Examen para HE03.

Intento 1.

Pregunta 1

¿Cuál de las siguientes herramientas se pueden utilizar en un escaneo de red?:

a. arp-scan.
b. GVM.
c. Maltego.
d. Nessus.

Pregunta 2

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

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

Pregunta 3

Indica el tipo de shellcode que utilizarías para establecer una shell en un sistema expuesto en internet de una compañía objetivo de la auditoría:

a. Shellcode local tipo bind.
b. Shellcode local tipo reverse.
c. Shellcode remota tipo bind.
d. Shellcode remota tipo reverse.

Pregunta 4

En cuáles de los siguientes recursos y herramientas se pueden encontrar exploits públicos. (Respuesta múltiple):

a. searchexploit.
b. Github.
c. Metasploit.
d. exploit-db.

Pregunta 5

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

Verdadero
Falso

Pregunta 6

Uno de los requerimientos de la técnica ARP Spoofing, es que el atacante y la víctima han de estar en el mismo dominio de colisión broadcast. ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 7

¿En cuál de los siguientes portales NO podemos buscar vulnerabilidades?:

a. Shodan.
b. vulners.
c. Common vulnerabilities and Exposures (CVE).
d. exploit-db.

Pregunta 8

Indica cuál de los siguientes comandos nos permite ver las opciones de configuración que tiene un determinado módulo en Metasploit:
a. show.
b. set.
c. info.
d. search.

Pregunta 9

Un escaneo de red permite localizar vulnerabilidades basadas en el software y versión utilizadas en un determinado servicio, ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 10

Indica cuáles de las siguientes herramientas se utilizan para detectar vectores de elevación de privilegios en sistemas Linux. (Respuesta múltiple):
a. LinPEAS.
b. Watson.
c. Linenum.
d. PrivescCheck.

Intento 2.

Pregunta 1

La herramienta msfvenom dispone de los mismos exploits disponibles en la herramienta Metasploit, ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 2

Los payloads de tipo Staged se transmite en varias partes con la finalidad de evitar posibles bloqueos que pudieran realizarse debido a los dispositivos de seguridad existentes en la red. ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 3

¿Qué es un payload?:

a. Es el código o set de instrucciones que se ejecutan una vez explotada la vulnerabilidad.
b. Es el código encargado de comprobar si una determinada vulnerabilidad existe en el sistema.
c. Es el código encargado de explotar la vulnerabilidad.
d. Es la parte de código de nmap que se encarga de comprobar si un determinado está abierto o cerrrado.

Pregunta 4

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

Verdadero
Falso

Pregunta 5

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 cuyo objetivo es modificar el código del payload con la intención de ofuscarlo y evadir elementos de seguridad como Antivirus o IDS.
d. 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.

Pregunta 6

Los tipos de exploits pueden clasificarse en Remotos o Locales, ¿Verdadero o Falso?:
Seleccione una:

Verdadero
Falso

Pregunta 7

Indica cuáles de los siguientes vectores nos permite elevar los privilegios en un sistema Linux. (Respuesta múltiple):
a. Modificación de claves del registro.
b. Escritura de cron.
c. Binarios con ZUID.
d. Binarios con SUID.

Pregunta 8

Indica cuáles de las siguientes herramientas se utilizan para realizar un escaneo en frameworks específicos (Respuesta múltiple):

a. nc.
b. CMSMap.
c. Wpscan.
d. JoomScan.

Pregunta 9

La correcta ejecución de las técnicas de elevación de privilegios nos otorga un primer acceso al sistema remoto ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 10

Indica cuáles de las siguientes técnicas se pueden utilizar para realizar una interceptación de las comunicaciones (Respuesta múltiple):

a. SNMP Spoofing.
b. ARP Spoofing.
c. ICMP Spoofing.
d. Punto de Acceso falso.

Intento 3.

Pregunta 1

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

Seleccione una:

Verdadero
Falso

Pregunta 2

¿Qué tipos de reconocimiento conoces? (Respuesta múltiple):

a. Reconocimiento de vulnerabilidades.
b. Reconocimiento híbrido.
c. Reconocimiento pasivo.
d. Reconocimiento activo.

Pregunta 3

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

Verdadero
Falso

Pregunta 4

En la Fase de reconocimiento se pueden ejecutar técnicas de escaneo de vulnerabilidades ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso

Pregunta 5

¿Qué es un Escaneo de servicios?:

a. Un escaneo que tiene como objetivo identificar los servicios que se ofrecen en la red escaneada.
b. Un escaneo destinado a obtener mayor información sobre la red objetivo, direccionamiento IP y la arquitectura utilizada para sustentar toda la infraestructura objetivo.
c. En este tipo de escaneo se obtienen posibles usuarios en el sistema remoto.
d. En este tipo de escaneo se comprueba si existe algún tipo de vulnerabilidad en base al tipo de servicio y la versión del mismo.

Pregunta 6

¿Cuáles de los siguientes son vectores de acceso válidos en la fase de explotación? (Respuesta múltiple):

a. Ejecución remota de comandos.
b. Ejecución de un programa malintencionado (Malware).
c. Explotación de una vulnerabilidad conocida.
d. Contraseñas por defecto o poco robustas.

Pregunta 7

Indica cuál es el tipo de phishing en el que el intento de engaño se realiza a través de SMS:

a. Vishing.
b. Whaling.
c. Smishing.
d. Pharming.

Pregunta 8

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

a. Enumeración DNS.
b. Email harvesting.
c. Recopilación de información en redes sociales.
d. Recopilación de información en buscadores.

Pregunta 9

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

a. Binarios con SUID.
b. dllHijacking.
c. Configuración incorrecta de sudo.
d. Unquoted paths.

Pregunta 10

Un escaneo de red permite localizar vulnerabilidades basadas en el software y versión utilizadas en un determinado servicio, ¿Verdadero o Falso?:

Seleccione una:

Verdadero
Falso