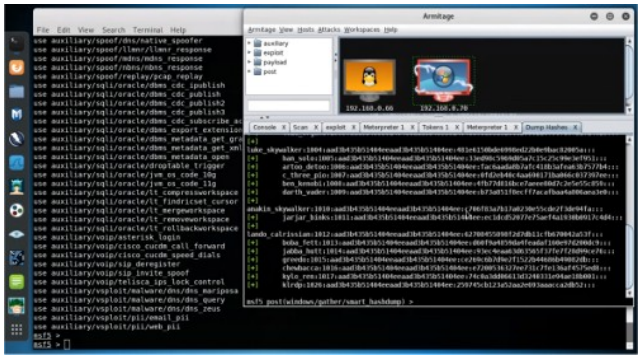
Metasploit Framework

Curso Virtual - 2020



Único Curso del Año 2020

Fechas:

Sábados 18 y 25 de Abril del 2020

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:

Metasploit Framework es actualmente una de las herramientas de auditoría más útil disponible para profesionales de seguridad. Incluye una amplia cantidad de exploits de nivel comercial, y un completo entorno para el desarrollo de exploits, aunado a herramientas las cuales permiten desde capturar información de la red, hasta la utilización de plugins para encontrar vulnerabilidades web. Metasploit Framework está lejos de ser únicamente una colección de exploits. Es una infraestructura la cual puede ser construida y utilizada para necesidades específicas.

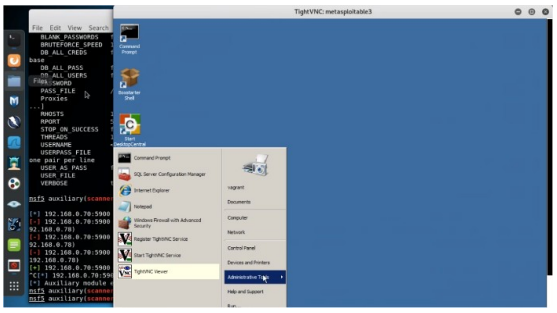
Metasploit está respaldada por una comunidad de más de 200,000 usuarios y contribuyentes. Es la solución de mayor impacto para pruebas de penetración del planeta. Siendo factible descubrir vulnerabilidades en las defensas, enfocarse en los riesgos más altos, y mejorar los resultados de seguridad.

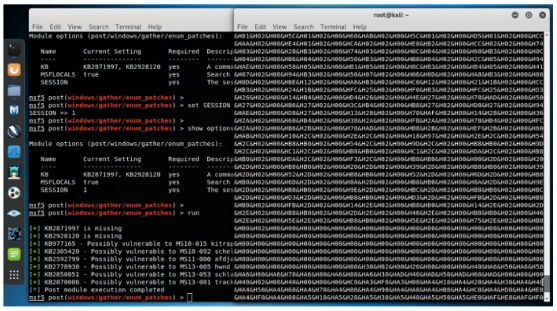
Metasploit permite conocer las debilidades, utiliza la mayor bases de datos sobre exploits cuyo código ha sido revisado, permite simular ataques del mundo real contra las defensas, y expone credenciales débiles o reutilizadas.

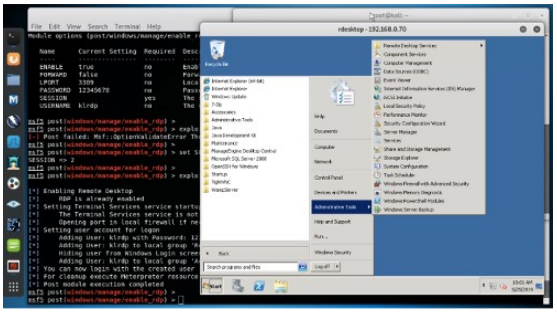
Este curso totalmente práctico expone las principales características, funcionalidades y capacidades proporcionadas por Metasploit Framework. Así mismo este curso es una excelente fuente de conocimiento tanto para quienes recién se inician con la utilización de esta herramienta, como para los profesionales quienes lo utilizan constantemente.

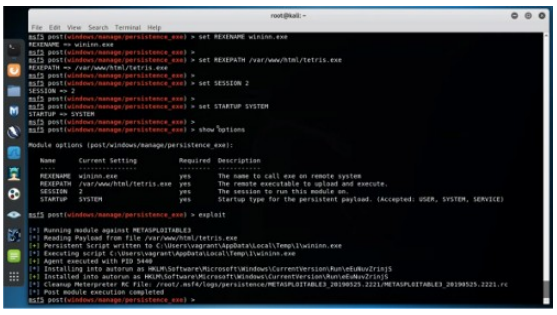
2. Temario:

- Introducción a Metasploit Framework
- Sistemas de Archivos y Librerías
- Módulos y Plugins
- Fundamentos de Metasploit Framework
- Consola de Metasploitt
- Exploits y Payloads
- Bases de Datos y Meterpreter
- Recopilación de Información
- Escaneo de Puertos
- Encontrando servidores MSSQL
- Identificación de Servicios
- Sniffing de Contraseñas
- Barridos SMNP.
- Enumerar Parches de Windows
- Escaneo de Vulnerabilidades
- Verificación de Login SMB
- Autenticación VNC
- Escaner Web WMAP
- Trabajando con Nessus.
- Exploits
- Ataques del lado del cliente
- Payloads Binarios
- Exploits del Lado del Cliente.
- Post Explotación con Metasploit Framework
- Escalado de Privilegios
- Gestión del Registro de Eventos
- Incognito
- Interactuando con el Registro
- Habilitar el Escritorio Remoto
- Sniffing de Paquetes
- TimeStomp
- Captura de Pantalla
- Buscar Contenidos
- John The Ripper.
- Meterpreter .
- Manteniendo el Acceso
- Atrapar Pulsaciones del Teclado
- Puerta Trasera con Meterpreter
- Puerta Trasera Persistente.
- Otros usos de Metasploit Framework









3. Material:

Todos los participantes al Curso Virtual de Metasploit Framework tendrán la posibilidad de descargar los videos de cada sesión, un día después de impartida la misma.

Adicionalmente el participante tiene la opción de adquirir por S/. 50 Soles adicionales, Un (1) DVD conteniendo 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 los DVDs, se le sugiere descargar y configurar las siguientes máquinas virtuales.

Kali Linux:

Link de Descarga: https://www.kali.org/downloads/

Metasploitable 2

Link de Descarga: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Metasploitable 3

Link de Descarga: https://github.com/rapid7/metasploitable3

4. Día y Horario:

El Curso Virtual de Metasploit Framework tiene una duración total de seis (6) horas, las cuales se dividen en dos (2) sesiones de tres (3) horas cada una.

- **Fechas:**
  Sábados 18 y 25 de abril del 2020
- **Horario:**
  De 9:00 am a 12:15 pm (UTC -05:00). 6 horas en total.

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

5. Inversión y Forma de Pago:

El Curso Virtual de Metasploit Framework tiene un costo de:

S/. 165 Soles o $ 50 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: Scotiabank ScotiaBank Cuenta de Ahorros en Soles: 324-0003164 A nombre de: Alonso Eduardo Caballero Quezada También puede realizar el depósito en un Agente Scotiabank. Encuentre el más cercano utilizando la siguiente página: https://intl.scotiabank.com/es-pe/locator/Default.aspx Una vez realizado el depósito, enviar por favor el voucher escaneado o sencillamente detallar los datos al siguiente correo: **caballero.alonso@gmail.com**	Transferencia o pago mediante Western Union o Moneygram, También mediante Paypal. MoneyGram WESTERN UNION WU moving money for better Paypal: PayPal Escríbame por favor un mensaje de correo electrónico para detallarle los datos necesarios para realizar la transferencia o el pago. Una vez realizada la transferencia o el pago, 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

6. Más Información:

Si requiere más información sobre el Curso Virtual de Metasploit Framework, tiene a su disposición los siguientes mecanismos de contacto:

Correo electrónico: caballero.alonso@gmail.com

Vía Web: http://www.reydes.com

Celular: +51 949 304 030

7. 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, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures y Pen Testing. 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 dieciséis años de experiencia en el área y desde hacen doce 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.