Dor Amihai – John Bryce – class 7736.37 – lecturer's name Erel Regev
Penetration testing Script (Project) – Summary

This Bash script automates network reconnaissance and weak-password brute forcing on Kali Linux.

1. **Environment setup** –
    - Creates a user-named results directory (checks for collisions, then mkdir).
    - Checks/installs required tools: nmap, masscan, hydra, medusa, exploitdb, zip, wget.
    - Ensures NSE scripts exist and installs if missing: telnet-brute.nse, vulners.nse (updates script DB).
    - Generates local defaults under $SCRIPT_DIR (no remote fetch): users.txt, passwords.txt, and weak_passwords.lst (username:password pairs for Hydra -C).
2. **User input** –
    - Prompts for target (single IP or CIDR like 192.168.1.0/24) and validates IP/CIDR strictly.
    - Prompts for output directory name (default: SCAN_RESULTS).
3. **Scanning options** –
    - Presents a menu: **BASIC** or **FULL**.
    - **BASIC**:
        - TCP scan with nmap -sV -T4 -Pn -n (top 1000 TCP).
        - UDP: masscan -pU:0-65535 discovery (rate 10k, --wait 2).
          • If CIDR was supplied, UDP discovery narrows to "live hosts" parsed from the TCP phase; otherwise scans the whole target.
          • Targeted nmap -sU -sV runs only on discovered UDP ports.
        - Normalizes results into BASIC_SCAN/open_services.txt with columns: PROTOCOL HOST PORT SERVICE VERSION.
        - Weak-password brute-force over discovered services:
          • **Default list (D)** – ssh/rdp via **Medusa**, ftp/telnet via **Hydra** (-C weak_passwords.lst).

•**Extended brute-force (P)** – user supplies a custom password list: ssh/rdp via **Medusa**, ftp via **Hydra** (-L users.txt -P <list>), telnet via **Nmap telnet-brute** (normalized output).

• **RDP detection** handles both rdp and ms-wbt-server.
• Results summarized to custome_brut_force_week_results.txt or .

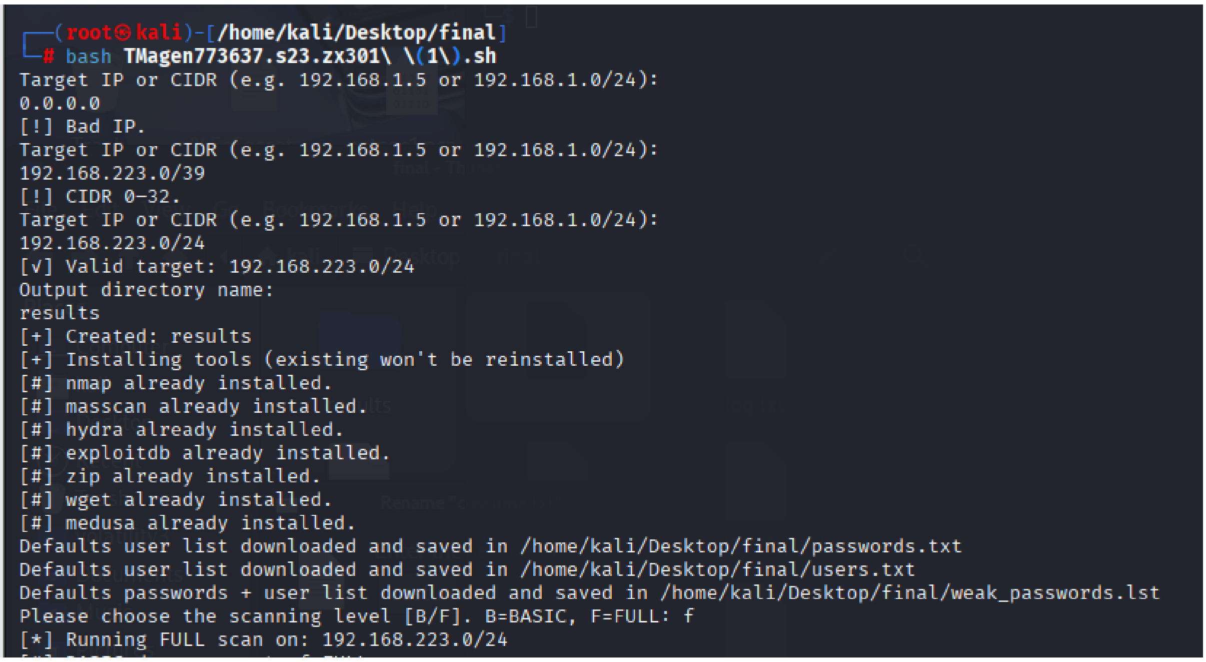
- **FULL**:
  - Runs BASIC as a sub-phase, then moves BASIC_SCAN into FULL_SCAN/.
  - Targeted NSE **vulners** scans on the discovered TCP/UDP ports only; outputs to nse_scan_tcp.txt / nse_scan_udp.txt.
  - Runs **searchsploit** (-w --disable-colour) against each discovered **service version** (where VERSION != "-") and exports to FULL_SCAN/searchsploit_results.

4. **Interactivity & Post-processing** –
   - Interactive search utility to grep -R -n -i keywords across the results folder.
   - Optional archiving of the entire results directory into a .zip.
   - Final printout of all generated logs/files (find "$OUTPUT_DIR" -type f).
5. **End result** –
   - A structured results tree containing:
     • TCP/UDP scan outputs
     • open_services.txt (normalized summary)
     • Brute-force results (default / custom)
     • NSE vulnerability outputs (vulners)
     • Searchsploit findings
   - All major activity is logged and neatly organized, with optional ZIP packaging and keyword search.

This ZIP file contains:
• The script TMagen773637.s23.zx301.sh
• This documentation summary

Task requirements:

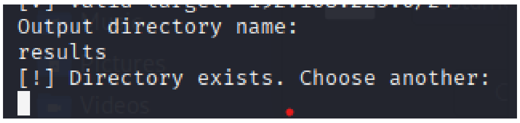
1. Getting the User Input 1.1 Get from the user a network to scan. 1.2 Get from the user a name for the output directory. 1.3 Allow the user to choose 'Basic' or 'Full'.



```
┌──(root㉿kali)-[/home/kali/Desktop/final]
└─# bash TMagen773637.s23.zx301\ \(1\).sh
Target IP or CIDR (e.g. 192.168.1.5 or 192.168.1.0/24):
0.0.0.0
[!] Bad IP.
Target IP or CIDR (e.g. 192.168.1.5 or 192.168.1.0/24):
192.168.223.0/39
[!] CIDR 0-32.
Target IP or CIDR (e.g. 192.168.1.5 or 192.168.1.0/24):
192.168.223.0/24
[√] Valid target: 192.168.223.0/24
Output directory name:
results
[+] Created: results
[+] Installing tools (existing won't be reinstalled)
[#] nmap already installed.
[#] masscan already installed.
[#] hydra already installed.
[#] exploitdb already installed.
[#] zip already installed.
[#] wget already installed.
[#] medusa already installed.
Defaults user list downloaded and saved in /home/kali/Desktop/final/passwords.txt
Defaults user list downloaded and saved in /home/kali/Desktop/final/users.txt
Defaults passwords + user list downloaded and saved in /home/kali/Desktop/final/weak_passwords.lst
Please choose the scanning level [B/F]. B=BASIC, F=FULL: f
[*] Running FULL scan on: 192.168.223.0/24
```

The script is checking if Ip input is correct, check if CIDR input is corret.

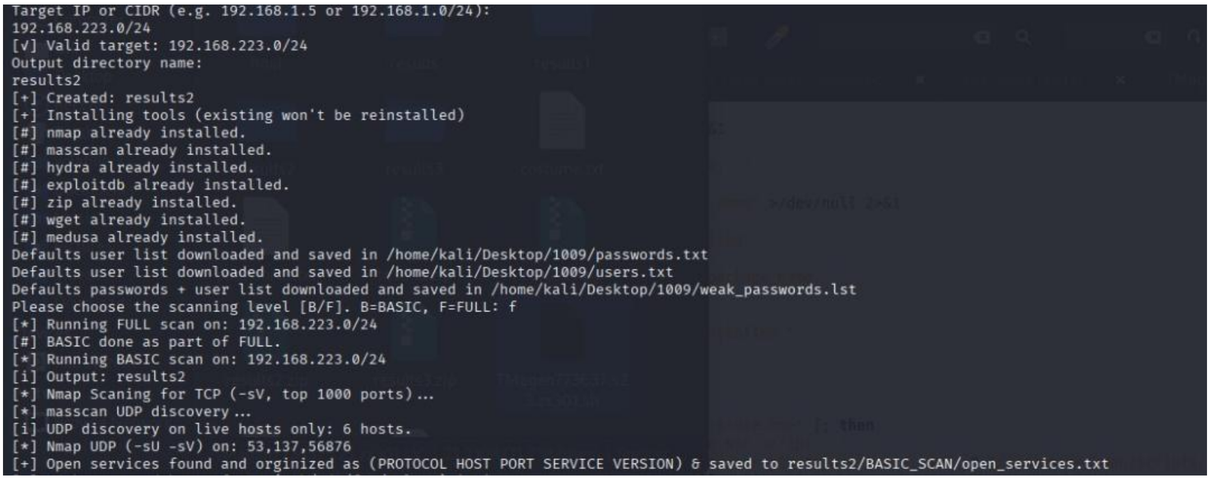
The script also checks that the result dir input is not existed . If it is, the script announce it and ask for different results input.



```
[√] Valid target: 192.168.223.0/24
Output directory name:
results
[!] Directory exists. Choose another:
```

1.4 Make sure the input is valid. – proven above.

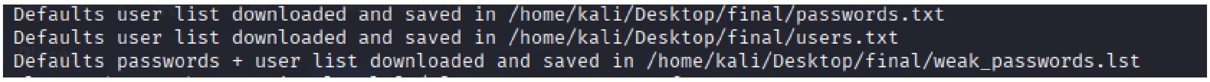
1.3.1 Basic: scans the network for TCP and UDP, including the service version and weak passwords.



```
Target IP or CIDR (e.g. 192.168.1.5 or 192.168.1.0/24):
192.168.223.0/24
[√] Valid target: 192.168.223.0/24
Output directory name:
results2
[+] Created: results2
[+] Installing tools (existing won't be reinstalled)
[#] nmap already installed.
[#] masscan already installed.
[#] hydra already installed.
[#] exploitdb already installed.
[#] zip already installed.
[#] wget already installed.
[#] medusa already installed.
Defaults user list downloaded and saved in /home/kali/Desktop/1009/passwords.txt
Defaults user list downloaded and saved in /home/kali/Desktop/1009/users.txt
Defaults passwords + user list downloaded and saved in /home/kali/Desktop/1009/weak_passwords.lst
Please choose the scanning level [B/F]. B=BASIC, F=FULL: f
[*] Running FULL scan on: 192.168.223.0/24
[#] BASIC done as part of FULL.
[*] Running BASIC scan on: 192.168.223.0/24
[i] Output: results2
[*] Nmap Scaning for TCP (-sV, top 1000 ports)...
[*] masscan UDP discovery ...
[i] UDP discovery on live hosts only: 6 hosts.
[*] Nmap UDP (-sU -sV) on: 53,137,56876
[+] Open services found and orginized as (PROTOCOL HOST PORT SERVICE VERSION) & saved to results2/BASIC_SCAN/open_services.txt
```

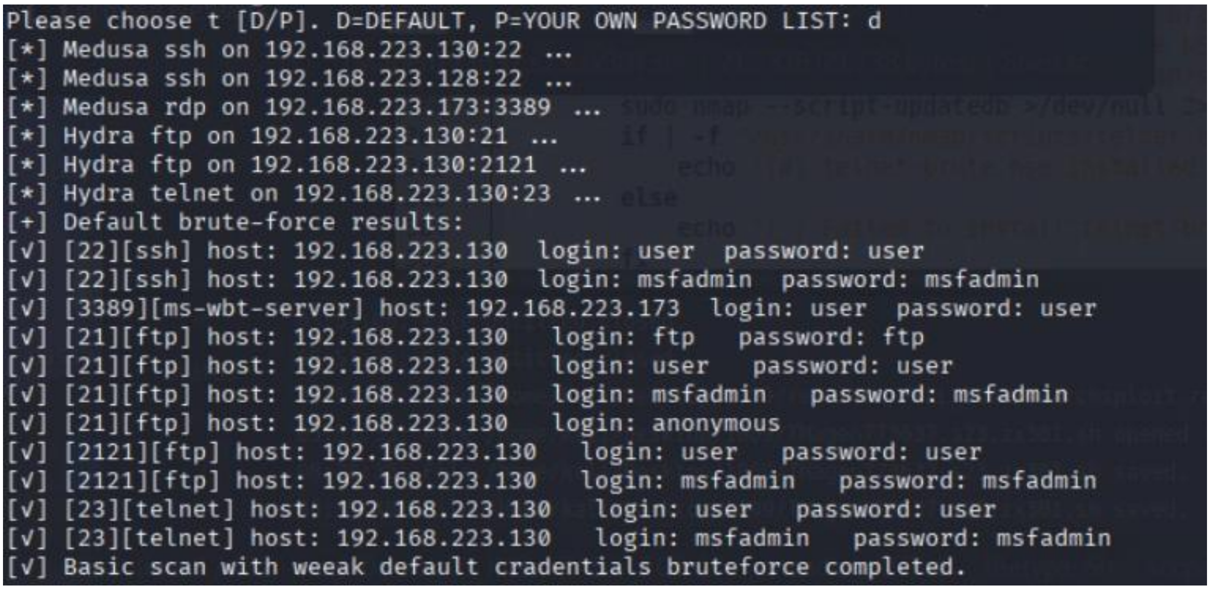
2. Weak Credentials 2.1 Look for weak passwords used in the network for login services. 2.1.1 Have a built-in password.lst to check for weak passwords. 2.1.2 Allow the user to supply their own password list. 2.2 Login services to check include: SSH, RDP, FTP, and TELNET.

The script creates weak credentials files:



```
Defaults user list downloaded and saved in /home/kali/Desktop/final/passwords.txt
Defaults user list downloaded and saved in /home/kali/Desktop/final/users.txt
Defaults passwords + user list downloaded and saved in /home/kali/Desktop/final/weak_passwords.lst
```

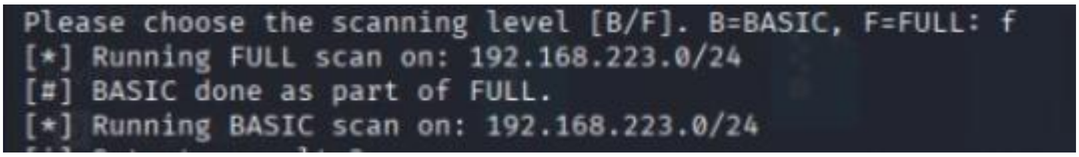
Then performs brute-force attack with week credentials by default or user passlist:



```
Please choose t [D/P]. D=DEFAULT, P=YOUR OWN PASSWORD LIST: d
[*] Medusa ssh on 192.168.223.130:22 ...
[*] Medusa ssh on 192.168.223.128:22 ...
[*] Medusa rdp on 192.168.223.173:3389 ...
[*] Hydra ftp on 192.168.223.130:21 ...
[*] Hydra ftp on 192.168.223.130:2121 ...
[*] Hydra telnet on 192.168.223.130:23 ...
[+] Default brute-force results:
[√] [22][ssh] host: 192.168.223.130  login: user  password: user
[√] [22][ssh] host: 192.168.223.130  login: msfadmin  password: msfadmin
[√] [3389][ms-wbt-server] host: 192.168.223.173  login: user  password: user
[√] [21][ftp] host: 192.168.223.130   login: ftp   password: ftp
[√] [21][ftp] host: 192.168.223.130   login: user   password: user
[√] [21][ftp] host: 192.168.223.130   login: msfadmin   password: msfadmin
[√] [21][ftp] host: 192.168.223.130   login: anonymous
[√] [2121][ftp] host: 192.168.223.130   login: user   password: user
[√] [2121][ftp] host: 192.168.223.130   login: msfadmin   password: msfadmin
[√] [23][telnet] host: 192.168.223.130   login: user   password: user
[√] [23][telnet] host: 192.168.223.130   login: msfadmin   password: msfadmin
[√] Basic scan with weeak default cradentials bruteforce completed.
```

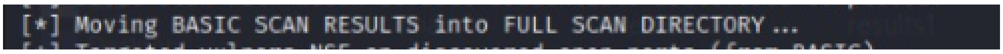
1.3.2 Full: include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.

The first task the script is doing is to use the BASIC function scan as a “base” for FULL function:



```
Please choose the scanning level [B/F]. B=BASIC, F=FULL: f
[*] Running FULL scan on: 192.168.223.0/24
[#] BASIC done as part of FULL.
[*] Running BASIC scan on: 192.168.223.0/24
```

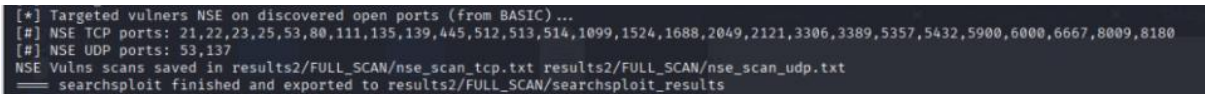
In the end it moves the results of thr BASIC function into FULL_SCAN dir.



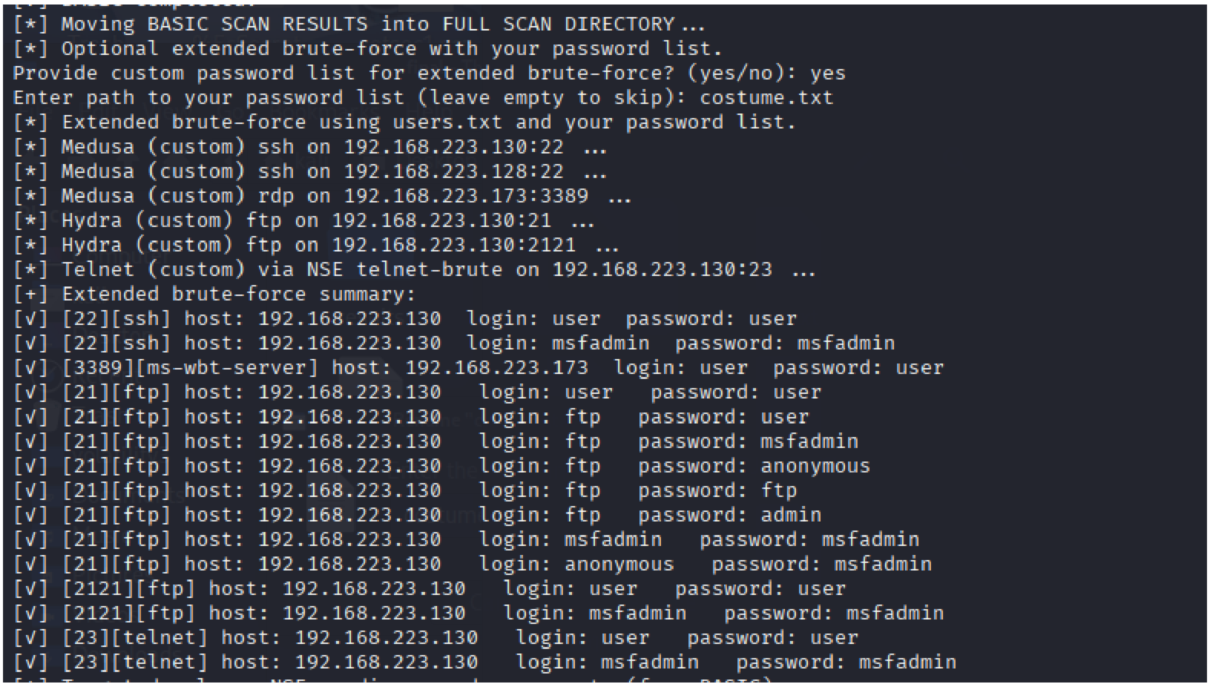
```
[*] Moving BASIC SCAN RESULTS into FULL SCAN DIRECTORY...
```

So it includes the weak password function inside.

3. Mapping Vulnerabilities 3.1 Mapping vulnerabilities should only take place if Full was chosen. 3.2 Display potential vulnerabilities via NSE and Searchsploit.

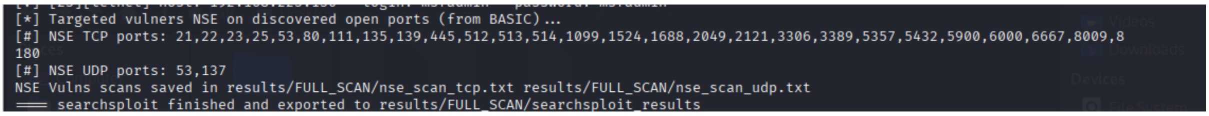


```
[*] Targeted vulners NSE on discovered open ports (from BASIC)...
[#] NSE TCP ports: 21,22,23,25,53,80,111,135,139,445,512,513,514,1099,1524,1688,2049,2121,3306,3389,5357,5432,5900,6000,6667,8009,8180
[#] NSE UDP ports: 53,137
NSE Vulns scans saved in results2/FULL_SCAN/nse_scan_tcp.txt results2/FULL_SCAN/nse_scan_udp.txt
═══ searchsploit finished and exported to results2/FULL_SCAN/searchsploit_results
```



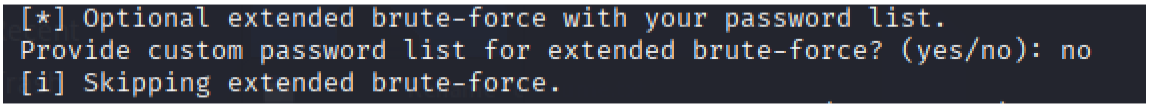
```
[*] Moving BASIC SCAN RESULTS into FULL SCAN DIRECTORY...
[*] Optional extended brute-force with your password list.
Provide custom password list for extended brute-force? (yes/no): yes
Enter path to your password list (leave empty to skip): costume.txt
[*] Extended brute-force using users.txt and your password list.
[*] Medusa (custom) ssh on 192.168.223.130:22  ...
[*] Medusa (custom) ssh on 192.168.223.128:22  ...
[*] Medusa (custom) rdp on 192.168.223.173:3389  ...
[*] Hydra (custom) ftp on 192.168.223.130:21  ...
[*] Hydra (custom) ftp on 192.168.223.130:2121  ...
[*] Telnet (custom) via NSE telnet-brute on 192.168.223.130:23  ...
[+] Extended brute-force summary:
[√] [22][ssh] host: 192.168.223.130  login: user  password: user
[√] [22][ssh] host: 192.168.223.130  login: msfadmin  password: msfadmin
[√] [3389][ms-wbt-server] host: 192.168.223.173  login: user  password: user
[√] [21][ftp] host: 192.168.223.130   login: user   password: user
[√] [21][ftp] host: 192.168.223.130   login: ftp   password: user
[√] [21][ftp] host: 192.168.223.130   login: ftp   password: msfadmin
[√] [21][ftp] host: 192.168.223.130   login: ftp   password: anonymous
[√] [21][ftp] host: 192.168.223.130   login: ftp   password: ftp
[√] [21][ftp] host: 192.168.223.130   login: ftp   password: admin
[√] [21][ftp] host: 192.168.223.130   login: msfadmin   password: msfadmin
[√] [21][ftp] host: 192.168.223.130   login: anonymous   password: msfadmin
[√] [2121][ftp] host: 192.168.223.130   login: user   password: user
[√] [2121][ftp] host: 192.168.223.130   login: msfadmin   password: msfadmin
[√] [23][telnet] host: 192.168.223.130   login: user   password: user
[√] [23][telnet] host: 192.168.223.130   login: msfadmin   password: msfadmin
```

3. Mapping Vulnerabilities 3.1 Mapping vulnerabilities should only take place if Full was chosen. 3.2 Display potential vulnerabilities via NSE and Searchsploit.



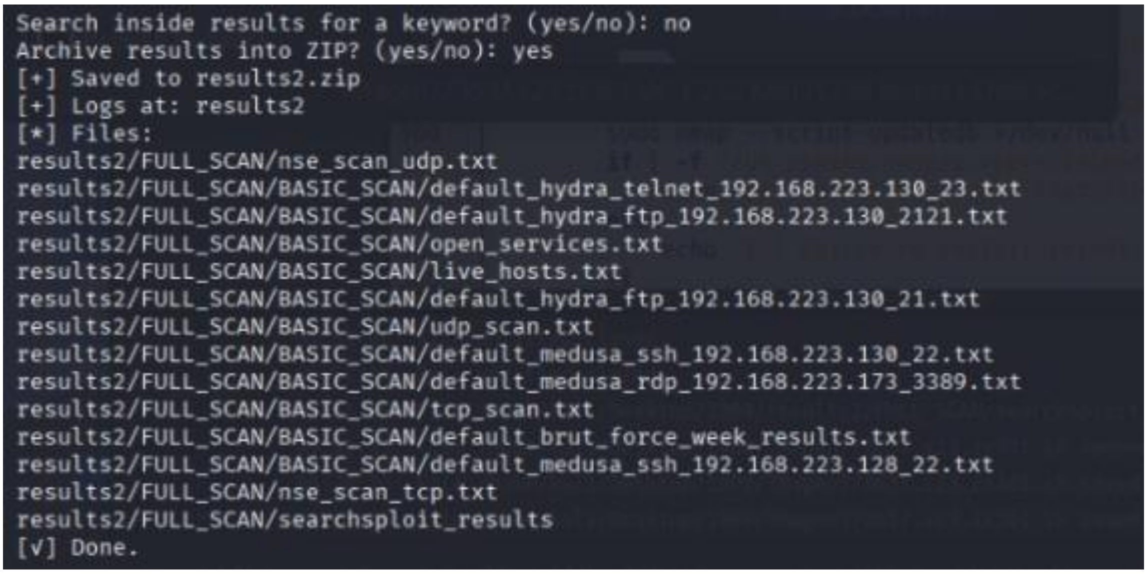
```
[*] Targeted vulners NSE on discovered open ports (from BASIC)...
[#] NSE TCP ports: 21,22,23,25,53,80,111,135,139,445,512,513,514,1099,1524,1688,2049,2121,3306,3389,5357,5432,5900,6000,6667,8009,8
180
[#] NSE UDP ports: 53,137
NSE Vulns scans saved in results/FULL_SCAN/nse_scan_tcp.txt results/FULL_SCAN/nse_scan_udp.txt
═══ searchsploit finished and exported to results/FULL_SCAN/searchsploit_results
```

The script also let the user to skip his own password list.



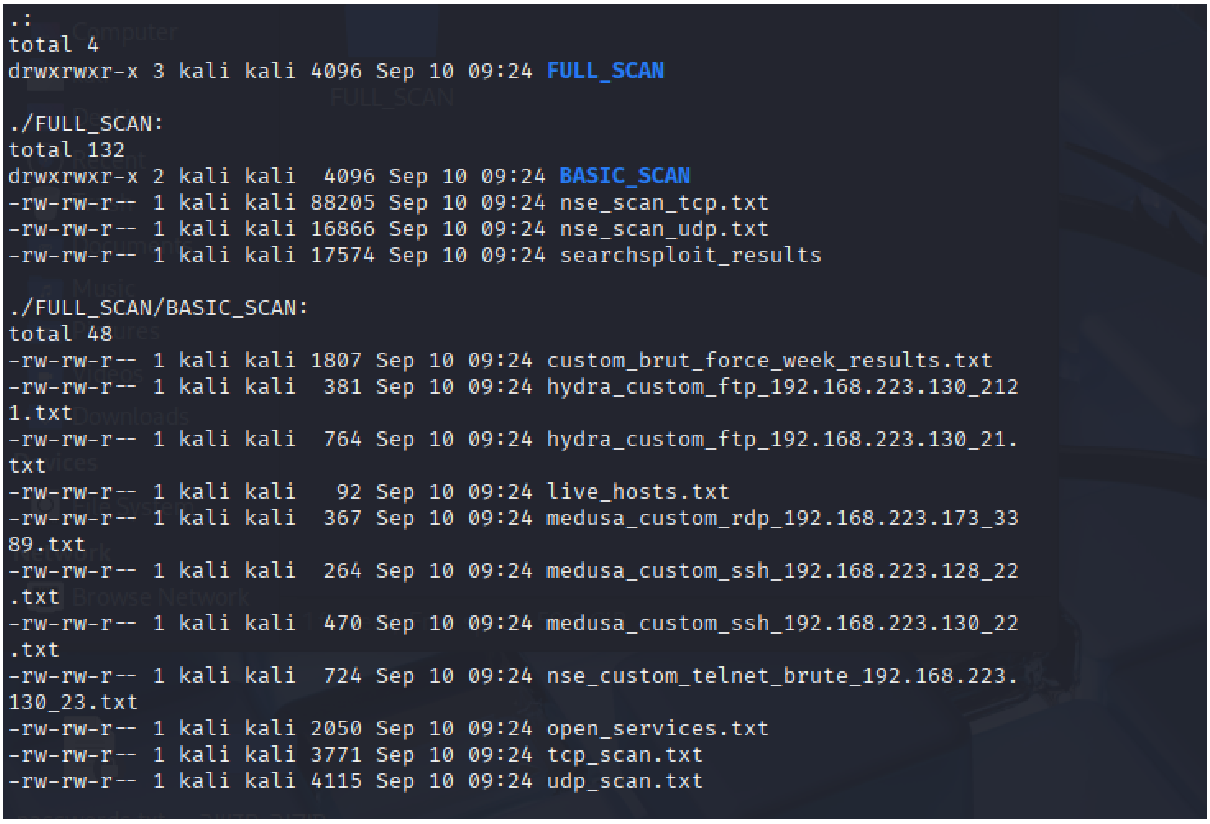
```
[*] Optional extended brute-force with your password list.
Provide custom password list for extended brute-force? (yes/no): no
[i] Skipping extended brute-force.
```

4. Log Results 4.1 During each stage, display the stage in the terminal. 4.2 At the end, show the user the found information. 4.3 Allow the user to search inside the results. 4.4 Allow to save all results into a Zip file.



```
Search inside results for a keyword? (yes/no): no
Archive results into ZIP? (yes/no): yes
[+] Saved to results2.zip
[+] Logs at: results2
[*] Files:
results2/FULL_SCAN/nse_scan_udp.txt
results2/FULL_SCAN/BASIC_SCAN/default_hydra_telnet_192.168.223.130_23.txt
results2/FULL_SCAN/BASIC_SCAN/default_hydra_ftp_192.168.223.130_2121.txt
results2/FULL_SCAN/BASIC_SCAN/open_services.txt
results2/FULL_SCAN/BASIC_SCAN/live_hosts.txt
results2/FULL_SCAN/BASIC_SCAN/default_hydra_ftp_192.168.223.130_21.txt
results2/FULL_SCAN/BASIC_SCAN/udp_scan.txt
results2/FULL_SCAN/BASIC_SCAN/default_medusa_ssh_192.168.223.130_22.txt
results2/FULL_SCAN/BASIC_SCAN/default_medusa_rdp_192.168.223.173_3389.txt
results2/FULL_SCAN/BASIC_SCAN/tcp_scan.txt
results2/FULL_SCAN/BASIC_SCAN/default_brut_force_week_results.txt
results2/FULL_SCAN/BASIC_SCAN/default_medusa_ssh_192.168.223.128_22.txt
results2/FULL_SCAN/nse_scan_tcp.txt
results2/FULL_SCAN/searchsploit_results
[√] Done.
```

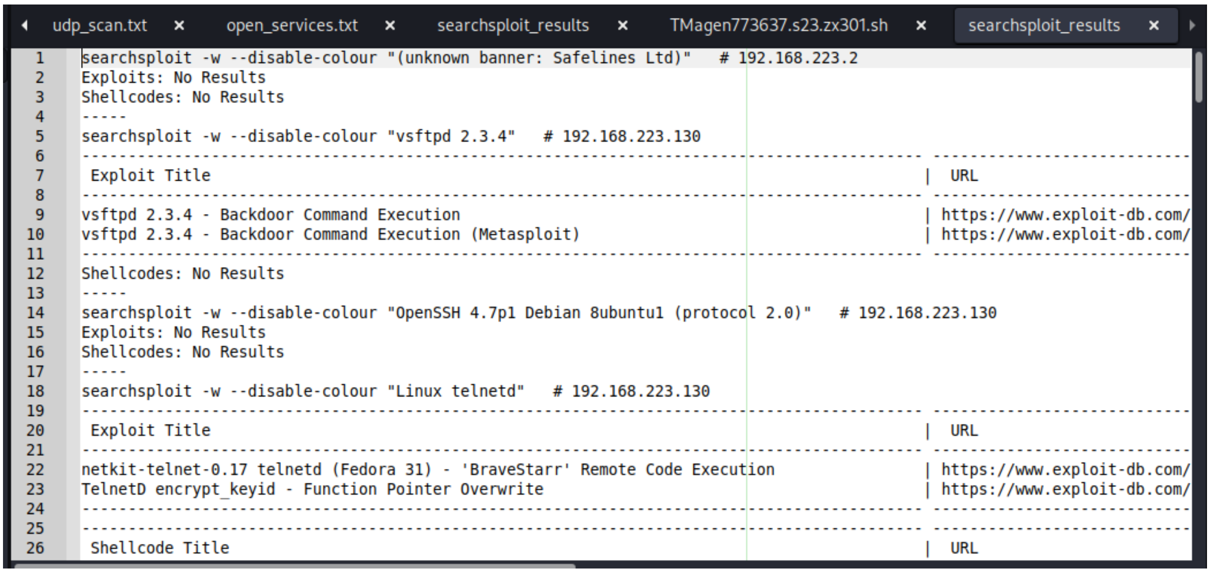
All stages are documents – every function/command being made. All is stored in the results directory:



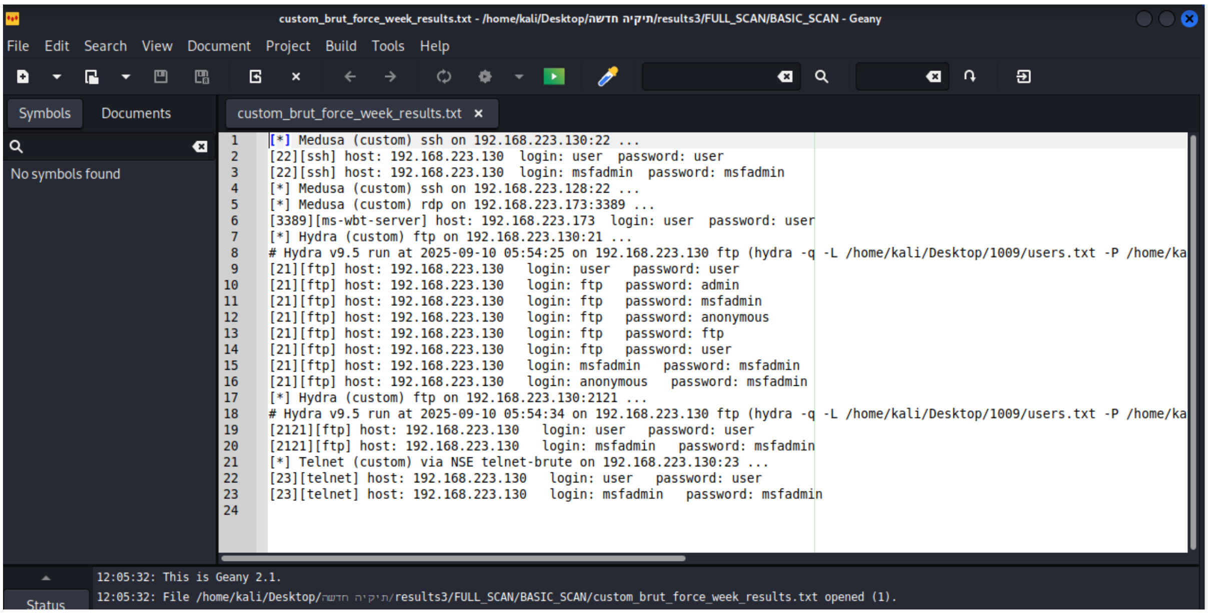
```
.:
total 4
drwxrwxr-x 3 kali kali 4096 Sep 10 09:24 FULL_SCAN

./FULL_SCAN:
total 132
drwxrwxr-x 2 kali kali  4096 Sep 10 09:24 BASIC_SCAN
-rw-rw-r-- 1 kali kali 88205 Sep 10 09:24 nse_scan_tcp.txt
-rw-rw-r-- 1 kali kali 16866 Sep 10 09:24 nse_scan_udp.txt
-rw-rw-r-- 1 kali kali 17574 Sep 10 09:24 searchsploit_results

./FULL_SCAN/BASIC_SCAN:
total 48
-rw-rw-r-- 1 kali kali 1807 Sep 10 09:24 custom_brut_force_week_results.txt
-rw-rw-r-- 1 kali kali  381 Sep 10 09:24 hydra_custom_ftp_192.168.223.130_212
1.txt
-rw-rw-r-- 1 kali kali  764 Sep 10 09:24 hydra_custom_ftp_192.168.223.130_21.
txt
-rw-rw-r-- 1 kali kali   92 Sep 10 09:24 live_hosts.txt
-rw-rw-r-- 1 kali kali  367 Sep 10 09:24 medusa_custom_rdp_192.168.223.173_33
89.txt
-rw-rw-r-- 1 kali kali  264 Sep 10 09:24 medusa_custom_ssh_192.168.223.128_22
.txt
-rw-rw-r-- 1 kali kali  470 Sep 10 09:24 medusa_custom_ssh_192.168.223.130_22
.txt
-rw-rw-r-- 1 kali kali  724 Sep 10 09:24 nse_custom_telnet_brute_192.168.223.
130_23.txt
-rw-rw-r-- 1 kali kali 2050 Sep 10 09:24 open_services.txt
-rw-rw-r-- 1 kali kali 3771 Sep 10 09:24 tcp_scan.txt
-rw-rw-r-- 1 kali kali 4115 Sep 10 09:24 udp_scan.txt
```

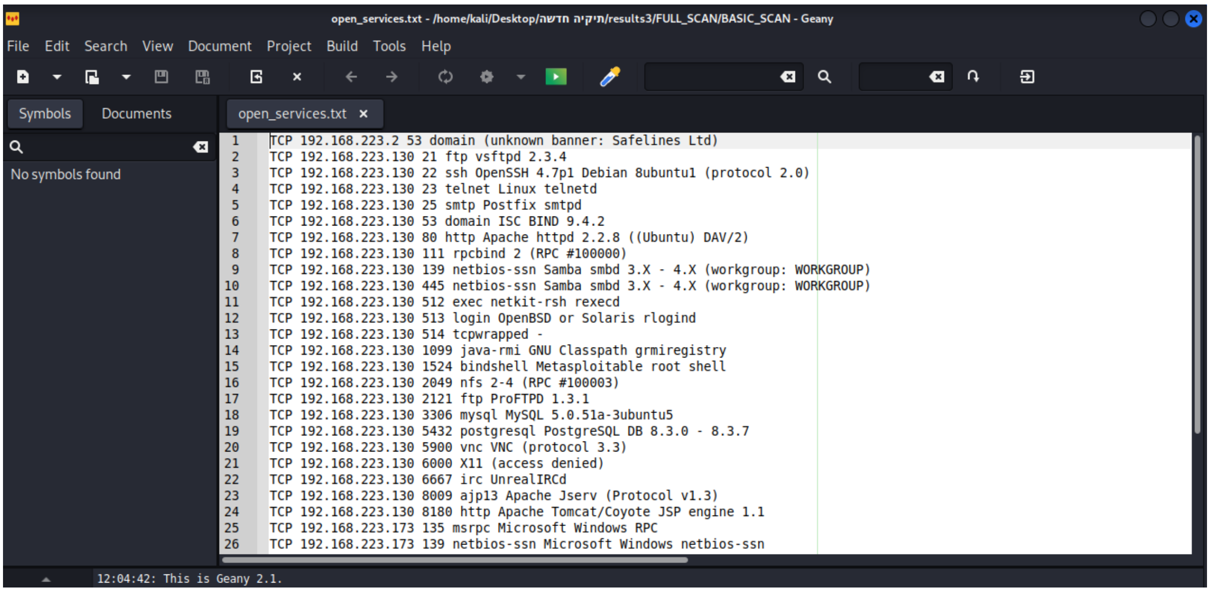


```
searchsploit -w --disable-colour "(unknown banner: Safelines Ltd)"   # 192.168.223.2
Exploits: No Results
Shellcodes: No Results
-----
searchsploit -w --disable-colour "vsftpd 2.3.4"   # 192.168.223.130
------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                            |  URL
------------------------------------------------------------------------------------------ ----------------------------
vsftpd 2.3.4 - Backdoor Command Execution                                                 | https://www.exploit-db.com/
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                    | https://www.exploit-db.com/
------------------------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
-----
searchsploit -w --disable-colour "OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)"   # 192.168.223.130
Exploits: No Results
Shellcodes: No Results
-----
searchsploit -w --disable-colour "Linux telnetd"   # 192.168.223.130
------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                            |  URL
------------------------------------------------------------------------------------------ ----------------------------
netkit-telnet-0.17 telnetd (Fedora 31) - 'BraveStarr' Remote Code Execution               | https://www.exploit-db.com/
TelnetD encrypt_keyid - Function Pointer Overwrite                                        | https://www.exploit-db.com/
------------------------------------------------------------------------------------------ ----------------------------
------------------------------------------------------------------------------------------ ----------------------------
 Shellcode Title                                                                          |  URL
```


custom_brut_force_week_results.txt - /home/kali/Desktop/תיקיה חדשה/results3/FULL_SCAN/BASIC_SCAN - Geany
File
Edit
Search
View
Document
Project
Build
Tools
Help
Symbols
Documents
custom_brut_force_week_results.txt
No symbols found
Status

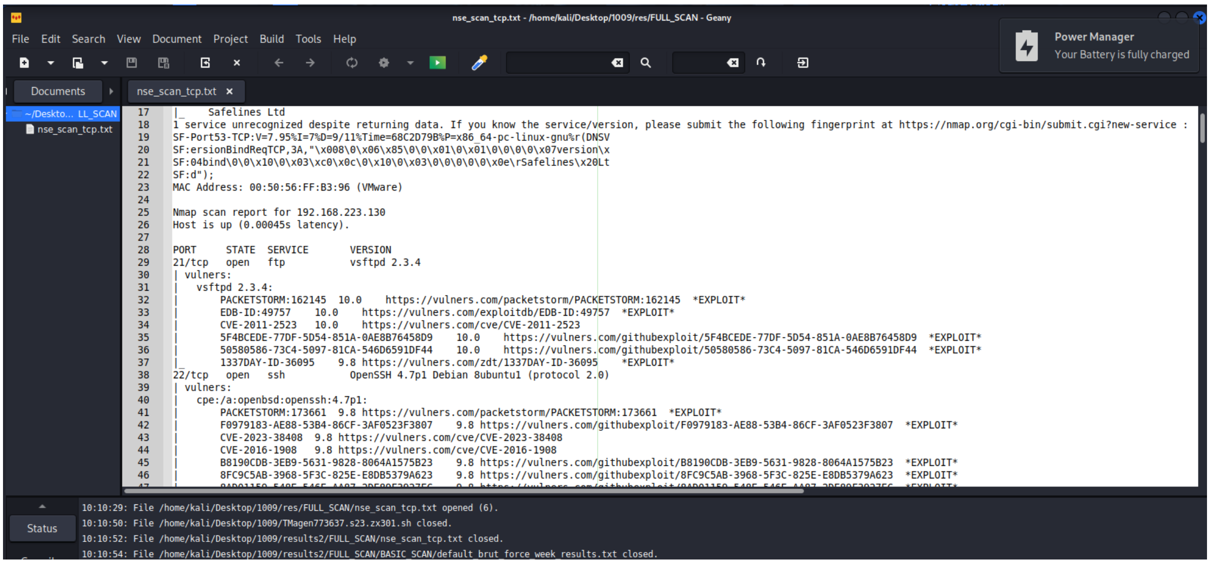
```
[*] Medusa (custom) ssh on 192.168.223.130:22 ...
[22][ssh] host: 192.168.223.130  login: user  password: user
[22][ssh] host: 192.168.223.130  login: msfadmin  password: msfadmin
[*] Medusa (custom) ssh on 192.168.223.128:22 ...
[*] Medusa (custom) rdp on 192.168.223.173:3389 ...
[3389][ms-wbt-server] host: 192.168.223.173  login: user  password: user
[*] Hydra (custom) ftp on 192.168.223.130:21 ...
# Hydra v9.5 run at 2025-09-10 05:54:25 on 192.168.223.130 ftp (hydra -q -L /home/kali/Desktop/1009/users.txt -P /home/ka
[21][ftp] host: 192.168.223.130   login: user   password: user
[21][ftp] host: 192.168.223.130   login: ftp   password: admin
[21][ftp] host: 192.168.223.130   login: ftp   password: msfadmin
[21][ftp] host: 192.168.223.130   login: ftp   password: anonymous
[21][ftp] host: 192.168.223.130   login: ftp   password: ftp
[21][ftp] host: 192.168.223.130   login: ftp   password: user
[21][ftp] host: 192.168.223.130   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.223.130   login: anonymous   password: msfadmin
[*] Hydra (custom) ftp on 192.168.223.130:2121 ...
# Hydra v9.5 run at 2025-09-10 05:54:34 on 192.168.223.130 ftp (hydra -q -L /home/kali/Desktop/1009/users.txt -P /home/ka
[2121][ftp] host: 192.168.223.130   login: user   password: user
[2121][ftp] host: 192.168.223.130   login: msfadmin   password: msfadmin
[*] Telnet (custom) via NSE telnet-brute on 192.168.223.130:23 ...
[23][telnet] host: 192.168.223.130   login: user   password: user
[23][telnet] host: 192.168.223.130   login: msfadmin   password: msfadmin
```

```
12:05:32: This is Geany 2.1.
12:05:32: File /home/kali/Desktop/תיקיה חדשה/results3/FULL_SCAN/BASIC_SCAN/custom_brut_force_week_results.txt opened (1).
```



```
TCP 192.168.223.2 53 domain (unknown banner: Safelines Ltd)
TCP 192.168.223.130 21 ftp vsftpd 2.3.4
TCP 192.168.223.130 22 ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
TCP 192.168.223.130 23 telnet Linux telnetd
TCP 192.168.223.130 25 smtp Postfix smtpd
TCP 192.168.223.130 53 domain ISC BIND 9.4.2
TCP 192.168.223.130 80 http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
TCP 192.168.223.130 111 rpcbind 2 (RPC #100000)
TCP 192.168.223.130 139 netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
TCP 192.168.223.130 445 netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
TCP 192.168.223.130 512 exec netkit-rsh rexecd
TCP 192.168.223.130 513 login OpenBSD or Solaris rlogind
TCP 192.168.223.130 514 tcpwrapped -
TCP 192.168.223.130 1099 java-rmi GNU Classpath grmiregistry
TCP 192.168.223.130 1524 bindshell Metasploitable root shell
TCP 192.168.223.130 2049 nfs 2-4 (RPC #100003)
TCP 192.168.223.130 2121 ftp ProFTPD 1.3.1
TCP 192.168.223.130 3306 mysql MySQL 5.0.51a-3ubuntu5
TCP 192.168.223.130 5432 postgresql PostgreSQL DB 8.3.0 - 8.3.7
TCP 192.168.223.130 5900 vnc VNC (protocol 3.3)
TCP 192.168.223.130 6000 X11 (access denied)
TCP 192.168.223.130 6667 irc UnrealIRCd
TCP 192.168.223.130 8009 ajp13 Apache Jserv (Protocol v1.3)
TCP 192.168.223.130 8180 http Apache Tomcat/Coyote JSP engine 1.1
TCP 192.168.223.173 135 msrpc Microsoft Windows RPC
TCP 192.168.223.173 139 netbios-ssn Microsoft Windows netbios-ssn
```

```
12:04:42: This is Geany 2.1.
```



Power Manager
Your Battery is fully charged

```
|_    Safelines Ltd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.95%I=7%D=9/11%Time=68C2D79B%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,3A,"\x008\0\x06\x85\0\0\x01\0\x01\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x0e\rSafelines\x20Lt
SF:d");
MAC Address: 00:50:56:FF:B3:96 (VMware)

Nmap scan report for 192.168.223.130
Host is up (0.00045s latency).

PORT     STATE  SERVICE       VERSION
21/tcp   open   ftp           vsftpd 2.3.4
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145  10.0    https://vulners.com/packetstorm/PACKETSTORM:162145  *EXPLOIT*
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757  *EXPLOIT*
|       CVE-2011-2523   10.0    https://vulners.com/cve/CVE-2011-2523
|       5F4BCEDE-77DF-5D54-851A-0AE8B76458D9    10.0    https://vulners.com/githubexploit/5F4BCEDE-77DF-5D54-851A-0AE8B76458D9  *EXPLOIT*
|       50580586-73C4-5097-81CA-546D6591DF44    10.0    https://vulners.com/githubexploit/50580586-73C4-5097-81CA-546D6591DF44  *EXPLOIT*
|_      1337DAY-ID-36095    9.8 https://vulners.com/zdt/1337DAY-ID-36095    *EXPLOIT*
22/tcp   open   ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       PACKETSTORM:173661  9.8 https://vulners.com/packetstorm/PACKETSTORM:173661  *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8 https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
|       CVE-2023-38408  9.8 https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8 https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8 https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8 https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
```

```
10:10:29: File /home/kali/Desktop/1009/res/FULL_SCAN/nse_scan_tcp.txt opened (6).
10:10:50: File /home/kali/Desktop/1009/TMagen773637.s23.zx301.sh closed.
10:10:52: File /home/kali/Desktop/1009/results2/FULL_SCAN/nse_scan_tcp.txt closed.
10:10:54: File /home/kali/Desktop/1009/results2/FULL_SCAN/BASIC_SCAN/default_brut_force_week_results.txt closed.
```