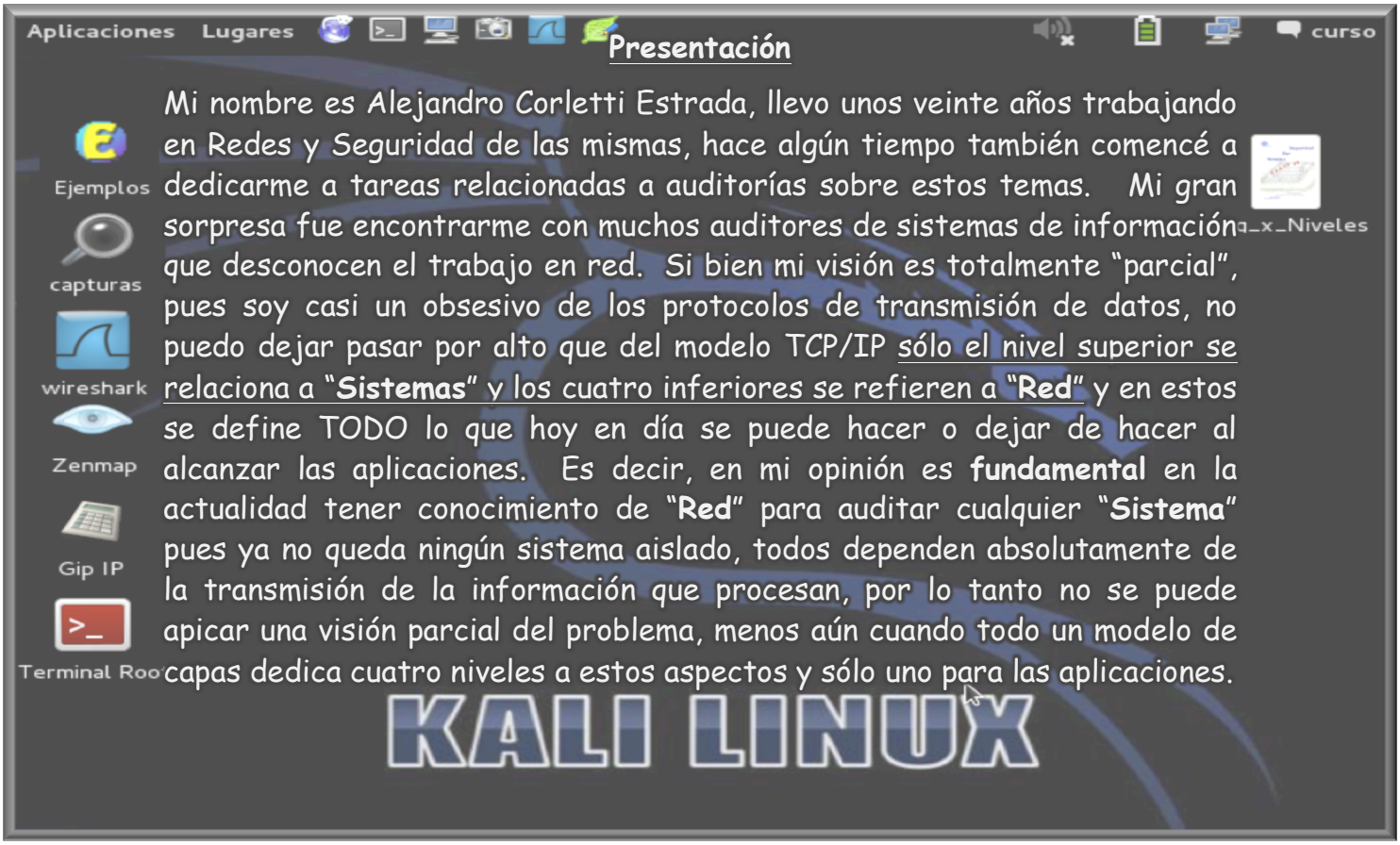
Curso: Auditoría de seguridad en redes TCP/IP.

(*Orientado a auditores de redes y sistemas*)



Duración: 16 horas (*en dos jornadas de 8 horas c/u*).

Público: Auditores de sistemas y red.

Objetivo: Ofrecer una base de conocimientos sobre la seguridad en redes TCP/IP, trabajar con ejercicios eminentemente prácticos empleando herramientas de red. Familiarización con los comandos y herramientas más comunes para poder ser empleadas en auditorías de sistemas y redes.

Bases del curso: Se trabajará con una máquina virtual (MV) que se distribuirá en un DVD e instalará previo a la inicialización del curso en la portátil de cada alumno. Sobre esta MV estará configurada una imagen personalizada de la distribución "**Kali**" (*Linux, Debian*), esta imagen reune todas las herramientas necesarias para cualquier tipo de trabajo de seguridad en redes como así también para tareas de Hackin ético, y será sobre la que se impartirá el curso.

Desarrollo del curso: Se dedicarán las primeras horas a nivelar conocimientos detallados de protocolos de nivel enlace, red, transporte y sus puertas de entrada al nivel de aplicación (*Ethernet, IP, TCP, UDP, http, TLS, telnet, SSH, etc.*), luego se continuará el resto del curso con prácticas sobre los mismos empleando herramientas de captura y análisis de tráfico, detección de vulnerabilidades, evaluación de configuraciones, análisis de reglas en FWs y Listas de control de acceso en routers. Por último y en cada tema se destacarán los aspectos fundamentales a auditar en cada uno de ellos.

Material del curso:

- DVD con el software "Virtual Box" y la imagen mencionada de "Kali".
- Manual del curso (documento pdf).
- Libro "**Seguridad por Niveles**" (Se entregará un ejemplar impreso por alumno).

Temario

1. Presentación del modelo de capas:
   Modelo OSI/ISO Vs TCP/IP.
   Funciones y servicios de cada una de sus capas.
   Presentación de los protocolos fundamentales en cada una de ellas.
   Metodología de capturas de tráfico (empleo de "tcpdump" y Wireshark).
   Metodología de análisis de protocolos (empleo de Wireshark).
   Metodología de "Scan" de redes (empleo de "nmap" y "Zenmap").
   Direccionamiento y máscara de red y subred (Público y privado).

2. Introducción a la auditoría:
   Penetration Test.
   Diagnóstico o evaluación de Seguridad.
   Auditoría de seguridad.
   - Definición del alcance del proyecto.
   - Penetration Test o evaluación Externo e Interno.
   - Definición de la metodología a utilizar
   - Aplicación de la metodología.
   - Recolección de evidencias.

3. Metodologías de trabajo:
   - Descubrimiento.
   - Exploración.
   - Evaluación.
   - Intrusión.

4. Fase de Descubrimiento:
   Recolección de información.
   Descubriendo la red.
   Fuentes de información en Internet.
   Dirección física.
   Detección de Redes WiFi.
   Números telefónicos.
   Nombres de personas y cuentas de correo electrónico.
   Rango de direcciones IP.
   Información de prensa sobre el lugar.
   Análisis de las páginas Web Institucionales y/o Intranet Corporativa.

5. Fase de Exploración:
   Detección de hosts y dispositivos activos.
   Detección y Análisis de servicios activos
   Detección remota de sistemas operativos.

Determinación de mecanismos de criptografía en redes Wi-Fi.
Relevamiento de aplicaciones.

6. Fase de Evaluación:
   Detección de vulnerabilidades en forma remota.
   Herramientas de detección de vulnerabilidades.
   Testing de seguridad en Routers/Firewalls/Dispositivos de Comunicaciones
   Testing de seguridad de un servidores de red.
   Testing de eficacia de Sistemas de Detección de Intrusiones.
7. Fase de Intrusión (*sólo se desarrollará la parte de planificación*):
   Planificación de la intrusión.
   Utilización de ingeniería social para obtención de información.
   Explotación de las vulnerabilidades detectadas.
   Acceso vía módems o accesos remotos detectados.
   Intrusiones vía web u otras aplicaciones.
   Intrusiones vía dispositivos de red.
   Escalada de privilegios.
   Combinación de vulnerabilidades para elevar el control.
   Acceso a información interna.
   Generación de evidencia de expuestos detectados.

Sobre Alejandro Corletti Estrada:

Fue militar Argentino y se desempeño como Jefe de Redes de esta institución durante tres años antes de venir a vivir a España. En ese País fue también formador de instructuros para las academias Cisco para todo Latinoamérica, profesor de las materias "Redes" y "Comunicaciones" en la Universidad Tecnológica nacional y en la Facultad del Ejército Argentino, fue Director del CISI.ar (Centro de Investigación en Seguridad Informática de Argentina) junto con Julio Ardita (famoso "hacker" internacional) hasta que el famoso "Corralito" desencadenó el cierre de sus puertas. En España, formó parte del grupo Altran coordinando temas de seguridad para las empresas del grupo, luego fundó su propia empresa: "*DarFe Learning Consulting S.L*", con la que continúa desarrollando actividades afines a redes y seguridad. Ha liderado la implantación de diez certificaciones ISO-27000, y se desempeña actualmente como consultor para auditorías de seguridad en redes y sistemas a nivel corporativo en una importante empresa de telecomunicaciones internacional.
Es Ingeniero en Informática, MBA y Doctor en Ingeniería. Ha publicado muchos artículos (todos disponibles en Internet), disertado en congresos internacionales casi todos los años y es autor del Libro "Seguridad por Niveles".

Inscripción: https://isacamadrid.stagehq.com/events/2921/booking/new