Examen Tema 3 y 4

Created	@11 de diciembre de 2024 9:33
Tags	

Preguntas Autoevaluación Teoría

Tema 3: Hacking Ético

Tipo de metodología en la que el atacante dispone de muchos tipos de información, incluso credenciales de acceso, del sistema objetivo.

Prueba de caja blanca

Tipo de hacker que trabaja como empleado o consultor en una organización con acceso a sus sistemas, al que causa daños con el fin de provocar pérdidas, vengarse por haber sido despedido u obtener información confidencial o estratégica.

Insider

Tipo de footprinting en el que se tiene interacción directa con la víctima o el objetivo.

Reconocimiento activo

Experto en atacar sistemas con propósito malicioso o beneficio personal. Quiere causar daño al sistema mediante borrado de ficheros, robo de información, modificación de sitios web...

Black hat

Conjunto de pruebas de intrusión llevadas a cabo por profesionales de seguridad con una metodología rigurosa.

Hacking Ético

Tipo de metodología en la que el atacante parte de alguna información del sistema objetivo.

Caja gris

Framework que proporciona un conjunto de herramientas con las que el auditor pueda desarrollar, ejecutar y lanzar exploits contra máquinas para comprobar si son seguras.

Metasploit

Fallo o una debilidad en los procedimientos, diseño, implementación o controles internos de seguridad del sistema, que puede ser activado intencionada o desintencionadamente y resultar en una brecha de seguridad o la violación de la política de seguridad del sistema.

Vulnerabilidad

Software dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones.

Rootkit

Pequeña aplicación implementada para aprovecharse de una vulnerabilidad conocida en un software.

Exploit

Informe verificado por auditores de ISECOM incluido en el manual OSSTMM que recapitula todas las evidencias encontradas durante las pruebas realizadas.

STAR

Atacante con gran conocimiento en telecomunicaciones que consigue acceder a sistemas o centrales telefónicos.

Phreaker

Metodología de hacking ético que se estructura en 7 secciones principales: interacciones previas al compromiso, recopilación de inteligencia, modelado de amenazas, análisis de vulnerabilidades, explotación, post-explotación e informes.

PTES

Primera fase del pentesting, consiste en descubrir toda la información relevante de la organización víctima o cliente.

Footprinting

Experto en seguridad informática que está especializado en realizar pruebas de intrusión para garantizar la seguridad de la información de los sistemas de una organización, a la que suele comunicar las brechas de seguridad.

Hacker Ético

Software encargado de capturar la información que recibe el equipo a través del teclado y ratón.

Keylogger

Base de conocimiento de técnicas adversas, que permite gestionar comportamientos adversos, modelos de ciclo de vida, aplicación a entornos reales y taxonomía común.

MITRE ATT&CK

Punto de acceso a un sistema que evita tener que volver a explotar una vulnerabilidad del mismo.

Backdoor

Base de datos de vulnerabilidades públicamente conocidas creada por el MITRE de libre acceso internacional.

CVE

Atacante inexperto capaz de ejecutar un script/aplicación desarrollado por un tercero para llevar a cabo un ataque. Carece de un buen nivel de programación o de las aplicaciones usadas, así que es fácil de rastrear al dejar una huella clara.

Script Kiddie

Framework para automatizar ataques de ingeniería social, como vectores de ataques web, generación de payloads para dispositivos USB, ataques de mailing masivo o phishing.

SET

Fase del pentesting en la que se identifican hosts activos, se buscan puertos abiertos y se obtiene información del sistema operativo, aplicaciones, servicios...

Fingerprinting

Tipo de metodología en la que el atacante no dispone de ningún tipo de información del sistema objetivo, por lo que la tarea más importante es la búsqueda de información.

Caja negra

Metodología de hacking ético que se estructura en 15 capítulos sobre conceptos básicos de seguridad, procesos para definir una prueba, aspectos legales, métricas, entre otros. Algunas pruebas son de seguridad física, inalámbrica, cumplimiento normativo... entre otras.

OSSTMM

Tipo de hacker que a veces respeta las leyes y otras veces actúa ilegalmente, con objetivos personales, con ánimo de lucro o protesta. Suele alertar de las vulnerabilidades encontradas a la comunidad hacker.

Grey hat

Base de datos de vulnerabilidades públicamente conocidas creada por el NIST de libre acceso internacional.

NVD

Parte del código de un exploit cuya finalidad es ejecutarse en la máquina víctima para llevar a cabo una acción, normalmente maliciosa.

Payload

Tipo de footprinting en el que no se tiene interacción directa con la víctima o el cliente.

Reconocimiento pasivo

Fundación sin ánimo de lucro que publica un top ten con las 10 vulnerabilidades más importantes, y herramientas y consejos para subsanarlos.

OWASP

Atacar diferentes entornos o sistemas con el objetivo de detectar y prevenir posibles fallos.

Pentesting

Tema 4: Notificación y Gestión de Ciberincidentes

Proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de un diccionario previamente generado con determinadas combinaciones de caracteres, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

Ataque por diccionario

Nombre que se emplea para designar a un conjunto de máquinas controladas remotamente con finalidad generalmente maliciosa.

Botnet

Paneles de mando y control, por los cuales atacantes cibernéticos controlan determinados equipos zombie infectados con muestras de la misma familia de software dañino.

Command & Control

Cualquier acción tipificada como delito de acuerdo a lo establecido en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Delito

Análisis local o remoto mediante software, del estado de los puertos de una máquina conectada a una red con la finalidad de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

Escaneo de puertos

Comunicaciones no esperadas o deseadas, así como acciones o expresiones que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

Mensajes ofensivos

Programa malicioso que tiene como característica principal su alto grado de dispersabilidad. Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P, etc.

Gusano

Todo intercambio de información a nivel de red local o pública, cuyo origen o destino no esté plenamente identificado, así como la legitimidad de los mismos.

Conexión sospechosa

Técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.

Ingeniería social

Ataques implementados con el objetivo de provocar la interrupción o degradación de la prestación de un servicio, provocando daños relevantes en la continuidad del servicio de una institución o daños reputacionales relevantes cometidos con propósitos ideológicos, políticos o religiosos.

Sabotaje

Conjunto de software dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones.

Rootkit

Exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor.

Apología del la violencia

Palabra que deriva de los términos malicious y software. Se trata de cualquier pieza de software que lleve a cabo acciones maliciosas.

Malware

Análisis mediante software del tráfico de una red con la finalidad de capturar información. El tráfico que viaje no cifrado podrá ser capturado y leído por un atacante.

Análisis de paquetes

Pieza de software maliciosa que recibe órdenes de un atacante principal que controla remotamente la máquina.

Bot dañino

Malware que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados o cifrados.

Ransomware

Ataque informático que aprovecha vulnerabilidades de los servidores DNS (Domain Name System). Al tratar de acceder el usuario al sitio web, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web maliciosa que suplanta la auténtica, y en la que el atacante podrá obtener información sensible de los usuarios.

Pharming

Tipo de explotación, consistente en la introducción de cadenas mal formadas de SQL, o cadenas que el receptor no espera o controla debidamente; las cuales provocan resultados no esperados en la aplicación o programa objetivo, y por la cual el atacante produce efectos inesperados y para los que no está autorizado en el sistema objetivo.

Inyección SQL

Cualquier infracción penal, incluyendo infracciones contra las personas o las propiedades, donde la víctima, el local o el objetivo de la infracción se elija por su real o percibida, conexión, simpatía, filiación, apoyo o pertenencia a un grupo social, raza, religión o condición sexual.

Racismo

Correo electrónico no solicitado que se envía a un gran número de usuarios, o bien una alta tasa de correos electrónicos enviados

a un mismo usuario en un corto espacio de tiempo.

Spam

Tipo de malware que se enmascara como software legítimo con la finalidad de convencer a la víctima para que instale la pieza en su sistema. No depende de una acción humana y no tiene la capacidad de replicarse.

Troyano

Vulnerabilidad que permite a un atacante mostrar o ejecutar archivos remotos alojados en otros servidores a causa de una mala programación de la página que contiene funciones de inclusión de archivos.

Local File Inclusion o Inclusión de Ficheros

Tipo de malware cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso o consentimiento del usuario. Se propaga mediante la ejecución en el sistema de software, archivos o documentos con carga dañina.

Virus

Protocolo de red utilizado para el intercambio de mensajes para la administración de dispositivos en red.

SNMP o Simple Network Management Protocol

Obligar a una persona o mercantil, mediante el empleo de violencia o intimidación, a realizar u omitir actos con la intención de

Extorsión

Tipo de malware que espía las actividades de un usuario sin su conocimiento o consentimiento. Estas actividades pueden incluir keyloggers, monitorizaciones, recolección de datos así como robo de datos.

Spyware

Amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

Ciberamenaza

Preguntas Autoevaluación Prácticas

Práctica 3: Recolección de información en fuentes abiertas I y II

Operador que permite suprimir elementos de la búsqueda.

-

Operador que permite hacer una búsqueda de más de un término.

|

Operador que permite filtrar la búsqueda a un solo dominio web.

site:dominio_web

Operador que permite filtrar la búsqueda para que solo muestre ficheros de una extensión determinada.

filetype:extension

Operador que busca un término dentro del contenido del título de una web. Puede combinarse con otros.

Intitle:texto

Operador que busca páginas web que enlacen hacia el dominio indicado.

Link:dominio

Operador que busca un término dentro de una URL. Puede combinarse con otros.

`inurl:texto`

Operador que busca artículos o noticias escritos por el autor indicado.

`Author:texto`

Operador que busca todo el texto especificado dentro del título de las web. No se puede usar junto a otros.

`Allintitle:texto`

Operador que permite acceder a la caché del dominio que se indique.

`Cache:dominio`

Operador que busca páginas web similares al dominio proporcionado.

`Related:dominio`

Operador utilizado para que la búsqueda filtre por ficheros del tipo Hoja de excel.

`filetype:xls`

Operador para eliminar de la búsqueda los resultados con la palabra seguridad.

`-seguridad`

Buscador adecuado para encontrar servidores web.

`Shodan`

Base de datos que contiene una recopilación de Google Dorks con diferentes propósitos.

`Google_Hacking_Database`

Información que podemos encontrar con los Google Dork que nos permite saber si una web tiene fallos de seguridad.

Mensaje_de_error

Categoría de Google Dork que nos permite encontrar servidores con backdoors y otras vulnerabilidades.

Escaneo_de_servidores_vulnerables

Operador para buscar todo el término Asignatura SSI en el título de una web y sin usar comillas dobles.

Allintext:Asignatura_SSI

DNS_dumpster: Repositorio mundial con información sobre DNS a nivel histórico.

Falso

DNS_Trails: Herramienta web sobre DNS que permite generar un mapa visual de los subdominios hallados.

Falsa

DNS: Tipo de registro que usan las empresas para mantener sus aplicaciones bajo un mismo dominio.

Verdadera

Whois_Here: Herramienta de DomainTools para obtener información más detallada sobre el dominio que estamos investigando.

Falsa

Tecnologias_Web: Elemento sobre el que podemos indagar, además de las DNS, durante la fase de reconocimiento.

Verdadera

Wappalyzer: Herramienta que recopila de forma anónima información sobre las tecnologías web.

Verdadera

Extensión: alternativa del navegador para hacer uso de Wappalyzer.

Verdadera

Namecheck: Herramienta para ver si una determinada persona está dada de baja en una red social.

Falsa

Phonebook: Herramienta para listar subdominios o correos electrónicos, dado un dominio determinado.

Verdadera

Práctica 4: Escaneo y Enumeración de activos I y II

Plataforma con máquinas virtuales con vulnerabilidades conocidas utilizada como víctima en esta práctica.

TryHackMe

Fase del pentesting en la que se identifican los host activos, comienza después de obtener el rango de direcciones IP de nuestro objetivo en la fase de reconocimiento

Escaneo

segunda fase del pentesting.

Fingerprinting

Fuente de donde podemos obtener información del sistema operativo, aplicaciones o servicios.

Puertos abiertos

Fase del pentesting en la que realizamos un escaneo intenso, de manera que obtendremos información más sensible como cuentas de usuario o procesos en ejecución.

Enumeración

Herramientas que nos permiten definir un rango de IPs donde enviar solicitudes de respuesta (echo request) utilizando el protocolo ICMP (Internet Control Message Protocol).

Ping Sweepers

Protocolo que permite comprobar si un host está activo.

TCP

Mecanismo que tenemos a nuestra disposición para hacer ping si el host ha bloqueado el protocolo ICMP.

Ping TCP

Herramienta de escaneo de puertos más conocida y usada en esta práctica.

Nmap

Host que responde a una solicitud PING.

Activo

Estado de puerto que significa que está accesible pero no tiene un servicio que responda a las peticiones.

Cerrado

Estado de puerto que nos indica que está disponible y escuchando.

Abierto

Estado de puerto que significa que no está accesible.

Filtrado

Estado de puerto que significa que está accesible, pero se desconoce si abierto o cerrado.

No-filtrado

Escaneo que envía una solicitud de sincronización SYN a la víctima.

Half-Open

Escaneo en el que una respuesta reset (RST) implica que el puerto está cerrado.

SYN

Escaneo en el que una respuesta que contenga un segmento UDP implicará que el puerto está abierto y una respuesta que contenga un mensaje ICMP port-unreacheable implicará que el puerto está cerrado.

UDP

Escaneo que permite comprobar la existencia de un firewall.

ACK

Riesgo que tiene una máquina con una o más vulnerabilidades que podrían ofrecer información al atacante.

Baja

Riesgo que tiene una máquina con una o más vulnerabilidades severas, pero que requieren cierta complejidad para explotarlas.

Media

Riesgo que tiene una máquina con una o más vulnerabilidades críticas y explotables fácilmente por un atacante.

Alta

Herramienta de código abierto que permite escanear puertos, abrir puertos de escucha, realizar conexiones remotas y transferir ficheros.

Netcat

Práctica 5: Explotación de redes, sistemas y contraseñas I y II

Protocolo para la ejecución de órdenes remotas, precursor de SSH.

Telnet

Protección habitual contra ataques de fuerza bruta.

Captcha

Tipo de ataque de fuerza bruta mediante el cual un usuario introduce usuarios y contraseñas a mano, sin ayuda de herramientas externas.

Ataque de fuerza bruta simple

Tipo de ataque de fuerza bruta mediante el cual se utiliza un fichero con usuarios y contraseñas, probando las combinaciones presentes de forma automática.

Ataque de fuerza bruta por diccionario

Tipo de ataque de fuerza bruta mediante el cual se conoce el usuario o la contraseña, y se trata de averiguar el que no conocemos.

Ataque de fuerza bruta inverso

Herramienta que permite realizar ataques de fuerza bruta especializada en redes locales.

Crackmapexec

Herramienta que permite realizar ataques de fuerza bruta especializada en servicios de login externos.

Hydra

Protocolo habitual en dispositivos como impresoras, por defecto en el puerto 445.

SMB

Puerto por defecto del protocolo SMB.

445

Herramienta que permite obtener información general de sistemas Windows y Linux a través del protocolo SMB.

Enum4linux

Herramienta que nos permite listar discos y directorios de un sistema remoto a través del protocolo SMB.

Smbmap

Máquina virtual preparada con múltiples vulnerabilidades conocidas

Metasploitable2

Fase previa a cualquier tipo de ataque donde se obtiene información sobre el sistema.

Information Gathering

Fase de recolección de toda la información de carácter público del sistema que queremos atacar, donde destacan los Google Dorks.

Footprinting

Fase de recolección de información donde obtenemos información más detallada del sistema (direcciones IP, estado de

puertos, etc.)

Fingerprinting

Ataque a contraseñas donde el atacante engaña a una víctima suplantando otra identidad (persona, empresa o servicio)

Phishing

Ataque a contraseña donde se averigua la contraseña probando todas las palabras de una determinada colección.

Ataque de diccionario

Framework que incluye payloads, exploits y herramientas auxiliares para realizar pruebas de intrusión.

Metasploit

Procedimiento creado con el fin de explotar o aprovechar una vulnerabilidad específica de un sistema, que puede venir dada por un fallo en la configuración, programación, diseño, etc.

Exploit

Programa que se ejecuta de manera remota después de que el exploit haya tenido éxito.

Payload

Aplicación informática cuya misión es capturar distintos paquetes que circulan por la red.

Sniffer

Es posible acceder a un sistema de manera remota si conocemos la IP y los puertos abiertos del mismo.

Es posible

Metasploit es un framework programado en C++ y desarrollado por la organización OWASP.

Falso

Como profesionales de la ciberseguridad, debemos atacar siempre sistemas reales, ya que si no, es imposible concienciar a la sociedad.

Falso

Metasploitable2 es una máquina utilizada como estación hacker para lanzar ataques.

Falso

Preguntas de otros exámenes

Un intruso envía un correo electrónico a un usuario autorizado de un sistema, haciéndose pasar por el administrador indicándole que se cambie la contraseña y cual se debe poner ¿Como clasificaría dicho ataque?

a. dejar en blanco
b. Basurero
c. Shoulder surfing
d. **Ingeniería Social**

Un virus se dice que es residente si:

a. **se instala en memoria principal.**
b. dejar en blanco.
c. Esta almacenado junto con el código de un programa.
d. esta almacenado en memoria secundaria.

Si en el fichero de configuración de la utilidad sudo aparece la Linea ALL AULA=/sbin/mount/media/usb, esta significa:

a. dejar en blanco.

b. **Todos los usuarios del sistema, desde las maquinas listadas en el alias AULA pueden montar memoria USB.**

c. Cuando un usuario se conecte a una maquina denomina AULA auto..

d. Los usuarios del sistema AULA pueden montar memorias USB.

¿Cual de las siguientes NO es una medida de seguridad aplicable para la mejora de la seguridad de una empresa frente a los ataques de su propio personal?

a. Dejar en blanco.

b. Rotacion de funciones.

c. Control Dual.

d. **Máximo privilegio.**

Si un programador al desarrollar una aplicación introduce una condición según la cual al dar la contraseña EXP2USER no le va a pedir ninguna otra contraseña y va tener acceso a todos los datos que maneja la app y esa característica se mantiene en el producto final, ¿que tipo de código malicioso ha introducido?

a. Un caballo de troya.

b. Dejar en blanco.

c. Una bomba lógica.

d. Una puerta trasera

¿Que Google Dork permite buscar enlaces que lleven a un determinado sitio web?

a. site:

b. Dejar en blanco.

c. related:

d. ~~link:~~

¿Cual de las siguientes medidas seria mas eficiente a la hora de prevenir ataques de seguridad interno?

a. Un único usuario del sistema debe poseer todos los privilegios...
b. **Rotación de funciones.**
c. Dejar en blanco.
d. Todos los usuarios del sistema deben poseer privilegios para...

Cuales de las siguientes afirmaciones sobre los virus es cierta

a. Los virus solo infectan ficheros ejecutables.
b. Los virus solo se propagan a través de la red.
c. **Los virus que infectan un fichero ejecutable pueden añadir su código al de su huésped.**
d. Dejar en blanco

Mediante la utilidad sudo el administrador de un sistema GNU/Linux puede establecer:

a. Qué usuarios pueden acceder al sistema sin contraseña.
b. Dejar en blanco.
c. Establecer alias que los usuarios pueden utilizar en lugar de su nombre de usuario.
d. **Qué usuarios del sistema pueden ejecutar ciertas órdenes para las que necesitarían inicialmente privilegios de superusuario.**

¿En qué categoría de ataques a la seguridad catalogaría el phishing?

a. **Ingeniería social.**
b. Basureo.
c. Dejar en blanco.
d. Shoulder surfing.

Una entrada secreta a un programa o sistema informático es:

a. Una bacteria.

b. Un gusano.

c. **Una puerta trasera.**

d. Dejar en blanco.

Un virus que hace cambios en el sistema de ficheros, creando otro fichero con el mismo nombre pero con otra extensión, de forma que al introducir el nombre sin extensión se ejecute el virus en vez del fichero original...

a. Es un virus de inserción.

b. Dejar en blanco.

c. Es un virus de enlace.

d. **Es un virus de compañía.**

¿En qué categoría de ataques a la seguridad catalogaría el vishing?

a. **Ingeniería social.**

b. Basureo.

c. Dejar en blanco.

d. Shoulder surfing.

El fichero de configuración de la utilidad sudo es:

a. /etc/visudo

b. Dejar en blanco.

c. /usr/sudoers.

d. **/etc/sudoers**

Los tipos de código malicioso que necesitan un programa anfitrión como soporte son:

a. Virus, gusanos y zombies.
b. **Virus, trampas, bombas lógicas y caballos de Troya.**
c. Dejar en blanco.
d. Trampas, virus y gusanos.

Los tipos de código malicioso que se reproducen son:

a. Zombis, gusanos y virus.
b. Gusanos, virus y caballos de Troya.
c. Gusanos y virus.
d. Dejar en blanco.

¿Cuál de las siguientes no es una medida de seguridad aplicable para la mejora de la seguridad de una empresa frente a los ataques de su propio personal?

a. **Mantener a los empleados vigilados constantemente y que ellos lo sepan.**
b. Rotación de funciones.
c. Separación de funciones.
d. Dejar en blanco.

Los virus son pequeños programas inspirados en:

a. Dejar en blanco.
b. **Técnicas de reproducción de bacterias, bombas lógicas y caballos de Troya.**
c. Técnicas de reproducción de bacterias, puertas traseras y zombies.
d. Bombas lógicas, puertas traseras y caballos de Troya.

¿Cuál de las siguientes afirmaciones acerca de un rootkit es cierta?

a. Es un conjunto de programas que permite verificar la integridad de los ficheros de un sistema.

b. **Es un conjunto de programas que introduce un intruso en un sistema y le asegura el acceso a éste de forma continua.**

c. Dejar en blanco.

d. Es un conjunto de programas que permite descubrir la actividad llevada a cabo por un intruso en un sistema.

Un intruso se hace pasar por un usuario autorizado de un sistema y mediante una llamada telefónica logra que el administrador le cambie la contraseña. ¿Cómo calificaría dicho ataque?

a. Basureo.

b. Shoulder surfing

c. **Ingeniería social.**

d. Dejar en blanco

Un usuario de un sistema informático no conoce las normas de seguridad básicas para los sistemas e introduce por teclado su nombre de usuario y contraseña delante de otra persona. Si ésta logra ver la contraseña, ¿cómo calificaría dicho ataque?

a. Dejar en blanco.

b. Ingeniería social.

c. Basureo.

d. **Shoulder surfing.**

¿Cuál de los siguientes no es un mecanismo de Prevención contra accesos físicos no autorizados?

a. Métodos biométricos.

b. Tarjetas inteligentes.

c. Control de las vías de acceso alternativas.

d. **Sensores de presencia.**

El código malicioso se favorece por:

a. **La navegación por internet.**
b. El uso de ordenadores de manera pasiva.
c. El uso de memoria secundaria.
d. Dejar en blanco.

Los códigos maliciosos independientes son:

a. **Gusanos y zombis.**
b. Gusanos y virus.
c. Zombis y caballos de Troya.
d. Dejar en blanco.