M-CIB-005
Metodología General De Pruebas De Intrusión A Aplicaciones Web

Responsables

Elaboró:	Especialista Ciberinteligencia
Revisó:	Control de Documentos
Aprobó:	Gerente de normatividad y cumplimiento

Control de versiones

Versión	Fecha	Descripción del cambio
1	29/09/2022	Emisión Inicial

Clave del formato de manual: F-SGI-004 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Introducción 3
2. Alcance 3
3. Definiciones 3
4. Descripción del manual 4
A. Técnicas de ataque por fase de la metodología 5
1. Reconocimiento 5
2. Enumeración 5
3. Análisis de vulnerabilidades 5
4. Explotación 7
5. Post explotación 7
6. House keeping 7
B. Herramientas por fases de la metodología 8
5. Anexos 11

1. Introducción

Silent4Business ha alineado las pruebas técnicas a metodologías mundialmente reconocidas como SEC542 del SANS Institute y OWASP. El equipo de Silent4Business utiliza las metodologías mencionadas para realizar las pruebas de penetración a cada una de las aplicaciones web.

A continuación, se muestra la metodología empleada para la realización de las pruebas de penetración a aplicaciones web en las modalidades de caja negra, gris y blanca, que contempla la ejecución de técnicas manuales, técnicas automatizadas y actividades de verificación que permiten al equipo de Silent4Business descubrir riegos antes de que se materialicen.

2. Alcance

Este proceso es de uso del área de ciberinteligencia, es aplicable para servicios ejecutados a clientes externos y/o para Silent4Business.

3. Definiciones

Activo

Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza

Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque

Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Comprometer

Evasión de controles de seguridad causando posible de pérdida o daño en un activo de cómputo.

Exploit

Código o técnica que es usada por una amenaza para tomar ventaja de una vulnerabilidad.

Impacto

Medición de la consecuencia al materializarse una amenaza.

Mitigación

Acciones para remediar vulnerabilidades identificadas en los activos.

Probabilidad

Es la posibilidad que existe entre una amenaza y las variables de entorno para que una vulnerabilidad sea aprovechada.

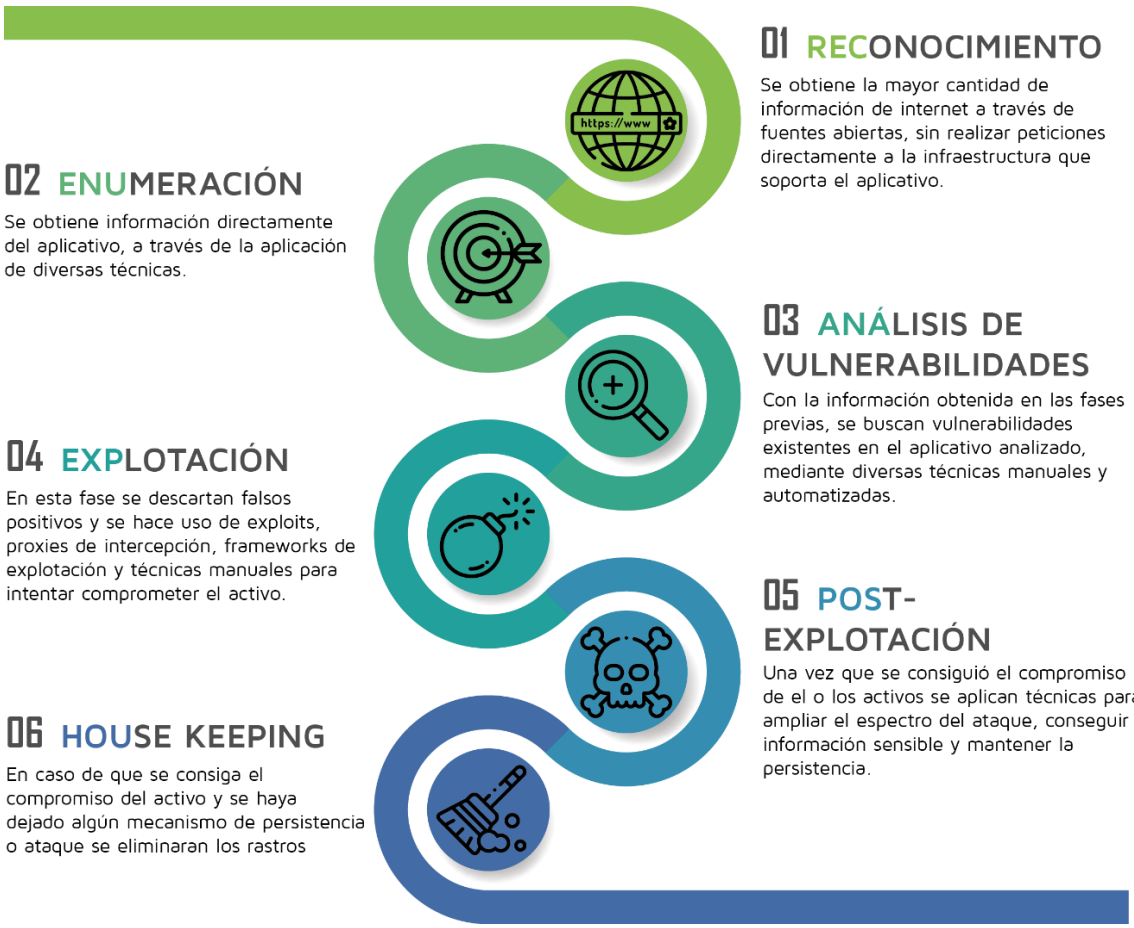
Riesgo

Es la probabilidad de que una amenaza explote una vulnerabilidad con su correspondiente impacto al negocio.

Vulnerabilidad

Son debilidades que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

4. Descripción del manual



Cada que se encuentre infraestructura que soporte aplicaciones o que este expuesta a internet se aplicara la metodología acorde a este, tomando como referencia la metodología OSCP y el SEC 560 del Sans Institute.

A. Técnicas de ataque por fase de la metodología

1. Reconocimiento

Se obtiene la mayor cantidad de información de internet a través de fuentes abiertas, sin realizar peticiones directamente a la infraestructura que soporta el aplicativo.

- Obtención de información desde internet abierta:
  - Registros de ARIN, ASNs, WHOIS, Netcraft, Robtex,
  - Información de buscadores, dominios, subdominios
  - Información de sitios especializados
- Obtención de información de metadatos de archivos

2. Enumeración

Se obtiene información directamente del aplicativo, a través de la aplicación de diversas técnicas.

- Reconocimiento de tecnología
- Identificación de flujos
- Identificación de lógica de negocio
- Identificación de puntos de entrada

3. Análisis de vulnerabilidades

Con la información obtenida en las fases previas, se buscan vulnerabilidades existentes en el aplicativo analizado, mediante diversas técnicas manuales y automatizadas.

- Búsqueda de vulnerabilidades de versión
- Búsqueda de vulnerabilidades de configuración
  - Configuraciones por defecto e inseguras
- Errores de configuración, lógica o programación
- Búsqueda de vulnerabilidades en tecnología
- Búsqueda de vulnerabilidades con herramientas automatizadas
- Intercepción de trafico
- Pruebas de configuración
  - Análisis de roles, privilegios y controles
  - Controles de monitoreo.
  - Prueba de HSTS
- Pruebas de gestión de implementación

- Controles de seguridad de las bases de datos.

- Pruebas de gestión de identidades
  - Análisis de usuarios y permisos.
- Pruebas de autenticación
  - Credenciales por defecto
  - Mecanismos de autenticación débiles
  - Almacenamiento de cache
  - Canal alternativo de autenticación
- Pruebas de autorización
  - Escalación de privilegios
  - Referencias directas a objetos inseguros
  - Directorio transversal
- Pruebas de manejo de sesión
  - Predicción de sesión
  - Secuestro de sesión
  - Reproducir sesión
  - Expiración de sesión insuficiente
  - Cross Site Request Forgery (CSRF)
  - Atributos de cookies
- Pruebas de validación de entradas
  - Inyección comando de SO
  - Inyección SQL
  - Inyección XML
  - Cross-site Scripting
  - Inyección LDAP
  - Parameters Tampering
  - Cookie Poisoning
  - Inyección de cookie
  - Hidden Field Manipulation
  - Ejecución de comandos, LFI, RFI
- Manejo de errores
- Criptografía débil
  - Fortaleza del algoritmo
  - Gestión de llaves
- Lógica de negocio
  - Carga de archivos maliciosos
  - Carga de archivos inesperados
  - Abuso de funciones
  - Tiempo de procesamiento
- Pruebas del lado del cliente
  - Inyección HTML

- Inyección CSS
- Cross-site Scripting DOM Based
- Clickjacking

4. Explotación

En esta fase se descartan falsos positivos y se hace uso de exploits, proxies de intercepción, frameworks de explotación y técnicas manuales para intentar comprometer el activo.

- Credenciales por defecto
- Tecnología vulnerable
- Ataque de diccionario
- Configuración vulnerable
- Explotación de vulnerabilidades encontradas en la fase anterior

5. Post explotación

Una vez que se consiguió el compromiso de el o los activos se aplican técnicas para ampliar el espectro del ataque, conseguir información sensible y mantener la persistencia.

- Búsqueda de información sensible
- Elevación de privilegios
- Intento de compromiso a infraestructura
- Persistencia de ataque
- Exfiltración de información

6. House keeping

En caso de que se consiga el compromiso del activo y se haya dejado algún mecanismo de persistencia o ataque, el equipo de Silent4Business eliminara los rastros que así lo permitan, y en caso de que no se pueda eliminar algún rastro se le notificara al dueño del activo para que haga lo consiguiente.

B. Herramientas por fases de la metodología

A continuación, se listan las herramientas que usa el equipo de SILENT4BUSINESS durante las diferentes fases de la metodología.

Fase de la Metodología	Herramienta	Descripción
Reconocimiento	**Robtex**	Robtex ofrece información acerca de un hosting e información relacionada con el mismo.
	Netcraft	Netcraft ofrece análisis de servidores y alojamiento web, incluyendo la detección del tipo de servidor web y de sistema operativo.
	Whois	WHOIS es un directorio público mediante el cual puede saber "quién es" el propietario de un dominio o dirección IP
	google	Google cuenta con un tipo de búsqueda que tiene como nombre "google dorks" se utiliza para buscar nombres de dominios, documentos, páginas de inicio de sesión o páginas por defecto dentro un dominio especifico, entre otras búsquedas interesantes.
	Shodan	Shodan es un buscador que permite conocer información especifica de un dominio o una ip, otorgando información puntual como los puertos, servicios y versiones que ejecuta la infraestructura.
	Censys	Censys es un buscador que permite conocer información específica de un dominio
	FOFA	Shodan es un buscador que permite conocer información específica de un dominio o una ip, otorgando información puntual como los puertos, servicios y versiones que ejecuta la infraestructura.
	Aquatone	Aquatone es una herramienta que permite enumerar los subdominios y direcciones IP relacionados con un dominio, hace uso de diversos buscadores para obtener mejores resultados.
	Exiftool	Herramienta que permite la visualización y edición e información existente en los metadatos de archivos.
	FOCA	FOCA (Fingerprinting Organizations with Collected Archives) es una herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina. Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar.

Fase de la Metodología	Herramienta	Descripción
Enumeración	**Nmap**	Nmap es una utilidad para el descubrimiento de redes y la auditoría de seguridad. Nmap utiliza paquetes IP sin procesar de formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación) están ofreciendo, qué sistemas operativos (y versiones de SO) están ejecutando, qué tipo de paquetes de filtros / firewalls están en uso, y docenas de otras características. Fue diseñado para escanear rápidamente redes grandes, pero funciona bien con hosts únicos.
	SSLScan	Sirve para comprobar el tipo de cifrado que utiliza un servicio.
	cURL	Herramienta para simular acciones de usuarios en un navegador a bajo nivel, usado para extraer información acerca del servidor web, tales como sistema operativo y tecnologías utilizadas.
	dirbuster	Usado para encontrar directorios ocultos por medio de un ataque de fuerza bruta
	whatweb	Usado para reconocimiento de tecnologías incluyendo CMS (content management system), bibliotecas JS, versión del servidor web y dispositivos embebidos.
	OwasZap	OwasZap es una herramienta desarrollada por OWASP, igual que Acunetix es una herramienta para detectar vulnerabilidades web, cuenta con un módulo de spyder entre varias funcionalidades más. Prueba directamente las posibles vulnerabilidades dentro de una aplicación web.
	Nikto	Nikto es una herramienta que se encarga de detectar malas configuraciones y vulnerabilidades dentro de un servidor específico.
	BurpSuite	Plataforma integrada para ejecutar pruebas de seguridad en aplicaciones web. Cuenta con proxy para interceptar los envíos y respuestas de un aplicativo web, descubrir directorios ocultos, mapear páginas web y realizar ataques web.

Fase de la Metodología	Herramienta	Descripción
Análisis de vulnerabilidades	**BurpSuite**	Plataforma integrada para ejecutar pruebas de seguridad en aplicaciones web. Cuenta con proxy para interceptar los envíos y respuestas de un aplicativo web, descubrir directorios ocultos, mapear páginas web y realizar ataques web.
	SqlMap	SqlMap prueba inyecciones SQL dentro de una aplicación, una vez identificada la vulnerabilidad es posible hacer una inyección de base de datos de manera relativamente sencilla con esta herramienta.
	Vega	Escáner de vulnerabilidades que encuentra XSS, SQL injections y fuga de información. Además, cuenta con una variedad de plugins para realizar ssl man in the middle, análisis de contenido, escaneo de directorios web, entre otros.
	Firebug	Complemento de navegador web que permite inspeccionar y editar el contenido de las aplicaciones web
	w3af	Escáner de vulnerabilidades del tipo SQL injection, XSS, credenciales fáciles de adivinar, mal manejo de errores y fallas de configuración.
	nikto	Nikto es una herramienta que se encarga de detectar malas configuraciones y vulnerabilidades dentro de un servidor específico. En esta etapa para verificar los métodos HTTP soportados por el servidor web así como la tecnología usada.
	Nessus	Nessus permite escanear redes en búsqueda de servicios vulnerables o fallos de seguridad conocidos en múltiples aplicaciones y diversos sistemas operativos.
Explotación	**Metasploit**	Metasploit es un framework de explotación, tiene los exploits más comunes cargados por defecto. Es posible crear y cargar nuevos exploits y ejecutarlos dentro de la herramienta.
	SqlMap	SqlMap prueba inyecciones SQL dentro de una aplicación, una vez identificada la vulnerabilidad es posible hacer una inyección de base de datos de manera relativamente sencilla con esta herramienta.
	EditThisCookie	Complemento de navegador web que permite editar

Fase de la Metodología	Herramienta	Descripción
		"cookies de sesión"
	User Agent switcher	Complemento de navegador web que permite editar "User agent"
	Hydra	Hydra es un programa que compara contraseñas y usuarios dentro del login de una aplicación con el objetivo de localizar credenciales validas de acceso. Se basa en un diccionario de usuarios y contraseñas. Soporta aplicaciones como SSH, FTP, TELNET, entre otras.
	XSSF	Cross-Site Scripting Framework diseñada para explotar vulnerabilidades XSS, creando un canal de comunicación entre el atacante y el objetivo a través de un túnel.
	sqlninja	Herramienta de explotación para realizar ataques SQL injection
Post-explotación	**BeEF**	Framework de explotación usado para explotar aplicaciones web y vulnerabilidades en el navegador.
	BurpSuite	Plataforma integrada para ejecutar pruebas de seguridad en aplicaciones web. Cuenta con proxy para interceptar los envíos y respuestas de un aplicativo web, descubrir directorios ocultos, mapear páginas web y realizar ataques web.
	SqlMap	SqlMap prueba inyecciones SQL dentro de una aplicación, una vez identificada la vulnerabilidad es posible hacer una inyección de base de datos de manera relativamente sencilla con esta herramienta.
	Metasploit	Metasploit es un framework de explotación, tiene los exploits más comunes cargados por defecto. Es posible crear y cargar nuevos exploits y ejecutarlos dentro de la herramienta.

5. Anexos

NA