```
\ | | ___| \ | | __| | | |  _  _ / \ | | __ _ ___ _ __
| \| |/ _ \ \| |/ _` | | |  | | | |/ _ \ | |/ _` |/ _ \ '__|
| |\ |  __/ |\ | (_| | | |__| |_| / ___ \| | (_| |  __/ |
|_| \_|\___|_| \_|\__,_| |_____\__, /_/  \_\_|\__,_|\___|_|
                                  |___/
```

Network Vulnerability & Enumeration Reconnaissance Tool

==========

>> Checking for required tools...

==========

[OK] nmap is installed.

[OK] masscan is installed.

[OK] hydra is installed.

[OK] searchsploit is installed.

[OK] zip is installed.

==========

>> Configuration

==========

Enter the network range to scan (e.g., 192.168.1.0/24): 192.168.80.1/24

Enter a name for the output directory: result

Results will be saved in '/home/kali/Documents/ZX301/lab9/result'

Choose scan type [B]asic or [F]ull: B

Enter path to a custom password list (or press Enter to use a default list):

Custom list not found or not provided. Creating a default password list.

==========

>> Phase 1: Host Discovery

```
======================================================================
Using masscan to quickly find live hosts...
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-06-07 10:46:07 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [6 ports/host]
Masscan found no hosts. Trying nmap ping scan as a fallback...
Discovery complete. Found 5 live host(s). List saved to 'live_hosts.txt'.

======================================================================
>> Phase 2: Basic Scan (Port & Service Enumeration)
======================================================================
Running a basic Nmap scan for TCP ports and service versions...
This may take a significant amount of time depending on the network size...
Nmap scan complete. Results saved to 'nmap_basic_scan.txt' and 'nmap_basic_scan.xml'.
Skipping vulnerability mapping (only available in Full scan mode).

======================================================================
>> Phase 4: Weak Credential Check
======================================================================
Scanning for open login services to test for weak passwords...

No open ports found for telnet.

No open ports found for rdp.

No open ports found for ssh.

No open ports found for ftp.
```

==========

>> Scan Summary & Final Report

==========

--- Live Hosts ---

192.168.80.1

192.168.80.2

192.168.80.132

192.168.80.254

192.168.80.128

--- Open Ports & Services ---

53/tcp open domain dnsmasq 2.51

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

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 OpenBSD or Solaris rlogind

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

3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

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

6697/tcp open irc UnrealIRCd

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

41287/tcp open status 1 (RPC #100024)

45630/tcp open java-rmi GNU Classpath grmiregistry

52296/tcp open mountd 1-3 (RPC #100005)

60120/tcp open nlockmgr 1-4 (RPC #100021)

22/tcp open ssh OpenSSH 9.9p1 Debian 3 (protocol 2.0)

80/tcp open http Apache httpd 2.4.63 ((Debian))

111/tcp open rpcbind 2-4 (RPC #100000)

43069/tcp open status 1 (RPC #100024)

--- Weak Credentials Found ---

None found.

Enter a term to [S]earch results, [Z]ip results, or [Q]uit: S

Enter search term: ftp

--- Searching for 'ftp' in all result files ---

./nmap_basic_scan.txt

./nmap_basic_scan.xml

./users.lst

Enter a term to [S]earch results, [Z]ip results, or [Q]uit: Q