Tarea online HE04.

Título de la tarea: Una vez dentro.

Curso de Especialización y módulo: Ciberseguridad en Entornos de las Tecnologías de la Información - Hacking Ético.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- **RA4. Consolida y utiliza sistemas comprometidos garantizando accesos futuros.**

Contenidos

1.- Administración de sistemas de manera remota.
    1.1.- Introducción a la administración de sistemas de manera remota.
    1.2.- Meterpreter.
2.- Ataques y auditorías de contraseñas.
    2.1.- Tipos de ataques a contraseñas.
    2.2.- Password guessing.
    2.3.- Password cracking.
    2.4.- Otros ataques a contraseñas.
3.- Pivotaje en la red.
    3.1.- Pivoting con SSH.
    3.2.- Pivoting con meterpreter.
    3.3.- Pivoting con HTTP.
    3.4.- Utilizando el proxy.
4.- Instalación de puertas traseras (Persistencia).
    4.1.- Introducción a la persistencia.
    4.2.- Tipos de persistencia.

1.- Descripción de la tarea.

Caso práctico

Una vez Paloma ha completado el curso, Paloma ha adquirido los conocimientos necesarios para poder realizar tareas propias de la fase de Postexplotación.

Al igual que hizo su compañero Luis, Paloma ha de realizar unas sesiones formativas con la finalidad de compartir estos conceptos con sus compañeros de trabajo. De esta manera, todos podrán tener, al menos, unas nociones básicas de ciertas técnicas de Postexplotación que ha podido aprender Paloma en el curso.

Direct Media (Dominio público)

Paloma cree que el enfoque que dio Luis a las sesiones formativas es el mejor sistema para poder afianzar los conceptos . De modo que configura un laboratorio de pruebas específico para esta temática y resolver de manera práctica algunas de las tareas aprendidas.

¿Qué te pedimos que hagas?

- **Apartado 1: Proceso de cracking de contraseñas**

  Utilizando la herramienta hashcat en vuestra máquina de ataque Kali Linux, y utilizando el diccionario de posibles contraseñas rockyou (disponible en /usr/share/wordlists/), se necesitan crackear los hashes de los siguientes algoritmos:

  Nota: hay que incluir en este fichero la palabra "hashcat". Se puede añadir esta palabra con el comando "echo hashcat >> /usr/share/wordlists/rockyou.txt"

  - **Hash MD5: "8743b52063cd84097a65d1633f5c74f5"**
  - **Hash NTLM: "b4b9b02e6f09a9bd760f388b67351e2b"**
  - **Hash NETNTLMv2:**
    "admin::N46iSNekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c
    7830310000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030"
  - **Hash Kerberos TGS:**
    "$krb5tgs$23$*user$realm$test/spn*$63386d22d359fe42230300d56852c9eb$891ad31d09ab
    89c6b3b8c5e5de6c06a7f49fd559d7a9a3c32576c8fedf705376cea582ab5938f7fc8bc741acf05c5990741b36ef4311fe
    3562a41b70a4ec6ecba849905f2385bb3799d92499909658c7287c49160276bca0006c350b0db4fd387adc27c01e9e9
    ad0c20ed53a7e6356dee2452e35eca2a6a1d1432796fc5c19d068978df74d3d0baf35c77de12456bf1144b6a750d11f55
    805f5a16ece2975246e2d026dce997fba34ac8757312e9e4e6272de35e20d52fb668c5ed"

- **Apartado 2: Instalación del Laboratorio**

  Para los siguientes ejercicios prácticos Paloma va a reutilizar el laboratorio realizado por Luis. Aprovechando el sistema Virtualbox existente con la configuración de la "RedNAT" se va a utilizar la misma máquina de ataque "Kali Linux". Sin embargo, en este caso la máquina de la víctima será un windows 7. Tienes que ayudar a Paloma a montar la máquina vulnerable Windows 7 con las siguientes características:

  - Utilizar VirtualBox con la "RedNAT" (la que ya disponéis de la unidad 3) con el direccionamiento de red 10.0.2.0/24.
  - Tener una máquina de ataque tipo Kali Linux. Podéis descargarla de este enlace . (Aunque también disponemos de ella de la Unidad 3)
  - Tener una máquina víctima Windows 7SP1. Podéis descargar una imagen de Windows7 32bits en el siguiente enlace . y una imágen de Windows7 64bits en el siguiente enlace .
  - Una vez instalado deshabilitar el firewall de Windows para exponer el puerto TCP 445 (Si el equipo estuviera en una red de Directorio Activo este paso no es necesario dado que el puerto ha de estar habilitado para poder formar parte del Directorio activo)

Has de detallar los pasos necesarios para instalar la Máquina Virtual Windows7SP1 y el proceso para deshabilitar el Firewall de Windows7

- **Apartado 3: Explotación de vulnerabilidad y configuración del servidor C2**

  Ayuda a Paloma a realizar la explotación de la máquina remota Windows7SP1 y a configurar el servidor C2:

  - Utilizando la máquina de ataque Kali Linux Explota la vulnerabilidad *EternalBlue (ms17_010)* en el sistema remoto Windows7 SP1. Documéntate previamente sobre esta vulnerabilidad.

  - Levanta un servidor C2 en Metasploit con el módulo multi_handler y ponlo a la escucha en el Puerto TCP 443 de la interfaz de red de tu máquina Linux de ataque.

- **Apartado 4: Ejecución de la persistencia.**

  Una vez está todo listo ayuda a Paloma a ejecutar las tareas de Persistencia.

  - Realizar la **persistencia en servicio** utilizando los módulos de Metasploit que se trabajaron en la unidad.
  - Realizar la **persistencia en registro** utilizando los módulos de Metasploit que se trabajaron en la unidad.

NOTA IMPORTANTE

Para los apartados en los que se solicita realizar una captura de pantalla hay que tener en cuenta que las capturas realizadas deben tener como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil. Aquellos apartados/subapartados que no cumplan esta condición no serán corregidos.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recursos necesarios

- Ordenador personal con, al menos, 4 Gigabytes de memoria RAM.
- Conexión a Internet para consultar ejemplos de la Unidad 4.
- Sistemas Operativos preferidos Kali Linux, Parrot Linux.
- Sistema Operativo de la víctima Windows7.
- Navegador web.
- Software para comprimir los archivos de la tarea.

Recomendaciones

- Antes de abordar la tarea:
  - Lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
  - Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- No olvides elaborar el documento explicativo.

Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_HE04_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la cuarta unidad del MP de HE**, debería nombrar esta tarea como...

sanchez_manas_begona_HE04_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación RA4

- a) Se han administrado sistemas remotos a través de herramientas de línea de comandos.
- b) Se han comprometido contraseñas a través de ataques de diccionario, tablas rainbow y fuerza bruta contra sus versiones encriptadas.
- c) Se ha accedido a sistemas adicionales a través de sistemas comprometidos.
- d) Se han instalado puertas traseras para garantizar accesos futuros a los sistemas comprometidos.

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Realiza correctamente el proceso de cracking del hash NTLM	1 punto
Apartado 1: Realiza correctamente el proceso de cracking del hash NETNTLMv2	1 punto
Apartado 1: Realiza correctamente el proceso de cracking del hash MD5	1 punto
Apartado 1: Realiza correctamente el proceso de cracking del TGS de Kerberos	1 punto
Apartado 2: Realiza y detalla correctamente el proceso de instalación de la Máquina Virtual Windows7.	1 punto
Apartado 2: Realiza y detalla correctamente la configuración del firewall de windows para permitir el puerto TCP 445 en una red sin dominio de Directorio Activo.	1 punto
Apartado 3: Realiza y detalla correctamente el proceso de explotación de la máquina Windows 7 mediante el exploit EternalBlue	1 punto
Apartado 3: Realiza y detalla correctamente el proceso de iniciar el	1 punto

Multihandler de Metasploit.	
Apartado 4: Realiza y detalla correctamente el proceso de persistencia en servicio.	1 punto
Apartado 4: Realiza y detalla correctamente el proceso de persistencia en registro.	1 punto
Redacción clara y correcta, sin errores ortográficos	**Se resta 0,1 puntos por cada error ortográfico o expresiones incorrectas.**

NOTA IMPORTANTE

Aquellos apartados/subapartados en los que las capturas de pantalla no sean claras o no tengan como fondo de pantalla la plataforma con tu usuario mostrando claramente la foto de tu perfil, no serán corregidos.