Cybersecurity Essentials Cheatsheet

A quick reference guide covering fundamental cybersecurity concepts, tools, and techniques for both beginners and professionals. This cheat sheet provides a concise overview of key topics to help you navigate the complex world of cybersecurity.

Core Concepts

Security Principles

Confidentiality	Ensuring that information is accessible only to authorized individuals or systems.
Integrity	Maintaining the accuracy and completeness of information; preventing unauthorized modification or deletion.
Availability	Ensuring that authorized users have timely and reliable access to information and resources.
Authentication	Verifying the identity of a user, device, or system attempting to access resources.
Non-Repudiation	Ensuring that parties cannot deny their actions or commitments related to data.
Defense in Depth	Implementing multiple layers of security controls to protect assets.

Common Threats

Malware	Malicious software (viruses, worms, Trojans) designed to harm or disrupt systems.
Phishing	Deceptive attempts to obtain sensitive information (usernames, passwords, credit card details) by disguising as a trustworthy entity.
Ransomware	Malware that encrypts a victim's files, demanding a ransom payment for the decryption key.
SQL Injection	An attack that exploits vulnerabilities in database queries to gain unauthorized access or modify data.
Cross-Site Scripting (XSS)	An attack where malicious scripts are injected into trusted websites, targeting users.
Denial of Service (DoS)	Overwhelming a system or network with traffic, making it unavailable to legitimate users.

Vulnerability Types

Buffer Overflow	Writing data beyond the allocated buffer, potentially overwriting adjacent memory and causing crashes or enabling code execution.
Integer Overflow	Performing an arithmetic operation that exceeds the maximum value representable by an integer type, leading to unexpected results and potentially exploitable conditions.
Format String Vulnerability	Exploiting improper use of format string functions (e.g., `printf` in C) to read from or write to arbitrary memory locations.
Race Condition	A situation where the behavior of a program depends on the unpredictable order in which multiple processes or threads access shared resources.
Use-After-Free	Accessing memory that has been freed, leading to unpredictable behavior, crashes, or potential security vulnerabilities.
Heap Overflow	Similar to buffer overflow, but occurring in the heap (dynamic memory allocation) region.

Cryptography

Symmetric Encryption

AES (Advanced Encryption Standard)	A widely used symmetric block cipher, known for its security and performance. Commonly used with key sizes of 128, 192, or 256 bits.
DES (Data Encryption Standard)	An older symmetric block cipher, now considered insecure due to its small key size (56 bits). Superseded by AES.
3DES (Triple DES)	A more secure variant of DES, applying the DES algorithm three times with multiple keys. However, it is slower than AES.
Blowfish/Twofish	Another symmetric block cipher algorithm.

Asymmetric Encryption

RSA (Rivest-Shamir-Adleman)	A widely used asymmetric algorithm for encryption and digital signatures. Relies on the difficulty of factoring large numbers.
ECC (Elliptic Curve Cryptography)	An asymmetric algorithm offering strong security with smaller key sizes compared to RSA. Commonly used in mobile devices and embedded systems.
Diffie-Hellman	A key exchange protocol that allows two parties to establish a shared secret key over an insecure channel.
DSA (Digital Signature Algorithm)	A standard for creating digital signatures.

Hashing Algorithms

SHA-256 (Secure Hash Algorithm 256-bit)	A cryptographic hash function that produces a 256-bit hash value. Widely used for data integrity and security applications.
SHA-3 (Secure Hash Algorithm 3)	The latest version of SHA algorithms.
MD5 (Message Digest Algorithm 5)	An older hash function that produces a 128-bit hash value. Considered insecure for many applications due to collision vulnerabilities.
bcrypt	A popular password-hashing function that incorporates salting to protect against rainbow table attacks.

Network Security

Common Ports

21	FTP (File Transfer Protocol)
22	SSH (Secure Shell)
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
53	DNS (Domain Name System)
80	HTTP (Hypertext Transfer Protocol)
443	HTTPS (HTTP Secure)
3389	RDP (Remote Desktop Protocol)

Firewalls

Firewalls control network traffic based on predefined rules.

Types:

- **Network Firewalls:** Protect entire networks.
- **Host-Based Firewalls:** Protect individual devices.

Functionality:

- **Packet Filtering:** Examines packets based on source/destination IP, port, and protocol.
- **Stateful Inspection:** Tracks the state of network connections to make more informed decisions.
- **Proxy Firewalls:** Act as intermediaries between clients and servers, providing additional security.

Intrusion Detection/Prevention Systems (IDS/IPS)

IDS/IPS monitor network traffic for malicious activity.

Types:

- **Network-Based:** Analyzes traffic on the network.
- **Host-Based:** Analyzes activity on individual systems.

Functionality:

- **Signature-Based:** Matches traffic against known attack patterns.
- **Anomaly-Based:** Detects deviations from normal behavior.
- **Prevention:** IPS can automatically block or mitigate detected threats, while IDS only alerts administrators.

Security Tools

Vulnerability Scanners

Tools that automatically scan systems and networks for known vulnerabilities.

Examples:

- Nessus
- OpenVAS
- Qualys

Key Features:

- Vulnerability Identification
- Reporting
- Compliance Checks

Penetration Testing Tools

Tools used to simulate real-world attacks to identify security weaknesses.

Examples:

- Metasploit
- Burp Suite
- Nmap

Key Features:

- Exploitation
- Reconnaissance
- Reporting

SIEM (Security Information and Event Management)

Tools that aggregate and analyze security logs and events from various sources.

Examples:

- Splunk
- QRadar
- ELK Stack (Elasticsearch, Logstash, Kibana)

Key Features:

- Log Management
- Threat Detection
- Incident Response