????

- [???????32?nmap??]

??ping?????????IP????????IP?????????

nmap -sP 192.168.1.0/24

???????IP???????????ping ???????

nmap -sL 192.168.1.0/24

??????????????????????????????ex. -PS22,23,80,25

nmap -PS 192.168.1.234

??UDP?? ping ??????

nmap -PU 192.168.1.0/24

?? UDP Port(SIP) ????

nmap -sT -sV -sU -p 5060 123.123.123.123

??TCP SYN??

nmap -sS 192.168.1.0/24

????SYN????????TCP connect ???????????????

nmap -sT 192.168.1.0/24

?UDP??????????

nmap -sU 192.168.1.0/24

?????????(Open)?????? TCP,UDP,ICMP,...

nmap -sO 192.168.1.19

PROTOCOL	STATE	SERVICE
1	open	icmp
2	open|filtered	igmp

6 open|filtered tcp
17 open udp
41 open|filtered ipv6

????????????

nmap -O 192.168.1.19
nmap -A 192.168.1.19

??????????????????

nmap -v scanme.nmap.org

?SYN???????scanme.nmap.org?? C ??????????????????
-iL ????????

nmap -sS -O scanme.nmap.org/24
nmap -sS -O -iL ip.list

???????TCP????????????????? 198.116.(0-255).(1-127) ????

nmap -sV -p 22?53?110?143?4564 198.116.0-255.1-127

????100000?????????? Web ???????????????-P0 ???????

nmap -v -iR 100000 -P0 -p 80

???? IP ??????????

$nmap -vv -n -sP --max-rtt-timeout 500ms 117.194.238.1-100 -T4 -oG - | grep 'Up'
Host: 117.194.238.6 () Status: Up
Host: 117.194.238.18 () Status: Up
Host: 117.194.238.19 () Status: Up
Host: 117.194.238.23 () Status: Up
Host: 117.194.238.24 () Status: Up

???? port

???? -p80
FTP -p21
MySQL -p3306

$ nmap -sS -vv -n -p80 -PN --max-rtt-timeout 500ms 117.194.238.1-100 -T4 -oG - | grep 'open'
Host: 117.194.238.67 () Ports: 80/open/tcp//http///
Host: 117.194.238.95 () Ports: 80/open/tcp//http///

????

- https://www.cyberciti.biz/security/n...les-tutorials/
- http://www.linuxandubuntu.com/home/h...-nmap-commands