Chapter 5: Scan a host using nmap

1. Start and login to your Kali Linux virtual machine as user **kali** with a password of **kali**.

2. Open a terminal window and start the ssh service by typing **sudo service ssh start**.

3. Type **sudo netstat -an | grep :22** to filter netstat output to show only lines containing :22, the port number used by ssh.

4. Type **sudo netstat -an | grep :123** to see if the Network Time Protocol (NTP) is listening on port 123. Nothing is shown.

5. Start NTP by typing **sudo service ntp start**.

6. Verify NTP is running with the **sudo service ntp status** command, as well as **the netstat -an | grep :123** command.

7. Perform a UDP (sU) and TCP (T) scan of the local Kali Linux host using the **sudo nmap 127.0.0.1 -sUT** command. Notice both NTP (UDP port 123) and SSH (TCP port 22) are listed in the scan output.

8. Perform an OS fingerprinting scan of the local Kali Linux host with the **sudo nmap -O 127.0.0.1** command. Notice the output shows that the host is running a Linux 2.6.X kernel.