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)

PAP4N01 PROGRAMA DE LA INDUSTRIA DE ALTA TECNOLOGIA II,

IT LEGAL SERVICES

PRESENTA

Alumno: ISI MARIO GALVEZ ORTIZ

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

Tlaquepaque, Jalisco, mayo de 2022.

ÍNDICE

Contenido

REPORTE PAP

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

El documento presentado tiene como finalidad reportar las actividades, tareas y procesos que se llevaron a cabo para completar el proyecto de análisis técnico de una incidencia informática, adicional a esto, existe un entregable en el que se hace más énfasis, este se trata del desarrollo de una herramienta forense de geolocalización que es necesario obtener para aportar información relevante al caso en que se estará trabajando.

Se utilizó una metodología de cascada en la que el objetivo sea tener una herramienta de geolocalización que se pueda utilizar mediante técnicas diversas incluyendo phishing, esta metodología es eficiente ya que al dividir el proyecto en procesos secuenciales se puede obtener una buena documentación estructurada y concisa, así mismo se realizaron las investigaciones necesarias durante todo el proceso para poder obtener los recursos teóricos y prácticos que sean relevantes a cada etapa.

Se planearon los entregables desde el primer levantamiento y se plasman a detalle y con fechas asignadas en el presente documento.

1. Introducción

1.1 Antecedentes

La empresa huésped se llama “IT Legal services”, es una firma especializada en temas de derecho informático y cibercriminalidad que cubre el ciclo legal, técnico y forense en problemáticas tecno-legales.
El mercado de la empresa es amplio cubriendo incidentes desde personas particulares, hasta grandes empresas de renombre e incluso de gobierno, enfocándose principalmente en México.

1.2 Justificación

Los proyectos en los que ITLS tienen como motivación ayudar a empresas o particulares con incidentes o ataques informáticos en los que son inexpertos y que cada vez son más recurrentes, esta empresa al tener dos partes (legal, técnica) hace que sea necesaria un área especializada y enfocada en los temas de ciberseguridad, mientras se trata la parte legal a la par.

En cuanto a mi motivación para intervenir con este proyecto, creo que la ciberseguridad siempre va a estar ligada a los aspectos legales y en esta empresa se puede aprender de ambas partes mientras se ayuda a combatir estos incidentes en busca de respuestas y justicia para las partes afectadas.

Habiendo dicho la importancia del proyecto, es necesario que me prepare de la manera adecuada y me esfuerce por apoyar con el proyecto que se lleve a cabo teniendo las precauciones necesarias en todo momento.

Creo que este sector tecno-legal tiene mucho potencial tomando en cuenta que no hay muchos peritos especializados en ciberseguridad en México, veo mucha oportunidad de crecimiento y desarrollo profesional ya sea participando en proyectos de este tipo como empleado y quizá en algún futuro creando una empresa que ofrezca estos servicios profesionales.

1.3 Objetivos

El principal y más importante objetivo del proyecto es poder evidenciar una incidencia o ciberataque de la empresa afectada hasta llegar a presentar de manera legal una denuncia contra los responsables de dicho ataque, para esto se requiere de un análisis técnico profundo y análisis forense de los equipos/servicios/plataformas involucradas.

Personalmente busco aprender a cerca de técnicas tanto de “penetration testing” como de informática forense y de manera secundaria aprender cómo se pueden presentar las evidencias para poder llegar a una solución legal para la empresa afectada.

Contexto

Este proyecto cabe en el área legal y en el área de informática forense y puede categorizarse como respuesta a una solicitud explicita de un cliente al ser un contexto especifico con un cierto incidente.

Mi rol en el proyecto será de becario con la tarea de asistir a las instalaciones de ITLS para poder realizar las actividades de análisis post-incidente y asistencia técnica con el material que nos otorguen para analizar, así mismo para poder apoyar de una manera optima será necesario tomar un curso en el cual se nos enseñe a utilizar técnicas y herramientas pertinentes a la ciberseguridad y análisis forense.

Entregables

Los principales entregables serán:

- Herramienta de geolocalización
- Laboratorios de practica resueltos (Entrenamiento)
- Certificado de curso CEH v11
- Registro de avances en el caso

El tipo de cliente al que se enfocará el proyecto es una empresa con recursos informáticos comprometidos, por lo que los beneficios de este proyecto se espera que tengan un alcance que impacte hasta los usuarios de dichos servicios informáticos.

Involucrados

Cliente externo: -
Responsable de la empresa ITSL: Carlos Gonzales Durón
Responsable PAP ITSL: Carlos Gonzales Durón
Instructor de curso CEH: Roberto Martínez
Rol que ejerce el alumno durante el proyecto: Becario en seguridad informática

2. Desarrollo del Proyecto PAP
2.1 Administración del Proyecto

Inicio: Primeramente, se debe tomar el curso CEH impartido por Roberto, el cual nos dará las herramientas y la preparación teórica y práctica para poder aportar en el análisis del futuro caso presentado.

Posterior a este curso, aplicando los conocimientos obtenidos se busca poder encontrar información relevante al caso analizando los activos informáticos comprometidos.
Planificación: La empresa se contacta con ITSL para realizar el levantamiento inicial, aclarar la situación y el contacto inicial, se habla de posibles fechas y resultados con los servicios ofrecidos, así como estimados de tiempo y precio.

Ejecución: En caso de aceptar los términos por ambas partes, se inicia por pedir los activos involucrados, recolección de evidencias, después se crean laboratorios en ambientes seguros con la información recabada para no afectar los activos y posteriormente se inicia con el análisis forense y obtención de datos relevantes para incluir en el reporte de evidencias.

Seguimiento y control: Se actualiza el reporte de evidencias conforme pasa el tiempo y se evalúan los activos, se reportan avances con el cliente.
Cierre: se entrega el reporte completo, así como las propuestas tanto de seguridad informática como las legales en caso de haber una solución o proceso que se pueda seguir.

2.2 Sustento Teórico y Metodológico

En este proyecto se seguirá la metodología de análisis forense aplicado al ataque informático, esta metodología consiste en 7 etapas que se listan a continuación:

Evaluación de la situación: Se informa a cerca del contesto de la empresa y el incidente
Identificación de la evidencia: Se adquiere conocimiento a cerca de los activos afectados y sus componentes.

Adquisición de la evidencia: Se reciben los activos físicos afectados, se realizan copias bit a bit de los sistemas de almacenamiento para poder analizar la información en un laboratorio con equipos y herramientas propios.

Preservación de la evidencia: Se etiqueta, fotografía y resguarda el hardware obtenido.

Análisis de la evidencia: Se usan herramientas forenses para analizar y evaluar los daños causados por el incidente.

Presentación del informe: en base a los resultados de la fase anterior se realiza un reporte o informe detallado de las causas y daños.

Devolución de la evidencia: una vez terminado el proceso se hace devolución de los activos que se proporcionaron

2.3 Descripción del Proyecto

Primeramente, se tomará el curso CEH impartido por Roberto que tiene como objetivo darnos el conocimiento necesario para poder apoyar en el análisis del caso.

Posteriormente se deberá brindar asistencia al director del proyecto realizando las primeras 5 fases de la metodología a utilizar, es decir, se avaluará la situación y ayudaremos a discutir y observar el contexto tanto de la empresa cliente como de sus activos y el incidente informático.

Después se deberá identificar la evidencia es decir los activos afectados, así como sus servicios tomando en cuenta la infraestructura con la que se cuenta.

Una vez identificados, se realiza la obtención de datos e infraestructura de los activos, esto se puede hacer de diversas maneras, pero principalmente usando software como autopsy para clonar los dispositivos de almacenamiento y así poder analizarlos sin afectar los originales ni modificar su estado actual.

Después de obtener estos datos, se etiquetan y resguardan los activos en un área segura con sus respectivas etiquetas y fotografías del estado físico del hardware.

A la par de estos procesos, debemos desarrollar una herramienta llamada “sistema forense de geolocalización”, esta herramienta buscamos que pueda obtener la localización geográfica de un dispositivo a través de “phishing” logrando ejecutar un script dentro del dispositivo objetivo que verifique si el GPS del mismo esta activado, en caso de que no, este se deberá activar y mandar la geolocalización, se debe crear la herramienta para que funcione en línea y automatizado para usarla en futuros casos.

Estas etapas dependen de la anterior en caso de los pasos de la metodología forense, sin embargo, el desarrollo de la herramienta de geolocalización se puede ir desarrollando a la par, tomando en cuenta que se necesita cierto conocimiento que se adquiere gracias al curso inicial CEH, por lo que una vez obteniendo el conocimiento se podrá ir desarrollando para obtener pruebas del resultado lo antes posible.

En el caso de la herramienta será necesario conocimiento a cerca de scripting y dispositivos móviles y en caso del análisis forense se necesita conocimiento tanto de redes y telecomunicaciones como de hardware y software de análisis como autopsy y diversas herramientas incluidas en “Tsurugi”.

Las competencias que se desarrollan son de distintos indoles, incluyendo competencias técnicas como evaluación de activos y hardware, análisis de información y datos, así como registros de logs y el “footprint” digital, utilización de software forense, realización de scripts, desarrollo de phishing personalizado, desarrollo móvil Android/IOS.

Alumno:	Mario Gálvez Ortiz	**Carrera:**	ISI
Empresa:	IT legal services		
Proyecto:	Analisis de incidencias y desarrollo de herramienta geolocalizacion		

Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	**Scripting**	5	2	3	3	A
1.1	Python	4	2	2	3	A
1.2	JavaScript	4	3	1	4	A
1.3	PHP	3	2	1	3	m
2	**Software forense**	4	3	1	4	A
2.1	Magnet forenscic	4	3	1	4	A
2.2	Volatility	3	3	0	4	A
2.3	pwdump	4	2	2	3	B
3	**Clonacion dispositivos de almacenamiento**	4	4	0	4	M
3.1	Autopsy	4	4	0	4	A
3.2	Magnet forenscic	3	2	1	4	M
4	**Phishing**	5	4	1	4	A
4.1	Linux phishing tools	5	3	2	4	A
4.2	Montado de servidor	4	4	0	4	M
4.3	Scripting	4	2	2	3	M
5	**Desarrollo movil**	5	1	4	3	A
5.1	Desarrollo Movil Android	5	1	4	3	A
5.2	Desarrollo Movil IOS	5	1	4	3	A

2.4 Plan de Trabajo

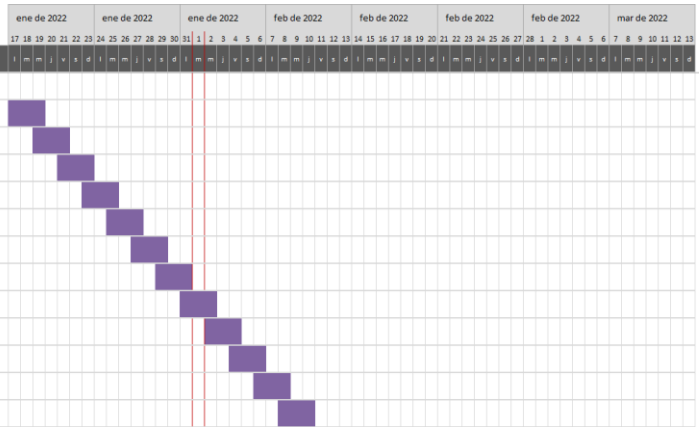
Sistema Forense de Geolocalización.

IT Legal Services

Inicio del proyecto: lun, 17/01/2022

Semana para mostrar: 1

TAREA	INICIO	FIN
Entrenamiento CEH		
Introduction to Ethical Hacking	17-1-22	19-1-22
Footprinting and Reconnaissance	19-1-22	21-1-22
Scanning Networks	21-1-22	23-1-22
Enumeration	23-1-22	25-1-22
Vulnerability Analysis	25-1-22	27-1-22
System Hacking	27-1-22	29-1-22
Malware Threats	29-1-22	31-1-22
Sniffing	31-1-22	2-2-22
Social Engineering	2-2-22	4-2-22
Denial-of-Service	4-2-22	6-2-22
Session Hijacking	6-2-22	8-2-22
Evading IDS, Firewalls, and Honeypots	8-2-22	10-2-22



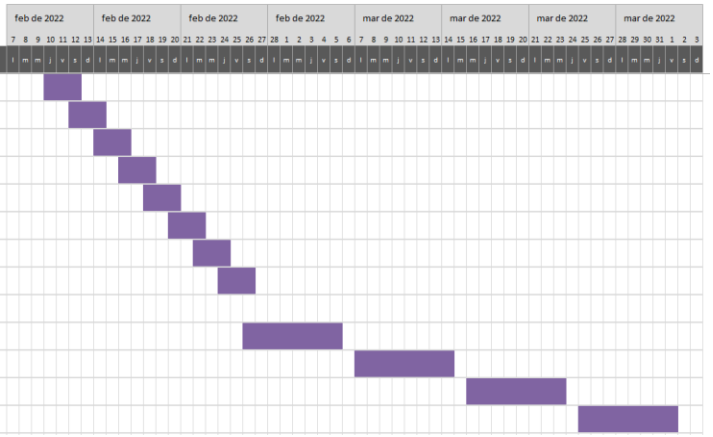
Sistema Forense de Geolocalización.

IT Legal Services

Inicio del proyecto: lun, 17/01/2022

Semana para mostrar: 4

TAREA	INICIO	FIN
Hacking Web Servers	10-2-22	12-2-22
Hacking Web Applications	12-2-22	14-2-22
SQL Injection	14-2-22	16-2-22
Hacking Wireless Networks	16-2-22	18-2-22
Hacking Mobile Platforms	18-2-22	20-2-22
IoT Hacking	20-2-22	22-2-22
Cloud Computing	22-2-22	24-2-22
Cryptography	24-2-22	26-2-22
Desarrollo de aplicación de geolocalización		
Investigación sistema Android y iOS	26-2-22	5-3-22
Pruebas de concepto	7-3-22	14-3-22
Desarrollo de scripts	16-3-22	23-3-22
Prueba práctica	25-3-22	1-4-22



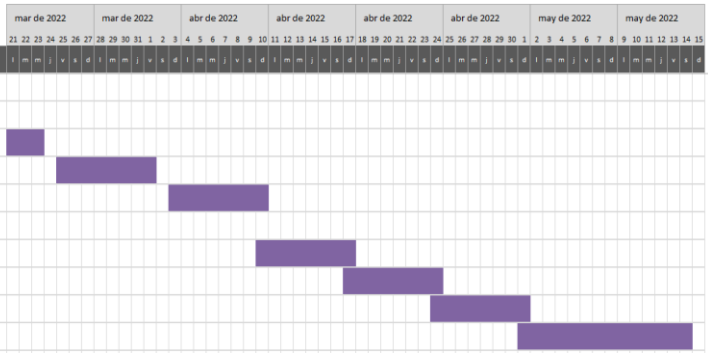
Sistema Forense de Geolocalización.

IT Legal Services

Inicio del proyecto: lun, 17/01/2022

Semana para mostrar: 10

TAREA	INICIO	FIN
Investigación sistema Android y iOS	26-2-22	5-3-22
Pruebas de concepto	7-3-22	14-3-22
Desarrollo de scripts	16-3-22	23-3-22
Prueba práctica	25-3-22	1-4-22
Documentación de resultados	3-4-22	10-4-22
Apoyo a caso real		
Análisis de caso	10-4-22	17-4-22
Planeación de estrategia	17-4-22	24-4-22
Implementación de la herramienta	24-4-22	1-5-22
Documentación de resultados	1-5-22	16-5-22



Plan de actividades educativas

Materia	PAP1- DESI	**Semestre:**	2021O
Profesor	Juan Manuel Islas	**Horario:**	Lun 16-18

Alumno:	Martín Casillas Ramos	Carrera:	ISI
PAP:	Data Center Grupo Omnilife		
Empresa:	Ingeniería en Telecomunicaciones e Informática SA de CV		

Plan de Actividades

No.	Actividad Educativa	Tipo Actividad	Prereq	Total Hrs	Fecha Inicio	Fecha Termino	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Obj
1	**Scripting**																						
1.1	Investigar y revisar la documentacion del lenguaje python para poder desarrollar scripts basicos de acuerdo a lo que se requiera	Autoestudio		1	17/1/2022	10/2/2022																	
1.2	Investigar y revisar la documentacion del lenguaje JavaScript para poder desarrollar scripts basicos de acuerdo a lo que se requiera	Autoestudio		2	24/1/2022	4/2/2022																	
1.3	Revisar y repasar el lenguaje PHP para poder evaluar aspectos de paginas web y sus funcionalidades	Autoestudio		2	1/2/2022	18/2/2022																	
2	**Software Forense**																						
2.1	Repasar el funcionamiento del software magnet forenscic y su alcance	Autoestudio		2	7/2/2022	9/2/2022																	
2.2	Repasar los comandos de volatility y sus funciones	Autoestudio		1	9/2/2022	11/2/2022																	
2.3	Revisar en que plataformas se puede utilizar pwdump y analizar si es de utilidad con la creacion de la herramienta de geolocalizacion	Autoestudio		6	16/2/2022	18/2/2022																	
3	**Clonacion dispositivos de almacenamiento**																						
3.1	Practicar el uso de la herramienta autopsy con discos de almacenamiento internos y externos	Autoestudio		3	14/2/2022	18/2/2022																	
3.2	investigar herramientas que tengan el mismo funcionamiento que autopsy pero en memorias ram y que sea bit a bit	Autoestudio	3.1	4	21/2/2022	24/2/2022																	
4	**Phishing**																						
4.1	Revisar que tipo de scripts se necesitan para realizar un ataque phishing convinvente	Autoestudio	1.1,1.2	1	27/2/2022	10/3/2022																	
4.2	Investigar a cerca de linux phishing tools y crear links de phishing en un ambiente controlado	Autoestudio	4.1	1	7/3/2022	25/3/2022																	
4.3	realizar pruebas del funcionamiento del phishing	Autoestudio	4.1, 4.2	2	14/3/2022	1/4/2022																	
5	**Desarrollo movil**																						
5.1	Investigar a cerca del desarrollo movil enfocado a sistemas Android	Autoestudio	1.1,1.2,1.3	2	4/3/2022	29/3/2022																	
5.2	Investigar a cerca del desarrollo movil enfocado a sistemas IOS	Autoestudio	1.1,1.2,1.3	2	25/4/2022	6/5/2022																	

2.5 Equipo de Trabajo

Rol	Responsabilidad	Nombre (opcional)
Director de la empresa	Dirigir y gestionar al equipo de trabajo para cumplir con las expectativas expuestas en el levantamiento del proyecto incluyendo fechas y resultados.	Carlos Gonzales Durón
Cliente externo	Proporcionar toda la información relevante tanto del caso como de la infraestructura de redes con la que se cuenta.	-
Encargado del proyecto	Ofrecer los recursos necesarios para llevar a cabo los objetivos del proyecto, así como orientar y revisar avances del mismo.	Carlos Gonzales Durón
Instructor	Capacitar a los becarios para que obtengan las competencias pertinentes al proyecto y así poder aportar valor y reducir tiempos.	Roberto Martínez
Becarios	Tomar el curso CEH par poder desarrollar una herramienta de geolocalización y poder aplicarlo al caso actual para aportar valor al mismo.	Mario Gálvez Ortiz / Martin Casillas Ramos

2.6 Plan de Comunicaciones

Emisor	Mensaje	Receptor	Medio	Frecuencia
Encargado del proyecto	Actividades que realizar	Becarios	Correo electrónico/whatsapp	Semanal
Encargado del proyecto	Información del caso	Becarios	Correo electrónico/whatsapp	Semanal
Cliente externo	Actualizaciones del caso	Director de la empresa	Correo electrónico	Cuando sea necesario
Instructor	Instrucciones y explicaciones	Becarios	En persona / whatsapp	Semanal
Director de la empresa	Actualización del progreso del caso	Cliente externo	Correo electrónico	Cuando haya información relevante

2.7 Plan de Calidad

Emisor: Quién Entrega	Entregable: Qué Entrega (Entregable)	Receptor: Quién recibe o Inspecciona	Criterios: Condiciones de Aceptación	Siguiente paso. Cuando se Autoriza.
Cliente externo	Informe con los datos relevantes del caso	Encargado del proyecto	Que sea objetivo y tenga los datos básicos del incidente (Fecha, involucrados, descripción etc.)	Director de la empresa revisa el informe y procede a seccionar las evidencias
Becario	Laboratorios montados y completados del entrenamiento	Instructor	Los ejercicios deben estar correctamente resueltos y con calificación aprobatoria	Se evalua si se debe proceder a la aplicación del examen de certificación
Becario	Pruebas de concepto y pruebas prácticas del desarrollo de la herramienta	Encargado del proyecto	Las pruebas están documentadas con los pasos que se siguió en cada una de ellas.	Encargado del proyecto analiza las pruebas y corrige en caso de ser necesario
Becario	Planeación de estrategia para utilizar la herramienta en caso real	Encargado del proyecto	La planeación tiene los permisos y restricciones normativas en orden previo a utilizarse en un ambiente real	Encargado del proyecto documenta y autoriza el plan de acción.
Encargado del proyecto	Documentación de resultados posterior a utilizar la herramienta de geolocalizacion	Cliente externo	La documentación se muestra de manera cronológica y clara incluyendo fechas y resultados	Se arma el caso por el encargado del proyecto para poder exponerlo

2.8 Seguimiento y Control

Las actividades que realizaremos y que nos asigna el encargado del proyecto son monitoreadas y controladas por el mismo a excepción de la primera etapa (Curso CEH) la cual está administrada por Roberto Martínez; En el caso del proyecto de desarrollo de herramienta de geolocalización se programan juntas semanales en las que se habla de los entregables esperados, resultados obtenidos, fechas limites y progreso de las tareas que se llevan a cabo en ese momento, en caso de que existan cambios o retrasos en el desarrollo de

dichos entregables, se comenta y corrige si es necesario, si se presenta algún percance urgente se contacta directamente al encargado del proyecto para informarle fuera de horas de junta.

Semanalmente se tienen estas sesiones presenciales en las que podemos utilizar los recursos disponibles para el desarrollo de la herramienta, así como la asistencia del caso si es necesario, así mismo en estas sesiones se discuten temas de teoría, temas técnicos y avances tanto de las actividades como del proceso del PAP en sí.

En el caso del programa PAP existen sesiones virtuales semanales en las que se adquiere teoría general del ámbito profesional y se revisan avances del reporte, así como consulta de dudas y correcciones por parte del profesor en caso de que existan.

2.9 Cierre del Proyecto

Al momento de cerrar una etapa del proyecto se realiza una reunión para exponer el proceso y los resultados y se discute de manera general el proceso y los siguientes pasos o etapas, evidentemente cada etapa es diferente y se hace un acercamiento distinto según los entregables.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

Los principales entregables se pueden resumir en los siguientes:

1. Herramienta de geolocalización: esta herramienta es el entregable principal y en el que se ha dedicado la mayor investigación, su función y utilidad recae en proyectos en los que sea necesario obtener una ubicación remota de ciertos dispositivos.
2. Reporte de investigación relacionado a las tecnologías que se requirieron para desarrollar la herramienta mencionada en el punto anterior y que cumplió con la función de reportar al director el proceso que se llevó a cabo.
3. Otros entregables relevantes son reportes de investigación de diversos dominios, personas u organizaciones, aplicando lo aprendido en el curso CEH, lo que incluye subdominios, correos relacionados con los involucrados, reconocimiento de personas y organizaciones en general, así como sistemas internos, sistemas operativos de dispositivos y puertos abiertos.

3.2 Estimación del Impacto

Los entregables del trabajo que produje en colaboración con mis compañeros y el encargado del proyecto tienen diferentes tipos de impacto, en su mayoría fueron entregables que tuvieron relevancia e impacto instantáneo, es decir se aplicaba su función en el momento como es el caso de los reportes de investigación de personas y de organizaciones, así como de dominios y de información mas técnica, estos reportes brindaban valor a la investigación del caso y a la primera fase del estudio de caso que es reconocimiento e investigación.

En el caso del entregable de la herramienta de geolocalización tiene un impacto tanto a corto plazo como a largo, a corto plazo ya que se utilizó en el caso actual en el que esta trabajando el encargado de proyecto, y al ser una herramienta ya desarrollada, se puede utilizar en un futuro en cualquier caso similar o que requiera de su funcionalidad por lo que tiene trascendencia en la organización y tiene un alcance potencialmente enorme.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

En cuanto a competencias técnicas que desarrolle durante el proyecto existen muchas herramientas de reconocimiento e investigación de sistemas digitales e infraestructura de red, entre ellos los más útiles fueron nmap, recon-ng, hunter, netcraft entre otras, para poder utilizar estas herramientas es necesario tener conocimiento previo básico de Linux y sus comandos ya que la mayoría de estas herramientas no tienen interfaz gráfica. Adicional a estas esto, para desarrollar la herramienta de geolocalización se utilizó un software llamado geowifi en el que era necesario conocimiento de Python, Linux e investigación en general de funcionalidad.

Hablando de competencias suaves hubo mucho desarrollo ya que fue necesario en todo momento tener una muy buena comunicación tanto con mi equipo de trabajo como con el encargado del proyecto, también se desarrolló, trabajo en equipo hubo en todo momento y cada que había dudas a cerca del desarrollo o del uso de una herramienta, y por ultimo se requirió de solución de problemas, siempre que se trabaja con sistemas y herramientas digitales es necesario tener esta habilidad desarrollada y practicarla.

En el campo de la informática forense existe mucho potencial y crecimiento tanto en la industria como en las soluciones que ofrece, al ser un campo relativamente virgen en México las posibilidades de obtener un empleo relacionado no son tan altas sin embargo ejercer como un particular o crear una empresa que cumpla con las necesidades del mercado actual podría ser una muy buena oportunidad, la problemática de los incidentes informáticos son cada vez mas recurrentes y se requiere de una gran cantidad de profesionales que puedan atacarla.

Para poder participar y aportar valor a este PAP se requirió de un gran conocimiento técnico, principalmente se requirió conocimiento de máquinas virtuales, Linux y conocimiento de programación y sus recursos como lo es github, vsc, lenguaje Python etc. Materias que aportaron a este conocimiento previo requerido son materias como servicios de internet ayudaron mucho con la parte de Linux, materias como desarrollo de aplicaciones y servicios web para comprender de programación y web en general, así como las materias de redes y seguridad informática.

En cuanto a mi capacidad para crear un proyecto o ser parte de uno parecido al desarrollado en este PAP creo que aprendí lo suficiente como para poder resolver una problemática como la que vimos en el caso trabajado sin embargo el conocimiento de derecho y de los procesos jurídicos son algo que no tengo desarrollado por lo que más bien pensaría en un proyecto compartido con alguien que tenga estos conocimientos, así como los técnicos.

4.2 Aprendizajes Sociales

En el sentido de que la informática forense es un área muy de nicho en México creo que aportar a la preparación de este tipo de profesionistas o incluso desarrollar una empresa que

atienda estos casos podría tener mucho impacto social positivo, esto beneficiaria no solo a organizaciones tanto pequeñas como grandes sino a particulares también que son los que desgraciadamente tienen problemas de incidentes informáticos o robo de identidad y dinero mas frecuentemente y los que están más desinformados al respecto.

En este proyecto en específico se produjeron resultados que pueden ayudar potencialmente a muchas organizaciones y personas que requieran una investigación con el tipo de herramienta que desarrollamos, de este esfuerzo se puede rescatar que los conocimientos conjuntos del encargado el proyecto, así como nosotros estudiantes podemos contribuir con nuestras capacidades para apoyar a la sociedad en este tipo de casos.

4.3 Aprendizajes Éticos

En general creo que mis valores personales están alineados a producir resultados útiles tanto para la organización con la que esté trabajando como con las personas a las que les ofrece su servicio, en ese sentido la empresa de ITLS tiene una visión muy parecida y por eso es que disfruté mucho esta experiencia y pude sentir satisfacción al trabajar con ellos y con sus objetivos.

Esta experiencia fue enriquecedora en los aspectos ya mencionados y creo que tiene mucho futuro sin embargo creo que me hizo darme cuenta que me hace falta mucho conocimiento en ramas secundarias como derecho por lo que creo que mi caminó se centrará mas hacia una parte mas técnica y menos aplicada como un caso a resolver, es decir me gustaría concentrarme en desarrollar la parte de “offensive security” para desarrollarme dentro de una empresa y en un futuro poder tener las habilidades necesarias para aportar valor en este tipo de proyectos o incluso crear una empresa que realice lo mencionado ya que creo que su misión es muy necesaria.

4.4 Aprendizajes Personales

Gracias a esta experiencia comprendí mucho a cerca de lo que me gusta y lo que quiero hacer con mi carrera profesional, creo que me aportó mucho conocimiento de la industria forense y lo necesario que es pero de la misma manera me mostró que en realidad no me veo ejerciendo hacia esa dirección.

Creo que me puede aportar mas empezar mi carrera especializándome en seguridad ofensiva y trabajando en diferentes casos de manera técnica y a partir de ahí evaluar las posibilidades de negocio en las que yo me pueda desenvolver con un conocimiento amplio y así poder aportar a la sociedad de manera más relevante.

En cuanto al trabajo en equipo y habilidades de comunicación creo que es muy enriquecedor conocer una segunda empresa (diferente a la del primer PAP) ya que eso te abre el panorama de manera empírica para evaluar y comparar actitudes y estructuras organizacionales para poder identificar una buena empresa cuando este trabajando de tiempo completo en alguna.

4.5 Tareas Aprendidas

Existieron muchos factores que hicieron que se dieran exitosamente los objetivos de este proyecto, no solo la parte técnica, también influyen las habilidades suaves, así como el apoyo en el encargado del proyecto y en nuestros compañeros para lograr los entregables en tiempo y forma.

En el caso de las habilidades técnicas evidentemente tuvieron mucho peso y no se hubieran podido lograr sin el tiempo de aplicar los conocimientos del curso, así como desarrollar los laboratorios para aprender a usar las diversas herramientas que en su momento nos ayudaron a realizar los reportes de investigación requeridos. La disposición al aprendizaje es necesaria ya que sin ella no se podría sacar provecho al curso y el tiempo de los entregables se vería afectado negativamente debido al tiempo de asesoramiento incrementado.

En cuanto a las actitudes que se presentaron durante el proyecto, en su mayoría fueron positivas y con mucha disposición a ayudar sin actitudes de superioridad, creo que esto ayudo mucho a que el ambiente tanto en la oficina cuando nos veíamos, así como en las sesiones que tuvimos virtualmente.

4.6 Desarrollo Profesional

Las tareas tecnológicas en las que más me interesa desarrollarme y el tipo de proyectos en los que me gusta trabajar son los siguientes:

1. Seguridad ofensiva o “pentesting” me gusta bastante por el potencial que tiene y las habilidades que desarrollas, así como el conocimiento profundo que se debe desarrollar en diferentes ámbitos para poder realizar tus tareas.
2. Informática forense me interesa mucho el tema de ciberataques y el proceso que se debe llevar para resolver estos problemas, esta experiencia en el PAP me ha ayudado mucho a ver en si como es el proceso.
3. Las redes y telecomunicaciones son un área que me interesa mucho y el PAP anterior me hizo ver su alcance y el tipo de trabajo que se debe realizar.

Las áreas tecnológicas en las que me desempeño con mayor destreza son las siguientes:

1. Administración de redes
2. Análisis de tráfico e investigación
3. Configuración de dispositivos de red

En cuanto a las ares del mercado laboral y servicios profesionales con mayor crecimiento en relación a mis intereses y habilidades creo que se resume en los siguientes:

1. Penetration tester: Este sector tiene mucho potencial y es de los mas interesantes a mi parecer, pero requiere de mucho conocimiento técnico en muchas áreas, por lo que la preparación tiene que ser constante incluso años después de entrar en la industria.

2. Ingeniero de redes: Este sector es en el que creo que hay más posibilidad de empezar sin embargo lo veo limitado hasta cierto punto en el sentido de crecimiento profesional, me parece muy interesante y me gusta, pero tengo más pasión por pentesting.

3. Informática forense: es muy interesante y el modelo de negocio es diferente, se basa en casos específicos que se tienen que atender h asta resolver y reportar lo referente a la incidencia, me gusta, pero hay una barrera de conocimiento (derecho).

Habiendo mencionado esto, los pasos que debo seguir para dirigirme a la posición objetivo que es la numero 1, penetration tester, seria realizar una preparación más especifica a ese ámbito además de aprender por mi cuenta todas las habilidades y conocimiento faltante, en este sentido estoy llevando un diplomado de seguridad ofensiva impartido por una empresa americana con mucha experiencia que creo que me va a ayudar a encaminarme hacia el objetivo.

Creo que este sector tiene mucho futuro debido a la necesidad global de tener mayor seguridad informática por el riesgo y frecuencia de los ataques actuales, debido a esto la remuneración económica tiende a ser mayor a medida que avanza el tiempo.

5. Conclusiones

En este proyecto de aplicación profesional he asimilado muchas cosas en cuanto al proyecto en si y en cuanto a la dirección de carrera profesional que quiero tomar, fue una experiencia muy enriquecedora en la que se utilizaron muchos conocimientos técnicos vistos durante la carrera, creo que el saber a cerca de Linux tuvo mucho peso para aprender a usar ciertas herramientas sobre todo en el apartado de reconocimiento para realizar los informes, en cuanto a aprendizajes también hubo avance tanto en el área de informática forense y en cómo funcionan los casos. En cuanto a los resultados del proyecto creo que tienen un a trascendencia en la empresa y en los casos futuros.

Durante el desarrollo del proyecto ocurrieron muchas situaciones que afectaron el plan inicial de las tareas asignadas, esta situación se repitió tomando en cuenta el PAP anterior, lo que me hace concluir que es normal que este plan inicial se modifique por incidentes externos o internos que están fuera de nuestro alcance, sin embargo, la comunicación y organización son clave para poder adaptarse y seguir progresando dentro del proyecto.

En cuanto a mi visión de trayectoria profesional, confirmé que la informática forense no es el camino que me gustaría seguir sino la seguridad ofensiva, es decir, aspirar a un trabajo de penetration tester es lo que me gustaría, para ello es necesario concentrar mis estudios y mi esfuerzo a completar el conocimiento faltante con el diplomado e investigación por mi cuenta.

En general me voy con una gran sensación de satisfacción por el proyecto en general y lo que he aprendido tanto técnicamente como de habilidades suaves y reflexiones personales.