Información General del Curso

UIT y INSTITUTO NACIONAL DE INVESTIGACIÓN Y CAPACITACIÓN DE TELECOMUNICACIONES

Título	Fundamentos de seguridad de red y sistemas de detección
Modalidad	Virtual
Fechas	1 -31 Agosto 2022
Duración	40 horas
Último día para registro	28 de Julio de 2022
Costo	Gratuito
Descripción	El presente curso aborda de una manera teórico/practica el funcionamiento de los principales protocolos que permiten la comunicación en una red de datos, además de explotarlos para generar ataques internos con el fin de comprometer la seguridad en la red. Asimismo, el curso abarca algunos mecanismos de detección de incidentes haciendo uso de sistemas honeypots, honeynets y sistemas de detección de intrusos (IDS).
Código del curso	22OI27842AMS-S

1.OBJETIVOS DEL CURSO

Comprender el funcionamiento de los protocolos de red bajo un enfoque de seguridad. Explorar sistemas de detección y análisis de incidentes que se puedan suscitar en una red de datos.

2. RESULTADOS DEL APRENDIZAJE

Al finalizar el curso el estudiante comprenderá los fundamentos de ciberseguridad, el funcionamiento de los principales protocolos de red y los ataques que implican el aprovechamiento de dichos protocolos. Asimismo, se brinda a los participantes los aspectos teóricos y prácticos asociados a técnicas de detección de incidentes.

3. A QUIÉN VA DIRIGIDO

Profesionales de Seguridad de información, Oficiales de Seguridad, Profesionales y técnicos de TI.

4.REQUISITOS DE ADMISIÓN

Conocimiento básico del sistema operativo GNU/LINUX

Conocimientos básicos de redes

5. TUTORES / INSTRUCTORES

Nombre del Tutor / Instructor	Información de Contacto
Daniel Diaz Ataucuri	ddiaz@inictel-uni.edu.pe
Experiencia del Tutor: Obtuvo su título profesional de Ingeniería Electrónica en la Universidad Nacional de Ingeniería en Lima-Perú; y su maestría en Electrónica por la Universidad Estatal del Sur Oeste de Rusia-UESOR de la ciudad de Kursk, y realizó estudios de alta especialización en Telecomunicaciones en la Universidad Politécnica de Madrid y en la NTT en Tokyo-Japón. Actualmente es Profesor titular de Telecomunicaciones en la Universidad Nacional de Ingeniería-UNI y en la Universidad Nacional Mayor de San Marcos-UNMSM. Participó desde los inicios en el proyecto CLARA para la formación de la red regional de investigación de Latinoamérica, RedCLARA. Ha asistido en diversos eventos académicos como: Diplomatura de Especialización en Tecnologías de Cloud Networking, CSX Packet Analysis Course Cetificate, Introducción al CISSP - Profesional certificado en seguridad de sistemas de información, entre otros. Es expositor en diversos cursos y eventos a nivel nacional e internacional en temas de telecomunicaciones.	
Jorge Buzzio Garcia	jbuzzio@inictel-uni.edu.pe
Especialista certificado en HCNA Routing & Switching, con Diplomatura de Especialización en Tecnologías Cloud, Bachiller en Ing. de Telecomunicaciones, con cursos de Ethical Hacking, Seguridad Informática, CSX Packet Analisis, Programa de Especialización en Ciberataques y Técnicas de prevención por el Indian Technical and Economic Cooperation. Expositor en congresos nacionales e internacionales con 6 años de experiencia en empresas de Telecomunicaciones, Sector Privado y Sector Estatal. Actualmente se desempeña como investigador en INICTEL-UNI en el área de redes y ciberseguridad.	
Victor Salazar Vilchez	vsalazar@inictel-uni.edu.pe
Profesional de telecomunicaciones certificado en los principales fabricantes de equipos de red (Cisco, Huawei y Fortinet), cuenta con una diplomado en tecnologías de la información y telecomunicaciones, una diplomatura en seguridad de las TICs y cursos de especialización CSX Packet Analysis, CISSP. Ha realizado una pasantía de investigación en el departamento de ingeniería de sistemas telemáticos de la Universidad Politécnica de Madrid. Actualmente se desempeña como asistente de investigación en el área de redes y ciberseguridad del INICTEL-UNI. Autor de artículos técnicos para congresos nacionales e internacionales.	

6. CONTENIDO DEL CURSO

Semana I:

Módulo 1: Fundamentos de ciberseguridad

- … Comprender la triada CIA
- … Mecanismos de protección
- … Ocultación de datos
- … Encriptación
- … Descripción de las capas OSI y modelo TCP/IP
- … Preparación del escenario de simulación

Semana II:

Módulo 2: Análisis de protocolos de red y escenarios de ataques – Parte I

- … Análisis del funcionamiento del protocolo IP, ARP e IPsec

- … Uso de la herramienta Wireshark para la captura de paquetes
- … Implementación de escenario de ataques basadas en herramientas opensource

Semana III:

Módulo 3: Análisis de protocolos y escenarios de ataques - Parte II

- … Análisis del funcionamiento del protocolo DHCP y DNS
- … Uso de la herramienta Wireshark para la captura de paquetes
- … Implementación de escenario de ataques basadas en herramientas opensource

Semana IV:

Módulo 4: Sistemas de detección

- … Honeypots/Honeynets
- … Introducción a IDS/IPS
- … Snort
- … Casos de estudio de los últimos ataques 2021.

7. CRONOGRAMA DEL CURSO

Semana / Sesión	Tema	Ejercicios e interacciones
Semana 1	Fundamentos de ciberseguridad	Despliegue del escenario de simulación
Semana 2	Análisis de protocolos de red y escenarios de ataques – Parte I	Laboratorio: Análisis del funcionamiento del protocolo ARP Laboratorio: Ejecución de ataques ARP
Semana 3	Análisis de protocolos y escenarios de ataques - Parte II	Laboratorio: Análisis del funcionamiento del protocolo DHCP Laboratorio: Ejecución de ataques en contra del servicio DHCP
Semana 4	Sistemas de detección	Laboratorio: Implementación de sistemas Honeypots Laboratorio: Implementación de sistemas IDS

8. 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

9. EVALUACIÓN Y CALIFICACIÓN

El curso propone un sistema de evaluación combinado el cual se compone de: foros de debate, actividades y evaluaciones. Las fechas de cada uno de estos ítems están definidas en el cronograma. El sistema de calificación de este curso se explica a continuación junto con los porcentajes de peso de cada una de las actividades a evaluar.

Pesos de evaluación

- Foro de debate (20%): Tendrán un peso del 20% sobre la calificación final. Se realizará 1u 2 foros de debate en el curso. Cada estudiante deberá participar un mínimo de dos veces en el foro con aportes de valor para obtener el 100% del porcentaje semanalmente. En caso de participar una vez obtendrá en 50% y en caso de no participar será un 0%.
- Actividades (60%): también denominados retos, actividades, laboratorios u trabajos individuales tendrán un peso total del 60% y estarán compuestas de algunas de estas opciones: desarrollo de trabajos individuales, retos trabajos grupales, actividades con entrega en la plataforma.
- Evaluaciones (20%): Las evaluaciones del presente curso tendrán un peso total del 20% y podrán efectuarse mediante dos exámenes en línea, El esquema para este curso está indicado en el cronograma de actividades.
- Aprobación: Para aprobar este curso se debe completar un acumulado de mínimo 60%.

10. COORDINACION DEL CURSO

Coordinación Académica	**Coordinador UIT**
Iris Pretel CoE INICTEL-UNI ipretel@inictel-uni.edu.pe	Rodrigo Robles Oficina Regional de la UIT para las Américas rodrigo.robles@itu.int