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:

Vulnerabilidades de los riesgos en el tráfico de la red informática del Infocentro de la Parroquia "Guare"

EGRESADA:

Herlinda Narcisa Mosquera Sánchez

TUTORA:

Ing. María Genoveva Moreira Santos, MIE

AÑO 2019

INTRODUCCIÓN

Los Infocentros comunitarios pertenecen a un proyecto destinado a la zona rural del Ecuador, con el objetivo de que la sociedad donde estos se encuentran tenga acceso a servicios informáticos, de internet y cursos de capacitación de forma gratuita, gestionado por el Ministerio de Telecomunicaciones (MINTEL) y las prefecturas provinciales.

En el infocentro ubicado en la parroquia Guare, del cantón Baba, provincia de Los Ríos brinda los moradores del sector cursos de capacitación de diferentes ámbitos como informática, de belleza y primeros auxilios destinados a personas de diferentes edades, quienes hacen uso de la tecnología que tiene ese centro de computo social.

Todas estas actividades se las realiza de forma gratuita, al estar libre para todo público se vuelve altamente vulnerable y esto a su vez el acceso el servidor correría el riesgo de ser atacado, el infocentro es administrado por un facilitador, quien es la persona que se encarga de gestionar los recursos tecnológicos con los que cuenta las instalaciones así como controlar las capacitaciones brindan a la comunidad.

El facilitador recolecta los datos personales de las personas que desean matricularse en los cursos que se brindan en el lugar, y estos datos son almacenados en el servidor permitiendo el control de asistencia de cada estudiante ya que al terminar el curso de capacitación cada estudiante recibe su certificado de aprobación que le otorga el infocentro.

Existen muchas maneras de reducir los riesgos de que la información sea extraída mediante la red es implementando normas que resguarden la información.

El uso de las Tecnologías de la información, actualmente está presenten en la mayoría de las organizaciones, y la información que en esta se gestiona es muy importante tanto para los usuarios como para la organización, es por eso que estas deben utilizar

mecanismos para garantizar la integridad confidencialidad y disponibilidad de la información a sus usuarios.

La seguridad informática también conocida como ciberseguridad o seguridad de tecnología de la información, es una relación entre el área de la informática y la telemática dedica específicamente a la protección de la infraestructura computacional y todos sus componentes que se encuentran relacionado lo cual se debe tener un debido cuidado para evitar que la información se filtre o hacer un mal uso de la información lo cual causaría pérdidas económicas en la institución.

El presente estudio de caso, se centra en efectuar un análisis del tráfico de datos de la red del Infocentro comunitario de la parroquia Guare, perteneciente al Cantón Baba, con el objetivo de encontrar vulnerabilidades que puedan afectar a la seguridad informática que la institución maneja.

Este análisis que realizará en el Infocentro Comunitario de la parroquia Guare, determinará si existen vulnerabilidades en la red, para luego establecer el nivel de riesgos que estas presentan y proponer operaciones pertinentes para mantener segura la información que gestiona el sistema informático del infocentro.

DESARROLLO

Actualmente un punto clave de investigación y control es la seguridad de la información, debido a avanza la tecnología cambia el ambiente de trabajo, y las empresas para adaptarse a estos cambios tienden a fijar nuevos horizontes, puesto que la aparición de nuevas amenazas, podrían poner en riesgo los activos de la organización.

La importancia de los sistemas de información surge desde 1970, permitiendo que la información sea más accesible, dando como resultado la implementación del internet en hogares, es por eso que hoy en día es fácil intercambiar información. Pero, lastimosamente así como se ha incrementado el uso de sistemas de informáticos, la piratería informática y hacking también lo han hecho, por lo que las empresas deben estar en constante actualización sobre seguridad informática se refiere.

Es por eso que actualmente las empresas al gestionar gran cantidad de información, ya que esta puede ser alterada, robada, infectada o dañada por software malintencionado lo que puede causar el deterioro del sistema operativo y grandes pérdidas para la organización, buscan soluciones óptimas para brindar seguridad a los sistemas informáticos. (BANCAL, DUMAS, & PUCHE, 2015).

Este proyecto se relaciona con la línea de investigación relacionada a los procesos de transmisión de datos y gestión de telecomunicaciones porque se efectuará un análisis tanto físico, como lógico a la red del área informática del infocentro de la parroquia Guare, ubicada en el Cantón Baba, provincia de Los Ríos.

La metodología usada en el presente caso de estudio para detectar las vulnerabilidades en la red del infocentro de Guare, es la cualitativa, porque se pretende encontrar los principales problemas que pueden existir en la infraestructura, como en la trasmisión de los datos; para explicar los principales riesgos que pueden surgir a largo

plazo, donde se utilizará como herramienta de investigación una entrevista con el facilitador del lugar, y un testeo en la red para lo cual se usaran como instrumento de investigación el cuestionario y el software de escaneo de vulnerabilidades Nessus Professional™, respectivamente. También se utilizó la observación directa para ver el estado de la infraestructura física de la red.

El presente caso de estudio consta de tres fases mediante las cuales se busca obtener las vulnerabilidades en los equipos de red, las cuales son: Fase I.- Reconocimiento y recolección de información, Fase II.- Escaneo de la red y detención de vulnerabilidades, y Fase III.- análisis de riesgos.

Durante la fase I, se planteó encontrar los problemas que existan en la red local del infocentro, los cuales serán especificados de acuerdo a la observación (ANEXO II) y la entrevista elaborada (ANEXO I) para el facilitador del lugar.

El infocentro de Guare se encuentra equipado aproximadamente con 8 terminales y un servidor Dual Boot (Windows Server R2 y Ubuntu 18.04.1 LTS). Los terminales son usadas por los usuarios con fines educativos, y actividades de ocio. En este infocentro se realizan capacitaciones que tienen duración de 3 o 4 meses lo que ayuda a mejorar los conocimientos de la informática a los moradores del sector.

El infocentro de Guare, como en todo centro informático de libre acceso se producen inconvenientes como la caída del internet, conexiones inestables, lentitud de carga de páginas webs y otros inconvenientes que impiden realizar actividades cotidianas de los ciudadanos de este lugar.

Windows Server R2 pertenece a la familia de sistemas operativos de Microsoft Corporation. Esta versión reúne toda la experiencia en administración, almacenamiento,

redes, seguridad, virtualización, plataforma de aplicaciones, web y servicios en la nube que facilitan las opciones de trabajo. (Flores Rosa, 2014)

En el infocentro el sistema operativo más utilizado es Ubuntu, puesto que Windows Server no cuenta con antivirus, y según el facilitador del infocentro, tiene virus de Acceso y este está replicado por medio de la red en las maquinas clientes, lo es muy fastidioso para los usuarios que consumen los servicios que ofrecen en el lugar y sobretodo que en el futuro la red podría infectarse con un virus más peligroso, como: suplantación de identidad, divulgación de contenido, modificación de mensajes, denegación de servicios o abrir puertas traseras.

Ubuntu es un sistema operativo de escritorio de código abierto, el cual es usado en millones de computadoras de escritorio y portátiles en todo el mundo. Todas las aplicaciones esenciales, como una suite de oficina, navegadores, correo electrónico y aplicaciones de medios vienen preinstaladas y miles de juegos y aplicaciones más están disponibles en el Centro de Software de Ubuntu. (Canonical Ltd. Ubuntu, 2019)

Por lo antes expuesto, en la Fase II (Anexo III),se realizó un estudio en la infraestructura lógica a la red del Infocentro de la Parroquia Guare, con el objetivo de obtener un análisis del grado de seguridad que existe en este lugar, y determinar que posibles soluciones se pueden aplicar para solucionar los problemas encontrados.

En el aspecto lógico se debe tomar en cuenta la configuración operativa de la red, y tener cuidado con personas ajenas a la organización que no tienen autorización para acceder a la información, ya que pueden ser piratas informáticos como hackers o crackers, que pueden usar la información con objetivos mal intencionados.

Como sugerencia se propone la instalación de un antivirus como Kaspersky™ Internet Security para desinfectar la red del virus de acceso directo, y garantizar a los usuarios de Windows que el servicio brindado sea de calidad y no se sientan incomodos al trabajar en los equipos que ofrece el infocentro.

También se propone que periódicamente (cada 3 meses) se realice un escaneo a la red para detectar si existen vulnerabilidades que vayan en contra de la seguridad de los servicios que ofrece el infocentro de Guare, usan herramientas de testeo, como le es Nessus Profesional. Con este proceso de testeo de la red se pretende informar al facilitador del Infocentro de riesgos en la red existentes, y tomar las medidas pertinentes.

Nessus es un escáner de vulnerabilidades de red de código abierto que utiliza la arquitectura de vulnerabilidades y exposiciones comunes para un fácil enlace entre las herramientas de seguridad compatibles. Nessus tiene una arquitectura modular que consta de servidores centralizados que realizan análisis y clientes remotos que permiten la interacción desde el panel de administración. (Kumar, 2014)

Nessus es una potente herramienta de testeo multiplataforma, que tiene una interfaz amigable que ayuda fácilmente a identificar y corregir vulnerabilidades existentes que puedan afectar la transmisión de los datos en la red. Existe una versión gratis de Nessus 8.1.2, la cual tiene limitaciones como la que sólo permite el escaneo de 16 terminales simultáneos, lo cual es un inconveniente para redes grandes, pero fue ideal para el infocentro de Guare que sólo cuenta con 9 terminales incluido el servidor.

Existe una versión de pago de Nessus Pro 8.1.2, la cual brinda una versión de prueba de 7 días, con la cual se puede realizar infinitos escaneos a infinitos terminales de red, además de incluir una función que permite hacer escaneos de vulnerabilidades de forma remota. El costo por año de la licencia de Nessus es de $ 2,190.00.

Si bien es cierto, es un costo muy elevado del servicio que ofrece Nessus, vale la pena pagarlo porque la información que se maneja en este lugar es muy importante para cada usuario, y podría provocar daños irreparables si existe el riesgo de que sea usada con fines ajenos que pueden dañar la integridad de alguna persona. No obstante la versión gratuita es perfecta para el infocentro de Guare debido al tamaño de la red.

Por último la fase III, se realizó un análisis de las vulnerabilidades encontradas en el escaneo de la red (ANEXO 4), para identificar los riesgos que pueden suceder en un futuro si no se toman las medidas pertinentes, para salvaguardar la información que se procesa en el infocentro.

El infocentro de la parroquia Guare, brinda diferentes servicios tecnológicos a los moradores del lugar, como uso de computadoras e internet, impresiones y además de impartir cursos de diferentes temáticas, todo esto de forma gratuita, financiado por parte del gobierno nacional. Los centros de cómputo deben seguir medidas de seguridad para reguardar el equipamiento físico y la infraestructura lógica de la red.

La tendencia de hoy en día es el uso que se le da a las Tecnologías de la Información y Comunicación (TIC’s), las cuales permiten a los usuarios a desarrollar su potencial en diferentes temáticas si se le da un uso debidamente correcto, pero si bien es cierto, hay muchas excepciones en este aspecto, ya que existen muchas personas mal intencionadas que usan las TIC’s para causar daños a los sistemas o robar información.

Ante esta situación, se puede expresar gran preocupación en lo que a seguridad se refiere en los centros de cómputo, como el Infocentro de Guare, puesto que existen riesgos que podrían causar daños en la infraestructura de la red, equipos e información si no se toman las medidas necesarias para garantizar la calidad de los servicios que se brindan en el lugar.

Una red computadoras conforma un conjunto de equipos informáticos y software conectados entre sí con la finalidad de compartir información, recursos y ofrecer servicios con el objetivo de brinda mucha facilidad en el acceso a la información y una gran capacidad de almacenaje de datos. (Jalca Regalado, y otros, 2018)

La red que se encuentra en el infocentro es LAN (Red de Área Local), es usada para navegar en internet, se encuentra compartida la impresora, brindando a los usuarios la facilidad de acceder a la información que ellos necesitan, la cual debe estar disponible y accesible de una manera rápida.

El tráfico de la red es el término que se le da cuando los datos viajan de un punto a otro usando los medios de la red. Estos datos, en forma de paquetes recorren una ruta para ingresar a un sistema y para salir de él por medio de las tarjetas de red. Estos paquetes pueden ser tráfico de voz, o tráfico de archivos, a los cuales se pueden dar un tratamiento especial, para disfrutar un servicio de calidad. (Marqués, 2016)

Uno de los tipos de redes por su extensión conocidos son las Redes LAN. El infocentro de Guare está constituido por dos redes LAN, una conmutada la cual usa la tecnología ETHERNET con conexión por cables a los terminales, y la otra es inalámbrica con la cual los usuarios del infocentro acceden al internet desde sus dispositivos portable por un tiempo limitado.

Según, (Fernández, 2015), Una red LAN (Red de Área Local) está constituida por un conjunto de equipos que pertenecen a la misma organización y se encuentran conectados dentro de un área geográfica pequeña por medio de una red, por lo general con la misma tecnología.

El sistema que se usa en las computadoras del infocentro de la parroquia Guare es Thin Client, donde un servidor comparte los recursos hardware y software a través de la red y los terminales solo se encargan se administrar los dispositivos como mouse,

teclado y pantalla. Este tipo de tecnologías permiten administrar la red de una mejor manera puesto que los recursos están centralizados.

Los inconvenientes, en este tipos de tecnologías es que si alguna de las maquinas cliente adquiere un virus por cualquiera de los medios de propagación (USB, la Web), el servidor también se verá afectado, y por ende los otros equipos clientes.

La información técnica del servidor se detalla en la siguiente tabla:

Marca	Kypus
Procesador	2* Intel Xeom E5-2043 (10M Cache, 1,8 GHz con 4 núcleos)
Memoria	16 GB DDR3
Disco Duro	2 TB, tecnología SATA.
Sistema Operativo	DUAL Boot: Ubuntu / Windows Server 2012 R2

Tabla 1 Información técnica del Servidor - Autor: Herlinda Mosquera

El atractivo de las computadoras Thin Client es que reemplaza se estaciones de trabajo de escritorio potentes con computadoras simples y simplificadas. Estos clientes ligeros manejan un número relativamente pequeño de operaciones; los Thin Client manejan de los dispositivos de entrada, pero todo lo demás lo maneja al menos un servidor de terminal. (Starinsky, 2016)

Información técnica de los equipos clientes

Marca	Kypus
Procesador	Intel Atom
Memoria	1 GB
Disco Duro	N/A
Sistema Operativo	Según el servidor.

Tabla 2 Información técnica de los equipo cliente - Autor: Herlinda Mosquera

Existen dos aspectos muy importantes para considerar que una red esté segura, los cuales son el aspecto físico y lógico. En el aspecto físico se deben tomar en cuenta medidas preventivas de los riesgos que pueden tener los equipos y la estructura de la red, como desastres naturales, terremotos, incendios, inundaciones.

Los piratas informáticos buscan vulnerabilidades para acceder a los datos que ellos quieren poseer, sea para probarse a sí mismos, o para robar información, que además se pueden aprovechar de la ingenuidad de los trabajadores a los cuales se les envían archivos desconocidos que al abrirlo infectan al sistema o abren puertos TCP, por medio de troyanos, creando vulnerabilidades a dicho sistema. (Universidad de San Carlos, 2014)

Una amenaza, en el contexto de la seguridad informática, se refiere a cualquier cosa que tenga el potencial de causar daños graves a un sistema informático. Es algo que puede suceder o no, pero tiene el potencial de causar un daño grave. Las amenazas pueden provocar ataques a sistemas informáticos, redes y más. Los principales de ataques tenemos.

Suplantación de identidad es un delito en el cual un impostor obtiene piezas clave de información de identificación personal, como las contraseñas, recursos de red o archivos, para hacerse pasar por otra persona. (Gomes Veitte, 2014)

Divulgación del contenido es causada cuando un individuo intercepta la información que se envía entre dos puntos de red, para luego hacer uso de los datos adquiridos. Modificación de mensajes consiste en cambiar el contenido de un determinado mensaje para que cuando llegue a su destino sea imposible ser descubierto.

Denegación del servicio quiere decir que el sistema ha sido modificado para que una persona no lo pueda manejar de forma normal, por ejemplo el sistema gestor de correos electrónicos. (Ríos Yáguez, 2014)

Los mecanismos que llevan a cabo un ataque informático tenemos:

Una puerta trasera es una técnica en la que un mecanismo de seguridad del sistema se pasa de manera indetectable para acceder a una computadora o sus datos. El método de acceso de puerta trasera a veces es escrito por el programador que desarrolla un programa.

Troyano es un programa aparentemente inofensivo, incrustado en algún archivo o que Parente serlo, que, cuando se activa, causa daños a un sistema informático. Virus es un tipo de software malicioso (malware) compuesto de pequeñas piezas de código adjuntas a programas legítimos. Cuando ese programa se ejecuta, el virus se ejecuta.

Vulnerabilidad, es un término de ciberseguridad que se refiere a un defecto en un sistema que puede dejarlo abierto para atacar. Una vulnerabilidad también puede referirse a cualquier tipo de debilidad en un sistema informático en sí mismo, en un conjunto de procedimientos o en cualquier cosa que deje la seguridad de la información expuesta a una amenaza. (Gomes Veitte, 2014)

Actualmente existen dos tipos de ataques, los intencionados y los no intencionados. Los usuarios de computadoras y el personal de la red pueden proteger los sistemas informáticos de las vulnerabilidades manteniendo actualizados los parches de seguridad del software. Estos parches pueden remediar fallas o agujeros de seguridad que se encontraron en la versión inicial. El personal informático y de red también debe

mantenerse informado sobre las vulnerabilidades actuales en el software que utilizan y buscar formas de protegerse contra ellas.

Ataques no intencionados: Es cuando la información personal, o la organización es afectada sin la intención a propósito de una persona. En este caso los ejemplos más habituales pueden ser: incendios, inundaciones, el fallo de la fuente de alimentación y errores del usuario.

Ataques intencionados: Son realizados por personas que no están autorizados para acceder al sistema de información, aquí descubren a los piratas informáticos que ingresan sin consentimiento de la organización, para plagiar información o modificarla. (Baca Urbina , 2016)

- Complejidad: Los sistemas grandes y complejos aumentan la probabilidad de fallas.

- Familiaridad: El uso de códigos, software, sistemas operativos y / o hardware comunes y conocidos aumenta la probabilidad ataque.

- Conectividad: Más conexiones físicas, privilegios, puertos, protocolos y servicios, y el tiempo en el que cada uno de ellos es accesible aumenta la vulnerabilidad.

- Defectos de administración de contraseñas: El usuario de la computadora usa contraseñas débiles.

- Defectos fundamentales en el diseño del sistema operativo: El diseñador del sistema operativo elige aplicar políticas que no son óptimas en la administración del usuario / programa.

- Búsqueda en el sitio web de Internet: Algunos sitios web de Internet pueden contener Spyware o Adware dañinos que se pueden instalar automáticamente en los sistemas informáticos.

- Errores de software: El programador deja un error explotable en un programa de software. Entrada de usuario no verificada: el programa asume que toda la entrada del usuario es segura.

Los Infocentros son centros de cómputos comunitarios, que aportan a la ciudadanía el acceso gratuito de las Tecnologías de Información y Comunicación, además de ofertar diversos cursos con el fin de erradicar la brecha tecnológica que aún existe en la sociedad. Brindan servicios tales como:

- Los tramites online.
- Ofrecen cursos y talleres para fomentar capacidades académicas
- Local para hacer reuniones o debates.
- Internet gratuito y uso de equipos informáticos.

CONCLUSIONES

El presente caso de estudio, tuvo como finalidad establecer en qué estado se encuentra, la seguridad de la red de datos del Infocentro de la parroquia Guare, del cantón Baba.

Es esencial tener en cuenta que la función de monitoreo de red debe ser una tarea continua y no solo ser considerada en alguna etapa de la implementación de una nueva solución de negocio.

El encargado del infocentro de Guare, debe estar debidamente capacitado para la correcta administración de la red, puesto que la mala configuración de algún dispositivo, puede provocar riegos en la seguridad de la red.

En lo que respecta a la herramienta utilizada en el presente caso de estudio, se puede concluir Nessus es una de las mejores herramientas para la detención y reparación de vulnerabilidades existentes en una Red, en comparación con otras herramientas, ya que Nessus posee más puglins destinados para el análisis de tráfico de red y sobre todo su facilidad de instalación y usabilidad.

BIBLIOGRAFÍA

Baca Urbina , G. (2016). *Introducción a la Seguridad Informática* . México: Ebook.

BANCAL, D., DUMAS, D., & PUCHE, D. (2015). *Seguridad informática - Hacking Ético.* Barcelona: Ediciones ENI.

Canonical Ltd. Ubuntu. (2019). *Canonical*. Obtenido de Ubuntu for desktops: https://www.ubuntu.com/desktop

Fernández, M. J. (2015). *MF1161_3 - Electrotécnia para instalaciones térmicas.* Madrid: Editorial Elearning, S.L.

Flores Rosa, M. A. (2014). *Windows Server 2012 R2.* Lima: Editorial Macro.

Gomes Veitte, A. (2014). *Enciclopedia de la seguridad Informatica 2a Edicion Actualizada.*

González, C. (2 de 10 de 2014). *Virus, Gusanos, Caballos de Troya y Spyware*. Obtenido de Prezi: https://prezi.com/0gtyjv4j7urp/virus-gusanos-caballos-de-troya-y-spyware/

Jalca Regalado, J. J., Castro Romero, V. F., Menéndez Azúa, M. D., Quimiz Murillo, L. R., Anzúles Parrales, G. R., Pilay Campozano, Y. H., & Pin Pin, Á. L. (2018). *REDES DE COMPUTADORAS.* Jipijapa: Área de Inovación y Desarrollo, S.L.

Kumar, H. (2014). *Learning Nessus for Penetration Testing.* Packt Publishing Ltd.

Marqués, G. (2016). *QoS en routers y switches Cisco.* Lulu.com.

Ríos Yáguez, J. (2014). *Técnicas y herramientas de análisis de vulnerabilidades.* Obtenido de http://oa.upm.es/32786/1/TFG_javier_rios_yaguez.pdf

Starinsky, R. W. (2016). *Maximizing Business Performance through Software Packages.* New York: CRC Press.

Universidad de San Carlos. (2014). *Seguridad de la Información. Segunda Cohorte del Doctorado en Seguridad Estratégica.*

ANEXOS

ANEXO I.

Entrevista al facilitador del Infocentro de la Parroquia Guare.

1. ¿Utiliza normas para la seguridad de información?

   a) Si
   b) No

2. ¿Cómo considera usted que se encuentra el nivel de seguridad de la red?

   a) Alta
   b) Media
   c) Baja

3. ¿Ha sido usted víctima de robos de información?

   a) Si
   b) No

4. ¿Cómo califica usted la cobertura y la señal WIFI?

   a) Buena
   b) Mala
   c) Regular

5. ¿Qué tipo de seguridad poseen las computadoras para evitar robos de información?

   a) Firewall
   b) Software de detección de malware
   c) Antivirus
   d) Ninguna

6. ¿Usted tiene conocimiento acerca de seguridad de información?

a) Si
b) No

7. ¿Conoce los riesgos a los que se presentan la organización al no tener las medidas necesarias en lo que respecta a la seguridad de información?

a) Si
b) No

Según esta entrevista, se pudo identificar que el facilitador del infocentro está poco capacitado en lo que seguridad informática de refiere.

ANEXO II.

Ficha de observación.

<table>
<tr><td rowspan="2">Ficha de Observación</td><td>Caso de Estudio: Vulnerabilidades de los Riesgos en el Tráfico de la Red Informática del Infocentro de la Parroquia "Guare"</td></tr>
<tr><td>Responsable: Herlinda Mosquera Sánchez</td></tr>
<tr><td>Fecha: 08 de enero de 2019

Hora: 14:30

Lugar: Infocentro de la Parroquia Guare, del Cantón Baba.</td><td>OBSERVACIÓN

El infocentro de Guare brinda servicios gratuitos a la comunidad como: acceso a internet, uso de computadoras, impresiones y cursos de diferentes temáticas.

Se observó una red LAN y cableado estructurado, 1 switch, 1 router, 10 máquinas clientes que dependen de un servidor local.

El cable es UTP categoría 6. Se usa una topología en Árbol, debido conectados desde al switch a los terminales, ya la salida al internet es por medio del router. Se notó que algunos cables se están deteriorando.

El servidor y los clientes son de marca Kypus. El servidor controla a las máquinas clientes los cuales usan la tecnología Thin client.

El servidor es doble Boot, con los sistemas operativos Windows Server y Ubuntu. Se pudo notar que sistema operativo Windows Server tiene el virus de Acceso directo.

Las maquinas clientes dependen de que el servidor esté encendido para que funcionen.

No se pudo encontrar más información usando esta técnica, para lo cual se procederá a hacer un testeo en la red. Se observó que algunos usuarios estaban usando las maquina cliente.</td></tr>
</table>

ANEXO III.

Herramienta Nessus

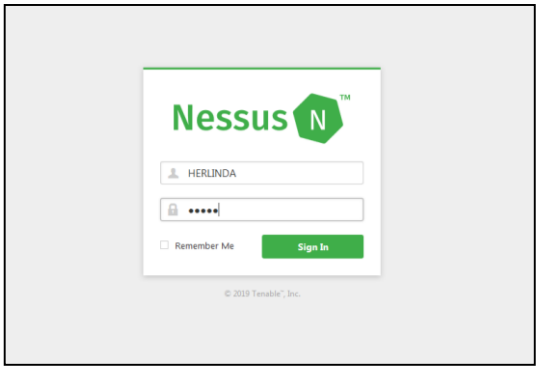


Fig. 1 Inicio de Sesión de Nessus

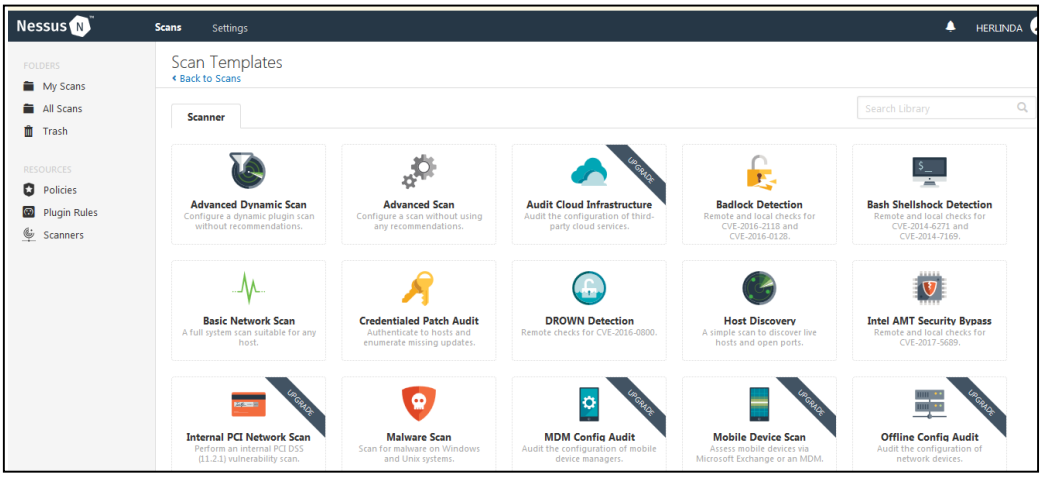


Fig. 2 Página de Inicio de Nessus

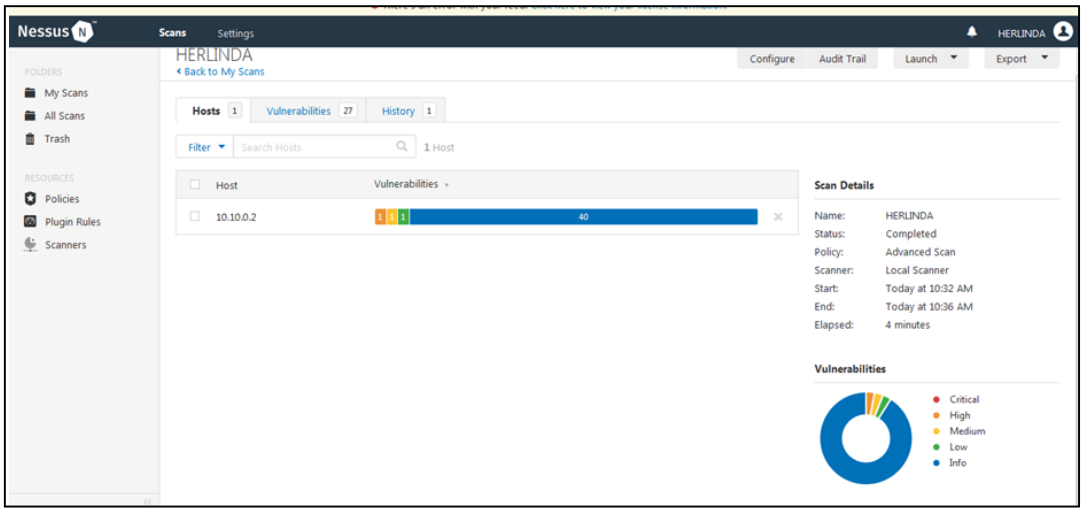


Fig. 3 Resultado de Escaneo

ANEXO IV.

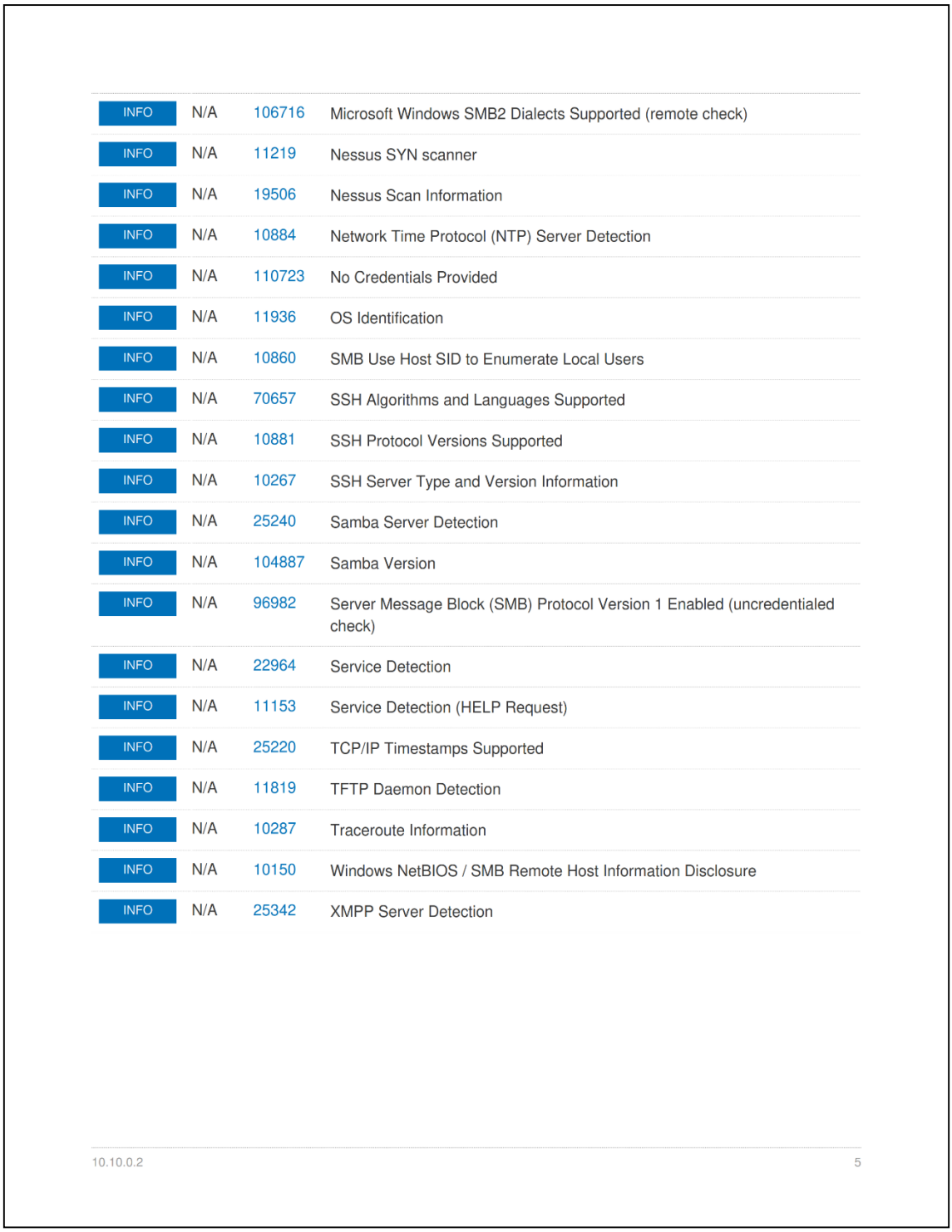
Resultado de Escaneo de Nessus

10.10.0.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	1	1	1	35

Vulnerabilities — Total: 38

SEVERITY	CVSS	PLUGIN	NAME
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
MEDIUM	5.0	57608	SMB Signing not required
LOW	3.3	10663	DHCP Server Detection
INFO	N/A	39520	Backported Security Patch Detection (SSH)
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
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	11819	TFTP Daemon Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	25342	XMPP Server Detection

10.10.0.2 5

En el resultado de este escaneo se muestra, que existen tres vulnerabilidades de estado alto, medio y bajo respectivamente.

La vulnerabilidad de estado alto, hace referencia que el servicio de compartir impresoras en la red no tiene privilegio, lo que quiere decir que cualquier usuario ajeno a

la institución que se conecte a red puede utilizar la impresora sin necesidad de autenticación.

La vulnerabilidad de estado medio representa que el mismo servicio de impresoras de red puede ser usado por un usuario que no tenga firma digital.

La vulnerabilidad de estado bajo, dice que se pudo detectar la información que del servicio de DHCP. Es decir que cualquier usuario ajeno a la institución tendrá acceso a la red.

Los otros 35 resultados son simple notificaciones que no tienen riesgo alguno en lo que a la seguridad se refiere, pero se deben tomar en cuenta ya que revelan información relevante de la red.

ANEXO V. Foto de la entrevista al Facilitador del infocentro de Guare.

Fig. 4 Entrevista al Facilitador

ANEXO VI. Oficio para solicitud de escaneo de la red.

Babahoyo, 28 de diciembre de 2018

Señor.-
Manuel Sacarías Litardo
FACILITADOR DEL INFOCENTRO DE GUARE
Presente.-

Des mis consideraciones:

Yo, Mosquera Sánchez Herlinda con cédula de ciudadanía # 1207764760, egresada de la carrera de **SISTEMAS**, en la **UNIVERSIDAD TÉCNICA DE BABAHOYO**, solicito a usted me autorice realizar un **ESTUDIO DE LAS VULNERABILIDADES DEL TRÁFICO DE RED**, en las instalaciones del infocentro que usted administra, con el objetivo de realizar un informe detallado de las posibles amenazas que podrían afectar a la red y como solucionarlas.

Dicho informe me servirá para sustentar mi trabajo de titulación, para la obtención del título de ingeniera en sistemas en la institución antes mencionada.

Por la atención que le brinde a la presente, le anticipo mis más sinceros agradecimientos.

Atentamente,

Herlinda Mosquera S.

Herlinda Mosquera Sánchez
EGRESADA DE LA CARRERA DE SISTEMAS

Infocentro
GUARE
LOS RIOS BABA

Fig. 5 Oficio dirigido al Facilitador del Infocentro de Guare

ANEXO VII. Oficio de respuesta para realizar el escaneo.

Babahoyo, 7 de enero de 2019

Señorita
Herlinda Mosquera Sánchez
EGRESADA DE LA CARRERA DE SISTEMAS
Presente.-

De mis consideraciones

Yo, Manuel Sacarías Litardo, en calidad de **FACILITADOR DEL INFOCENTRO DE GUARE**, y en respuesta del oficio enviado solicitándome utilizar las instalaciones del **INFOCENTRO** para realizar un **ESTUDIO DE LAS VULNERABILIDADES DEL TRÁFICO DE RED**, le autorizo a usted realice todas las tareas pertinentes para cumplir con el objetivo que usted muy cordialmente solicita.

El presente documento, la interesada podrá hacer de él, el uso que ella estime conveniente.

Atentamente,

Infocentro

Manuel Sacarías Litardo
FACILITADOR DEL INFOCENTRO DE GUARE

Fig. 6 Oficio expedido por el facilitador del Infocentro como respuesta para realizar el escaneo de la red