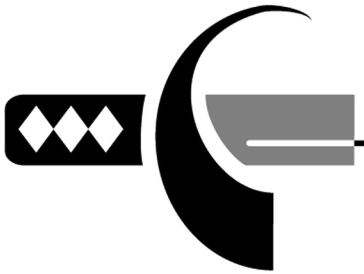
# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

LNXnetwork
SOLUCIONES ALTERNATIVAS



Centro de Ethical Hacking & Security

**www.lnxnetwork.com**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Cuál es la idea principal de un hacking ético (ethical hacking)?**

**El objetivo de Ethical Hacker es ayudar a la organización a tomar medidas preventivas en contra de ataques maliciosos atacando el sistema de manera proactiva,  manteniéndose siempre dentro de los límites legales permitidos (por la legislación en cada país).**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Hay un dicho que dice (que tiene cierto tipo de verdad): Que para atrapar a un ladrón, debes pensar como un ladrón.**

**Hoy en día la tecnología avanza a pasos agigantados y la organización depende cada vez más de ésta; en este punto es donde se vuelve crítico la protección de los activos de la empresa (especialmente donde está guardada la información).**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Una afirmación concreta: el "hackeo" involucra tener creatividad y un pensamiento "thinking out-of-the-box" (pensar fuera de la caja), entonces las pruebas de vulnerabilidad (PENTEST) y auditorias de seguridad no aseguran un blindaje en la seguridad de la organización, de forma permanente en el tiempo, tenga en cuenta que el informe presentado por el ethical hacking es una fotografía de la seguridad en un momento determinado en el tiempo.**

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**El nuevo enfoque que está fomentando la EC-Council para asegurar que las organizaciones eleven su nivel de protección, de una manera más adecuada de sus activos de información, es adoptando al enfoque de defensa un esquema de ataque ético proactivo en profundidad.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**En otras palabras, dentro del staff de seguridad debe haber un equipo de personas que estén permanentemente tratando de penetrar sus redes (realizando pruebas internas y externas), permitiendo evaluar el nivel de seguridad permanentemente, frente a las constantes vulnerabilidades y la exposición de información confidencial.**

LNXnetwork
SOLUCIONES ALTERNATIVAS

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**La definición de un Ethical Hacker es muy similar a la de una prueba de penetración, pero con una visión más ámplia. El Ethical Hacker (sombrero blanco) es un individuo que pertenece a la organización (o es contratado por ella) para hacer intentos de penetración en sus redes o sistemas informáticos, usando los mismos métodos que un Hacker (sombrero negro).**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**El Hackeo (o hacking) es considerado un delito cuando no hay un permiso, solicitud o contrato por parte de la organización; por este motivo, siempre es importante asegurarse de que están dentro del marco legal del contrato y de las Leyes.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

## OBJETIVO GENERAL

**Esta clase llevará al participante a conocer herramientas open source,que pueden ser usadas en un entorno interactivo, para un hackeo ético o pentest. Se le mostrará como explorar, probar, "hackear" y asegurar sus propios sistemas.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**El entorno intensivo del laboratorio da a cada estudiante el conocimiento y experiencia práctica de como identificar vulnerabilidades esenciales de seguridad. Los estudiantes empezarán por entender como funcionan las defensas periféricas que posteriormente podrán usar para explorar y atacar sus propias redes; ninguna red real es dañada.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Armandose un kit para ethical hacking**
**En su mayoría los ethical hacker usan como sistema Operativo GNU/Linux. Muchos prefieren bajar una distribución de preferencia y comenzar a instalar los paquetes o aplicaciones que va a ir utilizando, otros prefieren directamente consumir alguna .ISO ya armada como ser:**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**(solo citaré algunas destacadas)**

**Kali (basada en Debian)  https://www.kali.org**

**BackBox Linux (basada en Ubuntu)  https://backbox.org**

**Parrot  (basada en Debian)  https://www.parrotsec.org/**

**Pentoo (basada en Gentoo)  http://www.pentoo.ch**

**SamuraiWTF (ex SamuraiSTFU) basada en Ubuntu**
**https://www.owasp.org/index.php/OWASP_SamuraiWTF_Project**
**http://samurai.inguardians.com**

**Fedora Security Spin (basada en Fedora)**
**https://fedoraproject.org/wiki/Security_Lab**

**WifiSlax  (basada en Slackware)  http://www.wifislax.com/**

**Bugtraq  (basada en Ubuntu, Debian o openSUSE)**
**http://bugtraq-team.com**

Centro de Ethical Hacking & Security

LNXnetwork
SOLUCIONES ALTERNATIVAS

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**¿Qué debe tener una distro de seguridad mínimamente?:**

**-Anonimato e investigación:**
**Osiris, Proxys, Web Domain, Geolocalización, Investigaciones, Host redirección, borrado de logs.**
**-Enumeración: Fingerprint y reconocimiento**
**-Mapping: IPV6, análisis de puertos, VPN**
**-Auditoría Web: Bases de datos, analítica web, panel finders, spiders**
**-Detección de vulnerabilidades**
**-Pentesting: exploits, flooding, IPV6**
**-Sniffers**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**-Ataques de Fuerza Bruta: online, offline, hashing, diccionarios**

**-Comunicaciones: 802.11, GSM, HRPT | WEFAX | VOIP**

**-Malware Laboratorios: Host redireccion, Joiners & Crypters, Signature research, Webshells, botnets, troyanos, virus, spreaders & downloaders, backdoors, smart phones, SandBox.**
**-Antimalware: cortafuegos, antirootkits.**
**-Análisis forense: análisis de archivos ejecutables, disk analysis, digital forensics,  carving, debugger, documentos, hassing & passwords, memoria RAM, network.**
**-Seguridad movil**
**-Virtualización**

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Esta es una lista de programas de que debemos tener en nuestro servidor:**

**Wireless Hacking**

- **Aircrack-ng (suite para capturar redes wireless)**
- **Kismet (sniffer para redes wireless)**
- **inSSIDer (identificar redes wireless y conocer su intensidad de señal)**
- **KisMAC (buscador redes wireless abiertas)**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Intrusion Detection Systems**

**Snort (es un sniffer que detecta actividades inusuales de intrusos en la red)**

**NetCop (es UTM de seguridad)**

**Port Scanners**

**Nmap (suite de escaneo de puertos y servicios)**

**Superscan (herramienta para realizar escaneo de puertos y servicios)**

**Angry IP Scanner (scanner de direcciones IPs).**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Encryption Tools**

**TrueCrypt (es una suite para encriptar/desencriptar directorios y unidades). Actualmente está deprecado; un software similar es: veracrypt**

**OpenSSH (suite que permite establecer una conxión cifrada por medio de ssh)**

**Putty (suite que termine conectarse por ssh a equipos linux)**

**OpenSSL (es una suite que permite implementar Secure Sockets Layer (SSL))así como otros protocolos relacionados con la seguridad, como el Transport Layer**

**Security (TLS). OpenSSL también permite crear certificados digitales que pueden aplicarse a un servidor, por ejemplo Apache.**

**Tor ("The Onion Router" (traducido a español: El Encaminamiento/Enrutamiento de Cebolla))**

**OpenVPN (es una solución de conectividad basada en software libre: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada))**

**Stunnel (utilizado para la creación de túneles TLS/SSL)**

**KeePass (es una herramienta de administración de contraseñas segura y fácil de utilizar)**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Password Crackers**

**Ophcrack (es una herramienta para crackear las contraseñas de Windows basada en las tablas Rainbow)**

**Medusa (es una herramienta destinada a ser rápida en los ataques de fuerza bruta)**

**RainbowCrack (es un programa informático que genera tablas de "rainbow tables" para ser utilizado en el descifrado de contraseñas)**

**Wfuzz (es una herramienta diseñada por edge-security para la fuerza bruta aplicaciones web)**

**Brutus (es una herramienta de cracking de contraseñas)**

**L0phtCrack (es una herramienta de auditoría y recuperación de contraseñas (ahora llamada LC5))**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

fgdump (nos permite hacer un dump de los hashes de las contraseñas de un usuario Windows)

THC Hydra (es un Software que se usa para crakear por fuerza bruta la contraseñas)

John The Ripper (es un programa de criptografía que aplica fuerza bruta para descifrar contraseñas)

Aircrack (es una suite de software de seguridad inalámbrica. Consiste en un analizador de paquetes de redes, un crackeador de redes WEP, WAP, WPA2)

Cain and Abel (es una herramienta de recuperación de contraseñas para Microsoft Windows)

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

## Packet Crafting (trabajos con paquetes)

**Hping (es una herramienta en linea de comandos que nos permite crear y analizar paquetes TCP/IP)**

**Scapy ( es un manipulador de paquetes interactivo realmente potente y flexible escrito en Python que permite esnifar, generar paquetes manipulados).**

**Netcat (es una herramienta de red que permite a través de intérprete de comandos y con una sintaxis sencilla abrir puertos TCP/UDP en un HOST)**

**Yersinia (es una herramienta que es usada para analizar y probar las redes para aprovechar alguna debilidad en diferentes protocolos de red.)**

**Nemesis (Suite tiene la capacidad de recuperar datos de los códigos de producto).**

**Socat (Socket CAT es una aplicación igual que el Netcat pero utiliza un canal mucho más seguro "fue diseñado pensando en la seguridad" usando sockets, SSL, etc.)**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Traffic Moinitoring (monitoreo de tráfico)**

**Splunk (es un software para buscar, monitorear y analizar logs de aplicaciones, sistemas e infraestructura)**

**Nagios (es un sistema de monitorización de redes ampliamente utilizado, que vigila equipos (hardware) y servicios (software))**

**P0f (es una herramienta de identificación pasiva de sistema operativo, permite detectar el sistema y la versión de las maquinas conectadas a una red)**

**Ngrep (es una red que analiza paquetes. Se basa en el pcap y GNU/regex).**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Packet Sniffers (analizadores de paquetes)**

**Wireshark (antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes)**

**Tcpdump (es una herramienta cuya utilidad principal es analizar el tráfico que circula por la red)**

**Ettercap (este programa que nos permite sniffar el tráfico de red y obtener así las contraseñas)**

**dsniff (es una herramienta que analiza protocolos: FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS,etc)**

**EtherApe (es una aplicación que muestra gráficamente y en tiempo real la actividad de nuestra red.)**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Vunerability Exploitation**

**Metasploit (es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad, muy usado para test de seguridad)**

**sqlmap (es una de las herramienta más conocidas para hacer ataques SQLi (SQL Injection) escrita en Python.)**

**sqlninja (es una herramienta dirigida a aprovechar las vulnerabilidades de inyección SQL en una aplicación web)**

**Social Engineer Toolkit (SET - es un conjunto de herramientas especialmente diseñadas para realizar ataques de Ingeniería Social)**

**NetSparker (es un escáner de seguridad de aplicaciones web. Descubrirá automáticamente los defectos que podrían dejar que peligrosamente expuesto.)**

**BeEF (Es una herramienta de pruebas de penetración basada en la web.)**

**Dradis ( es una herramienta que permite la presentación de informes, muy usada por los profesionales en seguridad de TI.)**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

## Metodologías

**Se tienen en cuenta las metodologías OSSTMM, ISSAF y OWASP durante todo el proceso, aunque el equipo auditor podrá hacer chequeos adicionales no contemplados en estas metodologías fruto de experiencias previas.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**OSSTMM (www.isecom.org/)**

**Representa un estándar de referencia imprescindible, para todo aquel que quiera llevar a cabo un testeo de seguridad en forma ordenada y con calidad profesional.**

**A fin de organizar su contenido, la metodología se encuentra dividida en varias secciones. Del mismo modo, es posible identificar en ella, una serie de módulos de testeo específicos, a través de los cuales se observan cada una de las dimensiones de seguridad, integradas con las tareas a llevar a cabo en los diferentes puntos de revisión (Seguridad de la Información, Seguridad de los Procesos, Seguridad en las Tecnologías de Internet, Seguridad en las Comunicaciones, Seguridad Inalámbrica y Seguridad Física).**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**OSSTMM no solo alcanza los ámbitos técnicos y de operación de seguridad tradicionales, sino que, se encarga de normar aspectos tales como: las credenciales del profesional a cargo del test, la forma en la que el test debe ser comercializado, la forma en la que los resultados del mismo deben ser presentados, las normas éticas y legales que deben ser tenidas en cuenta al momento de concretar el test, los tiempos que deberían ser tenidos en cuenta para cada una de las tareas, y por sobre todas las cosas, incorpora el concepto de RAVs (Valores de Evaluación de Riesgo) y con ellos la frecuencia con la cual la prueba debe ser ejecutada a fin de proveer más que una instantánea en el momento de su ejecución.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**ISSAF (www.oissg.org/)**
**Constituye un framework detallado respecto de las prácticas y conceptos relacionados con todas y cada una de las tareas a realizar al conducir un testeo de seguridad. La información contenida dentro de ISSAF, se encuentra organizada alrededor de lo que se ha dado en llamar "Criterios de Evaluación", cada uno de los cuales ha sido escrito y/o revisado por expertos en cada una de las áreas de aplicación.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Estos criterios de evaluación a su vez, se componen de los siguientes elementos:**

- **Una descripción del criterio de evaluación**
- **Puntos y Objetivos a cubrir**
- **Los pre-requisitos para conducir la evaluación**
- **El proceso mismo de evaluación**
- **El informe de los resultados esperados**
- **Las contramedidas y recomendaciones**
- **Referencias y Documentación Externa.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Por su parte y a fin de establecer un orden preciso y predecible, dichos "Criterios de Evaluación", se encuentran contenidos dentro de diferentes dominios entre los que es posible encontrar, desde los aspectos más generales, como ser los conceptos básicos de la "Administración de Proyectos de Testeo de Seguridad", hasta técnicas tan puntuales como la ejecución de pruebas de Inyección de Código SQL (SQL Injection) o como las "Estrategias del Cracking de Contraseñas.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**A diferencia de lo que sucede con metodologías "más generales", si el framework no se mantiene actualizado, muchas de sus partes pueden volverse obsoletas rápidamente (específicamente aquellas que involucran técnicas directas de testeo sobre determinado producto o tecnología). Sin embargo esto no debería ser visto como una desventaja, sino como un punto a tener en cuenta a la hora de su utilización.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**OTP (OWASP Testitng Project)**
**https://www.owasp.org/index.php/OWASP_Testing_Project**
**OWASP Si bien no es un estandar, promete convertirse en uno de los proyectos más destacados en lo que al testeo de aplicaciones web se refiere. La metodología consta de 2 partes, en la primera se abarcan los siguientes puntos:**

- **Principios del testeo**
- **Explicación de las técnicas de testeo.**
- **Explicación general acerca del framework de testeo de OWASP.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Y en la segunda parte, se planifican todas las técnicas necesarias para testear cada paso del ciclo de vida del desarrollo de software. Incorpora en su metodología de testeo, aspectos claves relacionados con el "Ciclo de Vida del Desarrollo de Software" o SDCL (Por sus siglas en Ingles "Software Development Life Cycle Process") a fin de que el "ámbito" del testeo a realizar comience mucho antes de que la aplicación web se encuentre en producción.**

LNXnetwork
SOLUCIONES ALTERNATIVAS

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**De este modo, y teniendo en cuenta que un programa efectivo de testeo de aplicaciones web, debe incluir como elementos a testear: Personas, Procesos y Tecnologías, OWASP Testing Project delinea en su primera parte conceptos claves a la vez que introduce un framework específicamente diseñado para evaluar la seguridad de aplicaciones web a lo largo de su vida.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Paso 1 Antes de comenzado el desarrollo**

a) Revisión de Políticas y Estándares

b) Desarrollo de un Criterio de Medidas y Métricas (Aseguramiento de la Trasabilidad)

**Paso 2 Durante la definición y el diseño**

a) Revisión de los Requerimientos de Seguridad

b) Diseño de Revisión de Arquitectura

c) Creación y Revisión de modelos UML

d) Creación y Revisión de modelos de Amenazas

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Paso 3 Durante el desarrollo**

- a) Code Walkthroughs
- b) Revisión de Código

**Paso 4 Durante el deployment**

- a) Testeo de Penetración sobre la Aplicación
- b) Testeo sobre la Administración y Configuración

**Paso 5 Operación y mantenimiento**

- a) Revisión Operacional
- b) Conducción de Chequeos Periódicos
- c) Verificación del Control de Cambio

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Cuales son los pasos que se deben realizar?**

**La realización del test de penetración está regida por fases. Cada fase brinda información útil que el pentester debe tomar para recomendar como paliar cada debilidad encontrada.**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

**Las fases son:**

1. **Recopilación de información**
2. **Enumeración de la red**
3. **Exploración de los sistemas**
4. **Extracción de información**
5. **Acceso no autorizado a información sensible**
6. **Auditoría de las aplicaciones web**
7. **Elaboración de informes**
8. **Comprobación del proceso de parcheado de los sistemas**
9. **Informe final**

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS

## Preguntas?

# Laboratorio de ethical hacking utilizando herramientas OpenSource

LNXnetwork
SOLUCIONES ALTERNATIVAS


LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security