

Nmap - What is the switch for a ACK Scan?

Nmap - What is the switch for a FIN Scan?

Nmap - What is the switch for a IDLE Scan?

Nmap - What is the switch for a DNS/list Scan?

Nmap - What is the switch for a NULL scan?

Nmap - What is the switch for a Protocol Scan?

Nmap - What is the switch for a RPC scan?

Nmap - What is the switch for a RPC scan?

Nmap - What is the switch for a SYN Scan?

Nmap - What is the switch for a TCP connect(Full open) Scan?

-sF

-sA

-sL

-sI

-sO

-sN

-sR

-sP

-sT

-sS

Nmap - What is the switch for a Windows Scan?

Nmap - What is the switch for a XMAS scan?

Nmap - What is the switch for a ICMP ping?

Nmap - What is the switch for a NO Ping?

Nmap - What is the switch for a SYN Ping?

Nmap - What is the switch for a TCP Ping?

Nmap - What is the switch for a XML Output?

Nmap - What is the switch for a XML Output?

Nmap - What is the switches for the speed?

HPing3 – What is the switch for setting ICMP Mode?

-sX

-sW

-Po

-PI

-PT

-PS

-oX

-oN

Hping3 -1 <IP>

-T0 -T1 -T2 -T3 -T4

HPing3 – What is the switch for setting UDP mode?

HPing3 – What is the switch for setting Scan mode?

HPing3 – What is the switch for setting listening Mode?

HPing3 – What is the switch for flooding

HPing3 – What is the switch for collecting sequence numbers?

HPing3 – What are the flags?

Hping3 -8 <Set ports to scan range (1-20)>

Hping3 -2 <IP>

Hping3 --flood

Hping3 -9 HTTP <-I> eth0

-F Fin
-S Syn
-R RST
-P PSH
-A ACK
-U URG
-X XMAS

Hping3 -Q