

Real-World Scenario 12-2: Mapping and Scanning the Network

Scenario: Now that you have developed plans for risk assessment and vulnerability assessment, it's time to get your hands dirty and find out what's actually happening on your network. Your job is to use utilities that will help you identify the servers and other computers on the network, and scan for vulnerabilities on those computers.

Warning: The following should be performed on a test computer within a closed test network.

Access the Internet and locate two network mapping programs and two network scanning programs. Look for free utilities or utilities that have free trials. Download and install those programs, then create a basic map of the network and define some of the vulnerabilities, such as open ports on your computers.

Real-World Scenario 12-2 Solution

Remember to perform these types of tests on a closed network that you are allowed to have access to.

A couple examples of network scanning programs include Network Topology Mapper (previously LANsurveyor) and Spiceworks, but there are others as well. Use what works best for you. Two examples of port scanners are Nessus and Nmap (though these are actually full-blown vulnerability scanners). On a Windows client computer, type the command **netstat -an**. In the left column you will more than likely find that ports 135 and 139 are open (among many others). Some ports such as these need to be open so the computer can be "networkable," but other ports might need to be closed. From a remote system, scan the same computer with the Nessus and Nmap programs to find out what ports are visible from the network.

Video Solution: Watch the video solution "12-2: Mapping and Scanning the Network."