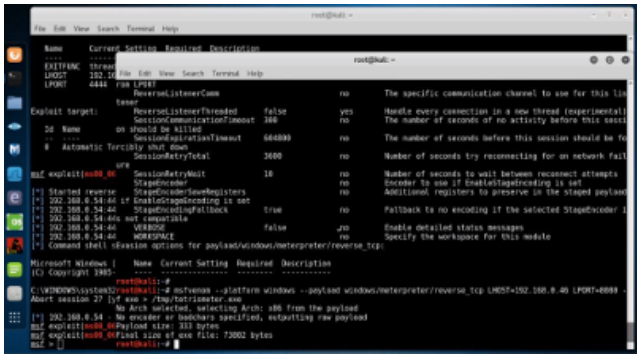
# Hacking con Kali Linux

## Curso Virtual - 2018



Último Curso del Año 2018

**Fechas**

Domingos 4, 11 y 18 de Noviembre del 2018

**Horario:**

De 9:00 am a 12:15 pm (UTC -05:00)

**Este curso virtual ha sido dictado a participantes residentes en los siguientes países:**

## 1. Presentación

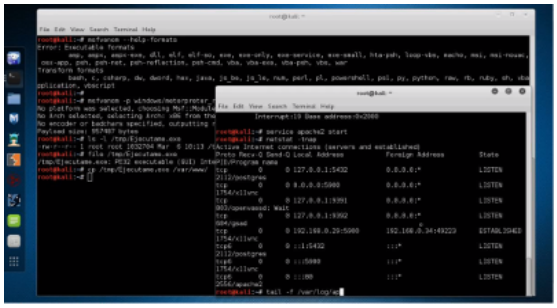
Kali Linux es una distribución basada en GNU/Linux Debian, dirigida a auditorias de seguridad y pruebas de penetración avanzadas. Kali Linux contiene cientos de herramientas destinadas a diversas tareas en seguridad de la información, tales como pruebas de penetración, investigación de seguridad, forense digital e ingeniería inversa. Kali Linux. Incluye herramientas para la captura de información, análisis de vulnerabilidades, análisis de aplicaciones web, evaluación para bases de datos, ataques a contraseñas, ataques inalámbricos, Ingeniería Inversa, herramientas para la explotación, sniffing y spoofing, explotación posterior, forense digital, y herramientas para el reporte.

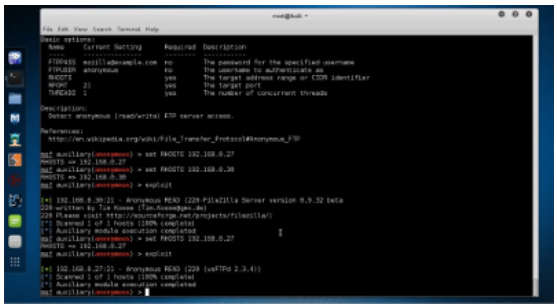
## 2. Objetivos

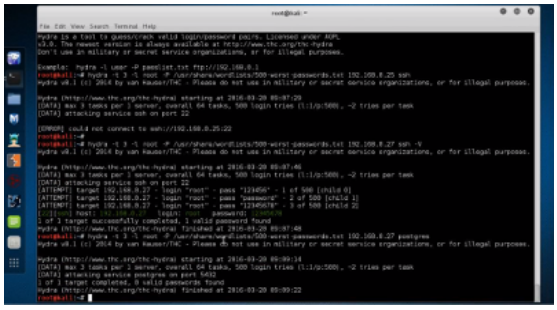
Este curso proporciona una excelente fuente de conocimiento para iniciarse en el área del Hacking Ético, además de ser una guía práctica para la utilización de las herramientas más populares durante la realización de Pruebas de Penetración. Así mismo este curso proporciona conocimientos fundamentales sobre pruebas de penetración utilizando Kali Linux, conceptos sobre programación, metasploit, captura de información, búsqueda de vulnerabilidades, técnicas para la captura de tráfico, explotación de vulnerabilidades, técnicas manuales de explotación, ataques a contraseñas, ataques del lado del cliente, ingeniería social, técnicas para evadir antivirus y técnicas de post-explotación.

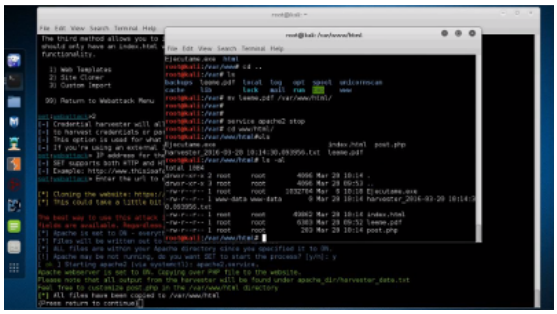
## 3. Temario

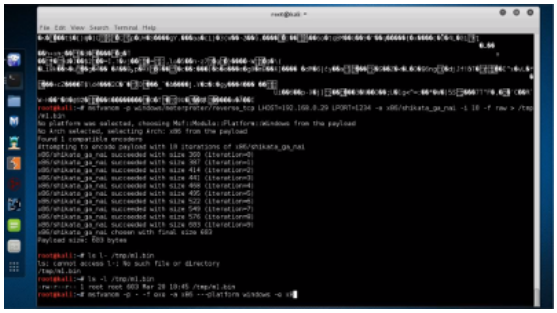
- Configurar un Laboratorio Virtual
- Introducción a Kali Linux
- Bases de Programación
- Scripting con Bash y Python
- Utilizando Metasploit Framework
- Payloads
- Tipos de Shells
- Configurar Manualmente un Payload
- Utilizar Módulos Auxiliares
- Captura de Información
- Captura OSINT
- Escaneo de Puertos
- Encontrar Vulnerabilidades
- Nessus
- Nmap Scripting Engine NSE
- Módulos para el Escaneo en Metasploit
- Escaneo de Aplicaciones Web
- Análisis Manual
- Captura de Tráfico
- Utilizando Wireshark
- Envenenamiento del Cache ARP y Cache DNS
- Ataques SSL y SSL Stripping
- Explotación Remota
- Explotación a WebDAV y PhpMyAdmin
- Descargar Archivos Sensibles
- Explotar Aplicaciones Web de Terceros, Servicios Comprometidos, Recursos Compartidos NFS.
- Ataques en Línea de Contraseñas
- Ataques Fuera de Línea de Contraseñas
- Explotación del Lado del Cliente
- Evadiendo Filtros con Payloads de Metasploit
- Ataques del Lado del Cliente
- Ingeniería Social
- Social Engineer Toolkit SET
- Ataques Web
- Evadir Antivirus
- Como Funcionan los Antivirus
- Evadiendo un Programa Antivirus
- Post Explotación
- Meterpreter
- Scripts de Meterpreter
- Módulos de Post Explotación en Metasploit
- Escalado de Privilegios Locales
- Captura de Información Local
- Movimiento Lateral
- Pivoting
- Persistencia







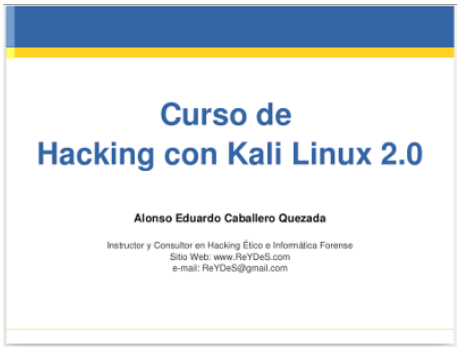




## 4. Material

Todos los participantes al Curso Virtual de Hacking con Kali Linux, recibirán las diapositivas en formato PDF, utilizadas durante el desarrollo del curso. Además tendrán la posibilidad de descargar los videos de cada sesión.

Adicionalmente el participante tiene la opción de adquirir por S/. 75 Soles adicionales, 2 (dos) DVD conteniendo el material y las máquinas virtuales utilizadas durante el desarrollo del curso. Este costo incluye los gastos de envío a cualquier lugar del Perú.




En caso el participante no adquiera el DVD, se le sugiere descargar y configurar las siguientes máquinas virtuales, para desarrollar el Curso.

- **Kali Linux**
  Imágenes de 64 bits o 32 bits para Vmware Player, Virtual Box o Hyper-V
  https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-hyperv-image-download/

- **Metasploitable 2**
  Enlace de Descarga:
  http://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download

- **Metasploitable 3**
  Enlace de Descarga:
  https://github.com/rapid7/metasploitable3

## 5. Fechas y Horarios

El Curso Virtual de Hacking con Kali Linux tiene una duración total de 9 (nueve) horas, las cuales se dividen en 3 (tres) sesiones de 3 (tres) horas.

**Fechas:**

Domingos 4, 11 y 18 de Noviembre del 2018

**Horario:**

De 9:00 am a 12:15 pm (UTC -05:00). 9 Horas en Total.

**[*]** El Curso se dicta sin ningún requisito mínimo en el número de participantes.

## 6. Inversión y Forma de Pago

El Curso Virtual de Hacking con Kali Linux tiene un costo de:

**S/. 250 Soles o $ 75 Dólares**

El pago del curso se realiza mediante alguno de los siguientes mecanismos:

| Residentes en Perú | Residentes en Otros Países |
|---|---|
| Deposito Bancario en la siguiente cuenta:<br>Scotiabank<br>ScotiaBank<br>Cuenta de Ahorros en Soles: 324-0003164<br>A nombre de: Alonso Eduardo Caballero Quezada<br><br>También puede realizar el depósito en un Agente Scotiabank. Encuentre el más cercano utilizando la siguiente página:<br><br>http://intl.scotiabank.com/es-pe/locator/Default.aspx<br><br>Una vez realizado el depósito, enviar por favor el voucher escaneado o sencillamente detallar los datos al siguiente correo: **caballero.alonso@gmail.com** | Transferencia de dinero mediante alguna de las siguientes empresas:<br><br>Western Union: http://www.westernunion.com<br>WESTERN UNION WU moving money for better<br><br>MoneyGram: https://www.moneygram.com<br>MoneyGram<br><br>Escribame por favor un mensaje de correo electrónico para detallarle los datos necesarios para realizar la transferencia.<br><br>Una vez realizada la transferencia, enviar por favor el documento escaneado al siguiente correo: **caballero.alonso@gmail.com** |

Confirmado el depósito o la transferencia se le enviará al correo electrónico del participante los datos necesarios para conectarse al sistema, además del material utilizado durante el desarrollo del curso.

El curso se realiza utilizando el sistema de video conferencias Anymeeting. El cual proporciona la transmisión de audio y video en tiempo real de alta calidad, tanto para el instructor como también para los participantes, entre otras características ideales para impartir cursos de manera virtual.

INTERMEDIA ANYMEETING

http://www.anymeeting.com

## 7. Más Información

Si requiere más información sobre el Curso Virtual de Hacking con Kali Linux tiene a su disposición los siguientes mecanismos de contacto:

- **Correo electrónico:** caballero.alonso@gmail.com
- **Vía Web:** http://www.reydes.com/d/?q=contact
- **Teléfono:** (+51) 949304030

# 8. Instructor

**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, Cybersecurity Management y Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals y Phishing Countermeasures.. Ha sido instructor en el OWASP LATAM Tour Lima, Perú del año 2014 y expositor en el 0x11 OWASP Perú Chapter Meeting 2016, además de Conferencista en PERUHACK 2014, instructor en PERUHACK2016NOT, y conferencista en 8.8 Lucky Perú 2017. Cuenta con más de catorce años de experiencia en el área y desde hace diez años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. 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, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: http://www.ReYDeS.com.