ISBN: 978-99923-993-7-8

ESCUELA ESPECIALIZADA EN INGENIERÍA ITCA – FEPADE

DIRECCIÓN DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

PROGRAMA DE INVESTIGACIÓN APLICADA

INFORME FINAL DE INVESTIGACIÓN

"ESTUDIO DE LA SEGURIDAD DE LA RED DE DATOS DE LA ESCUELA ESPECIALIZADA EN INGENIERÍA ITCA-FEPADE."

SEDES Y ESCUELAS PARTICIPANTES:	SEDE CENTRAL ESCUELA DE INGENIERÍA EN COMPUTACIÓN
DOCENTE INVESTIGADOR RESPONSABLE:	TÉC. EDUARDO ADALBERTO GUILLÉN
DOCENTES INVESTIGADORES PARTICIPANTES:	LIC. MARIO ERNESTO QUINTANILLA LIC. DENIS ISAÍAS CERVANTES

SANTA TECLA, ENERO 2013

ISBN: 978-99923-993-7-8

ESCUELA ESPECIALIZADA EN INGENIERÍA ITCA – FEPADE

DIRECCIÓN DE INVESTIGACIÓN Y PROYECCIÓN SOCIAL

PROGRAMA DE INVESTIGACIÓN APLICADA

INFORME FINAL DE INVESTIGACIÓN

"ESTUDIO DE LA SEGURIDAD DE LA RED DE DATOS DE LA ESCUELA ESPECIALIZADA EN INGENIERÍA ITCA-FEPADE."

SEDES Y ESCUELAS PARTICIPANTES:	SEDE CENTRAL ESCUELA DE INGENIERÍA EN COMPUTACIÓN
DOCENTE INVESTIGADOR RESPONSABLE:	TÉC. EDUARDO ADALBERTO GUILLÉN
DOCENTES INVESTIGADORES PARTICIPANTES:	LIC. MARIO ERNESTO QUINTANILLA LIC. DENIS ISAÍAS CERVANTES

SANTA TECLA, ENERO 2013

Autores
Téc. Eduardo Adalberto Guillén
Lic. Mario Ernesto Quintanilla

004.6
G855e Guillén, Eduardo Adalberto
Estudio de la seguridad de red de datos de la Escuela Especializada en
sv Ingeniería ITCA-FEPADE / Eduardo Adalberto Guillén, Lic. Mario Ernesto Quintanilla. --1ª ed. -- San Salvador, El Salvador: ITCA Editores, 2013.

33 p.: il. ; 28 cm.
ISBN: 978-99923-993-7-8

1. Redes neurales (Computación). 2. Seguridad en computadores.
I. Quintanilla, Mario Ernesto, coaut. II. Escuela Especializada en Ingeniería ITCA-FEPADE.

Sitio web: www.itca.edu.sv
Correo electrónico: bibliotecologos@itca.edu.sv
Tiraje: 16 ejemplares
PBX: (503) 2132 – 7400
FAX: (503) 2132 – 7423
ISBN: 978-99923-993-7-8
Año 2013

ÍNDICE

CONTENIDO **PÁGINA**

1. INTRODUCCIÓN

El presente informe de resultados tiene por objetivo presentar los logros obtenidos en el proyecto titulado “Estudio de la seguridad de la red de datos de la Escuela Especializada en Ingeniería ITCA-FEPADE”.

La motivación principal para llevar a cabo el proyecto se basa en la necesidad de identificar posibles factores que ponen en riesgo la transferencia de datos a través de la infraestructura de red institucional.

En el desarrollo del proyecto se consideraron las recomendaciones técnicas que establecen los estándares internacionales sobre seguridad física y lógica de las redes, así mismo contamos con herramientas de software de libre distribución orientadas a analizar las vulnerabilidades de las redes de datos, las cuales facilitaron la realización del proyecto.

Los resultados obtenidos del proyecto muestran que ciertas áreas de la institución deben fortalecer la seguridad física de los equipos de comunicación. De igual forma se lograron detectar vulnerabilidades en los servidores institucionales, que podrían representar un riesgo para la seguridad de los datos.

Finalmente, las recomendaciones proporcionadas en el informe ayudarán a mejorar los niveles de seguridad física y lógica en la red institucional de ITCA-FEPADE.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DEFINICIÓN DEL PROBLEMA

La centralización y comunicación de la información de una empresa o institución a través de redes de datos, genera riesgos de ataque debido a que su volumen de operación y administración crece constantemente y se torna difícil controlar aquellos puntos de la red de datos identificados como vulnerables, especialmente los llamados dispositivos intermediarios, que son los encargados de suministrar y administrar el flujo de tráfico a través de la red. Dichos dispositivos son objeto frecuente de ataques, tanto por parte de software o código malicioso, como de personas que se dedican a la tarea de dañar estos dispositivos, lo que genera pérdida de la información, retraso en los procesos productivos de la institución e incluso pérdidas económicas. Es necesario por tanto, realizar un estudio detallado de todos aquellos elementos que interactúan en el proceso de comunicación pertinentes a la red de datos de la Escuela Especializada de Ingeniería ITCA-FEPADE, los cuales involucran la estructura física de la red y los elementos lógicos como sistemas

operativos y aplicaciones de software, hasta las políticas administrativas para controlar el acceso a los mismos.

Por lo que como resultado del estudio se pretende brindar información sobre la situación actual de la red frente a las diferentes amenazas internas y externas, así como la identificación de posibles vulnerabilidades, que pongan en riesgo la integridad, confidencialidad y disponibilidad de la misma.

2.2 ANTECEDENTES

La red institucional de la Escuela Especializada en Ingeniería ITCA-FEPADE centraliza sus operaciones en la sede de Santa Tecla, desde allí se establecen los enlaces de comunicación a cada regional en Santa Ana, San Miguel, Zacatecoluca y La Unión, a través de un proveedor de servicios de telecomunicaciones. La red local en cada sede cuenta con diferentes equipos de comunicación que permiten a los usuarios conectarse a la red y acceder a los recursos compartidos, como por ejemplo: impresoras, medios de almacenamiento, servidores institucionales o internet.

En la medida que la red institucional ha ido creciendo, se hace necesario mejorar las medidas de seguridad para controlar el acceso físico y lógico a los recursos compartidos. De allí la necesidad de realizar un estudio que ayude a determinar la situación actual de la red en relación a la seguridad.

Actualmente la institución no cuenta con un estudio previo que ayude a determinar las vulnerabilidades que pueda presentar la red de datos, y que pueden ser explotadas por usuarios expertos para causar algún daño a la información.

2.3 JUSTIFICACIÓN

Las redes de datos a través del tiempo han sido objetivo de constantes amenazas y ataques por ser un recurso indispensable en la labor cotidiana de toda empresa. En el caso particular de la Escuela Especializada en Ingeniería ITCA-FEPADE, la red institucional representa un pilar fundamental en el flujo efectivo de la información, por lo que debe mantenerse en una constante revisión mediante la realización de procesos de auditoria física y lógica que ayuden a mejorar la seguridad de la red.

La falta de mecanismos de seguridad en un entorno de red puede ser explotada por usuarios expertos, que les permita interceptar, alterar o eliminar datos confidenciales.

Lo anteriormente expuesto ha servido como base para dedicar esfuerzos en realizar un estudio que ayude a identificar las debilidades físicas que puedan poner en riesgo los

equipos de comunicación que forman parte de la red, así como también identificar las debilidades tecnológicas que permitan el acceso no autorizado a la información que intercambian los usuarios en la red.

El estudio dará como resultado un informe que describa el estado de la red de datos en materia de seguridad, detectando las vulnerabilidades a nivel físico y lógico en la infraestructura de red.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar un estudio detallado sobre la seguridad de la red de datos de la Escuela Especializada en Ingeniería ITCA-FEPADE.

3.2 OBJETIVOS ESPECÍFICOS

- Elaborar un inventario de los dispositivos intermediarios de la red de datos.
- Elaborar un diseño lógico de la red de datos en las regionales.
- Realizar pruebas del flujo del tráfico de la red.
- Detectar las fallas de seguridad de la red a nivel físico y lógico.
- Realizar un análisis de vulnerabilidades de la red mediante herramientas de software libre
- Elaborar una guía de propuestas de solución a los problemas detectados.

4. HIPÓTESIS

Llevar a cabo un proceso de auditoría a la red de datos para identificar las vulnerabilidades físicas y lógicas permitirá a los administradores de red contar con información pertinente para mejorar su seguridad, minimizando posibles ataques y fallas en la red de datos.

5. MARCO TEÓRICO DE LA INVESTIGACIÓN

Concepto de seguridad informática

Existen múltiples conceptos de seguridad informática, tanto en bibliografías como los que se publican en la web, sin embargo todos se unifican en el siguiente: "*La seguridad informática es una disciplina que se deriva de las ciencias informáticas y que se enfoca en los*

mecanismos, procedimientos y herramientas de hardware/software orientados a la protección de la información de una organización".

Principios de la seguridad informática

Existe información que debe o puede ser pública: puede ser visualizada por cualquier persona; y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella. En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo.

La integridad de la información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La disponibilidad u operatividad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La privacidad o confidencialidad de la información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño o volverse obsoleta.

El control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

La autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- Protección a la réplica: mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- No Repudio: mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

- Consistencia: se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- Aislamiento: este aspecto, íntimamente relacionado con la Confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- Auditoria: es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuándo las realiza.

Seguridad Física

La seguridad física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

Instalación eléctrica

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa.

Cableado

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

1. Interferencia: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica

no sufren el problema de alteración por acción de campos eléctricos, que si sufren los cables metálicos.

2. Corte del cable: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
3. Daños en el cable: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales. Sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

1. Desviando o estableciendo una conexión no autorizada en la red: un sistema de administración y procedimiento de identificación de acceso adecuado hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.
2. Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos. Luego, no hace falta penetrar en los cables físicamente para obtener los datos que transportan.

Sistema de Aire Acondicionado

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

Control de accesos

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cierre de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

Control de personas

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

Sistemas biométricos

Definimos a la Biometría como “la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos”.
La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.
La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

Circuitos cerrados de televisión

Permiten el control de todo lo que sucede en la planta según lo captado por las cámaras estratégicamente colocadas. Los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad. Las cámaras pueden estar a la vista (para ser utilizada como medida disuasiva) u ocultas (para evitar que el intruso sepa que está siendo captado por el personal de seguridad).

Seguridad lógica

La Seguridad Lógica consiste en la “aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.”
Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la Seguridad Lógica.
Los objetivos que se plantean son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

- Asegurar que la información transmitida cumpla con los criterios de integridad, confidencialidad y disponibilidad.
- Disponer de pasos alternativos de emergencia para la transmisión de información.

Controles de acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Identificación y autenticación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

1. Clave secreta
2. Tarjeta magnética.
3. Huellas digitales o la voz.
4. Patrones de escritura.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: programador,

líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

Limitaciones a los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.

Modalidad de acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.
- Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.
- Borrado: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- Todas las anteriores. Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación.
- Creación: permite al usuario crear nuevos archivos, registros o campos.
- Búsqueda: permite listar los archivos de un directorio determinado.

Palabras claves o contraseñas

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Listas de control de acceso

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

Firewalls o cortafuegos

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa. Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización.

6. METODOLOGÍA DE LA INVESTIGACIÓN

Para llevar a cabo el estudio de la seguridad en la red de datos se realizan dos procesos de auditoria que permitan recopilar toda la información relacionada con los controles de acceso físico y lógico de los equipos de red.

Auditoría Física

En la auditoría física se realiza un inventario de los equipos de comunicación que forman parte de la red institucional, esto comprende dispositivos de conmutación (switches), enrutadores (routers) y puntos de acceso inalámbrico; así como los servidores institucionales, que son los equipos donde se almacenan los principales aplicativos que utilizan los usuarios. Los principales aspectos que se toman en cuenta en la auditoria física son:

- Asegurar que el inventario de la red esté completo y actualizado.
- Identificar las especificaciones técnicas de los equipos y entender la función de estos componentes.
- Determinar si los componentes de la red mantienen niveles de seguridad física adecuados para la protección del personal, información, software y hardware.
- Asegurar que estos componentes son accesibles sólo por el personal autorizado.
- Elaborar los diagramas de topología, mostrándonos la forma en que se encuentran conectados los equipos de red.

Auditoria Lógica

La auditoría lógica comprende los siguientes aspectos:

- Determinar los controles de acceso lógico a los equipos.
- Identificar los niveles de cifrado de información.
- Determinar los niveles de acceso a los aplicativos institucionales.
- Identificar las rutas alternativas de comunicación en caso de fallas.

A continuación se detallan las actividades que se realizan en las auditorías física y lógica.

Fase1. Actividades para la auditoría física

Actividad	Participantes	Resultado Esperado
Elaborar el inventario de los equipos de red.	- Docentes investigadores - Estudiantes de la Sede Central y Regional San Miguel	- Reporte de inventario de equipos y ficha técnica.
Elaborar el diagrama de topología de la red.	- Docentes investigadores - Estudiantes de la Sede Central y Regional San Miguel	- Diagrama de topología de red en cada sede.
Identificar los controles de acceso físico a la red.	-Docentes investigadores -Estudiantes de la Sede Central y Regional San Miguel	- Reporte con evidencia fotográfica.

Fase2. Actividades de la auditoría lógica

Actividad	Participantes	Resultado Esperado
Escanear los equipos de red usando software libre.	-Docentes investigadores -Estudiantes de la Sede Central y Regional San Miguel	- Reporte de escaneo de los equipos de red.
Verificar los controles de acceso remoto a los equipos de red.	-Docentes investigadores -Estudiantes de la Sede Central y Regional San Miguel	- Comprobar las medidas de seguridad para acceder local y remotamente a los equipos de red.
Identificar las vulnerabilidades de la red usando software libre.	-Docentes investigadores -Estudiantes de la Sede Central y Regional San Miguel	- Reporte con las vulnerabilidades detectadas con el software libre.

Nota: Todas las actividades de prueba que se desarrollaron en la red de datos fueron previamente autorizadas y monitoreadas por el personal técnico de la Gerencia de Informática.

7. RESULTADOS Y ALCANCES

En la realización del proyecto titulado “Estudio de la seguridad de la red de datos en la Escuela Especializada en Ingeniería ITCA-FEPADE” se lograron obtener los siguientes resultados:

- Inventario de dispositivos intermediarios en todas las sedes de ITCA-FEPADE.
- Recolección de evidencias fotográficas de la infraestructura física de las redes de datos de las sedes de Santa Ana, Zacatecoluca y Santa Tecla.
- Elaboración del diseño lógico de la red de datos en las regionales de ITCA-FEPADE.
- Elaboración de los formularios para evaluar el estado de la seguridad física y lógica de la red de datos.
- Implementación de herramientas de software libre para escanear los equipos de comunicación instalados en la red de datos de Santa Tecla.
- Implementación de herramientas de software libre para analizar las vulnerabilidades en los equipos de comunicación y servidores institucionales en la red de datos de Santa Tecla.
- Generación de reportes de las vulnerabilidades detectadas en los equipos de red y servidores institucionales de la red de datos de Santa Tecla, los cuales fueron entregados a la Gerencia de Informática vía correo electrónico.

8. CONCLUSIONES

- Se ha cumplido la fase de auditoria física en la Sede Central de la Escuela Especializada en Ingeniería ITCA-FEPADE y las regionales de Santa Ana y Zacatecoluca, en las cuales se evidenciaron los controles de acceso a los equipos de interconexión de redes.
- Se han identificado los equipos de interconexión de redes instalados en las redes de las regionales de Santa Ana y Zacatecoluca, los cuales han permitido elaborar los diagramas lógicos de dichas regionales.
- Se ha cumplido la fase de auditoria lógica en la Sede Central de la Escuela Especializada en Ingeniería ITCA-FEPADE, por medio del escaneo a los equipos intermediarios de la red como switches de distribución y routers.

- Las pruebas de escaneo en los dispositivos intermediarios de red de la Sede Central revelaron vulnerabilidades de seguridad que han sido calificadas en niveles de riesgo que van de medio a crítico.
- Las pruebas de escaneo a los servidores institucionales de la Sede central revelaron vulnerabilidades de seguridad que están calificadas en nivel de riesgo de medio a crítico.
- Por razones de seguridad los resultados específicos de las pruebas de vulnerabilidad se entregaron a la Gerencia de Informáticas.

9. RECOMENDACIONES

Con el fin de superar las dificultades que fueron detectadas en la red institucional se presentan las siguientes recomendaciones:

- Mejorar las condiciones de seguridad física y ambiental de los equipos de red instalados principalmente en la regional de Santa Ana, acorde a lo sugerido en las normas ISO/EIC 27002:2005.
- Mejorar los controles de acceso lógico en los equipos de red y servidores institucionales, siguiendo las recomendaciones de la norma IOS/EIC 27002:2005.
- Aplicar las soluciones que propone el software Nessus para reducir el grado de vulnerabilidad detectado en los equipos de interconexión y servidores institucionales.
- Establecer una auditoria lógica de forma periódica que permita darle seguimiento a la detección de nuevas vulnerabilidades.
- Actualizar periódicamente los diagramas de las topologías físicas y lógicas de la red.
- Implementar un servidor de monitoreo de la red con herramientas de software libre como Nessus y Nmap u otras herramientas de seguridad.
- Elaborar un manual de políticas de seguridad acorde a las necesidades de la institución.

10. GLOSARIO

- **Ancho de banda:** Capacidad de transmisión de un dispositivo o red determinado.
- **Conmutador:** dispositivo de interconexión de redes informáticas. Término equivalente en inglés: Switch.
- **Enrutador:** Dispositivo de red que conecta redes múltiples, tales como una red local e Internet.

- **Infraestructura:** Equipo de red e informático actualmente instalado.
- **IP:** (Protocolo Internet) Protocolo utilizado para enviar datos a través de una red.
- **Red:** Serie de equipos o dispositivos conectados con el fin de compartir datos, almacenamiento y la transmisión entre usuarios.
- **Servidor:** Cualquier equipo cuya función en una red sea proporcionar acceso al usuario a archivos, impresión, comunicaciones y otros servicios.
- **Topología de red:** Es la disposición física en la que se conecta una red de ordenadores.

11. REFERENCIAS BIBLIOGRÁFICAS

[1] Mitnick, Kevin D.
El arte de la Intrusión.
Editorial Ra-ma.
España, 2007

[2] Stallings, William.
Fundamentos de seguridad en redes.
Editorial Prentice Hall.
España, 2004

[3] Maiwald, Erick.
Fundamentos de seguridad de redes.
Editorial Mc Graw Hill.
España, 2004

[4] Cisco Systems Inc.
Fundamentos de seguridad de redes: Especialista en Firewall Cisco
Editorial Pearson Educación S.A.
España, 2005

[5] Cano Martinez, Jeimy L.
Computación forense: descubriendo los rastros informáticos
Editorial AlfaOmega.
México, 2008

12. ANEXOS

Anexo1

Resumen de las especificaciones técnicas de los equipos de red instalados en Santa Tecla.

Producto	Tipo	Densidad de puerto	Desempeño
Dell PowerConnect 6224F	Switch	24 Puertos GbE Fibra óptica	Capacidad de fábrica de 136 Gb/s Tasa de reenvío hasta de 95 Mpps Hasta 16.000 direcciones MAC
Dell PowerConnect 5524	Switch	24 puertos 10/100/1000BASE-T Gigabit Ethernet 2 puertos SFP+ (10Gb/1Gb)	Capacidad de fábrica de 128 Gbps Tasa de reenvío de 65.47 Mpps Hasta 16.000 direcciones MAC
Dell PowerConnect 5324	Switch	24 Puertos 10/100/1000 Base-T Gigabit Ethernet	Capacidad de fábrica de 48 Gbps Tasa de reenvío de 35.6 Mpps Hasta 8.000 direcciones MAC
Dell PowerConnect 3548	Switch	48 Puertos 10/100/1000 Base-T	Capacidad de fábrica de 17.6 Gbps Tasa de reenvío de 13.1 Mpps Hasta 8.000 direcciones MAC
Dell PowerConnect 3524	Switch	24 Puertos 10/100 Base-T	Capacidad de fábrica de 12.8 Gbps Tasa de reenvío de 9.5 Mpps Hasta 8.000 direcciones MAC
Dell PowerConnect 3448	Switch	48 Puertos 10/100 Base-T	Capacidad de fábrica de 17.6 Gbps Tasa de reenvío de 13.1 Mpps Hasta 8.000 direcciones MAC
Dell PowerConnect 3424	Switch	24 Puertos 10/100 Base-T	Capacidad de fábrica de 12.8 Gbps Tasa de reenvío de 9.5 Mpps Hasta 8.000 direcciones MAC

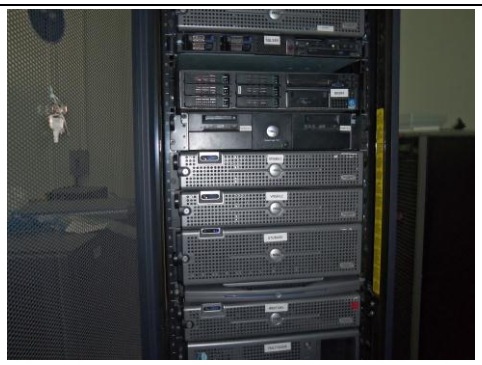
Resumen de las especificaciones técnicas de los equipos de red instalados en Zacatecoluca.

Producto	Tipo	Densidad de Puerto	Desempeño
D-LINK DES1252	Switch	48-port 10/100Mbps 4-port Gigabit cobre	17.6 Gbps
D-Link DES3028	Switch	24 Ports 10/100BASE-TX 2 Ports 10/100/1000BASE-T 2 Combo SFP Slots	12.8Gbps
3COM 3C16980A	Switch	24 Ports 10/100BASE-TX	No especificado

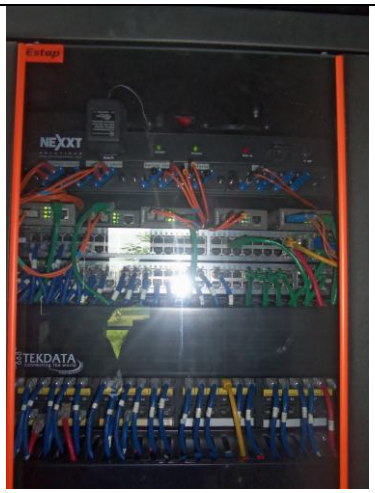
Producto	Tipo	Interfaces	Desempeño
TP-Link TLWA701ND	Access Point	1-port RJ45 10/100 auto	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n*

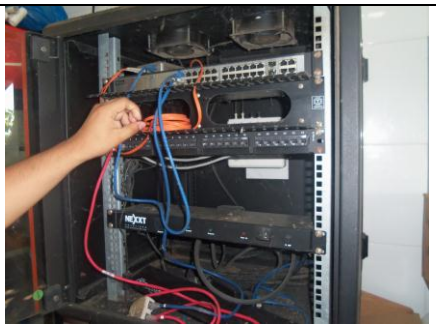
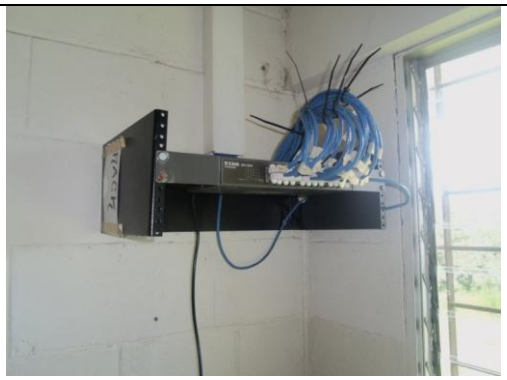
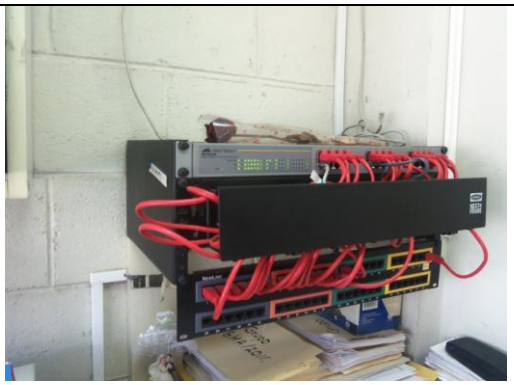
Anexo 2

Recolección de evidencias fotográficas de la infraestructura física en las sedes de Santa Tecla, Zacatecoluca y Santa Ana.

Evidencia fotográfica – Sede Central	
	
Servidores institucionales	Control de temperatura
	
Enlaces de fibra óptica	Protectores de alto voltaje

	
Cámara IP	Sistema de aire acondicionado

Evidencia fotográfica – Regional Zacatecoluca	
	
Servidor institucional	Cuarto de comunicaciones
	
Enlaces de fibra óptica	Protectores de alto voltaje

	
Cámara IP	Equipo de red
Evidencia fotográfica – Regional Santa Ana	
	
Cuarto de comunicaciones	Equipo de red
	
Equipo de red	Cableado estructurado
	
Equipo de red	Sala de docentes

Anexo 3

Las visitas técnicas realizadas a las regionales de Zacatecoluca y Santa Ana permitieron elaborar los respectivos diagramas topológicos. Por indicaciones de la Gerencia de Informática, no se incluye el diagrama topológico de la Sede Central.

Diagrama topológico de Zacatecoluca

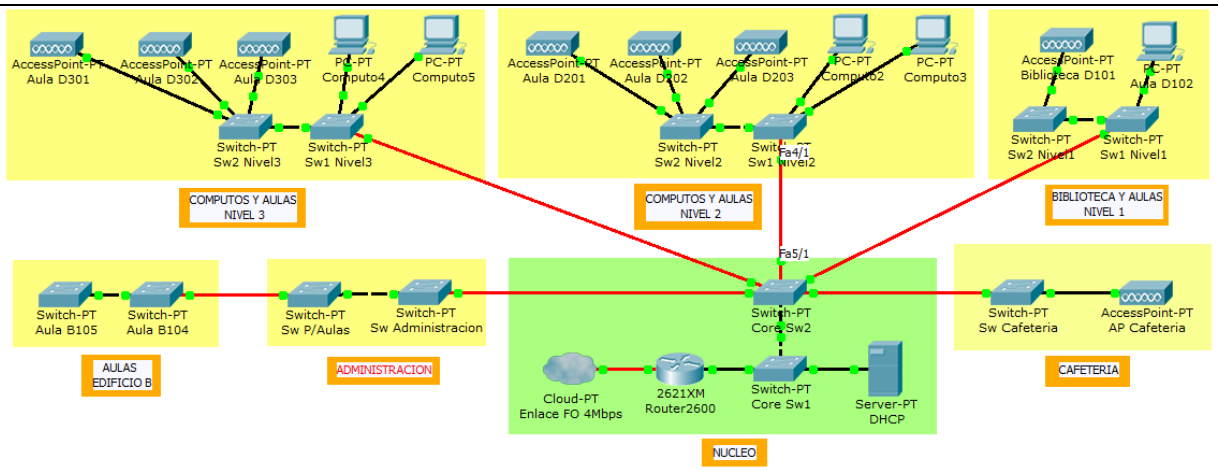
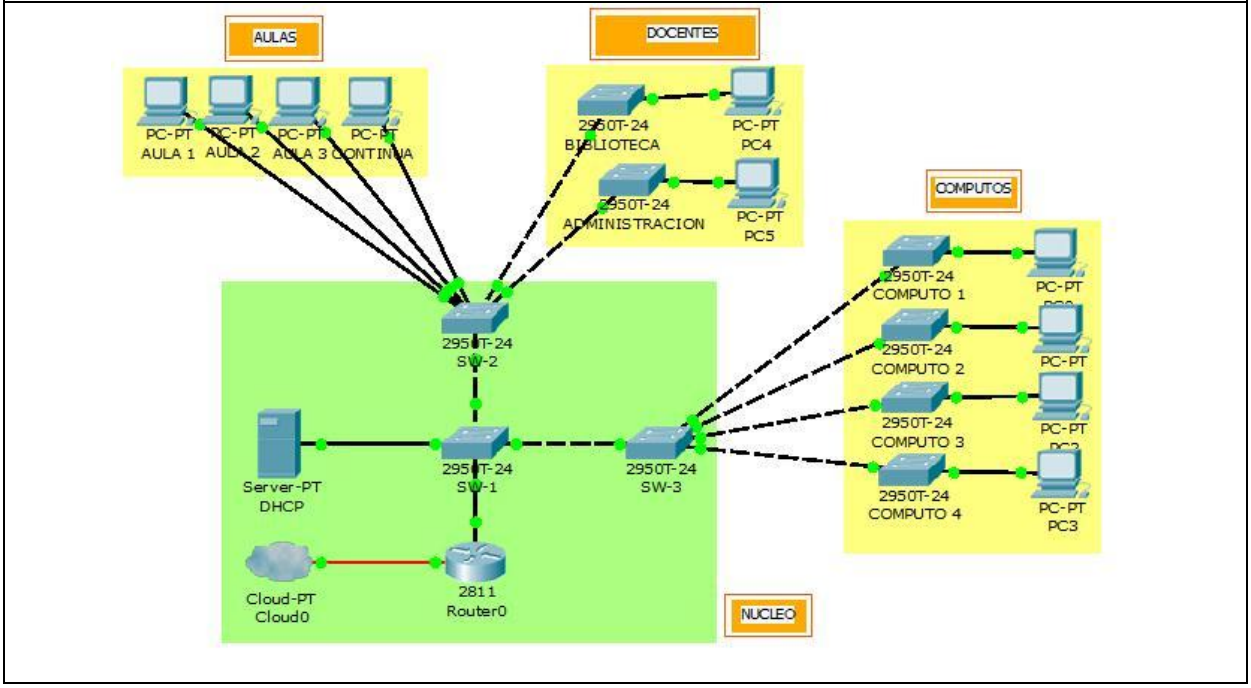


Diagrama topológico de Santa Ana



Anexo 4

Los formularios utilizados para evaluar el estado de la seguridad física y lógica de la red de datos se detallan a continuación.

INSTRUMENTO DE EVALUACIÓN 01

Objetivo:

Comprobar las medidas y procedimientos que se aplican para controlar el acceso físico a los recursos informáticos.

No.	Actividad	Evaluación		Observaciones
		Si	No	
1	El centro de datos cuenta con controles de temperatura recomendados para el alto desempeño de los equipos.	☐	☐	
2	Los equipos de comunicación en todo el campus están protegidos por un gabinete bajo llave.	☐	☐	
3	El centro de datos cuenta con cámaras de vigilancia.	☐	☐	
4	Los extintores contra incendios están ubicados cerca de los equipos de comunicación.	☐	☐	
5	El acceso al centro de datos posee cerraduras electrónicas.	☐	☐	
6	El cableado estructurado está etiquetado según estándares.	☐	☐	
7	El cableado estructurado usa canaletas transportadoras de cable a las áreas de trabajo.	☐	☐	
8	Los puntos de acceso inalámbricos están identificados en el campus.	☐	☐	
9	Equipos portátiles ajenos a la institución acceden a la red institucional mediante DHCP.	☐	☐	
10	Los equipos de conmutación bloquean respuestas de servidores DHCP ajenos a la institución.	☐	☐	
11	Los equipos de conmutación bloquean los bucles de capa 2.	☐	☐	
12	Existe un diagrama topológico de la red institucional en	☐	☐	

	cada sede.			
13	Existen enlaces redundantes en aquellas áreas que requieren alta disponibilidad.	☐	☐	
14	Los respaldos de servidores de datos se realizan periódicamente.	☐	☐	
15	La información respaldada se almacena en lugares seguros.	☐	☐	

INSTRUMENTO DE EVALUACIÓN 02

Objetivo:

Comprobar las medidas y procedimientos que se aplican para controlar el acceso lógico a los recursos informáticos.

No.	Actividad	Evaluación		Observaciones
		SI	NO	
1	El acceso remoto a servidores institucionales se encuentra inhabilitado.	☐	☐	
2	Se utilizan protocolos de seguridad para garantizar el uso de contraseñas encriptadas en los sistemas institucionales.	☐	☐	
3	Los usuarios cuentan con los derechos y privilegios de acceso mínimos para el cumplimiento de sus funciones.	☐	☐	
4	Existen políticas de seguridad de contraseñas definidas en los sistemas.	☐	☐	
5	Existe un registro histórico de los accesos exitosos y fallidos a los servidores institucionales.	☐	☐	
6	Las cuentas de usuario de ex empleados han sido dadas de baja.	☐	☐	
7	Las cuentas de usuario del sistema están claramente identificadas.	☐	☐	
8	Las cuentas de usuario que manipulan información institucional tienen un horario de acceso que bloquea la conexión a los sistemas en horas no laborales.	☐	☐	

9	Se utilizan protocolos de seguridad para el intercambio de datos confidenciales.	☐	☐	
10	El tráfico de la red interna está debidamente segmentado.	☐	☐	
11	Las áreas de acceso público pueden acceder a los servicios institucionales.	☐	☐	
12	Se han modificado los puertos por defecto para acceder a servicios específicos.	☐	☐	

INSTRUMENTO DE EVALUACIÓN 03

Objetivo:

Determinar si la institución cuenta con distintas herramientas de software para brindar una protección efectiva a los servidores y estaciones de trabajo.

No.	Descripción	Evaluación		Observaciones
		SI	NO	
1	Se ha implementado software antivirus en todos los servidores y estaciones de trabajo.	☐	☐	
2	Se realizan actualizaciones programadas o automáticas de las bases de datos del software antivirus.	☐	☐	
3	Los sistemas operativos y aplicativos cuentan con los parches de seguridad más recientes proporcionados por los fabricantes.	☐	☐	
4	Los servidores y equipos de comunicación son monitoreados a través de herramientas de detección de vulnerabilidades.	☐	☐	
5	La red institucional cuenta con sistemas de detección de intrusos.	☐	☐	
6	El tráfico interno y externo se filtra a través de dispositivos de seguridad como cortafuegos.	☐	☐	

7	Ante una eventualidad en la red se cuenta con un sistemas de alarmas por diferentes medios (correo electrónico, mensajería instantánea, etc.)	☐	☐	

Anexo 5

Los resultados de la detección de vulnerabilidades detectadas en los servidores institucionales instalados en Santa Tecla se muestran en detalle a continuación:

Nombre de la vulnerabilidad	**Descripción**	**Solución**	**Nivel de riesgo**
Apache 2.2 < 2.2.15 Multiple Vulnerabilities	La versión de apache 2.2 presenta múltiples vulnerabilidades de seguridad	Actualizar a una versión Apache 2.2.21 o superior	Critico
Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Algunos módulos de Apache pueden provocar desbordamientos de pila	Actualizar a una versión Apache 2.2.21 o superior	Critico
Samba 'AndX' Request Heap-Based Buffer Overflow	El servicio Samba es vulnerable a un desborde de pila	Aplicar parches del sitio oficial del producto	Critico
PHP Unsupported Version Detection	La versión de PHP no está soportada y puede contener vulnerabilidades de seguridad	Actualizar a una versión de PHP soportada	Critico
ISC BIND < 9.2.2 DNS Resolver Functions Remote Overflow	El servidor DNS es vulnerable a un desborde remoto que permitiría a un atacante deshabilitar el servidor	Actualizar a BIND 9.2.2	Critico
Apache HTTP Server Byte Range DoS	La versión de Apache está afectada por una vulnerabilidad de denegación de servicio	Actualizar Apache 2.2.21 o usar una de las soluciones del sitio oficial	Alto
PHP < 5.2.8 Multiple Vulnerabilities	El servidor web usa una versión de PHP afectada por múltiples vulnerabilidades o fallos	Actualizar PHP a la versión 5.2.8 o superior	Alto
Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	El servidor remoto DNS no usa puertos aleatorios cuando hace consultas a servidores de terceros. Está expuesto a ataques de DNS	Contactar a su proveedor de resolución de DNS	Alto
HTTP TRACE / TRACK Methods Allowed	El servidor web soporta los métodos TRACE y TRACK que son usados para depurar conexiones al servidor web	Deshabilitar estos métodos	Medio
SSL Certificate Cannot Be Trusted	El certificado X.509 no tiene una firma de una autoridad certificadora de confianza	Comprar o generar un certificado apropiado	Medio
Apache HTTP Server httpOnly Cookie Information Disclosure	El servidor Apache tiene una vulnerabilidad de revelación de información que puede comprometer el contenido de las cookies	Actualizar Apache 2.2.21 o superior	Medio

Nombre de la vulnerabilidad	Descripción	Solución	Nivel de riesgo
SSL Medium Strength Cipher Suites Supported	El host soporta cifrado SSL que ofrece un nivel de encriptación medio. Esto es más fácil de aprovechar por los atacantes	Reconfigurar la aplicación afectado y cambiar el nivel de cifrado	Medio
SSL / TLS Renegotiation DoS	La encriptación de trafico usando SSL/TLS renegociando conexiones permite abrir varias conexiones simultaneas llegando a la condición de denegación de servicio	Contactar al vendedor para obtener información específica de parches	Medio
TLS CRIME Vulnerability	El servicio remoto tiene una o dos configuraciones conocidas que se requieren para el ataque CRIME	Deshabilitar la compresión y el servicio SPDY	Medio
SSL Version 2 (v2) Protocol Detection	El servicio remoto acepta conexiones encriptadas SSL 2.0 el cual tiene varias fallas criptográficas y ya es obsoleto. Esto puede aprovecharse para realizar ataques de tipo MITM	Consultar la documentación de la aplicación para deshabilitar SSL 2.0 y usar SSL 3.0	Medio
mDNS Detection	El servicio remoto entiende el protocolo Bonjour que permite obtener información del host	Filtrar trafico entrante al puerto UDP 5353	Medio
SMB Signing Disabled	La firma esta deshabilitada en el servidor SMB. Esto puede permitir ataque de tipo MITM contra el servidor SMB	Reforzar la firma de mensajes en la configuración del host	Medio
SSL Certificate Expiry	El script chequea la fecha de expiración del certificado SSL	Comprar o generar un certificado apropiado	Medio
SSL Certificate with Wrong Hostname	El nombre común (CN) del certificado SSL presentado en este servicio es de una PC diferente	Comprar o generar un certificado apropiado	Medio
SSH Protocol Version 1 Session Key Retrieval	El daemon SSH soporta conexiones usando la versión 1.33 o 1.5 del protocolo SSH. Estas versiones no son criptográficamente seguras	Deshabilitar la compatibilidad con la versión 1	Medio
PHP Mail Function Header Spoofing	La función Mail() no limpia la entrada del usuario. Esto permite a los usuarios falsificar el correo.	Actualizar PHP a la versión 5.2.8 o superior	Medio
DNS Server Cache Snooping Remote Information Disclosure	El servidor remoto DNS responde a consultas de terceros que no tienen activo el bit de recursión. Esto permite a un atacante conocer los dominios que han sido resueltos	Contactar al vendedor del software DNS para repararlo	Medio

Nombre de la vulnerabilidad	Descripción	Solución	Nivel de riesgo
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	La versión del protocolo RDP es vulnerable a ataques MITM. RDP no valida la identidad del servidor cuando configura la encriptación, permitiendo incluso obtener las credenciales de autenticación	Forzar el uso de SSL o seleccionar "Permitir conexiones solo de computadoras con Escritorio Remoto usando Autenticación a Nivel de Red"	Medio
Terminal Services Encryption Level is Medium or Low	El servicio de Terminal Services no está configurado para usar encriptación fuerte. Un atacante puede obtener secuencias de teclas	Cambiar el nivel de encriptación de RDP a alto	Medio
Unencrypted Telnet Server	El servidor remoto está usando Telnet en un canal sin encriptación. Esto hace que las claves se transfieran en texto plano	Deshabilite el servicio SSH y use SSH en su lugar	Bajo

Anexo 6

Los resultados de la detección de vulnerabilidades detectadas en los equipos de red instalados en Santa Tecla se muestran en detalle a continuación:

Nombre de la Vulnerabilidad	57620 (1) - Small SSH RSA Key	
Descripción	El mando a distancia remoto del servicio SSH tiene un tamaño pequeño clave, que es inseguro. Con la tecnología actual, debe ser 768 bits como mínimo.	
Solución	Generar una clave nueva y más grande para el servicio.	
Nivel de Riesgo	Alto	N° Escaneo: 1

Nombre de la Vulnerabilidad	15901 (4) - SSL Certificate Expiry	
Descripción	Este script comprueba las fechas de caducidad de los certificados SSL asociados con los servicios habilitados en el objetivo y los informes de cualquiera que ya han expirado.	
Solución	Comprar o generar un nuevo certificado SSL para reemplazar el existente.	
Nivel de Riesgo	Medio	N° Escaneo: 2

Nombre de la Vulnerabilidad	26928 (4) - SSL Weak Cipher Suites Supported	
Descripción	El host remoto admite el uso de algoritmos de cifrado SSL que ofrecen el cifrado débil o no cifrado. Nota: Esto es considerablemente más fácil explotar si el atacante está en la misma red física.	
Solución		
Nivel de Riesgo	Medio	N° Escaneo: 3

Nombre de la Vulnerabilidad	35291 (4) - SSL Certificate Signed using Weak Hashing Algorithm	
Descripción	El servicio remoto utiliza un certificado SSL que se ha firmado con un algoritmo de hash criptográficamente débil. - MD2, MD4, MD5 o. Estos algoritmos de firma se sabe que son vulnerables a los ataques de colisión. En teoría, un atacante determinado puede ser capaz de aprovechar esta debilidad para generar otro certificado con el mismo contenido digital firma, que le podría permitir a pasar por el servicio afectado.	
Solución	Póngase en contacto con la entidad emisora de certificados para que el certificado sea reeditado.	
Nivel de Riesgo	Medio	N° Escaneo: 4

Nombre de la Vulnerabilidad	42873 (4) - SSL Medium Strength Cipher Suites Supported	
Descripción	El host remoto admita el uso de algoritmos de cifrado SSL que ofrece cifrado de tipo medio, que actualmente consideramos como aquellos con longitudes de clave por lo menos 56 bits y bits de menos de 112. Nota: Esto es considerablemente más fácil explotar si el atacante está en la misma red física	
Solución	Vuelva a configurar la aplicación afectada, si es posible evitar el uso de sistemas de cifrado de fuerza media.	
Nivel de Riesgo	Medio	N° Escaneo: 5

Nombre de la Vulnerabilidad	51192 (4) - SSL Certificate Cannot Be Trusted
Descripción	El certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Esta situación puede ocurrir de tres maneras diferentes, cada una de las cuales da lugar a una ruptura en la cadena de certificados por debajo del cual no se puede confiar.

Solución	Adquirir o generar un certificado apropiado para este servicio.	
Nivel de Riesgo	Medio	N° Escaneo: 6

Nombre de la Vulnerabilidad	57582 (4) - SSL Self-Signed Certificate	
Descripción	La cadena de certificados X.509 para este servicio no está firmado por una autoridad certificadora reconocida. Si el host remoto es un host público en la producción, esto anula el uso de SSL como cualquiera podría establecer un hombre en medio del ataque contra el host remoto.	
Solución	Adquirir o generar un certificado apropiado para este servicio.	
Nivel de Riesgo	Medio	N° Escaneo: 7

Nombre de la Vulnerabilidad	60108 (4) - SSL Certificate Chain Contains Weak RSA Keys	
Descripción	Al menos uno de los certificados X.509 enviados por el host remoto tiene una clave que es más corto que 1024 bits. Estas claves son consideradas débiles debido a los avances en la potencia de cálculo disponible, disminuyendo el tiempo necesario para factorizar llaves criptográficas. Algunas implementaciones de SSL, en particular de Microsoft, puede considerar esta cadena SSL no válido debido a la longitud de uno o más de las claves RSA que contiene.	
Solución	Vuelva a colocar el certificado de la cadena con la clave RSA débil con una llave más fuerte, y vuelva a emitir los certificados que firmó.	
Nivel de Riesgo	Medio	N° Escaneo:8

Nombre de la Vulnerabilidad	20007 (2) - SSL Version 2 (v2) Protocol Detection	
Descripción	El servicio remoto acepte conexiones cifradas con SSL 2.0, que al parecer sufre de mostrar distintas fallas y ya no se utiliza desde hace varios años. Un atacante podría explotar estas cuestiones para llevar a cabo ataques o descifrar las comunicaciones entre el servicio afectado y los clientes.	
Solución	Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y Usar SSL 3.0, TLS 1.0, o en su lugar un cifrado más alto.	
Nivel de Riesgo	Medio	N° Escaneo:9

Anexo 7

Las herramientas de software libre utilizadas en el proyecto para escanear los equipos de red y detectar las vulnerabilidades de seguridad se describen a continuación:

NMAP

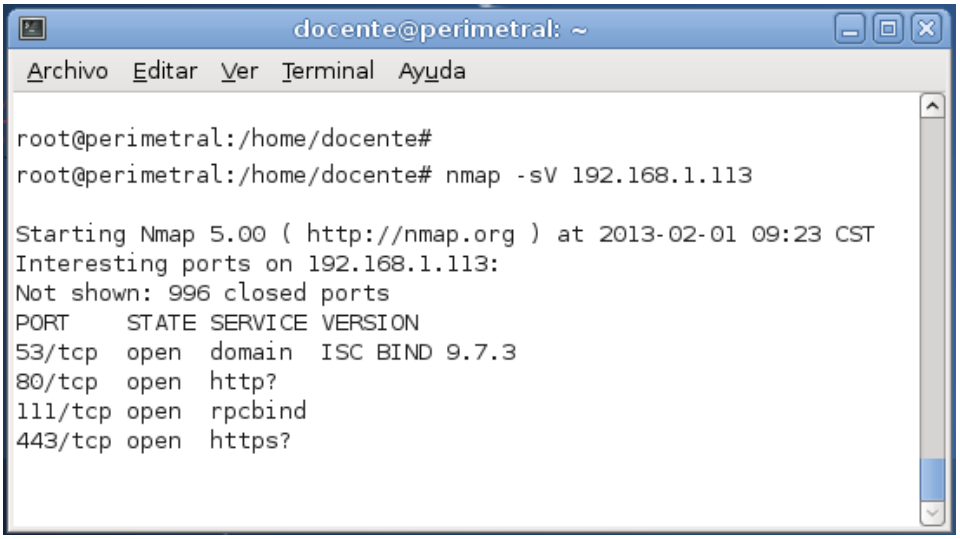
El escaneo de puertos es una técnica que emplean los administradores de red para auditar computadoras y redes con el fin de obtener información del estado de los puertos, los servicios que ofrece, verificar la existencia de un firewall, entre otras cosas.

Nmap es un programa que sirve para efectuar rastreo de puertos y se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

Nmap es bien conocido por sus imprescindibles funciones de seguridad y administración de servidores, como por ejemplo:

- Descubrimiento de equipos instalados en la red.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios se están ejecutando en la computadora objetivo.
- Determinar qué sistema operativo y versión utiliza dicha computadora.
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

La captura de pantalla que se muestra a continuación es un ejemplo del escaneo de puertos en un servidor de pruebas:



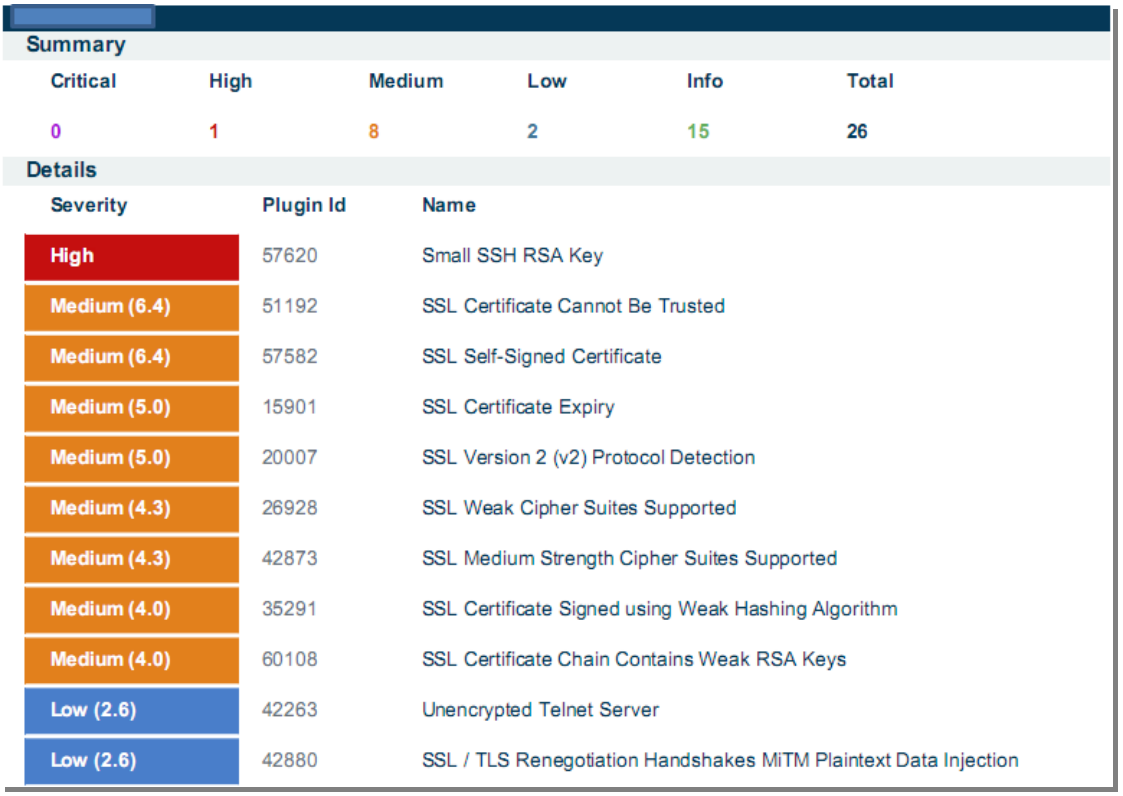
Nessus

Nessus es un analizador de seguridad de red desarrollado por Tenable Network Security. Actualmente se encuentra entre los productos más importantes de este tipo en todo el sector de la seguridad y cuenta con el respaldo de organizaciones profesionales de seguridad de la información, tales como SANS Institute. Nessus le permite realizar auditorías de forma remota en una red en particular y determinar si alguien accedió de manera ilegal a ella o la usó de alguna forma inadecuada. Nessus también proporciona la capacidad de auditar de forma local un equipo específico para analizar vulnerabilidades, especificaciones de compatibilidad, violaciones de directivas de contenido y más. Entre las características más importantes del producto están:

- **Análisis inteligente:** a diferencia de muchos otros analizadores de seguridad, Nessus no da nada por hecho. Es decir, no supondrá que un servicio dado se ejecuta en un puerto fijo. Esto significa que si usted ejecuta su servidor web en el puerto 1234, Nessus lo detectará y probará su seguridad según corresponda. Cuando sea posible, intentará validar una vulnerabilidad a través de su explotación. En los casos en los que no sea confiable o se pueda afectar de manera negativa el destino, Nessus puede basarse en un banner del servidor para determinar la presencia de la vulnerabilidad. En tales casos, quedará registrado en el informe resultante si se usó este método.
- **Arquitectura modular:** la arquitectura cliente/servidor proporciona la flexibilidad necesaria para implementar el analizador (servidor) y conectarse con la GUI (cliente) desde cualquier equipo mediante un explorador web, con lo cual se reducen los costos de administración (varios clientes pueden acceder a un único servidor).
- **Arquitectura de plugins:** cada prueba de seguridad está diseñada como plugin externo, y se agrupan en una de 42 familias. De esta forma, usted puede añadir fácilmente sus propias pruebas, seleccionar plugins específicos o elegir una familia entera sin tener que leer el código del motor de servidores Nessus, nessusd. La lista completa de los plugins de Nessus se encuentra disponible en http://www.nessus.org/plugins/index.php?view=all.
- **Base de datos actualizada de vulnerabilidades de seguridad:** Tenable se centra en el desarrollo de comprobaciones de seguridad correspondientes a vulnerabilidades recientemente divulgadas. Nuestra base de datos de comprobaciones de seguridad se actualiza diariamente, y todas las comprobaciones de seguridad más recientes se encuentran disponibles en http://www.nessus.org/scripts.php.

- **Cooperación de plugins:** las pruebas de seguridad realizadas por los plugins de Nessus cooperan de manera tal que no se lleven a cabo comprobaciones innecesarias. Si su servidor FTP no ofrece inicios de sesión anónimos, no se realizarán comprobaciones de seguridad relacionadas con estos.

En la siguiente captura de pantalla se muestra el resumen de vulnerabilidades detectadas en un servidor de pruebas:



Summary

Critical	High	Medium	Low	Info	Total
0	1	8	2	15	26

Details

Severity	Plugin Id	Name
High	57620	Small SSH RSA Key
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 (v2) Protocol Detection
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.0)	35291	SSL Certificate Signed using Weak Hashing Algorithm
Medium (4.0)	60108	SSL Certificate Chain Contains Weak RSA Keys
Low (2.6)	42263	Unencrypted Telnet Server
Low (2.6)	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

www.itca.edu.sv

Sede Central Santa Tecla
Km. 11 Carretera a Santa Tecla.
Tel. (503) 2132-7400
Fax. (503) 2132-7599

MEGATEC La Unión
C. Santa María, Col. Belén, atrás del
Instituto Nacional de La Unión.
Tel. (503) 2668-4700

MEGATEC Zacatecoluca
Km. 64 1/2, desvío Hacienda El Nilo,
sobre autopista a Zacatecoluca y
Usulután. Tel. (503) 2334-0763, (503)
2334-0768 Fax. (503) 2334-0462

Centro Regional San Miguel
Km. 140, Carretera a Santa Rosa de Lima.
Tel. (503) 2669-2292, (503) 2669-2299
Fax. (503) 2669-0961

Centro Regional Santa Ana
Final 10a. Av. Sur, Finca Procavia
Tel. (503) 2440-4348, (503) 2440-2007
Tel. Fax. (503) 2440-3183