HE04 - Test
Su calificación final en este cuestionario es 10,00/10,00.
Promedio clasificación intento 1: 10,00/10,00

1- Para poder ejecutar la persistencia necesitamos un servidor de tipo C2 ¿Verdadero o Falso?:
- **a) Verdadero**

2- Las técnicas de Password Guessing pueden provocar bloqueos de cuentas de usuario, ¿Verdadero o Falso?:
- **a) Verdadero**

3- Para poder utilizar técnicas de pivoting necesitamos tener previamente el control de una máquina víctima, ¿Verdadero o Falso?
- **a) Verdadero**

4- Las contraseñas por defecto de muchos dispositivos pueden encontrarse en los propios manuales del producto, ¿Verdadero o Falso?:
- **a) Verdadero**

5- Es posible inyectar meterpreter enteramente en la memoria del equipo víctima ¿Verdadero o Falso?:
- **a) Verdadero**

6- ¿Cuál de las siguientes herramientas se puede utilizar para realizar técnicas de password Guessing?:
- **a) Patator.**
- b) hashcat.
- c) JohnTheRipper.
- d) CeWL.

7- ¿En qué Sistemas operativos puede utilizarse el payload meterpreter? (Respuesta múltiple):
- **a) Microsoft Windows.**
- **b) Android.**
- c) Linux.
- d) iOS.

8- ¿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 cargado en memoria.
- b) Necesitas que meterpreter esté inyectado en el proceso del explorer.exe.
- **c) Necesitas disponer de privilegios elevados.**
- d) Necesitas que el equipo víctima confíe en la máquina del atacante.

9- Las técnicas de Password Cracking pueden provocar bloqueos de cuentas de usuario, ¿Verdadero o Falso?:
- **b) Falso**

10- Indica que es lo que hace la técnica del Pivoting SSH:
- **a) Inicia un proxy Local en el equipo del atacante y tuneliza las comunicacionse por SSH a la víctima.**
- b) Inicia un proxy Remoto en el equipo del atacante y tuneliza las comunicacionse por SSH a la víctima.
- c) Inicia un proxy Remoto en el equipo de la víctima y tuneliza las comunicacionse por SSH al atacante.
- d) Inicia un proxy Local en el equipo de la víctima y tuneliza las comunicacionse por SSH al atacante.

Promedio clasificación intento 2: 10,00/10,00

1- Meterpreter permite realizar volcado de los hases del sistema ¿Verdadero o Falso?:

a) Verdadero

2- Indica cuáles de de los siguientes requisitos son necearios para poder realizar un ataque de Password guessing (Respuesta múltiple):

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

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

a) Verdadero

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

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

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

b) Falso

6- ¿Qué es una rainbow table?:

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

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

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

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

a) Módulos que realizan la explotación de vulnerabilidades.
b) Módulos que nos ayudan en las actividades posteriores a la explotación de un sistema.
c) 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.
d) Módulos cuyo objetivo es modificar el código del payload con la intención de ofuscarlo y evadir elementos de seguridad como Antivirus o IDS.

9- 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?:

b) Falso

10- 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?:

a) Verdadero