

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 TECNOLOGIA II

BISHOP FOX, MEXICO

PRESENTA

Alumno: ISI, Jorge Mario Arozarena Argotte

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

Tlaquepaque, Jalisco, mayo 2024

ÍNDICE

Contenido

REPORTE PAP.....	3
<i>Presentación Institucional de los Proyectos de Aplicación Profesional.....</i>	<i>3</i>
<i>Resumen.....</i>	<i>4</i>
<i>1. Introducción.....</i>	<i>5</i>
<i>1.1 Antecedentes.....</i>	<i>5</i>
<i>1.2 Justificación.....</i>	<i>6</i>
<i>1.3 Objetivos.....</i>	<i>6</i>
<i>1.4 Contexto.....</i>	<i>7</i>
<i>1.5 Inventario de Competencias.....</i>	<i>8</i>
<i>1.6 Plan Educativo.....</i>	<i>8</i>
<i>1.7 Entregables.....</i>	<i>9</i>
<i>1.8 Involucrados.....</i>	<i>9</i>
<i>2. Desarrollo del Proyecto PAP.....</i>	<i>10</i>
<i>2.1 Administración del Proyecto.....</i>	<i>10</i>
<i>2.2 Sustento Teórico y Metodológico.....</i>	<i>10</i>
<i>2.3 Descripción del Proyecto.....</i>	<i>10</i>
<i>2.4 Tipo de Proyecto.....</i>	<i>11</i>
<i>2.5 Plan de Trabajo.....</i>	<i>12</i>
<i>2.6 Equipo de Trabajo.....</i>	<i>13</i>
<i>2.7 Plan de Comunicaciones.....</i>	<i>14</i>
<i>2.8 Plan de Calidad.....</i>	<i>15</i>
<i>2.9 Seguimiento y Control.....</i>	<i>15</i>
<i>3. Resultados del Trabajo Profesional.....</i>	<i>16</i>
<i>3.1 Productos Obtenidos.....</i>	<i>16</i>
<i>3.2 Estimación del Impacto.....</i>	<i>16</i>
<i>4. Reflexiones del alumno.....</i>	<i>17</i>
<i>4.1 Aprendizajes Profesionales.....</i>	<i>17</i>
<i>4.2 Aprendizajes Sociales.....</i>	<i>17</i>
<i>4.3 Aprendizajes Éticos.....</i>	<i>17</i>
<i>4.4 Aprendizajes Personales.....</i>	<i>18</i>
<i>4.5 Tareas Aprendidas.....</i>	<i>19</i>

4.6 Desarrollo Profesional..... 19
5. Conclusiones.....20

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

La ciberseguridad hoy en día ha adquirido una importancia crucial en la sociedad actual, ya que la tecnología está presente en casi todos los aspectos de nuestras vidas. A medida que la tecnología crece y es utilizada por más gente, también crecen las amenazas cibernéticas, y con ello, los riesgos para las organizaciones.

Bishop Fox es una empresa con sede en Estados Unidos, la cual se dedica a brindar ciberseguridad ofensiva a empresas privadas y es reconocida como el líder en su área y un gran lugar para trabajar.

Con 16 años de experiencia, entre los mayores logros de Bishop Fox destacan: haber trabajado con 26 empresas del "Fortune 100", completado más de 20,000 proyectos, asesorado a 5 del top 5 global de compañías de entretenimiento, entre otros más.

Para este PAP, trabajaré como "Attack Surface Intern" en el área de COSMOS, la cual se dedica a realizar pruebas de penetración automatizadas continuas.

El 'proyecto que se me fue asignado es el definir la superficie de ataque de diversos clientes de Bishop Fox, poniendo en práctica la etapa de "Reconocimiento" de la metodología de hacking ético. Para definir la superficie de ataque de estos clientes, es necesario hacer un mapeo de todo su perímetro externo, el cual consiste en identificar sus dominios, subdominios, rangos de red, infraestructuras de terceros, entre otras cosas más.

Esta etapa es crucial para el área de COSMOS, ya que es la base para poder encontrar la mayor cantidad de vulnerabilidades con una alta precisión.

1. Introducción

1.1 Antecedentes

Durante el PAP I. el cual realicé en el Observatorio de Seguridad Informática del ITESO, analicé de manera detallada el funcionamiento del aplicativo del botón de pánico, realizado por el C5. Dicho proyecto se concluyó de manera satisfactoria al haber realizado una prueba de penetración y un reporte con las vulnerabilidades encontradas. En este PAP mi papel fue de consultor externo, ya que, aunque tuve contacto con gente de la empresa huésped, la mayor parte fue a través del Observatorio. En este proyecto aprendí a trabajar con una metodología ágil, a hacer reportes de vulnerabilidades, y cumplir con los tiempos definidos tanto por la empresa huésped como por el Observatorio.

Ahora, como parte de mi Proyecto de Aplicación Profesional II, estaré trabajando como “Attack Surface Intern” en Bishop Fox.

Bishop Fox es la principal autoridad en seguridad ofensiva, ofreciendo soluciones que van desde pruebas de penetración continuas, simulaciones de ataque (red teaming) y gestión de superficie de ataque, hasta evaluaciones de seguridad de productos, nubes y aplicaciones. Ha colaborado con más del 25% de las empresas Fortune 100, la mitad de las Fortune 10, ocho de las 10 principales empresas tecnológicas a nivel mundial y todas las principales empresas de medios globales.

Misión: “Hacer que el mundo digital sea más seguro para todos. Nuestra misión es inclusiva y, para lograrla, necesitamos crear un entorno diverso y equitativo donde las personas de todos los orígenes e identidades puedan prosperar. Cuando nuestros colaboradores pueden mostrar su verdadero ser en el trabajo, impulsamos la innovación y logramos resultados sorprendentes tanto para nuestros clientes como para nuestro negocio.”

Visión: “Ser la firma líder en consultoría de seguridad de la información en el universo.”

Valores:

- *Sé Excelente con los Demás:*
 - *Nos tratamos mutuamente con respeto, es parte de nuestro modelo de negocios. Nuestros clientes y compañeros de trabajo saben que los cuidaremos.*
- *Haz lo que Dices que Harás*
 - *Nuestro compromiso con la calidad exige que asumamos nuestra responsabilidad y cumplamos nuestras promesas. Juramos doblemente cumplirlo.*
- *Haz lo Correcto*
 - *Nuestros clientes confían en nosotros con su información más preciada. Nunca comprometemos sus intereses para avanzar en los nuestros.*

- *Mejora Juntos*
 - *Creemos que el statu quo está ahí por una razón: para ser derribado. Y estamos aprendiendo, mejorando y volviéndonos más inteligentes juntos de manera incansable.*

1.2 Justificación

Este proyecto se adecúa completamente a mis intereses personales y profesionales, ya que tiene como objetivo el definir la superficie de ataque de diversos clientes, para así poder encontrar y reportar vulnerabilidades antes de que algún agente malicioso lo haga. Trabajar con una empresa que esta inmersa en este mundo de la ciberseguridad me aportará mucho a mi formación profesional, ya que pondré en práctica lo aprendido a lo largo de mi carrera.

Por otro lado, trabajar en un proyecto que pertenece a la empresa líder de la ciberseguridad ofensiva es un gran valor añadido a mi currículum. Tomando en cuenta que me resta alrededor del 15% de créditos para concluir mi carrera, el esfuerzo en horas que aplicaré es de 20 horas semanales a Bishop Fox y 8 horas semanales a la documentación y aprendizaje requerido para llevar a cabo los trabajos. Es importante el tener una buena administración del tiempo para poder cumplir con ambas partes y poder sacar el mayor provecho a este proyecto.

1.3 Objetivos

El objetivo que Bishop Fox busca con el proyecto en el que participo es el definir la superficie de ataque de diversos clientes. El entregable principal consistirá en proporcionar una lista detallada de dominios, subdominios y rangos de redes de cada cliente.

Los objetivos que yo busco en este proyecto son: conocer como es que funciona una empresa de ciberseguridad ofensiva, conocer como automatizan sus procesos, aprender como puedo definir la superficie de ataque de un cliente con sus herramientas, y, lo más importante, ganar experiencia profesional en la empresa líder de ciberseguridad ofensiva. Al culminar con este proyecto pretendo alcanzar el nivel requerido para una posición de tiempo completo en la compañía.

Los objetivos necesarios para llevar a cabo este proyecto se pueden agrupar en tres categorías: competencias técnicas, personales, y organizacionales; que detallare a continuación.

- *Competencias Técnicas*
 - *Python – Capacidad de elaborar/entender scripts*

- OWASP – Conocimiento y entendimiento del top 10
- Redes – Entendimiento de los protocolos de comunicación y rangos de red
- Linux – Manejo de terminal, servidores, y ejecución de scripts
- Pentesting – Seguridad ofensiva, capacidad de encontrar vulnerabilidades
- Competencias Personales
 - Ética – Se requiere confidencialidad al manejar datos sensibles
 - Inglés – La mayoría de la información se encuentra en este idioma
 - Autoaprendizaje – La ciberseguridad requiere de ser autodidacta
 - Orientado a Resultados – Siempre buscar resultados personales, profesionales, y para la empresa.
- Competencias Organización
 - Trabajo en Equipo – Importante trabajar en equipo para lograr los resultados en tiempo y calidad
 - Comunicación Oral y Escrita – Requerida para elaborar los reportes y documentación relacionada a las vulnerabilidades encontradas

1.4 Contexto

Para este proyecto tomaré el rol de “Attack Surface Intern”, donde la principal función es apoyar a los Analistas de mayores rangos con una parte del proceso para definir la superficie de ataque de los clientes, la cual llamaremos “Discovery”. Por lo tanto, corresponde al tipo de proyecto de Apoyo a Áreas Operativas.

Los beneficios que se buscan con mi participación es el poder hacerme cargo de los “Discoveries” para que los Analistas puedan poner sus esfuerzos en tareas más complejas. Para lograr este objetivo, estaré guiado por un Analista hasta que pueda hacer el proceso por mi cuenta.

1.5 Inventario de Competencias

No.	Competencia	Req	Adq	GAP	Obj	Prior
1	Python	3	2	1	3	M
1.1	Ingeniería inversa	3	3	0	3	M
1.2	Desarrollo de scripts	3	3	0	3	M
1.3	Automatización	3	2	1	3	M
2	OWASP	3	3	0	3	A
2.1	Capacidad análisis owasp top 10	3	3	0	3	A
2.2	Capacidad práctica owasp top 10	3	3	0	3	A
3	Redes	3	2	1	3	A
3.1	Conocimiento protocolos de red	3	3	0	3	A
3.2	Conocimiento segmentacion de IPs	3	2	1	3	M
4	Linux	3	3	0	3	A
4.1	Manejo terminal	3	3	0	3	A
4.2	Bash scripting	3	3	0	3	A
4.3	Explotación	3	3	0	3	A
5	Shell	3	2	1	3	M
5.1	Desarrollo scripts	3	3	0	3	M

1.6 Plan Educativo

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	Python																							
1.1	Ingeniería inversa	Autoestudio		8	22/01/2024	26/01/2024																		
1.2	Desarrollo de scripts	Autoestudio		6	29/01/2024	02/02/2024																		
1.3	Automatización	Autoestudio	1.2	4	05/02/2024	08/01/2024																		
2	OWASP																							
2.1	Capacidad análisis owasp top 10	Autoestudio		4	15/02/2024	17/02/2024																		
2.2	Capacidad práctica owasp top 10	Autoestudio	2.1	4	16/02/2024	18/02/2024																		
3	Redes																							
3.1	Conocimiento protocolos de red	Autoestudio		6	22/01/2024	26/01/2024																		
3.2	Conocimiento segmentación de Ips	Autoestudio		8	22/01/2024	26/01/2024																		
4	Linux																							
4.1	Manejo terminal	Autoestudio		40	18/02/2024	10/05/2024																		
4.2	Bash scripting	Autoestudio		40	18/02/2024	10/05/2024																		
4.3	Explotación	Autoestudio		10	05/05/2024	10/05/2024																		
5	Shell																							
5.1	Desarrollo scripts	Autoestudio	4.2	48	22/01/2024	10/05/2024																		

1.7 Entregables

El entregable consiste en la documentación de dominios, subdominios y rangos de redes que pertenecen al cliente que se le haga el “Discovery”. Se manejará por fases, y los entregables quedarán de la siguiente manera:

- *Fase0: lista de subsidiarias*
- *Fase1: Lista de dominios*
- *Fase2: Lista de subdominios*
- *Fase3: Lista de rangos de red*

1.8 Involucrados

- *Líder de squad de Analistas*
- *Cliente externo*
- *Analista que tomará el rol de mentor el primer mes*
- *Attack Surface Analyst – Jorge Mario Arozarena Argotte*

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

La administración del proyecto se basa en fases, donde el líder técnico proporcionará los objetivos que tengo que cumplir, así como los tiempos de acuerdo con el objetivo principal del proyecto. Para cada uno de los “Discoveries” realizados, aplican las siguientes etapas:

- *Discovery en Backlog*
- *Discovery en proceso*
- *Discovery listo para QA*
- *QA completo*
- *Discovery finalizado*

2.2 Sustento Teórico y Metodológico

Para realizar el proyecto haremos uso de la metodología propia de BishopFox, la cual consta de 4 fases:

- *Fase0: Investigación del cliente, subsidiarias, dominios principales.*
- *Fase1: Encontrar dominios asociados a sus subsidiarias, a través de diferentes técnicas como reverse lookup, tls cert reverse lookup, redirects, entre otras.*
- *Fase2: Subdomain enumeration utilizando diferentes herramientas como DNSX, bynaryedge, entre otras.*
- *Fase3: Investigación de rangos de redes que pertenecen al cliente.*
- *Fase4: Documentar la evidencia y cerrar el procedimiento.*

2.3 Descripción del Proyecto

Este proyecto forma parte de un proyecto de mayor alcance, ya que trabajaré únicamente en el dibujo de la superficie externa de los clientes. Posterior a esto, otros equipos tomarán mi trabajo para poder realizar las pruebas de penetración y finalmente reportar al cliente.

Los recursos que voy a utilizar son en su mayoría propiedad de Bishop Fox, sin embargo, las siguientes herramientas son públicas y también son parte del proceso de “Discovery”:

- *ARIN*
- *Subdover*
- *Wayback machine*
- *Whoxy*
- *DNSlytics*
- *DNSX*
- *Binaryedge*

2.4 Tipo de Proyecto

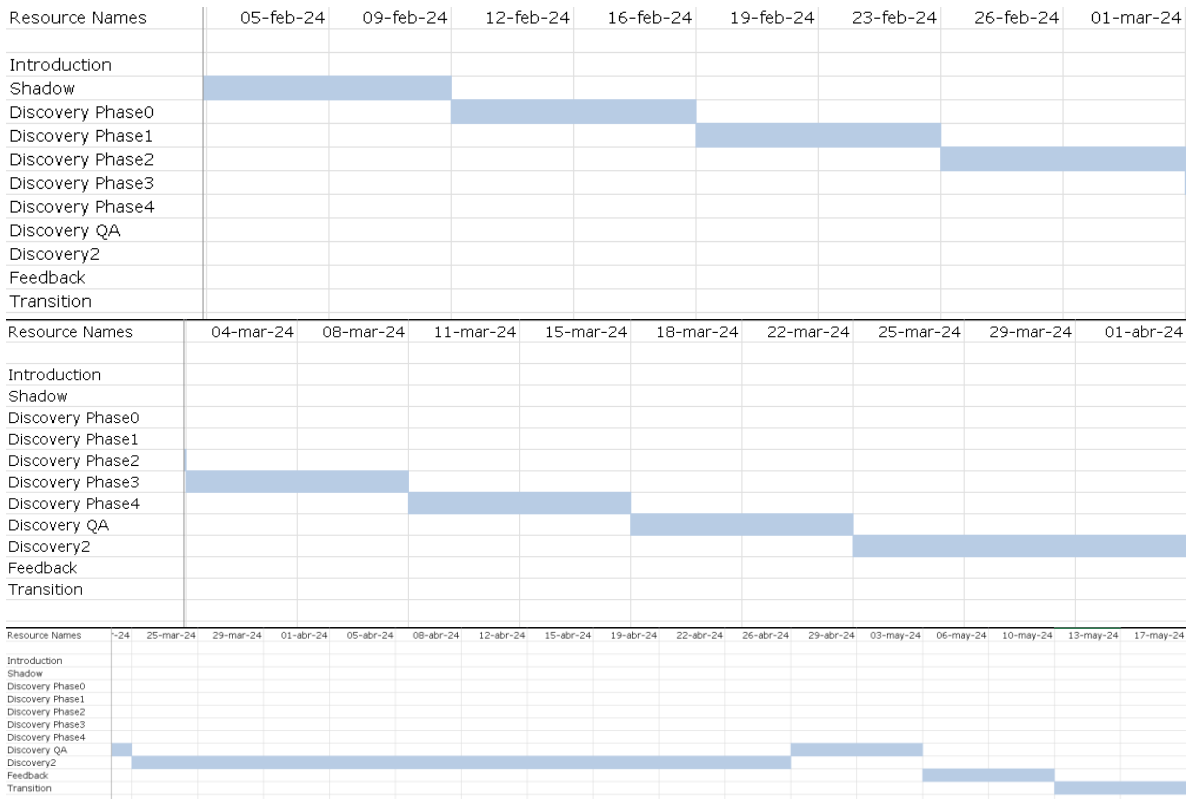
El Ciclo de Vida del Proyecto es de tipo Cascada, ya que cada fase del Discovery necesita que se haya completado la fase anterior. Por ejemplo, la fase 2, que es enumerar los subdominios, requiere que la fase 1 haya sido completada, ya que es la fase en la cual se listan los dominios.

2.5 Plan de Trabajo

No.	Competencia	Nivel Adquirido al Inicio	Nivel Objetivo al final PAP	Objetivo final PAP	Prior
1	Python: ingeniería inversa, scripting y automatización	1	2	2	A
2	OWASP: reconocimiento top 10	2	2	2	A
3	Redes: Segmentación	3	3	3	A
4	Linux	3	3	3	A
5	Shell scripting	2	3	2	A

ID	Task Name	Duration	Start	Finish	Predecessor
1	Introduccion	5 days	01/01/2024	05/01/2024	
2	Shadow	5 days	08/01/2024	12/01/2024	
3	Shadow	5 days	15/01/2024	19/01/2024	
4	Shadow	5 days	22/01/2024	26/01/2024	
5	Shadow	5 days	29/01/2024	02/02/2024	
6	Shadow	5 days	05/02/2024	09/02/2024	
7	Discovery Phase0	5 days	12/02/2024	16/02/2024	02:06
8	Discovery Phase1	5 days	19/02/2024	23/02/2024	
9	Discovery Phase2	5 days	26/02/2024	01/03/2024	
10	Discovery Phase3	5 days	04/03/2024	08/03/2024	
11	Discovery Phase4	5 days	11/03/2024	15/03/2024	
12	Discovery QA	5 days	18/03/2024	22/03/2024	08:11
13	Discovery2	5 days	25/03/2024	29/03/2024	12
14	Discovery2	5 days	01/04/2024	05/04/2024	
15	Discovery2	5 days	08/04/2024	12/04/2024	
16	Discovery2	5 days	15/04/2024	19/04/2024	
17	Discovery2	5 days	22/04/2024	26/04/2024	
18	Discovery QA	5 days	29/04/2024	03/05/2024	13:17
19	Feedback	5 days	06/05/2024	10/05/2024	
20	Transition	5 days	13/05/2024	17/05/2024	01:19

Resource Names	05-ene-24	08-ene-24	12-ene-24	15-ene-24	19-ene-24	22-ene-24	26-ene-24	29-ene-24	02-feb-24
Introduction									
Shadow									
Discovery Phase0									
Discovery Phase1									
Discovery Phase2									
Discovery Phase3									
Discovery Phase4									
Discovery QA									
Discovery2									
Feedback									
Transition									



2.6 Equipo de Trabajo

Rol	Responsabilidad	Nombre (opcional)
<i>Squad Lead de Analistas</i>	<i>Gestionar el avance del proyecto</i>	
<i>Analista Mentor</i>	<i>Apoyar con capacitaciones</i>	
<i>Intern</i>	<i>Realizar Discoveries a los diferentes clientes</i>	<i>Jorge Mario Arozarena Argotte</i>

2.7 Plan de Comunicaciones

<i>Emisor</i>	<i>Mensaje</i>	<i>Receptor</i>	<i>Medio</i>	<i>Frecuencia</i>
<i>Squad Lead de Analistas</i>	<i>Nuevas tareas</i>	<i>Intern</i>	<i>Slack</i>	<i>Periódicamente</i>
<i>Intern</i>	<i>Tareas ya realizadas</i>	<i>Squad Lead de Analistas</i>	<i>Slack</i>	<i>periódicamente</i>
<i>Intern</i>	<i>Dudas, avances</i>	<i>Analista Mentor</i>	<i>Slack</i>	<i>Diario</i>
<i>Intern</i>	<i>Comunicación tareas que se están realizando</i>	<i>Squad</i>	<i>Videoconferencia</i>	<i>Diario</i>
<i>Alumno PAP</i>	<i>Avance reporte PAP</i>	<i>Profesor PAP</i>	<i>Canvas</i>	<i>Semanal</i>

2.8 Plan de Calidad

<i>Emisor: Quién Entrega</i>	<i>Entregable: Qué Entrega (Entregable)</i>	<i>Receptor: Quién recibe o Inspecciona</i>	<i>Criterios: Condiciones de Aceptación</i>	<i>Siguiente paso. Cuando se Autoriza.</i>
<i>Intern</i>	<i>Fases Discovery</i>	<i>Mentor QA</i>	<i>Cada fase realizada debe haber contemplado cada uno de los pasos descritos</i>	<i>Squad Lead Analistas</i>
<i>Alumno PAP</i>	<i>Avances en el reporte final</i>	<i>Profesor PAP</i>	<i>Cada punto esta completado correctamente</i>	<i>Librería PAP</i>

2.9 Seguimiento y Control

Para facilitar el seguimiento y control de este proyecto, fui integrado al espacio de trabajo del área de COSMOS en Slack para estar en constante comunicación. Además, se tienen sesiones diarias para decir en que estamos trabajando y si hay algún “blocker”. Finalmente, cada 2 semanas tendré un 1 a 1 con el líder de los Analistas para recibir feedback y más tareas.

En cuanto a las sesiones con la Coordinación del PAP, el profesor PAP Juan Manuel Islas Espinoza estableció espacios de 2 horas los martes y viernes, en donde se hará una revisión de los avances en el reporte PAP y se brindará la asesoría requerida.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

- 1. En el Discovery realizado resultaron 200 nuevos dominios importados a la superficie de ataque del cliente, Lo cual representa un aumento del 50% de su tamaño.*
- 2. Se importaron un total de 1,019 subdominios a su superficie de ataque, lo cual representa un aumento del 30% de su superficie de ataque.*
- 3. Se importaron 3 rangos de IPs registrados por el cliente, lo cual representa un aumento del 20% de su superficie de ataque.*
- 4. Se corrió un escaneo de Log4j, no hubo ningún hit.*
- 5. Ya se reportaron los primeros findings relacionados a los nuevos assets que se importaron durante este Discovery. Esto indica que el Discovery fue exitoso y que estamos abarcando toda la superficie del cliente visible para un atacante externo.*

3.2 Estimación del Impacto

El impacto que tiene este Discovery en el cliente es que su superficie de ataque creció en un 50% en sus dominios, 30% en subdominios y 20% en sus rangos de IP.

Esta actualización nos brinda la certeza de que estamos escaneando todos los posibles puntos de entrada y áreas vulnerables dentro de la infraestructura del cliente. Al tener una cobertura más amplia, podemos identificar y abordar posibles vulnerabilidades antes de que sean explotadas por un atacante externo.

Hasta ahora, ya se reportaron las primeras vulnerabilidades asociadas a estos nuevos assets que fueron encontrados:

- 1 critical*
- 1 medium*
- 2 lows*

Con una visión más completa de la superficie de ataque, podemos trabajar proactivamente para proteger los activos críticos del cliente y mantener su entorno seguro y protegido contra posibles ataques.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

Gracias a la naturaleza de este proyecto, pude desarrollar y usar satisfactoriamente las siguientes competencias técnicas:

- *Descubrimiento de dominios*
- *Enumeración de dominios*
- *Descubrimiento de rangos de redes*
- *Escaneo de potenciales subdomain takeovers*
- *Bash y Python scripting*

Del mismo modo, trabajar con un equipo con compañeros en México como en Estados Unidos e incluso Inglaterra, me ayudó a desarrollar las siguientes soft skills:

- *Trabajo en equipo*
- *Comunicación*
- *Capacidad de resolución de problemas*

Al concluir este proyecto, considero que tengo las suficientes habilidades técnicas para ejercer el trabajo como Analista de superficie de ataque en Bishop Fox.

4.2 Aprendizajes Sociales

Bishop Fox se dedica a brindar servicios de seguridad informática a una amplia gama de empresas privadas, ayudándolas a protegerse contra amenazas cibernéticas y vulnerabilidades potenciales. Durante mi tiempo en la empresa, aprendí que una de las primeras y más importantes tareas en cualquier proyecto de seguridad es definir la superficie de ataque de un cliente. Esto implica identificar y comprender todos los puntos de entrada potenciales a la red y los sistemas de la empresa, así como evaluar la exposición a posibles vulnerabilidades.

El impacto social de este proyecto fue significativo. Al contribuir directamente a garantizar la confidencialidad de los datos de los clientes de la empresa, no solo estábamos protegiendo a la empresa misma, sino también a sus clientes y usuarios finales. Al evitar la exposición de datos sensibles y prevenir posibles brechas de seguridad, estábamos desempeñando un papel activo en la protección de la privacidad y la seguridad de las personas y las organizaciones.

4.3 Aprendizajes Éticos

Trabajar en ciberseguridad ofensiva es una responsabilidad que va más allá de las competencias técnicas, ya que tener buenos fundamentos de los valores éticos y la responsabilidad moral que conlleva manejar información confidencial y participar en actividades que podrían tener un impacto significativo en la seguridad y la privacidad de las personas y las organizaciones.

Dentro de este proyecto, estás al tanto de todas las vulnerabilidades de clientes muy importantes a nivel mundial, por lo que es esencial contar con valores bien definidos para garantizar la integridad y confidencialidad de todas las partes involucradas.

Agradezco a la Universidad ITESO por su dedicación en inculcar estos valores éticos mí. La educación ética y moral que proporcionan es fundamental para el desarrollo profesional de quienes trabajamos en este campo. Nos brinda las herramientas y el conocimiento necesarios para enfrentar los desafíos éticos de manera responsable y para tomar decisiones informadas que protejan los intereses y la seguridad de todas las partes involucradas.

4.4 Aprendizajes Personales

Mi experiencia en el proyecto PAP me ha proporcionado valiosos aprendizajes personales que han contribuido significativamente a mi desarrollo profesional y personal. Destaco especialmente dos aspectos que han sido fundamentales para mí: la organización y la responsabilidad.

La organización ha sido clave para poder llevar a cabo todas las tareas requeridas en cada fase del proceso de Discovery. Cada paso requiere una planificación cuidadosa y una gestión eficiente del tiempo. A lo largo del proyecto, he aprendido a priorizar tareas, establecer plazos realistas y mantener un enfoque disciplinado para cumplir con los objetivos establecidos.

La responsabilidad también ha sido un aprendizaje crucial. Cada tarea y decisión que he tomado durante el proyecto ha sido la responsabilidad hacia el equipo, el cliente y la empresa. Este sentido de responsabilidad me ha impulsado a esforzarme por alcanzar los objetivos del proyecto.

Además, esta experiencia PAP ha sido un paso importante en la realización de mi meta de trabajar en Bishop Fox. Desde que la empresa llegó a México, he aspirado a formar parte de su equipo y esta oportunidad me ha permitido demostrar mi capacidad y habilidades en el campo de la ciberseguridad. Ahora, una vez finalizado el proyecto, tengo la confianza y la determinación para buscar una posición como Analista de Superficie de Ataque a tiempo completo en la empresa.

Finalmente, este proyecto PAP me ayuda a confirmar que este es el rumbo por el cual quiero seguir. Me ha brindado claridad sobre mis objetivos y me ha motivado a trabajar con mayor determinación para alcanzarlos. Estoy agradecido por esta experiencia y estoy emocionado por las oportunidades futuras que me esperan en el campo de la ciberseguridad.

4.5 Tareas Aprendidas

a. Factores, acciones y actitudes que influyeron favorablemente en los resultados exitosos del proyecto:

- *Comunicación*
- *Planificación adecuada*
- *Colaboración y trabajo en equipo*
- *Flexibilidad y adaptabilidad*
- *Responsabilidad y compromiso*

b. Situaciones, acciones y actitudes que podrían haberse manejado de manera más efectiva:

- *Gestión de tiempo*
- *Comunicación interna*
- *Gestión de riesgos*
- *Mejora continua*

4.6 Desarrollo Profesional

1. Tareas tecnológicas y Proyectos de Interés:

- a. Desarrollo de habilidades de OSINT y reconocimiento de vulnerabilidades*
- b. Participación en eventos de CTF con el fin de mejorar la habilidad de hacking*
- c. Investigación y desarrollo en técnicas avanzadas de reconocimiento y automatización de la superficie de ataque*

2. Áreas Tecnológicas de Destreza:

- a. Ciberseguridad*

3. Áreas del Mercado Laboral con Mayor Crecimiento

- a. Ciberseguridad Ofensiva*
- b. Automatización de procesos*
- c. Threat Hunter*

Para dirigirme hacia mi objetivo, seguiré los siguientes pasos:

- 1. Obtener certificaciones como la Certified OSINT del MCSI*
- 2. Participar en conferencias y eventos de ciberseguridad*
- 3. Buscar el puesto de Analista de Superficie de Ataque al terminar mi proyecto PAP*

Los principales factores que justifican mi inversión de esfuerzo en este sector son la creciente demanda de profesionales especializados en seguridad informática, las oportunidades de desarrollo profesional y la capacidad de contribuir a la protección de la información y la privacidad en el mundo digital.

5. Conclusiones

Después de documentar y analizar mi experiencia PAP, puedo afirmar que ha sido una gran etapa de aprendizaje y crecimiento tanto personal como profesional. A continuación, mis reflexiones finales:

La importancia y beneficio de documentar mis experiencias, aprendizajes y reflexiones es innegable. Elaborar un documento de este tipo me permite ver como visualizaba el proyecto al principio, como se fue desarrollando, y como culminó. Además, me prepara para futuras presentaciones formales, donde puedo compartir de manera clara y estructurada la información requerida.

Encontré varias situaciones imprevistas que surgieron durante el desarrollo del proyecto, sin embargo, estas situaciones me brindaron enseñanzas más allá de lo técnico, especialmente en áreas como la comunicación efectiva en inglés, la gestión del tiempo y resolución de problemas.

En cuanto al grado de satisfacción personal, puedo decir que me siento completamente satisfecho con los resultados obtenidos. El esfuerzo invertido ha valido la pena, y siento que he crecido tanto en conocimientos como en habilidades durante este proceso.

Por último, me gustaría agradecer al ITESO por ofrecer la vinculación con empresas tecnológicas para poder elaborar el PAP, ya que garantiza que el proyecto esté completamente relacionado con mis intereses, y es una gran manera de demostrar los conocimientos que tengo en un ambiente real. Este último PAP me ha proporcionado experiencia que llevaré conmigo en mi viaje personal y profesional. Estoy agradecido por la oportunidad y emocionado por el futuro que me depara.