M-CIB-006
Metodología General de Pruebas de Intrusión a Cajeros Automáticos

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

Silent4Business ha alineado las pruebas técnicas a metodologías mundialmente reconocidas como OSSTMM, PCI ATM Security Guidelines así como a las mejores prácticas emitidas por ATM Industry Association. El equipo de Silent4Business utiliza las metodologías mencionadas para realizar las pruebas de penetración a cajeros automáticos (ATM).

A continuación, se muestra la metodología empleada para la realización de las pruebas de penetración a cajeros automáticos en las modalidades de caja negra, que contempla la ejecución de técnicas manuales, técnicas automatizadas y actividades de verificación que nos permiten 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

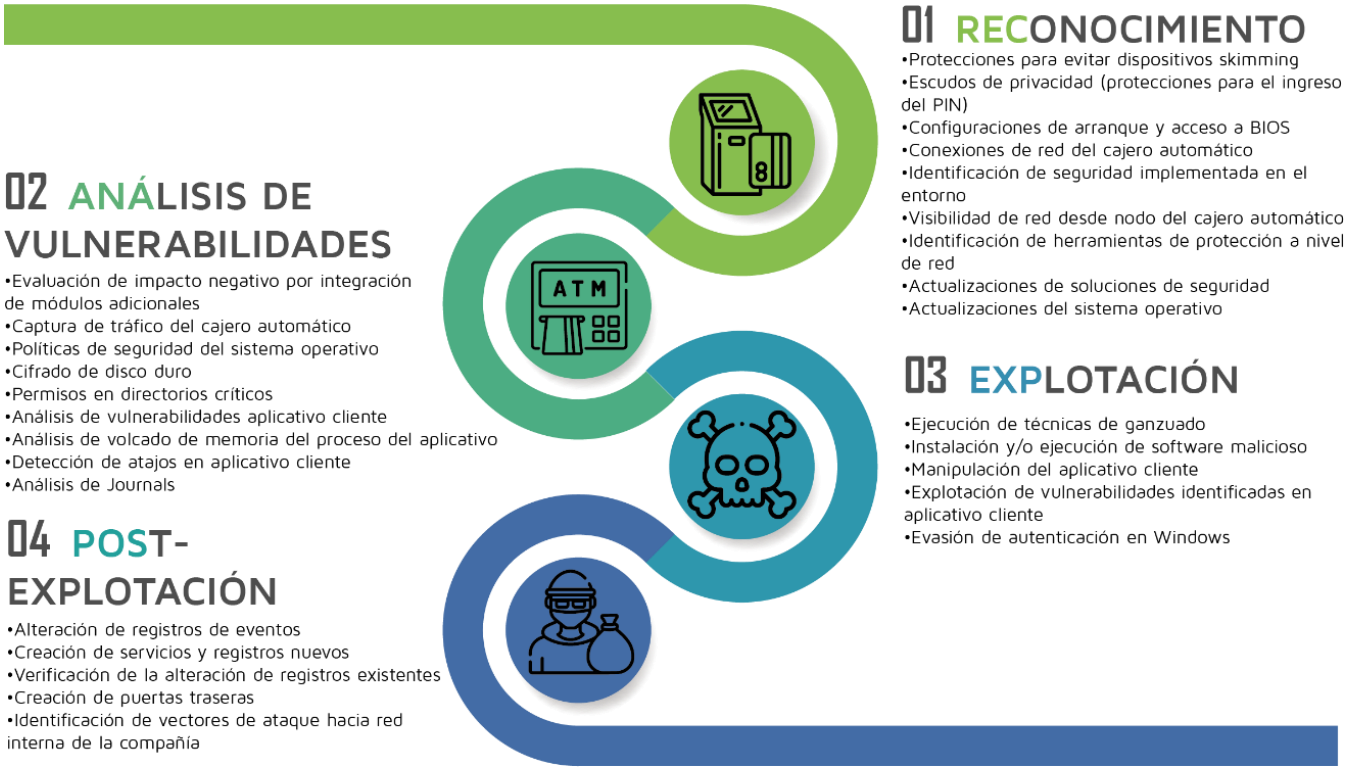
Es la probabilidad de que una amenaza explote una vulnerabilidad con su correspondiente impacto al negocio.

Vulnerabilidad

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

4. Descripción del manual

Describir el contenido del manual de acuerdo con las secciones requeridas.



A. Técnicas de ataque por fase de la metodología

Por cada fase de la metodología, el equipo de SILENT4BUSINESS está capacitado para realizar técnicas de ataques específicos a cajeros automáticos. A continuación, se detallan algunas técnicas de ataque:

1. Reconocimiento

- Identificación de protecciones para evitar dispositivos skimming
- Identificación de escudos de privacidad (protecciones para el ingreso del PIN)
- Revisión de configuraciones de arranque y acceso a BIOS
- Revisión de conexiones de red del cajero automático
- Identificación de seguridad implementada en el entorno
- Identificación de protecciones externas del cajero automático
- Identificación de dispositivos de red desde nodo del cajero automático
- Identificación de herramientas de protección a nivel de red red
- Verificación de actualizaciones de soluciones de seguridad
- Verificación de actualizaciones del sistema operativo
- Identificación de cifrados empleados en transporte y almacenamiento de datos sensibles
- Identificación de utilerías habilitadas, pero no necesarias para el funcionamiento del cajero automático

2. Análisis de vulnerabilidades

- Evaluación de impacto negativo por integración de módulos adicionales
- Verificación de cumplimiento de componentes del cajero automático con PCI
- Captura de tráfico del cajero automático
- Evaluación de servicios en escucha del cajero automático
- Evaluación de políticas de seguridad del sistema operativo
- Evaluación de cifrado de disco duro
- Evaluación de permisos en directorios críticos
- Evaluación de robustecimiento de puertos USB
- Evaluación de datos en memoria RAM
- Análisis de vulnerabilidades aplicativo cliente
    - Reconocimiento
        - Identificación de flujos del aplicativo
        - Identificación de información de compilación
        - Identificación de comunicaciones realizadas
        - Identificación de archivos en uso por la aplicación
    - Enumeración
        - Revisión de archivos en carpetas de instalación de la aplicación
        - Protocolos y suites de cifrado empleadas
        - Llaves de registro empleadas por la aplicación
        - Librerías dinámicas empleadas por la aplicación
        - Campos de entrada del aplicativo
    - Análisis de vulnerabilidades

        - Identificación de inyecciones (SQLi, comandos, XXE, etc.)
        - Fuzzing de campos de entrada
        - Validación de lógica de negocio
        - Almacenamiento de información sensible en registro
        - Evaluación de información en memoria RAM
        - Descompilar aplicación
        - Validación de software firmado
        - Evaluación de mitigaciones implementadas contra explotación de binarios
        - Ejecución de ingeniería inversa
    - Explotación
        - Buffer Overflow
        - Inyección SQL
        - Ejecución de comandos
        - Alteración de la aplicación
        - Secuestro de DLL
        - Evasión de controles implementados
- Análisis de volcado de memoria del proceso del aplicativo
- Detección de atajos en aplicativo cliente
- Análisis de Journals

3. Explotación

- Ejecución de técnicas de ganzuado
- Instalación y/o ejecución de software malicioso
- Manipulación del aplicativo cliente
- Explotación de vulnerabilidades identificadas en aplicativo cliente
- Evasión de autenticación en Windows

4. Post-Explotación

- Alteración de registros de eventos
- Creación de servicios y registros nuevos
- Verificación de la alteración de registros existentes
- Creación de puertas traseras
- Identificación de vectores de ataque hacia red interna de la compañía

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	**Técnicas manuales**	Se realizan diversas técnicas y revisiones manuales sobre el cajero automático así como en el entorno para verificar la seguridad implementada.
	Router	Un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.
	WMI	Windows Management Instrumentation o WMI (en español, Instrumentación de Administración Windows) es la implementación de WBEM (Web-Based Enterprise Management) de Microsoft, una iniciativa que pretende establecer normas estándar para tener acceso y compartir la información de administración a través de la red de una empresa. WMI proporciona compatibilidad integrada para el Modelo de Información Común (CIM, Common Information Model), :Y que describe los objetos existentes en un entorno de administración.
	SSLScan	Es un escáner de puertos SSL la cual nos facilita información sobre qué tipo de cifrado soporta el puerto al que nos conectamos, que tipo de cifrado es el preferido, que protocolos SSL están soportados, información sobre el certificado instalado, permitiéndonos una salida a fichero en formato XML con el que, posteriormente, se pueden elaborar informes.
	Wireshark	Wireshark tiene un conjunto de características que incluye lo siguiente: Inspección profunda de cientos de protocolos, y se agregan más todo el tiempo Captura en vivo y análisis fuera de línea Soporte de descifrado para muchos protocolos, incluidos IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP y WPA / WPA2
	Powershell	Es una interfaz de consola (CLI) con posibilidad de escritura y unión de comandos por medio de instrucciones (scripts en inglés). Esta interfaz de consola está diseñada para su uso por parte de administradores de sistemas, con el propósito de automatizar tareas o realizarlas de forma más controlada.
Análisis de vulnerabilidades	**Lan Tap**	Es un conector Ethernet pasivo, que no requiere alimentación para funcionar. Existen métodos activos para aprovechar las conexiones Ethernet (por ejemplo, un puerto espejo en un conmutador), pero ninguno puede vencer a las derivaciones pasivas para la portabilidad. Para la red de destino, el LAN Tap se parece a una

Fase de la Metodología	Herramienta	Descripción
		sección de cable, pero los cables en el cable se extienden a los puertos de monitoreo además de conectar un puerto de destino al otro.
	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.
	Netstat	Es una herramienta de línea de comandos que muestra un listado de las conexiones activas de una computadora, tanto entrantes como salientes. Existen versiones de este comando en varios sistemas como Unix, GNU/Linux, Mac OS X, Windows y BeOS. La información que resulta del uso del comando incluye el protocolo en uso, las tablas de ruteo, las estadísticas de las interfaces y el estado de la conexión. Existen, además de la versión para línea de comandos, herramientas con interfaz gráfica (GUI) en casi todos los sistemas operativos desarrollados por terceros.
	Powershell	Es una interfaz de consola (CLI) con posibilidad de escritura y unión de comandos por medio de instrucciones (scripts en inglés). Esta interfaz de consola está diseñada para su uso por parte de administradores de sistemas, con el propósito de automatizar tareas o realizarlas de forma más controlada.
	icacls	Muestra o modifica listas de control de acceso discrecional (DACL) en archivos específicos y aplica DACL almacenadas a archivos en directorios específicos.
	reg	Realiza operaciones sobre información de subclave de registro y valores en entradas de registro. Algunas operaciones le permiten ver o configurar entradas de registro en computadoras locales o remotas, mientras que otras le permiten configurar solo computadoras locales. El uso de reg para configurar el registro de computadoras remotas limita los parámetros que puede usar en algunas operaciones.
	CFF Explorer	CFF Explorer fue diseñado para hacer que la edición de PE sea lo más fácil posible, pero sin perder de vista la estructura interna del ejecutable portátil. Esta aplicación incluye una serie de herramientas que pueden ayudar no solo para ingeniería inversa sino también para programación. Ofrece un entorno de múltiples archivos y una interfaz conmutable.
	SysInternals	Pensadas para desarrolladores de software, administradores y

Fase de la Metodología	Herramienta	Descripción
	suite	expertos en IT, Windows Sysinternals es un paquete de utilidades que simplifica realizar determinadas tareas de administración de una PC. Esta suite fue creada por Mark Russinovich y Bryce Cogswell. En 1996 Microsoft la compró, ahora ocupa lugar entre los programas de mantenimiento que ofrece la empresa. Se encuentra dividido en grupos que permiten trabajar sobre el disco, la red, los procesos, seguridad y otras tantas cosas más.
	Wireshark	Wireshark tiene un conjunto de características que incluye lo siguiente: Inspección profunda de cientos de protocolos, y se agregan más todo el tiempo Captura en vivo y análisis fuera de línea Soporte de descifrado para muchos protocolos, incluidos IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP y WPA / WPA2.
	Echo Mirage	Es una herramienta gratuita que se conecta al proceso de una aplicación y nos permite monitorear las interacciones de red que se realizan. Este proceso puede realizarse con un proceso en ejecución, o puede ejecutar la aplicación en nombre del usuario. Este tipo de pruebas de seguridad se incluye en Pruebas de seguridad de aplicaciones de cliente grueso.
	Regshot	Regshot es una utilidad de comparación de registros de código abierto (LGPL) que le permite tomar rápidamente una instantánea de su registro y luego compararlo con un segundo, hecho después de hacer cambios en el sistema o instalar un nuevo producto de software.
	Process Hacker	Process Hacker es Una herramienta gratuita, potente y multipropósito que lo ayuda a monitorear los recursos del sistema, depurar software y detectar malware.
	dotPeek	dotPeek es una herramienta independiente gratuita basada en el descompilador incluido en ReSharper. Puede descompilar de forma segura cualquier ensamble .NET a código equivalente C# o IL. El descompilador admite varios formatos, incluidas bibliotecas (.dll), ejecutables (.exe), y archivos de metadatos de Windows (.winmd).
	ildasm	Ildasm.exe es un desensamblador incluido con .NET Framework SDK y puede analizar cualquier ensamblado .NET Framework .exe o .dll y muestra la información en un formato legible para humanos conocido como CIL (Common Intermediate Language).
	ilasm	Ilasm.exe es un ensamblador IL, que toma el código IL como entrada y genera un archivo ejecutable portátil (PE). Esta herramienta viene preinstalada con Visual Studio, y se encuentra

Fase de la Metodología	Herramienta	Descripción
		en la siguiente ubicación en mi caso.
	BinScope	BinScope es una herramienta de verificación de Microsoft que analiza los archivos binarios a nivel de todo el proyecto para garantizar que se hayan creado de conformidad con los requisitos y recomendaciones del Ciclo de vida de desarrollo de seguridad (SDL) de Microsoft.
	ILSpy	ILSpy es el navegador y descompilador de ensamblado de código abierto .NET.
	Reflexil	Reflexil es un editor de ensamblaje y se ejecuta como un complemento para Reflector de Red Gate, ILSpy y JustDecompile de Telerik. Reflexil está utilizando Mono.Cecil, escrito por Jb Evain y puede manipular el código IL y guardar los ensamblados modificados en el disco. Reflexil también es compatible con la inyección de código C # / VB.NET.
	tcpreplay	Tcpreplay es un conjunto de utilidades gratuitas de código abierto para editar y replicar el tráfico de red previamente capturado. Originalmente diseñado para replicar patrones de tráfico malicioso en los sistemas de detección/prevención de intrusiones, ha visto muchas evoluciones, incluidas las capacidades para replicar servidores web.
	dd	dd es un comando de la familia de los sistemas operativos Unix que permite copiar y convertir datos de archivos a bajo nivel.
	fdisk	Fdisk es un software que está disponible para varios sistemas operativos, el cual permite dividir en forma lógica un disco duro, siendo denominado este nuevo espacio como partición. La descripción de las particiones se guarda en la tabla de particiones que se localiza en el sector 0 de cada disco.
	Ghidra	Ghidra es un marco de ingeniería inversa de software (SRE) desarrollado por la Dirección de Investigación de la NSA para la misión de ciberseguridad de la NSA. Ayuda a analizar códigos maliciosos y malware como los virus, y puede brindar a los profesionales de ciberseguridad una mejor comprensión de las posibles vulnerabilidades en sus redes y sistemas.
	IDA	IDA Disassembler and Debugger es un desensamblador interactivo, programable, extensible y multiprocesador alojado en Windows, Linux o Mac OS X. IDA se ha convertido en el estándar de facto para el análisis de código hostil, investigación de vulnerabilidades y validación COTS.
	WinDBG	WinDbg es un depurador multipropósito para el sistema operativo Microsoft Windows, distribuido por Microsoft.
	GDB	GDB o GNU Debugger es el depurador estándar para el compilador

Fase de la Metodología	Herramienta	Descripción
		GNU. Es un depurador portable que se puede utilizar en varias plataformas Unix y funciona para varios lenguajes de programación como C, C++ y Fortran. GDB fue escrito por Richard Stallman en 1986. GDB es software libre distribuido bajo la licencia GPL.
	bootcode_parser	Es un script Python diseñado para realizar un análisis rápido fuera de línea de los registros de arranque utilizados por los sistemas basados en BIOS (UEFI no es compatible). Su objetivo es ayudar al analista a probar volcados de registros de arranque individuales o imágenes de disco completo. Se prefiere este último ya que permite que el script realice verificaciones adicionales que no serían posibles solo en volcados individuales.
	Nessus	Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente que muestra el avance e informa sobre el estado de los escaneos.
	Metasploit	Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en pentesting y el desarrollo de firmas para sistemas de detección de intrusos.
Explotación	**Ganzúas**	La ganzúa es una herramienta manual que se utiliza para manipular los elementos mecánicos de una cerradura, para realizar su apertura sin llave.
	Kon-boot	Kon-Boot es una utilidad que permite a los usuarios evitar las contraseñas de Microsoft Windows y Apple macOS sin cambios duraderos o persistentes al sistema en el que se ejecuta. También es la primera herramienta capaz de evitar contraseñas de Windows 10 online y soporta tanto sistemas Windows como macOS
	Exploit-DB	Es una herramienta de búsqueda de línea de comandos para Exploit-DB que también le permite llevar una copia de Exploit Database con usted, donde quiera que vaya. SearchSploit le brinda el poder de realizar búsquedas fuera de línea detalladas a través de su copia del repositorio extraída localmente. Esta capacidad es particularmente útil para evaluaciones de seguridad en redes segregadas o con espacios de aire sin acceso a Internet. Muchos exploits contienen enlaces a archivos binarios que no están incluidos en el repositorio estándar, pero que se pueden encontrar en nuestro repositorio Bits Exploits de la base de datos de exploits. Si anticipa que no tendrá acceso a Internet en una evaluación, asegúrese de revisar ambos repositorios para obtener el conjunto de datos más completo.
	Metasploit	Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de

Fase de la Metodología	Herramienta	Descripción
		vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.
Post-explotación	**Powershell**	Es una interfaz de consola (CLI) con posibilidad de escritura y unión de comandos por medio de instrucciones (scripts en inglés). Esta interfaz de consola está diseñada para su uso por parte de administradores de sistemas, con el propósito de automatizar tareas o realizarlas de forma más controlada.
	Invoke-ACLPwn	Invoke-ACLpwn es una herramienta que automatiza el descubrimiento y explotación de ACL en Active Directory que no están configurados de forma segura.
	InvokePhant0m	Es una herramienta que facilita la interrupción del proceso de registro de eventos de Windows.
	Eventlogedit-evtx--Evolution	Esta herramienta permite eliminar líneas individuales de los archivos EVTX sin necesidad de realizar inyección de librerías.

5. Anexos

NA