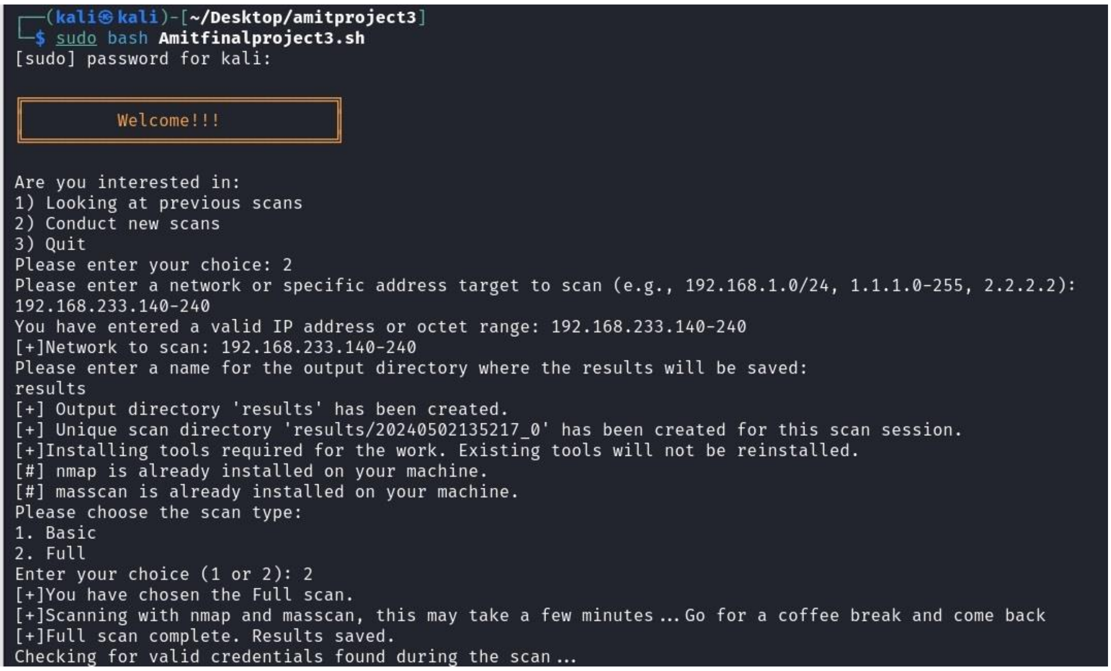
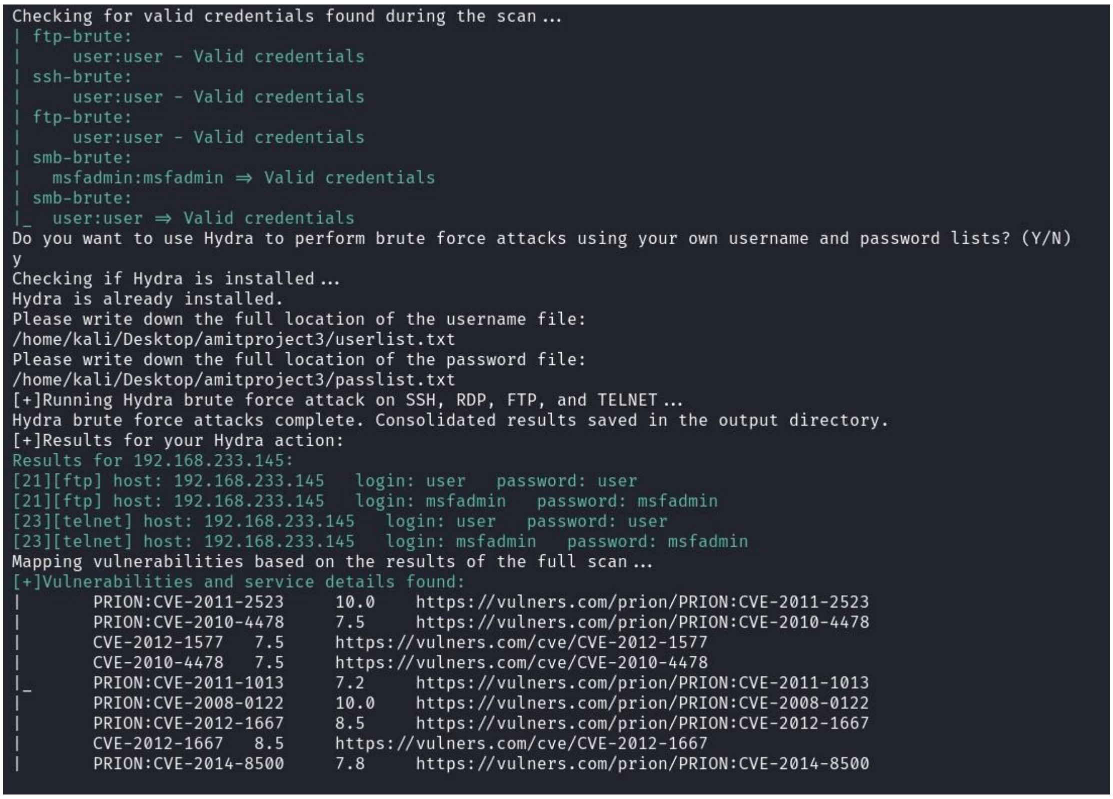
VULNERABILITIES TOOL PROJECT - AMIT PERSKY

This project involves creating a script for comprehensive network device mapping, identifying ports, services, and vulnerabilities. The user defines the network range, after which the program deploys tools like nmap and masscan for scanning and mapping purposes, storing the data in a newly created directory. The script also probes for network vulnerabilities, employing nmap, searchsploit, hydra, and medusa to identify security gaps, such as weak passwords. Finally, the scan summary and findings are presented to the user.

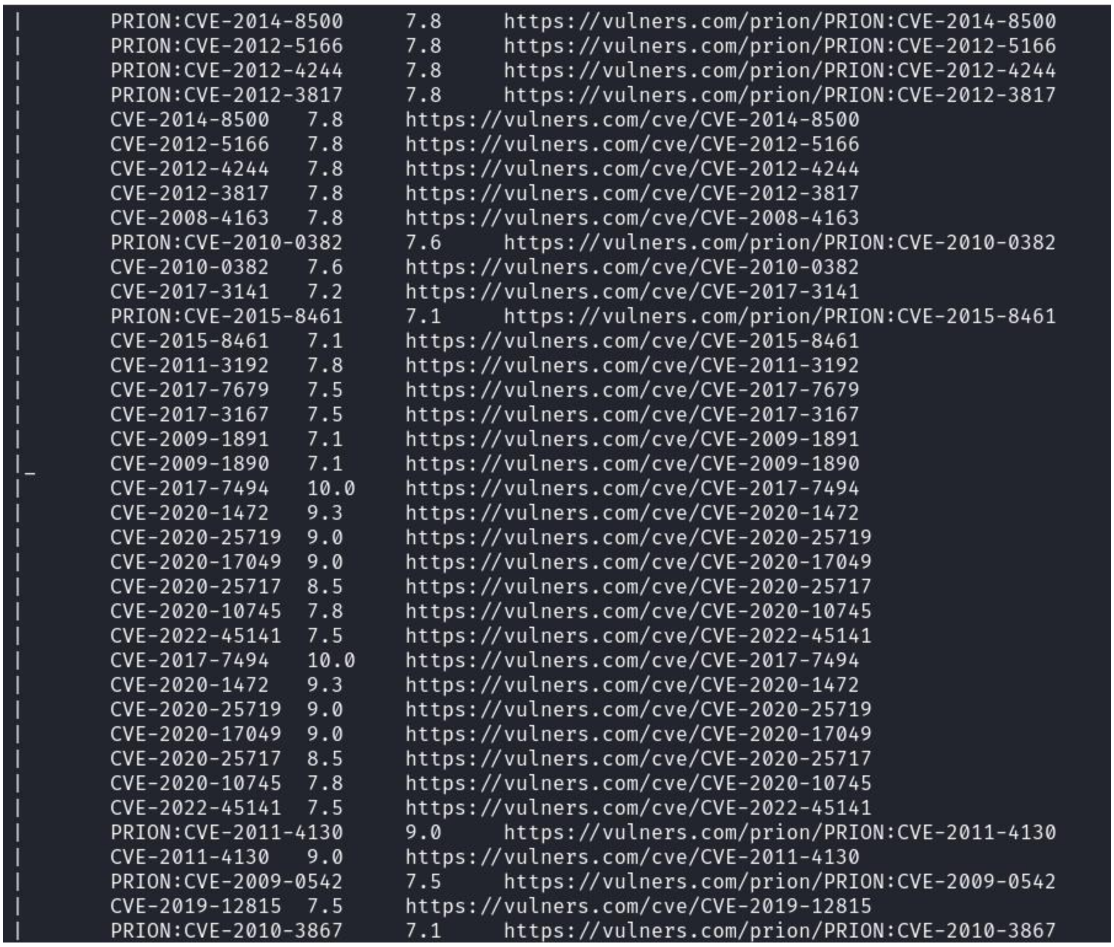
Output of my script:



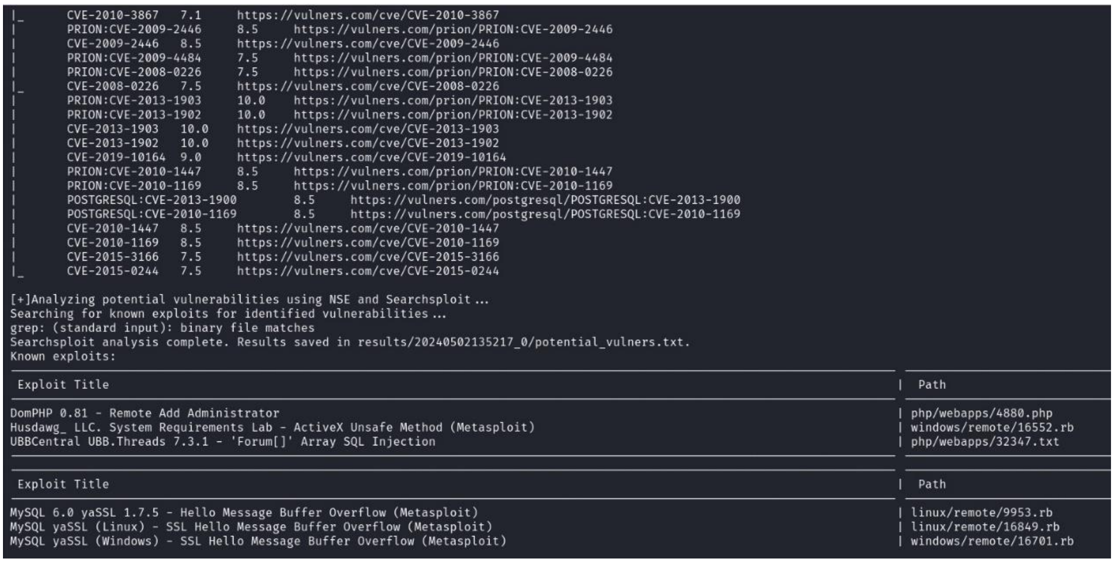
```
┌──(kali㉿kali)-[~/Desktop/amitproject3]
└─$ sudo bash Amitfinalproject3.sh
[sudo] password for kali:

        Welcome!!!

Are you interested in:
1) Looking at previous scans
2) Conduct new scans
3) Quit
Please enter your choice: 2
Please enter a network or specific address target to scan (e.g., 192.168.1.0/24, 1.1.1.0-255, 2.2.2.2):
192.168.233.140-240
You have entered a valid IP address or octet range: 192.168.233.140-240
[+]Network to scan: 192.168.233.140-240
Please enter a name for the output directory where the results will be saved:
results
[+] Output directory 'results' has been created.
[+] Unique scan directory 'results/20240502135217_0' has been created for this scan session.
[+]Installing tools required for the work. Existing tools will not be reinstalled.
[#] nmap is already installed on your machine.
[#] masscan is already installed on your machine.
Please choose the scan type:
1. Basic
2. Full
Enter your choice (1 or 2): 2
[+]You have chosen the Full scan.
[+]Scanning with nmap and masscan, this may take a few minutes ... Go for a coffee break and come back
[+]Full scan complete. Results saved.
Checking for valid credentials found during the scan ...
```



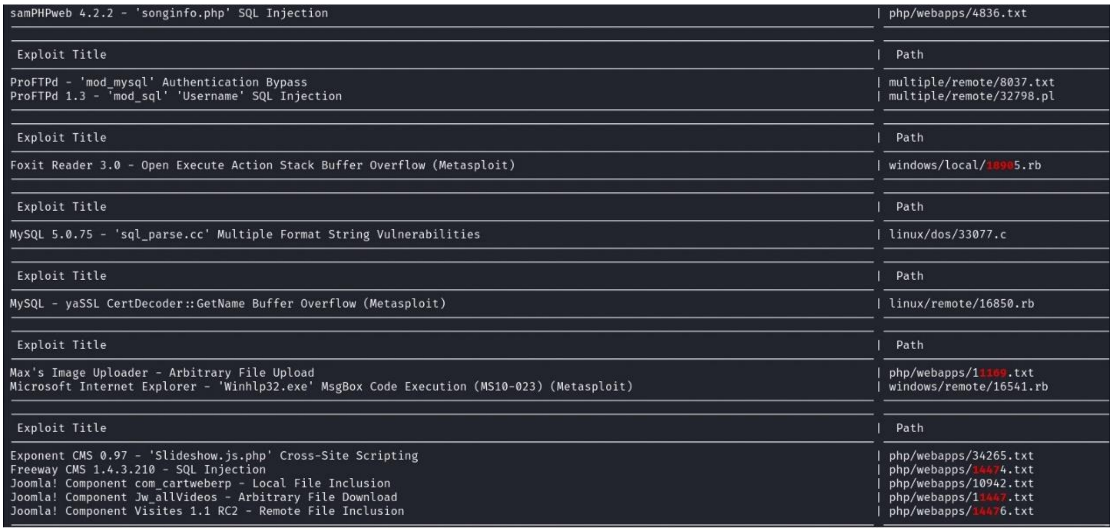
```
Checking for valid credentials found during the scan ...
| ftp-brute:
|     user:user - Valid credentials
| ssh-brute:
|     user:user - Valid credentials
| ftp-brute:
|     user:user - Valid credentials
| smb-brute:
|   msfadmin:msfadmin => Valid credentials
| smb-brute:
|_  user:user => Valid credentials
Do you want to use Hydra to perform brute force attacks using your own username and password lists? (Y/N)
y
Checking if Hydra is installed ...
Hydra is already installed.
Please write down the full location of the username file:
/home/kali/Desktop/amitproject3/userlist.txt
Please write down the full location of the password file:
/home/kali/Desktop/amitproject3/passlist.txt
[+]Running Hydra brute force attack on SSH, RDP, FTP, and TELNET ...
Hydra brute force attacks complete. Consolidated results saved in the output directory.
[+]Results for your Hydra action:
Results for 192.168.233.145:
[21][ftp] host: 192.168.233.145   login: user   password: user
[21][ftp] host: 192.168.233.145   login: msfadmin   password: msfadmin
[23][telnet] host: 192.168.233.145   login: user   password: user
[23][telnet] host: 192.168.233.145   login: msfadmin   password: msfadmin
Mapping vulnerabilities based on the results of the full scan ...
[+]Vulnerabilities and service details found:
|       PRION:CVE-2011-2523     10.0    https://vulners.com/prion/PRION:CVE-2011-2523
|       PRION:CVE-2010-4478     7.5     https://vulners.com/prion/PRION:CVE-2010-4478
|       CVE-2012-1577   7.5     https://vulners.com/cve/CVE-2012-1577
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|_      PRION:CVE-2011-1013     7.2     https://vulners.com/prion/PRION:CVE-2011-1013
|       PRION:CVE-2008-0122     10.0    https://vulners.com/prion/PRION:CVE-2008-0122
|       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
|       PRION:CVE-2014-8500     7.8     https://vulners.com/prion/PRION:CVE-2014-8500
```



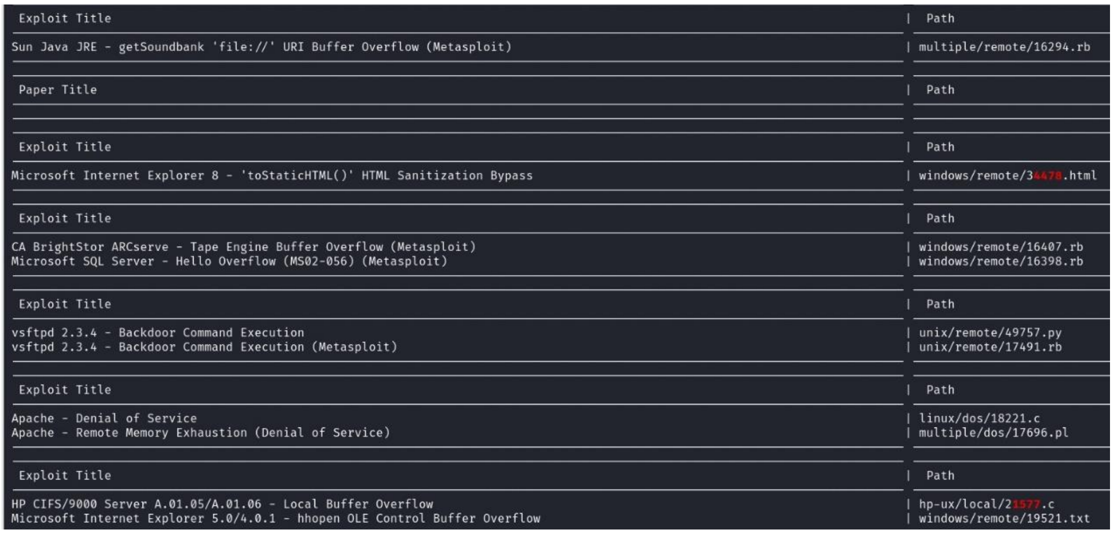
```
|       PRION:CVE-2014-8500     7.8     https://vulners.com/prion/PRION:CVE-2014-8500
|       PRION:CVE-2012-5166     7.8     https://vulners.com/prion/PRION:CVE-2012-5166
|       PRION:CVE-2012-4244     7.8     https://vulners.com/prion/PRION:CVE-2012-4244
|       PRION:CVE-2012-3817     7.8     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
|       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
|       CVE-2015-8461   7.1     https://vulners.com/cve/CVE-2015-8461
|       CVE-2011-3192   7.8     https://vulners.com/cve/CVE-2011-3192
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-3167   7.5     https://vulners.com/cve/CVE-2017-3167
|       CVE-2009-1891   7.1     https://vulners.com/cve/CVE-2009-1891
|_      CVE-2009-1890   7.1     https://vulners.com/cve/CVE-2009-1890
|       CVE-2017-7494   10.0    https://vulners.com/cve/CVE-2017-7494
|       CVE-2020-1472   9.3     https://vulners.com/cve/CVE-2020-1472
|       CVE-2020-25719  9.0     https://vulners.com/cve/CVE-2020-25719
|       CVE-2020-17049  9.0     https://vulners.com/cve/CVE-2020-17049
|       CVE-2020-25717  8.5     https://vulners.com/cve/CVE-2020-25717
|       CVE-2020-10745  7.8     https://vulners.com/cve/CVE-2020-10745
|       CVE-2022-45141  7.5     https://vulners.com/cve/CVE-2022-45141
|       CVE-2017-7494   10.0    https://vulners.com/cve/CVE-2017-7494
|       CVE-2020-1472   9.3     https://vulners.com/cve/CVE-2020-1472
|       CVE-2020-25719  9.0     https://vulners.com/cve/CVE-2020-25719
|       CVE-2020-17049  9.0     https://vulners.com/cve/CVE-2020-17049
|       CVE-2020-25717  8.5     https://vulners.com/cve/CVE-2020-25717
|       CVE-2020-10745  7.8     https://vulners.com/cve/CVE-2020-10745
|       CVE-2022-45141  7.5     https://vulners.com/cve/CVE-2022-45141
|       PRION:CVE-2011-4130     9.0     https://vulners.com/prion/PRION:CVE-2011-4130
|       CVE-2011-4130   9.0     https://vulners.com/cve/CVE-2011-4130
|       PRION:CVE-2009-0542     7.5     https://vulners.com/prion/PRION:CVE-2009-0542
|       CVE-2019-12815  7.5     https://vulners.com/cve/CVE-2019-12815
|       PRION:CVE-2010-3867     7.1     https://vulners.com/prion/PRION:CVE-2010-3867
```



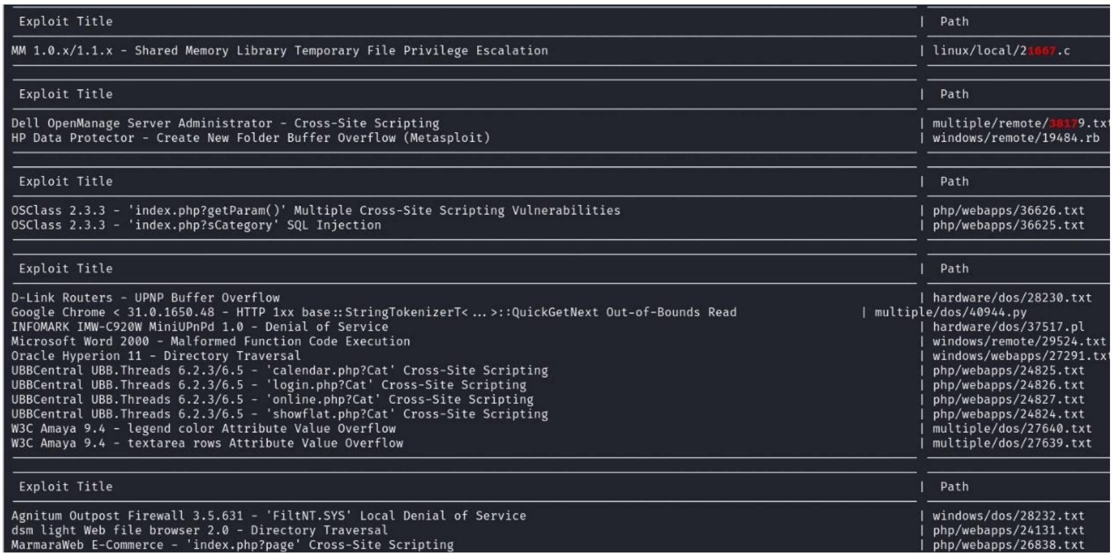
```
|_      CVE-2010-3867   7.1     https://vulners.com/cve/CVE-2010-3867
|       PRION:CVE-2009-2446     8.5     https://vulners.com/prion/PRION:CVE-2009-2446
|       CVE-2009-2446   8.5     https://vulners.com/cve/CVE-2009-2446
|       PRION:CVE-2009-4484     7.5     https://vulners.com/prion/PRION:CVE-2009-4484
|       PRION:CVE-2008-0226     7.5     https://vulners.com/prion/PRION:CVE-2008-0226
|_      CVE-2008-0226   7.5     https://vulners.com/cve/CVE-2008-0226
|       PRION:CVE-2013-1903     10.0    https://vulners.com/prion/PRION:CVE-2013-1903
|       PRION:CVE-2013-1902     10.0    https://vulners.com/prion/PRION:CVE-2013-1902
|       CVE-2013-1903   10.0    https://vulners.com/cve/CVE-2013-1903
|       CVE-2013-1902   10.0    https://vulners.com/cve/CVE-2013-1902
|       CVE-2019-10164  9.0     https://vulners.com/cve/CVE-2019-10164
|       PRION:CVE-2010-1447     8.5     https://vulners.com/prion/PRION:CVE-2010-1447
|       PRION:CVE-2010-1169     8.5     https://vulners.com/prion/PRION:CVE-2010-1169
|       POSTGRESQL:CVE-2013-1900        8.5     https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900
|       POSTGRESQL:CVE-2010-1169        8.5     https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169
|       CVE-2010-1447   8.5     https://vulners.com/cve/CVE-2010-1447
|       CVE-2010-1169   8.5     https://vulners.com/cve/CVE-2010-1169
|       CVE-2015-3166   7.5     https://vulners.com/cve/CVE-2015-3166
|_      CVE-2015-0244   7.5     https://vulners.com/cve/CVE-2015-0244

[+]Analyzing potential vulnerabilities using NSE and Searchsploit...
Searching for known exploits for identified vulnerabilities...
grep: (standard input): binary file matches
Searchsploit analysis complete. Results saved in results/20240502135217_0/potential_vulners.txt.
Known exploits:
------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------
DomPHP 0.81 - Remote Add Administrator                                                    | php/webapps/4880.php
Husdawg_ LLC. System Requirements Lab - ActiveX Unsafe Method (Metasploit)                | windows/remote/16552.rb
UBBCentral UBB.Threads 7.3.1 - 'Forum[]' Array SQL Injection                              | php/webapps/32347.txt
------------------------------------------------------------------------------------------ ---------------------------
------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------
MySQL 6.0 yaSSL 1.7.5 - Hello Message Buffer Overflow (Metasploit)                        | linux/remote/9953.rb
MySQL yaSSL (Linux) - SSL Hello Message Buffer Overflow (Metasploit)                      | linux/remote/16849.rb
MySQL yaSSL (Windows) - SSL Hello Message Buffer Overflow (Metasploit)                    | windows/remote/16701.rb
```



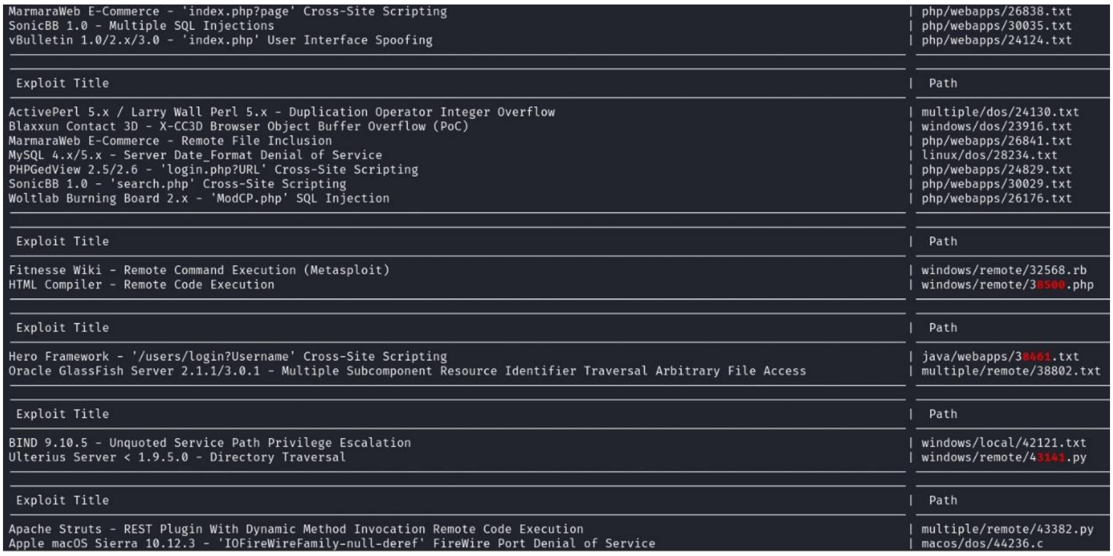
```
samPHPweb 4.2.2 - 'songinfo.php' SQL Injection                                                     | php/webapps/4836.txt

 Exploit Title                                                                                     |  Path

ProFTPd - 'mod_mysql' Authentication Bypass                                                        | multiple/remote/8037.txt
ProFTPd 1.3 - 'mod_sql' 'Username' SQL Injection                                                   | multiple/remote/32798.pl

 Exploit Title                                                                                     |  Path

Foxit Reader 3.0 - Open Execute Action Stack Buffer Overflow (Metasploit)                          | windows/local/18905.rb

 Exploit Title                                                                                     |  Path

MySQL 5.0.75 - 'sql_parse.cc' Multiple Format String Vulnerabilities                               | linux/dos/33077.c

 Exploit Title                                                                                     |  Path

MySQL - yaSSL CertDecoder::GetName Buffer Overflow (Metasploit)                                    | linux/remote/16850.rb

 Exploit Title                                                                                     |  Path

Max's Image Uploader - Arbitrary File Upload                                                       | php/webapps/11169.txt
Microsoft Internet Explorer - 'Winhlp32.exe' MsgBox Code Execution (MS10-023) (Metasploit)         | windows/remote/16541.rb

 Exploit Title                                                                                     |  Path

Exponent CMS 0.97 - 'Slideshow.js.php' Cross-Site Scripting                                        | php/webapps/34265.txt
Freeway CMS 1.4.3.210 - SQL Injection                                                              | php/webapps/14474.txt
Joomla! Component com_cartweberp - Local File Inclusion                                            | php/webapps/10942.txt
Joomla! Component Jw_allVideos - Arbitrary File Download                                           | php/webapps/11447.txt
Joomla! Component Visites 1.1 RC2 - Remote File Inclusion                                          | php/webapps/14476.txt
```



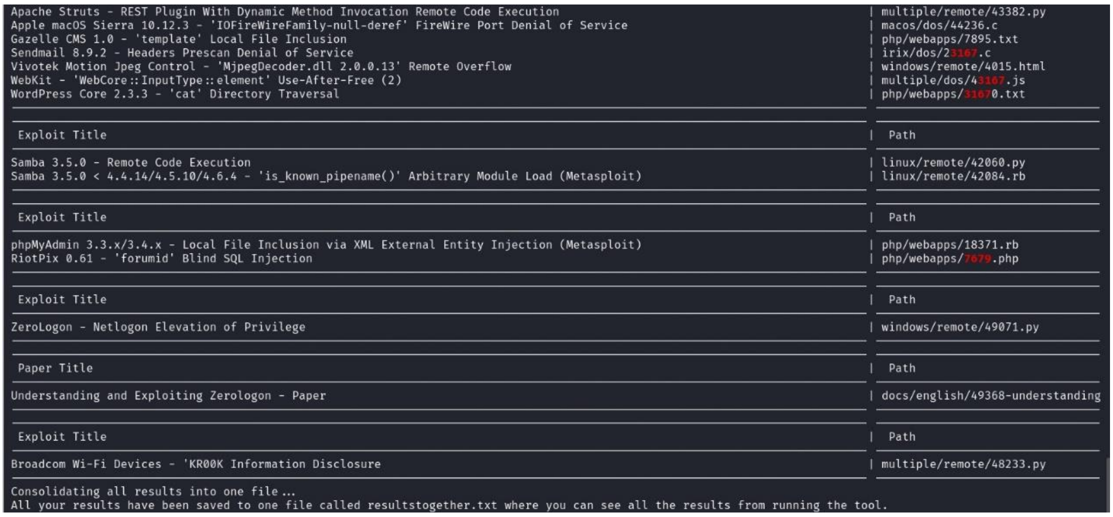
```
 Exploit Title                                                                                        |  Path

Sun Java JRE - getSoundbank 'file://' URI Buffer Overflow (Metasploit)                                | multiple/remote/16294.rb

 Paper Title                                                                                          |  Path


 Exploit Title                                                                                        |  Path

Microsoft Internet Explorer 8 - 'toStaticHTML()' HTML Sanitization Bypass                             | windows/remote/34478.html

 Exploit Title                                                                                        |  Path

CA BrightStor ARCserve - Tape Engine Buffer Overflow (Metasploit)                                     | windows/remote/16407.rb
Microsoft SQL Server - Hello Overflow (MS02-056) (Metasploit)                                         | windows/remote/16398.rb

 Exploit Title                                                                                        |  Path

vsftpd 2.3.4 - Backdoor Command Execution                                                             | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                                | unix/remote/17491.rb

 Exploit Title                                                                                        |  Path

Apache - Denial of Service                                                                            | linux/dos/18221.c
Apache - Remote Memory Exhaustion (Denial of Service)                                                 | multiple/dos/17696.pl

 Exploit Title                                                                                        |  Path

HP CIFS/9000 Server A.01.05/A.01.06 - Local Buffer Overflow                                           | hp-ux/local/21577.c
Microsoft Internet Explorer 5.0/4.0.1 - hhopen OLE Control Buffer Overflow                            | windows/remote/19521.txt
```



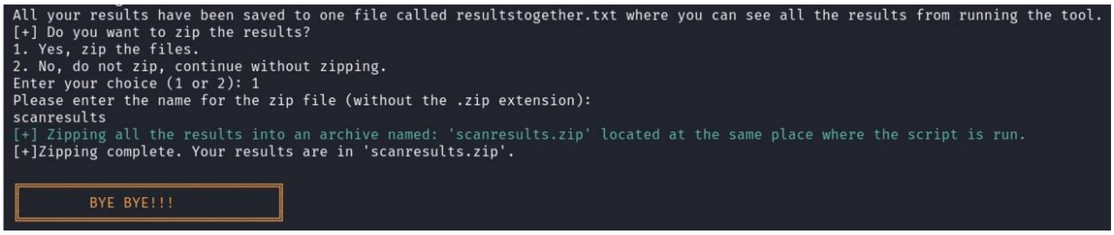
```
 Exploit Title                                                                                         |  Path

MM 1.0.x/1.1.x - Shared Memory Library Temporary File Privilege Escalation                             | linux/local/21667.c

 Exploit Title                                                                                         |  Path

Dell OpenManage Server Administrator - Cross-Site Scripting                                            | multiple/remote/38179.tx
HP Data Protector - Create New Folder Buffer Overflow (Metasploit)                                     | windows/remote/19484.rb

 Exploit Title                                                                                         |  Path

OSClass 2.3.3 - 'index.php?getParam()' Multiple Cross-Site Scripting Vulnerabilities                   | php/webapps/36626.txt
OSClass 2.3.3 - 'index.php?sCategory' SQL Injection                                                    | php/webapps/36625.txt

 Exploit Title                                                                                         |  Path

D-Link Routers - UPNP Buffer Overflow                                                                  | hardware/dos/28230.txt
Google Chrome < 31.0.1650.48 - HTTP 1xx base::StringTokenizerT<...>::QuickGetNext Out-of-Bounds Read          | multiple/dos/40944.py
INFOMARK IMW-C920W MiniUPnPd 1.0 - Denial of Service                                                   | hardware/dos/37517.pl
Microsoft Word 2000 - Malformed Function Code Execution                                                | windows/remote/29524.txt
Oracle Hyperion 11 - Directory Traversal                                                               | windows/webapps/27291.tx
UBBCentral UBB.Threads 6.2.3/6.5 - 'calendar.php?Cat' Cross-Site Scripting                             | php/webapps/24825.txt
UBBCentral UBB.Threads 6.2.3/6.5 - 'login.php?Cat' Cross-Site Scripting                                | php/webapps/24826.txt
UBBCentral UBB.Threads 6.2.3/6.5 - 'online.php?Cat' Cross-Site Scripting                               | php/webapps/24827.txt
UBBCentral UBB.Threads 6.2.3/6.5 - 'showflat.php?Cat' Cross-Site Scripting                             | php/webapps/24824.txt
W3C Amaya 9.4 - legend color Attribute Value Overflow                                                  | multiple/dos/27640.txt
W3C Amaya 9.4 - textarea rows Attribute Value Overflow                                                 | multiple/dos/27639.txt

 Exploit Title                                                                                         |  Path

Agnitum Outpost Firewall 3.5.631 - 'FiltNT.SYS' Local Denial of Service                                | windows/dos/28232.txt
dsm light Web file browser 2.0 - Directory Traversal                                                   | php/webapps/24131.txt
MarmaraWeb E-Commerce - 'index.php?page' Cross-Site Scripting                                          | php/webapps/26838.txt
```



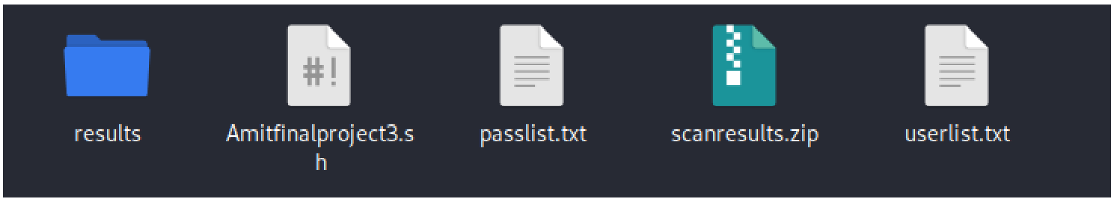
```
MarmaraWeb E-Commerce - 'index.php?page' Cross-Site Scripting                              | php/webapps/26838.txt
SonicBB 1.0 - Multiple SQL Injections                                                      | php/webapps/30035.txt
vBulletin 1.0/2.x/3.0 - 'index.php' User Interface Spoofing                                | php/webapps/24124.txt

 Exploit Title                                                                             |  Path

ActivePerl 5.x / Larry Wall Perl 5.x - Duplication Operator Integer Overflow               | multiple/dos/24130.txt
Blaxxun Contact 3D - X-CC3D Browser Object Buffer Overflow (PoC)                           | windows/dos/23916.txt
MarmaraWeb E-Commerce - Remote File Inclusion                                              | php/webapps/26841.txt
MySQL 4.x/5.x - Server Date_Format Denial of Service                                       | linux/dos/28234.txt
PHPGedView 2.5/2.6 - 'login.php?URL' Cross-Site Scripting                                  | php/webapps/24829.txt
SonicBB 1.0 - 'search.php' Cross-Site Scripting                                            | php/webapps/30029.txt
Woltlab Burning Board 2.x - 'ModCP.php' SQL Injection                                      | php/webapps/26176.txt

 Exploit Title                                                                             |  Path

Fitnesse Wiki - Remote Command Execution (Metasploit)                                      | windows/remote/32568.rb
HTML Compiler - Remote Code Execution                                                      | windows/remote/38500.php

 Exploit Title                                                                             |  Path

Hero Framework - '/users/login?Username' Cross-Site Scripting                              | java/webapps/38461.txt
Oracle GlassFish Server 2.1.1/3.0.1 - Multiple Subcomponent Resource Identifier Traversal Arbitrary File Access | multiple/remote/38802.txt

 Exploit Title                                                                             |  Path

BIND 9.10.5 - Unquoted Service Path Privilege Escalation                                   | windows/local/42121.txt
Ulterius Server < 1.9.5.0 - Directory Traversal                                            | windows/remote/43141.py

 Exploit Title                                                                             |  Path

Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution           | multiple/remote/43382.py
Apple macOS Sierra 10.12.3 - 'IOFireWireFamily-null-deref' FireWire Port Denial of Service | macos/dos/44236.c
```



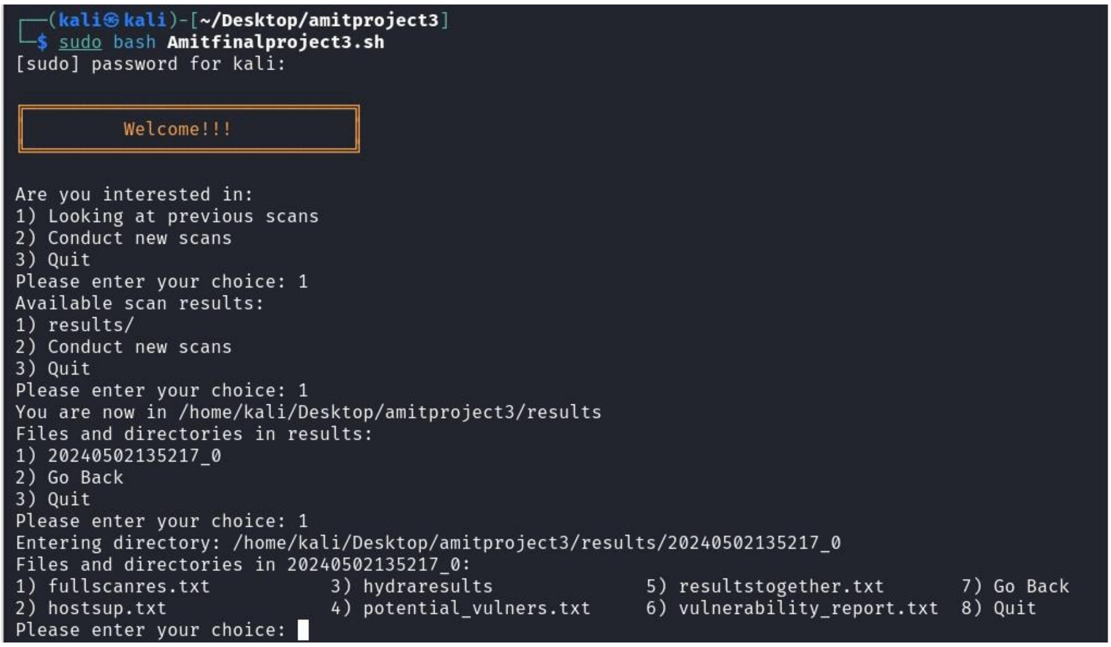
```
Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution           | multiple/remote/43382.py
Apple macOS Sierra 10.12.3 - 'IOFireWireFamily-null-deref' FireWire Port Denial of Service | macos/dos/44236.c
Gazelle CMS 1.0 - 'template' Local File Inclusion                                          | php/webapps/7895.txt
Sendmail 8.9.2 - Headers Prescan Denial of Service                                         | irix/dos/23167.c
Vivotek Motion Jpeg Control - 'MjpegDecoder.dll 2.0.0.13' Remote Overflow                  | windows/remote/4015.html
WebKit - 'WebCore::InputType::element' Use-After-Free (2)                                  | multiple/dos/43167.js
WordPress Core 2.3.3 - 'cat' Directory Traversal                                           | php/webapps/31670.txt

 Exploit Title                                                                             |  Path

Samba 3.5.0 - Remote Code Execution                                                        | linux/remote/42060.py
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load (Metasploit) | linux/remote/42084.rb

 Exploit Title                                                                             |  Path

phpMyAdmin 3.3.x/3.4.x - Local File Inclusion via XML External Entity Injection (Metasploit) | php/webapps/18371.rb
RiotPix 0.61 - 'forumid' Blind SQL Injection                                               | php/webapps/7679.php

 Exploit Title                                                                             |  Path

ZeroLogon - Netlogon Elevation of Privilege                                                | windows/remote/49071.py

 Paper Title                                                                               |  Path

Understanding and Exploiting Zerologon - Paper                                             | docs/english/49368-understanding

 Exploit Title                                                                             |  Path

Broadcom Wi-Fi Devices - 'KR00K Information Disclosure                                     | multiple/remote/48233.py

Consolidating all results into one file...
All your results have been saved to one file called resultstogether.txt where you can see all the results from running the tool.
```



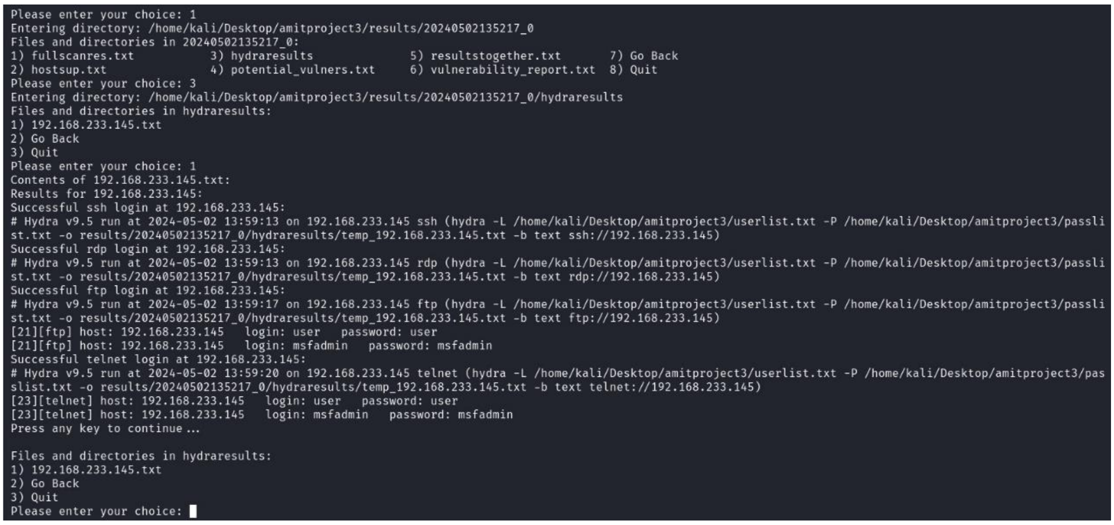
```
All your results have been saved to one file called resultstogether.txt where you can see all the results from running the tool.
[+] Do you want to zip the results?
1. Yes, zip the files.
2. No, do not zip, continue without zipping.
Enter your choice (1 or 2): 1
Please enter the name for the zip file (without the .zip extension):
scanresults
[+] Zipping all the results into an archive named: 'scanresults.zip' located at the same place where the script is run.
[+]Zipping complete. Your results are in 'scanresults.zip'.

 BYE BYE!!!
```



#4.3 Allow the user to search inside the results.- menu output:



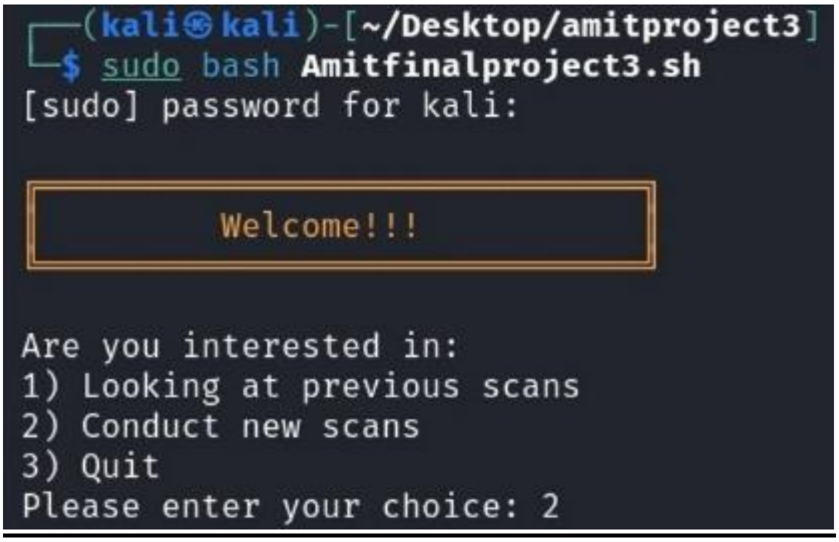
```
┌──(kali㉿kali)-[~/Desktop/amitproject3]
└─$ sudo bash Amitfinalproject3.sh
[sudo] password for kali:

 ┌────────────────────────┐
 │        Welcome!!!      │
 └────────────────────────┘

Are you interested in:
1) Looking at previous scans
2) Conduct new scans
3) Quit
Please enter your choice: 1
Available scan results:
1) results/
2) Conduct new scans
3) Quit
Please enter your choice: 1
You are now in /home/kali/Desktop/amitproject3/results
Files and directories in results:
1) 20240502135217_0
2) Go Back
3) Quit
Please enter your choice: 1
Entering directory: /home/kali/Desktop/amitproject3/results/20240502135217_0
Files and directories in 20240502135217_0:
1) fullscanres.txt          3) hydraresults              5) resultstogether.txt       7) Go Back
2) hostsup.txt              4) potential_vulners.txt     6) vulnerability_report.txt  8) Quit
Please enter your choice: 
```



```
Please enter your choice: 1
Entering directory: /home/kali/Desktop/amitproject3/results/20240502135217_0
Files and directories in 20240502135217_0:
1) fullscanres.txt          3) hydraresults              5) resultstogether.txt       7) Go Back
2) hostsup.txt              4) potential_vulners.txt     6) vulnerability_report.txt  8) Quit
Please enter your choice: 3
Entering directory: /home/kali/Desktop/amitproject3/results/20240502135217_0/hydraresults
Files and directories in hydraresults:
1) 192.168.233.145.txt
2) Go Back
3) Quit
Please enter your choice: 1
Contents of 192.168.233.145.txt:
Results for 192.168.233.145:
Successful ssh login at 192.168.233.145:
# Hydra v9.5 run at 2024-05-02 13:59:13 on 192.168.233.145 ssh (hydra -L /home/kali/Desktop/amitproject3/userlist.txt -P /home/kali/Desktop/amitproject3/passli
st.txt -o results/20240502135217_0/hydraresults/temp_192.168.233.145.txt -b text ssh://192.168.233.145)
Successful rdp login at 192.168.233.145:
# Hydra v9.5 run at 2024-05-02 13:59:13 on 192.168.233.145 rdp (hydra -L /home/kali/Desktop/amitproject3/userlist.txt -P /home/kali/Desktop/amitproject3/passli
st.txt -o results/20240502135217_0/hydraresults/temp_192.168.233.145.txt -b text rdp://192.168.233.145)
Successful ftp login at 192.168.233.145:
# Hydra v9.5 run at 2024-05-02 13:59:17 on 192.168.233.145 ftp (hydra -L /home/kali/Desktop/amitproject3/userlist.txt -P /home/kali/Desktop/amitproject3/passli
st.txt -o results/20240502135217_0/hydraresults/temp_192.168.233.145.txt -b text ftp://192.168.233.145)
[21][ftp] host: 192.168.233.145   login: user   password: user
[21][ftp] host: 192.168.233.145   login: msfadmin   password: msfadmin
Successful telnet login at 192.168.233.145:
# Hydra v9.5 run at 2024-05-02 13:59:20 on 192.168.233.145 telnet (hydra -L /home/kali/Desktop/amitproject3/userlist.txt -P /home/kali/Desktop/amitproject3/pas
slist.txt -o results/20240502135217_0/hydraresults/temp_192.168.233.145.txt -b text telnet://192.168.233.145)
[23][telnet] host: 192.168.233.145   login: user   password: user
[23][telnet] host: 192.168.233.145   login: msfadmin   password: msfadmin
Press any key to continue ...

Files and directories in hydraresults:
1) 192.168.233.145.txt
2) Go Back
3) Quit
Please enter your choice: 
```

Explanation of output according to the project structure:

4.3 Allow the user to search inside the results.



```
┌──(kali㉿kali)-[~/Desktop/amitproject3]
└─$ sudo bash Amitfinalproject3.sh
[sudo] password for kali:

        Welcome!!!

Are you interested in:
1) Looking at previous scans
2) Conduct new scans
3) Quit
Please enter your choice: 2
```

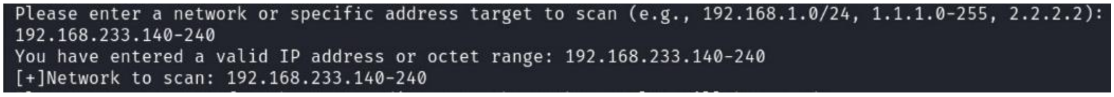
As you can see the tool gives the user the option to search in previous scans or perform a new scan.

In the output above I gave pictures of the possibility to see previous scans and how the menu navigation is done.

1. Getting the User Input

1.1 Get from the user a network to scan.

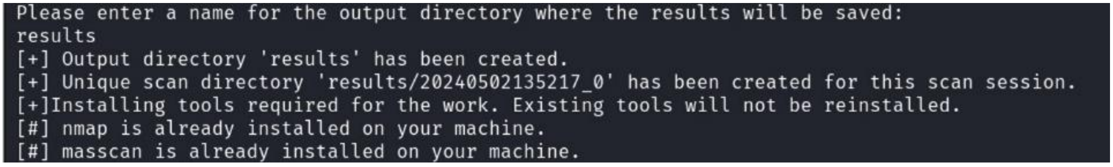
1.4 Make sure the input is valid.



```
Please enter a network or specific address target to scan (e.g., 192.168.1.0/24, 1.1.1.0-255, 2.2.2.2):
192.168.233.140-240
You have entered a valid IP address or octet range: 192.168.233.140-240
[+]Network to scan: 192.168.233.140-240
```

We can see that the user asks to enter an address or an address range, then the script verifies that the address or range is valid and can be worked with, as well as examples are shown to him. After that, an indication is shown to the user which address or network he chose to scan.

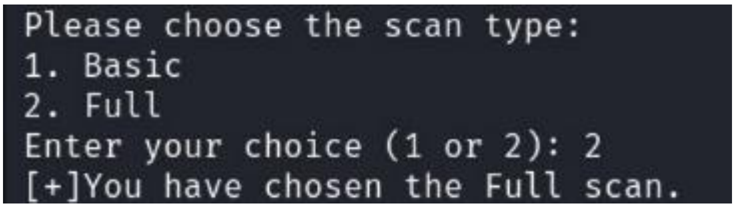
1.2 Get from the user a name for the output directory.



```
Please enter a name for the output directory where the results will be saved:
results
[+] Output directory 'results' has been created.
[+] Unique scan directory 'results/20240502135217_0' has been created for this scan session.
[+]Installing tools required for the work. Existing tools will not be reinstalled.
[#] nmap is already installed on your machine.
[#] masscan is already installed on your machine.
```

We can see that the user is asked to enter a name for the folder that will be created and in addition a unique folder is created within that folder for his scans so that if he enters the same folder name next time a separation will be created between the scans. In addition, it can be seen that the tool checks whether the scanning programs are installed or not, and if they are installed, they are not installed again and the user receives an indication of this.

1.3 Allow the user to choose 'Basic' or 'Full'.

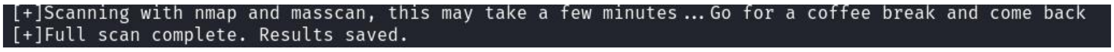


```
Please choose the scan type:
1. Basic
2. Full
Enter your choice (1 or 2): 2
[+]You have chosen the Full scan.
```

The user is asked to select which type of scan he wants, and is shown an indication of this.

1.3.1 Basic: scans the network for TCP and UDP, including the service version and weak passwords.

1.3.2 Full: include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.



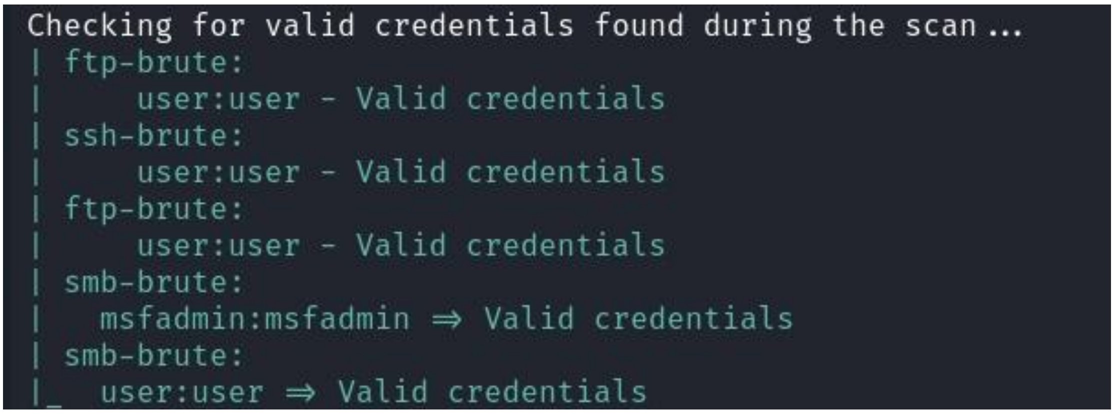
```
[+]Scanning with nmap and masscan, this may take a few minutes ... Go for a coffee break and come back
[+]Full scan complete. Results saved.
```

It can be seen that the user receives an indication of the scan being performed, and is shown that the scan is finished according to the type of scan, and a file is also saved about it.

2. Weak Credentials

2.1 Look for weak passwords used in the network for login services.

2.1.1 Have a built-in password.lst to check for weak passwords.

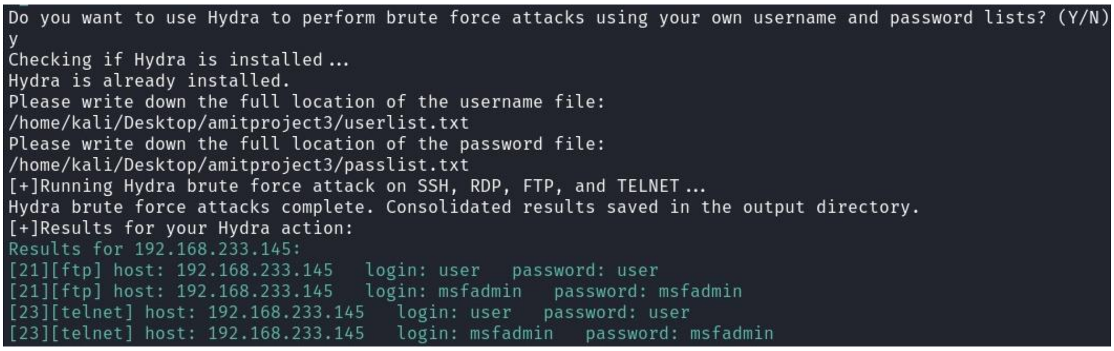


```
Checking for valid credentials found during the scan ...
| ftp-brute:
|     user:user - Valid credentials
| ssh-brute:
|     user:user - Valid credentials
| ftp-brute:
|     user:user - Valid credentials
| smb-brute:
|   msfadmin:msfadmin ⇒ Valid credentials
| smb-brute:
|_  user:user ⇒ Valid credentials
```

During the scan, the tool automatically checks from a database of passwords that it already has whether they work, and the user receives an indication of this if the tool finds, as you can see it is shown to him.

2.1.2 Allow the user to supply their own password list.

2.2 Login services to check include: SSH, RDP, FTP, and TELNET.

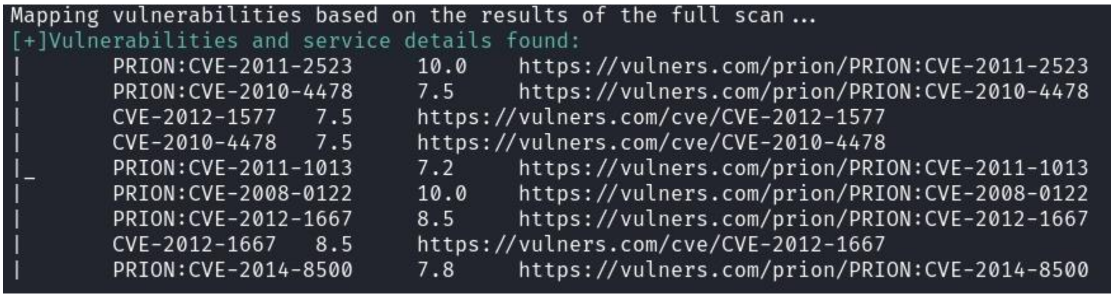


```
Do you want to use Hydra to perform brute force attacks using your own username and password lists? (Y/N)
y
Checking if Hydra is installed...
Hydra is already installed.
Please write down the full location of the username file:
/home/kali/Desktop/amitproject3/userlist.txt
Please write down the full location of the password file:
/home/kali/Desktop/amitproject3/passlist.txt
[+]Running Hydra brute force attack on SSH, RDP, FTP, and TELNET...
Hydra brute force attacks complete. Consolidated results saved in the output directory.
[+]Results for your Hydra action:
Results for 192.168.233.145:
[21][ftp] host: 192.168.233.145   login: user   password: user
[21][ftp] host: 192.168.233.145   login: msfadmin   password: msfadmin
[23][telnet] host: 192.168.233.145   login: user   password: user
[23][telnet] host: 192.168.233.145   login: msfadmin   password: msfadmin
```

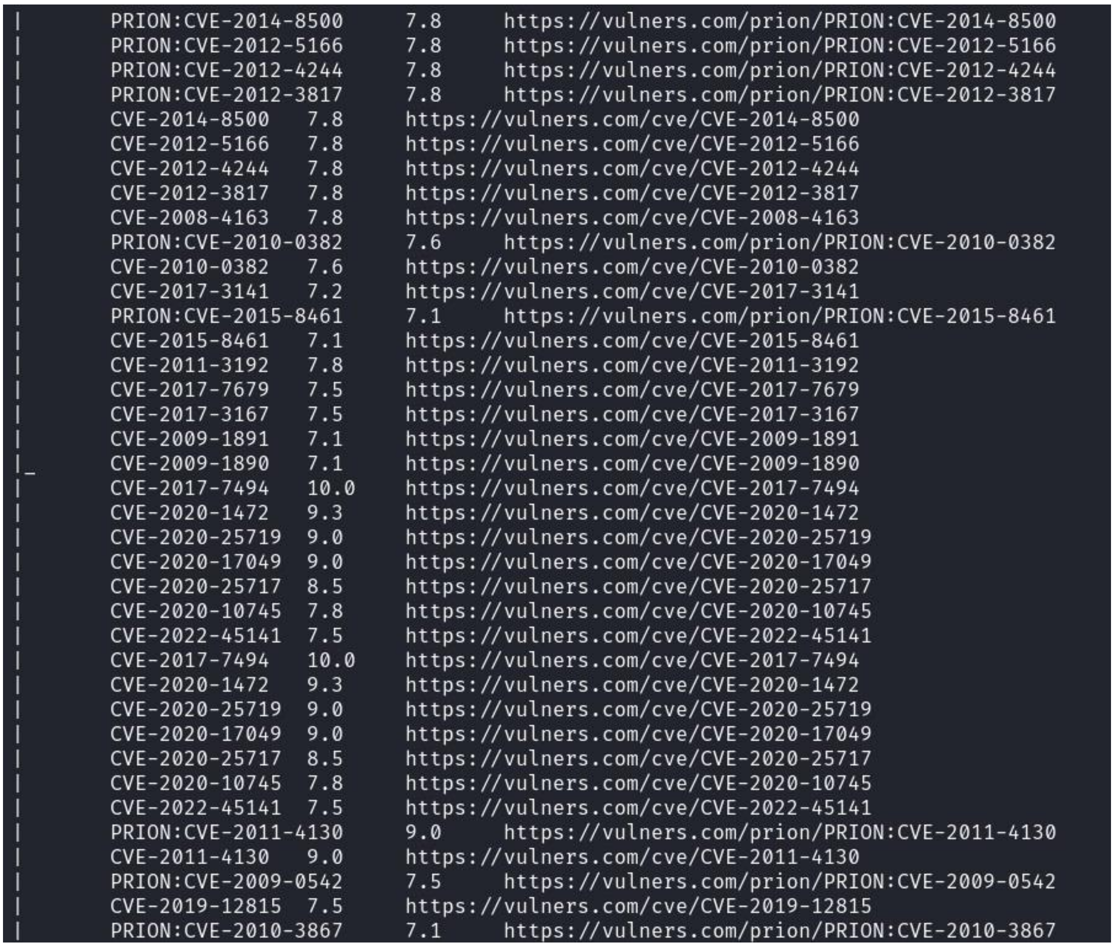
You can see that the tool asks the user if he wants to use Hydra and give his own usernames and passwords so that the tool tries to check them on the SSH, RDP, FTP, and TELNET services, when he marks yes and gives the required lists, the results are saved and of course shown to him in a direct indication.

3. Mapping Vulnerabilities

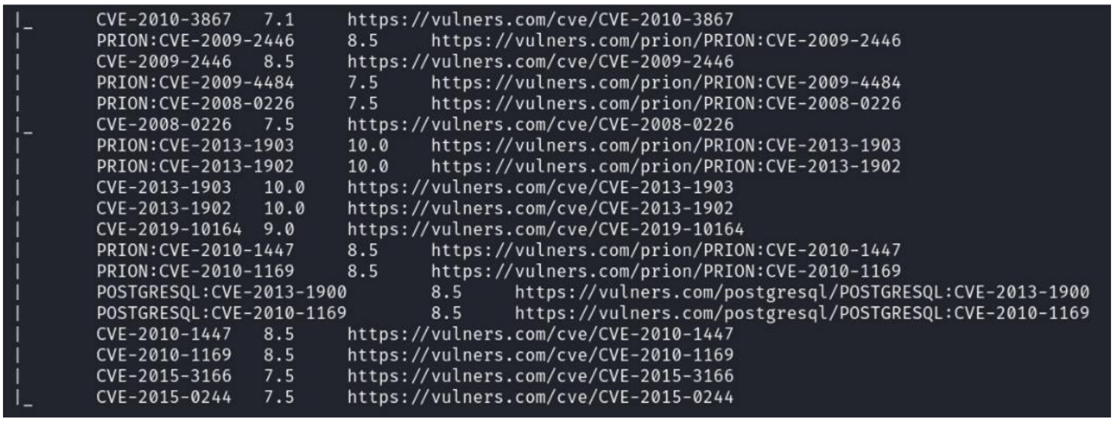
3.1 Mapping vulnerabilities should only take place if Full was chosen.



```
Mapping vulnerabilities based on the results of the full scan...
[+]Vulnerabilities and service details found:
|       PRION:CVE-2011-2523     10.0    https://vulners.com/prion/PRION:CVE-2011-2523
|       PRION:CVE-2010-4478     7.5     https://vulners.com/prion/PRION:CVE-2010-4478
|       CVE-2012-1577   7.5     https://vulners.com/cve/CVE-2012-1577
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|_      PRION:CVE-2011-1013     7.2     https://vulners.com/prion/PRION:CVE-2011-1013
|       PRION:CVE-2008-0122     10.0    https://vulners.com/prion/PRION:CVE-2008-0122
|       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
|       PRION:CVE-2014-8500     7.8     https://vulners.com/prion/PRION:CVE-2014-8500
```



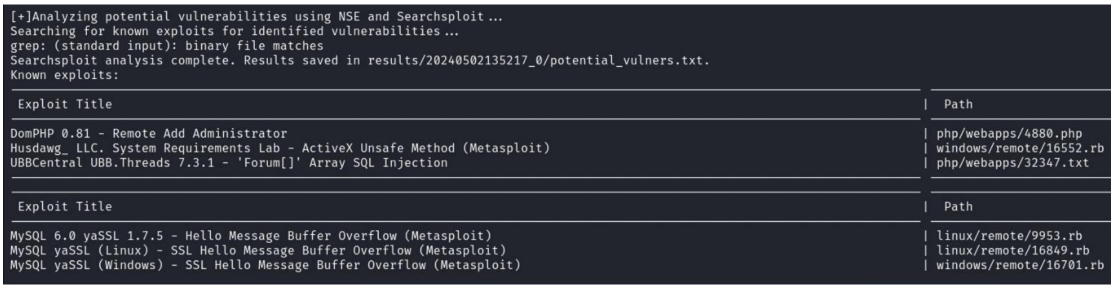
```
|       PRION:CVE-2014-8500     7.8     https://vulners.com/prion/PRION:CVE-2014-8500
|       PRION:CVE-2012-5166     7.8     https://vulners.com/prion/PRION:CVE-2012-5166
|       PRION:CVE-2012-4244     7.8     https://vulners.com/prion/PRION:CVE-2012-4244
|       PRION:CVE-2012-3817     7.8     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
|       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
|       CVE-2015-8461   7.1     https://vulners.com/cve/CVE-2015-8461
|       CVE-2011-3192   7.8     https://vulners.com/cve/CVE-2011-3192
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-3167   7.5     https://vulners.com/cve/CVE-2017-3167
|       CVE-2009-1891   7.1     https://vulners.com/cve/CVE-2009-1891
|_      CVE-2009-1890   7.1     https://vulners.com/cve/CVE-2009-1890
|       CVE-2017-7494   10.0    https://vulners.com/cve/CVE-2017-7494
|       CVE-2020-1472   9.3     https://vulners.com/cve/CVE-2020-1472
|       CVE-2020-25719  9.0     https://vulners.com/cve/CVE-2020-25719
|       CVE-2020-17049  9.0     https://vulners.com/cve/CVE-2020-17049
|       CVE-2020-25717  8.5     https://vulners.com/cve/CVE-2020-25717
|       CVE-2020-10745  7.8     https://vulners.com/cve/CVE-2020-10745
|       CVE-2022-45141  7.5     https://vulners.com/cve/CVE-2022-45141
|       CVE-2017-7494   10.0    https://vulners.com/cve/CVE-2017-7494
|       CVE-2020-1472   9.3     https://vulners.com/cve/CVE-2020-1472
|       CVE-2020-25719  9.0     https://vulners.com/cve/CVE-2020-25719
|       CVE-2020-17049  9.0     https://vulners.com/cve/CVE-2020-17049
|       CVE-2020-25717  8.5     https://vulners.com/cve/CVE-2020-25717
|       CVE-2020-10745  7.8     https://vulners.com/cve/CVE-2020-10745
|       CVE-2022-45141  7.5     https://vulners.com/cve/CVE-2022-45141
|       PRION:CVE-2011-4130     9.0     https://vulners.com/prion/PRION:CVE-2011-4130
|       CVE-2011-4130   9.0     https://vulners.com/cve/CVE-2011-4130
|       PRION:CVE-2009-0542     7.5     https://vulners.com/prion/PRION:CVE-2009-0542
|       CVE-2019-12815  7.5     https://vulners.com/cve/CVE-2019-12815
|       PRION:CVE-2010-3867     7.1     https://vulners.com/prion/PRION:CVE-2010-3867
```



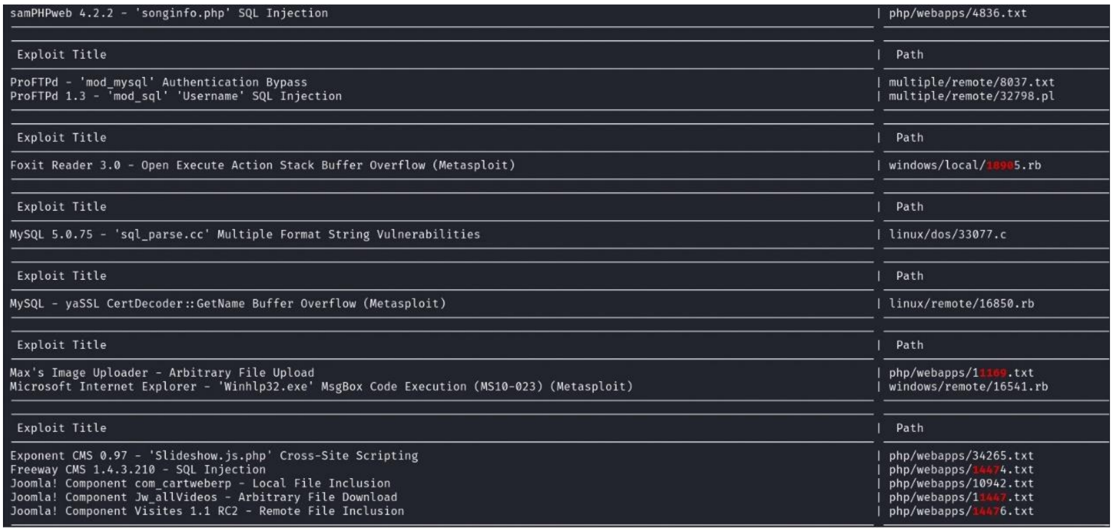
```
|_      CVE-2010-3867   7.1     https://vulners.com/cve/CVE-2010-3867
|       PRION:CVE-2009-2446     8.5     https://vulners.com/prion/PRION:CVE-2009-2446
|       CVE-2009-2446   8.5     https://vulners.com/cve/CVE-2009-2446
|       PRION:CVE-2009-4484     7.5     https://vulners.com/prion/PRION:CVE-2009-4484
|       PRION:CVE-2008-0226     7.5     https://vulners.com/prion/PRION:CVE-2008-0226
|_      CVE-2008-0226   7.5     https://vulners.com/cve/CVE-2008-0226
|       PRION:CVE-2013-1903     10.0    https://vulners.com/prion/PRION:CVE-2013-1903
|       PRION:CVE-2013-1902     10.0    https://vulners.com/prion/PRION:CVE-2013-1902
|       CVE-2013-1903   10.0    https://vulners.com/cve/CVE-2013-1903
|       CVE-2013-1902   10.0    https://vulners.com/cve/CVE-2013-1902
|       CVE-2019-10164  9.0     https://vulners.com/cve/CVE-2019-10164
|       PRION:CVE-2010-1447     8.5     https://vulners.com/prion/PRION:CVE-2010-1447
|       PRION:CVE-2010-1169     8.5     https://vulners.com/prion/PRION:CVE-2010-1169
|       POSTGRESQL:CVE-2013-1900        8.5     https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900
|       POSTGRESQL:CVE-2010-1169        8.5     https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169
|       CVE-2010-1447   8.5     https://vulners.com/cve/CVE-2010-1447
|       CVE-2010-1169   8.5     https://vulners.com/cve/CVE-2010-1169
|       CVE-2015-3166   7.5     https://vulners.com/cve/CVE-2015-3166
|_      CVE-2015-0244   7.5     https://vulners.com/cve/CVE-2015-0244
```

We see that since the user performed a full scan, he receives an indication of known weaknesses with a high level of risk to his services.

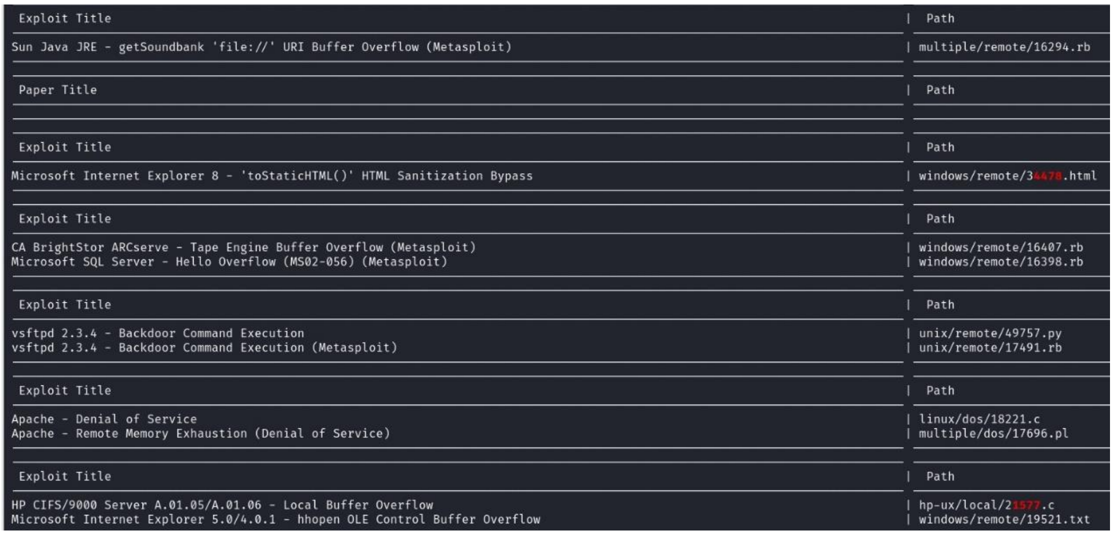
3.2 Display potential vulnerabilities via NSE and Searchsploit.



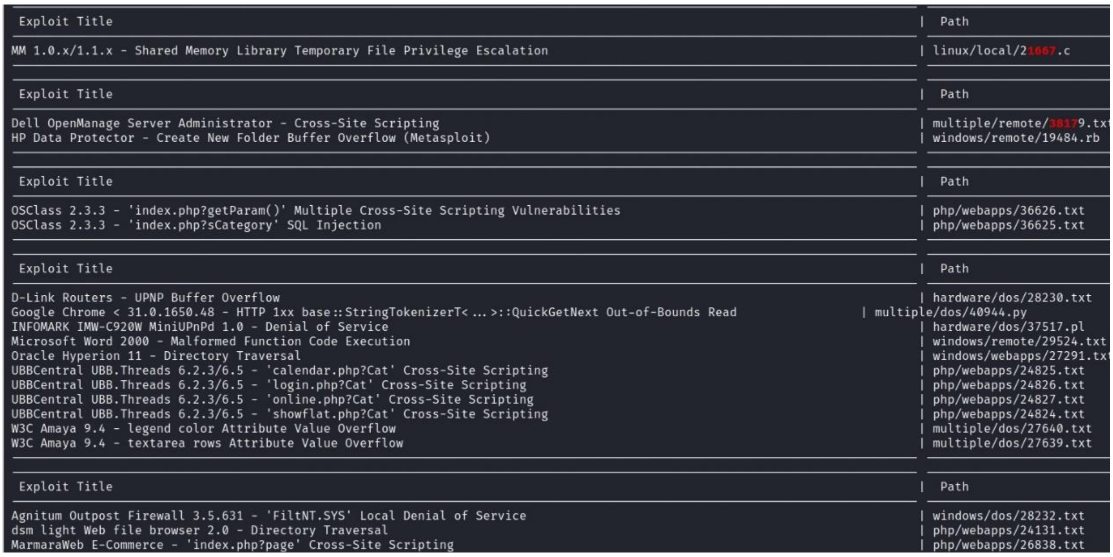
```
[+]Analyzing potential vulnerabilities using NSE and Searchsploit...
Searching for known exploits for identified vulnerabilities...
grep: (standard input): binary file matches
Searchsploit analysis complete. Results saved in results/20240502135217_0/potential_vulners.txt.
Known exploits:
----------------------------------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                                               |  Path
----------------------------------------------------------------------------------------------------------------------------- ---------------------------
DomPHP 0.81 - Remote Add Administrator                                                                                       | php/webapps/4880.php
Husdawg_ LLC. System Requirements Lab - ActiveX Unsafe Method (Metasploit)                                                   | windows/remote/16552.rb
UBBCentral UBB.Threads 7.3.1 - 'Forum[]' Array SQL Injection                                                                 | php/webapps/32347.txt
----------------------------------------------------------------------------------------------------------------------------- ---------------------------
----------------------------------------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                                               |  Path
----------------------------------------------------------------------------------------------------------------------------- ---------------------------
MySQL 6.0 yaSSL 1.7.5 - Hello Message Buffer Overflow (Metasploit)                                                           | linux/remote/9953.rb
MySQL yaSSL (Linux) - SSL Hello Message Buffer Overflow (Metasploit)                                                         | linux/remote/16849.rb
MySQL yaSSL (Windows) - SSL Hello Message Buffer Overflow (Metasploit)                                                       | windows/remote/16701.rb
```



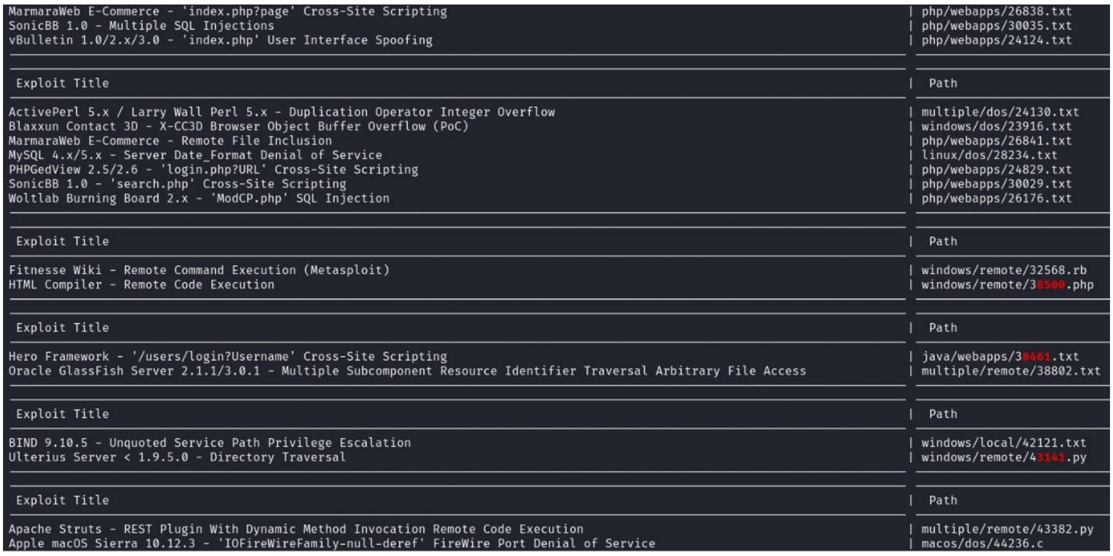
```
samPHPweb 4.2.2 - 'songinfo.php' SQL Injection                                        | php/webapps/4836.txt
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
ProFTPd - 'mod_mysql' Authentication Bypass                                           | multiple/remote/8037.txt
ProFTPd 1.3 - 'mod_sql' 'Username' SQL Injection                                      | multiple/remote/32798.pl
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
Foxit Reader 3.0 - Open Execute Action Stack Buffer Overflow (Metasploit)             | windows/local/18905.rb
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
MySQL 5.0.75 - 'sql_parse.cc' Multiple Format String Vulnerabilities                  | linux/dos/33077.c
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
MySQL - yaSSL CertDecoder::GetName Buffer Overflow (Metasploit)                       | linux/remote/16850.rb
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
Max's Image Uploader - Arbitrary File Upload                                          | php/webapps/11169.txt
Microsoft Internet Explorer - 'Winhlp32.exe' MsgBox Code Execution (MS10-023) (Metasploit) | windows/remote/16541.rb
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
Exponent CMS 0.97 - 'Slideshow.js.php' Cross-Site Scripting                           | php/webapps/34265.txt
Freeway CMS 1.4.3.210 - SQL Injection                                                 | php/webapps/14474.txt
Joomla! Component com_cartweberp - Local File Inclusion                               | php/webapps/10942.txt
Joomla! Component Jw_allVideos - Arbitrary File Download                              | php/webapps/11447.txt
Joomla! Component Visites 1.1 RC2 - Remote File Inclusion                             | php/webapps/14476.txt
-------------------------------------------------------------------------------------- ----------------------------
```



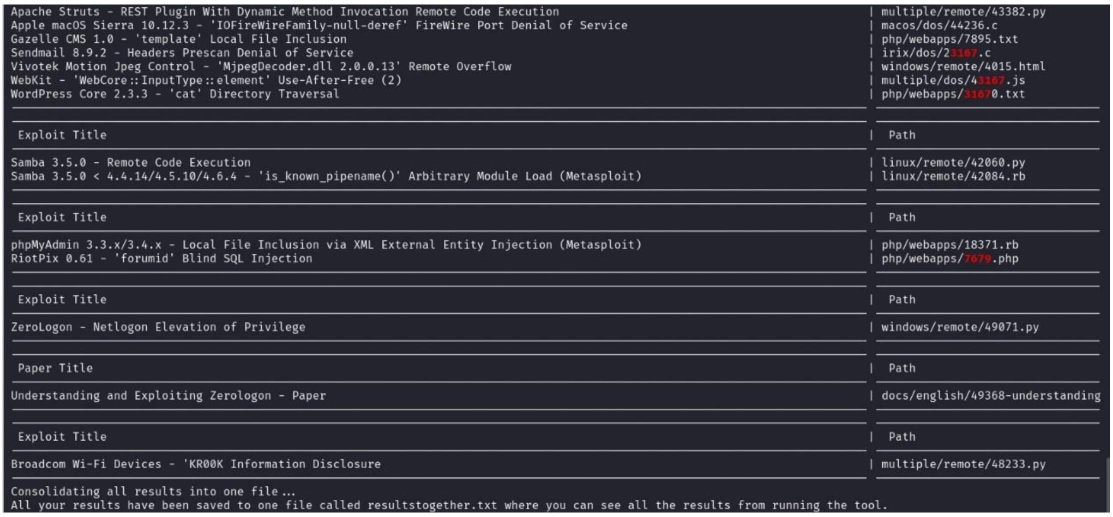
```
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
Sun Java JRE - getSoundbank 'file://' URI Buffer Overflow (Metasploit)                | multiple/remote/16294.rb
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Paper Title                                                                           |  Path
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
Microsoft Internet Explorer 8 - 'toStaticHTML()' HTML Sanitization Bypass             | windows/remote/34478.html
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
CA BrightStor ARCserve - Tape Engine Buffer Overflow (Metasploit)                     | windows/remote/16407.rb
Microsoft SQL Server - Hello Overflow (MS02-056) (Metasploit)                         | windows/remote/16398.rb
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
vsftpd 2.3.4 - Backdoor Command Execution                                             | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                | unix/remote/17491.rb
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
Apache - Denial of Service                                                            | linux/dos/18221.c
Apache - Remote Memory Exhaustion (Denial of Service)                                 | multiple/dos/17696.pl
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
HP CIFS/9000 Server A.01.05/A.01.06 - Local Buffer Overflow                           | hp-ux/local/21577.c
Microsoft Internet Explorer 5.0/4.0.1 - hhopen OLE Control Buffer Overflow            | windows/remote/19521.txt
```



```
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
MM 1.0.x/1.1.x - Shared Memory Library Temporary File Privilege Escalation            | linux/local/21667.c
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
Dell OpenManage Server Administrator - Cross-Site Scripting                           | multiple/remote/38179.txt
HP Data Protector - Create New Folder Buffer Overflow (Metasploit)                    | windows/remote/19484.rb
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
OSClass 2.3.3 - 'index.php?getParam()' Multiple Cross-Site Scripting Vulnerabilities  | php/webapps/36626.txt
OSClass 2.3.3 - 'index.php?sCategory' SQL Injection                                   | php/webapps/36625.txt
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
D-Link Routers - UPNP Buffer Overflow                                                 | hardware/dos/28230.txt
Google Chrome < 31.0.1650.48 - HTTP 1xx base::StringTokenizerT<...>::QuickGetNext Out-of-Bounds Read | multiple/dos/40944.py
INFOMARK IMW-C920W MiniUPnPd 1.0 - Denial of Service                                  | hardware/dos/37517.pl
Microsoft Word 2000 - Malformed Function Code Execution                               | windows/remote/29524.txt
Oracle Hyperion 11 - Directory Traversal                                              | windows/webapps/27291.txt
UBBCentral UBB.Threads 6.2.3/6.5 - 'calendar.php?Cat' Cross-Site Scripting            | php/webapps/24825.txt
UBBCentral UBB.Threads 6.2.3/6.5 - 'login.php?Cat' Cross-Site Scripting               | php/webapps/24826.txt
UBBCentral UBB.Threads 6.2.3/6.5 - 'online.php?Cat' Cross-Site Scripting              | php/webapps/24827.txt
UBBCentral UBB.Threads 6.2.3/6.5 - 'showflat.php?Cat' Cross-Site Scripting            | php/webapps/24824.txt
W3C Amaya 9.4 - legend color Attribute Value Overflow                                 | multiple/dos/27640.txt
W3C Amaya 9.4 - textarea rows Attribute Value Overflow                                | multiple/dos/27639.txt
-------------------------------------------------------------------------------------- ----------------------------
-------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ----------------------------
Agnitum Outpost Firewall 3.5.631 - 'FiltNT.SYS' Local Denial of Service               | windows/dos/28232.txt
dsm light Web file browser 2.0 - Directory Traversal                                  | php/webapps/24131.txt
MarmaraWeb E-Commerce - 'index.php?page' Cross-Site Scripting                         | php/webapps/26838.txt
```



```
MarmaraWeb E-Commerce - 'index.php?page' Cross-Site Scripting                    | php/webapps/26838.txt
SonicBB 1.0 - Multiple SQL Injections                                            | php/webapps/30035.txt
vBulletin 1.0/2.x/3.0 - 'index.php' User Interface Spoofing                      | php/webapps/24124.txt
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------- ---------------------
ActivePerl 5.x / Larry Wall Perl 5.x - Duplication Operator Integer Overflow     | multiple/dos/24130.txt
Blaxxun Contact 3D - X-CC3D Browser Object Buffer Overflow (PoC)                 | windows/dos/23916.txt
MarmaraWeb E-Commerce - Remote File Inclusion                                    | php/webapps/26841.txt
MySQL 4.x/5.x - Server Date_Format Denial of Service                             | linux/dos/28234.txt
PHPGedView 2.5/2.6 - 'login.php?URL' Cross-Site Scripting                        | php/webapps/24829.txt
SonicBB 1.0 - 'search.php' Cross-Site Scripting                                  | php/webapps/30029.txt
Woltlab Burning Board 2.x - 'ModCP.php' SQL Injection                            | php/webapps/26176.txt
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------- ---------------------
Fitnesse Wiki - Remote Command Execution (Metasploit)                            | windows/remote/32568.rb
HTML Compiler - Remote Code Execution                                            | windows/remote/38500.php
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------- ---------------------
Hero Framework - '/users/login?Username' Cross-Site Scripting                    | java/webapps/38461.txt
Oracle GlassFish Server 2.1.1/3.0.1 - Multiple Subcomponent Resource Identifier Traversal Arbitrary File Access | multiple/remote/38802.txt
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------- ---------------------
BIND 9.10.5 - Unquoted Service Path Privilege Escalation                         | windows/local/42121.txt
Ulterius Server < 1.9.5.0 - Directory Traversal                                  | windows/remote/43141.py
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------- ---------------------
Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution | multiple/remote/43382.py
Apple macOS Sierra 10.12.3 - 'IOFireWireFamily-null-deref' FireWire Port Denial of Service | macos/dos/44236.c
```



```
Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution | multiple/remote/43382.py
Apple macOS Sierra 10.12.3 - 'IOFireWireFamily-null-deref' FireWire Port Denial of Service | macos/dos/44236.c
Gazelle CMS 1.0 - 'template' Local File Inclusion                                | php/webapps/7895.txt
Sendmail 8.9.2 - Headers Prescan Denial of Service                               | irix/dos/23167.c
Vivotek Motion Jpeg Control - 'MjpegDecoder.dll 2.0.0.13' Remote Overflow        | windows/remote/4015.html
WebKit - 'WebCore::InputType::element' Use-After-Free (2)                        | multiple/dos/43167.js
WordPress Core 2.3.3 - 'cat' Directory Traversal                                 | php/webapps/31670.txt
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------- ---------------------
Samba 3.5.0 - Remote Code Execution                                              | linux/remote/42060.py
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load (Metasploit) | linux/remote/42084.rb
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------- ---------------------
phpMyAdmin 3.3.x/3.4.x - Local File Inclusion via XML External Entity Injection (Metasploit) | php/webapps/18371.rb
RiotPix 0.61 - 'forumid' Blind SQL Injection                                     | php/webapps/7679.php
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------- ---------------------
ZeroLogon - Netlogon Elevation of Privilege                                      | windows/remote/49071.py
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Paper Title                                                                     |  Path
---------------------------------------------------------------------------------- ---------------------
Understanding and Exploiting Zerologon - Paper                                   | docs/english/49368-understanding
---------------------------------------------------------------------------------- ---------------------
---------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------- ---------------------
Broadcom Wi-Fi Devices - 'KR00K Information Disclosure                           | multiple/remote/48233.py
---------------------------------------------------------------------------------- ---------------------
Consolidating all results into one file ...
All your results have been saved to one file called resultstogether.txt where you can see all the results from running the tool.
```

It can be seen that the tool analyzes the known weaknesses and presents the user with the existing exploits for what is found. The user receives a direct indication of exactly where he is vulnerable, and here the results are also saved to a file.

4. Log Results

4.1 During each stage, display the stage in the terminal.-

displayed to the user

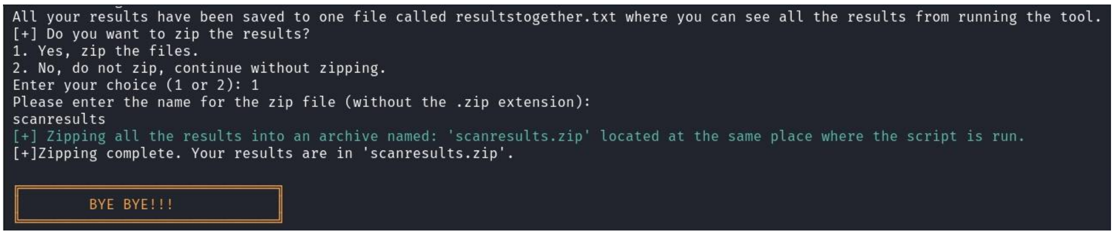
4.2 At the end, show the user the found information.

All results are displayed to the user during the use of the tool and are also saved.

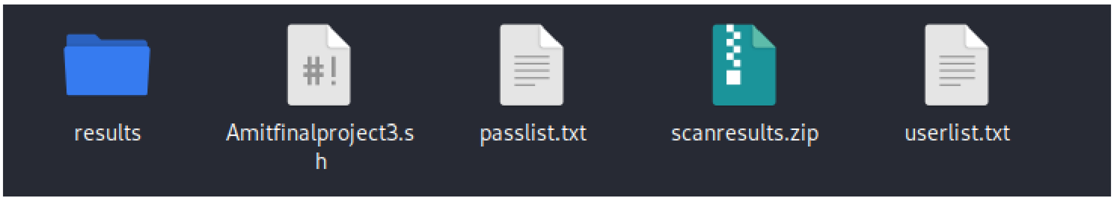
4.3 Allow the user to search inside the results.

Appears at the start of the tool's startup.

4.4 Allow to save all results into a Zip file.



```
All your results have been saved to one file called resultstogether.txt where you can see all the results from running the tool.
[+] Do you want to zip the results?
1. Yes, zip the files.
2. No, do not zip, continue without zipping.
Enter your choice (1 or 2): 1
Please enter the name for the zip file (without the .zip extension):
scanresults
[+] Zipping all the results into an archive named: 'scanresults.zip' located at the same place where the script is run.
[+]Zipping complete. Your results are in 'scanresults.zip'.

  BYE BYE!!!
```



It can be seen that the tool offers the user to save all the results to a ZIP file and lets him choose the name of the file. And after that the file is created.