HACKING GLADIATOR

Antecedentes

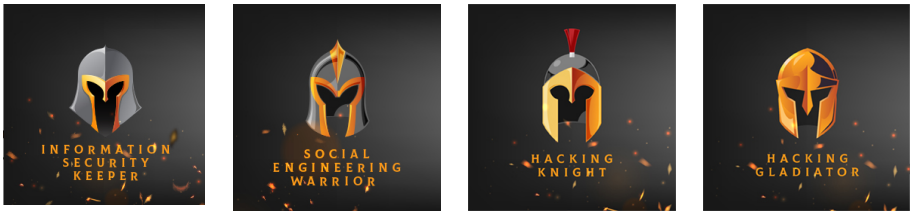
Debido a la dependencia actual en la tecnología, las empresas no se pueden dar el lujo de desproteger el acceso a sus redes y sistemas con el riesgo de ver comprometida su información, operatividad y reputación. Por esta razón la profesión de "Hacker Ético" o “Hacker de sombrero blanco” está siendo altamente demandada a nivel mundial.

Objetivos

El curso de Hacking Gladiator tiene como objetivo profundizar en los mecanismos y técnicas de hacking utilizadas por los hackers para explotar dispositivos informáticos de todo tipo.

La metodología del curso está enfocada en “aprender haciendo”, por este motivo casi todos los capítulos incluyen laboratorios en donde los estudiantes practican cómo explotar vulnerabilidades de forma segura.

Hacking Gladiator es uno de cuatro cursos, que preparan al estudiante en la carrera de pentesting.



A quién va dirigido

El curso está orientado a estudiantes y profesionales de informática que desean aprender técnicas avanzadas de Hacking Ético y prepararse para la certificación CEH.

Prerrequisitos

- Conocimientos básicos de hacking ético (saber efectuar reconocimiento, escaneo, enumeración y explotación básica usando el Metasploit Framework), manejar la línea de comandos de Linux, poseer conocimientos sobre programación de scripts.
- Se recomienda haber tomado previamente el curso Hacking Knight.

Modalidades:

- **LIVE-ONLINE:**
  - Duración: 40 horas (20 horas de sesiones live, 20 horas de aprendizaje autónomo)
  - Clases en vivo con el instructor a través de nuestra plataforma e-learning que hace uso de virtual classrooms.
  - Todas las clases se graban para que los alumnos puedan volver a reproducirlas.
  - Incluye material descargable como diapositivas, ebooks, manuales de laboratorio, papers, etc.
  - Acceso al virtual classroom por tiempo limitado dentro de las fechas de inicio y finalización del curso.
  - Exámenes online finales práctico y téorico.
  - Certificado de aprobación emitido por Academia Hacker y avalado por Consulting Systems.

- **ONLINE SELF-PACED**
  - Lecciones pregrabadas en video, lecturas, manuales, quizzes y laboratorios paso a paso disponibles de forma online a través de nuestro LMS (learning management system).

- El estudiante estudia a su propio paso, en su propio horario y bajo sus propios términos.
- Interacción con el instructor y compañeros de curso a través del foro.
- Acceso de por vida al contenido del curso, el cual se actualiza periódicamente.
- Exámenes online finales práctico y teórico (opcionales).
- Certificado de Completar el curso emitido por Academia Hacker, al finalizar el contenido.

Metodología

- El curso es una combinación de clases magistrales, análisis de casos y laboratorios.
- Usamos la metodología de "aprender haciendo".
- Gamificación a través de quizzes y distintas actividades.

Contenido

TÓPICO	DETALLE

1. ESCANEO AVANZADO	• Escaneo avanzado con NMAP
	  ○ Detección de firewalls
	  ○ Uso de temporizadores
	  ○ Uso de señuelos
	  ○ Ejecutando scripts de NMAP
	• Scapy y Hping
	• Opciones avanzadas de escaneo de vulnerabilidades
	  ○ Perfiles de escaneo
	  ○ Detección de congestión
	  ○ Mecanismos de evasión

2. CRACKING DE CLAVES Y ATAQUES MITM	• Ataques de claves
	  ○ Fuerza bruta vs diccionario vs tablas rainbow
	  ○ Password crackers y diccionarios propios
	• Ataques MITM
	  ○ Tipos de ataques MITM
	  ○ Sniffers de red

3. METASPLOIT KUNG-FU	• Uso avanzado del Metasploit Framework
	  ○ Comandos del msfconsole para la búsqueda de módulos auxiliares y exploits compatibles con una vulnerabilidad particular hallada en un sistema
	  ○ Importación de exploits desde exploit-db
	  ○ Encoders y payloads
	  ○ Módulos de evasión
	• Social Engineering Toolkit (SET)

4. HACKEANDO PROTOCOLOS DE NETWORKING E IPV6	• Ataques a los protocolos DHCP, DNS, CDP, STP, DTP y HSRP • Ataques a IPv6 • El emulador de red GNS3 • Ataques de Capa 2
5. POST-EXPLOTACIÓN	• ¿En qué consiste la post-explotación? • Cómo usar módulos post en el Metasploit Framework • Usando el payload Meterpreter: listado de procesos, captura de tokens, migración de procesos, uso de keyloggers, captura de pantalla, encender el micrófono o la webcam, robo de hashes de la SAM, etc. • Escalamiento de privilegios y búsqueda de información relevante • Rootkits y Backdoors. Pivoteo y reconocimiento interno

BIBLIOGRAFÍA	• Karina Astudillo B. Hacking Ético 101 – Cómo hackear profesionalmente en 21 días o menos. RA-MA; 3ra edición (Diciembre, 2018). • Karina Astudillo. (2017). Hacking Wireless 101 - ¡Cómo hackear redes inalámbricas fácilmente! 1ra Ed – Create Space. • Velu, V. K. (2017). Mastering Kali Linux for advanced penetration testing: Secure your network with Kali Linux, the ultimate hackers arsenal. Birmingham, UK: Packt Publishing.

Facilidades y materiales

- Plataforma e-learning (LMS y Virtual Classrooms)
- Materiales del curso disponibles a través de la plataforma online

Nota importante:

- Para la participación en el taller *cada estudiante debe tener su propia laptop*.
- Requisitos mínimos de hardware: 8GB RAM, 200GB de espacio libre en disco, procesador de doble núcleo (64 bits recomendados), tarjeta inalámbrica y capacidad para bootear de CD/DVD y/o USB.
- Requisitos de software: sistema operativo host Windows, Linux o MacOS, software de virtualización instalado (VmWare o VirtualBox recomendados), simulador de redes GNS3.
- Máquinas Virtuales: Kali Linux, Metasploitable 2, Metasploitable 3. La instructora se tomará parte de la primera sesión para orientar a los estudiantes sobre la configuración del laboratorio de hacking.

Acerca de la instructora

Karina Astudillo B. es la autora del bestseller de Amazon Books "Hacking Ético 101 – ¡Cómo hackear profesionalmente en 21 días o menos!" y es una profesional experta en seguridad informática con más de 20 años de experiencia en tecnologías de información.

Karina se desempeña además como docente de la Escuela Superior Politécnica del Litoral desde 1996 y es Consultora de Seguridad IT y CEO de Consulting Systems desde el año 2002.

Entre sus certificaciones internacionales están: Certified Ethical Hacker (CEH), Computer Forensics US, CCNA Security, CCNA Wireless, CCNA R&SW, Cisco CCAI, HCSA, HCSP, VMware VTP y SCSA.

Conoce más a Karina en https://www.KarinaAstudillo.com.