5.2.2 Banner Grabbing Facts

Banner grabbing is another common method for obtaining information about a system. You can grab a banner by connecting to a host, sending a request to a port, or analyzing network traffic. The targeted system returns a snippet of information, including information about its operating system and the services that are running on it. Banner grabbing tools include the following:

Tool	Description
Telnet	*Telnet* is many hackers' tool of choice for banner grabbing. It operates on port 23. If you type **telnet *ip_address*** at a command prompt, you'll send TCP packets to the destination port 23. However, by tacking a port number on to the end of the same command, you can check for other openings. If the port you specify is open, you'll receive a banner response for that port. These banners can include some interesting information about the target system, including software type, software version, services, patches, and the last modification date.
Netcraft	*Netcraft* is an online tool that is used to obtain server and web server information.
P0f	*P0F* is a Linux tool that analyzes network traffic and returns information on operating systems. Because it is passively viewing traffic, it is a stealthy method for gathering information.
nmap	nmap is another tool for banner grabbing. nmap connects to an open TCP port and returns anything sent in a five second period. The command syntax is **nmap –sV –script=banner *ip_address***. The -sV option probes open ports to determine service/version info.