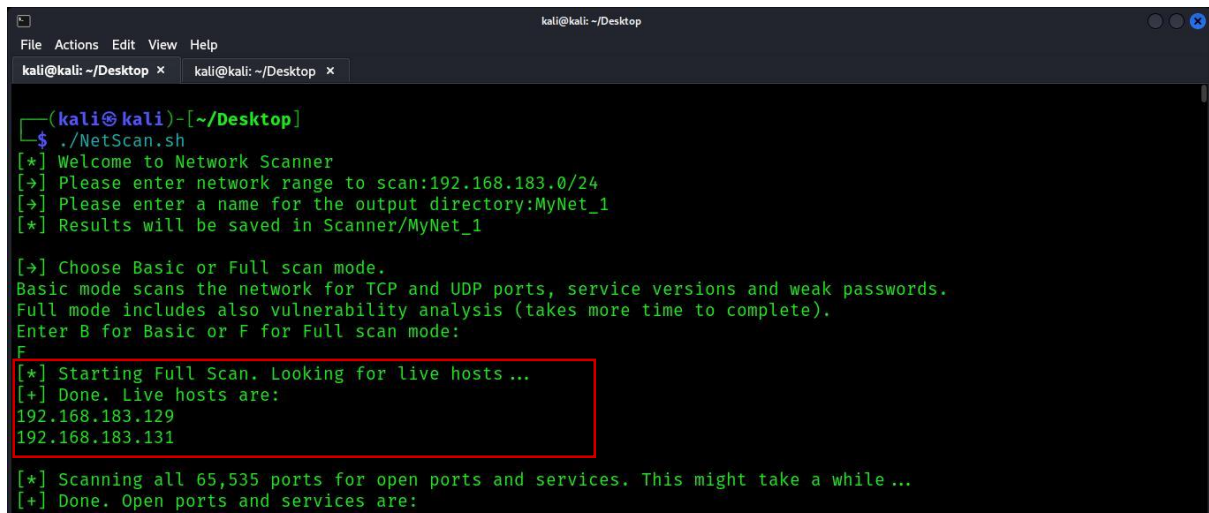


## NetScan

1. Get from the user a network range and a name for the output directory
2. The user can choose Basic or Full Scan Mode
3. Identify and display live hosts:

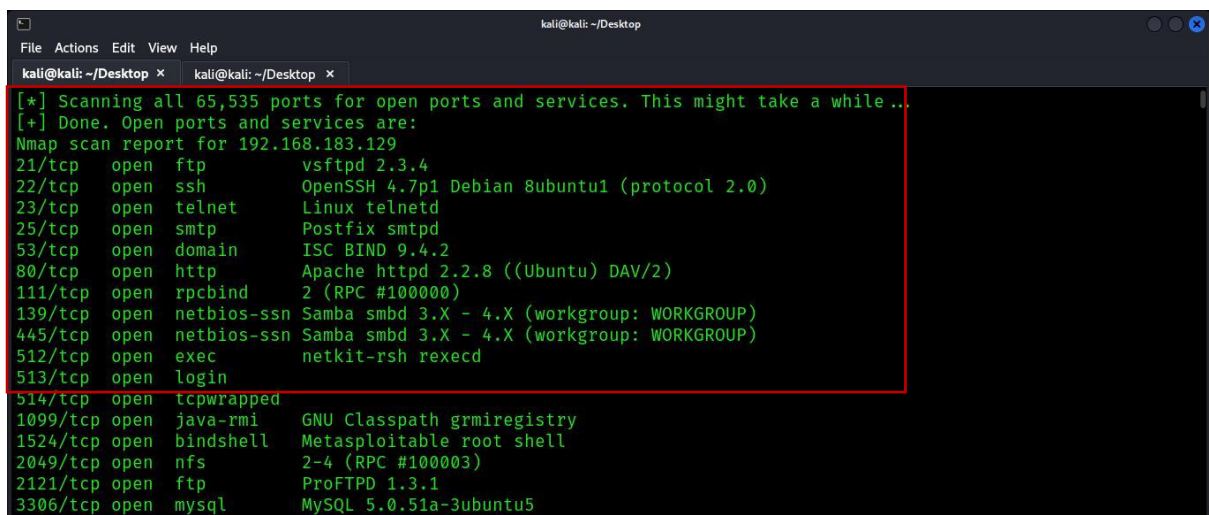


```
(kali@kali)-[~/Desktop]
$ ./NetScan.sh
[*] Welcome to Network Scanner
[+] Please enter network range to scan:192.168.183.0/24
[+] Please enter a name for the output directory:MyNet_1
[*] Results will be saved in Scanner/MyNet_1

[+] Choose Basic or Full scan mode.
Basic mode scans the network for TCP and UDP ports, service versions and weak passwords.
Full mode includes also vulnerability analysis (takes more time to complete).
Enter B for Basic or F for Full scan mode:
F
[*] Starting Full Scan. Looking for live hosts ...
[+] Done. Live hosts are:
192.168.183.129
192.168.183.131

[*] Scanning all 65,535 ports for open ports and services. This might take a while ...
[+] Done. Open ports and services are:
```

1. Scan live hosts for open ports, services and service versions
2. Display the results



```
[*] Scanning all 65,535 ports for open ports and services. This might take a while ...
[+] Done. Open ports and services are:
Nmap scan report for 192.168.183.129
21/tcp open  ftp          vsftpd 2.3.4
22/tcp open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open  telnet       Linux telnetd
25/tcp open  smtp         Postfix smtpd
53/tcp open  domain       ISC BIND 9.4.2
80/tcp open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind      2 (RPC #100000)
139/tcp open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open  exec         netkit-rsh rexecd
513/tcp open  login
514/tcp open  tcpwrapped
1099/tcp open java-rmi      GNU Classpath grmiregistry
1524/tcp open bindshell     Metasploitable root shell
2049/tcp open nfs          2-4 (RPC #100003)
2121/tcp open ftp          ProFTPD 1.3.1
3306/tcp open mysql        MySQL 5.0.51a-3ubuntu5
```

1. Prompt the user to upload a list of accounts to check
2. Option to get passwords list from the user or download most common passwords list from GitHub
3. Make sure that the input was submitted correctly

```
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop x kali@kali: ~/Desktop x
2121/tcp open  ftp      ProFTPD 1.3.1
3306/tcp open  mysql    MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc      VNC (protocol 3.3)
6000/tcp open  X11      (access denied)
6667/tcp open  irc      UnrealIRCd
8009/tcp open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp open  http     Apache Tomcat/Coyote JSP engine 1.1
Nmap done: 1 IP address (1 host up) scanned in 53.09 seconds
Nmap scan report for 192.168.183.131
22/tcp open  ssh      OpenSSH 9.4p1 Debian 1 (protocol 2.0)
Nmap done: 1 IP address (1 host up) scanned in 16.50 seconds

[*] Check for weak passwords
[+] Please upload users list into /home/kali/Desktop/Scanner/MyNet_1
[+] Once uploaded, enter file name:users
[+] You submitted: users
[+] Do you want to submit your own password list? [y/n]y
[+] Please upload your password list into /home/kali/Desktop/Scanner/MyNet_1
[+] Once uploaded, enter file name:pass
```

1. Brute-force attack
2. Display cracked passwords:

```
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop x kali@kali: ~/Desktop x
[+] Please upload your password list into /home/kali/Desktop/Scanner/MyNet_1
[+] Once uploaded, enter file name:pass
[+] You submitted: pass
[*] Checking for login weak passwords. This might take a while ...
NOTICE: ftp.mod: failed to connect, port 21 was not open on 192.168.183.131
NOTICE: smbnt.mod Failed to establish WIN2000_NATIVE mode. Attempting WIN_NETBIOS mode.)
ERROR: smbnt.mod: failed to connect, port 139 was not open on 192.168.183.131

[*] Weak passwords (if found):
ACCOUNT FOUND: [ssh] Host: 192.168.183.129 User: msfadmin Password: msfadmin [SUCCESS]
ACCOUNT FOUND: [ssh] Host: 192.168.183.131 User: kali Password: kali [SUCCESS]
ACCOUNT FOUND: [ftp] Host: 192.168.183.129 User: msfadmin Password: msfadmin [SUCCESS]
ACCOUNT FOUND: [smbnt] Host: 192.168.183.129 User: msfadmin Password: msfadmin [SUCCESS (ADMIN$ - Access Allowed)]
[*] Scanning for vulnerabilities. Might take a few minutes ...
[+] Done. Discovered vulnerabilities are:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 16:10 EDT
Nmap scan report for 192.168.183.129
Host is up (0.21s latency).
Not shown: 977 closed tcp ports (conn-refused)
```

1. If Full Scan was chosen scan for potential vulnerabilities (nse category "vuln")
2. Display the results

```

kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop x kali@kali: ~/Desktop x

| Disclosure date: 2011-07-03
| Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
| References:
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   https://www.securityfocus.com/bid/48539
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_ 22/tcp open ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|   SSV:78173      7.8   https://vulners.com/seebug/SSV:78173      *EXPLOIT*
|   SSV:69983      7.8   https://vulners.com/seebug/SSV:69983      *EXPLOIT*
|   EDB-ID:24450   7.8   https://vulners.com/exploitdb/EDB-ID:24450 *EXPLOIT*
|   EDB-ID:15215   7.8   https://vulners.com/exploitdb/EDB-ID:15215 *EXPLOIT*
|   SECURITYVULNS:VULN:8166 7.5   https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|   PRION:CVE-2010-4478 7.5   https://vulners.com/prion/PRION:CVE-2010-4478
|   CVE-2010-4478 7.5   https://vulners.com/cve/CVE-2010-4478

```

1. Option to search within the results:

```

kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop x kali@kali: ~/Desktop x

Nmap done: 1 IP address (1 host up) scanned in 91.37 seconds

[+] Full scan completed.
[+] Do you want to search within the results? [y/n] y
[+] Enter key word
sql
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| http-sql-injection:
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| Possible sql injection queries:
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| http://192.168.183.129:80/dav/?C=N%3B0%3DD%27%20OR
| %20sqlspider
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| http://192.168.183.129:80/dav/?C=D%3B0%3DA%27%20OR
| %20sqlspider
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| http://192.168.183.129:80/dav/?C=M%3B0%3DA%27%20OR
| %20sqlspider
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| http://192.168.183.129:80/dav/?C=S%3B0%3DA%27%20OR
| %20sqlspider
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| http://192.168.183.129:80/mutillidae/index.php?page
| e=view-someones-blog.php%27%20OR%20sqlspider
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| http://192.168.183.129:80/mutillidae/index.php?page
| e=login.php%27%20OR%20sqlspider

```

1. Option to save all results into a Zip file
2. Bye-Bye

```
kali@kali: ~/Desktop
File Actions Edit View Help
kali@kali: ~/Desktop x kali@kali: ~/Desktop x
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| POSTGRESQL:CVE-2012-0867 4.3 https:/
/vulners.com/postgresql/POSTGRESQL:CVE-2012-0867
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| POSTGRESQL:CVE-2014-0066 4.0 https:/
/vulners.com/postgresql/POSTGRESQL:CVE-2014-0066
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| POSTGRESQL:CVE-2014-0060 4.0 https:/
/vulners.com/postgresql/POSTGRESQL:CVE-2014-0060
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| POSTGRESQL:CVE-2012-3489 4.0 https:/
/vulners.com/postgresql/POSTGRESQL:CVE-2012-3489
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| POSTGRESQL:CVE-2012-2655 4.0 https:/
/vulners.com/postgresql/POSTGRESQL:CVE-2012-2655
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| POSTGRESQL:CVE-2009-3229 4.0 https:/
/vulners.com/postgresql/POSTGRESQL:CVE-2009-3229
/home/kali/Desktop/Scanner/MyNet_1/vulnerabilities.txt:| POSTGRESQL:CVE-2009-0922 4.0 https:/
/vulners.com/postgresql/POSTGRESQL:CVE-2009-0922
[+] Do you want to search within the results? [y/n]n
[+] Do you want to save results into a Zip file? [y/n]y
[+] Archive MyNet_1.zip created in /home/kali/Desktop/Scanner. Bye-Bye
(kali@kali)-[~/Desktop]
$
```