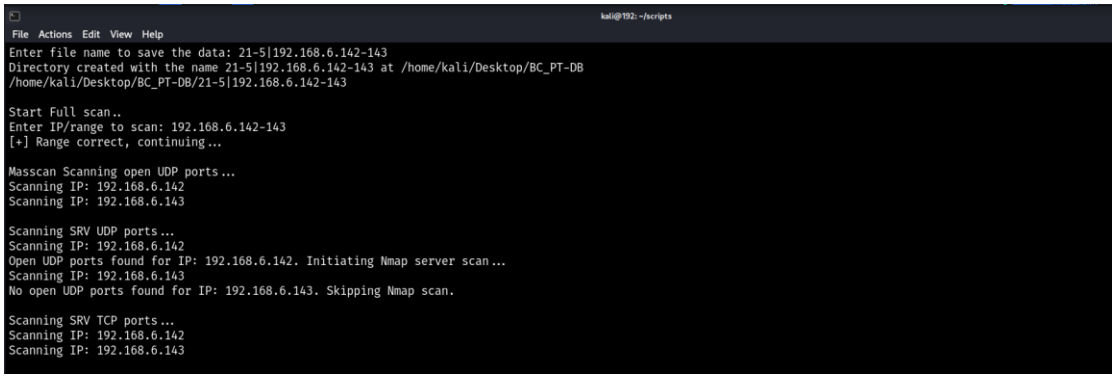
```
bc_pt> A -S
[*]geoip-bin:[ ✔ ]
[*]tor:[ ✔ ]
[*]nipe:[ ✔ ]

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





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: bdb
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

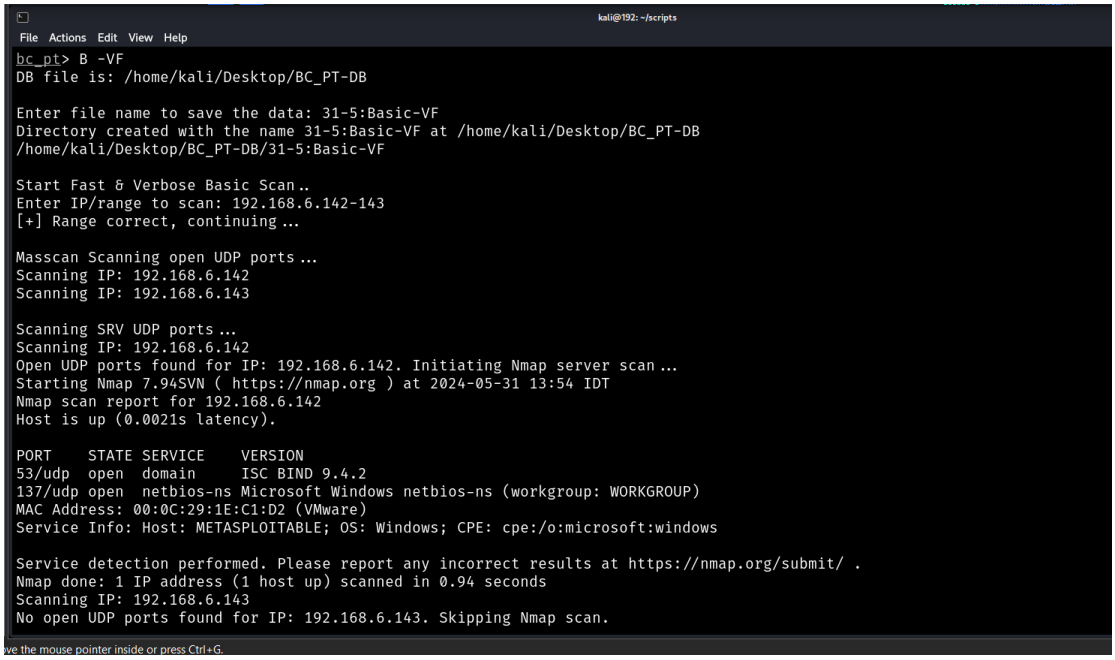
```
kali@192: ~/scripts
File  Actions  Edit  View  Help
Scanning IP: 192.168.6.142
Open UDP ports found for IP: 192.168.6.142. Initiating Nmap server scan...
Scanning IP: 192.168.6.143
No open UDP ports found for IP: 192.168.6.143. Skipping Nmap scan.

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
```

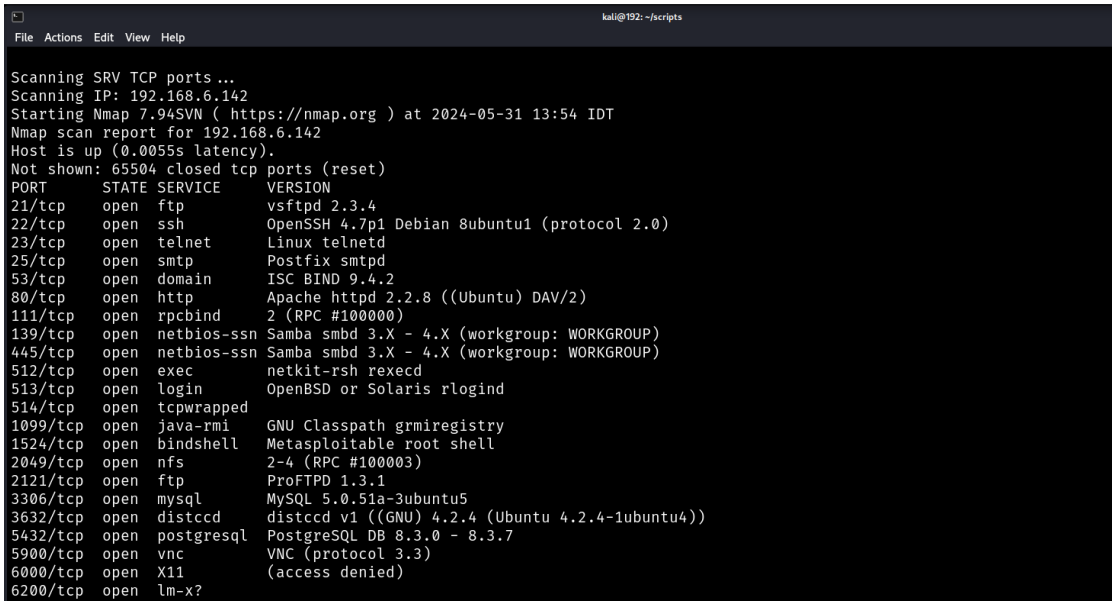
Help Manual Basic & Full Scan

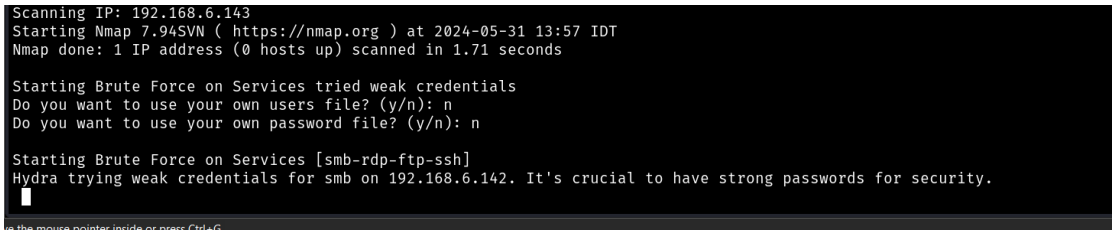
```
[*] Additional Scanning Options:

[*] 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)

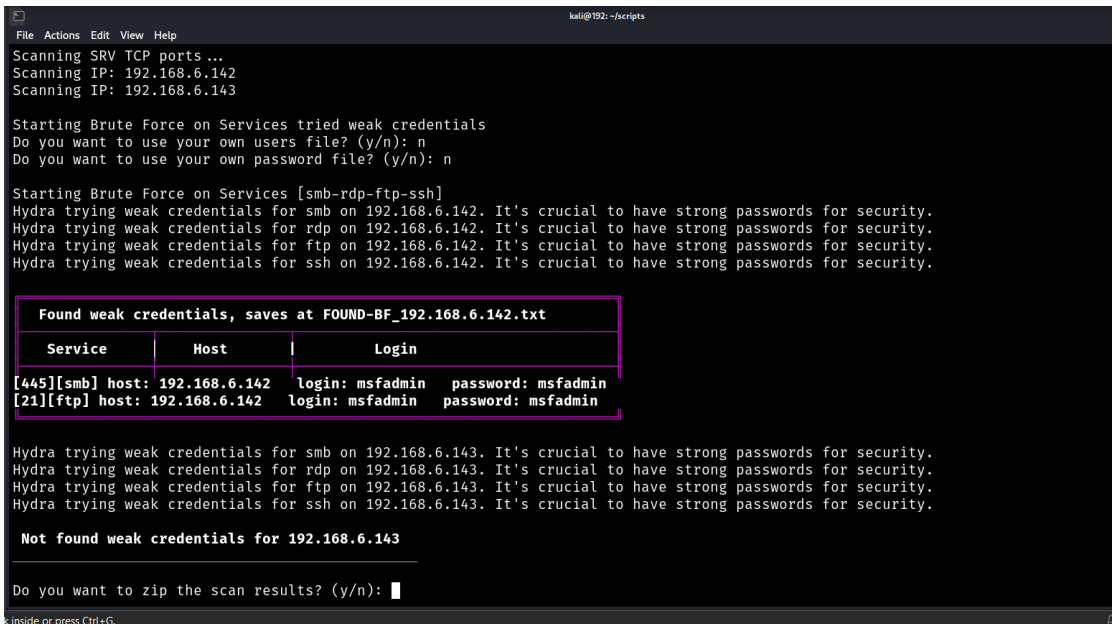






End Basic Scan

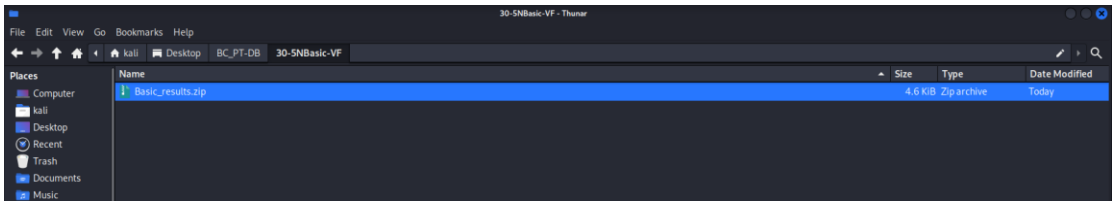
Zip the result?

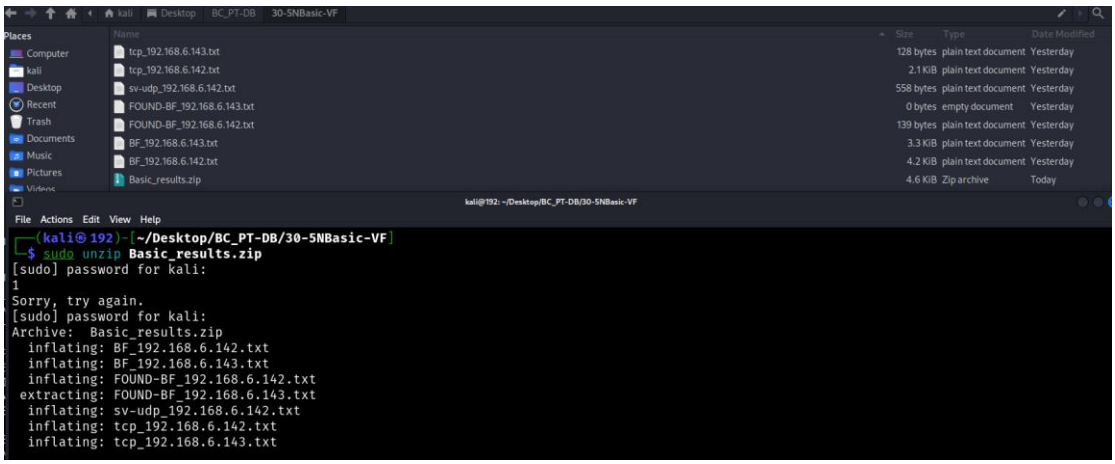


*Note:

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

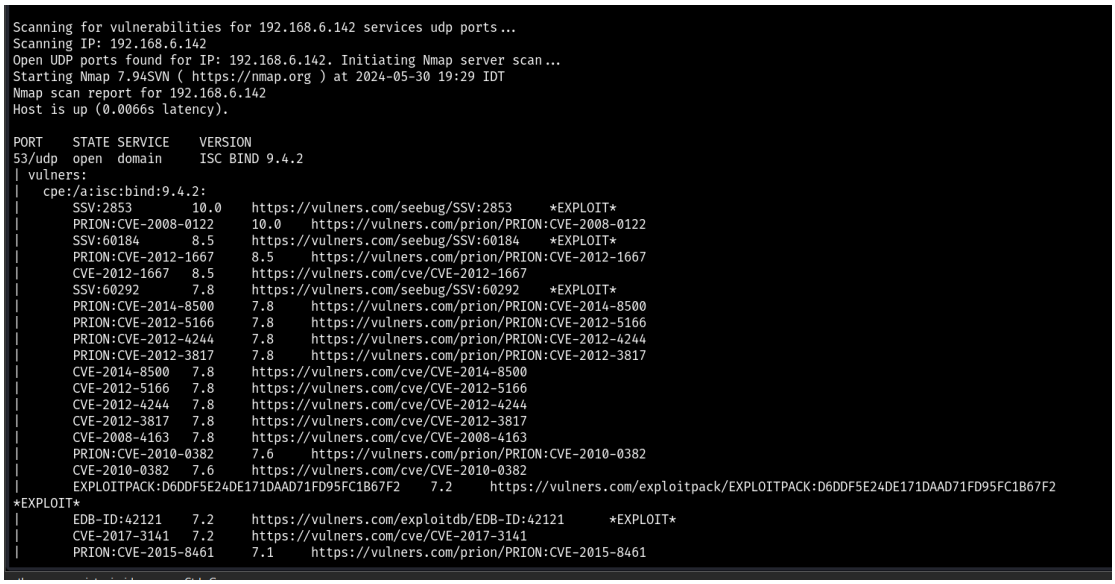
The Files FOUND-BF_$IP.txt Are Saving The Weak Credentials if Found



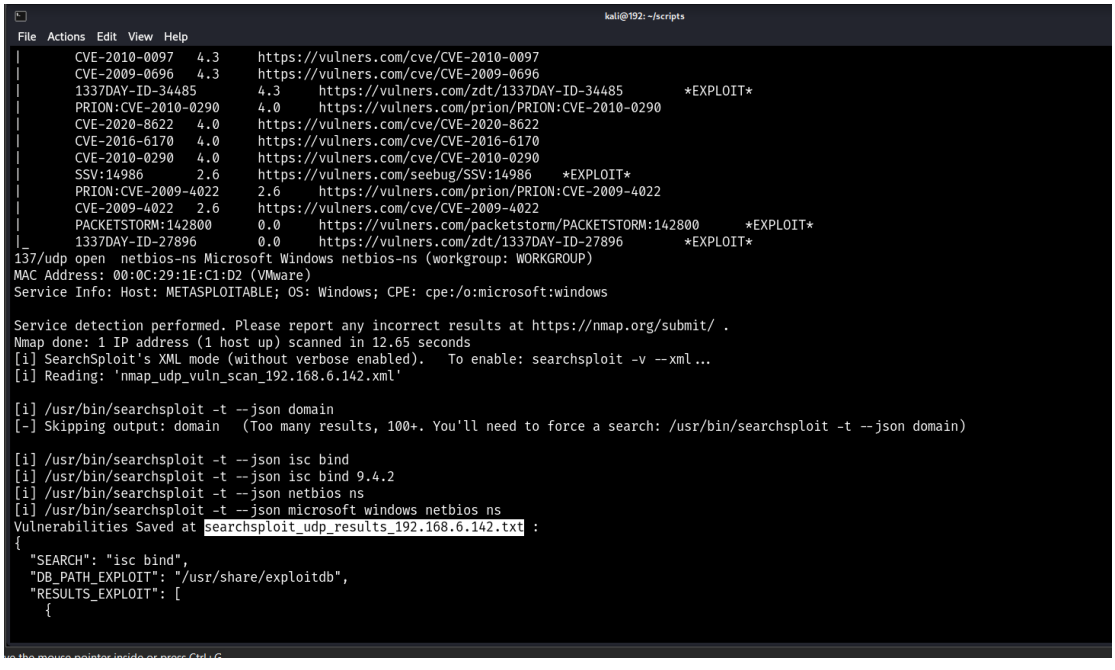


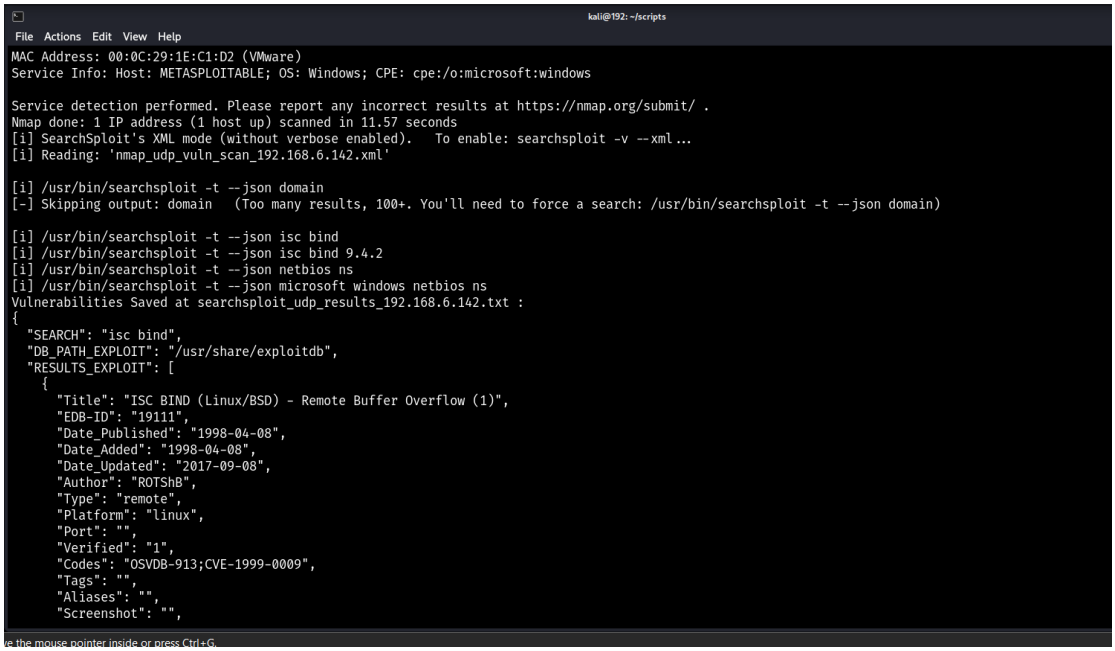
Full Scan (+ Vulnerabilities)

Start Vulnerability's Scan UDP Ports If found open

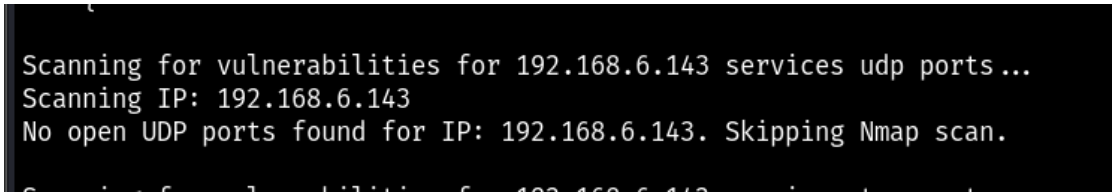


Nmap scanning NSE script engine- vuln, then to Searchsploit

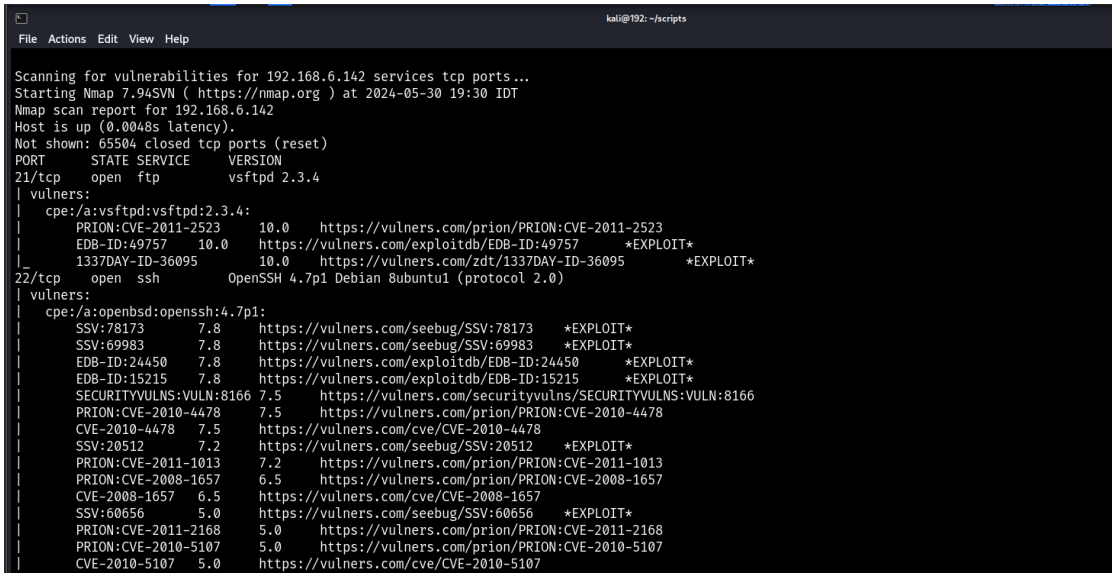




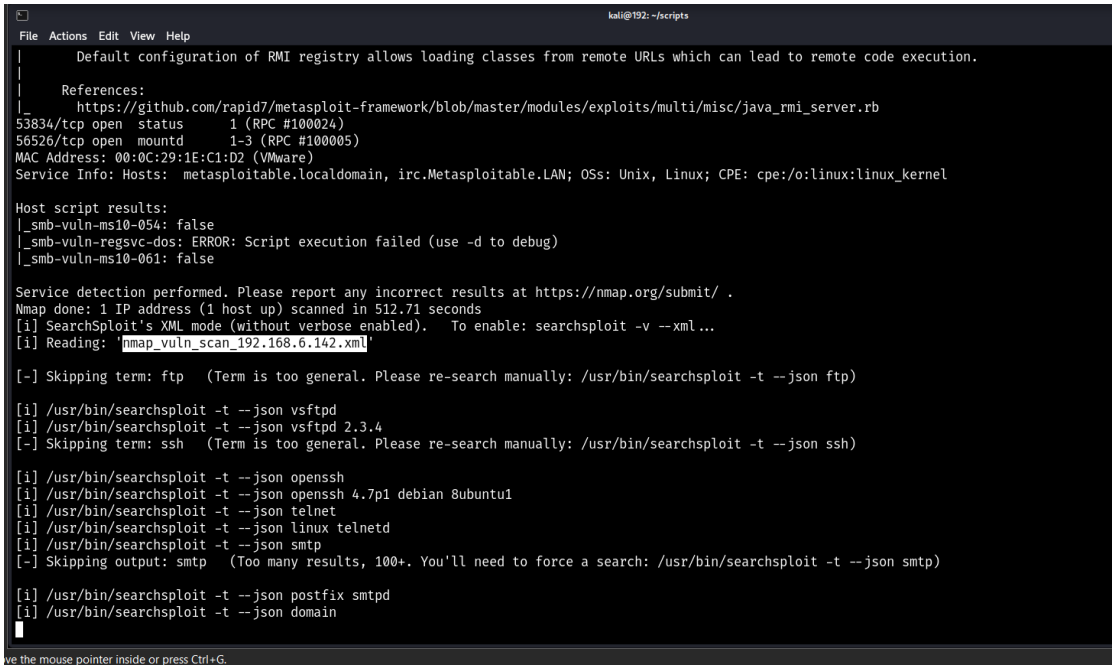
If not found open UDP ports Skipping

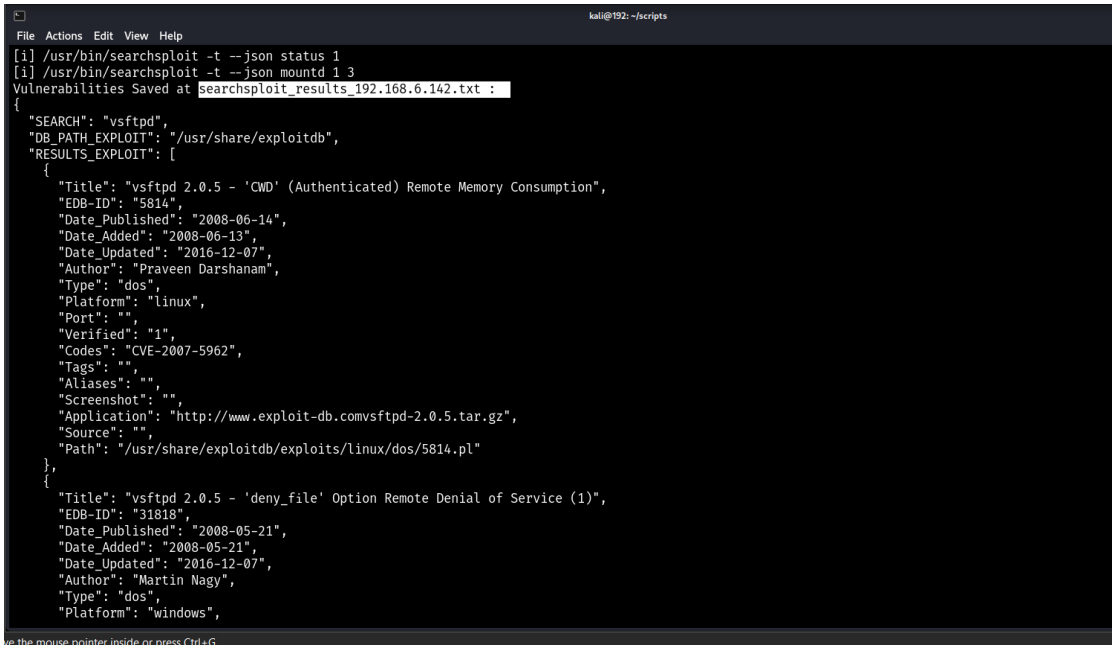


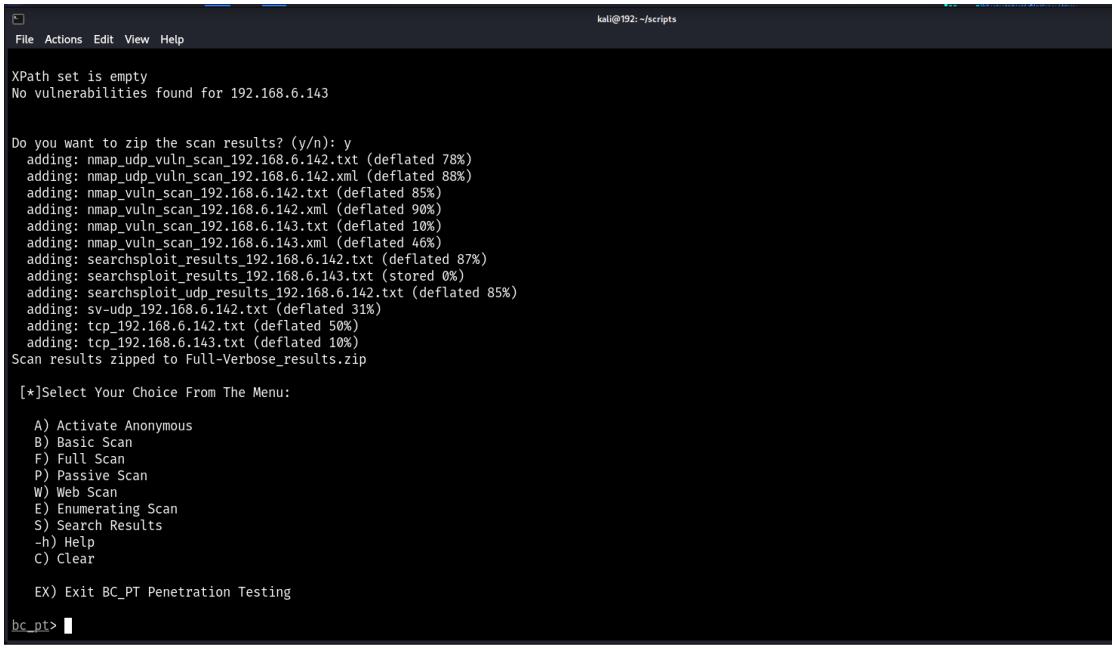
Scan TCP ports Vulnerability's



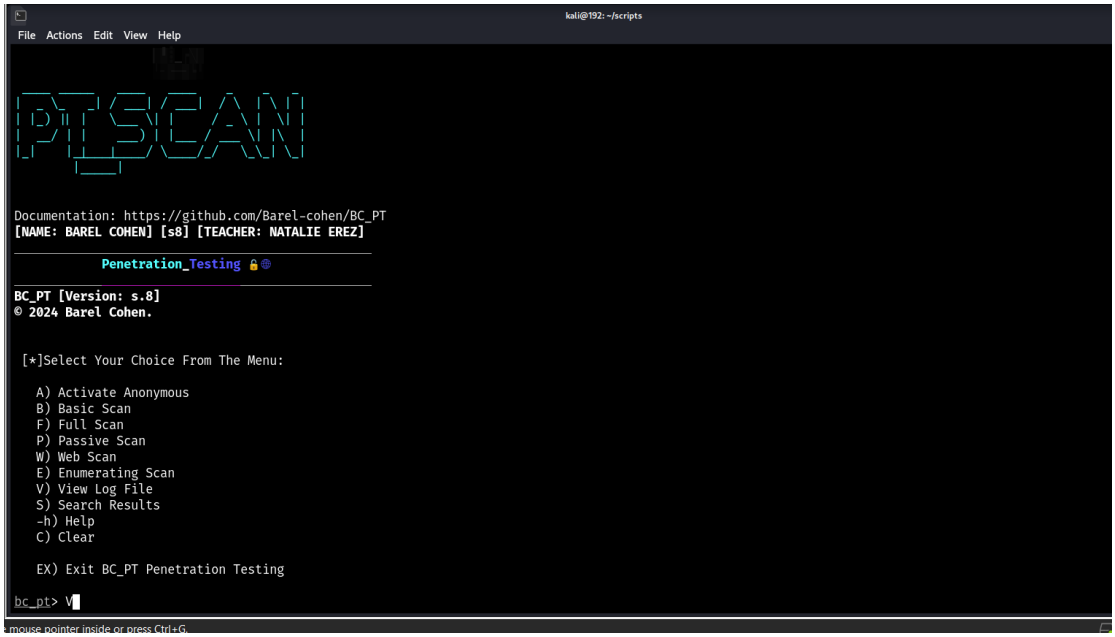
Nmap results to Searchsploit

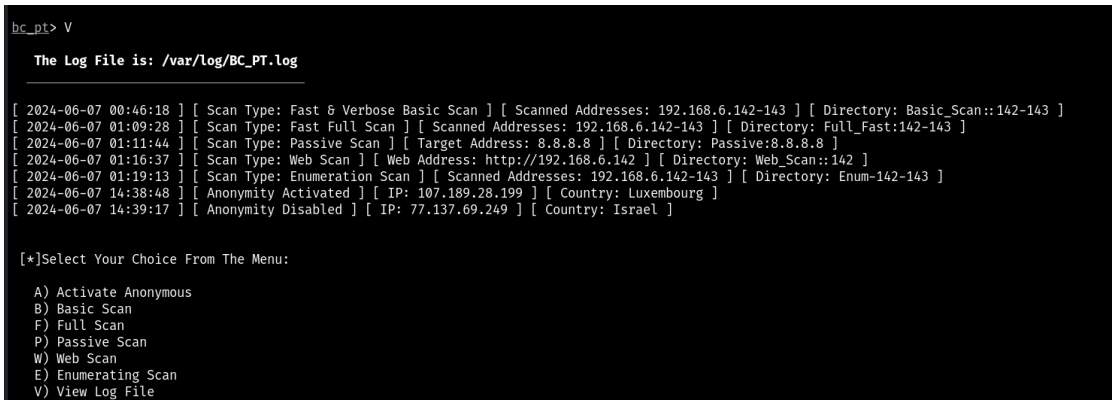


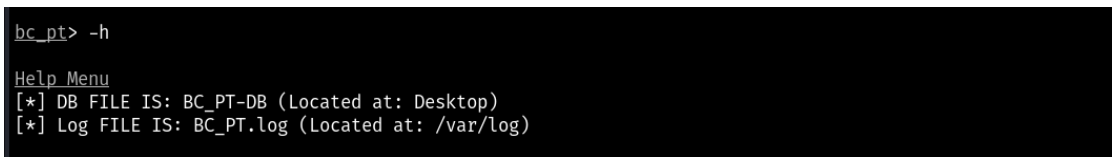



kali@192: ~/scripts
File Actions Edit View Help
XPath set is empty
No vulnerabilities found for 192.168.6.143
Do you want to zip the scan results? (y/n): y
adding: nmap_udp_vuln_scan_192.168.6.142.txt (deflated 78%)
adding: nmap_udp_vuln_scan_192.168.6.142.xml (deflated 88%)
adding: nmap_vuln_scan_192.168.6.142.txt (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>

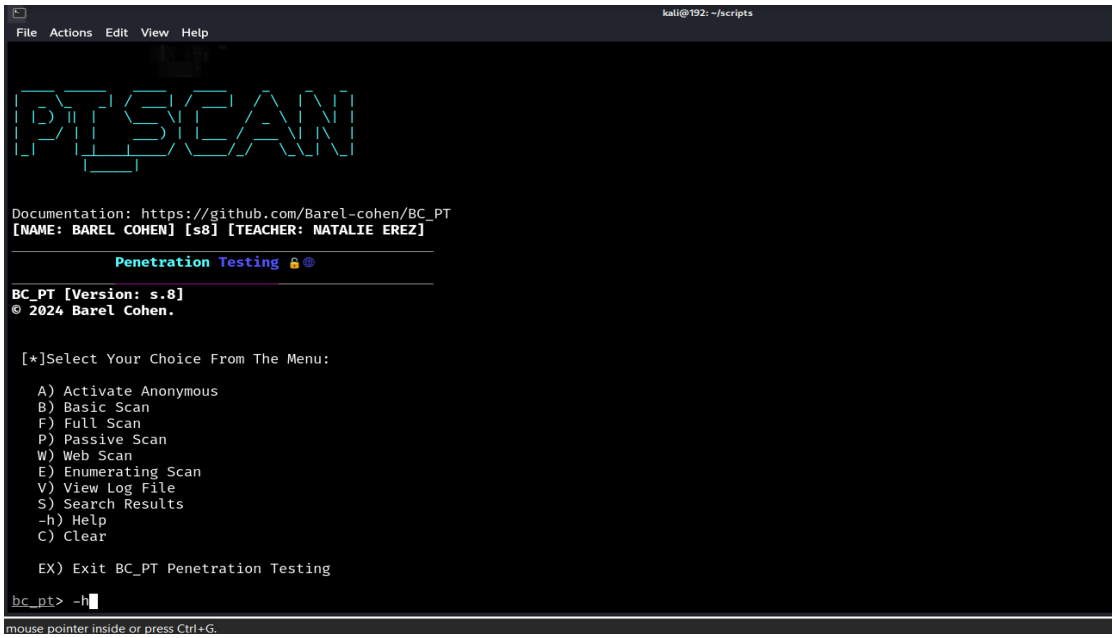
Log File

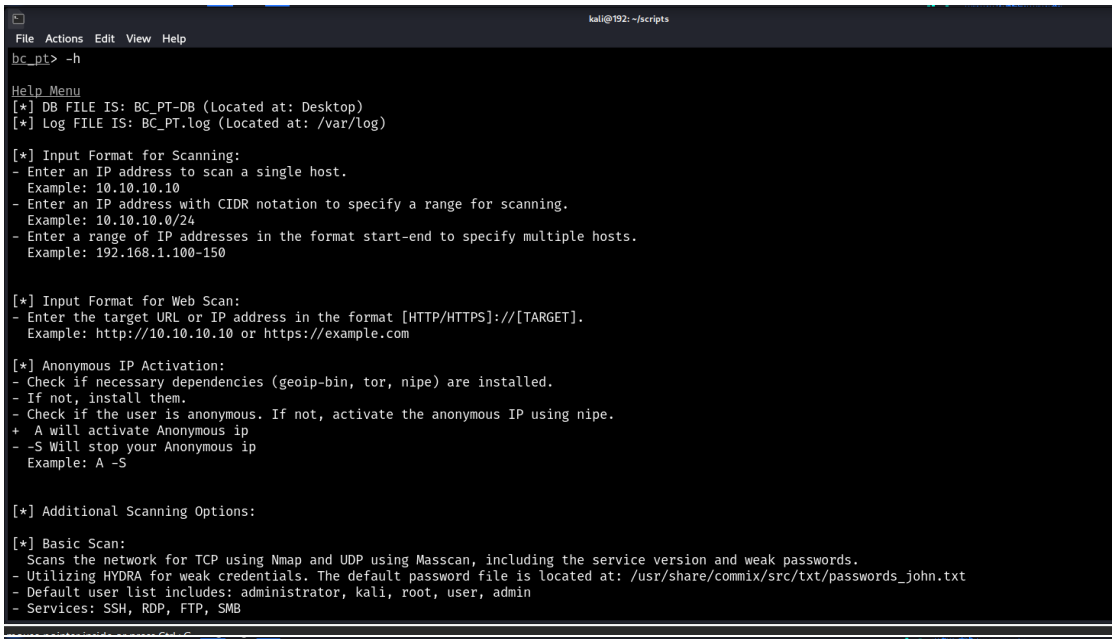

kali@192: ~/scripts
File Actions Edit View Help
Documentation: https://github.com/Barel-cohen/BC_PT
[NAME: BAREL COHEN] [s8] [TEACHER: NATALIE EREZ]
Penetration_Testing
BC_PT [Version: s.8]
© 2024 Barel Cohen.
[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive 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> V

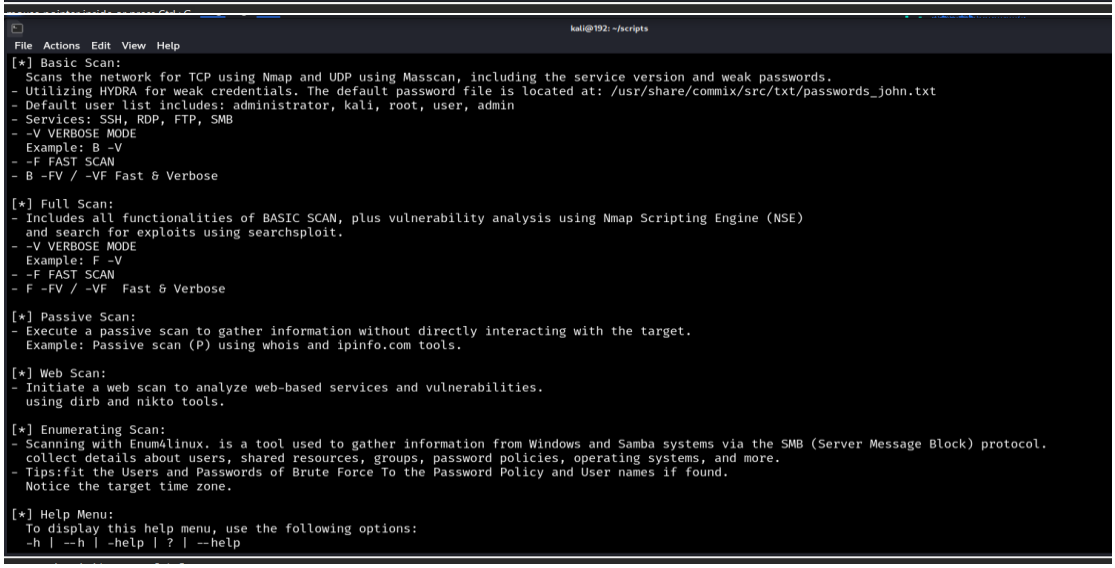

bc_pt> V
The Log File is: /var/log/BC_PT.log
[2024-06-07 00:46:18] [Scan Type: Fast & Verbose Basic Scan] [Scanned Addresses: 192.168.6.142-143] [Directory: Basic_Scan::142-143]
[2024-06-07 01:09:28] [Scan Type: Fast Full Scan] [Scanned Addresses: 192.168.6.142-143] [Directory: Full_Fast:142-143]
[2024-06-07 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)

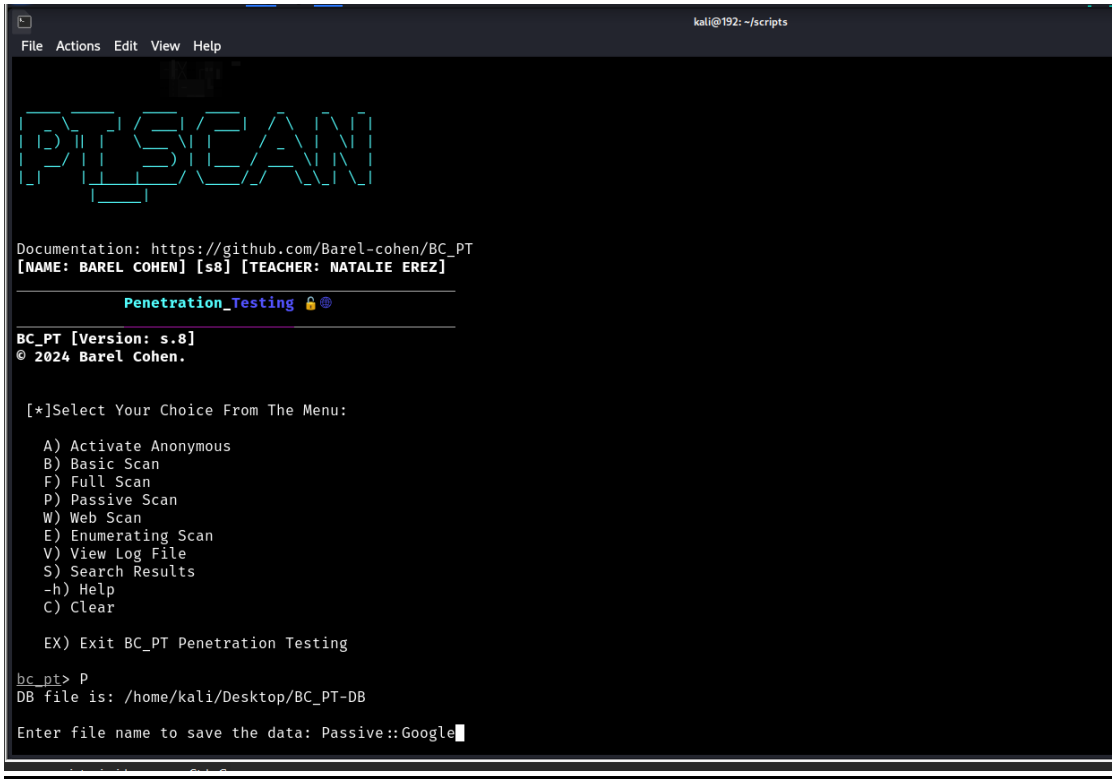
Help Manual

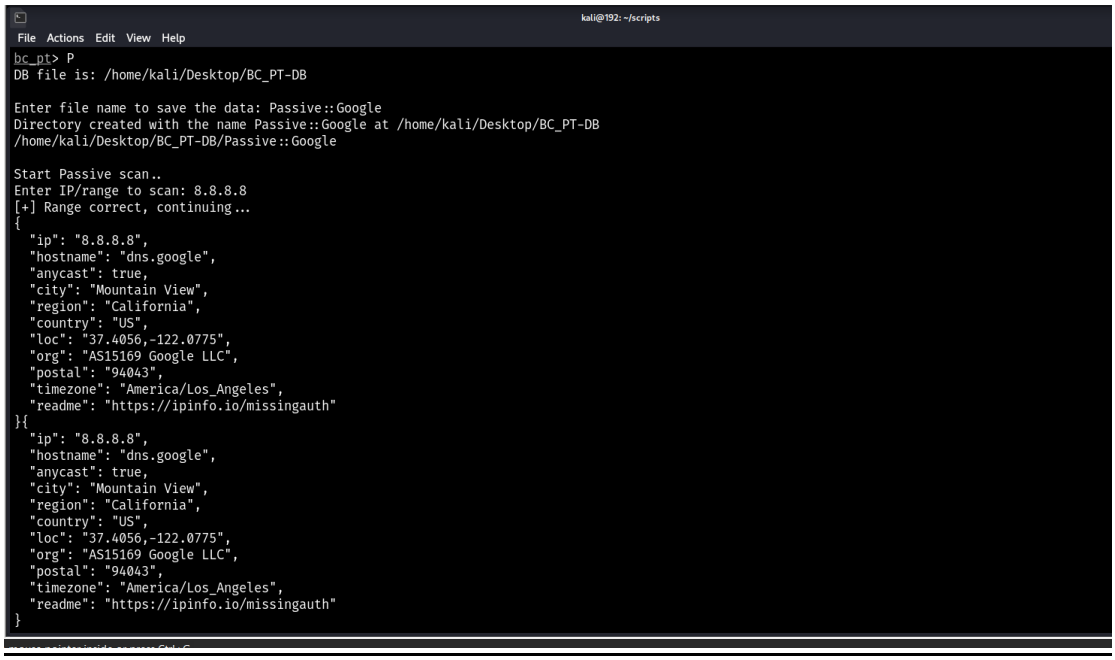

kali@192: ~/scripts
File Actions Edit View Help
Documentation: https://github.com/Barel-cohen/BC_PT
[NAME: BAREL COHEN] [s8] [TEACHER: NATALIE EREZ]
Penetration Testing
BC_PT [Version: s.8]
© 2024 Barel Cohen.
[*]Select Your Choice From The Menu:
A) Activate Anonymous
B) Basic Scan
F) Full Scan
P) Passive 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

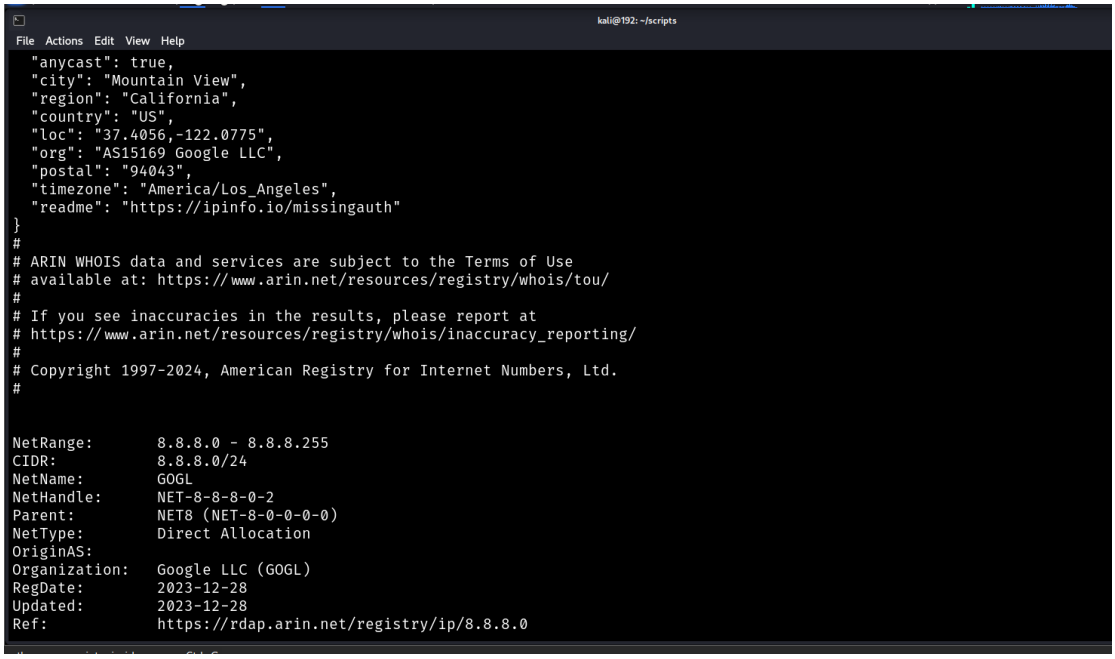

kali@192: ~/scripts
File Actions Edit View Help
bc_pt> -h
Help Menu
[*] DB FILE IS: BC_PT-DB (Located at: Desktop)
[*] Log FILE IS: BC_PT.log (Located at: /var/log)
[*] Input Format for Scanning:
- Enter an IP address to scan a single host.
Example: 10.10.10.10
- Enter an IP address with CIDR notation 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

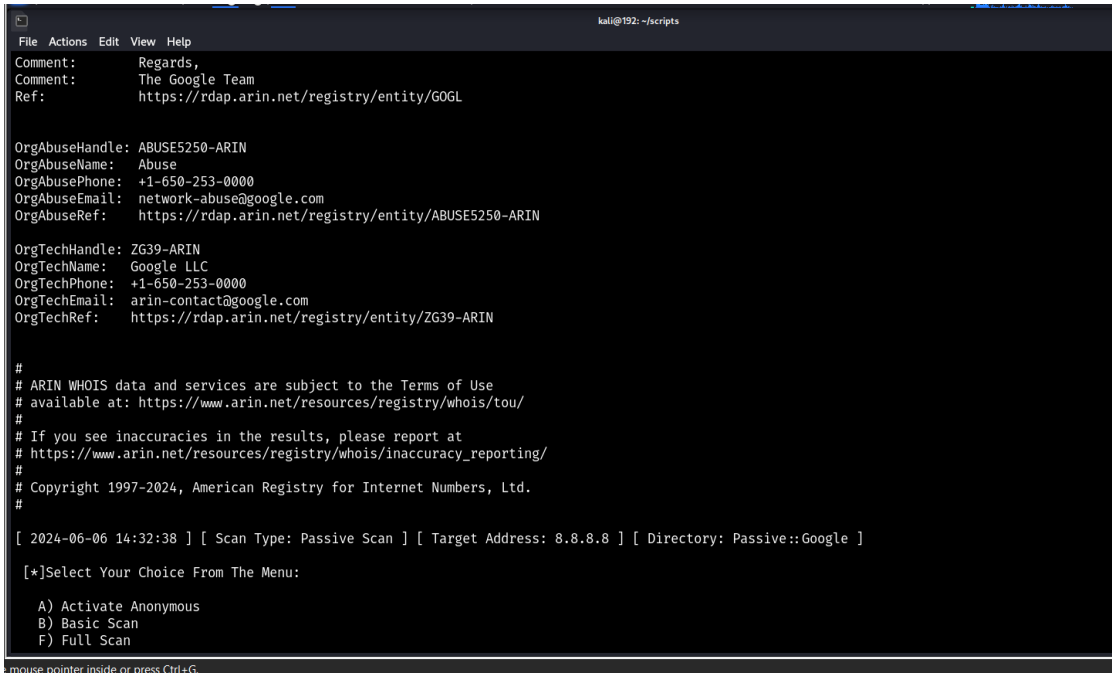

kali@192: ~/scripts
File Actions Edit View Help
[*] Basic Scan:
Scans the network for TCP using Nmap and UDP using Masscan, including the service version and weak passwords.
- Utilizing HYDRA for weak credentials. The default password file is located at: /usr/share/commix/src/txt/passwords_john.txt
- 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

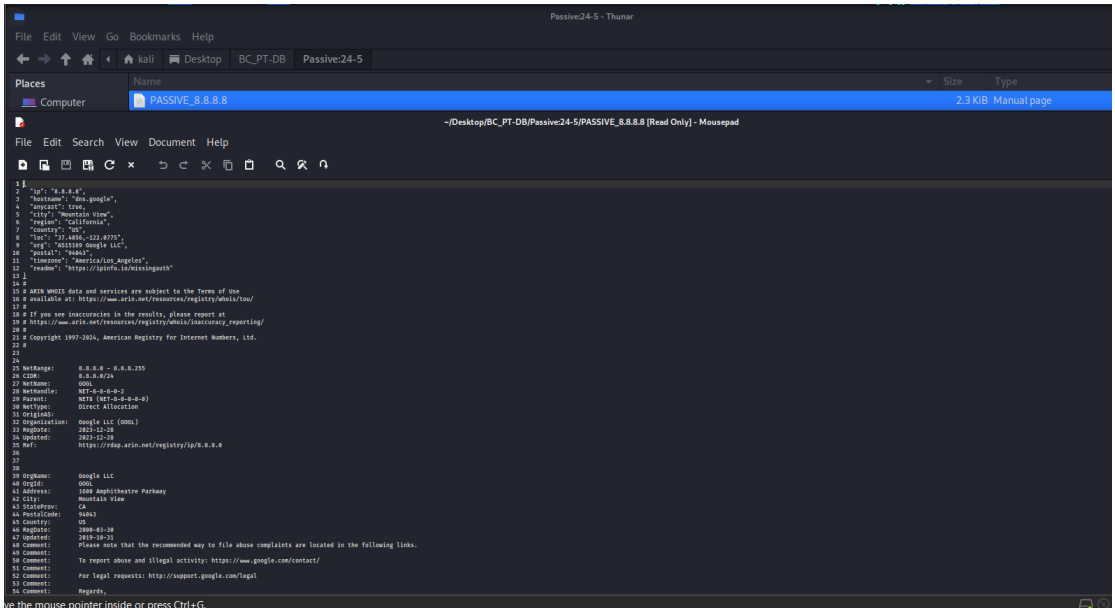
Passive Scan






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

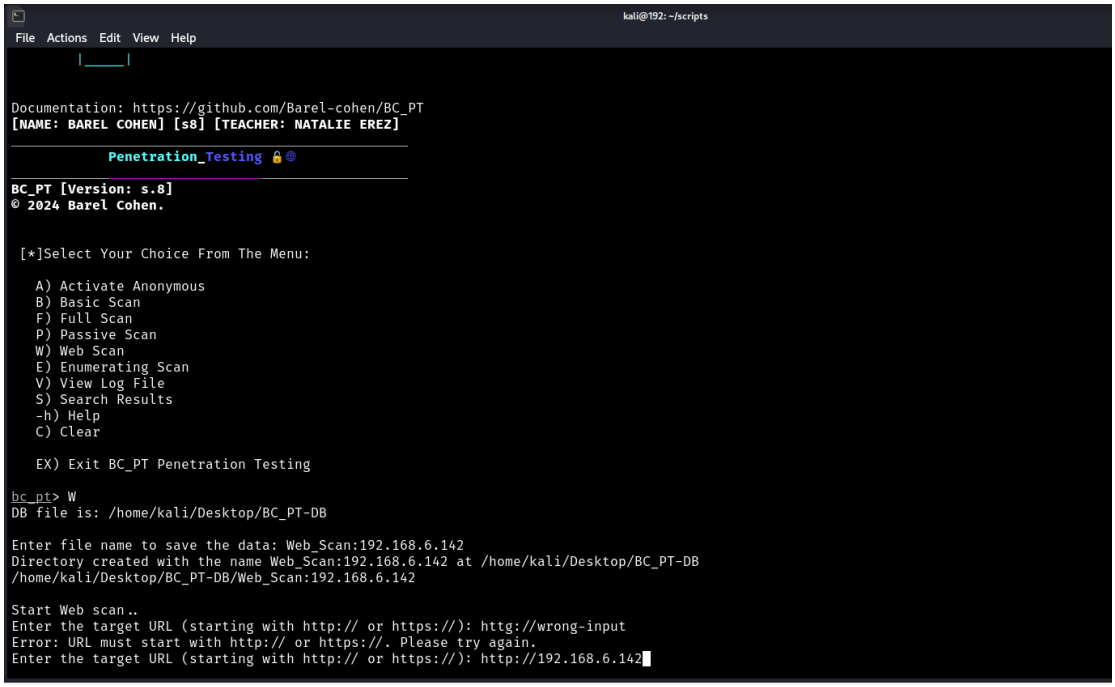

kali@192: ~/scripts
File Actions Edit View Help
Comment: Regards,
Comment: The Google Team
Ref: https://rdap.arin.net/registry/entity/GOGL
OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-650-253-0000
OrgAbuseEmail: network-abuse@google.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE5250-ARIN
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



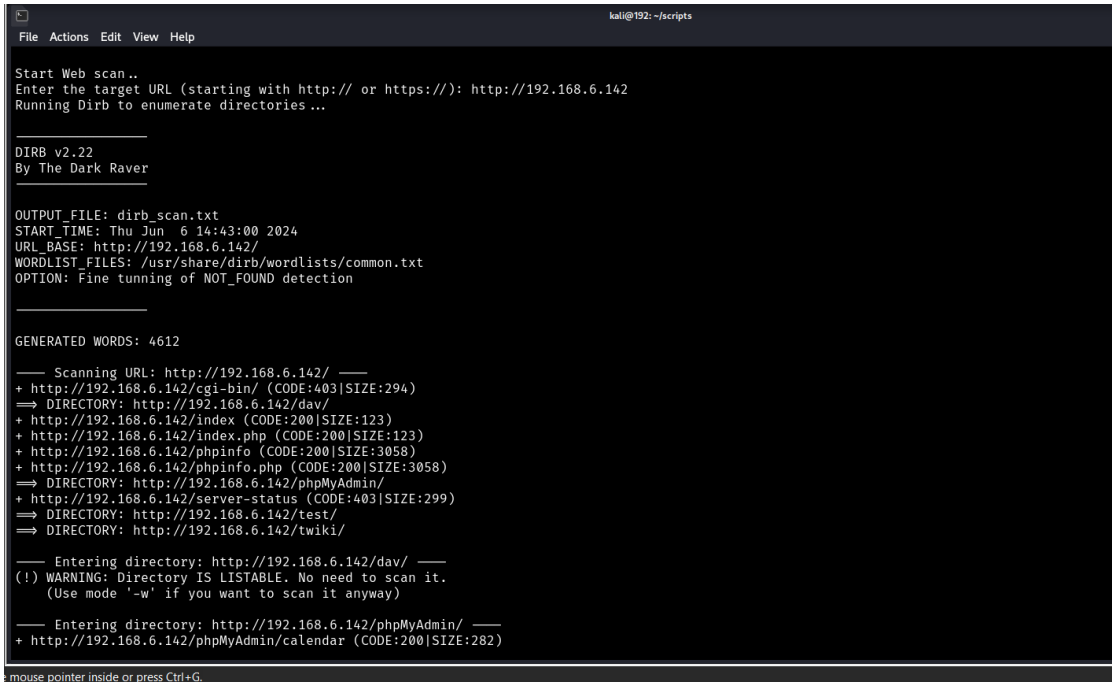
Passive Scan Help Menu

```
[*] 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.
```

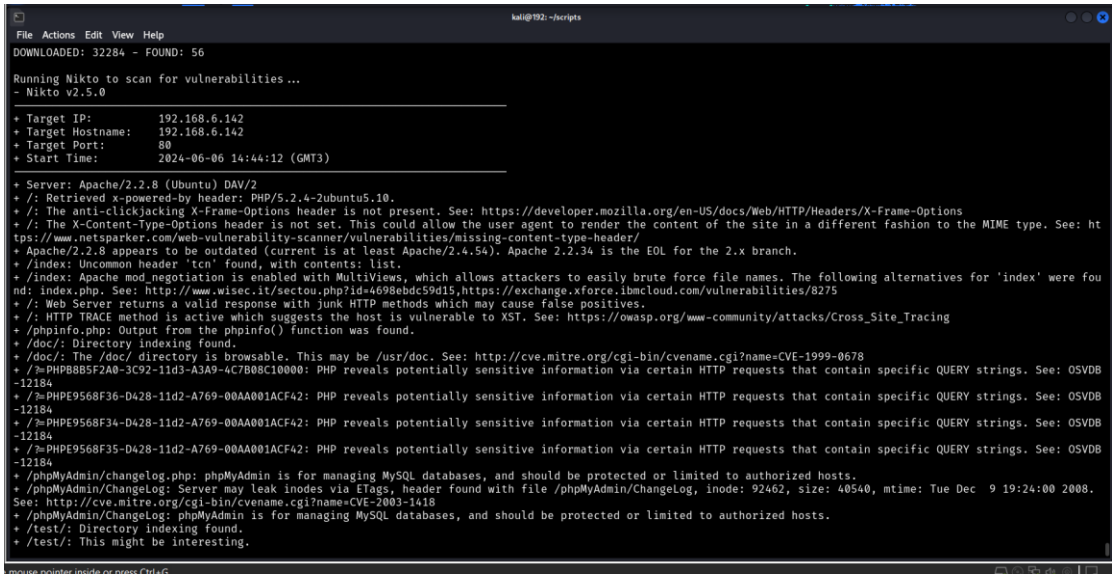
Web Scan

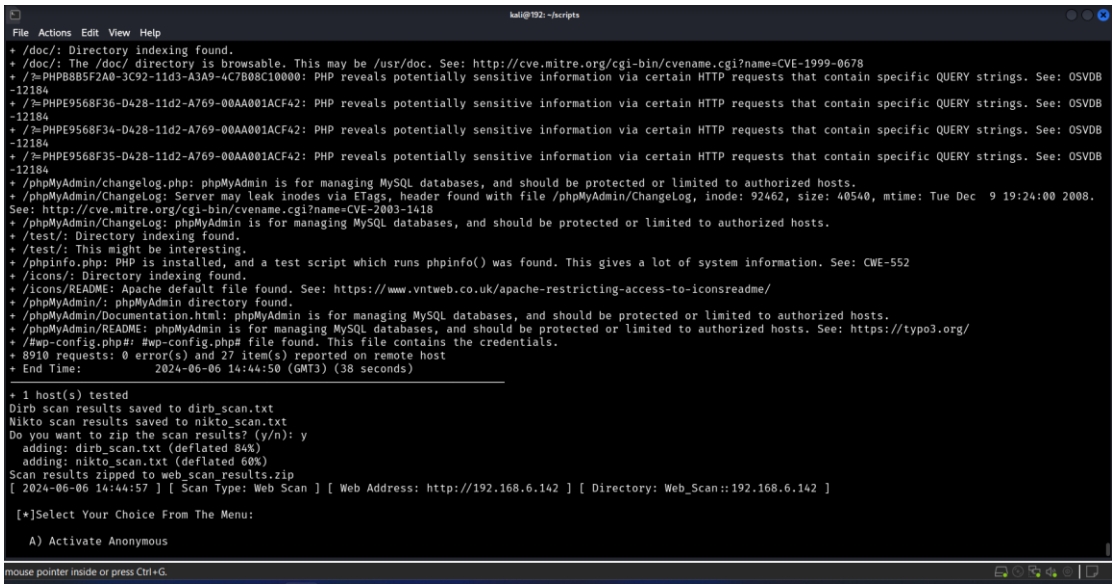


dirb

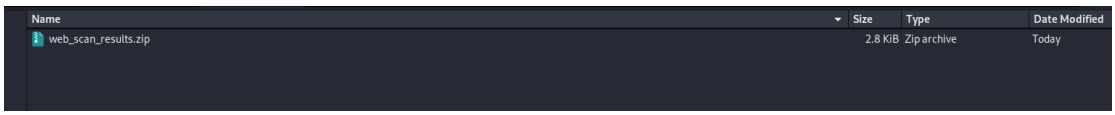


Nikto





if choose y:



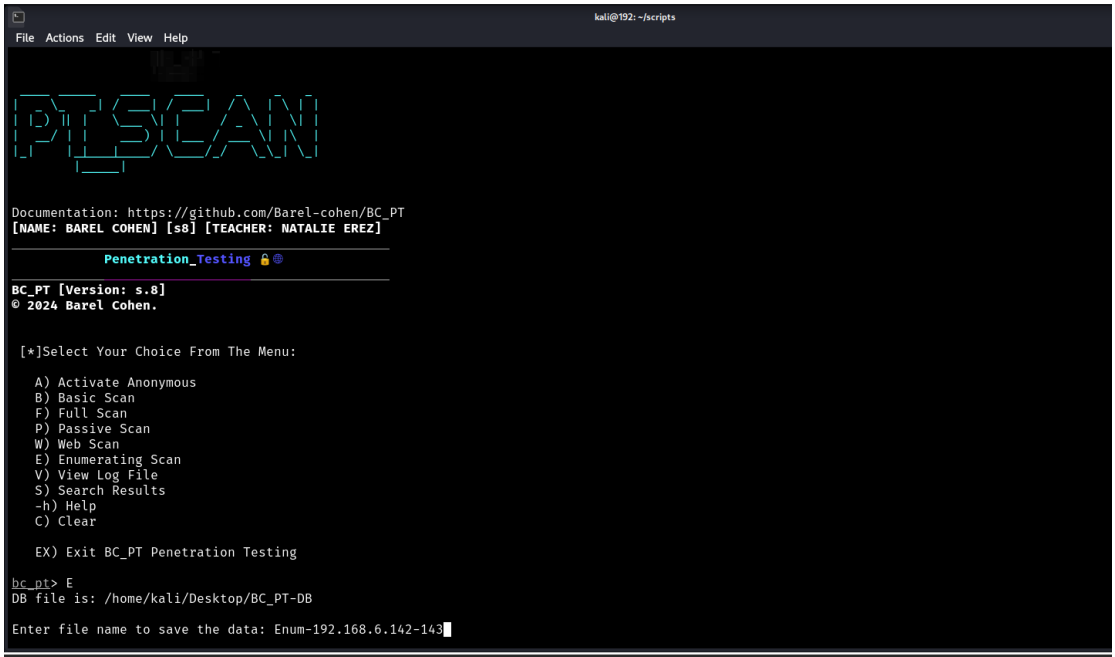
if choose n:

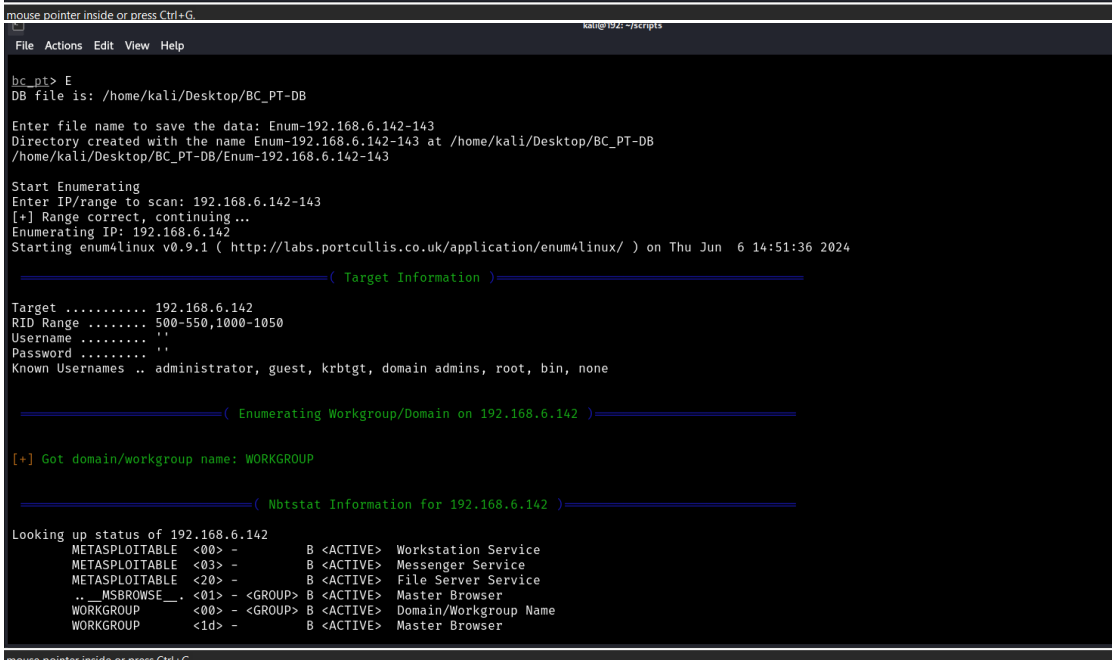
both under the name file you gave at the start

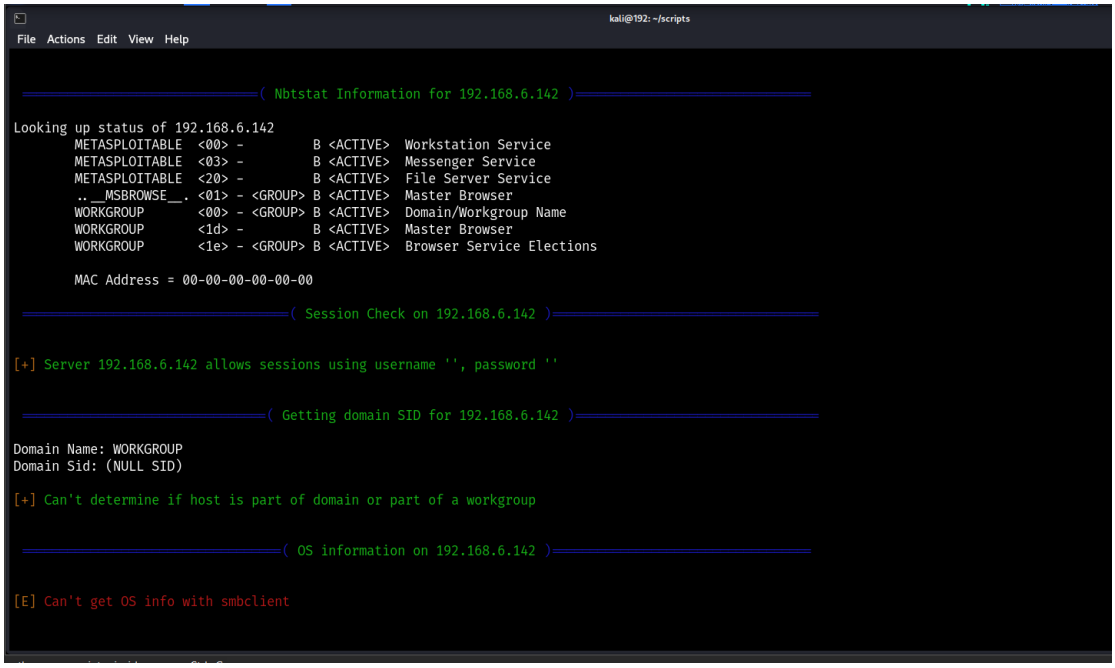
Web Scan Help Menu

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

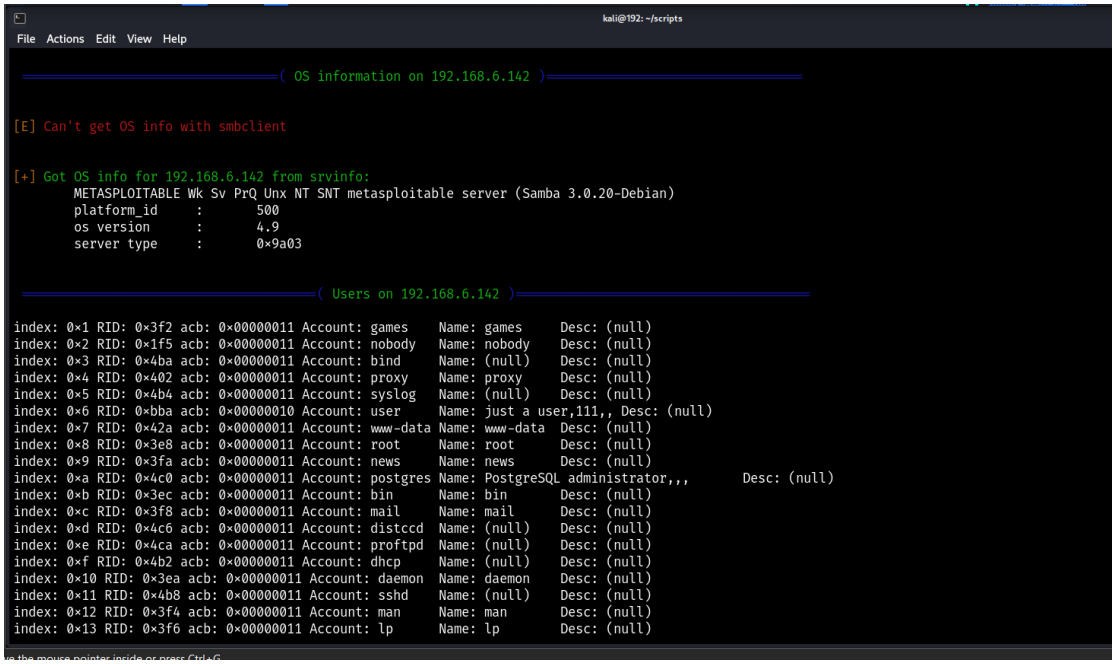
Enumerating Scan



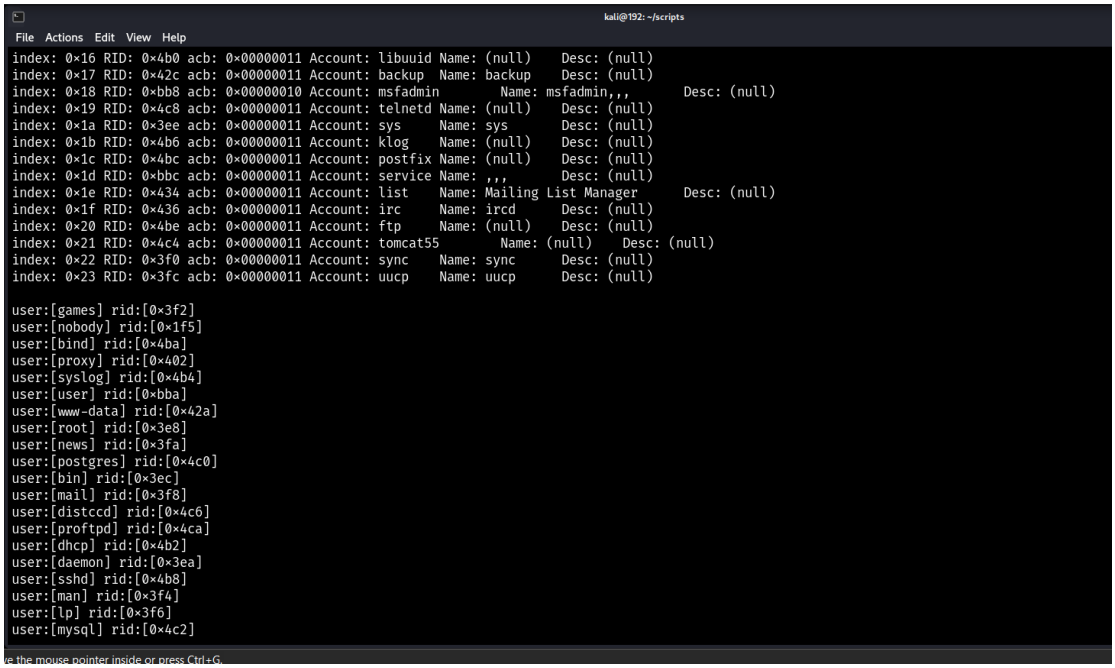




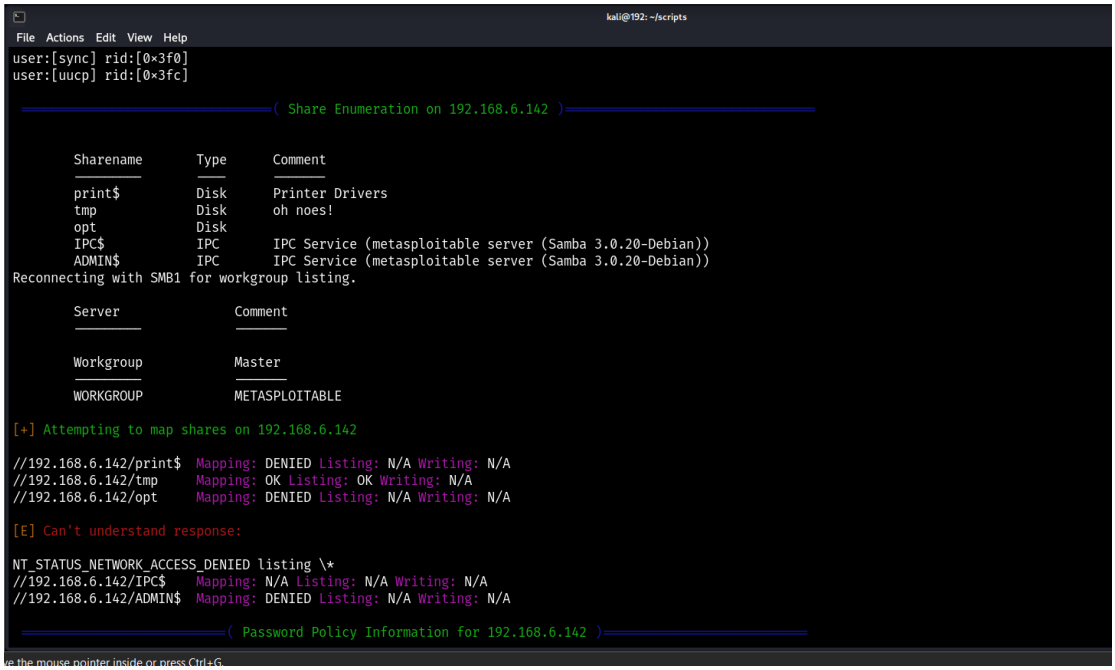
Domain name



Users and rids

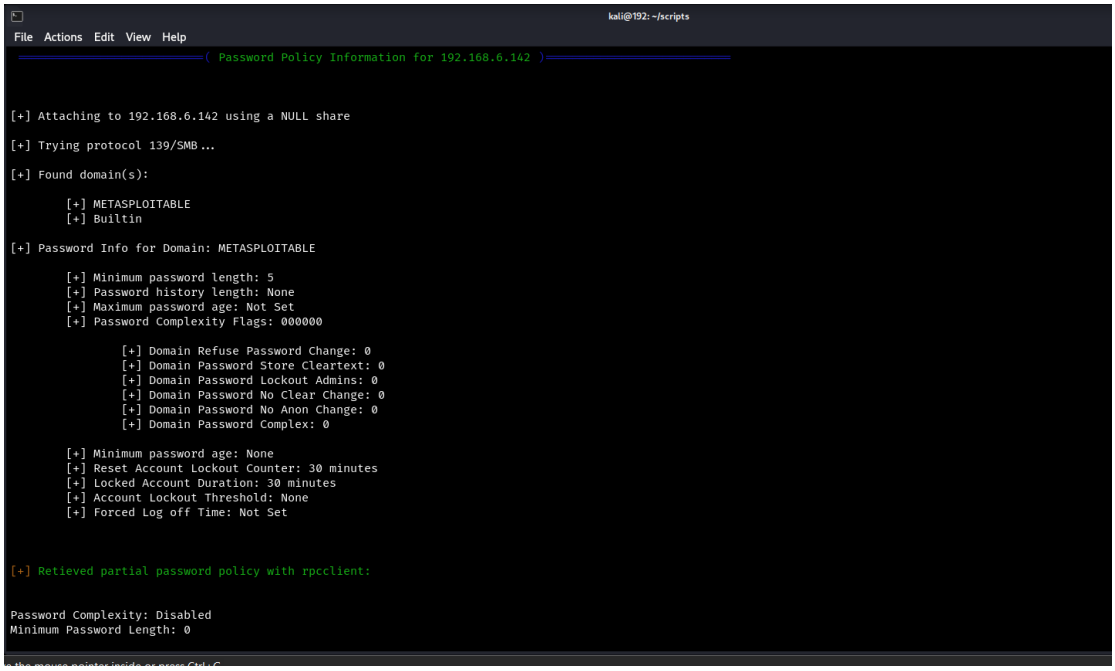


Shared Folders

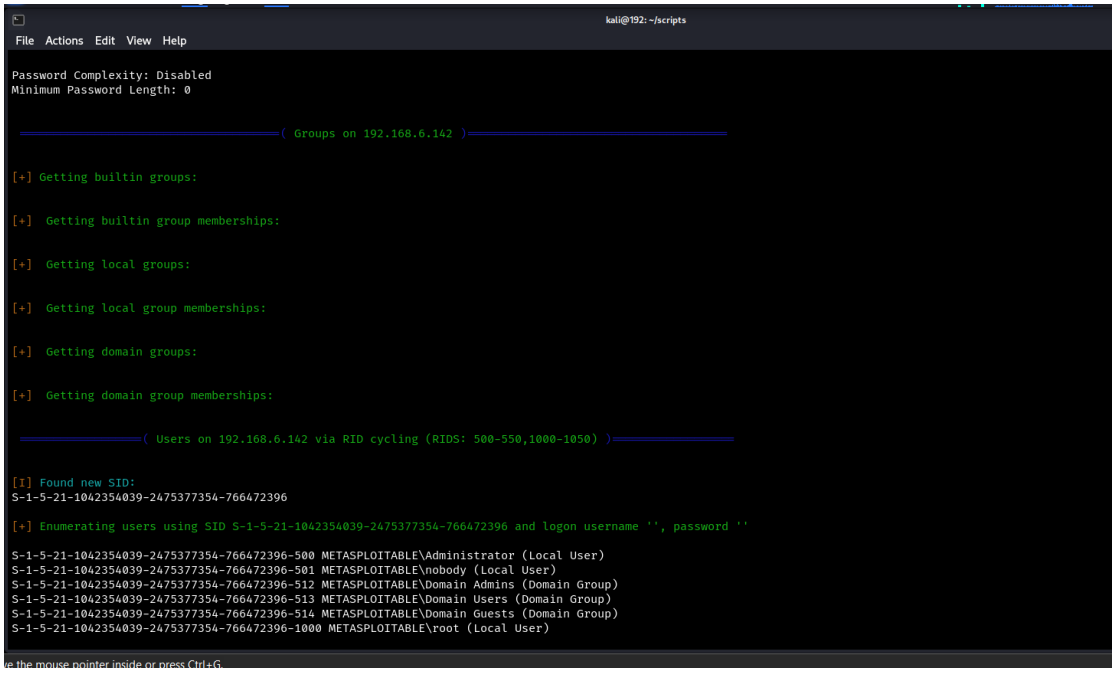


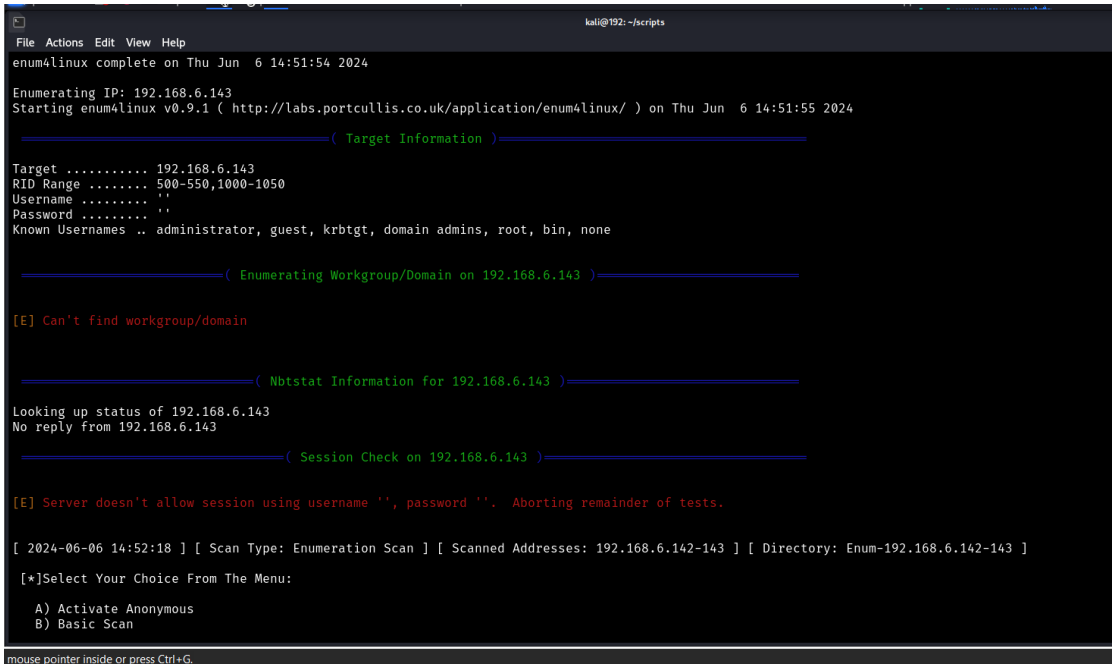
Password Policy

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



Groups and Sids





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

Linkdin: www.linkedin.com/in/barel-cohen-7699b3281

CREDITS:

LOGO CREDIT: https://smashinglogo.com

Ethical Penetration Testing