Perfect 👍 You want **precise WSTG notes** for **Testing for Weak Transport Layer Security (TLS)** with **sslyze/sslscan, testssl.sh, and nmap scripts**.  
Here’s a clean breakdown:

**📝 Notes: Testing for Weak TLS (WSTG-CRYP-02)**

**🎯 Purpose**

To identify weak or misconfigured **TLS/SSL implementations** used by the web application.  
Weak TLS allows:

* MITM attacks
* Downgrade attacks
* Cipher-suite exploitation

**🔍 What to Check**

* Supported TLS/SSL versions (SSLv2, SSLv3, TLS 1.0/1.1 = **weak**)
* Cipher suites (EXPORT, NULL, RC4, 3DES, weak key lengths)
* Certificate issues (expired, self-signed, weak algorithms like MD5/SHA1)
* Insecure renegotiation, compression (CRIME), or key exchange

**⚡ Tools & Commands**

**1. sslscan (fast TLS check)**

sslscan <target>:443

* Shows supported TLS versions & cipher suites
* Look for: SSLv2/3 enabled, weak ciphers (RC4, DES, EXPORT)

**2. testssl.sh (comprehensive script)**

./testssl.sh -U --openssl=openssl <target>

or

./testssl.sh <target>:443

* Checks protocol support, ciphers, vulnerabilities (BEAST, POODLE, Heartbleed)
* Flags misconfigurations in detail

**3. nmap TLS scripts**

nmap --script ssl-enum-ciphers -p 443 <target>

* Enumerates supported ciphers & key strengths

nmap --script ssl-cert -p 443 <target>

* Fetches SSL certificate details (expiry, issuer, algorithms)

nmap --script ssl-dh-params -p 443 <target>

* Checks for weak Diffie-Hellman parameters

**🛡️ Mitigation**

* Disable **SSLv2/SSLv3, TLS 1.0/1.1** → enforce **TLS 1.2+**
* Remove weak ciphers (RC4, DES, EXPORT, NULL)
* Use **AES-GCM / ChaCha20-Poly1305** with strong PFS (ECDHE)
* Deploy strong certs (RSA ≥ 2048-bit, SHA-256 or higher, ECDSA preferred)
* Enable **HSTS** and secure renegotiation

✅ **Key Takeaway:**  
Use **sslscan** for quick checks, **testssl.sh** for deep analysis, and **nmap scripts** for automation across multiple targets.

Do you want me to also prepare a **ready-to-run bash script** combining sslscan, testssl.sh, and nmap checks for one-shot testing?