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 la alumna: **Bricia Almaraz Cruz** 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 la alumna 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.
Bricia Almaraz Cruz. – Alumna Técnico Superior Universitario en Ciberseguridad.- Para su conocimiento.

Reporte final

Por Bricia Almaraz Cruz

Datos eliminados: matrícula, correo, celular; 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.

Reporte final

Persona estudiante: Bricia Almaraz Cruz

TSU: Ciberseguridad.

Primera revisión: 25 de noviembre de 2024
Segunda revisión: 24 de enero de 2025

Índice

Contenido

Introducción

En la actualidad las organizaciones esperan que el personal se encuentre capacitado en áreas tecnológicas, pero, además, demandan competencias interpersonales o habilidades blandas necesarias para el desempeño exitoso profesional.

Los procesos administrativos en las organizaciones son vehículos para potenciar las capacidades humanas, estructuran y organizan actividades que promueven el crecimiento personal o profesional. Están diseñados para garantizar un funcionamiento eficiente y proporcionar una base sólida para el desarrollo profesional de quienes se incorporan al ámbito laboral. Reconociendo que, si bien las habilidades técnicas permiten llevar a cabo un trabajo físico, las habilidades blandas garantizan que se pueda trabajar coordinadamente en equipo de trabajo llevando a cabo una comunicación efectiva. Estas habilidades permiten que los miembros del grupo se entiendan mucho mejor, se apoyen entre ellos y trabajen hacia objetivos comunes, incluso en situaciones de presión.

La invitación para llevar a cabo mi estancia en INFOTEC fue ese impulso que necesitaba para notar la gran oportunidad, abriéndome los ojos a nuevas perspectivas. Al analizar de forma directa la identidad, organización y estructura de INFOTEC, reconocí su compromiso con la sociedad mexicana en el aspecto tecnológico, el funcionamiento de sus áreas, sus estándares académicos altos, el acceso a recursos, tecnologías y profesores de excelencia, así como su gran trayectoria en general.

Durante el desarrollo de la estancia aprendí a realizar el procedimiento para reconocer vulnerabilidades en aplicativos mediante escaneos con herramientas avanzadas, en un horario planificado y bajo la observación del asesor en todo momento, permitiendo identificar puertos UDP y TCP. Aprendí a configurar una máquina virtual y el uso de comandos Kali Linux.

Esta estancia en INFOTEC representa un proceso continuo de aprendizaje que me ha permitido descubrir conocimientos técnicos y habilidades. De forma general, cada una de las materias y mentorías que se llevaron a cabo durante la carrera TSU Ciberseguridad me permitió obtener habilidades clave, logrando ver el camino hacia nuevas posibilidades de desarrollo. Aunque sin duda es una carrera en constante cambio, la experiencia es enriquecedora, la formación es de calidad, preparándonos para enfrentar desafíos reales en el mundo laboral, impulsándonos y dándonos la pauta a especializarnos sobre temas de interés y el establecimiento de objetivos específicos profesionales.

Práctica profesional

Datos personales del estudiante			
Nombre completo:	Bricia Almaraz Cruz		
Matrícula:	[redacted]	Teléfono:	[redacted]
Correo:	[redacted]		
Especialidad de TSU:	Tecnologías Emergentes, de la Información, de Internet y la nube.		
Año:	2024	Celular:	[redacted]
Número de horas de práctica profesional:		280 horas.	

Datos de la institución	
Nombre de la institución:	Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC).
Departamento en el que realizarás tus prácticas:	Dirección Adjunta de Desarrollo Tecnológico.
Nombre de la persona responsable del departamento:	Ing. Ulises Arturo López Montoya

Estructura organizacional

- **El sector de actividad**

INFOTEC, se encuentra en el sector de servicios y consultoría de TI.

- **Presentación e historia de la empresa**

INFOTEC, es un Centro Público Educativo, de Investigación y desarrollo de productos y servicios TIC del Gobierno Federal, fundada en 1974, con sede en la Ciudad de México. Dentro de la formación académica ofrecen estudios en Posgrados, Educación Continua y Maestrías en TIC's. Abarcando tanto al sector público como al privado.

"[…] impulsamos la innovación como el motor de transformación de nuestra comunidad y del país al que servimos; contagiamos el espíritu de colaboración y compromiso para lograr nuestros propósitos; somos transparentes con el uso de recursos y en la toma de decisiones; estamos abiertos a escuchar ideas, propuestas y pensamientos divergentes; y aspiramos a ser congruentes y confiables en nuestro quehacer y en el cumplimiento de los compromisos que adquirimos […]"

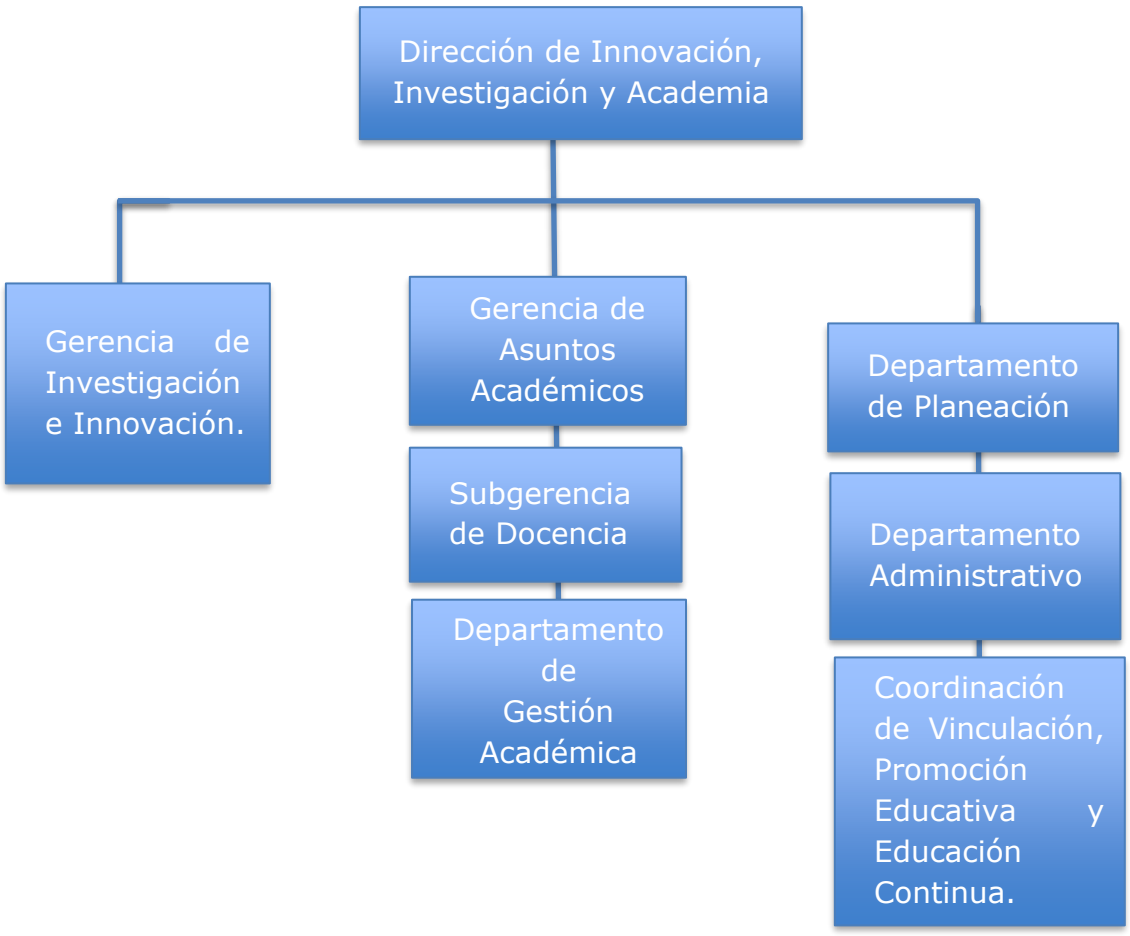
No es difícil darse cuenta de que la identidad corporativa del centro de investigación INFOTEC es muy sólida, ya que se trata de una Institución mexicana con más de 40 años de trayectoria, dedicada a impulsar el desarrollo e inclusión tecnológica del país.

Su logotipo es un elemento clave de su identidad siendo un centro público de investigación perteneciente a la red de centros del Consejo Nacional de Ciencia y Tecnología CONAHCYT, su tipografía con estilo minimalista permite proyectar una imagen seria y profesional, pero no solo se define por el logotipo, la tipografía y los colores, sino que le ha llevado a un proceso donde con hechos ha definido sus elementos representativos acordes con su visión, misión, valores y cultura dando coherencia.

Organización INFOTEC.

De acuerdo con el Manual de organización aprobado en el 2024, de forma oficial disponible en: https://infotec.mx/work/models/Infotec/Resource/22/37/images/Manual_Organizacion_INFOTEC_2024.pdf. El área donde se realizó esta práctica se encuentra a cargo de la Dirección de Innovación, Investigación y Academia, la cual se compone de las siguientes áreas:

- **Organigrama.**



Informe de la práctica profesional

- **Descripción de las funciones.**

La finalidad de esta práctica es identificar la existencia de vulnerabilidades conocidas en las aplicaciones INFOTEC y analizar, si es posible, la explotación de estas por parte de un potencial atacante, midiendo el nivel de intrusión que podría obtener.

- **Desglose de actividades.**

La primera fase de la gestión de vulnerabilidades se denomina ***"Reconocimiento o Footprinting"*** el cual es un proceso mediante el cual se recopilan datos sobre una red, un sistema, u organización a fin de comprender su estructura y vulnerabilidades y así determinar el tipo de ataque. En este caso, se llevó a cabo el método de footprinting activo mediante el uso de la herramienta de escaneo de puertos, Nmap, con el cual se analizó el sistema objetivo para recopilar información más detallada sobre pruebas de respuesta de servidores y consultas a servicios de red. (Peña (2021). Escaneo y enumeración).

- **Herramientas y técnicas utilizadas para el reconocimiento.**

- Consulta de Whois,
- Detecciones de direcciones IP,
- Nombres de dominio,
- Configuración de red (tamaño),
- Escaneo de puertos abiertos,
  - ICMP
  - TCP
  - UDP
- Ubicación de sistemas en vivo,
- Servicios en ejecución,
- Software utilizado y
- Versión de sistemas operativos.

Después del reconocimiento, se procedió a la investigación de vulnerabilidades por medio de la herramienta Nikto en Kali Linux. Posterior a esto, se documentan todos los pasos y evidencias obtenidas durante el reconocimiento para poder crear un informe detallado de cada una de las aplicaciones donde se señalan las principales vulnerabilidades encontradas con la herramienta Nikto.

Nota: Cumpliendo el primer objetivo se sigue a la explotación de vulnerabilidades, la obtención de acceso y la mitigación de riesgos, sin embargo, para fines de esta estancia, no se llevó a cabo.

Bitácora de práctica (Semana 1 a 2)

Semana	Actividades realizadas	Observaciones
1 a 2	A. (Recopilación de información sobre la aplicación **cloud.infotec.mx**). El reconocimiento u obtención de huellas es un proceso que consta de recopilar información del dispositivo, navegador o red que utiliza la aplicación. Esta parte del reconocimiento se divide en tres partes: **1. Huella:** De manera pasiva, se recopilan datos e información sobre la organización: • Descubrir Sistema de Nombres de Dominio (DNS). • Consulta del Whois. • Búsqueda y análisis de la información obtenida en la red pública de internet. **2. Escaneo:** Aquí es donde ya se utilizan los métodos y herramientas de reconocimiento activo, como el escaneo de Nmap, para extraer información sobre la red y/o sistema. **3. Enumeración:** Posterior a completar la huella y el escaneo, se utiliza la herramienta Nikto para determinar el área de ataque. B. Retroalimentación del profesor. C. Elaboración del Informe Ejecutivo con: • Lista de Vulnerabilidades. D. Búsqueda de información relacionada con la vulnerabilidad detectada para observar él: • Grado de severidad (baja, media, alta o crítica). • Impacto potencial de cada vulnerabilidad. • Sugerencias para corregir cada vulnerabilidad y elevar la seguridad general de la aplicación.	Mantener y mejorar la conexión a internet, así como la descarga y configuración de la máquina virtual en Kali Linux, descarga de herramientas que se requieren como Nmap, Nikto. Resolución de contratiempos relacionados con la máquina, se desarrolla un plan de trabajo para realizar cada una de las actividades de forma coordinada.
Durante la estancia se llevaron a cabo actividades complementarias entregadas en aula virtual, de la cual grosso modo de la primera unidad se realizaron lecturas las cuales tratan básicamente en introducirnos a los procesos administrativos que se siguen dentro de una organización con la finalidad de obtener conocimientos y criterios suficientes para incorporarnos al ámbito laboral.		

Bitácora de práctica (Semana 3 a 4)

Semana	Actividades realizadas	Observaciones
3 a 4	A. (Recopilación de información sobre la aplicación **zabbix-106.infotec.mx**). El reconocimiento u obtención de huellas es un proceso que consta de recopilar información del dispositivo, navegador o red que utiliza la aplicación. Esta parte del reconocimiento se divide en tres partes: **1. Huella:** De manera pasiva, se recopilan datos e información sobre la organización: E. Descubrir Sistema de Nombres de Dominio (DNS). F. Consulta del Whois. G. Búsqueda y análisis de la información obtenida en la red pública de internet. **2. Escaneo:** Aquí es donde ya se utilizan los métodos y herramientas de reconocimiento activo, como el escaneo de Nmap, para extraer información sobre la red y/o sistema. **3. Enumeración:** Posterior a completar la huella y el escaneo, se utiliza la herramienta Nikto para determinar el área de ataque. B. Retroalimentación del profesor. C. Elaboración del Informe Ejecutivo con: H. Lista de Vulnerabilidades. D. Búsqueda de información relacionada con la vulnerabilidad detectada para observar él: I. Grado de severidad (baja, media, alta o crítica). J. Impacto potencial de cada vulnerabilidad. K. Sugerencias para corregir cada vulnerabilidad y elevar la seguridad general de la aplicación. E. Desarrollo de actividades 1 y 2 de la materia de Estancia en aula virtual.	Para continuar con la práctica es necesario la retroalimentación del profesor, misma que se ha llevado a cabo de forma puntual donde se me ha permitido expresar mis dudas y de esa forma he recibido el feedback para continuar. Aunado a que esta aplicación ya fue retirada por cuestiones de seguridad, lo que nos explicó el asesor Arturo López M.

Unidad 2: Incorporación a la vida laboral.

El ámbito de las Tecnologías de la Información (TI), se encuentra en constante evolución lo que requiere una combinación de habilidades técnicas y competencias interpersonales para destacar, por lo que de acuerdo con el material proporcionado: lecturas, videos y sesiones grabadas, se pudo comprender la importancia del desarrollo de las siguientes actividades:

- Actividad 1. Bolsa de trabajo en el área de TI
- Actividad 2. Desarrollo de Currículum.

Bitácora de práctica (Semana 5 a 6)

Semana	Actividades realizadas	Observaciones
5 a 6	A. (Recopilación de información sobre la aplicación **portal-psp.infotec.mx**). El reconocimiento u obtención de huellas es un proceso que consta de recopilar información del dispositivo, navegador o red que utiliza la aplicación. Esta parte del reconocimiento se divide en tres partes: **1. Huella:** De manera pasiva, se recopilan datos e información sobre la organización: • Descubrir Sistema de Nombres de Dominio (DNS). • Consulta del Whois. • Búsqueda y análisis de la información obtenida en la red pública de internet. **2. Escaneo:** Aquí es donde ya se utilizan los métodos y herramientas de reconocimiento activo, como el escaneo de Nmap, para extraer información sobre la red y/o sistema. **3. Enumeración:** Posterior a completar la huella y el escaneo, se utiliza la herramienta Nikto para determinar el área de ataque. B. Retroalimentación del profesor. C. Elaboración del Informe Ejecutivo con: • Lista de Vulnerabilidades. D. Búsqueda de información relacionada con la vulnerabilidad detectada para observar él: • Grado de severidad (baja, media, alta o crítica). • Impacto potencial de cada vulnerabilidad. • Sugerencias para corregir cada vulnerabilidad y elevar la seguridad general de la aplicación.	Constantemente estoy revisado documentos y videos. Esto me permite aprender a resolver al momento mis dudas y aprendiendo nuevas formas de hacer las cosas y mejorando mis habilidades, ya que muchos vienen en idioma inglés.

Unidad 3: Reporte Fase 1. Organización en el trabajo.

Gracias a las lecturas de apoyo y sesiones grabadas en esta unidad, se comprendió el objeto de estudio permitiendo analizar la identidad, organización y estructura de la empresa para llevar a cabo la estancia, reconociendo en INFOTEC su compromiso con la sociedad mexicana en el aspecto tecnológico, el funcionamiento de sus áreas y su gran trayectoria en general.

Bitácora de práctica (Semana 7 a 8)

Semana	Actividades realizadas	Observaciones
7a 8	A. (Recopilación de información sobre la aplicación **207.249.123.243:8898/**). El reconocimiento u obtención de huellas es un proceso que consta de recopilar información del dispositivo, navegador o red que utiliza la aplicación. Esta parte del reconocimiento se divide en tres partes: **1. Huella:** De manera pasiva, se recopilan datos e información sobre la organización: • Descubrir Sistema de Nombres de Dominio (DNS). • Consulta del Whois. • Búsqueda y análisis de la información obtenida en la red pública de internet. **2. Escaneo:** Aquí es donde ya se utilizan los métodos y herramientas de reconocimiento activo, como el escaneo de Nmap, para extraer información sobre la red y/o sistema. **3. Enumeración:** Posterior a completar la huella y el escaneo, se utiliza la herramienta Nikto para determinar el área de ataque. B. Retroalimentación del profesor. C. Elaboración del Informe Ejecutivo con: • Lista de Vulnerabilidades. D. Búsqueda de información relacionada con la vulnerabilidad detectada para observar él: • Grado de severidad (baja, media, alta o crítica). • Impacto potencial de cada vulnerabilidad. • Sugerencias para corregir cada vulnerabilidad y elevar la seguridad general de la aplicación.	Optimizar y gestionar el tiempo para llevar a cabo las lecturas que se facilitaron para llevar a cabo los reportes de actividades en plataforma
Unidad 4: Reporte Fase 2. Habilidades Profesionales. Se llevaron a cabo para esta unidad análisis de material proporcionado: lecturas, videos y sesiones grabadas. Reconociendo que, si bien las habilidades técnicas permiten llevar a cabo un trabajo físico, las habilidades blandas garantizan que se pueda trabajar coordinadamente en equipo de trabajo llevando a cabo una comunicación efectiva.		

Bitácora de práctica (Semana 9 a 10)

Semana	Actividades realizadas	Observaciones
9 a 10	A. (Recopilación de información sobre la aplicación **posgrados.infotec.mx.**). El reconocimiento u obtención de huellas es un proceso que consta de recopilar información del dispositivo, navegador o red que utiliza la aplicación. Esta parte del reconocimiento se divide en tres partes: **1. Huella:** De manera pasiva, se recopilan datos e información sobre la organización: • Descubrir Sistema de Nombres de Dominio (DNS). • Consulta del Whois. • Búsqueda y análisis de la información obtenida en la red pública de internet. **2. Escaneo:** Aquí es donde ya se utilizan los métodos y herramientas de reconocimiento activo, como el escaneo de Nmap, para extraer información sobre la red y/o sistema. **3. Enumeración:** Posterior a completar la huella y el escaneo, se utiliza la herramienta Nikto para determinar el área de ataque. B. Retroalimentación del profesor. C. Elaboración del Informe Ejecutivo con: • Lista de Vulnerabilidades. D. Búsqueda de información relacionada con la vulnerabilidad detectada para observar él: • Grado de severidad (baja, media, alta o crítica). • Impacto potencial de cada vulnerabilidad. • Sugerencias para corregir cada vulnerabilidad y elevar la seguridad general de la aplicación.	Atender las indicaciones en la plataforma respecto a las actividades pendientes y las lecturas proporcionadas para llevar a cabo dichas actividades. Continuar con el objetivo de terminar el análisis sobre el aplicativo.
Unidad 5. Reporte Fase 3. Conclusión del informe y Reporte final. Reflexión sobre los conocimientos y habilidades adquiridos en Tecnologías de la Información. En la actualidad la evaluación de competencias es sumamente importante, por lo que las organizaciones esperan que los interesados combinen habilidades técnicas con capacidades de negocio e interpersonales.		

Bitácora de práctica (Semana 11 a 12)

Semana	Actividades realizadas	Observaciones
11 a 12	A. (Recopilación de información sobre la aplicación **biblioteca.infotec.mx.**). El reconocimiento u obtención de huellas es un proceso que consta de recopilar información del dispositivo, navegador o red que utiliza la aplicación. Esta parte del reconocimiento se divide en tres partes: **1. Huella:** De manera pasiva, se recopilan datos e información sobre la organización: • Descubrir Sistema de Nombres de Dominio (DNS). • Consulta del Whois. • Búsqueda y análisis de la información obtenida en la red pública de internet. **2. Escaneo:** Aquí es donde ya se utilizan los métodos y herramientas de reconocimiento activo, como el escaneo de Nmap, para extraer información sobre la red y/o sistema. **3. Enumeración:** Posterior a completar la huella y el escaneo, se utiliza la herramienta Nikto para determinar el área de ataque. B. Retroalimentación del profesor. C. Elaboración del Informe Ejecutivo con: • Lista de Vulnerabilidades. D. Búsqueda de información relacionada con la vulnerabilidad detectada para observar él: • Grado de severidad (baja, media, alta o crítica). • Impacto potencial de cada vulnerabilidad. • Sugerencias para corregir cada vulnerabilidad y elevar la seguridad general de la aplicación.	Se realizan el escaneo de la aplicación acorde a lo que se había establecido inicialmente para hacer la entrega en tiempo y forma. Entrega de reportes finales.

Conclusiones

El desarrollo de los reportes finales, implicaron la recopilación y el análisis de la información previamente recabada, tratando de dar sentido de manera clara y concisa. La comunicación entre el asesor y nosotros los practicantes ha sido efectiva lo que ha permitido cumplir el objetivo de realizar el reconocimiento de vulnerabilidades sobre cada uno de los aplicativos llevando a cabo una metodología, y documentarme para llevar a cabo el análisis de resultados de cada uno de ellos, sobre todo el aprendizaje que ha sido significativo.

Tal cual si fuéramos todos unos hackers éticos utilizamos los conocimientos y habilidades adquiridos en INFOTEC para identificar y explotar vulnerabilidades sobre los aplicativos indicados, en todo momento de manera controlada y autorizada, iniciado con la recopilación de ciertas huellas, ya que sin estas sería difícil entrar en el sistema. Por lo tanto, es significativo el tiempo que se dedica a recopilar información sobre los aplicativos para llevar a cabo una explotación de la vulnerabilidad esto, aunque no lo llevamos a la práctica, nos permitiría crear una estrategia teniendo en cuenta información detallada sobre los problemas de seguridad encontrados y recomendaciones para solucionarlos.

Esta actividad básicamente se trata sobre buscar activamente las debilidades en los sistemas antes de que lo hagan los cibercriminales. Elaborando los informes ejecutivos de forma detallada sobre las aplicaciones web designadas. En estos informes se identifica, clasifica y proporcionan recomendaciones de remediación de vulnerabilidades encontradas va dirigido al representante de la organización contratante por lo que se busca brindar sugerencias de forma específicas para que corrijan cada vulnerabilidad y fortalezcan la seguridad en general de cada aplicación.

Así mismo al revisar las sesiones en línea sobre la materia de la estancia me han permitido vislumbrar que se requiere mayormente de habilidades sociales blandas como la comunicación efectiva, el trabajo en equipo, la resolución de problemas, la creatividad que permiten interactuar eficientemente con otros, permitiendo gestionar conflictos, liderar equipos y adaptarte a nuevos entornos, lo que hace a un profesional mucho más eficaz en sus métodos profesionales.

El autoconocimiento y el desarrollo profesional van de la mano conociendo nuestras fortalezas, debilidades, valores, intereses y motivaciones podemos tomar decisiones más acertadas e incluso al combinar conocimientos técnicos y habilidades blandas, se puede destacar más alcanzando las metas u objetivos profesionales.

Cuadro CQA de mi estancia en la organización

C ¿Qué **C**onozco?	Q ¿**Q**ué aporte?	A ¿Qué **A**prendí?
1. Se utilizar la computadora con sistema Microsoft Windows. 2. Formación informática y tecnológica. 3. Conocimientos indispensables de programación. 4. Terminología. 5. Gestión del tiempo (Organización).	1. Voluntad. 2. Proactiva y resuelta. 3. Análisis y organización de información de manera coherente para presentarla de forma clara y concisa. 4. Pensamiento crítico.	1. Más terminología. 2. Herramientas. 3. Realizar escaneo de puertos. 4. Identificar puertos UDP y TCP. 5. Reconocer vulnerabilidades. 6. Comprender posturas de seguridad. 7. Configurar la máquina virtual y solucionar algunas posibles fallas. 8. Comandos Kali Linux.

Evaluación de desempeño

Este proceso de evaluación es fundamental para identificar mis fortalezas, áreas de mejora y oportunidades de desarrollo profesional.

Por lo que, principalmente, agradezco la oportunidad que INFOTEC me ha brindado por el hecho de haber adquirido conocimientos y habilidades relevantes para mi desarrollo personal y profesional. Al ser, un actor importante de la innovación tecnológica en América Latina, sus contenidos y recursos ofrecidos son relevantes, acorde a los cambios sociales y tecnológicos que vivimos en México, garantizando educación de calidad.

Con esta estancia el objetivo fue explotar en la práctica los conocimientos adquiridos, robusteciendo con ello mis habilidades técnicas.

La modalidad a distancia me resulto flexible, accesible y me brindo la posibilidad de aprender al propio ritmo, pero es importante considerar la disciplina y las habilidades tecnológicas que son necesarias para estudiar de forma independiente.

Esta modalidad a distancia me permitió tomar el control de mi aprendizaje, aplicando habilidades como el análisis y la reflexión que me permitió llevar a cabo ese proceso de aprendizaje e identificar áreas que requerían mejorar, y con ello estableciendo metas realistas y alcanzables. Mi compromiso era realizar las entregas de actividades en tiempo y forma, así como la calidad de mis participaciones en los foros, pero sobre todo en la comprensión de los contenidos y el aprendizaje obtenido de ello.

La modalidad a distancia se presentó, como un reto para mí, ya que me instó a disponer de un horario específico, siendo flexible para con mi horario laboral, para analizar las lecturas, planificar las actividades desde el primer día, logrando concluir de forma satisfactoria.

Referencias

- Peña (2021). Escaneo y enumeración Recuperado de: https://eiposgrados.com/blog-ciberseguridad/segunda-fase-del-hacking/.
- Castro, C. (2019). Pruebas de penetración e intrusión. Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6273/00005218.pdf?sequence=1&isAllowed=y
- EC-Council. (19 de enero de 2024). What is Ethical Hacking? https://www.eccouncil.org/ethical-hacking/#:~:text=Ethical%20hacking%20is%20a%20process,and%20looking%20for%20weak%20points
- UGT Madrid. (2017). Manual informativo de PRL: Organización del trabajo. (pp. 43-50).
- Azuax Informática. (2017). El Reporte Técnico de un Pentest. https://www.azuax.com/2017/6/13/el-reporte-tecnico-de-un-pentest/index.html
- Hacker Mentor (2021), Guía para reportes de pentesting. Hacker Mentor Offensive Security. (2013). Penetration Test Report. https://www.offensive-security.com/reports/penetration-testing-sample-report-2013.pdf
- Rinku. (20 de mayo de 2024). Cómo hacer un informe de Pentesting para el eCPPTv2. [video]. YouTube. https://www.youtube.com/watch?v=vMeemXJVfRk&lc=UgwbQ7gDC6ZeP1CWAMF4AaABAg
- INFOTEC (01 de enero del 2012). Manual de organización. (Vol. S/N). CDMX: Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC). Recuperado de: https://educacionejecutiva.infotec.mx/work/models/Infotec/normateca/admin/manual_de_organizacion_del_infotec.pdf
- Ramírez Chávez, M. y Manjarrez Fuente, N. (2022). Habilidades blandas y habilidades duras, clave para la formación profesional integral. Revista Ciencias Sociales y Económicas-UTEQ.
- Víquez Jerez, L. (2020). Análisis comparativo de habilidades blandas deseables en profesionales de TI por empleadores de la empresa privada y pública costarricense.
- Soto, B. (S.F.) Descubre los 3 tipos de motivación y cómo pueden transformar tu vida. Recuperado de: https://liderazgoempresarial.info/cuales-son-los-3-tipos-de-motivacion
- Ebac (19 de junio de 2023) ¿Por qué debes invertir en ti mismo y cómo puedes hacerlo? Recuperado de: https://ebac.mx/blog/invertir-en-ti-mismo
- Iberdrola. (2022) ¿Afecta tu personalidad a tu desarrollo profesional? Recuperado de: https://www.iberdrola.com/talento/personalidad-en-el-trabajo
- Losa Nicolás, F. (2002). El desarrollo profesional de los trabajadores como ventaja competitiva de las empresas. Universidad de La Rioja. (pp. 26). Recuperado de: http://www.ehu.eus/cuadernosdegestion/documentos/214.pdf
- Talent Coaching de Negocios. (2016). El autoconocimiento como herramienta para tu desarrollo profesional. [Video]. YouTube. https://www.youtube.com/watch?v=9h94dE0PN10
- TEDx Talks (2017) ¿Quién soy?: ¿Qué significa hacernos esta pregunta? Gabriel Pereyra. [Video]. YouTube. https://www.youtube.com/watch?v=9l0lJ_7N_Vc.