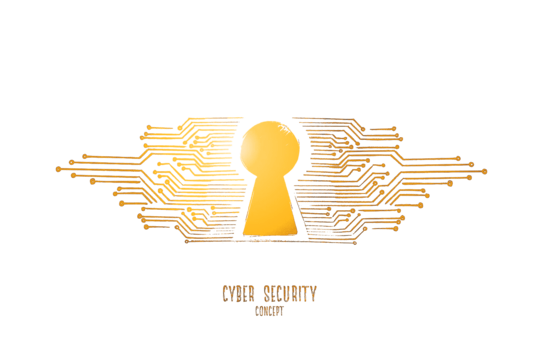
Bastionado de redes 

y sistemas.



| Práctica (Kali-Linux) |
| --- |
| Comencemos a escuchar sin filtro por Wireshark |
| **Sudo wireshark** |
| Seleccionamos la interfaz de red |
|  |
| \*\* Realizar algunas búscadas en el browser para obtener algunos registros. |
| Es útil ver las conversaciones antes de ver los paquetes stadistics > conversations |
|  |
| Buscamos una conexión TCP sobre ipv4 así que podemos hacer uso de los filtro de esta pestaña |
|  |
| La primera conexión ordenada por el número de bytes parece muy interesante para comenzar el estudio |
| Click derecho > follow y nos aplicará el filtro de esta conversación. |
|  |
| TCP HandShake |
|  |
| TLS HandShake |
|  |
| Datos encriptados de la web |
|  |
|  |
|  |

| ¿Qué es SSL/TLS? |
| --- |
| SSL(Secure Socket Layer) |
| SSL o Secure Sockets Layer es un [protocolo](https://www.cloudflare.com/learning/network-layer/what-is-a-protocol/) de seguridad de Internet basado en el [cifrado](https://www.cloudflare.com/learning/ssl/what-is-encryption/). Inicialmente fue desarrollado para garantizar la   * **Privacidad** * **Autenticación** * **Integridad**   de los datos en las comunicaciones de Internet. SSL es el predecesor del cifrado [TLS](https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/) moderno que se utiliza hoy en día. |
| Los sitios web que implementan SSL/TLS tienen "[HTTPS](https://www.cloudflare.com/learning/ssl/what-is-https/)" en su URL en lugar de "[HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/)". |
| SSL inicia un proceso de **autenticación**, conocido como [establecimiento de comunicación](https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/), entre dos dispositivos que se comunican para garantizar que ambos sean lo que aparentan. |
|  |
| **SSL firma digitalmente** los datos para proporcionar **integridad de datos** , que verifica que no se hayan manipulado los datos antes de alcanzar al destinatario designado. |
| “ Un Certificado Electrónico (o **certificado digital**) es un fichero digital emitido por una tercera parte de confianza (una Autoridad de Certificación) que garantiza la vinculación entre la identidad de una persona o entidad y su clave pública ” |
| Tipos de certificado SSL |
| * **Un solo dominio:** el certificado SSL para un solo dominio se aplica a un solo dominio (un "dominio" es el nombre de un sitio web, como www.cloudflare.com). * **Comodín:** al igual que el certificado de un solo dominio, el certificado SSL comodín se aplica a un solo dominio. Sin embargo, también incluye los subdominios de ese dominio. Por ejemplo, un certificado comodín podría abarcar www.cloudflare.com, blog.cloudflare.com, y developers.cloudflare.com, mientras que un certificado de dominio único solo incluiría el primero. * **Multidominio:** como su nombre indica, los certificados SSL multidominio pueden aplicarse a varios dominios no relacionados. |
| Diferentes niveles de validación. Un nivel de validación es como una revisión de antecedentes, y el nivel cambia dependiendo de la exhaustividad de la revisión.   * **Validación del dominio**: es el nivel de validación menos estricto y el más barato. Lo único que el negocio debe hacer es probar que controla el dominio. * **Validación de la organización:** es un proceso más práctico; la AC se pone en contacto directamente con la persona o empresa que solicita el certificado. Estos certificados son más fiables para los usuarios. * **Validación extendida:** requiere una comprobación completa de los antecedentes de una organización antes de que se pueda emitir el certificado SSL. |
| ¿Qué es TLS? |
| 1. El cliente envía una lista de todas las versiones de TLS junto con sugerencias para un conjunto de cifrado y genera un número aleatorio que se utilizará posteriormente. 2. El servidor confirma qué opciones utilizará para iniciar la conexión. 3. El servidor envía un certificado TLS al cliente para el proceso de autenticación. 4. Después de validar el certificado, el cliente crea y envía una clave pre-matriz cifrada por la clave pública del servidor y descifrada por la clave privada del servidor. 5. El cliente y el servidor generan las claves de sesión utilizando los números aleatorios generados previamente y la clave premaster. 6. Tanto el cliente como el servidor tienen un mensaje terminado que ha sido cifrado con una clave de sesión. 7. El proceso de negociación TLS ha finalizado, y tanto el cliente como el servidor han creado un cifrado simétrico seguro. |
| **Diferencia entre TLS y SSL, y cómo saber cuál estás utilizando** Ambos protocolos de seguridad funcionan de forma similar, utilizando claves criptográficas en varios protocolos de la capa de aplicación, como HTTP, FTP, IMAP y SMTP.  TLS ofrece un proceso de negociación diferente, algoritmos de cifrado más robustos y suites de cifrado más seguras.  código de autenticación de mensajes  TLS   * Auth HMAC * Varios mensajes de error   SSL   * Auth MAC * Varios mensajes de error   Sin embargo, ambos términos suelen utilizarse indistintamente, ya que la primera versión de TLS se lanzó como una actualización de SSL 3.0. Por ello, mucha gente utiliza el término TLS/SSL para referirse al protocolo.  Si estás utilizando un sitio web con TLS, debería aparecer un icono de candado junto a la barra de URL, que indica que la conexión es segura. Al hacer clic en él, puedes ver detalles de información, como los de su certificado TLS/SSL. |
| HTTPS y TLS |
| [HTTPS](https://www.cloudflare.com/learning/ssl/what-is-https/) es una implementación de la encriptación TLS en el protocolo [HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/), usado por todos los sitios web así como otros servicios web. Todos los sitios web que usan HTTPS emplean por tanto la encriptación TLS. |

**Bibliografía:**

* <https://www.digicert.com/es>
* <https://www.golinuxcloud.com/wireshark-decrypt-ssl-tls-tutorial/>
* <https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls>
* <https://www.ssl.com/article/ssl-tls-handshake-overview/>
* <https://www.clickssl.net/blog/what-is-ssl-tls-handshake-ssl-handshake-explained>
* <https://www.linuxbabe.com/security/ssltls-handshake-process-explained-with-wireshark-screenshot>
* Interesante dato sobre la importancia en la ciberseguridad: <https://www.clickssl.net/blog/port-443>
* Seguridad en el endpoint

<https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=e612e657-698c-4241-93ff-a7ca15210c27&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>

* <https://www.baeldung.com/cs/tcp-protocol-syn-ack>
* <https://www.baeldung.com/cs/tcp-fin-vs-rst>
* <https://www.youtube.com/watch?v=QRRHA_5hS2c>