CHEAT SHEETS HERO

Cybersecurity & Networking Cheatsheet

A comprehensive cheat sheet covering essential Cybersecurity and Networking concepts, tools, and best practices.

Networking Fundamentals

OSI Model Layers

Layer 7: Application	Provides network services to applications (e.g., HTTP, SMTP, FTP).
Layer 6: Presentation	Handles data representation, encryption, and decryption.
Layer 5: Session	Manages connections between applications.
Layer 4: Transport	Provides reliable data transfer (TCP) or best-effort delivery (UDP).
Layer 3: Network	Handles routing of data packets (IP).
Layer 2: Data Link	Provides error-free transmission between adjacent nodes (Ethernet).
Layer 1: Physical	Defines physical characteristics of the network (cables, signals).

Common Network Protocols

TCP	Transmission Control Protocol: Connection-oriented, reliable data transfer.
UDP	User Datagram Protocol: Connectionless, fast, but unreliable data transfer.
IP	Internet Protocol: Handles addressing and routing of data packets.
HTTP	Hypertext Transfer Protocol: Used for web browsing.
HTTPS	HTTP Secure: Secure web browsing with encryption (SSL/TLS).
DNS	Domain Name System: Translates domain names to IP addresses.
DHCP	Dynamic Host Configuration Protocol: Automatically assigns IP addresses to devices.

Networking Devices

Router	Forwards data packets between networks.
Switch	Connects devices within a network.
Firewall	Controls network traffic based on security rules.
Load Balancer	Distributes network traffic across multiple servers.

Cybersecurity Essentials

Common Security Threats

Malware: Malicious software (viruses, worms, trojans).
Phishing: Deceptive attempts to obtain sensitive information.
Ransomware: Encrypts data and demands ransom for decryption key.
DDoS: Distributed Denial of Service, overwhelming a service with traffic.

SQL Injection: Exploiting vulnerabilities in database queries.
Cross-Site Scripting (XSS): Injecting malicious scripts into websites.
Man-in-the-Middle (MitM): Intercepting communication between two parties.
Zero-Day Exploit: Exploiting unknown vulnerabilities.

Security Principles

Principle of Least Privilege	Grant users only the minimum necessary access rights.
Defense in Depth	Implement multiple layers of security controls.
Zero Trust	Trust no one, verify everything.
Separation of Duties	Divide critical tasks among multiple individuals.

Authentication Methods

Password	A secret word or phrase used for verification.
Multi-Factor Authentication (MFA)	Requires multiple verification factors (e.g., password + code from phone).
Biometrics	Uses unique biological traits for verification (e.g., fingerprint, facial recognition).
Certificates	Digital documents used to verify identity.

Security Tools & Techniques

Network Security Tools

Wireshark	Network protocol analyzer for capturing and analyzing network traffic.
Nmap	Network scanner for discovering hosts and services on a network.
Snort	Intrusion detection and prevention system (IDS/IPS).
Metasploit	Penetration testing framework for exploiting vulnerabilities.

Cryptography Basics

Symmetric Encryption	Uses the same key for encryption and decryption (e.g., AES).
Asymmetric Encryption	Uses a public key for encryption and a private key for decryption (e.g., RSA).
Hashing	Creates a fixed-size string (hash) from an input (e.g., SHA-256).
Digital Signatures	Uses asymmetric encryption to verify the authenticity and integrity of data.

Vulnerability Scanning

Vulnerability scanning involves identifying and assessing security weaknesses in systems and applications. Tools like Nessus, OpenVAS, and Qualys can automate the process of scanning for known vulnerabilities. Regular vulnerability scans help organizations proactively address security risks and prevent exploitation.

Examples of vulnerability scanning include:

- **Network scanning:** Identifying open ports and services.
- **Web application scanning:** Detecting common web vulnerabilities like SQL injection and XSS.
- **Host-based scanning:** Examining operating systems and applications for missing patches and misconfigurations.

Incident Response & Forensics

Incident Response Lifecycle

The Incident Response Lifecycle typically includes these phases:

1. **Preparation:** Establishing policies, procedures, and tools for incident response.
2. **Identification:** Detecting and analyzing security incidents.
3. **Containment:** Limiting the impact of the incident.
4. **Eradication:** Removing the cause of the incident.
5. **Recovery:** Restoring systems and data to normal operation.
6. **Lessons Learned:** Reviewing the incident and improving security measures.

Digital Forensics Principles

Chain of Custody	Maintaining a documented record of the handling of evidence.
Data Preservation	Protecting the integrity and availability of digital evidence.
Forensic Imaging	Creating a bit-by-bit copy of a storage device.
Analysis	Examining digital evidence to identify relevant information.

Log Analysis

Log analysis involves reviewing system and application logs to identify security incidents, performance issues, and other anomalies. Tools like Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), and Graylog can be used to collect, analyze, and visualize log data.

Common log sources include:

- **System logs:** Operating system events and errors.
- **Application logs:** Application-specific events and errors.
- **Security logs:** Authentication attempts, firewall events, and intrusion detection alerts.
- **Network logs:** Network traffic and connectivity information.