

Red de Centros de Excelencia de la UIT para la Región de las Américas

INSTITUTO NACIONAL DE INVESTIGACIÓN Y CAPACITACIÓN DE TELECOMUNICACIONES

INICTEL-UNI

Curso en línea:

GESTIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD

Del 9 de septiembre al 4 de octubre de 2019

INFORMACIÓN GENERAL

DESCRIPCIÓN DEL CURSO

Título	Gestión de Infraestructuras y Ciberseguridad
Modalidad	Curso a distancia a través de la plataforma ITU Academy (Moodle)
Objetivo	El objetivo principal de este curso es analizar y emplear diversas herramientas y técnicas que se utilizan para afectar la ciberseguridad y conocer cuáles son las contramedidas para estos ciberataques.
Fecha	Del 9 de septiembre al 4 de octubre de 2019
Duración	4 semanas
Fecha límite para registro	2 de septiembre de 2019
Costo	USD 300 (Se aplica un descuento de 10% para grupos de participantes de una misma institución y de 5% para grupos de 3 a 5 participantes)
Código del Curso	19OI24224AMS-S

OBJETIVOS ESPECIFICOS

- Dar a conocer las etapas que se realiza en un Ethical Hacking
- Utilizar diversas herramientas y técnicas que utilizan los delincuentes informáticos y conocer cuáles son las contramedidas para estos ciberataques.
- Aplicar los fundamentos del análisis de vulnerabilidades bajo la metodología definida por OSSTMM.
- Planificar y gestionar los recursos propios.
- Realizar informes conducidos y evaluados por el instructor.

A QUIÉN VA DIRIGIDO

- Profesionales de la seguridad informática que deseen ampliar sus conocimientos en técnicas y herramientas usadas por atacantes (hacker) necesarias para evaluar su propia infraestructura.
- Profesionales de la seguridad informática que deseen hacer carrera como hacker éticos.

TUTOR

Prof. Daniel Taipe	Contacto: dtaped@icloud.com
Licenciado en Ciencias de la Administración Aeroespacial, Certificado Internacional en “Certified Ethical Hacker” (CEH), Certificado Internacional en “EC-Council Certified Security Analyst” (ECSA), Certificado Internacional en “Certified EC-Council Instructor” (CEI), por EC-Council; Certificado Internacional en ITIL foundation otorgado por EXIN y Certificado como Auditor de Sistemas, otorgado por ISEC. Diplomado en Ciberseguridad por el Centro de Altos Estudios Nacionales (CAEN), Diplomado en Seguridad Informática y Técnicas de Anti hacking por la Institución StackOverflow en Madrid-España, asimismo, tiene una Maestría en Administración y Doctrina Aeroespacial, egresado de la Maestría en Informática, y es egresado del Doctorado en Educación.	

PROGRAMA DEL CURSO POR SEMANA

Semana I

Módulo 1: Introducción a la Gestión de Ciberseguridad

- Introducción EH y Metodologías.
- Fases del Hacking
- Herramientas esenciales.

Reconocimiento del Objetivo

- Técnicas de reconocimiento pasivo (Motores de búsqueda, Internet).
- Técnicas de reconocimiento activo (DNS, Whois, SNMP, etc).
- Escaneo de Puertos
- NMAP – Análisis de Vulnerabilidades + Explotación con Metasploit.

Atacando a nivel de la red y local

- Email extractor
- Extracción de meta data con Foca
- Sniffing con Wireshark.
- ARP y Ataques MiTM.

Semana II

Módulo 2:

- Scanner universal para IPv4/IPv6
- Extrayendo contraseñas de Email con Hack Mail
- Encontrando la ruta de los objetivos
- Uso de troyanos y backdoors con NetCat

- Uso y pruebas de Keyloggers
- Extracción de data
- Crack Passwords
- Scaneadores de vulnerabilidades
- USB Forense
- Obtención de User y Password, de usuarios de Windows
- Ciberguerra, uso de botnes
- Denegación de servicio
- Uso de Joiners, ocultar virus en otros softwares.

Semana III

Módulo 3: Análisis y Explotación de Vulnerabilidades

- Ataque Man in the Middle con CAIN
- Google Hacking
- Como se hace un virus Indetectable
- Clonado de páginas web
- Uso de la técnica de steganografía
- Análisis de vulnerabilidades con herramientas automatizadas (Nessus).
- Explotación Vulnerabilidades en Windows XP, Windows 2008 (Metasploit).
- Explotación Vulnerabilidades en Linux (Metasploit).
- Explotación Vulnerabilidades en Bases de Datos MSSQL y Oracle (Metasploit).
- Introducción vulnerabilidades web.

Semana IV

Módulo 4:

- OWASP "Testing Guide" – "TOP 10 OWASP".
- Inyección SQL
- Cross-site scripting (XSS)
- Criptografía
- Explotación de vulnerabilidades Wireless.
- Análisis de Aplicaciones con Herramientas Automatizadas (ZAP, Acunetix).
- Análisis de Aplicaciones con Herramientas Automatizadas (SQLmap).
- Uso de Anonimizadores en Internet.

Trabajo aplicativo

- Realización de Informe de Ethical Hacking, con las principales herramientas prendidas.
- Presentación y Evaluación de los Informes.

METODOLOGIA

El presente curso es en línea/asincrónico. La metodología que orienta este curso será eminentemente participativa. La estrategia metodológica utilizada para el desarrollo de curso propone al participante una diversidad de actividades. Se espera que cada estudiante participe mediante la lectura del material que estará disponible desde el inicio del curso, aportes escritos a los debates, foros, actividades, ejercicios de refuerzo y exámenes que serán definidos y los cuales serán realizadas en forma asincrónica. Esta técnica asegurará la flexibilidad de tiempo necesaria para que cada participante pueda organizarse de la manera que mejor le convenga.

Los participantes aprobados en el curso según los criterios de evaluación que sean indicados por los tutores y todos aquellos que sean aprobados recibirán un Certificado que será emitido por vía electrónica.

COORDINACION DEL CURSO

Coordinación Académica Iris Pretel Trejo INICTEL-UNI ipretel@inictel-uni.edu.pe	Coordinador UIT Ana Veneroso Oficina Regional de la UIT para las Américas Ana.veneroso@itu.int
---	--

REGISTRO Y PAGO PASO A PASO (A ser completado por la UIT)

1. Creación de la cuenta en ITU Academy

El proceso de registro y pago debe ser realizado a través del [Portal ITU Academy](#). Para registrarse en un curso es necesario [crear una cuenta en la plataforma](#).

2. Inscripción en el curso

- Una vez creada la cuenta ya se puede realizar la inscripción en la página del curso pulsando en la opción "[Apply here](#)".
- También es posible registrarse en el curso deseado por medio de nuestro [portafolio de cursos](#).

3. Pago del curso:

Este curso tiene un costo por participantes de **USD 300**. El proceso de pago podrá ser realizado en línea a través del mismo enlace del curso informado arriba.

- Pago en Línea mediante tarjeta de crédito:** El proceso de pago podrá ser realizado en línea a través del mismo enlace arriba indicado.
- Transferencia bancaria internacional:** En el caso de que no sea posible realizar el pago en línea es posible seleccionar la opción "offline payment" y el sistema generará la factura a través del mismo enlace del curso. Baje la factura para realizar la transferencia bancaria a la cuenta de la UIT que se indica abajo y remita el comprobante de la transferencia, conjuntamente con la factura, para el Coordinador de Curso en UIT, con copia a hcbmail@itu.int. Todas las tasas que incidan sobre la transferencia bancaria deben de ser sufragadas por el participante. En el caso de que los documentos referentes al pago no sean enviados, la inscripción en el curso no será confirmada.
- Pago en grupo:** Si desea pagar por más de un participante mediante transferencia bancaria y necesita una factura para todos ellos, cree una cuenta como **Contacto institucional**. Los **contactos institucionales** son usuarios que representan una organización. Cualquier estudiante puede solicitar ser un contacto institucional o pertenecer a cualquier organización existente.

Para hacer esto, diríjase a su página de perfil haciendo clic en el botón "**Mi cuenta**" en el menú de usuario. En la parte inferior de esta página debería ver dos botones:

- Si desea **convertirse en un contacto institucional**, haga clic en el botón "**Solicitar ser un contacto institucional**". Esto lo redireccionará a un formulario pequeño que solicitará el nombre de la organización. Después de completar el nombre de la organización que desea representar, haga clic en "**continuar**" y se creará una solicitud. Un administrador de la Academia de la UIT revisará manualmente esta solicitud y la aceptará o rechazará en consecuencia.
- Si desea **pertenecer a una organización existente**, haga clic en el botón "**Solicitar pertenecer a un contacto institucional**". Esto lo redireccionará a un formulario pequeño que le pedirá que seleccione la organización a la que desea unirse desde una lista de organizaciones. Después de seleccionar la organización correcta, haga clic en "**continuar**", se creará una solicitud. El contacto institucional que representa a esa organización aceptará o denegará manualmente su solicitud para unirse a la organización.

Cuenta bancaria de la UIT	
Nombre y dirección del banco:	UBS Switzerland AG Case Postale 2600 CH 1211 Geneva 2 Switzerland
Beneficiario:	Union Internationale des Télécommunications
Número de cuenta:	240-C8108252.2 (USD)
Swift:	UBSWCHZH80A
IBAN:	CH54 0024 0240 C810 8252 2
Monto:	USD 300
Referencia del pago	CoE-AMS – 24224 - P.40591.1.02

4. **Otros métodos de pago:** En caso de que las regulaciones nacionales restrinjan la posibilidad de completar el pago mediante las opciones informadas, le solicitamos contactar al Coordinador de la UIT para mayor asistencia.