Único Curso del Año 2016

Domingos 12 y 19 de Junio del 2016
De 9:00am a 12:00m (UTC -05:00) – 6 Horas en Total

1. Presentación:

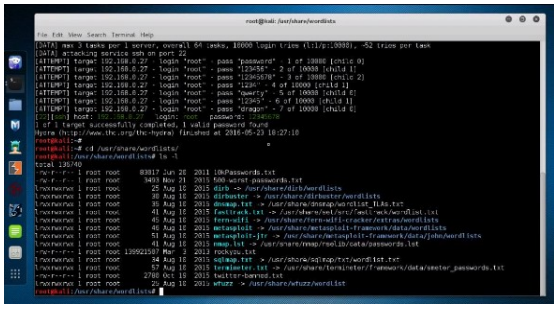
El Sistema Operativo GNU/Linux ha incrementado notablemente su difusión y utilización a nivel mundial. GNU/Linux funciona en servidores proporcionando diversos servicios como web, correo electrónico, servidores de nombres. También funciona en computadoras personales, y en dispositivos móviles como teléfonos inteligentes. GNU/Linux basa su fortaleza en código open-source o de fuente abierta, además de una gran comunidad de desarrolladores.

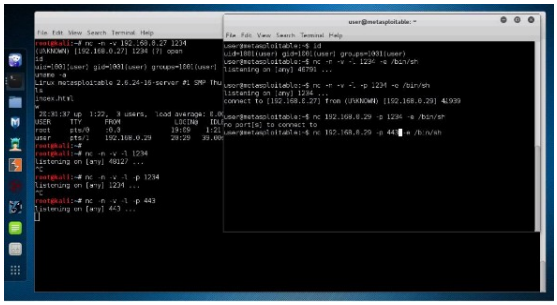
GNU/Linux es uno de los territorios más anhelados por los profesionales del área, pues sus posibilidades son casi infinitas. Cualquier cosa requerida a intentar y construir, hace a una computadora con GNU/Linux atractiva para muchas personas. La dificultad empieza cuando se necesita asegurar el sistema. Pues primero se deben identificar todas las posibles vulnerabilidades, fallas, o malas configuraciones. Los esfuerzos entonces deben enfocarse en asegurarlo, y consecuentemente evaluar o probar si todo esto se ha realizado adecuadamente.

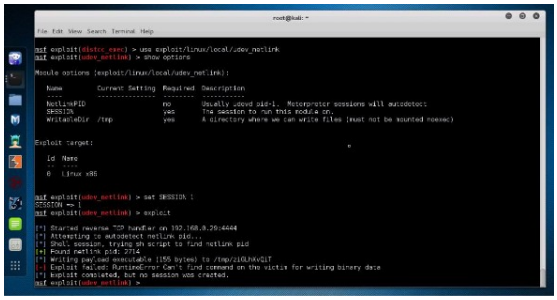
Este curso completamente práctico expone una metodología y herramientas esenciales para realizar una pruebas de penetración adecuada contra Sistemas GNU/Linux. Todo el curso se desarrolla en un entorno de laboratorio controlado utilizando máquinas virtuales.

2. Temario:

- Captura de Información
- Enumeración Whois y DNS
- Consultas a los DNS
- Cuentas de Correo
- Identificación del Perímetro y Sondeo de la Red
- Escaneos Activos y Pasivos
- Escaneo de Puertos TCP y UDP
- Identificación Activa y Pasiva del Sistema Operativo
- Captura de los Banners
- Enumeración de Servicios Desconocidos
- Identificación y Explotación de Vulnerabilidades
- Scripts de Nmap y Escaneos de Logins por defecto
- OpenVas
- Metasploit Framework (FTP, SMTP, SMB, NFS, MySQL PostgreSQL, VNC)
- Vulnerabilidades Internas
- Shells y Shell inversos
- Escalado de Privilegios
- Ataques Remotos y Locales contra las Contraseñas
- Sniffing de Paquetes de Red.







3. Material:

Se sugiere al participante descargar como mínimo los siguientes archivos en su sistema para desarrollar el Curso.

Kali Linux 2.0
Nombre del Archivo: Kali-Linux-2016.1-vm-i686.7z
Link de Descarga: https://images.offensive-security.com/virtual-images/Kali-Linux-2016.1-vm-i686.7z

Hackerdemia
Nombre del Archivo: De-ICE_S1.123.iso
Link de Descarga: https://www.vulnhub.com/?q=hackerdemia&sort=date-asc&type=vm

Metasploitable 2.
Nombre del Archivo: metasploitable-linux-2.0.0.zip
Link de Descarga: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

[*] Si el participante lo requiere se le puede enviar un DVD con las máquinas virtuales, añadiendo S/. 45 Soles por el concepto de gastos de envío a cualquier lugar del Perú.

4. Día y Horario:

La duración total del Curso es de 6 (seis) horas. El Curso se dictará en los siguientes días y horarios.

Domingos 12 y 19 de Junio del 2016
De 9:00am a 12:00m (UTC -05:00) - 6 Horas en Total

[*] No habrá reprogramaciones. El Curso se dictará **sin** ningún requisito mínimo de participantes.

5. Inversión y Forma de Pago:

El Curso tiene un costo de:

S/. 115 Soles o $ 35 Dólares

El pago del Curso se realiza mediante un depósito bancario en la siguiente cuenta:

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

Una vez realizado el depósito, enviar por favor el voucher escaneado o sencillamente detallar los datos al siguiente correo: **caballero.alonso@gmail.com**.

Para residentes en otros países por favor escribir un mensaje de correo electrónico para consultar el mecanismo de pago. Confirmado el depósito se enviará al correo electrónico del participante, los datos necesarios para conectarse al Sistema y poder participar en el Curso.

6. Más Información:

Si desea mayor información sobre el Curso Virtual de Hacking Linux, tiene a su disposición los siguientes mecanismos de contacto:

Correo electrónico: caballero.alonso@gmail.com

Vía Web: http://www.reydes.com

Celular: (+51) 949304030

7. Sobre el Instructor:

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPI Linux Essentials Certificate, Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management. Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de trece años de experiencia en el área y desde hace nueve años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. 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, Informática Forense, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: http://www.ReYDeS.com.