Mayo

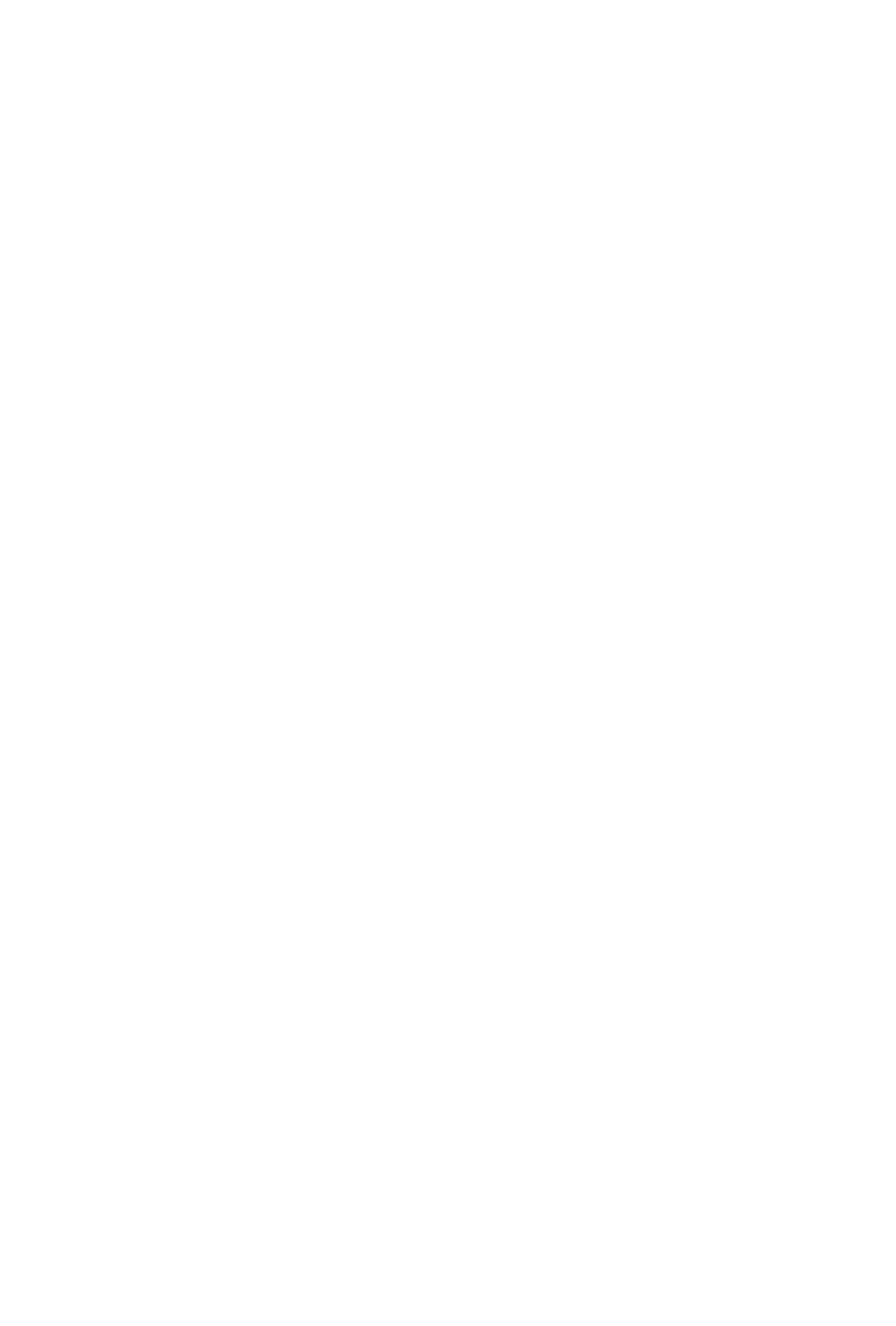
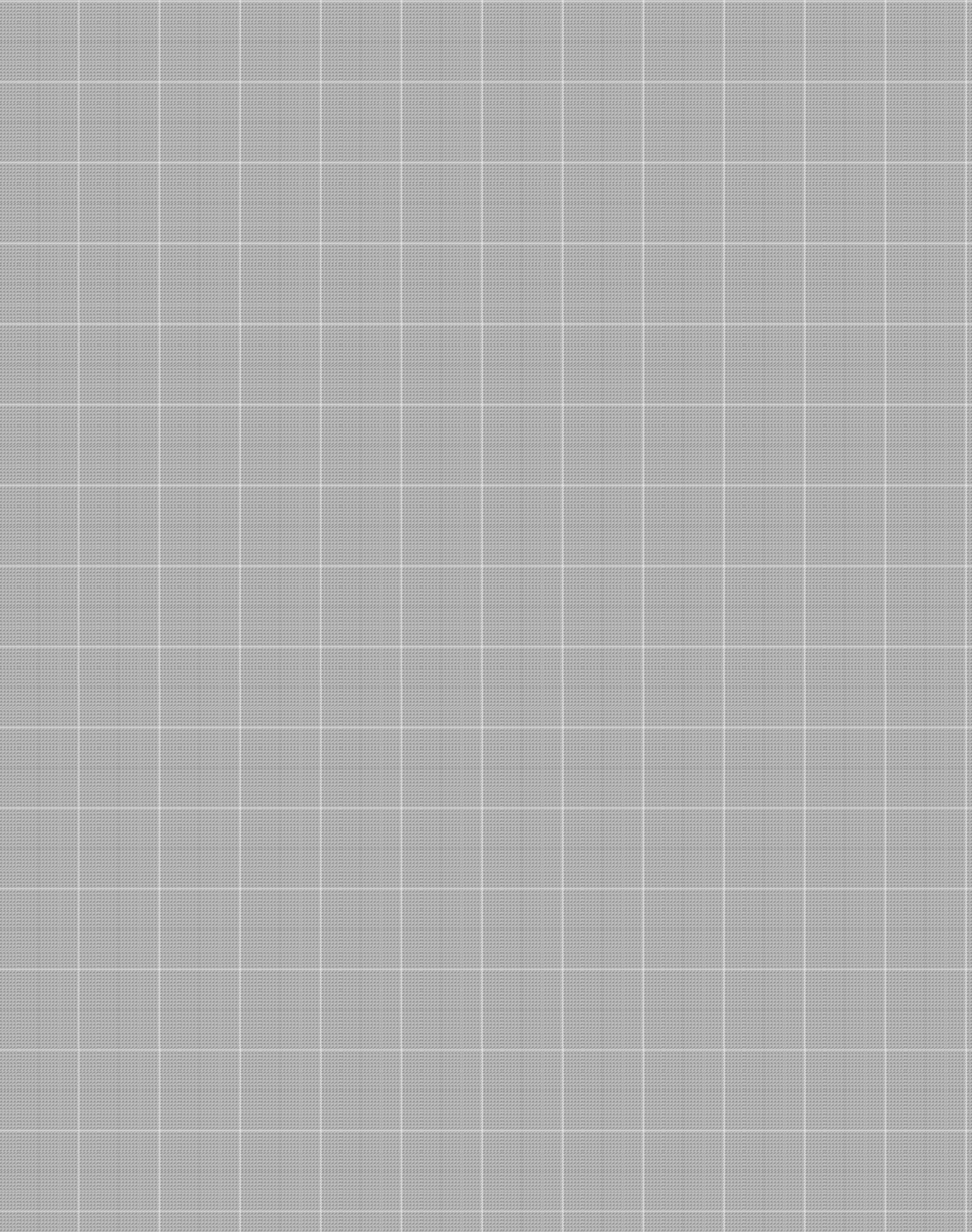
2018

Evaluación de

Seguridad

Pruebas de Penetración Kali Linux

Elaborado por Juan Felipe Marín y stephany Ramírez



A. Lozano y Rafael Gil =)

Windows XP

Mayo 2018

**Índice**

1. [Resumen Ejecutivo 5](#_TOC_250028)
   1. [Contexto 5](#_TOC_250027)
      1. [Objetivo 5](#_TOC_250026)
      2. [Pruebas realizadas 6](#_TOC_250025)
      3. [Resultados de la prueba de penetración 6](#_TOC_250024)
      4. [Escala de Medición 7](#_TOC_250023)
   2. [Resultados 8](#_TOC_250022)
      1. [Principales Fortalezas 8](#_TOC_250021)
      2. [Principales Vulnerabilidades Externas 9](#_TOC_250020)
      3. [Conclusiones 12](#_TOC_250019)
      4. [Implicaciones 13](#_TOC_250018)
   3. [Plan de Mitigación 14](#_TOC_250017)
2. [Introducción 15](#_TOC_250016)
   1. [Consideraciones Generales 15](#_TOC_250015)
   2. [Acerca de Proveedor 15](#_TOC_250014)
   3. [Herramientas y Técnicas 15](#_TOC_250013)
   4. [Políticas y Procedimientos 16](#_TOC_250012)
3. [Bases de la Prueba de Penetración 18](#_TOC_250011)
   1. [Objetivo de la prueba 18](#_TOC_250010)
   2. [Meta de la prueba 18](#_TOC_250009)
   3. [Estrategia 18](#_TOC_250008)
   4. [Metodología 18](#_TOC_250007)
   5. [Especificación de prueba 19](#_TOC_250006)
      1. [Objetivos Específicos 19](#_TOC_250005)
   6. [Pruebas Realizadas 20](#_TOC_250004)
      1. [Penetración por Red Externa 20](#_TOC_250003)
      2. [Expansión de Influencia 20](#_TOC_250002)
4. [Resultados de la prueba 21](#_TOC_250001)

Página 2

* 1. [Escala de Medición 22](#_TOC_250000)
  2. Resultados 23
  3. Principales Fortalezas Externas 24
  4. Principales Vulnerabilidades Externas 24
     1. Protocolos en texto claro - Operación Parcial – Conocimiento en Seguridad 24
     2. Validación de Entradas y Manejo de Errores Operación – Experto en Tecnología 25
     3. Inyección SQL - Administración – Conocimientos en Seguridad 26
  5. Conclusiones 28
     1. Implicaciones 29
  6. Plan de Mitigación 30
     1. Protocolos en texto claro 31
     2. Manejo de Errores 32
     3. Inyección SQL 32

1. Detalle Técnico 35
   1. Visibilidad externa 35
      1. Información Pública 35
      2. Recopilación de Información en Internet 38
      3. Dominios 39
      4. Exploración 39
   2. Configuración General Externa 43

5.2.1 200.xx.xx.80 43

5.2.2 200.xx.xx.xx 45

5.2.3 200.xx.xx.xx 47

5.2.4 201.159.142.138 ........................................................................................................... 49

5.2.5 201.xx.xx.xx 51

5.2.6 201.xx.xx.xx 53

5.2.7 200.xx.xx.xx 55

1. Screenshots 58
2. Anexos 59
   1. Actividades Post Pen Test 59

Página 3

* + 1. Cambiar todas las contraseñas 59



Página 4

# 1 Resumen Ejecutivo

Las pruebas de penetración tienen como objetivo analizar qué tan vulnerable es Windows XP a un ataque informático perpetrado desde otra maquina. Se analiza la seguridad desde el punto de vista de un atacante externo con acceso a Internet.

## 1.1 Contexto

### 1.1.1 Objetivo

Evaluar la preparación y que tan seguro es Windows XP para resistir y detectar un ataque sofisticado desde la red externa (Internet) de la máquina. Para esto se definieron varios escenarios externos que emulaban a un atacante externo desde Internet a través de una maquina kali linux.

#### Alcance

Se probó la seguridad desde internet hacia la red externa de Windows XP.

#### Objetivos Específicos

Se definieron varios objetivos externos que correspondían, principalmente, a toda la información y a la vulnerabilidad a los que están expuestos a Internet.

**Objetivos**

* Obtención de información
* Análisis de vulnerabilidades
* Enumeración de sistemas
* Explotación de vulnerabilidades
* Pos-Explotación de vulnerabilidades
* Evasión de medidas de seguridad
* Ataques contra credenciales



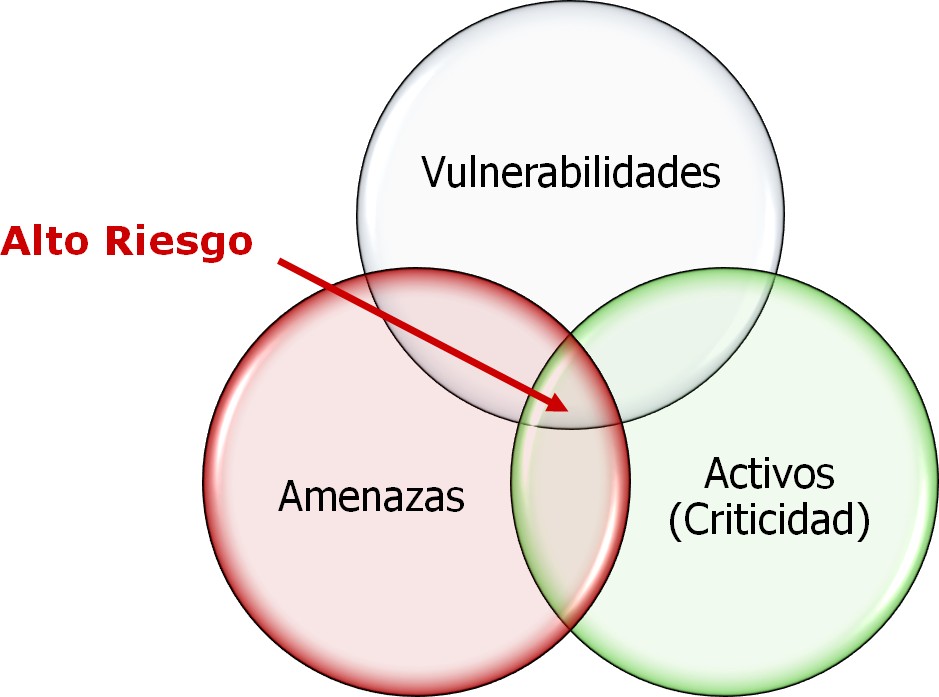
Página 5

### Pruebas realizadas

Las pruebas que se realizaron consistieron en: Ingresar desde una maquina kali linux a sistema operativo Windows xp, adivinar o romper contraseñas, descubrir y abusar vulnerabilidades, revisión del proceso de respuesta a incidentes, así como la intercepción de comunicaciones.

Estas pruebas son elaboradas desde diferentes capas de la infraestructura que incluyen software propietario, servidores de base de datos, sistemas operativos, dispositivos de red, consolas de administración y diferentes puntos y formas de conexión.

### Resultados de la prueba de penetración

Los resultados de la prueba están divididos en tres categorías principales: Fortalezas, Vulnerabilidades y Recomendaciones. Estos resultados se midieron definiendo el nivel de seguridad y la probabilidad de un ataque.

El nivel de Acceso está basado en los privilegios que se pueden obtener, siendo los privilegios de administrador la mayor amenaza. La probabilidad de ataque está determinada por el perfil de atacante; mientras menos sofisticado sea el atacante para obtener privilegios y/o información crítica, la probabilidad de tener un ataque es mucho mayor. Uniendo estos dos

Página 6



Página 7

Factores y evaluando el nivel de criticidad de la información que se maneja, el nivel de riesgo puede ser calculado por la empresa.

### Escala de Medición

La escala que utilizamos para determinar el nivel de vulnerabilidad está basada en dos factores: el nivel de acceso y el perfil del atacante, como se describe a continuación:

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

## Resultados

El resultado qué a continuación se muestra está basado en una estadística que se lleva a cabo en Proveedor con los resultados de Hackeos Éticos que se han realizado a empresas semejantes y con un tamaño similar al de Windows XP.

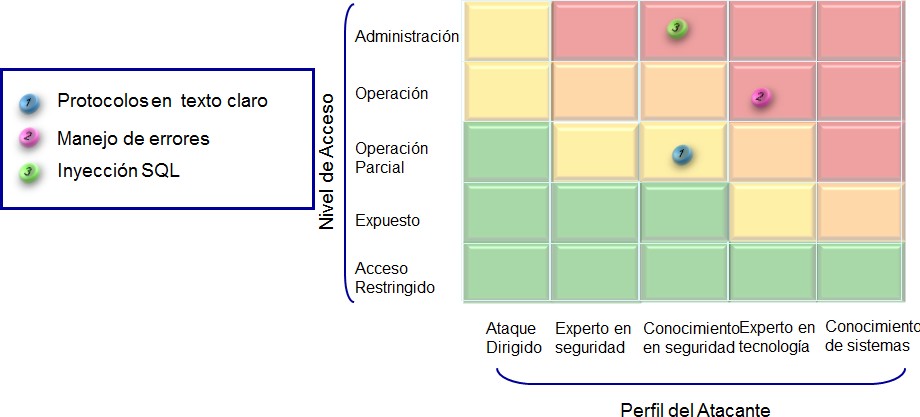


### Principales Fortalezas

* Los servidores expuestos a internet muestran una superficie de ataque reducida.
* El servidor de DNS no permite conocer su tabla de resolución de nombres.
* Los servicios SMTP en los servidores no permiten enviar correos electrónicos sin autenticación.
* Las contraseñas de los usuarios de las aplicaciones Web son almacenadas de forma cifrada en la base de datos.
* Los usuarios de bases de datos empleados por las aplicaciones tienen bajos privilegios.

Página 8

### Principales Vulnerabilidades Externas



**Protocolos texto claro**

Se identificaron protocolos de comunicación en texto claro, entre los que se encuentran: FTP y HTTP.

Todos estos protocolos envían tanto las contraseñas de usuario como todas las comunicaciones en texto claro, permitiendo a un atacante interceptar información sensible y comprometer las identidades de los usuarios legítimos.

Se encontró un servidor con el protocolo FTP habilitado lo cual puede representar una amenaza de intercepción de credenciales al ser usados.

Es posible acceder a los recursos de los sitios Web a través del protocolo inseguro HTTP colocando la ruta completa al recurso, evadiendo la redirección hacia el protocolo HTTPS; esto es debido a que únicamente la página de inicio de los sitios Web es la que ha sido redirigida al protocolo HTTPS. Esto puede ser utilizado por un usuario mal intencionado para interceptar información sensible, como credenciales de autenticación, de páginas de acceso, así como parámetros ocultos enviados por la aplicación.

**Manejo de errores**

A pesar que al ocurrir un error o una excepción relacionada con la validación de los parámetros de entrada la aplicación re direcciona al usuario a una página genérica de error, esta redirección no ocurre en todos los casos, principalmente en los errores de

Página 9

Bajo nivel en el servidor. Como por ejemplo un recurso no encontrado, o los errores provenientes de las Bases de Datos, los cuales son mostrados directamente en la aplicación o en el navegador.

Se pudo constatar la existencia de aplicaciones web que al suceder un error relacionada a la conexión o ejecución de consultas a la base de datos, muestran información detallada de la ocurrencia del mismo. Estas pantallas de error proporcionan a un usuario mal intencionado información importante para la comprensión a profundidad de la estructura de la base de datos, tipos de dato, tipo de información almacenada, así como versiones de software utilizado. Esto puede ser utilizado por un usuario mal intencionado para conseguir la extracción de información de la base de datos u obtener los detalles necesarios para identificar posibles vulnerabilidades al servidor de Bases de Datos.

**Inyección SQL**

Se observó que las aplicaciones web no realizan una correcta validación de las entradas de datos. Las aplicaciones efectúan una validación basada en los caracteres para palabras, y números, sin embargo, esta validación no contempla parámetros como máximo número de caracteres, o caracteres especiales para las contraseñas.

Como consecuencia de la forma en la que los datos son validados se identificaron páginas web con entradas de datos vulnerables a la inyección de código SQL para la manipulación maliciosa de su comportamiento normal. En ellos existe una validación básica de los campos que son mapeados a consultas a la base de datos, la cual consiste principalmente en eliminar algunos caracteres empleados en las consultas SQL así como espacios en blanco. Sin embargo esta validación de datos no considera la inyección de cadenas de texto codificadas como caracteres HTML, los cuales son considerados como válidos en la aplicación, pero son convertidos a texto al ser enviados a la base de datos. Por ejemplo: la cadena de texto= “’or 1=1- “puede ser codificada cómo “%18%20%6f%72%20%31%3d%31%20%13%2d para evadir la validación del campo y ejecutar la consulta efectivamente.

Página 10

Este fallo permite extraer, modificar e incluso borrar información sensible de la base de datos que van desde: el nombre de la base de datos usada, el nombre del usuario



Página 11

de base de datos, el nombre del servidor, la versión de la base de datos, etc. hasta información de la estructura de la base de datos como: nombre de tablas, nombre de columnas o campos, descripción de campos, número de registros en una tabla, etc.

La situación más grave con esta vulnerabilidad es que permite a un atacante extraer los registros almacenados en cualquier tabla del servidor en la cual el usuario de la base de datos tiene al menos permisos de lectura.



Página 12

### Conclusiones

Haciendo referencia a la gráfica de comparativo con la industria se concluye que la red externa de Windows XP permite obtener hasta un nivel de acceso **Administración** y puede ser vulnerada por una persona con un perfil de **Conocimientos en Seguridad**

Existen puntos vulnerables de la red externa de Windows XP como:

* + - * Se encontraron protocolos de red en texto claro que envían los datos sin ningún tipo de cifrado como HTTP y FTP.
      * Las aplicaciones web no manejan adecuadamente la ocurrencia de errores por lo cual son mostradas al usuario exponiendo información sensible.
      * La inyección SQL permite extraer información sensible de las bases de datos.

Página 13

### Implicaciones

Para lograr un mayor entendimiento de las vulnerabilidades anteriormente descritas se presentan adicionalmente algunas de las implicaciones posibles, enfocándonos principalmente desde la perspectiva de un atacante externo con acceso a internet y que pretenda abusar de estos puntos vulnerables.

**Probabilidad Alta**

**Robo de información de clientes**

Debido a que es posible extraer registros de clientes de las páginas de Windows XP, es posible automatizar estas extracciones para obtener toda la información de clientes y cualquier otra información contenida en la misma base de datos. La probabilidad de sufrir un robo de información aumenta debido a que existen ya a distribución gratuita aplicaciones o frameworks para explotar las vulnerabilidades de inyección de SQL que automáticamente extraen los registros de las bases de datos.

**Probabilidad Media**

**Que sufran un ataque informático y no se den cuenta**

En el transcurso de las pruebas no se mantuvo un perfil encubierto y tampoco se intentó ser silencioso o cuidadoso con el tipo de pruebas que se hacían. El nivel de tráfico generado durante las pruebas fue aumentando conforme pasó el tiempo. A pesar de todo, no se nos fue reportada la actividad por parte de los responsables de sistemas y tampoco se tomaron medidas preventivas al respecto.

Página 14

## Plan de Mitigación

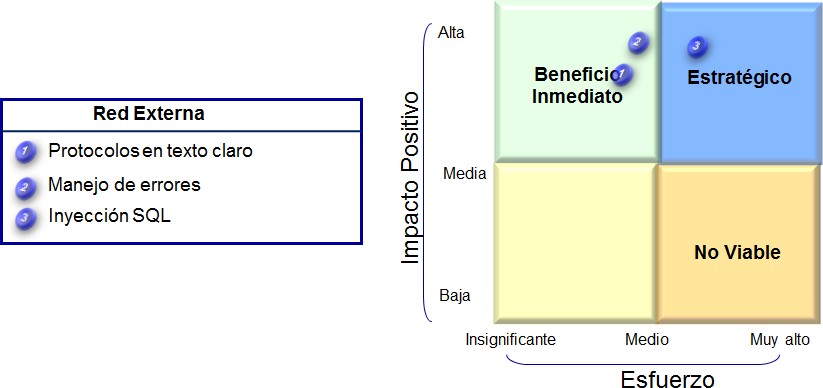
Para determinar un plan de mitigación se han priorizado las acciones requeridas de acuerdo a dos criterios: el impacto de las mejoras y el esfuerzo que se requiere.

En impacto se tomará 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 al Negocio – Percepción que el exterior tiene de la empresa. En esfuerzo se considerará:
* 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.

**Acciones Mitigantes y Mejoras Sugeridas**

Hay 2 grupos principales donde consideramos se deberá hacer un esfuerzo de corrección para mejorar la seguridad de la red externa de Windows XP:



# Introducción

## Consideraciones Generales

El presente documento contiene información sobre las vulnerabilidades y debilidades de la infraestructura informática de Windows XP que puede resultar sensible o confidencial. Se recomienda que se tomen precauciones especiales para mantener el estado confidencial de este reporte. Proveedor conserva de forma segura una copia de este documento para futura referencia.

Aun cuando Proveedor confía en haber identificado las principales vulnerabilidades de los sistemas objetivo, un estudio de esta naturaleza no puede garantizar la detección de la totalidad de las vulnerabilidades de la infraestructura informática de Windows XP. Los hallazgos y recomendaciones documentados en el presente reporte se realizaron con base en las tecnologías y vulnerabilidades conocidas al día de hoy. Las tecnologías y vulnerabilidades se modifican constantemente, por lo cual los riesgos y debilidades identificados en Windows XP y también pueden cambiar.

## Acerca de Proveedor

Proveedor es una empresa altamente especializada en el diagnóstico y corrección de problemas de seguridad informática. Nace como respuesta a una necesidad de las grandes empresas por garantizar la seguridad de su información. Esta necesidad surge recientemente por el crecimiento exponencial que ha habido en los ataques a empresas e instituciones. A través del tiempo Proveedor ha logrado reunir a uno de los grupos de expertos más prestigiados de México, al tiempo que ha trabajado para las principales empresas del sector comercial, industrial y financiero.

Proveedor valora por encima de todo la ética de sus consultores. Conscientes de que para ello es importante el medio en que se desenvuelve una persona, su edad y sus compromisos, se ha buscado en general que sean personas casadas y con hijos, adicional a que se les conozca con anterioridad y tengan referencias intachables.

## Herramientas y Técnicas

Los consultores de Proveedor se basan en metodologías de prueba que han sido revisadas y avaladas por la comunidad de seguridad informática para determinar si la red de Windows XP es susceptible de sufrir un ataque informático. Estas prácticas y técnicas de prueba han sido desarrolladas y refinadas constantemente para

Página 15

Representar las principales amenazas a las que se encuentra expuesta una empresa con presencia en Internet en la actualidad.

Proveedor utiliza diversos productos de escaneo que son reconocidos como estándares de la industria, como Retina (eEye), CANVAS (ImmunitySec), Nessus, N- Stealth, Wikto y otros. Se utilizan 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 se utiliza una variedad de herramientas reconocidas como estándares en la industria tales como, NMAP, SAM Spade, Solarwinds, hping2, metasploit, hydra, l0phtcrack, John-the-ripper, brutus, psexec y muchas otras hechas por profesionales de seguridad para profesionales de seguridad. Los consultores de Proveedor han desarrollado técnicas, scripts y programas en casa 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 Proveedor asumen 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 Proveedor tienen su base en “Open Source Security Testing Methodology Manual” una metodología aprobada y publicada por ISECOM.

## Políticas y Procedimientos

Las políticas en las cuales Proveedor se basa para proporcionar sus servicios son:

* + - En todas las pruebas que se hacen se busca no interferir ni afectar los sistemas ni 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 sabemos de antemano 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

Página 16

* + - * Con consentimiento expreso por parte del cliente
      * En una ventana de tiempo específica que no afecte la operación

Página 17

* + - * 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 de este reporte
    - En apego a la ley, respetamos las comunicaciones privadas y no se leerá ni monitoreará correos electrónicos, llamadas sobre IP ni navegación personal en Internet. Sólo se revisará información que parezca ser por su nombre o ubicación información relacionada a la empresa o sus actividades.
    - Toda la información derivada de la prueba será tratada como altamente confidencial y será destruida al término de la prueba.
    - No se copia información de la empresa a equipos de Proveedor, sólo se toman screen shots de las vulnerabilidades y se registra la información de contraseñas mencionadas anteriormente.
    - En el caso que haya información confidencial a la que se deseaba que no se tuviese acceso, se deberá haber especificado por escrito previo a la prueba.

# Bases de la Prueba de Penetración

## Objetivo de la prueba

Evaluar la preparación de Windows XP para resistir y detectar un ataque sofisticado desde el exterior.

La totalidad de las vulnerabilidades identificadas así como cualquier otra consideración de seguridad localizada fueron comunicadas a Windows XP a través de Juan Pedro Romero quien funge como principal punto de contacto para efecto de las pruebas.

Los servicios se limitaron exclusivamente a la infraestructura externa de Windows XP. No incluyen redes o sistemas de terceros que pueden resultar relacionadas con las redes de Windows XP debido a que se encuentran fuera del alcance de estas pruebas. Proveedor no realizó ningún ataque de negación de servicio en este proceso.

## Meta de la prueba

Lograr acceso a información crítica o sensible.

## Estrategia

Lograr acceso a información crítica o sensible y/o conseguir los máximos privilegios posibles dentro de la red y los servidores para este objetivo.

## Metodología

Las pruebas de penetración tienen como objetivo analizar que tan vulnerable es la empresa a un ataque sofisticado perpetrado desde el exterior de la Red de Windows XP. Se analiza la seguridad desde el punto de vista de un atacante externo con conexión a Internet. Un hacker siempre va a buscar el camino más fácil y va a revisar la seguridad en varios puntos, buscando entrar por la puerta más vulnerable.

De la misma forma nuestras pruebas pretenden encontrar las puertas vulnerables, probando a profundidad varias avenidas para poder 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.

Página 18

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

* + - Adivinando o descifrando contraseñas.
    - Explotando vulnerabilidades en el diseño o configuración de sistemas y equipos.
    - Interceptando comunicaciones.
    - Usando Ingeniería social para conseguir accesos o contraseñas.

El descifrado de contraseñas, la intercepción 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.

## Especificación de prueba

### 3.5.1 Objetivos Específicos

**Objetivos**

Servidores:

Dominios:

* WINDOWS XP 192.68.1.27

* +  Windows XP

## Pruebas Realizadas

Para hacer este diagnóstico se hicieron las pruebas siguientes:

### Penetración por Red Externa

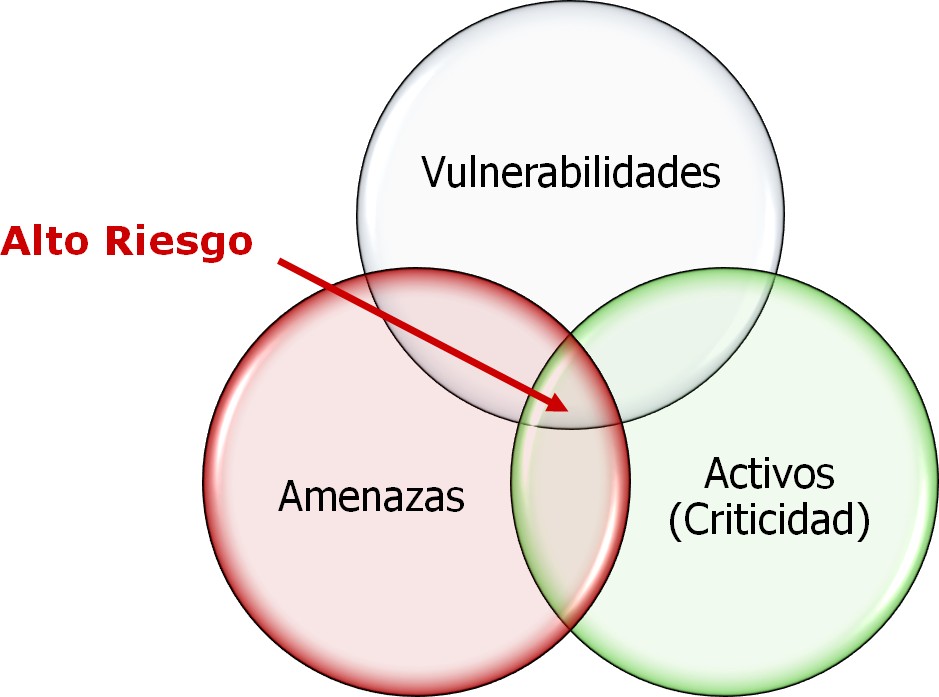
* + - * Analizar la red.
      * Identificar servidores y puertos.
      * Detectar vulnerabilidades en servidores.
      * Revisar debilidades de la red.
      * Determinar servidores críticos.
      * Determinar avenidas de acceso.
      * Enumerar usuarios.
      * Probar contraseñas.
      * Determinar vulnerabilidades.
      * Interceptar tráfico de red.
      * Lograr acceso a servidores.
      * Lograr acceso a aplicaciones.

### Expansión de Influencia

* + - * Explotar vulnerabilidades detectadas.
      * Conseguir acceso como administrador.
      * Lograr acceso interactivo a un servidor.
      * 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.

Página 20

# Resultados de la prueba

Los resultados de la prueba están divididos en tres categorías principales: Fortalezas, Vulnerabilidades y Recomendaciones. Estos resultados se midieron definiendo el nivel de acceso y la probabilidad de un ataque.

El nivel de Acceso está basado en los privilegios que se pueden obtener, siendo los privilegios de administrador la mayor amenaza. La probabilidad de ataque está determinada por el perfil de atacante; mientras menos sofisticado sea el atacante para obtener privilegios y/o información crítica, la probabilidad de tener un ataque es mucho mayor. Uniendo estos dos factores y evaluando el nivel de criticidad de la información que se maneja, el nivel de riesgo puede ser calculado por la empresa.

Página 21



Página 22

## Escala de Medición

La escala que utilizamos para determinar el nivel de vulnerabilidad potencial está basada en dos factores, el nivel de acceso y el perfil del atacante. En el siguiente cuadro se presenta la escala que utilizaremos para calificar la infraestructura externa de Windows XP.

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



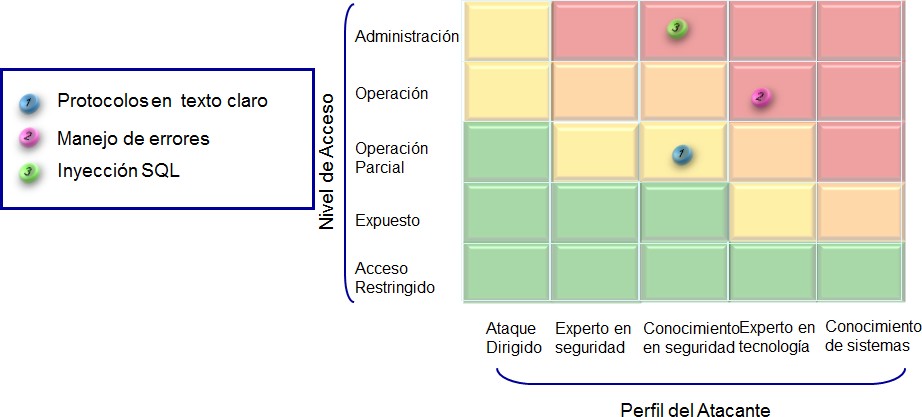
Página 23

## Resultados

El resultado qué a continuación se muestra está basado en una estadística que se lleva a cabo en Proveedor con los resultados de Hackeos Éticos que se han realizado a empresas semejantes y con un tamaño similar al de Windows XP.



* 1. **Principales Fortalezas Externas**
     + Los servidores expuestos a internet muestran una superficie de ataque reducida.
     + El servidor de DNS no permite conocer su tabla de resolución de nombres.
     + Los servicios SMTP en los servidores no permiten enviar correos electrónicos sin autenticación.
     + Las contraseñas de los usuarios de las aplicaciones Web son almacenadas de forma cifrada en la Base de Datos.
     + Los usuarios de bases de datos empleados por las aplicaciones tienen bajos privilegios.
  2. **Principales Vulnerabilidades Externas**



* + 1. **Protocolos en texto claro - Operación Parcial – Conocimiento en Seguridad**

Se identificaron protocolos de comunicación en texto claro, entre los que se encuentran: FTP y HTTP.

Todos estos protocolos envían tanto las contraseñas de usuario como todas las comunicaciones en texto claro, permitiendo a un atacante interceptar información sensible y comprometer las identidades de los usuarios legítimos.

Se encontraron cuatro servidores con el protocolo FTP habilitado lo cual puede representar una amenaza de intercepción de credenciales al ser usados.

Página 24

**IP**

|  |
| --- |
| 192.168.1.21 |
| 192.168.1.27 |
| 192.168.1.254 |
|  |

Las direcciones IP con el protocolo HTTP habilitado son:

|  |
| --- |
| **IP** |
| 192.168.0.103 |
|  |
|  |
|  |

Es posible acceder a los recursos de los sitios Web a través del protocolo inseguro HTTP colocando la ruta completa al recurso, evadiendo la redirección hacia el protocolo HTTPS; esto debido a que únicamente la página de inicio de los sitios Web es la que ha sido redirigida al protocolo HTTPS. Esto puede ser utilizado por un usuario mal intencionado para interceptar información sensible, como credenciales de autenticación, de páginas de acceso, así como parámetros ocultos enviados por la aplicación. Los sitios afectados por esta vulnerabilidad son:

* + - * Windows XP

**Nivel de Acceso**

* Operación Parcial

**Perfil del Atacante**

* Conocimiento en Seguridad
  + 1. **Validación de Entradas y Manejo de Errores Operación – Experto en Tecnología**

A pesar que al ocurrir un error o una excepción relacionada con la validación de los parámetros de entrada la aplicación re direcciona al usuario a una página genérica de error, esta redirección no ocurre en todos los casos, principalmente en los errores de

Página 25

bajo nivel en el servidor. Como por ejemplo un recurso no encontrado, o los errores provenientes de las Bases de Datos, los cuales son mostrados directamente en la aplicación o en el navegador.

Se pudo constatar la existencia de aplicaciones web que al suceder un error relacionada a la conexión o ejecución de consultas a la base de datos, muestran información detallada de la ocurrencia del mismo. Estas pantallas de error proporcionan a un usuario mal intencionado información importante para la comprensión a profundidad de la estructura de la base de datos, tipos de dato, tipo de información almacenada, así como versiones de software utilizado. Esto puede ser utilizado por un usuario mal intencionado para conseguir la extracción de información de la base de datos u obtener los detalles necesarios para identificar posibles vulnerabilidades al servidor de Bases de Datos. Algunas de las aplicaciones afectadas son:

* https://[www.dummy.com.mx/Empresa](http://www.dummy.com.mx/Empresa) Dummyingles/asp
* https://[www.dummy.com.mx/Empresa](http://www.dummy.com.mx/Empresa) Dummyingles
* https://[www.dumy.com.mx/Empresa](http://www.dumy.com.mx/Empresa) Dummyingles/asp/contrataciones/confirmInfo.asp
* https://[www.dummy.com.mx/asp/SalidaUsr/asp](http://www.dummy.com.mx/asp/SalidaUsr/asp)

**Nivel de Acceso –**

* + Operación

**Perfil del Atacante –**

* + Experto en Tecnología
    1. **Inyección SQL - Administración – Conocimientos en Seguridad**

Se observó que las aplicaciones web no realizan una correcta validación de las entradas de datos. Las aplicaciones efectúan una validación basada en los caracteres para palabras, y números, sin embargo, esta validación no contempla parámetros como máximo número de caracteres, o caracteres especiales para las contraseñas.

Como consecuencia de la forma en la que los datos son validados se identificaron páginas web con entradas de datos vulnerables a la inyección de código SQL para la manipulación maliciosa de su comportamiento normal. En ellos existe una validación básica de los campos que son mapeados a consultas a la base de datos, la cual consiste

Página 26

principalmente en eliminar algunos caracteres empleados en las consultas SQL así como espacios en blanco. Sin embargo esta validación de datos no considera la inyección de cadenas de texto codificadas como caracteres HTML, los cuales son considerados como válidos en la aplicación, pero son convertidos a texto al ser enviados a la base de datos. Por ejemplo: la cadena de texto= “’or 1=1- “puede ser codificada cómo “%18%20%6f%72%20%31%3d%31%20%13%2d para evadir la validación del campo y ejecutar la consulta efectivamente.

Este fallo permite extraer, modificar e incluso borrar información sensible de la base de datos que van desde: el nombre de la base de datos usada, el nombre del usuario de base de datos, el nombre del servidor, la versión de la base de datos, etc. hasta información de la estructura de la base de datos como: nombre de tablas, nombre de columnas o campos, descripción de campos, número de registros en una tabla, etc.

La situación más grave con esta vulnerabilidad es que permite a un atacante extraer los registros almacenados en cualquier tabla del servidor en la cual el usuario de la base de datos tiene al menos permisos de lectura.

Las direcciones o formas que fueron identificadas con problemas de Inyección SQL son:

* www.dummy.co.cr:443/asp/contrataciones/login.asp
* www.dummy.com.co:443/contrasena.asp
* www.dummy.com.mx:443/contrasena.asp
* www.dummy.com.mx:443/asp/contrataciones/administracion/admin\_ loguin.asp

**Nivel de Acceso –**

* + Administración

**Perfil del Atacante –**

* + Conocimientos en Seguridad

Página 27



Página 28

* 1. **Conclusiones**

Haciendo referencia a la gráfica de comparativo con la industria se concluye que la red externa de Windows XP permite obtener hasta un nivel de acceso **Administración** y puede ser vulnerada por una persona con un perfil de **Conocimientos en Seguridad**

Existen puntos vulnerables de la red externa de Windows XP como:

* Se encontraron protocolos de red en texto claro que envían los datos sin ningún tipo de cifrado como HTTP y FTP.
* Las aplicaciones web no manejan adecuadamente la ocurrencia de errores por lo cual son mostradas al usuario exponiendo información sensible.
* La inyección SQL permite extraer información sensible de las bases de datos.

.

Página 29

* + 1. **Implicaciones**

Para lograr un mayor entendimiento de las vulnerabilidades anteriormente descritas se presentan adicionalmente algunas de las implicaciones posibles, enfocándonos principalmente desde la perspectiva de un atacante externo con acceso a internet y que pretenda abusar de estos puntos vulnerables.

**Probabilidad Alta**

**Robo de información de clientes**

Debido a que es posible extraer registros de clientes de las páginas de Windows XP, es posible automatizar estas extracciones para obtener toda la información de clientes y cualquier otra información contenida en la misma base de datos. La probabilidad de sufrir un robo de información aumenta debido a que existen ya a distribución gratuita aplicaciones o frameworks para explotar las vulnerabilidades de inyección de SQL que automáticamente extraen los registros de las bases de datos.

**Probabilidad Media**

**Que sufran un ataque informático y no se den cuenta**

En el transcurso de las pruebas no se mantuvo un perfil encubierto y tampoco se intentó ser silencioso o cuidadoso con el tipo de pruebas que se hacían. El nivel de tráfico generado durante las pruebas fue aumentando conforme pasó el tiempo. A pesar de todo, no se nos fue reportada la actividad por parte de los responsables de sistemas y tampoco se tomaron medidas preventivas al respecto.



Página 30

* 1. **Plan de Mitigación**

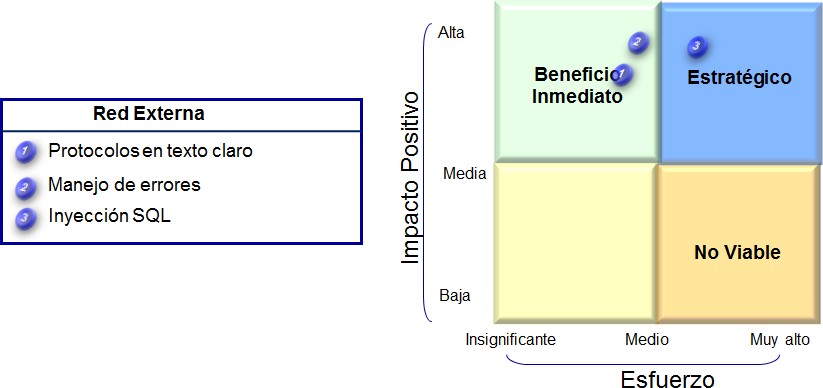
Para determinar un plan de mitigación se han priorizado las acciones requeridas de acuerdo a dos criterios: el impacto de las mejoras y el esfuerzo que se requiere.

En impacto se tomará 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 al Negocio – Percepción que el exterior tiene de la empresa. En esfuerzo se considerará:
* 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.

**Acciones Mitigantes y Mejoras Sugeridas**

Hay 2 grupos principales donde consideramos se deberá hacer un esfuerzo de corrección para mejorar la seguridad de la red externa de Windows XP:



* + 1. **Protocolos en texto claro**
       - Eliminar y migrar a versiones seguras los protocolos en texto claro como FTP y HTTP.

Para el caso de los protocolos en texto claro como FTP, HTTP se recomienda eliminar estos servicios y sustituirlos únicamente por sus versiones que incorporan cifrado a través de una capa de SSL. Las opciones disponibles son SFTP y HTTPS. La migración a estas versiones seguras es relativamente sencilla puesto que solo es necesario crear con una autoridad certificadora los certificados a intercambiar en los servidores, instalarlos y volver a poner los servicios.

La parte de esta mejora que necesita evaluarse es la capacidad de los clientes de estos servicios para manejar los certificados y los cifrados. La versión de SSL recomendada para efectuar estos cambios es SSLv3 o TLSv1.2.

Aunque las aplicaciones web, la mayoría tienen el puerto HTTPS configurado con un certificado, este canal no siempre es usado principalmente en las pantallas de lógin por lo que se recomienda forzar a las aplicaciones a transmitir los datos únicamente por este cana cifrado debido a que los usuarios pudieran ser engañados para enviar sus credenciales por el canal en texto claro.

Se debe de configurar el servidor de DNS para que las peticiones recibidas a los sitios Web:

* [http://www.dummy.com.mx](http://www.dummy.com.mx/)
* [http://www.dummy.com.co](http://www.dummy.com.co/)
* [http://www.dummy.com.pe](http://www.dummy.com.pe/)
* [http://www.dummyca.co.cr](http://www.dummyca.co.cr/)

El servidor responda con un MOVED PERMANENTLY que los referencie al puerto del servicio HTTPS de cada uno de los sitios Web.

Las rutas establecidas en las formas Web de los sitios, deben de ser dirigidas explícitamente a las rutas del servicio seguro HTTPS y la ruta del archivo ASP que manejará dicha acción. Por ejemplo:

<form method="get"

Página 31

action="[https://www.server.com.mx/simpleform.asp">](http://www.server.com.mx/simpleform.asp) First Name: <input type="text" name="fname"/><br/> Last Name: <input type="text" name="lname"/><br/><br/>

<input type="submit" value="Submit"/>

</form>

* + 1. **Manejo de Errores**
       - Crear un módulo de manejo de errores que encapsule adecuadamente la totalidad de los fallos o errores, desde los provenientes del servidor Web, los errores y excepciones generados por la aplicación, y también aquellos generados por la base de datos o cualquier otro repositorio de datos, es decir, al incurrir en una excepción o error, los detalles de estos no deben de ser presentados al cliente, en este caso en su navegador, puesto que estos detalles ofrecen información importante de la implementación, programación, despliegue o infraestructura usada por la aplicación web. Todos los errores en primer lugar deben de ser almacenados en bitácoras y debe de presentarse una código genérico al usuario que no le permita saber el tipo de error ocurrido a un usuario malicioso pero que si permita, en caso de comunicarse con una mesa de ayuda, hacer una depuración adecuada de la aplicación.
       - Configurar el servidor IIS para que en caso de ocurrir una Excepción no manejada o soportada por la aplicación, la página sea redirigida a un manejador tipo Global Exception a una página de error preestablecida.
    2. **Inyección SQL**
       - Establecer política y normas de programación segura y se incluyan en los contratos y documentos de requerimientos celebrados con los desarrolladores internos o despachos externos de desarrollo. Estos contratos deben establecer requerimientos mínimos de módulos especializados en:
         * Autenticación: implementación de mecanismos que eviten a un usuario mal intencionado comprometer contraseñas, llaves, tokens de sesión o que eviten que sea explotada alguna vulnerabilidad que permita suplantar identidades.

Página 32

* + - * + Autorización: implementación de mecanismos que eviten que usuarios no autorizados accedan a recursos no autorizados.
        + Validación de entradas: implementación de mecanismos que eviten posibles inyecciones de entradas no esperadas por la aplicación, que en algún momento puedan poner en riesgo la integridad de la aplicación.
        + Manejo de errores: implementación de módulos de error genérico que eviten ofrecer información no necesaria al usuario.
        + Bitácoras: implementación de sistemas de loggueo que permitan mantener trazabilidad ante cualquier incidente de aplicaciones o infraestructura.

Forzar la validación de los datos de entrada a las aplicaciones web tanto del lado del cliente como del lado del servidor. Este objetivo se logra a través de establecer controles más estrictos sobre la validación hecha con javascript en el cliente, y aún más importante que existan controles de validación de los datos que llegan al servidor antes de ser procesados dichos datos. Estos controles deben ser “validadores positivos”, es decir, que describan los caracteres permitidos para cada tipo de dato diferentes y tan específicos como los datos requieran, lo cual puede hacerse con el uso de expresiones regulares para definir los datos y compararlos contra ellas. Esta práctica asegura que los usuarios no podrán ingresar datos diferentes a los estrictamente necesarios para la información requerida, ni información basura sin formato.

Se requiere revisar las aplicaciones para reparar las fallas de Inyección SQL, derivadas de la mala validación de los datos de entrada a la aplicación. Se debe de verificar que todas las entradas de datos sean validadas antes de efectuar cualquier tipo de procesamiento de las mismas. Estas validaciones deben basarse en la comparación de los datos contra una lista de caracteres esperados, como pudiera ser el caso de expresiones regulares.

Es necesario crear un procedimiento más completo que vaya más allá de eliminar espacios (funciones trim) y eliminar caracteres peligrosos al momento de validar los datos que serán utilizados en una consulta o actualización a base de datos, de tal forma que:

Página 33

* + - * + Se utiliza una codificación estándar de caracteres que convierta los datos enviados en HTML o ASCII a una codificación como UTF8.



Página 34

* + - * + Se validen contra una lista blanca o *white list* de caracteres validos
        + Que definan más claramente los datos para determinar mínimo y máximo de caracteres.

1. **Detalle Técnico**
   1. **Visibilidad externa**
      1. **Información Pública**

#### Whois

#### Windows XP

|  |  |
| --- | --- |
| **Tipo de Información** | **Datos** |
| **Nombre del dominio** |  |
| Fecha de creación | |
| Fecha de expiración |  |
| Fecha de última modificación | |
| **Contacto Registrante** |  |
| Nombre | |
| Ciudad |  |
| Estado | |
| País | Colombia |
| **Contacto administrativo** | |
| Nombre |  |
| Ciudad | Colombia |
| Estado | Cartago |
| País | Colombia |
| **Contacto técnico** |  |
| Nombre Stephany Ramírez | |
| Ciudad | Colombia |
| Estado | Cartago |
| País | Colombia |
| **Contacto de pago** | |
| Nombre | Juan Felipe Marin |
| Ciudad | Colombia |
| Estado | Cartaago |
| País | Colombia |
| **Servidores DNS** |  |
| ns1.dummy.com.mx | |
| ns2.dummy.com.mx |  |

#### dummy.co.cr

**Tipo de Información Datos**

Página 35

|  |  |
| --- | --- |
| **Nombre del dominio** | Microsoft |
| Fecha de creación 04 abril 1975 | |
| Fecha de expiración |  |
| Fecha de última modificación | |
| **Contacto Registrante** |  |
| Nombre | |
| **Contacto administrativo** |  |
| Nombre | |
| e-mail |  |
| Empresa | |
| Dirección |  |
| **Contacto técnico** | |
| Nombre |  |
| e-mail | |
| Empresa |  |
| Dirección | |
| **Servidores DNS** |  |
| ns1.dummy.com.mx | |
| ns2.dummy.com.mx |  |

#### dummy.com.pe

|  |  |
| --- | --- |
| **Tipo de Información Datos** | |
| **Contacto Registrante** |  |
| **Contacto administrativo** | |
| Nombre |  |
| **Servidores DNS** | |
| ns1.dummy.com.mx |  |
| ns2.dummy.com.mx | |

#### dummy.com.co

Página 36

|  |  |
| --- | --- |
| **Tipo de Información Datos** | |
| **Nombre del dominio** | dummy.com.co |
| Fecha de creación Wed Sep 09 00:00:00 GMT 2009 | |
| Fecha de expiración | Fri Sep 09 23:59:59 GMT 2011 |
| Fecha de última modificación Mon Dec 06 14:45:38 GMT 2010 | |
| **Contacto Registrante** |  |
| Nombre | |
| Dirección |  |

Página 37

|  |  |
| --- | --- |
| Estado | |
| País |  |
| Teléfono | |
| e-mail |  |
| **Contacto administrativo** | |
| Nombre |  |
| Dirección | |
| Estado |  |
| País | |
| Teléfono |  |
| e-mail | |
| **Contacto técnico** |  |
| Nombre | |
| Dirección |  |
| Estado | |
| País |  |
| Teléfono | |
| e-mail |  |
| **Contacto de pago** | |
| Nombre |  |
| Dirección | |
| Estado |  |
| País | |
| Teléfono |  |
| e-mail | |
| **Servidores DNS** |  |
| ns1.dummy.com.mx | |
| ns2.dummy.com.mx |  |

#### Dominios

|  |  |
| --- | --- |
| IP Dominio | |
| 200.xx.xx.xx | dummy.com.mx |
| 200.xx.xx.xx | Empresa Dummy.com.pe |
| 200.xx.xx.xx | Empresa Dummyca.co.cr |
| 200.xx.xx.xx dummy.com.co | |

#### Listado de Rangos

|  |  |  |
| --- | --- | --- |
| Rango Registrado en Propietario | | |
| 200.xx.xx.xx/27 | LACNIC | Empresa Dummy |
| 200.xx.xx.xx/28 | LACNIC | Empresa Dummy |
| 200.xx.xx/19 | LACNIC | Empresa Dummy |

* + 1. **Recopilación de Información en Internet**

#### Contactos

|  |
| --- |
| **dummy.com.mx** |
| [postmaster@dummy.com.mx](mailto:postmaster@dummy.com.mx) |
| [jromero@dummy.com.mx](mailto:jromero@dummy.com.mx) |
| [mgonzalez@dummy.com.mx](mailto:mgonzalez@dummy.com.mx) |
| [ventas@dummy.com.mx](mailto:ventas@dummy.com.mx) |
| [mespinosa@dummy.com.mx](mailto:mespinosa@dummy.com.mx) |
| [emartina@dummy.com.mx](mailto:emartina@dummy.com.mx) |
| [spatlan@dummy.com.mx](mailto:spatlan@dummy.com.mx) |
| [ahidalgo@dummy.com.mx](mailto:ahidalgo@dummy.com.mx) |
| [ahernandez@dummy.com.mx](mailto:ahernandez@dummy.com.mx) |
| [coceguera@dummy.com.mx](mailto:coceguera@dummy.com.mx) |
| [x3d@dummy.com.mx](mailto:x3d@dummy.com.mx) |

#### Google hacking

* Haciendo uso de búsquedas en recursos abiertos de Internet se encontraron credenciales de acceso válidas para el sitio [www.dummy.com.mx,](http://www.dummy.com.mx/) en un foro de usuarios público.

El usuario que colocó esta información, buscaba ayuda para la creación de una macro de Excel, en la cual utilizada un URL con estas credenciales de acceso. http://…-public-es-excel/907741-cambio-de-ruta-en-archivos.html

URLDownloadToFile 0,

"http://USUARIO:CONTRASEÃ‘A\*\*\*[www.dummy.com.mx/aspnet/archivo](http://www.dummy.com.mx/aspnet/archivo) s/detalle.aspx?ruta=/VectorConsar/"

& "24" & strArchivo & "CONSAR.zip", "F:\VECTORES\24" & strArchivo & "Consar.zip", 0, 0

Página 38

[http://www](http://www/)…../respuesta/ruta-acceso-virtual-sacar-ruta-acceso-fisica-ayuda-

|  |  |  |
| --- | --- | --- |
| 204061512.html  "http://HEIDILAN:HE\*\*\*\*\*\*\*@[www.dummy.com.mx/Empresa](http://www.dummy.com.mx/Empresa) files//VectorConsar/" |  | Dummy-  & |
| "24" & strArchivo & "CONSAR.zip", "F:\VECTORES\24"  "Consar.zip", 0, 0 | & | strArchivo & |

* + 1. **Dominios**

#### DNS Zone transfer

**DNS Servers**

|  |  |
| --- | --- |
| **IP Dominio** | |
| **dummy.com.mx** |  |
| 200.xx.xx.xx | ns1.dummy.com.mx |
| 200.xx.xx.xx | ns2.dummy.com.mx |
|  |  |
| **dummyEmpresa Dummy.com.pe** |  |
| 200.xx.xx.xx | ns1.dummy.com.mx |
| 200.xx.xx.xx | ns2.dummy.com.mx |
|  |  |
| **Empresa Dummyca.co.cr** |  |
| 200.xx.xx.xx | ns1.dummy.com.mx |
| 200.xx.xx.xx | ns2.dummy.com.mx |
|  |  |
| **dummy.com,co** |  |
| 200.xx.xx.xx | ns1.dummy.com.mx |
| 200.xx.xx.xx | ns2.dummy.com.mx |

**Información Obtenida**

* Ninguno de los servidores de DNS permitió consultar su tabla Zone Transfer.
  + 1. **Exploración**

#### Equipos Activos

Página 39

**IP NOMBRE TIPO**



Página 40

|  |  |  |
| --- | --- | --- |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx | ns1.dummy.com.mx | Windows |
| 200.xx.xx.xx | ns2.dummy.com.mx | Windows |
| 200.xx.xx.xx | ftp.dummy.com.mx | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx | | |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx | | |
| 200.xx.xx.xx |  |  |
| 200.xx.xx.xx | mail.dummy.com.mx | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  | Windows |
| 200.xx.xx.xx |  |  |
| 200.xx.xx.xx | | |
| 200.xx.xx.xx |  |  |
| 200.xx.xx.xx | | |
| 200.xx.xx.xx |  |  |
| 200.xx.xx.xx | | |

|  |  |  |
| --- | --- | --- |
| 200.xx.xx.xx |  |  |
| 200.xx.xx.xx | | |
| 200.xx.xx.xx |  |  |
| 200.xx.xx.xx | | |
| 200.xx.xx.xx |  |  |
| 200.xx.xx.xx | | |
| 200.xx.xx.xx |  |  |
| 200.xx.xx.xx | | |

#### Aplicaciones Web

|  |  |  |  |
| --- | --- | --- | --- |
| **IP URL Lenguaje Interactividad** | | | |
| 200.xx.xx.xx | https[://w](http://www.dummy.com.mx/index.asp)ww.[dummy.com.mx/index.asp](http://www.dummy.com.mx/index.asp) | ASP | Si |
| 200.xx.xx.xx https[://w](http://www.dummy.com.mx/ASPNET/Benchma)ww.[dummy.com.mx/ASPNET/Benchma](http://www.dummy.com.mx/ASPNET/Benchma) ASP rks/FormularioDJ\_2.aspx | | | Si |
| 200.xx.xx.xx | https[://w](http://www.dummy.com.mx/ASPNET/Benchma)ww.[dummy.com.mx/ASPNET/Benchma](http://www.dummy.com.mx/ASPNET/Benchma) rks/indexDJ.aspx | ASP | Si |
| 200.xx.xx.xx https[://w](http://www.dummy.com.mx/asp/contrataciones)ww.[dummy.com.mx/asp/contrataciones](http://www.dummy.com.mx/asp/contrataciones) ASP  /administracion/admin\_login1.asp | | | Si |
| 200.xx.xx.xx | https://Empresa Dummyca.co.cr/ | ASP | Si |

**Vulnerabilidades**

* Las siguientes aplicaciones son vulnerables a ataques de SQL Injection:
  + https:[//w](http://www.dummy.com.mx/contrasena.asp)ww[.dummy.com.mx/contrasena.asp](http://www.dummy.com.mx/contrasena.asp)
  + https://[www.dummy.com.mx/contrataciones/administracion/admin\_l](http://www.dummy.com.mx/contrataciones/administracion/admin_l) ogin.asp
  + www.Empresa Dummyca.co.cr:443/asp/contrataciones/login.asp
  + www.dummy.com.co:443/contrasena.asp
* Se encontraron sitios Web que presentan un deficiente manejo de errores.
  + https://[www.dummy.com.mx/asp/SalidaUsr.asp](http://www.dummy.com.mx/asp/SalidaUsr.asp)
  + https://[www.dummy.com.mx/asp/contrataciones/confirmInfo.asp](http://www.dummy.com.mx/asp/contrataciones/confirmInfo.asp)
  + https://[www.dummy.com.mx/Empresa](http://www.dummy.com.mx/Empresa) Dummyingles/
  + https://[www.dummy.com.mx/Empresa](http://www.dummy.com.mx/Empresa) Dummyingles/asp/

Página 41

* Se encontraron sitios Web con lógica de programación de lado del cliente, lo cual permite hacer modificaciones a conveniencia del usuario.



Página 42

* + https://[www.dummy.com.mx/asp/contrataciones/confirmInfo.asp](http://www.dummy.com.mx/asp/contrataciones/confirmInfo.asp)
* Se encontraron sitios de autenticación que no tienen implementado un número máximo de intentos fallidos, antes de bloquear la cuenta del usuario o la dirección origen.
  + https://[www.dummy.com.mx/acceso.aspx](http://www.dummy.com.mx/acceso.aspx)

**Recomendaciones**

* Realizar una validación exhaustiva de todas las entradas y salidas en la aplicación, haciendo énfasis en las partes expuestas como los login. Se deben de hacer validaciones positivas de los parámetros recibidos, tanto del lado del cliente como del servidor para capturar todos aquellos intentos de inyección y desecharlos.
* Crear excepciones para el manejo de errores en las aplicaciones web, de esta forma las excepciones genéricas no mostraran información valiosa para los atacantes.
* Evitar colocar parte de la lógica de programación del lado del cliente, un usuario mal intencionado siempre podrá modificar información del lado del cliente, así como obtener información sobre el flujo de la aplicación en el lado del servidor.
  1. **Configuración General Externa**

**5.2.1 200.xx.xx.80**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dirección IP Nombre en el Dominio Tipo Uso** | | | |
| 200.xx.xx.xx | EMPRESA DUMMYWEB12 | Windows | Servidor Web |

#### Servicios

|  |  |  |
| --- | --- | --- |
| **Puerto Estado Protocolo** | | |
| 21/tcp | open | ftp |
| 25/tcp | open | smtp |
| 80/tcp | open | http |
| 110/tcp | open | pop3 |
| 443/tcp | open | https |
| 1723/tcp | open | pptp |
| 6666/tcp | open | irc |
| 6667/tcp | open | irc |
| 6668/tcp | open | irc |

#### Encabezados

|  |  |  |
| --- | --- | --- |
| **Puerto Protocolo Encabezado** | | |
| 21/tcp | ftp |  |
| 25/tcp | smtp |  |
| 80/tcp | http |  |
| 110/tcp | pop3 |  |
| 443/tcp | https |  |
| 1723/tcp | pptp |  |
| 6666/tcp | irc |  |
| 6667/tcp | irc |  |
| 6668/tcp | irc |  |

#### Fortalezas

* El servicio de SMTP del servidor no permite enviar correos electrónicos sin autenticación.

Página 43



Página 44

#### Vulnerabilidades

* Se hace uso del protocolo inseguro SMTP el cual está diseñado para transferir correo de manera eficaz, sin embargo, este protocolo envía su información en texto claro lo que puede permitir a un atacante realizar ataques de ‘man in the middle’ y de esta manera obtener la información que se está enviando.
* Se hace uso del protocolo inseguro HTTP, el cual envía la información en texto claro por la red, esto implica que un atacante puede interceptar las comunicaciones y de esta forma hacerse de datos sensibles como lo son usuarios y contraseñas.

#### Recomendaciones

* Sustituir el SMTP por su versión con SSL integrado, esto le dará una capa extra de seguridad a la información que es transmitida entre cliente y servidor evitando que un atacante obtenga la información transmitida.
* Es necesario no utilizar el protocolo HTTP para transferencia de información, sino sustituirlo por aplicaciones equivalentes pero que utilicen cifrado para la transmisión de datos, HTTPS es el más común.
  + 1. **200.xx.xx.xx**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dirección IP Nombre en el Dominio Tipo Uso** | | | |
| 200.xx.xx.xx | EMPRESA DUMMYDNS | Windows | Servidor de DNS |

#### Servicios

|  |  |  |
| --- | --- | --- |
| **Puerto Estado Protocolo** | | |
| 21/tcp | open | ftp |
| 53/tcp | open | domain |
| 80/tcp | open | http |
| 1723/tcp | open | pptp |
| 6666/tcp | open | irc |
| 6667/tcp | open | irc |
| 6668/tcp | open | irc |

#### Encabezados

|  |  |  |
| --- | --- | --- |
| **Puerto Protocolo Encabezado** | | |
| 21/tcp | ftp |  |
| 53/tcp | domain | Microsoft DNS |
| 80/tcp | http |  |
| 1723/tcp | pptp | Microsoft (Firmware: 3790) |
| 6666/tcp | irc |  |
| 6667/tcp | irc |  |
| 6668/tcp | irc |  |

#### Fortalezas

* El servidor de DNS no permite conocer su tabla de resolución de forma pública.

#### Vulnerabilidades

* El servidor tiene varios servicios de administración y transferencia remota como FTP y HTTP, la mayoría de ellos envían las credenciales y datos en texto claro, lo cual un atacante puede interceptar y así suplantar la identidad del usuario que esté utilizando estos servicios.

Página 45



Página 46

#### Recomendaciones

* Es necesario no utilizar estos protocolos para conexiones remotas, sino sustituirlo por aplicaciones equivalentes pero que utilicen cifrado para la transmisión de datos: SFTP, SSH y HTTPS son las más comunes. En esto caso se requiere además de la parte cliente en nuestro equipo, la parte servidora en la máquina remota escuchando en un puerto determinado.
  + 1. **200.xx.xx.xx**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dirección IP Nombre en el Dominio Tipo Uso** | | | |
| 200.xx.xx.xx | EMPRESA DUMMYEXDB1  mail.dummy.com.mx | Windows | Servidor de Correo Electrónico |

#### Servicios

|  |  |  |
| --- | --- | --- |
| **Puerto Estado Protocolo** | | |
| 25/tcp | open | smtp |
| 110/tcp | open | pop3 |
| 443/tcp | open | ssl/http |
| 1723/tcp | open | pptp |
| 6666/tcp | open | irc |
| 6667/tcp | open | irc |
| 6668/tcp | open | irc |

#### Encabezados

|  |  |  |
| --- | --- | --- |
| **Puerto Protocolo Encabezado** | | |
| 25/tcp | smtp | Microsoft ESMTP |
| 110/tcp | pop3 |  |
| 443/tcp | ssl/http | Microsoft IIS httpd 7.0 |
| 1723/tcp | pptp |  |
| 6666/tcp | irc |  |
| 6667/tcp | irc |  |
| 6668/tcp | irc |  |

#### Fortalezas

* El servicio de SMTP del servidor no permite enviar correos electrónicos sin autenticación.

#### Vulnerabilidades

* Se hace uso del protocolo inseguro SMTP el cual está diseñado para transferir correo de manera eficaz, sin embargo, este protocolo envía su información en texto claro lo que puede permitir a un atacante realizar ataques de ‘man in the middle’ y de esta manera obtener la información que se está enviando.

Página 47

* Se hace uso del protocolo inseguro HTTP, el cual envía la información en texto claro por la red, esto implica que un atacante puede interceptar las



Página 48

comunicaciones y de esta forma hacerse de datos sensibles como lo son usuarios y contraseñas.

#### Recomendaciones

* Sustituir el SMTP por su versión con SSL integrado, esto le dará una capa extra de seguridad a la información que es transmitida entre cliente y servidor evitando que un atacante obtenga la información transmitida.
* Es necesario no utilizar el protocolo HTTP para transferencia de información, sino sustituirlo por aplicaciones equivalentes pero que utilicen cifrado para la transmisión de datos, HTTPS es el más común.

**5.2.4 201.159.142.138**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dirección IP Nombre en el Dominio Tipo Uso** | | | |
| 201.xx.xx.xx | [www.dummy.com.mx](http://www.dummy.com.mx/) | Windows | Servidor Web |

#### Servicios

|  |  |  |
| --- | --- | --- |
| **Puerto Estado Protocolo** | | |
| 21/tcp | open | ftp |
| 25/tcp | open | smtp |
| 80/tcp | open | http |
| 110/tcp | open | pop3 |
| 443/tcp | open | https |
| 1723/tcp | open | pptp |
| 6666/tcp | open | irc |
| 6667/tcp | open | irc |
| 6668/tcp | open | irc |

#### Encabezados

|  |  |  |
| --- | --- | --- |
| **Puerto Protocolo Encabezado** | | |
| 21/tcp | ftp | Microsoft ftpd |
| 25/tcp | smtp |  |
| 80/tcp | http |  |
| 110/tcp | pop3 |  |
| 443/tcp | https | Microsoft IIS httpd 6.0 |
| 1723/tcp | pptp |  |
| 6666/tcp | irc |  |
| 6667/tcp | irc |  |
| 6668/tcp | irc |  |

#### Fortalezas

* El servicio de SMTP del servidor no permite enviar correos electrónicos sin autenticación.

#### Vulnerabilidades

* Se hace uso del protocolo inseguro SMTP el cual está diseñado para transferir correo de manera eficaz, sin embargo, este protocolo envía su información en

Página 49



Página 50

texto claro lo que puede permitir a un atacante realizar ataques de ‘man in the middle’ y de esta manera obtener la información que se está enviando.

* Se hace uso del protocolo inseguro HTTP, el cual envía la información en texto claro por la red, esto implica que un atacante puede interceptar las comunicaciones y de esta forma hacerse de datos sensibles como lo son usuarios y contraseñas.

#### Recomendaciones

* Sustituir el SMTP por su versión con SSL integrado, esto le dará una capa extra de seguridad a la información que es transmitida entre cliente y servidor evitando que un atacante obtenga la información transmitida.
* Es necesario no utilizar el protocolo HTTP para transferencia de información, sino sustituirlo por aplicaciones equivalentes pero que utilicen cifrado para la transmisión de datos, HTTPS es el más común.
  + 1. **201.xx.xx.xx**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dirección IP Nombre en el Dominio Tipo Uso** | | | |
| 201.xx.xx.xx | Empresa Dummyca.co.cr | Windows | Servidor Web |

#### Servicios

|  |  |  |
| --- | --- | --- |
| **Puerto Estado Protocolo** | | |
| 21/tcp | open | ftp |
| 25/tcp | open | smtp |
| 80/tcp | open | http |
| 110/tcp | open | pop3 |
| 443/tcp | open | https |
| 1723/tcp | open | pptp |
| 6666/tcp | open | irc |
| 6667/tcp | open | irc |
| 6668/tcp | open | irc |

#### Encabezados

|  |  |  |
| --- | --- | --- |
| **Puerto Protocolo Encabezado** | | |
| 21/tcp | ftp | Microsoft ftpd |
| 25/tcp | smtp |  |
| 80/tcp | http |  |
| 110/tcp | pop3 |  |
| 443/tcp | https | Microsoft IIS httpd 6.0 |
| 1723/tcp | pptp |  |
| 6666/tcp | irc |  |
| 6667/tcp | irc |  |
| 6668/tcp | irc |  |

#### Fortalezas

* El servicio de SMTP del servidor no permite enviar correos electrónicos sin autenticación.

#### Vulnerabilidades

* Se hace uso del protocolo inseguro SMTP el cual está diseñado para transferir correo de manera eficaz, sin embargo, este protocolo envía su información en

Página 51



Página 52

texto claro lo que puede permitir a un atacante realizar ataques de ‘man in the middle’ y de esta manera obtener la información que se está enviando.

* Se hace uso del protocolo inseguro HTTP, el cual envía la información en texto claro por la red, esto implica que un atacante puede interceptar las comunicaciones y de esta forma hacerse de datos sensibles como lo son usuarios y contraseñas.

#### Recomendaciones

* Sustituir el SMTP por su versión con SSL integrado, esto le dará una capa extra de seguridad a la información que es transmitida entre cliente y servidor evitando que un atacante obtenga la información transmitida.
* Es necesario no utilizar el protocolo HTTP para transferencia de información, sino sustituirlo por aplicaciones equivalentes pero que utilicen cifrado para la transmisión de datos, HTTPS es el más común.
  + 1. **201.xx.xx.xx**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dirección IP Nombre en el Dominio Tipo Uso** | | | |
| 201.xx.xx.xx | www.dummyEmpresa Dummy.com.pe | Windows | Servidor Web |

#### Servicios

|  |  |  |
| --- | --- | --- |
| **Puerto Estado Protocolo** | | |
| 21/tcp | open | ftp |
| 25/tcp | open | smtp |
| 80/tcp | open | http |
| 110/tcp | open | pop3 |
| 443/tcp | open | https |
| 1723/tcp | open | pptp |
| 6666/tcp | open | irc |
| 6667/tcp | open | irc |
| 6668/tcp | open | irc |

#### Encabezados

|  |  |  |
| --- | --- | --- |
| **Puerto Protocolo Encabezado** | | |
| 21/tcp | ftp | Microsoft ftpd |
| 25/tcp | smtp |  |
| 80/tcp | http |  |
| 110/tcp | pop3 |  |
| 443/tcp | https | Microsoft IIS httpd 6.0 |
| 1723/tcp | pptp |  |
| 6666/tcp | irc |  |
| 6667/tcp | irc |  |
| 6668/tcp | irc |  |

#### Fortalezas

* El servicio de SMTP del servidor no permite enviar correos electrónicos sin autenticación.

#### Vulnerabilidades

* Se hace uso del protocolo inseguro SMTP el cual está diseñado para transferir correo de manera eficaz, sin embargo, este protocolo envía su información en

Página 53



Página 54

texto claro lo que puede permitir a un atacante realizar ataques de ‘man in the middle’ y de esta manera obtener la información que se está enviando.

* Se hace uso del protocolo inseguro HTTP, el cual envía la información en texto claro por la red, esto implica que un atacante puede interceptar las comunicaciones y de esta forma hacerse de datos sensibles como lo son usuarios y contraseñas.

#### Recomendaciones

* Sustituir el SMTP por su versión con SSL integrado, esto le dará una capa extra de seguridad a la información que es transmitida entre cliente y servidor evitando que un atacante obtenga la información transmitida.
* Es necesario no utilizar el protocolo HTTP para transferencia de información, sino sustituirlo por aplicaciones equivalentes pero que utilicen cifrado para la transmisión de datos, HTTPS es el más común.
  + 1. **200.xx.xx.xx**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dirección IP Nombre en el Dominio Tipo Uso** | | | |
| 200.xx.xx.xx | [www.dummy.com.co](http://www.dummy.com.co/) | Windows | Servidor Web |

#### Servicios

|  |  |  |
| --- | --- | --- |
| **Puerto Estado Protocolo** | | |
| 21/tcp | open | ftp |
| 25/tcp | open | smtp |
| 80/tcp | open | http |
| 110/tcp | open | pop3 |
| 443/tcp | open | ssl/http |
| 1723/tcp | open | pptp |
| 6666/tcp | open | irc |
| 6667/tcp | open | irc |
| 6668/tcp | open | irc |

#### Encabezados

|  |  |  |
| --- | --- | --- |
| **Puerto Protocolo Encabezado** | | |
| 21/tcp | ftp | Microsoft ftpd |
| 25/tcp | smtp |  |
| 80/tcp | http |  |
| 110/tcp | pop3 |  |
| 443/tcp | ssl/http | Microsoft IIS httpd 6.0 |
| 1723/tcp | pptp |  |
| 6666/tcp | irc |  |
| 6667/tcp | irc |  |
| 6668/tcp | irc |  |

#### Fortalezas

* La superficie de expuesta es limitada, ya que solo son visibles pocos puertos del servidor.
* Se hace uso del protocolo de transferencia segura HTTPS, con lo que se evita que un usuario mal intencionado pueda interceptar datos en texto claro que se transmitan por este medio.

Página 55

#### Vulnerabilidades

* Se encontraron en las aplicaciones problemas de validación de datos que permiten inyectar código SQL a la aplicación para extraer información sensible almacenada en las Bases de Datos. A continuación se enlistan las URLs que presentan dicho problema:
  + https:[//w](http://www.dummy.com.mx/contrasena.asp)ww[.dummy.com.mx/contrasena.asp](http://www.dummy.com.mx/contrasena.asp)
  + https://[www.dummy.com.mx/contrataciones/administracion/admin\_l](http://www.dummy.com.mx/contrataciones/administracion/admin_l) ogin.asp
* Se encontraron en las aplicaciones diversos problemas en el manejo de errores, lo cual permite obtener información sobre la aplicación. Esto puede ser utilizado por un usuario malintencionado para enumerar servicios, entender el funcionamiento de la aplicación e inclusive aprovecharse de los errores. A continuación se enlistan las URLs que presentan dicho problema:
  + https://[www.dummy.com.mx/asp/SalidaUsr.asp](http://www.dummy.com.mx/asp/SalidaUsr.asp)
  + https://[www.dummy.com.mx/asp/contrataciones/confirmInfo.asp](http://www.dummy.com.mx/asp/contrataciones/confirmInfo.asp)
  + https://[www.dummy.com.mx/Empresa](http://www.dummy.com.mx/Empresa) Dummyingles/
  + https://[www.dummy.com.mx/Empresa](http://www.dummy.com.mx/Empresa) Dummyingles/asp/
  + https://[www.dummy.com.co/asp/SalidaUsr.asp](http://www.dummy.com.co/asp/SalidaUsr.asp)
  + https://[www.dummy.com.co/asp/contrataciones/confirmInfo.asp](http://www.dummy.com.co/asp/contrataciones/confirmInfo.asp)
  + https://[www.dummy.com.co/Empresa](http://www.dummy.com.co/Empresa) Dummyingles/
  + https://[www.dummy.com.co/Empresa](http://www.dummy.com.co/Empresa) Dummyingles/asp/
* Se encontró que el sitio Web no limita el número de intentos fallidos que puede realizar un usuario, esto facilitaría a un usuario mal intencionado el uso de ataques por fuerza bruta para buscar credenciales de autenticación válidas. El URL con este problema es:
  + https://[www.dummy.com.mx/acceso.aspx](http://www.dummy.com.mx/acceso.aspx)
  + https://[www.dummy.com.co/acceso.aspx](http://www.dummy.com.co/acceso.aspx)
* Se encontró que única la página de inicio del sitio Web es forzada a consultarse usando el protocolo seguro HTTPS, pero las rutas secundarias de la aplicación pueden ser consultadas mediante el protocolo inseguro HTTP.

Página 56

Página 57

* Se encontró que el sitio Web mantiene lógica de programación del lado del cliente, está puede ser modificada por el usuario sin algún control sobre ella. La URL con este problema es:
  + https://[www.dummy.com.mx/asp/contrataciones/confirmInfo.asp](http://www.dummy.com.mx/asp/contrataciones/confirmInfo.asp)
  + https://[www.dummy.com.co/asp/contrataciones/confirmInfo.asp](http://www.dummy.com.co/asp/contrataciones/confirmInfo.asp)

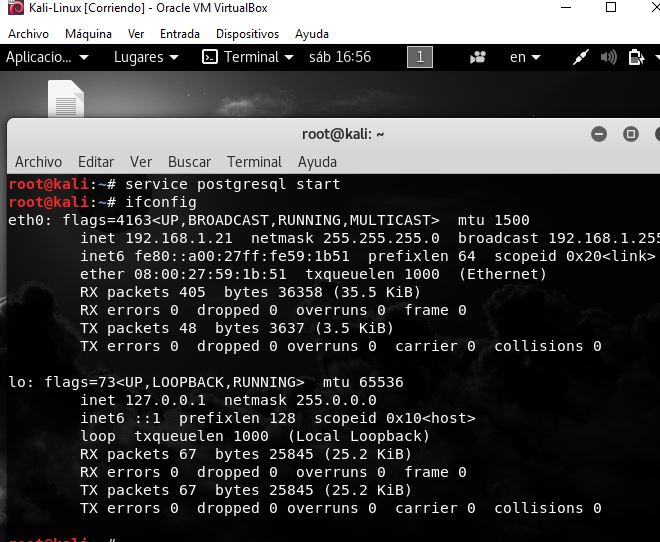
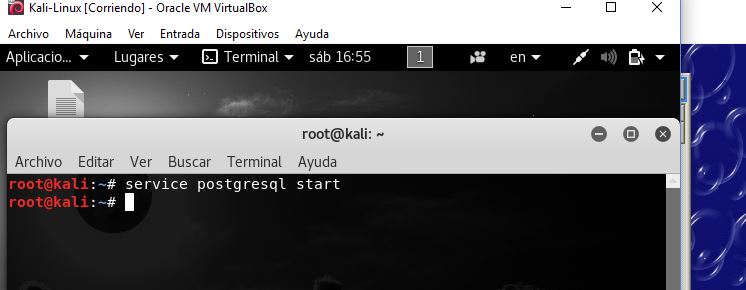
#### Recomendaciones

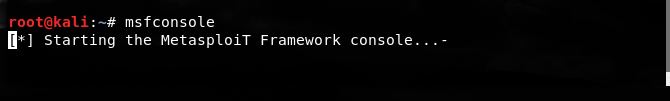
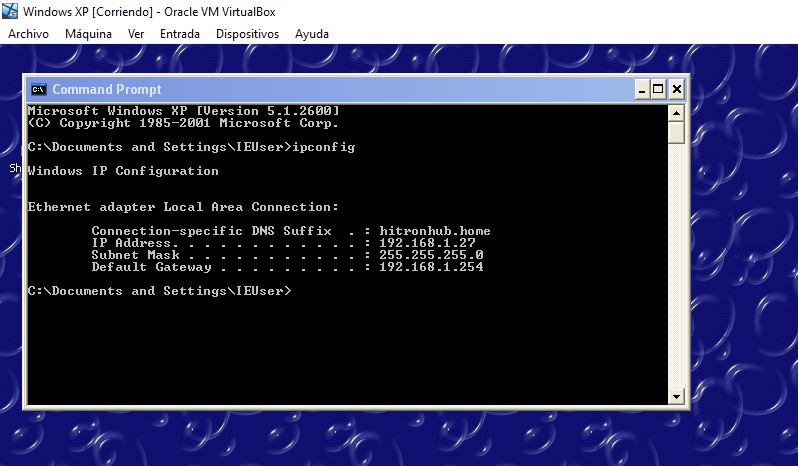
* Implementar un módulo de manejo de errores, el cual atrape cualquier error ocurrido en la aplicación y que solo muestre un código de error al usuario.
* Realizar una validación exhaustiva de todas las entradas y salidas en la aplicación, haciendo énfasis en las partes expuestas como los login. Se deben de hacer validaciones positivas de los parámetros recibidos, tanto del lado del cliente como del servidor para capturar todos aquellos intentos de inyección y desecharlos.
* Evitar colocar parte de la lógica de programación del lado del cliente, un usuario mal intencionado siempre podrá modificar información del lado del cliente, así como obtener información sobre el flujo de la aplicación en el lado del servidor.
* Es necesario redirigir el tráfico transmitido por el protocolo inseguro HTTP al canal seguro, que usa el protocolo HTTPS, y no únicamente rutas específicas de la aplicación.

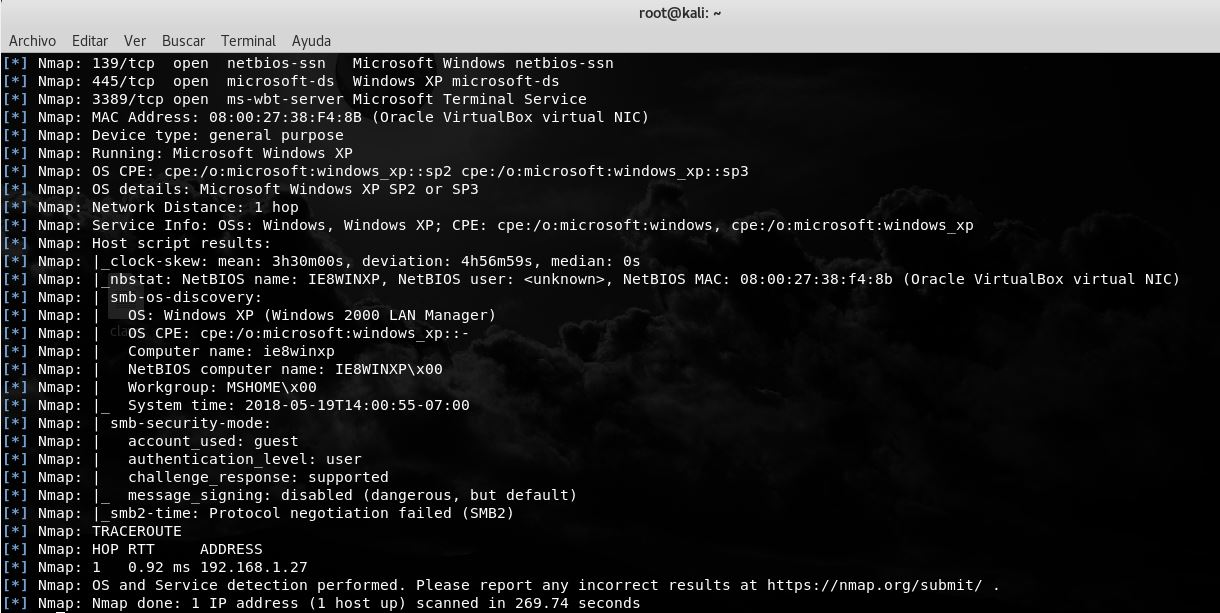
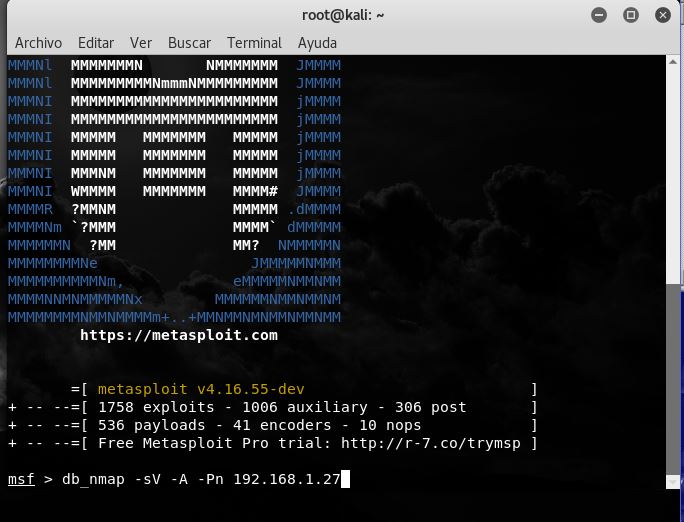


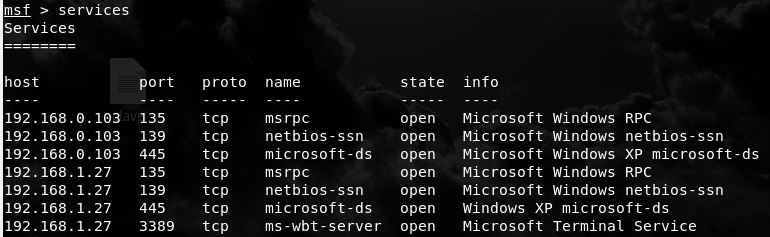
Página 58

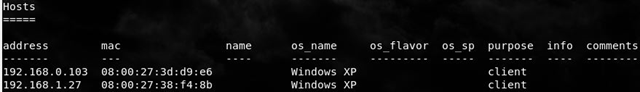
1. **Screenshots**

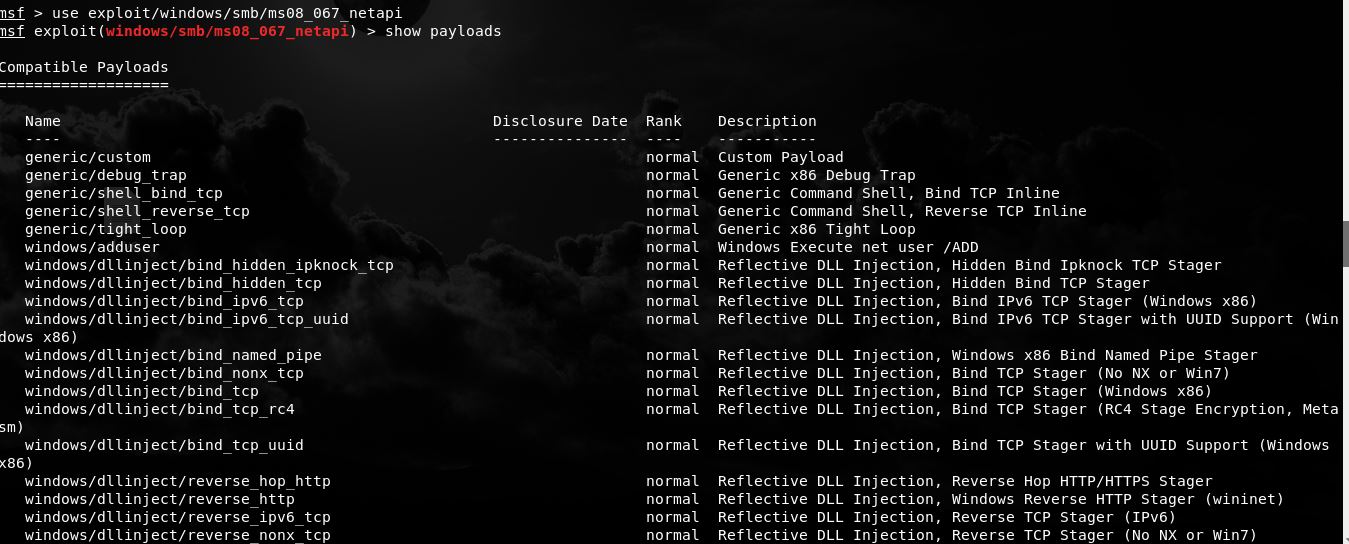
****

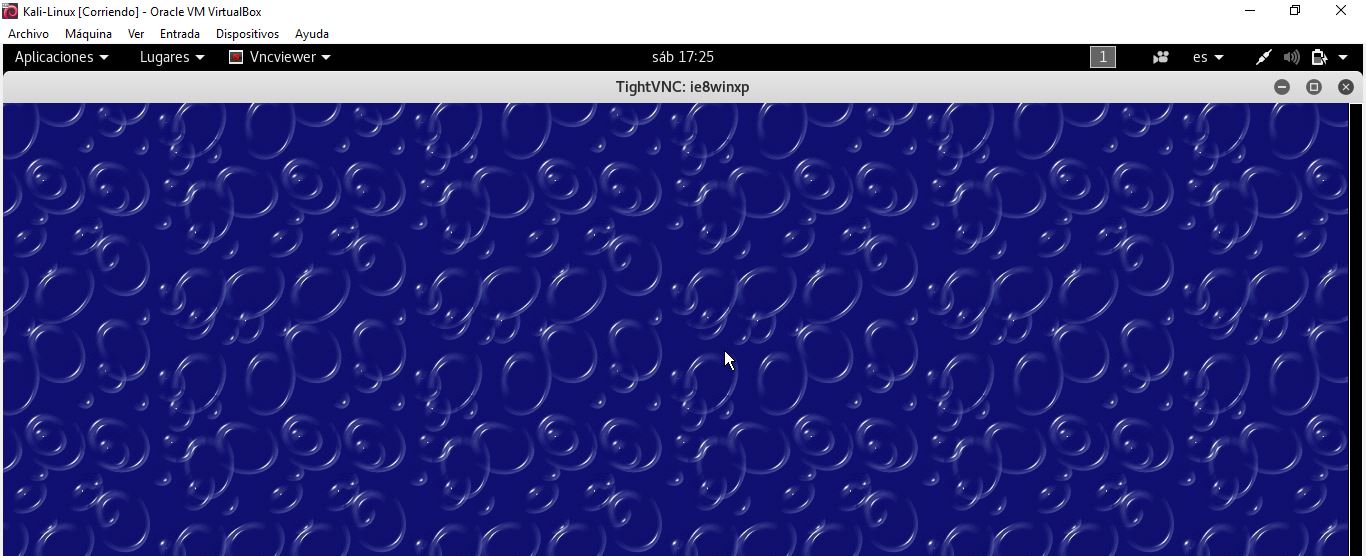
****

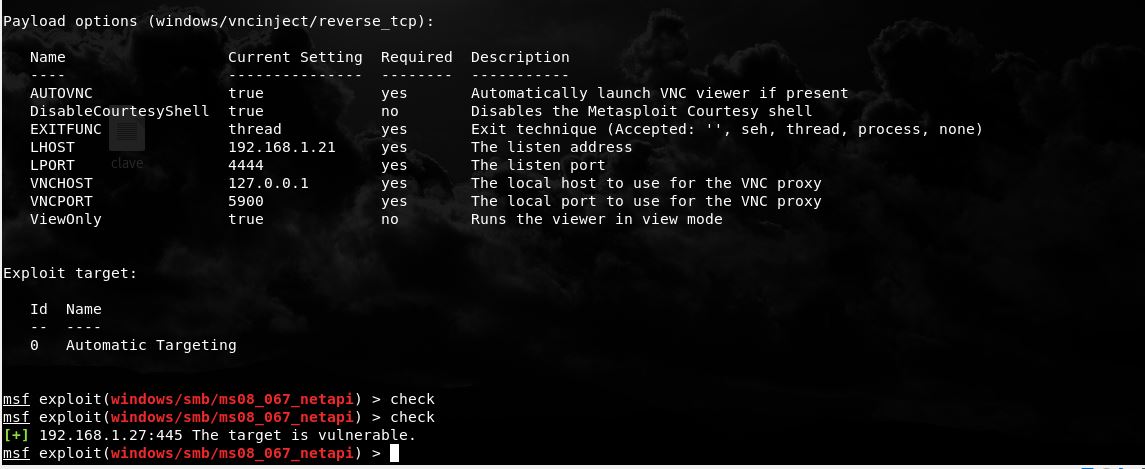
****

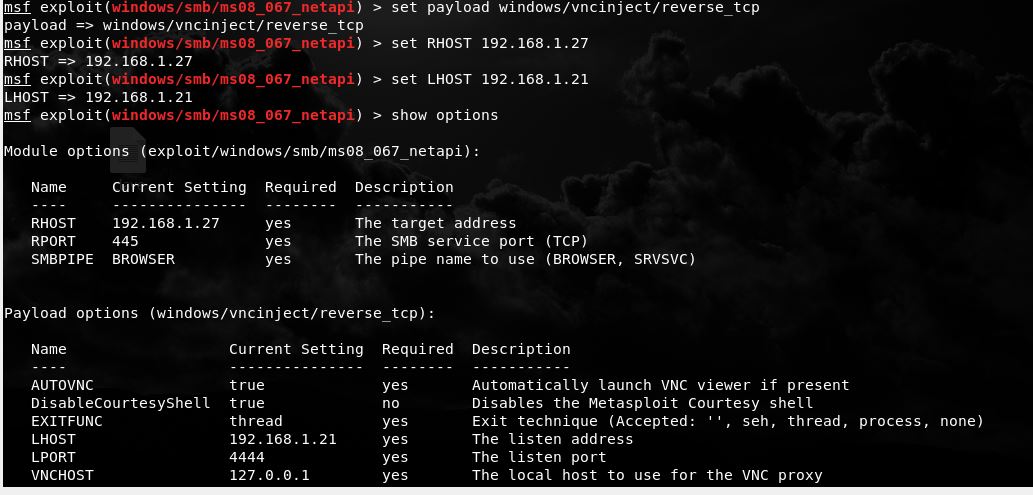
****

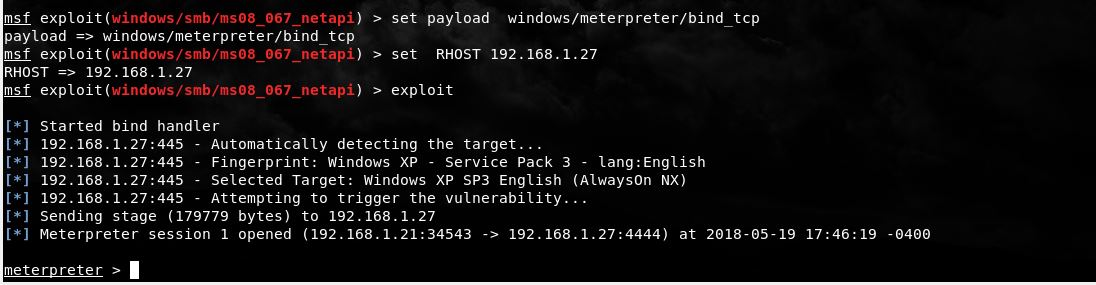
****

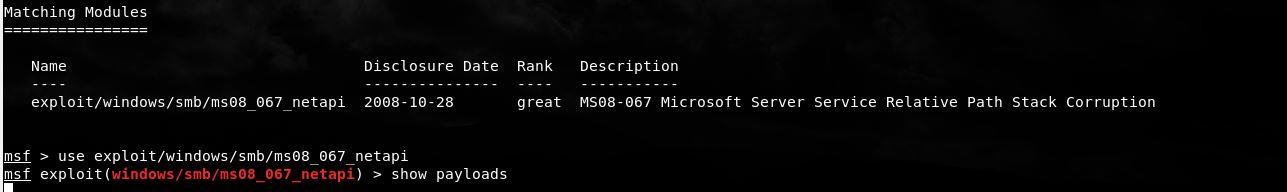
**C:\Users\Tepha\Desktop\carlos\10.JPG**

****

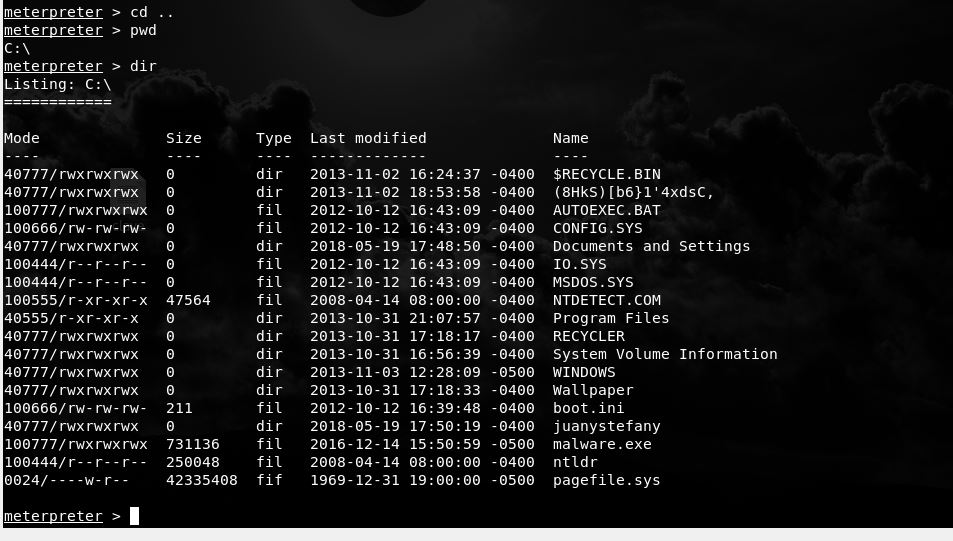
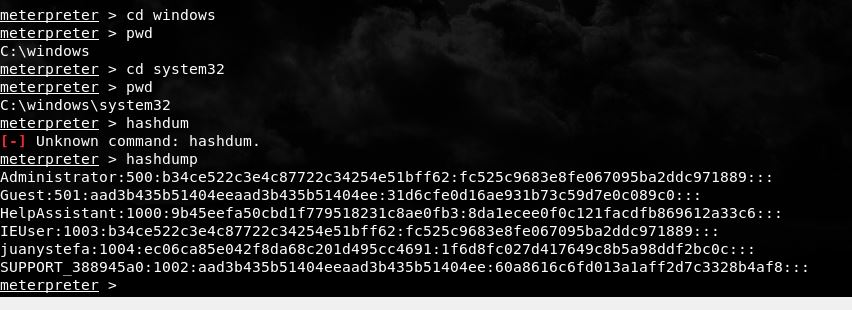
****

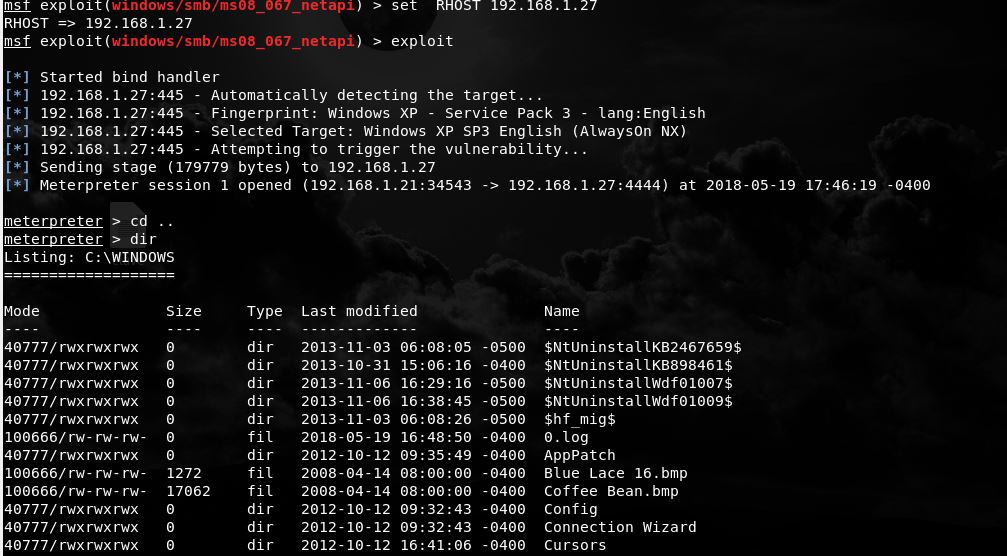
****

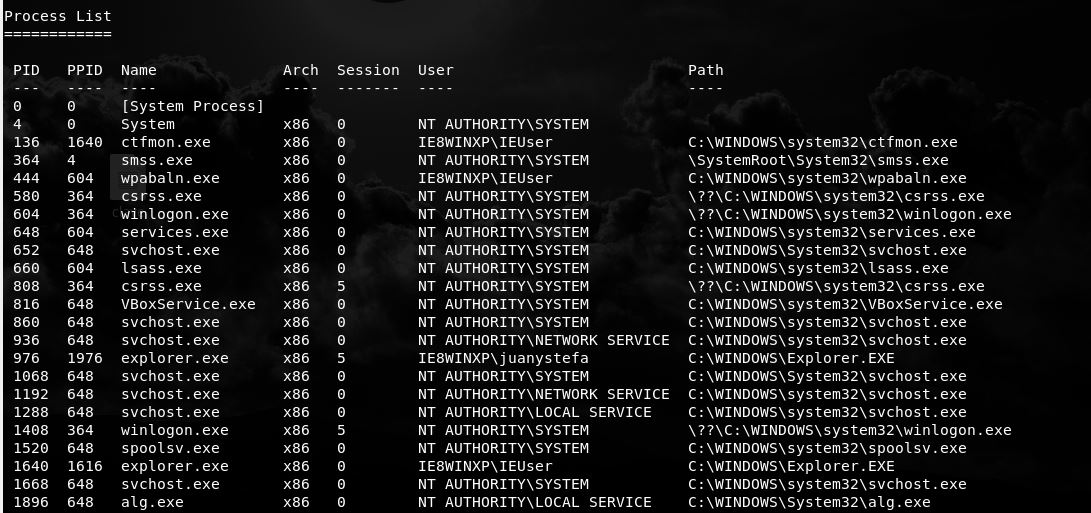
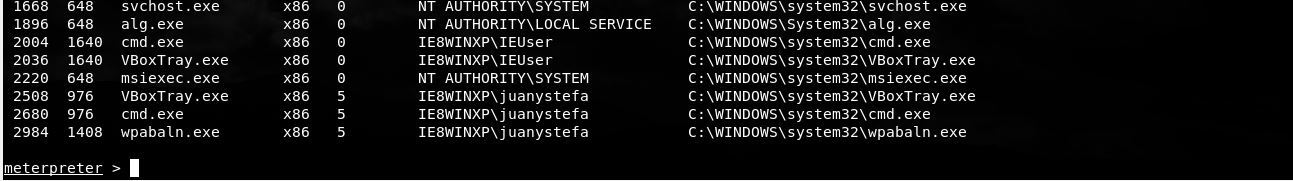
****

****

****

****

****

****

Protocolos inseguros: Uso del protocolo inseguro FTP en el servidor xxx.xxx.xxx.xxx



Página 59

1. **Anexos**
   1. **Actividades Post Pen Test**
      1. **Cambiar todas las contraseñas**

Siempre sugerimos que después de una prueba de penetración, todas las contraseñas de la red, de los sistemas operativos y de las aplicaciones deberán ser forzadas a cambiar. Para el caso específico de Windows XP, las siguientes contraseñas deberán ser consideradas:

* Contraseñas de cuentas de las aplicaciones Web.