

Nmap Lab

Installation:

Install the nmap rpm package that comes with the RedHat CD distro or download it from www.insecure.org/nmap or www.rpmfind.net

```
# rpm -ivh nmap-3.00-1.i386.rpm
```

Usage:

1. This option scans all reserved TCP ports on the machine target.example.com . The -v means turn on verbose mode.

```
nmap -v target.example.com
```

2. Launches a stealth SYN scan against each machine that is up out of the 255 machines on class 'C' where target.example.com resides. It also tries to determine what operating system is running on each host that is up and running. This requires root privileges because of the SYN scan and the OS detection.

```
nmap -sS -O target.example.com/24
```

3. Sends an Xmas tree scan to the first half of each of the 255 possible 8 bit subnets in the 198.116 class 'B' address space. We are testing whether the systems run sshd, DNS, pop3d, mapd, or port 4564. Note that Xmas scan doesn't work on Microsoft boxes due to their deficient TCP stack. Same goes with CISCO, IRIX, HP/UX, and BSDI boxes.

```
nmap -sX -p 22,53,110,143,4564 198.116.*.1-127
```

4. Rather than focus on a specific IP range, it is sometimes interesting to slice up the entire Internet and scan a small sample from each slice. This command finds all web servers on machines with IP addresses ending in .2.3, .2.4, or .2.5

```
nmap -v --randomize_hosts -p 80 '*.*.2.3-5'
```

5. Launch a stealth scan with OS detection on all privileged ports against 255 hosts in the network, output the results into the file /root/nmap.scan

```
nmap -sS -O 192.168.10.0/24 -oN /root/nmap.scan
```

6. Launch a stealth scan with OS detection on specified ports against 255 hosts in the network, in verbose mode.

```
nmap -sS -O -v 192.168.10.0/24 -p '1-1024,1080,3128'
```