PRUEBAS DE PENETRACION LIS Feb-Jul 2023

Exam: 1er Examen Parcial Pruebas de Penetración - Teórico

Correct Partial Correct Incorrect Pending to qualify

Preguntas

Responde a cada pregunta. Recuerda que es posible consultar fuentes externas.

1. **Broken Authentication**

¿En qué consiste la vulnerabilidad?

¿De qué tipos es (interna, externa)?

¿Cómo puede explotarse?

Ejemplo de herramienta que automatiza la explotación de esa vulnerabilidad

¿Cómo puede mitigarse?

Response

se refiere a un defecto de seguridad en el proceso de autenticación de un sistema que permite a un atacante tomar el control de una cuenta de usuario legítima sin la necesidad de conocer las credenciales de autenticación válidas del usuario. Esta vulnerabilidad puede ser interna o externa, dependiendo de si el ataque se realiza desde dentro o fuera de la red del sistema en cuestión. En general, una vulnerabilidad de autenticación rota puede explotarse a través de varias técnicas, como la fuerza bruta de contraseñas, la suplantación de identidad o la inyección de comandos, que permiten al atacante eludir los mecanismos de autenticación para acceder a una cuenta de usuario legítima. las herramientas que pueden ayudar serian Burp Suite, OWASP ZAP, Nmap y Metasploit. Para mitigar esta vulnerabilidad, es importante implementar medidas de seguridad en el proceso de autenticación, como la implementación de contraseñas robustas y políticas de expiración de contraseñas, la autenticación de múltiples factores y la implementación de medidas de seguridad para detectar y bloquear intentos de acceso no autorizados.

2. **Cross-Site Scripting XSS**

¿En qué consiste la vulnerabilidad?¿De qué tipos es (interna, externa)?

¿Cómo puede explotarse?

Ejemplo de herramienta que automatiza la explotación de esa vulnerabilidad

¿Cómo puede mitigarse?

Response

La vulnerabilidad de Cross-Site Scripting (XSS) se refiere a un tipo de ataque que permite a un atacante inyectar código malicioso en un sitio web vulnerable, que luego se ejecuta en el navegador web de un usuario legítimo. Esto puede permitir al atacante robar información sensible, como contraseñas, sesiones de usuario y otra información personal. implica la inserción de código malicioso en una URL que luego se muestra en una página web a través de una vulnerabilidad en la entrada del usuario. La vulnerabilidad de Almacenado, por otro lado, permite que el código malicioso se almacene en una base de datos en el servidor web y luego se muestre a los usuarios legítimos que acceden a esa página. puede utilizar técnicas como la ingeniería social, la inyección de código malicioso a través de formularios web y la explotación de vulnerabilidades de seguridad en aplicaciones web. Las herramientas utilizadas la vulnerabilidades de XSS incluyen Burp Suite, OWASP ZAP y BeEF Para mitigar la vulnerabilidad, se pueden utilizar técnicas de validación de entrada para asegurarse de que los datos ingresados por el usuario sean seguros y no contengan código malicioso, por ejemplo, validar los espacios y limites de entrada en los campos cuyos valores se escriban en una base de datos

3. **Sensitive Data Exposure**

¿En qué consiste la vulnerabilidad?

¿De qué tipos es (interna, externa)?

¿Cómo puede mitigarse?

Response

se refiere a la exposición de información confidencial, como contraseñas, datos de tarjetas de crédito y otros datos personales, debido a una mala configuración o falta de protección adecuada. Esta vulnerabilidad puede ser tanto interna como externa. La exposición de información confidencial puede ocurrir desde dentro de la organización, como resultado de una mala configuración o una violación de seguridad por parte de un empleado, o desde fuera de la organización, como resultado de un ataque de un hacker. hay varias herramientas que pueden automatizar la explotación de la vulnerabilidad de Sensitive Data Exposure, como los escáneres de vulnerabilidades, los sniffers de red y los kits de herramientas de hacking. para mitigar esta vulnerabilidad, se debe implementar medidas de seguridad adecuadas, como la encriptación de datos confidenciales en reposo y en tránsito, la implementación de firewalls y el uso de software de detección de intrusiones para detectar y prevenir ataques.

4. **Injection**

¿En qué consiste la vulnerabilidad?

¿De qué tipos es (interna, externa)?

¿Cómo puede explotarse?

Ejemplo de herramienta que automatiza la explotación de esa vulnerabilidad

¿Cómo puede mitigarse?

Response

la vulnerabilidad injection se refiere a un tipo de ataque en el que un atacante puede insertar código malicioso en un sistema vulnerable. Esta vulnerabilidad puede permitir al atacante tomar el control del sistema o acceder a información sensible, como contraseñas, datos de usuario y otra información personal. La vulnerabilidad de Inyección puede ser interna o externa, dependiendo de si el ataque se realiza desde dentro o fuera de la red del sistema en cuestión. En general, la vulnerabilidad de Inyección se divide en varios tipos, como Inyección SQL, Inyección de comandos, Inyección de código y otras. Para explotar la vulnerabilidad de Inyección, un atacante puede utilizar técnicas como la ingeniería social, la inyección de código malicioso a través de formularios web y la explotación de vulnerabilidades de seguridad en aplicaciones web. Las herramientas comúnmente para explotar esta vulnerabilidad de Inyección incluyen SQLMap, Metasploit y BeEF. Para mitigar se puede optar por implementar técnicas de validación de entrada de datos y una limpieza de los mismos para asegurarse de que los datos ingresados por el usuario sean seguros y no contengan código malicioso. también utilizar lenguajes de programación que tengan protecciones integradas contra vulnerabilidades de Inyección, como PHP y Java. además de utilizar herramientas de seguridad como firewalls de aplicaciones web (WAF) y software de detección de intrusos (IDS) para proteger contra ataques de Inyección.

5. **Insufficient Logging & Monitoring**

¿En qué consiste la vulnerabilidad?

¿De qué tipos es (interna, externa)?

¿Cómo puede explotarse?

Ejemplo de herramienta que automatiza la explotación de esa vulnerabilidad

¿Cómo puede mitigarse?

Response

se refiere a la falta de registro y supervisión adecuados de los eventos y actividades que ocurren en un sistema, lo que puede permitir a los atacantes realizar actividades maliciosas sin ser detectados. Esta vulnerabilidad se considera interna ya que se refiere a la falta de monitoreo y registro dentro de un sistema, es posible explotar esta vulnerabilidad para realizar acciones maliciosas en un sistema sin dejar rastro o para evadir la detección durante un ataque. sin un registro adecuado, estos ataques pueden pasar desapercibidos, permitiendo que los atacantes continúen su actividad maliciosa sin ser detectados. las herramientas que pueden explotar la vulnerabilidad son diversas, siempre incluyen el escaneo de vulnerabilidades y herramientas de explotación de redes. para mitigar se puede implementar un sistema de registro y monitoreo adecuado en un sistema, incluyendo la implementación de políticas y procedimientos adecuados de registro y monitoreo, así como la implementación de herramientas y tecnologías adecuadas para el registro y monitoreo en tiempo real de los eventos del sistema.

6. **Security Misconfiguration**

¿Cómo puede explotarse?

Ejemplo de herramienta que automatiza la explotación de esa vulnerabilidad

¿Cómo puede mitigarse?

Response

se refiere a la mala configuración de los sistemas, aplicaciones y dispositivos, lo que puede dejarlos vulnerables a ataques maliciosos. Esta vulnerabilidad puede ser causada por una variedad de factores, como configuraciones predeterminadas inseguras, permisos excesivos o falta de actualizaciones de software. esta vulnerabilidad puede ser tanto interna como externa. La mala configuración puede ser causada por una configuración incorrecta del sistema o la aplicación por parte de un empleado, o por la falta de actualización del software y la configuración insegura por parte de los administradores del sistema. para explotar se puede intentar identificar vulnerabilidades conocidas en sistemas y aplicaciones mal configuradas, o realizar pruebas de penetración para explotar las configuraciones inseguras. se pueden utilizar muchas herramientas para explotar las vulnerabilidades, como los escáneres de vulnerabilidades y las herramientas de pruebas de penetración. para mitigar esta vulnerabilidad, es importante implementar prácticas de seguridad adecuadas, como la actualización regular del software y la aplicación de parches de seguridad, la eliminación de las configuraciones predeterminadas inseguras y la restricción de los permisos de acceso solo a usuarios autorizados.

7. **Using Components with Known Vulnerabilities**

¿En qué consiste la vulnerabilidad?

¿De qué tipos es (interna, externa)?

¿Cómo puede explotarse?

Ejemplo de herramienta que automatiza la explotación de esa vulnerabilidad

¿Cómo puede mitigarse?

Response

Consiste en vulnerabilidades en los paquetes/librerias de terceros que utilizamos en nuestro proyecto/software es de tipo interna, debido a que los programadores hacen la selección de dichos paquetes, de los cuales es su responsabilidad investigar sobre sus vulnerabilidades. se pueden utilizar herramientas de analisis, para el caso de aplicaciones web, podemos utilizar servicios como shodan para ver el stack tecnologico y expllotar sus vulnerabilidades individualmente. se puede mitigar teniendo un buen control de paquetes y dependencias, ademas antes de utilizar cualquier paquete externo, realizar un analisis para asegurarnos que el paquete es confiable

8. Describe con tus propias palabras, ¿qué es un Rootkit Hunter (rkhunter)?

Response

Rootkit Hunter (rkhunter) es una herramienta de detección de rootkits, que son tipos de malware que se utilizan para ocultar procesos maliciosos y actividades de un sistema comprometido.es una herramienta gratuita y open source que se ejecuta sistemas UNIXLIKE como Linux y puede ayudar a detectar rootkits y otras amenazas en un sistema. Rkhunter realiza una exploración del sistema en busca de rootkits y otras amenazas comunes, como troyanos y puertas traseras, y puede proporcionar informes detallados sobre cualquier actividad sospechosa que encuentre. Además, rkhunter también puede realizar comprobaciones de integridad de archivos y detectar cambios no autorizados en los archivos del sistema.

9. Describe la línea del siguiente comando y ¿cual será su posible resultado?

Hydra: hydra -l root -P rockyou ssh://192.168.86.47

Response

hydra es una herramienta de craking de contraseñas, por lo que el utilizar el comando anterior es un intento de hacer crack a un sistema -l root se refiere al usuario al cual atacar -P rockyou se refiere al archivo de contraseñas posibles el cual tomara por ultimo ssh://192.168.86.47 se refiere a la direccion del sistema, en este caso es un cliente ssh localizado en 192.168.86.47 como salida, puede ser que hydra tega exito y logre entrar al sistema, o en caso contrario agotar las contraseñas posibles en el archivo

Response

funciona de forma similar a lo que funciona hydra, en este caso, damos 2 archivos FILE0 que contiene a los usuarios y FILE1 que contiene las posibles contraseñas y su tarea es crackear la contraseña por fuerza bruta, haciendo un todos contra todos, tiene una complejidad exponencial, siendo O(n^2) debido a que puede tener el mismo numero de usuarios que de contraseñas en el peor de los casos. lo que ejecutara es el intento de acceso y autentificacion utilizando los archivos FILE0 y FILE1 en el host 192.168.86.61

11. ¿Qué es Shodan?

- ○ Un motor de búsqueda para dispositivos conectados a Internet ✔
- ◉ Un analizador de servicios Web ✘
- ○ Un scanner de puertos UDP
- ○ Un scanner de protocolos de tipo TCP/UDP/ICMP
- ○ Un scanner de puertos TCP

12. ¿Los ataques del día 0 son aquellos que explotan vulnerabilidades bien conocidas?

- ○ Si
- ◉ No ✔

13. ¿Un ataque de día 0 se prepara con anticipación con un exploit, pero esta información se mantiene en privado?

- ◉ Si ✔
- ○ No

14. ¿Se puede descubrir una vulnerabilidad de día 0 con Nessus?

- ○ Si ✔
- ◉ No ✔
- ○ Talvez

15.

CAT -h host -a diccionario

¿Se utiliza para intentar logins a dispositivos que utiliza Telnet para intentar conexiones?

- ○ Si ✔
- ◉ No ✘

16. CISCOTorch ¿se utiliza para encontrar dispositivos Cisco y hacer fingerprinting?

- ◉ Si ✔
- ○ No

17. SFUZZ

- ○ Si ✔
- ◉ No ✘

18. ¿Los crawlers son programas que analizan páginas web?

- ◉ Si ✔

tener?

Verdadero

Falso

20. cge.pl

¿Es un script para encontrar vulnerabilidades específicas de dispositivos Cisco?

Verdadero

Falso

21. ZZUF

¿Es capaz de inyectar archivos a aplicaciones que esperan archivos de entrada?

Verdadero

Falso

22. Define con tus propias palabras

¿Qué es la ciberseguridad?

Diferencia entre un Hacker y un Ciberdelicuente

Response

la ciberseguridad es una disciplina enfocada en mantener la seguridad de sistemas informaticos expuestos en la red, esta disciplina abarca muchos campos incluyendo campos sociales, debido a que fuera de las redes, es posible encontrar vulnerabilidades que puedan afectar la integridad de un sistema un hacker y un ciberdelincuente son personas con conocimientos informaticos bastos principalmente enfocados en la ciberseguridad, la principal diferencia es que un hacker encuentra y explota vulnerabilidades a fin de ayudar a fortalecer la seguridad de un sistema, mientras que el ciberdelincuente utiliza este conocimiento con fines malignos, explotando las vulnerabilidad para su propio beneficio

23. Define con sus propias palabras

¿Qué es un Script Kiddies?

¿Qué es un Phreakers?

Response

en palabras simples Script Kiddies es un término utilizado para describir a personas que utilizan herramientas y scripts de hacking creados por otros sin entender completamente cómo funcionan. Es decir, no tienen conocimientos profundos de programación o seguridad informática, y se limitan a utilizar herramientas preconfiguradas para atacar sistemas informáticos sin comprender la naturaleza de los ataques que están realizando. en cambio los Phreakers es un término que se utiliza para describir a personas que se dedican a manipular sistemas de telecomunicaciones para obtener beneficios personales. Los phreakers suelen utilizar técnicas como el "phreaking" (ataque a sistemas telefónicos), el "wardialing" (marcado de números telefónicos para encontrar líneas activas) o el "blueboxing" (uso de tonos de marcado para hacer llamadas gratuitas).

24. En forma de lista ordenada, menciona las 5 fases del hacking:

Response

1. Reconocimiento 2. Escaneo 3. Ganar Acceso 4. Mantenimiento 5. Cobertura de las huellas

25. Completa la frase

Una vulnerabilidad es una debilidad en un sistema que puede ser aprovechada por un atacante.

27. El payload es el código que el atacante quiere ejecutar una vez que el proceso de explotación abrió un hueco.

28. El impacto es la posibilidad de dañar a un sistema o hacerlo no disponible.

29. El riesgo es la probabilidad de tener una cierta pérdida medible.

30. Describe 3 las metodologías PTES, OSTMM 2 e ISAFF utilizadas para pruebas de penetración, su enfoque y las etapas o secciones que tiene.

Response

PTES (Penetration Testing Execution Standard): Es una metodología para pruebas de penetración que se enfoca en proporcionar un enfoque estandarizado y estructurado para llevar a cabo pruebas de penetración. PTES está diseñada para proporcionar un marco de trabajo que pueda ser utilizado por cualquier persona que esté involucrada en las pruebas de penetración, independientemente de su nivel de experiencia. Las fases de PTES son: Pre-engagement Interactions: Esta fase incluye las actividades que se llevan a cabo antes de comenzar la prueba de penetración, como la negociación del alcance, la obtención de autorización y la definición de los objetivos de la prueba. Intelligence Gathering: Esta fase implica la recopilación de información sobre el objetivo de la prueba, como la identificación de sistemas, puertos abiertos y servicios en ejecución. Threat Modeling: En esta fase se lleva a cabo un análisis de riesgos para identificar las vulnerabilidades y los vectores de ataque potenciales. Vulnerability Analysis: En esta fase se lleva a cabo un análisis de vulnerabilidades para identificar las vulnerabilidades que pueden ser explotadas. Exploitation: En esta fase se llevan a cabo las actividades de explotación de las vulnerabilidades identificadas para obtener acceso al sistema o datos. Post-Exploitation: En esta fase se llevan a cabo actividades posteriores a la explotación, como la escalada de privilegios y la persistencia. Reporting: En esta fase se documentan los hallazgos y se presenta un informe al cliente. OSTMM 2 (Open Source Security Testing Methodology Manual): Es una metodología para pruebas de penetración que se enfoca en proporcionar un enfoque basado en el riesgo. OSTMM 2 es una metodología de pruebas de penetración de código abierto que ofrece un conjunto completo de técnicas y herramientas para evaluar la seguridad de los sistemas. Las fases de OSTMM 2 son: Pre-engagement Interactions: Esta fase incluye las actividades que se llevan a cabo antes de comenzar la prueba de penetración, como la negociación del alcance, la obtención de autorización y la definición de los objetivos de la prueba. Intelligence Gathering: Esta fase implica la recopilación de información sobre el objetivo de la prueba, como la identificación de sistemas, puertos abiertos y servicios en ejecución. Threat Profiling: En esta fase se lleva a cabo una evaluación del riesgo para identificar los posibles ataques. Vulnerability Assessment: En esta fase se lleva a cabo una evaluación de vulnerabilidades para identificar las vulnerabilidades que pueden ser explotadas. Exploitation: En esta fase se llevan a cabo las actividades de explotación de las vulnerabilidades identificadas para obtener acceso al sistema o datos. Post-Exploitation: En esta fase se llevan a cabo actividades posteriores a la explotación, como la escalada de privilegios y la persistencia. Reporting: En esta fase se documentan los hallazgos y se presenta un informe al cliente. ISAFF es una metodología de pruebas de penetración que se centra en la evaluación de la seguridad de los sistemas de información. Esta metodología se basa en un enfoque sistemático y estructurado para la realización de pruebas de penetración, que incluyen la identificación de activos, la evaluación de la vulnerabilidad y la explotación de las debilidades. Las principales secciones de la metodología ISAFF son: Planificación y preparación: En esta etapa se identifican los objetivos de la evaluación, se definen los límites del alcance de la evaluación y se recopila información sobre el objetivo. Recopilación de información: En esta fase se recopila información sobre el objetivo, incluyendo información sobre la infraestructura, los sistemas operativos y las aplicaciones. Identificación de vulnerabilidades: En esta etapa se identifican las vulnerabilidades de los sistemas de información mediante el uso de herramientas automatizadas y técnicas de análisis manual. Análisis y evaluación de riesgos: En esta fase se evalúa el impacto potencial y la probabilidad de explotación de las vulnerabilidades identificadas, lo que permite identificar los riesgos asociados. Explotación de vulnerabilidades: En esta fase se explotan las vulnerabilidades identificadas para determinar si pueden ser utilizadas para comprometer la seguridad del objetivo. Documentación y presentación de resultados: En esta etapa se documentan los resultados de la evaluación y se presentan al cliente en un informe detallado. La metodología ISAFF se centra en el análisis profundo de los sistemas de información, lo que la hace especialmente adecuada para entornos empresariales complejos y críticos.

31. El cracking de passwords puede considerarse una labor que se encuentra entre lo legal y lo ilegal .

32. Usualmente las contraseñas se " encriptan " en un sistema operativo.

33. Menciona 4 funciones de hash más utilizadas en la actualidad:

Response

No ✔

Depende

35. Menciona las 4 técnicas que se utilizan para el crack de contraseñas:

Response

ataques de diccionario, ataques de fuerza bruta, ataques por rainbown, ataques de ingenieria social

Exit