

## EXERCISE-1 :NMAP SCAN

OUTPUT:

```
kali@kali:~$ nmap --help
File Actions Edit View Help
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-tracer: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--noninteractive: Disable runtime interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
NMAP:
--G: Enable IPv6 scanning
--A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/24 -p 80 -o 0.0.0.0
nmap -v -iR 10000 -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
kali@kali:~$ nmap -v -sn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 23:38 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds
kali@kali:~$ nmap -p 1-99 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 23:38 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.04 seconds
kali@kali:~$ nmap -F 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-24 23:39 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds
kali@kali:~$
```