Y **ADRIAN VARGAS CASTRILLON**

**CARLOS ALBERTO LONDOÑO LOIZA**

**SEGURIDAD EN SISTEMAS DE INFORMACION**

**CORPORACION DE ESTUDIOS TECNOLOGICOS**

**COTECNOVA**

**CARTAGO**

**2017**

2018

Evaluación de

Seguridad

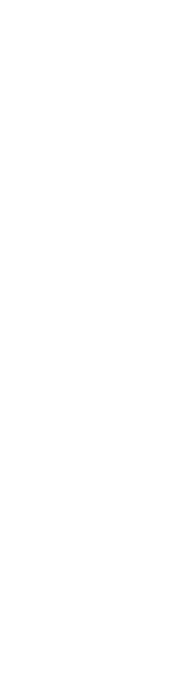
Pruebas de Penetración con Kali Linux

Windows Windows XP

Mayo 2018

Windows

Mayo 2018



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 fuera de la máquina. 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 el Sistemas Operativo 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.

#### Alcance

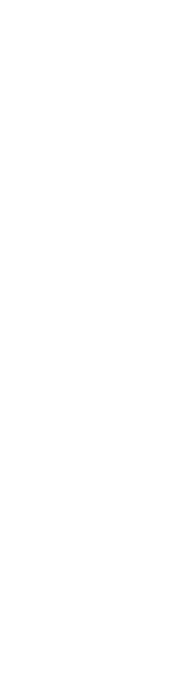
Se probó la seguridad desde internet hacia la red externa de Windows XP.

#### Objetivos Específicos

Se definieron varios objetivos externos que correspondían, principalmente, a la obtención de información que están expuestos a Internet.

**Objetivos**

* **Obtención de información**
* **Enumeración de sistemas**
* **Análisis de vulnerabilidades**
* **Explotación de vulnerabilidades**
* **Ataques contra credenciales**
* **Evasión de medidas de seguridad**
* **Post explotación al sistema**
* **Subir archivos equipo victima**
* **Puerta trasera**



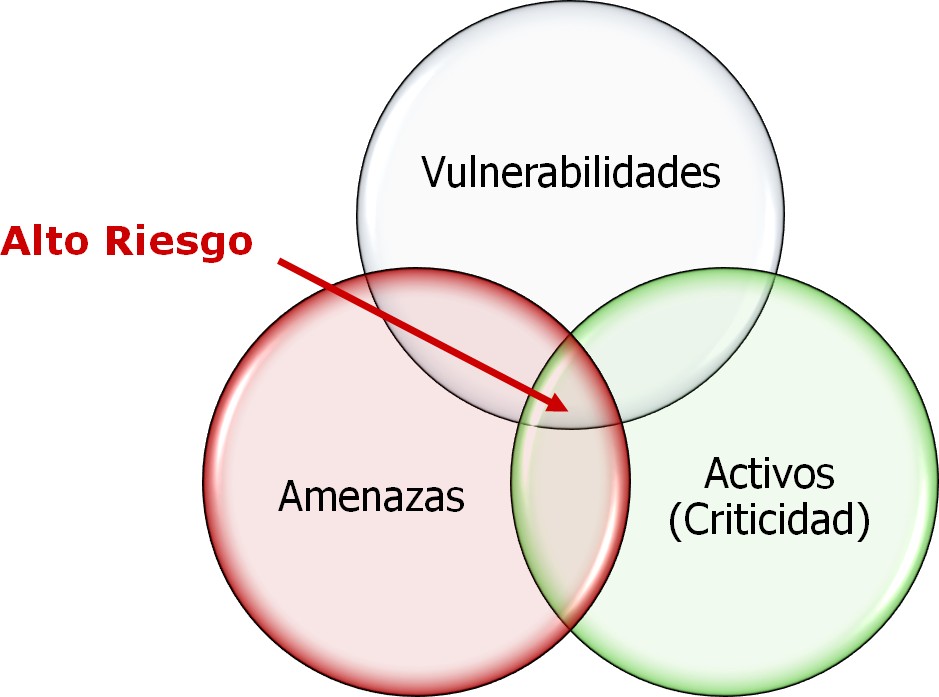
Página 5

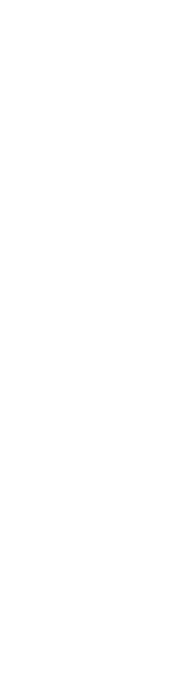
### Pruebas realizadas

Las pruebas que se realizaron consistieron en: Ingresar a sistemas y aplicaciones, adivinar o romper contraseñas, descubrir y abusar vulnerabilidades, revisión del proceso de respuesta a incidentes, así como la intercepción de comunicaciones.

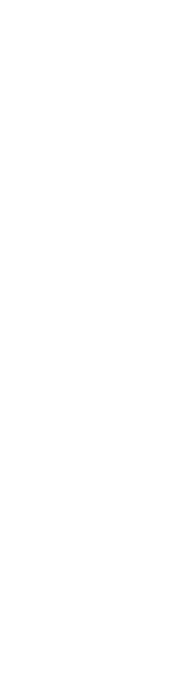
Estas pruebas son elaboradas desde diferentes capas de la infraestructura que incluyen software propietario, servidores de base de datos, sistemas operativos, dispositivos de red, consolas de administración y diferentes puntos y formas de conexión.

### 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 | | |

# Introducción

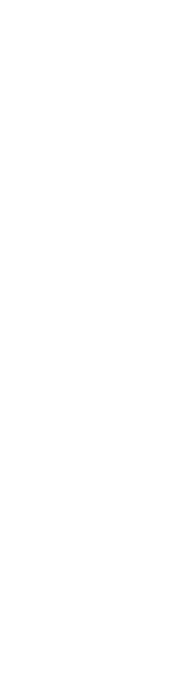
## Consideraciones Generales

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 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

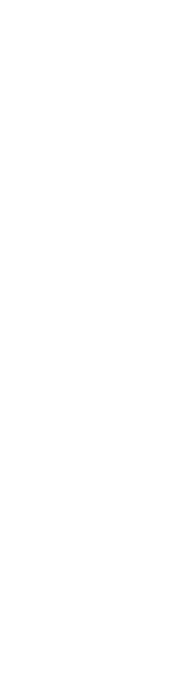
representar las principales amenazas a las que se encuentra expuesta una empresa con presencia en Internet en la actualidad.

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

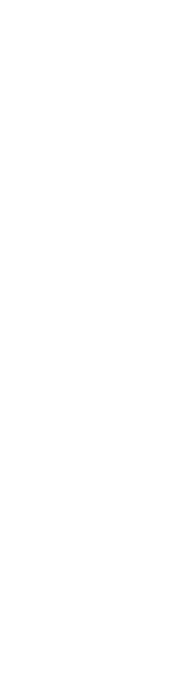
Las políticas en las cuales Proveedor se basa para proporcionar sus servicios son:

* + - 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 Carlos Londoño 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.

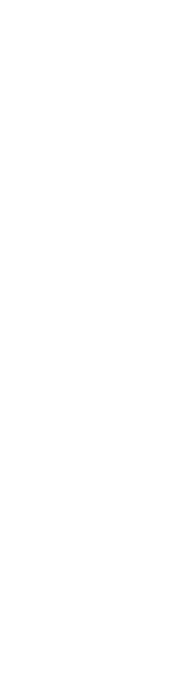
## Meta de la prueba

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:

* **Obtención de información**
* **Enumeración de sistemas**
* **Análisis de vulnerabilidades**
* **Explotación de vulnerabilidades**
* **Ataques contra credenciales**
* **Evasión de medidas de seguridad**
* **Post explotación al sistema**

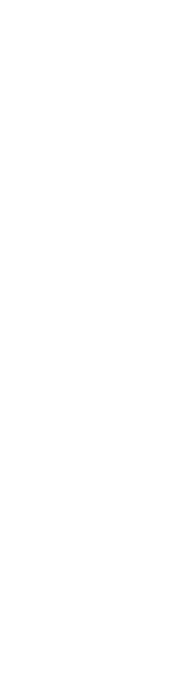
## Pruebas Realizadas

Para hacer este diagnóstico se hicieron las pruebas siguientes:

### Penetración por Red Externa

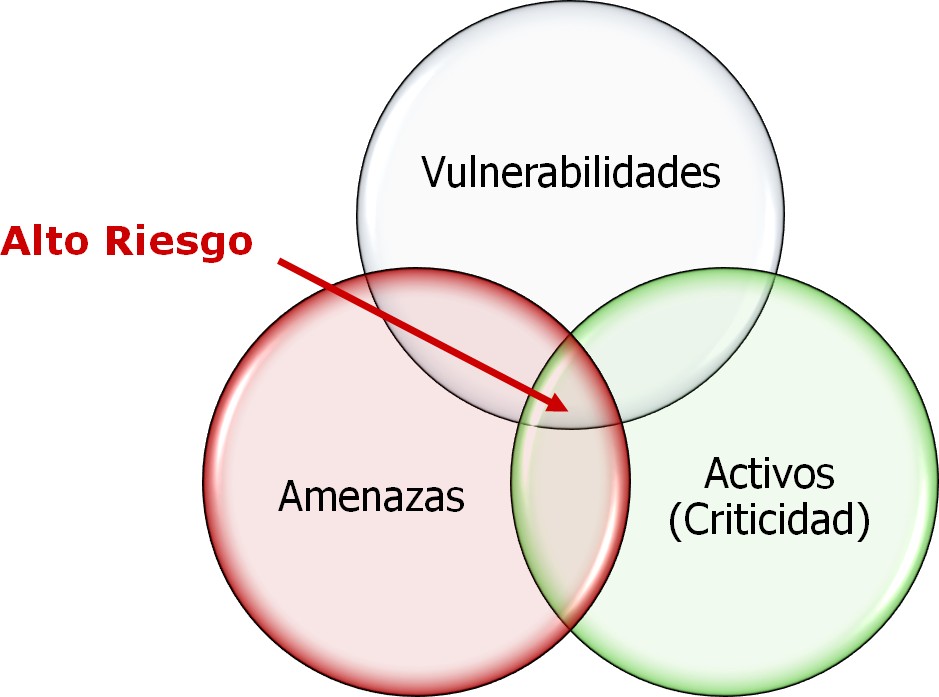
* + - * Analizar la red.
      * Identificar servidores y puertos.
      * Detectar vulnerabilidades en servidores.
      * Revisar debilidades de la red.
      * Determinar servidores críticos.
      * Determinar avenidas de acceso.
      * Enumerar usuarios.
      * Probar contraseñas.
      * Determinar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

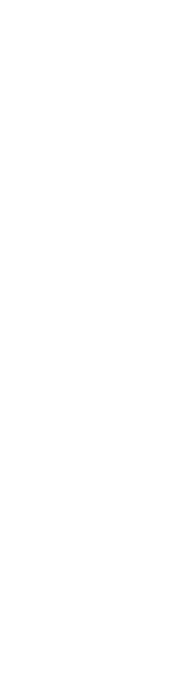
### Expansión de Influencia

* + - * 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

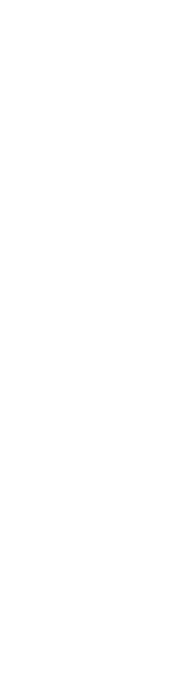
Página 20

# 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

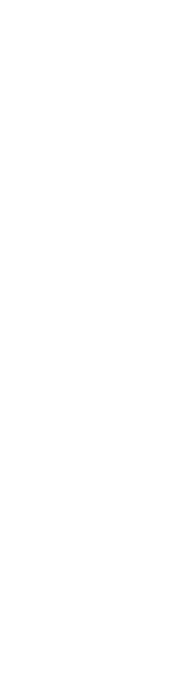


Página 22

## 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.

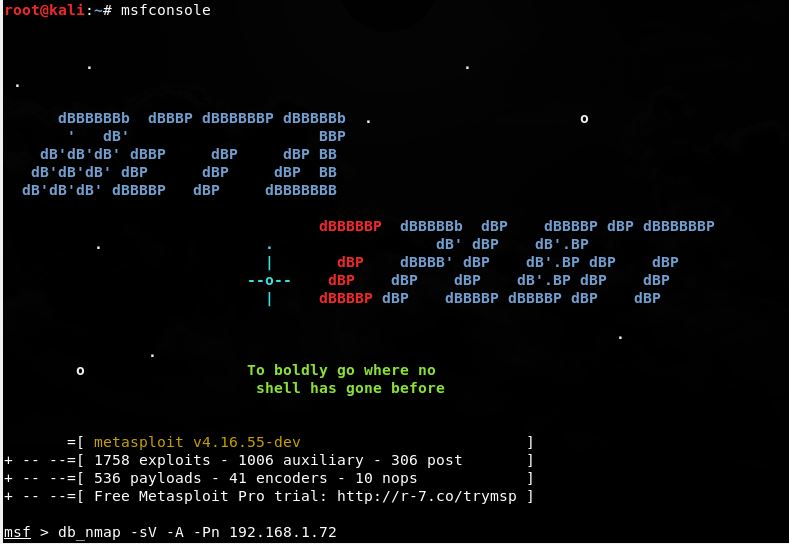
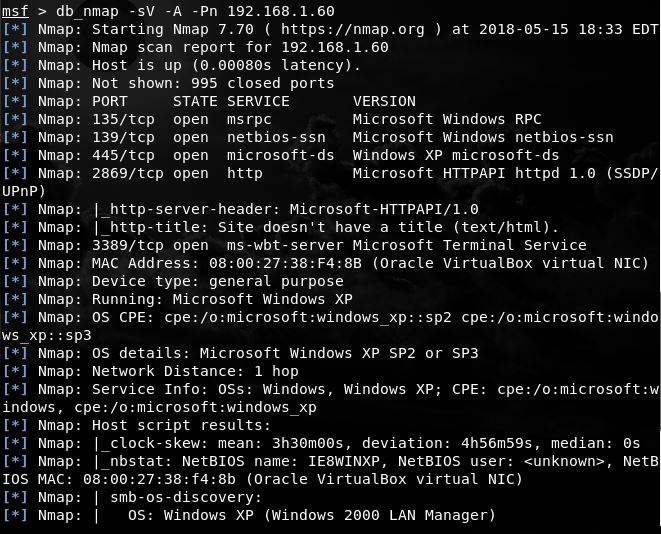
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Nivel de Acceso** | | **Perfil del Atacante** | |  |  |
| **Acceso Restringido** | | No es posible tener comunicación con el sistema en cuestión | **Ataque Dirigido** | Un grupo de personas con complicidad con el personal de la 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 | | |



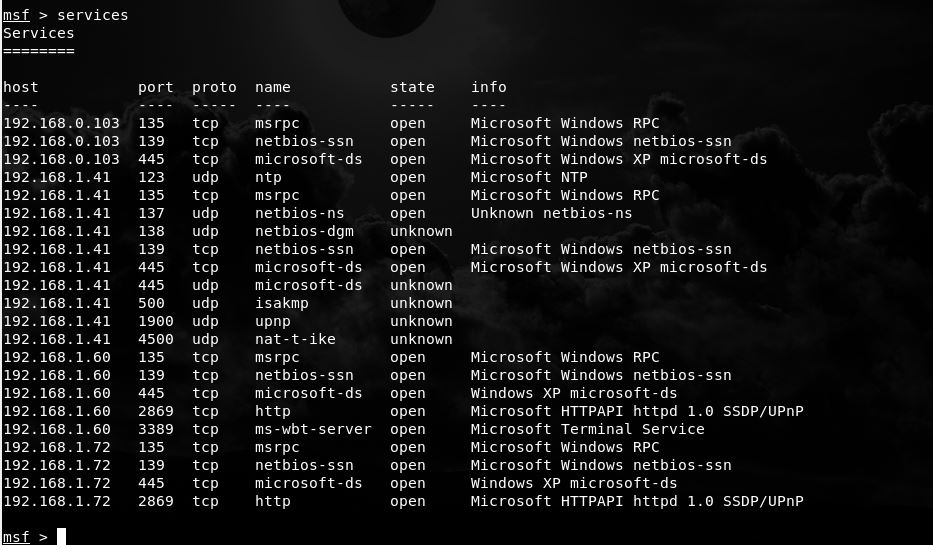
Página 23

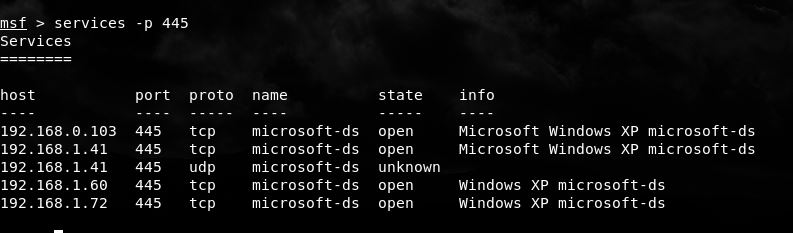
## Resultados

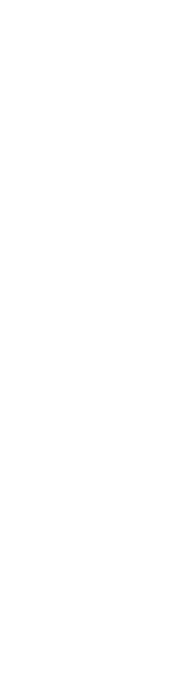
El resultado qué a continuación se muestra está basado en una estadística que se lleva a cabo en Proveedor con los resultados de Hackeos Éticos que se han realizado a empresas semejantes y con un tamaño similar al de Windows XP.



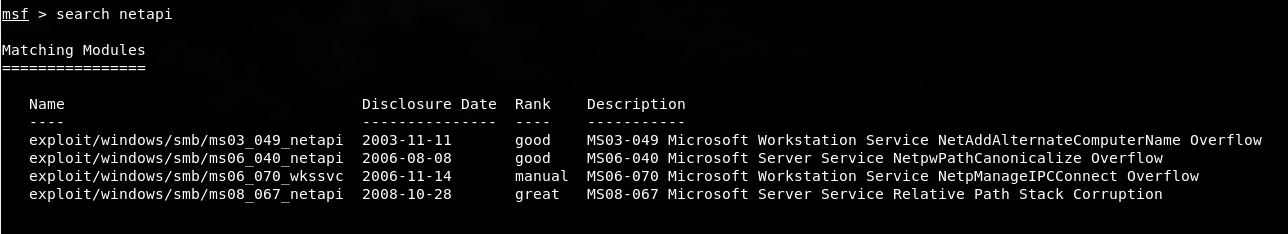


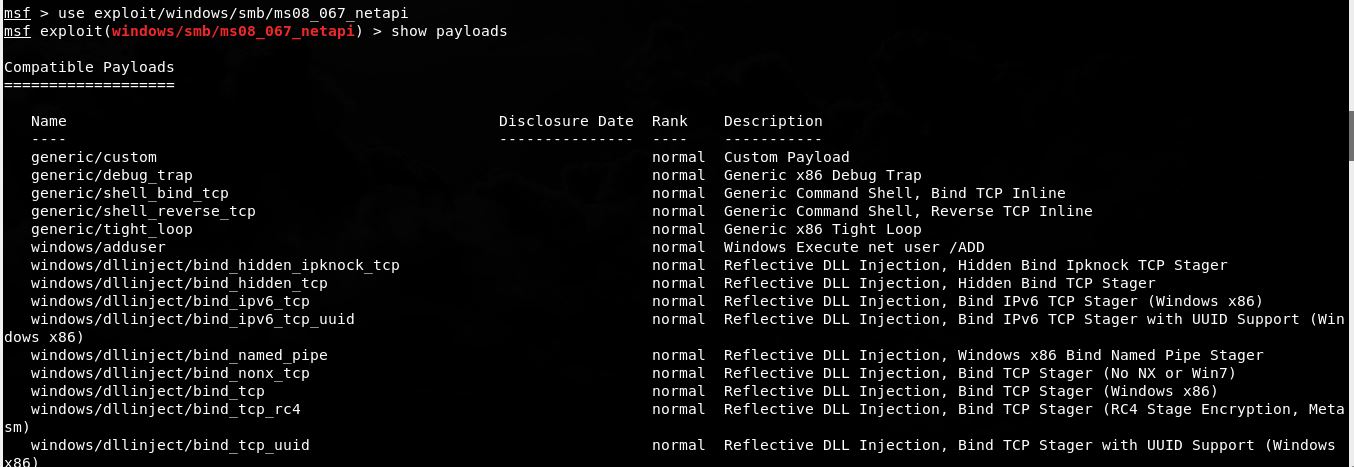


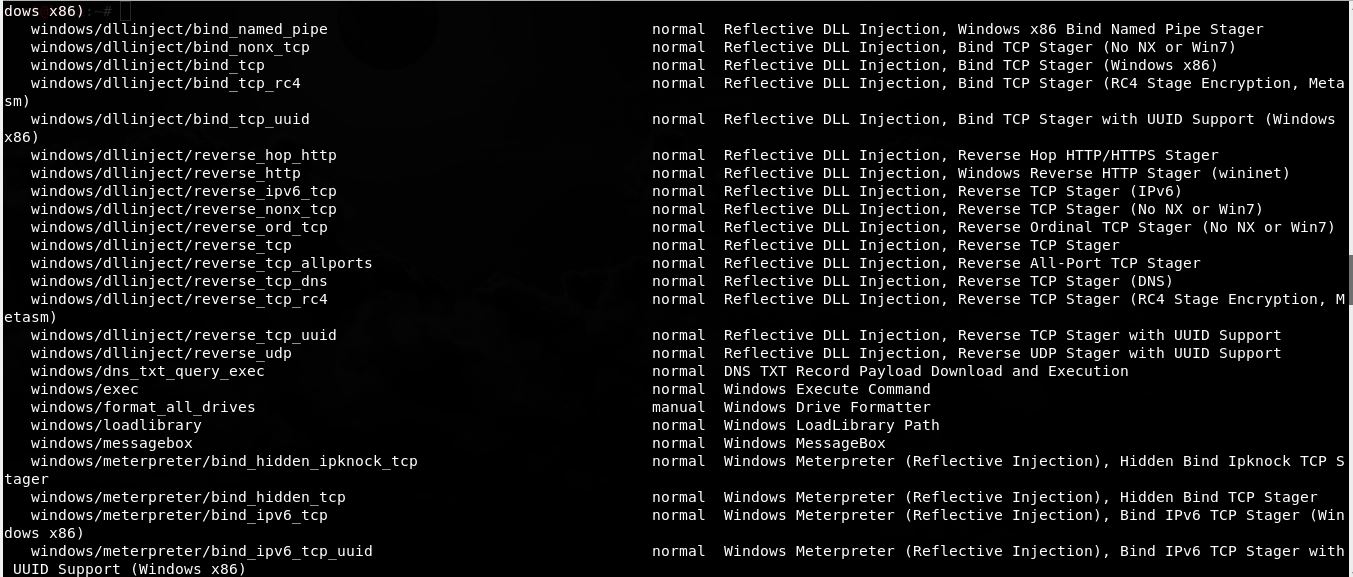




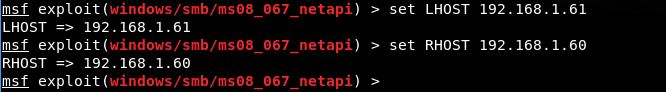
Página 28

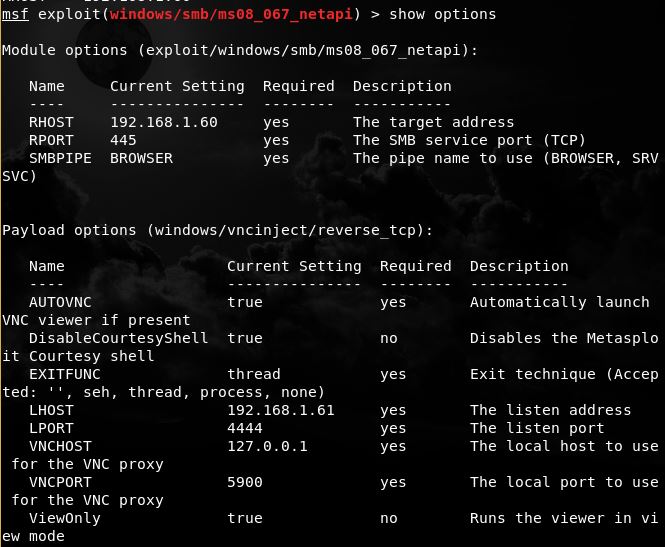


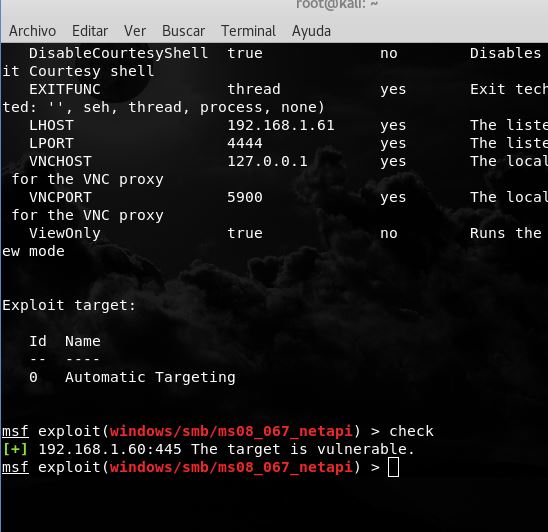




C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\8.JPG









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.

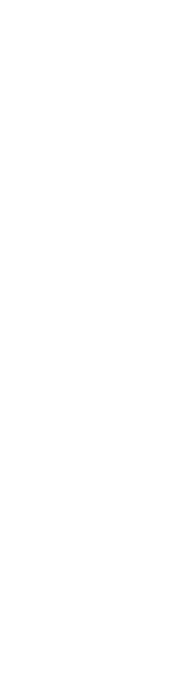
**Probabilidad Alta**

**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.

# Listado de accione ejecutadas

# obtención de usuarios y creación de directorio C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\14 mostra usuarios del sistema.JPG

# C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\15.JPG

# C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\15_1.JPG

# C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\15-2.JPG

# C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\16_loque estacorriendo en windows.JPG

# C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\17-1diretoriopropio.JPG

# C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\17-direcotio.JPG

# Ataques

# C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\12.JPGC:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\11ataque.JPG

# C:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\10ataque.JPGC:\Users\SALA E-13\Desktop\segurida_en la red 2\trabajo metasploi_meteperte\10_1_1.JPG+

# 

# Armitage

# C:\Users\SALA E-13\Desktop\segurida_en la red 2\armitage\11-1.JPGC:\Users\SALA E-13\Desktop\segurida_en la red 2\armitage\11.JPGC:\Users\SALA E-13\Desktop\segurida_en la red 2\armitage\6.JPGC:\Users\SALA E-13\Desktop\segurida_en la red 2\armitage\5ataque.JPGC:\Users\SALA E-13\Desktop\segurida_en la red 2\armitage\4ataque.JPGC:\Users\SALA E-13\Desktop\segurida_en la red 2\armitage\3puertos.JPGC:\Users\SALA E-13\Desktop\segurida_en la red 2\armitage\2pign.JPGC:\Users\SALA E-13\Desktop\segurida_en la red 2\armitage\1detetarsitemaoperativo.JPG

# Recomendaciones

# Se pueden realizar trabajos de investigación relacionados para:

# • Comparar las herramientas comerciales más destacadas en este campo con

# las seleccionadas y más destacadas de Kali para detectar aquellas

# características que quizás pueden ser complementadas con más de una

# herramienta de código abierto.

# • Contrastar herramientas que existen en la distribución que puedan estar

# proporcionando características similares que otras existentes dentro del

# mismo grupo.

# • Investigar como se puede asegurar la seguridad en campos específicos

# como: industriales, administrativos, tecnológicos, comerciales de tal forma

# que la utilización de un compendio de herramientas de código abierto

# permita asegurar entornos específicos.

# Además es posible encaminar este tipo de investigaciones hacia trabajos totalmente

# prácticos que permitan:

# • La creación y configuración de ambientes o laboratorios de pruebas que

# ofrezcan un entorno local para el entrenamiento y capacitación del hacker

# ético.

# • Creación de una academia virtual que permita la capacitación y medición de

# conocimientos del principiante de hacker ético, basándose en herramientas

# de código abierto.

# Bibliografía

# [1] A. Charles. (2014, Septiembre) The Guardian. [Online].

# http://gu.com/p/4x7fv/sbl

# [2] D. Sanger and J. Hirschfeld. (2015, Junio) The New York Times. [Online].

# http://nyti.ms/1M8MiRG

# [3] 2013/2014 Informe Global sobre Fraude. (2014) Kroll. [Online].

# http://fraud.kroll.com/wp-content/uploads/Reporte de Fraude Kroll 2013-2013

# Espanol - WEB.pdf

# [4] R. Aguirre. (2006) Libro electrónico de Seguridad Informática y Criptografía.

# [5] C. Tori, Hacking Ético, 1st ed. Buenos Aires, Argentina: Mastroianni Impresiones,

# 2008.

# [6] M. Rhodes-Ousley, Information Security The Complete Reference, 2nd ed. Estados

# Unidos: McGraw-Hill, 2013.

# [7] D. Kim and M. Salomon, Fundamentals of Information Systems Security.: McGrawHill,

# 2010.

# [8] K. Astudillo B., Hacking ético 101: Cómo hackear profesionalmente en 21 días o menos.

# Guayaquil, Ecuador, 2013.

# [9] P. González Pérez, Metasploit para Pentesters. Madrid, España: 0xWORD

# Computing S.L., 2014, pp. 26-29.

# [10] J. Muniz, Web Penetration Testing with Kali Linux.: Packt Publishing Ltd, 2013.

# [11] M. Ramilli M. Prandini, Towards a practical and effective security testing

# methodology, 2010, pp. 320-325.

# [12] OSSTMM 3 – The Open Source Security Testing Methodology Manual. (2010)

