PRUEBAS DE PENETRACION LIS Feb-Jul 2023

Exam: 2o Examen Parcial Pruebas de Penetración - Teórico

Correct Partial Correct Incorrect Pending to qualify

Metodologías de Pruebas de Penetración

1. Ordena de menor a mayor las 5 fases del hacking.

Response

1. Reconocimiento 2. Escaneo 3. Enumeración 4. Obtención de acceso 5. Mantenimiento del acceso

2. Respecto al estándar PTES, menciona ¿Cuántas y cuáles son las secciones que tiene? y ¿en qué versión se encuentra actualmente?

Response

Consta de 7 secciones y son: 1. Pre-engagement Interactions 2. Intelligence Gathering 3. Threat Modeling 4. Vulnerability Analysis 5. Exploitation 6. Post Exploitation 7. Reporting la version actual es la 1.0 sin embargo, de acuerdo a la pagina de PTES, oficialmente seria como 0.9 ya que en su modelo de versionamiento, aun no llegarian a la 1.0, pero actualmente es esa.

3. El estándar OSSTMM 2.1 es una metodología abierta generalmente utilizada en auditorías de:
seguridad y pruebas de pene

4. OSSTMM (Open Source Security Testing Methodology Manual) es una metodología abierta de comprobación de la seguridad creada por la organización: ISECOM

5. ISSAF (Information Systems Security Assessment Framework) es un framework de la OISSG (Open Information Systems Security Group) que clasifica las distintas técnicas de auditoria de seguridad de los sistemas de información en varios dominios y detalla los aspectos concretos de evaluación de cada uno de estos dominios.

ISSAF clasifica las pruebas técnicas con base a niveles:

(Especifica los 4 niveles)

Response

Nivel 1: Pruebas Funcionales: Se centra en la evaluación de la funcionalidad de los sistemas de información, incluyendo la verificación de la correcta ejecución de procesos y la validación de los datos de entrada y salida. Nivel 2: Pruebas de Control: Se enfoca en la evaluación de los controles de seguridad implementados en los sistemas de información, como políticas, procedimientos y mecanismos de autenticación, autorización y auditoría. Nivel 3: Pruebas de Vulnerabilidad: Se concentra en la identificación y explotación de vulnerabilidades en los sistemas de información, incluyendo la búsqueda de fallos en la configuración, puertos abiertos, servicios expuestos y debilidades en el software. Nivel 4: Pruebas de Impacto: Se trata de evaluar el impacto potencial de un ataque o incidente de seguridad en los sistemas de información. Esto implica simular ataques reales y medir el impacto en la disponibilidad, integridad y confidencialidad de los datos y los servicios.

6. Si deseamos realizar una auditoría de seguridad a una red inalámbrica, ¿Qué metodología es la más conveniente utilizar?

- PTES
- OWISAM ✓
- ISAAF
- OSSTM 3.0

8. ¿Qué significa el acrónimo OWASP?

Response

Open Web Application Security Project

Herramientas de pruebas de penetración

Herramientas de análisis

1. Para buscar directorios, utilizamos una herramienta de enumeración de directorios web o contenido oculto que pueda tener esta aplicación web, ¿Qué comando o programa le falta a la sentencia siguiente para ejecutarse?

gobuster dir -u http://172.16.1.158/ -w directory-list-2.3-big.txt -t 50 –e

2. La siguiente sentencia de comandos, le falta el programa principal que analiza algo, ¿Qué instrucción le falta?

sqlmap -u http://172.16.1.158/openemr/interface/login/validateUser.php?u= --dbs --batch

3. ¿Qué es una función HASH?

Response

es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud

4. ¿Qué es un ataque de diccionario?

Response

Un ataque de diccionario es un intento de descifrar contraseñas probando palabras o combinaciones de palabras predefinidas en bancos de contraseñas

5. ¿En qué consiste un ataque de fuerza bruta?

Response

Un ataque de fuerza bruta consiste en probar sistemáticamente todas las combinaciones posibles de contraseñas o claves de acceso hasta encontrar la correcta, esto se hace con cualquier algoritmo brute force, generalmente estos algoritmos tienen una complejidad alta O(n^m) osea exonencial, probando los caracteres posibles por el número de caracteres de la contraseña

6. ¿Qué son las tablas de búsqueda?

Response

Las tablas de búsqueda o "rainbow tables", son estructuras de datos precalculadas que se utilizan en ataques de recuperación de contraseñas. Estas tablas almacenan una gran cantidad de hashes (representaciones criptográficas de contraseñas) junto con sus correspondientes contraseñas originales.

7. ¿Qué son las tablas arcoiris y en qué consiste dicha técnica?

Response

son estructuras de datos precalculadas, básicamente es una técnica utilizada en criptografía para acelerar la búsqueda de contraseñas a partir de sus hashes. Esta técnica es un compromiso entre el almacenamiento y el tiempo de cálculo necesario para romper las contraseñas.

9. De la siguiente lista, ¿Qué herramienta podemos utilizar para realizar cracking local?

- ○ HashCat
- ○ CrackPWD
- ◉ John The Ripper ✓
- ○ Rainbow tables

Cracking de Contraseñas

Descifra las siguientes contraseñas

1.Con la herramienta John The Ripper (Vista en clase) descifra la siguientes contraseñas.

pepe:6yQVL/XM8/ZZ9S2IR$yOiJozomFYVYkdeOiXO7OGrceqiVdc6aBeb9yO4QnW.DiQQf9yEBKtm8J4F0Vu2JDXwIJtTKWfUyqMoqKqDNv/:18420:0:99999:7

maria:$6$2t4URKFkY/8Maj.I$mo2yfY0iAMXE60qWxiuKwXMOhexJiPIHYPVL6A7iBNBqV7H5IRLySeTc6dqREkBSflbjuQJlZO2tXEFXYidkK/:18420:0:99999:7:::

admin:$6$0tr5dcVdjueqvQna$LQu.ul4LmYbaNG8/lnx7LBwlW5RxFBEUqjE.sLRlYHeeGkKzz5TZHZ5foe.HEW2hrjNw0Q3sxTMRHFkYmp9uN0:18419:0:99999:7:

Coloca el resultado en el cuadro de texto.

Response

Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-opencl" Use the "--format=sha512crypt-opencl" option to force loading these as that type instead Using default input encoding: UTF-8 Loaded 1 password hash (sha512crypt, crypt(3) 6 [SHA512 128/128 AVX 2x]) Cost 1 (iteration count) is 5000 for all loaded hashes Will run 8 OpenMP threads Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 14 candidates buffered for the current salt, minimum 16 needed for performance. Warning: Only 10 candidates buffered for the current salt, minimum 16 needed for performance. Warning: Only 13 candidates buffered for the current salt, minimum 16 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Warning: Only 11 candidates buffered for the current salt, minimum 16 needed for performance. Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist Proceeding with incremental:ASCII

Exit