nmap

Network exploration tool and security/port scanner

. SYN scan) activate only when `nmap` is run with root privileges

<table>
<tr><td><code>nmap -v1|2|3 ip_or_hostname</code></td><td>Scan the top 1000 ports of a remote host with various [v]erbosity levels</td></tr>
<tr><td><code>nmap -T5 -sn 192.168.0.0/24|ip_or_hostname1,ip_or_hostname2,...</code></td><td>Run a ping sweep over an entire subnet or individual hosts very aggressively</td></tr>
<tr><td><code>nmap -p port1,port2,... ip_or_host1,ip_or_host2,...</code></td><td>Scan a specific list of ports (use `-p-` for all ports from 1 to 65535)</td></tr>
<tr><td><code>nmap -sC -sV -oA top-1000-ports ip_or_host1,ip_or_host2,...</code></td><td>Perform service and version detection of the top 1000 ports using default NSE scripts, writing results (`-oA`) to output files</td></tr>
<tr><td><code>nmap --script "default and safe" ip_or_host1,ip_or_host2,...</code></td><td>Scan target(s) carefully using `default and safe` NSE scripts</td></tr>
<tr><td><code>nmap --script "http-*" ip_or_host1,ip_or_host2,... -p 80,443</code></td><td>Scan for web servers running on standard ports 80 and 443 using all available `http-*` NSE scripts</td></tr>
</table>