Proyecto 4: Hunting Vulnerabilities

> *1 De Abril de 2024*

Índice

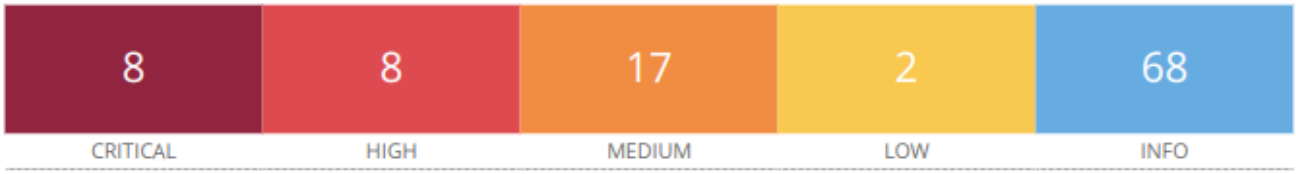
Resumen Ejecutivo

En este documento se presenta la evaluación básica inicial de dos de los servidores de la empresa contratante *SecureLogistics* por parte del equipo de seguridad de nuestra empresa *NETMANCER Incorporated*.

El objetivo principal de este análisis ha sido comprobar si existen motivos para creer que dos de los servidores de *SecureLogistics* presentan efectivamente problemas de seguridad grave, y como resultado final del análisis se concluye que efectivamente **sí existen**.

A continuación se presenta un gráfico resumen con vulnerabilidades encontradas en las máquinas clasificadas por severidad:

Servidor 1 con sistema operativo Windows:



- Puntuación CVSS más alta: **10**

Servidor 2 con sistema operativo Linux:

- Puntuación CVSS más alta: **10**

Teniendo en cuenta que una vulnerabilidad con una puntuación *CVSS* de **10** significa que, de explotarla, se alcanzaría un nivel de compromiso máximo en cuanto a la confidencialidad, integridad y disponibilidad de la información, podemos afirmar que estos dos servidores poseen efectivamente niveles absolutamente críticos de riesgo.

En el presente informe se detalla más información sobre los resultados obtenidos.

Introducción

Para este informe se nos solicitaba un análisis básico de dos servidores de la infraestructura de *SecureLogistics*. El motivo presentado fue la sospecha de posibles problemas de seguridad y la necesidad de acotamiento de los mismos, para garantizar la máxima optimización de una posible inversión en la seguridad de la empresa.

Es por ello que ha decidido realizar un escáner de puertos básico inicial con el propósito de detectar, si es que existen, las vulnerabilidades más comunes en los servidores indicados.

En este informe se realizará un listado de las vulnerabilidades encontradas junto a una breve descripción y evaluación correspondientes utilizando la métrica de evaluación CVSS (*Common Vulnerability Scoring System*).

Alcance

El alcance del mismo se limitará a un escaneo de tipo ***caja negra***, que consiste en inspeccionar y testear todos los puertos de la máquina, sin ayuda de credenciales de acceso y sin realizar intento alguno de vulnerar manualmente ninguna de las máquinas.

Objetivos

El principal objetivo de este informe es determinar mediante herramientas de escaneo básico si existen vulnerabilidades en alguna de las dos máquinas especificadas de inspección por *SecureLogistics*.

Metodología

Para realizar los escaneos se hará uso de la herramienta análisis de vulnerabilidades automático *Nessus Tenable®*.

Esta herramienta realizará un test automático en los puertos vulnerables más comunes y realizará pruebas automatizadas de penetración basadas en las vulnerabilidades y brechas de seguridad más habituales registradas en su base de datos. Tras realizar el test, la misma herramienta generará un reporte que será utilizado para realizar un desglose de las posibles vulnerabilidades encontradas, las cuáles serán examinadas, descritas y evaluadas.

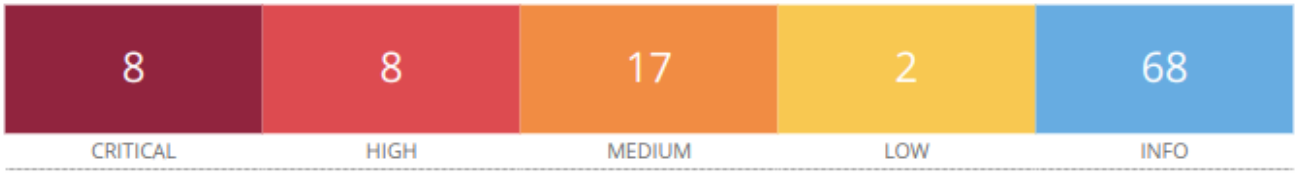
La métrica de evaluación será la proporcionad por CVSS 3.0, *un framework abierto y universalmente utilizado que establece unas métricas para la comunicación de las características, impacto y severidad de vulnerabilidades que afectan a elementos del entorno de seguridad IT* (INCIBE, 2023)

Resultados Obtenidos

Podemos encontrar a continuación una lista en detalle de cada una de las vulnerabilidades encontradas para los servidores especificados:

Servidor 1 - Windows

Resumen gráfico de vulnerabilidades encontradas



CVSS más alto obtenido: **10**

Nivel Crítico

Apache Tomcat AJP Connector Request Injection (Ghostcat)

Gravedad	CVSSv3	CVSSv2	ID
Critical	9.8	9.0	134862

Descripción: Esta vulnerabilidad permite a un atacante remoto leer y escribir archivos en un servidor afectado mediante solicitudes especialmente diseñadas a través del conector AJP.

Solución: Actualizar a una versión parcheada de Apache Tomcat.

Elasticsearch ESA-2015-06

Gravedad	CVSSv3	CVSSv2	ID
Critical	9.8	6.7	119499

Descripción: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema afectado a través de una explotación de tipo escalamiento de privilegios.

Solución: Aplicar el parche de seguridad proporcionado por Elasticsearch.

Elasticsearch Transport Protocol Unspecified Remote Code Execution

Gravedad	CVSSv3	CVSSv2	ID
Critical	9.8	6.7	105752

Descripción: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema afectado a través de una explotación de tipo ejecución remota de código.

Solución: Actualizar Elasticsearch a una versión que solucione este problema.

ManageEngine Desktop Central < 10 Build 10.0.533 Integer Overflow

Gravedad	CVSSv3	CVSSv2	ID
Critical	9.8	5.9	139377

Descripción: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema afectado a través de una explotación de desbordamiento de entero.

Solución: Actualizar a una versión parcheada de ManageEngine Desktop Central.

Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

Gravedad	CVSSv3	CVSSv2	ID
Critical	9.8	9.7	125313

Descripción: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema afectado a través de una explotación de tipo ejecución remota de código.

Solución: Aplicar el parche de seguridad proporcionado por Microsoft.

Unsupported Windows OS (remote)

Gravedad	CVSSv3	CVSSv2	ID
Critical	10.0	-	108797

Descripción: Esta vulnerabilidad indica que el sistema operativo Windows utilizado no tiene soporte, lo que puede dejar el sistema vulnerable a varias amenazas de seguridad.

Solución: Actualizar a una versión compatible y compatible con el sistema operativo.

MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

Gravedad	CVSSv3	CVSSv2	ID
Critical	10.0	7.3	53514

Descripción: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema afectado a través de una explotación de tipo ejecución remota de código.

Solución: Aplicar el parche de seguridad proporcionado por Microsoft.

ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE

Gravedad	CVSSv3	CVSSv2	ID
Critical	10.0*	7.3	90192

Descripción: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema afectado a través de una explotación de tipo ejecución remota de código.

Solución: Aplicar el parche de seguridad proporcionado por ManageEngine.

Nivel Alto

MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)

Gravedad	CVSSv3	CVSSv2	ID
High	8.8	7.4	79638

Descripción: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema afectado a través de una explotación de tipo ejecución remota de código.

Solución: Aplicar el parche de seguridad proporcionado por Microsoft.

ManageEngine Desktop Central 10 < Build 100282 Remote Privilege Escalation

Gravedad	CVSSv3	CVSSv2	ID
High	8.8	6.7	117639

Descripción: Esta vulnerabilidad permite a un atacante escalar privilegios en el sistema afectado.

Solución: Actualizar a una versión parcheada de ManageEngine Desktop Central.

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Gravedad	CVSSv3	CVSSv2	ID
High	8.1	9.7	97833

Descripción: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema afectado a través de una explotación de tipo ejecución remota de código.

Solución: Aplicar el parche de seguridad proporcionado por Microsoft.

Oracle GlassFish Server Path Traversal

Gravedad	CVSSv3	CVSSv2	ID

Gravedad	CVSSv3	CVSSv2	ID
High	7.5	4.4	110192

Descripción: Esta vulnerabilidad permite a un atacante remoto acceder a archivos y directorios sensibles en el sistema afectado.

Solución: Aplicar las medidas de seguridad recomendadas por Oracle o parches proporcionados.

Oracle GlassFish Server URL normalization Denial of Service

Gravedad	CVSSv3	CVSSv2	ID
High	7.5	-	110612

Descripción: Esta vulnerabilidad permite a un atacante remoto realizar un ataque de denegación de servicio en el sistema afectado mediante la manipulación de URLs.

Solución: Aplicar las medidas de seguridad recomendadas por Oracle o parches proporcionados.

SSL Certificate Signed Using Weak Hashing Algorithm

Gravedad	CVSSv3	CVSSv2	ID
High	7.5	4.9	35291

Descripción: Esta vulnerabilidad indica que el certificado SSL está firmado utilizando un algoritmo de hash débil, lo que puede comprometer la integridad del certificado.

Solución: Renovar el certificado SSL utilizando un algoritmo de hash más seguro.

SSL Medium Strength Cipher Suites Supported (SWEET32)

Gravedad	CVSSv3	CVSSv2	ID
High	7.5	6.1	42873

Descripción: Esta vulnerabilidad indica que el servidor admite suites de cifrado de longitud media, lo que puede exponer la comunicación a ataques criptográficos.

Solución: Deshabilitar las suites de cifrado de longitud media y utilizar cifrados más fuertes.

MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

Gravedad	CVSSv3	CVSSv2	ID

Gravedad	CVSSv3	CVSSv2	ID
High	9.3*	9.7	58435

Descripción: Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema afectado a través de una explotación de tipo ejecución remota de código.

Solución: Aplicar el parche de seguridad proporcionado por Microsoft.

Nivel Medio

MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.8	6.0	90510

Descripción: Esta vulnerabilidad afecta a los protocolos remotos SAM y LSAD y permite a un atacante realizar ataques de tipo man-in-the-middle en la comunicación.

Solución: Aplicar el parche de seguridad proporcionado por Microsoft.

Remote Desktop Protocol Server Man-in-the-Middle Weakness

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	2.5	18405

Descripción: Esta vulnerabilidad indica una debilidad en el protocolo Remote Desktop Protocol (RDP) que podría ser explotada por un atacante para realizar ataques de tipo man-in-the-middle.

Solución: Utilizar un canal seguro como VPN o configurar RDP con autenticación de red.

SSL Certificate Cannot Be Trusted

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	-	51192

Descripción: Esta vulnerabilidad indica que el certificado SSL del sitio web no es confiable, lo que puede indicar un problema de certificación o una autoridad de certificación no confiable.

Solución: Renovar el certificado SSL de una autoridad de certificación confiable.

SSL Self-Signed Certificate

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	-	57582

Descripción: Esta vulnerabilidad indica que el certificado SSL del sitio web es auto-firmado, lo que puede indicar un problema de certificación o falta de confiabilidad en el certificado.

Solución: Obtener un certificado SSL de una autoridad de certificación confiable.

TLS Version 1.0 Protocol Detection

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	-	104743

Descripción: Esta vulnerabilidad indica la detección de la versión 1.0 del protocolo TLS, que es conocida por tener vulnerabilidades de seguridad.

Solución: Desactivar el soporte para TLS 1.0 y migrar a versiones más seguras como TLS 1.2 o TLS 1.3.

TLS Version 1.1 Protocol Deprecated

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	-	157288

Descripción: Esta vulnerabilidad indica que la versión 1.1 del protocolo TLS está marcada como obsoleta, lo que puede exponer el sistema a vulnerabilidades conocidas.

Solución: Desactivar el soporte para TLS 1.1 y migrar a versiones más seguras como TLS 1.2 o TLS 1.3.

ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.1	3.0	108752

Descripción: Esta vulnerabilidad afecta a versiones específicas de ManageEngine Desktop Central y permite a un atacante llevar a cabo diversas acciones maliciosas.

Solución: Actualizar a una versión parcheada de ManageEngine Desktop Central.

SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Gravedad	CVSSv3	CVSSv2	ID

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.9	6.7	187315

Descripción: Esta vulnerabilidad permite a un atacante truncar el prefijo SSH Terrapin, lo que puede resultar en una reducción de la seguridad.

Solución: Aplicar las actualizaciones y configuraciones de seguridad adecuadas.

SSL Anonymous Cipher Suites Supported

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.9	3.6	31705

Descripción: Esta vulnerabilidad indica que el servidor admite suites de cifrado anónimas, lo que puede exponer la comunicación a ataques criptográficos.

Solución: Deshabilitar las suites de cifrado anónimas y utilizar cifrados más seguros.

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.9	3.6	65821

Descripción: Esta vulnerabilidad indica que el servidor admite suites de cifrado RC4, que son conocidas por tener vulnerabilidades de seguridad.

Solución: Deshabilitar las suites de cifrado RC4 y utilizar cifrados más seguros.

Elasticsearch Unrestricted Access Information Disclosure

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.3	-	101025

Descripción: Esta vulnerabilidad indica que Elasticsearch permite el acceso no restringido, lo que puede exponer información sensible.

Solución: Configurar adecuadamente los permisos de acceso en Elasticsearch.

SMB Signing not required

Gravedad	CVSSv3	CVSSv2	ID

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.3	-	57608

Descripción: Esta vulnerabilidad indica que SMB Signing no está requerido, lo que puede exponer el sistema a ataques de suplantación de identidad.

Solución: Configurar SMB Signing para que sea obligatorio.

SSL Certificate Expiry

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.3	-	15901

Descripción: Esta vulnerabilidad indica que el certificado SSL del sitio web está próximo a expirar, lo que puede resultar en una interrupción del servicio.

Solución: Renovar el certificado SSL antes de su fecha de vencimiento.

SSL Certificate with Wrong Hostname

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.3	-	45411

Descripción: Esta vulnerabilidad indica que el certificado SSL del sitio web tiene un nombre de host incorrecto, lo que puede indicar un problema de configuración o una posible suplantación de identidad.

Solución: Corregir la configuración del certificado SSL para que coincida con el nombre de host del sitio web.

Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Gravedad	CVSSv3	CVSSv2	ID
Medium	4.0	-	58453

Descripción: Esta vulnerabilidad indica que Terminal Services no utiliza solo la Autenticación de Nivel de Red (NLA), lo que puede exponer el sistema a ataques de fuerza bruta.

Solución: Configurar Terminal Services para utilizar exclusivamente la Autenticación de Nivel de Red (NLA).

Elasticsearch 'source' Parameter RCE

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.8*	9.7	76572

Descripción: Esta vulnerabilidad afecta a Elasticsearch y permite a un atacante ejecutar código arbitrario a través de un parámetro 'source'.

Solución: Actualizar a una versión parcheada de Elasticsearch.

Terminal Services Encryption Level is Medium or Low

Gravedad	CVSSv3	CVSSv2	ID
Medium	4.3*	-	57690

Descripción: Esta vulnerabilidad indica que el nivel de cifrado de Terminal Services es medio o bajo, lo que puede exponer la comunicación a ataques criptográficos.

Solución: Configurar el nivel de cifrado de Terminal Services en Alto para utilizar cifrados más seguros.

Nivel Bajo

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Gravedad	CVSSv3	CVSSv2	ID
Low	3.7	4.5	83875

Descripción: Esta vulnerabilidad indica que el tamaño del módulo Diffie-Hellman en el intercambio de claves SSL/TLS es menor o igual a 1024 bits, lo que puede permitir a un atacante realizar un ataque de fuerza bruta para descifrar la comunicación.

Solución: Aumentar el tamaño del módulo Diffie-Hellman a más de 1024 bits y preferiblemente a 2048 bits o más.

Terminal Services Encryption Level is not FIPS-140 Compliant

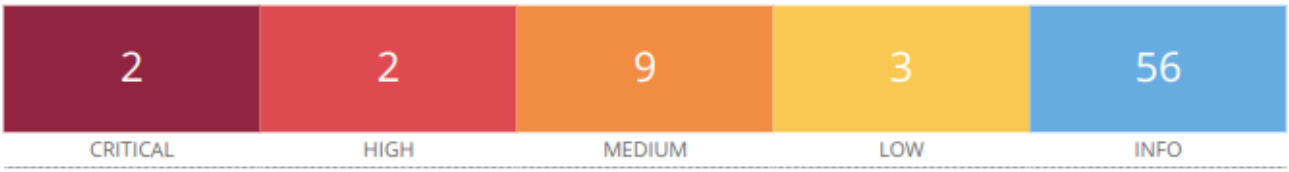
Gravedad	CVSSv3	CVSSv2	ID
Low	2.6*	-	30218

Descripción: Esta vulnerabilidad indica que el nivel de cifrado de Terminal Services no cumple con los estándares FIPS-140, lo que puede implicar una debilidad en la seguridad del sistema.

Solución: Configurar el nivel de cifrado de Terminal Services para que cumpla con los estándares FIPS-140.

Servidor 2 - Linux

Resumen gráfico de vulnerabilidades encontradas



CVSS más alto obtenido: **10**

Nivel Crítico

ProFTPD mod_copy Information Disclosure

Gravedad	CVSSv3	CVSSv2	ID
Critical	9.8	7.4	84215

Descripción: Esta vulnerabilidad en el módulo ProFTPD mod_copy permite a un atacante obtener información sensible de forma no autorizada.

Solución: Aplicar el parche de seguridad proporcionado por ProFTPD y/o deshabilitar el módulo mod_copy si no es necesario.

Drupal Coder Module Deserialization RCE

Gravedad	CVSSv3	CVSSv2	ID
Critical	10.0*	-	92626

Descripción: Esta vulnerabilidad en el módulo Drupal Coder permite a un atacante ejecutar código arbitrario en el servidor afectado a través de una deserialización no segura de datos.

Solución: Actualizar a una versión parcheada del módulo Drupal Coder y revisar las configuraciones de seguridad de Drupal para mitigar el riesgo de deserialización no segura.

Nivel Alto

SSL Medium Strength Cipher Suites Supported (SWEET32)

Gravedad	CVSSv3	CVSSv2	ID
High	7.5	6.1	42873

Descripción: Esta vulnerabilidad indica que el servidor SSL/TLS admite suites de cifrado de fuerza media, lo que puede permitir a un atacante realizar ataques de cifrado de texto plano para comprometer la comunicación.

Solución: Deshabilitar o eliminar las suites de cifrado de fuerza media y actualizar la configuración del servidor SSL/TLS para utilizar suites de cifrado más seguras.

Drupal Database Abstraction API SQLi

Gravedad	CVSSv3	CVSSv2	ID
High	7.5*	7.4	78515

Descripción: Esta vulnerabilidad en la API de Abstracción de Base de Datos de Drupal permite a un atacante realizar ataques de inyección SQL (SQLi) y comprometer la integridad y confidencialidad de la base de datos.

Solución: Aplicar el parche de seguridad proporcionado por Drupal para corregir la vulnerabilidad SQLi en la API de Abstracción de Base de Datos.

Nivel Medio

IP Forwarding Enabled

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	4.9	50686

Descripción: Esta vulnerabilidad indica que el reenvío de IP está habilitado en el sistema, lo que puede permitir que un atacante realice ataques de reenvío de paquetes y redirija el tráfico de red a destinos no autorizados.

Solución: Deshabilitar el reenvío de IP en el sistema si no es necesario para el funcionamiento normal.

SSL Certificate Cannot Be Trusted

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	-	51192

Descripción: Esta vulnerabilidad indica que el certificado SSL no se puede considerar confiable, lo que puede indicar un certificado autofirmado o emitido por una autoridad de certificación no confiable.

Solución: Obtener un certificado SSL firmado por una autoridad de certificación confiable y reemplazar el certificado no confiable.

SSL Self-Signed Certificate

Gravedad	CVSSv3	CVSSv2	ID

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	-	57582

Descripción: Esta vulnerabilidad indica que el certificado SSL del servidor es autofirmado, lo que puede no ser confiable para los clientes que intentan establecer una conexión segura.

Solución: Obtener un certificado SSL firmado por una autoridad de certificación confiable y reemplazar el certificado autofirmado.

TLS Version 1.0 Protocol Detection

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	-	104743

Descripción: Esta vulnerabilidad indica que el sistema es compatible con el protocolo TLS versión 1.0, que es conocido por tener vulnerabilidades de seguridad y debilidades criptográficas.

Solución: Deshabilitar el soporte para TLS 1.0 y usar versiones más seguras del protocolo TLS, como TLS 1.2 o superior.

TLS Version 1.1 Protocol Deprecated

Gravedad	CVSSv3	CVSSv2	ID
Medium	6.5	-	157288

Descripción: Esta vulnerabilidad indica que el sistema está utilizando el protocolo TLS versión 1.1, que está marcado como obsoleto debido a vulnerabilidades de seguridad y debilidades criptográficas.

Solución: Actualizar a versiones de protocolo TLS más recientes y seguras, como TLS 1.2 o TLS 1.3.

SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.9	6.7	187315

Descripción: Esta vulnerabilidad en SSH indica una debilidad en el manejo de los prefijos de Terrapin, lo que podría permitir a un atacante truncar los prefijos de SSH y evadir restricciones de seguridad.

Solución: Aplicar el parche de seguridad proporcionado por el proveedor de SSH o actualizar a una versión corregida del software.

Apache Multiviews Arbitrary Directory Listing

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.3	2.2	10704

Descripción: Esta vulnerabilidad indica que el servidor Apache está configurado para permitir listados de directorios arbitrarios, lo que podría exponer información sensible de los archivos en el servidor.

Solución: Deshabilitar la opción de Multiviews en la configuración de Apache o configurar adecuadamente las reglas de acceso para evitar la enumeración de directorios.

SMB Signing not required

Gravedad	CVSSv3	CVSSv2	ID
Medium	5.3	-	57608

Descripción: Esta vulnerabilidad indica que el servidor SMB no requiere la firma de mensajes (SMB Signing), lo que puede permitir a un atacante realizar ataques de manipulación de datos en la comunicación SMB.

Solución: Habilitar SMB Signing para garantizar la integridad y autenticidad de los mensajes SMB.

SSH Weak Algorithms Supported

Gravedad	CVSSv3	CVSSv2	ID
Medium	4.3*	-	90317

Descripción: Esta vulnerabilidad indica que el servidor SSH admite algoritmos de cifrado débiles o desactualizados, lo que puede comprometer la seguridad de la comunicación SSH.

Solución: Deshabilitar los algoritmos de cifrado débiles y utilizar algoritmos de cifrado más seguros y actualizados en la configuración del servidor SSH.

Nivel Bajo

SSH Server CBC Mode Ciphers Enabled

Gravedad	CVSSv3	CVSSv2	ID
Low	3.7	3.6	70658

Descripción: Esta vulnerabilidad indica que el servidor SSH está configurado para admitir cifrados en modo CBC (Cipher Block Chaining), que pueden ser vulnerables a ataques de cifrado en bloque.

Solución: Deshabilitar los cifrados en modo CBC y utilizar modos de cifrado más seguros, como GCM (Galois/Counter Mode) o CTR (Counter Mode).

SSH Weak Key Exchange Algorithms Enabled

Gravedad	CVSSv3	CVSSv2	ID
Low	3.7	-	153953

Descripción: Esta vulnerabilidad indica que el servidor SSH está configurado para admitir algoritmos de intercambio de claves débiles, lo que puede comprometer la seguridad de la comunicación SSH.

Solución: Deshabilitar los algoritmos de intercambio de claves débiles y utilizar algoritmos más seguros, como Diffie-Hellman (DH) o Elliptic Curve Diffie-Hellman (ECDH).

SSH Weak MAC Algorithms Enabled

Gravedad	CVSSv3	CVSSv2	ID
Low	2.6*	-	71049

Descripción: Esta vulnerabilidad indica que el servidor SSH está configurado para admitir algoritmos de código de autenticación de mensajes (MAC) débiles, lo que puede comprometer la integridad de la comunicación SSH.

Solución: Deshabilitar los algoritmos de MAC débiles y utilizar algoritmos más seguros, como HMAC-SHA256 o HMAC-SHA512.

Conclusiones y Recomendaciones

En base a los resultados obtenidos mediante el escaneo superficial básico de puertos comunes, podemos determinar que los dos

Glosario de Términos

- **Puerto:**
  Un puerto es un punto de conexión en un dispositivo informático que permite la comunicación entre diferentes programas o dispositivos. Es como una puerta de entrada o salida que facilita el intercambio de datos entre el dispositivo y su entorno. En un ordenador existen los puertos del 0 al 65535.

- **MAC (Dirección MAC):**
  La Dirección MAC (Media Access Control) es un identificador único asignado a una interfaz de red de un dispositivo. Funciona como una "huella digital" para dispositivos conectados a una red, permitiendo la identificación precisa de cada uno de ellos.

- **Protocolo:**
  Un protocolo es un conjunto de reglas y convenciones que determinan cómo se comunican entre sí los dispositivos y sistemas informáticos en una red. Define el formato, la secuencia y las acciones a tomar durante la transmisión de datos para asegurar una comunicación efectiva y confiable.

- **Vulnerabilidad:**
  Una vulnerabilidad es una debilidad o fallo en un sistema informático que puede ser explotado por un atacante para comprometer la seguridad y el funcionamiento del sistema. Las vulnerabilidades pueden surgir debido a errores de diseño, configuración incorrecta o falta de actualizaciones de software, entre otras causas.

- **Exploit:**
  Un exploit es un programa o técnica diseñada para aprovechar una vulnerabilidad específica en un sistema informático. Se utiliza para comprometer la seguridad del sistema, ejecutar código malicioso o realizar acciones no autorizadas, lo que puede provocar daños o comprometer la integridad de los datos.

- **Autenticación de Mensajes:**
  La autenticación de mensajes es un proceso que verifica la integridad y la autenticidad de los datos transmitidos entre sistemas o dispositivos. Se utiliza para garantizar que los mensajes no hayan sido alterados o manipulados durante la transmisión y que provengan de una fuente confiable.

- **Algoritmo de Encriptación:**
  Un algoritmo de encriptación es un conjunto de reglas matemáticas y operaciones que se utilizan para codificar datos de forma que solo puedan ser decodificados por aquellos que tengan la clave de desencriptación adecuada. Se emplea para proteger la confidencialidad y la seguridad de la información en las comunicaciones electrónicas.

- **Funciones Hash Criptográficas:**
  Las funciones hash criptográficas son algoritmos matemáticos que transforman datos de entrada en una cadena de caracteres de longitud fija. Estas funciones se utilizan en seguridad informática para verificar la integridad de los datos y generar resúmenes únicos para identificar los archivos o mensajes.

- **HMAC-SHA256:**
  HMAC-SHA256 es un algoritmo de autenticación de mensajes basado en funciones hash criptográficas. Se utiliza para garantizar la integridad y autenticidad de los datos transmitidos a través de una red, proporcionando una capa adicional de seguridad contra la manipulación o falsificación de datos.

- **HMAC-SHA512:**
  HMAC-SHA512 es similar a HMAC-SHA256, pero utiliza una longitud de hash más larga para mayor seguridad. Proporciona una autenticación robusta y una protección adicional contra ataques de fuerza bruta y manipulación de datos.

- **SSH (Secure Shell):**
  Secure Shell (SSH) es un protocolo de red que permite a los usuarios acceder de forma segura a un dispositivo remoto a través de una conexión cifrada. Se utiliza comúnmente para administrar servidores y realizar tareas de mantenimiento en sistemas informáticos de forma remota, proporcionando una capa adicional de seguridad mediante la encriptación de datos durante la transmisión.

- **Fuerza Bruta:**
  La fuerza bruta es un método utilizado en ciberseguridad para descifrar contraseñas o claves de forma sistemática y exhaustiva, probando todas las combinaciones posibles hasta encontrar la correcta. Es un enfoque intensivo en recursos que puede ser efectivo pero requiere tiempo y poder computacional.

- **Firewall:**
  Un firewall es un dispositivo o software diseñado para controlar y filtrar el tráfico de red entrante y saliente en función de un conjunto de reglas de seguridad predefinidas. Se utiliza para proteger los sistemas informáticos contra amenazas externas y evitar accesos no autorizados o actividades maliciosas.

- **Inyección de Código:**
  La inyección de código es una técnica utilizada por los atacantes para insertar y ejecutar código malicioso en una aplicación o sistema informático. Puede aprovechar vulnerabilidades en el software o la falta de validación de datos para manipular el comportamiento del programa y comprometer la seguridad del sistema.

- **Cifrado de Extremo a Extremo:**
  El cifrado de extremo a extremo es un método de encriptación que protege los datos durante su transmisión desde el remitente hasta el destinatario, impidiendo que terceros intercepten o accedan a la información. Se utiliza comúnmente en servicios de mensajería y comunicaciones electrónicas para garantizar la privacidad y la confidencialidad de los mensajes.

- **Autenticación Multifactorial:**
  La autenticación multifactorial es un método de verificación de identidad que requiere múltiples formas de autenticación para conceder acceso a un sistema informático o servicio. Combina dos o más factores de autenticación, como contraseñas, tokens de seguridad, huellas dactilares o reconocimiento facial, para aumentar la seguridad y reducir el riesgo de acceso no autorizado.

Referencias

Antonio López INCIBE. (2023). CVSS v3.0.
Recuperado el 1 de Abril 2024, de https://www.incibe.es/incibe-cert/blog/cvss3-0

Grupo 3

- **Sergio Guerrero Merlo**
- **Juan Manuel Cumbrera López**
- **Christian Romero Oliva**