M-CIB-007
Metodología general de pruebas de intrusión en infraestructura

Responsables

Elaboró:	Especialista Ciberinteligencia
Revisó:	Control de Documentos
Aprobó:	Dirección General

Control de versiones

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

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

Contenido

1. Introducción

Silent4Business ha alineado las pruebas técnicas a metodologías mundialmente reconocidas como SEC560 del SANS Institute, a OSCP de Offensive Security, OSSTMM e ISSAF PTF. El equipo de Silent4Business utiliza las metodologías mencionadas para realizar las pruebas de penetración a infraestructura.

A continuación, se muestra la metodología empleada para la realización de las pruebas de penetración a infraestructura 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.

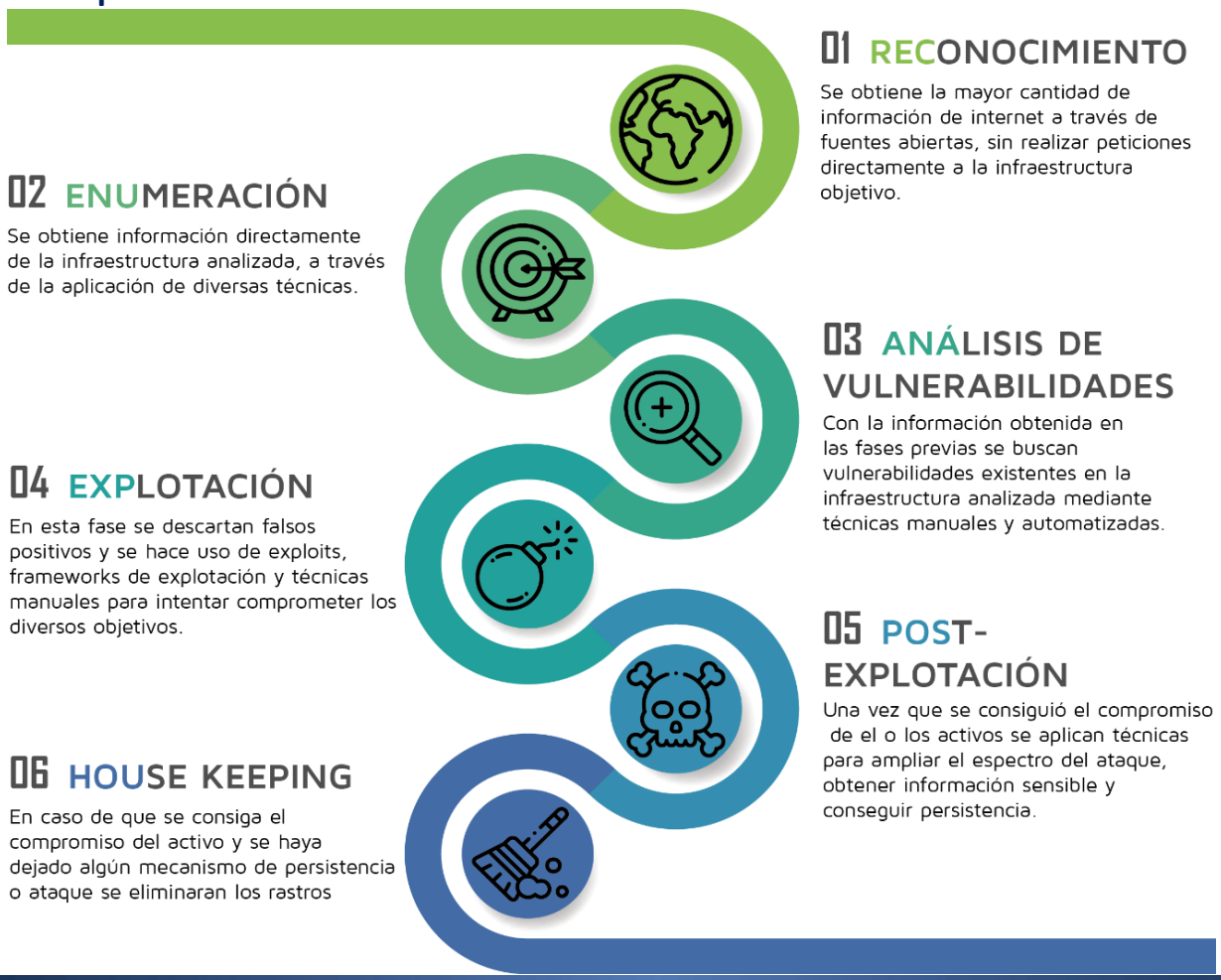
Riesgo

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



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 objetivo.

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

2. Enumeración

Se obtiene información directamente de la infraestructura analizada, a través de la aplicación de diversas técnicas.

- Enumeración de DNS
- Escaneo de puertos TCP y UDP
- Escaneo de servicios
- Banner grabbing
- Reconocimiento de sistema operativo
- Enumeración de SMB
- Enumeración de SMTP
- Enumeración de SNMP

3. Análisis de vulnerabilidades

Con la información obtenida en las fases previas se buscan vulnerabilidades existentes en la infraestructura analizada mediante 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
- Uso de protocolos no seguros
- Búsqueda de vulnerabilidades de diseño
- Búsqueda de vulnerabilidades con herramientas automatizadas
- Intercepción de trafico

4. Explotación

En esta fase se descartan falsos positivos y se hace uso de exploits, frameworks de explotación y técnicas manuales para intentar comprometer los diversos objetivos.

- Credenciales por defecto
- Tecnología vulnerable
- Ataque de diccionario
- Configuración vulnerable
- Evasión de antivirus

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 conseguir persistencia.

- Búsqueda de información sensible
- Elevación de privilegios
- Dumpeo de hashes
- Movimientos laterales
- Crakeo de hashes mediante:
    - Lista de palabras
    - Diccionario
    - Fuerza bruta
    - Ataques híbridos
- Persistencia de ataque

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.

En caso de que se consiga el compromiso del activo y se haya dejado algún mecanismo de persistencia o ataque se eliminaran los rastros

Cada que se encuentren aplicativos web se aplicara la metodología acorde a este, tomando como referencia la metodología OWASP y el SEC 542 del SANS Institute.

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.
	Maltego	Maltego es una aplicación de inteligencia y análisis forense de código abierto. Es una herramienta de recolección de información, así como la representación de esta información en un formato fácil de entender.
	Exiftool	Herramienta que permite la visualización y edición e información existente en los metadatos de archivos.

Fase de la Metodología	Herramienta	Descripción
	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.
Enumeración	**Dig**	Herramienta para realizar consultas a los servidores DNS y solicitar información sobre direcciones de host.
	DNSrecon	herramienta de escaneo y enumeración DNS, la cual permite realizar diferentes tareas, como enumeración de registros estándar para un dominio definido (A, NS, SOA y MX
	DNSenum	Herramienta utilizada para recopilar información sobre un sistema objetivo muy similar a un comando Domain Information Groper (DIG). Donde cada uno de los registros DNS puede dar un poco de información sobre el objetivo.
	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.
	Massscan	Escáner de puertos ágil, capaz de enviar 10 millones de paquetes por segundo.
Análisis de vulnerabilidades	**Nbtscan**	Busca en la red nodos que tengan el servicio NetBios activado y muestra información de ellos por ejemplo el nombre, IP, MAC, etc.
	Snmpwalk	Sirve para solicitar registros de datos con el protocolo simple de administración de red (SNMP).
	Smbclient	Herramienta de conexión con SMB, que permite la transferencia de archivos.
	Smbinfo	Herramienta que permite hacer consultas de

Fase de la Metodología	Herramienta	Descripción
		información a un servidor.
	rpcinfo	Herramienta que obtiene información sobre el servicio de llamada de procedimiento remoto RPC que se está ejecutando en un sistema
	Enum4linux	herramienta para enumerar información desde sistemas Windows y Samba
	Netcat	Herramienta de red que permite a través de intérprete de comandos y con una sintaxis sencilla abrir e interactuar con puertos TCP/UDP en un HOST
	Onesixtyone	escáner de SNMP que envía múltiples peticiones SNMP a varias direcciones IP, para intentar descubrir la comunidad a la que pertenece.
	Arpspoof	Herramienta que puede manipular el mapeo de direcciones IP a MAC enviando mensajes dentro de la red LAN.
	Tcpnice	Herramienta que inyecta paquetes TCP con modificaciones de tamaño.
	Filesnarf	Guarda los archivos capturados desde NFS
	Mailsnarf	Guarda los correos electrónicos capturados desde SMTP y POP
	URLsnarf	Captura todas las URL desde el tráfico HTTP
	Ettercap	Es una herramienta de sniffing activo con técnicas de envenenamiento de ARP cache, es capaz de insertar caracteres en los protocolos. Pose diversas utilerías para intercepción captura de passwords y reconocimiento de sistema operativo
	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.

Fase de la Metodología	Herramienta	Descripción
	Nessus	Nessus permite escanear redes en búsqueda de servicios vulnerables o fallos de seguridad conocidos en múltiples aplicaciones y diversos sistemas operativos.
Enumeración	**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.
	Ollydbg	Es un depurador de código ensamblador mediante el cual se puede realizar el análisis de archivos binarios de pudiesen presentar vulnerabilidades.
	ExploitDB	Base de datos de exploits donde muchos académicos, investigadores y hackers suben vulnerabilidades de aplicaciones y cómo aprovecharse de ellas, con instrucciones especificas para comprometer la vulnerabilidad.
	Empire	Herramienta de post-explotación de PowerShell construido sobre comunicaciones cripto-lógicamente seguras y una arquitectura flexible.
	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.
Post-explotación	**Impacket**	Es una suite que posee diversas herramientas para la explotación y extracción de un controlador de dominio.
	Hashcat	Hashcat es un crakeador de contraseñas el cual puede ejecutar diversos ataques offline a archivos extraídos con herramientas como metasploit o impacket.
	Psexec	Utilidad perteneciente a la suite “Sysinternals” que permite la interacción y comunicación en sistemas Windows.
	John the Ripper	John the ripper es un crackeador de contraseñas, generalmente se usa para recuperación de contraseñas.

Fase de la Metodología	Herramienta	Descripción
	Ophcrack	Ophcrack es un crackeador de contraseñas basado en Rainbow Tables. Es muy fácil de implementar y muy eficiente. Para usarlo deberemos tener los archivos extraídos con herramientas como metasploit o fgdump.
	PACK	Es una suite de análisis de contraseñas, mediante la cual se pueden crear estadísticas de repetición de caracteres, tendencias y generar máscaras de ataque a partir de estas.

Haciendo uso de las mismas fases anteriormente mencionadas, se aplicarán pruebas puntuales sobre los aplicativos web que existan, estas pruebas estarán en estricto apego al OWASP versión 2017 y a SEC542 del SANS Institute.

5. Anexos

NA