Cybersecurity Protocols Cheatsheet

A quick reference guide to essential cybersecurity protocols, their functions, and configurations, designed to help security professionals and developers implement robust security measures.

Encryption Protocols

SSL/TLS

Purpose:	Secures communication over networks; encrypts data between client and server.
Function:	Uses certificates to authenticate the server; negotiates encryption algorithms and keys.
Configuration:	Configured on web servers; requires a valid SSL/TLS certificate obtained from a Certificate Authority (CA).
Cipher Suites:	Negotiate encryption algorithm. Examples: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384.
Common Issues:	Certificate expiration, weak cipher suites, protocol downgrade attacks (e.g., POODLE, BEAST).
Best Practices:	Regularly update certificates, use strong cipher suites, disable SSLv3/TLS 1.0, enforce HTTPS with HSTS.

IPsec

Purpose:	Secures IP communications by authenticating and encrypting each IP packet.
Function:	Operates at the network layer; provides security for VPNs and other network connections.
Configuration:	Configured on routers, firewalls, and servers; involves setting up Security Associations (SAs) using IKE.
Protocols:	Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE).
Common Issues:	NAT traversal issues, incorrect SA configuration, key management complexities.
Best Practices:	Use strong encryption algorithms (e.g., AES), implement perfect forward secrecy (PFS), regularly update keys.

SSH

Purpose:	Provides secure remote access to systems; encrypts communication channels.
Function:	Uses public-key cryptography to authenticate clients and encrypt data; replaces insecure protocols like Telnet and FTP.
Configuration:	Configured on servers; involves setting up SSH keys and configuring SSH daemon (sshd).
Authentication Methods:	Password authentication, public-key authentication, Kerberos, GSSAPI.
Common Issues:	Weak password policies, insecure SSH configurations, brute-force attacks.
Best Practices:	Disable password authentication, use public-key authentication, regularly update SSH server, use fail2ban to block brute-force attacks.

Authentication Protocols

Kerberos

Purpose:	Provides strong authentication for client/server applications using secret-key cryptography.
Function:	Relies on a trusted third party (Key Distribution Center - KDC) to authenticate users and issue tickets.
Configuration:	Configured on domain controllers; involves setting up realms and registering services.
Components:	Authentication Server (AS), Ticket Granting Server (TGS), Kerberos clients.
Common Issues:	Clock synchronization issues, KDC compromise, replay attacks.
Best Practices:	Maintain clock synchronization, secure KDC, regularly update Kerberos software, monitor for suspicious activity.

RADIUS

Purpose:	Provides centralized authentication, authorization, and accounting (AAA) for network access.
Function:	Authenticates users connecting to network devices (e.g., routers, switches, wireless access points).
Configuration:	Configured on RADIUS servers; involves setting up clients (network devices) and user accounts.
Attributes:	Username, password, service type, Framed-IP-Address, NAS-IP-Address.
Common Issues:	Shared secret compromise, dictionary attacks, denial-of-service attacks.
Best Practices:	Use strong shared secrets, implement rate limiting, monitor for suspicious activity, use RADIUS over IPsec.

LDAP

Purpose:	Provides directory services for managing user accounts, resources, and policies.
Function:	Allows applications to authenticate users and retrieve information from a directory.
Configuration:	Configured on LDAP servers; involves setting up directory structure and user accounts.
Operations:	Bind, search, add, modify, delete.
Common Issues:	LDAP injection, anonymous binds, weak access controls.
Best Practices:	Disable anonymous binds, enforce strong access controls, sanitize user inputs, use LDAP over TLS (LDAPS).

Network Security Protocols

DNSSEC

Purpose:	Secures the Domain Name System (DNS) by adding cryptographic signatures to DNS records.
Function:	Prevents DNS spoofing and cache poisoning attacks by verifying the authenticity of DNS data.
Configuration:	Configured on DNS servers; involves generating and managing cryptographic keys and signing DNS zones.
Record Types:	RRSIG, DNSKEY, DS, NSEC.
Common Issues:	Key management complexities, zone signing errors, algorithm vulnerabilities.
Best Practices:	Regularly rotate keys, use strong cryptographic algorithms, monitor for DNSSEC validation failures, implement NSEC3 for zone enumeration protection.

HTTPS

Purpose:	Secure version of HTTP which enables encrypted communication with Transport Layer Security (TLS) or Secure Sockets Layer (SSL)
Function:	Protects the integrity and confidentiality of data transmitted between web browsers and web servers
Configuration:	Requires an SSL/TLS certificate to be installed on the web server. The server is configured to listen for incoming connections on port 443
Protocols:	TLS (Transport Layer Security) and SSL (Secure Sockets Layer)
Common Issues:	Weak cipher suites, mixed content warnings, and vulnerabilities related to SSL/TLS protocols (e.g., Heartbleed, POODLE).
Best Practices:	Always use HTTPS, enforce HTTP Strict Transport Security (HSTS) to prevent protocol downgrade attacks, regularly update SSL/TLS certificates.

SFTP

Purpose:	Secure File Transfer Protocol. Provides secure file transfer over a reliable data stream. Uses SSH to establish secure connections
Function:	Performs all operations over an encrypted SSH transport.
Configuration:	SFTP server is part of SSH server package.
Common Issues:	Man-in-the-middle attacks, brute force attacks.
Best Practices:	Enforce strong password policies, monitor SFTP activity, use key-based authentication, disable password-based authentication.

Wireless Security Protocols

WPA3

Purpose:	Latest wireless security protocol to replace WPA2.
Function:	Offers improved encryption and authentication compared to WPA2.
Configuration:	Configure on wireless routers and devices. Requires compatible hardware.
Key Features:	Simultaneous Authentication of Equals (SAE) - protects against dictionary attacks, enhanced encryption.
Common Issues:	Compatibility issues with older devices, configuration errors.
Best Practices:	Use WPA3 where possible, update firmware regularly, use strong passwords.

WPA2

Purpose:	Wireless security protocol to secure Wi-Fi networks.
Function:	Uses Advanced Encryption Standard (AES) with Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).
Configuration:	Configured on wireless routers and devices. Choose WPA2-Personal (PSK) or WPA2-Enterprise (802.1X).
Key Features:	CCMP encryption, stronger than WEP and WPA.
Common Issues:	PSK cracking, vulnerabilities like KRACK attack.
Best Practices:	Use strong passwords, update firmware regularly, consider WPA3 if available.

WEP

Purpose:	Legacy wireless security protocol. Obsolete and insecure.
Function:	Uses RC4 encryption with a 40-bit or 104-bit key.
Configuration:	Avoid using WEP. If unavoidable, change the WEP key frequently.
Key Features:	Simple to configure, but easily cracked.
Common Issues:	Easily cracked using readily available tools.
Best Practices:	Do not use WEP. Upgrade to WPA2 or WPA3 immediately.