## Scan a Single Target

Executing Nmap with no command line options will perform a basic scan on the target system. A target can be specified as an IP address or host name (which Nmap will try to resolve).

Usage syntax: nmap [target]

**$ nmap 192.168.1.1**

Starting Nmap 6.47 ( http://nmap.org ) at 2015-01-13 19:23 CST

Nmap scan report for 192.168.1.1

Host is up (0.00084s latency).

Not shown: 994 closed ports

PORT STATE SERVICE

53/tcp open domain

139/tcp open netbios-ssn

445/tcp open microsoft-ds

548/tcp open afp

5009/tcp open airport-admin

10000/tcp open snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 12.32 seconds

*Single target scan*

The resulting scan shows the status of ports detected on the specified target along with other helpful information such as the protocol in use and service associated with the port. The table below describes the output fields displayed by the scan.

**PORT**Port number/protocol

**STATE**Status of the port

**SERVICE**Type of service associated with the port

A default Nmap scan will check for the 1000 most commonly used TCP/IP ports. Ports that respond to a probe are classified into one of six port states: open, closed, filtered, unfiltered, open|filtered, closed|filtered. Descriptions of these port states are described on the following page.