Tecnológico de Monterrey

Reporte técnico

15/06/2023

Por

Erik Ernesto Ocegueda Sambrano A01639749

Luis Jesús Castillo Goyenechea A01275697

Paola Enríquez Reyes A01741055

Juan Pablo Bernal Lafarga A01742342

Kun Pan A01641987

Materia:

Análisis de criptografía y seguridad (Grupo 301)

Profesores:

Dr. Francisco Javier Alvarado Chacón

Oscar Eduardo Labrada Gómez

- Introducción

En este reporte técnico presentaremos diversos puntos importantes en cuanto a nuestra investigación respecto a la empresa a la que logramos contactar para llevar a cabo el análisis de seguridad gracias a herramientas computacionales y con apoyo de los conceptos vistos en clase durante nuestro curso de 5 semanas. Sin embargo en esta introducción nos gustaría dar a conocer un poco más sobre el programa Nessus, el cual fue nuestra principal herramienta durante el desarrollo del proyecto, además de algunos conceptos necesarios para una mejor comprensión de lo que se presentará en este reporte.

Nessus

Este es un programa de escaneo de seguridad de red, bastante conocido y utilizado, que ayuda a identificar vulnerabilidades en sistemas informáticos y redes. Nessus realiza análisis exhaustivos en busca de posibles puntos débiles en dispositivos, sistemas operativos, aplicaciones y servicios de red. Su principal objetivo es proporcionar a los administradores de sistemas y a los profesionales de seguridad, en este caso nosotros como equipo de investigación, una visión clara de la postura de seguridad de sus activos digitales. El programa realiza una variedad de pruebas automatizadas, como escaneos de puertos, detección de servicios y análisis de configuraciones, para identificar posibles vulnerabilidades conocidas.

Nessus directamente genera un informe detallado que nos enumera las vulnerabilidades encontradas, junto con recomendaciones para solucionarlas y ya está en nuestra responsabilidad hacer una investigación más profunda y presentar en este caso un plan viable para la empresa.

Por otro lado, es también parte de nuestro objetivo, el concientizar la importancia de la ciberseguridad, ya que pudimos notar también durante la búsqueda de empresa que realmente son pocas las empresas que saben o entienden de la importancia del mismo. La concientización de la ciberseguridad en el ámbito empresarial es crucial para proteger su información confidencial, siendo los principales: activos digitales, salvaguardar la información confidencial y mantener la continuidad de las operaciones.

Es fundamental educar a los empleados sobre las amenazas y riesgos cibernéticos que enfrenta la empresa, y no únicamente a los encargados de la parte tecnológica y estadística de la empresa. Además es recomendable que se establezcan políticas claras de seguridad cibernética que definan las responsabilidades y expectativas de los empleados en relación con la protección de la información y los sistemas de la empresa. También es importante saber sobre las mismas vulnerabilidades que se pueden encontrar en la empresa para trabajarlo y así optar por mantener los sistemas, aplicaciones y dispositivos actualizados

con los últimos parches y actualizaciones de seguridad. Esto ayuda a cerrar las brechas de seguridad conocidas y reduce las vulnerabilidades explotables.

La concientización de la ciberseguridad en empresas debe ser un esfuerzo continuo, por lo que definitivamente no hay que esperar que esté se cumpla en un periodo de tiempo breve. Ya que se tendría que buscar involucrar a todos los niveles de la organización, desde los empleados de base hasta los altos directivos. Al fomentar una cultura de seguridad cibernética, las empresas pueden fortalecer su postura de seguridad y minimizar el riesgo de violaciones de datos y ataques cibernéticos que podrían tener graves consecuencias financieras y reputacionales.

- Análisis de riesgos

Host

192.168.0.9

1. Severity: critical - SSL Version 2 and 3 Protocol Detection:
Esta vulnerabilidad implica la detección de los protocolos SSL versión 2 y 3 en un host. Estos protocolos son considerados inseguros debido a las vulnerabilidades conocidas que presentan. La recomendación es desactivar o bloquear el uso de SSLv2 y SSLv3 y migrar a versiones más seguras como TLS.

2. Severity: critical - Microsoft DNS Server Remote Code Execution (SIGRed):
Esta vulnerabilidad se refiere a una falla crítica en el Servidor DNS de Microsoft que permite la ejecución remota de código. Un atacante puede explotar esta vulnerabilidad para tomar control total del servidor DNS. La recomendación es aplicar los parches y actualizaciones correspondientes proporcionados por Microsoft y asegurarse de mantener el sistema actualizado.

3. Severity: critical - Unsupported Web Server Detection:
Esta vulnerabilidad indica que se ha detectado un servidor web incompatible o desactualizado en el host. Los servidores web no compatibles pueden tener vulnerabilidades conocidas y no recibir actualizaciones de seguridad. Se recomienda migrar a una versión compatible o un servidor web más seguro y mantenerlo actualizado.

4. Severity: critical - Unsupported Windows OS (remote): Esta vulnerabilidad señala que se ha detectado un sistema operativo Windows no compatible o desactualizado en el host. Los sistemas operativos no compatibles pueden tener vulnerabilidades conocidas y no recibir actualizaciones de seguridad. Se recomienda migrar a una versión compatible o un sistema operativo más reciente que reciba soporte y actualizaciones.

5. Severity: high - SSL Certificate Signed Using Weak Hashing Algorithm:
Esta vulnerabilidad implica que el certificado SSL utilizado en el host ha sido firmado utilizando un algoritmo de hashing débil. Los algoritmos de hashing débiles pueden ser vulnerables a ataques de fuerza bruta o colisión. Se recomienda renovar el certificado SSL y utilizar algoritmos de hashing seguros, como SHA-256 o SHA-3.

6. Severity: high - SSL Medium Strength Cipher Suites Supported (SWEET32):
Esta vulnerabilidad indica que el host admite suites de cifrado SSL de fuerza media, conocidas como SWEET32. Estas suites de cifrado son susceptibles a ataques de criptoanálisis y pueden comprometer la confidencialidad de la comunicación. Se recomienda desactivar o eliminar las suites de cifrado débiles y utilizar suites de cifrado más seguras.

Host
192.168.0.30

1. Severity: critical - Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper): Esta vulnerabilidad implica una falla crítica en el servicio de Colas de Mensajes de Microsoft (Microsoft Message Queuing) que permite la ejecución remota de código. Un atacante puede aprovechar esta vulnerabilidad para tomar control total del sistema afectado. La recomendación es aplicar los parches y actualizaciones proporcionados por Microsoft para corregir esta vulnerabilidad y proteger el sistema.

2. Severity: critical - Unsupported Windows OS (remote): Esta vulnerabilidad señala que se ha detectado un sistema operativo Windows no compatible o desactualizado en el host. Los sistemas operativos no compatibles pueden tener vulnerabilidades conocidas y no recibir actualizaciones de seguridad. Se recomienda migrar a una

versión compatible o un sistema operativo más reciente que reciba soporte y actualizaciones.

3. Severity: critical - Microsoft Windows 8 Unsupported Installation Detection: Esta vulnerabilidad se refiere a la detección de una instalación no compatible o desactualizada del sistema operativo Microsoft Windows 8 en el host. Los sistemas operativos no compatibles pueden tener vulnerabilidades conocidas y no recibir actualizaciones de seguridad. Se recomienda migrar a una versión compatible y recibir soporte continuo para mantener la seguridad del sistema.

4. Severity: high - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check): Esta vulnerabilidad se refiere a la actualización de seguridad MS17-010 de Microsoft para el Servidor SMB de Windows que aborda múltiples vulnerabilidades, incluyendo EternalBlue, EternalChampion, EternalRomance, EternalSynergy, WannaCry, EternalRocks, Petya, etc. Estas vulnerabilidades permiten la ejecución remota de código y propagación de malware. La recomendación es aplicar urgentemente la actualización de seguridad MS17-010 y asegurarse de que los sistemas estén protegidos contra estas amenazas conocidas.

Host

192.168.0.13

1. Severidad: Media Vulnerabilidad - SSL Certificate Cannot Be Trusted: El certificado SSL del host no puede ser considerado confiable, lo que implica que la comunicación entre el cliente y el servidor puede ser interceptada o manipulada por un atacante. Recomendación: Se recomienda reemplazar el certificado SSL actual por uno emitido por una autoridad de certificación confiable. Esto garantizará que la comunicación encriptada sea segura y confiable.

2. Severidad: Media Vulnerabilidad - SSL Self-Signed Certificate: El certificado SSL utilizado por el host es autofirmado, lo que significa que no ha sido emitido por una autoridad de certificación confiable. Esto puede llevar a que los clientes no confíen en la identidad del servidor y se expongan a ataques de suplantación de identidad. Recomendación: Se recomienda obtener un certificado SSL emitido por una autoridad de certificación confiable. Al utilizar un certificado confiable, se asegura que los clientes puedan verificar la autenticidad del servidor y establecer una comunicación segura.

3. Severidad: Media Vulnerabilidad - SMB signing not required: La firma SMB (Server Message Block) no está habilitada o requerida en el host. Esto puede permitir a un atacante interceptar o modificar los datos transmitidos a través del protocolo SMB, lo que potencialmente podría llevar a la ejecución de ataques de tipo man-in-the-middle o manipulación de datos. Recomendación: Se recomienda habilitar la firma SMB en el host. Esto garantiza la integridad y autenticidad de los datos transmitidos a través del protocolo SMB, evitando así posibles ataques de manipulación o suplantación.

4. Severidad: Media Vulnerabilidad - SSL Certificate with Wrong Hostname: El certificado SSL utilizado en el host tiene un nombre de host incorrecto. Esto puede indicar una configuración errónea o maliciosa, lo que puede permitir ataques de suplantación de identidad o phishing. Recomendación: Se recomienda corregir la configuración del certificado SSL para que coincida con el nombre de host correcto del servidor. Esto asegura que los clientes puedan verificar la identidad del host y evita posibles ataques de suplantación o phishing.

Host

192.168.0.44

1. Severity: high - SSL Medium Strength Cipher Suites Supported (SWEET32): El host remoto admite el uso de cifrados SSL que ofrecen un nivel de encriptación de fuerza media. Nessus considera fuerza media a cualquier encriptación que utilicé longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el conjunto de

encriptación 3DES. Es importante tener en cuenta que es considerablemente más fácil evitar la encriptación de fuerza media si el atacante se encuentra en la misma red física. Se recomienda reconfigurar la aplicación afectada para evitar el uso de cifrados de fuerza media.

Host

192.168.0.52

1. Severity: critical - SSL Version 2 and 3 Protocol Detection: El servicio remoto acepta conexiones cifradas con SSL 2.0 y/o SSL 3.0, que tienen vulnerabilidades criptográficas. Estas vulnerabilidades permiten a un atacante realizar ataques de intermediario o descifrar comunicaciones. Se recomienda desactivar por completo estos protocolos, ya que SSL 3.0 ya no es seguro según NIST y ninguna versión de SSL cumple con los estándares de criptografía sólida de PCI SSC. Se recomienda consultar la documentación de la aplicación para desactivar SSL 2.0 y 3.0. En su lugar, utiliza TLS 1.2 (con conjuntos de cifrado aprobados) o una versión superior.

2. Severity: high - SSL Medium Strength Cipher Suites Supported (SWEET32): Se refiere al soporte de suites de cifrado de fuerza media en el protocolo SSL/TLS. Esta vulnerabilidad se debe a la debilidad del algoritmo de cifrado Triple DES (3DES) cuando se utiliza en modo de cifrado de flujo.El cifrado 3DES es vulnerable a un ataque de criptoanálisis conocido como "ataque de cumpleaños" cuando se utiliza en un contexto de larga duración y grandes volúmenes de datos. Este ataque aprovecha la probabilidad estadística de que dos bloques de datos cifrados con una clave de 3DES sean idénticos. A medida que se cifran más bloques de datos, aumenta la posibilidad de que se produzcan colisiones. Un atacante podría utilizar esta debilidad para recuperar información sensible. Se recomienda deshabilitar las suites de cifrado débiles que utilizan 3DES y utilizar algoritmos de cifrado más fuertes, como Advanced Encryption Standard (AES). Se debe configurar el servidor SSL/TLS para priorizar los algoritmos de cifrado seguros y eliminar cualquier suite de cifrado que utilicé 3DES. Además, se recomienda utilizar una versión actualizada del protocolo TLS, como TLS 1.2 o una versión superior, que tenga algoritmos de cifrado más fuertes y no sea vulnerable a los ataques asociados con 3DES.

3. Severity: high - Apache Tomcat 7.0.x < 7.0.57 Multiple Vulnerabilities (POODLE): "POODLE" (Padding Oracle On Downgraded Legacy Encryption) que afectan a las versiones antiguas de Apache Tomcat 7.0.x hasta la versión 7.0.57. POODLE aprovecha una debilidad en el protocolo SSL 3.0 para realizar ataques de intermediario y descifrar comunicaciones cifradas. SSL 3.0 utiliza un modo de cifrado vulnerable conocido como "cifrado en bloque" que no proporciona autenticación de integridad de mensajes. Esto permite a un atacante realizar ataques de inyección de contenido malicioso en una conexión cifrada y descifrar información sensible. Se recomienda desactivar completamente el soporte para SSL 3.0 en Apache Tomcat 7.0.x. En su lugar, se debe utilizar el protocolo TLS (Transport Layer Security) y configurar Tomcat para utilizar versiones seguras de TLS, como TLS 1.2 o superior.

4. Severity: high - Apache Tomcat 7.0.x < 7.0.60 Multiple Vulnerabilities (FREAK): "FREAK" (Factoring RSA Export Keys) que afectaron a las versiones antiguas de Apache Tomcat 7.0.x hasta la versión 7.0.60. FREAK es una vulnerabilidad que explota el soporte de cifrado débil en los protocolos SSL/TLS. Se basa en un antiguo requisito de exportación de cifrado implementado en algunas implementaciones de SSL/TLS, que permitía a los gobiernos acceder a claves de cifrado débiles. Los atacantes pueden aprovechar esta vulnerabilidad para realizar ataques de intermediario y descifrar la comunicación cifrada. Se recomienda que para mitigar la vulnerabilidad FREAK actualiza Apache Tomcat a una versión posterior a la 7.0.60, ya que se corrigieron las vulnerabilidades relacionadas. La versión 7.0.60 o superior soluciona el problema y elimina el soporte para cifrados débiles.

5. Severity: high -Java JMX Agent Insecure Configuration: En el host remoto, un agente Java JMX está configurado sin autenticación SSL ni contraseña. Esto permite a un atacante remoto y no autenticado conectarse al agente JMX y controlar la aplicación Java que lo ha habilitado. Además, esta configuración insegura permite al atacante crear objetos MBean utilizando URL arbitrarias, lo que le permite ejecutar código arbitrario en el host remoto con el contexto de seguridad de la máquina virtual Java. Se recomienda habilitar la autenticación de cliente SSL o de contraseña para el agente JMX.

Host

192.168.0.205

1. Severity: Critical - SSL Version 2 and 3 Protocol Detection: El servicio remoto acepta conexiones cifradas con SSL 2.0 y/o SSL 3.0, que tienen vulnerabilidades criptográficas. Estas vulnerabilidades permiten a un atacante realizar ataques de intermediario o descifrar comunicaciones. Se recomienda desactivar por completo estos protocolos, ya que SSL 3.0 ya no es seguro según NIST y ninguna versión de SSL cumple con los estándares de criptografía sólida de PCI SSC.

2. Severity: high - SSL Certificate Signed Using Weak Hashing Algorithm: El servicio remoto utiliza un certificado SSL firmado con un algoritmo de hash débil, como MD2, MD4, MD5 o SHA1. Estos algoritmos son vulnerables a ataques de colisión, lo que permite a un atacante generar un certificado falso con la misma firma. Esto podría permitir al atacante suplantar al servicio afectado. Se considera vulnerable cualquier cadena de certificados SSL firmada con SHA-1 y con fecha de vencimiento posterior al 1 de enero de 2017, de acuerdo con la eliminación gradual de Google del algoritmo SHA-1.Se recomienda contactar a la Autoridad de Certificación (Certificate Authority) para solicitar la emisión del certificado SSL.

3. Severity:high - SSL Medium Strength Cipher Suites Supported (SWEET32):
   El host remoto admite el uso de cifrados SSL que ofrecen un nivel de encriptación de fuerza media. Nessus considera fuerza media a cualquier encriptación que utilicé longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el conjunto de encriptación 3DES.Es importante tener en cuenta que es considerablemente más fácil evitar la encriptación de fuerza media si el atacante se encuentra en la misma red física

- Objetivo de mitigación

El objetivo de este plan de mitigación es reducir los impactos negativos de la situación actual que puedan llegar a poner en algún estado crítico a la empresa y prevenir futuros incidentes similares. Buscamos garantizar la seguridad y el bienestar de las personas, minimizar los daños materiales y preservar el medio ambiente.

- Estrategias de mitigación

1. Se realiza un análisis exhaustivo de los riesgos asociados a la situación actual y futuros posibles escenarios. Esto incluye la identificación de posibles amenazas, como desastres naturales, fallos en la infraestructura, ciberataques u otros eventos que puedan afectar la seguridad y el bienestar de las personas, así como los activos y el medio ambiente. Además, evaluaremos la probabilidad de ocurrencia de cada riesgo y su impacto potencial. Esta evaluación nos permitirá priorizar los riesgos y asignar recursos de manera efectiva para abordarlos.
2. Tomar acciones para prevenir o reducir los riesgos identificados. Estas medidas pueden incluir mejoras en la infraestructura existente, como fortalecer edificaciones, implementar sistemas de drenaje o establecer barreras de protección. Asimismo, se pueden adoptar tecnologías más seguras, como sistemas de seguridad informática, sistemas de alerta temprana o sistemas de monitoreo ambiental. Además, se capacitará al personal en prácticas de seguridad, incluyendo la formación en protocolos de respuesta a emergencias y la promoción de una cultura de seguridad en toda la organización.
3. La sensibilización y educación son elementos fundamentales para lograr la participación activa de la comunidad y promover prácticas seguras. Llevaremos a cabo campañas de divulgación que abordarán diferentes aspectos, como la concienciación sobre los riesgos existentes, la promoción de comportamientos seguros, la difusión de información sobre cómo actuar en caso de emergencia y la capacitación en habilidades específicas relacionadas con la mitigación de riesgos. Estas campañas se desarrollarán a través de diversos canales, como medios de comunicación locales, redes sociales, boletines informativos y la organización de reuniones comunitarias, talleres y simulacros de emergencia.

- Recursos para poder llevar a cabo el plan de mitigación

Para cumplir lo propuesto anteriormente, en las estrategias de mitigación. Debemos ser conscientes de los recursos requeridos para conseguirlos.

1. Personal capacitado: Asignaremos un equipo especializado encargado de desarrollar e implementar el plan de mitigación. Este equipo contará con expertos en gestión de riesgos, técnicos especializados y profesionales en comunicación.
2. Fondos adecuados: Destinaremos recursos financieros suficientes para cubrir los costos asociados con la implementación del plan de mitigación. Esto incluye la adquisición de equipos, capacitación, divulgación y cualquier otra actividad necesaria.

3. Tecnología y herramientas: Utilizaremos tecnología avanzada y herramientas adecuadas para el monitoreo, la evaluación de riesgos, la comunicación y la respuesta eficiente a cualquier emergencia.

- Plan de acción

Fase de preparación: En esta fase, estableceremos el equipo encargado de implementar el plan de mitigación. Se designarán roles y responsabilidades específicas para cada miembro del equipo, asegurando que cuenten con las habilidades y conocimientos necesarios. Además, se llevará a cabo la identificación y evaluación de los riesgos, mediante la recopilación de datos, el análisis de escenarios y la consulta con expertos. Con base en esta evaluación, se diseñarán estrategias y medidas preventivas adecuadas para cada riesgo identificado. Se establecerán objetivos claros y se elaborará un cronograma detallado que guíe la implementación del plan.

Fase de implementación: En esta fase, se llevarán a cabo las acciones necesarias para implementar las estrategias de mitigación. Esto puede incluir mejoras en la infraestructura existente, como reforzar estructuras, mejorar sistemas de drenaje o implementar medidas de protección adicionales. También se podrán adquirir equipos y recursos necesarios, como equipos de respuesta a emergencias, sistemas de monitoreo y comunicaciones. Además, se proporcionará capacitación al personal para que estén preparados y capacitados para actuar de manera adecuada en caso de emergencia. Asimismo, se establecerán sistemas de alerta temprana, que permitan una detección y respuesta rápida ante posibles eventos adversos.

Fase de monitoreo: Durante esta fase, se supervisará de manera continua la eficacia de las medidas implementadas. Se busca recopilar datos relevantes, realizando análisis comparativos y se evaluarán los resultados obtenidos. Esto permitirá determinar si las estrategias de mitigación están cumpliendo con los objetivos establecidos y si se requieren ajustes o mejoras. En caso de identificar deficiencias o áreas de mejora, se tomarán acciones correctivas oportunamente para fortalecer el plan de mitigación. Además, se fomentará el intercambio de información y retroalimentación con el equipo encargado, el personal involucrado y la comunidad en general, para asegurar una mejora continua y una mayor eficacia en la respuesta a los riesgos identificados.

- Plan de divulgación

Desarrollaremos un plan de divulgación para informar a la comunidad sobre el plan de mitigación, los riesgos asociados y las medidas preventivas. Se utilizarán diversos canales de comunicación para alcanzar a diferentes audiencias. Por ejemplo, se difundirán comunicados de prensa a través de medios de comunicación locales, se utilizarán plataformas de redes sociales para compartir información relevante, se elaborarán boletines informativos que se distribuirán a los residentes y se organizarán reuniones comunitarias para brindar un espacio de diálogo y respuesta a preguntas o inquietudes. El plan de divulgación se basará en un enfoque claro y accesible, utilizando un lenguaje comprensible para todos los miembros de la comunidad y aprovechando la participación activa de líderes comunitarios y organizaciones locales.

- Evaluación y revisión continua del plan

Realizaremos evaluaciones periódicas para medir el progreso y la efectividad del plan de mitigación. Estas evaluaciones se basarán en indicadores clave de desempeño previamente establecidos. Se recopilará información sobre el desempeño y los resultados obtenidos en la implementación de las medidas de mitigación. Se analizará si se han alcanzado los objetivos establecidos y si las estrategias implementadas han sido efectivas para reducir los riesgos identificados. Durante estas evaluaciones, se busca recopilar datos relevantes, como registros de incidentes, retroalimentación de la comunidad y métricas de rendimiento. Estos datos se analizarán para identificar posibles deficiencias, brechas o áreas de mejora en el plan de mitigación. En caso de identificar algún problema, se tomarán acciones correctivas de manera oportuna para fortalecer el plan y garantizar su efectividad a largo plazo.

Además, de que se realizarán revisiones regulares del plan de mitigación para asegurarse de que esté actualizado y adaptado a cualquier cambio en el entorno. Esto puede incluir la revisión de la evaluación de riesgos, la actualización de las estrategias de mitigación y la incorporación de nuevas medidas preventivas en función de la evolución de las amenazas o de las lecciones aprendidas de incidentes anteriores.

Es importante destacar que la evaluación y revisión continua del plan de mitigación no solo se enfocará en aspectos técnicos y operativos, sino también en la participación y retroalimentación de la comunidad. Se buscará involucrar a los residentes, empresas locales y otras partes interesadas en el proceso de evaluación y revisión, para obtener diferentes perspectivas y garantizar que el plan de mitigación sea efectivo y tenga el respaldo de la comunidad.