Webinar Gratuito

Hacking Ético

v.3

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: http://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 3 de Enero del 2019

Presentación

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals y Phishing Countermeasures.

Ha sido instructor y expositor en OWASP Perú, PERUHACK, 8.8 Lucky Perú. Cuenta con más de 16 años de experiencia y desde hace 12 años labora como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

http://www.reydes.com

https://www.linkedin.com/in/alonsocaballeroquezada/

reydes@gmail.com

Hacking Ético, Pruebas de Penetración, etc.

Existen diversos términos o denominaciones, los cuales se utilizan de manera similar, generando algo de confusión. Por lo tanto se proceden a definir los siguientes términos.

- Hacking Ético (Ethical Hacking)
- Pruebas de Penetración (Penetration Testing)
- Evaluaciones de Seguridad / Evaluaciones de Vulnerabilidades (Vulnerability Assessment)
- Auditorias de Seguridad (Security Audit)

Hacking Ético

Definición Tradicional de Hacking

El termino se refiere a la exploración de la tecnología, intentando conocerla al nivel más profundo, para ser capaz de manipularla y hacer algo para lo cual no fue diseñada.

Definición “Mala” de Hacking

Muchas personas piensan en el término como la irrupción en las computadoras y redes sin permiso.

Ético

El uso del término “Ético”, implica la no connotación “Mala” del termino Hacking.

El Hacking Ético utiliza técnicas de ataque de computadora para encontrar fallas con el permiso del propietario, y con el propósito de mejorar su seguridad.

Pruebas de Penetración

Las Pruebas de Penetración se orientan en encontrar vulnerabilidades de seguridad, las cuales podrían permitir a un atacante penetrar la red o computadoras, o robar información.

Esto se realiza utilizando técnicas y herramientas similares a las utilizadas por los criminales y atacantes del mundo real.

El propósito de una Prueba de Penetración es comprometer los sistemas y obtener acceso hacia la información, para poder determinar su impacto en la empresa.

El Hacking Ético es un termino amplio abarcando todas las técnicas de Hacking Ético utilizados para propósitos benignos, mientras las Pruebas de Penetración se enfocan en el proceso de encontrar vulnerabilidades. Desde este perspectiva la Prueba de Penetración es un subconjunto del Hacking Ético.

Evaluaciones de Seguridad

También se les denomina como “Evaluación de Vulnerabilidades”. Estos términos son utilizados de manera similar al termino Pruebas de Penetración, pero existen diferencias.

Las Pruebas de Penetración se enfocan en ingresar o robar datos. Penetrar el entorno explotando las vulnerabilidades descubiertas.

Las Evaluaciones de Seguridad o de Vulnerabilidades se enfocan en encontrar vulnerabilidades de seguridad, frecuentemente sin explotarlas ni obtener ingreso.

Por lo tanto las Pruebas de Penetración son más profundas, con el propósito de controlar los sistemas y robar datos, mientras las evaluaciones de seguridad y vulnerabilidades, implican el proceso de buscar fallas de seguridad. Estas evaluaciones también incluyen frecuentemente revisión de políticas y procedimientos, las cuales no están incluidas en una Prueba de Penetración.

Auditorias de Seguridad

Las auditorias de Seguridad implican realizar una medición contra un conjunto riguroso de estándares, previamente determinado y fijo.

Estas auditorias son casi siempre realizadas con listas de verificación detalladas.

Algunas organizaciones de Pruebas de Penetración y Hacking Ético han creado sus propias listas de verificación internas para temas requeridos de ser descubiertos durante una prueba, pero esas listas de verificación no son tan detalladas como una auditoria exhaustiva.

Definición de Hacker Ético

Es una persona asignada para realizar Pruebas de Penetración, con el propósito de mejorar la postura de seguridad de una organización, entidad, empresa, etc.

Es contratado por una organización para intentar penetrar en la infraestructura de red o sistemas de computadoras, utilizando los mismo métodos de un Hacker “Malicioso”, con el propósito de encontrar y solucionar las vulnerabilidades de seguridad en las computadoras.

Las Pruebas de Penetración son realizadas por solicitud del propietario de los sistemas o redes objetivos, siendo totalmente legales.

Tipos de Hackers

- **Sombrero Blanco:** (White hat) Hackers Éticos los cuales utilizan sus conocimientos para propósitos defensivos. Son profesionales de seguridad utilizando sus conocimientos para ubicar debilidades e implementar medidas correctivas.

- **Sombrero Negro:** (Black Hat) Son Hackers “maliciosos” o “Crackers”, quienes utilizan sus conocimientos para propósitos ilegales o maliciosos. Rompen o violan la integridad de los sistemas remotos con intenciones dañinas.

- **Sombrero Gris:** (Gray hat) Son Hackers trabajando de manera ofensiva o defensiva, dependiendo de la situación. Esta es la línea que divide a un Hacker y un Cracker. Muchos individuos caen en ambas categorías.

Tipos de Pruebas

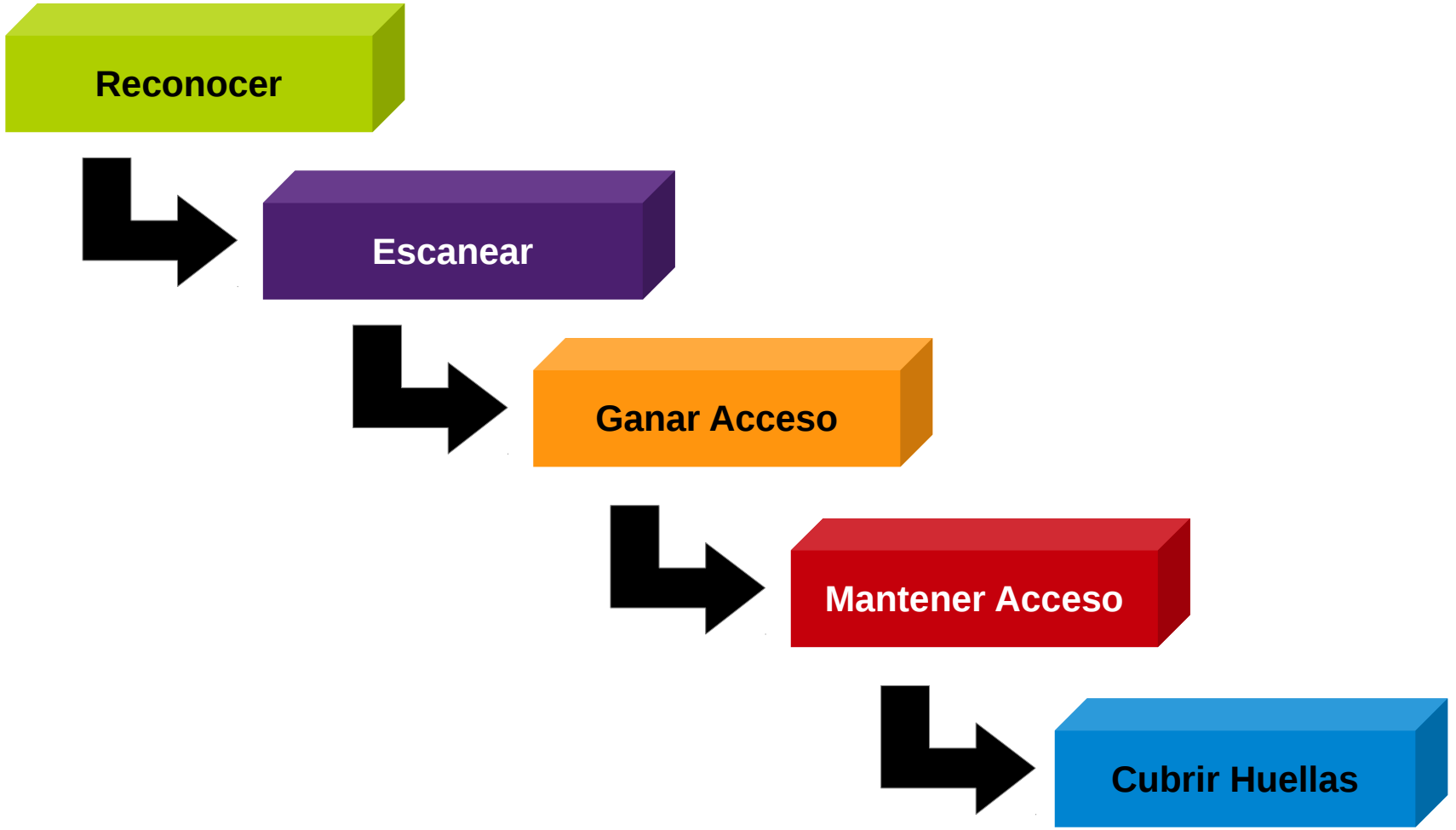
- **Caja Negra:** (Black box) Realiza pruebas de seguridad sin un conocimiento previo sobre la infraestructura de red o sistemas a ser evaluados. Este tipo de pruebas simula el ataque de un Hacker malicioso externo al perímetro de seguridad de la empresa.

- **Caja Blanca:** (White box) Realiza evaluaciones de seguridad con un conocimiento pleno de la infraestructura de la red, tal como lo tendría el administrador de la red.

- **Caja Gris:** (Gray box) Involucra realizar una evaluación de seguridad de manera interna. Este tipo de pruebas examina el alcance del acceso de un insider (interno) dentro de la red.

Etapas de Hacking Ético

Un Hacker Ético sigue una metodología similar a la utilizada por un Hacker “Malicioso”. Los fases o etapas son idénticas, sin importar las intenciones del Hacker.



Reconocimiento

Reconocimiento Pasivo

Captura información relacionada al objetivo sin conocimiento del individuo o empresa. Este proceso se denomina captura de información. Algunos métodos implican la búsqueda en la basura e ingeniería social. El Sniffing es también un mecanismo utilizado.

Reconocimiento Activo

Evalúa la red para descubrir hosts únicos, direcciones IP, y servicios en la red. Implica un mayor riesgo de detección comparado al reconocimiento pasivo. Proporciona indicios de los mecanismos de seguridad, pero el proceso también incrementa las posibilidades de ser detectado.

* Ambos tipos de reconocimiento permiten descubrir información útil a ser utilizado en un ataque.

Escaneo

Implica tomar la información descubierta durante la fase de Reconocimiento y utilizarla para examinar la red. Entre las herramientas que el Hacker utiliza durante la fase de Escaneo se incluyen:

- Marcadores (Dialers)
- Escaners de puertos /Port Scanners)
- Mapeadores de Red (Network Mappers)
- Barredores (Sweepers)
- Escaners de Vulnerabilidades (Vulnerability Scanners)

Los Hackers Éticos buscan cualquier información útil para realizar el ataque; como por ejemplo el nombre de las computadoras, las direcciones IP, cuentas de usuario, etc.

Ganar Acceso

Aquí es donde se manifiesta el Hacking “Real”. Las vulnerabilidades descubiertas durante la fase de Reconocimiento y Escaneo ahora se explotan para intentar ganar acceso u otro tipo de acción.

El método de conexión utilizado por el Hacker Ético para realizar la explotación puede ser una Red de Área Local (LAN, ya sea cableada o inalámbrica), acceso local al objetivo, Internet, o fuera de línea (off-line).

Algunas de las técnicas utilizadas incluyen, desbordamiento de buffer (buffer overflow) basados en pila, secuestro e interceptación de sesiones, obtención de credenciales por defecto o débiles, inadecuadas configuraciones en el software, etc.

Mantener el Acceso

Cuando se gana el acceso, por cualquier mecanismo o técnica, se desea mantener este acceso para realizar posteriores ataques y explotaciones.

El Hacker Ético entonces “fortalece” el sistema de otros Hackers o personal de seguridad, asegurando su acceso exclusivo con puertas traseras (backdoors), rootkits, troyanos u otros mecanismos.

Si el Hacker Ético se apropia del sistema, puede utilizarlo como base para lanzar ataques hacia otros sistemas o redes, es decir como un “Pivot”.

A este sistema también se le denomina un sistema zombi.

Cubrir Huellas

Cuando el Hacker Ético ha ganado acceso y lo mantiene en las redes y sistemas, generalmente deseará cubrir sus huellas para evitar ser detectado por el personal de seguridad, y así poder seguir utilizando el sistema comprometido, eliminar evidencia de su intrusión, o evitar acciones legales.

Se intenta eliminar los rastros del ataque, tales como archivos de registros (logs), o alarmas generados por los IDS (Intrusion Detection System) o IPS (Intrusion Prevention System).

Entre las actividades realizadas en esta etapa se incluyen la esteganografía, utilizar protocolos “tunneling” y alterar los archivos de registros.

Procedimiento para un Hacking Ético

Un Hacking Ético se realiza de una manera organizada y estructurada, como parte de una Prueba de Penetración o Auditoría de Seguridad.

La intensidad y alcance de los sistemas y aplicaciones a ser evaluados son determinadas por los requerimientos del cliente.

- Hablar con el cliente, discutir sus requerimientos de pruebas.
- Preparar y firmar un documento de acuerdo de NO divulgación (Acuerdo de Confidencialidad) con el cliente.
- Organizar al equipo de Hackers Éticos, y preparar los horarios para realizar las pruebas.
- Realizar las pruebas.
- Analizar los resultados de las pruebas, y preparar un reporte.
- Presentar el reporte al cliente.

Curso Virtual Hacking Ético 2019

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:

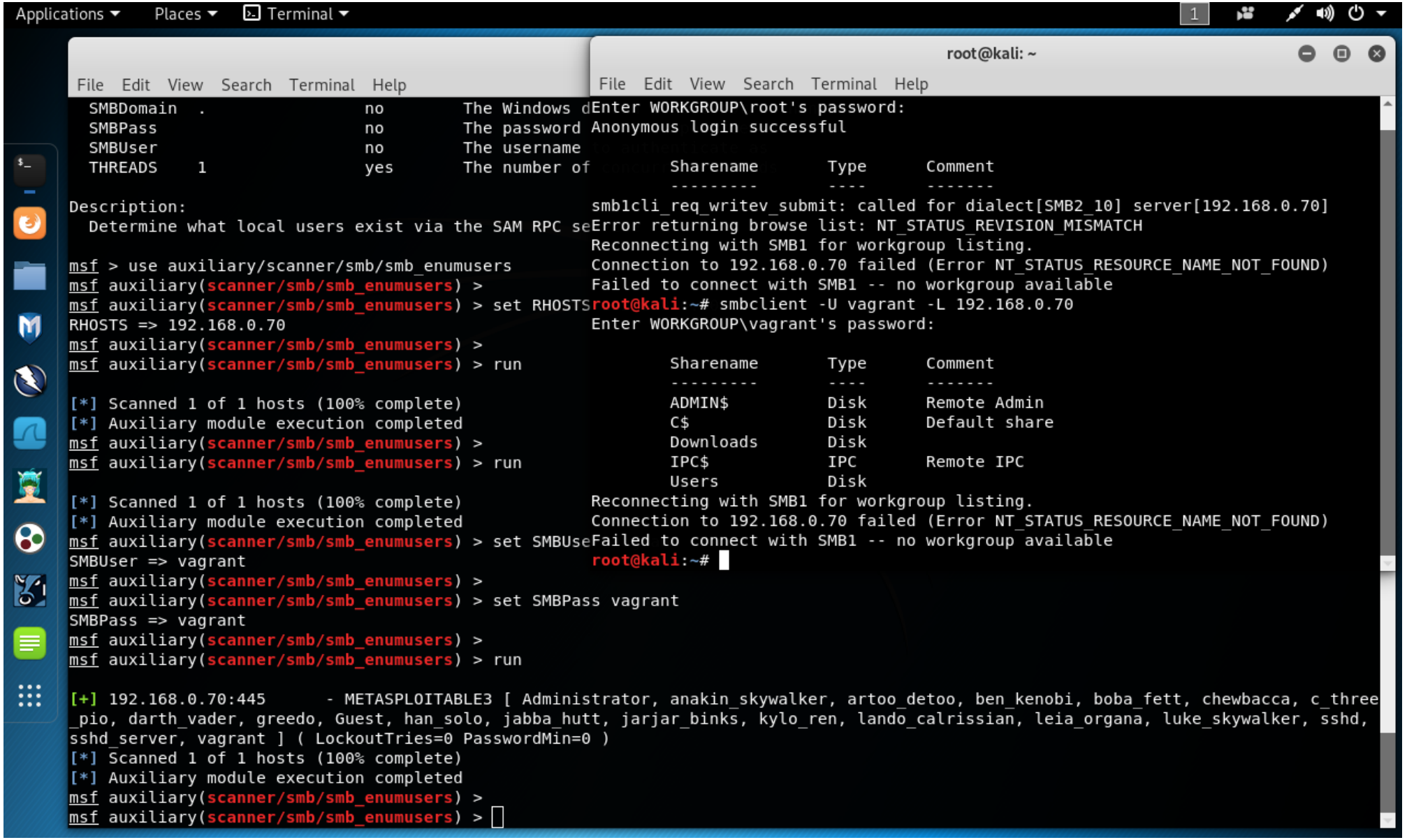
Como profesionales en ciberseguridad, se tiene la única responsabilidad de encontrar y entender las vulnerabilidades de la organización, para trabajar diligentemente en mitigarlas antes de estas sean aprovechadas por atacantes maliciosos. Este curso abarca las herramientas, técnicas y metodologías para 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.

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

Información: http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

e-mail: reydes@gmail.com Sitio web: http://www.reydes.com

Demostraciones



Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
http://www.reydes.com/d/?q=Curso_de_Informatica_Forense

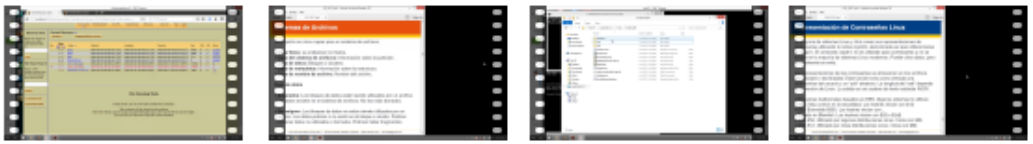
Curso Virtual Hacking con Kali Linux
http://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso Virtual OSINT - Open Source Intelligence
http://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes
http://www.reydes.com/d/?q=Curso_Forense_de_Redes

Y todos los cursos virtuales:

http://www.reydes.com/d/?q=cursos



Más Contenidos

Videos de 43 webinars gratuitos

http://www.reydes.com/d/?q=videos

Diapositivas de los webinars gratuitos

http://www.reydes.com/d/?q=node/3

Artículos y documentos publicados

http://www.reydes.com/d/?q=node/2

Blog sobre temas de mi interés.

http://www.reydes.com/d/?q=blog/1

Webinar Gratuito

Hacking Ético

v.3

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: http://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 3 de Enero del 2019