Curso Virtual de Hacking Ético 2019

Domingos 6, 13, 20 y 27 de Enero del 2019. De 9:00 am a 12:15 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación:

Como profesionales en ciberseguridad, se tiene la única responsabilidad de encontrar y entender las vulnerabilidades de la organización, para trabajar diligentemente en mitigarlas antes de estas sean aprovechadas por atacantes maliciosos. Este curso abarca las herramientas, técnicas y metodologías para hacer pruebas de penetración contra redes, preparando para realizar proyectos de pruebas de penetración paso a paso. Todas las organizaciones necesitan personal experimentados en seguridad de la información, quien pueda encontrar vulnerabilidades y mitigar sus efectos. Con este curso se estará en la capacidad de realizar pruebas de penetración, aplicando los conocimientos, herramientas, y principios abarcados a través del mismo. Descubriendo y explotando vulnerabilidades en entornos reales, demostrando así los conocimientos asimilados.

Objetivos:

Este curso enseña a los participantes a realizar un reconocimiento detallado, estudiando la infraestructura del objetivo mediante búsquedas en blogs, motores de búsqueda, redes sociales y otras infraestructuras en Internet e Intranet. Se escanean las redes objetivo utilizando las mejores herramientas disponibles. Se abarcan las mejores opciones, configuraciones y capacidades de las herramientas para pruebas de penetración. Luego se exponen diversos métodos de explotación para ganar acceso hacia los sistemas objetivo, y de esta manera medir el riesgo real para la organización. Después se realizan acciones posteriores a la explotación y ataques a contraseñas. Todos los ataques se desarrollan en un laboratorio de pruebas controlado.

Fechas & Horarios:

El Curso Virtual de Hacking Ético tiene una duración de doce (12) horas, divididas en cuatro (4) sesiones de tres (3) horas de duración.

Fechas:

Domingos 6, 13, 20 y 27 de Enero del año 2019

Horario:

De 9:00 am a 12:15 pm (UTC -05:00)

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals y Phishing Countermeasures. Ha sido instructor y expositor en OWASP LATAM Tour Lima, Perú, 0x11 OWASP Perú Chapter Meeting, PERUHACK 2014, PERUHACK2016NOT, y 8.8 Lucky Perú 2017. Cuenta con más de catorce años de experiencia en el área y desde hace diez años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad RareGaZz y al grupo peruano de seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital y GNU/Linux. Su correo electrónico es ReYDeS@gmail.com y su página personal es: http://www.ReYDeS.com.

Más Información:

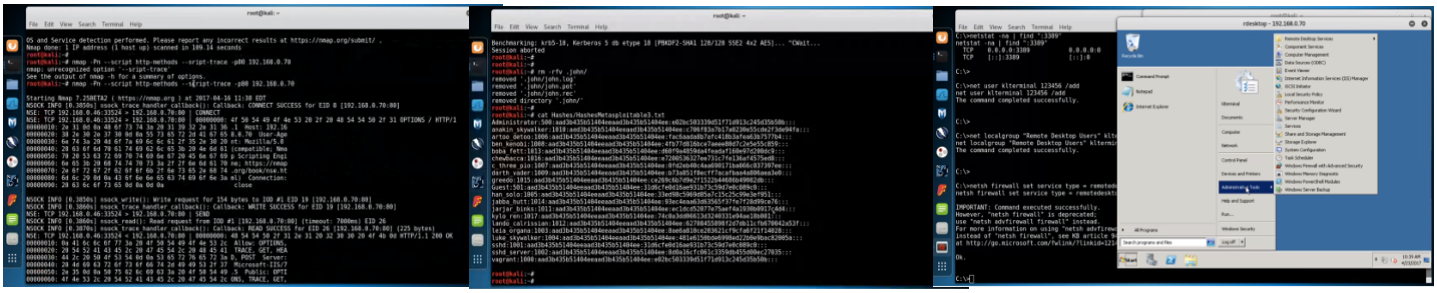
Para obtener más información sobre este curso virtual, tiene a su disposición los siguientes mecanismos de contacto.

Correo electrónico:

caballero.alonso@gmail.com

Teléfono: (+51) 949304030

Sitio Web: http://www.reydes.com



Temario: (Actualizado)

- Tipos de Hacking Ético
- Metodologías Libres e Infraestructura de Pruebas
- Reglas del Contrato, Alcance y Reporte
- Reconocimiento
- Consultas Whois
- Búsqueda en Sitios Web
- Análisis de Metadatos en Documentos
- Consultas DNS
- Reconocimiento con Maltego
- Encontrar Vulnerabilidades en Motores de Búsqueda & Shodan
- Objetivos y Tipos de Escaneo
- Consejos Generales para el Escaneo
- Sniffing y Trazado de la Red
- Escaneo de Puertos
- Nmap y Soporte para IPv6
- Huella del Sistema Operativo
- Escaneo de Versión
- Manipular Paquetes con Scapy
- Escaneo de Vulnerabilidades
- Nmap Scipting Engine
- Nessus
- Enumerar Usuarios
- Netcat para pruebas de penetración
- Explotación
- Categorías de Exploits
- Metasploit Framework & Meterpreter
- Base de Datos de Metasploit Framework e Integración
- Explotación Posterior
- Shell de Comandos y. Acceso Terminal
- Mover Archivos con Exploits
- PowerShell para Hacking Ético
- Acciones utilizando PowerShell
- Consejos para Atacar Contraseñas y Bloqueo de Cuentas
- Adivinar Contraseñas con THC-Hydra
- Formatos para Representar Contraseñas
- Obtener Hashes
- John The Ripper y Cain
- Ataques con Tablas Arco Iris
- Ataques Pass-The-Hash

Material:

- Kali Linux
- Metasploitable 2 y Metasploitable 3

***** Si el participante lo requiere se le enviarán dos (2) DVDs conteniendo el material utilizado en el curso, por S/. 75 Soles adicionales. Esto incluye los gastos de envío hacia cualquier lugar del Perú.

Inversión y Forma de Pago:

El curso tiene un costo de:

S/. 350 Soles o $ 110 Dólares

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

Residentes en Perú

Depósito Bancario en la siguiente cuenta:

Scotiabank

ScotiaBank
Cuenta de Ahorros en Soles: 324-0003164
A nombre de: Alonso Eduardo Caballero Quezada

Residentes en Otros Países

Transferencia de dinero mediante Western Union o MoneyGram.

Western Union — moving money for better

MoneyGram

Escribir por favor un mensaje de correo electrónico para enviarle los datos necesarios para realizar la transferencia.

Confirmado el depósito o la transferencia se enviará al correo electrónico del participante, los datos necesarios para conectarse al sistema, además del material para su participación en el curso.

INTERMEDIA ANYMEETING

El curso se realiza utilizando el sistema para video conferencias de nombre Anymeeting. El cual proporciona transmisión de audio y video HD de alta calidad para el instructor y los participantes, entre otras características ideales para el dictado de cursos virtuales.