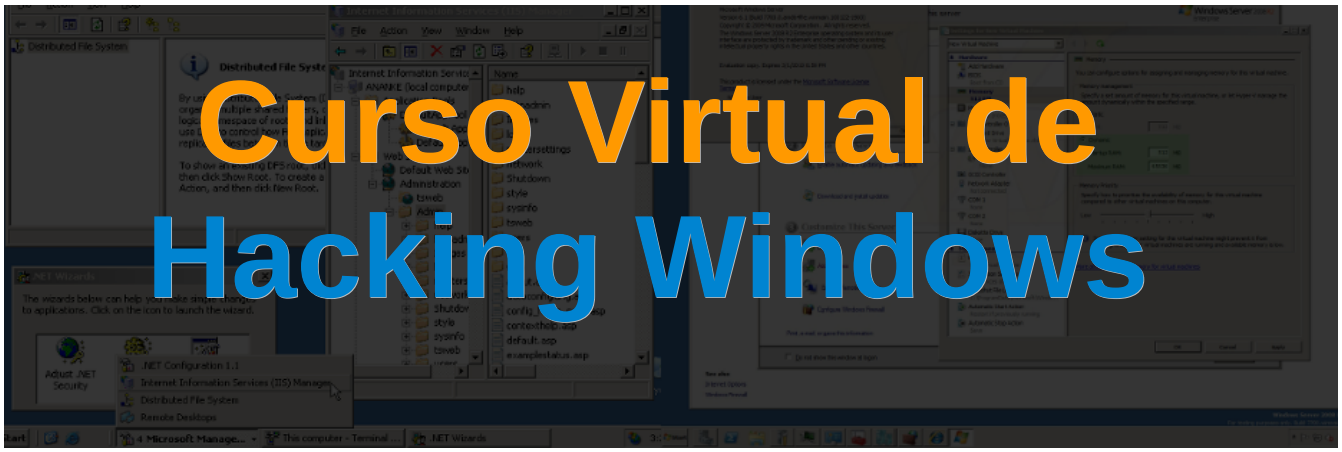


Curso Virtual de Hacking Windows

Único Curso del Año 2018

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

Domingos 6 y 13 de Mayo del 2018

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

1. Presentación:

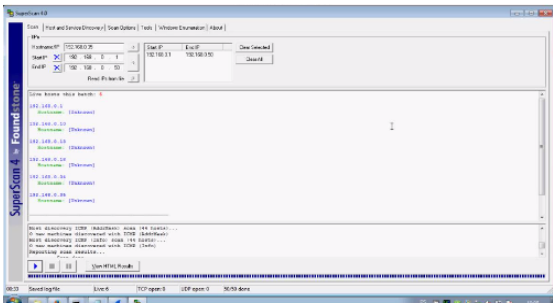
Windows es un sistema operativo gráfico desarrollado y vendido por Microsoft. Existen diversas versiones para computadoras de escritorio, servidores y dispositivos móviles. Actualmente es innegable la amplia utilización. Microsoft controla un amplio mercado de los sistemas operativos, como también software para navegación web, ofimática, multimedia, entre otros.

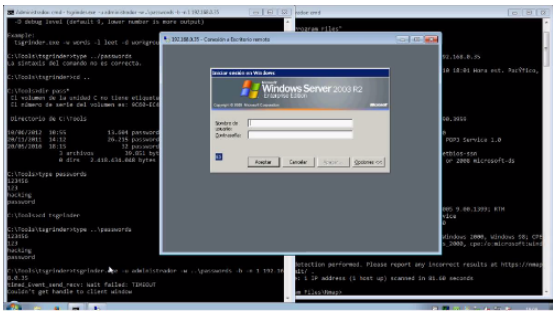
Windows ha ganado adeptos debido principalmente a su entorno visual y facilidad de uso. Desde la perspectiva de la seguridad esto tiene sus beneficios y debilidades. Windows ha sido diseñado para maximizar su facilidad de uso, lo cual frecuentemente afecta la seguridad. Se puede pensar en la seguridad como en algo continuo entre polos extremos, donde el 100% de seguridad es igual a 0% de usabilidad, y de otro lado, 100% de usabilidad es igual a 0% de seguridad. Con el transcurrir de los años Microsoft ha aprendido a encontrar un balance entre estos dos polos. Además dado el hecho de ser unos de los sistemas operativos más utilizados, es también uno de los más atacados.

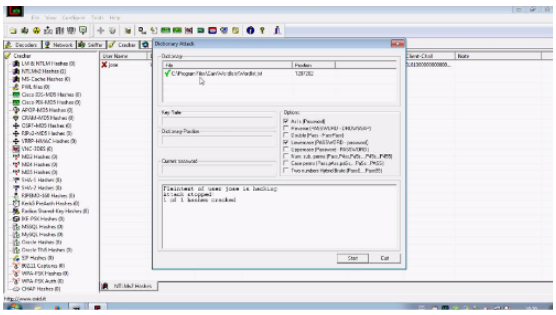
Este curso completamente práctico expone la metodología y herramientas esenciales para realizar una prueba de penetración contra sistemas Microsoft Windows.

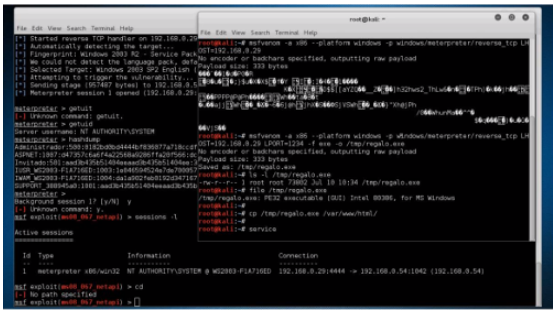
2. Temario:

- Introducción a la Arquitectura de Seguridad de Windows
- Reconocimiento
- Escaneo
- Revisión de los resultados del Escaneo
- Enumeración
- Enumeración de servicios de nombre NetBIOS
- Enumeración RPC
- Enumeración SMB
- Enumeración DNS
- Enumeración SMTP
- Herramientas Automáticas para Enumeración
- Pruebas contra Servicios Específicos de Windows
- Servicios Específicos de Windows
- Adivinar Contraseñas
- Evitar el Bloqueo de Cuentas
- Interceptar la Autenticación en Windows
- Subvertir la Autenticación en Windows
- Explotar Servicios Específicos de Windows
- Descubrir y Explotar Vulnerabilidades en Windows
- Vulnerabilidades de Seguridad
- Encontrar Vulnerabilidades de Seguridad
- Explotar Vulnerabilidades en Windows
- Explotación Posterior
- Transferir Archivos hacia el Sistema Windows
- Elevar Privilegios en un Sistema Windows
- Control Remoto Interactivo
- Extracción de Contraseñas
- Romper Contraseñas
- Romper Hashes LM y NT
- Mantener el Acceso en un Sistema Windows
- Hacking al SQL Server
- Obtener Información de SQL Server
- Herramientas y Técnicas para Atacar SQL Server
- Atacar Aplicaciones Clientes Microsoft
- Explotar Internet Explorer
- Explotar Aplicaciones de Terceros









3. Material:

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

- **Kali Linux 2018.1**
  Enlace de Descarga (32 Bit)
  https://images.offensive-security.com/virtual-images/kali-linux-2018.1-vm-i386.7z

  Enlace de Descarga (64 Bit)
  https://images.offensive-security.com/virtual-images/kali-linux-2018.1-vm-amd64.7z

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

[*] Si el participante lo requiere se le puede enviar 1 DVD con las máquinas virtuales, Kali Linux, y Metasploitable 3 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 6 y 13 de Mayo 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 o MoneyGram. 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 de Hacking Windows, 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, 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.