

	IP	nmap 192.168.1.1
	IP	nmap 192.168.1.1 192.168.2.1
		nmap 192.168.1.1-254
	CIDR	nmap 192.168.1.0/24
		nmap scanme.nmap.org
-iL		nmap -iL targets.txt
-iR		nmap -iR 100
--exclude		nmap --exclude 192.168.1.1
--excludefile		nmap --excludefile notargets.txt

-p	x	nmap -p 21 192.168.1.1
-p		nmap -p 21-100 192.168.1.1
-p	TCP UDP	nmap -p U:53, T:21-25,80 192.168.1.1
-p-		nmap -p- 192.168.1.1
-F	(TOP100)	nmap -F 192.168.1.1
--top-ports number	number	nmap --top-ports 2000 192.168.1.1
-r	(nmap	nmap -p- -r 192.168.1.1
--port-ratio <ratio>	(0~1)	nmap -port-ratio 0.9 192.168.1.1

-sL	List scan()	nmap -sL 192.168.1-3
-sn	Ping scan()	-sP nmap -sn 192.168.1.1/24
-Pn	Port scan()	nmap -Pn 192.168.1-5
-PS [portlist]	x TCP SYN 80	nmap -PS22-25,80 192.168.1.1-5
-PA [portlist]	x TCP ACK 80	nmap -PA22-25,80 192.168.1.1-5



By **fkbug**
cheatography.com/fkbug/

Not published yet.
 Last updated 18th June, 2019.
 Page 1 of 5.

Sponsored by **ApolloPad.com**
 Everyone has a novel in them. Finish Yours!
<https://apollopad.com>

(cont)

-PU [portlist]	x	UDP	40125	nmap -PU53 192.168.1.1-5
-PY [portlist]	x	SCTP		nmap -PY22-25,80 192.168.1.1-5
-PE		ICMP echo		nmap -PE 192.168.1.1
-PP		ICMP timestamp		nmap -PP 192.168.1.1
-PM		ICMP netmask		nmap -PM 192.168.1.1
-PO		IP		nmap -PO 192.168.1.1
-PR		ARP		nmap -PR 192.168.1.1/24
-n		dns	(dns nmap dns)	nmap -n 192.168.1.1
-R		dns		nmap -R 192.168.1.1
--system-dns		dns	nmap	nmap --system-dns 192.168.1.1
--dns-servers <serv1[,serv2],...>		dns		nmap --dns-servers dnsIP1 dnsIP2 192.168.1.1
--traceroute		-sT	-sl)	nmap --traceroute 192.168.1.1
--resolve-all		()	nmap --resolve-all baidu.com

-sS		TCP SYN	()	nmap -sS 192.168.1.1
-sT		TCP	(root)	nmap -sT 192.168.1.1
-sA		TCP ACK		nmap -sA 192.168.1.1
-sW		TCP		nmap -sW 192.168.1.1
-sM		TCP Maimon		nmap -sM 192.168.1.1
-sU		UDP		nmap -sU 192.168.1.1
-sN		TCP Null		nmap -sN 192.168.1.1
-sF		TCP FIN		nmap -sF 192.168.1.1
-sX		TCP Xmas		nmap -sX 192.168.1.1
--scanflags <flags>		TCP		nmap --scanflags URGFIN 192.168.1.1



By **fkbug**
[cheatography.com/fkbug/](https://www.cheatography.com/fkbug/)

Not published yet.
 Last updated 18th June, 2019.
 Page 2 of 5.

Sponsored by **ApolloPad.com**
 Everyone has a novel in them. Finish
 Yours!
<https://apollopad.com>

(cont)

-sl	Idle (IP Zombie)	nmap -Pn -p- -sl Zombie.com target.com
-sY	SCTP INIT (SCTP TCP INIT	nmap -sY 192.168.1.1
-sZ	SCTP COOKIE_ECHO	nmap -sZ 192.168.1.1
-sO	IP (IP TCP ICMP IGMP	nmap -sO 192.168.1.1
-b <FTP relay host>	FTP (FTP	nmap -Pn -b ftp.microsfot.com google.com

-sV		nmap -sV 192.168.1.1
--version-intensity <level>	(0-9), 7	nmap -sV --version-intensity 8 192.168.1.1
--version-light	(intensity=2)	nmap -sV --version-light 192.168.1.1
--version-all	(intensity=9)	nmap -sV --version-all 192.168.1.1
--version-trace		nmap -sV --version-trace 192.168.1.1

-O	TCP/IP	nmap -O 192.168.1.1
-O --osscan-limit	TCP	nmap -O --osscan-limit 192.168.1.1
-O --osscan-guess	nmap	nmap -O --osscan-guess 192.168.1.1
-O --max-os-tries	OS	nmap -O --max-os-tries 1
-A		nmap -A 192.168.1.1



By **fkbug**
cheatography.com/fkbug/

Not published yet.
 Last updated 18th June, 2019.
 Page 3 of 5.

Sponsored by **ApolloPad.com**
 Everyone has a novel in them. Finish Yours!
<https://apollopad.com>

-T0							nmap -T0 192.168.1.1	
-T1							nmap -T1 192.168.1.1	
-T2							nmap -T2 192.168.1.1	
-T3							nmap -T3 192.168.1.1	
-T4							nmap -T4 192.168.1.1	
-T5							nmap -T5 192.168.1.1	
--host-timeout <time>			time				nmap --host-timeout 30m 192.168.1.1	
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>							nmap --min-rtt-timeout 2s 192.168.1.1	
--scan-delay/--max-scan-delay <time>							nmap --scan-delay 3min 192.168.1.1	
--max-retries <tries>							nmap --max-retries 3 192.168.1.1	
--min-rate <number>				number			nmap --min-rate 100 192.168.1.1	
--max-rate <number>				number			nmap --max-rate 100 192.168.1.1	
-T	nmap	IDS	T4 nmap	T3	T2	T3	T3	IDS

-oN							nmap 192.168.1.1 -oN normal.file
-oX	XML						nmap 192.168.1.1 -oX xml.file
-oG							nmap 192.168.1.1 -oG grep.file
-oA							nmap 192.168.1.1 -oA results
-oG -		-oN -, -oX -					nmap 192.168.1.1 -oG -
--append							nmap 192.168.1.1 -oN file.file --append-output
-v		(-vv)					nmap -v 192.168.1.1
-d		(-dd)					nmap -d 192.168.1.1
--reason		(-vv)					nmap --reason 192.168.1.1
--open							nmap --open 192.168.1.1
--packet-trace							nmap -T4 --packet-trace 192.168.1.1



By [fkbug](https://cheatography.com/fkbug/)
cheatography.com/fkbug/

Not published yet.
 Last updated 18th June, 2019.
 Page 4 of 5.

Sponsored by [ApolloPad.com](https://apollopad.com)
 Everyone has a novel in them. Finish Yours!
<https://apollopad.com>

(cont)

```
--iflist          nmap --iflist
--resume         nmap --resume result.file
```

```
web              nmap -p80 -sV -oG - --open 192.168.1.1/24 | grep open
                 nmap -iR 10 -n -oX out.xml | grep "Nmap" | cut -d " " -f5 >> live-host.txt
                 nmap -iR 10 -n -oX out2.xml | grep "Nmap" | cut -d " " -f5 >> live-host.txt
nmap :          ndiff scan.xml scan2.xml
xml  html      xsltproc nmap.xml -o nmap.html
                 grep "open" results.nmap | sed -r 's / + // g' | sort | uniq -c | sort -rn | less
grep sed sort less  bash          windows
```

```
-6              IPv6          nmap -6 192.168.1.1
-A              traceroute    nmap -A 192.168.1.1
--data-dir <dirname>      nmap          nmap --data-dir /root/ 192.168.1.1
--send-eth/--send-ip      IP          nmap --send-eth 192.168.1.1
--privileged
--unprivileged          nmap --privileged 192.168.1.1
--unprivileged          nmap --unprivileged 192.168.1.1
-V              nmap          nmap -V
-h/--help        nmap          nmap -h
```

/IDS

```
-f
```



By **fkbug**
cheatography.com/fkbug/

Not published yet.
 Last updated 18th June, 2019.
 Page 5 of 5.

Sponsored by **ApolloPad.com**
 Everyone has a novel in them. Finish
 Yours!
<https://apollopad.com>