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

PAP4N01A PROGRAMA DE LA INDUSTRIA DE ALTA TECNOLOGIA I, BISHOP FOX

PRESENTA

Alumno: ISI Sarah Lizeth MURIEL Ramirez

Profesor PAP: Juan Manuel Islas Espinoza, PMP®

Tlaquepaque, Jalisco, julio de 2022.

ÍNDICE

Contenido

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

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

Este trabajo ha sido elaborado con el objetivo de exponer las características del Proyecto PAP, abarcando la informacion de la empresa huésped y detalles sobre el proyecto en el que se participa dentro de ella, así como los resultados obtenidos e impactos del proyecto tanto en el ámbito profesional como en el personal.

1. Introducción

1.1 Antecedentes

Bishop Fox es una de las empresas líder en el ámbito de la seguridad informática, proveyendo soluciones principalmente en las áreas de pruebas de penetración, administración de superficies de ataque, y evaluaciones de seguridad. La empresa brinda sus servicios a las principales empresas tecnológicas más importantes a nivel mundial, enfocándose en la seguridad ofensiva, asistiendo en el descubrimiento y eliminación de vulnerabilidades antes de que puedan ser explotadas.

Bishop Fox está comprometida con la seguridad informática y la investigación, apostando por el desarrollo de herramientas y la realización de investigaciones que son compartidas de manera libre para asistir en la habilitación de la seguridad informática en cualquier empresa. La compañía cree en que la seguridad informática debería de ser para todos, no solo quien trabaja junto a ella.

1.2 Justificación

Las actividades y compromisos por completar y la formación que se me ha dado durante la carrera se encuentran estrechamente ligados, a través de mi educación universitaria he adquirido lo que se podría considerar conocimientos básicos para la interacción con la seguridad informática, gracias a estos conocimientos previamente adquiridos es posible desarrollarme en áreas más especializadas de la seguridad informática mediante el trabajo a realizar durante este proyecto. Realizare veinte horas de trabajo con la empresa a la semana, durante las cuales llevare a cabo las diferentes tareas asignadas y de desarrollo de competencias.

Durante los primeros días se me asignara un miembro del equipo para asistir en mi orientación, posteriormente todos los miembros del equipo de trabajo estarán disponibles para responder preguntas y dar tutorías, y tendré reuniones periódicas con el líder de equipo para orientar y discutir objetivos y logros. Adicionalmente, la documentación y material didáctico del equipo estará disponible para autoestudio.

Me interesa trabajar en áreas de la seguridad informática relacionadas con la inteligencia y análisis, por lo que me gustaría continuar desarrollando actividades similares a las que se llevaran a cabo durante este proyecto.

1.3 Objetivos

El propósito de este proyecto es el habilitar a un intern para que sea capaz de realizar las actividades de administración de superficie de ataque de los clientes.

Mis objetivos respecto al proyecto es obtener los conocimientos y habilidades necesarios para desarrollar las tareas propias de un analista de superficie de ataque, y obtener experiencia realizando actividades dentro de un equipo de trabajo dedicado a la inteligencia.

1.4 Contexto

Cosmos (previamente llamado CAST) es un servicio de pruebas de superficie de ataque continuas, en el que se realiza el descubrimiento de la superficie de ataque del cliente y posteriormente pruebas de penetración dependientes de lo previamente identificado como vulnerable. Dentro de este, el equipo de Inteligencia de Superficies de Ataque se encarga del descubrimiento y validación de la superficie de ataque del cliente de manera continua.

Dentro del proyecto en el que estaré participando se espera entregar al cliente el nivel de servicio estipulado respecto a la administración de su superficie de ataque durante la duración de su contrato, realizando el descubrimiento de la superficie de ataque de manera periódica, y su validación constante para habilitar el trabajo de pruebas de penetración.

Como Attack Surface Analyst Intern, realizare las funciones de asistir a los miembros del equipo de Inteligencia de Superficies de Ataque con las diferentes actividades de administración de la superficie de ataque de los clientes asignados, completando (inicialmente con apoyo de los analistas) las tareas delegadas para habilitar el trabajo del equipo de Operación de Pruebas de Penetración o responder directamente a una necesidad del cliente.

1.5 Entregables

Participare en el proceso recurrente de administración de superficies de ataque, lo cual incluye el descubrimiento y validación de la superficie de ataque para la habilitación del trabajo del equipo de Operación de Pruebas de Penetración, y la respuesta a necesidades del cliente.

1.6 Involucrados

Los interesados en los resultados del proyecto serán:

- *Clientes asignados*
- *Líder de analistas de Inteligencia de Superficies de Ataque*
- *Miembros del equipo de trabajo*
- *Equipo de analistas de Inteligencia de Superficies de Ataque*
- *Equipo de operadores de Pruebas de Penetración*
- *Intern de Inteligencia de Superficies de Ataque*

2. Desarrollo del Proyecto PAP

2.1 Administración del Proyecto

El proceso de inicio determina la propuesta del proyecto y los objetivos, los cuales son principalmente la habilitación de interns para las actividades de administración de superficie de ataque de los clientes. El proceso de planificación establece las actividades necesarias para lograr el objetivo definido, tomando en cuenta la interacción con el equipo de trabajo. Durante el proceso de ejecución del proyecto se lleva a cabo las actividades previamente establecidas para los participantes del proyecto. Durante el proceso de seguimiento y control se aseguran los objetivos del proyecto mediante actividades de seguimiento, contando con los miembros del equipo participante en el proyecto. En el proceso de cierre se evalúan los resultados obtenidos contra los objetivos establecidos y se finaliza el proyecto.

2.2 Sustento Teórico y Metodológico.

El procedimiento para la realización del proyecto ha sido desarrollado por la empresa, abarca procesos de orientación, mentoría, entrenamiento, e integración al equipo de trabajo. Se han realizado modificaciones a un procedimiento previamente utilizado para la integración de nuevos miembros al equipo de trabajo, con el fin de adaptarlo para su utilización con interns.

2.3 Descripción del Proyecto

La secuencia de procesos que son realizados por el equipo de Inteligencia de Superficies de Ataque según su orden de realización es: el descubrimiento de la superficie de ataque, la validación de la superficie de ataque, la identificación de posibles vulnerabilidades, y la depuración de superficie de ataque e identificación de vulnerabilidades concretas.

El proyecto se desarrolla de manera iterativa, con cada iteración se obtiene mayor control sobre la superficie de ataque del cliente mediante la administración y validación, y el equipo de Inteligencia de Superficies de Ataque continúa desarrollando sus habilidades para realizar las tareas de manera más eficiente y efectiva. Mediante esta iteración se habilita a los interns para obtener las habilidades necesarias para realizar las actividades requeridas.

El proyecto es clasificado como de entrega continua de seguridad a la ofensiva, se habilita a los interns a realizar actividades con el objetivo de la protección de superficies de ataque dinámicas y la entrega al cliente del nivel de servicio estipulado. Los recursos utilizados para el proyecto son plataformas y herramientas

desarrolladas dentro de Bishop Fox para el servicio de Cosmos, herramientas de pruebas de penetración y descubrimiento de superficies de ataque de fuente abierta y propietarias, y recursos de aprendizaje. La mayoría del trabajo es realizado de manera remota mediante equipo de cómputo.

El alcance de mi proyecto educativo contempla las siguientes competencias a desarrollar: investigación de fuentes abiertas, fundamentos de redes de computadoras, manejo de herramientas, interacción con el cliente, y colaboración.

No.	Competencia	Nivel que tiene el Alumno	Nivel Requerido PAP	Objetivo al Final del PAP	Prioridad
1	Investigación de fuentes abiertas	2	3	4	A
2	Fundamentos de redes de computadoras	2	3	3	A
3	Manejo de herramientas	1	3	2	M
4	Interacción con el cliente	1	3	3	M
5	Colaboración	2	3	3	A

2.4 Plan de Trabajo

	Actividad	Fecha Inicio	Fecha Termino	Dias habiles	Dependencias
1	**Orientacion**	23/Mayo	3/Junio	10	
1.1	Onboarding				
1.2	Setup				
2	**Shadowing**	6/Junio	24/Junio	15	1
2.1	Administracion de superficies de ataque				
2.1.1	Descubrimiento de superficies de ataque				
2.1.2	Validacion de superfices de ataque				
2.2	Atencion a solicitudes del cliente				
2.3	Manejo de amenazas				
2.4	Desarrollo de automatizacion de analisis				
3	**Hands-on**	27/Junio	15/Julio	15	1, 2
3.1	Administracion de superficies de ataque				
3.2	Descubrimiento de superficies de ataque				
3.3	Atencion a solicitudes del cliente				

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	**Investigacion de fuentes abiertas**																						
1.1	Conocer y estudiar tecnicas de investigacion de fuentes abiertas referentes a organizaciones	Autoestudio / Tutoria		12	30/Mayo	14/Junio																	
1.2	Conocer y utilizar herramientas y tecnicas para el descubrimiento de superficies de ataque (dominios, subdominios, y direccionamiento)	Autoestudio / Tutoria		12	30/Mayo	14/Junio																	
2	**Fundamentos de redes de computadoras**																						
2.1	Estudio de protocolos de red (IPv4, IPv6)	Curso en linea		6	30/Mayo	6/Junio																	
2.2	Estudio de protocolos de aplicación mas utilizados (DNS, HTTP, HTTPS, etc.)	Curso en linea	2.2	12	7/Junio	22/Junio																	
3	**Manejo de herramientas**																						
3.1	Estudio de uso de sistema operativo Linux y herramientas basicas	Curso en linea		12	30/Mayo	14/Junio																	
3.2	Conocer y utilizar scripts utilizados por el equipo	Autoestudio / Tutoria	3.1	10	15/Junio	28/Junio																	
3.3	Estudiar la automatizacion de actividades realizada por el equipo	Tutoria	3.2	10	29/Junio	12/Julio																	
4	**Interaccion con el cliente**																						
4.1	Estudio de estilo de comunicación realizado por el equipo	Autoestudio / Tutoria		10	23/Junio	6/Julio																	
5	**Colaboracion**																						
5.1	Atender y estudiar la participacion en los canales de comunicación del equipo	Autoestudio		6	15/Junio	22/Junio																	
5.2	Conocer y estudiar la colaboracion en la documentacion para el equipo	Autoestudio / Tutoria		12	15/Junio	30/Junio																	

2.5 Equipo de Trabajo

Rol	*Responsabilidad*	*Nombre (opcional)*
Líder de analistas	*Asignación de equipos* *Asignación de clientes*	*Attack Surface Analyst Team Lead*
Analista	*Manejo de amenazas* *Descubrimiento de superficies de ataque* *Atención a solicitudes del cliente* *Validación de superficies de ataque* *Desarrollo de automatización de análisis*	*Attack Surface Analyst*
Intern	*Descubrimiento de superficies de ataque* *Atención a solicitudes del cliente* *Validación de superficies de ataque*	*Sarah Lizeth Muriel Ramirez*

2.6 Plan de Comunicaciones

Emisor	*Mensaje*	*Receptor*	*Medio*	*Frecuencia*
Intern	*Reporte*	*Líder de equipo*	*Plataforma y video conferencia*	*d*
Intern	*Reporte*	*Líder de analistas*	*Plataforma*	*s*
Intern	*Informacion*	*Líder de analistas*	*Videoconferencia*	*2s*
Estudiante	*Documento*	*Profesor PAP*	*Plataforma*	*3s*
Estudiante	*Documento*	*Profesor PAP*	*Videoconferencia*	*3s*

2.7 Plan de Calidad

Emisor: *Quién Entrega*	***Entregable:*** *Qué Entrega (SubEntregable)*	***Receptor:*** *Quién recibe o Inspecciona*	***Criterios:*** *Condiciones de Aceptación*	***Siguiente paso.*** *Donde va Cuando se Autoriza.*
Intern	*Reporte*	*Analista*	*Cumple procedimiento y/o realiza necesidad del cliente*	*Reporte a cliente y/o seguimiento por el equipo de Operación de Pruebas de Penetración*

2.8 Seguimiento y Control

Se reporta diariamente lo que se planea realizar durante el día de trabajo y lo que se realizó el día previo de manera escrita, posteriormente se reporta al líder del equipo de manera oral en una videoconferencia que abarca a todos los miembros del equipo. Se realiza un reporte semanal al líder de analistas de manera escrita, adicionalmente se realiza una videoconferencia uno a uno con el líder de analistas cada dos semanas.

Se entrega un avance del documento a redactar para su revisión por el profesor PAP, posteriormente se tiene una sesión de revisión uno a uno por medio de una videoconferencia y se determina los cambios a realizar en el documento para su posterior entrega.

3. Resultados del Trabajo Profesional

3.1 Productos Obtenidos

Durante mi participación en el proyecto produje principalmente reportes respecto al descubrimiento y validación de la superficie de ataque, y contribuí al histórico de la superficie de ataque de los clientes asignados.

3.2 Estimación del Impacto

Los reportes respecto al descubrimiento y validación de la superficie de ataque producidos durante el proyecto contribuyen a la habilitación de la realización de trabajo de pruebas de penetración y la entrega al cliente del nivel de servicio estipulado. Mis contribuciones al histórico de la superficie de ataque de los clientes asignados son utilizadas para la continuidad de actividades que realiza el equipo de Inteligencia de Superficies de Ataque parte del servicio de Cosmos, aumentando la eficiencia y efectividad del equipo, y por lo tanto, del servicio.

4. Reflexiones del alumno

4.1 Aprendizajes Profesionales

Las competencias técnicas más importantes que desarrolle durante el proyecto fueron dos, la primera, directamente relacionada a la seguridad informática, fue la investigación de fuentes abiertas, y la segunda, adicionalmente relacionada a redes de computadoras, fue el manejo de protocolos de red para el descubrimiento de superficies de ataque. Otras competencias técnicas genéricas que desarrolle fueron el manejo de herramientas diversas que son útiles para cualquier ámbito en el que se trabaje con sistemas computacionales. La principal competencia suave que desarrolle durante el proyecto fue la colaboración.

Durante el proyecto pude poner en práctica varios de los conocimientos que he adquirido durante mi educación universitaria, sin embargo la habilidad principal que ha sido integral para lograr los objetivos del proyecto ha sido el autoaprendizaje. Existe un gran número de habilidades y conocimientos que solo pude adquirir por medio de la experiencia, a diferencia del enfoque académico que se maneja en la universidad.

4.2 Aprendizajes Sociales

Durante el desarrollo del proyecto pude ver las repercusiones en el mundo real que puede tener la seguridad informática, e inversamente, las repercusiones que los eventos que ocurren en el mundo tienen en la seguridad informática. Estuve presente durante periodos de crisis en la seguridad informática y pude presenciar como miembros de mi equipo trabajaron en herramientas libremente distribuidas para mantener la seguridad informática de todo el mundo, no solo de los clientes asignados.

Adicionalmente, forme parte del primer grupo de Interns de origen mexicano dentro de los equipos que forman el servicio Cosmos de Bishop Fox, contribuyendo a la expansión de la compañía dentro del país y ayudando a cimentar el camino por el que podrán pasar futuros Interns mexicanos.

4.3 Aprendizajes Éticos

Durante el proyecto fue sumamente importante entender la importancia de la informacion con la que se trata al realizar tareas de seguridad informática, por lo tanto es igualmente importante contar con una ética y sentido de responsabilidad que se alinea con lo que la compañía espera.

También me enfrente a que durante el desarrollo del proyecto, debido a la naturaleza de las actividades de monitoreo de superficies de ataque, ocurre el encontrar fallos y vulnerabilidades que no pertenecen a la superficie de ataque del cliente con el que se trabaja. Lo encontrado puede representar un riesgo inminente para quien le pertenece, por lo tanto es parte de las decisiones que se deben tomar en la seguridad informática el cómo tratar estas situaciones.

4.4 Aprendizajes Personales

Durante el proyecto formé parte de un equipo conformado por personas provenientes de diferentes países del mundo, cada una de ellas con experiencias laborales y educativas diferentes antes de formar parte del equipo, con las cuales tuve la oportunidad de colaborar y convivir buscando una meta en común. Fue una experiencia importante el formar parte de un equipo en el que todos los miembros participan de manera equitativa.

Pude ver cuales habilidades son el fuerte de cada miembro del equipo, como las han desarrollado, y como desarrollarlas personalmente. También, pude evaluar cuales habilidades me gustaría desarrollar a futuro y como estas pueden ser útiles en la rama de la de la seguridad informática que he elegido relacionada a la inteligencia y análisis.

4.5 Tareas Aprendidas

El principal factor de éxito para los resultados del proyecto fue el contar con la disposición de todos los miembros del equipo para responder preguntas y dar tutorías, lo cual permitió inicialmente asistir a los miembros de equipo con tareas que me permitieron obtener experiencia y posteriormente poder realizar las actividades del proyecto con supervisión o por mi misma. Otro factor importante fue el contar con un tiempo establecido de reunión con el líder de equipo periódicamente, durante el cual pude hacer preguntas y enfocarme para poder lograr mis metas personales respecto al proyecto.

Una actitud personal que resulto necesaria para el desarrollo del proyecto fue la iniciativa propia, durante el proyecto fue necesario el autoestudio para realizar actividades y utilizar herramientas hasta ese momento desconocidas para mí, y también fue necesario interactuar con los miembros del equipo para encontrar oportunidades de aprendizaje durante las actividades diarias de trabajo a realizar.

5. Conclusiones

El haber participado en este proyecto resulto sumamente importante para mi desarrollo personal y profesional. El integrarme a esta empresa ha sido mi primera experiencia laboral y mi primera interacción profesional con el mundo de la seguridad informática, y simultáneamente ha sido la primera experiencia con interns mexicanos para el equipo al cual me integre. Durante la duración del proyecto pude interactuar con los miembros del equipo, aprendiendo sobre sus orígenes, los cuales van desde el sector financiero hasta el sector militar, y pudiendo ver las diferentes formas en las que se puede llegar a llenar un rol en áreas de la seguridad informática relacionadas a la inteligencia. Debido a que Bishop Fox es una empresa relativamente pequeña comparada con las grandes empresas tecnológicas que suelen dominar la industria, me fue posible llegar a conocer empleados de diferentes áreas y niveles que se ven interconectados con el puesto en el que estuve trabajando durante el proyecto.

Al ser la primera vez realizando trabajo no académico, pude evaluar el nivel de los conocimientos que he adquirido a través de mis estudios universitarios contra los conocimientos y habilidades requeridos para realizar las actividades presentes en un trabajo de la industria. El proyecto en el que participe estuvo estructurado de manera que pude experimentar integralmente el cómo es realizar el trabajo del puesto para el que se habilita el intern, en mi caso para el rol de analista de superficie de ataque.

Al finalizar el proyecto obtuve los objetivos esperados, obtuve los conocimientos y habilidades necesarios para desarrollar las tareas, pero más allá de ello obtuve experiencia trabajando de manera conjunta y experimente por primera vez lo que conlleva un trabajo dentro de la industria con la que se encuentra relacionada mi carrera universitaria, preparándome para los siguientes pasos a tomar tras la conclusión de mis estudios.