

WINDOWS COMMANDS FOR SOC

FOLLOW :- MAHESH
GIRHE

System Information



- systeminfo – Displays system details like OS version, patches, and uptime.



- hostname – Shows the computer's hostname.



- tasklist – Lists running processes.

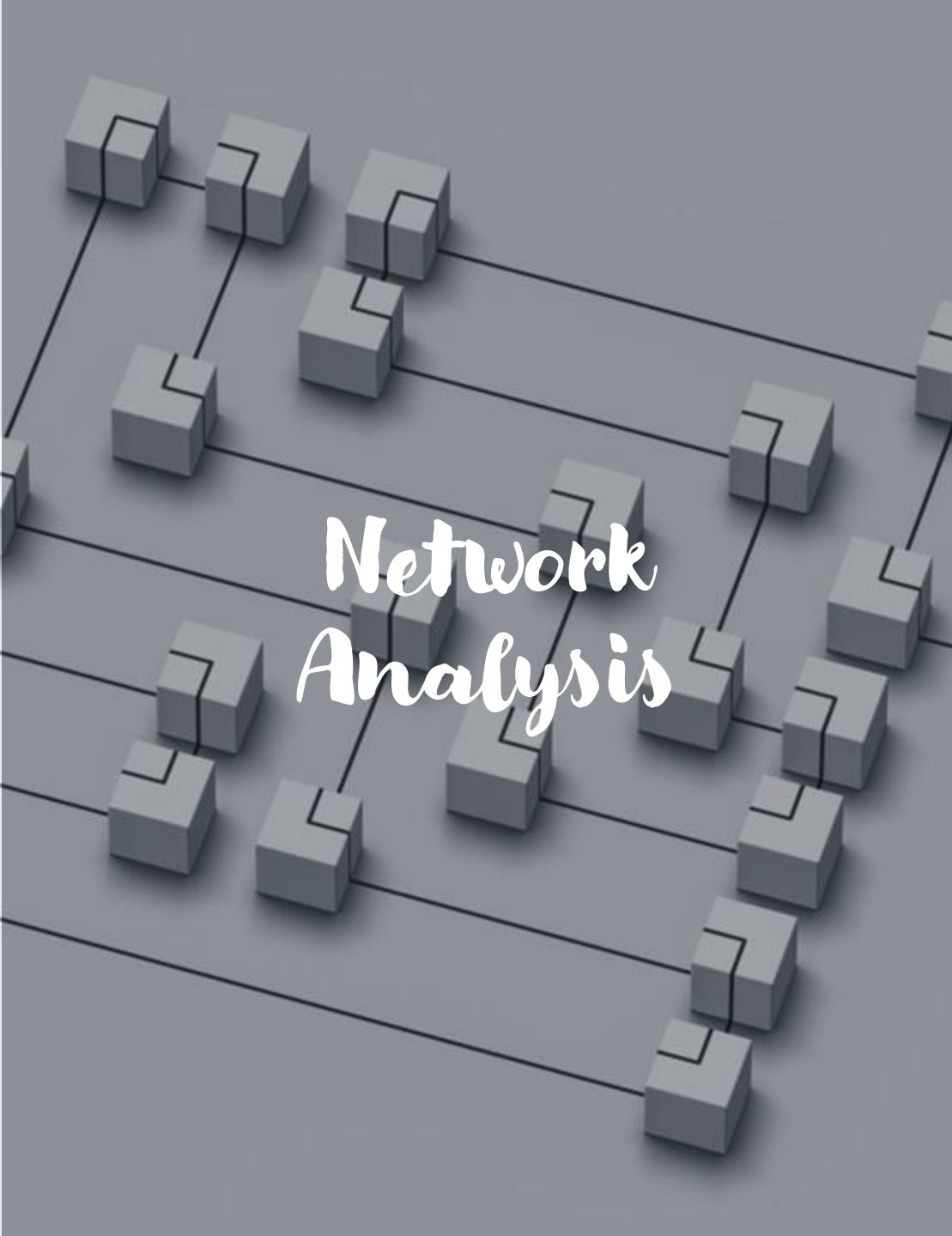


- taskkill /PID <ProcessID> /F – Terminates a process by PID.



User Management

- `net user` - Lists all users on the system.
- `net user <username>` - Displays details of a specific user.
- `whoami` - Shows the current logged-in user.



Network Analysis

- • ipconfig /all - Displays full network configuration.
- • ping <IP/Hostname> - Tests connectivity to a host.
- • tracert <IP/Hostname> - Traces the path to a host.
- • netstat -ano - Shows active connections, ports, and processes.
- • nslookup <domain> - Resolves domain to IP.

File and Directory Investigation



- `dir /s /p` – Lists files in a directory (recursive).



- `attrib -h -s <filename>` – Removes hidden and system attributes from a file.



- `fc file1.txt file2.txt` – Compares two files.



- `findstr <string> <filename>` – Searches for specific strings in a file.

Event Log Analysis



- `wevtutil qe Security /f:text /c:<number>` - Queries the Security event log.



- `Get-EventLog -LogName Security` (PowerShell) - Retrieves Windows Security events.

Important Event IDs:

- 4624: Successful login.



- 4625: Failed login.



- 4688: Process creation.



- 4697: Service installation.





Services and Scheduled Tasks

- `sc query` - Lists all services on the system.
- `schtasks /query /fo LIST /v` - Lists scheduled tasks with verbose output.



Registry Investigation

- reg query
HKLM\Software\Microsoft\Windows\CurrentVersion\Run - Lists startup programs.
- autorunc (Sysinternals) - Checks all auto-start programs.



Permissions and Ownership

- `icacs <file>` - Displays or changes file permissions.
- `takeown /f <file>` - Takes ownership of a file or folder.

Malware Analysis and Cleanup

- • wmic process list - Lists detailed process information.
- • sfc /scannow - Scans and repairs corrupted system files.
- • mrt - Runs the Malicious Software Removal Tool.

Advanced Tools (Sysinternals)



- autoruns – Identifies startup items and persistence mechanisms.



- process explorer – Monitors live processes and their properties.



- tcpview – Tracks real-time TCP/UDP connections.



- procdump – Captures memory dump of a process.



- This cheatsheet covers critical commands for system monitoring, file analysis, network investigation, and threat detection.

Thank You !



Follow :- MAHESH SARJERAO GIRHE



LIKE AND SHARE THIS POST TO GET MORE INTERESTING TIPS .