5.1.3 Scanning Tool Facts

This lesson covers the following topics:

- Scanning tools
- Network mapping tools

Scanning Tools

The following tools can be used during the scanning phase of your investigation.

Tool	Description
CurrPorts	CurrPorts lists all open UDP and TCP/IP ports on your computer. It also provides information about the process that opened the port, the user who created the process, and what time the port was created.
ping	ping uses Internet Control Message Protocol (ICMP) messaging to determine whether a remote system is live.
hping3	hping3 sends packets across a network and can also create custom packets that can analyze the host. In addition to the normal ICMP pings, hping3 supports TCP and UDP, has a traceroute mode, and can send and receive files. This tool was primarily designed for the Linux operating system, but does have cross-platform capabilities.
Colasoft	Colasoft is a packet crafting software that can modify flags and adjust other packet content.
Angry IP Scanner	Angry IP Scanner is a network scanner. It scans local and remote networks and returns an IP range via a command-line interface.
SolarWinds Port Scanner	SolarWinds Port Scanner is a command line tool that provides a list of open, closed, or filtered ports.
IP-Tools	IP-Tools has 20 scanning utilities, including SNMP Scanner, UDP Scanner, Trace, Finger, Telnet, IP-Monitor, and Trap Watcher. The program supports multitasking so that you can use all utilities at once. IP-Tools is designed to work on a Windows system.

Network Mapping Tools

The following tools can be used for mapping network resources. Many are marketed as a system inventory tool for use inside of an organization, but, as with most tools, can serve multiple purposes depending on the user's intentions.

Tool	Description
NetAuditor	NetAuditor reports, manages, and diagrams network configurations.
SolarWinds Network Topology Manager	SolarWinds Network Topology Manager provides automated network discovery and mapping.
Scany	Scany is a scanner application for iOS devices. It scans networks, websites, and ports to find open network devices. It can obtain domain and network names and includes basic networking utilities such as ping, traceroute, and whois.