LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

Fundación Universitaria Los Libertadores
Facultad de Ingeniera
Especialización En Seguridad De La Información

SEGURIDAD, CONFIDENCIALIDAD Y CONFIABILIDAD DE PROCESOS Y DOCUMENTACIÓN CONTABLE EN TIEMPOS DE TRABAJO REMOTO EN LA COMPAÑÍA KLUGER TECH.

SECURITY, CONFIDENTIALITY AND RELIABILITY OF ACCOUNTING PROCESSES AND DOCUMENTATION IN REMOTE WORKING TIMES IN THE COMPANY KLUGER TECH.

Proyecto para optar al grado de Especialista en Seguridad de la Información

Juan Sebastian Perez Sequera
José Luis Ramirez Galeano
Juan Manuel Sanchez Becerra

Bogotá-Colombia
2021

Glosario:

BYOD: Estrategia alternativa que permite a los empleados, socios comerciales y otros usuarios utilizar un dispositivo cliente seleccionado y comprado personalmente para ejecutar aplicaciones empresariales y acceder a datos.

CIBERSEGURIDAD: Práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

CONFIDENCIALIDAD: Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información."

DISPONILIBILDAD: Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

FUGA DE DATOS: La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que a priori no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

FUGA DE INFORMACIÓN: Proceso por el cual se produce una fuga de la información almacenada en una red interna o en dispositivos físicos provocada por un atacante malintencionado y que es volcada o publicada en Internet para su libre consulta por parte de terceros sin autorización.

INFRAESTRUCTURA CRITICA: Activos de carácter esencial e indispensable cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

INTEGRIDAD: La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software, errores de hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

MTD: Maximum Tolerable Downtime. Tiempo de inactividad máximo tolerable, resultado de la suma de RTO + WRT. Que define la cantidad total de tiempo que un

proceso puede ser interrumpido sin causar consecuencias irreparables.

POLÍTICA DE SEGURIDAD: Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos.

RDP: Remote Desktop Protocol. Protocolo encapsulado y encriptado dentro de TCP, para la comunicación entre Terminal Server y Terminal Server Client.

RPO: Recovery Point Objective. Factor determinante de la cantidad máxima aceptable de pérdida de datos que establece el tiempo entre la ultima copia de seguridad creada y un eventual desastre que involucre perdida de datos.

RTO: Recovery Time Objective. Factor determinante de la cantidad máxima de tiempo permitido para la recuperación y puesta en linea de sistemas críticos.

SANS Institute: Lanzada en 1989 como una cooperativa para el liderazgo intelectual en seguridad de la información, la misión continua de SANS es capacitar a los profesionales de la seguridad cibernética con las habilidades prácticas y conocimiento

SHADOW IT: Dispositivos, software y servicios de TI fuera de la propiedad o el control de las organizaciones de TI.

VULNERABILIDAD: Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

WRT: Working Recovery Time Factor determinante de la cantidad máxima de tiempo tolerable que se necesita para verificación de la integridad de los datos y/o puesta en producción de los sistemas críticos.

ZERO TRUST: Concepto alterno a la seguridad del perímetro. Supone la ausencia de zonas de confianza de cualquier tipo. En este modelo, los usuarios, los dispositivos y las aplicaciones se ven sometidos a procesos de verificación cada vez que solicitan el acceso a un recurso corporativo.

Índice

Índice de cuadros

Índice de figuras

CONTEXTUALIZACIÓN:

En la necesidad de una rápida adopción de metodologías de trabajo remoto en casa, impulsado principalmente por los confinamientos a nivel mundial. Es inevitable aumentar la exposición de los recursos de TI y datos corporativos hacia entornos vulnerables que puedan poner en riesgo la disponibilidad, confidencialidad o integridad. Estos nuevos escenarios contribuyen al crecimiento del hasta ahora conocido concepto de Shadow IT.

Las organizaciones pasaron de sistemas de TI centralizados protegidos con políticas, procesos y tecnologías probadas, a tener a la mayoría de su fuerza laboral distribuida.[5] Este nuevo esquema de trabajo sumado a las tendencias BYOD, hace que la frase *"El usuario, es el eslabón más débil de cadena"*. Tome cada vez más fuerza en discusiones sobre seguridad informática, y paradójicamente sea ratificado.

El mayor problema está relacionado con colaboradores negligentes o descuidados, que no solamente usan redes y dispositivos domésticos potencialmente inseguros. Practicas comunes como el hacer clic en enlaces desconocidos, crear contraseñas inseguras, entregar información por medio de ingeniera social. Significa que son propensos a representar un riesgo cibernético para las organizaciones y una gran oportunidad para los actores que buscan aprovechas estas malas practicas.

"El malware es efectivo cuando la seguridad de una organización está orientada a tecnologías de detección basadas en listas blancas o cuando no existen herramientas con capacidades avanzadas de detección. El uso de instrumentos como PowerShell y WMI (Windows Management Instrumentation) por parte de los atacantes es recurrente debido principalmente a sus características, ya que facilitan la automatización de tareas y la gestión de la configuración del sistema operativo"[1]

El drástico y acelerado cambio hacia el trabajo remoto, convirtió un problema ya conocido en uno de los desafíos mas grandes para los equipos de seguridad informática. De acuerdo con el reporte *"The Human Element of Cybersecurity"* Elaborado en conjunto por ESET y The Myers-Briggs Company.

- Se ha informado por parte de los CISO un aumento del 63 % en el delito cibernético durante los confinamientos. [6]
- El 80 % de las empresas ha experimentado un mayor riesgo de seguridad informática causado por un factor humano. [6]

Todos estos factores y estadísticas, generan la necesidad de reforzar o considerar nuevos modelos para la gestión de la seguridad que vayan más allá de las tecnologías y métodos reactivos.

Palabras Clave:

Shadow it, BYOD, Ingeniera social, Malware, Power Shell, CISO, seguridad informática

ABSTRACT:

In need of rapid adoption of remote work at home methodologies, driven primarily by global lockdowns. Increasing the exposure of corporate data and IT resources to vulnerable environments that can compromise availability, confidentiality and integrity is inevitable. These new scenarios contribute to the growth of the now known concept of Shadow IT.

Organizations went from centralized IT systems protected with proven policies, processes and technology to having the majority of their workforce distributed. This new work scheme, added to BYOD trends, makes the phrase "The user is the weakest link in the chain"to gain more and more force in discussions about cybersecurity, and paradoxically it has been ratified.

The biggest problem is related to negligent or careless employees. They don't just use potentially insecure home devices and networks. Clicking on unknown links, creating weak passwords, delivering information through social engineering. It means that they are prone to pose a cyber risk for organizations and a great opportunity for threat actors.

"Malware is effective when the security of an organization is oriented to detection technologies based on white lists or when there are no tools with advanced detection capabilities. The use of instruments such as Power Shell and WMI (Windows Management Instrumentation) by attackers is recurrent mainly due to their characteristics, since they facilitate the automation of tasks and the management of the operating system configuration"

The drastic and accelerated shift towards remote work turned a well-known problem into one of the biggest challenges for Cybersecurity teams. According to the report *"The Human Element of Cybersecurity"Prepared jointly by ESET and The Myers-Briggs Company.*

- CISOs reported a 63 % increase in cybercrime during lock downs.
- 80 % of companies have experienced a higher cybersecurity risk caused by a human factor.

All these factors and statistics generate the need to reinforce or consider new models for security management that go beyond reactive technologies and methods.

Key Words:

Shadow it, BYOD, Social Engineering, Malware, Power Shell, CISO, Cybersecurity

1. INTRODUCCIÓN:

Dada la necesidad particular de ejecutar labores corporativas bajo el concepto de trabajo en casa, se desplazo a la fuerza laboral en sitio hacia un nuevo entorno que no está adecuado para realizar dichas labores, que exigen ciertos niveles de madurez y eficiencia en la ejecución de procesos de seguridad, lo que conlleva al incremento del uso de malas prácticas frente al tratamiento de información corporativa y gestión de recursos tecnológicos que hacen que estos queden expuestos y vulnerables a cualquier tipo de fuga hablando en términos de la seguridad de la información y la ciberseguridad que podrían reflejarse en la afectación de la continuidad del negocio, ya que estos nuevos escenarios, no siempre están adaptados para hacer frente a las nuevas técnicas y tácticas efectuadas por los delincuentes informáticos, incluyendo como aspecto relevante, la falta de experiencia o desconocimiento de la fuerza laboral que no están directamente relacionados con las áreas de TI, Ciberseguridad o Seguridad de la información.

La implementación forzosa y acelerada que la compañía Kluger Tech ejecuto para la creación de un escenario de trabajo remoto, demuestra la ausencia de hitos de seguridad de la información y el incremento del mal manejo de los recursos tecnológicos enfocados a labores corporativas, específicamente actividades de tipo contable. Las cuales en mayor medidas son apalancadas sobre un único equipo de computo destinado a operar como herramienta de labores diarias y contenedor del software contable, donde se almacena y procesa la información de tipo administrativa y en mayor medida información contable.

Debido a los tiempos de pandemia a causa del COVID 19 [7]. La compañía se ha visto obligada a permitir que dicho equipo, sea extraído de las instalaciones físicas de la compañía para dar continuidad a las operaciones de negocio. Por lo anterior se despertó el interés de Kluger Tech, en validar estrategias de continuidad de negocio bajo los pilares de la disponibilidad y confidencialidad de la información contable. Por tal razón ha iniciado reconocimientos de metodologías y estrategias de seguridad que le permitan tener una perspectiva inicial hacia la implementación de técnicas, enfocadas al aseguramiento de sus datos corporativos e infraestructura tecnológica. Kluger Tech ha tenido un primer acercamiento, hacia la construcción del programa de seguridad por medio del paquete de herramientas del Security Awareness Planning kit, publicado por SANS Institute.

En este primer levantamiento de información, la compañía identifico parte de

los riesgos expuestos de acuerdo con la clasificación de su fuerza laboral por rol y línea de desempeño. Obteniendo como resultado principal, la identificación del vector de riesgo humano que radica en el área contable, bajo el cargo de Asistente contable. Lo cual a su vez permitió clasificar como activo critico el equipo de cómputo destinado a operar como equipo de trabajo diario, repositorio de datos contables y servidor de software World Office versión PYME.

En base a estas condiciones y adelantos efectuados por la compañía, este proyecto pretende entregar un modelo teórico enfocado a la planeación de estrategias y buenas prácticas en el uso y aseguramiento de datos contables, basado en los marcos de referencia del Security Awareness Planning[8], complementado con la evaluación y estrategias de remediación de vulnerabilidades del servidor contable que se cataloguen como críticas o altas de acuerdo con el Common Vulnerability Scoring System 3.0.[9] Buscando aclarar el panorama de seguridad de la información para la compañía Kluger Tech, y lograr abordar aspectos relacionados con el aseguramiento de datos e infraestructura corporativa, sin dejar de lado la adopción de nuevas metodologías y conceptos enfocados a las buenas prácticas que permitan que la compañía no se vea afectada frente a la pérdida o integridad de sus datos contables.

2. PROBLEMATICA:

La ausencia de normas y controles a nivel de seguridad, el manejo y consolidación de toda la información contable en un solo repositorio. Ahondando en la problemática de la compañía, la disposición de la infraestructura critica en una red poco segura dado el escenario de trabajo remoto, se suma la carencia de seguridad perimetral, junto con la falta de actualizaciones del sistema operativo sobre el cual trabajo el software contable.y adicional a esto el equipo servidor, no cuentan con políticas de control de acceso a la infraestructura por validación de contraseña, o gestión de usuarios privilegiados.

Complementando las malas practicas sobre la infraestructura critica, las actualizaciones de las bases de datos de las firmas de antivirus, la ausencia de políticas adecuadas de respaldo y copias de seguridad las cuales están dentro del mismo entorno de trabajo aportan a la baja postura de seguridad de la compañía.

Teniendo en cuenta que no existe un respaldo fuera de esta infraestructura, de llegar a presentarse algún tipo de aprovechamiento de las malas practicas ejecutadas, la compañía se expone a la afectación de la integridad, disponibilidad o confidencialidad de la información. Teniendo como consecuencias la posibilidad de perdida de su historial contable, el acceso no autorizado a plataformas bancarias, pago de seguridad social y nomina, perdida o degradación de información de facturación, cuentas por pagar o datos de clientes y terceros. Lo que repercu-

te en la degradación de la imagen corporativa. y ponen en riesgo la continuidad de las labores ejecutadas por la compañía.

Por lo anterior, se ve la necesidad de incluir dentro del alcance, el demostrar que tan vulnerable se encuentra la infraestructura en la que actualmente reposa el software contable, Pretendiendo inculcar a la gerencia y directivos, la importancia de reforzar su sistema y blindar sus datos contables ante cualquier vulnerabilidad, dicho proceso llevará a la compañía Kluger Tech. a reducir la probabilidad de que estas sean explotadas sobre el servidor contable.

3. OBJETIVOS:

3.1. General:

Proponer a la gerencia general de Kluger Tech, Guías dirigidas a la mejora de la postura de seguridad y trabajo seguro en casa para el tratamiento seguro de la información digital e infraestructura tecnológica critica del área contable.

3.2. Específicos:

- Determinar el nivel de madurez actual frente a la seguridad de la información, complementando los avances ejecutados por Kluger Tech en la implementación del modelo de evaluación entregado en el Security Awareness Maturity Model.
- Proponer un documento preliminar de evaluación de métricas dirigidas a un plan de concientización que mejore la seguridad de la información siguiendo la metodología del Security Awareness Planning kit. Permitiendo que la compañia Kluger Tech logre escalar al nivel 3 del Security Awareness Maturity Model.
- Identificar las vulnerabilidades catalogadas como criticas y altas. De acuerdo al reporte generado por medio de la ejecución de un escaneo de vulnerabilidades sobre la infraestructura critica del proceso contable, aplicando la herramienta de NESSUS SCANER.
- Proponer las acciones de mitigación de las vulnerabilidades identificadas como criticas y altas. Teniendo como referencia las recomendaciones entregadas por el Common Vulnerability Scoring System Version 3.0.

4. MARCO TEORICO

4.1. Telework Essentials Toolkit

La agencia de seguridad de infraestructura y seguridad informática, publica el tool Kit Telework Essentials Toolkit, diseñado para guiar a los lideres, personal

de TI y a los usuarios finales en la transición a un entorno de trabajo seguro y permanente en casa, a través de recomendaciones sencillas y prácticas. El kit de herramientas presenta 3 módulos para los lideres, profesionales de TI y los usuarios finales.

Después de adoptar el trabajo en casa a causa del COVID-19,[7] la agencia de seguridad de infraestructura y seguridad informática hace que todos sus actores planeen estrategias y recomendaciones que ayudan a las compañías adoptar practicas seguras que aportan en la protección de sus datos, reforzando la disponibilidad, confidencialidad y seguridad. Entre estas practicas podemos destacar los entrenamientos de seguridad, controles de seguridad enfocados en la infraestructura, implementación de factores de autenticación, practicas seguras en el uso, almacenamiento y transmisión de datos corporativos.

4.2. Security Awareness Planning

Publicado por el Instituto SANS, como recurso de acceso libre, El kit de herramientas de planificación de la conciencia de seguridad, habilita materiales y recursos destinados a la creación rápida u optimización de un plan de conciencia relacionado con aspectos de seguridad, que pueden ser utilizados por personas con una basta experiencia o con conocimientos mínimos.

El kit de herramientas, lista el orden en el cual se deberían abordar los recursos entregados para la creación de un nuevo plan de seguridad, dentro de los cuales resaltan la matriz de métricas la cual identifica y documenta numerosas formas de medir los comportamientos de seguridad, e impactos estratégicos del plan de concientización.

El modelo de madurez, actúa como como parte fundamental de la creación y comunicación de un nuevo plan, desglosando cada etapa referente al estado de madurez. El calendario de programa actual y la guía de presentación, proveen ejemplos de como documentar y presentar a los interesados el programa de concientización.

4.3. Guía para la implementación de seguridad de la información de las MIPYME.

De acuerdo con el ministerio de la comunicaciones MINTIC, las compañías cada vez dependen mas de sus sistemas de información, y por ende de la información que estos administran.

Por tal razón, esta entidad ha publicado una guía practica,[12] donde se detallan las consideraciones y recomendaciones que una MIPYME debería considerar para establecer un plan de implementación de seguridad de la información.

Como primer medida, el ministerio recomienda organizar la información al interior de la compañía. creando políticas de seguridad que incluyan procedimientos, practicas o estándares y controles. Sensibilizar a los empleados periódicamente sobre las políticas de seguridad implementadas, para lo cual se recomienda crear un plan de comunicaciones, entregando información detallada y clara.

El ministerio plantea que la identificación de los activos de información de la compañía, es la base para la gestión adecuada de los mismos. Determinar vulnerabilidades y amenazas de la arquitectura tecnológica que procesa la información. Realizada la identificación de activos, y vulnerabilidades, la evaluación de los riesgos asociados busca como objetivo principal generar procedimientos adecuados para la administración y tratamiento de riesgos que deberían ser ejecutados por la compañía.

4.4. Small Bussiness Cybersecurity Corner

A diferencia de las compañías con un amplio desarrollo. Las compañías pequeñas dependen de la tecnología de la información para administrar sus negocios, aunque con recursos tecnológicos y monetarios limitados. Por lo cual estas empresas requieren de una orientación más personalizada, soluciones y capacitación en aspectos de seguridad informática que les permitan gestionar de forma eficiente y rentable sus riesgos seguridad informática y seguridad de la información.

Bajo este escenario, el NIST (National Institute of Standards and Technology), en conjunto con el FBI (Federal Bureau of Investigation). Ha difundido recursos para ayudar a las pequeñas empresas a identificar, evaluar, gestionar y reducir los riesgos de seguridad informática.

Enumerando agencias federales, incluyendo el NIST. El Small Bussiness Cybersecurity Corner [11] se basa en recursos gratuitos y completos ayudando a las empresas más pequeñas a comprender sus riesgos específicos, así como las medidas utilizadas para mitigarlos.

4.5. Cybersecurity Framework

Framework basado en estándares, directrices y prácticas existentes para que las organizaciones gestionen y reduzcan mejor el riesgo de seguridad informática.

El marco está organizado por cinco funciones clave: **identificar, proteger, detectar, responder, recuperar.**

Los cuales permiten desarrollar una comprensión organizacional para gestionar el riesgo de seguridad informática de los sistemas, activos, datos y capaci-

dades, asegurando la entrega de servicios. e implementando actividades para la identificación de la ocurrencia de un evento. Pudiendo ser atendido por medio de la toma de acciones respecto al evento detectado, permitiendo restaurar las capacidades de los servicios que se pudiesen ver afectadas frente a la ocurrencia del evento de seguridad.

Cuando estos términos, son considerados en conjunto, brindan una visión integral del ciclo de vida para administrar la seguridad informática a lo largo del tiempo.[10]

4.6. Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia

Los activos destinado al almacenamiento de datos corporativos de tipo contable, diariamente se ven expuesto a un sin numero de amenazas a partir de vulnerabilidades que de llegar a materializarse, podrían acabar en accesos no autorizados con los suficientes privilegios para acceder a información corporativa, específicamente información contable como plantillas de pago de nomina, cuentas contables con información de activos y pasivos, contraseñas de portales bancarios entre otros datos con alta sensibilidad.

En Colombia, mas específicamente en la ciudad de Montería Córdoba, de acuerdo con los autores [4], pequeñas y medianas compañías, se han visto afectadas por programas con malware que han logrado ingresar a las plataformas de pago de seguridad social y extraer información de personal o credenciales de plataformas bancarias.

Estas situaciones, muchas veces se materializan, por falta de actualizaciones de las versiones de antivirus, por no contar con políticas de seguridad acorde a las operaciones de la compañía, por malas practicas en el almacenamiento de la información y copias de respaldo, pero en un contexto mas especifico, a la poca o en muchos casos ausente capacitación de la fuerza laboral, frente a aspectos clave como el manejo de datos corporativos sensibles o incluso la identificación de campañas de pishing.

Conforme a lo expuesto por los autores,[4] la implementación de sistemas de seguridad para la información contable y financiera, no siempre es efectivo ya que por lo general se deja de lado el factor humano, recayendo principalmente en los equipos delegado para labores de IT o resolución de incidentes.

4.7. Norma ISO 27002

En Colombia, publicada y ratificada en 2015 por el ICONTEC, como GTC-ISO-IEC 27002:2015 [2]. Establece una guía de buenas practicas y pautas fundamentadas en los pilares de confidencialidad, disponibilidad e integridad. Para

llevar a cabo la gestión de la seguridad de la información, independientemente del tamaño de la compañía que busque aplicar e implementar controles y desarrollar políticas propias para una protección adecuada de las compañías, maximizando el retorno de inversión y oportunidades de negocio.

Divida en 12 secciones y 144 controles, en conjunto logra cubrir la gestión de la seguridad de la información.[3]

- Evaluación y tratamiento de riesgos y amenazas.
- Política de seguridad.
- Aspectos organizacionales para la seguridad.
- Clasificación y control de activos.
- Seguridad ligada al personal.
- Seguridad física.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Gestión de continuidad de negocio.
- Conformidad con la legislación.
- Gestión de los incidentes de seguridad de la información.

La adopción de la norma ISO 27002, permite abrir el abanico para la identificación de falencias y malas practicas en la gestión de la seguridad de la información, que pueden ser corregidas bajo la aplicación de procesos y políticas que generan valor a las compañías frente a clientes y proveedores.

5. ESCENARIO ACTUAL

A continuación, se detalla la arquitectura actual de la red sobre la cual se establece la conexión hacia internet desde el servidor contable de la compañía Kluger Tech, en cual cuenta con un sistema operativo Windows 7.

Así mismo se indica que, dentro de la misma infraestructura de red destacan dispositivos de propósito corporativo y doméstico. Sin existir alguna segmentación de red, o protección a nivel perimetral. Y evidenciando una eventual conexión hacia el servidor contable por medio del protocolo de escritorio remoto RDP.

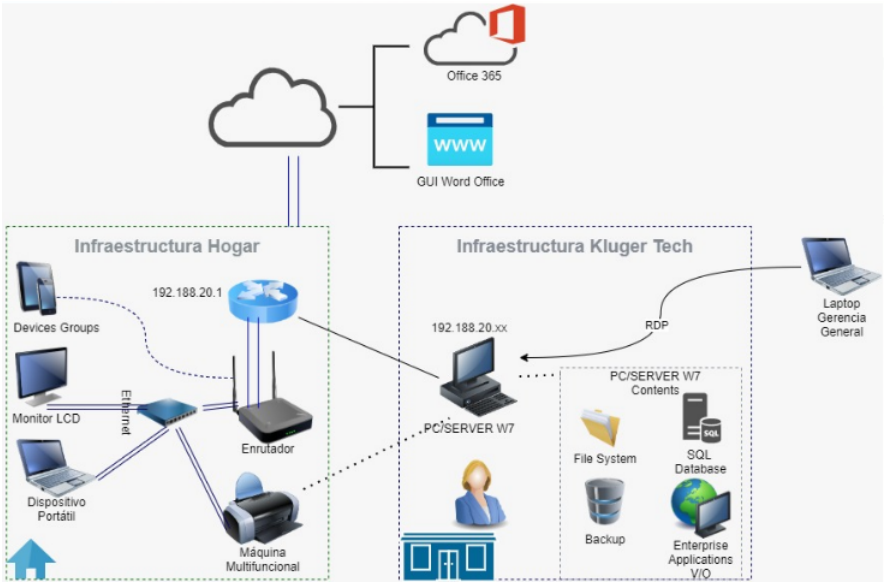


Figura 1: *Arquitectura de red; Fuente Propia*

6. METODOLOGIA

A continuación, se presenta la metodología seleccionada, basada en los ejercicios previos ejecutados por la compañía, frente a la determinación del estado de madurez a nivel de seguridad de la información. Es por ello, que la ejecución del proyecto sera dividida en cuatro fases principales, enfocadas a la identificación y remediación de la postura de seguridad actual, y las vulnerabilidades existentes en el servidor contable.

6.1. Determinación del estado de madurez.

Complementando la aproximación y ejercicios previos efectuados por la compañía, por medio del Security Awareness Planning Kit , entregado por el SANS Institute. Se dará continuidad al proceso de determinación del estado de madurez basado en la descripción de cada nivel propuesto y contrarrestándolo con los métodos o acciones existentes en la compañía. Una vez identificado el nivel de madurez actual se indicarán las acciones recomendadas por el Security Awareness Planning Kit, para escalar al siguiente nivel de madurez.

Como complemento, se ejecutar la herramienta Web de auto diagnostico publicada por INCIBE. Basada en un test, dirigido al administrador IT, que relaciona preguntas sobre el empleo de recursos y procesos relacionados a la seguridad informática de la compañía.

6.2. Evaluación de Métricas de impacto.

Aplicando la matriz, SecurityAwareness-Metrics. Contenida dentro del Security Awareness Planning Kit se determinará la forma mas adecuada para el desarrollo del plan de concientización, basado en la evaluación de métricas relacionadas con aspectos de comportamiento, culturales, estratégicos y humanos. Se entregaran las métricas que se relacionen al tamaño de la compañía, e impacten directamente el proceso contable.

6.3. Identificación de vulnerabilidades sobre infraestructura critica.

Ocupando la dirección IP asignada dentro de la red para el servidor contable. Por medio de un escaneo de vulnerabilidades de infraestructura, utilizando la herramienta NESUSS en su versión de evaluación. Se identificarán y reportarán las vulnerabilidades existentes sobre el equipo, indicando su estado actual frente a aspectos de seguridad de infraestructura.

La intención de este escaneo, se basa en encontrar un punto de partida para evaluar las vulnerabilidades existentes en el servidor contable, que puedan llegar a afectar la continuidad de las operación contables.

6.4. Evaluación y estrategias de remediación de vulnerabilidades

Con la identificación de vulnerabilidades, estas se categorizarán de acuerdo al puntaje asignado por el CVSS 3.0 según los criterios de explotabilidad e impacto. Así mismo, se indicarán las acciones recomendadas para proteger los datos contables o remediar la infraestructura frente a las vulnerabilidades existentes.

7. RESULTADOS

7.1. Definición del estado de madurez y evaluación de métricas de impacto

De acuerdo al nivel de madurez determinado para la empresa Kluger Tech conforme al Security Awareness Maturity model, se logra evidenciar que la compañía tiene varias falencias a nivel de seguridad, no solamente en los aspectos relacionados con el tratamiento de la información contable, evidenciando que no se cuenta con ningún lineamiento, política o proceso para el aseguramiento de datos corporativos o infraestructura critica.

Por tal razón, y complementado el primer acercamiento que la compañía a ejercido a la construcción de un plan de seguridad, se presentan algunas consi-

deraciones que llevaran a la compañía Kluger Tech a identificar y minimizar los riesgos que podrían afectar no solamente su proceso contable, sino también la continuidad y estabilidad de sus operaciones.

- No existe un modelo de seguridad implementado en la compañía capaz de detectar o disuadir cualquier tipo de vulnerabilidad.
- No se materializan iniciativas de aseguramiento de la información.
- Actualmente no existe un programa de concientización de seguridad en el área contable.

Buscando comparar el nivel de madurez determinado por medio del Security Awarness Madurity Model. Mediante la herramienta de auto diagnostico, publicada por el INCIBE se observo el nivel porcentual del estado actual de la compañía dando como resultado un 86.9 % de riesgo confirmando el bajo nivel en el cual se encuentra la compañia Kluger Tech. Validar documento anexo *Auto diagnóstico ligero, INCIBE - Kluger Tech*

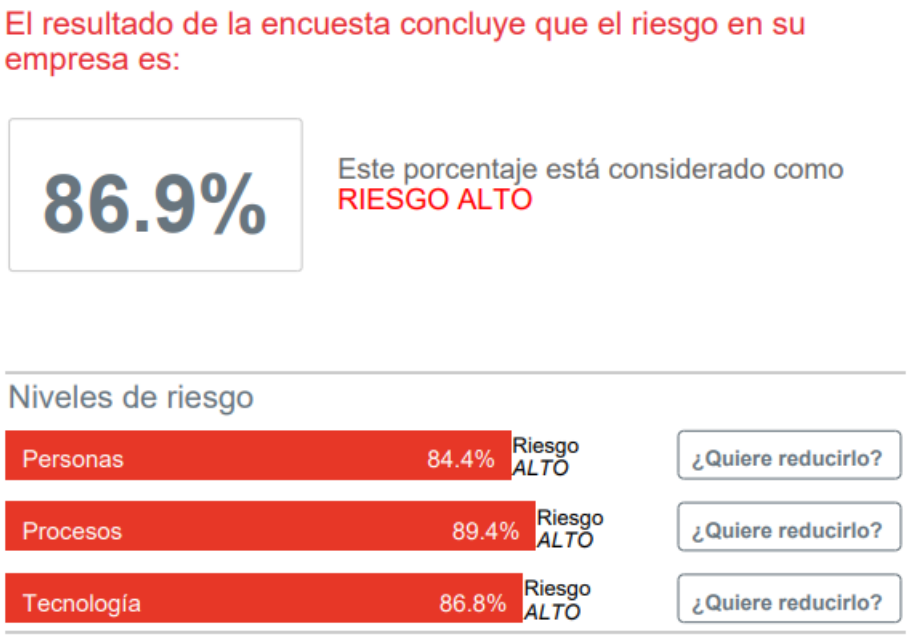


Figura 2: *Porcentaje de riesgo Kluger Tech; Fuente Propia*

Para lograr que la compañía Kluger Tech avance en el proceso de de establecerse en el nivel 3 del security Awareness Maturity model, se sugiere evaluar el nivel 2 cuyo valor es asegurar los requisitos legales de la compañía dentro del desarrollo del plan de madurez.

Nivel	ENFOQUE DEL NIVEL
1	Sin programa de concientización sobre seguridad
2	Centrado en el cumplimiento
3	Promover la conciencia y el cambio de comportamiento.

Figura 3: *Niveles de Madurez; Fuente Propia*

De acuerdo al modelo de madurez, el establecer un programa de concientización diseñado para cumplir requerimientos de cumplimiento a un costo limitados, bajo el designio de un líder de programa durante tiempo parcial.

Complementario a las actividades propuestas, El escalamiento hacia el nivel 3, se basa en la identificación de manera eficaz el riesgo humano por medio del programa, Donde se gestionan refuerzos continuos durante el transcurso del año con información y metodología de acuerdo con el tipo de usuario y el rol que ejerce dentro de la compañía. Esta actividad particular, se sugiere que sea acompañada de la ejecución de las campañas de concientización logrando que los usuarios reconozcan, prevengan y reporten incidentes de manera activa.

Dando continuidad y complemento a la estrategia de mejora de la postura de seguridad y metodología del Security Awarness Planning Kit de acuerdo con la información recopilada por security Awareness Maturity model Recomendamos que se tomen estrategias y lineamentos para mejorar el nivel de conciencia y seguridad hasta el nivel 3, el cual identifica los grupos de colaboradores , la formación genera impacto en el apoyo a la misión de la compañía y se centra en aspectos claves. El contenido se comunica de forma interactiva buscando cambiar el comportamiento del trabajo y en casa. Como resultado, el personal reconoce, previene y reporta incidentes de forma activa. Generando valor en la compañía siendo capaz de gestionar y medir eficazmente su riesgo humano. Basado en requisitos de cumplimiento.

A continuación, se listan las actividades y recomendaciones,para el escalamiento hacia el nivel 3 del Security Awarness Planning Kit.

Actividades	Recomendaciones
Identificar las regulaciones o estándares que debe cumplir.	Evaluar los alcances de la ley 1273 de 2009. Principalmente los artículos 269F y 269E

Identificar los requisitos de conciencia de seguridad para esos estándares	Dar enfoque hacia el conocimiento en la cultura de los colaboradores, para la manipulación de datos sensibles, identificación de Actividades de Phishing e Ingeniería social.
Identificar a alguien para que implemente la capacitación de conciencia de seguridad requerida.	Implementar capacitación al grupo completo de colaboradores de la compañía haciendo especial énfasis el personal del área contable.
Identificar y obtener el apoyo de las partes interesadas.	Presentar de forma concisa y clara la existencia de problemas en ámbitos de seguridad de al información, basados en el riesgo humano indicando sentido de urgencia fundamentado en datos sobre incidentes reales pasados.
Crear la Carta del Proyecto, identificando aspectos como el alcance, las metas, los objetivos, las suposiciones y las limitaciones.	Se sugiere referenciarse en el documento "03-ProjectPlan-Exampleçontenido dentro del security Awareness planing kit.
Identificar quién será responsable del programa de concientización. Para garantizar el mayor éxito, esa persona debe dedicarse a tiempo completo, tener habilidades sociales e informar y ser parte del equipo de seguridad.	Postular como responsable a aquel colaborador. Con acceso asertivo al equipo de recursos humanos, al equipo de tecnología o infraestructura y al nivel C.
Identifique los principales riesgos humanos que deberá gestionar, esto puede requerir una evaluación de riesgos humanos	Dar continuidad a la evaluación de riesgos de factor humano, desarrollada para el área contable, expandiendo la evaluación hacia las otras áreas de la compañía.
Identificar los comportamientos clave que mitigarán esos riesgos.	Validar métricas de comportamiento dirigidas hacia el reconocimiento de técnicas de ingeniería social, manejo de data sensible, y procedimiento de eliminación o destrucción de datos.

Identificar cómo se comunicará, involucrará y capacitará a su fuerza laboral, para incluir análisis cultural, capacitación primaria y capacitación de refuerzo.	Definir los medios que generen mas impacto en la fuerza laboral, y refuercen los objetivos de aprendizaje.
Desarrolle o compre sus materiales	Hacer uso de herramientas interactivas computer-based training en sus versiones de prueba o pagas. Complementado con recursos como Webcast, o blogs. Para lo cual se sugiere validar futuros proveedores mediante el gartner Peer Insigths Security Awareness Computer-Based Training.
Crear un plan de ejecución con hitos, para incluir métricas.	Se sugiere validar métricas contenidas en el Anexo Evaluación preliminar de métricas de seguridad Kluger Tech.
Haga que el líder senior anuncie el plan.	Anunciar el plan de concientización indicando objetivos, tiempos de ejecución, metodologías propuestas y medios de evaluación.
Implementar capacitación en concientización sobre seguridad	Definir los tiempos de implantación, de forma gradual, dando prioridad en los temas de identificación y manejo de datos sensibles.
Realizar un seguimiento y documentar quién completa la capacitación.	Realizar seguimiento anual por medio de encuestas de participación, o evaluaciones midiendo la actitudes hacia la seguridad informática.

Cuadro 1: *Actividades y recomendaciones nivel 3 del Security Awarness Planning Kit fuente propia*

Como indicadores del nivel 3 se determina que:

- Existe un plan estratégico que ha identificado el alcance del proyecto, metas, objetivos y justificación del programa.
- Se han identificado y puede explicar sus principales riesgos humanos y los comportamientos que manejan esos riesgos de manera más efectiva.
- El programa tiene suficiente apoyo de liderazgo para proporcionar los recursos necesarios.

- La conciencia de seguridad se considera parte del esfuerzo de seguridad general de la organización.
- El líder del programa se dedica a tiempo completo al esfuerzo, tiene fuertes habilidades de comunicación y es parte del equipo de seguridad.
- El programa coordina y colabora con varios departamentos dentro de la organización, incluidos Comunicaciones, Recursos Humanos y Mesa de Ayuda.
- El programa trabaja para involucrar positivamente a la fuerza laboral.

En contraste las métricas generales de evaluación para el nivel 3 propuestas son:

- Número o porcentaje de colaboradores que completan la formación.
- Número de sesiones de formación en un año.
- Número o frecuencia de materiales de sensibilización distribuidos.
- Tasa de clicks en informes de simulación de phishing.
- Número de infracciones de la política de seguridad.

Complementado las actividades propuestas, se plantea un primer modelo de evaluación de métricas, dirigidas a la elaboración de un plan de formación enfocado en la mejora de concientización del personal de Kluger Tech, principalmente al área contable. Para conocer detalle de la evaluación de métricas, validar documento anexo *Evaluación preliminar de métricas de seguridad Kluger Tech.*

7.2. Identificación, Evaluación y Estrategias de remediación de vulnerabilidades sobre infraestructura critica

Como resultado de escaneo ejecutado por medio de la herramienta NESSUS, se evidencian las vulnerabilidades y sus respectivos niveles de clasificación como criticas o altas a las que se encuentran expuestos el servidor contable y los datos contables gestionados localmente y a través del software contable World Office. Dada la alta disponibilidad requerida para el servidor contable es importante resaltar a nivel de infraestructura el bajo nivel de actualización y ausencia de medidas de protección ante cualquier ciberataque a nivel perimetral o de punto final, y en contra parte la falta de medios de respaldo externos, procesos o políticas frente al uso, administración y almacenamiento de datos contables reflejan una ampliación en el panorama de exposición frente a la perdida o disponibilidad de los mismos.

Como resultado del escaneo, se validaron y documentaron las recomendaciones de las vulnerabilidades que se consideraban como críticas y altas. Lo que

permitirá tener un punto de partida hacia la mejora de la infraestructura critica para el manejo de los datos contables, que al mismo tiempo permitirán la evolución de la postura de seguridad de la compañía.

A continuación, se listan las vulnerabilidades clasificadas como criticas o altas, junto con las recomendaciones para la evaluación y mitigación de acuerdo al reporte de escaneo de vulnerabilidades sobre el servidor contable.

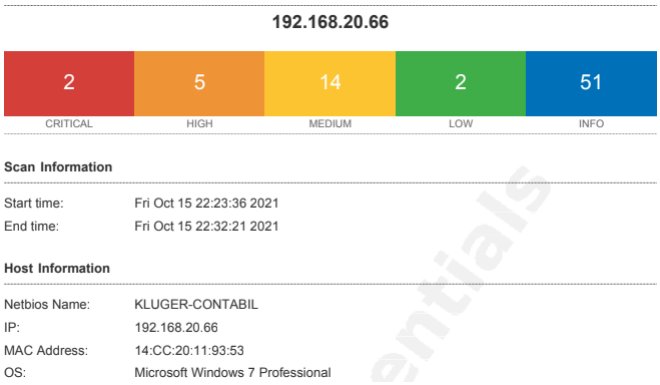


Figura 4: *Vulnerabilidades de Servidor Contable; Fuente Propia*

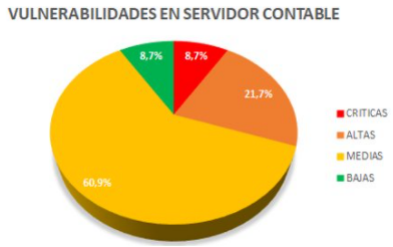


Figura 5: *Porcentaje de Vulnerabilidades de Servidor Contable; Fuente Propia*

A continuación se detalla información relevante de las vulnerabilidades clasificadas como criticas o altas, de acuerdo al escaneo de vulnerabilidades ejecutado sobre el servidor contable.

Vulnerabilidad Critica 1	
Detección de versiones no admitidas de Microsoft SQL Server	
ID Vulnerabilidad	737565
Nivel de Criticidad	Alto
Nivel de riesgo (CVSS 3.0)	10.0

Descripción	Ejecución de una versión no compatible de un servidor de base de datos en el host remoto.
Riesgos asociados	Ejecución de código remoto no autorizado sobre el servidor de World Office, permitirá que un atacante informático inyecte código a una aplicación o sistema. Afectando la integridad de las bases de datos del software contable.
Remediación	Se recomienda la instalación de actualizaciones de seguridad de SQL server y la prohibición del acceso anónimo, permitiendo solo las conexiones de los usuarios autenticados. Importante reforzar con un cambio de contraseña periódica para la explotación de la vulnerabilidad.

Cuadro 2: *Vulnerabilidad Critica 1; fuente propia*

Vulnerabilidad Critica 2	
SO Windows no compatible	
ID Vulnerabilidad	108797
Nivel de Criticidad	Alto
Nivel de riesgo (CVSS 3.0)	9.8
Descripción	A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Riesgos asociados	▪ Aumento de brechas de seguridad en el servidor contable que pueden ser aprovechadas por los ciberdelincuentes. ▪ Afectación de la confidencialidad, integridad y disponibilidad de la información alojada en el servidor contable ya que está expuesta a ataques de ramsomware por vulnerabilidades como el bluekeep que aprovecha el uso de protocolo de escritorio remoto debido a que el sistema operativo de Windows 7 dejo de recibir soporte y publicación de parches de seguridad por parte de Microsoft desde enero del 2020.

Remediación	Actualizar el servidor contable a un sistema operativo vigente. En caso de Microsoft, se recomienda actualizar a Windows 10, el cual tiene soporte y constantemente repara los bugs y errores descubiertos y limitar los protocolos de escritorio remoto.

Cuadro 3: *Vulnerabilidad Critica 2; fuente propia*

Vulnerabilidad Alta 1	
Certificado SSL firmado mediante un algoritmo de hash débil	
ID Vulnerabilidad	35291
Nivel de Criticidad	Alto
Nivel de riesgo (CVSS 3.0)	9.8
Descripción	A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Riesgos asociados	Al tener un certificado de seguridad débil, la compañía puede estar expuesta a cualquier tipo de vulneración con la información de los pagos de nómina o cualquier tipo de transacción electrónica, si no se tiene un certificado robusto, puede provocar que los datos del servidor estén desprotegidos.
Remediación	Adquirir un certificado SSL emitido por organizaciones de certificación confiables y legales permite que los datos estén seguros, ayudando con la autenticación y cifrado de cualquier sitio web o tránsito de datos.

Cuadro 4: *Vulnerabilidad Alta 1; fuente propia*

Vulnerabilidad Alta 2	
Certificado SSL firmado mediante un algoritmo de hash débil	
ID Vulnerabilidad	35291
Nivel de Criticidad	Alto
Nivel de riesgo (CVSS 3.0)	9.8
Descripción	A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Riesgos asociados	Al tener un certificado de seguridad débil, la compañía puede estar expuesta a cualquier tipo de vulneración con la información de los pagos de nómina o cualquier tipo de transacción electrónica, si no se tiene un certificado robusto, puede provocar que los datos del servidor estén desprotegidos.
Remediación	Adquirir un certificado SSL emitido por organizaciones de certificación confiables y legales permite que los datos estén seguros, ayudando con la autenticación y cifrado de cualquier sitio web o tránsito de datos.

Cuadro 5: *Vulnerabilidad Alta 2; fuente propia*

Vulnerabilidad Alta 3	
SSL Medium Strength Cipher Suites Supported (SWEET32)	
ID Vulnerabilidad	20007
Nivel de Criticidad	Alto
Nivel de riesgo (CVSS 3.0)	7.5
Descripción	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0. Estas versiones de SSL son afectadas por varios defectos criptográficos, que incluye un esquema inseguro con cifrados CBC. - Esquemas inseguros de renegociación y reanudación de sesiones.
Riesgos asociados	▪ Materialización de ataques man-in-the-middle. ▪ Descifrar las comunicaciones entre el servicio y los clientes afectados. ▪ interrupciones en la disponibilidad de recursos.
Remediación	Deshabilitar protocolo SSL 2.0 y 3.0. Posteriormente, habilitar protocolo TLS 1.2

Cuadro 6: *Vulnerabilidad Alta 3; fuente propia*

Vulnerabilidad Alta 4	
Servidor de protocolo de escritorio remoto de Microsoft Windows permitido	
ID Vulnerabilidad	18405
Nivel de Criticidad	Media
Nivel de riesgo (CVSS 3.0)	4.9

Descripción	El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y / o SSL 3.0. Estas versiones de SSL son afectadas por varios defectos criptográficos, que incluye un esquema inseguro con cifrados CBC. - Esquemas inseguros de renegociación y reanudación de sesiones.
Riesgos asociados	▪ Falsificación de claves públicas de servidores legítimos y realizar ataques man-in-the-middle. ▪ Permite XSS (Cross-site scripting) a través de un atributo o error elaborado de un elemento IMG. ▪ Permiso de operaciones arbitrarias de lectura de archivos debido a la lógica de modificación de .htaccess de respaldo (SEC-345).
Remediación	▪ Forzar el uso de SSL como capa de transporte para este servicio si es compatible. ▪ Permitir únicamente conexiones desde computadoras que ejecutan el protocolo de escritorio remoto con autenticación de nivel de red

Cuadro 7: *Vulnerabilidad Alta 4; fuente propia*

Vulnerabilidad Alta 5	
No se requiere firma SMB	
ID Vulnerabilidad	57608
Nivel de Criticidad	Media
Nivel de riesgo (CVSS 3.0)	5.3
Descripción	Indica que el servidor SMB no requiere firma cuando es alcanzado de manera remota, lo cual permite a un atacante remoto no autenticarse, permitiéndole aprovechar esto para realizar ataques de intermediario contra el servidor SMB.
Riesgos asociados	Modificación de archivos o información del sistema.

Remediación	Deshabilitar al cliente de red de Microsoft para que firme digitalmente las comunicaciones en todo momento, deshabilitar el servidor de red de Microsoft para que firma digitalmente los comunicados en todo momento. Para lo anterior, se debe dejar como condición, que el servidor este de acuerdo con la firma.

Cuadro 8: *Vulnerabilidad Alta 5; fuente propia*

8. CONCLUSIONES

Las áreas contables, suelen ser en mayor medida un objetivo principal para los ciberdelincuentes que buscan obtener acceso a las plataformas o equipos destinado a la ejecución de labores contables, con los suficientes privilegios para la extracción de datos corporativos, personales o financieros.

La seguridad de los programas, o activos de labores contables, no debe ser delegada a un solo equipo o responsable directo, ya que la efectividad de los procesos de seguridad de la información, en mayor medida son el resultado de la integración de procesos, buenas practicas y los conocimientos y acciones seguras que la fuerza laborar ponga en practica.

La actualización anual de planes de concientización, enfocados a temarios específicos como la evaluación del riesgo humano, la identificación temprana de técnicas de pishing o ingeniería social, la aplicación de buenas practicas para establecer conexiones remotas y trabajo en casa, políticas de autenticación fuerte, manejo y administración de datos sensibles, sensibilización a la exposición de riesgos. son aspectos altamente relevantes en el ejercicio de minimizar el nivel de riesgo al cual se expone la fuerza labora, sino también y de por medio la credibilidad, rentabilidad de la compañía y la continuidad de negocio.

La adopción del modelo de trabajo en casa, implementado por la compañía Kluger Tech, ha dejado al descubierto la ausencia de medidas de seguridad y procedimientos para la ejecución de labores corporativas, aportando en el incremento de de brechas de seguridad y exposición de datos contables. En respuesta a este escenario se propone una guía básica para el trabajo seguro en casa.Validar documento Anexo *Guía básica de trabajo seguro en casa Kluger Tech.*

Conforme a los resultados obtenidos bajo la evidencia de la ausencia de planes a nivel de seguridad de la información y seguridad informática, es pertinente sugerir a la gerencia de Kluger Tech, se permita evaluar las siguientes conside-

raciones basadas en controles, metodologías y mejores practicas que permitan que la compañía logre abordar los aspectos relacionados con la gestión y control de riesgos en ámbitos de seguridad de la información y seguridad informática y de un modo directamente proporcional mejorar su postura de seguridad.

- Implementar y actualizar anualmente un programa de concienciación y entrenamiento de seguridad, tomando como referencia inicial el anexo *Evaluación preliminar de métricas de seguridad Kluger Tech* complementándolo conforme a la Publicación 800-50 del NIST, *Building An Information Technology Security Awareness and Training Program.*

- Definir un modelo de respuesta a incidentes que incluyan la definición de planes, documentación de procedimientos, funciones y supervisión de la gestión de incidentes a los que pueda enfrentarse la organización. para lo que sugiere validar el Marco de Gestión de Riesgos (RMF) del NIST el cual proporciona un proceso de 7 pasos que la compañía podría utilizar para gestionar la seguridad de la información y el riesgo de privacidad.

- Validar herramientas, e instaurar procedimientos para respaldar adecuadamente y de manera oportuna la información crítica. Verificando trimestralmente que los datos restaurados se encuentren intactos y funcionales. Se sugiere validar el blog INCIBE DLP protege tus datos contra fugas de información junto con el gartner peer insights Enterprise Data Loss Prevention (DLP) Reviews and Ratings a fin de Definir procesos y herramientas para prevenir la filtración de datos, y asegurar la privacidad e integridad de la información sensible identificada.

- Asignar políticas que aseguren el buen uso de los sistemas de IT y los datos corporativos bajo una revisión y actualización continua para reflejar los riesgos o vulnerabilidades actuales. Por tal razón se sugiere tomar como referencia las Plantillas de políticas de seguridad publicadas por el SANS institute

- Construir un plan de recuperación de destares y continuidad de negocio, fundamentado en la identificación y tratamiento eficiente de riesgos principalmente ante la perdida de datos contables o corporativos, por lo que se sugiere iniciar con practicas de almacenamiento y copias de respaldo fuera de infraestructura critica.

- Establecer objetivos e intervalos de tiempo de recuperación de desastres, que incluyan la cantidad máxima aceptable frente a la pérdida de datos **(RPO)**, tiempo de recuperación de los sistemas críticos **(RTO)**,tiempo de recuperación de operaciones **(WRT)**, tiempo de inactividad máxima **(MTD)**, resultado de la suma de **RTO + WRT**.

- Evaluar iniciativas de migración al entorno de nube segura para el hospedaje de la infraestructura critica del proceso contable.

- Programar y ejecutar tareas de mantenimiento de hardware y actualización de software a las versiones mas estables a nivel de seguridad y rendimiento.
- Asegurar la red por medio de la implementación de protecciones perimetrales que limiten los movimientos laterales, permitan segmentación de red y separación virtual de los datos sensibles. Para lo cual se sugiere validar el Security Tip (ST18-001) publicado por el Cybersecurity and Infrastructure Security Agency CISA.
- Apoyarse periódicamente en las publicaciones y recursos entregados por entidades nacionales o internacionales de carácter privado o gubernamental, dentro de las cuales se recomiendan:
    - IFAC Guide to Practice Management for Small- and Medium-Sized Practices
    - ISO/IEC 27002:2013. "Guía de buenas prácticas en base a objetivos controles recomendables para seguridad de la información"
    - Federal Trade Commission Cibersecurity for Small Busines.
    - Federal Trade Commission "Privacy and Security.
    - NIST Small Business Cybersecurity Corner. principalmete los titulos
    - Ministerio de Tecnologías de la Información y las Comunicaciones Guía para la Implementación de Seguridad de la Información en una MIPYME.
    - Ministerio de Tecnologías de la Información y las Comunicaciones Guía para la Implementación de Seguridad de la Información en una MIPYME.
    - Ministerio de Tecnologías de la Información y las Comunicaciones Modelo de Seguridad y Privacidad de la Información.
    - CISA Infraestructure Security
    - INCIBE "Herramientas"; "Formación"; "Guías"

Referencias

[1] Camilo Gutiérrez Amaya. *2021 un año desafiante en materia de ciberseguridad*. 2021. URL: `https://www.itseller.cl/2021/09/15/2021-un-ano-desafiante-en-materia-de-ciberseguridad/` (visitado 30-06-2019).

[2] ICONTEC. *GTC-ISO-IEC 27002:2015*. 2016. URL: `https://ecollection.icontec.org/normavw.aspx?ID=308` (visitado 06-11-2021).

[3] Execellence ISOTools. *Novedades de la ISO 27002 de mejores prácticas en la gestión de seguridad de la información*. 2016. URL: https://www.isotools.org/2016/01/05/novedades-de-la-iso-27002-de-mejores-practicas-en-la-gestion-de-seguridad-de-la-informacion/ (visitado 06-11-2021).

[4] Muñoz Hernández Helmer; Zapata Cantero Laura Giseth; Requena Vidal Dina Marcela; Ricardo Villadiego Leonela. "Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia". En: *Revista Venezolana de Gerencia* 2 (2019), págs. 528-541. URL: https://www.redalyc.org/journal/290/29063446029/html/.

[5] Phil Muncaster. *Los riesgos de las amenazas internas en el modelo de trabajo híbrido*. 2021. URL: https://www.welivesecurity.com/la-es/2021/09/06/riesgos-amenazas-internas-modelo-trabajo-hibrido/ (visitado 17-09-2021).

[6] Myers-Briggs. "The Human Element of Cybersecurity". En: (2020). URL: https://www.itseller.cl/2021/09/15/2021-un-ano-desafiante-en-materia-de-ciberseguridad/ (visitado 30-06-2019).

[7] Organizacion Mundial de la Salud. *Información basíca sobre la COVID-19*. 2020. URL: https://www.who.int/es/news-room/q-a-detail/coronavirus-disease-covid-19 (visitado 27-10-2021).

[8] Lance Spitzner. *The SANS Security Awareness Planning Kit*. 2020. URL: https://www.sans.org/blog/the-sans-security-awareness-planning-kit/ (visitado 27-10-2021).

[9] National Institute of Standars y Technology. *Collaborative Vulnerability Metadata Acceptance Process (CVMAP)*. 2020. URL: https://nvd.nist.gov/vuln/cvmap (visitado 27-10-2021).

[10] National Institute of Standars y Technology. *Cybersecurity Framework CSF*. 2021. URL: https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide (visitado 22-09-2021).

[11] National Institute of Standars y Technology. *SMALL BUSINESS CYBERSECURITY CORNER*. 2020. URL: https://www.nist.gov/itl/smallbusinesscyber/about-contact-us (visitado 21-10-2021).

[12] Ministerio de Tecnologías de la Información y las Comunicaciones. "Guía para la Implementación deSeguridad de la Información en una MIPYME." En: (2016). URL: https://mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf.

9. ANEXOS

9.1. Autodiagnóstico ligero, INCIBE - Kluger Tech.

9.2. Evaluación preliminar de métricas de seguridad Kluger Tech.

9.3. Kluger Tech Scan Nessus.

9.4. Guía básica de trabajo seguro en casa Kluger Tech.

Dependencia tecnológica - teletrabajo

Reiniciar

Tecnología sí pero con seguridad

Seleccione las tecnologías que utiliza en su negocio o aquellas para las que quiera calcular el riesgo.

¿Qué tecnologías utiliza en su empresa?

- [x] Correo electrónico
- [ ] Página web
- [x] Servidor(es) propio(s)
- [x] Teletrabajo
- [ ] Dispositivos móviles (tablet / smartphone / portátiles) con información de empresa

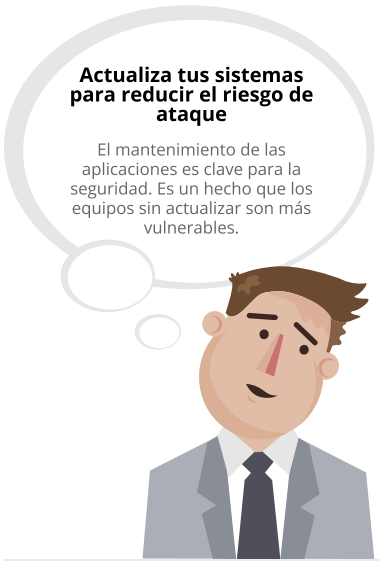
Siguiente pregunta

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar



¿Cómo mantiene sus sistemas informáticos al día?

- (●) Tratamos de mantenerlos nosotros mismos como podemos
- ( ) Nos los mantiene un amigo
- ( ) Tenemos informático en plantilla
- ( ) Subcontratamos el mantenimiento informático

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Tiene algún sistema de protección en sus ordenadores?, y ¿lo utiliza?

- (●) No lo sé
- ( ) No, ninguno
- ( ) Todos los equipos tienen un a… instalado
- ( ) Además de los antivirus tener… cortafuegos implantado en la… empresa
- ( ) Además de antivirus y cortafu… ciframos discos y equipos

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Ha formado recientemente a sus empleados en ciberseguridad?

- (●) Considero que no es necesario
- ( ) Les dimos información para leer
- ( ) Recibieron una charla
- ( ) Fueron a un curso de unos días
- ( ) Al contratar empleados requerimos que hayan recibido algún cursillo

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

No descuides el control de accesos físicos a tu empresa

Los medios tradicionales de seguridad en oficinas han de estar presentes en las salas de equipos y allí donde esté nuestra información.

¿Controla el acceso a sus dependencias?

- [ ] No, el acceso es libre
- [ ] Usamos tarjetas de acceso / llaves
- [ ] Tenemos elementos físicos que bloquean la entrada (por ejemplo, tornos o puertas con control de acceso); solo se permite el acceso identificado
- [ ] Tenemos cámaras de seguridad
- [x] Tenemos un guardia de seguridad que controla los accesos

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

No bajes la guardia con las contraseñas

Las contraseñas dan acceso a nuestros sistemas. Sólo ha de tenerlas quien las necesite y esté autorizado.

¿Tiene definida algún tipo de política de gestión de contraseñas?

- (●) No
- ( ) Sí, el usuario escoge su contraseña
- ( ) Nuestro servidor central nos obliga a cambiar la contraseña cada cierto tiempo
- ( ) Sí, tenemos una política de gestión de contraseñas, bien definida y de obligado cumplimiento

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Cómo se deshace de la información, los soportes y sistemas que no va a utilizar?

- ○ Los tiramos a la basura
- ◉ Tenemos, una destructora de papel, el resto a la basura
- ○ Subcontratamos su destrucción
- ○ Disponemos de una política de destrucción de papeles y soportes; formateamos los soportes y destruimos los papeles según la normativa vigente

Siguiente pregunta

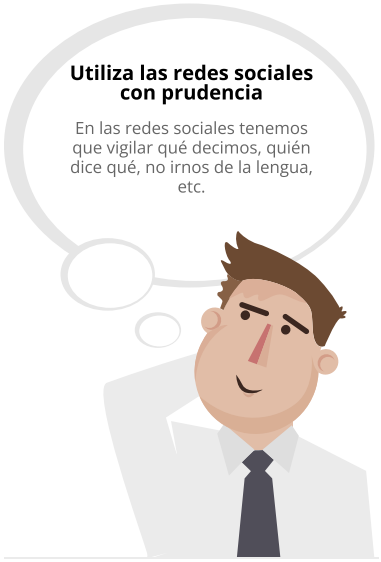
Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar



¿Tiene presencia su empresa en las redes sociales?

- ○ Sí, tenemos una cuenta de Twitter o Facebook... creo
- ◉ Tenemos cuenta en un par de redes sociales, pero las actualizamos sólo cuando hay algo importante
- ○ Tenemos presencia en varias redes sociales y una persona que las mantiene actualizadas (Community Manager)
- ○ No, en ninguna

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Cuánto tiempo podría estar su empresa sin acceso al correo electrónico sin que esto le supusiera un problema?

- ○ Menos de 4 horas
- ◉ Más de 4 horas pero menos de un día
- ○ Entre 1 y 5 días
- ○ Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Con qué frecuencia realiza copias de seguridad de sus equipos y del correo electrónico?

- ○ Cuando me acuerdo
- ◉ Nunca / No lo sé
- ○ Una vez al mes
- ○ Cada semana
- ○ Todos los días

Siguiente pregunta

Pregunta anterior

100
90
80
70
60
50
40
30
20
10
0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Qué servicio de correo electrónico utilizan?

- ○ Usamos un correo gratuito (Gmail, Yahoo, etc.)
- ○ Mantenemos nuestro propio servidor de correo electrónico
- ○ Tenemos nuestro propio servidor de correo, lo mantiene un técnico externo
- ◉ Lo tenemos contratado a una empresa de servicios

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Quién crea y elimina las cuentas de correo electrónico de su empresa?

- ○ Todos los usuarios
- ◉ Algunos usuarios autorizados
- ○ Nuestro informático en plantilla
- ○ La empresa de servicios que nos gestiona el correo

Siguiente pregunta

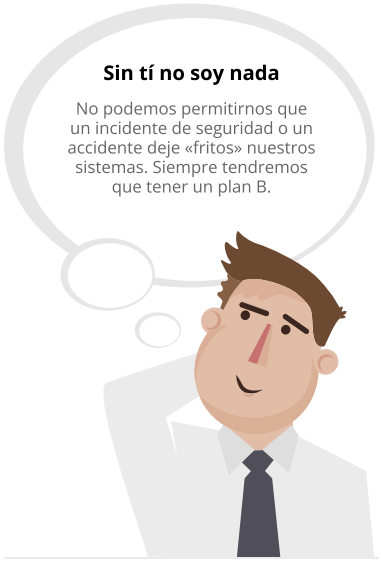
Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar



¿Cuánto tiempo podría estar su empresa con sus sistemas caídos sin que las pérdidas sean considerables?

- ○ Menos de 4 horas
- ◉ Más de 4 horas pero menos de un día
- ○ Entre 1 y 5 días
- ○ Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Con qué frecuencia realiza copias de seguridad de sus sistemas?

Cuando me acuerdo | Nunca / No lo sé | Una vez al mes | Cada se

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Se realizan conexiones remotas a sus sistemas?

- ○ Empleados y clientes a través de la página web
- ◉ Los empleados accediendo a través de una aplicación web / intranet
- ○ Solo yo, de forma segura
- ○ Los empleados pueden acceder a aplicaciones internas en remoto y usar escritorio remoto
- ○ No, nunca

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

Permisos, los justos

Los privilegios y cuentas de administrador estarán restringidos. El daño que se puede causar si se hace un mal uso de los mismos es elevado.

¿Quién tiene privilegios para administrar las aplicaciones internas de la empresa?

- ○ Todos los usuarios
- ◉ Algunos usuarios autorizados
- ○ Solo yo
- ○ Nuestro informático en plantilla
- ○ La empresa de mantenimiento informático que tenemos contratada

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Dónde se encuentran los servidores y routers de su organización?

- (●) Están en una zona de paso
- ( ) En un cuarto compartido
- ( ) En un espacio con acceso restringido
- ( ) En las instalaciones del proveedor

Siguiente pregunta

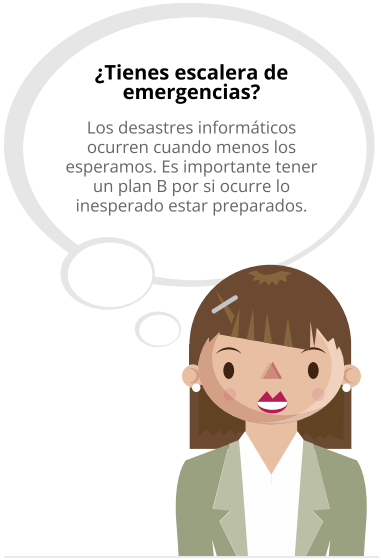
Pregunta anterior

100
90
80
70
60
50
40
30
20
10
0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar



¿Tiene un plan B por si ocurre algún desastre que le impida utilizar sus sistemas de información?

- (●) No
- ( ) Algo pero no lo he probado
- ( ) Sí, está definido pero no lo hemos comprobado
- ( ) Sí, bien definido y comprobado; con copias de seguridad en local
- ( ) Sí, bien definido y comprobado; con copias de seguridad en otra ubicación fuera de la empresa
- ( ) Sí, tenemos incluso servidores redundantes

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Cuánto tiempo podría estar su empresa sin que sus trabajadores puedan trabajar en remoto?

- ○ Menos de 4 horas
- ◉ Más de 4 horas pero menos de un día
- ○ Entre 1 y 5 días
- ○ Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa

Siguiente pregunta

Pregunta anterior

100
90
80
70
60
50
40
30
20
10
0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

Cuestión de cantidad

Cuantas más personas accedan desde el exterior, más riesgos. Recuerda que para gestionar los riesgos tienes que controlar el acceso.

¿Quién realiza conexiones remotas a sus sistemas?

- ○ Empleados accediendo a una aplicación web / intranet sin usar HTTPS
- ○ Los empleados accediendo de forma segura a una aplicación web / intranet (HTTPS)
- ◉ Los empleados pueden acceder a aplicaciones internas en remoto y usar escritorio remoto
- ○ Solo yo, de forma segura

Siguiente pregunta

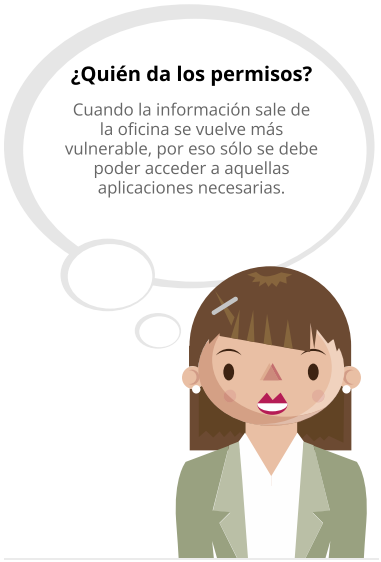
Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar



¿Quién autoriza a qué aplicaciones internas acceden los teletrabajadores?

- ○ Todos los usuarios
- ◉ Algunos usuarios autorizados
- ○ Solo yo
- ○ Nuestro informático de plantilla
- ○ La empresa de mantenimiento informático que tenemos contratada

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Dependencia tecnológica - teletrabajo

Reiniciar

¿Tiene un plan B por si ocurre algún desastre que le impida acceder a los trabajadores remotos?

- ○ No, se quedarían sin trabajar
- ◉ No, tendrían que acudir a las instalaciones de la empresa
- ○ Si, tengo una segunda línea de comunicaciones

Siguiente pregunta

Pregunta anterior

100 90 80 70 60 50 40 30 20 10 0

100.0%

Sector profesional al que pertenece

- ○ No contesta
- ○ Industria
- ○ Construcción
- ○ Salud
- ○ Comercio mayorista
- ○ Comercio minorista
- ○ Ocio
- ○ Logística
- ○ Educación
- ○ Asociaciones
- ◉ Servicios profesionales

Número de empleados

- ○ No contesta
- ○ Gran empresa (> 250 empleados)
- ○ Mediana empresa (50-249 empleados)
- ○ Pequeña empresa (10-49 empleados)
- ◉ Micropyme (1-9 empleados)

¿Contratas servicios externos en ciberseguridad?"

- ○ No contesta
- ○ Sí
- ◉ No

Enviar Omitir

Resumen del diagnóstico

Aún no considera que la seguridad de la información es importante para su empresa o bien cree que la información no es muy esencial para su actividad.

- Analice y clasifique la información que maneja en su empresa (facturas, bases de datos de clientes, contratos, etc.) en función de su confidencialidad, integridad y disponibilidad. Consulte la sección de **Protección de la información**.
- Revise si la información que maneja está sujeta al RGPD y si en su web tiene que cumplir con la LSSI según el apartado de **Cumplimiento Legal**.
- Considere empezar a formar a sus empleados, como indica el apartado de **Desarrollar una cultura de seguridad**.

Ahora que ya conoce el nivel de riesgo de su empresa, ¿quiere conocer el estado de seguridad de sus datos? Puede hacerlo con la **herramienta FACILITA** de la Agencia Española del Protección de Datos.

¿Qué le ha parecido la Herramienta de Autodiagnóstico? Su opinión nos importa, ayúdenos a mejorarla completando la siguiente **Encuesta de Valoración**

El resultado de la encuesta concluye que el riesgo en su empresa es:

86.9%

Este porcentaje está considerado como RIESGO ALTO

Niveles de riesgo

Personas	84.4%	Riesgo *ALTO*	¿Quiere reducirlo?
Procesos	89.4%	Riesgo *ALTO*	¿Quiere reducirlo?
Tecnología	86.8%	Riesgo *ALTO*	¿Quiere reducirlo?

Comparta esta herramienta en las redes sociales

Permita que sus contactos y amigos evalúen los riesgos de seguridad de su negocio en tan solo cinco minutos.

Evaluación preliminar de métricas de seguridad, dirigidas a un programa de concienciación:

Kluger Tech

Contenido

1 Resumen Ejecutivo

La validación de métricas dirigidas a un programa de concientización sobre seguridad de la información repercute en la administración efectiva del riesgo humano, mejorando los comportamientos de la fuerza laboral a través de iniciativas de capacitación basada en identificar las debilidades y falencias del elemento humano principalmente en el área contable debido a que esta se encuentra regulada bajo la protección de datos de terceros.

Un esfuerzo que involucra la fuerza laboral en todos los niveles, con capacitaciones básicas, y capacitaciones dirigidas para abordar roles y riesgos específicos. Como consecuencia, esta iniciativa apoyará de manera segura los datos corporativos de terceros de los cuales depende la operación de la compañía, al tiempo que se da cumplimiento a requisitos reglamentarios, fundamentándose en la identificación del riesgo humano basado en factores comportamentales, culturales y estratégicos asegurando el valor de los datos corporativo a corto y mediano plazo midiendo regularmente el impacto del programa e informando los resultados.

2 Administración de riesgo humano

La identificación y gestión del riesgo humano de forma eficaz no garantiza la eliminación de todos los riesgos, para lo cual para la gestión e identificación de los comportamientos que gestionan esos riesgos de forma más eficaz. Complementan las actividades previas ejecutadas por la compañía, Kluger Tech, identificando como mayor riesgo humano el área contable debido a la inmensa interacción con datos corporativos y de terceros que son clasificados como sensibles y sobre los cuales recae regulaciones como lo son los artículos 269F y 269E contenidos dentro de la ley 1273 de 2009.

Dentro de los riesgos latentes accidentales cómo el envío de un documento por correo electrónico a la persona equivocada debido a la función de autocompletar y deliberados como un ataque de phishing dirigido y actividades que impacten directamente el proceso contable. En adición también se incluyen varios temas de formación complementaria que afectan a otras áreas o roles de la compañía.

La división de riesgos en dos categorías, garantiza brindar capacitación adecuada a las personas adecuadas, aprovechando los recursos limitados de presupuesto de la compañía.

- General: Estos son los riesgos fundamentales compartidos por todos en la organización. Los temas abordan riesgos humanos comunes, como contraseñas y ataques de ingeniería social.

- Área Contable: Estos son riesgos exclusivos de funciones, departamentos o regiones específicos y, a menudo, son impulsados por los datos o sistemas a los que tienen acceso.

2.1 Temario de capacitación

A continuación, se relacionan los temas sugeridos para el inicio de las sesiones de capacitación de acuerdo a la evaluación de riesgos basado en el factor comportamental, estratégico y riesgo humano. Se sugieren temarios distribuidas en una asignación específica hacia el área contable complementaria a la formación dirigida a todo el grupo de colaboradores independiente de su función o rol dentro de la compañía.

Tópico	Factor de riesgo	General	Área contable
Informes de suplantación de identidad (phishing)	Comportamental	X	X
Ingeniería Social	Comportamental	X	X

BYOD	Comportamental	X	X
Seguridad física de dispositivos	Comportamental	X	X
Escritorio Seguro	Comportamental	X	X
Prevención de Ramsomware	Comportamental	X	X
Contraseñas seguras	Comportamental	X	X
Manejo de datos sensibles	Comportamental	X	X
Perdida de datos	Estratégico	X	X
Abuso de privilegios	Estratégico	X	X
Percepción de seguridad	Riesgo Humano	X	X
Disposición de documentos sensibles	Riesgo Humano		X
Destrucción segura de datos sensibles	Riesgo Humano		X

3 Entrenamiento

Se sugiere que previo al lanzamiento del plan de capacitación, este sea comunicado a la fuerza laboral comunicando los objetivos, el alcance y principalmente el PORQUE.

Entrenamiento Primario: El método principal sugerido para ejecutar el programa es el entrenamiento basado en computadora (CBT) lo que permitiría a la fuerza laboral tomar la capacitación a demanda según lo permita su horario e incluir evaluaciones como parte de la capacitación.

Entrenamiento Reforzado: El refuerzo continuo frente a los comportamientos clave a través de múltiples métodos de refuerzo durante el resto del año reforzando un tema clave cada mes. Cada tema reforzado cubrirá material ya cubierto en la capacitación primaria. Aprovechando los eventos públicos, hojas blancas, infografías o blogs publicados por entidades expertas o fabricantes dedicadas a temas relacionados con seguridad de la información o ciberseguridad.

4 Métricas

A continuación, se listan los impactos de las Métricas, que se relacionan directamente con el entorno de la compañía haciendo énfasis en los aspectos comportamentales, culturales, estratégicos, cumplimiento y riesgo humano. Detallando el cómo, quien, cuando medir el impacto.

4.1 Impactos comportamentales:

Métrica	Detalle	Como medir	Quien mide	Cuando Medir
Tasa de clics de phishing	El objetivo es medir quién es víctima de tales ataques. Este número debería disminuir con el tiempo a medida que cambian los comportamientos.	Evaluación de phishing	Equipo de seguridad	Mensual
Informes de phishing	Número de personas que detectan y denuncian un correo electrónico de phishing (independientemente de si se trata de una evaluación o un ataque real).	Evaluación de phishing	Equipo de seguridad	Mensual
Reincidentes de phishing	Número de trabajadores que repetidamente son víctimas de simulaciones de phishing. Estas personas representan un alto riesgo para una organización y deben ser abordadas.	Evaluación de phishing	Equipo de conciencia de seguridad	Mensual
Dispositivos perdidos/robados	Número de dispositivos (computadoras portátiles, teléfonos inteligentes, tabletas) que se perdieron o fueron robados. ¿Qué porcentaje de esos dispositivos estaban encriptados?	Informes al equipo de seguridad o mediante auditorías de activos físicos	Equipo de seguridad o gestión de activos	Mensual
Gestión de Contraseñas	Número de empleados que utilizan contraseñas seguras.	Fuerza bruta de contraseñas	Equipo de seguridad	Mensual o trimestral
Ingeniería Social	Número de empleados que pueden identificar, detener y reportar un ataque de ingeniería social. El equipo de seguridad llama a empleados al azar, atacándolos como lo haría un atacante cibernético real al intentar diseñar socialmente a la víctima.	Evaluaciones de llamadas telefónicas	Equipo de seguridad	Mensual o trimestral
Datos Confidenciales	Número de empleados que publican información confidencial de la organización en los sitios de redes sociales.	Búsquedas en línea de términos clave	Equipo de seguridad	Mensual o trimestral
Borrado destrucción de datos	Número de empleados que siguen correctamente los procesos de destrucción de datos.	Verificación de los dispositivos digitales que se desechan para una limpieza adecuada. Búsqueda de documentos confidenciales.	Aleatorio	Equipo de seguridad de la información

4.2 Impactos culturales.

Métrica	Detalle	Como medir	Quien mide	Cuando Medir
Encuesta de Cultura	Similar a una encuesta de compromiso, pero midiendo las actitudes hacia la ciberseguridad	Encuesta	Equipo de Seguridad o Recursos Humanos	Anual
Grupos Focales	interactúe con un grupo de empleados para comprender mejor sus pensamientos y preocupaciones hacia la ciberseguridad	Entrevistas	Equipo de Seguridad o Recursos Humanos	Trimestral

4.3 Impactos estratégicos

Métrica	Detalle	Como medir	Quien mide	Cuando Medir
Tiempo para detectar un incidente	El tiempo para detectar un incidente debe disminuir a medida que se desarrolla el factor Humano. Esta es una métrica crítica, ya que es clave para crear una organización resiliente.	Seguimiento de informes de incidentes	Equipo de respuesta a incidentes	Mensual
Incidentes de pérdida de datos	Número de veces que hay un incidente de pérdida de datos, ya sea accidental o debido a un ataque deliberado.	Seguimiento de informes de incidentes	Equipo de seguridad	Mensual
Abuso de cuentas privilegiadas	Número de usuarios privilegiados que utilizan indebidamente o abusan de su acceso privilegiado.	Proceso de notificación de infracciones	Equipo de seguridad	Mensual

4.4 Impactos de cumplimiento

Métrica	Detalle	Como medir	Quien mide	Cuando Medir
Finalización de la capacitación	Quién ha completado o no la capacitación anual de concientización sobre seguridad	Hojas de inicio de sesión de talleres	Responsable de la formación primaria	Anual

4.5 Impactos de riesgo humano

Métrica	Detalle	Como medir	Quien mide	Cuando Medir	Como se clasifica
Incidentes de pérdida de datos	Divulgación accidental de datos	Prevención de pérdida de datos (DLP) o algunos otros controles de perímetro	Equipo de seguridad	Mensual	0-2 veces al mes - Muy Bajo (1) 3-5 veces al mes - Baja (2) 5-10 veces al mes - Medio (3) 10-20 veces al mes - Alto (4) Más de 20 veces al mes - Muy alto (5)

Equipos infectados	Número de computadoras infectadas cada mes debido a la acción humana	Solución antivirus centralizada	Equipo de seguridad	Mensual	0-2 veces al mes - Muy Bajo (1) 3-5 veces al mes - Baja (2) 5-10 veces al mes - Medio (3) 10-20 veces al mes - Alto (4) Más de 20 veces al mes - Muy alto (5)
Eliminación de documentos sensibles	Como se están desechando de forma segura cualquier documento confidencial	Búsqueda en contenedores de basura	Equipo de Seguridad de la Información	Mensual	0-2 veces al mes - Muy Bajo (1) 3-5 veces al mes - Baja (2) 5-10 veces al mes - Medio (3) 10-20 veces al mes - Alto (4) Más de 20 veces al mes - Muy alto (5)
Percepciones de seguridad	Medir las percepciones de seguridad de las fuerzas de trabajo, para incluir si se sienten responsables de la seguridad, si saben que son un objetivo.	Aleatorio 5% de la fuerza laboral cada mes.	Equipo de seguridad	Mensual	Medido en una escala de 1-5.

klueger tech.1

Report generated by Nessus™ Fri, 15 Oct 2021 22:32:21 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.20.66

2	5	14	2	51
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Fri Oct 15 22:23:36 2021
End time: Fri Oct 15 22:32:21 2021

Host Information

Netbios Name: KLUGER-CONTABIL
IP: 192.168.20.66
MAC Address: 14:CC:20:11:93:53
OS: Microsoft Windows 7 Professional

Vulnerabilities

73756 - Microsoft SQL Server Unsupported Version Detection (remote check)

Synopsis

An unsupported version of a database server is running on the remote host.

Description

According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

See Also

http://www.nessus.org/u?d4418a57

Solution

Upgrade to a version of Microsoft SQL Server that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

References

XREF IAVA:0001-A-0560

Plugin Information

Published: 2014/04/29, Modified: 2021/04/26

Plugin Output

tcp/49644/mssql

```
The following unsupported installation of Microsoft SQL Server was
detected :


  Installed version : 9.0.4035.0
  Fixed version     : This version is no longer supported.

  SQL Server Instance  : WORLDOFFICE
```

108797 - Unsupported Windows OS (remote)

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

References

XREF IAVA:0001-A-0501

Plugin Information

Published: 2018/04/03, Modified: 2020/09/22

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:

Microsoft Windows 7 Professional
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : CN=Kluger-contabil
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Jul 05 15:30:08 2021 GMT
|-Valid To            : Jan 04 15:30:08 2022 GMT
```

35291 - SSL Certificate Signed Using Weak Hashing Algorithm

Synopsis

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

See Also

https://tools.ietf.org/html/rfc3279

http://www.nessus.org/u?9bb87bf2

http://www.nessus.org/u?e120eea1

http://www.nessus.org/u?5d894816

http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2009/01/05, Modified: 2020/04/27

Plugin Output

tcp/49644/mssql

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

|-Subject             : CN=SSL_Self_Signed_Fallback
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Oct 15 19:51:53 2021 GMT
|-Valid To            : Oct 15 19:51:53 2051 GMT
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

  Name                         Code             KEX           Auth     Encryption             MAC
  ---------------------        ----------       ---           ----     ---------------------  ---
```

```
    DES-CBC3-SHA                0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

References

CVE CVE-2016-2183

Plugin Information

Published: 2009/11/23, Modified: 2021/02/03

Plugin Output

tcp/49644/mssql

```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

  Name                          Code             KEX           Auth     Encryption             MAC
  ----------------------        ----------       ---           ----     ---------------------  ---
```

```
    DES-CBC3-SHA                0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

http://www.nessus.org/u?b06c7e95

http://www.nessus.org/u?247c4540

https://www.openssl.org/~bodo/ssl-poodle.pdf

http://www.nessus.org/u?5d15ba70

https://www.imperialviolet.org/2014/10/14/poodle.html

https://tools.ietf.org/html/rfc7507

https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

High

CVSS v3.0 Base Score

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Plugin Information

Published: 2005/10/12, Modified: 2020/05/06

Plugin Output

tcp/49644/mssql

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                                   RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA                             DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                             DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA                           ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA                           ECDH          RSA      AES-CBC(256)
 SHA1
    AES128-SHA                                     RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                     RSA           RSA      AES-CBC(256)
 SHA1
    RC4-MD5                                        RSA           RSA      RC4(128)               MD5
    RC4-SHA                                        RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Synopsis

It may be possible to get access to the remote host.

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

See Also

http://www.nessus.org/u?8033da0d

http://technet.microsoft.com/en-us/library/cc782610.aspx

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and

- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

Risk Factor

Medium

References

BID	13818
CVE	CVE-2005-1794

Plugin Information

Published: 2005/06/01, Modified: 2021/03/30

Plugin Output

tcp/3389/msrdp

57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

http://www.nessus.org/u?df39b8b3

http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Plugin Information

Published: 2012/01/19, Modified: 2021/03/15

Plugin Output

tcp/445/cifs

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=Kluger-contabil
|-Issuer  : CN=Kluger-contabil
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

Plugin Information

Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/49644/mssql

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=SSL_Self_Signed_Fallback
|-Issuer  : CN=SSL_Self_Signed_Fallback
```

45411 - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Plugin Information

Published: 2010/04/03, Modified: 2020/04/27

Plugin Output

tcp/49644/mssql

```
The identities known by Nessus are :

  192.168.20.66
  192.168.20.66

The Common Name in the certificate is :

  SSL_Self_Signed_Fallback
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    RC4-MD5                       0x00, 0x04        RSA           RSA      RC4(128)               MD5
    RC4-SHA                       0x00, 0x05        RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac7327a0

http://cr.yp.to/talks/2013.03.12/slides.pdf

http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

CVSS v3.0 Base Score

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

References

BID	58796
BID	73684
CVE	CVE-2013-2566
CVE	CVE-2015-2808

Plugin Information

Published: 2013/04/05, Modified: 2021/02/03

Plugin Output

tcp/49644/mssql

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX           Auth     Encryption             MAC
    ----------------------        ----------        ---           ----     ---------------------  ---
    RC4-MD5                       0x00, 0x04        RSA           RSA      RC4(128)               MD5
    RC4-SHA                       0x00, 0x05        RSA           RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/3389/msrdp

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=Kluger-contabil
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

Plugin Information

Published: 2012/01/17, Modified: 2020/04/27

Plugin Output

tcp/49644/mssql

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=SSL_Self_Signed_Fallback
```

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

CVSS v3.0 Base Score

6.8 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N)

References

BID	70574
CVE	CVE-2014-3566

XREF CERT:577193

Plugin Information

Published: 2014/10/15, Modified: 2020/06/12

Plugin Output

tcp/49644/mssql

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/3389/msrdp

```
TLSv1 is enabled and the server supports at least one cipher.
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

Plugin Information

Published: 2017/11/22, Modified: 2020/03/31

Plugin Output

tcp/49644/mssql

```
TLSv1 is enabled and the server supports at least one cipher.
```

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Synopsis

The remote Terminal Services doesn't use Network Level Authentication only.

Description

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)

http://www.nessus.org/u?e2628096

Solution

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Risk Factor

Medium

CVSS v3.0 Base Score

4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N)

Plugin Information

Published: 2012/03/23, Modified: 2021/07/12

Plugin Output

tcp/3389/msrdp

```
Nessus was able to negotiate non-NLA (Network Level Authentication) security.
```

57690 - Terminal Services Encryption Level is Medium or Low

Synopsis

The remote host is using weak cryptography.

Description

The remote Terminal Services service is not configured to use strong cryptography.

Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

Solution

Change RDP encryption level to one of :

3. High

4. FIPS Compliant

Risk Factor

Medium

Plugin Information

Published: 2012/01/25, Modified: 2021/07/12

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :

2. Medium
```

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Synopsis

The X.509 certificate chain used by this service contains certificates with RSA keys shorter than 2048 bits.

Description

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

See Also

https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Risk Factor

Low

Plugin Information

Published: 2013/09/03, Modified: 2018/11/15

Plugin Output

tcp/49644/mssql

```
The following certificates were part of the certificate chain
sent by the remote host, but contain RSA keys that are considered
to be weak :

|-Subject        : CN=SSL_Self_Signed_Fallback
|-RSA Key Length : 1024 bits
```

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant

Synopsis

The remote host is not FIPS-140 compliant.

Description

The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant.

Solution

Change RDP encryption level to :

4. FIPS Compliant

Risk Factor

Low

Plugin Information

Published: 2008/02/11, Modified: 2021/07/12

Plugin Output

tcp/3389/msrdp

```
The terminal services encryption level is set to :

2. Medium (Client Compatible)
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

See Also

http://cpe.mitre.org/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2021/07/22

Plugin Output

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_7:::professional

Following application CPE matched on the remote system :

  cpe:/a:microsoft:sql_server:9.0.4035.0
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/135/epmap

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc08CDD0

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc08CDD0

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
```

```
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-10cdc6ac2275ca4531

Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc0918A1

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc0918A1

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4b112204-0e19-11d3-b42b-0000f81feb9f, version 1.0
Description : SSDP service
Windows process : unknow
Type : Local RPC service
Named pipe : LRPC-9f5f7b9fc4ff2b1336

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Local RPC service
Named pipe : LRPC-da28439b4b066c8cb8

Object UUID : 00000000- [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/445/cifs

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\KLUGER-CONTABIL

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\KLUGER-CONTABIL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f1343fe-50a9-4927-a778-0c5859517bac, version 1.0
Description : Unknown RPC service
Annotation : DfsDs service
Type : Remote RPC service
Named pipe : \PIPE\wkssvc
Netbios name : \\KLUGER-CONTABIL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b58aa02e-2884-4e97-8176-4ee06d794184, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
```

```
Named pipe : \pipe\trkwks
Netbios name : \\KLUGER-CONTABIL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\KLUGER-CONTABIL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 1.0
Description : Unknown RPC service
Annotation : KeyIso
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\KLUGER-CONTABIL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\KLUGER-CONTABIL

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\KLUGER-CONTABIL

Obj [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49152/dce-rpc

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.20.66
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49153/dce-rpc

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 06bba54a-be05-49f9-b0a0-30f790261023, version 1.0
Description : Unknown RPC service
Annotation : Security Center
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.20.66
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49154/dce-rpc

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
```

```
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.20.66

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1.0
Description : Unknown RPC service
Annotation : AppInfo
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.20.66

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1.0
Description : Unknown RPC service
Annotation : AppInfo [...]
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49156/dce-rpc

```
The following DCERPC services are available on TCP port 49156 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
TCP Port : 49156
IP : 192.168.20.66
```

10736 - DCE Services Enumeration

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2020/08/20

Plugin Output

tcp/49213/dce-rpc

```
The following DCERPC services are available on TCP port 49213 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49213
IP : 192.168.20.66
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 99
```

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

https://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/02/19, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :

14:CC:20:11:93:53 : TP-LINK TECHNOLOGIES CO.,LTD.
```

86420 - Ethernet MAC Addresses

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/10/16, Modified: 2020/05/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
  - 14:CC:20:11:93:53
```

108761 - MSSQL Host Information in NTLM SSP

Synopsis

Nessus can obtain information about the host by examining the NTLM SSP message.

Description

Nessus can obtain information about the host by examining the NTLM SSP challenge issued during NTLM authentication, over MSSQL.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/03/30, Modified: 2021/09/27

Plugin Output

tcp/49644/mssql

```
Nessus was able to obtain the following information about the host, by
parsing the MSSQL server's NTLM SSP message:

Target Name:           KLUGER-CONTABIL
NetBIOS Domain Name:   KLUGER-CONTABIL
NetBIOS Computer Name: KLUGER-CONTABIL
DNS Domain Name:       Kluger-contabil
DNS Computer Name:     Kluger-contabil
DNS Tree Name:         unknown
Product Version:       6.1.7601
```

69482 - Microsoft SQL Server STARTTLS Support

Synopsis

The remote service supports encrypting traffic.

Description

The remote Microsoft SQL Server service supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.

See Also

https://msdn.microsoft.com/en-us/library/dd304523.aspx

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/07/04, Modified: 2021/02/24

Plugin Output

tcp/49644/mssql

```
Here is the Microsoft SQL Server's SSL certificate that Nessus
was able to collect after sending a pre-login packet :

------------------------------ snip ------------------------------
Subject Name:

Common Name: SSL_Self_Signed_Fallback

Issuer Name:

Common Name: SSL_Self_Signed_Fallback

Serial Number: 49 7E 4D 7A D9 61 F0 BC 44 AD EE 72 CA D7 72 76

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 15 19:51:53 2021 GMT
Not Valid After: Oct 15 19:51:53 2051 GMT

Public Key Info:
```

```
Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 CD B7 02 A9 50 6E 15 0A BF D7 BF 87 3F CB 74 EF 8F 7F 6C
            E0 CC FC C6 12 F9 BE D4 95 60 82 E9 0C 45 E6 9A F7 4C C6 E4
            E2 0B 36 D8 7E A4 37 65 2A 4A 0A C7 8B F9 30 66 31 B3 AC A1
            79 C9 AF 44 C7 95 FD 32 55 84 69 4F 79 F1 14 C9 48 11 98 5F
            5E D6 1A 12 0E 5D 8F 23 A0 A8 BA 40 62 DB 80 72 04 B1 4C FA
            62 C2 79 4F 0D AC A2 E8 04 90 54 91 2F 94 DE D6 37 6D 66 58
            14 90 C2 8A A8 BA BD 3C CD
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 4C 17 5D C3 1D DD 30 41 BB 84 22 02 08 45 D3 61 EA 98 4C
           31 74 89 17 D8 2D DA 6F 8A 03 EE DB 49 7E DA 36 93 A8 79 48
           4D E6 4B 5F 83 ED 2E 4E 77 36 30 AC 51 15 29 57 82 A1 BB 2A
           28 35 40 E3 66 97 2B 0A FA A8 80 90 E7 C3 F7 E4 62 2C DA FC
           6F C4 E1 8D 2B 0A 5F 06 D0 11 2B 3D 3A 93 4D D7 23 CF 73 78
           19 DC 86 2A E2 92 BA 2C 0D D0 2C ED AA 17 D3 B9 97 85 1A 7A
           EA 04 78 E8 B3 67 F3 51 93


------------------------------ snip ------------------------------


  SQL Server Version   : 9.0.4035.0
  SQL Server Instance  : WORLDOFFICE
```

10144 - Microsoft SQL Server TCP/IP Listener Detection

Synopsis

A database server is listening on the remote port.

Description

The remote host is running MSSQL, a database server from Microsoft. It is possible to extract the version number of the remote installation from the server pre-login response.

Solution

Restrict access to the database to allowed IPs only.

Risk Factor

None

References

XREF IAVT:0001-T-0800

Plugin Information

Published: 1999/10/12, Modified: 2021/03/15

Plugin Output

tcp/49644/mssql

```
Service      : mssql-WORLDOFFICE
Version      : 9.0.4035.0
InstanceName : WORLDOFFICE
Note         : The remote MSSQL server accepts cleartext logins.
```

10674 - Microsoft SQL Server UDP Query Remote Version Disclosure

Synopsis

It is possible to determine the remote SQL server version.

Description

Microsoft SQL server has a function wherein remote users can query the database server for the version that is being run. The query takes place over the same UDP port that handles the mapping of multiple SQL server instances on the same machine.

It is important to note that, after Version 8.00.194, Microsoft decided not to update this function. This means that the data returned by the SQL ping is inaccurate for newer releases of SQL Server.

Solution

If there is only a single SQL instance installed on the remote host, consider filter incoming traffic to this port.

Risk Factor

None

Plugin Information

Published: 2001/05/25, Modified: 2018/03/13

Plugin Output

udp/1434

```
A 'ping' request returned the following information about the remote
SQL instance :

  ServerName   : KLUGER-CONTABIL
  InstanceName : WORLDOFFICE
  IsClustered  : No
  Version      : 9.00.4035.00
  tcp          : 49644
  np           : \\KLUGER-CONTABIL\pipe\MSSQL$WORLDOFFICE\sql\query
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows 7 Professional 7601 Service Pack 1
The remote native LAN manager is : Windows 7 Professional 6.1
The remote SMB Domain Name is : KLUGER-CONTABIL
```

26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

Synopsis

Nessus is not able to access the remote Windows Registry.

Description

It was not possible to connect to PIPE\winreg on the remote host.

If you intend to use Nessus to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access'

service (winreg) has been disabled on the remote host or can not be connected to with the supplied credentials.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0506

Plugin Information

Published: 2007/10/04, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
Could not connect to the registry because:
Could not connect to \winreg
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

```
A CIFS server is running on this port.
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/09, Modified: 2020/03/11

Plugin Output

tcp/445/cifs

```
The remote host supports the following SMB dialects :
_version_  _introduced in windows version_
2.0.2      Windows 2008
2.1        Windows 7

The remote host does NOT support the following SMB dialects :
_version_  _introduced in windows version_
2.2.2      Windows 8 Beta
2.2.4      Windows 8 Beta
3.0        Windows 8
3.0.2      Windows 8.1
3.1        Windows 10
3.1.1      Windows 10
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/135/epmap

```
Port 135/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/139

```
Port 139/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/445/cifs

```
Port 445/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2021/09/16

Plugin Output

tcp/3389/msrdp

```
Port 3389/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2021/09/27

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.15.1
Nessus build : 20272
Plugin feed version : 202110020341
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : klueger tech.1
```

```
Scan policy used : Advanced Scan
Scanner IP : 10.0.5.4
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 65.776 ms
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/10/15 22:23 EDT
Scan duration : 504 sec
```

24786 - Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.

Description

The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third-party patch auditing tools) or to false negatives (not all patches can be detected through the registry).

Solution

Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor

None

References

XREF IAVB:0001-B-0505

Plugin Information

Published: 2007/03/12, Modified: 2020/09/22

Plugin Output

tcp/0

```
It was not possible to connect to '\\KLUGER-CONTABIL\ADMIN$' with the supplied credentials.
```

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2021/09/27

Plugin Output

tcp/0

```
Remote operating system : Microsoft Windows 7 Professional
Confidence level : 99
Method : MSRPC


The remote host is running Microsoft Windows 7 Professional
```

117886 - OS Security Patch Assessment Not Available

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.

This does not necessarily indicate a problem with the scan.

Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

  - Plugin      : no_local_checks_credentials.nasl
    Plugin ID   : 110723
    Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
    Message     :
Credentials were not provided for detected SMB service.
```

66173 - RDP Screenshot

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/22, Modified: 2021/07/12

Plugin Output

tcp/3389/msrdp

```
It was possible to gather the following screenshot of the remote login screen.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2021/02/03

Plugin Output

tcp/49644/mssql

```
This port supports SSLv3/TLSv1.0.
```

45410 - SSL Certificate 'commonName' Mismatch

Synopsis

The 'commonName' (CN) attribute in the SSL certificate does not match the hostname.

Description

The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens.

Solution

If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate.

Risk Factor

None

Plugin Information

Published: 2010/04/03, Modified: 2021/03/09

Plugin Output

tcp/49644/mssql

```
The host name known by Nessus is :

  kluger-contabil

The Common Name in the certificate is :

  ssl_self_signed_fallback
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: Kluger-contabil

Issuer Name:

Common Name: Kluger-contabil

Serial Number: 3D A5 E8 E1 C1 22 01 A9 4B AF DC 9F CB DE EF AB

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jul 05 15:30:08 2021 GMT
Not Valid After: Jan 04 15:30:08 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A8 FF A6 F6 B6 71 25 16 6A 30 71 FA B3 18 28 48 45 8E C6
            EF CC F3 6D 93 88 22 7D 89 7D 95 4D F5 DA CC D1 6E 1D 46 B0
            68 B5 9B A6 1D 4A 05 97 8F 3E 3C 95 A1 F8 1B 09 07 3C D2 AA
            D3 68 22 04 FD 3B 20 B3 B7 82 48 82 5D A8 A1 8A 81 78 36 65
            45 0E 3A 3F 9F 54 24 92 A2 90 6A 07 DD 15 DB E1 D6 64 C1 DE
            A4 D3 57 84 CD 10 6C 08 71 19 23 F5 09 B9 11 C2 FC 91 4A C9
            6A 65 DA 31 4C 97 6A 75 B2 16 70 B7 6C A1 47 F9 4A B7 C2 D7
            D4 F3 17 32 3C FA D8 05 AF 26 31 90 AA C2 37 34 D9 94 F0 52
            0B 96 B9 75 EC 0D 35 0C 0C 3D 3B 8E D5 7D 29 52 A7 EC 10 CF
            87 AC 75 20 B6 CF 37 18 3F 5B 7A 2B A1 67 B1 EF 0F 49 A2 95
            C3 84 97 C6 E2 E0 4A 58 BE 9C 4B A9 98 68 60 3D 73 D5 E0 21
```

```
             72 48 20 F6 16 51 F0 32 FD 47 76 0A 62 64 B3 23 F5 8C F1 EA
             48 20 AB 5B EB 1C C4 C8 5B 1B 96 E5 D3 0A 83 0C 5F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 07 E6 E5 5E 6C 98 6E 74 8B 6B 20 6C 31 AA C0 8C 88 5D 78
           94 FD CD B3 43 43 97 CF 9B BB EA F9 90 B4 47 89 0F F1 3E F4
           9F 26 01 C5 F2 BA 4B EB 4E 60 91 4C 16 B3 30 12 B2 C5 6E 5A
           50 49 40 F4 C1 06 25 7D CF 5A CC 93 C5 AB 79 47 8B 2F 2C D5
           2D F5 CE 6F 0F 5B A0 F2 91 50 3F 4B 10 62 D1 E6 9C C1 19 23
           37 9B 2F 0E 29 95 9E 1D 97 87 C5 89 BC 09 71 4F 64 ED 8B E3
           ED F7 7E 3C 92 DC 6F 1C 43 E3 DF B2 00 A5 07 D4 82 32 89 9B
           B3 0C 7A 1E F7 93 4E 47 5C A3 4A 94 AB E6 B7 30 6E B9 D0 F3
           62 6E 45 3D 28 2D 6A 61 CF 4E 4C 11 89 51 3F DD 79 D0 31 2C
           BB 56 EF 0E 89 83 27 [...]
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2021/02/03

Plugin Output

tcp/49644/mssql

```
Subject Name:

Common Name: SSL_Self_Signed_Fallback

Issuer Name:

Common Name: SSL_Self_Signed_Fallback

Serial Number: 49 7E 4D 7A D9 61 F0 BC 44 AD EE 72 CA D7 72 76

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Oct 15 19:51:53 2021 GMT
Not Valid After: Oct 15 19:51:53 2051 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 1024 bits
Public Key: 00 CD B7 02 A9 50 6E 15 0A BF D7 BF 87 3F CB 74 EF 8F 7F 6C
            E0 CC FC C6 12 F9 BE D4 95 60 82 E9 0C 45 E6 9A F7 4C C6 E4
            E2 0B 36 D8 7E A4 37 65 2A 4A 0A C7 8B F9 30 66 31 B3 AC A1
            79 C9 AF 44 C7 95 FD 32 55 84 69 4F 79 F1 14 C9 48 11 98 5F
            5E D6 1A 12 0E 5D 8F 23 A0 A8 BA 40 62 DB 80 72 04 B1 4C FA
            62 C2 79 4F 0D AC A2 E8 04 90 54 91 2F 94 DE D6 37 6D 66 58
            14 90 C2 8A A8 BA BD 3C CD
Exponent: 01 00 01

Signature Length: 128 bytes / 1024 bits
Signature: 00 4C 17 5D C3 1D DD 30 41 BB 84 22 02 08 45 D3 61 EA 98 4C
```

```
            31 74 89 17 D8 2D DA 6F 8A 03 EE DB 49 7E DA 36 93 A8 79 48
            4D E6 4B 5F 83 ED 2E 4E 77 36 30 AC 51 15 29 57 82 A1 BB 2A
            28 35 40 E3 66 97 2B 0A FA A8 80 90 E7 C3 F7 E4 62 2C DA FC
            6F C4 E1 8D 2B 0A 5F 06 D0 11 2B 3D 3A 93 4D D7 23 CF 73 78
            19 DC 86 2A E2 92 BA 2C 0D D0 2C ED AA 17 D3 B9 97 85 1A 7A
            EA 04 78 E8 B3 67 F3 51 93

Fingerprints :

SHA-256 Fingerprint: 30 E2 B9 A2 EA EF 3A 9A 7F 2E C3 5D 87 9E 7D 70 27 51 9D AF
                     0D D0 C3 58 79 7C 20 D0 6B 47 CB 4F
SHA-1 Fingerprint: 45 46 B8 5C 64 03 B4 0E 66 C0 B3 4B CD B5 F0 69 C5 36 ED D0
MD5 Fingerprint: 3E 13 5A 22 8E 61 8B FA 9D 16 C7 27 AA 20 21 A4


PEM certificate :

-----BEGIN CERTIFICATE-----
MIIB
+zCCAWSgAwIBAgIQSX5Netlh8LxEre5yytdydjANBgkqhkiG9w0BAQUFADA7MTkwNwYDVQQDHjAAUwBTAEwAXwBTAGUAbABmAF8AUwBpAGcAbgBlAG
 [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
```

```
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH           RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH           RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA            RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH           RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH           RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA            RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA            RSA      AES-CBC(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2021/02/03

Plugin Output

tcp/49644/mssql

```
Here is the list of SSL CBC ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DES-CBC3-SHA                  0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption             MAC
    ----------------------        ----------       ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA            0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA            0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
```

```
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDH           RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH           RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA            RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA            RSA      AES-CBC(256)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code             KEX           Auth     Encryption             MAC
    ----------------------      ----------       ---           ----     --------------------   ---
    DES-CBC3-SHA                0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                        Code             KEX           Auth     Encryption             MAC
    ----------------------      ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA256       0x00, 0x9E       DH            RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384       0x00, 0x9F       DH            RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256           0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384           0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
```

```
   DHE-RSA-AES128-SHA          0x00, 0x33      DH          RSA     AES-CBC(128)
SHA1
   DHE-RSA-AES256-SHA          0x00, 0x39      DH          RSA     AES-CBC(256)
SHA1
   ECDHE-RSA-AES128-SHA        0xC0, 0x13      ECDH        RSA     AES-CBC(128)
SHA1
   ECDHE-RSA-AES256-SHA        0xC0, 0x14      ECDH        RSA     AES-CBC(256)
SHA1
   AES128-SHA                  0x00, 0x2F      RSA         RSA     AES-CBC(128)
SHA1
   AES256-SHA                  0x00, 0x35      RSA         RSA     AES-CBC(256)
SHA1
   RC4-MD5                     0x00, 0x04      RSA         RSA     RC4(128)              MD5
   RC4-SHA                     0x00, 0x05      RSA         RSA     RC4(128)
SHA1
   ECDHE-RSA-AES128-SHA256     0xC0, 0x27      ECDH        RSA     AE [...]
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2021/03/09

Plugin Output

tcp/49644/mssql

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv1
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code             KEX           Auth     Encryption             MAC
    ----------------------      ----------       ---           ----     --------------------   ---
    DES-CBC3-SHA                0x00, 0x0A       RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                        Code             KEX           Auth     Encryption             MAC
    ----------------------      ----------       ---           ----     --------------------   ---
    DHE-RSA-AES128-SHA          0x00, 0x33       DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA          0x00, 0x39       DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA        0xC0, 0x13       ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
```

```
    AES128-SHA                  0x00, 0x2F      RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                  0x00, 0x35      RSA           RSA      AES-CBC(256)
 SHA1
    RC4-MD5                     0x00, 0x04      RSA           RSA      RC4(128)              MD5
    RC4-SHA                     0x00, 0x05      RSA           RSA      RC4(128)
 SHA1


SSL Version : SSLv3
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code            KEX           Auth     Encryption            MAC
    ----------------------      ----------      ---           ----     --------------------  ---
    DES-CBC3-SHA                0x00, 0x0A      RSA           RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                        Code            KEX      [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/3389/msrdp

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                         Code             KEX          Auth     Encryption             MAC
    ----------------------       ----------       ---          ----     ---------------------  ---
    DHE-RSA-AES128-SHA256        0x00, 0x9E       DH           RSA      AES-GCM(128)
 SHA256
    DHE-RSA-AES256-SHA384        0x00, 0x9F       DH           RSA      AES-GCM(256)
 SHA384
    DHE-RSA-AES128-SHA           0x00, 0x33       DH           RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA           0x00, 0x39       DH           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA         0xC0, 0x13       ECDH         RSA      AES-CBC(128)
 SHA1
```

```
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDH          RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDH          RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDH          RSA      AES-CBC(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

https://en.wikipedia.org/wiki/Perfect_forward_secrecy

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2021/03/09

Plugin Output

tcp/49644/mssql

```
Here is the list of SSL PFS ciphers supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    Name                        Code              KEX           Auth     Encryption             MAC
    ----------------------      ----------        ---           ----     ---------------------  ---
    DHE-RSA-AES128-SHA          0x00, 0x33        DH            RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA          0x00, 0x39        DH            RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA        0xC0, 0x13        ECDH          RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA        0xC0, 0x14        ECDH          RSA      AES-CBC(256)
 SHA1

The fields above are :
```

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/3389/msrdp

```
This port supports resuming TLSv1 / TLSv1 / TLSv1 sessions.
```

51891 - SSL Session Resume Supported

Synopsis

The remote host allows resuming SSL sessions.

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/02/07, Modified: 2021/09/13

Plugin Output

tcp/49644/mssql

```
This port supports resuming SSLv3 sessions.
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/help/2696547/how-to-detect-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?234f8ef8

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2020/09/22

Plugin Output

tcp/445/cifs

```
The remote host supports SMBv1.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2020/08/07

Plugin Output

tcp/3389/msrdp

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information

Published: 2020/05/04, Modified: 2020/05/04

Plugin Output

tcp/3389/msrdp

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2021/08/30

Plugin Output

tcp/0

```
SMB was detected on port 445 but no credentials were provided.
SMB local checks were not enabled.
```

64814 - Terminal Services Use SSL/TLS

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2021/02/24

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: Kluger-contabil

Issuer Name:

Common Name: Kluger-contabil

Serial Number: 3D A5 E8 E1 C1 22 01 A9 4B AF DC 9F CB DE EF AB

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Jul 05 15:30:08 2021 GMT
Not Valid After: Jan 04 15:30:08 2022 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 A8 FF A6 F6 B6 71 25 16 6A 30 71 FA B3 18 28 48 45 8E C6
            EF CC F3 6D 93 88 22 7D 89 7D 95 4D F5 DA CC D1 6E 1D 46 B0
            68 B5 9B A6 1D 4A 05 97 8F 3E 3C 95 A1 F8 1B 09 07 3C D2 AA
            D3 68 22 04 FD 3B 20 B3 B7 82 48 82 5D A8 A1 8A 81 78 36 65
            45 0E 3A 3F 9F 54 24 92 A2 90 6A 07 DD 15 DB E1 D6 64 C1 DE
            A4 D3 57 84 CD 10 6C 08 71 19 23 F5 09 B9 11 C2 FC 91 4A C9
            6A 65 DA 31 4C 97 6A 75 B2 16 70 B7 6C A1 47 F9 4A B7 C2 D7
            D4 F3 17 32 3C FA D8 05 AF 26 31 90 AA C2 37 34 D9 94 F0 52
            0B 96 B9 75 EC 0D 35 0C 0C 3D 3B 8E D5 7D 29 52 A7 EC 10 CF
            87 AC 75 20 B6 CF 37 18 3F 5B 7A 2B A1 67 B1 EF 0F 49 A2 95
            C3 84 97 C6 E2 E0 4A 58 BE 9C 4B A9 98 68 60 3D 73 D5 E0 21
```

```
             72 48 20 F6 16 51 F0 32 FD 47 76 0A 62 64 B3 23 F5 8C F1 EA
             48 20 AB 5B EB 1C C4 C8 5B 1B 96 E5 D3 0A 83 0C 5F
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 07 E6 E5 5E 6C 98 6E 74 8B 6B 20 6C 31 AA C0 8C 88 5D 78
           94 FD CD B3 43 43 97 CF 9B BB EA F9 90 B4 47 89 0F F1 3E F4
           9F 26 01 C5 F2 BA 4B EB 4E 60 91 4C 16 B3 30 12 B2 C5 6E 5A
           50 49 40 F4 C1 06 25 7D CF 5A CC 93 C5 AB 79 47 8B 2F 2C D5
           2D F5 CE 6F 0F 5B A0 F2 91 50 3F 4B 10 62 D1 E6 9C C1 19 23
           37 9B 2F 0E 29 95 9E 1D 97 87 C5 89 BC 09 71 4F 64 ED 8B E3
           ED F7 7E 3C 92 DC 6F 1C 43 E3 DF B2 00 A5 07 D4 82 32 89 9B
           B3 0C 7A 1E F7 93 4E 47 5C A3 4A 94 AB E6 B7 30 6E B9 D0 F3
           62 6E 45 3D 28 2D 6A 61 CF 4E 4C 11 89 51 3F DD 79 D0 31 2C
           BB 56 EF 0E 89 83 27 [...]
```

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2020/08/20

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.5.4 to 192.168.20.66 :
10.0.5.4
192.168.20.66

Hop Count: 1
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.

Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2020/04/21, Modified: 2021/09/27

Plugin Output

tcp/445/cifs

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 6 NetBIOS names have been gathered :

 KLUGER-CONTABIL  = File Server Service
 KLUGER-CONTABIL  = Computer name
 WORKGROUP        = Workgroup / Domain name
 WORKGROUP        = Browser Service Elections
 WORKGROUP        = Master Browser
 __MSBROWSE__     = Master Browser

The remote host has the following MAC address on its adapter :

   14:cc:20:11:93:53
```

10940 - Windows Terminal Services Enabled

Synopsis

The remote Windows host has Terminal Services enabled.

Description

Terminal Services allows a Windows user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable Terminal Services if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2020/07/08

Plugin Output

tcp/3389/msrdp

Guía básica de trabajo seguro en casa:

Kluger Tech

Contenido

1 Resumen Ejecutivo

La implantación de escenarios de trabajo remoto, en gran medida no cuentan con modelos adecuados para el tratamiento de información corporativa lo que incrementa las posibilidades de materialización de riesgos asociados con la seguridad de la información o seguridad informática. Desencadenando en una serie de posibles problemáticas que podrían afectar directamente la continuidad de las operaciones a través de perdida de información sensible, pérdidas económicas o reputacionales.

El uso de una única contraseña, corta o predecible, la exposición constante a ataques de phishing, la poca actualización de firmware o parches, y sobre todo el uso de una red domestica insegura. Son algunos de los factores que ponen en riesgo la integridad, disponibilidad y confidencialidad de la información corporativa.

Buscando reducir la brecha de exposición, es pertinente establecer procedimientos y acciones preventivas que extiendan las capas de seguridad de nivel corporativo hacia el entorno hogar. Fundamentado en buenas prácticas y en los resultados de planes de concientización, lograr espacios de trabajo remoto seguro, podría dejar de ser una labor extra para la compañía, que requiera grandes inversiones monetarias a formar parte de la estrategia y acciones de seguridad de la información e informática.

2 Introducción.

Esta guía busca entregar recomendaciones prácticas que mejoren aspectos de seguridad de la información e informática principalmente en el área contable. Siendo complemento al modelo de plan de concientización basado en el factor humano, esta guía busca minimizar la exposición de brechas de seguridad basado en prácticas que no requerían gran experiencia en la administración o configuración de equipos informáticos o de seguridad o que representen gran inversión económica para la compañía Kluger Tech.

La creación de políticas ayudara a tener una guía del procedimiento adecuado frente al manejo de malas practicas o brechas de seguridad que puedan presentarse en el entorno hogar. EN cuanto la aplicación de acciones preventivas minimizara la materialización de los riesgos a los que se exponen la fuerza laboral y el entono corporativo en una red insegura.

3 Recomendaciones generales

Precauciones generales que no requieren de gran experiencia técnica son puntos de partida para el aseguramiento del trabajo remoto en casa, y minimizar los riesgos asociado a malas practicas presentes en una red hogar.

A continuación, se listan recomendaciones de buenas prácticas de acuerdo al nivel de experiencia o requerimiento técnico dirigidas a la fuerza laboral con actividades de trabajo en casa.

Nivel de experiencia o requerimiento técnico	**Ninguno**
• Utilizar únicamente las aplicaciones autorizadas por la compañía para sesiones de video conferencia.	
• Reportar de manera proactiva y a tiempo posibles incidentes de seguridad detectados.	
• Evitar el uso compartido con familiares de los equipos o dispositivos móviles destinados a la ejecución de labores corporativas.	
• Asignar o crear contraseñas con un nivel de seguridad que no incluyan frases o combinaciones numéricas predecibles.	

Tabla 1 Recomendaciones generales de nivel 0; Fuente Propia

Nivel de experiencia o requerimiento técnico	**Básico**
• Configurar actualizaciones automáticas sobre los equipos de trabajo de punto final.	
• Evitar presentar de forma visual o accidental, información sensible o personal, al momento activar cámara web o al entrar en el modo de pantalla compartida.	
• Evitar el uso compartido con familiares de los equipos o dispositivos móviles destinados a la ejecución de labores corporativas.	

• Habilitar bloqueo de pantalla programado para equipos o dispositivos móviles destinados a la ejecución de labores corporativas.
• Habilitar inicios de sesión con doble factor de autenticación, para aplicaciones o dispositivos en los cuales se encuentre disponible.

Tabla 2Recomendaciones generales de nivel Básico; Fuente Propia

Nivel de experiencia o requerimiento técnico	**Intermedio**
• Cambio de contraseña por defecto de routers, por contraseñas fuertes que incluyan frases o combinaciones de dígitos predecibles.	
• Configuración sobre routers par la actualización de versiones de Firmware.	
• Creación de una red de invitados, limitando acceso completo a internet o dispositivos sobre la red.	

Tabla 3Recomendaciones generales de nivel Intermedio; Fuente Propia

4 Recomendaciones especificas

Aplicando buenas prácticas, y extendiendo los sistemas implantados en un entorno corporativo basado en un modelo de capas, los entornos de trabajo en casa pueden ser reforzados a nivel de seguridad informática.

A continuación, se indican las recomendaciones de buenas practicas dirigidas a la implantación de sistemas y prácticas de seguridad informática a cargo de Kluger Tech.

Ilustración 1 Modelo de capas de seguridad; Fuente propia

5 Referencias

[1] SANS Institute, «Work from Home Precautions, Risks ando Potential Outcomes,» [En línea]. Available: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltb74d19704d59a6e7/60806f21b35a7a3c69a378cd/EndUser_Working_From_Home_Infographic.pdf.

[2] L. Spitzner, «www.sans.org,» 26 04 2020. [En línea]. Available: https://www.sans.org/blog/top-5-tips-for-working-from-home-securely/.

[3] J. Willert, «Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters,» 2001.