Simulation transcript
Perform network reconnaissance by using network scanning tools

Task 1: Explore the command prompt

1. In this simulation, you will explore how to perform network reconnaissance by using network scanning tools to gather information about a computer network. Select the **Next arrow** to continue.

2. First, you'll use command-line tools. A command-line interface (CLI) is a user interface in which users type commands to navigate and manage the system. With it, you can complete some tasks more quickly and even automate them. Select the **Next arrow** to continue. (Note that the Windows version of the CLI is called the command prompt. Select **X** to close this window and continue.)

3. You can access the command prompt in different ways. In this simulation, you'll open it from the **Start menu**. First, select the **Start** icon, which is the Windows icon on the taskbar.

4. The **Start** menu opens. Scroll to the end of the list of applications, and then select **Windows System**.

5. Select **Command Prompt** from the list.

6. The Command Prompt window displays. The prompt includes the current directory, or folder, in which you are working. Currently, you are working in `C:\Users\cyber`. Select the **Next arrow** to continue.

7. Now, let's explore some helpful commands for network reconnaissance. You'll run these commands on scanme.nmap.org. Nmap's creator, Gordon Lyon, has set up this host so that you can scan it to test Nmap. But for now, you'll scan it by using command-line tools. Select the **Next arrow** to continue.

8. Nslookup is a command-line tool commonly used to troubleshoot network issues, verify DNS configurations, and gather information about specific domain names. Type `nslookup scanme.nmap.org` at the command prompt, and then press **Enter**.

9. The output includes the IP address, 45.33.32.156, associated with the given domain name. Select the **Next arrow** to continue.

10. Now, you will run a Ping test to discover how far into its network the host is located. Type `ping 45.33.32.156` at the command prompt, and then press **Enter**.

11. Review the output. The reply time, measured in milliseconds, indicates how long it took for each packet to reach its destination, and each packet's time to live (TTL) is 53. The Ping statistics section lists the total number of packets sent and received. Select the **Next arrow** to continue.

12. Now, you will run a traceroute to map the connection between your device and the target host. Type `tracert 45.33.32.156` at the command prompt, and then press **Enter**.

13. The output indicates that 14 switches or routers exist between your device and the host. It also reveals information about each device in the path, including its IP address and the length of time for each hop in the packet's journey. Select the **Next arrow** to continue.

14. You'll now close the Command Prompt window and return to the desktop. Select the **Close** button.

Task 2: Scan a network with Zenmap

15. Another network scanning tool is Nmap, a command-line program. In this simulation, you'll use Zenmap, the official GUI of Nmap. Select **Nmap – Zenmap GUI**.

16. The Zenmap window displays. To perform a scan, first, you must provide the target host's web address. Type `scanme.nmap.org` in the **Target** field, and then press **Enter**.

17. Throughout this simulation, notice how the text in the **Command** field updates as you change the **Target** and **Profile** fields. The text in the **Command** field is the command that you would run if performing the scan from the Nmap command-line tool. Select the **Next arrow** to continue.

18. Zenmap can perform scans that vary by the number of ports scanned and other information collected. The deeper the scan, the longer the scan takes. For the first test, you'll choose a quick scan. Select the arrow for the **Profile** list. Then, select **Quick Scan**.

19. Select **Scan** to start scanning.

20. View the scan's output in the Nmap Output pane in the Zenmap dashboard. When finished viewing the output, select the **Next arrow** to continue.

21. Notice that the output lists the target host's *interesting* ports. Interesting ports include open ports, which are the most susceptible to attacks, and ports in an unusual state for that system. Select the **Next arrow** to continue.

22. Now let's perform a slower but more comprehensive scan. Select the arrow for the **Profile** list. Then, select **Intense scan**.

23. Select **Scan**.

24. View the output in the Nmap Output pane. Notice that it includes details such as the host's operating system and kernel version, as well as traceroute results. Scroll to the end to view all the output. When finished viewing the output, select the **Next arrow** to continue.

25. The other panes in the dashboard highlight parts of this output. Select the **Ports/Hosts** tab to view all the target system's interesting ports.

26. In the Ports/Hosts pane, a green circle indicates an open port. A red circle indicates that the port is closed or that Zenmap cannot determine the port's state. Notice that this pane also lists the version number for any application corresponding to the port. Select the **Next arrow** to continue.

27. Select the **Topology** tab to view an interactive map of hosts on a network.

28. The Topology pane shows the network path from your computer to the target host and it includes each host encountered along the way. Select the **Next arrow** to continue.

29. A host’s color indicates its number of open ports: green means fewer than 3, yellow means 3–6, and red means more than 6. White means that Zenmap did not scan the host, so the host’s number of open ports is unknown. Select the **Next arrow** to continue.

30. Select the **Host Details** tab to view a neatly organized breakdown of details about the target host.

31. The Host Details pane includes details such as the target host’s status, addresses, hostnames, and operating system. Scroll to the end to view all the output. When finished viewing the output, select the **Next arrow** to continue.

32. Note that the icon by the “Last boot” line indicates estimated vulnerability based on the number of open ports. The treasure chest shown here means 3–4 open ports. Select the **Next arrow** to continue.

Conclusion

You’ve successfully performed network reconnaissance to gather information about a computer network. You did so by using several command-line tools and Zenmap.