INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE OCCIDENTE

Departamento de Electrónica, Sistemas e Informática

Desarrollo Tecnológico y Generación de Riqueza Sustentable

PROYECTO DE APLICACIÓN PROFESIONAL (PAP)

ITESO, Universidad Jesuita de Guadalajara

PAPN01B - PAP PROGRAMA DE LA INDUSTRIA DE ALTA TECNOLOGÍA II

SOCIALTIC

PRESENTA

Alumno: IC, ANA CRISTINA ZALDÍVAR SANROMÁN
Carrera: Ingeniería en Ciberseguridad

Profesor PAP: Act. Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, mayo 2026

Contenido

ÍNDICE

Presentación Institucional de los Proyectos de Aplicación Profesional

Los Proyectos de Aplicación Profesional (PAP) son una modalidad educativa del ITESO en la que el estudiante aplica sus saberes y competencias socio-profesionales para el desarrollo de un proyecto que plantea soluciones a problemas de entornos reales. Su espíritu está dirigido para que el estudiante ejerza su profesión mediante una perspectiva ética y socialmente responsable.

A través de las actividades realizadas en el PAP, se acreditan el servicio social y la opción terminal. Así, en este reporte se documentan las actividades que tuvieron lugar durante el desarrollo del proyecto, sus incidencias en el entorno, y las reflexiones y aprendizajes profesionales que el estudiante desarrolló en el transcurso de su labor.

Resumen

Este reporte PAP describe y documenta el proceso de realización de mi segundo proyecto académico-profesional desarrollado en la empresa SocialTIC, una organización con sede en la Ciudad de México que se enfoca en el uso de la tecnología para la defensa de los derechos humanos y la justicia social. A través de este proyecto, se busca aplicar y ampliar los conocimientos adquiridos durante mi formación académica, específicamente en el área de seguridad informática y análisis de amenazas digitales.

Mi primer proyecto PAP fue realizado en conjunto con un profesor del ITESO y estuvo enfocado en un proyecto de investigación relacionado con la criptografía postcuántica. Dicho proyecto tenía un carácter principalmente teórico y de investigación, orientado al análisis de algoritmos criptográficos resistentes a ataques realizados por computadoras cuánticas. En contraste, el segundo proyecto PAP presenta un enfoque más práctico y aplicado, ya que se centra en el análisis de malware en dispositivos móviles con sistema operativo Android, una de las plataformas más utilizadas a nivel mundial.

El origen de este proyecto se dio a partir de contactos profesionales que realicé durante una estancia en Colombia, donde tuve la oportunidad de conocer a un representante de una organización social dedicada a concientizar a personas de bajos recursos sobre los riesgos asociados al uso de internet y la exposición de datos personales. Al compartirle mi interés en temas de ciberseguridad y protección de la información, surgió la posibilidad de colaborar con SocialTIC, organización que posteriormente me presentó el proyecto y con la cual se inició el proceso administrativo y académico para su validación como PAP2.

El proyecto desarrollado con esta ONG consiste en analizar, desarrollar y recrear una posible línea de ataque hacia un dispositivo Android, con el objetivo de comprender a profundidad el funcionamiento de distintas vulnerabilidades, técnicas de explotación y métodos utilizados por el malware móvil. El propósito final del proyecto es la elaboración de un documento detallado y comprensible que explique cómo operan estos ataques, con el fin de generar conciencia sobre los riesgos que implica la falta de medidas adecuadas de seguridad de la información y promover mejores prácticas de protección digital entre la población.

1. Introducción

1.1 Antecedentes

La organización en la que estoy haciendo mi proyecto PAP es Social TIC. Es una organización sin fines de lucro que busca capacitar e informar a las personas sobre ciberseguridad y seguridad de la información y datos personales.

Su misión es “SocialTIC existe para empoderar de manera segura a actores de cambio en América Latina reforzando sus acciones de análisis, comunicación social e incidencia a través del uso estratégico de tecnologías digitales y datos”

Y su visión es: “Que los actores de cambio entiendan su contexto digital y que tengan las capacidades para utilizar estratégicamente y de manera segura las diversas herramientas tecnológicas para analizar, comunicar, incidir y fomentar la participación cívica relacionada con su propia causa y contexto local.

Que existan ecosistemas Latinoamericanos en donde se viva una colaboración multidisciplinaria, se ofrezcan de servicios y tecnologías cívicos, se brinde entrenamiento de tecnología digital para acciones de cambio social y se apoyen las necesidades de seguridad y privacidad digital”

1.2 Justificación

Entre las razones que me motivan para trabajar en este proyecto está que esta es el área de la ciberseguridad que más me llama la atención. Desde que comencé la carrera supe que quería hacer una especialidad en forense digital y ahora tuve la oportunidad de trabajar un rato en esto y ver si realmente es para mi y si es todo lo que yo esperaba.

1.3 Objetivos

Objetivo del proyecto y de la empresa huésped:

El propósito de la empresa huésped al desarrollar este proyecto es fortalecer sus capacidades de análisis y comprensión de amenazas de seguridad en dispositivos móviles Android, particularmente en lo relacionado con la identificación de comportamientos maliciosos, riesgos para la privacidad y posibles vectores de ataque. A través del proyecto, la organización busca generar conocimiento técnico que contribuya a la protección de usuarios y al fortalecimiento de prácticas de seguridad digital.
El entregable principal del proyecto consiste en la documentación técnica del análisis de aplicaciones Android, incluyendo la identificación de comportamientos sospechosos o maliciosos, el uso de herramientas de análisis y la sistematización de resultados que puedan ser reutilizados en proyectos similares.

Objetivos personales de aprendizaje profesional:

Durante el desarrollo del Proyecto PAP, mis objetivos de aprendizaje profesional se centran en fortalecer mis conocimientos técnicos en ciberseguridad, particularmente en el análisis de malware y vulnerabilidades en sistemas Android, así como en el uso de herramientas especializadas para análisis estático, dinámico y forense.
Asimismo, busco desarrollar un perfil profesional con mayor autonomía técnica, capacidad de investigación, pensamiento crítico y habilidades para documentar y comunicar resultados técnicos de forma clara y estructurada.

1.4 Contexto

El proyecto en el que participo corresponde principalmente a un proyecto de Investigación y Desarrollo, enfocado en el análisis de malware y amenazas de seguridad en dispositivos móviles Android. Este tipo de proyecto busca generar conocimiento técnico, metodologías de análisis y evidencia que pueda ser utilizada para la concientización, prevención y fortalecimiento de la seguridad digital.

El proyecto está orientado a usuarios, organizaciones y colectivos interesados en la seguridad y privacidad digital, con beneficios que pueden extenderse a nivel nacional e incluso regional, al tratarse de problemáticas comunes en el uso de dispositivos móviles.

Dentro de la empresa, mi rol corresponde al de practicante, participando activamente en tareas técnicas bajo la supervisión de un líder técnico. Mis funciones incluyen el apoyo en actividades de investigación, análisis de aplicaciones Android, ejecución de pruebas controladas, documentación de hallazgos y elaboración de reportes técnicos relacionados con el proyecto.

1.5 Inventario de Competencias

Materia	PAP1 DESI	**Semestre**	2016V
Profesor	Juan Manuel Islas	**Carrera:**	IC

Alumno:	Ana Cristina Zaldívar Sanromán
Puesto:	**Practicante**

Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	Proactividad en investigación y autoaprendizaje técnico					
1.1	Búsqueda autónoma de información técnica	4	3	1	4	M
1.2	Análisis crítico de documentación técnica	4	3	1	4	M
2	Comprensión lectora técnica					
2.1	Lectura de documentación y papers técnicos	4	3	1	4	B
3	Diseño y gestión de proyectos y actividades					
3.1	Planeación y seguimiento de tareas técnicos	5	4	1	5	M
4	Manejo de sistemas tipo UNIX					
4.1	Uso básico del sistema y navegación	2	1	1	2	A
4.2	Manejo de terminal y comandos esenciales	2	1	1	2	A
5	Scripting y programación					
5.1	Automatización de tareas	4	2	2	4	A
	Desarrollo de scripts para análisis técnico	4	2	2	4	A

6	Pentesting y análisis de vulnerabilidades					
6.1	Identificación de vulnerabilidades comunes	3	1	2	3	A
7	Arquitectura de computadoras y sistemas operativos					
7.1	Comprensión del funcionamiento del ISO	4	2	2	4	M
8	Arquitecturas cliente-servidor					
8.1	Comunicación entre servicios y sistemas	3	1	2	3	M
9	Explotación básica de sistemas de cómputo					
9.1	Comprensión de vectores de ataque	3	1	2	3	A
10	Forense digital					
10.1	Análisis básico de evidencias digitales	3	2	1	3	A
11	Ecosistema de software libre y código abierto					
11.1	Uso y comprensión de herramientas FOSS	3	2	1	3	M
12	Escritura y redacción de reportes técnicos					
12.1	Documentación técnica estructurada	4	3	1	4	B
13	Habilidades orales y de presentación técnica					
13.1	Exposición de resultados técnicos	4	3	1	4	B

1.6 Plan Educativo

No.	Actividad principal	Competencias asociadas	Semanas
1	Inducción al proyecto, lineamientos y acuerdos de confidencialidad	1, 2, 3	1
2	Revisión teórica de malware móvil y seguridad en Android	1, 2, 7	1 – 2
3	Familiarización con entorno de trabajo UNIX	4	2 – 3
4	Estudio del ecosistema Android y arquitectura cliente-servidor	7, 8	3 – 4
5	Uso inicial de herramientas de análisis de malware Android	4, 11	4 – 5
6	Introducción al análisis estático de aplicaciones Android	5, 6	5 – 7
7	Introducción al análisis dinámico en	6, 9	7 – 9

	entornos controlados		
8	Desarrollo de scripts de apoyo al análisis técnico	5	8 – 10
9	Análisis de comunicación y comportamiento de red	8, 6	9 – 11
10	Introducción al análisis forense digital básico	10	10 – 12
11	Ejecución de análisis completos de muestras seleccionadas	6, 9, 10	11 – 13
12	Documentación técnica de hallazgos	12	12 – 14
13	Presentación de avances y retroalimentación	13, 3	14
14	Integración de resultados finales	3, 12	15
15	Cierre del proyecto y reflexión académica	1, 12	16

1.7 Entregables

- Cadena de ataque explotando vulnerabilidades de dispositivos móviles Android
- Documento donde se registre todo el proceso de investigación y explotación
- Diseñar recomendaciones técnicas

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

PROCESO	Num. Aprox. Horas
INICIO	20
PLANEACIÓN	30
EJECUCIÓN	120
SEGUIMIENTO Y CONTROL	40
CIERRE	20

2.2 Sustento Teórico y Metodológico

El desarrollo del proyecto se sustenta en principios teóricos relacionados con la seguridad informática, el análisis de malware y la seguridad en sistemas operativos móviles, particularmente Android. Desde el punto de vista teórico, se consideran conceptos como malware móvil, ingeniería inversa, análisis estático y dinámico, permisos en Android, así como modelos de amenazas en dispositivos móviles.

En cuanto a la metodología, la empresa utiliza una combinación de procedimientos técnicos propios y metodologías comúnmente empleadas en la industria de la ciberseguridad para el análisis de software malicioso. Estas metodologías no se describen de manera detallada por motivos de confidencialidad; sin embargo, de forma general, el proceso seguido incluye:

- Recolección y clasificación de muestras.
- Análisis estático del código de aplicaciones Android.
- Análisis dinámico mediante entornos controlados
- Identificación de comportamientos maliciosos y vectores de ataque.
- Documentación técnica de hallazgos.

Para la administración y seguimiento del proyecto, se emplean prácticas inspiradas en metodologías ágiles, principalmente para organizar el trabajo, priorizar tareas y dar seguimiento al progreso. Es importante señalar que dichas metodologías se utilizan como herramientas de gestión y control del proyecto, y no como procedimientos directos para la generación de los entregables técnicos.

De esta manera, el proyecto integra un enfoque metodológico mixto, donde las metodologías ágiles apoyan la coordinación y seguimiento, mientras que los procedimientos técnicos especializados permiten la producción de los resultados relacionados con el análisis de malware en dispositivos Android.

2.3 Descripción del Proyecto

Dentro de la organización se cuenta con un equipo de seguridad digital que realiza actividades de respuesta a incidentes y forense digital.

El proyecto de este PAP contribuirá a los fines de investigación forense para la detección de spyware avanzado en Android, la cual se utiliza para el apoyo a periodistas, activistas y personas defensoras de derechos, y para compartir con otros equipos de investigación en ciberseguridad.

Algunos de los recursos más importantes de este proyecto son las herramientas y software de emuladores y para hacer análisis forense de dispositivos. Entre las herramientas que más usamos está Android QF que un software de análisis de malware para usar MVT que es otra herramienta, y emuladores de Android para hacer pruebas.

2.4 Objetivos del Proyecto

Los objetivos del proyecto son diseñar o replicar cadenas de ataque basadas en vulnerabilidades conocidas en Android que simulen el ataque de un spyware.

Los objetivos que debe cumplir el alumno son las siguientes:

- Diseñar una cadena de ataque basada en vulnerabilidades de Android conocidas.
- Implementar una prueba de concepto de la cadena de ataque para vulnerar un dispositivo Android.
- Documentar los impactos de la cadena de ataque en el dispositivo desde una perspectiva forense.
- Diseñar recomendaciones técnicas para la prevención y mitigación de ataques con spyware en Android.

2.5 Plan de Trabajo

No.	Competencia	Nivel Adquirido al Inicio	Nivel Objetivo al final PAP	Objetivo final PAP	Prior
1	Proactividad en investigación y autoaprendizaje técnico	3	4	4	M
2	Comprensión lectora técnica	3	4	4	B
3	Diseño y gestión de proyectos y actividades	4	5	5	M
4	Manejo de sistemas tipos UNIX	1	2	2	A
5	Scripting y programación	2	4	4	A
6	Pentesting y análisis de vulnerabilidades	1	3	3	A
7	Conocimiento de arquitectura de computadoras y sistemas operativos	2	4	4	M

8	Conocimiento de arquitecturas y sistemas tipo cliente-servidor o similares	1	3	3	M
9	Conocimientos básicos de explotación de sistemas de cómputo	1	3	3	A
10	Conocimientos básicos de forense digital	2	3	3	A
11	Conocimientos básicos del ecosistema de software libre y de código abierto.	2	3	3	M
12	Escritura y redacción de reportes técnicos	3	4	4	B
13	Habilidades orales y de presentación técnica	3	4	4	B

2.6 Equipo de Trabajo

Rol	*Responsabilidad*	*Nombre (opcional)*
Practicante	*Hacer una línea de ataque explotando las vulnerabilidades elegidas*	*(todos los que estamos llevando este PAP)*
Jefe y encargado	*Guiar y ponernos actividades y objetivos semanales*	*Paul Aguilar*

2.7 Plan de Comunicaciones

Emisor	Mensaje	Receptor	Medio	Frecuencia
Ana Cristina	*Reportes y entregables*	*Paul Aguilar*	*Signal*	*Semanal*

2.8 Plan de Calidad

Emisor: Quién Entrega	Entregable: Qué Entrega	Receptor: Quién Inspecciona	Criterios: Condiciones de Aceptación	Siguiente paso: Donde va cuando se Autoriza.
Ana Cristina	*Línea de ataque*	*Paul Aguilar*	*Que funcione y tenga sentido*	*NA*

2.9 Seguimiento y Control

El seguimiento del proyecto se hace cada semana en una junta de una hora con nuestro jefe directo, no tenemos contacto con nadie más de la empresa entonces es muy sencillo en las sesiones de seguimiento y control

2.10 Cierre del Proyecto

El proyecto termina al momento de presentar las tres vulnerabilidades explotadas y un reporte explicando cómo es que lo hicimos y toda la justificación forense.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

A continuación, se presentan los principales entregables generados durante la participación en el proyecto:

1. Reporte de análisis de vulnerabilidades: Documento técnico en el que se describen las vulnerabilidades evaluadas, incluyendo su identificación mediante códigos CVE, el análisis de su aplicabilidad en el dispositivo y la justificación técnica correspondiente.
2. Resultados de pruebas de validación: Evidencia obtenida mediante el uso de herramientas como ADB y pruebas manuales, que permiten verificar la existencia o ausencia de vulnerabilidades específicas en el dispositivo analizado.
3. Matriz de compatibilidad de vulnerabilidades: Tabla comparativa donde se clasifica cada vulnerabilidad en función de si afecta o no al dispositivo, considerando factores como versión del sistema operativo, nivel de parche de seguridad y configuraciones del sistema.
4. Documentación técnica de procedimientos: Guía detallada de los pasos realizados durante el análisis, incluyendo comandos utilizados, configuraciones necesarias y metodología aplicada para replicar las pruebas
5. Conclusiones y recomendaciones de seguridad: Apartado en el que se sintetizan los hallazgos más relevantes del análisis, así como sugerencias para mitigar riesgos o mejorar la postura de seguridad del dispositivo.

3.2 Estimación del Impacto

Los entregables generados en este proyecto tienen el potencial de ser utilizados en diversos contextos relacionados con la ciberseguridad, especialmente en la evaluación de dispositivos móviles que operan bajo el sistema Android. Su aplicación puede extenderse a entornos educativos, donde sirve como material de aprendizaje, así como en escenarios profesionales donde se requiere validar la seguridad de dispositivos antes de su uso en redes corporativas.

A nivel organizacional, estos productos pueden contribuir a mejorar los procesos de análisis de vulnerabilidades, permitiendo una identificación más precisa de riesgos y facilitando la toma de decisiones informadas respecto a la actualización, mantenimiento o reemplazo de dispositivos. Además, la documentación generada puede servir como base para la estandarización de metodologías de evaluación de seguridad.

En un contexto más amplio, el proyecto aporta a la concientización sobre la importancia de mantener actualizados los dispositivos y comprender las implicaciones de las vulnerabilidades reportadas mediante identificadores CVE. Esto resulta especialmente relevante en un entorno donde los dispositivos móviles son ampliamente utilizados para actividades personales y profesionales, y donde la seguridad de la información es un aspecto crítico.

4. Aprendizajes del alumno

4.1 Aprendizajes Profesionales

En cuanto a competencias técnicas, las más significativas fueron:

- Análisis de vulnerabilidades en sistemas Android, entiendo cómo interpretar CVEs y validar si realmente aplican en un dispositivo
- Uso de herramientas como ADB, que me permitió interactuar directamente con el sistema y obtener información relevante para el análisis
- Interpretación de evidencia técnica, algo muy relacionado con el forense digital, ya que no solo se trata de encontrar datos sino de entender qué significan.
- Documentación técnica, aprendiendo a justificar cada resultado y no solo reportarlo
- Pensamiento crítico aplicado a ciberseguridad, especialmente para descartar falsos positivos

En cuanto a habilidades blandas, creo que crecí bastante en:

- La paciencia y tolerancia a la frustración, porque muchas pruebas no salían como esperaba.
- La autonomía, ya que muchas veces tuve que investigar por mi cuenta
- La organización del trabajo, sobre todo para documentar todo de forma clara
- La capacidad de análisis, que fue clave durante todo el proyecto

Algo que me sorprendió fue darme cuenta de que, aunque existen muchas vulnerabilidades reportadas, no todas son aplicables en la práctica. También entendí mejor cómo factores como las actualizaciones y parches de seguridad influyen directamente en la exposición al riesgo.

Por otro lado, sí hubo momentos en los que sentí que me faltaban bases más sólidas en temas como análisis profundo de sistemas Android o metodologías más formales de testing, lo cual me hizo ver áreas en las que necesito seguir preparándome.

Finalmente, considero que ahora tengo una mejor idea de cómo desarrollar un proyecto técnico desde cero. Aún no me siento completamente lista para liderar uno grande, pero definitivamente con más práctica y experiencia podría hacerlo en un futuro cercano.

4.2 Aprendizajes Sociales

Este proyecto aporta principalmente a la concientización sobre la seguridad en dispositivos móviles, algo que hoy en día impacta directamente a la sociedad, ya que prácticamente todos usamos smartphones para actividades personales y laborales.

Considero que los principales beneficiados son:

- Usuarios de dispositivos móviles, que pueden entender mejor los riesgos
- Estudiantes y personas interesadas en ciberseguridad, como material de aprendizaje
- Organizaciones que necesitan evaluar la seguridad de sus dispositivos

Aunque el proyecto es académico, sí genera un bien público, ya que la información sobre vulnerabilidades y buenas prácticas puede ser compartida y utilizada por otras personas.

También creo que este tipo de trabajo puede ayudar a largo plazo a mejorar la cultura de seguridad digital, lo cual tiene impacto tanto social como económico, ya que previene pérdidas de información y posibles ataques.

En lo personal, este proyecto sí cambió un poco mi forma de ver la seguridad, antes pensaba más en teoría, y ahora entiendo mejor cómo se aplica en la vida real.

4.3 Aprendizajes Éticos

En este proyecto, uno de los aspectos más importantes fue mantener la honestidad en los resultados. En ciberseguridad, es muy fácil caer en la tentación de exagerar hallazgos o asumir que algo es vulnerable sin tener evidencia suficiente, pero aprendí que es fundamental respaldar todo con pruebas.

También reflexioné sobre el manejo de la información, ya que trabajar con vulnerabilidades implica una responsabilidad importante. Aunque en este caso fue un entorno controlado, es claro que en un contexto real el uso indebido de esta información podría generar daños.

No identifiqué conflictos directos entre mis valores personales y el trabajo realizado, pero sí entendí que en el ámbito profesional pueden existir situaciones donde lo técnico y lo ético no siempre coinciden, por ejemplo, al manejar datos sensibles o al reportar fallas de seguridad.

Sobre el uso de inteligencia artificial, considero que es una herramienta muy útil para apoyar en análisis y documentación, pero también es importante usarla con criterio, verificando siempre la información.

En general, esta experiencia me ayudó a reforzar la importancia de actuar con responsabilidad, especialmente en un campo como la ciberseguridad.

4.4 Aprendizajes Personales

A nivel personal, este proyecto me ayudó a desarrollar más confianza en mis habilidades, especialmente en temas técnicos que antes me parecían más complicados.

También noté cambios en mi forma de trabajar, ya que ahora soy más organizada y más consciente de la importancia de documentar todo. En cuanto a mis relaciones, creo que aprendí a ser más paciente y a trabajar mejor de forma independiente.

Definitivamente, esta experiencia me dio más seguridad en mis decisiones y en la forma en la que enfrento problemas técnicos.

También considero que me ayudó a conocer mejor mis fortalezas y debilidades, lo cual es muy importante en esta etapa antes de entrar al mundo laboral.

4.5 Tareas Aprendidas

Factores que influyeron positivamente:

- La constancia durante el desarrollo del proyecto.
- La investigación autónoma.
- La correcta documentación de cada paso.
- El uso de herramientas adecuadas para las pruebas.
- La disposición para aprender de errores.

Aspectos que se pudieron mejorar:

- Profundizar más en algunos conceptos desde el inicio.
- Planear mejor los tiempos de ejecución.
- Validar más rápido ciertas hipótesis para no perder tiempo.
- Buscar más apoyo cuando surgían dudas complejas.

Estos puntos son importantes porque me ayudan a identificar qué debo repetir y qué debo mejorar en futuros proyectos.

4.6 Desarrollo Profesional

Este proyecto reforzó mucho mi interés en el área de ciberseguridad, especialmente en el campo del forense digital, ya que disfruté mucho la parte de análisis e interpretación de información.

1. Tareas tecnológicas de interés:
    a. Análisis forense en dispositivos móviles.
    b. Investigación de incidentes de seguridad.
    c. Análisis de vulnerabilidades.
2. Áreas tecnológicas con mayor destreza:
    a. Uso básico-intermedio de herramientas como ADB.
    b. Análisis de sistemas Android.
    c. Documentación técnica.
3. Áreas del mercado con mayor crecimiento:
    a. Ciberseguridad.
    b. Forense digital.
    c. Análisis de incidentes.
4. Rol que pretendo alcanzar:
    a. Me gustaría comenzar como analista de ciberseguridad o forense digital en el corto plazo (1–2 años).
5. Factores que justifican este objetivo:
    a. Alta demanda en el área.

b. Interés personal en la investigación digital.
c. Posibilidad de crecimiento profesional.

6. Tendencias del mercado:
    a. El crecimiento de ataques informáticos y el uso masivo de dispositivos móviles hacen que el forense digital sea cada vez más relevante, tanto a nivel nacional como global.
7. Estrategia para alcanzar el objetivo:
    a. Seguir formándome en ciberseguridad.
    b. Practicar en plataformas como TryHackMe.
    c. Obtener certificaciones.
    d. Desarrollar más proyectos prácticos.
    e. Mantenerme actualizada en tendencias del área.

5. Conclusiones

En general, este proyecto fue una experiencia bastante completa, ya que no solo implicó aplicar conocimientos técnicos de ciberseguridad, sino también desarrollar habilidades de análisis, documentación y reflexión. El hecho de tener que documentar todo el proceso me ayudó a entender mejor lo que estaba haciendo, ya que no es lo mismo realizar pruebas que explicarlas y justificarlas de manera clara.

Además, este ejercicio de documentación resulta muy útil pensando en una presentación formal del proyecto, porque permite identificar fácilmente los puntos más importantes, los hallazgos clave y el proceso que se siguió. Esto facilita comunicar la experiencia de forma más estructurada ante profesores, compañeros o incluso en un entorno profesional.

Durante el desarrollo del PAP también surgieron situaciones imprevistas, como pruebas que no daban los resultados esperados o dificultades para validar ciertas vulnerabilidades. Aunque en su momento fueron frustrantes, terminaron siendo de las experiencias más valiosas, ya que me obligaron a investigar más, cuestionar resultados y no asumir cosas sin evidencia. Estas son habilidades que definitivamente me van a servir en el futuro, especialmente si quiero dedicarme al área de forense digital.

En cuanto al nivel de satisfacción, considero que fue alto. El proyecto sí representó un reto, especialmente por la parte técnica y la necesidad de ser muy precisa en los resultados, pero el esfuerzo valió la pena al ver todo lo que logré al final. Me quedo con la sensación de haber aprendido cosas que realmente son útiles para mi desarrollo profesional.

Finalmente, creo que una posible mejora para este tipo de proyectos sería contar con una guía más clara desde el inicio sobre las metodologías de análisis o ejemplos más prácticos, ya que eso ayudaría a optimizar tiempos y a enfocar mejor el trabajo desde etapas tempranas. Aun así, la experiencia fue muy enriquecedora y me ayudó a tener una visión más real de lo que implica trabajar en el área de ciberseguridad.

6. Bibliografía y Anexos

- Google Project Zero. (2022). A very powerful clipboard: Samsung in-the-wild exploit chain. Recuperado de https://projectzero.google/2022/11/a-very-powerful-clipboard-samsung-in-the-wild-exploit-chain.html
- DEV Community. (2023). How to make a simple flash light Android app (step by step detailed guide with code). Recuperado de https://dev.to/dhruvjoshi9/how-to-make-a-simple-flash-light-android-app-step-by-step-detailed-guide-with-code-4coo