Nmap TCP scan

nmap -sT Ip address –>basic tcp scan, it will scan 1000 ports by default

nmap -sT –sV Ip address –> version scan included

nmap -sT -sV -O ip address → version operating system included

nmap -sT -p 80 ip address → for specific port

nmap –sT –p 80, 21 ip address → for multiple ports

nmap –sT –p 0-100 ip address → for range of ports

nmap –sT –sV –O –p 0-65535 ip address → entire scan

Nmap ACK scan

nmap -sA Ip address –>basic tcp scan, it will scan 1000 ports by default

nmap -sA –sV Ip address –> version scan included

nmap -sA -sV -O ip address → version operating system included

nmap -sA -p 80 ip address → for specific port

nmap –sA –p 80, 21 ip address → for multiple ports

nmap –sA –p 0-100 ip address → for range of ports

nmap –sA –sV –O –p 0-65535 ip address → entire scan

Nmap FIN scan

nmap -sF Ip address –>basic tcp scan, it will scan 1000 ports by default

nmap -sF –sV Ip address –> version scan included

nmap -sF -sV -O ip address → version operating system included

nmap -sF -p 80 ip address → for specific port

nmap –sF –p 80, 21 ip address → for multiple ports

nmap –sF –p 0-100 ip address → for range of ports

nmap –sF –sV –O –p 0-65535 ip address → entire scan

Nmap xmas scan

nmap -sX Ip address –>basic tcp scan, it will scan 1000 ports by default

nmap -sX –sV Ip address –> version scan included

nmap -sX -sV -O ip address → version operating system included

nmap -sX -p 80 ip address → for specific port

nmap –sX –p 80, 21 ip address → for multiple ports

nmap –sX –p 0-100 ip address → for range of ports

nmap –sX –sV –O –p 0-65535 ip address → entire scan

Nmap udp scan

nmap -sU Ip address –>basic tcp scan, it will scan 1000 ports by default

nmap -sU -sV Ip address –> version scan included

nmap -sU -sV -O ip address → version operating system included

nmap -sU -p 53 ip address → for specific port

nmap -sU -p 53, 110 ip address → for multiple ports

nmap -sU -p 0-100 ip address → for range of ports

nmap -sU -sV -O -p 0-65535 ip address → entire scan

nmap fast scan

by default it will scan for scandard ports – 0-1023, so no need to mention port information

nmap -F -sV -O Ip addess

nmap Aggressive scan

by default this will identify service operating system all required information – indepth scan

nmap –A Ip address

nmap domain scanning

nmap domain name

example: nmap vulnweb.com

nmap multiple ip scanning

nmap 192.168.0.1 192.168.0.2

nmap 192.168.0.1-5

nmap output formats

nmap outputs can be saved to a file using below mentioned operators

-oN	nmap 192.168.1.1 -oN normal.file	Normal output to the file normal.file
-oX	nmap 192.168.1.1 -oX xml.file	XML output to the file xml.file
-oG	nmap 192.168.1.1 -oG grep.file	Grepable output to the file grep.file