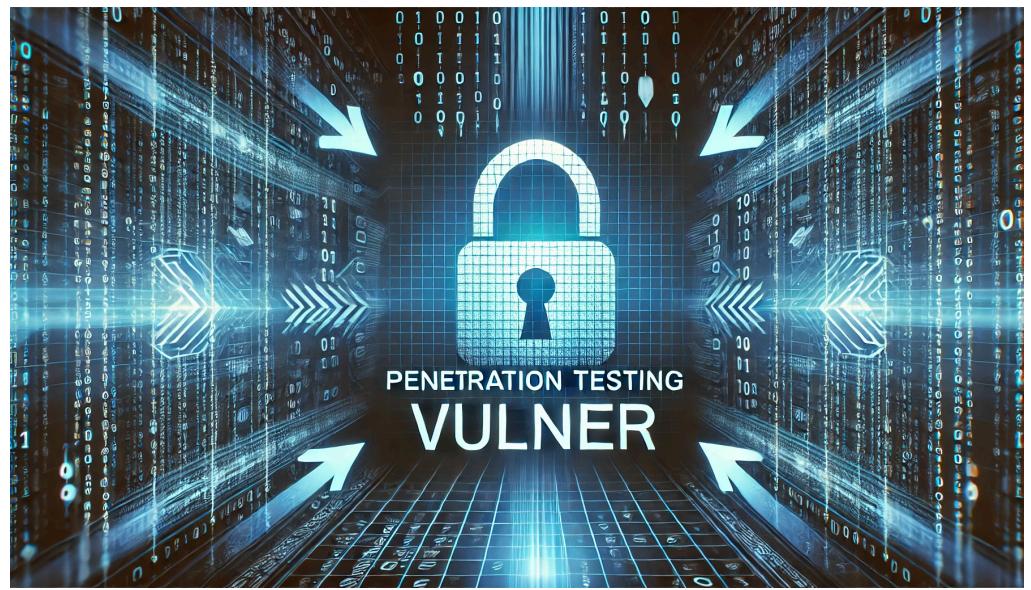


# Project : Vulner



This project focuses on penetration testing and vulnerability assessment using automated tools. It includes:

## Brute-Forcing:

- Allows the user to choose from:
    - rockyou.txt list.
    - Default weak passwords list.
    - A user-supplied list.
  - Includes a specific function for brute-forcing RDP using Hydra tool.

## Tool Checks and Installation:

- Verifies the presence of tools like nmap, hydra, masscan, and searchsploit and installs them if missing.

## Post-Processing:

- Compresses results into a .zip archive for easier sharing or reporting.
  - Offers an optional search function within the results.

```
(root㉿kali)-[~/home/kali/Desktop]
# bash TMagen773632.s16.ZX301.sh
----- Starting START at Mon Feb  3 06:55:25 AM EST 2025 -----


You are root.. continuing..
Enter a valid network (e.g., 10.0.0.0/24): 192.168.44.0/24
Valid network: 192.168.44.0/24
searchsploit is already installed.
hydra is already installed.
nmap is already installed.
masscan is already installed.
Creating a directory for the penetration testing...
Please provide path+name of the output directory (e.g., /home/kali/Desktop/Testing)
Testing
Please choose a mode:
1) Basic - Scans the network for TCP and UDP, including the service version and weak passwords
2) Full - Include NSE, weak passwords, and vulnerability analysis.
Enter your choice (1 or 2):
```

The script checks Root Permission:

- Ensures the script runs with root privileges for proper functionality.

## Network Validation:

- Prompts the user to input a valid network range (e.g., 10.0.0.0/24) and validates it.

## Two Modes of Testing:

### Basic Mode:

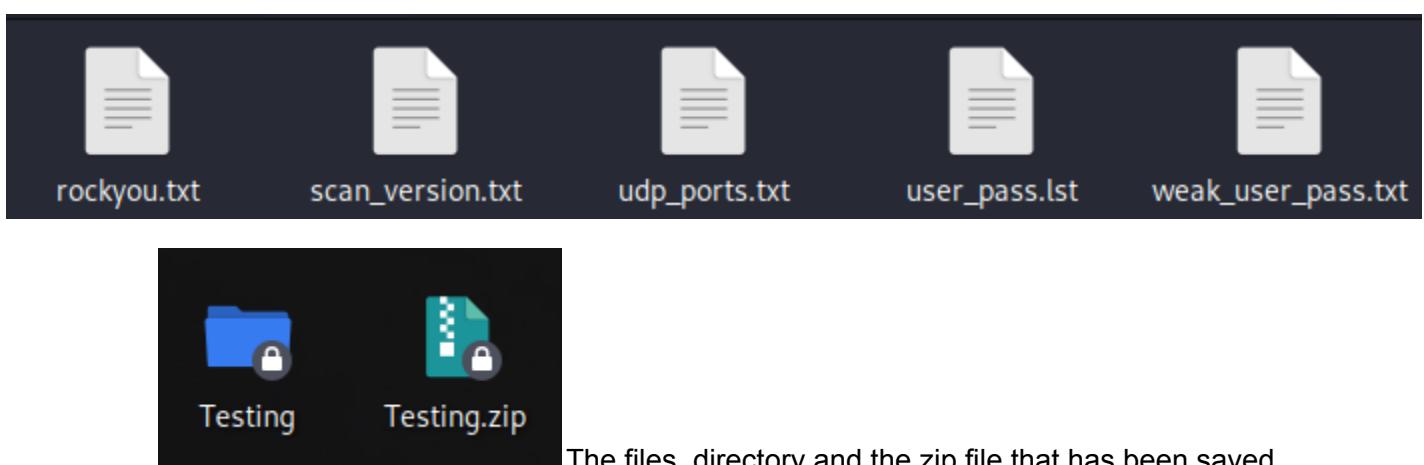
- Performs a simple scan for open TCP/UDP ports using nmap and masscan.
  - Attempts basic brute-forcing for weak credentials.

Full Mode:

- Includes vulnerability scanning with NSE scripts (`nmap --script vuln`) and uses `searchsploit` for exploit matching.
  - Offers an option to brute-force login services like RDP, FTP, SSH, and Telnet.

```
Enter your choice (1 or 2): 1
You selected Basic Mode.
Scanning the network...
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-02-03 15:31:13 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [65535 ports/host]
Detecting weak passwords...
----- Finished at Mon Feb 3 11:04:38 AM EST 2025 -----
The result saved into text files. Would you like to search inside the results? [Y/N]
y
You chose to search in the results files. What keyword would you like to use?
vsftpd
Testing/scan_version.txt:21/tcp open  ftp      vsftpd 3.0.3
Testing/user_pass.lst:21/tcp open  ftp      vsftpd 3.0.3
Now proceeding to save the files into a ZIP archive.
----- Output directory has been zipped to Testing.zip -----
```

- After selecting basic mode, the script runs nmap on the given network with -sV flag to save the services version. Furthermore it extracts weak passwords with NSE brute force. Finally in basic mode the user can search a keyword from every file that has been saved into the directory.



The files, directory and the zip file that has been saved.

```

Enter your choice (1 or 2): 2
You selected Full Mode.
Enter a valid IP address: 192.168.44.133
Scanning the IP address for vulnerabilities and weak passwords...
Potential vulnerabilities via NSE and searchsploit:
-----
Exploit Title | Path
vsftpd 3.0.3 - Remote Denial of Service | multiple/remote/49719.py
-----
Shellcodes: No Results
Exploits: No Results
Shellcodes: No Results
-----
Exploit Title | Path
Apache - Arbitrary Long HTTP Headers (Denial of Service) | multiple/dos/360.pl
Apache - Arbitrary Long HTTP Headers Denial of Service | linux/dos/371.c
Apache 0.8.x/1.0.x / NCSA HTTPd 1.x - 'test-cgi' Directory Listing | cgi/remote/20435.txt
Apache 1.1 / NCSA HTTPd 1.5.2 / Netscape Server 1.12/1.1/2.0 - a nph-test-cg | multiple/dos/19536.txt
Apache 1.3.x < 2.0.48 mod_userdir - Remote Users Disclosure | linux/remote/132.c
Apache 2.0.44 (Linux) - Remote Denial of Service | linux/dos/11.c
Apache 2.0.45 - 'APR' Crash | linux/dos/38.pl
Apache 2.0.49 - Arbitrary Long HTTP Headers Denial of Service | multiple/dos/1056.pl
Apache 2.0.52 - GET Denial of Service | multiple/dos/855.pl
Apache 2.4.23 mod_http2 - Denial of Service | linux/dos/40909.py
Apache 2.x - Memory Leak | windows/dos/9.c
Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE) | multiple/webapps/50383.sh
Apache Httpd mod_proxy - Error Page Cross-Site Scripting | multiple/webapps/47688.md
Apache Httpd mod_rewrite - Open Redirects | multiple/webapps/47689.md
Apache Tomcat mod_jk 1.2.20 - Remote Buffer Overflow (Metasploit) | windows/remote/16798.rb
NCSA 1.3/1.4.x/1.5 / Apache HTTPd 0.8.11/0.8.14 - ScriptAlias Source Retrie | multiple/remote/20595.txt
-----
Shellcodes: No Results
Looking for weak login passwords. For brute-forcing, please choose a password list:
[1] rockyou.txt
[2] Default list
[3] I want to supply my own list

Choose 1, 2, or 3: ■

```

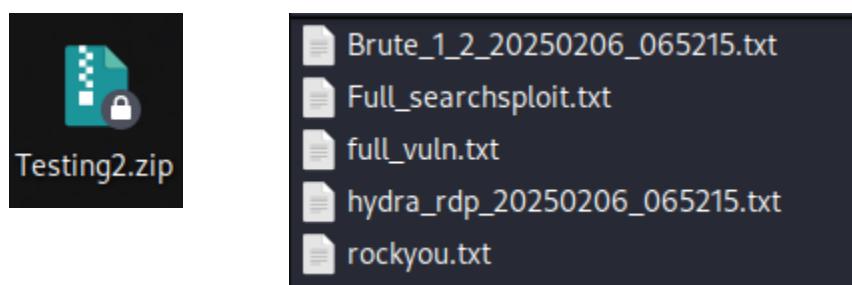
- In Full Mode, the script performs a detailed penetration test by:
  1. Service Detection: Using nmap -sV to identify open ports and service versions.
  2. Brute-Force Testing: Running NSE scripts (e.g., ftp-brute, ssh-brute) to test for weak credentials.
  3. Vulnerability Search: Using searchsploit to identify known exploits for detected services.
  4. For the brute force the user has 3 list options: rockyou.txt, default list (weak credentials) and the last option is to supply a full path to the list.

```
Choose 1, 2, or 3: 1
Using rockyou.txt for brute-forcing.
Would you like to brute-force RDP service? [y/n] y
You chose to brute force RDP service. Please wait.
Starting Hydra brute-force for RDP service... Do you want to use rockyou.txt file or your own? p
/home/kali/Desktop/rockyou.txt
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-06 07:13:13
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 205761782671201 login tries (l:14344399/p:1434
[DATA] attacking rdp://192.168.44.133:3389/
[3389][rdp] account on 192.168.44.133 might be valid but account not active for remote desktop:
[3389][rdp] account on 192.168.44.133 might be valid but account not active for remote desktop:
```

- The script in the brute force phase, asks the user if he/she would like to brute-rdp service. Therefore the script uses hydra to brute force rdp service. The user needs to choose a list to brute force with.

```
^CHydra brute-force completed. Results saved in Testing2/hydra_rdp_20250206_065215.txt
----- Finished at Thu Feb 6 10:40:22 AM EST 2025 -----
The result saved into text files. Would you like to search inside the results? [Y/N]
y
You chose to search in the results files. What keyword would you like to use?
vsftpd
Testing2/Brute_1_2_20250206_065215.txt:21/tcp open  ftp      vsftpd 3.0.3
Testing2/Brute_1_2_20250206_065215.txt:21/tcp open  ftp      vsftpd 3.0.3
Testing2/Brute_1_2_20250206_065215.txt:21/tcp open  ftp      vsftpd 3.0.3
Testing2/Full_searchsploit.txt:vsftpd 3.0.3 - Remote Denial of Service
multiple/remote/49719.py
Testing2/full_vuln.txt:21/tcp open  ftp      vsftpd 3.0.3
Now proceeding to save the files into a ZIP archive.
----- Output directory has been zipped to Testing2.zip -----
```

- After performing brute force, the user can search keyword in all of the files created.



- The directory is compressed into a ZIP file with all the data that has been investigated.