SSL TLS Scan Checklist

This checklist is designed to evaluate SSL/TLS implementations on servers and services (web, mail, APIs) from a defensive perspective. It aligns with **NIST SP 800-52r2**, **OWASP Transport Layer Protection Cheat Sheet**, **Mozilla SSL Guidelines**, **CIS Benchmarks**, and **PCI DSS v4.0**.

Category	Checkpoint	Detail / Best Practice	Status
Protocols	TLS Versions	Only **TLS 1.2** and **TLS 1.3** enabled. TLS 1.0, 1.1, SSLv2, SSLv3 must be disabled.	☐
	DTLS	If using datagram services, DTLS config should mirror TLS standards.	☐
Cipher Suites	Strong Ciphers	Prefer **AES-GCM**, **AES-CCM**, or **CHACHA20-POLY1305**.	☐
	Forward Secrecy	Use **ECDHE** or **DHE** for key exchange to protect past sessions.	☐
	Weak/Deprecated Ciphers	Disable **RC4, DES, 3DES, NULL, EXPORT**, MD5-based ciphers.	☐
	Cipher Order	Server should **prefer its own cipher order** over client order.	☐
Certificates & Keys	Certificate Validity	Validity ≤ 398 days (as per CA/B Forum). Avoid expired certs.	☐
	Key Strength	**RSA ≥ 2048 bits**, **ECC ≥ 256 bits**.	☐
	CN/SAN	Matches server domain name; covers all hostnames.	☐
	Trusted CA	Use certificates issued by **trusted Certificate Authorities**.	☐
	Intermediate Certificates	Proper chain installed; no broken chains.	☐
	Revocation Check	OCSP stapling enabled; CRL or OCSP accessible.	☐
	Certificate Rotation	Certificates renewed **before expiry** and rotated securely.	☐
TLS Features / Configuration	HSTS	HTTP Strict Transport Security enabled; max-age ≥ 6 months; include subdomains.	☐
	TLS Compression	Disabled to prevent CRIME attacks.	☐

Category	Checkpoint	Detail / Best Practice	Status
	Secure Renegotiation	Must be enabled or insecure renegotiation disabled.	☐
	Session Resumption	Use **secure session tickets**; TLS session IDs properly configured.	☐
	ALPN/NPN	Proper configuration for HTTP/2 negotiation.	☐
	HTTP/2 Enforcement	TLS configuration should support HTTP/2 where applicable.	☐
Mail / STARTTLS	STARTTLS Enforcement	STARTTLS must be advertised and enforced on SMTP, IMAP, POP3.	☐
	No Plaintext Fallback	Disallow fallback to unencrypted communication.	☐
	Certificate Verification	Valid certificates presented during negotiation.	☐
	Strong Cipher Enforcement	Only strong ciphers used for STARTTLS connections.	☐
Vulnerability Protection	Known Exploits	Test for **Heartbleed, BEAST, POODLE, DROWN, FREAK, Logjam**. None should be exploitable.	☐
	TLS Downgrade	TLS downgrade protection enabled (RFC 7507).	☐
	Scan Tools	Regular scans using **sslscan, testssl.sh, sslyze**.	☐
	Misconfigurations	Check for weak DH params (< 2048 bits), insecure cipher suites, improper certificate chains.	☐
Monitoring & Governance	Certificate Inventory	Maintain centralized inventory of all TLS certificates in use.	☐
	Expiry Alerts	Automated alert for upcoming certificate expiry.	☐
	Configuration Review	TLS configs reviewed quarterly or after major updates.	☐
	Audit Compliance	Verify alignment with **NIST, CIS, OWASP, PCI DSS** standards.	☐
Logging / Alerting	TLS Errors	Log TLS handshake failures and unusual patterns.	☐
	STARTTLS / SMTP Alerts	Monitor mail server logs for downgrade or invalid cert attempts.	☐

Category	Checkpoint	Detail / Best Practice	Status
	Vulnerability Alerts	Correlate CVE alerts with SSL/TLS vulnerabilities in deployed services.	☐
Additional / Optional	Perfect Forward Secrecy	Ensure all ciphers used provide forward secrecy.	☐
	Certificate Pinning	For critical applications, pin certificates to prevent MITM attacks.	☐
	Secure Renegotiation Testing	Verify that client-initiated renegotiation does not allow injection.	☐
	TLS 1.3 Features	Ensure 0-RTT and other TLS 1.3 features are configured securely.	☐

> **Scan Recommendations:** `sslscan`, `testssl.sh`, `sslyze`, `nmap --script ssl-enum-ciphers`