HE03.- Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros

Orientaciones Alumnado

En esta unidad de trabajo aprenderás los conceptos generales de "Ataque y defensa en entorno de pruebas, de redes y sistemas".

Se desarrollan las técnicas comúnmente utilizadas para realizar un primer análisis del objetivo y obtener los servicios que ofrece el sistema remoto, así como la detección de posibles vulnerabilidades que puedan presentar los sistemas.

Se introducen herramientas estándar en el mercado de uso común para el reconocimiento del objetivo así como su posterior análisis y detección de vulnerabilidades así como el uso básico de estas herramientas.

También se muestra el desarrollo de parte de la fase de explotación en la que se explotan vulnerabilidades existentes en las infraestructuras y sistemas localizadas en la fase anterior.

Continuaremos explicando las técnicas de monitorización, interceptación e inyección de tráfico.

También se mostrarán los conceptos de ingeniería social y Phishing como otro vector de acceso adicional.

Para finalizar, se detalla el proceso de elevación de privilegios y sus técnicas más comunes.

Datos generales de la Unidad de Trabajo

Nombre completo del MP	Hacking Ético	**Siglas MP**	HE
Nº y título de la UT	03.- Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros.		
Índice o tabla de contenidos	1.- Fase de reconocimiento (Footprinting). 1.1.- Tipos de reconocimiento. 1.2.- Reconocimiento pasivo. 1.3.- Reconocimiento activo. 2.- Fase de escaneo (Fingerprinting). 2.1.- Tipos y enfoque de los escaneos. 2.2.- Escaneo de red 2.3.- Escaneo de servicios. 2.4.- Escaneo de vulnerabilidades. 2.5.- Opciones avanzadas de nmap. 2.6.- Herramientas adicionales de búsqueda de vulnerabilidades. 3.- Fase de explotación de vulnerabilidades (Exploitation). 3.1.- Vectores de ataque. 3.2.- Concepto de exploit. 3.3.- Concepto de payload. 3.4.- Herramienta Metasploit. 3.5.- Herramienta msfvenom. 4.- Interceptación, manipulación y monitorización del tráfico. 4.1.- Interceptación de comunicaciones y monitorización del tráfico. 4.2.- Manipulación e inyección de tráfico. 5.- Phishing. 5.1.- Introducción al phishing y sus tipos. 5.2.- Metodología y herramientas. 6.- Elevación de privilegios. 6.1.- Introducción a la elevación de privilegios. 6.2.- Elevación de privilegios en Linux. 6.3.- Elevación de privilegios en Windows. 6.4.- Herramientas de elevación de privilegios.		
Objetivos	**En esta unidad de trabajo deberás adquirir las siguientes habilidades.** ✓ Conocer los distintos tipos de reconocimiento, técnicas y herramientas utilizadas para localizar nuevos activos. ✓ Conocer los distintos tipos de escaneo (red, servicios y vulnerabilidades). herramientas utilizadas y opciones avanzadas de escaneo. ✓ Aprender distintos tipos de vectores de ataque que podemos utilizar en una intrusión. ✓ Conocimientos básicos de las herramientas Metasploit y msfvenom. ✓ Diferenciar los conceptos de exploit y payload así como los distintos tipos de shells. ✓ Aprender los conceptos básicos de la interceptación, manipulación y monitorización de tráfico, técnicas y herramientas. ✓ Aprender los conceptos básicos de las pruebas de Phishing, así como la metodología y herramientas. ✓ Aprender los conceptos básicos de las diferentes técnicas de elevación de privilegios así como las herramientas utilizadas para localizar estos vectores.		
Temporalización (estimación)	**Tiempo necesario para estudiar los contenidos (h)**	28	
	Tiempo necesario para completar la tarea (h)	6	
	Tiempo necesario para completar el examen (h)	2	
	Nº de días que se recomienda dedicar a esta unidad	36	
	La temporalización anterior no deja de ser una estimación media, ya que el tiempo a invertir va a depender mucho de las circunstancias personales de cada cual.		
Consejos y recomendaciones	Es aconsejable entender bien todos los conceptos puesto que en las unidades sucesivas se hará referencia a ellos.		