

Real-World Scenario 7-2: Scanning Ports

Scenario: Your organization has some concerns about the attack surface of its servers. It is unknown what the vulnerabilities to the servers are at this point. Your task is to find out which ports are open on a web server and an FTP server. If any are unnecessary, you are to close or shield them.

Which command-line tools can you use to find out which ports are open?

Where would you go in Windows to secure the unnecessary ports?

What is an example of a deprecated and most likely unnecessary port?

Real-World Scenario 7-2 Solution

Many command-line tools are available that can be used to scan for open ports on a computer. For example, in Windows you could use the `netstat` command or download the TCPView.exe or PortQry.exe tools from Microsoft's website. A third-party tool, Nmap, is very popular and can be used on Windows and Linux platforms. A common way to use this tool is to type the following syntax:

```
nmap [nd]ss [IP address]
```

You also can scan Internet-facing network adapters with syntax such as the following:

```
nmap -PO [public IP address]
```

If nonessential ports are open, turn off their corresponding unnecessary services. For example, if the web server shows that port 21 is open but doesn't need FTP running, stop the service (and disable it) in the services console window (Run > `services.msc`), or by using the `net` and `sc` commands in the Command Prompt. You could also can configure the Windows Firewall (the best option is with Advanced Security) to block or shield the appropriate ports, and create filters and rules.

An example of a deprecated port is port 23, used by Telnet. This utility is insecure and should be avoided. Windows XP was the last Microsoft operating system to use it, and although Microsoft no longer supports XP, you can easily find that operating system in use. In addition, some routers might have the Telnet protocol installed. The point is, you never know exactly what you might find on a network, even your own. Port scanning enables you to find the open doorways.

Video Solution: Watch the video solution "7-2: Scanning Ports."

Simulation: Complete the simulations "7-2: Understanding Port Numbers" Parts A, B, and C.