UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2017 – MARZO 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE

“INGENIERO EN SISTEMAS”

TEMA:

VULNERABILIDADES EN LA SEGURIDAD DE LA RED DE DATOS DE LA TIENDA SATELITE ARTEFACTA MONTALVO-2040.

EGRESADO:

XAVIER VICENTE MORETA GARCIA.

TUTOR:

ING. HUGO GUERRERO TORRES, MGRT.

AÑO:

2018

Introducción

Hoy día con el avance de la tecnología las redes son de mucha importancia ya que es por donde se transmite la información de manera diaria dentro de una empresa. Artefacta es una empresa comercial de electrodomésticos que cuenta con 98 tiendas a nivel nacional que pertenece al grupo unicomer, teniendo en cuenta que todas las tiendas conectadas entre sí con la finalidad de mejorar el servicio al cliente.

Desde sus inicios la compañía abrió dos tiendas en el país, una en Quito y otra en Guayaquil. En el transcurso de los años la empresa ya contaba con la proveeduría de las principales marcas nacionales e importadas. Como toda empresa innovadora decide extender su línea de productos hacia Motos y celulares, logrando así ser una de las primeras cadenas que abrió un canal de venta diferente para estos productos. Continuando con el avance de las nuevas tecnologías la empresa incursiona en la venta de computadores y portátiles, siendo hoy en día una de las líneas de mayor crecimiento de la compañía. (grupounicomer.com, 2018)

Para este estudio de caso se ha realizado la verificación de la TIENDA SATÉLITE ARTEFACTA MONTALVO-2040, ubicada en el cantón MONTALVO av. 25 de abril provincia de LOS RIOS, que tiene el sistema comercial (software) ARTEFACTA S.A MONTALVO-2040 y así encontrar las vulnerabilidades que pueden convertirse en una amenaza a la seguridad de la información.

El objetivo de esta investigación (estudio de caso) es encontrar las vulnerabilidades de la red y lograr la administración eficiente de las herramientas tecnológicas para la protección de la información dentro de la TIENDA SATELITE ARTEFACTA MONTALVO-2040, para lograr esto vamos a plantear como usar las normas de seguridad de forma correcta y así tener un óptimo funcionamiento de la red.

Desarrollo

Con el avance de la tecnología las empresas tienen su información en base de datos por lo tanto es muy importante encontrar las vulnerabilidades que pueden tener la red y a qué situaciones puede estar expuesta, antes de que otra persona lo haga de manera ilícita y que pueda robar información valiosa, para esto se debe hacer una investigación de manera profunda y buscar la solución como evitar esta vulnerabilidad de la red.

Las Vulnerabilidad de software **e**stá relacionado con los accesos indebidos a los sistemas informáticos sin el conocimiento del usuario o del administrador de red. Por ejemplo; la mala configuración e instalación de los programas de computadora, pueden llevar a un uso abusivo de los recursos por parte de usuarios mal intencionados. Los sistemas operativos son vulnerables ya que ofrecen una interfaz para su configuración y organización en un ambiente tecnológico y se realizan alteraciones en la estructura de una computadora o de una red. (Fong, 2015)

El proceso de recolección de información se realizará en base a la observación directa, por medio de una entrevista dirigida al supervisor de la tienda, una encuesta aplicada al personal que labora dentro de tienda con la finalidad de obtener información del funcionamiento de la red y así detectar los problemas donde la red es vulnerable.

Por medio de la observación directa se pudo constatar el equipamiento informático con que cuenta la tienda, todos los equipos son de marca hp con una memoria de 8gb instalados un sistema operativo Windows 7, con lo que respecta al tipo de red con que cuenta la tienda es una red de área local (LAN). También existen puntos de acceso a la red que se conectan a las computadoras.

Se realizó una entrevista a las personas más importantes dentro de la tienda como son el supervisor o jefe de tienda y el cajero que son los que tienen más privilegios al manejar los recursos de la red. Según el análisis una vez entrevistadas estas personas tenemos como resultado que el 50% dice que si ha existido robo de información.

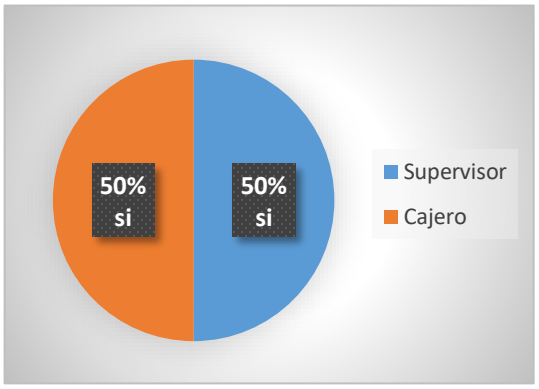

Figura 1: Existe robo de la información en la tienda.
Autor: Xavier Moreta

Según el análisis de que si existe normas de seguridad tenemos que solo el 25% dice que no y el 75% dice que sí.

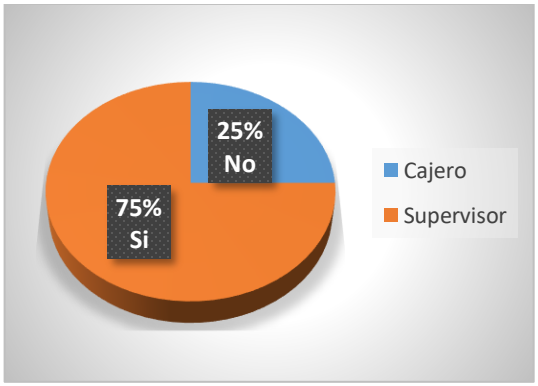

Figura 2: Existe normas de seguridad en la tienda
Autor: Xavier Moreta

Según el análisis de que si ha tenido problemas en la red de la tienda satélite artefacta montalvo-2040 los entrevistados dijeron que sí.

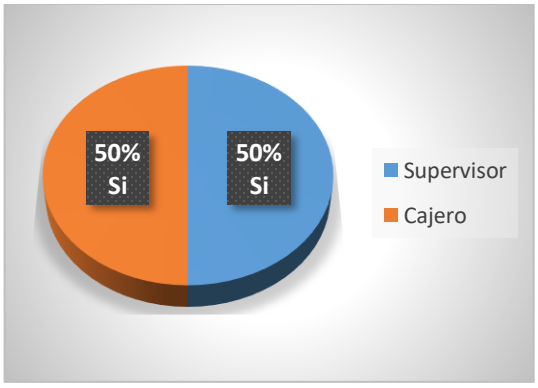

Figura 3: Problemas en la red de la tienda.
Autor: Xavier Moreta

Al hacer el análisis de que si se han dado acceso a la red de forma remota o externa a la tienda notamos que las dos personas dijeron que sí, obteniendo como resultado el 100%.

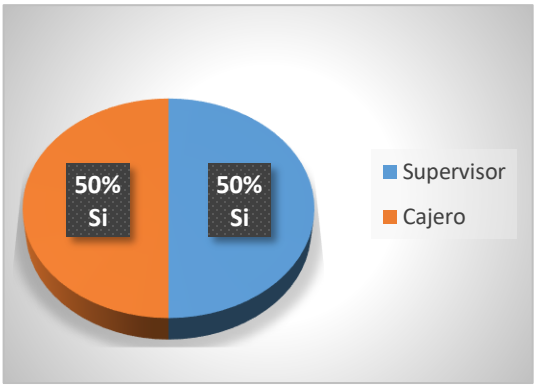

Figura 4: Acceso a la red de forma remota.
Autor: Xavier Moreta

Cuando se hiso el análisis que si se mantiene actualizados antivirus y otro software las respuestas fueron en un 50% que no d parte del cajero y el 50% de parte del supervisor.

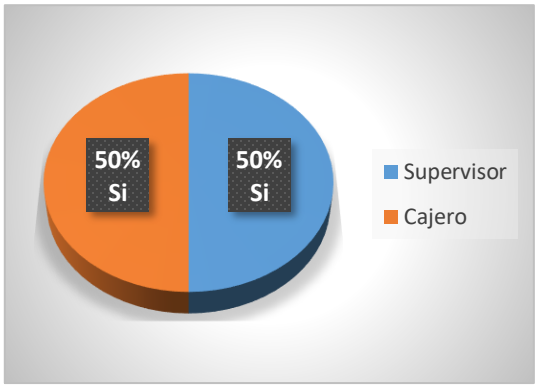

Figura 5: Actualizaciones de software.
Autor: Xavier Moreta

Una vez realizado un análisis profundo de las preguntas de entrevista note como existen vulnerabilidades en un 80%, esto dio paso a la investigación de este caso para buscar una solución adecuada a estos problemas de seguridad y disminuir las debilidades.

La infraestructura de red actual de la TIENDA SATÉLITE ARTEFACTA-2040 es la siguiente que mostramos en la figura 6 que muestra el estado actual de la red. Que está compuesta

por un switch que forma una red de área local y conectada un servidor computadores que son el usuario de caja, usuario de ventas 1, usuario de ventas 2 y a un administrador jefe de tienda.

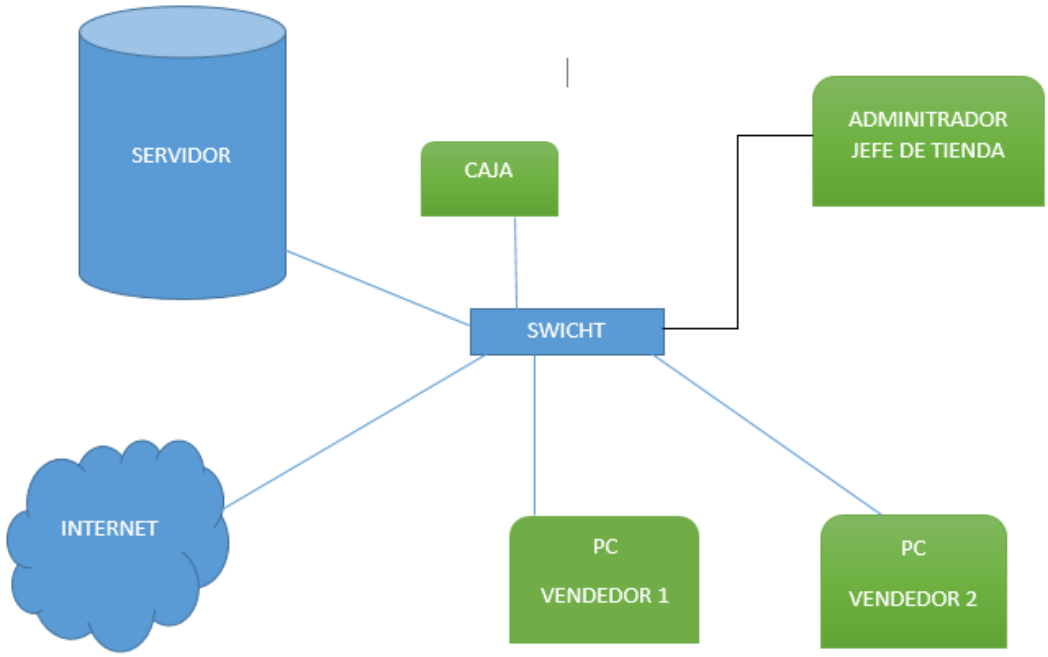

Figura 6. Estado actual de la Red de la Tienda Satélite Artefacta Montalvo 2040
Autor: Xavier Moreta

Dentro de la TIENDA SATÉLITE ARTEFACTA MONTALVO-2040 existe el SISTEMA COMERCIAL ARTEFACTA S.A MONTALVO-2040 que cumple muchas funciones como de ventas, caja y jefe de tienda uno de los problemas en la seguridad es que un usuario puede entrar a otro usuario de manera fácil ya que las contraseñas son de fácil acceso y no cuenta con una debida distancia de las máquinas de un vendedor a otro por lo cual pueden visualizar sus claves, esto hace que sea vulnerable la red para que puedan acceder personas ajenas a la empresa.

Cuando hablamos del término contraseñas fácil hacemos referencia a que no cumple con la los parámetros adecuados para que sea una clave segura, entonces es aquí donde nos preguntamos porque son fáciles cuantos caracteres o números contienen. Al realizar una investigación más profunda de los usuarios dentro de la tienda a las personas que trabajan ahí notamos que las contraseñas de acceso son números de cedula, nombres o los primeros 5 dígitos del teclado.

Para verificar si las contraseñas cumplen las debidas normas de seguridad se ha utilizado un software comprobador de contraseñas.

Aquí en la figura 7 haciendo el uso del software se realizó la prueba de una contraseña del cajero de la tienda, teniendo como análisis el uso de su primer nombre y el primer digito del teclado obteniendo como resultado una contraseña débil del 24% que no cumple ni los requerimientos mínimos de seguridad.

PARKING DEL DOMINIO

Prueba tu Contraseña		Requerimientos mínimos
Contraseña:	wilmer1	• Tamaño mínimo de 8 caracteres • Contener al menos 3-4 de las siguientes cosas: - Letras en Mayúsculas - Letras en Minúsculas - Números - Símbolos
Ocultar:	☐	
Resultado:	24%	
Complejidad:	Weak	

Adiciones		Tipo	Ratio	Contador	Bonos
✗	Número de Caracteres	Fijo	+(n*4)	7	+ 28
✗	Letras Mayúsculas	Cond/Incr	+((len-n)*2)	0	0
✓	Letras minúsculas	Cond/Incr	+((len-n)*2)	6	+ 2
✓	Números	Cond	+(n*4)	1	+ 4
✗	símbolos	Fijo	+(n*6)	0	0
✗	Mitad Números o símbolos	Fijo	+(n*2)	0	0
✗	Requerimientos	Fijo	+(n*2)	2	0
Deducciones					
✓	Solo Letras	Fijo	-n	0	0
✓	Solo Números	Fijo	-n	0	0
✓	Caracteres Repetidos (No sensible)	Incr	-(n(n-1))	0	0
✓	Letras Mayúsuculas consecutivas	Fijo	-(n*2)	0	0
!	Letras Minúsculas consecutivas	Fijo	-(n*2)	5	- 10

Figura 7. Comprobador de contraseñas del cajero
Autor: Xavier Moreta

En la figura 8 se muestra como la contraseña de un agente de ventas es su cedula, el software hace un análisis del 12% que significa muy débil por lo tanto se encontró evidencias de 10 contraseñas utilizadas el 60% son inadecuadas.

Para esto se sugiere la utilización de una letra mayúscula, una letra minúscula, símbolos, números, un cierto número de caracteres, también se califica los caracteres repetidos, mitad de número y símbolos.

PARKING DEL DOMINIO

Prueba tu Contraseña		Requerimientos mínimos
Contraseña:	1207348571	• Tamaño mínimo de 8 caracteres • Contener al menos 3-4 de las siguientes cosas: - Letras en Mayúsculas - Letras en Minúsculas - Números - Símbolos
Ocultar:	☐	
Resultado:	12%	
Complejidad:	Very Weak	

Adiciones		Tipo	Ratio	Contador	Bonos
✓	Número de Caracteres	Fijo	*+(n*4)*	10	+ 40
✗	Letras Mayúsculas	Cond/Incr	*+((len-n)*2)*	0	0
✗	Letras minúsculas	Cond/Incr	*+((len-n)*2)*	0	0
✓	Números	Cond	*+(n*4)*	10	0
✗	símbolos	Fijo	*+(n*6)*	0	0
✓	Mitad Números o símbolos	Fijo	*+(n*2)*	8	+ 16
✗	Requerimientos	Fijo	*+(n*2)*	2	0
Deducciones					
✓	Solo Letras	Fijo	*-n*	0	0
!	Solo Números	Fijo	*-n*	10	- 10
!	Caracteres Repetidos (No sensible)	Incr	*-(n(n-1))*	4	- 4
✓	Letras Mayúsuculas consecutivas	Fijo	*-(n*2)*	0	0
✓	Letras Minúsculas consecutivas	Fijo	*-(n*2)*	0	0

Figura 8. Comprobador de contraseñas de un agente de ventas
Autor: Xavier Moreta

De esta forma como demostramos en la figura 9 mediante el software una contraseña muy fuerte obteniendo una calificación del 100% es así como se deberían establecer todas las contraseñas para una mayor seguridad de la información.

PARKING DEL DOMINIO

Prueba tu Contraseña		Requerimientos mínimos
Contraseña:	Wm-10.Artefact	• Tamaño mínimo de 8 caracteres • Contener al menos 3-4 de las siguientes cosas: - Letras en Mayúsculas - Letras en Minúsculas - Números - Símbolos
Ocultar:		
Resultado:	100%	
Complejidad:	Very Strong	

Adiciones		Tipo	Ratio	Contador	Bonos
	Número de Caracteres	Fijo	*+(n*4)*	14	+ 56
	Letras Mayúsculas	Cond/Incr	*+((len-n)*2)*	2	+ 24
	Letras minúsculas	Cond/Incr	*+((len-n)*2)*	8	+ 12
	Números	Cond	*+(n*4)*	2	+ 8
	símbolos	Fijo	*+(n*6)*	2	+ 12
	Mitad Números o símbolos	Fijo	*+(n*2)*	4	+ 8
	Requerimientos	Fijo	*+(n*2)*	5	+ 10
Deducciones					
	Solo Letras	Fijo	*-n*	0	0
	Solo Números	Fijo	*-n*	0	0
	Caracteres Repetidos (No sensible)	Incr	*-(n(n-1))*	4	- 4
	Letras Mayúsuculas consecutivas	Fijo	*-(n*2)*	0	0
	Letras Minúsculas consecutivas	Fijo	*-(n*2)*	6	- 12

Figura 9. Propuesta de los requerimientos que debería tener una contraseña para que sea segura.
Autor: Xavier Moreta

También como medio de protección podemos utilizar un (IDS) Sistema de detección de intrusos este programa sirve para detectar el acceso no autorizado a la red por el administrador de personas con intenciones de espiar o sustraer información. Nos preguntamos porque utilizar un IDS y la respuesta luego de hacer un estudio es para evitar el robo de información de un usuario accediendo de otro usuario esto quiere decir que si un vendedor o agente de ventas quiere robar una información sin dejar rastro lo hace por medio de otro usuario de otro vendedor por lo que es recomendable utilizar un IDS software

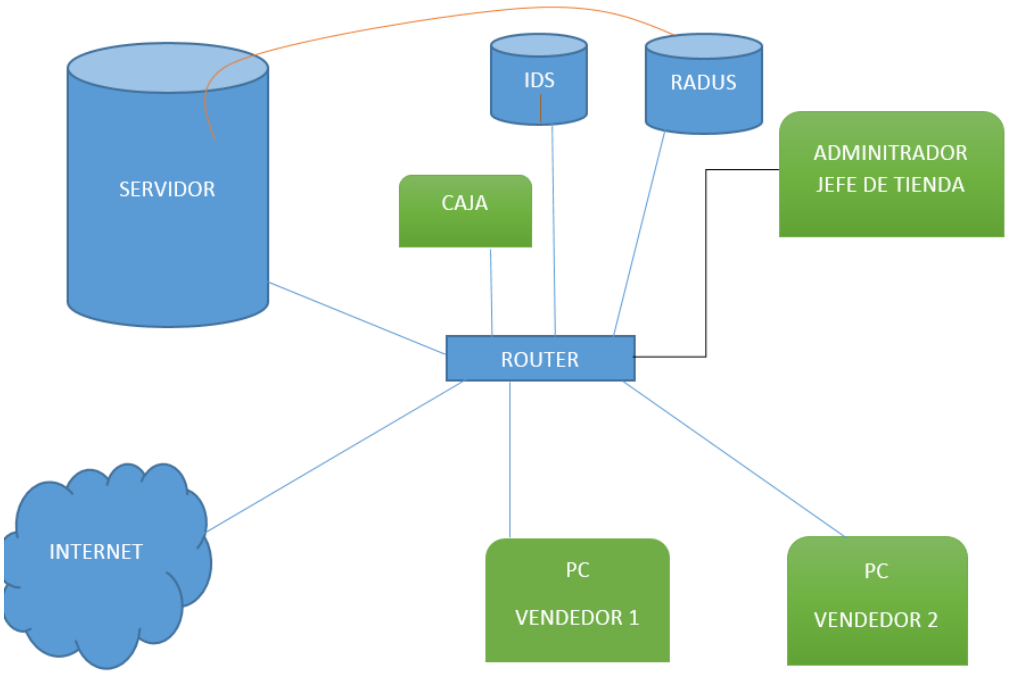

Figura 10. Propuesta de cambio de la Red de la Tienda Satélite Artefacta Montalvo 2040
Autor: Xavier Moreta

En la siguiente figura 10 lo que se propone es cambiar el switch por un router para mejorar la seguridad, adicional a eso agregar un servidor de autenticación RADIUS y sistema de detección de intrusos IDS para así reforzar la seguridad red.

El funcionamiento de estas herramientas se basa en un análisis de alto nivel del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico sino que también revisa el contenido y su comportamiento (Ecured.cu, 2018)

Lo primero que debemos saber antes de nada es que es un servidor RADIUS se encarga de gestionar el acceso a las redes. Es utilizado principalmente por los proveedores de servicios de internet para gestionar el acceso a internet de sus clientes.

Las funciones de un servidor RADIUS se resumen con las siglas "AAA" que significan: Autenticación, Autorización y Anotación. Los creadores de servidores no reciben conexiones

directas de los clientes sino que interactúan con las aplicaciones del cliente en otros equipos de la red. (group, 2016).

Autenticación: determina que una cuenta de usuario o equipo es quien dice ser.

Autorización: determina los permisos y privilegios de una cuenta autenticada.

Anotación: Registro de actividad. Llevar el control de quien hace el uso una actividad de un usuario.

Un problema de seguridad también está en si se conecta una memoria externa a la maquina no tiene una protección, hubo un caso el pasado 24 de noviembre del 2017 en alguien accedió a extraer información sobre los precios de viernes negro antes que sean lanzados a los clientes y de esta forma la competencia pudo armar una misma estrategia de marketing que ocasionó pérdidas de gran valor.

Teniendo en cuenta que la información es la parte más importante dentro de una empresa, por esto una vez realizado de cada equipo se confirmó que no tiene un software que limite el acceso a dispositivos USB.

Rob Fuller, ingeniero en seguridad, ha descubierto que el sistema operativo como Windows son propensos a robos de credenciales cuando están bloqueados con sesiones activas, ya que el ordenador mantiene activos muchos de los procesos en donde se tiene registrado una firma digital del usuario, incluso la conexión de red. (Xataka, 2017)

Para limitar el acceso de dispositivos USB se propone utilizar un software que bloquee los puertos de todo tipo de dispositivos externos y que no se pueda desactivar por cualquier usuario sino solo por el administrador para dar un acceso privilegiado. Después de haber realizado un estudio de diferentes software el más recomendables es Renovable Access Tool que limita el acceso a memorias USB además tienes otras opciones que solo puede realizar el administrador como de autorizar el acceso algún dispositivo.

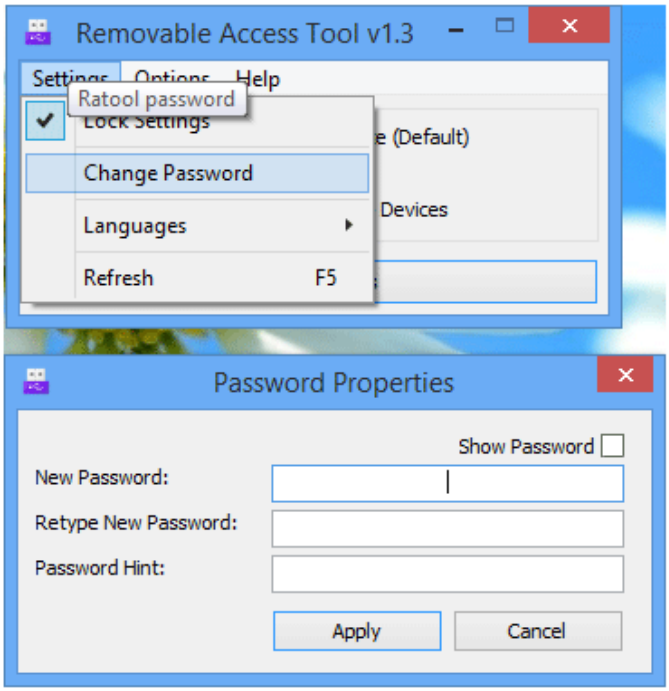

Figura 11. Configuración de clave acceso del administrador
Autor: Xavier Moreta

Acceso de personas no autorizadas por falta de actualización de las aplicaciones de software necesarias es aquí donde se revisó cada equipo y se comprobó que no se actualizan las aplicaciones de forma continua tales como antivirus caducados cortafuegos desactivados, para esto se propone comprar un software McAfee que va a mantener a los equipos con una seguridad reforzada contra amenazas.

También se recomienda mantener el computador libre de archivos que son basura para esto se propone instalar CCleaner que detecta y limpia archivos que ocupan espacio en el disco inútilmente, obteniendo como resultado que tu equipo funcione de manera más rápida.

A continuación demostramos en la figura 12 como el software McAfee nos brinda múltiples servicios de seguridad y también como nos muestra un cuadro de dialogo advertencia que alguien se quiere conectar al equipo, además podemos revisar el historial de actividades.

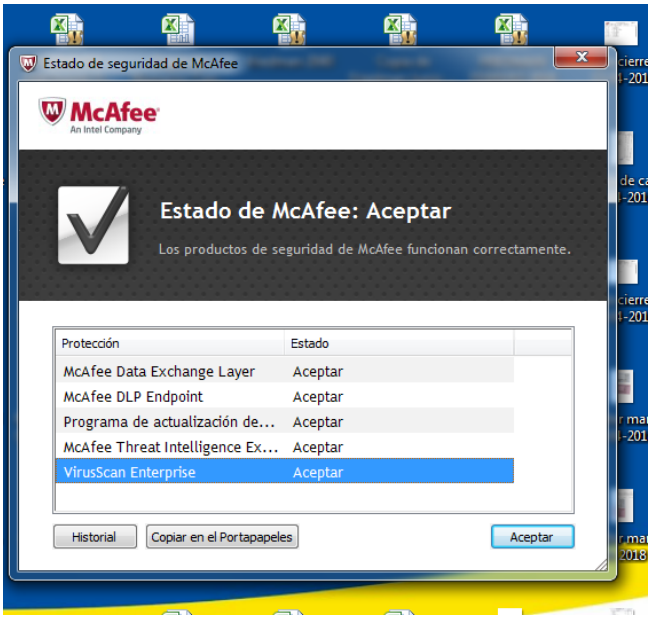

Figura 12. Configuración McAfee.
Autor: Xavier Moreta

En la figura 13 se hizo la prueba conectando un dispositivo externo y podemos observar como el software DLP prevención perdida de datos nos da un aviso y evita que se conecte sin autorización.

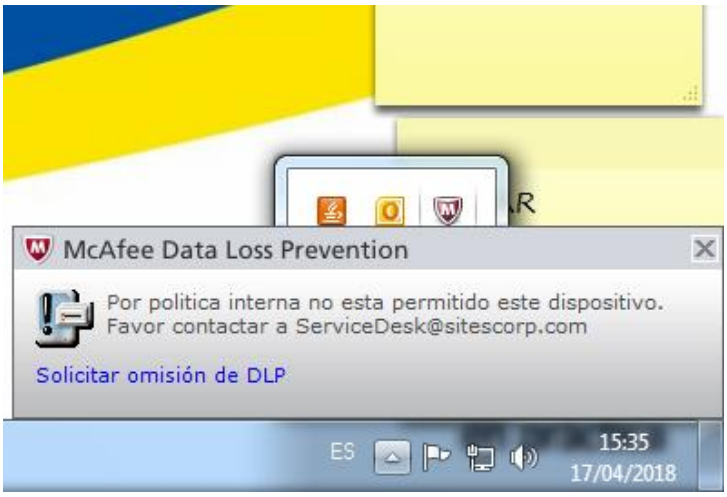

Figura 13. Advertencia McAfee.
Autor: Xavier Moreta

Conclusiones

1. Debido a que las contraseñas no cumplen con los requerimientos de seguridad necesarios, 60% de las claves utilizadas, se propone de la utilización de un servidor RADIUS para evitar la pérdida de información. También la utilización de normas para la creación de contraseñas adecuadas respetando las indicaciones de caracteres no repetidos, utilización de caracteres alfanuméricos, entre otros de manera que sean muy difícil de descifrar.

2. Después de haber comprobado que existió el robo de información de la tienda y no existe una limitación de acceso a los puertos USB se propone para tener más seguridad la utilización del software Removable Access Tool para el bloqueo de puertos USB en los equipos de los usuarios.

3. Para evitar esos problemas de los equipos que no cumplen con las funciones adecuadas y están expuestos a virus y ataques se propone tener software actualizado, así evitaremos la perdida de información, tales como precios promociones y lo más importante para la tienda que son los clientes.

Referencias

access.redhat.com. (31 de 01 de 2018). *access.redhat.com*. Obtenido de access.redhat.com: https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/sect-Security_Guide-Common_Exploits_and_Attacks#tabl-Security_Guide-Common_Exploits_and_Attacks-Common_Exploits

Ecured.cu. (11 de Enero de 2018). *Ecured.cu*. Obtenido de Ecured.cu: https://www.ecured.cu/IDS

Fong, R. (2015). Amenazas y Vulnerabilidades a la Seguridad Informatica . En R. Fong, *Amenazas y Vulnerabilidades a la Seguridad Informatica* (pág. 250). España: Panoram.

group, L. (09 de 11 de 2016). *www.geniolandia.com*. Obtenido de www.geniolandia.com: https://www.geniolandia.com/13167824/que-es-un-servidor-radius

grupounicomer.com. (01 de 01 de 2018). *grupounicomer.com*. Obtenido de grupounicomer.com: http://www.grupounicomer.com/cadenas/artefacta/

netcloudengineering.com. (04 de 12 de 2017). *netcloudengineering.com*. Obtenido de netcloudengineering.com: https://netcloudengineering.com/ciberseguridad-amenaza-vulnerabilidad/

Sánchez., B. G. (10 de 10 de 2016). *techclub.formaciontajamar.com*. Obtenido de Microsoft MCSE Private Cloud: https://techclub.formaciontajamar.com/instalacion-y-para-que-sirve-un-servidor-radius/

Tenenbaum, A. S. (2014). Red de computadoras . En A. S. Tenenbaum, *Red de computadoras* (pág. 819). mexico: PEARSON.

Xataka. (2017). Seguridad dispositos UBS. En Xataka, *Seguridad dispositos UBS* (pág. 115). madrid: Xataka.

Anexos

Preguntas de Entrevistas

1. ¿Ah tenido problemas de robo de información dentro de la tienda?
2. ¿Existen normas de seguridad de la información en la tienda satélite artefacta montalvo-2040?
3. ¿Qué problemas usted ha tenido en la red de la tienda satélite artefacta montalvo-2040?
4. ¿Supone usted que se han dado acceso a la red de forma remota o externa a la tienda?
5. ¿Mantiene actualizados antivirus y otro software para prevenir daños en sus equipos?