UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2018 – MARZO 2019

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

Estudio de Medidas y Protocolos de Seguridad en las Redes Informáticas del UPC (Unidad de Policía Comunitaria) de la Parroquia Barreiro

EGRESADA:

María Eugenia Cotto Soliz

TUTORA:

Ing. Gladys Patricia Guevara Albán, Msc.

AÑO 2019

INTRODUCCIÓN

El principal activo de gran importancia para las organizaciones en los actuales momentos es la información que estas poseen. La tendencia actual, obliga a las organizaciones a manejar su información por medio de las Tecnologías de la Información y Comunicación, por lo que su mayor interés es mantenerla a salvo.

La seguridad de la información implica crear medidas de seguridad en la infraestructura física de la red e implementar protocolos para gestionar la transmisión de los datos en la misma. Es por ello que es de vital importancia que las organizaciones implementen políticas de seguridad tanto para mantener a salvo sus equipos y sobre todo la información garantizando la integridad, confiabilidad y disponibilidad de la misma.

Las Unidades de Policía Comunitaria cuentan con una red que les permite gestionar la información tanto local, como en la nube. El papel fundamental de los UPC, es brindar a la policía nacional herramientas para garantizar la seguridad ciudadana, lo que significa que la información que se gestiona en estos lugares es muy importante.

Gracias a estos criterios anteriormente detallados, se pretende realizar un estudio sobre qué medidas y protocolos de seguridad se utilizan en las redes informáticas del UPC de la parroquia Barreiro, Cantón Babahoyo, Provincia de los Ríos, donde se pretende identificada si su infraestructura de red cumplen con ciertos estándares que podrían ayudar a garantizar la seguridad de sus redes. La Unidad de Policía Comunitaria realiza un papel de gran importancia en nuestra comunidad ya que ellos son los llamados a dar seguridad y protección a los habitantes de dicha parroquia y por ende manejan gran cantidad de datos e información confidencial la cual debe ser protegida mediante las correctas medidas de seguridad y usando los correspondientes protocolos.

El presente estudio por medio de una investigación de campo, y mediante entrevistas pretende medir cualitativamente las medidas y protocolos de seguridad que utilizan en el UPC, si estos están debidamente implementados, identificar si existen problemas y si es posible darle solución a estos.

La línea de investigación del presente estudio es específicamente en la línea de Desarrollo de Sistemas de la Información, Comunicación y emprendimientos empresariales y Tecnológicos, sublínea Proceso de Transmisión de Datos y Telecomunicaciones, ya que el objetivo principal del proyecto es identificar las medidas y protocolos de seguridad para la gestión de la información en el UPC de Barreiro.

DESARROLLO

La seguridad informática es la teoría y la práctica de solo permitir el acceso a la información a las personas en una organización que están autorizadas para verla. Si bien esto incluye la información que se encuentra almacenada en las computadoras, el concepto es mucho más amplio, que abarca todos los registros bajo el control. (Study Academy, 2017)

En la actualidad seguridad de la información es de vital importancia, puesto que las organizaciones utilizan en casi todas sus actividades equipos informáticos. El uso de las TICS, conlleva a tener el riesgo de que la trasmisión de los datos sea vulnerada, siendo la seguridad de la información uno de los temas con mayor preocupación en dicha área.

Si bien es cierto, en los últimos 50 años se ha ido implementado sistemáticamente el uso de las tecnologías de la información en las logísticas policiales. Los sistemas de información policial, que antes se basaban en el cotejo de fichas a cargo de un archivero, han evolucionado con el uso de las tecnologías de la información hasta convertirse en departamentos que utilizan programas informáticos especiales para garantizar la seguridad ciudadana, con la instalación de sistemas de cámaras, alertas.

La información que se maneja en la policía nacional, debe mantenerse segura para que esta no pueda ser alterada o robada, por terceros ajenos a la institución. Es por eso que la red donde se maneja este tipo de información debe estar acorde con los estándares calidad establecidos en la actualidad para salvaguardar los sistemas de información.

Las Unidades de Policía Comunitaria (UPC), son pequeños distritos de la policía para que esta participe activamente con la comunidad, y brindar seguridad a los ciudadanos de un determinado sector. El UPC de la Parroquia Barreiro, del Cantón Babahoyo, en sus inicios

contaba con instalaciones estructuradas tecnológicamente de acuerdo a los estándares establecidos en cuanto a seguridad se refiere, pero al paso del tiempo se han ido deteriorando ciertas estructuras donde se encuentra el cableado de red.

El presente estudio de caso usa como metodología la investigación cualitativa, porque se pretende analizar qué tipos de medidas y protocolos de seguridad se usan en el UPC de Barreiro, usando como herramienta la entrevista, el cuestionario como instrumento y la observación como técnica, donde se desea obtener información más detallada acerca de la red del lugar.

Además, también se utilizó una metodología para realizar la detención de vulnerabilidades en la red del UPC de Barreiro usando como herramienta Nessus Escáner. Esta metodología fue creada por profesionales cubanos (Iviricu Roba, Alvarez Vento, & Concepción García, 2016) los cuales tomaron como referencia a la metodología OSSTMM (The Open Source Security Testing Methodology Manual), pero adaptada a las condiciones de la organización, y las herramientas que se usaran.

El Manual de Metodología Pruebas de seguridad de código abierto (OSSTMM) es un sistema revisado por pares que describe las pruebas de seguridad. OSSTMM proporciona una metodología científica para evaluar la seguridad operacional basada en métricas analíticas Esta es una metodología para probar la seguridad operativa de las ubicaciones físicas, las interacciones humanas y todas las formas de comunicación. (Conklin & Shoemaker, 2013).

Esta metodología consta de tres etapas: Valoración, ejecución e informe, donde se detallan cada una de estas acciones en el orden respectivo que se llevaron a cabo, con el objetivo de mejorar el ambiente de seguridad del UPC de Barreiro y además lograr un resultado eficiente

que muestre las vulnerabilidades existentes estableciendo su prioridad para eliminarlas o mitigar su impactos ante incidentes de seguridad.

En la etapa de valoración se procedió en conocer las actividades de la organización, los recursos humanos y la arquitectura tecnología que tiene la organización para realizar el proceso de comunicación y procesamiento de la información. Para ello se realizó una visita al UPC de la Parroquia Barreiro, mediante una entrevista y la observación se pudo reconocer todos estos aspectos.

En la etapa de ejecución, se inició un proceso de escaneo de la red usando la herramienta Nessus, donde se encontraron vulnerabilidades las cuales ayudarán a detectar potenciales riesgos que pueden afectar la seguridad de la red del UPC de la parroquia Barreiro. El escaneo se realizó dentro de la institución desde un punto de red.

En la etapa del informe se da como resultado reporte de las amenazas y vulnerabilidades presentes después de realizar el escaneo de red con el objetivo de tomar los controles informáticos pertinentes y decidir las medidas que se deben tomar para eliminarlas o corregirlas con el propósito de optimizar la seguridad de la red.

Los problemas existentes en el UPC de la parroquia Barreiro son el poco cumplimiento de las medidas establecidas para garantizar la seguridad física y lógica de la red, así como el uso de protocolos de red desactualizados, pese a que existen otras versiones que brindan mayor seguridad al tráfico de datos; y el descuido físico de las instalaciones donde se encuentra la red.

Según el resultado obtenidos en la entrevista (ANEXO I), se pudo constatar que existen medidas de seguridad para salvaguardar tanto los equipos y la información, pero no se están cumpliendo correctamente su función, debido a que los inconvenientes que se presentan en la

seguridad no son conocidos por todo el personal de la policía nacional en el UPC ya que sus turnos son rotativos, y policías con poco conocimiento de seguridad informática hacen uso de los equipos y los servicios que ofrece la red y por ello no tienen el debido conocimiento para protegerse de las amenazas existentes. Es de mucha importancia que se apliquen medidas, para no desestabilizar la seguridad de la red y sus procesos.

Pese a que existe un manual (ANEXO IV), que explica como salvaguardar la red y que medidas de seguridad se deben tomar en cuenta para proteger la integridad de la transmisión de los datos de los diferentes servicios que se manejan en el lugar. Esto puede provocar riesgos que podrían dañar la seguridad de la red en un futuro.

En el manual, otorgado por el Ministerio del Interior a cada UPC, se expresan diferentes medidas y normas de seguridad para que el sistema de información usado trabaje perfectamente, que no sufra ningún daño y en caso de que algún equipo notificar al organismo competente para brindar solución inmediata.

Durante la observación (ANEXO III) se pudo notar que parte del tumbado (ANEXO V) se encuentran deteriorados, los cables, estos están expuestos a simple vista, pudiendo ocasionar ruido en la trasmisión de los datos y también puede albergar la presencia de roedores que pueden dañar los cables y ocasionar la desconexión de la red, lo cual sería un gran problema para los que trabajan en el lugar y al mismo tiempo afectaría también a los moradores.

Para comprobar el estado lógico de la red, se procedió a realizar un escaneo usando una herramienta de software denominada Nessus. Este escaneo permitió comprobar si existen amenazas y vulnerabilidades en la transmisión de datos de los diferentes equipos informáticos que se encuentran en la institución, para gestionar riesgos que atenten en contra se la seguridad de la información que se gestiona en el UPC.

Una vulnerabilidad de seguridad es una debilidad en un producto que podría permitir a un atacante comprometer la integridad, disponibilidad o confidencialidad de ese producto. Por ejemplo si un usuario sin privilegios pudiera acceder a la computadora de forma remota y cambiar el permiso de los archivos, instalar software, eliminar archivos, etc., eso constituiría una vulnerabilidad de seguridad. (Kremling & Parker, 2017)

Las vulnerabilidades pueden poner en riesgo los sistemas informáticos de las personas y a los equipos informáticos, por lo que estas deben solucionarse para que los atacantes no puedan infiltrarse en el sistema y causar daños como: adulteración, eliminación o robo de información. Las vulnerabilidades existentes en una red pueden ser una amenaza para integridad y confiabilidad de los procesos informáticos que se realicen en la institución.

Una amenaza, en el ámbito de seguridad informática, se refiere a cualquier cosa que pueda causar un daño grave a un sistema de información. Una amenaza es algo que puede o no puede ocurrir, pero tiene el potencial de causar daños graves. En efecto, una amenaza puede ocurrir a consecuencia de una vulnerabilidad si no se tratan a tiempo. (Techopedia Inc., 2019)

Las amenazas pueden incluir desde virus, troyanos, puertas traseras hasta ataques directos de piratas informáticos. Actualmente los criminales cibernéticos utilizan muchos métodos diferentes para obtener la información confidencial a las personas o instituciones, para usarlas con fines ilícitos.

Nessus es uno de los escáneres de vulnerabilidades más utilizados, que puede detectar las vulnerabilidades que permite a un hacker remoto controlar o dar acceso a datos del sistema, además de que también detecta fallas en la configuración, falla en los passwords, ataques de diccionario, negación de servicio contra TCP/IP que se han utilizado con más frecuencia e incluso puede preparar al sistema para auditoria sobre la seguridad (Urbina, 2016)

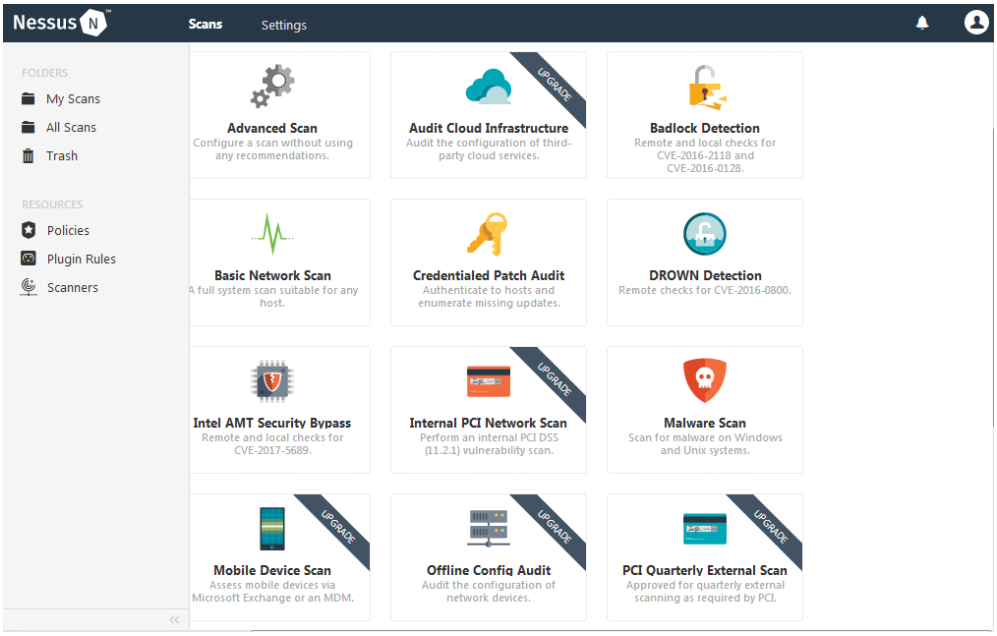


Fig. 1 Pantalla Inicial de Nessus

Autora María Cotto

Un escáner de vulnerabilidades intentará proporcionar el endurecimiento necesario en una red. Nessus es un escáner de vulnerabilidades que puede usarse contra una variedad de sistemas, incluidos servidores web, se puede usar para ejecutar un escaneo de vulnerabilidades en toda su subred o puede dirigirse a una sola máquina. (Walker, 2016)

El resultado del escaneo (ANEXO VI), muestra un reporte general de las vulnerabilidades presentes en la red del UPC de Barreiro, entre las cuales tenemos una de prioridad alta y otra de prioridad media. Existen 26 resultados de datos informativos accesibles de la red que no presentan riesgos en la transmisión de datos.

Dentro del informe detallado (ANEXO VII), se muestra información de las dos potenciales vulnerabilidades encontradas en el escaneo de la red. En este informe se muestra detallada la descripción de cada vulnerabilidad y la solución recomendada por el Nessus. Cabe mencionar que estas vulnerabilidades no son de prioridad crítica, pero de todas formas debe tomar las medidas pertinentes.

La vulnerabilidad de prioridad alta describe que: *la red compartida de Windows tiene acceso libre no privilegiado*. La descripción de la vulnerabilidad dice que se están compartiendo uno o más recursos que pueden ser accedidos; y dependiendo de los derechos compartidos, puede permitir que un atacante lea y/o escriba datos confidenciales. Como solución el Nessus plantea que se restringa el acceso desde el explorador de Windows, en opciones de recursos compartidos.

La vulnerabilidad de prioridad media indico que: "*La firma no es necesaria en el servidor remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques de intermediario contra el servido*r". Como recomendación se propone imponer la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de la política 'Servidor de red de Microsoft: firmar comunicaciones digitalmente'.

Se recomienda realizar los cambios oportunos, para que no se presenten los inconvenientes que podrían suceder si no se los hace de forma prudente. Es por eso que un escaneo de red de forma periódica para encontrar vulnerabilidades nos ayuda a prevenir riesgos.

Por otro lado, si bien es cierto existe un servidor proxy que gestiona el tráfico de red por medio de los protocolo de seguridad SOCKS4, permitiendo que los usuarios sólo usen los servicios de la red según las políticas establecidas por la policía nacional. Esta medida usada es muy útil para garantizar la calidad del servicio que se desea brindar. (Hontañón, 2016)

Un servidor proxy es responsable de aceptar solicitudes HTTP de un usuario. Los servidores proxy, proporcionan una forma de seguridad mucho más estricta que los filtros de paquetes, pero están diseñados para regular el acceso solo para una aplicación en particular a

través de protocolos. El protocolo SOCKS el cual está diseñado para enrutar paquetes entre aplicaciones cliente-servidor a través de un servidor proxy. (Kapadia, Rajana, & Varma, 2015)

Esto quiere decir, que un servidor proxy funciona como el intermediario entre el cliente y el servidor para un servicio en particular. El filtrado de paquetes se usa para denegar toda comunicación directa entre los clientes y servidores para ese servicio; todo el tráfico va al servidor proxy en su lugar.

Existen dos versiones del protocolo SOCKS están actualmente en uso, SOCKS4 y SOCKS5. Los dos protocolos no son compatibles, pero la mayoría de los servidores SCCKS5 detectarán los intentos de usar SCCKS4 y los manejarán adecuadamente. SOCKS5 brinda soporte para varias formas diferentes de autenticar usuarios, lo que le brinda un control y registro más precisos. (Zwicky, Cooper, & Chapman, 2014)

SOCKS4 no hace autenticación de usuario real. Basa sus decisiones en si permitir o denegar conexiones en el mismo tipo de información que utilizan los filtros de paquetes (puertos de origen y destino y direcciones IP), lo que hace que sea vulnerado fácilmente usando herramientas de cifrado que ocultan la dirección IP origen.

Socket Secure 5 (SOCKS5) es un protocolo de Internet para intercambiar datos de red entre un cliente y un servidor a través de un servidor proxy. El servidor proxy crea una conexión TCP en nombre del servidor cliente. La ventaja del proxy SOCKS5 es que le permite entregar datos a la nube sin una conexión VPN. Este protocolo proporciona autenticación adicional, que permite que solo los usuarios autorizados puedan acceder al servidor. Este protocolo hace que los paquetes enviados entre un cliente y un servidor se enruten con mayor facilidad a través de un servidor proxy.

Esto quiere decir que un proxy configurado en el UPC de Barreiro con SOCKS4, puede ser vulnerado muy fácilmente usando software de terceros (como UltraSurf) navegar en internet de forma anónima para acceder a para acceder a sitios web bloqueados por medio del servidor proxy. Esto puede ocasionar que se dañe la integridad de la información.

Por eso, como sugerencia ante este problema se expresa actualizar en el sistema informático UPC de Barreiro el protocolo SOCKS4 al protocolo SOCKS5, porque este tienes incorporado un poderoso sistema de autenticación, mientras que la versión 4 sólo ofrece un sistema de firewall inseguro basado en aplicaciones clientes servidor.

UltraSurf es un producto gratuito de evasión de censura de Internet creado por UltraReach Internet Corporation. El software pasa por alto la censura de Internet y los cortafuegos mediante un servidor proxy HTTP y emplea protocolos de cifrado para la privacidad. (ltraReach Internet Corp, 2018)

Pero según lo declarado, durante la entrevista como medida se tiene prohibido el uso de este tipo de software, pero nada garantiza que se cumpla esta medida. Sobre todo con el tema de la red inalámbrica, la cual no debería existir en el UPC, pero de todas formas está presente. UltraSurf es conocido también por divulgar información privada.

Esta conexión inalámbrica, tiene el mismo servicio de proxy ya que se encuentra conectada en el mismo segmento. El objetivo de una red inalámbrica es compartir internet principalmente a dispositivos móviles. Si las redes sociales están bloqueadas el usuario de la red inalámbrica usará aplicaciones para evadir el proxy local (existe una versión de UltraSurf para Android), lo cual conlleva riesgos en la seguridad.

Como sugerencia se propone que se dicten capacitación sobre las medidas que se deben tener para no poner en riesgo la información, también se recomienda que se gestione visitas de técnicos especializados en seguridad de redes para así asegurar que los servicios ofrecidos sean de calidad y además que garanticen los objetivos de los sistemas de gestión de seguridad de la información, que son la confiablidad, integridad y disponibilidad de la misma.

Según, (Pérez, 2016), se llama confiabilidad a uno de los primeros principios básicos de la seguridad de la información. Esto simplemente significa que la información no está disponible para las personas que no están autorizadas para verla. La información es el activo más importante de la empresa por lo tanto no debe ser alterada.

La confiabilidad, en términos técnicos es una métrica de la continuidad de un servicio. Esta garantiza con seguridad que el sistema no tendrá un efecto catastrófico en sus usuarios y el su entorno. Toda la información que se procesa en un sistema de información que certifique la confiabilidad de la misma, será de calidad y garantizará seguridad al sistema.

Por otro lado integridad en el contexto de la seguridad de la información significa que las personas pueden confiar en que la información de una organización no ha sido manipulada de alguna manera, para ello se deben aplicar medidas de seguridad como capacitación al personal, mecanismos y herramientas informáticas para que no suceda. (TecNoincer, 2017)

La definición de integridad de la información expuesta quiere decir que significa que los servicios proporcionados por el sistema son lo que los usuarios esperan y nadie puede corromper la información sin ser detectado, ya se deben implementar los mecanismos pertinentes para cumplir con este principio. (Marian, 2017)

Y por último, disponibilidad significa que las personas que están autorizadas para ver datos pueden hacerlo cuando necesitan acceso. Dado que tanta información está contenida en los sistemas informáticos, esto significa que los departamentos de TI deben asegurarse de que sus sistemas sean lo más confiables posible.

A pesar de que en la actualidad, todas las organizaciones almacenan datos en las computadoras, la seguridad de la información no los trata estrictamente. La seguridad de la información es ante todo un fenómeno de gestión. La buena seguridad de la información comienza desde arriba y se refleja en una buena política de TI. Las organizaciones no pueden esperar simplemente confiar en el departamento de TI para mantener la seguridad. Es realmente el deber de todos garantizar que la información, tanto pública como confidencial, se mantenga segura y confiable.

La seguridad de la información efectiva significa decidir quién debe tener acceso a qué información. Una de las mejores prácticas es el principio de privilegio mínimo. Esto significa que las personas solo deben tener acceso a la información que necesitan para hacer su trabajo y no más.

También se sugiere implementar controles (ANEXO IX) establecidos en la NORMA ISO/27002, la cual proporciona un conjunto de mejoras que se pueden utilizar para la seguridad de una red informática, es decir contiene buenas prácticas para garantizar la confiabilidad, integridad y disponibilidad de la información.

Según, Edward Humphreys, define a la ISO/27002 como principalmente un catálogo de controles de mejores prácticas, que los usuarios pueden seleccionar para implementar controles de administración de seguridad en su entorno empresarial para lograr una línea de base de protección de mejores prácticas. (Humphreys, 2016)

La ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y los indicadores recomendables en cuanto a seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Aunque no es certificable, su uso puede lograr grandes resultados para garantizar la seguridad de la información del UPC de Barreiro.

Uno de los objetivos de la ISO/27002, es el establecimiento de políticas de seguridad en la organización. El contenido de las políticas se basa en el contexto, la operación, la organización y la escritura para cumplir los objetivos. En este contexto el UPC, debe implementar políticas claras para garantizar la seguridad de la información.

La seguridad física también es otro objetivo de la norma ISO/27002, donde se establece que el establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección para las instalaciones de procesamiento de información crítica o sensible de la organización, contra el acceso físico no autorizado. (ISO27000 Español, 2015)

Esta norma también, también tiene como objetivo establecer métricas para el control de accesos. Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información.

La implementación de buenas prácticas para la correcta gestión de los recursos informáticos de un sistema de información, conlleva a garantizar que la información viaje segura desde su origen hacia su destino. Entre los controles de la Norma ISO/27002 se han escogido los más óptimos según el modelo de gestión y los problemas encontrados en el UPC de Barreiro. Entre los cuales se han escogido describiendo el objetivo que se desea cumplir:

Objetivo de control de acceso a terceros se debe:

- Identificación de los riesgos derivados del acceso de terceros.

- En el objetivo de la responsabilidad de activos
- Uso aceptable de activos

Objetivo ligado con los recursos humanos durante el empleo

- Responsabilidades de la Dirección.
- Concienciación, formación y capacitación en seguridad de la información.
- Proceso disciplinario.

Objetivo de la seguridad de los equipos

- Emplazamiento y protección de equipos.
- Seguridad del cableado.
- Mantenimiento de los equipos.
- Seguridad de los equipos fuera de las instalaciones
- Reutilización o retirada segura de equipos.
- Retirada de materiales propiedad de la empresa.

Objetivo de Control de acceso a las aplicaciones y a la información.

- Restricción del acceso a la información.
- Aislamiento de sistemas sensibles.

Objetivo de Control de acceso al sistema operativo.

- Procedimientos seguros de inicio de sesión.
- Identificación y autenticación de usuario.
- Sistema de gestión de contraseñas.
- Uso de los recursos del sistema.
- Desconexión automática de sesión.
- Limitación del tiempo de conexión.

Objetivo uso de ordenadores portátiles.

- Ordenadores portátiles y comunicaciones móviles.

Objetivo de notificación de eventos y puntos débiles de seguridad de la información.

- Notificación de los eventos de seguridad de la información.
- Notificación de puntos débiles de seguridad.

Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

- Cumplimiento de las políticas y normas de seguridad.
- Comprobación del cumplimiento técnico.

Para fortalecer caso de estudio se consultó con un experto en el tema de medidas y protocolos de seguridad de redes, el cual me supo contestar que la información que se administra en el UPC es bastante delicada, en consecuencia de esto los equipos deben estar correctamente configurados donde se apliquen todas las correcciones posibles de seguridad, y que además los equipos deben ser administrados por personal capacitado para gestionar información de ese tipo y debe ser responsable con las credenciales de acceso al sistema.

Si bien es cierto, los equipos que se encuentran en el UPC, fueron configurados por personal capacitado provenientes de la ciudad de Quito, lo cual corresponde un punto a favor a la seguridad para el UPC de Barreiro, pero según los resultados obtenido con la entrevista del cabo Tuaza y la del ingeniero Saltos se puede decir que existe un problema en cuanto a la capacitación del personal se refiere, ya que aunque el sistema de información este correctamente configurado, si el personal no está correctamente capacitado para administrarlo, puede ser un peligro en contra de la seguridad de la red del UPC de Barreiro.

Con el tema de las redes inalámbricas, el ingeniero Harry Saltos, da como recomendación que estas deben tener de niveles de seguridad para que la información que se manipula en el

lugar sea segura. Por ningún motivo este tipo de redes debe ser motivo de distracción y su uso no debe ser ajeno a los temas que tengan que ver con la seguridad de las personas. Por el ingeniero recomienda que estas redes también deben tener restricciones para que los dispositivos que se conecten gestionen sólo información relacionada con la institución.

En análisis de lo expuesto por el ingeniero, con respecto a las redes inalámbricas, tiene razón su criterio, ya que las redes inalámbricas tienen muchas brechas de seguridad, por lo que se recomienda que estén debidamente aseguradas, y además que su uso en este tipos de instituciones como es el UPC de Barreiro, su uso debe ser estrictamente para cumplir los objetivos de la institución y no para otro uso ajeno a estos objetivos.

Con respecto a las computadoras, el ingeniero recomienda como medida de seguridad que estén configuradas con políticas de seguridad específicas del sistema operativo, que sólo permitan la ejecución de software que sólo sean de uso concreto para procesar información del UPC, ya que el uso de programas no autorizados podrían crear agujeros de seguridad en la red. Esta medida se debe implementar para que los servidores de uso policial a nivel nacional sólo procesen la información que se gestionan en los UPC, para que esta no pueda ser vulnerada.

Otro punto a tomar en cuenta, para el UPC de Barreiro, según lo expuesto por el ingeniero Saltos, en cuanto al uso de las computadoras, se demuestra que el uso de software el cual no pertenezca para las gestiones que se realizan en la institución, ya que pude crear problemas en la seguridad de la información que se administra en este lugar.

Con respecto a los protocolos de seguridad el ingeniero manifiesta, que al tratarse de una entidad gubernamental la cual procesa grandes cantidades de información, ya que se usan bases de datos, entonces se usan puertos que trabajan bajo el protocolo TCP/IP y permiten enrutar información que se desarrolla para luego enviarla a las bases de datos nacionales.

Para garantizar la seguridad de la información en la red, siempre se deberá utilizar protocolos de seguridad, que permitan encaminar la información para que no sufran ningún tipo de adulteración o sea interceptada en el camino antes de que llegue al destino, además la información desarrollada en la institución es bastante extensa.

Por último, como medida de seguridad en cuanto a la verificación de la existencia vulnerabilidades en la red, el experto, recomienda que se debe ser un testeo de red cada seis meses, siempre y cuando los equipos se hayan instalado por personal calificado el cual haya configurado los permisos necesarios de accesos a los usuarios. También esta verificación lo debe hacer personal capacitado que entienda de seguridad de información.

La importancia de mantener la integridad de la red, da como consecuencia que los procesos que se realizan en ella, serán de calidad. Un sistema de información que esté correctamente configurado, con una ambiente cómo y un personal altamente calificado, cumplirá con los objetivos que se propone el estudio de la seguridad informática los cuales son garantizar la integridad, confiabilidad y disponibilidad de la información, ya que la información es el activo más importante de las instituciones, y sobre todo las instituciones como la policía.

CONCLUSIONES

Entre las principales conclusiones encontramos que el UPC de Barreiro, tiene problemas en el cumplimiento de las medidas de seguridad establecidas, lo cual es muy peligroso si no se efectúan, ya que pueden atentar la seguridad de la red que existe en esta institución. Las medidas de seguridad tanto física y lógicas dentro de una red, aseguran que el proceso de transmisión de datos y los procesos de la organización sean de calidad.

La seguridad de las redes está en constante actualización, la cual tiene que garantizar que los procesos informáticos se realicen de forma íntegra y confiable. Gracias a los protocolos de seguridad se optimizan procesos de conexión para responder según el modelo de negocio de la organización. Es por eso que los protocolos de seguridad, que se utilizan en el UPC deben actualizarse a su última versión constantemente.

También se pudo concluir que realizar un escaneo en la red periódicamente, ayuda a conocer si existen vulnerabilidades y reducir el nivel de riesgos de seguridad que se pueden presentar si no se toman las medidas de seguridad necesarias para que la información sea de calidad y fiable.

Cabe afirmar que la información que se maneja en esta institución es muy importante y exclusiva para la Policía Nacional, por lo que esta tiene que ser procesada dentro de un ambiente seguro, utilizando buenas prácticas de seguridad informática, donde tanto los usuarios como la infraestructura intervienen para que la información sea integra y confiable.

Las autoridades superiores del UPC deben constatar si su personal está aplicando de manera correcta el manual técnico, y si no llegase ser así, capacitar al personal para que conozcan tales medidas y sobre todo concientizar que al no aplicarlas podrían poner en riesgo la información que se maneja en la Institución.

Los controles que la institución debe implementar para salvaguardar la red de riesgos que atenten ante la seguridad de la información, se escogieron de acuerdo a las necesidades del UPC de Barreiro. La información es el activo más importante de las instituciones, es por eso que se deben cumplir normas de seguridad para protegerla.

Por ultimo como conclusión se afirma que los sistemas de información son los encargados de procesar la información por lo que hay que asegurarse que este cumpla con su objetivo de manera óptima teniendo en cuenta, que un sistema de información no sólo está conformado por equipos informáticos, sino que también forman parte las instalaciones, el medio que lo rodea y sobre todo el personal, el cual debe estar debidamente capacitado para gestionar de forma segura los equipos encargados para el procesamiento de la información.

BIBLIOGRAFÍA

Techopedia Inc. (2019). *Techopedia*. Obtenido de Threat: https://www.techopedia.com/definition/25263/threat

Ariganello, E. (2016). *REDES CISCO. Guía de estudio para la certificación CCNA Routing y Switching. 4ª edición actualizada.* Grupo Editorial RA-MA.

Conklin, W. A., & Shoemaker, D. P. (2013). *CSSLP Certification All-in-One Exam Guide.* McGraw Hill Professional.

Hontañón, R. J. (2016). *Linux Security.* John Wiley & Sons.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001:2013 ISMS Standard.* Artech House.

ISO27000 ESPAÑOL. (2015). *Control de Accesos*. Obtenido de http://www.iso27000.es/iso27002_9.html

ISO27000 Español. (2015). *El portal de ISO 27002 en Español*. Obtenido de Seguridad física y Ambiental: http://www.iso27000.es/iso27002_11.html

Ivan Mistrik, R. B. (2014). *Relating System Quality and Software Architecture.* Morgan Kaufmann.

Iviricu Roba, L. R., Alvarez Vento, J. R., & Concepción García, L. E. (2016). *Metodología para la Detección de Vulnerabilidades en las Redes de Datos utilizando Kali-Linux.* Pinar del Río.

Kapadia, A., Rajana, K., & Varma, S. (2015). *OpenStack Object Storage (Swift) Essentials.* Birmingham: Packt Publishing Ltd.

Kremling, J., & Parker, A. M. (2017). *Cyberspace, Cybersecurity, and Cybercrime.* SAGE Publications.

ltraReach Internet Corp. (2018). *Ultrasurf*. Obtenido de https://ultrasurf.us/about/

Luque, J. J., & Luque, D. B. (2016). *Montaje de infraestructuras de redes locales de datos. ELES0209.* IC Editorial.

Marian, Q. (2017). *Encyclopedia of Information Ethics and Security.* New York: Idea Group Inc (IGI).

Ministerio del Interior. (2014). *Policia Nacional.* Obtenido de MANUAL DE GESTIÓN ADMINISTRATIVA Y OPERATIVA: http://www.policiaecuador.gob.ec/wp-content/uploads/downloads/2014/06/INSTRUCTIVO-DE-CUIDADO-Y-MANTENIMIENTO-DE-UPC-36-PAGINAS-1.pdf

Pérez, P. M. (2016). *UF1879 - Equipos de interconexión y servicios de red.* Editorial Elearning, S.L.

Quigley, M. (2017). *Encyclopedia of Information Ethics and Security.* New York: Idea Group Inc (IGI).

Richarte, J. (2018). Fundamentos de redes. *RedUsers*, 24 .

Study Academy. (2017). *What is Information Security? - Definition & Best Practices*. Obtenido de https://study.com/academy/lesson/what-is-information-security-definition-best-practices.html

TecNoincer. (2017). *ecNoincer*. Obtenido de https://www.tecnoinver.cl/uso-de-protocolos-seguros-para-la-transferencia-de-datos-en-internet/

Urbina, G. B. (2016). *Introduccion a la Seguridad Informatica.* Mexico: Grupo Editorial Patria.

Walker, M. (2016). *CEH Certified Ethical Hacker All-in-One Exam Guide, Third Edition.* New York: McGraw Hill Professional.

Zwicky, E. D., Cooper, S., & Chapman, D. B. (2014). *Building Internet Firewalls.* Sebastopol : O'Reilly Media, Inc.

ANEXO I.

Entrevista

1. **¿Utiliza usted medidas para la seguridad de la red y de información?**

Como policías, es nuestra obligación salvaguardar la información y la infraestructura de esta Unidad, ninguna persona ajena a la institución puede manipular los dispositivos informáticos sin autorización.

2. **¿Qué tipos de medidas de seguridad están obligados a llevar ustedes los policías para proteger la red?**

Existe un manual técnico que debemos seguir, la policía en los diferentes UPC's al nivel nacional. Dicho manual se encuentra en el repositorio del Ministerio del Interior.

3. **¿Cómo considera usted que se encuentra el nivel de seguridad física de la red?**

El nivel de seguridad física es media, debido a que el servidor se encuentra en un pequeño cuarto, en el cual es de libre acceso de los policías, considerando que alguno de ellos no conocen ciertos parámetros que se deben llevar para la seguridad informática. Pero de todos modos se les advierte que no pueden tocar nada.

4. **¿Esta unidad cuenta con una conexión inalámbrica?**

Ciertamente no debería existir una red inalámbrica en la unidad, pero con el permiso de los superiores se hizo la instalación de un router inalámbrico, para que el grupo policial puede navegar desde sus dispositivos móviles.

5. **¿Cuántas computadoras de escritorio existen en la unidad?**

Actualmente, existen dos computadoras una para la administración de las cámaras de seguridad, otra para la recepción y otra para la secretaria de la unidad.

6. ¿Poseen antivirus las computadoras?

Sí, poseen el Avast versión free. Aunque no debería haber, porque existe un servidor en la unidad que garantiza la seguridad de la red y de los datos.

7. ¿Qué características de software tiene el servidor proxy?

Está implementado en CentOS 7 1611, usando la herramienta proxy Squid. El soporte y las actualizaciones se hacen desde Quito.

8. ¿Qué protocolos de seguridad usa el servidor?

El servidor es un proxy, que limita el acceso a la web, las redes sociales como Facebook, YouTube, WhatsApp y otras, están bloqueadas, por medio del SOCKS4 el cual sirve para controlar el tráfico de peticiones de los protocolos HTTP, FTP entre el computador cliente y el servidor, con cifrado SSL y TCL.

9. ¿Es altamente confiable el proxy que está implementado en la RED?

Lastimosamente no, porque .se pueden usar programas túneles, los cuales re-direccionan hacia otro servidor proxy, ajeno a la institución para poder acceder a las páginas bloqueadas.

10. ¿Conoce los riesgos a los que se exponen a utilizar ese tipo de software?

Sí, es por eso que se recomienda a cada uno de los policías de turno que están a cargo de las computadoras que no utilicen ese tipo de software.

_____

P.N Tuaza Mauricio

ANEXO II.

Entrevista al Ing. Harry Saltos

1. **Los que se manejan en la UPC de Barreiro son datos preliminares informativos (parte policial) y datos de inteligencia que son gestionados en el sistema informático local previo a subirlo al sistema nacional. ¿Qué medidas de seguridad de la Usted sugiere?**

   En primer lugar considero que el UPC debería tener equipos preconfigurados para que la información no sea adulterada o vulnerada, por ejemplo equipos hardening, es decir con todas la correcciones de seguridad posibles, por ejemplo la desactivación de la detección de dispositivos USB, y la apertura de puertos de red específicos por donde se transmita información sólo hacia los sistemas nacionales de la policía, en efecto se debe crear políticas de seguridad para el tratamiento de información. En segundo lugar pienso que en el UPC debe manejarse información preliminar, esta información tiene que ser administrada por personal que esté altamente capacitado para trabajar con información de esta naturaleza, ciertamente puede ser un oficial, pero con funciones específicas de tratamiento de los datos que se gestionan en este lugar como lo es un parte policial, este personal debe tener bajo su responsabilidad todos los accesos, claves y electrónicas.

2. **¿Cuál sería su recomendación en cuanto a redes inalámbricas en una institución pública como el UPC?**

   Bueno mi recomendación cuanto redes inalámbricas sería de ponerle los niveles de seguridad necesaria con claves complicadas y con cifrado. En este caso en un UPC se supone que la información que se va tener que transmitir por las redes inalámbricas no debería ser ajena para la institución, porque es una entidad de gobierno en la que se debe de estar dedicada netamentemente durante su tiempo completo en atender temas de seguridad de la ciudadanía, entonces pues no debería una red inalámbrica distraer a estos servidores públicos en temas ajenos a la seguridad de la gente. Por eso creo que las redes inalámbricas también tendrían que tener restricciones, que sólo permitan conectar ciertos dispositivos y conectarse a orígenes y destinos orientados a procesar información útil relacionada con la finalidad de la institución, que es de servir y proteger al ciudadano.

3. **¿Qué medidas de seguridad debería tener las computadoras de los UPC según su criterio?**

   Las computadoras del UPC deberían tener medidas de seguridad que permitan manejar información inherente a las actividades diarias de la policía, que sólo permitan la ejecución de aplicaciones dedicadas solamente a procesar información del UPC, y no de programas que puedan ocasionar algún agujero de seguridad, como por ejemplo navegadores no permitidos, juegos o cualquier software no permitidos. Estos computadores deberían estar apegados a políticas de seguridad de sistemas operativos muy específicas, para que los servidores policiales se dediquen netamente a sus actividades que permitan transmitir a escalas nacionales sólo la información que se procesa sea relacionada con los diferentes UPC del país y el UPC de Barreiro.

4. **¿Qué protocolos usted recomienda utilizar en el UPC?**

   Yo creo que se debería utilizar protocolos apegados a lo que demanda la escala nacional, por ejemplo estoy seguro que a escala nacional están utilizando bases de datos, entonces deberían usar puertos necesarios que corren sobre protocolos TCP/IP o que se abren bajo estos protocolos y estos puertos permiten enrutar información desarrollada en los UPC y depositada en las bases de datos a nivel nacional.

5. **¿Cada cuánto tiempo recomienda usted que se debe hacer un escaneo de vulnerabilidades para salvaguardar la integridad física y lógica de la red?**

   Bueno se puede hacer un escaneo de vulnerabilidades cada seis meses, es decir si realmente la computadora fue instalada por personal calificado y esta tiene el debido proceso de instalación donde se le han activado solamente ciertos permisos y ciertos accesos por usuario. Entonces se puede recomendar que cada seis meses se haga una verificación. Esta verificación la debe hacer personal adecuado que entienda netamente de informática y sobre todo sobre la seguridad de la información.

_____

Ing. Harry Saltos

ANEXO III.

Ficha de observación.

<table>
<tr><td rowspan="2">Ficha de Observación</td><td>Caso de Estudio: Estudio de Medidas y Protocolos de Seguridad en las Redes Informáticas del UPC (Unidad de Policía Comunitaria) de la Parroquia Barreiro</td></tr>
<tr><td>Responsable: María Cotto Solís</td></tr>
<tr><td>Fecha: 18 de diciembre de 2018

Hora: 09:30

Lugar: UPC de Barreiro, cantón Babahoyo, provincia de los Ríos</td><td>OBSERVACIÓN

El UPC de Barreiro brinda servicios de seguridad ciudadana a los moradores del lugar.

Se observó una red LAN y cableado estructurado, 2 máquinas clientes y un cuarto donde se encuentra el rad junto con el Switch y el servidor.

El cable es UTP categoría 6. Se usa una topología en Árbol.

El servidor usa CentOS 7, con los sistemas operativos de los equipos de escritorio Windows 7.

Se notó que parte del tumbado o techo falso se encuentra deteriorado.</td></tr>
</table>

ANEXO IV.

Manual técnico de las medidas de seguridad informática en los UPC

PROCEDIMIENTO PARA LA UTILIZACIÓN DE LOS EQUIPOS DE COMPUTACIÓN:

- Cada equipo está preparado con el Hardware y Software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y lógico del mismo incluyendo sus periféricos. (está prohibido descargar o mantener en el CPU música, películas, pornografía, archivos personales entre otros)
- Por ningún motivo se deberá abrir los equipos, o reparar cualquier daño o cambio al hardware, será responsabilidad de la persona a quien este resguardado, únicamente deberá informar de la posible falla al área de informática de Fabrec.
- En caso de presentar una falla física o lógica se deberá notificar al área de informática de Fabrec y en el caso de ser requerido enviar el equipo para su revisión y/o reparación de acuerdo al procedimiento establecido.
- En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.
- Solo se utilizara el equipo para funciones de interés de la UPC y de ninguna manera para asuntos personales.
- El personal asignado deberá comprobar sus conocimientos y/o experiencia, se notificara al área de sistemas para su correspondiente capacitación.
- La salida del equipo de cómputo del UPC, será total responsabilidad del oficial a cargo.
- Cada equipo contiene el software de acuerdo a las necesidades del área de trabajo.

- Existe un computador con el programa informático para receptar el enlace telefónico de auxilio. En este equipo se registra el auxilio que llega al teléfono movitalk, mismo que se constituye en el archivo histórico de registros de llamadas de auxilio en el sub-circuito.
- El computador con el programa informático que será utilizado por el jefe de la unidad para efectuar trabajos inherentes al servicio policial. Se recomienda hacer buen uso de los computadores, en vista que son equipos frágiles y delicados; evite ingresar Pen Drive infectados con virus, en vista que puede dañar el software del computador.

CABLEADO ESTRUCTURADO

- Es el equipamiento tecnológico de Hardware que permite la comunicación entre el equipo de computación y otros medios.
- En caso de existir daños en el cableado estructurado o en los equipos que conforman la red LAN (Switch, Router, Canaleta, etc.) se comunicará de forma inmediata a la empresa encargada del mantenimiento de este equipamiento, para la respectiva asistencia técnica.
- El cableado estructurado y equipos que conforman la red LAN serán de exclusiva responsabilidad de las Unidades Policiales a las que fueron entregadas dicho equipamiento.
- Todos los equipos de la red LAN, deben estar encendidos las 24 horas del día y los 365 días del año.
- Concienciar a los usuarios de los equipos entregados sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

- Exigir a los usuarios el cuidado, respeto y buen uso de los recursos de cómputo y red LAN, de acuerdo con los criterios que en este documento se mencionan.

- La protección física de los equipos de comunicación corresponde a quienes en un principio se les asigne y entregue.

- Proporcionar y garantizar condiciones de seguridad física y ambiental a todo el equipo de comunicación, protegiéndolo contra el acceso no autorizado, de personas ajenas que puedan causar daño al cableado de datos o robar la información que circula en ella.

- La pérdida o robo de cualquier componente de la red LAN del SII-PNE, debe ser reportada inmediatamente al Jefe de la UPC y este a su vez a los Coordinadores de Comunicaciones de los Distitos de la Dirección Nacional de Telecomunicaciones e Informática.

- El mantenimiento corresponderá a quienes en un principio se les asigne y entregue los equipos de comunicación, además velará por la conservación de sus instalaciones, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar, para lo cual deberán realizar las siguientes actividades de manera preventiva:

    - Monitorear la red LAN y sus componentes, para detectar posibles inconvenientes y brindar la respectiva solución.

    - Verificar posibles daños en las canaletas de protección del cable eléctrico y de datos.

    Obtenido de (Ministerio del Interior, 2014)

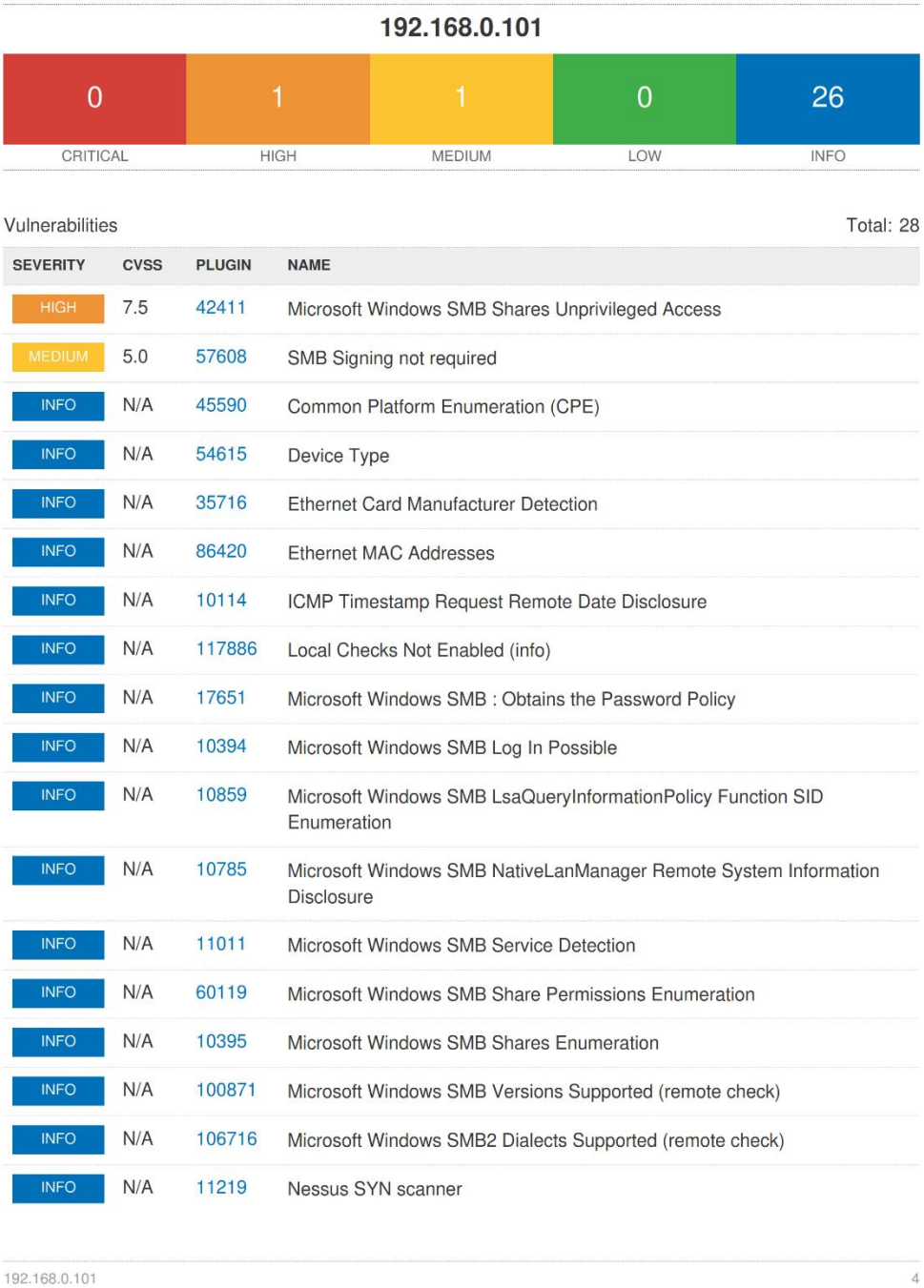
ANEXO V.

Estado del tumbado del UPC

Fig. 2 Estado del tumbado del UPC. Autora María Cotto

ANEXO VI.

Resultado del escaneo de la red del UPC con Nessus.



192.168.0.101

0	1	1	0	26
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 28

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner

192.168.0.101 4

Fig. 3 Reporte general de escaneo con Nessus. Autora María Cotto

ANEXO VII.

Informe detallado de vulnerabilidades encontradas.

42411 (1) - Microsoft Windows SMB Shares Unprivileged Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read/write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

High

CVSS Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVSS Temporal Score

5.5 (CVSS2#E:U/RL:OF/RC:C)

References

BID	8026
CVE	CVE-1999-0519
CVE	CVE-1999-0520

Plugin Information:

Published: 2009/11/06, Modified: 2018/07/27

Plugin Output

192.168.0.101 (tcp/445)

```
The following shares can be accessed using a NULL session  :

- COMPATIR  - (readable,writable)
  + Content of this share :
..
\n
```

Fig. 4 Informe detallado de Vulnerabilidad 1. Autora María Cotto

57608 (1) - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information:

Plugin Output

192.168.0.101 (tcp/445)

Fig. 5 Informe detallado de Vulnerabilidad 2. Autora María Cotto

ANEXO VIII.

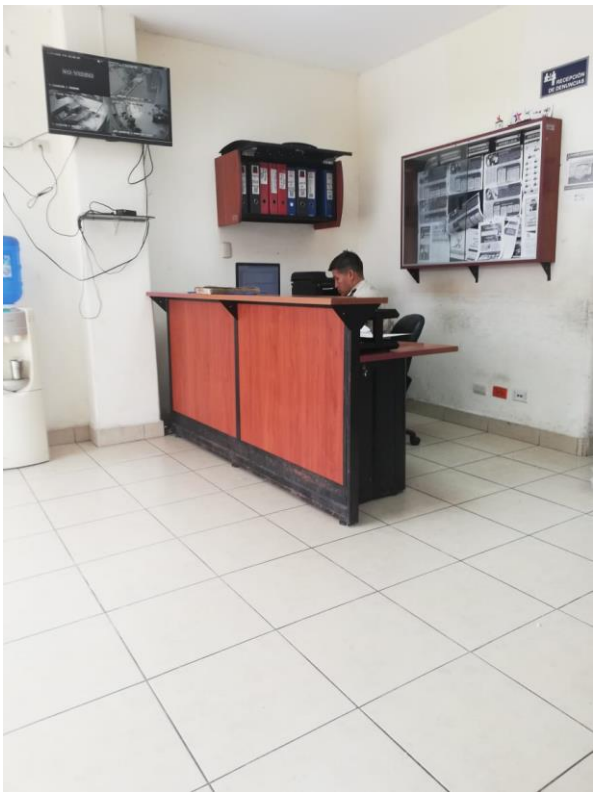


Fig. 6 Visita al UPC de Barreiro

Fig. 7 Entrevista al Sargento William Zapata

Fig. 8 Servidor del UPC

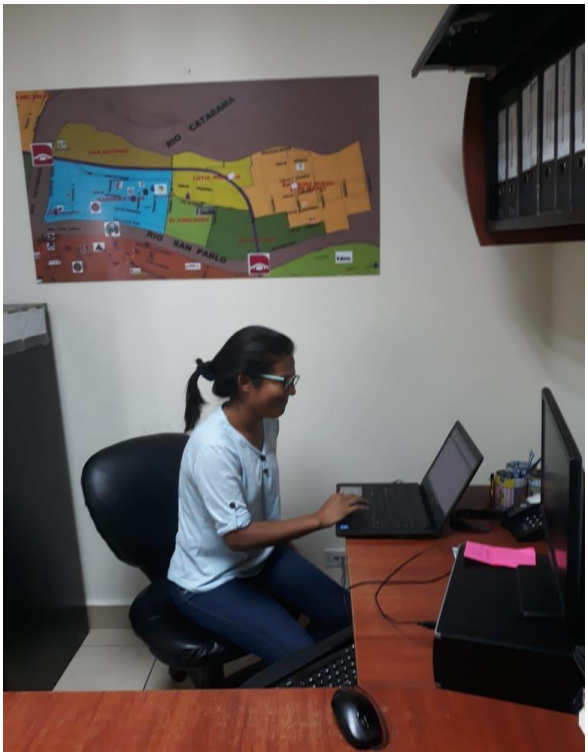


Fig. 9 Realizando el respectivo escaneo en la RED del UPC de Barrero

ANEXO IX. Controles de la Norma 27002

ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

5. POLÍTICA DE SEGURIDAD.
- **5.1 Política de seguridad de la información.**
  - 5.1.1 Documento de política de seguridad de la información.
  - 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- **6.1 Organización interna.**
  - 6.1.1 Compromiso de la Dirección con la seguridad de la información.
  - 6.1.2 Coordinación de la seguridad de la información.
  - 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
  - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
  - 6.1.5 Acuerdos de confidencialidad.
  - 6.1.6 Contacto con las autoridades.
  - 6.1.7 Contacto con grupos de especial interés.
  - 6.1.8 Revisión independiente de la seguridad de la información.
- **6.2 Terceros.**
  - 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
  - 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
  - 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.
- **7.1 Responsabilidad sobre los activos.**
  - 7.1.1 Inventario de activos.
  - 7.1.2 Propiedad de los activos.
  - 7.1.3 Uso aceptable de los activos.
- **7.2 Clasificación de la información.**
  - 7.2.1 Directrices de clasificación.
  - 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- **8.1 Antes del empleo.**
  - 8.1.1 Funciones y responsabilidades.
  - 8.1.2 Investigación de antecedentes.
  - 8.1.3 Términos y condiciones de contratación.
- **8.2 Durante el empleo.**
  - 8.2.1 Responsabilidades de la Dirección.
  - 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
  - 8.2.3 Proceso disciplinario.
- **8.3 Cese del empleo o cambio de puesto de trabajo.**
  - 8.3.1 Responsabilidad del cese o cambio.
  - 8.3.2 Devolución de activos.
  - 8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.
- **9.1 Áreas seguras.**
  - 9.1.1 Perímetro de seguridad física.
  - 9.1.2 Controles físicos de entrada.
  - 9.1.3 Seguridad de oficinas, despachos e instalaciones.
  - 9.1.4 Protección contra las amenazas externas y de origen ambiental.
  - 9.1.5 Trabajo en áreas seguras.
  - 9.1.6 Áreas de acceso público y de carga y descarga.
- **9.2 Seguridad de los equipos.**
  - 9.2.1 Emplazamiento y protección de equipos.
  - 9.2.2 Instalaciones de suministro.
  - 9.2.3 Seguridad del cableado.
  - 9.2.4 Mantenimiento de los equipos.
  - 9.2.5 Seguridad de los equipos fuera de las instalaciones.
  - 9.2.6 Reutilización o retirada segura de equipos.
  - 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
- **10.1 Responsabilidades y procedimientos de operación.**
  - 10.1.1 Documentación de los procedimientos de operación.
  - 10.1.2 Gestión de cambios.
  - 10.1.3 Segregación de tareas.
  - 10.1.4 Separación de los recursos de desarrollo, prueba y operación.
- **10.2 Gestión de la provisión de servicios por terceros.**
  - 10.2.1 Provisión de servicios.
  - 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
  - 10.2.3 Gestión del cambio en los servicios prestados por terceros.
- **10.3 Planificación y aceptación del sistema.**
  - 10.3.1 Gestión de capacidades.
  - 10.3.2 Aceptación del sistema.
- **10.4 Protección contra el código malicioso y descargable.**
  - 10.4.1 Controles contra el código malicioso.
  - 10.4.2 Controles contra el código descargado en el cliente.
- **10.5 Copias de seguridad.**
  - 10.5.1 Copias de seguridad de la información.
- **10.6 Gestión de la seguridad de las redes.**
  - 10.6.1 Controles de red.
  - 10.6.2 Seguridad de los servicios de red.
- **10.7 Manipulación de los soportes.**
  - 10.7.1 Gestión de soportes extraíbles.
  - 10.7.2 Retirada de soportes.
  - 10.7.3 Procedimientos de manipulación de la información.
  - 10.7.4 Seguridad de la documentación del sistema.
- **10.8 Intercambio de información.**
  - 10.8.1 Políticas y procedimientos de intercambio de información.
  - 10.8.2 Acuerdos de intercambio.
  - 10.8.3 Soportes físicos en tránsito.
  - 10.8.4 Mensajería electrónica.
  - 10.8.5 Sistemas de información empresariales.
- **10.9 Servicios de comercio electrónico.**
  - 10.9.1 Comercio electrónico.
  - 10.9.2 Transacciones en línea.
  - 10.9.3 Información públicamente disponible.
- **10.10 Supervisión.**
  - 10.10.1 Registros de auditoría.
  - 10.10.2 Supervisión del uso del sistema.
  - 10.10.3 Protección de la información de los registros.
  - 10.10.4 Registros de administración y operación.
  - 10.10.5 Registro de fallos.
  - 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.
- **11.1 Requisitos de negocio para el control de acceso.**
  - 11.1.1 Política de control de acceso.
- **11.2 Gestión de acceso de usuario.**
  - 11.2.1 Registro de usuario.
  - 11.2.2 Gestión de privilegios.
  - 11.2.3 Gestión de contraseñas de usuario.
  - 11.2.4 Revisión de los derechos de acceso de usuario.
- **11.3 Responsabilidades de usuario.**
  - 11.3.1 Uso de contraseñas.
  - 11.3.2 Equipo de usuario desatendido.
  - 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
- **11.4 Control de acceso a la red.**
  - 11.4.1 Política de uso de los servicios en red.
  - 11.4.2 Autenticación de usuario para conexiones externas.
  - 11.4.3 Identificación de los equipos en las redes.
  - 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
  - 11.4.5 Segregación de las redes.
  - 11.4.6 Control de la conexión a la red.
  - 11.4.7 Control de encaminamiento (routing) de red.
- **11.5 Control de acceso al sistema operativo.**
  - 11.5.1 Procedimientos seguros de inicio de sesión.
  - 11.5.2 Identificación y autenticación de usuario.
  - 11.5.3 Sistema de gestión de contraseñas.
  - 11.5.4 Uso de los recursos del sistema.
  - 11.5.5 Desconexión automática de sesión.
  - 11.5.6 Limitación del tiempo de conexión.
- **11.6 Control de acceso a las aplicaciones y a la información.**
  - 11.6.1 Restricción del acceso a la información.
  - 11.6.2 Aislamiento de sistemas sensibles.
- **11.7 Ordenadores portátiles y teletrabajo.**
  - 11.7.1 Ordenadores portátiles y comunicaciones móviles.
  - 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
- **12.1 Requisitos de seguridad de los sistemas de información.**
  - 12.1.1 Análisis y especificación de los requisitos de seguridad.
- **12.2 Tratamiento correcto de las aplicaciones.**
  - 12.2.1 Validación de los datos de entrada.
  - 12.2.2 Control del procesamiento interno.
  - 12.2.3 Integridad de los mensajes.
  - 12.2.4 Validación de los datos de salida.
- **12.3 Controles criptográficos.**
  - 12.3.1 Política de uso de los controles criptográficos.
  - 12.3.2 Gestión de claves.
- **12.4 Seguridad de los archivos de sistema.**
  - 12.4.1 Control del software en explotación.
  - 12.4.2 Protección de los datos de prueba del sistema.
  - 12.4.3 Control de acceso al código fuente de los programas.
- **12.5 Seguridad en los procesos de desarrollo y soporte.**
  - 12.5.1 Procedimientos de control de cambios.
  - 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 12.5.3 Restricciones a los cambios en los paquetes de software.
  - 12.5.4 Fugas de información.
  - 12.5.5 Externalización del desarrollo de software.
- **12.6 Gestión de la vulnerabilidad técnica.**
  - 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- **13.1 Notificación de eventos y puntos débiles de seguridad de la información.**
  - 13.1.1 Notificación de los eventos de seguridad de la información.
  - 13.1.2 Notificación de puntos débiles de seguridad.
- **13.2 Gestión de incidentes y mejoras de seguridad de la información.**
  - 13.2.1 Responsabilidades y procedimientos.
  - 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
  - 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- **14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.**
  - 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
  - 14.1.2 Continuidad del negocio y evaluación de riesgos.
  - 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
  - 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
  - 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.
- **15.1 Cumplimiento de los requisitos legales.**
  - 15.1.1 Identificación de la legislación aplicable.
  - 15.1.2 Derechos de propiedad intelectual (DPI).
  - 15.1.3 Protección de los documentos de la organización.
  - 15.1.4 Protección de datos y privacidad de la información de carácter personal.
  - 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
  - 15.1.6 Regulación de los controles criptográficos.
- **15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.**
  - 15.2.1 Cumplimiento de las políticas y normas de seguridad.
  - 15.2.2 Comprobación del cumplimiento técnico.
- **15.3 Consideraciones sobre las auditorías de los sistem. de información.**
  - 15.3.1 Controles de auditoría de los sistemas de información.
  - 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.