Curso Virtual Metasploit Framework

Único Curso del Año 2018

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

Domingos 3 y 10 de Junio del 2018

De 9:00 am a 12:15 pm (UTC -05:00) – 6 horas en Total

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.

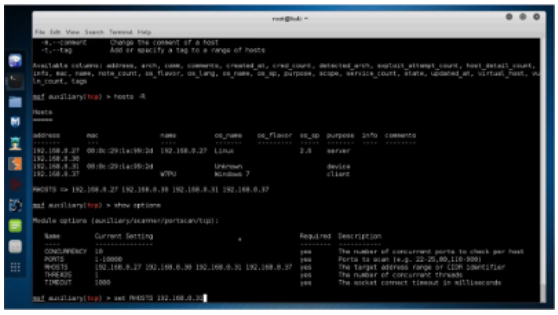
Metasploit está respaldada por una comunidad de más de 200,000 usuarios y contribuyentes. Es la solución de mayor impacto para pruebas de penetración del planeta. Siendo factible descubrir vulnerabilidades en las defensas, enfocarse en los riesgos más altos, y mejorar los resultados de seguridad.

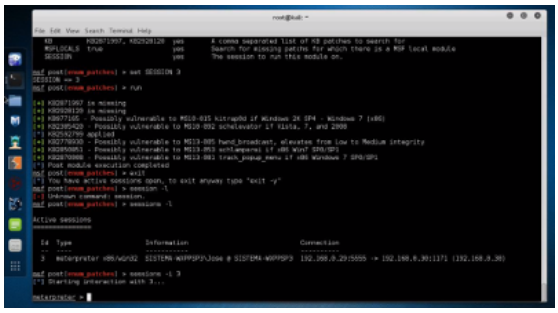
Metasploit permite conocer las debilidades, utiliza la mayor bases de datos de exploits cuyo código ha sido revisado, permite simular ataques del mundo real contra las defensas, y expone credenciales débiles o reutilizadas.

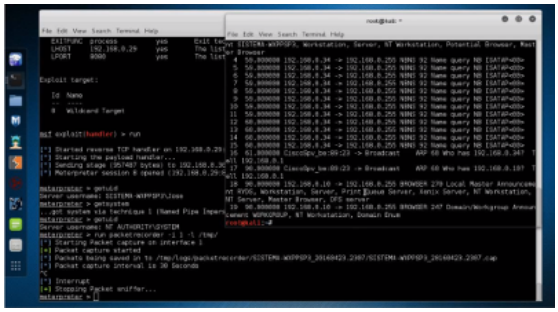
Este curso completamente práctico expone las principales características, funcionalidades y capacidades proporcionadas por Metasploit Framework. De igual manera este curso es una excelente fuente de conocimiento tanto para aquellos recién iniciándose con esta herramienta, como para aquellos profesionales ya utilizándola.

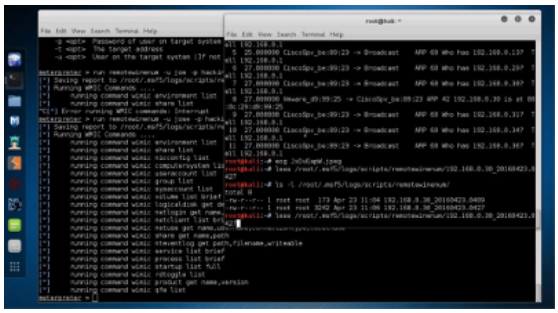
2. Temario:

- Introducción a Metasploit Framework
- Sistemas de Archivos y Librerías
- Módulos y Ubicaciones
- Plugins
- Fundamentos de Metasploit Framework
- Consola de Metasploitt
- Exploits
- Payloads
- Bases de Datos
- 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:

Se sugiere al participante descargar como mínimo las siguientes máquinas virtuales en su sistema para desarrollar el curso.

- **Kali Linux 2018.2**
  Enlace de Descarga (32 Bit)
  https://images.offensive-security.com/virtual-images/kali-linux-2018.2-vm-i386.zip

  Enlace de Descarga (64 Bit)
  https://images.offensive-security.com/virtual-images/kali-linux-2018.2-vm-amd64.zip

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

  Metasploitable 3
  Link de Descarga: https://github.com/rapid7/metasploitable3/

[*] Si el participante lo requiere se le puede enviar 1 DVD con las máquinas virtuales añadiendo S/. 75 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 3 y 10 de Junio del 2018
De 9:00 am a 12:15 pm (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/. 165 Soles o $ 50 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 comprobante escaneado a la siguiente dirección de correo electrónico: **caballero.alonso@gmail.com**.

Otros Países

Para residentes en otros países el pago se realiza mediante una transferencia de dinero utilizando Western Union. Por favor escribir un mensaje de correo electrónico a **caballero.alonso@gmail.com**. para coordinarlos datos para realizar la transferencia.

Confirmado el depósito o transferencia, se enviará al correo electrónico del participante, los datos necesarios para conectarse hacia el sistema y poder participar en el curso.

6. Más Información:

Si desea mayor información sobre el Curso Virtual 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 949304030

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 y Enterprise Cyber Security Fundamentals. 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 es: http://www.ReYDeS.com.