|  |
| --- |
| R\_Dex Cyber Solution |
| “NMAP CHEAT SHEET” |
| PRESENTING BY RAHUL |

|  |
| --- |
| Rahul majhi  4/27/2023 |

**#NMAP BASIC SCANING**

1. nmap -sV [host] //version Detection default Scan
2. nmap –sS [host] //‘SYN’ Stealth Scan
3. nmap –sU [host] // ‘UDP’ Scan
4. nmap –sT [host] // ‘TCP’ Null Scan
5. nmap –sF [host] // ‘TCP’ Fin Scan

**#HOST DISCOVERY**

1. nmap –sL [host/Network] //List Scan –Discover Targates by Querying DNS Or The Targates in A Network
2. nmap –sn [host/Network] // ping Scan Determine If host are Alive
3. nmap –pri [host/Network] // Skip Host Discovery

**#nmap port SCaning**

1. nmap –sC [host] // Script Scan Execute Deafult Nmap Scripts
2. nmap –p [ports] [host] // Scan Specific Ports
3. nmap –F [host] // Fast Scan For The Most Commonly Used Ports

**#nmap advertising scaning**

1. nmap –oA {Filename} [host] // output Scan All Formats
2. nmap –O [host] probe.. O/S Operating System Fingerprinting
3. nmap [host] –traceroute // Trace Host Hops

**#nmap – version .Detection**

1. nmap –sV [host] // Show Versions Of Services And OS
2. nmap –A [host] //Advance Aggressive OS & Servicxe Version On Script Scaning

**#nmap timing option’s**

1. nmap –T [0-5] [host] // Timing For Scan

**#nmap –firewall/(ids) –evasion**

1. nmap --spoof-mac [address] // change Source MAC Address
2. nmap –D RND:10 [host] // “DECOYN SCAN” \_Appears To Scan From Multiple Host
3. nmap –f Fragmented Packets – Fragment packets.
4. nmap –Pn [host] // Skip Host Discovery
5. nmap –data-length [length] // Append random data To A Packet

**#using nmap –also we can run a particular inbuilt script to exploit particular ‘vulnerability’**

1. nmap –script=[name] [host] // Execute A Custom Script