Cybersecurity & Networking Tools Cheatsheet

A comprehensive cheat sheet covering essential cybersecurity and networking security tools, their functions, and common use cases.

Network Security Monitoring

Wireshark

Description:	A network protocol analyzer that captures and analyzes network traffic in real-time.
Key Features:	Packet capture, protocol dissection, VoIP analysis, live data capture.
Common Uses:	Troubleshooting network issues, analyzing network security, examining protocol implementations.
Capture Filter:	`tcp port 80` (HTTP traffic), `ip.addr == 192.168.1.1` (Specific IP address)
Display Filter:	`http.request.method == "POST"` (POST requests), `tcp.analysis.retransmission` (TCP Retransmissions)
Command Line:	`tshark -i eth0 -w capture.pcap` (Capture to file), `tshark -r capture.pcap` (Read from file)

tcpdump

Description:	A command-line packet analyzer that captures network traffic.
Key Features:	Packet capture, filtering, analysis, and saving to file.
Common Uses:	Network troubleshooting, security analysis, and packet inspection.
Basic Syntax:	`tcpdump -i eth0` (Capture on interface eth0)
Filters:	`tcpdump port 80` (HTTP traffic), `tcpdump src 192.168.1.1` (Source IP address)
Saving Capture:	`tcpdump -i eth0 -w capture.pcap` (Save to capture.pcap file)

Vulnerability Scanning and Penetration Testing

Nmap

Description:	A network scanner used to discover hosts and services on a computer network by sending packets and analyzing the responses.
Key Features:	Host discovery, port scanning, service version detection, OS detection.
Common Uses:	Network inventory, security auditing, vulnerability detection.
Basic Scan:	`nmap target_ip` (Scan target IP address)
Port Scan:	`nmap -p 1-100 target_ip` (Scan ports 1-100)
OS Detection:	`nmap -O target_ip` (Detect operating system)
Service Version Detection:	`nmap -sV target_ip` (Detect service versions)

Nessus

Description:	A comprehensive vulnerability scanner that identifies vulnerabilities, misconfigurations, and malware.
Key Features:	Vulnerability scanning, compliance auditing, configuration auditing, malware detection.
Common Uses:	Identifying and remediating vulnerabilities, ensuring compliance with security policies.
Scan Types:	Basic Network Scan, Web Application Scan, Compliance Checks
Reporting:	Generates detailed reports of vulnerabilities and their severity.

Metasploit

Description:	A penetration testing framework that provides tools for developing and executing exploit code against a remote target.
Key Features:	Exploit development, payload generation, vulnerability exploitation, post-exploitation.
Common Uses:	Penetration testing, vulnerability validation, security research.
Basic Usage:	`msfconsole` (Launch Metasploit console)
Module Search:	`search ms08_067` (Search for exploit modules)
Exploit Usage:	`use exploit/windows/smb/ms08_067_netapi` (Use specific exploit)

SIEM and Log Analysis

Splunk

Description:	A platform for collecting, indexing, searching, and analyzing machine-generated data.
Key Features:	Log aggregation, indexing, searching, alerting, reporting, dashboarding.
Common Uses:	Security monitoring, threat detection, compliance reporting, operational intelligence.
Basic Search:	`index=main sourcetype=access_combined` (Search access logs)
Alerting:	Create alerts based on specific search criteria.
Dashboards:	Visualize data using dashboards and charts.

ELK Stack (Elasticsearch, Logstash, Kibana)

Description:	A suite of open-source tools for log management and analysis.
Key Features:	Log aggregation (Logstash), indexing and searching (Elasticsearch), visualization (Kibana).
Common Uses:	Security information and event management (SIEM), log analysis, application monitoring.
Elasticsearch Query:	`GET /_search` (Basic search)
Kibana Visualization:	Create visualizations and dashboards to analyze data.
Logstash Configuration:	Configure Logstash to ingest and process logs from various sources.

Incident Response Tools

Autopsy

Description:	A digital forensics platform used to investigate and analyze computer systems and storage devices.
Key Features:	Disk imaging, file system analysis, keyword searching, timeline analysis.
Common Uses:	Incident response, forensic investigation, data recovery.
Data Sources:	Supports various data sources like disk images, logical files, and unallocated space.
Modules:	Extensible through modules for additional functionality.

TheHive

Description:	A scalable, open-source and free Security Incident Response Platform (SIRP), tightly integrated with MISP.
Key Features:	Case management, collaboration, task management, alerting.
Common Uses:	Incident response, security operations, threat intelligence management.
Integration:	Integrates with various security tools for automated incident handling.
Collaboration:	Enables collaboration among incident response teams.