SENIOR PROJECT II

SECURITY IMPROVEMENT ON THE TLS-ALERT SUP PROTOCOL

Student: Badr AL Deen Abo loubada

Supervised by: Dr. Wassim Juneidi

Faculty of Operating systems and information security

الجامعة السورية الخاصة

SYRIAN PRIVATE UNIVERSITY

الفهرس

الأهداف والمشاكل العلمية

- الأهداف
  - تحسين مستوى الأمان ضمن البروتوكول الفرعي **Alert TLS** عبر إضافة تنبيه جديد *Downgrade attempt detected*
  - تحليل ومقارنة فعالية التنبيه المضاف وهل اضافته مجدية بالنسبة لمعايير البرتوكول
- المشاكل
  - عدم القدرة على معرفة إمكانتيات المحاسبية للطرف المتصل
  - كثرة الأخطاء الغير موصوفة بدقة تؤدي الى ضغط بمحاولات الاتصال

المراجع النظرية

البحث	اسم البحث	تاريخ النشر	هدف البحث	مواطن قوة البحث	علاقة البحث بالمشروع	power
[1]	Secure Socket Layer (SSL)/TLS in Transport Layer Security	2025	توصيف عام للبرتوكول و توضيح المخاطر العامة و التوصيات لأفضل استخدام	لإثبات أن نسخة البتوكول TLS 1.3 تحقق المتطلبات الأساسية للأمان	الاستفادة من المعلومات الاساسية حول بروتوكول TLS 1.3	متوسط
[2]	A cryptographic analysis of the TLS 1.3 handshake protocol.	2021	وصف واضح غير معقد للبروتوكول و مقارنة بين جميع نسخه	وصف دقيق ل Handshake	الاستفادة من المعلومات حول البروتوكول الفرعي Handshake	متوسط
[3]	An Efficient Integrity and Authenticated Elliptic Curve Cryptography Algorithm for Secure Storage and Routing in TLS/SSL	2025	تحسين TLS عبر استخدام ECC-based schemeمعدلة وذات خطوات أقل	يدعم الأهداف الأمنيه المطلوبة مع وقت تكلفة أقل	مقارنة التحسين على البروتوكول وفعاليته بمجال	قوي (مقارنة عملية)
[4]	Assessing SSL/TLS Certificate Centralization: Implications for Digital Sovereignty	2025	دراسة جدوى حول فوائد استخدام CA مركزي لجميع الدول	توصيف مشكلة عامة و مدى تأثيرها على الدول	مقارنة التحسين على البروتوكول وفعاليته بمجال	قوي (مقارنة عملية)

المراجع النظرية

البحث	اسم البحث	تاريخ النشر	هدف البحث	مواطن قوة البحث	علاقة البحث بالمشروع	power
[5]	Handling SSL CertificateChallenges &Solutions Properly For Improved NetworkSecurity	2023	دراسة مشكلة عملية في تنظيم شهادات ال SSL، و وصف الحلول لتلك المشكلة	توصيلت عملية قابلة للتطبيق الفعلي على البتوكول لتحسينه	مقارنة التحسين على البروتوكول وفعاليته بمجال	متوسط
[6]	A taxonomy of downgrade attacks in the TLS	2018	بناء بحث حول downgrade ومقارنة بين حالات هجوم سابقة	القدرة على التعرف على الهجوم في المرات القادمة	بحث مقارنة عملية بين 15 محاولة downgrade	قوي
[7]	Evolution of SSL/TLS indicators and warnings in web browser	2019	تتبع كيف يتعامل عارض الويب مع أحطاء ال TLS	فهم كيفيه تطور التفسير الاخطاء من قبل عارض الويب	دراسة حول التطويرات على التنبيهات	متوسط
[8]	Guidelines for the selection, configuration, and use of transport layer security (tls)implementations (sp 800-52 rev. 2)	2009	المعيار العالمي من منظمة الNIST	معيار عالمي	لمقارنة نتائج البحث بالمعايير العالمية	قوي جدا

المراجع النظرية

البحث	اسم البحث	تاريخ النشر	هدف البحث	مواطن قوة البحث	علاقة البحث بالمشروع	power
[9]	The Transport Layer Security (TLS) Protocol Version 1.3	2018	التوصيف العام لبروتوكول TLS 1.3	-------	التوصيف الاساسي للبروتوكول بنسخته الحديثة	قوي
[10]	The Transport Layer Security (TLS) Protocol Version 1.2	2008	التوصيف العام لبروتوكول TLS 1.2	-------	التوصيف الاساسي للبروتوكول لاخر نسخة موافق على استخادامها	وسط

الدراسة النظرية

- Alert sup protocol:

Type 21	Version 3 : 0	Length 0
2	Level 1/2	Description

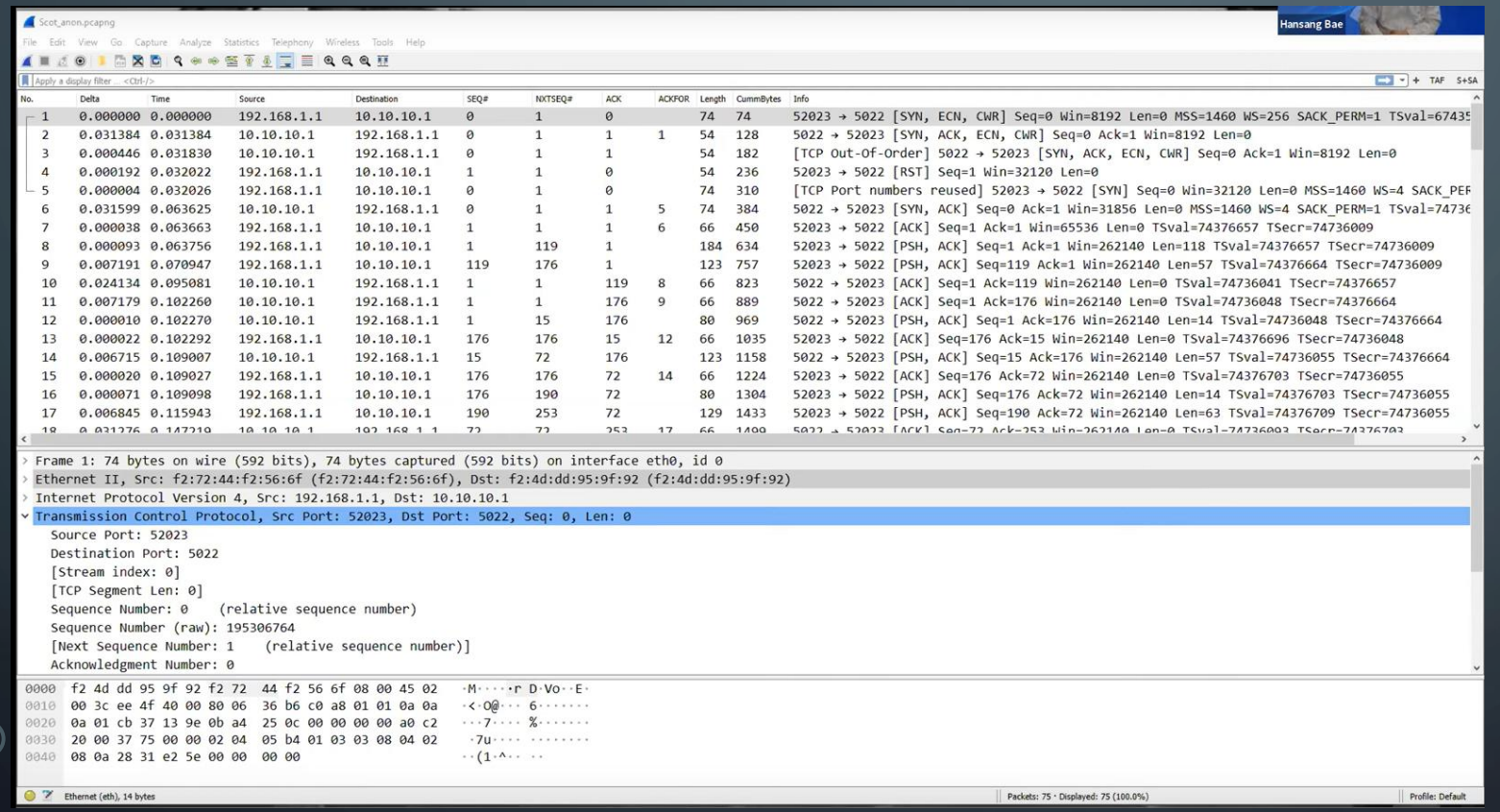
تجهيز بيئة العمل

الأدوات المستخدمة

- Wireshark
- OpenSSl
- Git/GitHub
- vscode

تجهيز بيئة العمل

- Wireshark



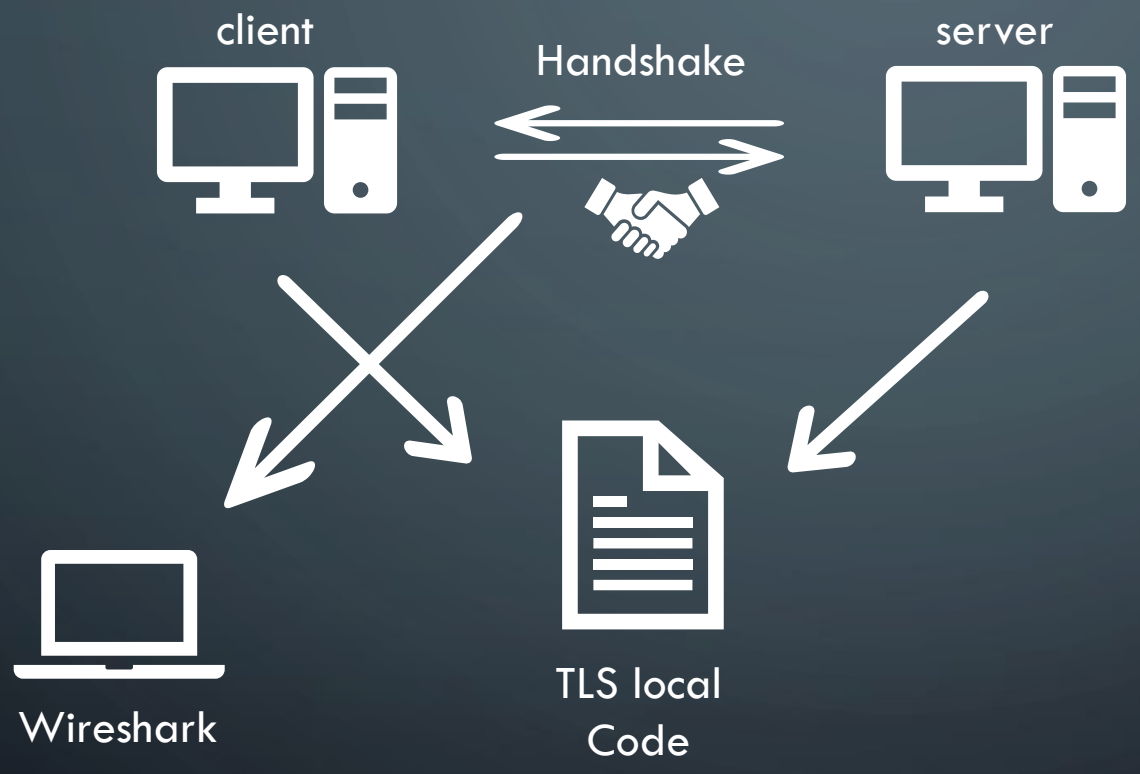
تجهيز بيئة العمل

OpenSSL

- **Testing implementation**
  - s_server -accept 4433 -cert cert.pem -key key.pem
  - s_client -connect localhost:4433
- **Debugging**
  - openssl x509 -noout -modulus -in certificate.crt | openssl md5
- **Generate a certificate**
  - openssl req -out CSR.csr -key privateKey.key -new

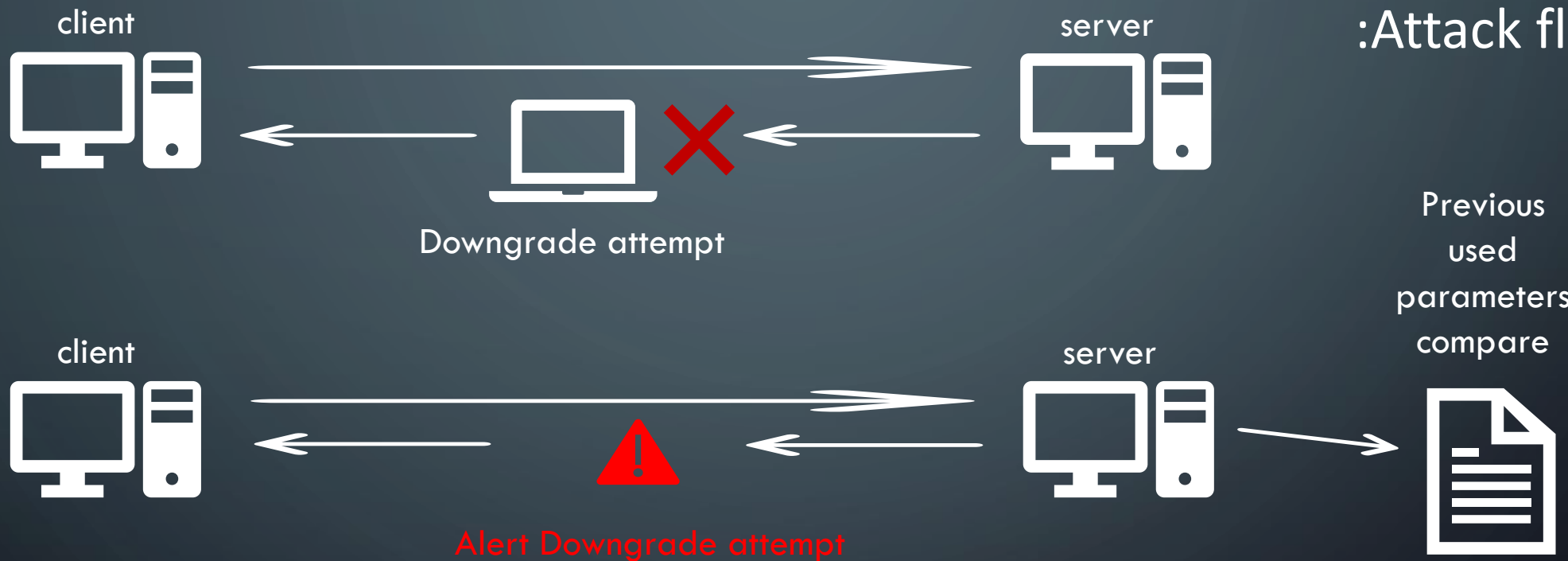
تجهيز بيئة العمل

- القسم الفيزيائي:



الحل المقترح

:Attack flow



المراجع

[1] Chakkour, Souhail. "Secure Socket Layer (SSL)/TLS in Transport Layer Security", Mississippi State University, 2025.

[2]Dowling, Benjamin, Marc Fischlin, Felix Günther, and Douglas Stebila. "A cryptographic analysis of the TLS 1.3 handshake protocol." *Journal of Cryptology* 34, no. 4 (2021): 37.

[3]Menandas, Josepha, and Mary Subaja. "An Efficient Integrity and Authenticated Elliptic Curve Cryptography Algorithm for Secure Storage and Routing in TLS/SSL." *International Arab Journal of Information Technology (IAJIT)* 22, no. 5 (2025)

[4]Azevedo, Andrei Cordova, Eder John Scheid, Muriel Figueredo Franco, and Lisandro Zambenedetti Granville. "Assessing SSL/TLS Certificate Centralization: Implications for Digital Sovereignty." (2025).

[5]Kodurupati, Prashanth. "Handling SSL CertificateChallenges &Solutions Properly For Improved NetworkSecurity." Journal of Technological Innovations 4, no. 3 (2023).

[6]Alashwali, Eman Salem, and Kasper Rasmussen. "What's in a downgrade? A taxonomy of downgrade attacks in the TLS protocol and application protocols using TLS." In *International Conference on Security and Privacy in Communication Systems*, pp. 468-487. Cham: Springer International Publishing, 2018.

[7]Kraus, Lydia, Martin Ukrop, Vashek Matyas, and Tobias Fiebig. "Evolution of SSL/TLS indicators and warnings in web browsers." In *Cambridge International Workshop on Security Protocols*, pp. 267-280. Cham: Springer International Publishing, 2019.

[8]Sunshine, Joshua, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. "Crying wolf: An empirical study of ssl warning effectiveness." In *USENIX security symposiu* , pp. 399-416. 2009.

[9]Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8447, August 2018

[10]Dierks, T., and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, August 2008.

تجهيز بيئة العمل