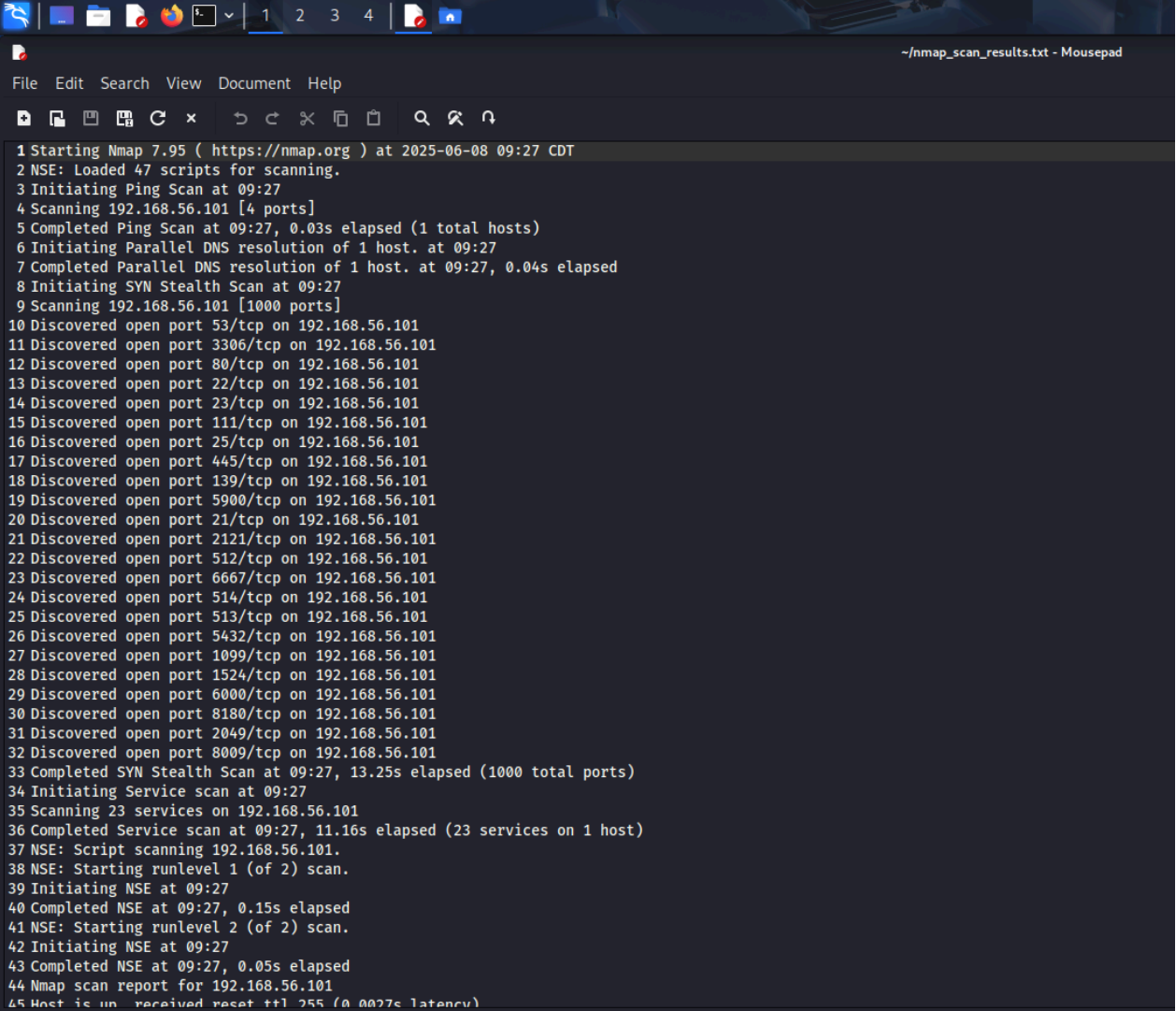


NMAP SCAN OUTPUT SCREENSHOTS



The screenshot shows a terminal window with a dark background and light-colored text. The window title is "~nmap_scan_results.txt - Mousepad". The menu bar includes File, Edit, Search, View, Document, and Help. The toolbar contains icons for file operations and search. The terminal output is a list of numbered steps from 1 to 45, detailing the Nmap scan process. The scan is performed on 192.168.56.101. It starts with a ping scan, followed by a SYN Stealth scan of 1000 ports. The scan discovers 32 open ports: 53/tcp, 3306/tcp, 80/tcp, 22/tcp, 23/tcp, 111/tcp, 25/tcp, 445/tcp, 139/tcp, 5900/tcp, 21/tcp, 2121/tcp, 512/tcp, 6667/tcp, 514/tcp, 513/tcp, 5432/tcp, 1099/tcp, 1524/tcp, 6000/tcp, 8180/tcp, 2049/tcp, and 8009/tcp. The scan is completed at 09:27, 13.25s elapsed. The next step is to initiate a service scan. The scan is completed at 09:27, 11.16s elapsed (23 services on 1 host). The NSE script scanning is initiated. The NSE runlevel 1 scan is initiated. The NSE runlevel 2 scan is initiated. The NSE scan is completed at 09:27, 0.05s elapsed. The Nmap scan report for 192.168.56.101 is generated. The final output is: 45 Host is up, received reset ttl 255 (0.0027s latency).

```
1 Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-08 09:27 CDT
2 NSE: Loaded 47 scripts for scanning.
3 Initiating Ping Scan at 09:27
4 Scanning 192.168.56.101 [4 ports]
5 Completed Ping Scan at 09:27, 0.03s elapsed (1 total hosts)
6 Initiating Parallel DNS resolution of 1 host. at 09:27
7 Completed Parallel DNS resolution of 1 host. at 09:27, 0.04s elapsed
8 Initiating SYN Stealth Scan at 09:27
9 Scanning 192.168.56.101 [1000 ports]
10 Discovered open port 53/tcp on 192.168.56.101
11 Discovered open port 3306/tcp on 192.168.56.101
12 Discovered open port 80/tcp on 192.168.56.101
13 Discovered open port 22/tcp on 192.168.56.101
14 Discovered open port 23/tcp on 192.168.56.101
15 Discovered open port 111/tcp on 192.168.56.101
16 Discovered open port 25/tcp on 192.168.56.101
17 Discovered open port 445/tcp on 192.168.56.101
18 Discovered open port 139/tcp on 192.168.56.101
19 Discovered open port 5900/tcp on 192.168.56.101
20 Discovered open port 21/tcp on 192.168.56.101
21 Discovered open port 2121/tcp on 192.168.56.101
22 Discovered open port 512/tcp on 192.168.56.101
23 Discovered open port 6667/tcp on 192.168.56.101
24 Discovered open port 514/tcp on 192.168.56.101
25 Discovered open port 513/tcp on 192.168.56.101
26 Discovered open port 5432/tcp on 192.168.56.101
27 Discovered open port 1099/tcp on 192.168.56.101
28 Discovered open port 1524/tcp on 192.168.56.101
29 Discovered open port 6000/tcp on 192.168.56.101
30 Discovered open port 8180/tcp on 192.168.56.101
31 Discovered open port 2049/tcp on 192.168.56.101
32 Discovered open port 8009/tcp on 192.168.56.101
33 Completed SYN Stealth Scan at 09:27, 13.25s elapsed (1000 total ports)
34 Initiating Service scan at 09:27
35 Scanning 23 services on 192.168.56.101
36 Completed Service scan at 09:27, 11.16s elapsed (23 services on 1 host)
37 NSE: Script scanning 192.168.56.101.
38 NSE: Starting runlevel 1 (of 2) scan.
39 Initiating NSE at 09:27
40 Completed NSE at 09:27, 0.15s elapsed
41 NSE: Starting runlevel 2 (of 2) scan.
42 Initiating NSE at 09:27
43 Completed NSE at 09:27, 0.05s elapsed
44 Nmap scan report for 192.168.56.101
45 Host is up, received reset ttl 255 (0.0027s latency)
```

```
File Edit Search View Document Help
~/nmap_scan_results.txt - Mousepad

34 Initiating Service Scan at 09:27
35 Scanning 23 services on 192.168.56.101
36 Completed Service scan at 09:27, 11.16s elapsed (23 services on 1 host)
37 NSE: Script scanning 192.168.56.101.
38 NSE: Starting runlevel 1 (of 2) scan.
39 Initiating NSE at 09:27
40 Completed NSE at 09:27, 0.15s elapsed
41 NSE: Starting runlevel 2 (of 2) scan.
42 Initiating NSE at 09:27
43 Completed NSE at 09:27, 0.05s elapsed
44 Nmap scan report for 192.168.56.101
45 Host is up, received reset ttl 255 (0.0027s latency).
46 Scanned at 2025-06-08 09:27:30 CDT for 25s
47 Not shown: 977 filtered tcp ports (no-response)
48 PORT      STATE SERVICE      REASON      VERSION
49 21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.3.4
50 22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
51 23/tcp    open  telnet       syn-ack ttl 64 Linux telnetd
52 25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
53 53/tcp    open  domain       syn-ack ttl 64 ISC BIND 9.4.2
54 80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
55 111/tcp   open  rpcbind      syn-ack ttl 64 2 (RPC #100000)
56 139/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
57 445/tcp   open  netbios-ssn  syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
58 512/tcp   open  exec         syn-ack ttl 64 netkit-rsh rexecd
59 513/tcp   open  login?       syn-ack ttl 64
60 514/tcp   open  shell        syn-ack ttl 64 Netkit rshd
61 1099/tcp  open  java-rmi     syn-ack ttl 64 GNU Classpath grmiregistry
62 1524/tcp  open  bindshell    syn-ack ttl 64 Metasploitable root shell
63 2049/tcp  open  nfs          syn-ack ttl 64 2-4 (RPC #100003)
64 2121/tcp  open  ftp          syn-ack ttl 64 ProFTPD 1.3.1
65 3306/tcp  open  mysql        syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
66 5432/tcp  open  postgresql   syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
67 5900/tcp  open  vnc          syn-ack ttl 64 VNC (protocol 3.3)
68 6000/tcp  open  X11          syn-ack ttl 64 (access denied)
69 6667/tcp  open  irc          syn-ack ttl 64 UnrealIRCd
70 8009/tcp  open  ajp13        syn-ack ttl 64 Apache Jserv (Protocol v1.3)
71 8180/tcp  open  http         syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
72 Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
73
74 Read data files from: /usr/share/nmap
75 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
76 Nmap done: 1 IP address (1 host up) scanned in 25.02 seconds
77      Raw packets sent: 2968 (130.552KB) | Rcvd: 2135 (85.492KB)
78
```