Biblioteca INFOTEC

Ciudad de México, a 28 de abril de 2025

VISTO BUENO DE TRABAJO TERMINAL

Técnico Superior Universitario en Ciberseguridad

UNIDAD DE POSGRADOS
PRESENTE

Por medio de la presente se hace constar que el **Reporte final** desarrollado por el alumno: **Juan Carlos Bonifacio Ramírez** cumple con el formato de Biblioteca, así mismo, se ha verificado la correcta citación para la prevención del plagio; por lo cual, se expide la presente autorización para entrega en digital del proyecto terminal al que se ha hecho mención. Se hace constar que el alumno no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión digital del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Dr. Juan Antonio Vega Garfias
Subgerente de Innovación Gubernamental

JAVG/jah

C.c.p. Mtra. Analy Mendoza Rosales. – Encargada de la Gerencia de Capital Humano. - Para su conocimiento.
Juan Carlos Bonifacio Ramírez. – Alumno Técnico Superior Universitario en Ciberseguridad.- Para su conocimiento.

Reporte final

Datos eliminados: matrícula, correo, celular, teléfono; con fundamento en lo establecido en los artículos 65, fracción II, 98, fracción III, 113, fracción I y último párrafo de la Ley Federal de Transparencia y Acceso a la Información Pública, 44, fracción II, 106, fracción III y 116 de la Ley General de Transparencia y Acceso a la Información Pública, así como a lo establecido en los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas, por tratarse de datos personales concernientes a una persona física identificada, en la modalidad de confidencial. Área Dirección Adjunta de Innovación y Conocimiento. Periodo indefinido, toda vez que no está sujeta a temporalidad alguna y solo podrán tener acceso a ella los titulares de la misma. Aprobada en la Primera Sesión Extraordinaria del Comité de Transparencia de INFOTEC ejercicio 2025.

Índice

Introducción

En este reporte se muestra de manera simplifica el desarrollo de las prácticas profesionales que realicé en INFOTEC en el departamento de ciberseguridad, en las cuales se me asignó la tarea de llevar a cabo un análisis de vulnerabilidades para algunos sitios web.

Durante las prácticas fue necesario adquirir nuevos conocimientos, principalmente en el uso de herramientas especializadas, así como la aplicación de conceptos adquiridos durante el desarrollo de las actividades académicas del programa de técnico superior universitario en ciberseguridad.

Los aprendizajes que obtuve durante el desarrollo de las prácticas profesionales me serán de utilidad para lograr mi objetivo profesional de migrar hacia el campo de la ciberseguridad en un futuro próximo.

Práctica profesional

Datos personales del estudiante			
Nombre completo:	Juan Carlos Bonifacio Ramírez		
Matrícula:	Eliminado	Teléfono:	Eliminado
Correo:	Eliminado		
Especialidad de TSU:	Ciberseguridad		
Año:	2024	Celular:	Eliminado
Número de horas de práctica profesional:		280 horas cubiertas	

Datos de la institución	
Nombre de la institución:	INFOTEC
Departamento en el que realizarás tus prácticas:	Departamento de ciberseguridad
Nombre de la persona responsable del departamento:	Arturo Montoya

Estructura organizacional

El INFOTEC es un Centro Público de Investigación del Gobierno Federal, que contribuye a la Transformación Digital de México, a través de la investigación, la innovación, la formación académica y el desarrollo de productos y servicios TIC. Sus alcances abarcan al sector público y privado, habilitando caminos que conduzcan hacia un México moderno y de inclusión digital (www.infotec.mx/Infotec).

El INFOTEC se creó a través de un fideicomiso denominado Fondo de Información y Documentación para la Industria, con la finalidad de establecer un mecanismo de comunicación y transferencia de conocimientos científicos y tecnológicos existentes en el país y en el extranjero (Manual de organización de INFOTEC).

La estructura del INFOTEC se compone de las siguientes direcciones:

- Dirección ejecutiva
- Dirección de administración y finanzas
- Dirección de asuntos jurídicos
- Dirección de innovación, investigación y academia
- Dirección de infraestructura y seguridad de la información
- Dirección de desarrollo de aplicaciones y productos
- Dirección comercial

En particular, las prácticas de la estancia profesional las realizo en la Dirección de infraestructura y seguridad de la información, en el área de ciberseguridad.

Tengo asignadas las tareas relacionadas con el análisis de vulnerabilidades de cada uno de los sitios asignados.

Para mi estancia tengo que trabajar con los siguientes sitios:

- Plataformas-dadt.infotec.mx (207.249.96.179)
- Zabbix-42.infotec.mx (207.249.101.66)
- Console.infotec.mx (207.249.123.161)
- Infotec.repositorioinstitutcional.mx/jspui/ (207.249.123.186)
- Espacioeducativo.infotec.mx/ (207.249.28.17)
- Biblioteca-intra.infotec.mx/ (207.249.96.141)

Una vez que se realiza el análisis de vulnerabilidades con herramientas como Nikto, se deben buscar las referencias de la vulnerabilidad para entender su alcance e integrarlas al reporte correspondiente.

En particular, las actividades se dividieron del siguiente modo:

- Revisión de principales herramientas usadas para el análisis de vulnerabilidades
- Instalación del software necesario para las pruebas a sitios web
- Reconocimiento de sitios web y escaneo de puertos
- Pruebas de vulnerabilidad a los puertos susceptibles de recibir ataques
- Entendimiento y descripción de las vulnerabilidades encontradas
- Integración del reporte técnico de vulnerabilidades
- Reuniones semanales de seguimiento de actividades

- Bitácora de prácticas

Semanas	Actividades realizadas	Observaciones
1 a 2	Revisión de conceptos de ciberseguridad y realización de pruebas de pentesting Instalación de máquina virtual y Kali Linux, revisión de documentación de Kali para conocer a fondo los comandos a usar durante la realización de pruebas	Fue necesario repetir el proceso de instalación en algunos casos
3 a 4	Identificación de sitios asignados y la función que cumplen Primeras pruebas de herramientas a utilizar	
5 a 6	Escaneo de puertos para cada sitio web asignado Confirmación del escaneo mediante una segunda herramienta	Para algunos sitios el escaneo de puertos tardaba más de lo esperado y era necesario ajustar

		parámetros de los comandos utilizados para el escaneo
7 a 8	Integración de la primera parte del reporte de vulnerabilidades Identificación de puertos a explotar	
9 a 10	Análisis de vulnerabilidades Confirmación de primeros resultados mediante el uso de una segunda herramienta Entendimiento de vulnerabilidades encontradas Integración y clasificación de vulnerabilidades en el reporte técnico	
11 a 12	Análisis de vulnerabilidades Confirmación de primeros resultados mediante el uso de una segunda herramienta Entendimiento de vulnerabilidades encontradas Integración y clasificación de vulnerabilidades en el reporte técnico	

Conclusiones

Durante la estancia profesional logré integrar una serie de habilidades técnicas a mis habilidades actuales, pude aplicar técnicas de pentesting y con ello entender mejor el camino que se debe tomar para realizar este tipo de pruebas. Desde cuáles son las herramientas adecuadas para realizar el análisis hasta las implicaciones éticas y legales que pueden tener la realización de dichas pruebas.

En cada reporte describí una parte de las actividades realizadas, conforme estas se desarrollaban y sin tener un conocimiento pleno del rumbo que tomarían las pruebas.

Puedo señalar que la realización de reuniones de seguimiento continuas fue crucial para que las actividades se llevarán a cabo de manera continua y a un ritmo que permitió lograr los objetivos planteados al inicio de las prácticas.

La integración de los reportes técnicos fue un aprendizaje que considero muy útil para mi futuro profesional, ya que me permitió entender la esencia de este tipo de reportes en el ámbito profesional y conocer cuáles son las mejores prácticas que se deben seguir para lograr que estos reportes cumplan con su función hacia los clientes o usuarios de dichos reportes. Estos reportes cumplen todo un ciclo cuando es posible implementar la solución que elimina o disminuye el riesgo de sufrir un ataque por parte de agentes maliciosos. Considero que solo me hizo falta llegar al punto de realizar la explotación de vulnerabilidades de manera completa, para así ver de manera integral el ciclo que se sigue en ciberseguridad, pero lo visto en las prácticas me resulta sumamente útil.

Cuadro CQA de mi estancia en la organización

C ¿Qué **C**onozco?	Q ¿**Q**ué aporte?	A ¿Qué **A**prendí?
El alcance del campo de la ciberseguridad La importancia de la ciberseguridad en la actualidad y su posible futuro Conceptos usados en ciberseguridad La importancia de la comunicación para mostrar los resultados obtenidos	Capacidad de análisis en situaciones diversas Capacidad para encontrar información que me permita entender los escenarios que se presentan Planteamiento de dudas en las reuniones semanales que apoyaron a otros compañeros	Técnicas de escaneo de puertos Cómo realizar un análisis de vulnerabilidades Cómo buscar información de las vulnerabilidades encontradas Cómo integrar un reporte técnico

Evaluación de desempeño

En general, puedo describir mi desempeño como bueno, ya que se lograron los objetivos planteados al inicio de las prácticas, si bien se tuvieron algunos problemas con el tiempo que tomó el desarrollo de las prácticas en algunos momentos, al final logré completar las actividades asignadas.

Me hubiese gustado contar con más tiempo para llevar el análisis de vulnerabilidades hacia la explotación plena de dichas vulnerabilidades, lo cual hubiese sido sumamente enriquecedor al conocer la parte ofensiva de la ciberseguridad.

Los conceptos que aprendí durante el programa de técnico superior universitario en ciberseguridad me resultaron cruciales para el desarrollo de las actividades y pude apreciar cómo estos se relacionaban en las distintas técnicas que se aplicaban en las vulnerabilidades detectadas. También pude apoyarme en las notas de los cuatrimestres que cursé para volver a los temas que me hacía falta recordar para que las actividades se completaran de mejor manera.

Lo aprendido durante las prácticas profesionales me resultará útil para lograr las metas personales y profesionales que me he planteado para los próximos años.

Referencias

Reglamento interior de trabajo del INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. Tomado de https://www.infotec.mx/work/models/Infotec/normateca/admin/reglamento_interior_de_trabajo_del_infotec.pdf

Manual de organización de INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. Tomado de https://www.diputados.gob.mx/LeyesBiblio/norma/manual/man352_01jul24.pdf