UNIVERSIDAD NACIONAL DE INGENIERÍA

OTI UNI

TRANSFORMACIÓN digital

PROGRAMA DE INICIACIÓN TECNOLÓGICA PIT 2024

Curso gratuito de

Ciberseguridad: Ethical Hacking

DESCRIPCIÓN

El presente curso es una forma de llevar la capacitación que reciben todos los estudiantes de la UNIVERSIDAD NACIONAL DE INGENIERÍA por parte de la Oficina de Tecnologías de la Información. Este curso busca dotar a los participantes de las capacidades básicas necesarias para empezar en el mundo de la ciberseguridad.

Durante el desarrollo de las sesiones, se abordarán temas cruciales como la recopilación de información, la enumeración y el escalamiento de privilegios. Se explorará el uso de técnicas avanzadas como el Pivoting para acceder a redes internas, así como el análisis de vulnerabilidades tanto en redes como en aplicaciones web. Los estudiantes adquirirán habilidades prácticas para realizar escaneos, identificar vulnerabilidades y generar informes detallados que incluyan recomendaciones de seguridad.

Nuestro enfoque práctico te permitirá aplicar tus conocimientos en escenarios reales, resolviendo desafíos y problemas comunes en el campo de la ciberseguridad.

INFORMACIÓN GENERAL

Modalidad

Virtual
(Zoom + YouTube)

Duración

8 Sesiones

Horas

16 horas

¿QUÉ APRENDERÁS EN ESTE CURSO?

- En este curso, aprenderás a cómo enumerar de manera efectiva en un objetivo, identificar sus vulnerabilidades y explotar dichas debilidades para evaluar su seguridad. Al final del curso, estarás capacitado para aplicar estos conocimientos en escenarios reales, fortaleciendo la seguridad de las redes y aplicaciones.

- Los materiales del curso los podrán encontrar en PIT Virtual, así como los links de las grabaciones de las clases.

DIRIGIDO A

Este curso está dirigido a alumnos de pregrado de todas las universidades.

BENEFICIOS

- Acceso al aula virtual (PIT Virtual).
- Grabaciones de las clases.
- Materiales descargables.

Certificado

El certificado digital es opcional. Al aprobar el curso con un promedio final mayor o igual a 12, el participante recibirá un certificado digital emitido por la Universidad Nacional de Ingeniería.

Los alumnos que no hayan aprobado el curso podrán recibir una constancia digital de asistencia, emitida por la Universidad Nacional de Ingeniería, si han asistido al menos al 75% de las clases.

EVALUACIÓN

- En cada sesión se realizará una evaluación la cual estará sujeta a una calificación.

- **La nota del curso se obtendrá de la siguiente manera:**

  Si el curso cuenta con cuatro minitest, se deberá eliminar la menor de estas notas. Las más altas se sumarán al doble de la evaluación final según la siguiente fórmula:

$$Nota\ Final = \frac{Suma\ (P_1 + P_2 + P_3 + P_4) - Min(P_1 + P_2 + P_3 + P_4) + 2 * Ex_{final}}{5}$$

- La asistencia a cada sesión se apertura automáticamente en la plataforma PIT VIRTUAL durante el horario de la clase.

TEMARIO
DEL CURSO

SESIÓN 1
INTRODUCCIÓN AL CURSO

1.Conceptos básicos
2.Despliegue de los ambientes de pruebas
3.Fundamentos de la seguridad informática
4.Tipos de amenazas y vulnerabilidades

SESIÓN 2
RECOPILACIÓN DE INFORMACIÓN

1.Introducción a la recopilación de información
2.Herramientas de recopilación pasiva y activa
3.Concepto y objetivos de la enumeración
4.Herramientas y técnicas de enumeración de redes
5.Enumeración de servicios y sistemas operativos

SESIÓN 3
ESCALAMIENTO DE PRIVILEGIOS

1.Vulnerabilidades comunes utilizadas para escalar privilegios
2.Herramientas de escalamiento de privilegios en Kali Linux
3.Técnicas de post-explotación
4.Uso de pivoting para acceder a redes internas
5.Herramientas para pivoting en Kali Linux

SESIÓN 4
ATAQUES DE FUERZA BRUTA

1.Herramientas para ataques de fuerza bruta
2.Técnicas de mitigación y defensa
3.Estudios de caso y ejemplos prácticos

TEMARIO
DEL CURSO

SESIÓN 5
ANÁLISIS BÁSICO DE VULNERABILIDAD DE REDES

1.Herramientas para el escaneo y análisis de redes
2.Identificación y evaluación de vulnerabilidades
3.Recomendaciones y soluciones de seguridad

SESIÓN 6
ANÁLISIS BÁSICO DE VULNERABILIDAD EN APLICACIONES WEB

1.Técnicas de análisis de vulnerabilidades en aplicaciones web
2.Herramientas específicas para el análisis web
3.Mitigación de vulnerabilidades en aplicaciones web

SESIÓN 7
GENERACIÓN DE INFORMES

1.Importancia de la generación de informes en ciberseguridad
2.Estructura y contenido de un informe de seguridad
3.Herramientas para la generación de informes
4.Presentación de hallazgos y recomendaciones

SESIÓN 8
EVALUACIÓN

1.Simulacros de examen basado en certificaciones actuales.
2.Consejos y técnicas de estudio

DOCENTE

Manuel Flores

Bachiller de la carrera Ciencias de la Computación Especialista en ciberseguridad con experiencia en pentesting, seguridad aplicativa y ciberinteligencia en los sectores de telecomunicaciones y finanzas del pais.
Posee certificaciones relevantes que incluyen eWPTXv2, eMAPT y CEH Master.

UNIVERSIDAD NACIONAL DE INGENIERÍA

OTI UNI

TRANSFORMACIÓN digital