



Actividad 1 Pérdida de Autenticación y Gestión de Sesiones.

Auditoría Informática.

Ingeniería en Desarrollo de Software



TUTOR: Jessica Hernández Romero.

ALUMNO: Homero Ramirez Hurtado.

FECHA: 13 de Febrero del 2024.

Índice.

. Introducción.

. Descripción.

. Justificación.

. Descripción del Sitio Web.

. Ataque al Sitio.

. Conclusión.

. Referencias.

Introducción.

La auditoría informática es una disciplina clave en el ámbito de la tecnología de la información y la gestión empresarial, cuyo propósito principal es evaluar y mejorar la eficiencia, seguridad y confiabilidad de los sistemas informáticos de una organización. A través de un enfoque sistemático y estructurado, la auditoría informática analiza los controles internos, procesos y procedimientos relacionados con el uso, gestión y protección de los recursos tecnológicos.

La importancia de la auditoría informática radica en su capacidad para identificar y mitigar riesgos asociados con la pérdida de datos, accesos no autorizados, fallos en la infraestructura tecnológica y otros incidentes que puedan afectar la continuidad operativa y la integridad de la información. Además, esta práctica contribuye a garantizar el cumplimiento de normativas legales y regulaciones específicas del sector, así como a mejorar la toma de decisiones estratégicas mediante la provisión de información precisa y oportuna sobre el estado de los sistemas informáticos.

El proceso de auditoría informática abarca diversas etapas, incluyendo la planificación, ejecución, informe de hallazgos y seguimiento de recomendaciones. Durante la planificación, se definen los objetivos, alcances y criterios de la auditoría. En la fase de ejecución, se llevan a cabo pruebas y evaluaciones técnicas para verificar la efectividad de los controles implementados. Los hallazgos y recomendaciones se documentan en un informe detallado, que es presentado a la alta dirección para su revisión y acción. Finalmente, el seguimiento asegura que las recomendaciones sean implementadas y que los riesgos identificados sean gestionados adecuadamente.

En resumen, la auditoría informática es una herramienta esencial para proteger y optimizar los recursos tecnológicos de una organización, asegurando su buen funcionamiento y contribuyendo a su éxito a largo plazo.

Descripción.

La auditoría informática ofrece una amplia gama de beneficios que contribuyen significativamente a la estabilidad, seguridad y eficiencia de las organizaciones. En primer lugar, uno de los principales beneficios es la **identificación y mitigación de riesgos**. Al evaluar y mejorar los controles internos, la auditoría informática ayuda a prevenir incidentes como la pérdida de datos, accesos no autorizados y fallos en la infraestructura tecnológica, lo que asegura la continuidad operativa de la empresa.

Otro beneficio crucial es el **cumplimiento normativo y regulatorio**. La auditoría informática garantiza que la organización cumpla con las leyes y regulaciones aplicables, evitando sanciones y multas que puedan resultar de incumplimientos. Esto es especialmente relevante en sectores altamente regulados, como el financiero y el sanitario, donde la protección de datos y la privacidad son fundamentales.

Además, la auditoría informática **mejora la eficiencia operativa**. Al identificar áreas de mejora en los procesos y sistemas, se pueden implementar soluciones que optimicen el rendimiento y la productividad de la organización. Esto no solo reduce costos, sino que también permite a la empresa aprovechar al máximo sus recursos tecnológicos.

La **protección de la información** es otro aspecto destacado. La auditoría informática asegura que los datos críticos estén adecuadamente protegidos contra amenazas internas y externas, lo que fortalece la confianza de los clientes y socios comerciales en la organización.

Por último, la **toma de decisiones informadas** es facilitada por la auditoría informática. Al proporcionar información precisa y oportuna sobre el estado de los sistemas y procesos, los líderes empresariales pueden tomar decisiones estratégicas basadas en datos concretos y fiables.

En resumen, la auditoría informática no solo protege y optimiza los recursos tecnológicos, sino que también contribuye al cumplimiento normativo, la eficiencia operativa y la toma de decisiones informadas, asegurando el éxito y la sostenibilidad a largo plazo de la organización.

Justificación.

Wireshark es una herramienta de software de código abierto que se utiliza para el análisis de redes y el diagnóstico de seguridad. Es ampliamente reconocido por su capacidad para capturar y analizar datos en tiempo real, lo que permite a los administradores de red y profesionales de la seguridad examinar el tráfico de red de manera detallada. Esta capacidad es fundamental para identificar posibles vulnerabilidades y amenazas en una red.

Una de las principales ventajas de Wireshark es su interfaz gráfica intuitiva, que facilita la visualización y el análisis del tráfico de red. Los usuarios pueden aplicar filtros avanzados para enfocarse en datos específicos y utilizar una variedad de comandos y sintaxis para interpretar los protocolos y detectar patrones maliciosos. Además, Wireshark permite la exportación de datos en diferentes formatos, lo que facilita la creación de informes y la colaboración con otros equipos.

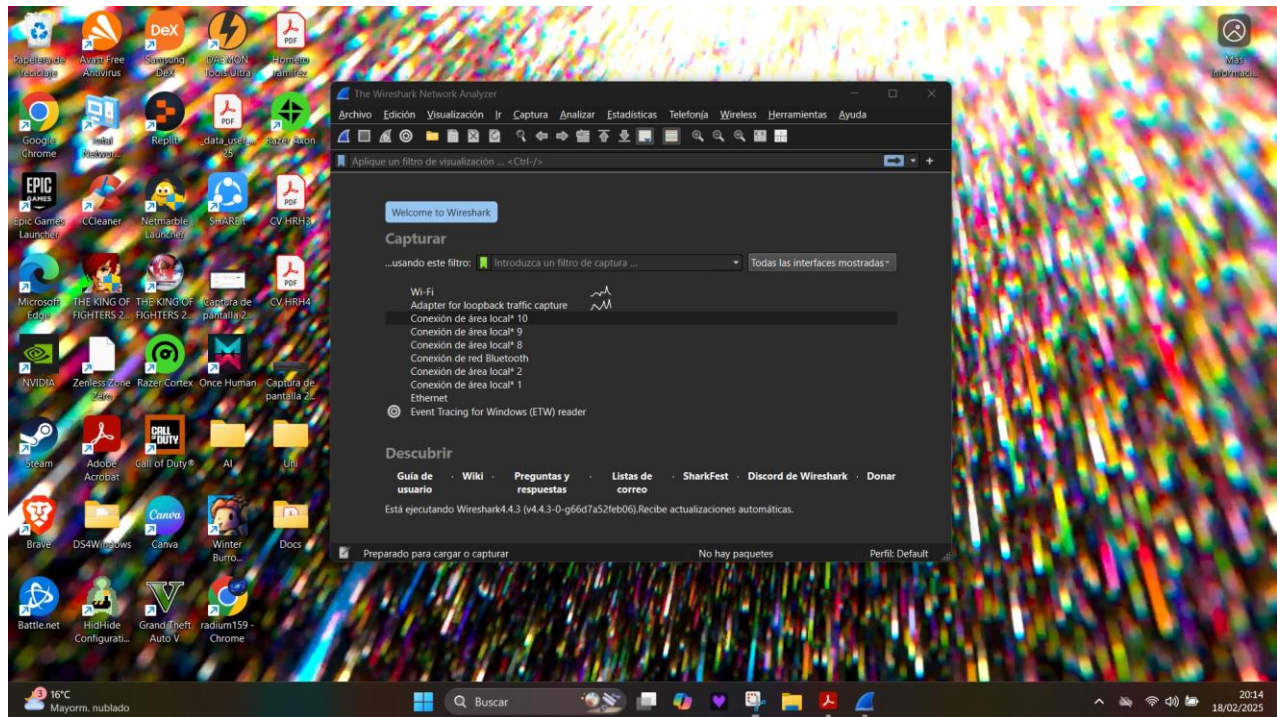
En el contexto de la auditoría informática, Wireshark se utiliza para diagnosticar problemas de seguridad, como ataques DDoS, intrusiones y fugas de datos. Al interceptar y analizar el tráfico de red, los profesionales pueden identificar paquetes sospechosos y tomar medidas de contención para mitigar las amenazas. La herramienta también es útil para realizar auditorías de seguridad, proporcionando informes detallados sobre las vulnerabilidades encontradas y recomendaciones para mejorar la seguridad de la red.

En resumen, Wireshark es una herramienta esencial para la auditoría informática debido a su capacidad para capturar, analizar y solucionar problemas del tráfico de red, garantizando así la integridad y seguridad de la información en cualquier organización.

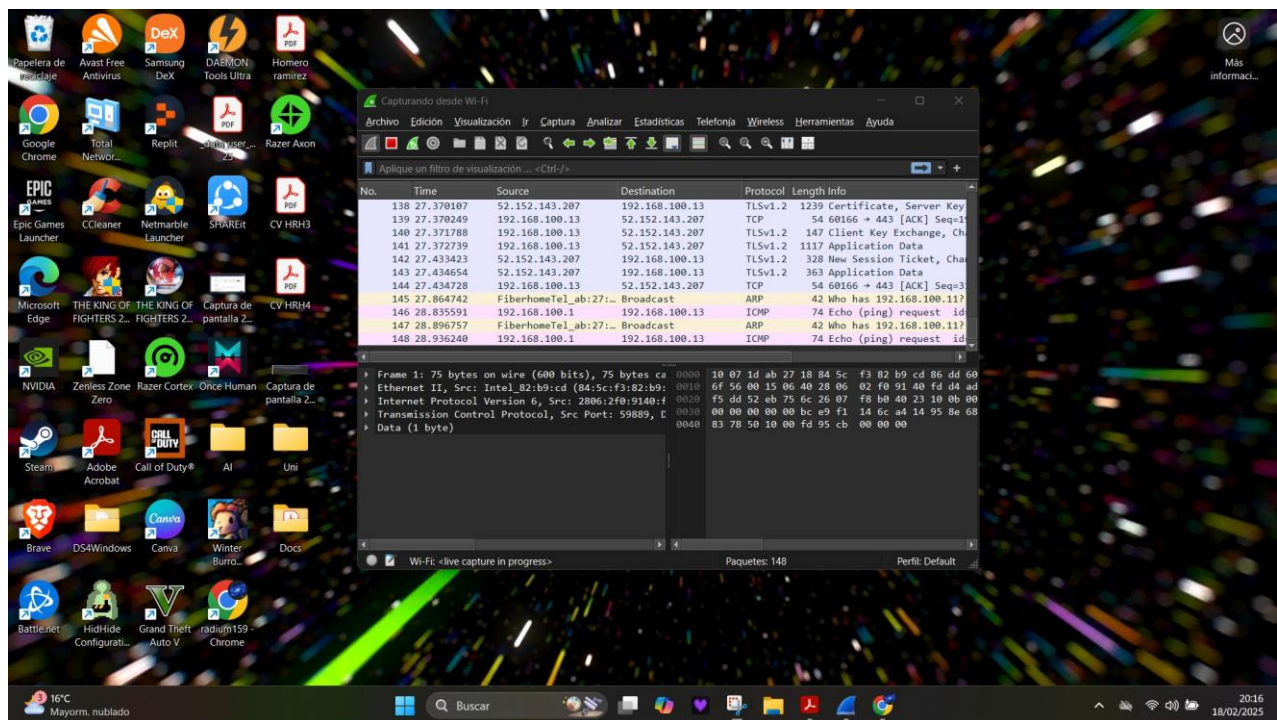
Descripción del Sitio Web.

Hostinger es una plataforma en línea que ofrece servicios de alojamiento web y dominios a precios asequibles. Fundada en 2004, Hostinger se ha convertido en uno de los proveedores líderes en el mercado, con más de 3 millones de usuarios en más de 150 países. Su creador de sitios web permite a los usuarios construir sitios web sin necesidad de conocimientos técnicos avanzados. Ofrece más de 150 plantillas personalizables, un editor de arrastrar y soltar, y funciones eCommerce integradas. Además, cuenta con herramientas de marketing e inteligencia artificial nativas, configuración de posicionamiento SEO, certificado SSL gratuito y guardado automático de versiones web.

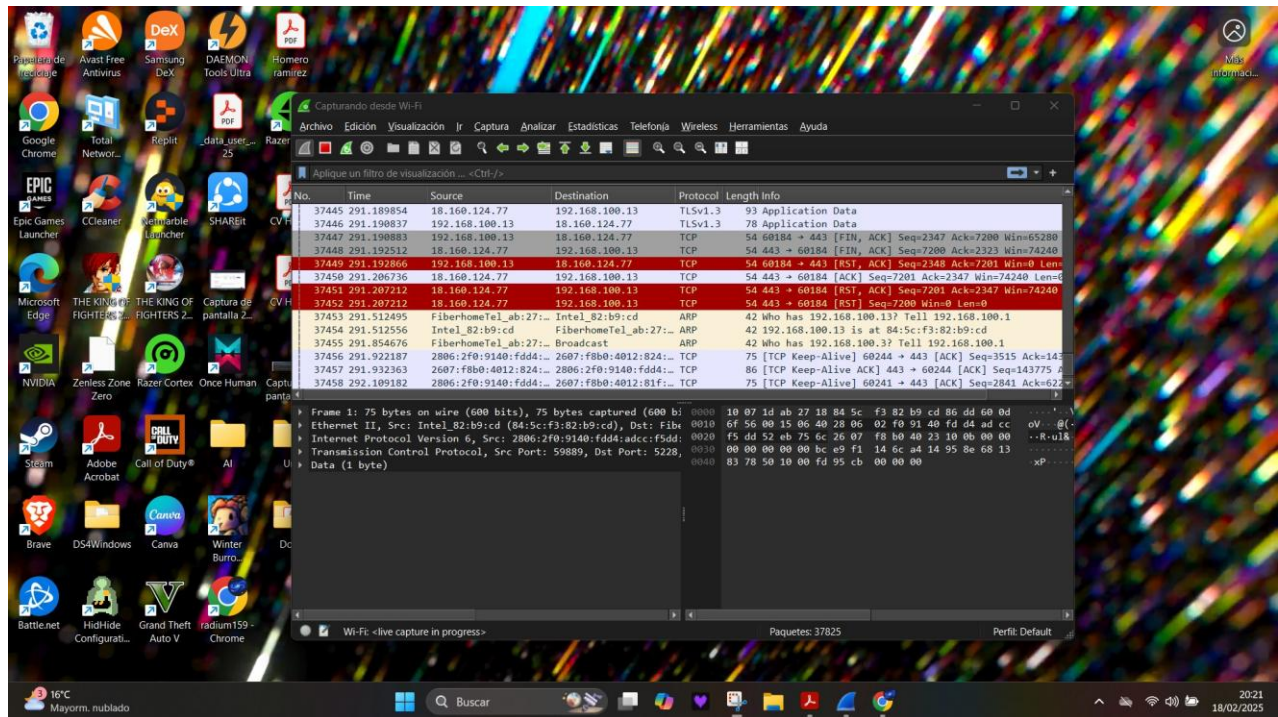
Ataque al Sitio.



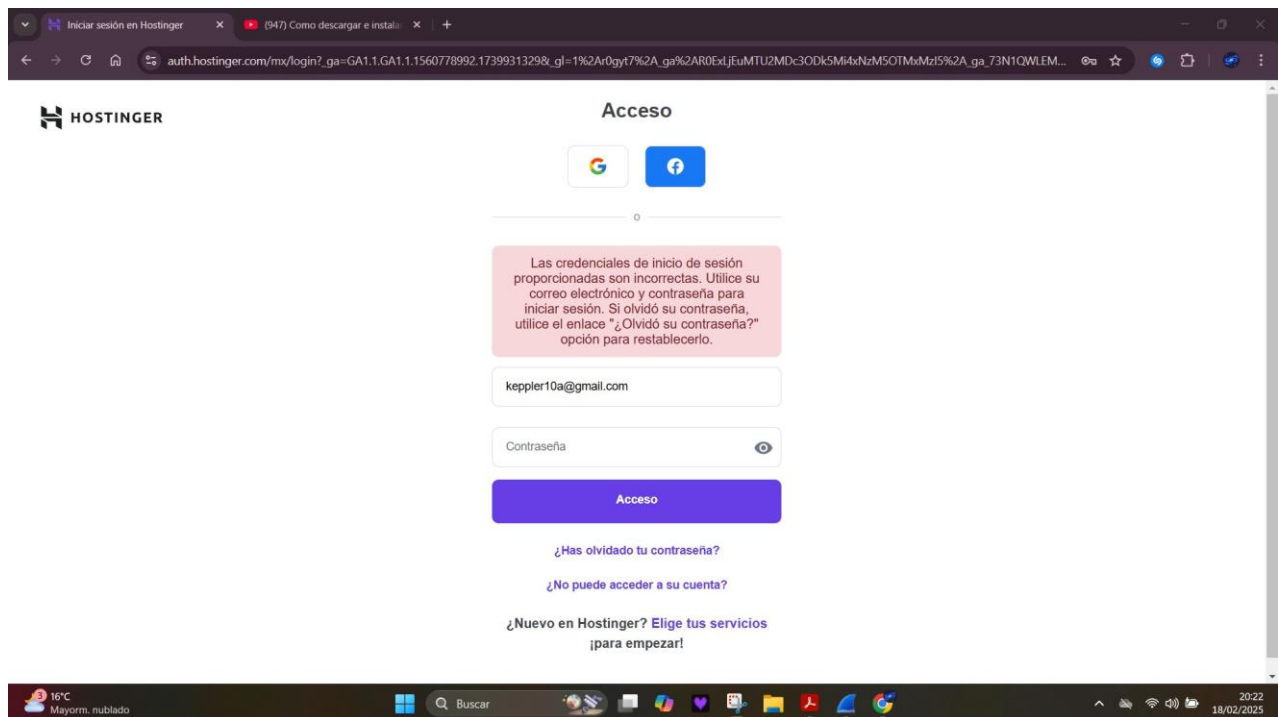
Se inicia WireShark.



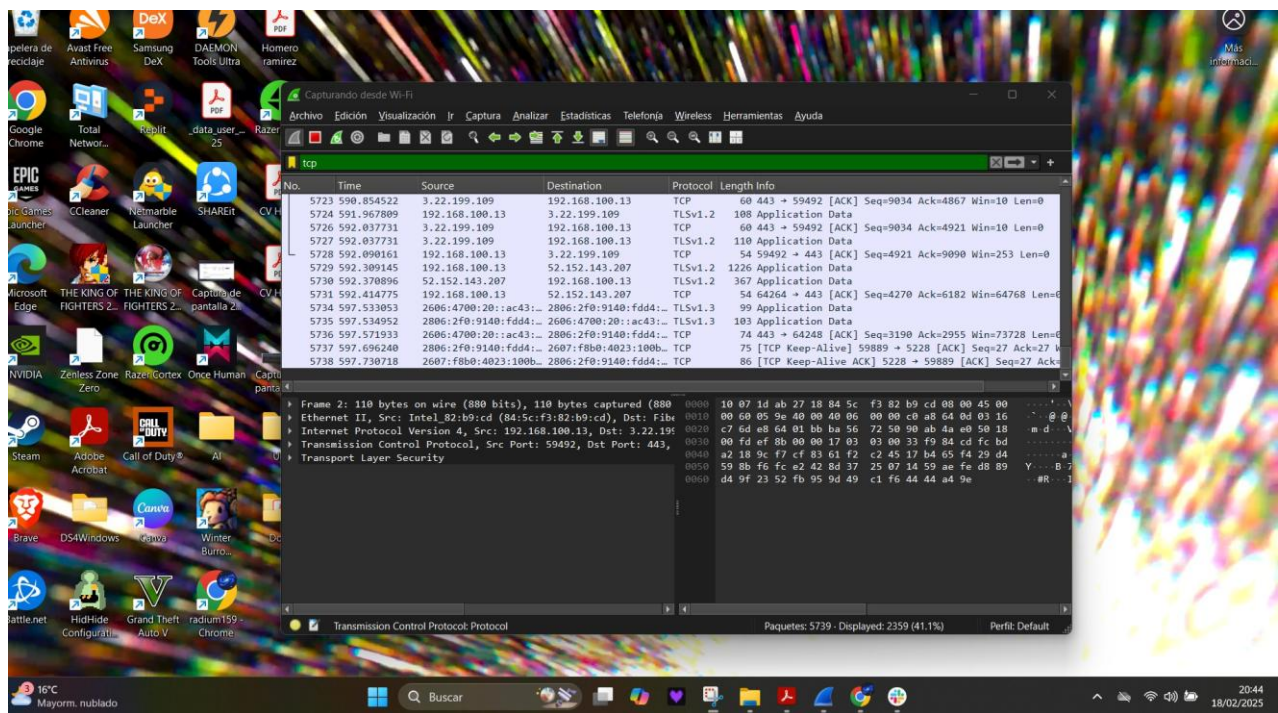
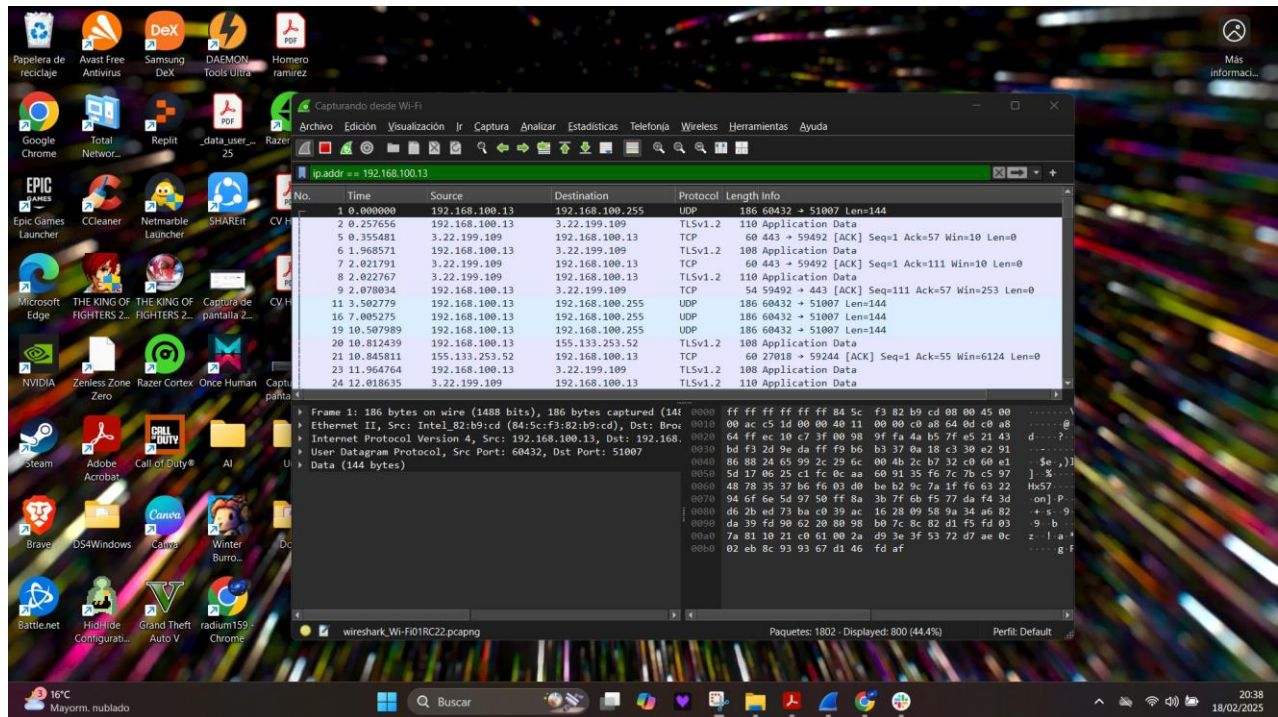
Se ingresa en la opción de WiFi.

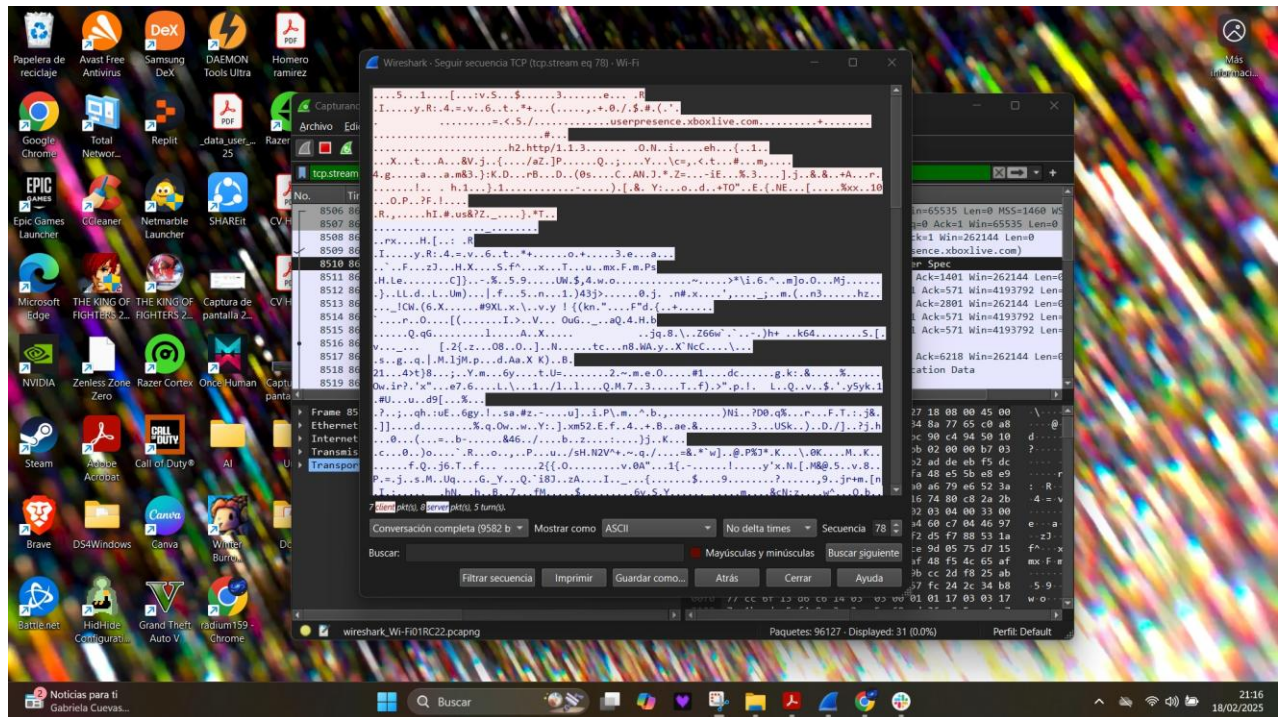


Se observan los detalles.



Se elige sitio web.





Resultado final del ataque.

Conclusión.

Realizar un ataque a un sitio web utilizando una herramienta como Wireshark no solo es ilegal, sino también éticamente incorrecto. Wireshark es una herramienta poderosa y educativa que permite a los profesionales de TI y a los entusiastas de la tecnología analizar el tráfico de la red para diagnosticar problemas, mejorar la seguridad y optimizar el rendimiento. Sin embargo, como todas las herramientas, su uso indebido puede tener consecuencias negativas.

Wireshark no se diseñó para llevar a cabo ataques cibernéticos, sino para proporcionar una visión detallada y analítica del tráfico de la red. Utilizarla con fines maliciosos va en contra de los principios de ética en la ciberseguridad. El conocimiento y las habilidades en el ámbito de la ciberseguridad deben ser aplicados para proteger y fortalecer infraestructuras, no para explotarlas.

Es crucial comprender que los ataques a sitios web pueden causar daños significativos, desde pérdidas financieras hasta la destrucción de la reputación de una empresa. Además, las consecuencias legales pueden ser severas, incluyendo multas y penas de cárcel.

En lugar de centrar nuestros esfuerzos en actividades maliciosas, deberíamos enfocarnos en aprender cómo defender nuestras redes y sistemas de estos ataques. El papel de un profesional de la ciberseguridad es proteger y defender, no atacar. Al utilizar herramientas como Wireshark de manera ética y responsable, podemos contribuir a un entorno digital más seguro y confiable.

En resumen, el valor real de aprender sobre herramientas de análisis de red como Wireshark radica en mejorar nuestras capacidades defensivas, fortaleciendo así la seguridad de nuestras propias infraestructuras y contribuyendo positivamente al campo de la ciberseguridad.

Referencias.

Video de la Tutoria 1.

https://academiaglobal-mx.zoom.us/rec/share/Dw_ZpEByC2X1lOO42AFV2z1i-XoahDqjpPsIjgdXLh_mvDf-H2fGuOfW7jfR8YhA.RO_xAp7BfCo665ju