Curso de hacking con Powershell

Pregúntame por LinkedIn y te doy más información sobre profesores y precios, nosotros no enseñamos lo típico que puedes leer en cualquier sitio… Deja de hacer cursos vacuos, confía en nosotros, vas a aprender cosas interesantes de verdad.

- https://www.linkedin.com/in/jesuspowershell/

El resumen es… **Entender la seguridad**, lo que ya ha ocurrido en la historia (ataques conocidos) e intentar **llevar a cabo técnicas por nosotros mismos que normalmente se realizan mediante programas,** esas técnicas se realizarán **mediante lenguaje de scripting en PowerShell combinado con comandos de Linux y otras tecnologías y lenguajes de programación.**

La idea es **entender conceptos básicos** para empezar a navegar por el mundo de la seguridad, importante **relacionarlo con el riesgo** y cómo se mitiga. Dar mucha importancia a los **procedimientos de seguridad** que habrá que implantar en la empresa o en el lugar que sea, sin procedimientos no hay forma de saber qué hay que hacer. Después se ven ataques conocidos y se intenta explicar qué ocurrió.

La seguridad desde el punto de vista del concepto es genial pero ahora hay que ver cómo se pueden llevar a cabo ataques o realizar desde un ordenador alguna acción, **aunque normalmente se utilizan herramientas para realizar dichas tareas nosotros vamos a intentar crearlas**, por eso toda la parte de PowerShell, es el lenguaje de scripting que junto con **comandos en Linux y .NET** vamos a utilizar para llevar a cabo tareas. Es un lenguaje bastante simple, que además se puede relacionar con otras tecnologías y lenguajes de programación.

Ya estamos en la parte del curso que va a tratar la seguridad de lleno, el recorrido que haremos será el siguiente…

Saber qué hay por la **red**, conceptos que se relacionan con la red, después establecer un **mapa de red**, saber crear **conexiones UDP y TCP** para analizar equipos y extraer información de los mismos de forma masiva, recorriendo todo lo que haya por la red y si puede ser **sin ser detectados**, utilizar técnicas para identificar dispositivos o fallos, por la red hay mucha información olvidada.

Después pasamos a la **criptografía**, que nos introduce en el mundo de los **credenciales** y la **seguridad lógica** para después vulnerar dicha seguridad analizando equipos desde dicho punto de vista. La creación de **malware** junto con los exploits es la forma de **tomar el control** de la máquina que al final se reduce a una conexión UDP o TCP. Aquí estamos hablando de ataques para eso es importante saber qué atacamos en el sistema operativo y qué puede ser vulnerado, por ejemplo mediante **técnicas de inyección**.

Después nos vamos a la **Web** para recorrerla, pasando por los dispositivos **móviles** y sus permisos.

A continuación tratamos **tecnologías físicas** y cómo se consideran fuente de numerosos ataques.

Finalizamos el curso con la parte de **ingeniería social y forense**, es decir acabamos entendiendo cómo se engaña y cómo se analiza cuando ha ocurrido cualquiera de las cosas que hemos visto durante el curso, para explicarnos mejor… Con la ingeniería social empieza todo y acaba con el análisis forense… **Por último** y antes de acabar el resumen, planteamos el tema estrella que es el **DDoS, buscando un DDoS de calidad…**

Con el curso no te certificas en nada, de eso ya hay mucho y dudamos de la eficacia de tanta certificación, con nuestro curso aprendes de verdad, los fundamentos y a poder realizar ataques por ti mismo sin utilizar herramientas. Y por cierto…

Fuera la teoría, viva la práctica real!!!!

¿Comenzamos el curso?

Temario

- Generalidades de la seguridad
- Generalidades de PowerShell
- Network
- Cryptography
- Footprinting
- Logical security
- Scanning and enumeration
- Pentesting
- Attacks
- Malware
- Web
- Mobil Device Security
- Physical Security
- Social Engineering
- Post- Exploitation
- Forensic
- Casos de estudio

⚠ Comenzar el curso (pulsar aquí) ⚠