Activity 6-1: Using the NBTscan Tool

Time Required: 5 minutes

Objective: Learn how to use the NBTscan tool.

Description: In this activity, you work with a partner and use the NBTscan tool to find systems running NetBIOS.

1. Discuss with your partner and decide which one will boot into Windows and which one will boot into Linux with the Kali Linux DVD.
2. Open a Terminal shell, type **nbtscan -h | less**, and press **Enter** to view the help page. Using this information, enter the `NBTscan` command to scan a range of IP addresses on your network and see whether any computers are identified. Can you identify your partner's Windows computer in the output? Figure 6-1 shows an example of output from the `NBTscan` command. Note the computers with NetBIOS names. The command also reveals the computers' MAC addresses.

Figure 6-1 NBTscan finds computers running NetBIOS

3. Shutdown Kali Linux and boot into Windows. Your partner should boot into Linux with the Kali Linux DVD and do Steps 1 and 2.
4. If necessary, shutdown Linux and boot into Windows for the next activity.

Enumerating Windows Operating Systems

To understand how an attacker might gain access to resources or shares on a Windows network, in this section you take a brief look at Windows OSs. Chapter 8 delves into more detail