Promedio de calificaciones: 9,50 / 10,00

Pregunta 1

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

La herramienta nmap se puede utilizar en la fase de escaneo de vulnerabilidades, ¿Verdadero o Falso?:

Seleccione una:

- (●) Verdadero
- ( ) Falso

Siguiente página

Pregunta 2

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

¿Cuáles de las siguientes técnicas o herramientas NO se utilizan durante un escaneo pasivo?:

- ( ) a. Email harvesting.
- ( ) b. Recopilación de información en buscadores.
- ( ) c. Recopilación de infoormación en redes sociales.
- (●) d. Enumeración DNS.

Quitar mi elección

Página anterior

Siguiente página

Pregunta 3

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Indica cuáles de las siguientes herramientas se utilizan para detectar vectores de elevación de privilegios en sistemas Linux. (Respuesta múltiple):

- [ ] a. PrivescCheck.
- [x] b. LinPEAS.
- [ ] c. Watson.
- [x] d. Linenum.

Página anterior

Siguiente página

Pregunta **4**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

En un reconocimiento activo se utilizan fuentes de terceros para obtener información del objetivo ¿Verdadero o Falso?:

Seleccione una:

- Verdadero
- Falso

Página anterior

Siguiente página

Pregunta **5**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Una shellcode de tipo Bind es adecuada para conseguir una shell remota en un equipo que se encuentra tras un firewall, ¿Verdadero o Falso?:

Seleccione una:

- Verdadero
- Falso

Página anterior

Siguiente página

Pregunta **6**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

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

- a. Módulos que nos ayudan en las actividades posteriores a la explotación de un sistema.
- b. Módulos que realizan la explotación de vulnerabilidades.
- 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.

Quitar mi elección

Página anterior

Siguiente página

Pregunta 7

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

La enumeración SMTP nos permite verificar si una dererminada cuenta de correo es válida ¿Verdadero o Falso?:

Seleccione una:

- (•) Verdadero
- ( ) Falso

Página anterior

Siguiente página

Pregunta 8

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

La herramienta nmap soporta varios tipos de escaneo TCP distintos para tratar de evadir los sitemas firewalls. ¿Verdadero o Falso?:

Seleccione una:

- (•) Verdadero
- ( ) Falso

Página anterior

Siguiente página

Pregunta 9

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Indica cuáles de las siguientes acciones son acciones englobadas en la metodología de phishing (Respuesta múltiple):

- [x] a. Recopilar datos del objetivo.
- [x] b. Establecer el tipo de phishing.
- [x] c. Generar la campaña.
- [x] d. Comprar dominios necesarios.

Página anterior

Siguiente página

Pregunta **10**

Sin responder aún

Se puntúa como 0 sobre 1,00

Marcar pregunta

Indica cuáles de los siguientes vectores nos permite elevar los privilegios en un sistema Windows. (Respuesta múltiple):

- [x] a. Unquoted paths.
- [ ] b. Configuración incorrecta de sudo.
- [x] c. dllHijacking.
- [ ] d. Binarios con SUID.

Página anterior

Terminar intento...