Nmap CheatSheet

Azlan

Nmap basic command’s

nmap –iR (num of targets with a space) = used to scan targets randomly

nmap (target ip) –exclude (document in which ip is stored) = to exclude a target ip from nmap

nmap -6 (target ip) – to target an (ipv6) ip

command’s used with nmap at the beginning

nmap –O (ip address) = use for os detection

nmap -–osscan-guess = attempt to guess an unknown os

nmap –sV = for service version detection

nmap –version-trace = perform an RPC scan

nmap – sR = troubleshooting version scans

Commands to save actions

# In the last of the command type –

-oN (filename you want).txt [remember the file will be saved in the directory/folder you are]

-oX (filename you want).xml [remember the file will be saved in the directory/folder you are]