Examen para HE04.

Intento 1.

Pregunta 1

Las técnicas de Password Cracking pueden provocar bloqueos de cuentas de usuario, ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 2

Indica cuáles de las afirmaciones son correctas a la hora de configurar el multihandler de Metasploit como C2. (Respuesta múltiple):

a. Es necesario iniciar el multihandler como un job de metasploit e indicar que no se detenga tras la primera comunicación con la shell.
b. El Multihandler ha de tener la misma configuración que la shell remota (IP del C2, Puerto y Payload).
c. El Multihandler ha de tener la misma configuración que la shell remota en cuanto a IP del C2 y Puerto, pero puede utilizar un Payload distinto al que utilice la shell remota.
d. Es necesario iniciar el multihandler como un job de metasploit de esta manera puede establecer comunicación con distintas shells remotas a la vez.

Pregunta 3

Las tareas de pivoting son propias de la fase de explotación. ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 4

Indica que es lo que hace la técnica del Pivoting SSH:

a. Inicia un proxy Remoto en el equipo del atacante y tuneliza las comunicaciones por SSH a la víctima.
b. Inicia un proxy Remoto en el equipo de la víctima y tuneliza las comunicaciones por SSH al atacante.
c. Inicia un proxy Local en el equipo de la víctima y tuneliza las comunicaciones por SSH al atacante.
d. Inicia un proxy Local en el equipo del atacante y tuneliza las comunicaciones por SSH a la víctima.

Pregunta 5

¿Qué requisito es indispensable para que meterpreter pueda volcar los hashes de las contraseñas de un usuario local en Microsoft Windows?:
a. Necesitas que meterpreter esté inyectado en el proceso del explorer.exe.
b. Necesitas que el equipo víctima confíe en la máquina del atacante.
c. Necesitas que meterpreter esté cargado en memoria.
d. Necesitas disponer de privilegios elevados.

Pregunta 6

Las contraseñas por defecto de muchos dispositivos pueden encontrarse en los propios manuales del producto, ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 7

Para poder ejecutar la persistencia necesitamos un servidor de tipo C2 ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 8

Indica cuál de los siguientes requerimientos es necesario para poder realizar la técnica del pivoting HTTP:

a. Hay que utilizar HTTP.
b. Hay que subir un agente a una aplicativo web comprometido.
c. Hay que utilizar un certificado firmado por un agente de confianza.
d. Hay que utilizar el protocolo HTTPS.

Pregunta 9

En las técnicas de Password Guessing hay que utilizar un diccionario que no sea muy extenso. ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 10

Las técnicas de Password Guessing pueden provocar bloqueos de cuentas de usuario, ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Intento 2.

Pregunta 1

Es posible inyectar meterpreter enteramente en la memoria del equipo víctima ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 2

Indica cuál es la afirmación correcta que describe los módulos de tipo "Auxiliary" en Metasploit:

a. Módulos de apoyo que nos proporcionan herramientas propias de la Fase de Enumeración y Escaneo así como otras herramientas para realizar ataques de fuerza bruta.
b. Módulos que realizan la explotación de vulnerabilidades.
c. Módulos que nos ayudan en las actividades posteriores a la explotación de un sistema.
d. Módulos cuyo objetivo es modificar el código del payload con la intención de ofuscarlo y evadir elementos de seguridad como Antivirus o IDS.

Pregunta 3

Uno de los requerimientos de las técnicas de pivoting es que necesitamos disponer de privilegios elevados en la máquina que realizará el pivot. ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 4

¿Cuáles de las siguientes no es una características propia de meterpreter?:

a. Permite la carga dinámica de módulos.
b. Permite utilizar la máquina víctima como pivoting.
c. Permite cifrar el disco de la víctima (Simulación de ransomware).
d. Permite Elevar privilegios.

Pregunta 5

Indica cuales de los siguientes son tipos de persistencia comunes (Respuesta múltiple):

a. Persistencia en registro.
b. Persistencia en servico.
c. Persistencia en Tareas programadas.
d. Persistencia en CRON.

Pregunta 6

¿Cuáles de los siguientes problemas se solucionan estableciendo una persistencia? (Respuesta múltiple):

a. Perdida de shell por apagado del equipo.
b. Perdida de shell por caída del servicio o proceso.
c. Perdida de shell debido a los mecanismos de defensa.
d. Perdida de shell por falta de privilegios en el sistema remoto.

Pregunta 7

Indica cuales de los siguientes son técnicas específicas de pivoting. (Respuesta múltiple):

a. Pivoting por SSH.
b. Pivoting utilizando meterpreter.
c. Pivoting por HTTP.
d. Pivoting utilizando SMTP.

Pregunta 8

Meterpreter permite realizar volcado de los hashes del sistema ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 9

Indica de qué manera puedes utilizar un servidor proxy (Respuesta múltiple):

a. Utilizando clientes específicos para proxy como proxychains.
b. Utilizando el navegador Web indicando que nos conectaremos a través de un proxy.
c. configurando el proxy como la puerta de enlace por defecto.
d. Utilizando una cadena de certificados.

Pregunta 10

Una vez que se establece el pivoting con meterpreter se puede utilizar el pivoting desde cualquier herramienta fuera de Metasploit sin realizar ninguna tarea adicional. ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Intento 3.

Pregunta 1

En términos de Postexplotación ¿Qué es lo que conocemos como persistencia?:

a. A la capacidad de poder utilizar varios vectores sobre un mismo objetivo.
b. A la capacidad de obtener un acceso más privilegiado en el sistema.
c. A la capacidad de mantener el acceso en un equipo comprometido.
d. A la capacidad de obtener nuevas credenciales en el sistema.

Pregunta 2

Indica cuál de las siguientes afirmaciones es cierta para la herramienta hashcat:

a. Utiliza rainbow tables.
b. Hascat siempre tarda el mismo tiempo en averiguar una contraseña.
c. Hashcat tiene que utilizar algoritmos de hashing para generar el hash de posibles contraseñas.
d. Dispone funciones matemáticas que permiten revertir un hash a su contraseña original.

Pregunta 3

Si utilizamos la técnica del pivoting con meterpreter, para poder utilizar el pivot con herramientas fuera de Metasploit habrá que iniciar un proxy en el propio Metasploit. ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 4

Indica cuáles son los motivos por los que utilizar un servidor C2 en la fase de persistencia:

a. Permiten elevar privilegios más fácilmente.
b. Permiten poder establecer una comunicación con las shells remotas.
c. Permiten manejar varias shells a la vez.
d. Permiten tener un punto de fallo.

Pregunta 5

¿En qué Sistemas operativos puede utilizarse el payload meterpreter? (Respuesta múltiple):

a. Linux.
b. Android.
c. Microsoft Windows.
d. iOS.

Pregunta 6

¿Cuál de las siguientes herramientas se puede utilizar para realizar técnicas de password Guessing?:

a. JohnTheRipper.
b. hashcat.
c. Patator.
d. CeWL.

Pregunta 7

Para poder utilizar técnicas de pivoting necesitamos tener previamente el control de una máquina víctima. ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 8

¿Qué es una rainbow table?:

a. Es un listado que únicamente contiene hashes.
b. Listados de credenciales tipo usuario:contraseñas.
c. Listados de correos electrónicos y contraseñas obtenidos de "leaks".
d. Listados en los que se proporciona posibles contraseñas en claro junto con su hash (hash:contraseña) en algoritmos específicos.

Pregunta 9

Indica cuáles de de los siguientes requisitos son necesarios para poder realizar un ataque de Password guessing:

a. Disponer de un listado de nombres de usuario.
b. Utilizar aplicaciones de hashing.
c. Disponer de un listado de posibles contraseñas.
d. Utilizar aplicaciones de fuerza bruta.

Pregunta 10

Indica cuales de las siguientes técnicas se utilizan para realizar ataques contra las contraseñas:

a. Rainbow Tables.

b. Proceso de cracking de contraseñas.

c. Ataques de fuerza bruta en la autenticación de una aplicación o servicio.

d. Contraseñas por defecto.