4.1.3 Reconnaissance Tool Facts

There are several reconnaissance tools that you can use to gather information.

This lesson covers the following topics:

- Internet research tools
- Google hacking
- Network footprinting tools

Internet Research Tools

The following table identifies several internet research tools:

Tool	Description
Google Earth	*Google Earth* is a satellite imagery tool that provides current and historical images of most locations. Images can date back over several decades.
Google Maps	*Google Maps* is a web mapping service that provides a street view of houses, businesses, roadways, and topologies.
Webcams	*Webcams* are online streaming digital cameras that can provide video of places, people, and activity in an area.
Echosec	*Echosec* is a tool that can be used to pull information from social media postings that were made using location services. You can select a location on a map and view all posts that have occurred at that location. These results can be filtered by user, date, or keyword.
Maltego	*Maltego* is an open-source forensics tool that can be used to pull information from social media postings and find relationships between companies, people, email addresses, and other information.
Wayback Machine	The *Wayback Machine* is a nonprofit catalog of old site snapshots. It may contain information that your target thought they had removed from the internet.

Google Hacking

Despite its name, Google Hacking is legal because all of the results are pulled from public websites. By adding a few operators, you can use the Google search engine to provide filtered information about a specific topic as shown below:

Operator/Syntax	Description
info:*website*	Provides all information about a website.
link:*website*	Lists web pages that contain links to websites.
related:*website*	Displays websites similar to the one listed.
index of /*keyword*	Displays websites where directory browsing has been enabled.
intitle:*keyword*	Shows results in pages that contain the keyword in the title.
allinurl:*keywords*	Shows results in pages that contain all of the listed keywords.

Network Footprinting Tools

Although similar to reconnaissance, footprinting refers more specifically to information that is accidentally shared publicly or that is outdated and has not been properly disposed of. Website and email footprinting can provide details on information flow, operating systems, filenames, and network connections.

Depending on the level of security within an organization, it is possible to create a network map without stepping foot into the building. Just as a mailman can find a mailbox using a mailing address, a hacker can find hosts and other objects on a network using DNS network addressing. An IP address can direct you to a network access point such as an email server or a web server.

The following table lists several network footprinting tools.

Tool	Description
Whois	*Whois* is a utility used to gain information about a target network. It can gather information about ownership, IP addresses, domain name, location, server type, and the date the site was created. The syntax is **Whois *domain_name***.
Nslookup	*Nslookup* is a utility used to query DNS servers to obtain information about the host network, including DNS records and host names.
ARIN	*ARIN* is a website that will provide you with information about a network's name, range, origination dates, and server details.