- https://www.cyberciti.biz/security/n...les-tutorials/
- https://www.lijyyh.com/2012/03/nmap-...y-scanner.html (??)

1. ??????

Scan a single ip address
nmap 192.168.1.1

Scan a host name
nmap server1.cyberciti.biz

Scan a host name with more info###
nmap -v server1.cyberciti.biz

2. ??????

nmap 192.168.1.1 192.168.1.2 192.168.1.3

works with same subnet i.e. 192.168.1.0/24
nmap 192.168.1.1,2,3

You can scan a range of IP address too:
nmap 192.168.1.1-20

You can scan a range of IP address using a wildcard:
nmap 192.168.1.*

you scan an entire subnet:
nmap 192.168.1.0/24

3. ????? IP ??

nmap -iL /tmp/ip.txt

4. ?? IP ???

nmap 192.168.1.0/24 --exclude 192.168.1.5
nmap 192.168.1.0/24 --exclude 192.168.1.5,192.168.1.254

nmap -iL /tmp/scanlist.txt --excludefile /tmp/exclude.txt

5. ??????????

nmap -A 192.168.1.254
nmap -v -A 192.168.1.1
nmap -A -iL /tmp/scanlist.txt

6. ???????????

nmap -A 192.168.1.254
nmap -v -A 192.168.1.1
nmap -A -iL /tmp/scanlist.txt

7. ????(??????)

nmap -PN 192.168.1.1
nmap -PN server1.cyberciti.biz

8. ?? IPv6 ??

nmap -6 IPv6-Address-Here
nmap -6 server1.cyberciti.biz
nmap -6 2607:f0d0:1002:51::4
nmap -v A -6 2607:f0d0:1002:51::4

9. ????????????/??

nmap -sP 192.168.1.0/24

10. ??????

nmap -F 192.168.1.1

11. ?????????(Reason)

nmap --reason 192.168.1.1

12. ?????????

nmap --open 192.168.1.1

13. ?????/?????

nmap --packet-trace 192.168.1.1

14. ????????????

nmap --iflist

15. ???????

nmap -p [port] hostName
Scan port 80
nmap -p 80 192.168.1.1

Scan TCP port 80
nmap -p T:80 192.168.1.1

```
## Scan UDP port 53
nmap -p U:53 192.168.1.1

## Scan two ports ##
nmap -p 80,443 192.168.1.1

## Scan port ranges ##
nmap -p 80-200 192.168.1.1

## Combine all options ##
nmap -p U:53,111,137,T:21-25,80,139,8080 192.168.1.1
nmap -p U:53,111,137,T:21-25,80,139,8080 server1.cyberciti.biz
nmap -v -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.1.254

## Scan all ports with * wildcard ##
nmap -p "*" 192.168.1.1

## Scan top ports i.e. scan $number most common ports ##
nmap --top-ports 5 192.168.1.1
nmap --top-ports 10 192.168.1.1
```

16. ??????????????/??

```
nmap -T5 192.168.1.0/24
```

17.