ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD MEDIANTE CONTROLES CIS PARA REDES DE ACCESO. CASO INSTITUTO NACIONAL DE EVALUACIÓN EDUCATIVA (INEVAL)

LUCY JOHANNA HONORES CHUCHUCA

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA - ECUADOR

Septiembre 2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** denominado: DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD MEDIANTE CONTROLES CIS PARA REDES DE ACCESO. CASO INSTITUTO NACIONAL DE EVALUACIÓN EDUCATIVA (INEVAL), de responsabilidad de la señorita Lucy Johanna Honores Chuchuca, ha sido minuciosamente revisado y se autoriza su presentación.

Tribunal:

LUIS EDUARDO HIDALGO ALMEIDA

Firmado digitalmente por:Luis Eduardo Hidalgo Almeida DN: cn=Luis Eduardo Hidalgo Almeida gn=Luis Eduardo Hidalgo Almeida c=EC Ecuador l=EC Ecuador o=ESPOCH ou=Instituto de Posgrado y Educacion continua e=l_hidalgo@espoch.edu.ec Motivo: Soy el autor de este documento Ubicación: Fecha:2021-08-27 16:40-05:00

Ing. Luis Eduardo Hidalgo Almeida; PhD.
PRESIDENTE **Firma**

Firmado electrónicamente por:
JORGE IGNACIO MOYA POLANCO

Ing. Jorge Ignacio Moya Polanco; Mag.
DIRECTOR **Firma**

Firmado electrónicamente por:
PAUL XAVIER PAGUAY SOXO

Ing. Paúl Xavier Paguay Soxo; Mag
MIEMBRO DEL TRIBUNAL **Firma**

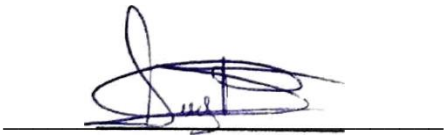
Firmado electrónicamente por:
WILIAN XAVIER SANCHEZ LABRE

Ing. Wilian Xavier Sánchez Labré; Mag
MIEMBRO DEL TRIBUNAL **Firma**

Riobamba, septiembre 2021

DERECHOS INTELECTUALES

Yo, Lucy Johanna Honores Chuchuca, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.



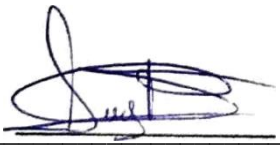
Lucy Johanna Honores Chuchuca

Nro. de Cédula: 070454820-5

DECLARACIÓN DE AUTENTICIDAD

Yo, Lucy Johanna Honores Chuchuca, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.



Lucy Johanna Honores Chuchuca

Nro. Cédula: 070454820-5

DEDICATORIA

Quiero dedicar este trabajo de tesis a mis padres, mamá gracias, sin ti no sería nada. Papá lo siento por demorarme tanto y hacerlo sin ti, sé que desde el cielo me estás viendo, te amo mi Honores.

Mi querido DFI, todo esto empezó a su lado, no hay día en que no los extrañe (Mirian, Ingrid, Edison, Stalin, Ceci, Audrey).

Finalmente quiero dedicar esta tesis, a todos mis amigos, por apoyarme cuando más lo necesité, por extenderme su mano en mis momentos difíciles, por el amor y la comprensión brindados cada día.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

En la presente investigación se plantea la implementación de un sistema de seguridad para mitigación de vulnerabilidades en la red LAN, con base en los controles de ciberseguridad del Center of internet Security (CIS). En primer lugar se realizó un análisis de herramientas tecnológicas para la gestión de vulnerabilidades en una red LAN, la seleccionada fue InsightVM de Rapid7 este software permite verificar la correcta implementación de las plantillas de configuración CIS, siendo por esto, la que se apega más a las necesidades de la investigación, después se realizó un escaneo de vulnerabilidades a los equipos críticos del INEVAL teniendo como resultado 58 vulnerabilidades de las cuales 12 fueron críticas, 11 severas y 35 moderadas, para la realización de este caso de estudio se tomó en cuenta las dos primeras categorías ya que, son más factibles de ser explotadas. Para el diseño del sistema de seguridad antes mencionado se realizó una selección de los controles CIS que fueron aplicados a las 23 vulnerabilidades tratadas en este estudio. Luego de la aplicación del sistema de seguridad se realizó un segundo escaneo de la red LAN en donde se obtuvo un porcentaje del 47.8 % de vulnerabilidades gestionadas. Es por ello que se recomienda realizar un análisis periódico de vulnerabilidades en los equipos críticos de la red LAN para así poder remediar estas brechas de seguridad antes de que sean explotadas por terceros y ocasionen pérdida de información o fallos en los sistemas.

Palabras claves: <CIS(CONTROLES)>, <VULNERABILIDADES>, <LAN(RED)>, <INSIGHTVM(SOFTWARE)>

ABSTRACT

This research proposes the implementation of a security system for vulnerability mitigation in the LAN network, based on the cybersecurity controls of the Center of Internet Security (CIS). In the first place, an analysis of technological tools for the management of vulnerabilities in a LAN was carried out, the one selected was InsightVM from Rapid7. This software allows to verify the correct implementation of the CIS configuration templates, being therefore the one that sticks more to the needs of the research, after a scan of vulnerabilities to the critical teams of INEVAL was performed, resulting in 58 vulnerabilities of which 12 were critical, 11 severe and 35 moderate, for the realization of this case study the first two categories were taken into account since, they are more likely to be exploited. For the design of the security system mentioned above, a selection of CIS controls was made and applied to the 23 vulnerabilities treated in this study. After the implementation of the security system, a second scan of the LAN was performed, obtaining a percentage of 47.8% of managed vulnerabilities. Therefore, it is recommended to perform a periodic vulnerability analysis on critical computers in the LAN network in order to remedy these security gaps before they are exploited by third parties and cause loss of information or system failures.

Keywords: <CIS(CONTROLS)>, <VULNERABILITIES>, <LAN(NETWORK)>, <INSIGHTVM(SOFTWARE)>

CAPÍTULO I

1 INTRODUCCIÓN

En la actualidad la mayoría de las vulnerabilidades y de los ataques a las infraestructuras tanto a empresas públicas como privadas, se basan en la explotación de las debilidades existentes en las redes informáticas, ejecutadas a través de mecanismos tecnológicos de ciberterrorismo, ciberdelito, cibercrimen e infiltración de los sistemas informáticos, convirtiéndose en una potente amenaza contra las infraestructuras de las instituciones, pudiendo comprometer la seguridad de la información (Defensa,2018).

Constantemente se realizan estudios en los cuales se determina los últimos ataques cibernéticos que se han realizado a las organizaciones mostrando su forma de ataque y su impacto en las organizaciones afectadas, con la finalidad de establecer controles de seguridad más sólidos y fiables, para garantizar la disponibilidad, integridad y confidencialidad de la información, ya que es de gran valor para la empresa o institución afectada.

En la primera fase de este documento se describe la problemática y la justificación del presente trabajo de investigación.

En la segunda fase se realiza un estudio de las herramientas especializadas para la gestión de las vulnerabilidades, con el fin de poder realizar un cuadro comparativo y seleccionar la herramienta más idónea para la elaboración de la investigación, también se describirá los controles de ciberseguridad del Center of Internet Security (CIS) que serán utilizados para el desarrollo del sistema de seguridad.

En la tercera fase de esta investigación se detalla la metodología, tipo de estudio, población, muestra, métodos y técnicas utilizadas para el desarrollo de la misma, esta sección también se realiza el escaneo de vulnerabilidades en la red del caso de estudio planteado.

En la cuarta y última fase se escogen los controles CIS y se desarrolla el sistema de seguridad el cual nos permitirá medir el porcentaje de vulnerabilidades gestionadas en la red del INEVAL. Finalmente se desarrollarán las conclusiones y recomendaciones que se obtuvieron con el estudio realizado.

1.1. Planteamiento del problema

Con los avances de la tecnología las instituciones públicas y privadas realizan actualizaciones para proteger o incrementar las seguridades y así poder resguardar la información, ya que es el activo más importante de cualquier institución.

El departamento de Tecnologías de la Información y Comunicación (TIC) de cada institución o empresa es el encargado de brindar la protección necesaria a los diferentes sectores de la institución. "Aplicando siempre los principios básicos de: confidencialidad, disponibilidad e integridad", pero no solo con estos principios se puede garantizar la seguridad efectiva, para que estos principios funcionan en pro de las instituciones deben ir de la mano de la implementación de controles o políticas de seguridad, buscando minimizar las vulnerabilidades encontradas en las redes LAN y aumentar la seguridad de la información. (Garzón, 2016)

Las vulnerabilidades en las redes LAN "son fallas en los sistemas, no son puertas diseñadas deliberadamente, son errores en diseño, configuración o implementación que generan oportunidades de ataques". (Romero, 2018, p.38)

Las instituciones públicas del Ecuador no cuentan con las seguridades adecuadas en las redes LAN para afrontar ataques cibernéticos y esto se pudo evidenciar el pasado mes de abril de 2019 cuando el Ecuador fue víctima de más de 40 millones de ataques a instituciones públicas y privadas. Los ataques provinieron de países como Estados Unidos, Brasil, Holanda, Alemania, Rumania, Francia, Austria, Gran Bretaña y Ecuador después de que se retirara el asilo político de Julian Assange. (Comercio, 2019)

Los ataques fueron realizados a: Cancillería, Banco Central, Presidencia de la República, Ministerio del Interior, Servicio de Rentas Internas, CNT, varios Gobiernos Autónomos Descentralizados, Consejo de la Judicatura, Ministerio de Telecomunicaciones y de la Sociedad de la Información, Ministerio de Turismo, Ministerio de Ambiente y algunas universidades. (CEDIA, 2019)

Entre los incidentes efectuados a las diversas instituciones públicas y privadas fueron: fuga de información de alrededor de una docena de sitios, desfiguración de sitios web mediante inyección de código malicioso, accesos no autorizados, negación de servicios a sitios web y a redes, todos estos ataques fueron atendidos por el CSIRT de CEDIA en colaboración con otros CSIRTs del país.

El Instituto Nacional de Evaluación Educativa (INEVAL) al igual que todas las instituciones públicas en el Ecuador cuenta con una infraestructura de red, la cual no está exenta de ataques y

amenazas cibernéticas, como accesos no autorizados o alteración a la información que maneja la institución. En los últimos 2 años, no se ha realizado ningún tipo de auditoría informática por lo cual era necesario un análisis de vulnerabilidades.

La protección contra ataques con la que cuenta la institución, es un firewall que le permite restringir los accesos no autorizados a la red, al no contar con un análisis de vulnerabilidades de los equipos activos conectados a la red LAN del Instituto un atacante podría explotar una de estas vulnerabilidades y conectarse a la red afectando a los servicios del INEVAL.

Basándose en el problema expuesto se propone disminuir las brechas de seguridad, para lo cual se plantea realizar un proceso de gestión de vulnerabilidades, de tal manera que, a través de procedimientos de escaneos a los equipos de red, se identifican las vulnerabilidades, para posteriormente, diseñar el sistema de seguridad y realizar la remediación de las vulnerabilidades encontradas.

Cabe recalcar que el sistema de seguridad mediante controles CIS podrá ser aplicado en las instituciones públicas que cuente con una infraestructura similar al del caso estudio planteado.

1.2. Formulación del problema

¿Con el diseño e implementación de un sistema de seguridad mediante controles CIS se reducirá las vulnerabilidades en la red LAN del INEVAL?

1.3. Sistematización del problema

- ¿Qué herramientas tecnológicas permiten la detección de vulnerabilidades en redes LAN?
- ¿Cuáles son las vulnerabilidades existentes en la red LAN del INEVAL?
- ¿Qué controles se utilizarán para disminuir la probabilidad de explotación de vulnerabilidades en la red LAN del INEVAL?
- ¿Cómo ayudaría la implementación de un sistema de seguridad en la red LAN del INEVAL?
- ¿Cuáles son los resultados obtenidos después de implementar el sistema de seguridad en el INEVAL?

1.4. Justificación

Actualmente con la evolución de la tecnología, la masificación del uso del internet y el uso de aplicaciones en red también han crecido los ataques informáticos, los cuales pueden provocar desde la infección de una computadora con virus hasta interrumpir completamente la funcionalidad de un sistema empresarial.

“Una red LAN siempre se encuentra bajo constantes ataques y amenazas ocasionadas por circunstancias internas y externas, sin embargo, es tiempo de implementar técnicas o controles para reducir las vulnerabilidades y los riesgos a los que está sometido constantemente” (Franco, 2013, p.49).

La presente investigación trata de orientar al Instituto Nacional de Evaluación Educativa (INEVAL), a mejorar las formas y prevenir los riesgos a las que están expuestas las redes LAN, para ello se propone el diseño y la implementación de un sistema de seguridad que permita tratar las vulnerabilidades encontradas a fin de salvaguardar la información y a los equipos que hagan parte de la red.

La metodología que se utilizará para la realización del sistema de seguridad serán los controles desarrollados por Center for Internet Security (CIS) los cuales permitirá proporcionar una defensa eficaz contra los ciberataques.

1.5. Objetivos

1.5.1. General

Diseñar e implementar un sistema de seguridad mediante controles CIS para redes de acceso local

1.5.2. Específicos

- Diagnosticar las mejores herramientas para la detección de vulnerabilidades de la red LAN del INEVAL.
- Analizar las vulnerabilidades existentes en la red LAN del INEVAL mediante escaneos que permitan la identificación de vulnerabilidades.
- Identificar, priorizar y aplicar los controles del Center for Internet Security (CIS) que permitirá disminuir la probabilidad de explotación de las vulnerabilidades encontradas.
- Diseñar e implementar el sistema de seguridad que permitirá mitigar las brechas de seguridad identificadas.
- Evaluar el nivel de mejora en la seguridad de la red LAN del INEVAL conforme a las vulnerabilidades detectadas.

CAPÍTULO II

2. MARCO REFERENCIAL

2.1. Antecedentes del problema

Desde la aparición de la primera red LAN comercial en el 1977 en el Chase Manhattan Bank en New York, actualmente se cuenta con millones de redes LAN en todo el mundo, estas pueden ser de 2 o 3 nodos hasta grandes data centers de 1000 nodos. Con esto han surgido numerosos problemas tanto a nivel físico, en la interconexión y en la seguridad. (Reinoso, 2017)

Los ataques y vulneración a las infraestructuras críticas de las instituciones públicas, se basan en la explotación de las debilidades de las redes informáticas, ejecutadas a través de mecanismos tecnológicos de ciberterrorismo, ciberdelito, cibercrimen, ciberespionaje e infiltración de los sistemas informáticos, convirtiéndose en un potente instrumento de agresión contra las infraestructuras de las instituciones públicas, lo cual podría comprometer la seguridad de la información (Defensa, 2018).

En Ecuador desde el año 2009 se han reportado varias denuncias relacionadas con el robo de contraseñas, clonación de tarjetas de crédito, ataques a páginas web de instituciones públicas, falsificación o fraude informático, entre otros delitos informáticos. (Enrriquez, 2015)

Dado esto se realizan constantemente estudios en los cuales se determina los ciberataques acontecidos, su forma de ataque y su impacto en las instituciones afectadas por el mismo, con la finalidad de establecer controles de seguridad más sólidas y fiables, para garantizar la disponibilidad, integridad y confidencialidad de la información que es de inestimable valor para la empresa o institución afectada.

Con todo lo expuesto previamente, surge la necesidad de desarrollar un estudio que permita realizar un escaneo para encontrar las vulnerabilidades en los equipos activos de una red LAN y realizar un sistema de seguridad para contrarrestar las vulnerabilidades encontradas antes de que sean explotadas por terceros y salvaguardar la seguridad de la información de las instituciones públicas del Ecuador.

2.2. Bases teóricas

2.2.1. Seguridad informática

La seguridad informática se la puede definir como el proceso, procedimiento o tareas que ayudan a controlar, proteger y detectar los accesos no autorizados a un recurso informático (información, equipos, etc.). La principal acción de la seguridad informática es la de minimizar los riesgos tanto del medio que transporta la información, del hardware utilizado para transmitir y recibir los datos, usuarios y de los protocolos que están siendo utilizados. (Romero, 2018)

El objetivo principal de la seguridad informática es que un sistema cumpla con los tres principios fundamentales: confiabilidad, integridad y disponibilidad.

Confiabilidad garantiza que la información almacenada en los sistemas informáticos no sea accedida por personas no autorizadas. La disponibilidad permite asegurar que la infraestructura, sistemas y los datos estén disponibles para el usuario en todo momento. Integridad este objetivo es primordial, ya que permite garantizar que la información que los datos no han sido modificados sin autorización.

2.2.2. Amenazas y vulnerabilidades informáticas

Para mejorar la seguridad informática de una organización o institución se debe tener en cuenta varios aspectos como:

- Amenazas
- Vulnerabilidades

Amenazas informáticas

Regularmente se denomina como virus a cualquier amenaza informática, lo que no es del todo correcto. Las amenazas son la fuente o la causa principal de incidentes o eventos que pueden resultar en daños a los sistemas informáticos o a la información de la organización. (Voutssas, 2010)

Cuando una amenaza llega a tener efecto puede ocurrir la interrupción de un servicio, modificación o eliminación de la información perdiendo así unos de los objetivos más relevantes de la seguridad de la información como es la integridad de la información almacenada.

Como se había mencionado las amenazas informáticas son todos los programas que de una u otra manera pueden dañar a un sistema informático se los conoce como malware, bugs o agujeros. (Business School, 2019)

Entre las amenazas más comunes se tiene:

- **Adware**

  Son programas diseñados que muestran publicidad de productos o servicios recopilando información de los sitios web navegados.
- **Backdoors**

  Es un programa que se introduce en el computador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado.
- **Bombas lógicas**

  Son aplicaciones o software que van insertados en otros códigos teniendo como objetivo principal, realizar un ataque malicioso a la parte lógica del computador, como borrar archivos, alterar el sistema llegando a inhabilitar por completo el sistema operativo.
- **Exploit**

  Son programas o técnicas que aprovechan una vulnerabilidad. Los exploit dependen de los sistemas operativos y sus configuraciones.
- **Malware**

  Son programas que están diseñados para insertar virus, gusanos o troyanos que permiten obtener información del computador infectado.
- **Phishing**

  Es un ataque de ingeniería social cuyo objetivo principal es obtener información confidencial de manera fraudulenta.
- **Ransomware**

  Últimamente es una de las amenazas que está creciendo tanto como para computadoras y teléfonos móviles, el dispositivo infectado se bloquea mostrando un mensaje pidiendo un rescate para que el usuario pueda volver a tener el control. Se exige un rescate en Bitcoin para que no pueda ser rastreado el atacante.

Estas son solo algunas de las amenazas a las que están expuestos los sistemas informáticos.

Vulnerabilidades informáticas

Una vulnerabilidad es una debilidad que compromete la seguridad de un sistema informático, por el cual se pueden presentar amenazas poniendo en peligro la confidencialidad e integridad de la información. A pesar de contar con los últimos software y hardware y de cuan buenos sean los procesos y el personal, siempre se tendrán vulnerabilidades es por eso que los administradores deben implementar estrategias que permita eliminar los factores que aumentan los riesgos e incorporar controles para reducir las amenazas. (Quishpe, 2016)

Con la mitigación de las vulnerabilidades existentes se tiene ventajas como:

- Los ataques serán más difíciles de llevar a cabo.
- Ayuda a mitigar el efecto de las nuevas vulnerabilidades en los activos.

Causas de las vulnerabilidades

Existen varias causas que son las responsables de las vulnerabilidades que afectan los sistemas informáticos, para la realización del estudio solo se tomarán en cuenta las siguientes:

- Debilidad en el diseño de protocolos utilizados en las redes.
- Errores de programación.
- Existencia de puertas traseras.
- Descuido de los fabricantes.
- Configuración inadecuada de los sistemas informáticos.
- Desconocimiento de las herramientas que facilitan los ataques.

2.3. Herramientas para la gestión de vulnerabilidades

Los escáneres de vulnerabilidades son herramientas que permiten identificar los fallos de seguridad de un sistema operativo y de sus servicios. Estas herramientas utilizan varias bases de datos de vulnerabilidades conocidas las cuales tienen un registro de todos los fallos de seguridad recientemente publicados.

Estas bases utilizan una métrica CVSS (Common Vulnerability Scoring System) que permite identificar una vulnerabilidad asignándole un código de identificación único. Para determinar el impacto, los escáneres de vulnerabilidades usan una escala de 0 a 10 donde: (Technology, 2019)

Tabla 2-1: Calificaciones de la severidad de las vulnerabilidades

Gravedad	Clasificación CVSS
Bajo	0.0 - 3.9
Medio	4.0 - 6.9
Alto	7.0 - 10.0

Fuente: (Technology, 2019)
Realizado por: Honores, L. 2019

2.3.1. Nessus

Es un programa que permite realizar escaneo de vulnerabilidades en diferentes sistemas operativos (Windows, Linux, Mac), encuentra errores de configuraciones ya sea por falta de actualizaciones del sistema operativo o por errores humanos en su despliegue (Tenable, 2019).

Características

- Nessus comenzó a trabajar con una licencia abierta y finalmente se convirtió en un producto pago.
- La licencia otorgada con la descarga de la versión Free es única y sólo para uso doméstico.
- Existen dos versiones: “Home” y “Work” esta última de pago y sin restricciones.
- Permite la generación de informes personalizados permitiendo ordenar por vulnerabilidades o servidor, crea un resumen ejecutivo y compara resultados de escaneos para descartar cambios.
- Envía notificaciones por correo electrónico sobre los resultados del escaneo con las recomendaciones de las correcciones y qué mejoras se puede realizar en las configuraciones de escaneos.
- Descubrimiento y etiquetado de activos.
- Posee auditoría de botnets, contenido malicioso y procesos.

2.3.2. OpenVas

Es la herramienta principal de OSSIM (Open Source Security Information Management) es una colección de herramientas diseñadas para ayudar la administración de red y la identificación de vulnerabilidades, detección de intrusos (Mendoza, 2014).

Características

- Escaneo concurrente de múltiples nodos.
- Escaneo automático.
- Servidor web integrado.
- Multiplataforma.
- Reportes en varios formatos (xml, html, LaTeX, etc.).
- Soporta el protocolo SSL.
- El tiempo de análisis es largo, comparado con otras herramientas que arrojan resultados en tiempos más cortos.
- La configuración puede llegar a ser complicada si se instala manualmente, mientras que si se usa desde Kali Linux resulta fácil, ya que viene integrada.

2.3.3. InsightVM

Es un escáner de vulnerabilidades y a su vez un sistema de gestión local, desde la consola de seguridad se realizan los informes y las configuraciones. Esta consola permite que los usuarios se conecten por medio de un navegador web para interactuar con el sistema.

Al aplicar un análisis para encontrar vulnerabilidades en el sistema la consola de seguridad aplica motores de escaneo para realizar un trabajo de escaneo real y paralelamente podrá configurarlos o distribuirlos en el entorno (Rapid7, 2019).

Este software proporciona una cobertura para más de 1500 tipos de sistemas, especialmente realiza una revisión de parches de los sistemas Windows, Apple, Linux para garantizar que los sistemas estén actualizados. Permite monitorear continuamente los puertos abiertos en los escaneos de los elementos de borde o perimetrales.

Características

- Identificar el riesgo en el entorno.
- Organizar sus dispositivos.
- Priorizar la corrección.
- Las plantillas de escaneo pueden personalizarse con el propósito de facilitar el escaneo y encontrar rápidamente vulnerabilidades.
- Permite crear cronogramas de escaneo para automatizar sus trabajos de escaneo.
- Al activar búsquedas por activos filtrados, el escaneado estará basado en más de 40 parámetros únicos.
- Permite generar informes de resultados de análisis, resolviendo las interrogantes de qué equipo se necesita arreglar y cómo.
- Descubrimiento y etiquetado de activos.

2.3.4. Qualys

Permite el análisis de vulnerabilidades, esta herramienta es muy utilizada en entornos empresariales, dispone de muchos nodos para el análisis, gestión y el monitoreo de vulnerabilidades, se puede realizar un análisis previo el cual permite conocer el número de activos antes de realizar el escaneo (TrendMicro, 2019).

Características

- Automatiza la detección de vulnerabilidades.
- Prioriza las remediaciones basándose en los riesgos.
- Por su escalabilidad lo hace ideal para organizaciones grandes.
- Realiza monitorización continua.

A continuación, en la **Tabla 2-2** se realiza la comparación de las características más significativas de las herramientas analizadas anteriormente:

Tabla 2-2: Cuadro comparativo de las herramientas para la gestión de vulnerabilidades

Característica	Nessus	OpenVas	InsightVM	Qualys
Licencia	Pagado	Libre	Pagado	Pagado
Identificación de equipos	Si	No	Si	No
Clasificación de Vulnerabilidades	Si	Si	Si	Si
Solución a las vulnerabilidades	No	No	Si	No
Multiplataforma	Si	Si	Si	Si
Generación de reportes	Si	Si	Si	Si
Plantillas de escaneo	No	No	Si	No

Realizado por: Honores, L. 2019

Una vez realizado el análisis de cada herramienta se ha procedido a comparar sus características principales. Nessus es una herramienta muy potente y muy utilizada por los administradores de infraestructuras para la búsqueda de vulnerabilidades en los equipos, su limitación es la licencia gratuita que es de tipo doméstico la cual restringe el uso de sus características.

OpenVas, es un Fork de Nessus antes que dejara de ser de código abierto, es un escáner completo de vulnerabilidades permitiendo evaluar los riesgos de seguridad en los equipos de una red y cerrar sus vulnerabilidades proactivamente utilizando herramientas, el limitante de esta herramienta es su base de datos de vulnerabilidades no es tan extensa como las de las herramientas pagadas.

Qualys, es pionero y líder realiza escaneos de cumplimiento de políticas, que incluyen normas internacionales, como PCI, se tiene la misma limitante que Nessus en cuanto se refiere al tipo de licencia.

La herramienta seleccionada es InsightVM este software permite verificar la correcta implementación de las plantillas de configuración CIS siendo el que se apega más a las necesidades para la elaboración del sistema de seguridad, además InsightVM es un escáner de vulnerabilidades que permite el descubrimiento, detección, verificación, clasificación del riesgo, impacto que la vulnerabilidad puede causar, lo más importante es que se puede emitir un reporte y mitigación de cada una de las vulnerabilidades encontradas.

2.4. Controles CIS

Los controles críticos de seguridad del Centro de Seguridad de Internet (Controles CIS) se crearon en el 2008 en colaboración con el gobierno de Estados Unidos y organizaciones de investigación de seguridad del sector privado, los cuales son un conjunto de técnicas dirigidas a detener los ciberataques, estas técnicas propuestas son pasos prácticos específicos que una organización o institución podría optar para evitar que las ciberamenazas más comunes comprometan sus sistemas de información (Ramiro, 2018).

Los controles CIS desde su creación han madurado por una comunidad internacional de personas e instituciones que:

- Toda la información obtenida sobre ataques y atacantes es compartida para identificar la causa de estos y realizar acciones defensivas.
- Comparten herramientas, ayudas de trabajo y traducciones para resolver los problemas.
- Dan seguimiento a la evolución de las amenazas, las capacidades de los adversarios y los vectores actuales de intrusiones.
- Se identifican los problemas comunes y se los resuelve como una comunidad.

Con la aplicación de estas actividades se asegura que los Controles CIS no solo sea una lista de buenas prácticas, sino un conjunto de acciones priorizadas y altamente focalizadas que tiene un soporte comunitario que los hace implementables, utilizables, escalables y compatibles con todos los requerimientos de seguridad.

Los controles CIS actualmente se encuentran en su versión 7 la cual sienta las bases para una implementación, medición y automatización más directa y manejable se tiene 20 controles distribuidos de la siguiente manera:

2.4.1. Controles básicos

Los controles CIS del 1 al 6 son los más esenciales permiten realizar inventarios y control de activos tanto de hardware como de software, gestión continua de vulnerabilidades uso controlado

de derechos de administrador y la configuración segura de hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores (Security, 2019).

Tabla 2-3: Controles CIS básicos

Control	Descripción
CCS1	Inventario de dispositivos autorizados y no autorizados
CCS2	Inventario de software autorizados y no autorizados
CCS3	Gestión continua de vulnerabilidades
CCS4	Uso controlado de privilegios administrativos
CCS5	Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores
CCS6	Mantenimiento, monitoreo y análisis de logs de auditoría.

Fuente: (Security, 2019)
Realizado por: Honores, L. 2019

2.4.2. Controles funcionales

La categoría fundamental tiene 10 controles que permiten la protección de correo electrónico y navegador web, defensas de malware, limitación y control de protocolos y servicios de puertos de red, capacidades de recuperación de datos, configuración segura para dispositivos de red, defensas de límites, protección de datos, acceso controlado, control de acceso inalámbrico y monitoreo y control de cuentas (Security, 2019).

Tabla 2-4: Controles CIS funcionales

Control	Descripción
CCS7	Protección de correo electrónico y navegador web
CCS8	Defensa contra malware
CCS9	Limitación y control de puertos de red, protocolos y servicios
CCS10	Capacidad de recuperación de datos
CCS11	Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores
CCS12	Defensa de borde
CCS13	Protección de datos
CCS14	Control de acceso basado en la necesidad de conocer
CCS15	Control de acceso inalámbrico
CCS16	Monitoreo y control de cuentas

Fuente: (Security, 2019)
Realizado por: Honores, L. 2019

2.4.3. Controles organizacionales

La categoría organizacional incluye controles para implementar un programa de capacitación y conciencia de seguridad, seguridad de software de aplicación, respuesta y gestión de incidentes, pruebas de penetración. Estos controles juntos forman una red que proporciona las mejores prácticas para mitigar ataques comunes contra sistemas y redes (Security, 2019).

Tabla 2-5: Controles CIS organizacionales

Control	Descripción
CCS17	Implementar un programa de concienciación y capacitación en seguridad
CCS18	Seguridad del software de aplicación
CCS19	Respuesta y gestión de incidentes
CCS20	Pruebas de penetración y ejercicios de Equipo Rojo

Fuente: (Security, 2019)
Realizado por: Honores, L. 2019

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

3.1. Tipo de investigación

La metodología de investigación es de tipo aplicativa porque busca dar solución a una situación o problema identificado en la investigación. También es de tipo descriptivo debido a que será posible realizar la detección de vulnerabilidades de la red LAN del INEVAL y será factible establecer y documentar recomendaciones para la mitigación de las vulnerabilidades encontradas lo cual permitirá reducir las brechas de seguridad en la red LAN.

3.2. Diseño de la investigación

El tipo de la investigación es experimental en donde luego de analizar los 20 controles de ciberseguridad del Center of Internet Security (CIS), se definió un sistema de seguridad para la mitigación de vulnerabilidades, y que fue evaluado con un segundo escaneo de la red LAN del INEVAL.

3.3. Métodos y Técnicas de investigación

3.3.1. Métodos

El método de investigación a aplicar en este estudio será el analítico: porque se realizará un análisis de los 20 controles de ciberseguridad los cuales permitirán tener un sistema de seguridad para mitigación de vulnerabilidades.

Método inductivo a partir de los controles de ciberseguridad, se diseñará e implementará un sistema de seguridad que mejore el nivel de seguridad de la red del INEVAL.

3.3.2. Técnicas de investigación

Para la realización de la presente investigación se utilizaron las siguientes técnicas:

- **Búsqueda de Información:** Permite obtener la información necesaria sobre los controles de Ciberseguridad de CIS, utilizando fuentes primarias y secundarias disponibles.
- **Test de penetración:** Permite determinar las vulnerabilidades existentes en la red.
- **Análisis:** Determinar los resultados de la investigación.

3.4. Instrumentos

Para la presente investigación se utilizará una herramienta que permitirá detectar y gestionar las vulnerabilidades existentes.

InsightVM: es un escáner de vulnerabilidades que permite el descubrimiento, detección, verificación, clasificación del riesgo, impacto que la vulnerabilidad puede causar, lo más importante es que se puede emitir un reporte y mitigación de cada una de las vulnerabilidades encontradas.

Los requisitos de hardware para la ejecución de InsightVM son:

Tabla 3-1: Requisitos de hardware – InsightVM

Volumen	Procesador	Memoria	Almacenamiento
Mínimo	Doble núcleo	8GB	100 GB
Hasta 5.000 activos	Cuatro núcleos	16GB	1 TB
Hasta 20.000 activos	2 x núcleo hexagonal	64GB	2 TB
Hasta 150.000 activos	2 x núcleo hexagonal	128GB	4 TB
Hasta 400.000 activos	2 x núcleo hexagonal	256GB	8 TB
Hasta 5.000 activos / día	Cuatro núcleos	8GB	100 GB
Hasta 20.000 activos / día	Ocho núcleos	16GB	200GB

Fuente: (Rapid, 2019)
Realizado por: Honores, L. 2019

No todos los navegadores son compatibles y solo soporta sistemas operativos de 64 bit como se muestra en la Tabla 3-2.

Tabla 3-2: Requisitos del sistema – InsightVM

Plataforma	Opciones
Sistema Operativo	● Ubuntu Linux 20.04 LTS ● Ubuntu Linux 18.04 LTS ● Ubuntu Linux 16.04 LTS ● Microsoft Windows Server 2019 ● Microsoft Windows Server 2016 ● Microsoft Windows Server 2012 R2 ● Microsoft Windows 8.1 ● Red Hat Enterprise Linux Server 8 ● Red Hat Enterprise Linux Server 7 ● Servidor Red Hat Enterprise Linux 6 ● CentOS 7 ● Oracle Linux 7

	• SUSE Linux Enterprise Server 12
Navegadores	• Google Chrome (más reciente) (RECOMENDADO) • Mozilla Firefox (más reciente) • Mozilla Firefox ESR (más reciente) • Microsoft Edge (más reciente)

Realizado por: Honores, L. 2019

3.5. Fuentes de información

Las fuentes de información utilizadas para el desarrollo de este proyecto son:

Primarias

- Análisis de vulnerabilidades en la red LAN del INEVAL

Secundarias

- Artículos científicos
- Trabajos de investigación
- Tesis relacionadas con el tema de investigación
- Sitios web de contenido confiable

3.6. Planteamiento de la hipótesis

3.6.1. Hipótesis general

¿Con la implementación de un sistema de seguridad se reducirá las vulnerabilidades en la red LAN del INEVAL?

3.6.2. Identificación de variables

De acuerdo a la hipótesis planteada, se determina las siguientes variables:

Variable independiente: Sistema de seguridad.

Variable dependiente: Vulnerabilidades en redes LAN

3.6.3. Operacionalización conceptual de variables

La Tabla 3-3, muestra la operacionalización conceptual de las variables determinadas.

Tabla 3-3: Variables e indicadores

Variable	Tipo	Concepto
Sistema de seguridad	Independiente	● Un sistema de seguridad es un conjunto de acciones diseñadas para proteger la integridad y privacidad de la información almacenada en su sistema informático. ● La remediación de vulnerabilidades es un proceso continuo y consciente que ayuda a contrarrestar las debilidades de TI.
Vulnerabilidades en redes LAN	Dependiente	Fallos en los sistemas que amenazan la estabilidad o la seguridad de la red al ser explotados.

Realizado por: Honores, L. 2019

3.6.4. Operacionalización metodológica de variables

La Tabla 3-4, muestra la operacionalización metodológica de las variables determinadas.

Tabla 3-4: Operacionalización metodológica

Variable	Indicador	Técnica	Instrumento / Fuente
Sistema de seguridad	● % de aplicación del sistema de seguridad	● Observación ● Pruebas ● Análisis	Controles CIS (Center of Internet Security)
Vulnerabilidades en redes LAN	● % de vulnerabilidades gestionadas	● Observación ● Pruebas ● Análisis	Herramienta de escaneo de vulnerabilidades InsightVM

Realizado por: Honores, L. 2019

3.7. Población y muestra

3.7.1. Población

Se tomó como población todos los equipos que estén conectados a la red LAN del INEVAL como se detalla a continuación:

Tabla 3-5: Población

Nro.	Equipos de la red LAN
35	Servidores
10	Router
180	Equipos de computo
8	Cámara IP

Realizado por: Honores, L. 2019

3.7.2. Selección de la muestra

Para el desarrollo del tema de investigación se utilizó como muestra los equipos que forman parte del Core de la institución, esta información fue proporcionada por el departamento de TIC del INEVAL siendo una cantidad de 35 servidores que serán escaneados para encontrar las vulnerabilidades.

3.8. Procedimientos generales

Para la recolección de información que valide la investigación se utilizó la observación con la finalidad de verificar si el sistema de seguridad propuesto reduce las vulnerabilidades existentes en la red LAN.

Tabla 3-6: Técnicas de demostración de hipótesis

Variable	Indicador	Técnicas
Sistema de seguridad	% de aplicación del sistema de seguridad	Sistema realizado con los controles CIS (Center of Internet Security)
Vulnerabilidades en redes LAN	% de vulnerabilidades gestionadas	Utilización de la herramienta InsigthVM para el escaneo de vulnerabilidades

Realizado por: Honores, L. 2019

Para el desarrollo del presente trabajo de investigación se definieron algunos lineamientos que permitieron cumplir con los objetivos planteados.

1. Análisis de las herramientas para el escaneo de vulnerabilidades en la red del INEVAL.
2. Selección de los equipos críticos que están conectados a la red del INEVAL.
3. Selección de la herramienta para el escaneo de vulnerabilidades.
    a. Instalación del software InsightVM.
4. Escaneo de las vulnerabilidades de la muestra seleccionada.

a. Ingreso de las IP de los servidores.

5. Selección de las vulnerabilidades críticas y severas encontradas en el escaneo de la red.
6. Aplicación de los controles CIS.
7. Remediación de las vulnerabilidades críticas y severas.
8. Observación y análisis de los resultados mediante la generación de datos estadísticos.

3.9. Escaneo de vulnerabilidades

El INEVAL proporcionó una lista con los equipos que consideran críticos o sensibles para la red LAN de la institución, estos son lo que finalmente se someten al análisis de vulnerabilidades, para lo que se utilizará la herramienta antes seleccionada que es InsightVM. Con la utilización de esta herramienta se podrá detectar los fallos de seguridad que existen en los equipos de la institución, InsightVM permite generar reportes en donde indica la descripción de cada una de las vulnerabilidades encontradas con la remediación de cada una de ellas.

3.9.1. Escaneo de vulnerabilidades lógicas a los equipos de red con INSIGHTVM

En la Tabla 3-7 se detalla la clasificación de vulnerabilidades que utiliza InsightVM con su respectiva puntuación.

Tabla 3-7: Clasificación de vulnerabilidades

Clasificación De Vulnerabilidades				
Crítica	**Severa**	**Media**	**Baja**	**Info**
8 – 10	7 – 7.9	4 – 6.9	1 – 39	0

Realizado por: Honores, L. 2019

Vulnerabilidades críticas son aquellas que pueden traernos consecuencias negativas a nuestro sistema, este tipo de vulnerabilidad puede causar extracción de información confidencial, ejecución de código remoto sin necesidad de autentificarse, desarrollo o expansión de un gusano por la red sin ninguna acción del usuario, entre otros.

Vulnerabilidades severas son aprovechadas para atacar rápidamente un sistema informático o un servicio. En este caso la pérdida de la confidencialidad e integridad de los datos es el mayor impacto negativo.

Vulnerabilidades medias son fáciles de reparar utilizando herramientas de auditoría o configuraciones que se han establecido de manera previa.

Vulnerabilidades bajas son las que menos afectan a los sistemas informáticos o aplicación porque tendrá un impacto menor en el mismo.

Vulnerabilidades informativas son las que no representan riesgos a los sistemas, un atacante solo puede obtener información del equipo.

Las vulnerabilidades que serán tratadas en el plan de remediación son las de nivel crítico y severa ya que son las de mayor prioridad, de no existir las vulnerabilidades antes mencionadas se tratarán las de nivel medio.

3.9.2. Esquema de red del INEVAL

En la red LAN del INEVAL se encuentran los equipos tales como servidores, PC's de escritorios, laptops, impresoras, teléfonos IP, etc. En la red DMz se localizan los servidores de correo electrónico, página web, DHCP, los que permiten realizar las publicaciones hacia el exterior.

En el tema de seguridad cuenta con un firewall y VPN check point, la red está segmentada por VLANs, las cuales están configuradas por pisos o departamentos.

Entre los servicios críticos que soporta la red tenemos:

- Correo electrónico
- Navegación web
- Aplicaciones (ser bachiller, ser maestro)
- Base de datos

A continuación, en la Figura 1-3, se muestra el diagrama de red y la conexión de cada uno de los dispositivos descritos anteriormente, la red cuenta con un firewall check point, en el cual está configurado todos los servicios de ingreso y salida, y que a través de políticas permite el acceso a red interna y a la DMz con el internet, el equipo utilizado para realizar el escaneo de las vulnerabilidades fue conectado a la VLAN del personal de TIC.

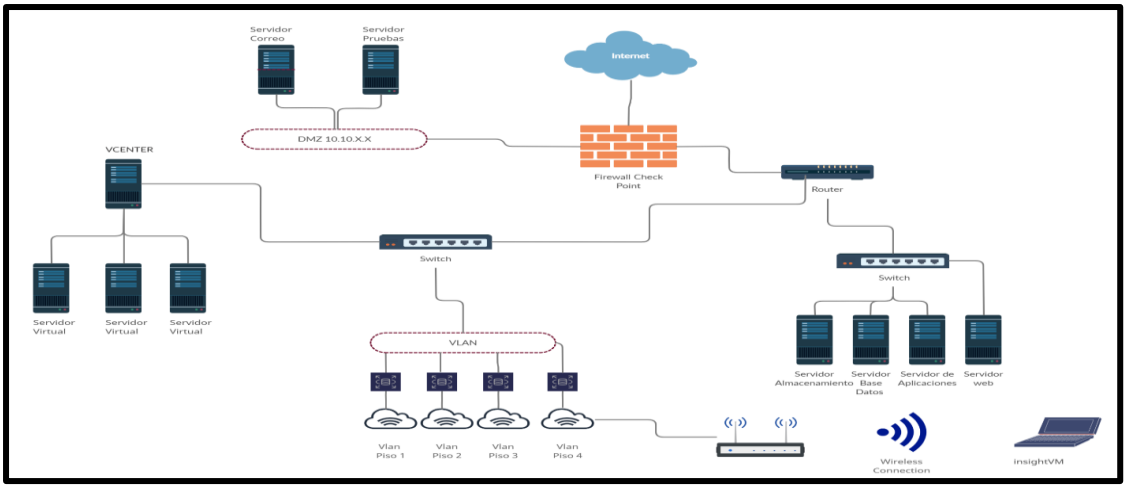


Figura 3-1: Esquema de la red
Realizado por: Honores, L. 2019

3.9.3. Equipos escaneados con INSIGHTVM

En Tabla 3-8, se muestra la lista de los 35 equipos críticos o sensibles que fueron escaneados con InsightVM para la detección de vulnerabilidades, de los cuales 16 son de criticidad alta y 19 de criticidad media.

Tabla 3-8: Equipos críticos del INEVAL

Nro.	Dirección Ip	Nombre Del Servidor	Criticidad
1	10.10.X. A	Server	Alta
2	192.168. X.B	Server	Media
3	192.168. X.C	Server	Media
4	192.168. X.D	Server	Media
5	192.168. X.E	Server	Media
6	192.168. X.F	Server	Alta
7	192.168. X.G	Server	Alta
8	192.168. X.H	Server	Media
9	192.168. X.I	Server	Media
10	192.168. X.J	Server	Media
11	192.168. X.K	Server	Media
12	192.168. X.L	Server	Alta
13	192.168. X.M	Server	Alta
14	192.168. X.N	Server	Alta
15	192.168. X.Ñ	Server	Media
16	192.168. X.O	Server	Media
17	192.168. X.P	Server	Media
18	192.168. X.Q	Server	Media
19	192.168. X.R	Server	Media
20	192.168. X.S	Server	Media

21	192.168. X.T	Server	Media
22	192.168. X.U	Server	Media
23	192.168. X.V	Server	Media
24	192.168. X.W	Server	Alta
25	192.168. X.X	Server	Alta
26	192.168. X.Y	Server	Alta
27	192.168. X.Z	Server	Alta
28	192.168. X.1	Server	Media
29	192.168. X.2	Server	Alta
30	192.168. X.3	Server	Media
31	192.168. X.4	Server	Alta
32	192.168. X.5	Server	Alta
33	192.168. X.6	Server	Alta
34	192.168. X.7	Pc	Alta
35	192.168. X.8	Pc	Alta

Realizado por: Honores, L. 2019

3.9.4. Vulnerabilidades detectadas

El informe de auditoría generado desde el software InsightVM muestra una cantidad de 58 vulnerabilidades entre críticas, severas y moderadas detectadas en los equipos críticos del INEVAL, como se muestra en la Tabla 3-9.

Tabla 3-9: Vulnerabilidades detectadas

DEVICE	RISK INDEX	RISK FACTORS
192.168.X.B	27,255	Se descubrieron 5 vulnerabilidades críticas. Se descubrieron 3 vulnerabilidades severas. Se descubrieron 8 vulnerabilidades moderadas. Se descubrió un servicio de Postgres. Se descubrió un servicio SSH. Se descubrió un servicio HTTP. Se descubrió un servicio HTTPS
10.10.X.A	5,055	Se descubrieron 2 vulnerabilidades severas. Se descubrieron 5 vulnerabilidades moderadas. Se descubrieron 3 servicios HTTPS. Se descubrieron 2 servicios SMTP. Se descubrió un servicio <unknown>. Se descubrió un servicio POPS. Se descubrió un servicio POP. Se descubrió un servicio SMTPS. Se descubrió un servicio IMAPS. Se descubrió un servicio de protocolo de configuración de llamadas H.323. Se descubrió un servicio SSH. Se descubrió un servicio IMAP.
192.168.X.C	573	Se descubrió 1 vulnerabilidad grave. Se descubrieron 3 vulnerabilidades moderadas. Se descubrió un servicio de Postgres. Se descubrieron 2 servicios portmapper. Se descubrieron 2 servicios de estado. Se descubrió un servicio SSH
192.168.X.M	105,650	Se descubrieron 3 vulnerabilidades críticas. Se descubrieron 3 vulnerabilidades severas. Se descubrieron 9 vulnerabilidades moderadas.

		Se descubrió un servicio MySQL. Se descubrieron 3 servicios HTTP. Se descubrió un servicio <unknown>. Se descubrió un servicio SSH
192.168.X.X	8,601	Se descubrió 1 vulnerabilidad crítica. Se descubrieron 2 vulnerabilidades severas. Se descubrieron 2 vulnerabilidades moderadas. Se descubrieron 6 servicios DCE RPC. Se descubrieron 2 servicios CIFS. Se descubrió un servicio de resolución de punto final DCE. Se descubrió un servicio RDP
192.168.X.P	9,255	Se descubrieron 8 vulnerabilidades moderadas. Se descubrió un servicio TDS. Se descubrieron 10 servicios HTTP. Se descubrieron 9 servicios HTTPS. Se descubrieron 8 servicios DCE RPC. Se descubrieron 7 servicios <desconocidos>. Se descubrieron 2 servicios CIFS. Se descubrió un servicio Kerberos. Se descubrió un servicio de resolución de punto final DCE. Se descubrió un servicio LDAP. Se descubrió un servicio de servicio de nombres CIFS. Se descubrió un servicio Microsoft SQL Monitor. Se descubrió un servicio LDAPS. Se descubrió un servicio ajp13 (Apache JServ Protocol 1.3)
192.168.X.S	6,392	Se descubrieron 7 vulnerabilidades moderadas. Se descubrieron 7 servicios DCE RPC. Se descubrieron 3 servicios <desconocidos>. Se descubrieron 2 servicios UPnP-HTTPU. Se descubrió un servicio de resolución de punto final DCE.
192.168. X.4	8,032	Se descubrieron 2 vulnerabilidades críticas. Se descubrió un servicio SSH. Se descubrió un servicio HTTPS. Se descubrió un servicio Telnet. Se descubrió un servicio de instalación inteligente. Se descubrió un servicio HTTP.
192.168. X.5	9,268	Se descubrieron 1 vulnerabilidades críticas. Se descubrieron 2 servicios portmapper. Se descubrió un servicio HTTP. Se descubrió un servicio SSH. Se descubrió un servicio Telnet. Se descubrió un servicio SNMP. Este dispositivo está en el sitio server5 con importancia normal. Se descubrieron 9 vulnerabilidades críticas. Se descubrieron 2 vulnerabilidades severas. Se descubrió una vulnerabilidad moderada

Realizado por: Honores, L. 2019

- **12 vulnerabilidades críticas:** Requieren atención inmediata ya que pueden ser explotadas por los atacantes fácilmente y tomar el control de los sistemas afectados.
- **11 vulnerabilidades severas:** Estas vulnerabilidades son más difíciles de ser explotadas y no proporcionan el mismo acceso a los sistemas afectados.
- **35 vulnerabilidades moderadas:** Estas proporcionan información del equipo que puede ser utilizado en futuros ataques.

Las vulnerabilidades que serán tratadas en este proyecto de investigación son las críticas y las severas, se debe tomar en cuenta que las vulnerabilidades moderadas también deben ser tratadas, pero se dará prioridad a las dos primeras ya que son de carácter urgente.

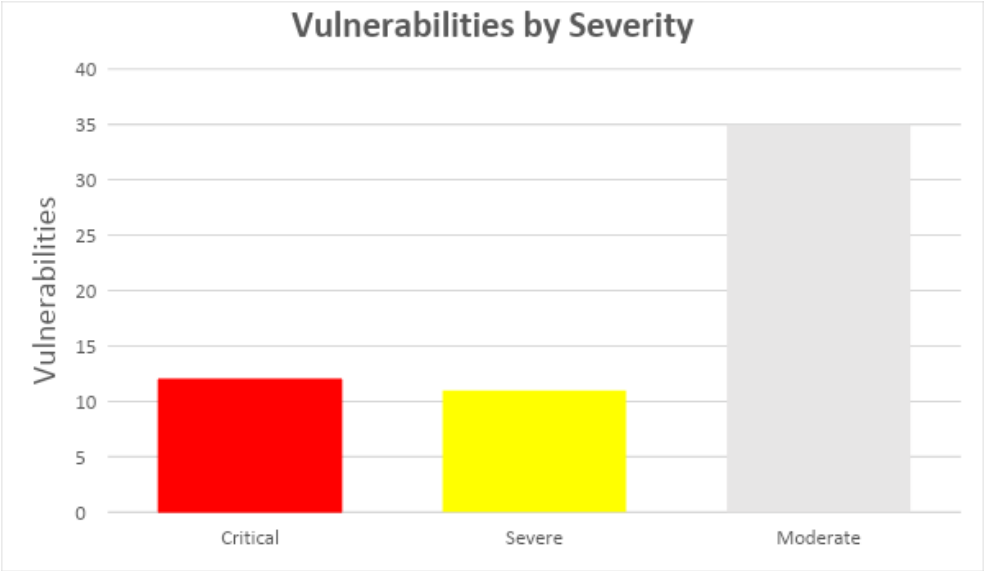


Gráfico 3-1: Vulnerabilidades detectadas primer escaneo
Fuente: (InsightVM, 2019)
Realizado por: Honores, L. 2019

En el Gráfico 3-1 se puede observar que existen 12 vulnerabilidades críticas, 11 severas y 35 moderadas.

3.9.4.1. Vulnerabilidades críticas

Las vulnerabilidades críticas encontradas en los equipos escaneados se detallan en el Anexo A, este tipo de vulnerabilidades requieren una atención inmediata ya que representan una puerta abierta para que un atacante ingrese en los sistemas, de no tratarlas oportunamente se puede tener las siguientes consecuencias.

- Negación de servicios.
- Pérdida o modificación de la información.
- Accesos no autorizados.
- Divulgación de la información.
- Interrupción de los servicios.

Tabla 3-10: Vulnerabilidades críticas

192.168.X.B	
Número:	**1**
Vulnerabilidad:	Apache HTTPD
Severidad:	7.5
CVE-ID	CVE-2017-7679
Descripción	Es un error de overread cuando el servidor apache en versiones 2.4 o anteriores el archivo de configuración “mod_mime” lee un byte más allá del final del búfer causando una respuesta “Content-Type” maliciosa.
Número:	**2**
Vulnerabilidad:	PHP

Severidad:	7.5
CVE-ID	CVE-2019-9641
Descripción	Se detectó problemas con el componente EXIF en PHP donde existe una lectura no inicializada en exif_IFD_in_TIFF y exif_IFD_in_MAKERNOTE respectivamente esta vulnerabilidad afecta directamente a la confidencialidad de la información, además para explotar este fallo no es necesario protocolos de autenticación y su complejidad de acceso es muy bajo.
Número:	**3**
Vulnerabilidad:	Apache HTTPD
Severidad:	7.5
CVE-ID	CVE-2017-3167
Descripción	En versiones de Apache anteriores a 2.4.26 surge una fase de autenticación que puede ser alterada, en donde el ataque al método "ap_get_basic_auth_pw()" genera un bypass y omite la autenticación lo que abre una brecha de seguridad que afecta críticamente a la integridad, disponibilidad y confidencialidad del sistema.
Número:	**4**
Vulnerabilidad:	Apache HTTPD
Severidad:	7.5
CVE-ID	CVE-2017-3169
Descripción	El activo afectado es vulnerable solo si ejecuta uno de los siguientes módulos: mod_ssl.
192.168.X.M	
Número:	5
Vulnerabilidad:	PHP
Severidad:	10
CVE-ID	CVE-2015-4599
Descripción	Las versiones de PHP antes de 5.4.40, 5.5.x antes de 5.5.24 y 5.6.x antes de 5.6.8 permite a los atacantes remotos obtener información confidencial y provocar una denegación de servicio (falla de la aplicación), o posiblemente ejecutar código arbitrario a través de un tipo de datos inesperado, relacionado con un problema de "confusión de tipos".
Número:	**6**
Vulnerabilidad:	PHP
Severidad:	7.5
CVE-ID	CVE-2015-6836
Descripción	La versión de PHP es propensa a la ejecución de código remoto, si se explota esta debilidad puede permitir al atacante ejecutar código malicioso cuando el usuario ejecute una aplicación afectada. Los intentos fallidos pueden causar negación de servicios.
192.168.X.X	
Número:	**7**
Vulnerabilidad:	Windows SMB Remote Code Execution
Severidad:	9.3
CVE-ID	CVE- 2017-0146
Descripción	Existe una vulnerabilidad de ejecución remota de código en la forma en que el servidor Microsoft Server Message Block 1.0 (SMBv1) maneja ciertas solicitudes.
192.168.X.Y	
Número:	**8**
Vulnerabilidad:	Default Password Telnet
Severidad:	10
CVE-ID	--
Descripción	Se debe cambiar la contraseña por defecto.
Número:	**9**
Vulnerabilidad:	Default Password SSH
Severidad:	10
CVE-ID	--
Descripción	Se debe cambiar la contraseña por defecto.
Número:|	**10**
Vulnerabilidad:	Code execution via specially crafted environment variables
Severidad:	10
CVE-ID	CVE-2014-6278
Descripción	GNU Bash a través de 4.3 bash43-026 no analiza correctamente las definiciones de funciones en los valores de las variables de entorno, lo que permite atacantes remotos para ejecutar

	comandos arbitrarios a través de un entorno diseñado, como lo demuestran los vectores que involucran el ForceCommand característica en OpenSSH sshd, los módulos mod_cgi y mod_cgid en el Servidor Apache HTTP, scripts ejecutados por DHCP no especificado clientes y otras situaciones en las que la configuración del entorno se produce a través de un límite de privilegios desde la ejecución de Bash.
Número:	**11**
Vulnerabilidad:	Untrusted pointer use issue leading to code execution
Severidad:	10
CVE-ID	CVE-2014-6277
Descripción	GNU Bash hasta 4.3 bash43-026 no analiza correctamente las definiciones de función en los valores de las variables de entorno, lo que permite a los atacantes remotos ejecutar código arbitrario o provocar una denegación de servicio (acceso a memoria no inicializado y operaciones de lectura y escritura de puntero no confiable) a través de un entorno diseñado, como lo demuestran los vectores que involucran la función ForceCommand en OpenSSH sshd, los módulos mod_cgi y mod_cgid en el servidor HTTP Apache, scripts ejecutados por clientes DHCP no especificados y otras situaciones en las que la configuración del entorno ocurre a través de un límite de privilegios desde la ejecución de Bash
Número:	**12**
Vulnerabilidad:	Nombres por defecto en las comunidades SNMP
Severidad:	10
CVE-ID	CVE-1999-0186, CVE-1999-0254, CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-1999-0792
Descripción	Esta vulnerabilidad permite realizar cambios en las configuraciones de los sistemas utilizando los nombres de las comunidades por defecto.

Realizado por: Honores, L. 2019

Se debe tener presente que las vulnerabilidades encontradas solo se las cuenta una vez así estén presentes en otros equipos.

3.9.4.2. Vulnerabilidades severas

Las vulnerabilidades severas son más difíciles que sean explotadas por un atacante y no proporcionan el mismo acceso a los sistemas que fueron comprometidos, el detalle de estas vulnerabilidades se encuentra en el Anexo B Vulnerabilidades severas.

Tabla 3-11: Vulnerabilidades severas

192.168.X.B	
Número:	**1**
Vulnerabilidad:	SSH Birthday attacks on 64-bit block ciphers (SWEET32)
Severidad:	5
CVE-ID	CVE-2016-2183
Descripción	Los cifrados de bloques heredados que tienen un tamaño de bloque de 64 bits son vulnerables a un ataque de colisión práctico cuando se utilizan en modo CBC.
10.10.10.3	
Número:	**2**
Vulnerabilidad:	TLS/SSL Server Supports Anonymous Cipher Suites with no Key Authentication
Severidad:	6
CVE-ID	--
Descripción	El servidor está configurado para admitir conjuntos de cifrados anónimos sin autenticación de clave. Estos cifrados son muy vulnerables a los ataques de hombre en el medio.
Número:	**3**
Vulnerabilidad:	TLS/SSL Server is enabling the BEAST attack

Severidad:	4.3
CVE-ID	CVE-2011-3389
Descripción	El protocolo SSL, tal como se usa en ciertas configuraciones de Windows y navegadores como Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera (y otros productos que negocian conexiones SSL) cifra los datos mediante el modo CBC con vectores de inicialización encadenados. Esto permite potencialmente que los atacantes del tipo "man-in-the-middle" obtengan encabezados HTTP en una sesión HTTPS.
192.168.X.M	
Número:	**4**
Vulnerabilidad:	HTTP TRACE Method Enabled
Severidad:	5.8
CVE-ID	CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386
Descripción	Un atacante podría abusar de la funcionalidad del método TRACE para ganar acceso a la información en los encabezados (headers) HTTP como las cookies y los datos autenticados.
Número:	**5**
Vulnerabilidad:	Apache HTTPD
Severidad:	6.8
CVE-ID	CVE-2018-1312
Descripción	El activo afectado es vulnerable solo si ejecuta uno de los siguientes módulos: mod_auth_digest. Revise la configuración del servidor para su validación. Cuando se genera un desafío de autenticación HTTP Digest, el nonce enviado para evitar los ataques de respuesta no se generó correctamente utilizando una semilla pseudoaleatoria. En un grupo de servidores que utilizan una configuración de autenticación Digest común, un atacante puede reproducir las solicitudes HTTP en un servidor sin ser detectado.
Número:	**6**
Vulnerabilidad:	Database Open Access
Severidad:	5
CVE-ID	--
Descripción	La base de datos permite que cualquier sistema remoto pueda conectarse a ella. Se recomienda limitar el acceso directo a sistemas confiables porque las bases de datos pueden contener datos confidenciales y de manera rutinaria se descubren nuevas vulnerabilidades y exploits para ellos.
Número:	**7**
Vulnerabilidad:	PHP
Severidad:	5
CVE-ID	CVE-2013-4248
Descripción	La función openssl_x509_parse en openssl.c en el módulo OpenSSL en PHP antes de 5.4.18 y 5.5.x antes de 5.5.2 no funciona correctamente manejar un carácter '\ 0' en un nombre de dominio en el campo Nombre alternativo del sujeto de un certificado X.509, que permite el atacante para falsificar servidores SSL arbitrarios a través de un certificado elaborado por una Autoridad de Certificación legítima.
192.168.X.C	
Número:	**8**
Vulnerabilidad:	Untrusted TLS/SSL server X.509 certificate
Severidad:	5.8
CVE-ID	--
Descripción	El certificado TLS / SSL del servidor está firmado por una autoridad de certificación (CA) que no es conocida ni confiable. Esto podría suceder si: falta el certificado intermedio / de cadena, está vencido o ha sido revocado; el nombre de host del servidor no coincide con el configurado en el certificado; la hora / fecha es incorrecta; o se está utilizando un certificado autofirmado. No se recomienda el uso de un certificado autofirmado, ya que podría indicar que se está produciendo un ataque de intermediario TLS / SSL.
Número:	**9**
Vulnerabilidad:	TLS/SSL Server Supports RC4 Cipher Algorithms
Severidad:	4.3
CVE-ID	CVE-2013-2566
Descripción	Los resultados de criptoanálisis recientes aprovechan los sesgos en el flujo de claves RC4 para recuperar textos sin cifrar repetidamente. Como resultado, ya no se puede considerar que RC4 proporcione un nivel suficiente de seguridad para las sesiones SSL / TLS. Tiene muchos sesgos de un solo byte, lo que facilita a los atacantes remotos realizar ataques de recuperación

	de texto sin formato a través del análisis estadístico de texto cifrado en una gran cantidad de sesiones que utilizan el mismo texto sin formato.
192.168.X.Y	
Número:|	**10**
Vulnerabilidad:	SSH Server Supports diffie-hellman-group1-sha1
Severidad:	4.3
CVE-ID	CVE-2015-4000
Descripción	El módulo principal ofrecido cuando se usa diffie-hellman-group1-sha1 solo tiene un tamaño de 1024 bits. Este tamaño se considera débil y dentro del rango teórico del llamado ataque Logjam.
Número:	**11**
Vulnerabilidad:	ICMP redirection enabled
Severidad:	6.8
CVE-ID	--
Descripción	Muchos sistemas operativos Linux habilitan una función llamada redirección ICMP, donde la máquina modificará su tabla de rutas en respuesta a un mensaje de redirección ICMP desde cualquier dispositivo de red. Existe el riesgo de que esta característica pueda usarse para subvertir la tabla de enrutamiento de un host con el fin de comprometer su seguridad (por ejemplo, engañándolo para que envíe paquetes a través de una ruta específica donde pueden ser detectados o alterados).

Realizado por: Honores, L. 2019

Las vulnerabilidades encontradas solo se tomarán en cuenta una sola vez así se encuentren presentes en otros equipos.

3.9.5. Análisis de las vulnerabilidades encontradas

Mediante el escaneo realizado a los equipos críticos de la red del INEVAL se pudo encontrar puertos abiertos algunos corresponden a los servicios que se están ejecutando otros pueden servir para que se efectúe un ataque.

A continuación, se detallará las vulnerabilidades más comunes encontradas como sistemas operativos y servicios de los equipos escaneados.

Vulnerabilidades comunes

El Gráfico 3-2, muestra 8 apariciones de la vulnerabilidad habilitada para tlsv1_1, lo que la convierte en la vulnerabilidad más común.

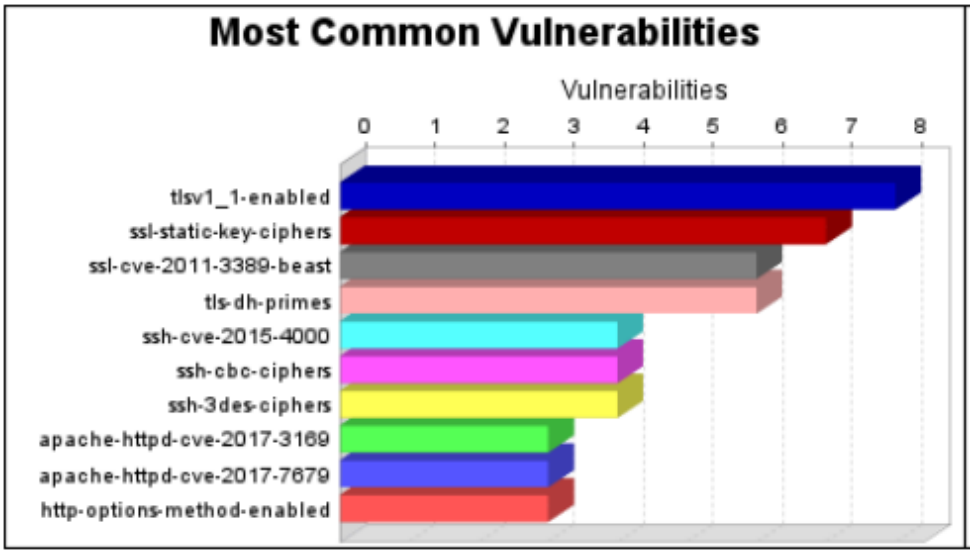


Gráfico 3-2: Vulnerabilidades comunes
Fuente: (InsightVM, 2019)
Realizado por: Honores, L. 2019

Categorías de las vulnerabilidades

El Gráfico 3-3, muestra que existen 52 ocurrencias de la vulnerabilidad en la categoría de red siendo esta la más común.

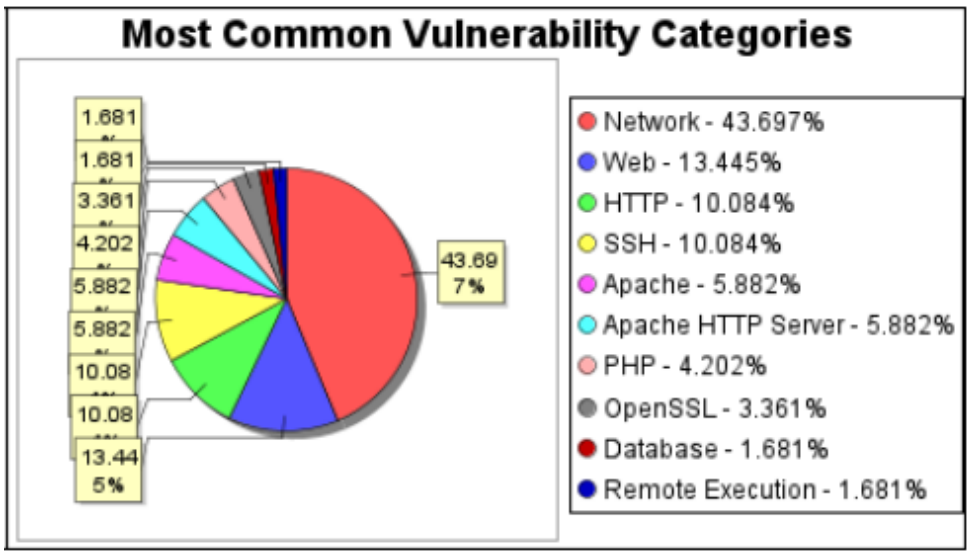


Gráfico 3-3: Categoría de las vulnerabilidades
Fuente: (InsightVM, 2019)
Realizado por: Honores, L. 2019

Sistemas operativos

El Gráfico 3-4, muestra que existen 3 sistemas operativos, siendo el más utilizado CentOs Linux.

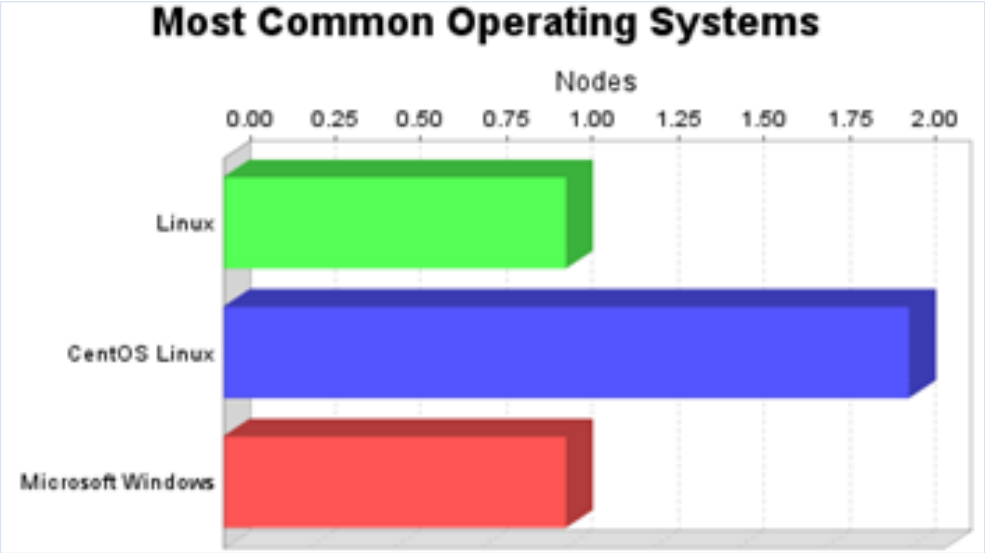


Gráfico 3-4: Sistemas operativos
Fuente: (InsightVM, 2019)
Realizado por: Honores, L. 2019

Servicios detectados

El Gráfico 3-5, muestra que el servicio SSH se encontró en 19 sistemas, por lo que es el servicio más común. Se descubrió que el servicio HTTPS tiene la mayoría de las vulnerabilidades durante este análisis con 80 vulnerabilidades.

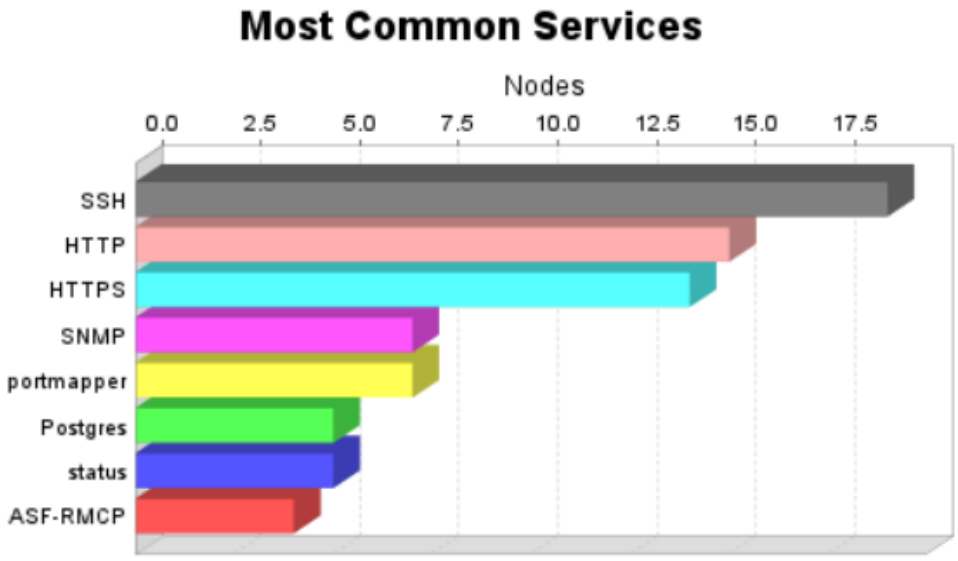


Gráfico 3-5: Servicios detectados
Fuente: (InsightVM, 2019)
Realizado por: Honores, L. 2019

En el Anexo C del reporte ejecutivo se detallan sobre los activos, vulnerabilidades y equipos detectados.

CAPÍTULO IV

4. PRESENTACIÓN DE RESULTADOS

En esta sección se presentan los resultados obtenidos al aplicar los controles CIS en las vulnerabilidades encontradas, así como su relación con la hipótesis y los objetivos planteados.

4.1. Valoración de la variable independiente

4.1.1. Variable independiente: Sistema de seguridad

Para su valoración se realizó un segundo escaneo en la red del INEVAL después de la aplicación del sistema de seguridad.

4.1.2. Indicador: Porcentaje de aplicación del sistema de seguridad

La medición de este indicador se basó en la aplicación del sistema de seguridad en la red del INEVAL.

Tabla 4-1: Porcentaje de aplicación del sistema se seguridad

	PRIMER ESCANEO	SEGUNDO ESCANEO DESPUÉS DE APLICAR EL SISTEMA DE SEGURIDAD	% APLICACIÓN DEL SISTEMA
VULNERABILIDADES	23	12	52%

Realizado por: Honores, L. 2019

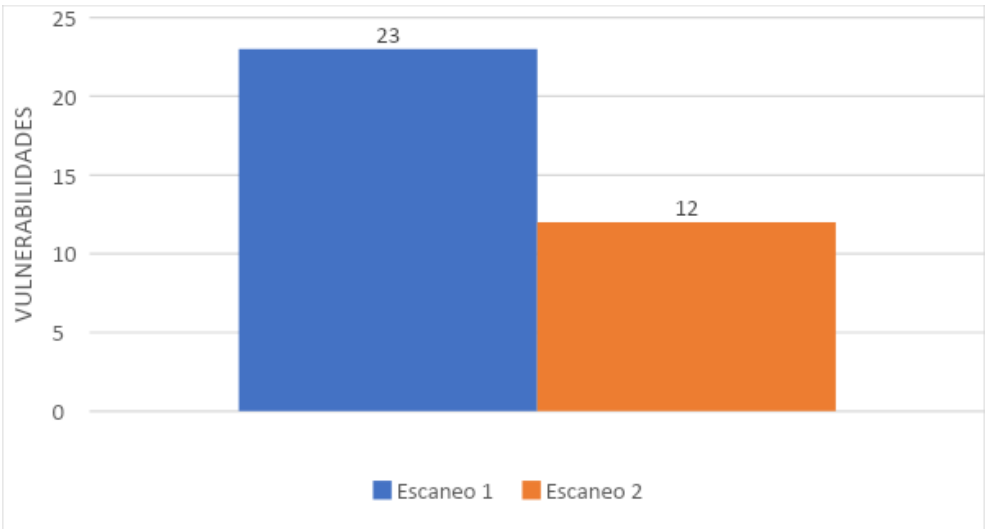


Gráfico 4-1: Porcentaje de aplicación del sistema
Realizado por: Honores, L. 2019

Análisis e interpretación de resultados

Con los datos obtenidos se puede observar que el porcentaje de aplicación del sistema de seguridad basado en controles CIS fue del 52%, por lo que se gestionaron 11 vulnerabilidades entre críticas y severas.

4.2. Valoración de la variable dependiente

4.2.1. Variable dependiente: Vulnerabilidad en redes LAN

Para su valoración se utilizó la herramienta InsightVM la cual sirvió para detectar el número de vulnerabilidades existentes en los equipos críticos del INEVAL.

4.2.2. Indicador: Porcentaje de vulnerabilidades gestionadas

Para la medición de este indicador se utilizó la herramienta InsightVM para escanear la red antes y después de la aplicación del sistema de seguridad.

Tabla 4-2: Resultado del indicador: Porcentaje de vulnerabilidades gestionadas

	VULNERABILIDADES ENCONTRADAS	VULNERABILIDADES GESTIONADAS	% DE VULNERABILIDADES GESTIONADAS
VULNERABILIDADES	23	11	47.8%

Realizado por: Honores, L. 2019

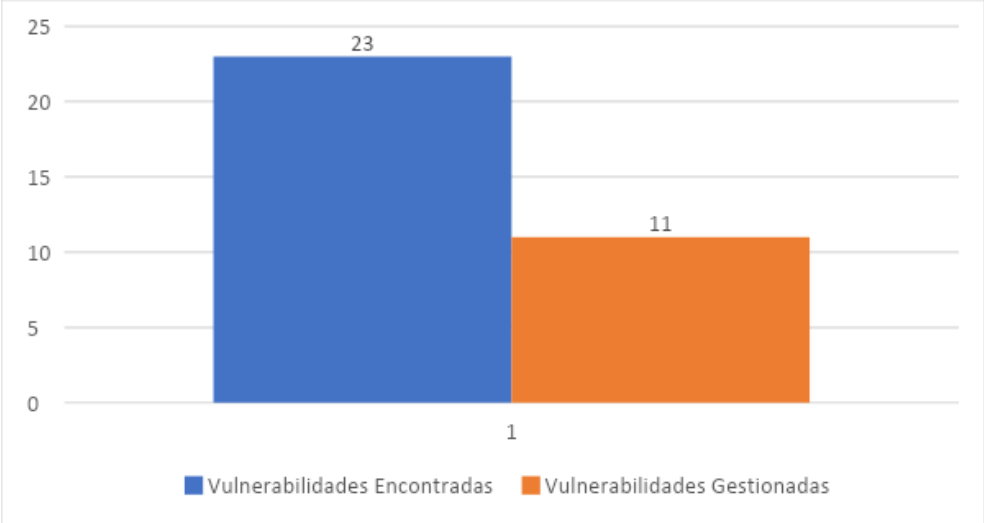


Gráfico 4-2: Porcentaje de Vulnerabilidades gestionadas
Realizado por: Honores, L. 2019

Análisis e interpretación de resultados

Con los datos obtenidos se puede observar que el porcentaje de vulnerabilidades gestionadas es del 47.8%.

4.3. Comprobación de la hipótesis

Para la hipótesis planteada se utilizó la prueba de Chi-cuadrado o X2, que es una prueba no paramétrica a través de la cual se mide la relación entre la variable dependiente e independiente.

Adicionalmente, se establece la hipótesis nula Ho y la hipótesis de investigación Hi.

Hi: *Con la implementación de un sistema de seguridad* ***se reducirán*** *las vulnerabilidades en la red LAN del INEVAL.*

Ho: *Con la implementación de un sistema de seguridad* ***no*** *reducirá las vulnerabilidades en la red LAN del INEVAL.*

La Tabla 4-3 contiene las frecuencias observadas de cada indicador, las mismas que serán utilizadas para el cálculo de chi-cuadrado.

Tabla 4-3: Tabla de contingencia de frecuencias observadas

	PRIMER ESCANEO	SEGUNDO ESCANEO	TOTAL
VULNERABILIDADES ENCONTRADAS	23	12	35
VULNERABILIDADES SOLVENTADAS	0	11	11
TOTAL	23	23	46

Realizado por: Honores, L. 2019

La tabla de contingencia de frecuencias esperadas son aquellos valores que se espera encontrar bajo el supuesto de independencia de las variables, el mismo que es usado por Chi-cuadrado para evaluar si es verdadero o falso, analizando si las frecuencias observadas difieren de lo esperado, en caso de no existir correlación.

La frecuencia esperada, se calcula mediante la siguiente fórmula:

$$Fe = \frac{total\ columna \times total\ fila}{suma\ total}$$

Aplicando la fórmula en cada valor de la tabla se obtiene la siguiente Tabla 4-4 de contingencia de frecuencias esperadas.

Tabla 4-4: Contingencia de frecuencias esperadas

	PRIMER ESCANEO	SEGUNDO ESCANEO	TOTAL
VULNERABILIDADES ENCONTRADAS	17.5	17.5	35
VULNERABILIDADES SOLVENTADAS	5.5	5.5	11
TOTAL	23	23	46

Realizado por: Honores, L. 2019

A continuación, se aplica chi-cuadrado a las frecuencias esperadas calculadas, mediante la fórmula.

$$x^2 = \sum \frac{(O-E)^2}{E}$$

En dónde:

O: frecuencia observada por celda

E: frecuencia esperada por celda

$$x^2 = \frac{(23-17.5)^2}{17.5} + \frac{(0-5.5)^2}{5.5} + \frac{(12-17.5)^2}{17.5} + \frac{(11-5.5)^2}{5.5}$$

$$x^2 = 1.72 + 5.5 + 1.72 + 5.5$$

$$x^2 = 14.45$$

Para determinar si el valor de x^2 es o no significativo, se debe determinar los grados de libertad mediante la siguiente fórmula.

$$v = (r-1) * (k-1)$$

En dónde:

r: número de filas

k: número de columnas

Por lo tanto:

$$v = (2-1) * (2-1)$$

$$v = 1$$

De acuerdo a la tabla de distribución de x^2 que se muestra en la Tabla 4-5 y eligiendo como nivel de significancia del 0.05 para disponer de un nivel de confianza del 95% y con el grado de libertad de 1, según la tabla de distribución de Chi-cuadrado se obtiene como x^2 crítico = 3.8415.

Tabla 4-5: Chi-cuadrado

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372

Realizado por: Honores, L. 2019

$$x^2 crítico = 3.8415$$

El valor de x^2 calculado en la investigación es de 14.46 que es superior al valor de la tabla de distribución de 3.8415, como se muestra en la figura 7-4.

Con los datos obtenidos anteriores, H_o debe ser aceptada si sucede el siguiente condicionante:

$$x^2\ calculado\ \leq\ x^2\ crítico$$

En caso contrario se rechaza H_o y se acepta H_i.

Con el valor de $x^2 = 14.45$ y $x^2\ crítico = 3.8415$ se aplica el criterio de decisión y se obtiene que:

$$x^2\ Crítico\ (3.8415) < x^2\ Calculado\ (14.45)$$

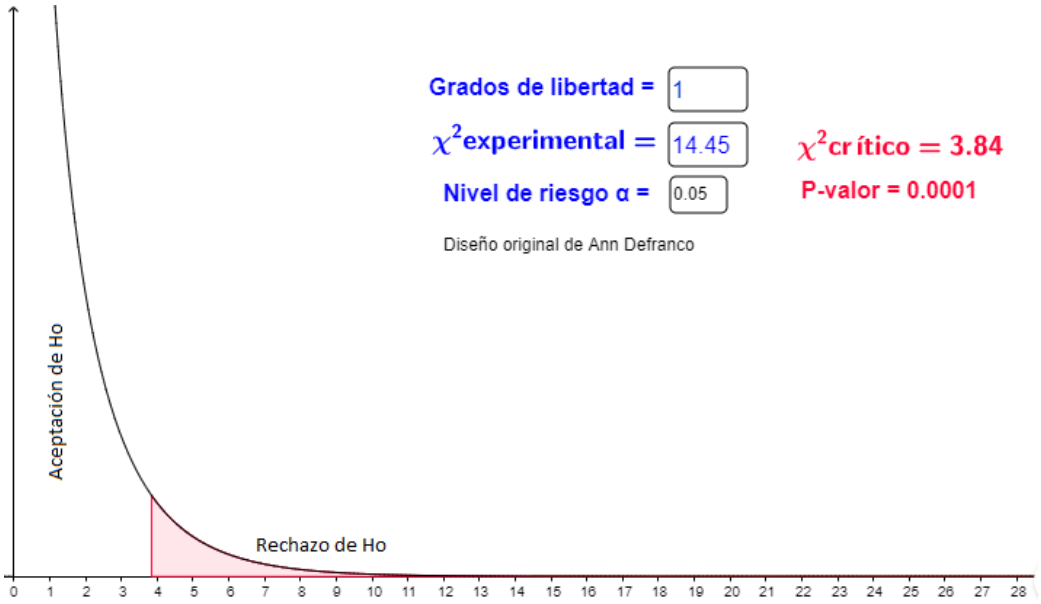


Figura 4-1: Curva de Chi-cuadrado
Realizado por: Honores, L. 2019

Por tanto, se valida que el valor calculado de Chi-cuadrado se localiza en la región de rechazo de la hipótesis nula H_o y se acepta la hipótesis de investigación H_i que es significativa, con un nivel de significancia de α=5% = 0.05 para obtener un nivel de confianza del 95%.

H_i: *Con la implementación de un sistema de seguridad* ***se reducirán*** *las vulnerabilidades en la red LAN del INEVAL.*

CAPÍTULO V

5. PROPUESTA DE UN SISTEMA DE SEGURIDAD MEDIANTE CONTROLES CIS PARA LA RED DEL INEVAL

Generalidades

Luego del análisis de las vulnerabilidades identificadas en el Capítulo III, se propone diseñar el sistema de seguridad que describe una serie de controles recomendados con el fin de mitigar las vulnerabilidades y poder reducir el riesgo de ataque a la red LAN.

Cabe recalcar que los controles aplicados en el sistema de seguridad se han definido como obligatorios para que sean cumplidos por el departamento de TIC del INEVAL. Además, dichos controles pueden ser aplicados en otras instituciones que cuenten con una red LAN similar y en base a las necesidades pueden ser modificados y adaptados.

5.1. Vulnerabilidades Críticas

- ***Vulnerabilidad de Apache HTTPD: CVE-2017-7679***

  Impacto: Afecta parcialmente a la integridad, confidencialidad y la disponibilidad del sistema.

  Subcontrol:

  9.5 Implementar firewalls de aplicación

  Remediación:

  Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC del INEVAL implementar un firewall de aplicaciones frente al servidor para verificar y validar el tráfico que va al servidor. Cualquier tráfico no autorizado debe ser bloqueado y registrado.

- ***Vulnerabilidad de PHP: CVE-2019-9641***

  Impacto: Afecta directamente a la confidencialidad de la información, para explotar este fallo no es necesario protocolos de autenticación y su complejidad de acceso es muy baja.

  Subcontrol:

  2.2 Asegurar que el software tenga soporte del fabricante.

Remediación:

Esta vulnerabilidad se la pudo corregir con la actualización de PHP 5.4.16 a la versión más reciente a la fecha actual del presente trabajo 7.1.27 la descarga se la realizó de la siguiente página:

- https://www.php.net/downloads.php

- ***Vulnerabilidad de Apache HTTPD: CVE-2017-3167***

  Impacto: Omite la autenticación lo que abre una brecha de seguridad que afecta críticamente a la integridad, disponibilidad y confidencialidad del sistema.

  Subcontrol:

  9.5 Aplicar firewalls de aplicaciones.

  Remediación:

  Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC del INEVAL implementar un firewall de aplicaciones frente al servidor para verificar y validar el tráfico que va al servidor. Cualquier tráfico no autorizado debe ser bloqueado y registrado.

- ***Vulnerabilidad de Apache HTTPD: CVE-2017-3169***

  Impacto: Afecta parcialmente a la integridad, confidencialidad y la disponibilidad del sistema.

  Subcontrol:

  9.5 Aplicar firewalls de aplicaciones.

  Remediación:

  Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC del INEVAL implementar un firewall de aplicaciones frente al servidor para verificar y validar el tráfico que va al servidor. Cualquier tráfico no autorizado debe ser bloqueado y registrado.

- ***Vulnerabilidad de PHP: CVE-2015-4599***

  Impacto: Permite el acceso remoto para obtener información confidencial o causar una denegación de servicio (bloqueo de la aplicación) y posiblemente ejecutar código arbitrario a través de un tipo de datos inesperado, relacionado con un problema de "confusión de tipos".

Subcontrol:

9.4 Aplicar firewalls basados en host o filtrado de puertos.

Remediación:

Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC del INEVAL implementar un firewall basado en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.

- ***Vulnerabilidad de PHP: CVE-2015-6836***

Impacto: Permite el acceso remoto para obtener información confidencial o causar una denegación de servicio (bloqueo de la aplicación) y posiblemente ejecutar código arbitrario a través de un tipo de datos inesperado, relacionado con un problema de "confusión de tipos".

Control:

9.4 Aplicar firewalls basados en host o filtrado de puertos.

Remediación:

Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC del INEVAL implementar un firewall basado en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.

- ***Vulnerabilidad de Windows SMB Remote Code Execution: CVE- 2017-0146***

Impacto: Permite la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor Microsoft Server Message Block 1.0 (SMBv1).

Control:

2.2 Asegurar que el software tenga soporte del fabricante.

Remediación:

La remediación se la realizó con la instalación del parche correspondiente al sistema operativo del servidor en este caso es Microsoft Windows Server 2008 R2, Standard Edition SP1 la descarga se la realizó de la siguiente página:

- https://www.catalog.update.microsoft.com/search.aspx?q=kb4012212

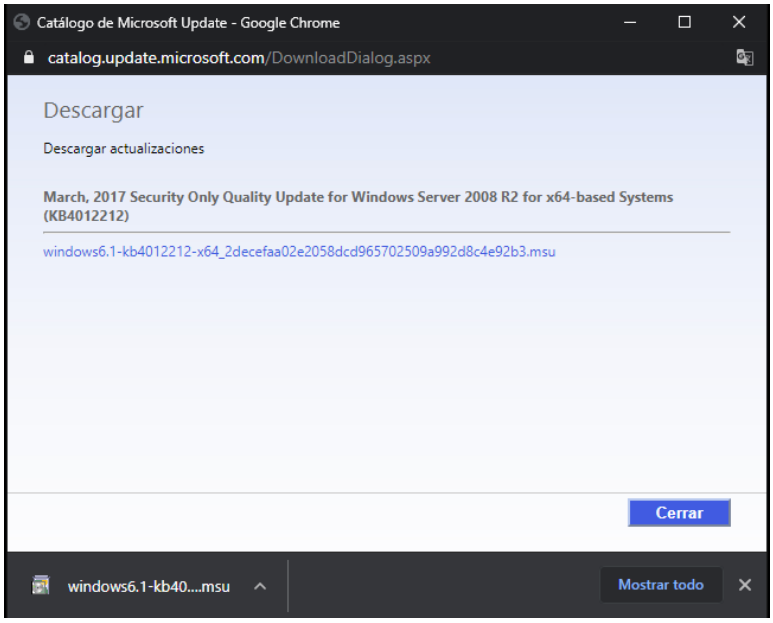


Figura 5-1: Parche de Windows KB4012212
Realizado por: Honores, L. 2019

- ***Vulnerabilidad Default Telnet Password***

  Impacto: Control total del sistema

  Subcontrol:

  4.2 Cambiar contraseñas por defecto.

  Remediación:

  La vulnerabilidad fue corregida cuando se ingresó a la consola y por medio del comando passwd se realizó el cambio de la contraseña por defecto.

- ***Vulnerabilidad Default Password SSH***

  Impacto: Control total del sistema

  Subcontrol:

  4.2 Cambiar contraseñas por defecto.

  Remediación:

  La vulnerabilidad fue corregida cuando se ingresó a la consola y por medio del comando passwd se realizó el cambio de la contraseña por defecto.

- ***Vulnerabilidad Code Execution Via Specially Crafted Environment Variables: CVE-2014-6278***

  Impacto: Permite a los atacantes de manera remota inyectar comandos Shell.

  9.4 Aplicar firewalls basados en host o filtrado de puertos.

Remediación

Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC del INEVAL implementar un firewall basado en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.

- ***Vulnerabilidad Untrusted Pointer Use Issue Leading to Code Execution: CVE-2014-6277***

  Impacto: Permite a atacantes remotos ejecutar código arbitrario o causar una denegación de servicio.

  Subcontrol:

  2.2 Asegurar que el software tenga soporte del fabricante.

  Remediación:

  Esta vulnerabilidad se la pudo corregir con la actualización de PHP 5.4.16 a la versión más reciente 8.0.6 la descarga se la realizó de la siguiente página:

  - https://www.php.net/downloads.php

- ***Vulnerabilidad Default or Guessable SNMP Community Names: CVE-1999-0186, CVE-1999-0254, CVE-1999-0472, CVE-1999-0516, CVE-1999-0517, CVE-1999-0792***

  Impacto: Afecta parcialmente a la integridad, confidencialidad y la disponibilidad del sistema.

  Subcontrol:

  5.1: Establecer configuraciones seguras.

  Remediación:

  Esta vulnerabilidad no fue remediada, se le recomendó al departamento de TIC que deshabilite el servicio de SNMP si no es necesario o actualice a la versión 3 que ofrece más autenticación y cifrado complejo.

5.2. Vulnerabilidades Severas

- ***Vulnerabilidad SSH Birthday attacks on 64-bit Block Ciphers (SWEET32): CVE-2016-2183***

  Impacto: Afecta parcialmente a la integridad del sistema, confidencialidad y la disponibilidad del sistema.

Subcontrol:

5.1: Establecer configuraciones seguras

Remediación:

Esta vulnerabilidad fue corregida para lo cual se deshabilitó todos los cifrados 3DES de la lista de cifrado especificada en el archivo sshd_config como se muestra:

1. Ingresar al archivo vi /etc /ssh /shh_config
2. Reemplace la línea #Cyphers y #MACs

   Ciphers aes128-ctr,aes192-ctr,aes256-ctr

   MACs hmac-sha1,umac-64@openssh.com,hmac-ripemd1

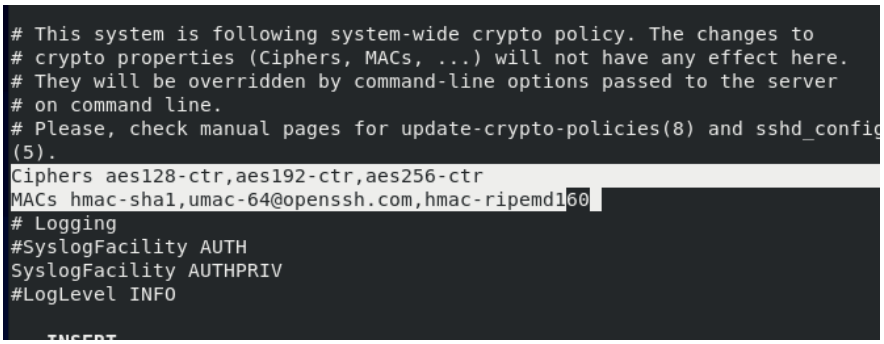


Figura 5-2: Cifrado Ciphers y Macs
Realizado por: Honores, L. 2019

3. Se debe guardar los cambios y reiniciar el servicio sshd.

- ***Vulnerabilidad HTTP TRACE Method Enabled: CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386***

  Impacto: Extracción de la información respecto al servidor e información relacionada con las sesiones de los usuarios conectados.

  Subcontrol

  5.1: Establecer configuraciones seguras.

  Remediación:

  Esta vulnerabilidad se la pudo corregir, se deshabilitó el método Trace en el servidor Apache httpd.conf como se muestra:

  1. Ingresar al archivo vi /etc/httpd/conf/httpd.conf
  2. Aumentar al final del archivo **TraceEnable off**

```
# files.  This usually improves server performance, but must
# be turned off when serving from networked-mounted
# filesystems or if support for these functions is otherwise
# broken on your system.
# Defaults if commented: EnableMMAP On, EnableSendfile Off
#
#EnableMMAP off
EnableSendfile on

# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
TraceEnable off
IncludeOptional conf.d/*.conf
:wq
```

Figura 5-3: Desactivar TraceEnable
Realizado por: Honores, L. 2019

3. Se debe guardar los cambios y reiniciar el servicio httpd.

- ***Vulnerabilidad de Apache HTTPD: CVE-2018-1312***

  Impacto: Ataques de reproducción contra el servidor, afecta parcialmente a la integridad del sistema, confidencialidad y la disponibilidad del sistema.

  Subcontrol:

  2.2: Asegurar que el software tenga soporte del fabricante.

  Remediación:

  Esta vulnerabilidad se la pudo corregir con la actualización de Apache 2.4.6 a la versión 2.4.33 la descarga se la realizó en la siguiente página:

  - http://archive.apache.org/dist/httpd/httpd-2.4.33.tar.gz

- ***Vulnerabilidad Database Open Access***

  Impacto: Un atacante puede obtener la información confidencial de la base de datos.

  Subcontrol:

  9.4: Aplicar firewalls basados en host o filtrado de puertos.

  Remediación:

  Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC del INEVAL implementar un firewall basado en host o herramientas de filtrado, para limitar el acceso directo a los sistemas de confianza.

- ***Vulnerabilidad de PHP CVE-2013-4248***

  Impacto: La modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que se puede modificar, o el alcance de lo que el atacante puede afectar es limitado

  Subcontrol:

  2.2: Asegurar que el software tenga soporte del fabricante.

Remediación:

Esta vulnerabilidad se la pudo corregir con la actualización de PHP 5.4.16 a la versión 5.4.18 la descarga se la realizó de la siguiente página:

- http://www.php.net/releases/

- ***Vulnerabilidad Untrusted TLS/SSL Server X.509 Certificate***

  Impacto: Un atacante podría usar esto para ataques MitM, acceder a datos sensibles y otros ataques.

  Subcontrol:

  5.1: Establecer configuraciones seguras.

  Remediación:

  Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC del INEVAL verificar que el nombre común (CN) refleje el nombre de la entidad que presenta el certificado. Si los certificados o cualquiera de los certificados de la cadena han expirado o han sido revocados, obtener un nuevo certificado de su Autoridad de Certificación (CA)**.**

- ***Vulnerabilidad TLS/SSL Server Supports RC4 Cipher Algorithms: CVE-2013-2566***

  Impacto: Un atacante podría usar esto para ataques MitM, acceder a datos sensibles y otros ataques.

  Subcontrol:

  5.1: Establecer configuraciones seguras.

  Remediación:

  Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC del INEVAL verificar que el nombre común (CN) refleje el nombre de la entidad que presenta el certificado. Si los certificados o cualquiera de los certificados de la cadena han expirado o han sido revocados, obtener un nuevo certificado de su Autoridad de Certificación (CA)**.**

- ***Vulnerabilidad: SSH Server Supports Diffie-Hellman-Group1-Sha1: CVE-2015-4000***

  Impacto: La modificación de algunos archivos o información del sistema es posible, pero el atacante no tiene control sobre lo que se puede modificar, o el alcance de lo que el atacante puede afectar es limitado.

  Subcontrol:

5.1: Establecer configuraciones seguras.

Remediación:

Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC que deshabilite todos los cifrados de exportación basados en Diffie-Hellman en los puntos finales del servidor SSL / TLS.

- ***Vulnerabilidad ICMP Redirection Enabled***

Impacto: Si un atacante puede falsificar paquetes de redireccionamiento ICMP, puede alterar las tablas de enrutamiento en el host y posiblemente subvertir la seguridad del host al hacer que el tráfico fluya a través de una ruta que no pretendía.

Subcontrol:

5.1: Establecer configuraciones seguras.

Remediación:

Esta vulnerabilidad se la corrigió deshabilitando la redirección ICMP de la siguiente manera:

1. Ingresar los siguientes comandos como root.
    - sysctl -w net.ipv4.conf.all.accept_redirects=0
    - sysctl -w net.ipv4.conf.default.accept_redirects=0
    - sysctl -w net.ipv4.conf.all.secure_redirects=0
    - sysctl -w net.ipv4.conf.default.secure_redirects=0

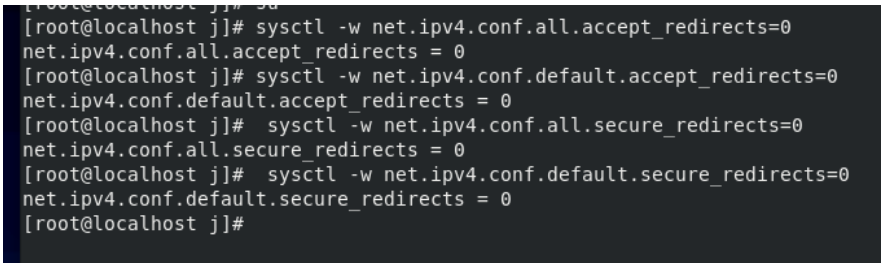


Figura 5-4: Desactivar la redirección ICMP
Realizado por: Honores, L. 2019

- ***Vulnerabilidad TLS/SSL Server Supports Anonymous Cipher Suites with no Key Authentication***

Impacto: Ataques man-in-the-middle, controlar o manipular los datos sensibles.

Subcontrol:

5.1: Establecer configuraciones seguras.

Remediación:

Esta vulnerabilidad se la corrigió deshabilitando el cifrado RC4 de la siguiente manera:

1. Ingresar a regedit.
2. Buscar la ruta HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Control \ SecurityProviders \ SCHANNEL \ Ciphers
3. Crear las 3 nuevas claves RC4 128/128, RC4 40/128, RC4 56/128

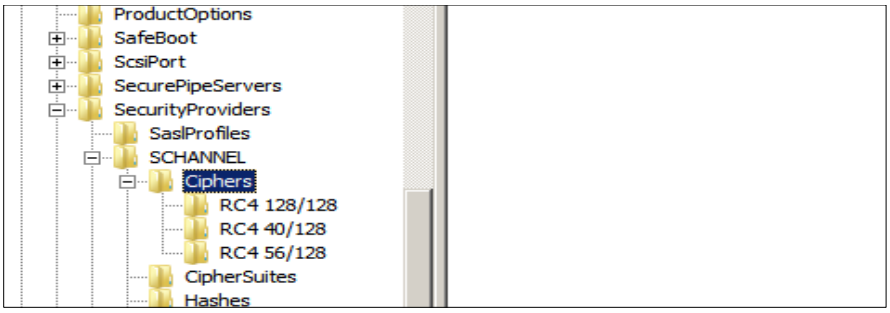


Figura 5-5: Claves RC4
Realizado por: Honores, L. 2019

4. Crear dentro de cada clave "Enabled"=dword:00000000.

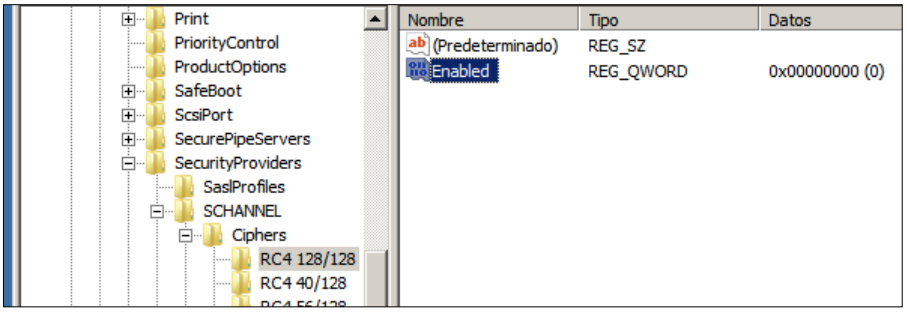


Figura 5-6: Creación de las claves RC4
Realizado por: Honores, L. 2019

- ***Vulnerabilidad TLS/SSL Server is Enabling the BEAST Attack: CVE-3389***

Impacto: Permite la divulgación no autorizada de información.

Subcontrol:

5.1: Establecer configuraciones seguras.

Remediación:

Esta vulnerabilidad no pudo ser remediada, por lo que se recomendó al departamento de TIC deshabilitar los protocolos afectados (SSLv3 y TLS 1.0). La única configuración completamente segura es utilizar el cifrado autenticado con datos asociados (AEAD), por ejemplo. AES-GCM, AES-CCM en TLS 1.2.

Posteriormente, se procede con el resumen de los subcontroles aplicados para cada una de las vulnerabilidades, con la respectiva actividad utilizada para la remediación, como se muestra en la Tabla 5-1:

Tabla 5-1: Resumen de controles aplicados

№	Vulnerabilidad	Subcontrol	Descripción	Remediación
VULNERABILIDADES CRÍTICAS				
1	Apache HTTPD: CVE-2017-7679	9.5	Implementar firewalls de aplicación.	Vulnerabilidad no corregida.
2	PHP: CVE-2019-9641	2.2	Asegurar que el software tenga soporte del fabricante.	Se actualizó la versión de PHP.
3	Apache HTTPD: CVE-2017-3167	9.5	Implementar firewalls de aplicación.	Vulnerabilidad no corregida.
4	Apache HTTPD: CVE-2017-3169	9.5	Implementar firewalls de aplicación.	Vulnerabilidad no corregida.
5	PHP: CVE-2015-4599	9.4	Aplicar firewalls basados en host o filtrado de puertos.	Vulnerabilidad no corregida.
6	PHP: CVE-2015-6836	9.4	Aplicar firewalls basados en host o filtrado de puertos.	Vulnerabilidad no corregida.
7	Windows SMB CVE-2017-0146	2.2	Asegurar que el software tenga soporte del fabricante.	Se instaló el parche correspondiente.
8	Default Password Telnet	4.2	Cambiar contraseñas por defecto.	Se realizó el cambio de contraseña.
9	Default Password SSH	4.2	Cambiar contraseñas por defecto.	Se realizó el cambio de contraseña.
10	Code Execution Via Specially Crafted Environment Variables CVE-2014-6278	9.4	Aplicar firewalls basados en host o filtrado de puertos.	Vulnerabilidad no corregida.
11	Untrusted pointer use issue leading to code execution CVE-2014-6277	2.2	Asegurar que el software tenga soporte del fabricante.	Se actualizó la versión de PHP.
12	Default or Guessable SNMP Community Names	5.1	Establecer configuraciones seguras.	Vulnerabilidad no corregida.
VULNERABILIDADES SEVERAS				
1	SSH Birthday attacks on 64-bit block ciphers (SWEET32) CVE-2016-2183	5.1	Establecer configuraciones seguras.	Se deshabilitó los cifrados 3DES .
2	HTTP TRACE Method Enabled	5.1	Establecer configuraciones seguras.	Se deshabilitó el método Tracer en el servidor Apache.
3	Apache HTTPD: CVE-2018-1312	2.2	Asegurar que el software tenga soporte del fabricante.	Se actualizó la versión de Apache.
4	Database Open Access	9.4	Aplicar firewalls basados en host o filtrado de puertos.	Vulnerabilidad no corregida.
5	PHP CVE-2013-4248	2.2	Asegurar que el software tenga soporte del fabricante.	Se actualizó la versión de PHP.
6	Untrusted TLS/SSL server X.509 certificate	5.1	Establecer configuraciones seguras.	Vulnerabilidad no corregida.
7	TLS/SSL Server Supports RC4 Cipher Algorithms CVE-2013-2566	5.1	Establecer configuraciones seguras.	Vulnerabilidad no corregida.
8	SSH Server Supports diffie-hellman-group1-sha1 CVE-2015-4000	5.1	Establecer configuraciones seguras.	Vulnerabilidad no corregida.
9	ICMP Redirection Enabled	5.1	Establecer configuraciones seguras.	Se deshabilitó la redirección ICMP del servidor.
10	TLS/SSL Server Supports Anonymous Cipher Suites with no Key Authentication	5.1	Establecer configuraciones seguras.	Se deshabilitó el cifrado RC4.
11	TLS/SSL Server is enabling the BEAST attack CVE-2011-3389	5.1	Establecer configuraciones seguras.	Vulnerabilidad no corregida.

Realizado por: Honores, L. 2019

En el primer escaneo de la red LAN se detectaron 23 vulnerabilidades entre críticas y severas ver Gráfico 3-1, después de la aplicación del sistema de seguridad basados en los controles CIS se encontraron 12 vulnerabilidades de las cuales 7 son críticas y 5 severas, como se muestra en el Gráfico 5-1.

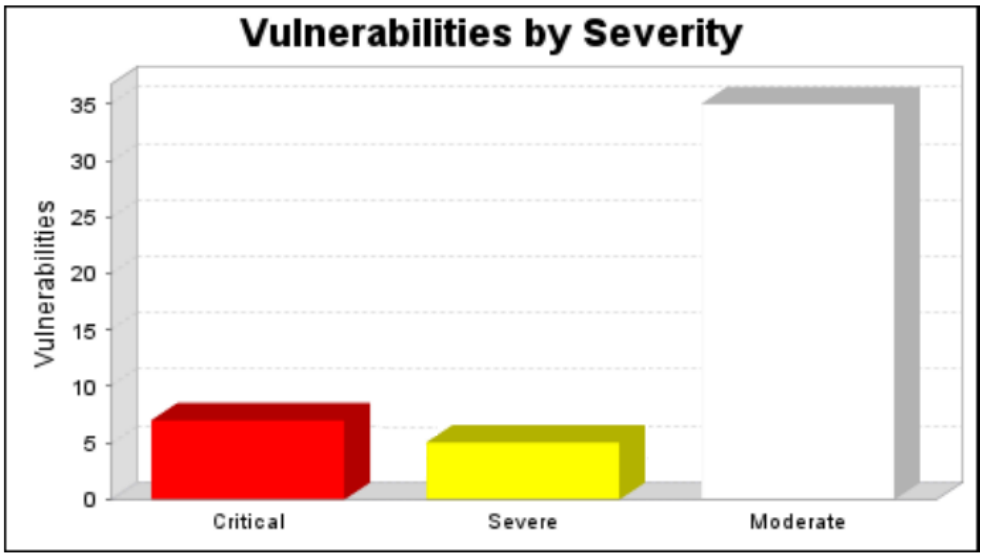


Gráfico 5-1: Vulnerabilidades detectadas segundo escaneo
Fuente: (InsightVM, 2019)
Realizado por: Honores, L. 2019

CONCLUSIONES

- Se realizó un análisis de las herramientas utilizadas para el escaneo de vulnerabilidades, lo que permitió escoger InsightVM ya que se apega más a las necesidades de la investigación.

- De las 58 vulnerabilidades encontradas en el análisis de los equipos críticos de la red LAN del INEVAL, 12 fueron críticas, 11 severas y 35 moderadas para el diseño del sistema de seguridad se tomaron en cuenta las dos primeras ya que estas son más factibles de ser explotadas, lo cual puede provocar pérdida de confidencialidad de los datos y de los recursos al igual que puede verse afectada la integridad de los mismos.

- Las vulnerabilidades con mayor ocurrencia fueron las de TS/SSL estas están presentes en la mayoría de servidores, seguidas de versiones obsoletas de PHP y Apache, así también cuentan con servicios y puertos activos los cuales deberían ser restringidos según la funcionalidad del servidor.

- De las 23 vulnerabilidades detectadas, se realizó la remediación de 11 vulnerabilidades entre críticas y severas, lo cual dio un porcentaje de implementación del Sistema de Seguridad del 52%.

- Con la demostración de la hipótesis, se comprobó que al implementar el Sistema de Seguridad basado en controles CIS hubo una reducción de vulnerabilidades del 42%.

RECOMENDACIONES

- Actualmente con la evolución de la tecnología y todos los ataques informáticos que se han realizado a las instituciones públicas en Ecuador, se recomienda realizar un análisis periódico de vulnerabilidades en los equipos críticos de la red LAN para así poder remediar estas brechas de seguridad antes de que sean explotadas por terceros y ocasionen pérdida de información o fallos en los sistemas.

- Implementar completamente el sistema se seguridad basado en controles CIS a fin que se pueda reducir las vulnerabilidades existentes en la red LAN de la institución.

- Incentivar a las instituciones públicas sobre la implementación de controles de ciberseguridad para que así se pueda reducir las brechas de seguridad existentes en sus equipos críticos.

- Dentro de esta investigación, siempre que se desee que haya una mejora continua del mismo; se recomienda a futuros estudiantes que tengan interés en el tema, la complementación del sistema de seguridad con la aplicación de más controles CIS y la utilización de varias herramientas para el escaneo de vulnerabilidades.

BIBLIOGRAFÍA

Business School. (2019). OBS BUSINESS SCHOOL. Obtenido de OBS BUSINESS SCHOOL: https://www.obsbusiness.school/blog/10-amenazas-informaticas-en-el-punto-de-mira

Castro, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. Ecuador: Universidad Estatal del sur de Manabí.

CEDIA. (2019). Acciones ante los ataques a infraestructura y servidores del país. Obtenido de CEDIA:https://www.cedia.edu.ec/es/noticias-y-eventos/noticias/noticias-2019/acciones-ante-los-ataques-a-infraestructura-y-servidores-del-pais

CIS Controls. (2019). Center for Internet Security. Obtenido de: https://www.cisecurity.org/controls/

El Comercio. (15 de abril de 2019). Ecuador denuncia 40 millones de ciberataques tras el retiro de asilo a Assange. Obtenido de: https://www.elcomercio.com/actualidad/seguridad/ecuador-denuncia-millones-ciberataques-assange.html

Ministerio de Defensa Nacional. (2018). Política de la Defensa Nacional del Ecuador. Ministerio de Defensa Nacional. Obtenido de: http://revistasdigitales.upec.edu.ec/index.php/sathiri/article/download/404/438/

Enrriquez, J. (2015). Los delitos informáticos y su penalización en el código orgánico integral penal ecuatoriano. Obtenido de: https://revistasdigitales.upec.edu.ec/index.php/sathiri/article/view/404/438

Franco, D. (2013). Herramienta para la detección de vulnerabilidades basadas en la identificación de servicios. Colombia: Universidad de Cartagena.

Garzón, D. (2016). Metodología de Análisis de Vulnerabilidades para pequeñas y medianas empresas. Bogotá: Pontificia Universidad Javeriana.

Mendoza, M. (2014). Cómo utilizar OpenVas para la evaluación de vulnerabilidades. Obtenido de:https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

Nacional Vulnerability Database. (2019). Metric CVSS. Obtenido de Technology National Institute of Standards: https://nvd.nist.gov/vuln-metrics/cvss

Quishpe, H. (2016). Análisis de vulnerabilidades en la red LAN jerárquica de la Universidad de Loja. Ecuador: Universidad de Loja.

Ramiro. (2018). Ciberseguridad. Obtenido de: https://ciberseguridad.blog/guia-practica-para-implementar-los-controles-criticos-de-seguridad/

Rapid7. (2019). Rapid7. Obtenido de Rapid7: https://insightvm.help.rapid7.com/docs/security-console-overview

Reinoso, A. (2017). Análisis y evaluación de riesgos de seguridad informática a través del análisis de tráfico en redes de área local.

Romero, M. (2018). Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades 3 ciencias. Obtenido de: 3 ciencias.

Tenable. (2019). Tenable. Obtenido de Tenable: https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/datasheets/NessusPro-%28DS%29-EsLa.pdf

TrendMicro. (2019). TrendMicro. Obtenido de TrendMicro: https://www.trendmicro.com/es_es/partners/explore-alliance-partners/qualys.html

Voutssas, M. (2010). Preservación documental digital y seguridad informática. Investigación bibliotecológica.

ANEXOS

ANEXO A: Remediación de Vulnerabilidades Críticas

Vulnerabilidad 1

3.1.10. Apache HTTPD: mod_mime Buffer Overread (CVE-2017-7679) (apache-httpd-cve-2017-7679)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_mime. Review your web server configuration for validation. mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.26

Upgrade to Apache HTTPD version 2.4.26

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.26.tar.gz

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

Vulnerabilidad 2

3.1.12. PHP Vulnerability: CVE-2019-9641 (php-cve-2019-9641)

Description:

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.

Vulnerability Solution:

•Upgrade to PHP version 7.1.27

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 7.2.16

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 7.3.3

Download and apply the upgrade from: http://www.php.net/releases/

Vulnerabilidad 3

3.1.8. Apache HTTPD: ap_get_basic_auth_pw() Authentication Bypass (CVE-2017-3167) (apache-httpd-cve-2017-3167)

Description:

Use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed. Third-party module writers SHOULD use ap_get_basic_auth_components(), available in 2.2.34 and 2.4.26, instead of ap_get_basic_auth_pw(). Modules which call the legacy ap_get_basic_auth_pw() during the authentication phase MUST either immediately authenticate the user after the call, or else stop the request immediately with an error response, to avoid incorrectly authenticating the current request.

Vulnerabilitv Solution:

•Apache HTTPD >= 2.2 and < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.26

Upgrade to Apache HTTPD version 2.4.26

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.26.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

Vulnerabilidad 4

3.1.9. Apache HTTPD: mod_ssl Null Pointer Dereference (CVE-2017-3169) (apache-httpd-cve-2017-3169)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_ssl. Review your web server configuration for validation. mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

Vulnerability Solution:

•Apache HTTPD >= 2.2 and < 2.2.34

Upgrade to Apache HTTPD version 2.2.34

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.2.34.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

•Apache HTTPD >= 2.4 and < 2.4.26

Upgrade to Apache HTTPD version 2.4.26

Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.26.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

Vulnerabilidad 5

3.1.2. PHP Vulnerability: CVE-2015-4599 (php-cve-2015-4599)

Description:

The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

Vulnerability Solution:

•Upgrade to PHP version 5.4.40

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.5.24

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.6.8

Download and apply the upgrade from: http://www.php.net/releases/

Vulnerabilidad 6

3.1.11. PHP Vulnerability: CVE-2015-6836 (php-cve-2015-6836)

Description:

The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage headers, which allows remote attackers to execute arbitrary code via crafted serialized data that triggers a "type confusion" in the serialize_function_call function.

Vulnerability Solution:

•Upgrade to PHP version 5.4.45

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.5.29

Download and apply the upgrade from: http://www.php.net/releases/

•Upgrade to PHP version 5.6.13

Download and apply the upgrade from: http://www.php.net/releases/

Vulnerabilidad 7

3.1.7. Microsoft CVE-2017-0146: Windows SMB Remote Code Execution Vulnerability (msft-cve-2017-0146)

Description:

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server. To exploit the vulnerability, in most situations, an authenticated attacker could send a specially crafted packet to a targeted SMBv1 server. The security update addresses the vulnerability by correcting how SMBv1 handles these specially crafted requests.

Vulnerability Solution:

•Microsoft Windows Embedded Standard 7 SP1 (x86)

March, 2017 Security Only Quality Update for Windows Embedded Standard 7 (KB4012212)

Download and apply the patch from: http://support.microsoft.com/kb/4012212

•Microsoft Windows Server 2008 R2 SP1 (ia64), Microsoft Windows Server 2008 R2, Enterprise Edition SP1 (ia64), Microsoft Windows Server 2008 R2, Standard Edition SP1 (ia64), Microsoft Windows Server 2008 R2, Datacenter Edition SP1 (ia64), Microsoft Windows Server 2008 R2, Web Edition SP1 (ia64)

March, 2017 Security Only Quality Update for Windows Server 2008 R2 for Itanium-based Systems (KB4012212)

Download and apply the patch from: http://support.microsoft.com/kb/4012212

•Microsoft Windows 7 SP1 (x86_64), Microsoft Windows 7 Home, Basic Edition SP1 (x86_64), Microsoft Windows 7 Home, Basic N Edition SP1 (x86_64), Microsoft Windows 7 Home, Premium Edition SP1 (x86_64), Microsoft Windows 7 Home, Premium N Edition SP1 (x86_64), Microsoft Windows 7 Ultimate Edition SP1 (x86_64), Microsoft Windows 7 Ultimate N Edition SP1 (x86_64), Microsoft Windows 7 Enterprise Edition SP1 (x86_64), Microsoft Windows 7 Enterprise N Edition SP1 (x86_64), Microsoft Windows 7 Professional Edition SP1 (x86_64), Microsoft Windows 7 Starter Edition SP1 (x86_64), Microsoft Windows 7 Starter N Edition SP1 (x86_64)

March, 2017 Security Only Quality Update for Windows 7 for x64-based Systems (KB4012212)

Download and apply the patch from: http://support.microsoft.com/kb/4012212

Vulnerabilidad 8

3.1.5. Default Telnet password: admin password "password" (telnet-default-account-admin-password-password)

Description:

The admin account uses a password of "password". This would allow anyone to log into the machine via telnet and take complete control.

Vulnerability Solution:

Change the password to a non-default value.

Vulnerabilidad 9

3.1.3. Default SSH password: admin password "password" (ssh-default-account-admin-password-password)

Description:

The admin account uses a password of "password". This would allow anyone to log into the machine via SSH and take complete control.

Vulnerability Solution:

Change the password to a non-default value.

Vulnerabilidad 10

3.1.2. CVE-2014-6278 bash: code execution via specially crafted environment variables (gnu-bash-cve-2014-6278)

Description:

GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary commands via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.

Vulnerability Solution:

Use your operating system's package manager to upgrade GNU bash to the latest version.

Vulnerabilidad 11

3.1.1. CVE-2014-6277 bash: untrusted pointer use issue leading to code execution (gnu-bash-cve-2014-6277)

Description:

GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access, and untrusted-pointer read and write operations) via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271 and CVE-2014-7169.

Vulnerability Solution:

Use your operating system's package manager to upgrade GNU bash to the latest version.

Vulnerabilidad 12

3.1.11. Default or Guessable SNMP community names: public (snmp-read-0001)

Description:

The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers, to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition many SNMP servers provide very simple default community strings. The community string "public" is a default on a number of SNMP servers.

This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.

Vulnerability Solution:

•Secure the SNMP installation

1. If you do not absolutely need SNMP, disable it. SNMP versions 1 and 2c are inherently insecure. SNMP version 3 provides more complex authentication and encryption.
2. If you must use SNMP be sure to use complex and difficult to guess community names. Use the same policy for community names as you use for passwords.
3. Try to make all your MIB's read only. This will limit the damage an attacker can do to your network.

ANEXO B: Remediación Vulnerabilidades Severas

Vulnerabilidad 1

3.2.135. SSH Birthday attacks on 64-bit block ciphers (SWEET32) (ssh-cve-2016-2183-sweet32)

Description:

Legacy block ciphers having a block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. The security of a block cipher is often reduced to the key size k: the best attack should be the exhaustive search of the key, with complexity 2 to the power of k. However, the block size n is also an important security parameter, defining the amount of data that can be encrypted under the same key. This is particularly important when using common modes of operation: we require block ciphers to be secure with up to 2 to the power of n queries, but most modes of operation (e.g. CBC, CTR, GCM, OCB, etc.) are unsafe with more than 2 to the power of half n blocks of message (the birthday bound). With a modern block cipher with 128-bit blocks such as AES, the birthday bound corresponds to 256 exabytes. However, for a block cipher with 64-bit blocks, the birthday bound corresponds to only 32 GB, which is easily reached in practice. Once a collision between two cipher blocks occurs it is possible to use the collision to extract the plain text data.

Vulnerability Solution:

Remove all 3DES ciphers from the cipher list specified in sshd_config.

Vulnerabilidad 2

3.2.41. HTTP TRACE Method Enabled (http-trace-method-enabled)

Description:

The HTTP TRACE method is normally used to return the full HTTP request back to the requesting client for proxy-debugging purposes. An attacker can create a webpage using XMLHTTP, ActiveX, or XMLDOM to cause a client to issue a TRACE request and capture the client's cookies. This effectively results in a Cross-Site Scripting attack.

Vulnerability Solution:

•Apache HTTPD, Apache Tomcat

Disable HTTP TRACE Method for Apache

Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a configuration directive called TraceEnable. To deny TRACE requests, add the following line to the server configuration:

TraceEnable off

For older versions of the Apache webserver, use the mod_rewrite module to deny the TRACE requests:

RewriteEngine On

RewriteCond %{REQUEST_METHOD} ^TRACE

RewriteRule .* - [F]

In Apache Tomcat, the HTTP Trace can be disabled by adding security constraints into the Java Servlet specification within the web.xml configuration file and by setting the attribute allowTrace="False" to the HTTP connector in server.xml. For Spring Boot embedded Tomcat configuration, please refer here

Vulnerabilidad 3

3.2.3. Apache HTTPD: Weak Digest auth nonce generation in mod_auth_digest (CVE-2018-1312) (apache-httpd-cve-2018-1312)

Description:

The affected asset is vulnerable to this vulnerability ONLY if it is running one of the following modules: mod_auth_digest. Review your web server configuration for validation. When generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Vulnerability Solution:

Apache HTTPD >= 2.4 and < 2.4.33
Download and apply the upgrade from: http://archive.apache.org/dist/httpd/httpd-2.4.33.tar.gz
Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

Vulnerabilidad 4

3.2.67. Database Open Access (database-open-access)

Description:

The database allows any remote system the ability to connect to it. It is recommended to limit direct access to trusted systems because databases may contain sensitive data, and new vulnerabilities and exploits are discovered routinely for them. For this reason, it is a violation of PCI DSS section 1.3.6 to have databases listening on ports accessible from the Internet, even when protected with secure authentication mechanisms.

Vulnerability Solution:

Configure the database server to only allow access to trusted systems. For example, the PCI DSS standard requires you to place the database in an internal network zone, segregated from the DMZ

Vulnerabilidad 5

3.2.160. PHP Vulnerability: CVE-2013-4248 (php-cve-2013-4248)

Description:

The openssl_x509_parse function in openssl.c in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

Vulnerability Solution:

- Upgrade to PHP version 5.4.18

  Download and apply the upgrade from: http://www.php.net/releases/
- Upgrade to PHP version 5.5.2

  Download and apply the upgrade from: http://www.php.net/releases/

Vulnerabilidad 6

3.2.50. Untrusted TLS/SSL server X.509 certificate (tls-untrusted-ca)

Description:

The server's TLS/SSL certificate is signed by a Certification Authority (CA) that is not well-known or trusted. This could happen if: the chain/intermediate certificate is missing, expired or has been revoked; the server hostname does not match that configured in the certificate; the time/date is incorrect; or a self-signed certificate is being used. The use of a self-signed certificate is not recommended since it could indicate that a TLS/SSL man-in-the-middle attack is taking place

Vulnerability Solution:

Ensure the common name (CN) reflects the name of the entity presenting the certificate (e.g., the hostname). If the certificate(s) or any of the chain certificate(s) have expired or been revoked, obtain a new certificate from your Certificate Authority (CA) by following their documentation. If a self-signed certificate is being used, consider obtaining a signed certificate from a CA.

References: Mozilla: Connection Untrusted ErrorSSLShopper: SSL Certificate Not Trusted ErrorWindows/IIS certificate chain config Apache SSL configNginx SSL configCertificateChain.io

Vulnerabilidad 7

3.2.178. TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566) (rc4-cve-2013-2566)

Description:

Recent cryptanalysis results exploit biases in the RC4 keystream to recover repeatedly encrypted plaintexts. As a result, RC4 can no longer be seen as providing a sufficient level of security for SSL/TLS sessions. It has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of ciphertext in a large number of sessions that use the same plaintext.

Vulnerability Solution:

Configure the server to disable support for RC4 ciphers.

For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling rc4 ciphers.

The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

Vulnerabilidad 8

3.2.179. SSH Server Supports diffie-hellman-group1-sha1 (ssh-cve-2015-4000)

Description:

The prime modulus offered when diffie-hellman-group1-sha1 is used only has a size of 1024 bits. This size is considered weak and within theoretical range of the so-called Logjam attack.

Vulnerability Solution:

Remove ssh-diffie-hellman-group1-sha1 from the KexAlgorithms list specified in sshd_config.

Vulnerabilidad 9

3.2.6. ICMP redirection enabled (linux-icmp-redirect)

Description:

By default, many linux systems enable a feature called ICMP redirection, where the machine will alter its route table in response to an ICMP redirect message from any network device.

There is a risk that this feature could be used to subvert a host's routing table in order to compromise its security (e.g., tricking it into sending packets via a specific route where they may be sniffed or altered).

Vulnerability Solution:

Linux

Issue the following commands as root:

```
sysctl -w net.ipv4.conf.all.accept_redirects=0
sysctl -w net.ipv4.conf.default.accept_redirects=0
sysctl -w net.ipv4.conf.all.secure_redirects=0
sysctl -w net.ipv4.conf.default.secure_redirects=0
```

These settings can be added to /etc/sysctl.conf to make them permanent.

Vulnerabilidad 10

3.2.49. TLS/SSL Server Supports Anonymous Cipher Suites with no Key Authentication (ssl-anon-ciphers)

Description:

The server is configured to support anonymous cipher suites with no key authentication. These ciphers are highly vulnerable to man in the middle attacks.

Vulnerability Solution:

Configure the server to disable support for anonymous cipher suites.

For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for instructions on disabling anonymous cipher suites.

The following recommended configuration provides a higher level of security. This configuration is compatible with Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

Vulnerabilidad 11

3.2.183. TLS/SSL Server is enabling the BEAST attack (ssl-cve-2011-3389-beast)

Description:

The SSL protocol, as used in certain configurations of Microsoft Windows and browsers such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera (and other products negotiating SSL connections) encrypts data by using CBC mode with chained initialization vectors. This potentially allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack. By supporting the affected protocols and ciphers, the server is enabling the clients in to being exploited.

Vulnerability Solution:

There is no server-side mitigation available against the BEAST attack. The only option is to disable the affected protocols (SSLv3 and TLS 1.0). The only fully safe configuration is to use Authenticated Encryption with Associated Data (AEAD), e.g. AES-GCM, AES-CCM in TLS 1.2.

ANEXO C: Reporte Ejecutivo

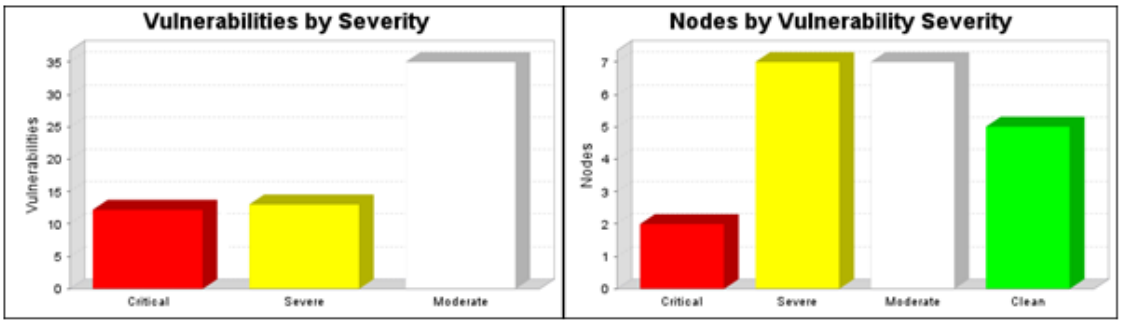
1. Executive Summary

This report represents a security audit performed by InsightVM from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

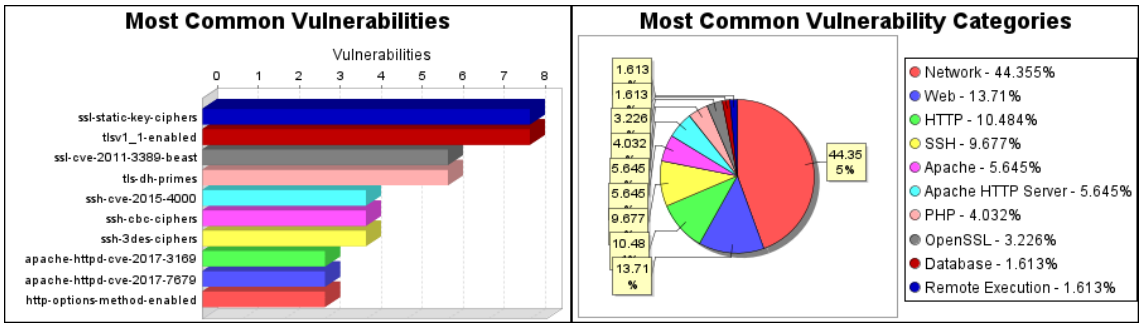
Site Name	Start Time	End Time	Total Time	Status
Server 1	Dec 17, 2019 12:12, COT	Dec 17, 2019 12:42, COT	30 minutes	Success
Server 4	Dec 17, 2019 16:14, COT	Dec 17, 2019 16:32 COT	18 minutes	Success
server 2	Dec 17, 2019 12:50, COT	Dec 17, 2019 13:20, COT	30 minutes	Success
server 6	Dec 17, 2019 13:16, COT	Dec 17, 2019 13:24, COT	77 minutes	Success
server 7	Dec 17, 2019 13:25, COT	Dec 17, 2019 13:36, COT	11 minutes	Success
Server 3	Dec 17, 2019 13:50, COT	Dec 17, 2019 13:21, COT	31 minutes	Success
Server 5	Dec 17, 2019 14:11, COT	Dec 17, 2019 14:15, COT	4 minutes	Success

There is not enough historical data to display the overall asset trend.

The audit was performed on 35 systems, 35 of which were found to be active and were scanned.

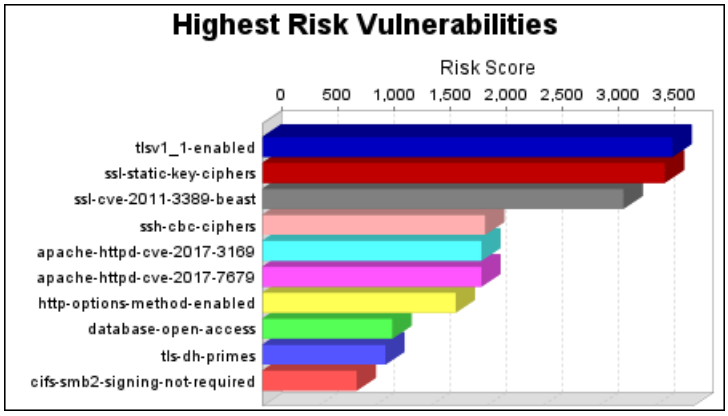


There were 58 vulnerabilities found during this scan. Of these, 11 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 12 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 35 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 7 of the systems, making them most susceptible to attack. 5 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 8 systems. No vulnerabilities were found on the remaining 5 systems.

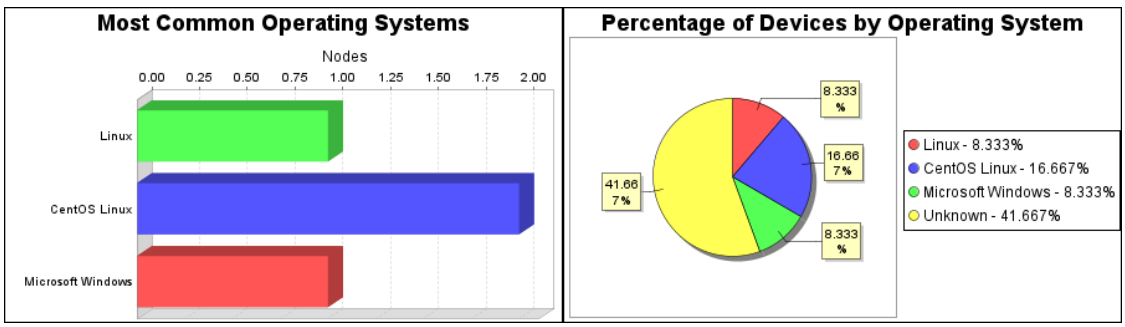


There were 8 occurrences of the ssl-static-key-ciphers and tlsv1_1-enabled vulnerabilities, making them the most common vulnerabilities. There were 55 vulnerability instances in the Network category, making it the most common vulnerability category.

The tlsv1_1-enabled vulnerability poses the highest risk to the organization with a risk score of 3,652. Risk scores are based on the types and numbers of vulnerabilities on affected assets.



There were 5 operating systems identified during this scan.



The Linux operating system was found on 3 systems, making it the most common operating system. There were 27 services found to be running during this scan.

The SSH service was found on 5 systems, making it the most common service. The HTTPS service was found to have the most vulnerabilities during this scan with 20 vulnerabilities.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS Y ANÁLISIS BIBLIOGRÁFICO Y DOCUMENTAL

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: *07 / 09 / 2021*

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: *Lucy Johanna Honores Chuchuca*
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: *Magíster en Seguridad Telemática*
f. Analista de Biblioteca responsable*:* *Lic. Luis Caminos Vargas Mgs.*

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602766974, cn=LUIS ALBERTO CAMINOS VARGAS
Fecha: 2021.09.07 12:35:58 -05'00'

0089-DBRAI-UPT-IPEC-2021