Cheat sheet

N-Map

VIEW NOW

SEKURENET

NMAP (NETWORK MAPPER) IS A POWERFUL AND WIDELY USED TOOL FOR NETWORK DISCOVERY AND SECURITY AUDITING.

BASIC USAGE

- SCAN A SINGLE HOST: NMAP <IP ADDRESS>
- SCAN A RANGE OF HOSTS: NMAP <START IP>-<END IP>
- SCAN FOR SPECIFIC SERVICES: NMAP -SV <IP ADDRESS>
- DISCOVER HOSTS ON A NETWORK: NMAP -SN <NETWORK ADDRESS>
- PERFORM A STEALTH SCAN: NMAP -SS <IP ADDRESS>

COMMON OPTIONS

- -P <PORT RANGE>: SPECIFY PORTS TO SCAN (E.G., -P 22,80,443)
- -O: ATTEMPT TO DETERMINE THE OPERATING SYSTEM
- -A: ENABLE AGGRESSIVE OS DETECTION
- -T <TIMING TEMPLATE>: SET TIMING TEMPLATE FOR SPEED (E.G., -T AGGRESSIVE)
- -ON <OUTPUT FILE>: SAVE SCAN RESULTS TO A NORMAL OUTPUT FILE

EXAMPLE COMMANDS

- SCAN A HOST FOR OPEN PORTS AND SERVICES: NMAP -SV 192.168.1.100
- DISCOVER HOSTS ON THE 192.168.1.0 NETWORK: NMAP -SN 192.168.1.0/24
- PERFORM AN AGGRESSIVE OS DETECTION SCAN: NMAP -A 192.168.1.100

KEY OUTPUTS

- HOST STATUS: UP, DOWN
- IP ADDRESS: HOST'S IP ADDRESS
- MAC ADDRESS: HOST'S HARDWARE ADDRESS
- OPEN PORTS: PORT NUMBER, SERVICE/APPLICATION
- OPERATING SYSTEM: DETECTED OPERATING SYSTEM (WITH CONFIDENCE LEVEL)