Instituto Universitario Aeronáutico

Facultad de Ingeniería

PROYECTO DE TRABAJO FINAL DE GRADO (TFG)

Reingeniería de la Red de Datos de la Empresa MR Seguridad S.A. y Formulación de un Diseño Basado en la Norma ISO 27000

Profesor/a Tutor:

- Ing. Eduardo Casanovas

Integrantes:

- Manzotti, Marcos Javier
- Rivilli, Diego Javier

Fecha:

- Febrero del año 2017

1. DEDICATORIA

Dedicamos este trabajo a nuestras familias, amigos, a nuestros compañeros de curso y laborales, que con su apoyo, paciencia y dedicación, logramos llevar a buen término este proyecto.

2. AGRADECIMIENTOS

Agradecemos especialmente a los ingenieros Eduardo Casanovas, por su colaboración, paciencia y dedicación para guiarnos con sus conocimientos en este proyecto.

Queremos agradecer también a los Gerentes de la Empresa MR Seguridad S.A., por brindarnos su colaboración e información y un entorno de trabajo apropiado para desarrollar este proyecto.

A nuestros familiares y aquellas personas que con su aporte y presencia, nos facilitaron la confección y conclusión de nuestro proyecto.

3. TÍTULO DEL PROYECTO

Reingeniería de la red de datos de la empresa MR Seguridad S.A. y formulación de un diseño basado en la norma ISO 27000.

4. HOJA DE ACEPTACIÓN DEL TRABAJO FINAL

5. ÍNDICE

5.1. ÍNDICE GENERAL

5.2. ÍNDICE DE FIGURAS Y TABLAS

6. GLOSARIO Y LISTADO DE SÍMBOLOS Y CONVENCIONES

- **ADSL:** es una tecnología de acceso a Internet de banda ancha, lo que implica una velocidad superior a una conexión por módem en la transferencia de datos. Consiste en la transmisión analógica de datos digitales apoyada en el cable de pares simétricos de cobre que lleva la línea telefónica convencional siempre y cuando la longitud de línea sea de hasta inclusive 5,5 km medidos desde la central telefónica, o no haya otros servicios por el mismo cable que puedan interferir.
- **Fingerprint:** es una técnica que consiste en analizar las huellas que deja un sistema operativo en sus conexiones de red. Está basada en los tiempos de respuesta a los diferentes paquetes, al establecer una conexión en el protocolo TCP/IP, que utilizan los diferentes sistemas operativo.
- **Firewall:** Un cortafuegos (firewall) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- **Hardware:** se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado
- **Interconexión:** es la conexión física y lógica entre dos o más redes de telecomunicaciones.
- **Latencia de Red:** se denomina latencia a la suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.
- **Modem:** dispositivo que convierte las señales digitales en analógicas (modulación) y viceversa (demodulación), permitiendo la comunicación entre computadoras a través de la línea telefónica o del cable módem. Este aparato sirve para enviar la señal *moduladora* mediante otra señal llamada *portadora*
- **MPLS:** es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP

- **PCs, Equipo de escritorio:** equipo informático personal.
- **Puerto:** Son puntos de acceso entre equipos para el uso de servicios y flujo de datos entre ellos, ejemplos: el puerto 21 correspondiente al servicio FTP (permite el intercambio de archivos) ó el puerto 515 que está asociado con el servicio de impresión.
- **Red de Datos (network):** conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.
- **Router:** es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra
- **Servidor:** Equipo informático en el que se ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes, tanto si se trata de un equipo informático central (*mainframe*), una equipo informático personal, una PDA o un sistema embebido; sin embargo, hay equipos informáticos destinados únicamente a proveer los servicios de estos programas: estos son los servidores por antonomasia.
- **Sistema Operativo, Software de Base:** es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes.
- **Software:** equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.
- **Software GNU:** es el software que respeta la libertad de los usuarios y la comunidad. En grandes líneas, significa que los usuarios tienen la libertad para ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software.
- **Switch:** es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.
- **VLAN:** acrónimo de *virtual LAN* (Red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico (Switch) o en una única red física.

- **VPN:** (Virtual Private Network), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
- **Vulnerabilidades:** En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

  Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro. Por lo tanto existen vulnerabilidades teóricas y vulnerabilidades reales (conocidas como exploits).

7. RESUMEN

Se realizó una reingeniería de la Red de Datos de la empresa MR Seguridad S.A., dedicada a brindar, por el momento, distintos servicios de seguridad física a diversas empresas y piensa extender sus prestaciones a servicios de consultoría e implementación de seguridad informática. Para esto, la empresa necesita llevar a cabo un análisis de su infraestructura de conectividad y seguridad de los datos.

Este trabajo tiene por objetivo identificar y evaluar, con distintas herramientas seleccionadas, el desempeño de los equipos que componen la red (PCs, Switchs, Routers, Servidores, etc), determinar el rendimiento y capacidad actual de toda la red, cuellos de botella, fallas y amenazas de seguridad. Con los datos obtenidos generar informes y recomendaciones para la optimización de la red.

Utilizando el método empírico-analítico a través de la observación científica y de la medición de variables seleccionadas, con diversas herramientas de testeo de red, fue posible recabar la información necesaria, siguiendo el lineamiento de las normas de seguridad actuales, cumpliendo con los objetivos planteados al comienzo del trabajo.

8. PALABRAS CLAVES

Sistema Operativo, Firewall, Hardware, Interconexión, Modem, MPLS, PC, Red de datos, Banda Ancha, Router, Conexiones de red, Servidores, Firewall, Switch, Software, Local, ISO 27000, Latencia de Red, Vulnerabilidades, Puertos, Retina CS, Zenmap, Escaneo, Fingerprint, Networking.

9. INTRODUCCIÓN

MR Seguridad S.A. es una empresa con sede central en la ciudad de Córdoba y dedicada a brindar distintos servicios de seguridad física a diversas empresas. MR Seguridad S.A. tiene una larga trayectoria en la provincia de Córdoba y se ha distinguido por tener un crecimiento vertiginoso en los últimos años. Geográficamente se distribuye en una casa matriz situada en Córdoba Capital; y diez locales, cinco en la ciudad de Córdoba y cinco en el interior de la provincia.

MR Seguridad S.A., se ha planteado como objetivo a futuro, prestar servicios de consultoría e implementación de seguridad informática en los sistemas de sus clientes, y como primera actividad, decide llevar a cabo un análisis de su infraestructura de conectividad y seguridad de los datos, con el fin de subsanar las irregularidades que se identifiquen y de obtener conocimientos y herramientas, que le sean de utilidad en el futuro.

10. OBJETIVO DEL PROYECTO

10.1. OBJETIVO GENERAL

Realizar el diagnóstico y recomendaciones para el funcionamiento optimizado y seguro de la red de la empresa MR Seguridad S.A.

10.2. OBJETIVOS ESPECÍFICOS

1) Identificar los equipos que componen la red de la empresa y los medios que se utilizan para su interconexión.
2) Evaluar el desempeño individual y colectivo de los elementos identificados utilizando distintas herramientas de prueba de red GNU y gratuitas.
3) Determinar el rendimiento y capacidad actual de toda la red, posibles cuellos de botella, puntos de falla y amenazas de seguridad.
4) Generar informes a la dirección que contengan los datos obtenidos y las recomendaciones para un funcionamiento óptimo y seguro de la red a mediano plazo.
5) Seleccionar herramientas de seguridad para ser utilizadas junto con los mecanismos de control implementados.

11. DESTINATARIOS

La empresa seleccionada para realizar el proyecto se denomina "MR Seguridad S.A.". Está dedicada a la prestación de servicios de seguridad física en la Ciudad de Córdoba y en distintas localidad de la provincia.

11.1.IDENTIFICACIÓN DE LA EMPRESA

Razón social:

MR Seguridad S.A.

Objeto social:

La entidad tendrá por objeto la prestación de servicios de seguridad.

Domicilio:

MR Seguridad S.A. Oficina Central, se encuentra ubicada en la calle Colón 1170. Córdoba Capital.

Teléfono:

4723351.

Clasificación:

- Según la integración del capital es privada.
- Organización con fines de lucro.
- Es una empresa mediana.
- El alcance geográfico es provincial.
- Según la duración es permanente.
- Tiene un tipo de actividad de prestaciones de servicios.

11.2. OBJETIVOS Y POLITICAS GENERALES

Ver Anexo 1 en la página 125.

11.3.RESEÑA HISTORICA

Ver Anexo 2 en la página 126.

11.4.DATOS DEL PERSONAL

Ver Anexo 3 en la página 127.

11.5.DATOS DEL ENTORNO ESPECÍFICO

Ver Anexo 4 en la página 130.

12. BENEFICIOS

La empresa MR Seguridad S.A. y sus empleados son los beneficiarios directos del proyecto, debido a que una actualización y mejora en la base de conocimientos del funcionamiento interno de la red de datos, mejora la eficacia y eficiencia de los recursos humanos que le dan soporte a la misma, lo que incide directamente en la operatividad de la red de la empresa.

Con el desarrollo del presente proyecto, la empresa obtuvo información de la capacidad que tienen los empleados para el manejo y configuración no solo de los equipos de red, sino también de los servidores y equipos de escritorio. Con la cual se logró realizar un esquema de las capacitaciones que les pueden ayudar a mejorar su desempeño en el trabajo, además una buena configuración de los mismos beneficia la seguridad de la red de datos de MR Seguridad S.A.

Con el relevamiento realizado, la empresa fue beneficiada en el conocimiento del diseño actual de su red y de los equipos de interconexión que la conforman, los cuales no se encontraban bien documentados y no estaban conformes a las normas ISO. Esto facilitará a la empresa resolver más rápidamente posibles problemas, incluso cualquier personal idóneo aun siendo externo a la misma, podrá informarse en la estructura de la red y la conformación de la misma.

También se informó a la empresa del estado de los equipos de red, y se determinó cuáles no reciben más soporte ni actualización de software por parte del fabricante. Con esta información, la empresa podrá desarrollar un diagrama de renovación, dándoles prioridad a los equipos que lo requieran, evitando así poner en riesgo la seguridad de la red, debido a posibles vulnerabilidades de equipos fuera de su vida útil.

Con el análisis de los equipos, puertos abiertos y de las vulnerabilidades, se puede generar en un futuro cercano, un esquema que proteja los activos más críticos de la empresa, en función de los distintos criterios de protección que puedan tener los responsables.

También se midió el estado y los tiempos de conexión entre distintos equipos, dentro la misma red y entre las distintas redes y Vlans, obteniendo una valoración que expresa el estado del funcionamiento de la red.

13. ESTUDIO TÉCNICO

El proyecto se realizará en base a elementos de hardware de conectividad de red que ya existen en la empresa.

Las herramientas de análisis de la red de datos serán:

- Un lan tester, se utilizará para verificar el correcto funcionamiento de la red a nivel de capa física.
- Una notebook con software de análisis de red previamente instalado, con la cual se llevará a cabo el análisis de los distintos elementos que componen la red de la empresa. Para evitar generar costos extras, se intentara utilizar software Libre (licencia GNU) o gratis y se pondrán en práctica los conocimientos adquiridos durante el cursado de la carrera de Ingeniería de Sistemas.

14. DESARROLLO DEL TRABAJO

14.1. RESUMEN TÉCNICO:

Este punto no aplica.

14.2. METODOLOGÍA:

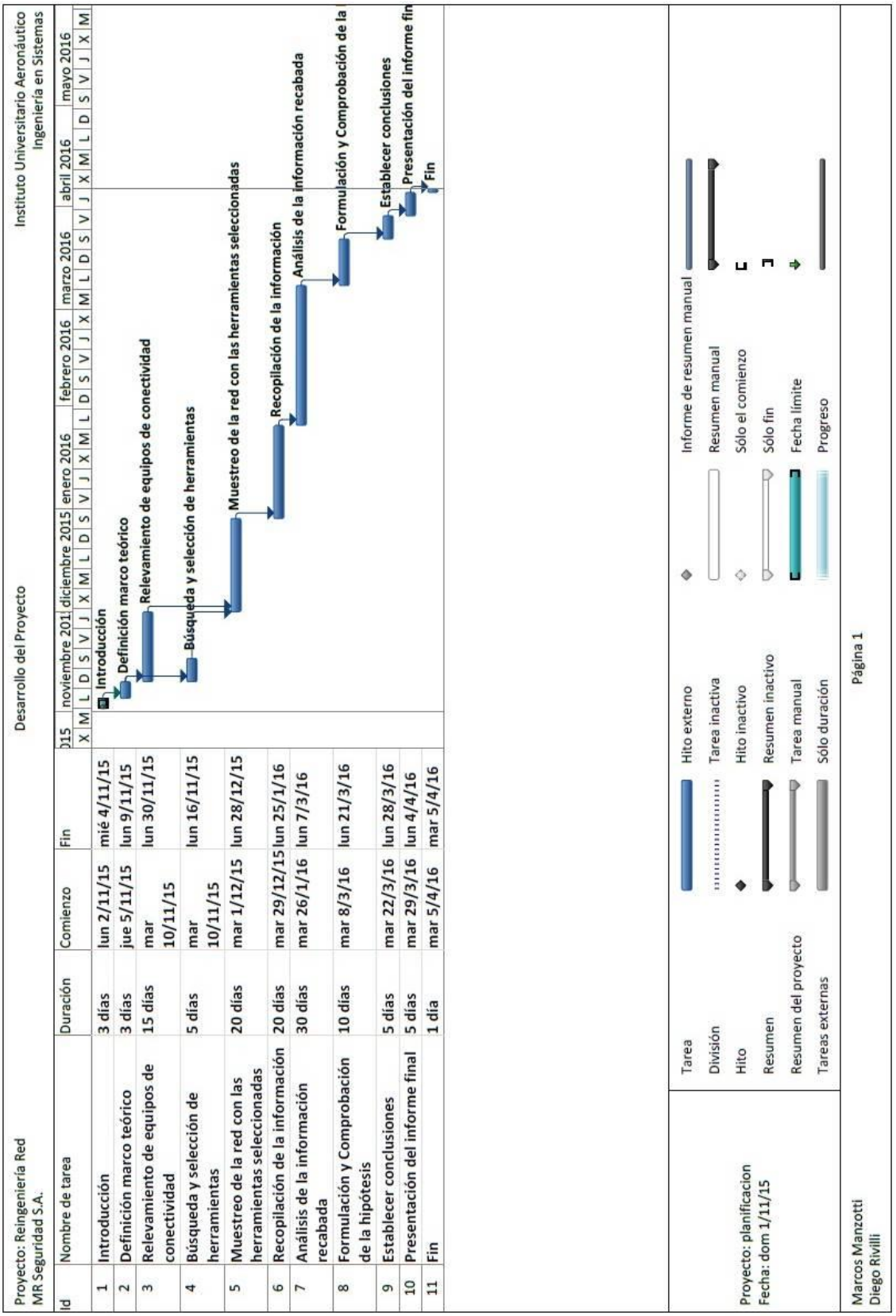
Se empleó el paradigma positivista, el mismo dio a través del empleo de la razón y las directrices propias del paradigma, una línea de pensamiento a seguir, para así, describir los fenómenos que acontecen en la red de la empresa, de manera realista y medible.

Utilizando el método empírico-analítico a través de la observación científica y de la medición de variables seleccionadas, con diversas herramientas de testeo de red, fue posible recabar la información necesaria y así poder cumplir con los objetivos planteados del proyecto.

14.2.1. ETAPAS, ACTIVIDADES Y DURACIÓN

Id.	Actividad	Duración
1	Introducción	3 días
2	Definición marco teórico	3 días
3	Relevamiento equipos de conectividad	15 días
4	Búsqueda y Selección de herramientas de prueba y medición de la conectividad	5 días
5	Muestreo de la red con las herramientas seleccionadas	20 días
6	Recopilación de la información	20 días
7	Análisis de la información recabada	30 días
8	Formulación y Comprobación de la hipótesis	10 días
9	Establecer conclusiones	5 días
10	Presentación del informe final	5 días

14.2.2. DIAGRAMA GANTT



Id	Nombre de tarea	Duración	Comienzo	Fin
1	Introducción	3 días	lun 2/11/15	mié 4/11/15
2	Definición marco teórico	3 días	jue 5/11/15	lun 9/11/15
3	Relevamiento de equipos de conectividad	15 días	mar 10/11/15	lun 30/11/15
4	Búsqueda y selección de herramientas	5 días	mar 10/11/15	lun 16/11/15
5	Muestreo de la red con las herramientas seleccionadas	20 días	mar 1/12/15	lun 28/12/15
6	Recopilación de la información	20 días	mar 29/12/15	lun 25/1/16
7	Análisis de la información recabada	30 días	mar 26/1/16	lun 7/3/16
8	Formulación y Comprobación de la hipótesis	10 días	mar 8/3/16	lun 21/3/16
9	Establecer conclusiones	5 días	mar 22/3/16	lun 28/3/16
10	Presentación del informe final	5 días	mar 29/3/16	lun 4/4/16
11	Fin	1 día	mar 5/4/16	mar 5/4/16

14.3.ACTIVIDADES REALIZADAS:

ETAPA 1: INTRODUCCIÓN

1) Identificación de la Empresa

Ver Punto 11.1 en la página 22.

2) Objetivos y políticas generales

Ver Anexo 1 en la página 125.

3) Reseña histórica

Ver Anexo 2 en la página 126.

4) Infraestructura

Se realizó el relevamiento de la infraestructura de la casa matriz MR Seguridad S.A. y de una de las sucursales del interior (Río Cuarto), esta última será a modo de ejemplo del resto de las sucursales, ya que las mismas son de dimensiones y funciones similares.

4.1) Superficie y localización de las instalaciones de la sucursal Av. Colón:

- Superficie de planta baja: 280 m2.
- Superficie de 1er Piso: 280 m2.

Distribución Física de sus instalaciones:

- Planta Baja:
  - Oficina Gerente General.
  - Recepción.
  - Administración de Recursos Humanos.
  - Logística.
  - Taller.
  - Administración de Servidores y Redes.
  - Sala de Conectividad y Servidores.
- 1er Piso:
  - Control de Cámaras.
  - Control de Alarmas.
  - Logística de Servicios.

- Gerente de Logística
- Gerente de Servicios.
- Sala de Conectividad y Servidores.

4.2) Superficie y localización de las instalaciones de la sucursal Rio IV:

- Superficie aproximada de: 320 m2.

Distribución Física de sus instalaciones:

- Planta:
  - Oficina de gerente.
  - Área administrativa.
  - Oficina secretaria gerente.
  - Control de cámaras.
  - Control de alamas.
  - Recepción.

4.3) Lay-Out o Plano de los edificios

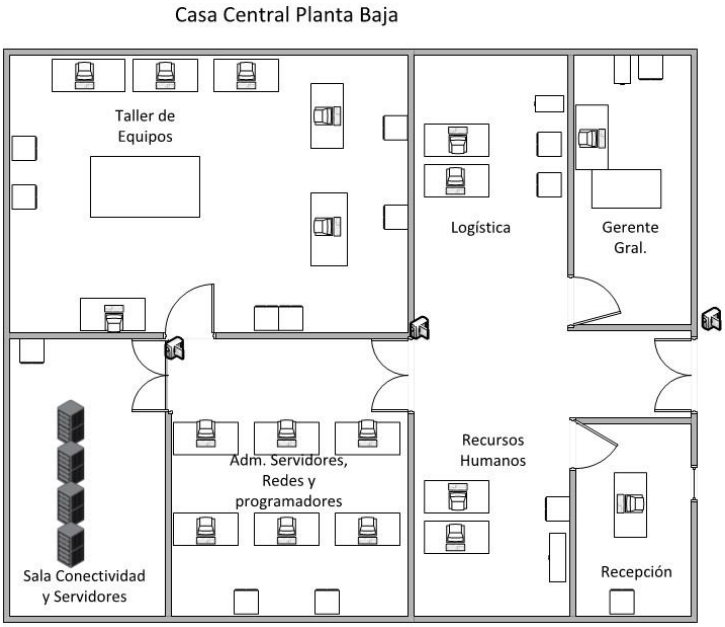


Fig. 14.3. Etapa 1: Lay-out Casa Central Planta Baja.

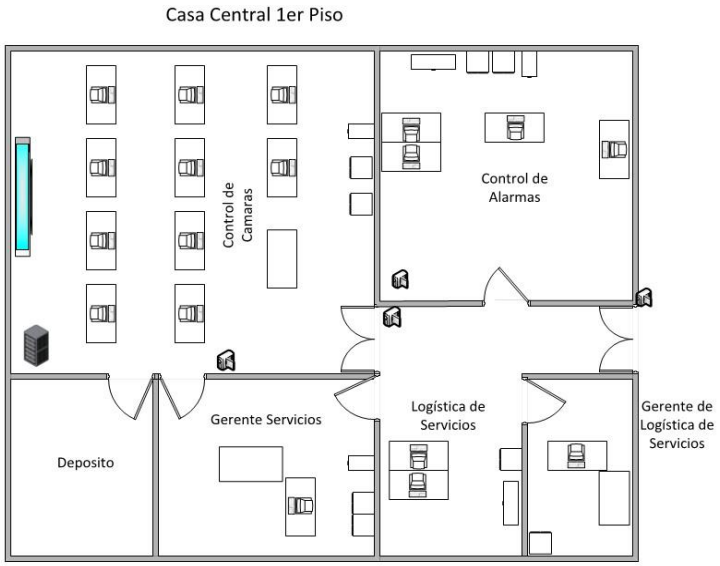


Fig. 14.3. Etapa 1: Lay-out Casa Central Primer Piso.

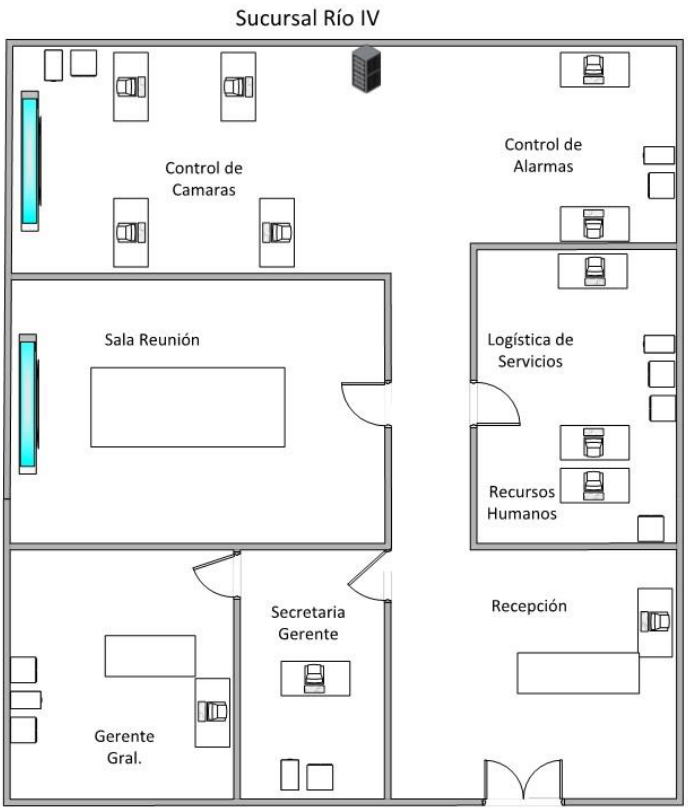


Fig. 14.3. Etapa 1: Lay-out Sucursal Río Cuarto.

5) Niveles de Actividad

Los niveles de actividad no son constantes durante el año, ya que se aprecia un leve incremento de las mismas en el periodo vacacional. Su participación en el mercado ronda los 3500 clientes en toda la provincia, siendo el monitoreo de alarmas donde se concentra la mayor cantidad de clientes y en menor medida el monitoreo de cámaras y vigilancia privada.

5.1) Niveles de Servicio

La relación que existe entre seguridad y los servicios que presta la empresa son directos, por lo cual, si en la provincia los niveles de robos aumentan, también crece la necesidad de seguridad de las personas, es por esto que actualmente, se produjo un incremento del 5% de clientes en relación al año anterior.

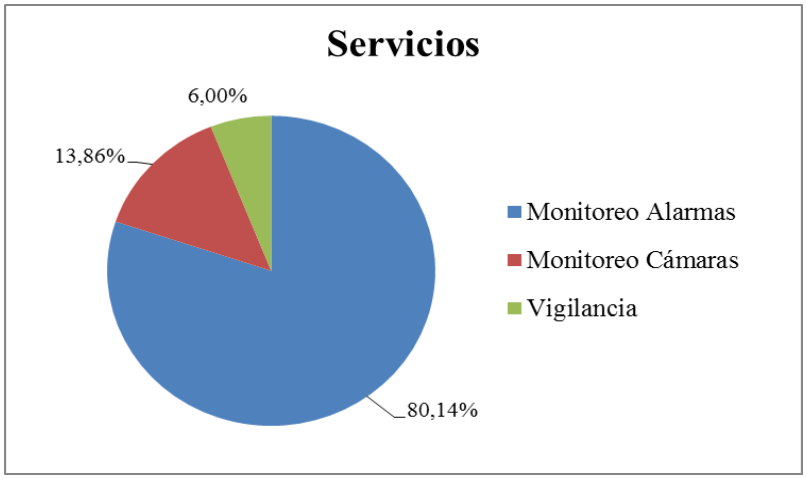


Fig. 14.3. Etapa 1: Niveles de Servicio.

Servicios	Clientes	Porcentaje
Monitoreo Alarmas	2805	80,14%
Monitoreo Cámaras	485	13,86%
Vigilancia	210	6,00%

Tabla. 14.3. Etapa 1: Niveles de Servicio.

5.2) Participación en el mercado

Actualmente hay alrededor de 100000 usuarios alarmas, 33 empresas de seguridad privada, de las cuales ADT posee el 40% de los clientes.

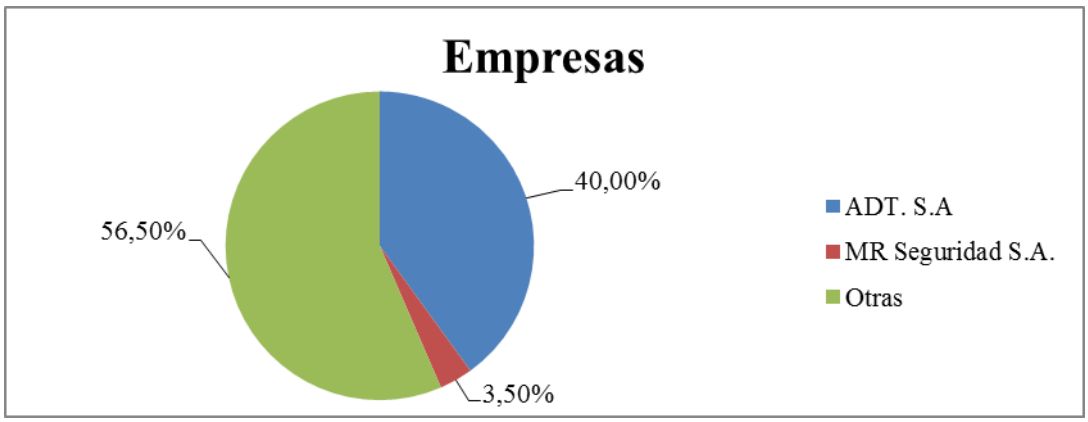


Fig. 14.3. Etapa 1: Participación del Mercado.

Empresas	Clientes	Porcentaje
ADT. S.A.	40000	40,00%
MR Seguridad S.A.	3500	3,50%
Otras	56500	56,50%

Tabla. 14.3. Etapa 1: Participación del Mercado.

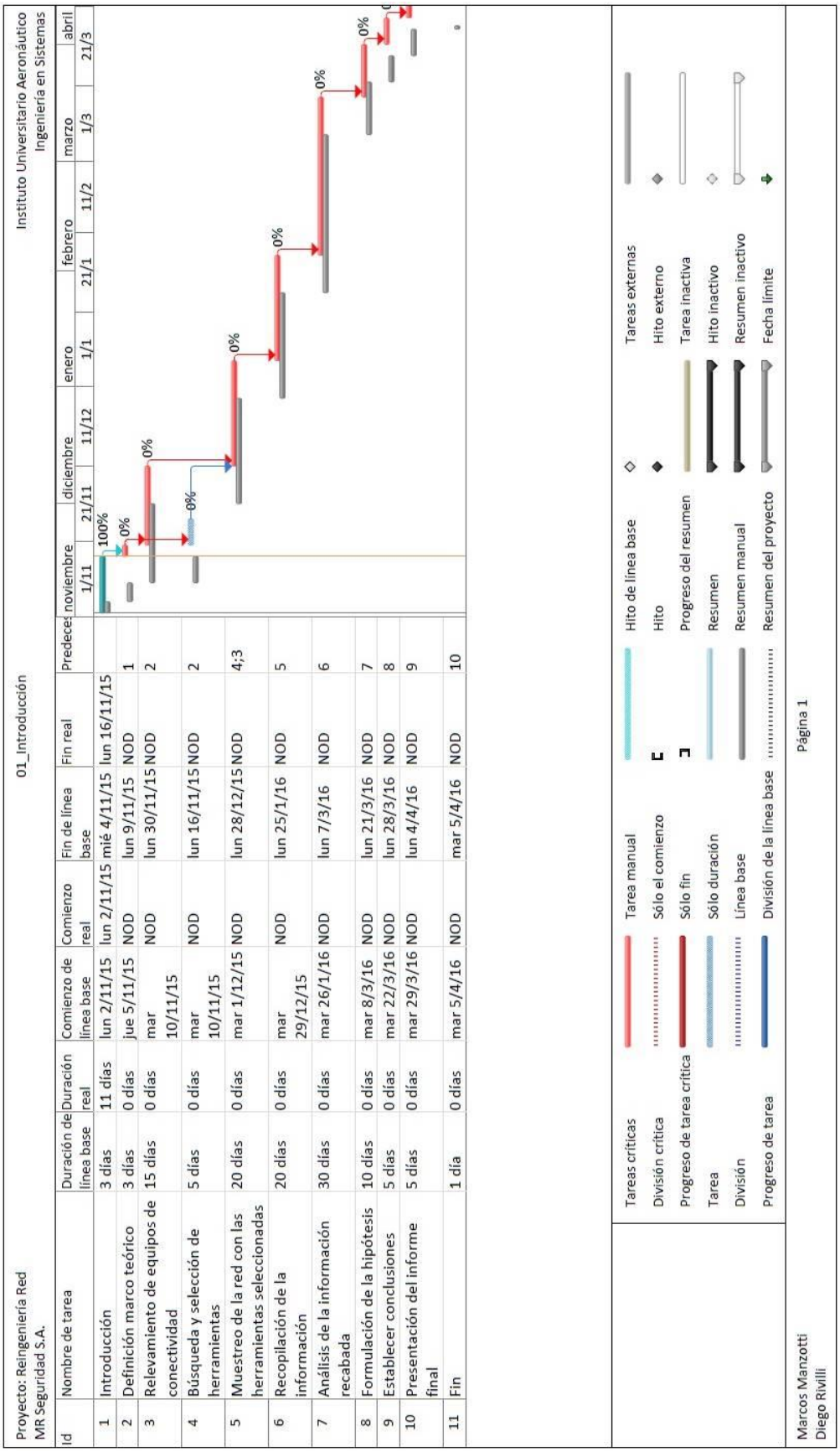
6) Datos del personal

Ver Anexo 3 en la página 127.

7) Datos del entorno específico

Ver Anexo 4 en la página 130.

8) Cronograma Real Vs. Previsto



Id	Nombre de tarea	Duración de línea base	Duración real	Comienzo de línea base	Comienzo real	Fin de línea base	Fin real	Predeces
1	Introducción	3 días	11 días	lun 2/11/15	lun 2/11/15	mié 4/11/15	lun 16/11/15	
2	Definición marco teórico	3 días	0 días	jue 5/11/15	NOD	lun 9/11/15	NOD	1
3	Relevamiento de equipos de conectividad	15 días	0 días	mar 10/11/15	NOD	lun 30/11/15	NOD	2
4	Búsqueda y selección de herramientas	5 días	0 días	mar 10/11/15	NOD	lun 16/11/15	NOD	2
5	Muestreo de la red con las herramientas seleccionadas	20 días	0 días	mar 1/12/15	NOD	lun 28/12/15	NOD	4;3
6	Recopilación de la información	20 días	0 días	mar 29/12/15	NOD	lun 25/1/16	NOD	5
7	Análisis de la información recabada	30 días	0 días	mar 26/1/16	NOD	lun 7/3/16	NOD	6
8	Formulación de la hipótesis	10 días	0 días	mar 8/3/16	NOD	lun 21/3/16	NOD	7
9	Establecer conclusiones	5 días	0 días	mar 22/3/16	NOD	lun 28/3/16	NOD	8
10	Presentación del informe final	5 días	0 días	mar 29/3/16	NOD	lun 4/4/16	NOD	9
11	Fin	1 día	0 días	mar 5/4/16	NOD	mar 5/4/16	NOD	10

ETAPA 2: MARCO TEÓRICO

Se hizo foco en los puntos 10, 11 y 13 de la Norma ISO 27002:2008 Técnicas de Seguridad, los cuales hacen referencia a la gestión de comunicaciones y operaciones, control de acceso y a la gestión de incidentes de seguridad.

Además se tomó en cuenta la Norma 27005:2008 de Gestión de los Riesgos de Seguridad de la Información, en aspectos referidos a las redes informáticas y a su hardware.

Descripción de los puntos que se tuvieron en cuenta de las Normas ISO 27002.

1) ISO 27002: Gestión de Comunicaciones y Operaciones (Punto 10)

1.1) PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS: Se recomienda que se establezcan responsabilidades y procedimientos para la gestión y funcionamiento de todas las instalaciones de procesamiento de datos.

1.1.1) Documentación de los procedimientos operativos: Es recomendable que los mismos sean documentados, y que se mantengan disponibles para todos los usuarios que los necesiten.

1.1.2) Gestión de cambios: Se recomienda que se controlen los cambios en los sistemas e instalaciones de procesamiento de datos.

1.2) PROTECCIÓN CONTRA CÓDIGO: Es necesario tomar precauciones para prevenir y detectar la introducción de virus informáticos, gusanos de red, troyanos y bombas lógicas.

1.2.1) Control contra código malicioso: Se recomienda implementar controles de detección y prevención de software malicioso y procedimientos para la concientización de los usuarios.

1.3) GESTIÓN DE LA SEGURIDAD DE LA RED: Garantizar la seguridad de la información en las redes y la protección de la infraestructura de soporte. La gestión segura de las redes requieren consideraciones cuidadosas, para el flujo de datos, implicaciones legales, seguimiento y protección.

1.3.1) Controles de redes: es recomendable que las redes estén adecuadamente gestionadas y controladas, para protegerlas de amenazas, y para mantener un ambiente seguro para los sistemas y aplicaciones que las utilizan.

1.3.2) Seguridad de los servicios de red: Los servicios de red incluyen la provisión de las conexiones, servicios de red privado, firewalls, etc, y se recomienda que se identifiquen los acuerdos de seguridad necesarios para los mismos,

tales como características de seguridad, niveles de servicios y los requerimientos de gestión.

1.3.3) Procedimientos para el manejo de la información: se recomienda establecer procedimientos para el manejo, procesamiento, almacenamiento y comunicación de la información para protegerla de uso inadecuado o divulgación no autorizada.

1.3.4) Seguimiento y control: se recomienda que los sistemas se sigan y se controlen y se lleve un registro de los eventos de seguridad de la información, tales como operadores y acciones fallidas.

1.3.5) Registro de auditoria: se recomienda que se produzcan y mantengan registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para ayudar en futuras investigaciones y en el seguimiento del control de acceso.

1.3.6) Seguimiento del uso del sistema: se recomienda que se establezcan procedimientos para supervisar el uso de las instalaciones de procesamiento de datos y que se revisen de forma regular los resultados de las actividades de seguimiento.

1.3.7) Protección de los "logs": se recomienda que los controles apunten a la protección contra cambios no autorizados y problemas operacionales con las instalaciones de registro de sesión, incluyendo:

- alteraciones de los tipos de mensajes que son grabados.
- que los archivos de sesión se editen o eliminen.
- que la capacidad de almacenamiento del medio del archivo de sesión se exceda, sin que se puedan registrar nuevos eventos o sobrescriban anteriores.

1.3.8) Registro de actividad de administrador y operador: se recomienda que los registros incluyan:

- fecha y hora de ocurrencia del evento.
- la información acerca del evento o la falla.
- qué cuenta o qué administrador u operador estuvo involucrado.
- qué procesos fueron involucrados.

2) ISO 27002: Control de Accesos (punto 11)

2.1) REQUERIMIENTOS PARA EL CONTROL DE ACCESOS: se recomienda que se controle el acceso a la información, a las instalaciones de procesamiento de la información y a los procesos de negocios, sobre la base de los requerimientos de seguridad y de los negocios.

2.1.1) Política de control de accesos: se recomienda que se determine claramente, en la política de control de accesos, las reglas y derechos del control de accesos para cada usuario o grupo de usuarios. Los controles de accesos son lógicos y físicos y se recomienda que se consideren en forma conjunta.

2.2) GESTIÓN DE ACCESOS DE USUARIOS: asegurar el acceso a usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información, estableciendo procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

2.2.1) Registro de usuarios: se recomienda que exista un procedimiento formal de registro de altas y bajas de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.

2.3) RESPONSABILIDADES DEL USUARIO: se recomienda que se concientice a los usuarios de sus responsabilidades para el mantenimiento efectivo de controles de acceso, particularmente los relacionados con el uso de contraseñas y la seguridad del equipamiento del usuario.

2.4) CONTROL DE ACCESO A LA RED: se recomienda que se controle el acceso a los servicios de la red, tanto internos como externos, para no comprometer la seguridad de los mismos.

2.4.1) Política de utilización de los servicios de red: se recomienda que se provea a los usuarios sólo el acceso a los servicios para los cuales han sido específicamente autorizados, formulando una política concerniente al uso de la red y los servicios de la misma.

2.4.2) Autenticación de usuarios para conexiones externas: se recomienda que se utilicen métodos de autenticación apropiados para el control de acceso de usuarios remotos.

2.4.3) Identificación del equipamiento de red: se recomienda que se considere la identificación automática de equipamiento como un medio para autenticar conexiones de ubicaciones y equipamiento específicos.

2.4.4) Protección de los puertos de diagnóstico y configuración remotos: se recomienda que se controle el acceso físico y lógico a los puertos de diagnóstico y configuración, mediante el uso de bloqueo con clave y procedimientos de soporte para controlar el acceso físico al puerto.

2.4.5) Separación de redes: Para controlar la seguridad de redes amplias, se recomienda que los grupos de servicios de la información, usuarios y sistemas de información se subdividan en redes, como por ejemplo, dominios de red internos y dominios de red externos a una organización, cada uno protegido por un perímetro de seguridad definido. Tal perímetro de red puede ser implementado mediante la instalación de un Gateway seguro entre dos redes que serán interconectadas para controlar el acceso y flujo de la información entre los dominios.

Las redes también pueden ser divididas usando funcionalidades de los dispositivos de red, por ejemplo IP Switching.

2.4.6) Control de conexión a la red: Para redes compartidas, especialmente aquellas que se extienden a través de los límites de la organización, se recomienda que se restrinja la capacidad de los usuarios para conectarse a la red, de acuerdo a la política de control y acceso y con los requerimientos de las aplicaciones de la actividad.

2.4.7) Control de enrutamiento de red: estos controles se deben aplicar para garantizar que las conexiones informáticas y los flujos de información no violen la política de control de acceso de las aplicaciones de negocio. Se recomienda que los controles de enrutamiento se basen en mecanismos de verificación de dirección de origen y destino.

2.4.8) Identificación y autenticación de usuarios: Se recomienda que todos los usuarios tengan un único identificador (identificador de usuario) para su uso personal, y que se elija una técnica adecuada de autenticación para sustentar la identidad segura del usuario.

2.5) COMPUTACIÓN MÓVIL Y TELETRABAJO: Se recomienda que la protección requerida sea proporcional a los riesgos que originan estas formas específicas de trabajo.

2.5.1) Computación y comunicaciones móviles: Cuando se utilizan computación e instalaciones móviles, por ejemplo: notebooks, teléfonos móviles, etc., se recomienda que se tenga especial cuidado en garantizar que no se

comprometa la información de la empresa. La política de computación móvil debería incluir los requerimientos para la protección física, controles de acceso, técnicas criptográficas, copias de respaldo, y protección de virus. Se recomienda que la política también incluya las reglas y avisos de conectar los recursos móviles a redes y guías en lugares públicos.

2.5.2) Teletrabajo: es conveniente que las organizaciones sólo autoricen actividades de teletrabajo si han comprobado satisfactoriamente que se han implementado disposiciones y controles adecuados en materia de seguridad y que estos cumplen con la política de seguridad de la organización.

3) ISO 27002: Gestión de los Incidentes de la Seguridad de la Información (punto 13)

3.1) INFORME DE LOS EVENTOS Y DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN: el objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información se comuniquen de forma tal que se apliquen las acciones correctivas en el tiempo correcto.

3.1.1) Reporte de los eventos de la seguridad de la información: Es conveniente que se establezca un procedimiento de reporte formal de eventos de seguridad de la información, junto con un procedimiento de respuesta a incidentes y escalonamiento, especificando la acción a realizar cuando se reciba un reporte de evento de seguridad de la información.

3.1.2) Reporte de las debilidades de la seguridad: Es conveniente que se requiera que todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información tomen nota y reporten cualquier acción sospechosa que observen o consideren que esté relacionada con las debilidades de seguridad de los sistemas o servicios.

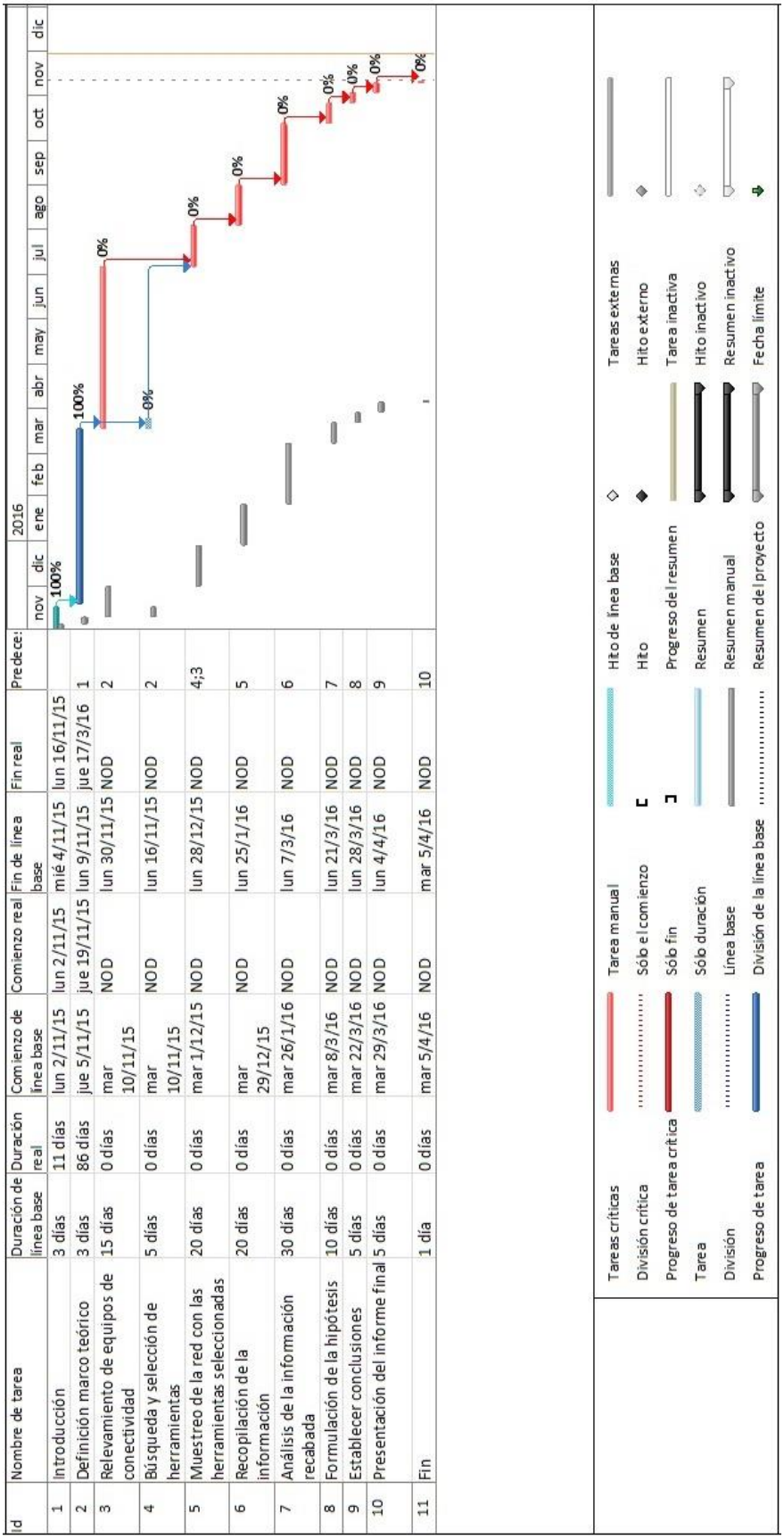
3.2) GESTIÓN DE LOS INCIDENTES Y MEJORAS DE LA SEGURIDAD DE LA INFORMACIÓN: Se recomienda que se establezcan las responsabilidades y procedimientos para manejar efectivamente los eventos y las debilidades de seguridad de la información una vez que hayan sido reportados.

3.2.1) Responsabilidades y procedimientos: se recomienda que se establezca una gestión de las responsabilidades y procedimientos para garantizar una respuesta rápida, efectiva y ordenada de los incidentes de la información.

3.2.2) Aprendizaje a partir de los incidentes de la seguridad de la información: se recomienda que existan mecanismos para permitir que se cuantifiquen y supervisen los tipos, volúmenes y costos de los incidentes de la seguridad de la información.

3.2.3) Recolección de la evidencia: se recomienda que se recolecte, retenga y presente evidencia para cumplir con los requerimientos legales en la jurisdicción que corresponda.

4) Cronograma Real Vs. Previsto



Id	Nombre de tarea	Duración de línea base	Duración real	Comienzo de línea base	Comienzo real	Fin de línea base	Fin real	Predece:
1	Introducción	3 días	11 días	lun 2/11/15	lun 2/11/15	mié 4/11/15	lun 16/11/15	
2	Definición marco teórico	3 días	86 días	jue 5/11/15	jue 19/11/15	lun 9/11/15	jue 17/3/16	1
3	Relevamiento de equipos de conectividad	15 días	0 días	mar 10/11/15	NOD	lun 30/11/15	NOD	2
4	Búsqueda y selección de herramientas	5 días	0 días	mar 10/11/15	NOD	lun 16/11/15	NOD	2
5	Muestreo de la red con las herramientas seleccionadas	20 días	0 días	mar 1/12/15	NOD	lun 28/12/15	NOD	4;3
6	Recopilación de la información	20 días	0 días	mar 29/12/15	NOD	lun 25/1/16	NOD	5
7	Análisis de la información recabada	30 días	0 días	mar 26/1/16	NOD	lun 7/3/16	NOD	6
8	Formulación de la hipótesis	10 días	0 días	mar 8/3/16	NOD	lun 21/3/16	NOD	7
9	Establecer conclusiones	5 días	0 días	mar 22/3/16	NOD	lun 28/3/16	NOD	8
10	Presentación del informe final	5 días	0 días	mar 29/3/16	NOD	lun 4/4/16	NOD	9
11	Fin	1 día	0 días	mar 5/4/16	NOD	mar 5/4/16	NOD	10

ETAPA 3: RELEVAMIENTO

1) Recopilación de documentos y manuales

En uno de los encuentros fueron obtenidos documentos que se utilizan a diario en sus actividades, y son los siguientes:

- Planilla de distribución de bocas de red.
- DOC TEC Servidores.
- DOC TEC Detalle Equipos Conectividad (Rack 3).
- Manuales de los Dispositivos de Red.
- Inst. Adición Teléfonos IP MR Seguridad S.A.
- Procedimiento soporte Sistemas Críticos MR Seguridad S.A.

Nombre del Documento: Planilla de distribución de bocas de red			
Uso: Documento Técnico con descripción de los puertos de los Switchs y de las bocas de red de las distintas oficinas de la casa matriz.			
Emisor: Administrador Redes y Servidores.			
Receptor: Técnicos redes y servidores.			
Versión: No contempla. **Fecha de Emisión:** 03/08/2013			
PREGUNTAS			
Necesidad:	**SI**	**NO**	**NA**
¿Se ha determinado el objetivo del documento?	X		
¿Existe algún documento similar?		X	
¿Economiza material y esfuerzo?	X		
¿Es posible simplificar su diseño?		X	
¿Se puede prescindir de algún dato?		X	
Claridad:	**SI**	**NO**	**NA**
¿Está claro el objetivo del documento?		X	
¿El ordenamiento de datos es de fácil seguimiento?	X		
¿Se han agrupado los datos relacionados?	X		
¿Hay contraste entre líneas y tipos de escrituras?	X		
¿La alineación o disposición vertical es clara?	X		
Utilización:	**SI**	**NO**	**NA**
¿Sus copias se distribuyen por color de papel?		X	
¿Se han tenido en cuenta los archivos existentes?			X

¿Se consideró su relación con otros documentos?			X
¿El tamaño impreso responde a las normas IRAM?		X	
¿El tamaño es adecuado?			X
Control y seguimiento:	**SI**	**NO**	**NA**
¿Posee referencias de seguridad?		X	
¿Se encuentra Versionado?		X	
¿Se tienen en cuenta las modificaciones?		X	
¿Es de fácil acceso para las personas autorizadas?	X		
¿Tiene contemplado la autoría de la última modificación?		X	
Disposición:	**SI**	**NO**	**NA**
¿La distribución general es satisfactoria?	X		
¿Los márgenes son adecuados para su almacenamiento?		X	
¿Es necesaria la descripción en dos idiomas más?		X	
¿Se usa el sistema de trascripción adecuado?			X
¿Se ha consignado la distribución o destino de cada copia?		X	
Observaciones: Este documento discierne en algunos puntos con las conexiones y las bocas de red dispuestas en la actualidad.			
Conclusión: Este documento, según lo manifestado por los empleados, cumple en parte con la funcionalidad para la cual fue creado.			

Nombre del Documento: DOC TEC Servidores			
Uso: Documento Técnico con descripción de los equipos Servidores.			
Emisor: Administrador Redes y Servidores.			
Receptor: Técnicos redes y servidores.			
Versión: No contempla. **Fecha de Emisión:** 03/08/2014			
PREGUNTAS			
Necesidad:	**SI**	**NO**	**NA**
¿Se ha determinado el objetivo del documento?	X		
¿Existe algún documento similar?		X	
¿Economiza material y esfuerzo?	X		
¿Es posible simplificar su diseño?		X	
¿Se puede prescindir de algún dato?		X	
Claridad:	**SI**	**NO**	**NA**

¿Está claro el objetivo del documento?	X		
¿El ordenamiento de datos es de fácil seguimiento?		X	
¿Se han agrupado los datos relacionados?		X	
¿Hay contraste entre líneas y tipos de escrituras?	X		
¿La alineación o disposición vertical es clara?	X		
Utilización:	**SI**	**NO**	**NA**
¿Sus copias se distribuyen por color de papel?		X	
¿Se han tenido en cuenta los archivos existentes?			X
¿Se consideró su relación con otros documentos?		X	
¿El tamaño impreso responde a las normas IRAM?	X		
¿El tamaño es adecuado?	X		
Control y seguimiento:	**SI**	**NO**	**NA**
¿Posee referencias de seguridad?		X	
¿Se encuentra Versionado?		X	
¿Se tienen en cuenta las modificaciones?		X	
¿Es de fácil acceso para las personas autorizadas?	X		
¿Tiene contemplado la autoría de la última modificación?		X	
Disposición:	**SI**	**NO**	**NA**
¿La distribución general es satisfactoria?	X		
¿Los márgenes son adecuados para su almacenamiento?	X		
¿Es necesaria la descripción en dos idiomas más?		X	
¿Se usa el sistema de trascripción adecuado?			X
¿Se ha consignado la distribución o destino de cada copia?		X	
Observaciones: Este documento discierne en algunos puntos con los equipos relevados en la actualidad.			
Conclusión: Este documento, según lo manifestado por los empleados, alcanza a cumplir con su funcionabilidad gracias a que se realizaron pocas actualizaciones de los equipos que contempla			

Nombre del Documento: DOC TEC Detalle Equipos Conectividad (Rack 3)	
Uso: Documento Técnico con descripción de los equipos dispuestos en los racks.	
Emisor: Administrador Redes y Servidores.	
Receptor: Técnicos redes.	
Versión: No contempla.	**Fecha de Emisión:** 05/09/2013

PREGUNTAS			
Necesidad:	**SI**	**NO**	**NA**
¿Se ha determinado el objetivo del documento?	X		
¿Existe algún documento similar?		X	
¿Economiza material y esfuerzo?	X		
¿Es posible simplificar su diseño?		X	
¿Se puede prescindir de algún dato?		X	
Claridad:	**SI**	**NO**	**NA**
¿Está claro el objetivo del documento?	X		
¿El ordenamiento de datos es de fácil seguimiento?	X		
¿Se han agrupado los datos relacionados?			X
¿Hay contraste entre líneas y tipos de escrituras?	X		
¿La alineación o disposición vertical es clara?	X		
Utilización:	**SI**	**NO**	**NA**
¿Sus copias se distribuyen por color de papel?		X	
¿Se han tenido en cuenta los archivos existentes?			X
¿Se consideró su relación con otros documentos?		X	
¿El tamaño impreso responde a las normas IRAM?	X		
¿El tamaño es adecuado?	X		
Control y seguimiento:	**SI**	**NO**	**NA**
¿Posee referencias de seguridad?		X	
¿Se encuentra Versionado?		X	
¿Se tienen en cuenta las modificaciones?		X	
¿Es de fácil acceso para las personas autorizadas?	X		
¿Tiene contemplado la autoría de la última modificación?		X	
Disposición:	**SI**	**NO**	**NA**
¿La distribución general es satisfactoria?	X		
¿Los márgenes son adecuados para su almacenamiento?	X		
¿Es necesaria la descripción en dos idiomas más?		X	
¿Se usa el sistema de trascripción adecuado?			X
¿Se ha consignado la distribución o destino de cada copia?		X	
Observaciones: Este documento discierne en algunos puntos con los equipos relevados en la actualidad.			
Conclusión: Este documento, según lo manifestado por los empleados, alcanza a cumplir con su funcionabilidad.			

Nombre del Documento: Inst. Adición Teléfonos IP MR Seguridad S.A.			
Uso: Instruir sobre las tareas a realizar para instalar satisfactoriamente un teléfono IP			
Emisor: Sistemas.			
Receptor: Instaladores redes y equipos.			
Versión: No contempla. **Fecha de Emisión:** 28/05/2013			
PREGUNTAS			
Necesidad:	**SI**	**NO**	**NA**
¿Se ha determinado el objetivo del documento?	X		
¿Existe algún documento similar?		X	
¿Economiza material y esfuerzo?	X		
¿Es posible simplificar su diseño?		X	
¿Se puede prescindir de algún dato?		X	
Claridad:	**SI**	**NO**	**NA**
¿Está claro el objetivo del documento?	X		
¿El ordenamiento de datos es de fácil seguimiento?	X		
¿Se han agrupado los datos relacionados?	X		
¿Hay contraste entre líneas y tipos de escrituras?	X		
¿La alineación o disposición vertical es clara?	X		
Utilización:	**SI**	**NO**	**NA**
¿Sus copias se distribuyen por color de papel?		X	
¿Se han tenido en cuenta los archivos existentes?			X
¿Se consideró su relación con otros documentos?		X	
¿El tamaño impreso responde a las normas IRAM?	X		
¿El tamaño es adecuado?	X		
Control y seguimiento:	**SI**	**NO**	**NA**
¿Posee referencias de seguridad?		X	
¿Se encuentra Versionado?		X	
¿Se tienen en cuenta las modificaciones?		X	
¿Es de fácil acceso para las personas autorizadas?	X		
¿Tiene contemplado la autoría de la última modificación?	X		
Disposición:	**SI**	**NO**	**NA**
¿La distribución general es satisfactoria?	X		
¿Los márgenes son adecuados para su almacenamiento?	X		

¿Es necesaria la descripción en dos idiomas más?		X	
¿Se usa el sistema de trascripción adecuado?			X
¿Se ha consignado la distribución o destino de cada copia?		X	
Observaciones: Este documento discierne en gran medida en la descripción con los equipos instalados en la actualidad.			
Conclusión: Este documento, según lo manifestado por los empleados, no cumple con la funcionalidad ya que se encuentra desactualizado con respecto a los teléfonos IP actuales.			

Nombre del Documento: Procedimiento soporte Sistemas Críticos MR Seguridad S.A.			
Uso: Contiene los procedimientos para brindar soporte técnico a los sistemas más críticos de la empresa.			
Emisor: Administrador Red y servidores.			
Receptor: Área informática.			
Versión: No contempla. **Fecha de Emisión:** 26/04/2012			
PREGUNTAS			
Necesidad:	**SI**	**NO**	**NA**
¿Se ha determinado el objetivo del documento?	X		
¿Existe algún documento similar?		X	
¿Economiza material y esfuerzo?	X		
¿Es posible simplificar su diseño?		X	
¿Se puede prescindir de algún dato?		X	
Claridad:	**SI**	**NO**	**NA**
¿Está claro el objetivo del documento?	X		
¿El ordenamiento de datos es de fácil seguimiento?	X		
¿Se han agrupado los datos relacionados?	X		
¿Hay contraste entre líneas y tipos de escrituras?	X		
¿La alineación o disposición vertical es clara?	X		
Utilización:	**SI**	**NO**	**NA**
¿Sus copias se distribuyen por color de papel?		X	
¿Se han tenido en cuenta los archivos existentes?			X
¿Se consideró su relación con otros documentos?		X	
¿El tamaño impreso responde a las normas IRAM?	X		
¿El tamaño es adecuado?	X		
Control y seguimiento:	**SI**	**NO**	**NA**

¿Posee referencias de seguridad?		X	
¿Se encuentra Versionado?		X	
¿Se tienen en cuenta las modificaciones?		X	
¿Es de fácil acceso para las personas autorizadas?	X		
¿Tiene contemplado la autoría de la última modificación?		X	
Disposición:	**SI**	**NO**	**NA**
¿La distribución general es satisfactoria?	X		
¿Los márgenes son adecuados para su almacenamiento?	X		
¿Es necesaria la descripción en dos idiomas más?		X	
¿Se usa el sistema de trascripción adecuado?			X
¿Se ha consignado la distribución o destino de cada copia?		X	
Observaciones: Este documento discierne en algunos puntos con los equipos relevados en esta etapa.			
Conclusión: Este documento, según lo manifestado por los empleados, cumple en parte con la funcionalidad para la cual fue creado, ya que aún se mantienen algunos sistemas detallados.			

2) Observación Directa: Resultados generales y por Área.

Para este punto se llevó a cabo un relevamiento visual de las instalaciones, las observaciones más importantes de la misma se detallan a continuación.

2.1) Casa Central: Sitio Informática

En el sitio los equipos informáticos están dispuestos en racks, los cuales no se encuentran cerrados con llave, instalados sobre un piso flotante, y los cableados de red y de energía ingresan por el mismo piso y por debajo de los racks.

El equipo informático se encuentra protegido energéticamente mediante tres UPS las cuales ante un corte de energía y hasta que inicie el grupo electrógeno les proveen energía estable.

Los cableados eléctricos y de red, en su mayoría se encuentran instalados sobre bandejas metálicas, respetando las distancias que debe existir entre los mismos.

También se observaron cableados más recientes que no van por las bandejas y no respetan las normas de cableado, los mismos se cruzan y juntan con cableados eléctricos. Además los mismos no se encuentran instalados en los patch panel, y se conectan directamente a los equipos informáticos. Tampoco se encuentran identificados.

Equipos Informáticos:

- Cuenta con 12 servidores, distribuidos en distintos racks.
- Cuenta con distintos dispositivos (Switch, Router, MPLS, Firewalls, etc) que realizan la conectividad con los equipos de la casa central y de los distintos locales, con los servidores e internet.

2.2) Casa Central: Oficinas

En las oficinas los equipos informáticos están dispuestos sobre o debajo de los escritorios, estos no presentan ningún dispositivo de seguridad para el encendido, los cableados de red y de energía ingresan por cable canal o piso canal según la disposición o la ubicación del equipo en la oficina.

El equipo informático no se encuentra protegido físicamente contra problemas eléctricos (cortes o variaciones de tensión), ya que no cuentan con un equipo UPS.

Se observó que los cableados eléctricos y de red, en su mayoría se encuentran instalados sobre bandejas metálicas sobre el cielo raso, respetando las distancias que debe existir entre los mismos.

También se observaron cableados más recientes que no van por las bandejas y que tampoco respetan las normas de cableado.

Equipos Informáticos por Área:

- Gerente Gral.: 1 PC, un teléfono IP y una Notebook.
- Logística: 2 PCs.
- Recepción: 1 PC.
- Recursos Humanos: 2 PCs.
- Adm. de Servidores: 6 PCs y 1 Notebook.
- Taller: 6 PCs
- Gerente de Logística Servicios: 1PC y 1 Notebook.
- Control de Cámaras: 10 PCs.
- Control Alarmas: 4 PCs y 3 Teléfonos IP.
- Logística de Servicios: 2 PCs.
- Gerente de Servicios: 1 PC y 1 Notebook.

2.3) Sucursal Rio IV

En las oficinas los equipos informáticos están dispuestos sobre o debajo de los escritorios, estos no presentan ningún dispositivo de seguridad para el encendido, los

cableados de red y de energía ingresan por cable canal o piso canal según la disposición o la ubicación del equipo en la oficina. Los equipos de conexión, aunque se encuentren en las mismas oficinas, se hallan instalados dentro de racks para una mayor protección, además, están alimentados por una UPS.

El equipo informático no se encuentra protegido físicamente contra problemas eléctricos (cortes o variaciones de tensión), ya que no cuentan con un equipo UPS. Tampoco cuentan con un sistema de refrigeración.

Se observó que los cableados eléctricos y de red, en su mayoría se encuentran instalados dentro de cable canal plástico de 100x50mm, respetando las distancias que debe existir entre los mismos. También se observaron cableados más recientes que no van por el cable canal, no respetando las normas de cableado.

Equipos Informáticos por Área:

- Gerente Gral. Región: 1 PC y una Notebook.
- Secretaria Gerente: 1 PC.
- Recepción: 1 PC.
- Logística de servicios: 1 PC.
- Recursos Humanos: 2 PCs.
- Control de Alarmas: 2 PCs.
- Control de Cámaras: 4 PCs.

3) Resumen de equipos de networking dispuestos en casa Central.

NOMBRE (según ubicación)	DESCRIPCIÓN	ACTIVO
Switch 1er Piso	Conectividad puestos 2do piso	SI
Switch de Core	Conectividad racks y servidores	SI
Switch Planta Piso	Conectividad servidores y puestos	SI
ASA 5520 Activo	Administración	SI
ASA 5520 Failover	Backup	SI en Stand by
Fortigate 1	Firewall	SI
Fortigate 2	Firewall	SI
RPS 675	Soporte Energético	SI
Switch RAS y DMZ	Conectividad DMZ	SI
Cisco 1841 Concent.MPLS	Conectividad de MPLS	SI

Tabla. 14.3. Etapa 3: Resumen Equipos de Networking.

4) Relevamiento. (Detalle)

4.1) Switch 1er Piso (SW1piso – WS-C2950Sx-24).

Función:

Cumple con la función de dar conectividad a los equipos que se encuentran en las oficinas del 1er. Piso. Esto es a través de 24 puertos Fast Ethernet (10mbps/100mbps) y dos (2) puertos de Fibra Óptica (1000mbps).

Este modelo de switch posee 16 MB de memoria DRAM y 8 MB de memoria Flash, dando 8.8 Gbps de máximo de banda ancha de reenvió. Permite trabajar hasta con 8000 MACs y soporta la configuración de Vlans.

4.2) Switch de Core (SWCore – WS-c3750G-24TS).

Función:

Este equipo cumple con la función de CORE de LAN (distribución) e interconexión con cada switches de piso y con los servidores de la empresa. Esto es a través de 24 puertos Giga Ethernet (10mbps/100bmps/1000mbps) y 4 puertos Duales Giga Ethernet (1000mbps UTP o Fibra Óptica)

Este modelo de switch posee 128 MB de memoria DRAM y 32 MB de memoria Flash, posee un ancho de banda de reenvió de 38.7 mbps. Permite trabajar hasta con 12000 MACs y además soporta la configuración de Vlans.

4.3) Switch de Planta Baja (SW0piso – WS-c2950SX-24).

Función:

Cumple con la función de distribución LAN a los equipos informáticos que se encuentran en la planta baja. Esto es a través de 48 puertos Fast Ethernet (100mb/s) y 2 puertos de Fibra Óptica (1000mb/s).

Este equipo posee 16 MB de memoria DRAM y 8 MB de memoria Flash, dando 8.8 Gbps de máximo de banda ancha de reenvió, también soporta la configuración de VLANs

4.4) ASA 5520.

Función:

Cumple con la función de administrar la red de la empresa, y de implementar las políticas de permisos en la red, también se definen las políticas para el

establecimiento de la VPN con todas las dependencias y la DMZ. Posee 4 puertos Giga Ethernet (100 mbps/1000 mbps).

Este equipo posee 2 GB de memoria RAM y 250 MB de memoria Flash, dando 450 Mbps de máximo de banda ancha de reenvió, soportando hasta 750 conexiones VPN de punta a punta, 280,000 conexiones concurrentes, 150 Vlans y permite la configuración de un máximo 20 contextos de seguridad.

4.5) ASA 5520 Failover.

Función:

Cumple con la función ser el backup del ASA 5520 principal ante cualquier falla. Posee 4 puertos Giga Ethernet (1000mb/s).

4.6) Fortigate 1 (fortigate 200A).

Función:

Cumple con la función de filtrar y controlar el tráfico de datos entre la red interna y Internet. El mismo cuenta con 4 puertos de red Fast Ethernet (100mb/s) para la red interna, 2 puertos de red Fast Ethernet (100mb/s) para la DMZ y 2 puertos de red Fast Ethernet (100mb/s) para Internet.

Este equipo cuenta con 150 Mbps de máximo de banda ancha de firewall, soportando hasta 200 conexiones VPN de punta a punta, 400,000 conexiones concurrentes, permite la configuración de un máximo 2000 políticas de seguridad y 8 Mbps de rendimiento del antivirus.

4.7) Fortigate 2 (Fortigate 200A).

Función:

Cumple con la función de Backup del Fortigate 1. El mismo cuenta con 4 puertos de red Fast Ethernet (100mb/s) para la red interna, 2 puertos de red Fast Ethernet (100mb/s) para la DMZ y 2 puertos de red Fast Ethernet (100mb/s) para Internet.

4.8) RPS 675 (PWR-675-AC-RPS-N1) 3750.

Función:

Cumple con la función de dar soporte energético a los equipos Cisco 3750, es en sí un soporte redundante de energía.

4.9) Switch RAS y AVL (WS-C2950-12).

Función:

Cumple con la función de conectar los diferentes equipos de la DMZ. Posee 16 puertos de red Fast Ethernet (100mb/s).

4.10) Cisco 1841 Concent.MPLS.

Función:

Concentra la conectividad de todos los equipos MPLS de la empresa. Todos los equipos MPLS que se encuentran en las dependencias forman una red LAN sobre la red de telefonía de Telecom.

5) Detalle de las conexiones del patch panel y de conexiones de los switch.

Estas planillas se realizaron en base a la planilla de conexiones existen, a la cual la actualizamos con los datos obtenidos de la observación directa.

5.1) Pach panel y switch planta baja.

PATCHERA	SWITCH	SECTOR	EQUIPO
A-01	SWCore P01		
A-02	SWCore P02	SITIO	ASA 5520
A-03	SWCore P03	SITIO	ASA 5520 (Failover)
A-04	SWCore P04	SITIO	
A-05	SWCore P05	SITIO	
A-06	SWCore P06	SITIO	Excent03
A-07	SWCore P07	SITIO	Dccent02
A-10	SWCore P08	SITIO	Dbcent01
A-13	SWCore P09	SITIO	Storage01
A-09	SWCore P10	SITIO	Ipcent01
A-08	SWCore P11	SITIO	Ipgrab01
A-12	SWCore P12	SITIO	Ipstorage01
A-11	SWCore P13	SITIO	Fortigate01
A-14	SWCore P14	SITIO	Fortigate02
A-15	SWCore P15	SITIO	Dbcent10
A-16	SWCore P16	SITIO	Dbcent13
A-17	SWCore P17		Vmware01
A-18	SWCore P18		Nvr01
A-19	SWCore P19		
A-20	SWCore P20		Rdcent01
A-21	SWCore P21		Dbcent08
A-22	SWCore P22		
A-23	SWCore P23		Rdcent02
A-24	SWCore P24		
	SWCore F01		SW0piso
	SWCore F02		SW1piso

	SWCore F03		
	SWCore F04		
A-25	**SW0Piso P01**		**SWCore**
A-26	**SW0Piso P02**		**PC Gerente Gral.**
A-27	**SW0Piso P03**		**PC Recepción**
A-28	**SW0Piso P04**		**CamSeg01_0Piso**
A-29	**SW0Piso P05**		**PC Logística 1**
A-30	**SW0Piso P06**		**PC Logística 2**
A-31	**SW0Piso P07**		**CamSeg02_0Piso**
A-32	**SW0Piso P08**		**PC Rec. Humanos 1**
A-33	**SW0Piso P09**		**PC Rec. Humanos 2**
A-34	**SW0Piso P10**		
A-35	**SW0Piso P11**		**PC Prog 01**
A-36	**SW0Piso P12**		**PC Prog 02**
A-37	**SW0Piso P13**		**PC Redes 01**
A-38	**SW0Piso P14**		**PC Redes 02**
A-39	**SW0Piso P15**		**PC Redes 03**
A-40	**SW0Piso P16**		**PC Serv 01**
A-41	**SW0Piso P17**		**CamSeg03_0Piso**
A-42	**SW0Piso P18**		**PC Taller 01**
A-43	**SW0Piso P19**		**PC Taller 02**
A-44	**SW0Piso P20**		**PC Taller 03**
A-45	**SW0Piso P21**		**PC Taller 04**
A-46	**SW0Piso P22**		**PC Taller 05**
A-47	**SW0Piso P23**		**PC Taller 06**
A-48	**SW0Piso P24**		**WIFI0Piso**
	SW0Piso F01		**SWCore F01**
	SW0Piso F02		

Tabla. 14.3. Etapa 3: Detalle Conexiones Patch-Panel Planta Baja.

5.2) Pach panel primer piso.

PATCHERA	SWITCH	SECTOR	EQUIPO
A-01	SW1PISO p01		SWCORE
A-02	SW1PISO p02		PC GerLog01
A-03	SW1PISO p03		PC LogServ01
A-04	SW1PISO p04		PC LogServ02
A-05	SW1PISO p05		PC GerServ01
A-06	SW1PISO p06		PC ContCam01
A-07	SW1PISO p07		PC ContCam02
A-10	SW1PISO p08		PC ContCam03
A-13	SW1PISO p09		PC ContCam04
A-09	SW1PISO p10		PC ContCam05
A-08	SW1PISO p11		PC ContCam06
A-12	SW1PISO p12		PC ContCam07
A-11	SW1PISO p13		PC ContCam08
A-14	SW1PISO p14		PC ContCam09
A-15	SW1PISO p15		PC ContCam10
A-16	SW1PISO p16		PC alarm 01 + Tel IP01
A-17	SW1PISO p17		PC alarm 02 + Tel IP02
A-18	SW1PISO p18		PC alarm 03 + Tel IP03
A-19	SW1PISO p19		PC alarm 04 + Tel IP04
A-20	SW1PISO p20		CamSeg01_1Piso
A-21	SW1PISO p21		CamSeg02_1Piso
A-22	SW1PISO p22		CamSeg03_1Piso
A-23	SW1PISO p23		CamSeg04_1Piso
A-24	SW1PISO p24		WIFI1Piso
	SW1PISO F01		SWCore F02
	SW1PISO F02		

Tabla. 14.3. Etapa 3: Detalle Conexiones Patch-Panel Primer Piso.

6) Diagrama de disposición de los equipos de networking en el Rack.

Este diagrama fue actualizado en base a los datos obtenidos de la observación directa del rack.

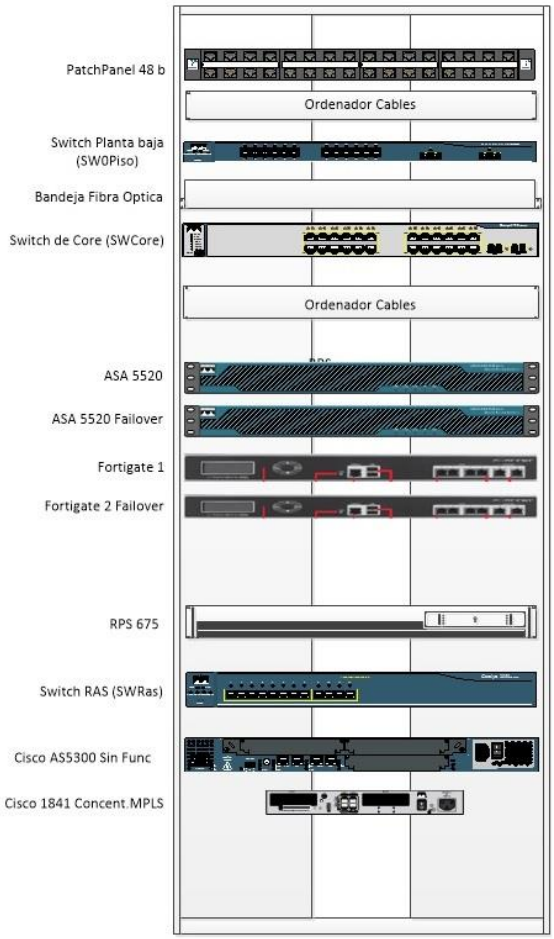


Fig. 14.3. Etapa 3: Diagrama de Disposición de equipos de Networking en Rack 3.

7) Diagrama de conexionado del core de red.

El diagrama fue actualizado en base a los datos obtenidos de la observación directa del cableado de la red y de la disposición de los equipos.

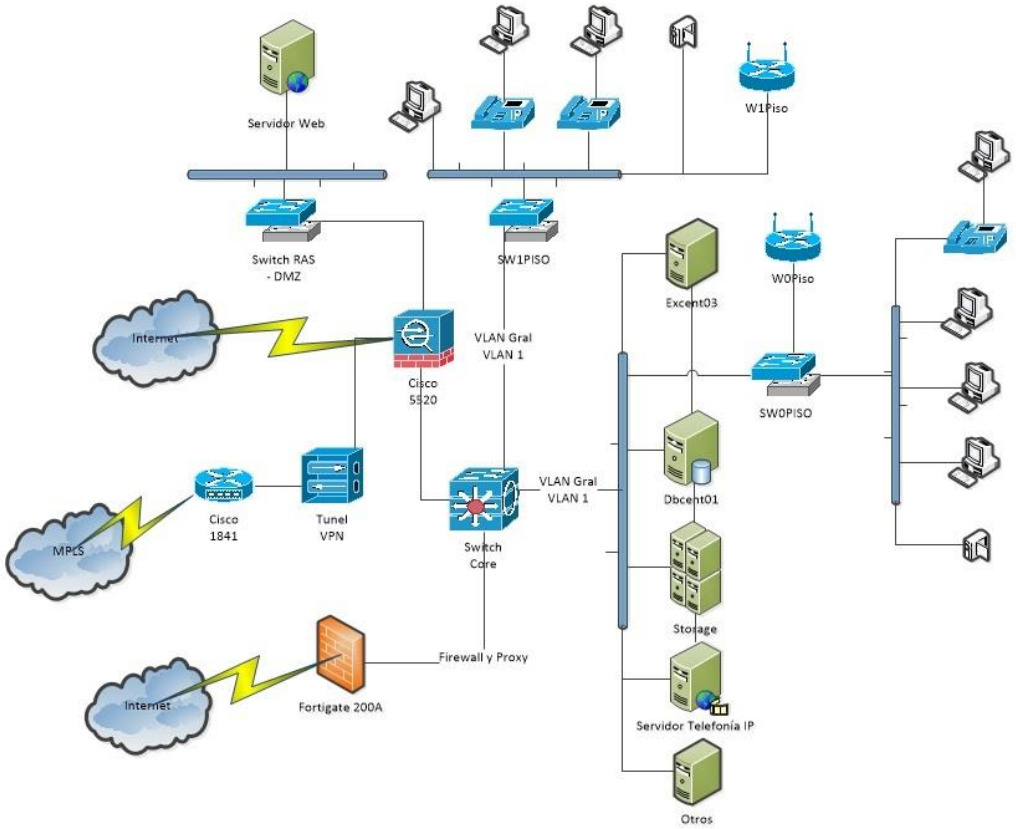


Fig. 14.3. Etapa 3: Diagrama de Conexionado del Core de Red.

8) Diagrama de conexión de los locales

Este diagrama fue realizado en base a los datos obtenidos de la observación directa del cableado de la red en los locales visitados.

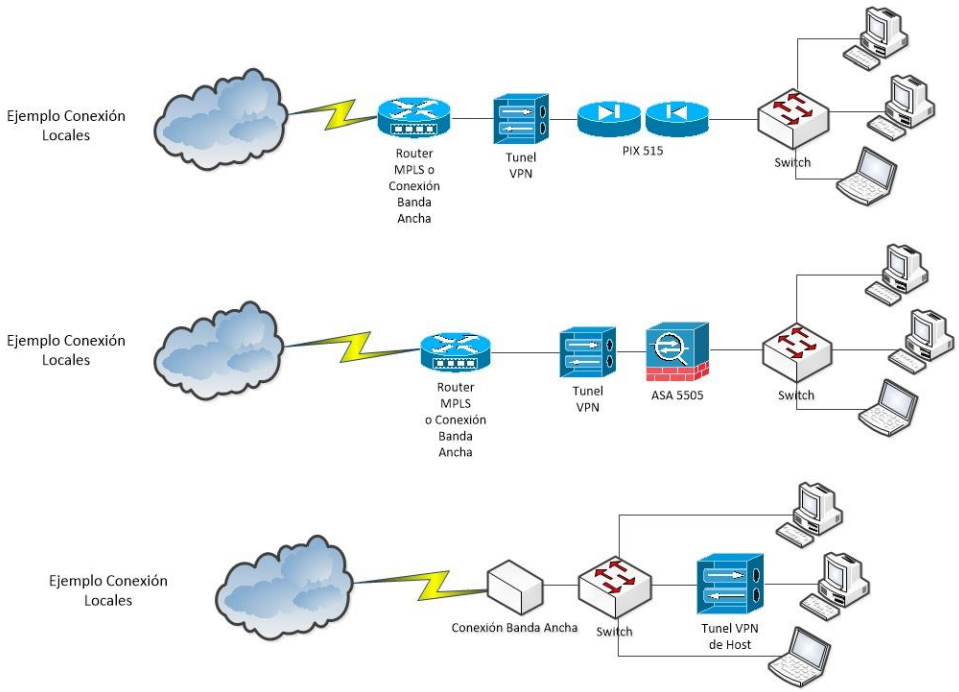


Fig. 14.3. Etapa 3: Diagrama de Conexión de los Locales.

9) Cronograma real vs. Cronograma previsto

Fecha	Fecha real	Actividad	Propósito	Responsable	Duración	Duración Real
02/05/2016	17/05/2016	Observación directa	Información Varia	Diego Rivilli	2h 30min	4hs
02/05/2016	17/05/2016	Recopilación documentos	Información Varia	Marcos Manzotti	2h 15min	2hs
03/05/2016	19/05/2016	Procesamiento observación directa		Diego Rivilli	20hs	40hs
13/05/2015	06/06/2015	Procesamiento documentos		Diego Rivilli	15hs	30hs
14/05/2015	07/06/2015	Actualización planilla boca de red y creación diagramas de conexión	Ejemplificar las conexiones de red de la empresa	Marcos Manzotti - Diego Rivilli	45hs	60hs

Tabla. 14.3. Etapa 3: Cronograma Real Vs Previsto.

ETAPA 4: HERRAMIENTAS

1) Herramientas de Microsoft

1.1) Sysinternals

Sitio Web: https://technet.microsoft.com/en-us/sysinternals/bb545027.aspx

Conjunto de herramientas imprescindibles para cualquier administrador y analista de seguridad.

Windows Sysinternals es un repositorio de utilidades de software gratuito de Microsoft. El sitio de Sysinternals contiene utilidades desarrolladas por Mark Russinovich y Bryce Cogswell.

Sysinternals ofrece programas bajo las siguientes categorías:

- Archivo y disco: contiene utilidades para controlar el uso de archivos y el estado de los discos.
- Trabajo en red: contiene aplicaciones como TCPview, que controla los extremos TCP y UDP.
- Process: la descarga más popular de Microsoft, Process Explorer, que controla de forma granular los archivos que un proceso en concreto ha abierto, está en esta categoría.
- Seguridad: RootkitRevealer, entre otras utilidades de seguridad incluidas en esta categoría.
- Información del sistema: esta categoría incluye productos que muestran información general sobre una estación de trabajo o un servidor.

1.1.1)TCPView

Esta herramienta trabaja en la mayoría de los sistemas operativos de Microsoft, y muestra una lista de conexiones establecidas con otros hosts, ya sean TCP o UDP.

Como resultado podemos observar:

- El nombre del proceso que realiza la conexión
- El PID, o número de identificación del proceso
- Que protocolo se utiliza en la conexión
- Puerto y nombre del host local que envía y recibe la conexión
- IP, DNS o nombre del host remoto que recibe y envía información
- Estado de la conexión (listening, etc).

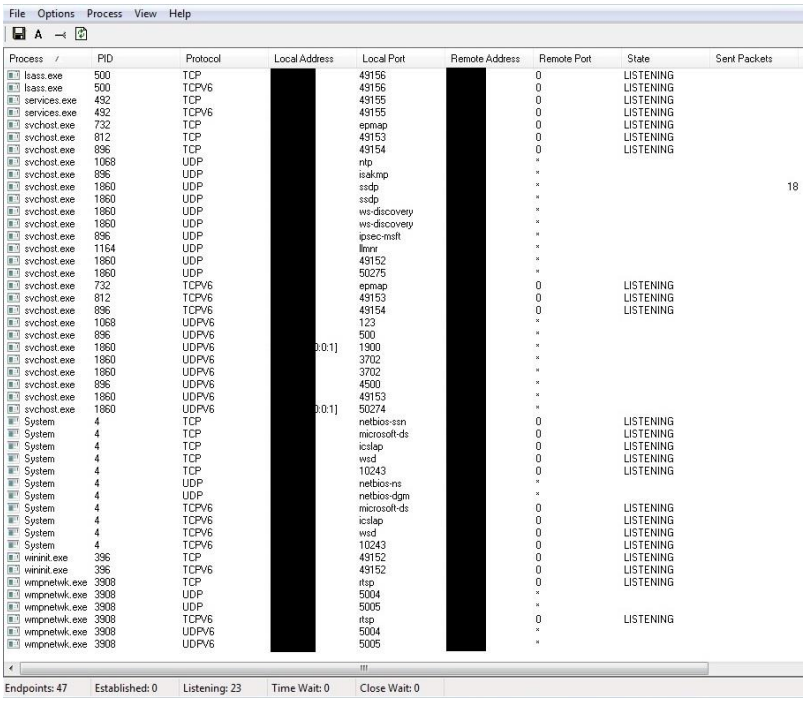


Fig. 14.3. Etapa 4: Herramientas, Microsoft. TCPView.

1.1.2)PsPing

Sencilla herramienta que nos deja ver el ancho de banda y latencia de nuestra red.

Estas son sus opciones:

psping -? [i | t | l | b]

-? i	Uso de ping ICMP.
-? t	Uso para el ping TCP.
-? l	Uso para la prueba de latencia.
-? b	Uso para la prueba de ancho de banda.

1.2) Microsoft Baseline Security Analyzer 2.3

Sitio Web: https://www.microsoft.com/en-us/download/details.aspx?id=7558

MBSA es una herramienta de Microsoft, de larga data y bien conocida por los profesionales de la seguridad informática. Este analizador de seguridad es fácil de utilizar y está adecuado para las pequeñas y medianas empresas para que puedan determinar, según los consejos de Microsoft, su estado de seguridad, y aconseja soluciones específicas.

Microsoft Baseline Security Analizer es compatible con los sistemas operativos de Microsoft; MBSA mejora el proceso de administración de seguridad detectando los errores más frecuentes de actualización y configuración de seguridad ausentes en los sistemas de información.

Fig. 14.3. Etapa 4: Herramientas, Microsoft Baseline Analyzer 2.3.

Ver capturas de pantalla en el Anexo 5 en la página 131.

2) SoftPerfect Network Scanner

Sitio Web: https://www.softperfect.com/download/

SoftPerfect Network Scanner es un software libre multi-threaded IP (multi-procesador IP), NetBios y SNMP scanner con una interfaz moderna y varias funciones avanzadas. Está destinado tanto para los administradores de sistemas como para usuarios en general interesados en la seguridad informática. El programa ping a computadoras, analiza puertos TCP en escucha y muestra los tipos de recursos compartidos en la red (incluido el sistema y ocultos).

Además permite mostrar las carpetas compartidas como unidades de red, navegar usando el explorador de Windows, filtro de la lista de resultados y mucho más. SoftPerfect Network Scanner también puede comprobar un puerto definido por el usuario y que informe si uno está abierto. También puede resolver nombres de host y detectar automáticamente el rango de IP local y externa. Es compatible con el apagado remoto (siempre y cuando se tengan privilegios de administrador, o los datos de una cuenta de usuario en dicho PC) y Wake-On-LAN (encendido remoto), así como hibernar o suspender.

Características principales:

- Ping a computadoras.
- No se requieren privilegios administrativos.
- Detecta el hardware (MAC), incluso a través de enrutadores.

- Detecta y oculta las carpetas compartidas (normalmente invisibles en la red) y escribe las cuotas de acceso.
- Detecta interna y externamente sus direcciones IP.
- Analiza para escuchar los puertos TCP y los servidores SNMP.
- Recupera la actualidad de los usuarios registrados.
- Se puede mostrar y explorar los recursos de la red.
- Puede lanzar aplicaciones externas de terceros.
- Los resultados se pueden exportar a HTML, XML, CSV y TXT.
- Soporta Wake-On-LAN, apagado remoto y el envío de mensajes a la red.
- Recupera potencialmente cualquier información a través de WMI.
- Recupera información de registro remoto.
- Es totalmente gratuito, no requiere instalación, y no contiene ningún tipo de adware, spyware y malware.

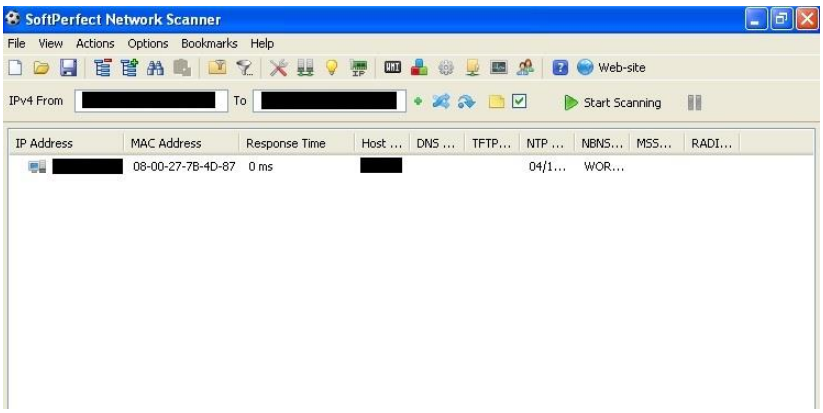


Fig. 14.3. Etapa 4: Herramientas, SoftPerfect Network Scanner.

3) IPTools

IP-Tools ofrece muchas utilidades de TCP / IP en un solo programa. Este galardonado programa puede funcionar en Windows 2000 / XP / Vista, Windows 7/8/10, Windows Server 2003/2008/2012 y es indispensable para cualquier persona que utiliza el Internet o Intranet. El mismo ofrece una prueba gratis por 21 días.

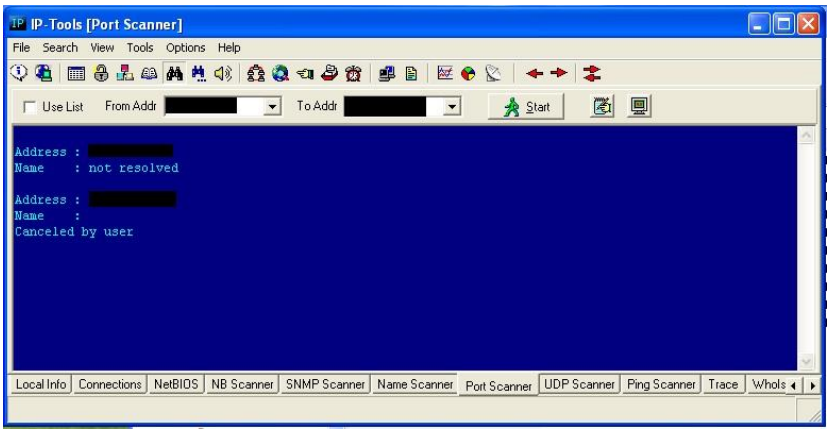


Fig. 14.3. Etapa 4: Herramientas, IP-Tools.

Características principales:

- El programa permite el funcionamiento multitarea - Es posible utilizar todos los servicios públicos al mismo tiempo.
- Las utilidades pueden recuperar información de un único host, desde todos los hosts dentro del rango especificado de direcciones IP (por ejemplo 195.128.74.1 -. 195.130.200.5) o trabajar con la lista de hosts y direcciones IP.
- IP-Tools puede guardar la información obtenida en un archivo de texto o crear informes HTML.
- La interfaz es altamente intuitiva y hace la operación fácil para los usuarios.

4) Retina CS

Sitio Web: https://www.beyondtrust.com/

Retina CS ofrece una prueba gratis del software por 365 días, es una herramienta diseñada para la administración de vulnerabilidades, donde se pueden realizar evaluaciones y análisis de riesgos de los puntos débiles de las áreas donde se encuentra expuesta la seguridad. Su diseño está orientado a los resultados y trabaja con los profesionales de la seguridad informática para analizar el impacto comercial, organizar y realizar correcciones de forma proactiva en toda la infraestructura, la cual puede ser móvil, virtual, de la web, de red y en la nube.

Retina CS fue creado para ser escalable y tiene buen rendimiento en entornos con dimensiones de magnitud. Ofrece control y comando de forma centralizada de las evaluaciones de una infraestructura heterogénea y dispar.

Esta plataforma facilita a gerentes y auditores tomar decisiones inteligentes, una comunicación eficaz de los riesgos y la presentación de informes con el detalle de avances en la administración de vulnerabilidades.

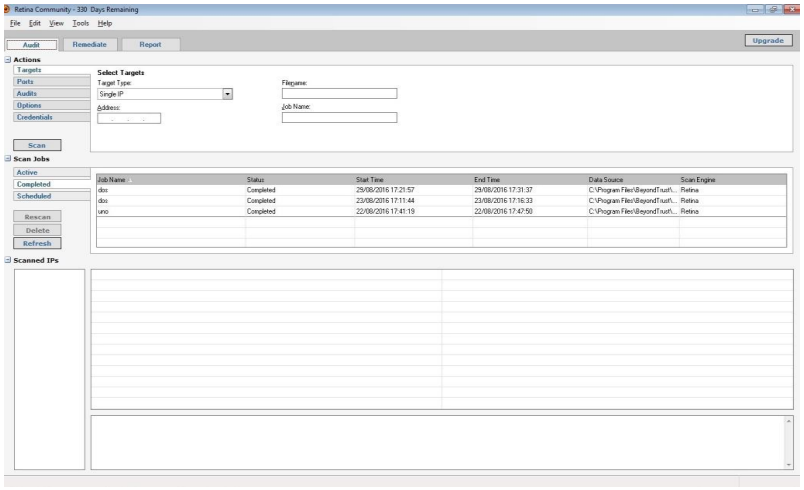


Fig. 14.3. Etapa 4: Herramientas Retina CS.

Ver capturas de pantalla en Anexo 6 en la página 133.

5) Nexpose

Sitio Web: https://www.rapid7.com/es/products/nexpose/compare-downloads.jsp

Nexpose es una herramienta que permite ejecutar diferentes tipos de escaneos en búsqueda de vulnerabilidades en un host o red, permite la definición de determinadas opciones que nos permiten acceder a un escaneo mucho más preciso con el uso de filtros por puertos, máquinas, segmentos de red, protocolos, etc. No es una herramienta gratis, pero existe una versión community, que no tiene todas las características.

Como mínimo requiere un Procesador de 2ghz, 8Gb de memoria RAM y 10Gb de espacio en disco. Es por esto que no logramos probarla

6) Kali Linux

Sitio web: https://www.kali.org/

Es una distribución de Linux desarrollada para la realización de pruebas de penetración y auditorías de seguridad.

Es una re-construcción de BackTrack Linux desde la base hacia arriba, respetando los estándares de desarrollo de Debian. Todas las herramientas presentadas en la nueva infraestructura fueron revisadas y probadas.

Las principales características que distinguen a kali de otros sistemas son las siguientes:

- Trae preinstalados más de 600 programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (un crackeador de passwords) y la suite Aircrack-ng (software para pruebas de seguridad en redes inalámbricas)..
- Es desarrollado bajo licencia GNU GLP por lo tanto es un software libre de uso y modificación.
- Puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal
- Soporta una gran variedad de dispositivos inalámbricos, gracias al gran repositorio de drives que posee la plataforma.

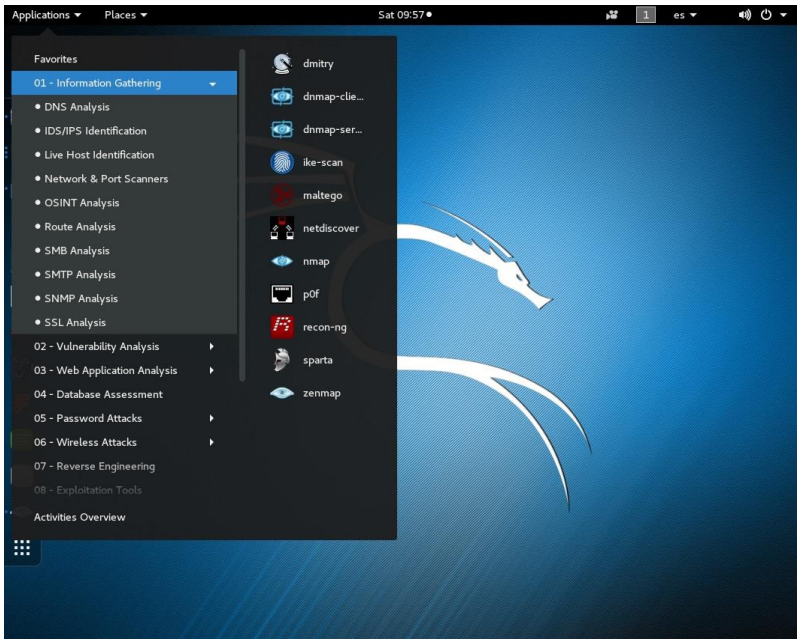


Fig. 14.3. Etapa 4: Herramientas, Kali Linux.

Dentro de este sistema seleccionamos las siguientes herramientas para testearlas y seleccionar las más apropiadas para desarrollar nuestro trabajo, en función de sus características y adaptabilidad.

6.1) OpenVas

Sitio web: http://www.openvas.org/

Se trata de un framework que tiene como base servicios y herramientas para el escaneo de redes y la evaluación de vulnerabilidades. Puede utilizarse de forma individual

o como parte del conjunto de herramientas de seguridad incluidas en OSSIM (Open Source Security Information Management).

Distribuciones como Kali Linux cuentan con esta herramienta instalada de forma predefinida, misma que puede ser utilizada a través de dos clientes, desde línea de comandos (OpenVAS CLI) o una interfaz web (Greenbone Security Assistant).

A través de las interfaces se interactúa con dos servicios: OpenVAS Manager y OpenVAS Scanner. El primero es el servicio que lleva a cabo tareas como el filtrado o clasificación de los resultados del análisis, control de las bases de datos que contienen la configuración o los resultados de la exploración y la administración de los usuarios, incluyendo grupos y roles.

Por su lado, el escáner ejecuta las denominadas NVT (Pruebas de vulnerabilidades de red), es decir, las pruebas de vulnerabilidades de red, conformadas por rutinas que comprueban la presencia de un problema de seguridad específico conocido o potencial en los sistemas. Las NVT se agrupan en familias de pruebas similares, por lo que la selección de las familias y/o NVT individuales es parte de la configuración de escaneo.

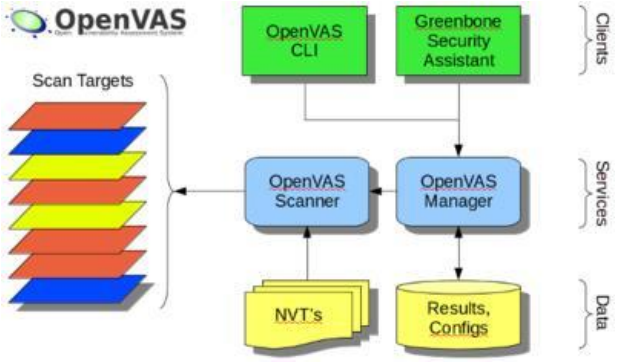


Fig. 14.3. Etapa 4: Herramientas, Kali Linux – OpenVAS Funcionamiento.

El proyecto OpenVAS mantiene una colección de NVT, que crece constantemente y que actualiza los registros semanalmente. Los equipos instalados con OpenVAS se sincronizan con los servidores para actualizar las pruebas de vulnerabilidades.

Las principales características son:

- Escaneo concurrente de múltiples nodos.
- Soporte SSL.
- Soporte para WMI
- Escaneo automático temporizado.
- Reportes en múltiples formatos (XML, HTML, LaTeX, entre otros)

- Servidor web integrado.
- Multiplataforma.

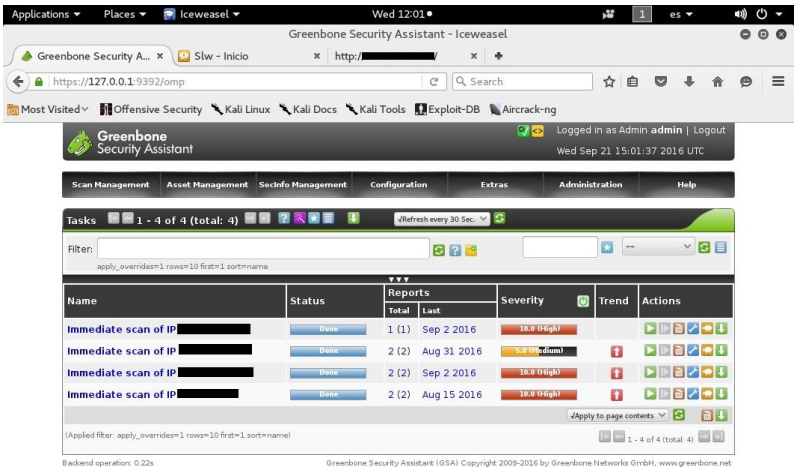


Fig. 14.3. Etapa 4: Herramientas, Kali Linux – OpenVAS Ejemplo 1.

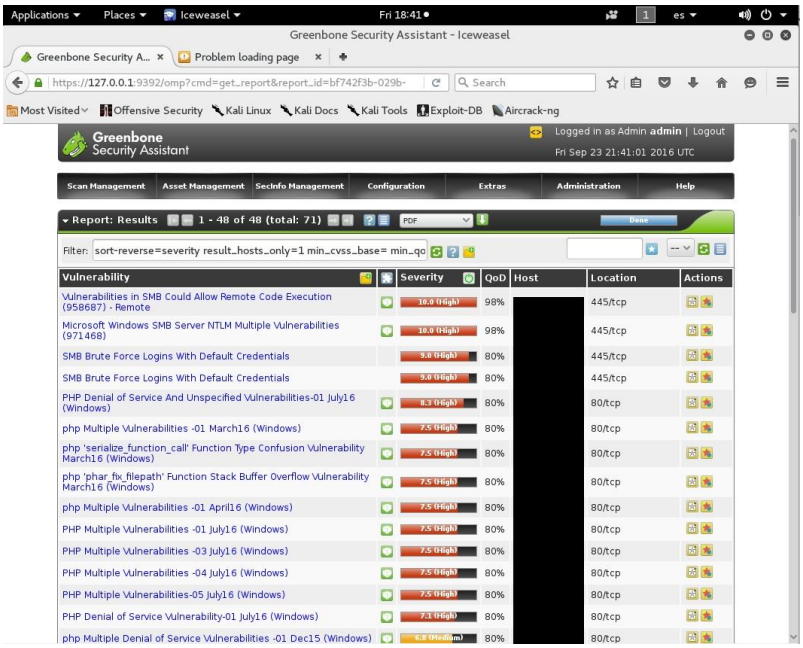


Fig. 14.3. Etapa 4: Herramientas, Kali Linux – OpenVAS Ejemplo 2.

6.2) <u>Nmap y Zenmap</u>

Sitio web: https://nmap.org/

Nmap un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich[cita requerida]) y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma. Y ZenMap es la misma aplicación con la adición de la interfaz gráfica.

Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir equipos, servicios y sistemas operativos en una red informática, estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la red incluyendo latencia y congestión de la misma, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Sus principales características son:

- Descubrimiento de equipos: Identifica computadoras en una red, por ejemplo listando aquellas que responden al ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

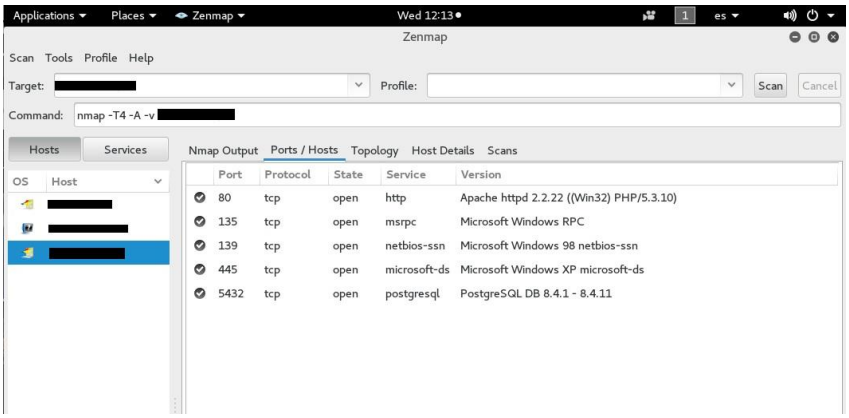


Fig. 14.3. Etapa 4: Herramientas, Kali Linux – ZenMap Ejemplo 1.

7) Resumen Análisis de Herramientas

Herramientas	Descubrimiento Red	Funcionamiento Red	Identificación Host	Escaneo Puertos Host	Análisis Vuln.	Sistema Operativo	Reportes	Licencia
Herramientas de Microsoft								
- Sysinternals								
*** PsPing**	SI	SI	NO	SI	NO	Windows	Básico	Free
***TCPView**	NO	NO	NO	SI	NO	Windows	NO	Free
- Baseline Security Analizer 2.3	SI	NO	SI	NO	SI	SI	SI	Free
SoftPerfect Network Scanner	SI	SI	SI	SI	NO	Windows	NO	Free
Retina CS	SI	SI	SI	SI	SI	Windows	SI	Free to trial 365 days
Nexpose	SI	SI	SI	SI	SI	SI	SI	
IpTools	SI	SI	SI	SI	NO	NO	NO	Free to trial 21 days
Kali Linux								
- OpenVas	SI	SI	SI	SI	SI	Linux -	SI	GPL2
- Zenmap - Nmap	SI	SI	SI	SI	--	Linux-Windows	SI	GPL2

Tabla. 14.3. Etapa 4: Herramientas, Resumen Análisis.

ETAPA 5: MUESTREO DE LA RED

1) Herramientas Seleccionadas Para Realizar el Muestreo

1.1) Zenmap

Esta es la primera herramienta que seleccionamos, debido a su simplicidad y facilidad de uso y además es la que mejor se adapta a nuestras necesidades, gracias a que:

- Puede realizar un escaneo completo de la red o realizarlo en un rango determinado especificado por el usuario, y detectar cuales son los equipos conectados.
- Puede realizar un escaneo de todos los puertos o simplemente de los puertos más conocidos, en los distintos equipos descubiertos en la red.
- Detectar el nombre, el sistema operativo y las características del hardware de red que posee el equipo escaneado.
- Puede medir la velocidad y latencia de la red.
- Es un software libre y gratuito, por lo que puede realizar todas estas tareas sin un límite de la cantidad de equipos con los que se puede trabajar.

1.2) Retina

Seleccionamos esta aplicación gracias a que tiene una gran cantidad de variables y al ser una aplicación tan flexible, es posible ajustarla a nuestros requerimientos, ya que:

- Puede realizar una gran variedad de escaneos a la red, según IP, rango de IPs, a puertos determinados, incluso a un grupo de usuarios, ya sea con usuario invitado o con un usuario propio de la red.
- Otra ventaja de esta herramienta, es la capacidad de seleccionar distintos tipos de reportes de la auditoría realizada, además de exportar el mismo en distintos formatos.
- También permite realizar una selección de tipo de prueba de vulnerabilidades, con lo cual es posible realizar pruebas específicas a un equipo.

2) Procedimiento de muestreo

El muestreo se llevó a cabo según estas distintas situaciones hipotéticas de exposición de la red:

1. *Equipo conectado en una boca de Red aleatoria, tomando número de IP del servidor DHCP*.

   El objetivo de este punto, es verificar cual es el nivel de exposición de la red y de los equipos conectados a la misma, ante un equipo desconocido que es conectado a la red.

2. *Equipo conectado en una boca de Red aleatoria, con un Número de IP Fijo de administración de red.*

   El objetivo de este punto es verificar el nivel de exposición de los equipos en la red, ante un equipo que posee un nivel de administración de red, además de contrastar el acceso a la red con el punto anterior.

Para mejor discernimiento de los resultados arrojados de las distintas situaciones hipotéticas, se optó por comprobar los resultados evaluando:

- *Acceso a la red de la empresa.*

  Se conectó un equipo a un puerto libre en cualquier ubicación, y se observó cómo interactuó el mismo con la red.

- *Conexión a los servidores y demás equipos de red.*

  Una vez que se ha conectado el equipo de prueba, se realizaron con la aplicación Zenmap un barrido de direcciones IP, para evaluar la respuesta de los distintos servidores y equipos, luego se realizó el mismo barrido, activando la opción de descubrimiento de puertos abiertos. Además se evaluaron con la aplicación retina, las vulnerabilidades de algunos equipos expuestos en la red.

- *Acceso a otras Vlans.*

  Además de la evaluación de la red interna general, basándonos en la documentación de la red, se evaluaron las Vlans realizando un barrido de IP con la aplicación Zenmap, también se realizó el mismo barrido, activando la opción de descubrimiento de puertos abiertos. Luego se evaluaron con la aplicación retina, las vulnerabilidades de algunos de los equipos descubiertos en la red.

- *Conexión a las redes internas de los locales.*

  Se evaluaron las redes propias de los locales, realizando también un barrido de la red con la aplicación Zenmap. Luego se realizaron las mismas pruebas del paso anterior, con lo que se relevaron las respuestas de los equipos que se encuentran en dicha red.

3) Resumen y Ejemplos del Muestreo a Realizar para cada situación hipotética

Actividad	Herramienta escaneo	Comando de muestreo (ejemplo)	Tiempo
Conexión Host	Comando Windows	IPconfig	5min
Escaneo Red zz	Zenmap	nmap –sn xx.yy.zz.1-35 nmap –PO xx.yy.zz.1-35	15min
Análisis completo red zz	Zenmap	nmap -T4 -A –v xx.yy.zz.1-35	25min
Análisis vulnerabilidades	Retina	Target single ip xx.yy.zz.2	25min

Tabla. 14.3. Etapa 5: Resumen y Ejemplos de Muestreo.

ETAPA 6: RECOPILACIÓN DE INFORMACIÓN DEL MUESTREO DE LA RED

1) Prueba Nº 1: equipo conectado a una boca de red aleatoria, tomando número de IP del servidor DHCP

El muestreo se llevó a cabo según las distintas situaciones hipotéticas planteadas en el punto anterior, para así conocer más las distintas respuestas que se obtienen de la red y de los equipos conectados a ella.

1.1) Acceso a la red de la empresa.

Al conectar el equipo a la red, se observó cómo interactuó el mismo con la red y negoció con el servidor de DHCP el sufijo DNS, la dirección IP, la máscara de red, la dirección del Gateway de red y de los Servidores DNS y Wins.

Las capturas de pantalla son a modo de ejemplo y no comprenden a la totalidad de las pruebas realizadas.

```
Configuraci¢n IP de Windows

   Nombre de host. . . . . . . . . : Test01
   Sufijo DNS principal  . . . . . : mrseguridad.com.ar
   Tipo de nodo. . . . . . . . . . : h¡brido
   Enrutamiento IP habilitado. . . : no
   Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Conexi¢n de  rea local:

   Sufijo DNS espec¡fico para la conexi¢n. . :
   Descripci¢n . . . . . . . . . . . . . . . : Adaptador de escritorio
Intel(R) PRO/1000 MT
   Direcci¢n f¡sica. . . . . . . . . . . . . : 08-00-27-1F-9E-DF
   DHCP habilitado . . . . . . . . . . . . . : s¡
   Configuraci¢n autom tica habilitada . . . : s¡
   Direcci¢n IPv4. . . . . . . . . . . . . . : xx.yy.zz.35(Preferido)
   M scara de subred . . . . . . . . . . . . : 255.255.252.0
   Consesi¢n obtenida. . . . . . . . . . . . : 05 de octubre de 2016
15:24:05
   La consesi¢n expira . . . . . . . . . . . : 07 de octubre de 2016
21:24:05
   Puerta de enlace predeterminada . . . . . : xx.yy.cc.1
   Servidor DHCP . . . . . . . . . . . . . . : xx.yy.cc.4
   Servidores DNS. . . . . . . . . . . . . . : xx.yy.cc.4
                                       xx.yy.cc.25
   Servidor WINS principal . . . . . . . . . : xx.yy.cc.4
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

Fig. 14.3. Etapa 6: Rec. de Información, Ipconfig: Conexión Red General Con Nº IP Del DHCP.

1.2) Conexión a los equipos del mismo segmento de red.

Al realizar con la aplicación Zenmap un escaneo a un rango de direcciones IP, del grupo de equipos que pertenecen al mismo segmento de red que el equipo de prueba, la aplicación devolvió información referida al Nº IP, Dirección MAC y tiempo de respuesta de los equipos que se encuentran conectados a la red (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-10-12 18:41 ART
Nmap scan report for xx.yy.zz.0
Host is up (0.00046s latency).
MAC Address: 00:0B:82:29:6D:DA (Grandstream Networks)
Nmap scan report for xx.yy.zz.1
Host is up (0.00033s latency).
MAC Address: 90:2B:34:04:7D:79 (Giga-byte Technology)
Nmap scan report for xx.yy.zz.3
Host is up (0.00077s latency).
MAC Address: 74:D4:35:E9:DA:28 (Giga-byte Technology)
Nmap scan report for xx.yy.zz.5
Host is up (0.00042s latency).
MAC Address: 50:E5:49:DB:9E:70 (Giga-byte Technology)
Nmap scan report for xx.yy.zz.6
Host is up (0.00039s latency).
MAC Address: 90:2B:34:01:A8:F1 (Giga-byte Technology)
Nmap scan report for xx.yy.zz.7
Host is up (0.00096s latency).
MAC Address: 74:D4:35:E8:1D:E9 (Giga-byte Technology)
Nmap scan report for xx.yy.zz.10
Host is up (0.014s latency).
          .
          .
          .
MAC Address: 90:2B:34:02:B3:C4 (Giga-byte Technology)
Nmap scan report for xx.yy.zz.28
Host is up (0.00038s latency).
MAC Address: 00:25:22:A7:30:F4 (ASRock Incorporation)
Nmap scan report for xx.yy.zz.29
Host is up (0.00050s latency).
MAC Address: 74:D4:35:E7:D6:D6 (Giga-byte Technology)
Nmap done: 32 IP addresses (24 hosts up) scanned in 26.44 seconds
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Descubriendo Red Mismo Segmento en Vlan General.

Posteriormente se realizó con la aplicación Zenmap, un análisis más profundo de los equipos detectados en el paso anterior y la aplicación devolvió información de Nº IP, Nombre del equipo, Sistema Operativo, puertos abiertos, etc; de los equipos que se encuentran conectados a la red (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-10-12 18:43 ART
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:43
Completed NSE at 18:43, 0.00s elapsed
Initiating NSE at 18:43
Completed NSE at 18:43, 0.00s elapsed
Initiating ARP Ping Scan at 18:43
Scanning 32 hosts [1 port/host]
Completed ARP Ping Scan at 18:43, 0.26s elapsed (32 total hosts)
Initiating Parallel DNS resolution of 32 hosts. at 18:43
Completed Parallel DNS resolution of 32 hosts. at 18:43, 26.01s elapsed
Nmap scan report for xx.yy.zz.2 [host down]
Nmap scan report for xx.yy.zz.4 [host down]
                .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos mismo Segmento en Vlan Gral.

```
                .
Nmap scan report for xx.yy.zz.30 [host down]
Nmap scan report for xx.yy.zz.31 [host down]
Initiating SYN Stealth Scan at 18:43
Scanning 24 hosts [1000 ports/host]
Discovered open port 23/tcp on xx.yy.zz.0
Discovered open port 80/tcp on xx.yy.zz.0
Discovered open port 445/tcp on xx.yy.zz.14
                .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos mismo Segmento en Vlan Gral.

```
                .
Discovered open port 49155/tcp on xx.yy.zz.28
Completed SYN Stealth Scan against xx.yy.zz.0 in 30.39s (23 hosts left)
Discovered open port 49161/tcp on xx.yy.zz.15
Discovered open port 6129/tcp on xx.yy.zz.15
Completed SYN Stealth Scan against xx.yy.zz.6 in 47.07s (22 hosts left)
Completed SYN Stealth Scan against xx.yy.zz.10 in 47.82s (21 hosts left)
                .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos mismo Segmento en Vlan Gral.

```
                .
Completed SYN Stealth Scan against xx.yy.zz.18 in 49.27s (1 host left)
Completed SYN Stealth Scan at 18:44, 49.30s elapsed (24000 total ports)
Initiating Service scan at 18:44
Scanning 92 services on 24 hosts
Completed Service scan at 18:45, 84.74s elapsed (92 services on 24 hosts)
Initiating OS detection (try #1) against 24 hosts
Retrying OS detection (try #2) against 2 hosts
                .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos mismo Segmento en Vlan Gral.

```
                .
Nmap scan report for xx.yy.zz.1
Host is up (0.00058s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows 10 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=pdi2243.mrseguridad.com.ar
| Issuer: commonName=pdi2243.mrseguridad.com.ar
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-06-21T13:49:38
| Not valid after:  2016-12-21T13:49:38
| MD5:   fc07 04a5 7fca f10a 3aea e8ae 8413 8348
|_SHA-1: c35a b3af e167 0e10 b94d fe0a dc9a 58ab 4d63 8208
|_ssl-date: 2016-10-12T21:49:35+00:00; +3m24s from scanner time.
49175/tcp open  msrpc              Microsoft Windows RPC
MAC Address: 90:2B:34:04:7D:79 (Giga-byte Technology)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7
cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1
OS details: Windows Server 2008 R2, Microsoft Windows Embedded Standard 7,
Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1,
Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows
7 SP1, or Windows Server 2008
Uptime guess: 0.055 days (since Wed Oct 12 17:29:29 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows 98, Windows 10; CPE:
cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98,
cpe:/o:microsoft:windows_10

Host script results:
| nbstat: NetBIOS name: PDI2243, NetBIOS user: <unknown>, NetBIOS MAC:
90:2b:34:04:7d:79 (Giga-byte Technology)
| Names:
|   PDI2243<00>          Flags: <unique><active>
|   mrseguridad<00>          Flags: <group><active>
|   PDI2243<20>          Flags: <unique><active>
|_  mrseguridad<1e>          Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional
6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: pdi2243
|   NetBIOS computer name: PDI2243
|   Domain name: mrseguridad.com.ar
|   Forest name: mrseguridad.com.ar
|   FQDN: pdi2243.mrseguridad.com.ar
|_  System time: 2016-10-12T18:51:16-03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.58 ms xx.yy.zz.1
                .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos mismo Segmento en Vlan Gral.

```
                .
Nmap scan report for xx.yy.zz.29
Host is up (0.0013s latency).
                .
                .
Host script results:
| nbstat: NetBIOS name: PDI5089, NetBIOS user: <unknown>, NetBIOS MAC:
74:d4:35:e7:d6:d6 (Giga-byte Technology)
| Names:
|   PDI5089<00>          Flags: <unique><active>
|   PDI5089<20>          Flags: <unique><active>
|   mrseguridad<00>          Flags: <group><active>
|_  mrseguridad<1e>          Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional
6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: pdi5089
|   NetBIOS computer name: PDI5089
|   Domain name: mrseguridad.com.ar
|   Forest name: mrseguridad.com.ar
|   FQDN: pdi5089.mrseguridad.com.ar
|_  System time: 2016-10-12T18:51:10-03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   1.32 ms xx.yy.zz.29
                .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos mismo Segmento en Vlan Gral.

```
                .
NSE: Script Post-scanning.
Initiating NSE at 18:48
Completed NSE at 18:48, 0.00s elapsed
Initiating NSE at 18:48
Completed NSE at 18:48, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 32 IP addresses (24 hosts up) scanned in 325.33 seconds
           Raw packets sent: 53746 (2.412MB) | Rcvd: 2184 (101.128KB)
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos mismo Segmento en Vlan Gral.

Luego se realizó una evaluación con la aplicación Retina CS, de las Vulnerabilidades de algunos equipos seleccionados de la red.

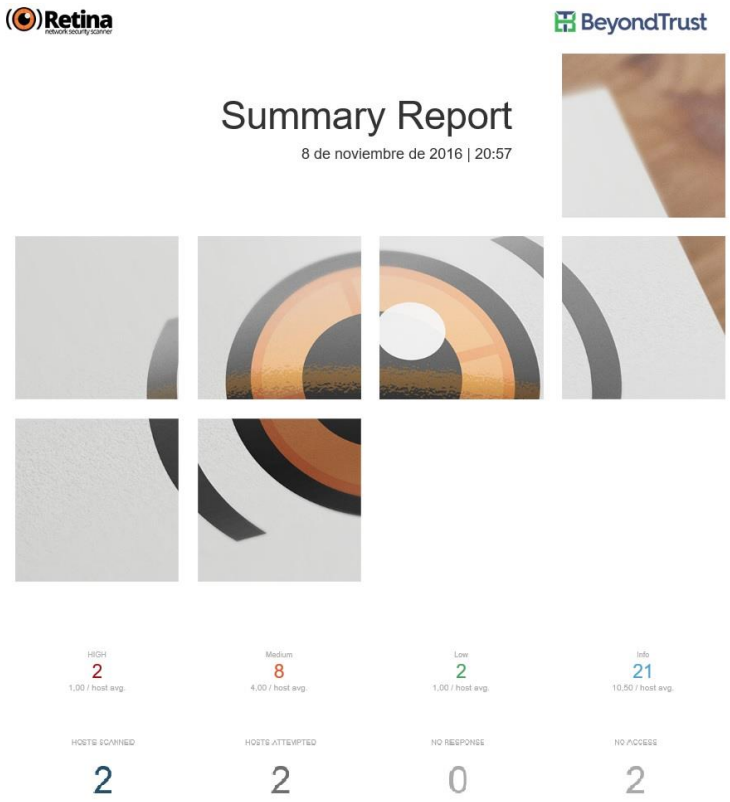


Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Equipos mismo Segmento en Vlan Gral.

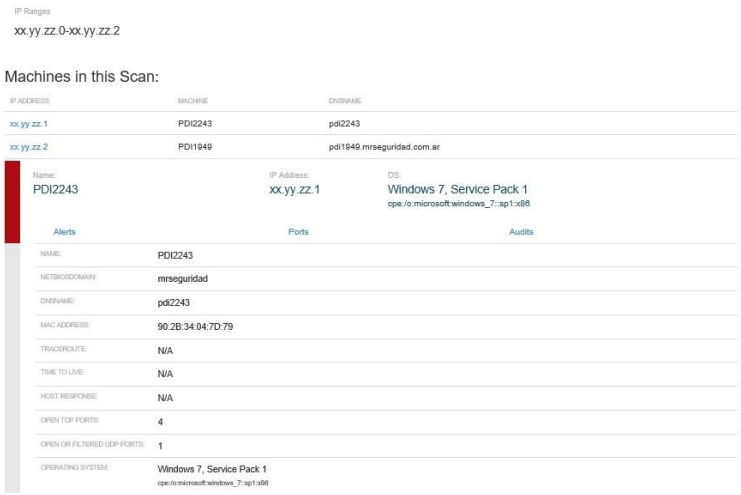
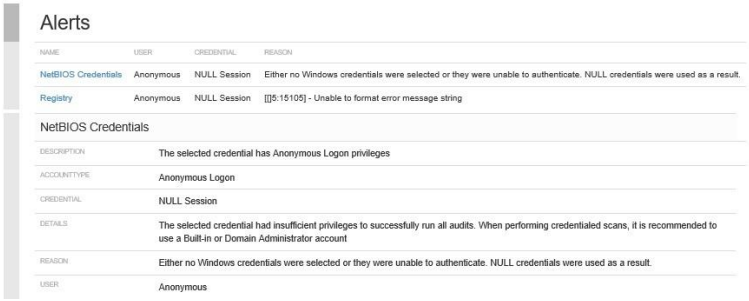


Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Equipos mismo Segmento en Vlan Gral.



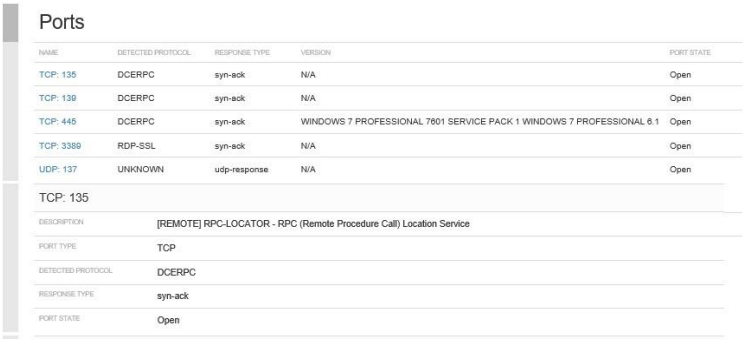
Alerts

NAME	USER	CREDENTIAL	REASON
NetBIOS Credentials	Anonymous	NULL Session	Either no Windows credentials were selected or they were unable to authenticate. NULL credentials were used as a result.
Registry	Anonymous	NULL Session	[[]5:15105] - Unable to format error message string

NetBIOS Credentials

DESCRIPTION	The selected credential has Anonymous Logon privileges
ACCOUNTTYPE	Anonymous Logon
CREDENTIAL	NULL Session
DETAILS	The selected credential had insufficient privileges to successfully run all audits. When performing credentialed scans, it is recommended to use a Built-in or Domain Administrator account
REASON	Either no Windows credentials were selected or they were unable to authenticate. NULL credentials were used as a result.
USER	Anonymous

Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Equipos mismo Segmento en Vlan Gral.



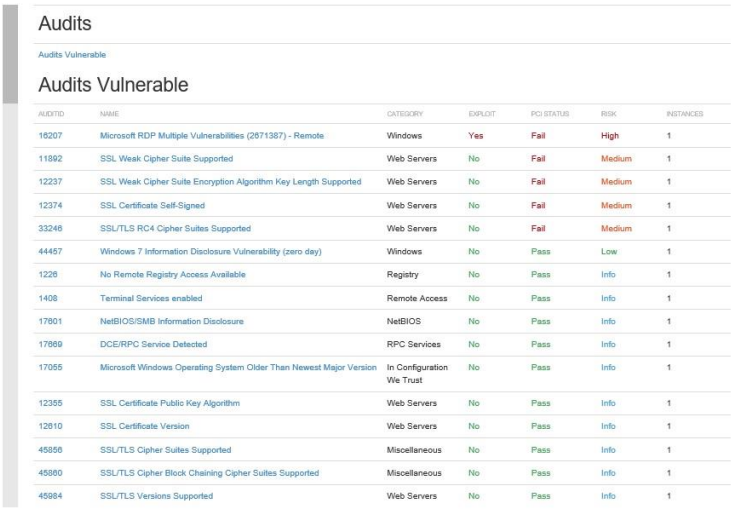
Ports

NAME	DETECTED PROTOCOL	RESPONSE TYPE	VERSION	PORT STATE
TCP: 135	DCERPC	syn-ack	N/A	Open
TCP: 139	DCERPC	syn-ack	N/A	Open
TCP: 445	DCERPC	syn-ack	WINDOWS 7 PROFESSIONAL 7601 SERVICE PACK 1 WINDOWS 7 PROFESSIONAL 6.1	Open
TCP: 3389	RDP-SSL	syn-ack	N/A	Open
UDP: 137	UNKNOWN	udp-response	N/A	Open

TCP: 135

DESCRIPTION	[REMOTE] RPC-LOCATOR - RPC (Remote Procedure Call) Location Service
PORT TYPE	TCP
DETECTED PROTOCOL	DCERPC
RESPONSE TYPE	syn-ack
PORT STATE	Open

Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Equipos mismo Segmento en Vlan Gral.



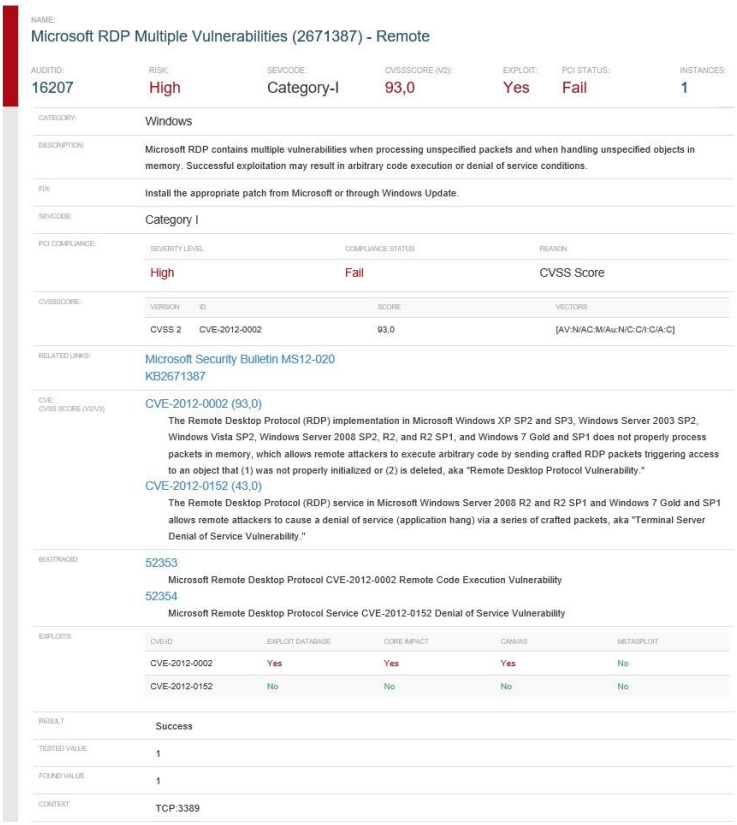
Audits

Audits Vulnerable

Audits Vulnerable

AUDITID	NAME	CATEGORY	EXPLOIT	PCI STATUS	RISK	INSTANCES
16207	Microsoft RDP Multiple Vulnerabilities (2671387) - Remote	Windows	Yes	Fail	High	1
11892	SSL Weak Cipher Suite Supported	Web Servers	No	Fail	Medium	1
12237	SSL Weak Cipher Suite Encryption Algorithm Key Length Supported	Web Servers	No	Fail	Medium	1
12374	SSL Certificate Self-Signed	Web Servers	No	Fail	Medium	1
33246	SSL/TLS RC4 Cipher Suites Supported	Web Servers	No	Fail	Medium	1
44457	Windows 7 Information Disclosure Vulnerability (zero day)	Windows	No	Pass	Low	1
1226	No Remote Registry Access Available	Registry	No	Pass	Info	1
1408	Terminal Services enabled	Remote Access	No	Pass	Info	1
17601	NetBIOS/SMB Information Disclosure	NetBIOS	No	Pass	Info	1
17669	DCE/RPC Service Detected	RPC Services	No	Pass	Info	1
17055	Microsoft Windows Operating System Older Than Newest Major Version	In Configuration We Trust	No	Pass	Info	1
12355	SSL Certificate Public Key Algorithm	Web Servers	No	Pass	Info	1
12610	SSL Certificate Version	Web Servers	No	Pass	Info	1
45856	SSL/TLS Cipher Suites Supported	Miscellaneous	No	Pass	Info	1
45860	SSL/TLS Cipher Block Chaining Cipher Suites Supported	Miscellaneous	No	Pass	Info	1
45984	SSL/TLS Versions Supported	Web Servers	No	Pass	Info	1

Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Equipos mismo Segmento en Vlan Gral.



NAME:
Microsoft RDP Multiple Vulnerabilities (2671387) - Remote

AUDITID:	RISK:	SEVCODE:	CVSSSCORE (V2):	EXPLOIT:	POI STATUS:	INSTANCES:
16207	High	Category-I	93,0	Yes	Fail	1

CATEGORY: Windows

DESCRIPTION: Microsoft RDP contains multiple vulnerabilities when processing unspecified packets and when handling unspecified objects in memory. Successful exploitation may result in arbitrary code execution or denial of service conditions.

FIX: Install the appropriate patch from Microsoft or through Windows Update.

SEVCODE: Category I

PCI COMPLIANCE:

SEVERITY LEVEL	COMPLIANCE STATUS	REASON
High	Fail	CVSS Score

CVSSSCORE:

VERSION	ID	SCORE	VECTORS
CVSS 2	CVE-2012-0002	93,0	[AV:N/AC:M/Au:N/C:C/I:C/A:C]

RELATED LINKS: Microsoft Security Bulletin MS12-020
KB2671387

CVE:
CVSS SCORE (V2/V3)

CVE-2012-0002 (93,0)
The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."

CVE-2012-0152 (43,0)
The Remote Desktop Protocol (RDP) service in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (application hang) via a series of crafted packets, aka "Terminal Server Denial of Service Vulnerability."

BUGTRAQID:

52353
Microsoft Remote Desktop Protocol CVE-2012-0002 Remote Code Execution Vulnerability

52354
Microsoft Remote Desktop Protocol Service CVE-2012-0152 Denial of Service Vulnerability

EXPLOITS:

CVEID	EXPLOIT DATABASE	CORE IMPACT	CANVAS	METASPLOIT
CVE-2012-0002	Yes	Yes	Yes	No
CVE-2012-0152	No	No	No	No

RESULT: Success

TESTED VALUE: 1

FOUND VALUE: 1

CONTEXT: TCP:3389

Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Equipos mismo Segmento en Vlan Gral.

1.3) Conexión a los servidores.

Luego se realizó un escaneo al grupo de direcciones IP de los equipos servidores de la red, la misma devolvió información con respecto al Nº IP, Dirección MAC y tiempo de respuesta de los equipos que se encuentran conectados a la red (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-02 19:23 ART
Nmap scan report for xx.yy.cc.1
Host is up (0.00048s latency).
MAC Address: 54:75:D0:DF:19:56 (Cisco Systems)
Nmap scan report for xx.yy.cc.2
Host is up (0.00052s latency).
MAC Address: 54:75:D0:F0:5D:BE (Cisco Systems)
Nmap scan report for xx.yy.cc.3
Host is up (0.00090s latency).
MAC Address: 00:11:BB:53:46:40 (Cisco Systems)
Nmap scan report for xx.yy.cc.4
Host is up (0.00018s latency).
MAC Address: 00:11:09:13:A2:6A (Micro-Star International)
Nmap scan report for xx.yy.cc.5
Host is up (0.00019s latency).
MAC Address: 00:09:0F:03:94:BE (Fortinet)
Nmap scan report for xx.yy.cc.7
Host is up (0.00052s latency).
MAC Address: 00:0C:29:C9:78:03 (VMware)
                    .
                    .
Nmap scan report for xx.yy.cc.20
Host is up (0.00044s latency).
MAC Address: 00:1C:C0:78:02:DB (Intel Corporate)
Nmap scan report for xx.yy.cc.25
Host is up (0.00033s latency).
MAC Address: 00:21:5E:67:EC:76 (IBM)
Nmap done: 21 IP addresses (19 hosts up) scanned in 13.42 seconds
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Descubriendo Red Segmento Servidores En Vlan Gral.

Posteriormente se realizó un Análisis más profundo de los equipos detectados en el paso anterior, la aplicación entregó la información referida al Nº IP, Nombre del equipo, Sistema Operativo, puertos abiertos, etc; de los equipos servidores que se encuentran conectados a la red (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-02 19:25 ART
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:25
Completed NSE at 19:25, 0.00s elapsed
Initiating NSE at 19:25
Completed NSE at 19:25, 0.00s elapsed
Initiating ARP Ping Scan at 19:25
Scanning 21 hosts [1 port/host]
Completed ARP Ping Scan at 19:25, 0.24s elapsed (21 total hosts)
Initiating Parallel DNS resolution of 21 hosts. at 19:25
Completed Parallel DNS resolution of 21 hosts. at 19:25, 13.01s elapsed
Nmap scan report for xx.yy.cc.6 [host down]
Nmap scan report for xx.yy.cc.12 [host down]
Initiating SYN Stealth Scan at 19:25
Scanning 19 hosts [1000 ports/host]
Discovered open port 80/tcp on xx.yy.cc.4
Discovered open port 80/tcp on xx.yy.cc.8
                    .
                    .
Completed SYN Stealth Scan against xx.yy.cc.3 in 49.51s (2 hosts left)
Completed SYN Stealth Scan against xx.yy.cc.2 in 49.67s (1 host left)
Completed SYN Stealth Scan at 19:26, 49.72s elapsed (19000 total ports)
Initiating Service scan at 19:26
Scanning 194 services on 19 hosts
Service scan Timing: About 33.51% done; ETC: 19:27 (0:01:02 remaining)
Service scan Timing: About 66.49% done; ETC: 19:28 (0:00:46 remaining)
Completed Service scan at 19:29, 178.59s elapsed (194 services on 19 hosts)
Initiating OS detection (try #1) against 19 hosts
Retrying OS detection (try #2) against 2 hosts
NSE: Script scanning 19 hosts.
Initiating NSE at 19:29
Completed NSE at 19:32, 169.73s elapsed
Initiating NSE at 19:32
Completed NSE at 19:32, 0.07s elapsed
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Segmento Servidores En Vlan Gral.

```
Nmap scan report for xx.yy.cc.1
Host is up (0.00040s latency).
All 1000 scanned ports on xx.yy.cc.1 are closed
MAC Address: 54:75:D0:DF:19:56 (Cisco Systems)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: firewall|webcam|router|WAP
Running: Cisco PIX OS 8.X, D-Link embedded, Linksys embedded
OS CPE: cpe:/o:cisco:pix_os:8.0 cpe:/h:dlink:dcs-6620g
cpe:/h:linksys:befsr41 cpe:/h:linksys:befw11s4
OS details: Cisco Adaptive Security Appliance 5510 or 5540 firewall (PIX OS
8.0), D-Link DCS-6620G webcam or Linksys BEFSR41 EtherFast router, Linksys
BEFSR81 router, Linksys BEFW11S4 WAP
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.40 ms xx.yy.cc.1
                    .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Segmento Servidores En Vlan Gral.

```
                    .
Nmap scan report for xx.yy.cc.3
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        Cisco SSH 1.25 (protocol 1.99)
| ssh-hostkey:
|   1024 d3:a5:7f:12:ad:6d:72:a9:44:f7:fb:a2:06:a2:cb:d0 (RSA1)
|_  1024 33:cb:5c:28:fb:1a:cc:a6:38:27:45:3b:6e:6e:ee:8a (RSA)
|_sshv1: Server supports SSHv1
23/tcp  open  telnet     Cisco IOS telnetd
80/tcp  open  http       Cisco IOS http config
| http-auth:
| HTTP/1.1 401 Unauthorized
|_  Basic realm=level_15_access
| http-methods:
|_  Supported Methods: POST
|_http-server-header: cisco-IOS
|_http-title: Site doesn't have a title.
443/tcp open  ssl/https?
|_ssl-date: 1993-05-29T09:03:48+00:00; -23y157d13h26m41s from scanner time.
MAC Address: 00:11:BB:53:46:40 (Cisco Systems)
Device type: switch
Running: Cisco IOS 12.X
OS CPE: cpe:/h:cisco:catalyst_1900 cpe:/h:cisco:catalyst_2820
cpe:/h:cisco:catalyst_2960 cpe:/h:cisco:catalyst_3560 cpe:/h:cisco:catalyst_
4500 cpe:/h:cisco:catalyst_6513 cpe:/o:cisco:ios:12.2
OS details: Cisco Catalyst 1900, 2820, 2960, 3560, 3750, 4500, or 6513
switch (IOS 12.2)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: IOS; Device: switch; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT     ADDRESS
1   1.37 ms xx.yy.cc.3
                    .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Segmento Servidores En Vlan Gral.

```
                    .
Nmap scan report for xx.yy.cc.4
Host is up (0.00026s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE       VERSION
42/tcp   open  wins          Microsoft Windows Wins
80/tcp   open  http          Microsoft IIS httpd 6.0
| http-auth:
| HTTP/1.1 401 Unauthorized
|_  Server returned status 401 but no WWW-Authenticate header.
|_http-server-header: Microsoft-IIS/6.0
|_http-title: No tiene autorizaci\xF3n para ver esta p\xE1gina
81/tcp   open  http          Microsoft IIS httpd 6.0
| http-auth:
| HTTP/1.1 401 Unauthorized
|   Negotiate
|_  NTLM
| http-ntlm-info:
|   Target_Name: mrseguridad
|   NetBIOS_Domain_Name: mrseguridad
|   NetBIOS_Computer_Name: DCCENT02
|   DNS_Domain_Name: mrseguridad.com.ar
|   DNS_Computer_Name: dccent02.mrseguridad.com.ar
|   DNS_Tree_Name: mrseguridad.com.ar
|_  Product_Version: 5.2 (Build 3790)
|_http-server-header: Microsoft-IIS/6.0
|_http-title: No tiene autorizaci\xF3n para ver esta p\xE1gina
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows 98 netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp open  msrpc         Microsoft Windows RPC
1072/tcp open  msrpc         Microsoft Windows RPC
1085/tcp open  msrpc         Microsoft Windows RPC
1086/tcp open  msrpc         Microsoft Windows RPC
1090/tcp open  msrpc         Microsoft Windows RPC
|_rmi-dumpregistry: Registry listing failed (Handshake failed)
3389/tcp open  ms-wbt-server Microsoft Terminal Service
6129/tcp open  damewaremr    DameWare Mini Remote Control
MAC Address: 00:11:09:13:A2:6A (Micro-Star International)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_
2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=250 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_server_2003

Host script results:
|_ms-sql-info:
| nbstat: NetBIOS name: DCCENT02, NetBIOS user: <unknown>, NetBIOS MAC:
00:11:09:13:a2:6a (Micro-Star International)
| Names:
|   DCCENT02<00>         Flags: <unique><active>
|   mrseguridad<00>          Flags: <group><active>
|   DCCENT02<20>         Flags: <unique><active>
|_  mrseguridad<1e>          Flags: <group><active>
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 2 (Windows Server 2003 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::sp2
|   Computer name: dccent02
|   NetBIOS computer name: DCCENT02
|   Domain name: mrseguridad.com.ar
|   Forest name: mrseguridad.com.ar
|   FQDN: dccent02.mrseguridad.com.ar
|_  System time: 2016-11-02T19:30:29-03:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE
HOP RTT     ADDRESS
1   0.26 ms xx.yy.cc.4
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos segmento servidores en Vlan Gral.

```
Nmap scan report for xx.yy.cc.5
Host is up (0.00044s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE VERSION
53/tcp   open   domain  Nortel Contivity firewall DNS
| dns-nsid:
|_  bind.version: Nominum Vantio 5.4.0.2
113/tcp  closed ident
541/tcp  open   osiris  osiris host IDS agent
8080/tcp open   socks5  (No authentication; connection failed)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION GET
|_http-title: 403 Forbidden: incorrect proxy service was requested
| socks-auth-info:
|_  No authentication
MAC Address: 00:09:0F:03:94:BE (Fortinet)
Device type: firewall
Running: Fortinet embedded
OS details: Fortinet FortiGate-50B or 310B firewall
Uptime guess: 174.701 days (since Thu May 12 02:43:14 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: Device: firewall; CPE: cpe:/h:nortel:contivity

TRACEROUTE
HOP RTT     ADDRESS
1   0.44 ms xx.yy.cc.5
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos segmento servidores en Vlan Gral.

```
Nmap scan report for xx.yy.cc.25
Host is up (0.00080s latency).
Not shown: 976 filtered ports
PORT     STATE  SERVICE            VERSION
25/tcp   open   smtp               Microsoft Exchange smtpd
| smtp-commands: EXCENT03.mrseguridad.com.ar Hello [xx.yy.zz.130], SIZE,
PIPELINING, DSN, ENHANCEDSTATUSCODES, X-ANONYMOUSTLS, AUTH NTLM, X-EXPS
GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, XEXCH50, XRDST,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA
RSET MAIL QUIT HELP AUTH BDAT
53/tcp   open   domain             Microsoft DNS 6.1.7601
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
80/tcp   open   http               Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
88/tcp   open   kerberos-sec       Windows 2003 Kerberos (server time:
2016-11-02 22:28:06Z)
113/tcp  closed ident
135/tcp  open   msrpc              Microsoft Windows RPC
139/tcp  open   netbios-ssn        Microsoft Windows 98 netbios-ssn
389/tcp  open   ldap
443/tcp  open   https?
445/tcp  open   microsoft-ds       (primary domain: mrseguridad)
464/tcp  open   kpasswd5?
587/tcp  open   smtp               Microsoft Exchange smtpd
| smtp-commands: EXCENT03.mrseguridad.com.ar Hello [xx.yy.zz.130], SIZE
10485760, PIPELINING, DSN, ENHANCEDSTATUSCODES, X-ANONYMOUSTLS, AUTH GSSAPI
NTLM, X-EXPS GSSAPI NTLM, 8BITMIME, BINARYMIME, CHUNKING, XEXCH50, XRDST,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA
RSET MAIL QUIT HELP AUTH BDAT
593/tcp  open   ncacn_http         Microsoft Windows RPC over HTTP 1.0
636/tcp  open   ssl/ldap
| ssl-cert: Subject: commonName=EXCENT03.mrseguridad.com.ar
| Issuer: commonName=mrseguridadcordoba-EXCENT04-CA
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-05-21T06:22:15
| Not valid after:  2017-05-21T06:22:15
| MD5:   d741 5f9a db3c a622 6ed4 ebb9 7ff1 bc61
|_SHA-1: 1e31 7d06 bab7 fcfa 8b7b c2f9 236b 4425 0f9e 0bda
|_ssl-date: 2016-11-02T22:31:18+00:00; +7s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
1029/tcp open   msrpc              Microsoft Windows RPC
1031/tcp open   msrpc              Microsoft Windows RPC
1033/tcp open   ncacn_http         Microsoft Windows RPC over HTTP 1.0
1034/tcp open   msrpc              Microsoft Windows RPC
1051/tcp open   msrpc              Microsoft Windows RPC
3268/tcp open   ldap
3269/tcp open   ssl/ldap
| ssl-cert: Subject: commonName=EXCENT03.mrseguridad.com.ar
| Issuer: commonName=mrseguridadcordoba-EXCENT04-CA
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-05-21T06:22:15
| Not valid after:  2017-05-21T06:22:15
| MD5:   d741 5f9a db3c a622 6ed4 ebb9 7ff1 bc61
|_SHA-1: 1e31 7d06 bab7 fcfa 8b7b c2f9 236b 4425 0f9e 0bda
|_ssl-date: 2016-11-02T22:30:37+00:00; +7s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos segmento servidores en Vlan Gral.

```
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
3389/tcp open   ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=EXCENT03.mrseguridad.com.ar
| Issuer: commonName=EXCENT03.mrseguridad.com.ar
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-07-16T20:53:15
| Not valid after:  2017-01-15T20:53:15
| MD5:   8977 757f eee3 2acf 3c55 ab3d 876a 5cd4
|_SHA-1: b570 d9a1 726b 4958 8fc0 7eca f7ed cc60 c97d 4f02
|_ssl-date: 2016-11-02T22:30:38+00:00; +7s from scanner time.
6004/tcp open   ncacn_http         Microsoft Windows RPC over HTTP 1.0
8008/tcp open   http-proxy         Fortinet FortiGuard http proxy
|_hadoop-datanode-info:
|_hadoop-jobtracker-info:
|_hadoop-tasktracker-info:
|_hbase-master-info:
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: Web Filter Block Override
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port445-TCP:V=7.01%I=7%D=11/2%Time=581A6879%P=i586-pc-linux-gnu%r(SMBPr
SF:ogNeg,73,"\0\0\0o\xffSMBr\0\0\0\0\x88\x01@\0\0\0\0\0\0\0\0\0\0\0\0\0@
SF:\x06\0\0\x01\0\x11\x07\0\x0f2\0\x01\0\x04A\0\0\0\0\x01\0\0\0\0\0\xfc\xf
SF:3\x01\0\x85\n\xf0dX5\xd2\x01\xb4\0\x08\*\0h\xe4T!\x80\x84\x067P\0O\0L\0
SF:I\0C\0I\0A\0\0\0E\0X\0C\0E\0N\0T\x000\x003\0\0\0");
MAC Address: 00:21:5E:67:EC:76 (IBM)
Device type: general purpose|firewall|specialized
Running (JUST GUESSING): Microsoft Windows Vista|2012|2008|7 (95%), Fortinet
embedded (87%), AVtech embedded (86%)
OS CPE: cpe:/o:microsoft:windows_vista::sp1:home_premium
cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_server_
2008::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8
Aggressive OS guesses: Microsoft Windows Vista Home Premium SP1 (95%),
Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Vista SP0 or SP1,
Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Vista SP2,
Windows 7 SP1, or Windows Server 2008 (91%), Microsoft Windows Server 2008
or 2008 Beta 3 (89%), Microsoft Windows Server 2012 (89%), Microsoft Windows
7 Professional or Windows 8 (89%), Microsoft Windows Server 2008 SP1 (88%),
Microsoft Windows 7 (88%), Fortinet FortiGate-50B or 310B firewall (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 40.308 days (since Fri Sep 23 12:08:16 2016)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: Hosts: EXCENT03.mrseguridad.com.ar, EXCENT03; OSs: Windows,
Windows 98; Device: firewall; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_server_2003, cpe:/o:microsoft:windows_98

Host script results:
| nbstat: NetBIOS name: EXCENT03, NetBIOS user: <unknown>, NetBIOS MAC:
00:21:5e:67:ec:76 (IBM)
| Names:
|   EXCENT03<00>         Flags: <unique><active>
|   mrseguridad<00>          Flags: <group><active>
|   mrseguridad<1c>          Flags: <group><active>
|_  EXCENT03<20>         Flags: <unique><active>
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows
Server 2008 R2 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: EXCENT03
|   NetBIOS computer name: EXCENT03
|   Domain name: mrseguridad.com.ar
|   Forest name: mrseguridad.com.ar
|   FQDN: EXCENT03.mrseguridad.com.ar
|_  System time: 2016-11-02T19:30:43-03:00
| smb-security-mode:
|   account_used: guest
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos segmento servidores en Vlan Gral.

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.80 ms xx.yy.cc.25

NSE: Script Post-scanning.
Initiating NSE at 19:32
Completed NSE at 19:32, 0.00s elapsed
Initiating NSE at 19:32
Completed NSE at 19:32, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 21 IP addresses (19 hosts up) scanned in 422.50 seconds
           Raw packets sent: 27781 (1.250MB) | Rcvd: 12198 (602.693KB)
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos segmento servidores en Vlan Gral.

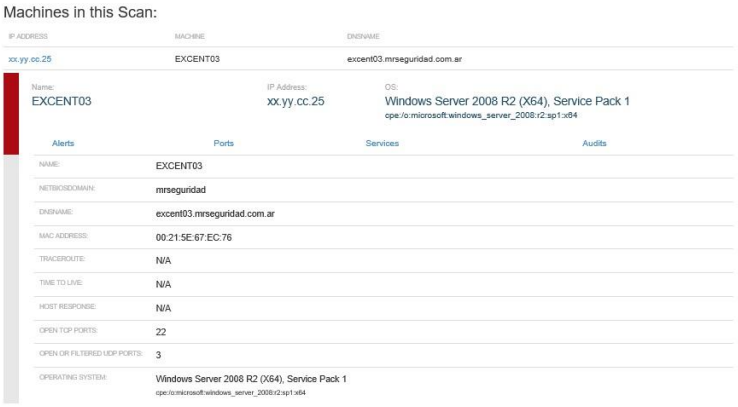


Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Servidor En Vlan Gral.

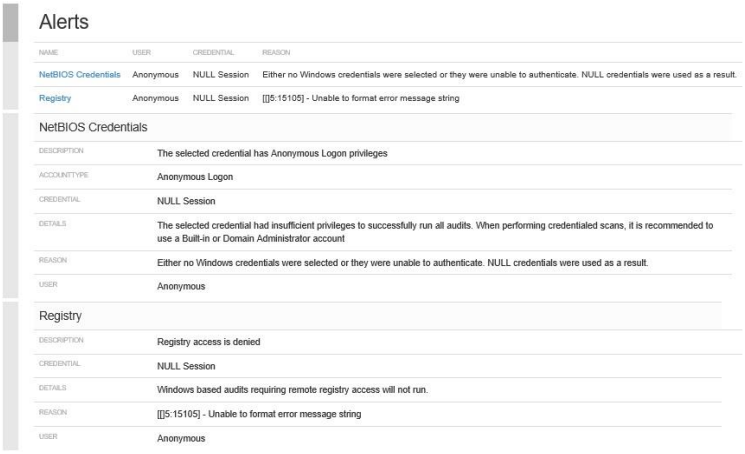


Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Servidor En Vlan Gral.

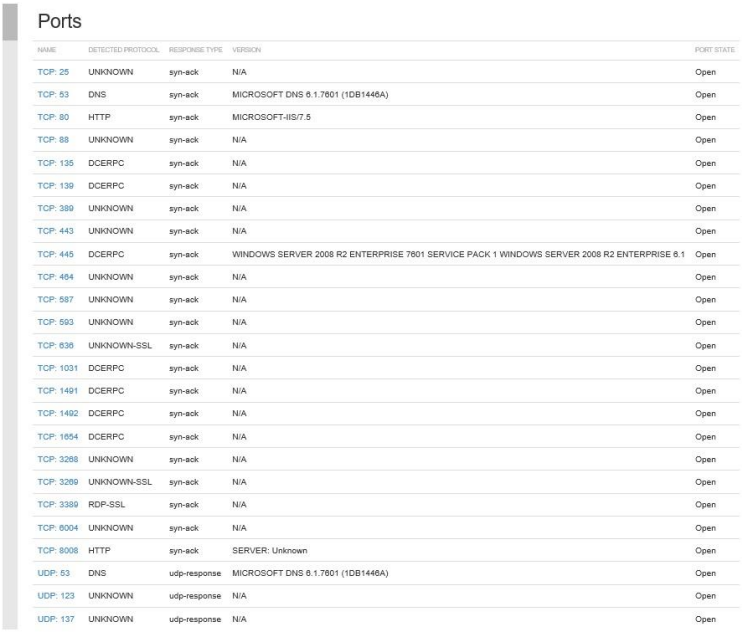
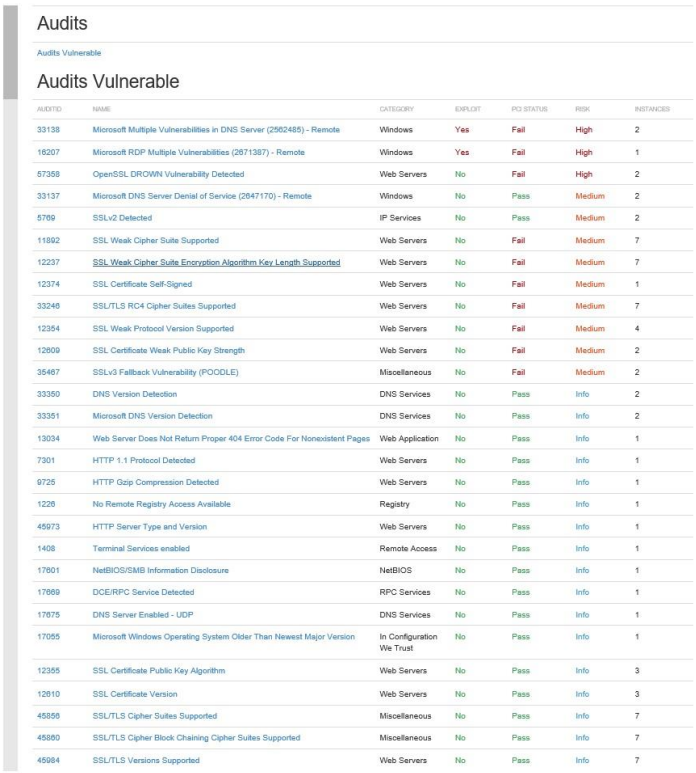


Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Servidor En Vlan Gral.



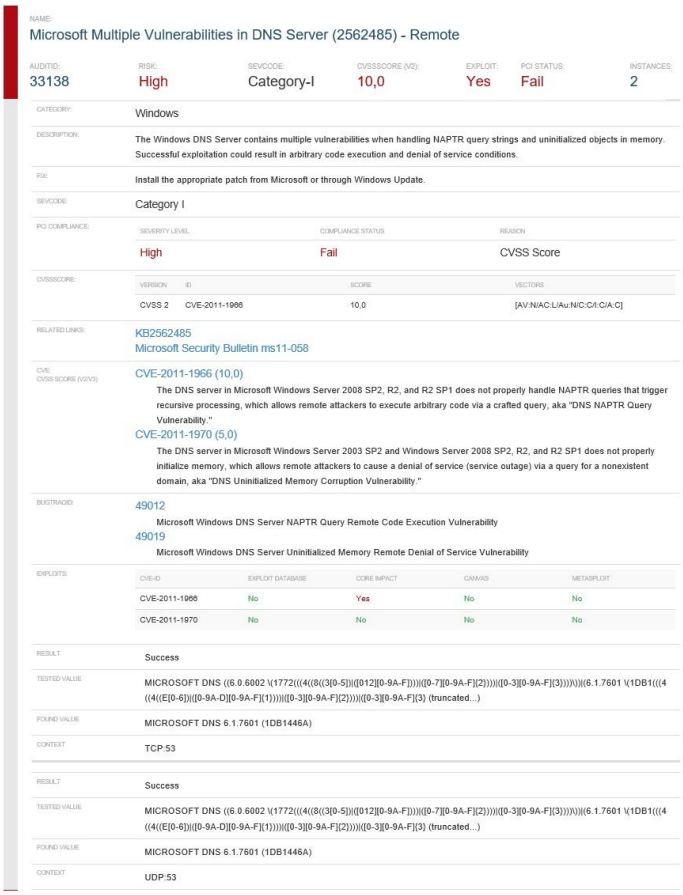
Audits

Audits Vulnerable

Audits Vulnerable

AUDITID	NAME	CATEGORY	EXPLOIT	PCI STATUS	RISK	INSTANCES
33138	Microsoft Multiple Vulnerabilities in DNS Server (2562485) - Remote	Windows	Yes	Fail	High	2
16207	Microsoft RDP Multiple Vulnerabilities (2671387) - Remote	Windows	Yes	Fail	High	1
57358	OpenSSL DROWN Vulnerability Detected	Web Servers	No	Fail	High	2
33137	Microsoft DNS Server Denial of Service (2647170) - Remote	Windows	No	Pass	Medium	2
5769	SSLv2 Detected	IP Services	No	Pass	Medium	2
11802	SSL Weak Cipher Suite Supported	Web Servers	No	Fail	Medium	7
12237	SSL Weak Cipher Suite Encryption Algorithm Key Length Supported	Web Servers	No	Fail	Medium	7
12374	SSL Certificate Self-Signed	Web Servers	No	Fail	Medium	1
33246	SSL/TLS RC4 Cipher Suites Supported	Web Servers	No	Fail	Medium	7
12354	SSL Weak Protocol Version Supported	Web Servers	No	Fail	Medium	4
12809	SSL Certificate Weak Public Key Strength	Web Servers	No	Fail	Medium	2
35467	SSLv3 Fallback Vulnerability (POODLE)	Miscellaneous	No	Fail	Medium	2
33350	DNS Version Detection	DNS Services	No	Pass	Info	2
33351	Microsoft DNS Version Detection	DNS Services	No	Pass	Info	2
13034	Web Server Does Not Return Proper 404 Error Code For Nonexistent Pages	Web Application	No	Pass	Info	1
7301	HTTP 1.1 Protocol Detected	Web Servers	No	Pass	Info	1
9725	HTTP Gzip Compression Detected	Web Servers	No	Pass	Info	1
1226	No Remote Registry Access Available	Registry	No	Pass	Info	1
45973	HTTP Server Type and Version	Web Servers	No	Pass	Info	1
1408	Terminal Services enabled	Remote Access	No	Pass	Info	1
17601	NetBIOS/SMB Information Disclosure	NetBIOS	No	Pass	Info	1
17669	DCE/RPC Service Detected	RPC Services	No	Pass	Info	1
17675	DNS Server Enabled - UDP	DNS Services	No	Pass	Info	1
17055	Microsoft Windows Operating System Older Than Newest Major Version	In Configuration We Trust	No	Pass	Info	1
12355	SSL Certificate Public Key Algorithm	Web Servers	No	Pass	Info	3
12610	SSL Certificate Version	Web Servers	No	Pass	Info	3
45856	SSL/TLS Cipher Suites Supported	Miscellaneous	No	Pass	Info	7
45860	SSL/TLS Cipher Block Chaining Cipher Suites Supported	Miscellaneous	No	Pass	Info	7
45984	SSL/TLS Versions Supported	Web Servers	No	Pass	Info	7

Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades de Servidor En Vlan Gral.



NAME:

Microsoft Multiple Vulnerabilities in DNS Server (2562485) - Remote

AUDITID:	RISK:	SEVCODE:	CVSSSCORE (V2):	EXPLOIT:	PCI STATUS:	INSTANCES:
33138	High	Category-I	10,0	Yes	Fail	2

CATEGORY: Windows

DESCRIPTION: The Windows DNS Server contains multiple vulnerabilities when handling NAPTR query strings and uninitialized objects in memory. Successful exploitation could result in arbitrary code execution and denial of service conditions.

FIX: Install the appropriate patch from Microsoft or through Windows Update.

SEVCODE: Category I

PCI COMPLIANCE:

SEVERITY LEVEL	COMPLIANCE STATUS	REASON
High	Fail	CVSS Score

CVSSSCORE:

VERSION	ID	SCORE	VECTORS
CVSS 2	CVE-2011-1966	10,0	[AV:N/AC:L/Au:N/C:C/I:C/A:C]

RELATED LINKS: KB2562485
Microsoft Security Bulletin ms11-058

CVE: CVSS SCORE (V2/V3):
CVE-2011-1966 (10,0)
The DNS server in Microsoft Windows Server 2008 SP2, R2, and R2 SP1 does not properly handle NAPTR queries that trigger recursive processing, which allows remote attackers to execute arbitrary code via a crafted query, aka "DNS NAPTR Query Vulnerability."
CVE-2011-1970 (5,0)
The DNS server in Microsoft Windows Server 2003 SP2 and Windows Server 2008 SP2, R2, and R2 SP1 does not properly initialize memory, which allows remote attackers to cause a denial of service (service outage) via a query for a nonexistent domain, aka "DNS Uninitialized Memory Corruption Vulnerability."

BUGTRAQID:
49012
Microsoft Windows DNS Server NAPTR Query Remote Code Execution Vulnerability
49019
Microsoft Windows DNS Server Uninitialized Memory Remote Denial of Service Vulnerability

EXPLOITS:

CVE-ID	EXPLOIT DATABASE	CORE IMPACT	CANVAS	METASPLOIT
CVE-2011-1966	No	Yes	No	No
CVE-2011-1970	No	No	No	No

RESULT: Success

TESTED VALUE: MICROSOFT DNS ((6.0.6002 \(1772(((4(((8(((3[0-5])|([012][0-9A-F]))))|([0-7][0-9A-F][2])))))|([0-3][0-9A-F][3]))))))|(6.1.7601 \(1DB1(((4(((4(((E[0-6])|([0-9A-D][0-9A-F][1])))))|([0-3][0-9A-F][2])))))|([0-3][0-9A-F]{3} (truncated...)

FOUND VALUE: MICROSOFT DNS 6.1.7601 (1DB1446A)

CONTEXT: TCP:53

RESULT: Success

TESTED VALUE: MICROSOFT DNS ((6.0.6002 \(1772(((4(((8(((3[0-5])|([012][0-9A-F]))))|([0-7][0-9A-F][2])))))|([0-3][0-9A-F][3]))))))|(6.1.7601 \(1DB1(((4(((4(((E[0-6])|([0-9A-D][0-9A-F][1])))))|([0-3][0-9A-F][2])))))|([0-3][0-9A-F]{3} (truncated...)

FOUND VALUE: MICROSOFT DNS 6.1.7601 (1DB1446A)

CONTEXT: UDP:53

Fig. 14.3. Etapa 6: Rec. de Información, Retina: analizando Vulnerabilidades de servidor en Vlan Gral.

1.4) Acceso a otras Vlans.

Posteriormente se efectuó un escaneo al grupo de direcciones IP de los equipos que pertenecen a una de las Vlans con mayor seguridad de la red, la aplicación entregó la información referida al Nº IP, Dirección MAC y tiempo de respuesta de los equipos que se encuentran conectados a la red (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-02 20:31 ART
Nmap scan report for xx.yy.aa.2
Host is up (0.0012s latency).
Nmap scan report for xx.yy.aa.3
Host is up (0.0012s latency).
Nmap scan report for xx.yy.aa.4
Host is up (0.0018s latency).
Nmap scan report for xx.yy.aa.5
Host is up (0.0017s latency).
Nmap scan report for xx.yy.aa.6
Host is up (0.0013s latency).
Nmap scan report for xx.yy.aa.7
Host is up (0.0015s latency).
Nmap scan report for xx.yy.aa.8
Host is up (0.0015s latency).
Nmap scan report for xx.yy.aa.9
Host is up (0.0042s latency).
Nmap scan report for xx.yy.aa.13
Host is up (0.0029s latency).
Nmap done: 13 IP addresses (9 hosts up) scanned in 14.42 seconds
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Descubriendo Equipos Vlan de seguridad desde Vlan General.

En el siguiente paso, se efectuó un análisis más profundo de los equipos detectados en el paso anterior, la aplicación devolvió la información de Nº IP, Nombre del equipo, Sistema Operativo, puertos abiertos, etc; de los equipos que se encuentran conectados a la red (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-02 20:31 ART
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:31
Completed NSE at 20:31, 0.00s elapsed
Initiating NSE at 20:31
Completed NSE at 20:31, 0.00s elapsed
Initiating Ping Scan at 20:31
Scanning 13 hosts [4 ports/host]
Completed Ping Scan at 20:31, 1.31s elapsed (13 total hosts)
Initiating Parallel DNS resolution of 13 hosts. at 20:31
Completed Parallel DNS resolution of 13 hosts. at 20:31, 13.01s elapsed
Nmap scan report for xx.yy.aa.1 [host down]
Nmap scan report for xx.yy.aa.10 [host down]
Nmap scan report for xx.yy.aa.11 [host down]
Nmap scan report for xx.yy.aa.12 [host down]
Initiating SYN Stealth Scan at 20:31
Scanning 9 hosts [1000 ports/host]
Discovered open port 139/tcp on xx.yy.aa.4
Discovered open port 139/tcp on xx.yy.aa.5
                    .
                    .
Completed SYN Stealth Scan against xx.yy.aa.4 in 25.55s (5 hosts left)
Completed SYN Stealth Scan against xx.yy.aa.5 in 26.56s (3 hosts left)
Completed SYN Stealth Scan at 20:32, 26.87s elapsed (9000 total ports)
Initiating Service scan at 20:32
Scanning 22 services on 9 hosts
Completed Service scan at 20:33, 54.61s elapsed (22 services on 9 hosts)
Initiating OS detection (try #1) against 9 hosts
Retrying OS detection (try #2) against 3 hosts
Retrying OS detection (try #3) against 3 hosts
Retrying OS detection (try #4) against 3 hosts
Retrying OS detection (try #5) against 3 hosts
Initiating Traceroute at 20:33
Completed Traceroute at 20:33, 0.03s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 20:33
Completed Parallel DNS resolution of 9 hosts. at 20:33, 13.01s elapsed
NSE: Script scanning 9 hosts.
Initiating NSE at 20:33
Completed NSE at 20:35, 114.66s elapsed
Initiating NSE at 20:35
Completed NSE at 20:35, 0.02s elapsed
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Vlan de seguridad desde Vlan General.

```
                    .
Nmap scan report for xx.yy.aa.3
Host is up (0.0015s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE      VERSION
139/tcp  open   netbios-ssn  Microsoft Windows 98 netbios-ssn
445/tcp  open   microsoft-ds Microsoft Windows XP microsoft-ds
6129/tcp closed unknown
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows_98,
cpe:/o:microsoft:windows_xp

Host script results:
| nbstat: NetBIOS name: PC44, NetBIOS user: <unknown>, NetBIOS MAC:
6c:f0:49:85:3e:fd (Giga-byte Technology)
| Names:
|   PC44<00>             Flags: <unique><active>
|   mrseguridad<00>          Flags: <group><active>
|   PC44<20>             Flags: <unique><active>
|_  mrseguridad<1e>          Flags: <group><active>
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: PC44
|   NetBIOS computer name: PC44
|   Domain name: mrseguridad.com.ar
|   Forest name: mrseguridad.com.ar
|   FQDN: PC44.mrseguridad.com.ar
|_  System time: 2016-11-02T20:33:24-03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE (using port 6129/tcp)
HOP RTT     ADDRESS
1   1.59 ms xx.yy.aa.3
                    .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Vlan de seguridad desde Vlan General.

```
NSE: Script Post-scanning.
Initiating NSE at 20:35
Completed NSE at 20:35, 0.00s elapsed
Initiating NSE at 20:35
Completed NSE at 20:35, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 13 IP addresses (9 hosts up) scanned in 242.92 seconds
           Raw packets sent: 16858 (766.740KB) | Rcvd: 3389 (148.558KB)
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Vlan de seguridad desde Vlan General.

1.5) Conexión a las redes internas de los locales.

Se intenta evaluar las redes propias de los locales, la cual no devuelve ningún resultado, ya que no está permitido que desde la vlan general se tenga acceso a las redes de los locales, definido en las reglas del firewalls de red.

En primera instancia se evalúa a un local que posee conexión a la red de la empresa con la tecnología MPLS y un equipo ASA 5505 y posteriormente a una red conectada a través de una conexión ADSL y con un equipo PIX 515 (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-10-12 19:20 ART
Nmap done: 35 IP addresses (0 hosts up) scanned in 29.10 seconds
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Descubriendo Equipos Vlan Locales con MPLS desde Vlan General.

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-02 22:00 ART
Nmap done: 24 IP addresses (0 hosts up) scanned in 15.26 seconds
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Descubriendo Equipos Vlan Locales con ADSL desde Vlan General.

2) Prueba Nº 2: equipo conectado en una boca de red aleatoria, con un número de IP Fijo de administración de red.

2.1) Acceso a la red de la empresa.

Al conectar el equipo de Prueba a la red, con la dirección IP, máscara de Red, Puerta de enlace, y servidores DNS, determinada según la documentación recolectada, se observó cómo interactúa el mismo con la red sin producir ningún error de red, ni conflicto con otro equipo (ver figuras de ejemplo siguientes).

```
Configuraci¢n IP de Windows

   Nombre de host. . . . . . . . . : Test01
   Sufijo DNS principal  . . . . . :
   Tipo de nodo. . . . . . . . . . : h¡brido
   Enrutamiento IP habilitado. . . : no
   Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Conexi¢n de  rea local:

   Sufijo DNS espec¡fico para la conexi¢n. . :
   Descripci¢n . . . . . . . . . . . . . . . : Adaptador de escritorio
Intel(R) PRO/1000 MT
   Direcci¢n f¡sica. . . . . . . . . . . . . : 08-00-27-1F-9E-DF
   DHCP habilitado . . . . . . . . . . . . . : no
   Configuraci¢n autom tica habilitada . . . : s¡
   Direcci¢n IPv4. . . . . . . . . . . . . . : xx.yy.cc.58(Preferido)
   M scara de subred . . . . . . . . . . . . : 255.255.252.0
   Puerta de enlace predeterminada . . . . . : xx.yy.cc.1
   Servidores DNS. . . . . . . . . . . . . . : xx.yy.cc.4
                                       xx.yy.cc.25
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

Fig. 14.3. Etapa 6: Rec. de Información, Ipconfig: Conexión Red General con IP Fija.

2.2) Conexión a los equipos del mismo segmento de red.

Luego de que el equipo de prueba se conecta a la red, se efectuó con la aplicación Zenmap un escaneo de direcciones IP y un análisis profundo de los equipos de la red general, obteniendo los mismos resultados que la prueba efectuada con Dirección IP tomada del Servidor DHCP.

2.3) Conexión a los servidores.

Al Igual que en el punto anterior, se obtuvieron los mismos resultados en las distintas pruebas realizadas a los servidores.

2.4) Acceso a otras Vlans.

Posteriormente se realizaron las mismas pruebas a la Vlan de seguridad. Al igual que el punto anterior, se consiguieron los mismos resultados que la prueba efectuada anteriormente, tomando Dirección Ip del Servidor DHCP.

2.5) Conexión a las redes internas de los locales.

Por último se evaluaron las redes propias de los locales, las cuales devolvieron un resultado positivo (anteriormente no se obtuvieron resultados en las pruebas realizadas con IP entregados por el servidor DHCP), debido a que está permitido por las reglas propias del firewalls de red.

En primera instancia se evaluó a un local que posee conexión a la red de la empresa con la tecnología MPLS y un equipo ASA 5505 (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-04 14:47 ART
Nmap scan report for xx.yy.bb.104
Host is up (0.033s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6129/tcp open  unknown

Nmap scan report for xx.yy.bb.106
Host is up (0.028s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6129/tcp open  unknown

Nmap scan report for xx.yy.bb.107
Host is up (0.029s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6129/tcp open  unknown

Nmap done: 11 IP addresses (3 hosts up) scanned in 29.42 seconds
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Descubriendo Equipos Vlan Locales con MPLS desde Vlan General IP Fija.

Al comprobar la conectividad con la red del local, posteriormente, se realizó un análisis más profundo de los equipos detectados en el paso anterior, la aplicación entregó la información con respecto al Nº IP, Nombre del equipo, Sistema Operativo, puertos abiertos, etc; de los equipos que se encuentran conectados a la red del local (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-04 14:48 ART
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:48
Completed NSE at 14:48, 0.00s elapsed
Initiating NSE at 14:48
Completed NSE at 14:48, 0.00s elapsed
Initiating Ping Scan at 14:48
Scanning 11 hosts [4 ports/host]
Completed Ping Scan at 14:48, 0.12s elapsed (11 total hosts)
Initiating Parallel DNS resolution of 11 hosts. at 14:48
Completed Parallel DNS resolution of 11 hosts. at 14:49, 23.84s elapsed
Initiating SYN Stealth Scan at 14:49
Scanning 11 hosts [1000 ports/host]
Discovered open port 445/tcp on xx.yy.bb.106
Discovered open port 445/tcp on xx.yy.bb.107
                    .
                    .
Completed SYN Stealth Scan against xx.yy.bb.106 in 37.63s (2 hosts left)
Completed SYN Stealth Scan against xx.yy.bb.107 in 38.18s (1 host left)
Completed SYN Stealth Scan at 14:50, 40.23s elapsed (11000 total ports)
Initiating Service scan at 14:50
Scanning 7 services on 11 hosts
Completed Service scan at 14:50, 6.09s elapsed (7 services on 11 hosts)
Initiating OS detection (try #1) against 11 hosts
Retrying OS detection (try #2) against 3 hosts
Initiating Traceroute at 14:50
Completed Traceroute at 14:50, 0.05s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 14:50
Completed Parallel DNS resolution of 11 hosts. at 14:50, 25.09s elapsed
NSE: Script scanning 11 hosts.
Initiating NSE at 14:50
Completed NSE at 14:51, 42.88s elapsed
Initiating NSE at 14:51
Completed NSE at 14:51, 0.01s elapsed
Nmap scan report for xx.yy.bb.100
Host is up (0.00052s latency).
All 1000 scanned ports on xx.yy.bb.100 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.39 ms xx.yy.bb.100
                    .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Vlan Locales con MPLS desde Vlan General IP Fija.

```
Nmap scan report for xx.yy.bb.104
Host is up (0.0086s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows 98 netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|2000 (94%)
OS CPE: cpe:/o:microsoft:windows_server_2003::sp1
cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_
2000::sp4:server
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (94%),
Microsoft Windows Server 2003 SP2 (94%), Microsoft Windows Server 2003 R2
SP2 (92%), Microsoft Windows 2000 Server SP4 (90%), Microsoft Windows 2000
SP4 (88%), Microsoft Windows Server 2003 R2 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows_98,
cpe:/o:microsoft:windows_xp

Host script results:
| nbstat: NetBIOS name: PDI1464, NetBIOS user: <unknown>, NetBIOS MAC:
00:11:25:0d:bc:91 (IBM)
| Names:
|   PDI1464<00>          Flags: <unique><active>
|   mrseguridad<00>          Flags: <group><active>
|   PDI1464<20>          Flags: <unique><active>
|   mrseguridad<1e>          Flags: <group><active>
|   mrseguridad<1d>          Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: pdi1464
|   NetBIOS computer name: PDI1464
|   Domain name: mrseguridad.com.ar
|   Forest name: mrseguridad.com.ar
|   FQDN: pdi1464.mrseguridad.com.ar
|_  System time: 2016-11-04T14:50:16-03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   13.37 ms xx.yy.bb.104
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Vlan Locales con MPLS desde Vlan General IP Fija.

```
NSE: Script Post-scanning.
Initiating NSE at 14:51
Completed NSE at 14:51, 0.00s elapsed
Initiating NSE at 14:51
Completed NSE at 14:51, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 11 IP addresses (11 hosts up) scanned in 148.01 seconds
           Raw packets sent: 23570 (1.063MB) | Rcvd: 365 (17.220KB)
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Vlan Locales con MPLS desde Vlan General IP Fija.

Comprobando que existe conexión con dicha Vlan, luego se realizó con la aplicación Retina CS, un análisis de las Vulnerabilidades de algunos de los equipos descubiertos en la red.

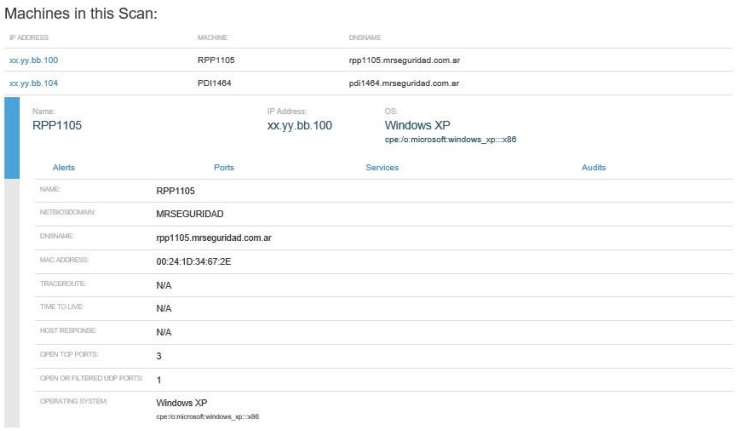


Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades Equipos Vlan Locales con MPLS.

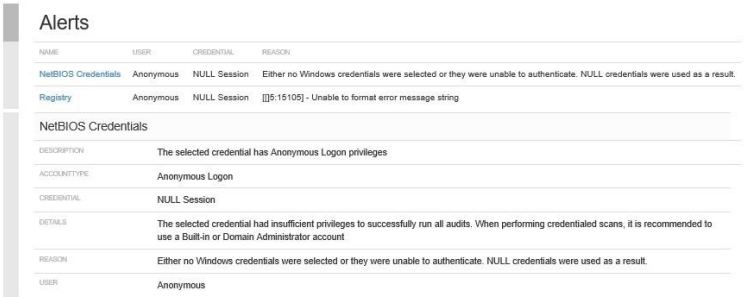


Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades Equipos Vlan Locales con MPLS.

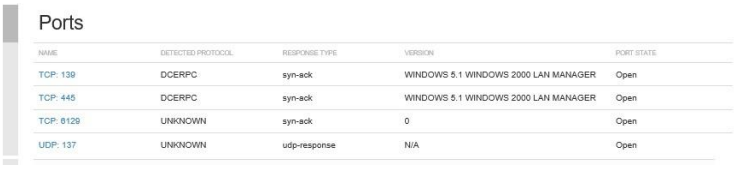


Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades Equipos Vlan Locales con MPLS.

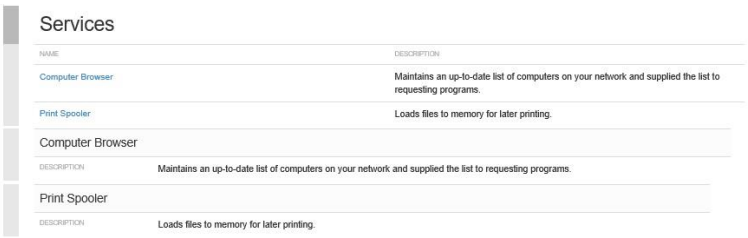
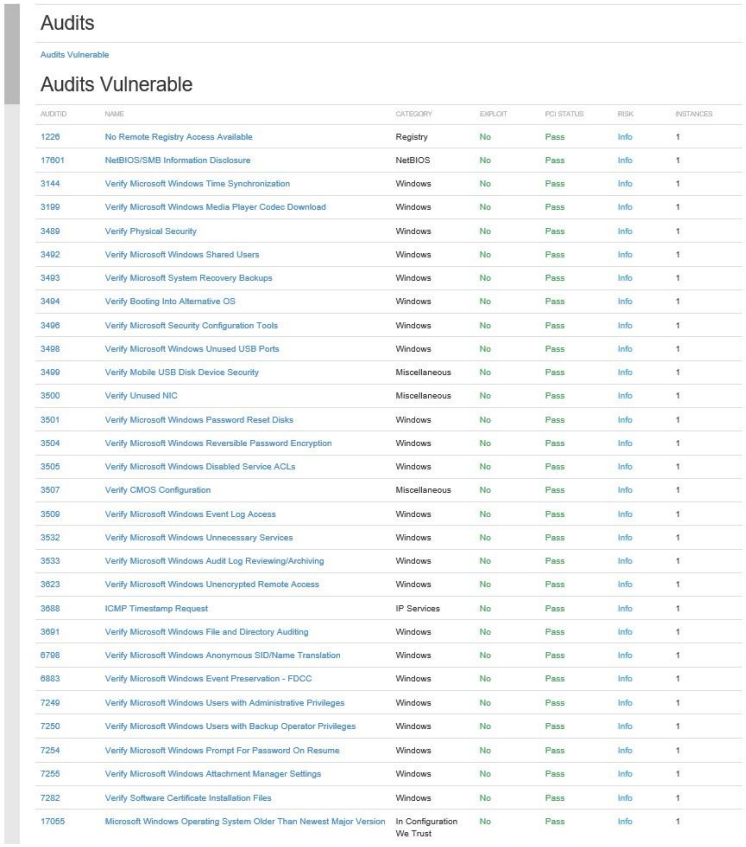


Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades Equipos Vlan Locales con MPLS.



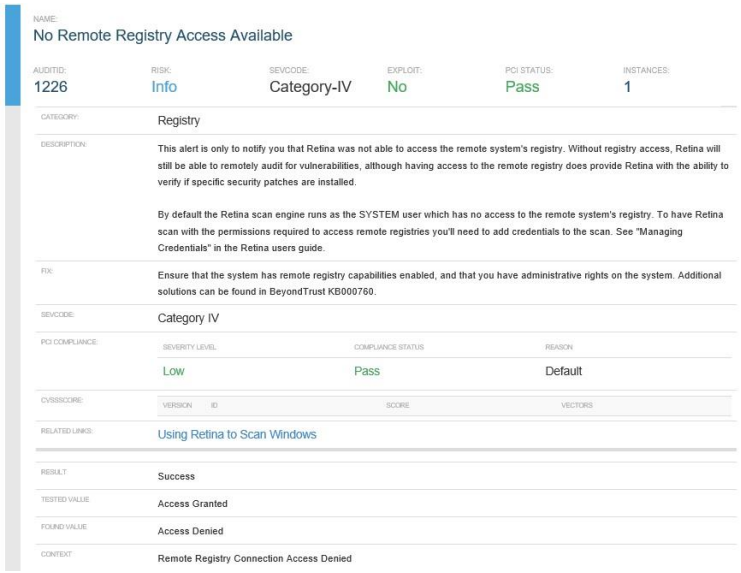
Audits

Audits Vulnerable

Audits Vulnerable

AUDITID	NAME	CATEGORY	EXPLOIT	PCI STATUS	RISK	INSTANCES
1226	No Remote Registry Access Available	Registry	No	Pass	Info	1
17601	NetBIOS/SMB Information Disclosure	NetBIOS	No	Pass	Info	1
3144	Verify Microsoft Windows Time Synchronization	Windows	No	Pass	Info	1
3199	Verify Microsoft Windows Media Player Codec Download	Windows	No	Pass	Info	1
3489	Verify Physical Security	Windows	No	Pass	Info	1
3492	Verify Microsoft Windows Shared Users	Windows	No	Pass	Info	1
3493	Verify Microsoft System Recovery Backups	Windows	No	Pass	Info	1
3494	Verify Booting Into Alternative OS	Windows	No	Pass	Info	1
3496	Verify Microsoft Security Configuration Tools	Windows	No	Pass	Info	1
3498	Verify Microsoft Windows Unused USB Ports	Windows	No	Pass	Info	1
3499	Verify Mobile USB Disk Device Security	Miscellaneous	No	Pass	Info	1
3500	Verify Unused NIC	Miscellaneous	No	Pass	Info	1
3501	Verify Microsoft Windows Password Reset Disks	Windows	No	Pass	Info	1
3504	Verify Microsoft Windows Reversible Password Encryption	Windows	No	Pass	Info	1
3505	Verify Microsoft Windows Disabled Service ACLs	Windows	No	Pass	Info	1
3507	Verify CMOS Configuration	Miscellaneous	No	Pass	Info	1
3509	Verify Microsoft Windows Event Log Access	Windows	No	Pass	Info	1
3532	Verify Microsoft Windows Unnecessary Services	Windows	No	Pass	Info	1
3533	Verify Microsoft Windows Audit Log Reviewing/Archiving	Windows	No	Pass	Info	1
3823	Verify Microsoft Windows Unencrypted Remote Access	Windows	No	Pass	Info	1
3888	ICMP Timestamp Request	IP Services	No	Pass	Info	1
3891	Verify Microsoft Windows File and Directory Auditing	Windows	No	Pass	Info	1
6798	Verify Microsoft Windows Anonymous SID/Name Translation	Windows	No	Pass	Info	1
6883	Verify Microsoft Windows Event Preservation - FDCC	Windows	No	Pass	Info	1
7249	Verify Microsoft Windows Users with Administrative Privileges	Windows	No	Pass	Info	1
7250	Verify Microsoft Windows Users with Backup Operator Privileges	Windows	No	Pass	Info	1
7254	Verify Microsoft Windows Prompt For Password On Resume	Windows	No	Pass	Info	1
7256	Verify Microsoft Windows Attachment Manager Settings	Windows	No	Pass	Info	1
7282	Verify Software Certificate Installation Files	Windows	No	Pass	Info	1
17055	Microsoft Windows Operating System Older Than Newest Major Version	In Configuration We Trust	No	Pass	Info	1

Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades Equipos Vlan Locales con MPLS.



NAME:
No Remote Registry Access Available

AUDITID:	RISK:	SEVCODE:	EXPLOIT:	PCI STATUS:	INSTANCES:
1226	Info	Category-IV	No	Pass	1

CATEGORY: Registry

DESCRIPTION: This alert is only to notify you that Retina was not able to access the remote system's registry. Without registry access, Retina will still be able to remotely audit for vulnerabilities, although having access to the remote registry does provide Retina with the ability to verify if specific security patches are installed.

By default the Retina scan engine runs as the SYSTEM user which has no access to the remote system's registry. To have Retina scan with the permissions required to access remote registries you'll need to add credentials to the scan. See "Managing Credentials" in the Retina users guide.

FIX: Ensure that the system has remote registry capabilities enabled, and that you have administrative rights on the system. Additional solutions can be found in BeyondTrust KB000760.

SEVCODE: Category IV

PCI COMPLIANCE:

SEVERITY LEVEL	COMPLIANCE STATUS	REASON
Low	Pass	Default

CVSSSCORE:

VERSION	ID	SCORE	VECTORS

RELATED LINKS: Using Retina to Scan Windows

RESULT: Success

TESTED VALUE: Access Granted

FOUND VALUE: Access Denied

CONTEXT: Remote Registry Connection Access Denied

Fig. 14.3. Etapa 6: Rec. de Información, Retina: Analizando Vulnerabilidades Equipos Vlan Locales con MPLS.

En la actividad siguiente, se comprueba la conexión con la aplicación Zenmap a una red de un local conectado a través de una conexión ADSL y con un equipo PIX 515 (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-04 14:59 ART
Nmap scan report for xx.yy.dd.198
Host is up (0.052s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6129/tcp open  unknown

Nmap scan report for xx.yy.dd.199
Host is up (0.053s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6129/tcp open  unknown

Nmap scan report for xx.yy.dd.202
Host is up (0.053s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6129/tcp open  unknown

Nmap done: 24 IP addresses (3 hosts up) scanned in 43.68 seconds
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Descubriendo Equipos Vlan Locales con ADSL desde Vlan General IP Fija.

Al comprobar la conectividad con la red del local, se realizó un análisis más profundo de los equipos detectados en el paso anterior, la aplicación devolvió la información de Nº IP, Nombre del equipo, Sistema Operativo, puertos abiertos, etc; de los equipos que se encuentran conectados a la red del local (ver figuras de ejemplo siguientes).

```
Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-04 14:55 ART
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:55
Completed NSE at 14:55, 0.00s elapsed
Initiating NSE at 14:55
Completed NSE at 14:55, 0.00s elapsed
Initiating Ping Scan at 14:55
Scanning 24 hosts [4 ports/host]
Completed Ping Scan at 14:55, 1.62s elapsed (24 total hosts)
Initiating Parallel DNS resolution of 24 hosts. at 14:55
Completed Parallel DNS resolution of 24 hosts. at 14:56, 38.34s elapsed
Initiating SYN Stealth Scan at 14:56
Scanning 24 hosts [1000 ports/host]
Discovered open port 139/tcp on xx.yy.dd.198
Discovered open port 139/tcp on xx.yy.dd.199
                    .
                    .
Completed SYN Stealth Scan against xx.yy.dd.199 in 24.34s (23 hosts left)
Completed SYN Stealth Scan against xx.yy.dd.212 in 25.55s (1 host left)
Discovered open port 6129/tcp on xx.yy.dd.198
Completed SYN Stealth Scan at 14:57, 35.04s elapsed (24000 total ports)
Initiating Service scan at 14:57
Scanning 7 services on 24 hosts
Completed Service scan at 14:57, 6.24s elapsed (7 services on 24 hosts)
Initiating OS detection (try #1) against 24 hosts
Retrying OS detection (try #2) against 5 hosts
WARNING: OS didn't match until try #2
WARNING: OS didn't match until try #2
Initiating Traceroute at 14:57
Completed Traceroute at 14:57, 0.11s elapsed
Initiating Parallel DNS resolution of 24 hosts. at 14:57
Completed Parallel DNS resolution of 24 hosts. at 14:57, 36.79s elapsed
NSE: Script scanning 24 hosts.
Initiating NSE at 14:57
Completed NSE at 14:58, 43.63s elapsed
Initiating NSE at 14:58
Completed NSE at 14:58, 0.01s elapsed
                    .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Vlan Locales con ADSL desde Vlan General IP Fija.

```
                    .
Nmap scan report for xx.yy.dd.199
Host is up (0.019s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows 98 netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|2000 (94%)
OS CPE: cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_
2000::sp4:server
Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (94%), Microsoft
Windows Server 2003 SP1 or SP2 (93%), Microsoft Windows Server 2003 R2 SP2
(92%), Microsoft Windows 2000 Server SP4 (90%), Microsoft Windows 2000 SP4
(88%), Microsoft Windows Server 2003 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=253 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows 98, Windows XP; CPE: cpe:/o:microsoft:windows_98,
cpe:/o:microsoft:windows_xp

Host script results:
| nbstat: NetBIOS name: PDI1007, NetBIOS user: <unknown>, NetBIOS MAC:
00:25:22:a8:0b:dd (ASRock Incorporation)
| Names:
|   PDI1007<00>          Flags: <unique><active>
|   PDI1007<20>          Flags: <unique><active>
|   mrseguridad<00>          Flags: <group><active>
|_  mrseguridad<1e>          Flags: <group><active>
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: pdi1007
|   NetBIOS computer name: PDI1007
|   Domain name: mrseguridad.com.ar
|   Forest name: mrseguridad.com.ar
|   FQDN: pdi1007.mrseguridad.com.ar
|_  System time: 2016-11-04T14:57:35-03:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.91 ms xx.yy.dd.199
                    .
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Vlan Locales con ADSL desde Vlan General IP Fija.

```
                    .
NSE: Script Post-scanning.
Initiating NSE at 14:58
Completed NSE at 14:58, 0.00s elapsed
Initiating NSE at 14:58
Completed NSE at 14:58, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 24 IP addresses (24 hosts up) scanned in 171.40 seconds
           Raw packets sent: 49173 (2.221MB) | Rcvd: 666 (29.172KB)
```

Fig. 14.3. Etapa 6: Rec. de Información, Zenmap: Analizando Equipos Vlan Locales con ADSL desde Vlan General IP Fija.

ETAPA 7: ANÁLISIS DE LA INFORMACIÓN OBTENIDA DEL MUESTREO DE LA RED

En las distintas pruebas realizadas a la red de la empresa, se logró recabar abundante información de la misma y de los equipos que la componen, ya que los parámetros de seguridad para las conexiones de red internas de la empresa son muy permeables, esto nos permitió, con pruebas sencillas, obtener información de las de Direcciones IP, Máscaras de Red, Descubrir equipos conectados, obtener información de los mismos, etc. A continuación se detalla la información obtenida en cada uno de los puntos de las pruebas.

1) Prueba Nº 1: equipo conectado a una boca de red aleatoria, tomando número de IP del servidor DHCP

En la Prueba Nº 1 se logró recabar abundante información de la red correspondiente a la Vlan General, ya que al conectar el equipo "test1", el servidor DHCP le otorga los parámetros propios de red, identificándose el mismo, sin solicitar ningún tipo de seguridad extra.

Además se determinó, gracias a la documentación recolectada y a la primera conexión del equipo de test, el rango de números IP en el cual se encuentran los equipos servidores y posteriormente, con la aplicación Zenmap, se obtuvieron también la marca de los equipos, los números IP y los puertos abiertos. A continuación se detalla el análisis producido en cada uno de los puntos de la primera prueba.

1.1) Acceso a la red de la empresa.

Al conectar el equipo "test1" a la red, el servidor de DHCP le entrega los siguientes parámetros de red: Número IP: "xx.yy.zz.35", sufijo DNS: "mrseguridad.com.ar", máscara de red: "255.255.252.0", Gateway de red: "xx.yy.cc.1", Servidores DNS: "xx.yy.cc.4, xx.yy.cc.25" y Wins "xx.yy.cc.4".

Con todos estos datos, es posible deducir que tipo de red se encuentra implementada en la empresa, cuales son los principales servidores y también se logra deducir, cual es uno de los segmentos de red que la componen.

1.2) Conexión a los equipos del mismo segmento de red.

Luego de realizado un escaneo con la aplicación Zenmap de un rango de 30 direcciones IP del mismo segmento del equipo de Test, se detectaron 24 equipos

conectados, de los cuales se determinó la dirección IP, dirección MAC, hardware de red, velocidad de conexión de 0.30 ms (el mínimo) y 0.96 ms (el máximo).

Posteriormente, con el análisis más profundo de la aplicación Zenmap, se determinó que:

- Microsoft Windows 7 es el sistema Operativo que poseen la mayoría de los equipos, se encuentra instalado en 21 puestos, el resto poseen Windows XP y Windows 10.
- La mayoría de los equipos (23) están unidos al dominio de la red de la empresa.
- 10 de los equipos escaneados, tiene abierto el puerto de administración remota de Windows, el puerto TCP 3389.
- En 23 de los equipos se encuentran abiertos los puertos TCP 135, 139 y 445. Además se encontraron abiertos en varios equipos los puertos TCP 6129 en 4 equipos, 5357 en 3 equipos y el 49175 en 3 equipos.
- El rango de la velocidad de respuesta de los equipos fue entre 0.48 ms (el mínimo) y 1.75 ms (el máximo).
- El análisis se llevó a cabo en un lapso de 325.30 segundos.

En el análisis de vulnerabilidades con la aplicación Retina CS de dos equipos seleccionados aleatoriamente, se determinó que:

- Los dos equipos tienen instalado el sistema operativo Microsoft Windows 7 SP1.
- Ambos equipos poseen NetBios activado.
- Se descubrió que ambos equipos tienen abiertos los puertos TCP 135, 139, 445, 3389 y el puerto UDP 137.
- La aplicación detectó que ambos equipos tienen una falla de seguridad en la aplicación de “escritorio remoto de Windows” catalogada como “Microsoft RDP Multiple Vulnerabilities (2671387) – Remote”, la cual se encuentra valuada como grave en la CVSS Score (sistema común de puntaje de vulnerabilidades).
- Las siguientes cuatro vulnerabilidades encontradas en los dos equipos tienen que ver con los algoritmos de cifrado de comunicaciones de la aplicación de “escritorio remoto de Windows”, ya que tiene configurado permitir algoritmos

de cifrado obsoletos, además que poseen un cifrado con menos de 128 bits de largo de la llave. También se detectó que los equipos poseen certificados que no son validados por una entidad de confianza (son auto firmados), estas vulnerabilidades están catalogadas con un riesgo medio según la CVSS Score.

- Luego detalla información adicional sobre otros puertos abiertos como el puerto UDP 137 que responde a peticiones de SMB, al igual que el puerto TCP 135 que corresponde al servicio de RPC (llamada a procedimientos remotos), ya que puede otorgar una conexión al equipo analizado.
- El análisis de los dos equipos se llevó a cabo en un lapso de 6,30 minutos.

1.3) Conexión a los servidores.

Luego de realizado el escaneo de direcciones IP con la aplicación Zenmap de un rango de 25 direcciones IP del segmento de red de los servidores, se detectaron 19 equipos conectados, de los cuales se determinó la dirección IP, dirección MAC, hardware de red.

La velocidad de conexión con los equipos fueron como mínimo de 0,19 ms y máximo de 0,52 ms.

En el escaneo se observó la gran variedad de productos entre ellos 5 servidores IBM, 3 Intel, 3 productos CISCO, 3 Micro-Star International, 2 Fortinet y dos VMware.

Posteriormente, con el análisis más profundo de la aplicación Zenmap, se determinó que:

- Microsoft Windows 2003 es el sistema Operativo que poseen la mayoría de los equipos, el mismo fue detectado en 9 servidores, el resto de los equipos poseen Windows 2008 (4 servidores), Cisco IOS (3 equipos), FortiGate-50B (2 equipos).
- Están unidos al dominio de la empresa 14 equipos.
- 13 de los equipos escaneados posee abierto el puerto de administración remota de Windows (puerto 3389).
- También se encontraron abiertos los puertos TCP 80 en 12 servidores, los puertos TCP 135, el 139 y el 445 en 14 servidores. También se detectaron puertos alternativos de servicios Web como el TCP 8081,8082, etc. Además se encontraron abiertos en varios equipos los puertos TCP 1433 en el cual se corren servicios de MSQL.

- En los equipos CISCO se encontraron abiertos los puertos TCP 22, el 23(en un solo equipo) y el 80, todos corresponden a administración remota.
- El rango de la velocidad de respuesta de los equipos fue el mínimo 0.26 ms y el máximo 1.4 ms.
- El análisis de los servidores se completó en un lapso de 422.50 segundos.

En el análisis de vulnerabilidades con la aplicación Retina CS del Servidor de Dominio de la empresa, se determinó que:

- El servidor tiene instalado el sistema operativo Microsoft Windows 2008 R2 SP1.
- El servidor posee la resolución de nombre de NetBios activado.
- Se descubrió que ambos equipos tienen abiertos los puertos TCP 25 (servicio de transferencia de correo), 53 (Resolución de nombres de dominio), 80 ("http" Servicio de información de Internet), 88 (Servicio de Kerberos), 135 (llamada a procedimiento remoto), 139 (llamada a procedimiento remoto), 389 (Protocolo ligero de acceso a directorios), 443 ("https" Servicio de información de Internet con capa de seguridad), 445 (llamada a procedimiento remoto), 3389, entre otros y los puertos UDP 53(Resolución de nombres de dominio), 123 (protocolo de servicio de tiempo) y 137 (servicio de nombres de Netbios).
- La aplicación detectó que el servidor posee tres fallas de seguridad graves en las aplicaciones de "DNS Server", "escritorio remoto de Windows" y en "Open SSL" catalogada como "Microsoft RDP Multiple Vulnerabilities (2671387) – Remote", las cuales se encuentran valuadas como graves en el CVSS Score (sistema común de puntaje de vulnerabilidades).
- Las siguientes nueve vulnerabilidades encontradas en el servidor, la primera tiene que ver con "Denegación de servicio en Microsoft DNS Server" y las siguientes tienen que ver con los algoritmos de cifrado de comunicaciones del servicio IP y de los servicios web, ya que tiene configurado permitir algoritmos de cifrado que ya son obsoletos, además que posee un cifrado con menos de 128 bits de largo de la llave. También se detectó que el certificado no es validado por una entidad de confianza (son auto firmados), estas vulnerabilidades están catalogadas con un riesgo medio según la CVSS Score.

- Luego, el análisis, detalla información adicional sobre 18 posibles vulnerabilidades como la detección de la versión del servidor DNS y del servidor HTTP, etc.
- El análisis de los dos equipos se llevó a cabo en un lapso de 6,19 minutos.

1.4) Acceso a otras Vlans.

Luego de realizado un escaneo con la aplicación Zenmap de un rango de 13 direcciones IP de la Vlan de red de mayor seguridad, se detectaron 9 equipos conectados, de los que se determinó la dirección IP y velocidad de conexión.

La velocidad de conexión con los equipos fueron como mínimo de 1,2 ms y máximo de 4,2 ms.

Posteriormente, en el análisis más profundo de la aplicación Zenmap, se determinó que:

- Microsoft Windows XP es el sistema Operativo que poseen la mayoría de los equipos, sumando un total de 5 equipos, de los cuales 4 están unidos al dominio de la empresa y un equipo con el sistema operativo Microsoft Windows 7.
- Se detectaron 3 equipos de telefonía IP con un sistema operativo "i586-pc-linux-gnu".
- En la mayoría de los equipos (6) se encuentran abiertos los puertos 139 y 445. Además se encontró abierto en un equipo el puerto TCP 135.
- En los Teléfonos IP analizados se encontraron abiertos los puertos TCP 12345, 443 y el 80, los dos últimos correspondes a la administración remota por Web.
- El análisis se llevó a cabo en un lapso de 242.92 segundos.

No se realizó un análisis con la aplicación Retina CS, ya que no se consideró necesaria debido a que los equipos instalados son similares a los que se encuentran en la Vlan General.

1.5) Conexión a las redes internas de los locales.

Al intentar evaluar las redes propias de los locales, no se obtuvo ningún resultado, ya que no está permitido, en las reglas de acceso de los firewall, que desde la Vlan general se tenga acceso a las redes de los locales.

2) Prueba Nº 2: equipo conectado en una boca de red aleatoria, con un número de IP Fijo de administración de red.

2.1) Acceso a la red de la empresa.

Se conectó el equipo de Prueba a la red con la dirección IP, máscara de Red, Puerta de enlace, y servidores DNS, determinada según la documentación recolectada, no se produce ninguna información aparte de la relevada de la documentación.

2.2) Conexión a los equipos del mismo segmento de red.

Se obtiene la misma información que en la prueba con un número de IP obtenido del DHCP.

2.3) Conexión a los servidores.

Al Igual que en el punto anterior, se obtuvieron los mismos resultados en las distintas pruebas realizadas a los servidores.

2.4) Acceso a otras Vlans.

Posteriormente se realizan las mismas pruebas a la Vlan de seguridad. Al igual que el punto anterior, se reproducen los mismos resultados que la prueba tomando Dirección Ip del Servidor DHCP.

2.5) Conexión a las redes internas de los locales.

Por último se intentó evaluar las redes propias de los locales, las cuales entregaron un resultado positivo, debido a que está permitido, en las reglas del firewalls de red, que accedan los equipos con un número de IP de administración.

En primera instancia se evaluó a un local que posee conexión a la red de la empresa con la tecnología MPLS y un equipo ASA 5505 (ver figuras de ejemplo siguientes).

Luego de realizado un escaneo con la aplicación Zenmap (en este caso se hizo uso del comando –PO, debido a que el firewall del local respondía el mismo cuando se escaneaba la red con el comando –sn), se detectaron 3 equipos conectados, de los cuales se

determinó la dirección IP y velocidad de conexión, siendo el equipo más rápido en responder en 28 ms y el más lento de 33 ms.

Posteriormente, con el análisis más profundo de la aplicación Zenmap, se determinó que:

- Los 3 equipos encendidos tienen el Sistema Operativo Microsoft Windows Xp.
- Estos equipos están unidos al dominio de la red de la empresa.
- Los equipos escaneados tienen abierto los puertos TCP 139 (Netbios) y 445 (Active Directory).
- Un equipo también tiene abierto el puerto TCP 6129 (Dameware, software de conexión remota)
- El análisis se llevó a cabo en un lapso de 148.01 segundos.

En el análisis de vulnerabilidades con la aplicación Retina CS de dos equipos seleccionados aleatoriamente, se determinó que:

- Los dos equipos tienen instalado el sistema operativo Microsoft Windows XP.
- Ambos equipos poseen NetBios activado.
- Se descubrió que ambos equipos tienen abiertos los puertos TCP 139, 445 y el puerto UDP 137.
- La aplicación no detectó fallas de seguridad según la CVSS Score.
- Se detalla información adicional sobre otros puertos abiertos como el puerto UDP 137 ya que responde a peticiones de SMB.
- También se detalla información extra de con respecto a la configuración propia del sistema operativo analizado, como la configuración de la sincronización de la hora, la desactivación de puertos USB, la actualización de distintos codecs, el funcionamiento de servicios no usados, etc.
- El análisis de los dos equipos se llevó a cabo en un lapso de 5,45 minutos.

En la actividad siguiente, se comprueba la conexión con la aplicación Zenmap a una red de un local conectado a través de una conexión ADSL y con un equipo PIX 515.

Luego de realizado un escaneo con la aplicación Zenmap (en este caso se hizo uso del comando –PO, debido a que el firewall del local respondía el mismo cuando se escaneaba la red con el comando –sn), se detectaron 3 equipos conectados, de los cuales se

determinó la dirección IP y velocidad de conexión, siendo el equipo más rápido en responder en 52 ms y el más lento 53 ms.

Posteriormente, en el análisis más profundo de la aplicación Zenmap, se determinó que:

- Los 3 equipos encendidos tienen el Sistema Operativo Microsoft Windows Xp.
- Estos equipos están unidos al dominio de la red de la empresa.
- Los equipos escaneados tienen abierto los puertos TCP 139 (Netbios) y 445 (Active Directory).
- Un equipo también tiene abierto el puerto TCP 6129 (Dameware, software de conexión remota)
- El análisis se llevó a cabo en un lapso de 171.40 segundos.

3) Resultados Generales

3.1) Equipo conectado en una boca de Red aleatoria, tomando número de IP del servidor DHCP.

- Se logró acceder a la red general, de la cual se obtuvo gran cantidad de información y de los equipos que la componen.
- Se logró realizar conexión con los equipos servidores y equipos en red general, a los cuales se los escaneo con la aplicación Zenmap y Retina CS.
- Se logró tener acceso a otras Vlans de seguridad, esto producto de una configuración reciente, y que provocó que la Vlan de seguridad sea visible desde la Vlan General, la cual fue escaneada con la aplicación Zenmap.
- No se realizó una conexión a las redes internas de los locales, dada la configuración en las reglas de acceso de los equipos PIX 515 y ASA5505.

3.2) Equipo conectado en una boca de Red aleatoria, con un Número de IP Fijo de administración.

- Se logró acceder a la red general.
- Se realizó una conexión a los servidores y equipos en general.
- Se logró tener acceso a otras Vlans.
- Se realizó una conexión a las redes internas de los locales, ya que está permitido el acceso con un número de IP de administración.

4) Tabla de Resumen de los Resultados Generales

	Nuestreo de la Red - Cant. Equipos	Equipos activos descubiertos	Velocidad promedio de Conexión	Equipos en Dominio	Análisis Puertos		Análisis S.O.		Análisis Vuln.	
					Puerto	Cantidad	S.O.	Cantidad	Riesgo	Cantidad
Red General	30	24	0,6 ms	23	135,139,445	23	Win. 7	21	Grave	2
					3389	10	Win. Xp	1	Medio	8
					6129	4	Win. 10	1	Bajo	2
					Otros	9	Otros	1	Informativa	21
Red Servidores	25	19	0,35 ms	14	135,139,445	14	Win. 2003	9	Grave	5
					3389	13	Win. 2008	4	Medio	34
					80	12	Cisco IOS	3	Bajo	0
					Otros	127	Otros	3	Informativa	41
Vlan de Seguridad	13	9	2,7 ms	4	139,445	6	Win. Xp	5	NA	NA
					80,443,12345	3	i586 linux	3	NA	NA
					135	1	Win. 7	1	NA	NA
					Otros	0	Otros	0	NA	NA
Vlan Local ASA 5505	11	3	30 ms	3	139,445	3	Win. Xp	3	Grave	0
					6129	3			Medio	0
									Bajo	0
					Otros		Otros		Informativa	60
Vlan Local PIX 515	20	3	53 ms	3	139,445	3	Win. Xp	3	NA	NA
					6129	1			NA	NA
									NA	NA
					Otros		Otros		NA	NA

Tabla 14.3. Etapa 7: Análisis de la Información, Cuadro Resumen de Resultados Generales.

ETAPA 8: FOMULACIÓN Y COMPROBACIÓN DE LA HIPÓTESIS

1) Formulación de la hipótesis

Teniendo en cuenta la situación crítica y los problemas planteados por la empresa en el anteproyecto, los cuales están referidos a su red de datos, tales como: interrupciones del servicio o lentitud en la misma, cuellos de botella e intrusiones. Es que se planteó la hipótesis que estos problemas pueden ocurrir por malas configuraciones de los equipos, utilización de equipos obsoletos o con mal funcionamiento, problemas en el cableado de la red de datos, falta de documentación de la misma y de la configuración de los equipos que la componen, además los recursos humanos no cuentan con una capacitación adecuada para la administración de la red y de los equipos.

2) Prueba de la Hipótesis

Dada la hipótesis se planteó como objetivo general relevar y analizar los elementos de la red de datos, su interconexión, características y funcionalidades, para evaluar y determinar su adecuada utilización en función de las necesidades de calidad de servicio y seguridad de la empresa.

Para el cumplimiento del objetivo general se plantearon objetivos específicos, de los cuales son tres los que serán utilizados para la evaluación y comprobación de la hipótesis planteada:

2.1) Identificar los equipos que componen la red de la empresa y los medios que se utilizan para su interconexión.

Para lo cual se realizó un relevamiento de los equipos que componen la red, de la documentación que tiene disponible la empresa y se llevó a cabo una observación de la disposición del cableado de red.

2.2) Evaluar el desempeño individual y colectivo de los elementos identificados, utilizando distintas herramientas de prueba de red GNU y gratuitas.

En este punto, fue necesario conectar un equipo de red con las herramientas de prueba ya instaladas, Zenmap y Retina CS, las cuales fueron seleccionadas previamente dadas sus características deseadas. Una vez conectado el equipo a la red de la empresa, se evaluó el desempeño individual de los equipos, tomando en cuenta distintas pruebas planteadas.

2.3) Determinar el rendimiento y capacidad actual de toda la red, posibles cuellos de botella, puntos de falla y amenazas de seguridad.

Ya con el equipo de prueba conectado a la red y utilizando la herramienta Zenmap, se evaluó el desempeño de la red.

3) Comprobación de la hipótesis

3.1) <u>Identificar los equipos que componen la red de la empresa y los medios que se utilizan para su interconexión.</u>

Al contrastar los datos obtenidos de los documentos relevados otorgados por la empresa, con los del relevamiento realizado en este trabajo, podemos concluir que los documentos no poseen información completa ni actualizada de la infraestructura de la red y de los equipos que la componen.

Las diferencias halladas se detallan a continuación:

- En los documentos "Diagrama de topología de la Red" y "Planilla de las conexiones de bocas de red" se describe la topología de la red de la empresa hasta el año 2013. La información que nos otorgan es correcta para los cableados de red y disposición de los equipos que ya existían en esa fecha. Para los equipos más nuevos, como las cámaras de seguridad, no se encontraron descriptos en el documento, al igual que el cableado de red que fue necesario instalar para la conexión de dichos equipos a la red.
- En el documento "Descripción de los racks y servidores" que describe los equipos que se encuentran instalados en los racks de la sala de servidores, tales como servidores, switch, firewalls, etc. El documento está actualizado hasta el año 2014. La descripción que hace de los mismos es correcta con respecto a la cantidad de racks en la sala, pero al observar los equipos que en ellos se encuentran instalados, se hallan algunas diferencias con respecto a los nombres de los servidores por ser más nuevos, al igual que no se encuentran varios equipos que fueron reemplazados por distintas razones.
- Además, surgió del relevamiento, que varios de los equipos de conectividad y de la red, ya se encuentran fuera del tiempo de vida útil determinada por los fabricantes, esto significa que no poseen soporte técnico, de hardware y tampoco se continúa con un ciclo de actualización de su firmware. Los equipos son los switch Cisco WS-C2950-12, WS-c2950SX-24 y los firewall Fortigate

200A. Esto supone un riesgo en la seguridad de la red, ya que los fabricantes no corrigen más posibles errores en el software de los equipos que podrían surgir.

3.2) Evaluar el desempeño individual y colectivo de los elementos identificados utilizando distintas herramientas de prueba de red GNU y gratuitas.

La evaluación de los distintos elementos de la red se llevó a cabo con las herramientas Zenmap y Retina CS, con las mismas, se logró obtener abundante información con respecto al funcionamiento de la red y se logró realizar un análisis de los equipos que la componen.

Las observaciones realizadas durante la evaluación se describen a continuación:

- Está permitido la conexión de cualquier equipo a la red y sin antes realizar una comprobación del mismo. Este punto en sí, puede generar grandes inconvenientes mientras existan bocas de red que se encuentren accesibles al personal no autorizado.
- Habiendo concretado el punto anterior, se evaluó la red interna con las herramientas seleccionas. En primera instancia fueron escaneados y evaluados el funcionamiento de los equipos que componen la Vlan General. Como resultado se obtuvo todo la información disponible de los servidores y demás equipos de la red, como el nombre del equipo, la dirección de red y de MAC, el sistema operativo que tiene instalado y vulnerabilidades y alertas del mismo, puertos abiertos, carpetas compartidas, etc. Dado que se obtuvo demasiada información y con un equipo que no pertenece a la empresa, supone un grave problema en lo que respecta a los controles de seguridad que deberían estar presentes.
- En segunda instancia fueron escaneados y evaluados el funcionamiento de los equipos que componen la Vlan de mayor seguridad, en la misma existen equipos que contienen información sensible de la empresa. Y al igual que en el punto anterior se obtuvo toda la información disponible de los equipos que en ella se encuentran. Lo que supone un mayor problema en lo que respecta a los controles de seguridad que deberían estar presentes, ya que a la misma no se debería poder acceder si no es de una Vlan de mayor nivel de seguridad.

3.3) Determinar el rendimiento y capacidad actual de toda la red, posibles cuellos de botella, puntos de falla y amenazas de seguridad.

A través de las pruebas realizadas anteriormente con la aplicación Zenmap, fue posible reunir los valores de velocidad de la red y de las conexiones existentes con los locales, las observaciones se describen a continuación:

- Cuando se realizaron las pruebas a la Vlan de mayor seguridad, nos llamó la atención la velocidad de conexión de la misma, de 2.7 ms, la que fue bastante menor que la velocidad de conexión con la Vlan General 0.6 ms. Al comprobar los equipos que conectan dicha Vlan, se encuentra el switch SW1PISO, el cual suponemos que puede encontrase colapsado su funcionamiento o el cable de red troncal que llega a él.
- En una prueba posterior se intentó realizar una conexión a las redes de dos locales; solo se logró acceder y probar ambas redes cuando se coloca al equipo de prueba un número de IP de Administración. Como resultado se observaron tiempos mucho mayores de la velocidad de conexión, siendo la de la red con ADSL y un PIX 515 de 53 ms. Con esta velocidad en la conexión podría llegar a generarse un cuello de botella en la conexión de dicho local.

ETAPA 9: CONCLUSIONES Y RECOMENDACIONES

1) Conclusiones

Ver Punto 22. Conclusiones en la página 120.

2) Recomendaciones

Mantener un programa de capacitación constante a los técnicos encargados de la red de datos, administración de los servidores y puestos de trabajo. Con una buena capacitación de los recursos humanos además de garantizarse la empresa el funcionamiento más eficiente de los sistemas, también genera en el empleado una más motivación mayor con el trabajo.

Actualización de la documentación de la infraestructura de la red y de los equipos, generando también manuales de procedimientos ante fallas, este último garantizaría la resolución más rápida de algunos inconvenientes.

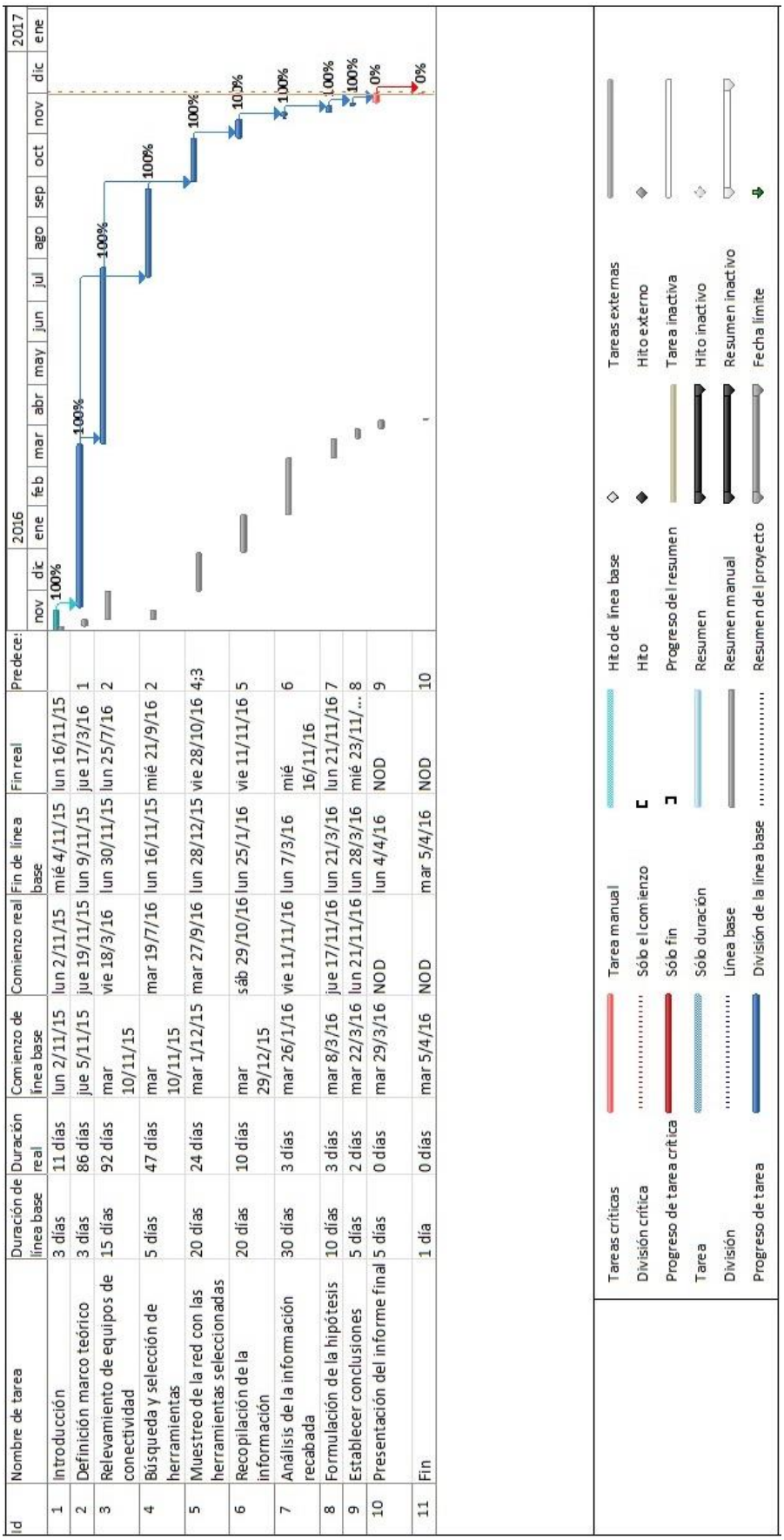
Reemplazar en el corto plazo todos los equipos que se encuentran obsoletos e implementar un calendario que tenga en cuenta el ciclo de vida útil de los distintos equipos.

Elaborar un calendario de mantenimiento de rutina periódico de los equipos de red, servidores y equipos de escritorio, así disminuirán las interrupciones en el sistema, asegurando una mayor disponibilidad de la información. Este punto deberá incluir las actualizaciones del Software de base, con lo cual los sistemas serán más seguros sin la existencia de las actuales vulnerabilidades.

Llevar a cabo un control de los puertos que se encuentran abiertos en los equipos, evaluando la real necesidad de los mismos, también realizar un control periódico de la red, para detectar distintas anomalías que podrían estar ocurriendo. El control puede llevarse a cabo con las herramientas utilizadas en este proyecto, ya que fueron muy eficientes a tal fin.

Llevar a cabo un chequeo de la configuración de los switchs para corregir distintos errores observados y además, desactivar todos los puertos que no sean utilizados, con lo que se impediría que se conecten equipos en las bocas de red que se encuentren libres. También llevar a cabo un control de direcciones MAC que se conecten a los puertos, para impedir que distintos números de MAC utilicen un mismo puerto del switch, impidiendo la conexión de otros switchs en un puerto que no haya sido aprobado previamente.

3) Cronograma Real Vs. Previsto



Id	Nombre de tarea	Duración de línea base	Duración real	Comienzo de línea base	Comienzo real	Fin de línea base	Fin real	Predece:
1	Introducción	3 días	11 días	lun 2/11/15	lun 2/11/15	mié 4/11/15	lun 16/11/15	
2	Definición marco teórico	3 días	86 días	jue 5/11/15	jue 19/11/15	lun 9/11/15	jue 17/3/16	1
3	Relevamiento de equipos de conectividad	15 días	92 días	mar 10/11/15	vie 18/3/16	lun 30/11/15	lun 25/7/16	2
4	Búsqueda y selección de herramientas	5 días	47 días	mar 10/11/15	mar 19/7/16	lun 16/11/15	mié 21/9/16	2
5	Muestreo de la red con las herramientas seleccionadas	20 días	24 días	mar 1/12/15	mar 27/9/16	lun 28/12/15	vie 28/10/16	4;3
6	Recopilación de la información	20 días	10 días	mar 29/12/15	sáb 29/10/16	lun 25/1/16	vie 11/11/16	5
7	Análisis de la información recabada	30 días	3 días	mar 26/1/16	vie 11/11/16	lun 7/3/16	mié 16/11/16	6
8	Formulación de la hipótesis	10 días	3 días	mar 8/3/16	jue 17/11/16	lun 21/3/16	lun 21/11/16	7
9	Establecer conclusiones	5 días	2 días	mar 22/3/16	lun 21/11/16	lun 28/3/16	mié 23/11/...	8
10	Presentación del informe final	5 días	0 días	mar 29/3/16	NOD	lun 4/4/16	NOD	9
11	Fin	1 día	0 días	mar 5/4/16	NOD	mar 5/4/16	NOD	10

ETAPA 10: INFORME DE LA AUDITORÍA

1) Identificación del Informe

Auditoría de la red de datos.

2) Identificación del Cliente

La red de datos.

3) Identificación de la Entidad Auditada

MR Seguridad S.A.

4) Objetivos

Relevar y analizar los elementos de la red de datos, su interconexión, características y funcionalidades, para evaluar y determinar su adecuada utilización en función de las necesidades de calidad de servicio y seguridad de la empresa.

5) Hallazgos Potenciales

- Información desactualizada o faltante de los equipos, de los procedimientos y de la infraestructura de la red.
- Controles de la red inexistentes.
- Equipos de conectividad fuera del tiempo de vida útil delimitado por el fabricante.
- Equipos conectados a la red con escaso control de los puertos que poseen abiertos y con software desactualizado, los cuales presentan muchas vulnerabilidades en la red de datos.
- Configuraciones defectuosas en los equipos de conectividad.

6) Alcance de la Auditoría

La auditoría comprende el período del año 2016 y se ha realizado en toda la red de datos de la empresa, bajo la norma ISO 27002.

El proyecto se limitará al relevamiento y análisis de la red de datos en la casa matriz, en tres sucursales de la Ciudad de Córdoba y en tres sucursales del interior provincial, lo que podrá según cuestiones propias del proyecto variar. Esto tendrá en cuenta los elementos de hardware y software que proveen la conectividad, hasta los elementos de hardware de red y su configuración en los servidores y PCs.

El trabajo no alcanzará a los elementos de software en los servidores y puestos de trabajo ni la seguridad en los mismos.

7) Debilidades Específicas Detectadas

- Los documentos "Diagrama de topología de la Red", "Planilla de las conexiones de bocas de red" y "Descripción de los racks y servidores" se encuentran desactualizados y por lo tanto la información que poseen no es congruente con el estado actual de la empresa.
- Los equipos switch Cisco WS-C2950-12, WS-c2950SX-24 y los firewall Fortigate 200A, se encuentran fuera de su tiempo de vida útil.
- Está permitido la conexión de cualquier equipo a la red y sin antes realizar una comprobación del mismo, permitiendo que se puedan realizar conexiones por parte de personal no autorizado.
- La información de los servidores y demás equipos de la red, se encuentra disponible sin ninguna restricción, permitiendo que un equipo no autorizado realice fingerprint de los equipos de la red (Ver tabla 1).
- No hay separación de las Vlan General con la Vlan de mayor seguridad, la cual contiene información sensible de la empresa.
- En la Vlan de mayor seguridad se midió una latencia en la red de 2.7 ms, el switch SW1PISO puede encontrase colapsado su funcionamiento o el cable de red troncal que llega a él (Ver tabla 1).
- Latencia en la red del local con ADSL y un PIX 515 de 53 ms. Podría llegar a generarse un cuello de botella en la conexión de dicho local (Ver tabla 1).

	Nuestreo de la Red - Cant. Equipos	Equipos activos descubiertos	Velocidad promedio de Conexión	Equipos en Dominio	Análisis Puertos		Análisis S.O.		Análisis Vuln.	
					Puerto	Cantidad	S.O.	Cantidad	Riesgo	Cantidad
Red General	30	24	0,6 ms	23	135,139,445	23	Win. 7	21	Grave	2
					3389	10	Win. Xp	1	Medio	8
					6129	4	Win. 10	1	Bajo	2
					Otros	9	Otros	1	Informativa	21
Red Servidores	25	19	0,35 ms	14	135,139,445	14	Win. 2003	9	Grave	5
					3389	13	Win. 2008	4	Medio	34
					80	12	Cisco IOS	3	Bajo	0
					Otros	127	Otros	3	Informativa	41
Vlan de Seguridad	13	9	2,7 ms	4	139,445	6	Win. Xp	5	NA	NA
					80,443,12345	3	i586 linux	3	NA	NA
					135	1	Win. 7	1	NA	NA
					Otros	0	Otros	0	NA	NA
Vlan Local ASA 5505	11	3	30 ms	3	139,445	3	Win. Xp	3	Grave	0
					6129	3			Medio	0
									Bajo	0
					Otros		Otros		Informativa	60
Vlan Local PIX 515	20	3	53 ms	3	139,445	3	Win. Xp	3	NA	NA
					6129	1			NA	NA
									NA	NA
					Otros		Otros		NA	NA

Tabla. 1. Cuadro Resumen de Resultados Generales.

8) Conclusiones del informe de Auditoría

Como resultado de las evaluaciones realizadas se puede informar que se ha cumplido con la evaluación de los objetivos indicados anteriormente.

- Se obtuvieron deficiencias con respecto al cumplimiento de las normas de seguridad; no se presentan los controles adecuados con respecto a los equipos de conectividad, servidores y puestos de trabajo.
- No existe documentación actualizada de los equipos e infraestructura, tampoco se encontraron manuales de procedimiento ante fallas, ni tampoco sobre mantenimiento preventivo de sus equipos de conectividad, PCs y servidores.
- Se detectaron equipos fuera del tiempo de vida útil determinado por el fabricante.
- Se detectaron fallas en la configuración de los switchs, ya que no hay separación entre Vlans, y en la configuración de los puertos.
- Se descubrieron puertos abiertos en los servidores y equipos de escritorio, además que se encontraron muchas vulnerabilidades de los sistemas operativos que tienen instalados.
- Se detectó una latencia de red superior en la Vlan de mayor seguridad y en la conexión a la red de local con conexión ADSL y PIX 515.
- No hay personal técnico debidamente capacitado.

9) Recomendaciones del informe de Auditoría

- Mantener un programa de capacitación constante a los técnicos encargados de la red de datos, administración de los servidores y puestos de trabajo.
- Actualizar la documentación de la infraestructura de la red y de los equipos, generando también manuales de procedimientos ante fallas.
- Reemplazar en el corto plazo todos los equipos que se encuentran obsoletos e implementar un calendario de renovación que tenga en cuenta el ciclo de vida útil de los distintos equipos.
- Elaborar un calendario de mantenimiento de rutina periódico de los equipos de red, servidores y equipos de escritorio, deberá incluir las actualizaciones del Software de base, con lo cual los sistemas serán más seguros sin la existencia de las actuales vulnerabilidades.
- Realizar un control y corrección de la configuración de los switchs, para solventar los problemas encontrados.

- Llevar a cabo un control periódico de los puertos que se encuentran abiertos en los equipos. Este control puede llevarse a cabo con las herramientas utilizadas en el presente trabajo.

10) Fecha de Informe

Diciembre del 2016.

14.4. CONTROL DE COSTOS:

No Incide.

14.5. DIFICULTADES QUE SE HAN PRESENTADO

En el transcurso del desarrollo del proyecto fueron varias las dificultades que han ido surgiendo, la primera de ellas estuvo relacionada a la dificultad de conseguir información de la competencia de la empresa y del posicionamiento que ocupa en el mercado, esto ocurrió debido a que el gremio (CESEC - Cámara de Empresas de Seguridad Electrónica del Centro) quien aglomera dicho mercado, esta enemistado con la policía y no quería brindar información de ninguna índole de sus integrantes, por lo que fue necesario, en primera instancia solicitar una constancia de alumno regular en el Instituto Universitario Aeronáutico, presentarla en el gremio, y luego solicitar audiencia con el presidente de dicha institución, quien nos brindó solo información informal, y nos indicó obtener la misma de internet.

Otro inconveniente ocurrió cuando estábamos terminando de desarrollar el Marco Teórico y por comenzar el relevamiento de la empresa, los directivos de la empresa por distintos motivos y prioridades solicitaron postergar el proyecto, lo que en total fueron aproximadamente siete meses, lo cual nos ocasiono una gran demora en distintas etapas del proyecto.

14.6. RESULTADOS ALCANZADOS

No Incide.

15. INVERSIÓN REQUERIDA

No Incide.

16. PROYECCIÓN DE COSTOS DE OPERACIÓN Y MANTENIMIENTO

Siguiendo con las recomendaciones declaradas en el informe entregado a la dirección, se plantean los siguientes costos, para la optimización de los recursos Humanos y materiales, los cuales detallan a continuación:

- Restructuración de cableado de Cámaras: este punto obedece a que el cableado únicamente no estaba prolijo y según normas, es por esto que no se plantea volver a realizar el cableado y solo acomodar y etiquetar los mismos.

- Reconfiguración de las Vlans: esta configuración es de suma importancia, ya que se detectó una irregularidad en la cual se podían ingresar a la Vlan de mayor seguridad sin tener un permiso extra, por lo cual debería ser implementada en el corto plazo, contratando un Administrador de Red de Cisco.
- Actualización de Sistemas Operativos: Los sistemas operativos que corren sobre servidores y Equipos de escritorio deberán ser actualizados, ya que se presentaron varias vulnerabilidades de los mismos por falta de actualización.
- Capacitación del Personal: En el presente proyecto se detectó la falta de capacitación existente, es por esto que se plantea en primer término una capación técnica en sistemas operativos y redes, con la instrumentación de las aplicaciones utilizadas en el proyecto para escaneo de la red. Posteriormente, en función de los requerimientos de la dirección, se planteara la profundización y especialización de la misma, teniendo en cuenta el manejo de los servidores, firewall y switch, ya que estas se realizan en periodos de tiempo mucho más largos (CCNA 4 semestres).
- Revisión de puertos y servicios activos: una que se completaron los puntos anteriores, se realizara junto al personal de la empresa una nueva revisión de la red, para certificar las mejoras realizadas.
- Compra de equipos Fortinet 300C: se recomienda esta compra, debido a que el equipo utilizado actualmente, el equipo fortinet 200A, se encuentra obsoleto.
- Compra Switch Cisco 2960 de 48 puertos: Al igual que el punto anterior, se recomienda comprar dos de estos equipos para remplazar los Switch Cisco 2950, los cuales se encuentran obsoletos.

Costos	Unidades	Valor Unitario Aproximado ($)	Valor Total Aproximado ($)
Restructuración de cableado	10 h	150	1500
Evaluación y Reconfiguración de Vlans	10 h	700	7000
Actualización Sistemas Operativos	25 h	370	9250
Capacitación del personal	20 h	300	6000
Revisión de puertos y servicios activos	7 h	370	2590
Compra de equipos Fortinet 300C	2	80000	160000
Compra de equipos 2960 48 puertos	2	35000	70000
TOTAL:			256340

17. ANÁLISIS DE VIABILIDAD COMERCIAL

No Incide.

18. ANÁLISIS FINANCIERO

No Incide.

19. ESTUDIO AMBIENTAL

No Incide.

20. ESTUDIO SOCIAL

No Incide.

21. EVALUACIÓN ECONÓMICA

No Incide.

22. CONCLUSIONES

Como resultado del trabajo los objetivos planteados al inicio fueron alcanzados, tanto el objetivo general como los objetivos específicos.

Para cumplir con:

1) *Identificar los equipos que componen la red de la empresa y los medios que se utilizan para su interconexión.*

Fue necesario realizar una observación directa en la casa matriz y una recopilación de los documentos disponibles de la infraestructura de red, dándonos un panorama del estado actual de la infraestructura de la red de la empresa.

En ese momento nos encontramos con diversos problemas, tales como la falta de información y formación que tienen los empleados con respecto a los equipos y su manejo, ya que muchos de los inconvenientes se refieren a malas configuraciones de los mismos, como por ejemplo, las configuraciones de la Vlans en los switchs, o por desconocimiento de las normas de seguridad vigentes, como por ejemplo las actualizaciones del software de base de los equipos, para corregir distintas vulnerabilidades.

Esta falta de información queda también a la vista al momento de relevar la documentación disponible de la red de datos de la empresa, debido a que se encontraron faltantes de documentación, principalmente las que deberían estar referidas a la configuración de los equipos de conectividad, de los Servidores y puestos de trabajo, siguiendo normas específicas de seguridad. Los documentos que existían están desactualizados, debido a que no reflejan el estado actual de los equipos de conectividad y la infraestructura de la red de datos.

2) *Evaluar el desempeño individual y colectivo de los elementos identificados utilizando distintas herramientas de prueba de red GNU y gratuitas.*

Se realizó un relevamiento y una prueba de la red con las cuales se concluyó que varios de los equipos de conectividad y de la red, ya se encuentran fuera del tiempo de vida útil determinada por los fabricantes. Los equipos son los switch Cisco WS-C2950-12, WS-c2950SX-24 y los firewall Fortigate 200A. Esto supone un riesgo en la seguridad de la red, ya que los fabricantes no corrigen más posibles errores en el software de los equipos que podrían surgir.

Al realizar las pruebas de red, se observó un posible problema de seguridad puesto que al conectar un equipo nuevo a la red, este obtuvo todos los datos de conectividad

necesarios y posteriormente obtuvo los datos de los equipos conectados a dicha red. Esto sucedió debido a la falta de controles de seguridad.

Posteriormente, otro inconveniente encontrado, fue que al escanear la red, se detectaron de los equipos conectados a la misma, muchos puertos abiertos, como por ejemplo el TCP 3389, el cual corresponde al escritorio remoto. Esto no es un problema en si en una red LAN con equipos de un dominio de confianza, pero sí lo sería, si el equipo que se está conectando no pertenece a ella.

En esta prueba también se encontró un problema de la configuración de las Vlan en los switchs, ya que se logró acceder desde la Vlan General con un número de IP otorgado por el servidor DHCP a la Vlan de mayor seguridad, lo que supone un mayor problema en lo que respecta a los controles de seguridad que deberían estar presentes.

Posteriormente se detectaron vulnerabilidades en los distintos sistemas operativos que tienen instalados los equipos en la empresa, como por ejemplo algunos equipos con el Sistema Operativo Microsoft Windows 7 tienen una falla de seguridad en la aplicación de "escritorio remoto de Windows", la cual se encuentra valuada como grave en la CVSS Score (sistema común de puntaje de vulnerabilidades).

3) Determinar el rendimiento y capacidad actual de toda la red, posibles cuellos de botella, puntos de falla y amenazas de seguridad.

Se realizaron distintas pruebas en la red, donde se detectó que la latencia de la conexión de la Vlan del local, la cual tiene implementada una conexión ADSL y un PIX 515, resultó con una diferencia elevada con respecto al resto de las pruebas. También se encontraron valores altos de latencia de red en la Vlan de mayor seguridad, la cual suponemos que puede deberse a que el switch SWP1 puede encontrase colapsado su funcionamiento o el cable de red troncal que llega a él. Además de las distintas amenazas de seguridad descriptas anteriormente.

4) Generar informes a la dirección que contengan los datos obtenidos y las recomendaciones para un funcionamiento óptimo y seguro de la red a mediano plazo.

Se elaboró un informe a la dirección detallando los distintos elementos de la red encontrados, el funcionamiento general de los mismos, la capacidad del funcionamiento en conjunto y los distintas recomendaciones para corregir las los problemas encontrados y fallas de seguridad.

5) Seleccionar herramientas de seguridad para ser utilizadas junto con los mecanismos de control implementados.

Se llevó a cabo un muestreo de las herramientas disponibles en internet, seleccionándolas según su funcionalidad, costo, tipo de licencia de uso, posibilidad de implementación en distintos sistemas operativos, etc.

Las herramientas seleccionadas pueden ser utilizas periódicamente facilitando los controles planteados en las recomendaciones.

Cabe agregar que la dirección de la empresa y sus empleados quedaron sumamente conformes con la auditoría y la documentación generada, ya que les permite conocer de manera clara y precisa como está conformada la estructura de la red, los equipos que la componen, incluyendo su estado y desempeño.

23. REFERENCIAS Y BIBLIOGRAFÍA

1) "Redes de Computadoras" de Adrew S. Tanenbaum. Editorial Pearson Educación. 2003.
2) "Redes de Computadoras, Internet e Interredes" de Douglas E. Comer. Editorial Prentice-Hall Hispanoamericana S.A. 1998.
3) Familia del Estándar de Seguridad Informática de la norma "IRAM-ISO IEC 27000".
4) Manuales y bibliografía del curso "Enterprise Security and Risk", dictado en el Colegio Taborín.
5) Manuales y bibliografía del curso de "Cisco CCNA", dictado en el Colegio Taborín.
6) Papers:
    - "Network Security : Attacks and Defence". Kartikey Agarwal*, Dr. Sanjay Kumar Dubey. Amity University, Noida, Uttar Pradesh, India. 2014.
    - "Network Security Issues and Solutions". Mrs. Bhumika S. Zalavadia. HOD-Diploma Computer Department Atmiya Institute of Technology and Science for Diploma Studies Rajkot, Gujrat. 2014.
    - "Modeling of Risk Factors in Determining Network Security Level". Martin Suhartana, Bens Pardamean and Benfano Soewito Universitas Bina Nusantara, Jakarta, Indonesia. 2014.
    - "Network Security: it's time to take it seriously". Deepak Gahlot, Abhimanyu Thakur, Akshat Pokhriyal, Divyanshu Kukreti Students, Dronacharya College of Engineering Gurgaon, India. 2014.
    - "Network Security: Penetration Tools for Network Security". Daniel Klasson, Kim Klasson, Anatoly Iourtchenko. School of Information Science, Computer and Electrical Engineering. Halmstad University Sweden. 2014.
    - "Auditoría de Redes" Patrick Hernández Cuamatzi. Universidad Autónoma de Tlaxcala. 2013.
    - "Analysis of Packet Filtering Technology in Computer Network Security". Miss. Rupali P. Hinglaspure1, Prof. B. R. Burghate. Department of

Computer Science and Engineering, Sant Gadge Baba Amravati University, India. 2014

- "UTM Technology: As a Solution for Network Security Systems". Mr Manish Kumar, O.P. Suthar. Jodhpur Institute of Engg. and Technology, Jodhur, Rajastahn. India. 2014.
- "Analysis of Firewall Technology Incomputer Network Security". Miss. Shwetambari G. Pundkar, Prof. Dr. G. R. Bamnote. Department of Computer Science and Engineering, Sant Gadge Baba Amravati University, India. 2014.

7) "Security Analysis of a Computer Network" Master's Thesis. Jan Vykopal. Masaryk University Faculty Of Informatics. Brno, 2008.
8) "Addressing practical challenges for anomaly detection in backbone networks" Ph Thesis Ignasi Paredes-Oliva en la universidad politécnica de Barcelona.
9) "Network Security Issues, Tools for Testing Security in Computer Network and Development Solution for Improving Security in Computer Network". Master's Thesis in Computer Network Engineering. Amir Reza Fazely Hamedani, Sherin Skaria School of Information Science, Computer and Electrical Engineering. Halmstad University. Halmstad, Sweden. February 2010.
10) Manuales y bibliografía del curso virtual de "Redes Informáticas", dictado por la Universidad de Washington.
11) "Paradigmas y Enfoques de la Investigación Científica" tomado del texto "Conocer y decidir". Federico Reyes Heroles.
12) "Métodos y técnicas de la investigación científica" de Guillermo Morone.
13) "El Proceso de Investigación" Carlos Sabino.

24. ANEXOS

24.1. ANEXO 1: OBJETIVOS Y POLITICAS GENERALES

El objetivo principal de la empresa es satisfacer la necesidad de seguridad de los distintos clientes, esto lo realiza de distintas formas, ya sea con personal propio de vigilancia destacado en el lugar que se requiere o disposición de distintos elementos como cámaras, alarmas, vallados, etc.

La empresa basa principalmente la prestación de los servicios de seguridad de las siguientes formas:

- *Vigilancia Privada:* Tiene como eje el personal altamente capacitado en la empresa, que son asignados a cubrir distintos requerimientos pactados con los clientes para la custodia de personas y bienes materiales.

  Una vez que cubren su objetivo, el vigilante informa por teléfono o radio frecuencia de su estado y posición. Y durante la jornada, va informando de cualquier hecho relevante a su supervisor.
- *Monitoreo de Alarmas y Cámaras:* Este es otro servicio que realiza la empresa, el cual se destaca gracias a la alta eficacia que tiene para prevenir y contrarrestar incidentes de seguridad.

  A esta actividad la realizan personal en la empresa o los vigiladores desde su objetivo, y se informa a los supervisores de cualquier hecho que sea relevante.

  En la sucursal, estos eventos se cargan en un sistema propio, el cual lleva el registro de los mismos, a la vez que se deja constancia de su seguimiento y resolución.

  Según la característica del evento se procede a informar a la policía local, para su presencia en el domicilio afectado.
- *Monitoreo y extinción de incendios:* Este es un servicio adicional que presta la empresa y en general se contrata junto con el servicio de alarmas.

24.2. ANEXO 2: RESEÑA HISTORICA

"MR Seguridad S.A." fue fundada en 1990 en Córdoba con el objetivo de prestar Servicios de seguridad al sector privado.

Actualmente, y con 25 años de trayectoria y crecimiento sostenido, es una empresa líder y reconocida a nivel provincial.

La empresa presta servicios en la Ciudad de Córdoba, teniendo su casa matriz en el centro de Córdoba y sucursales en los barrios Alta Córdoba, Nueva Córdoba, Cerro de las Rosas, Gral. Paz. Además posee locales en Río Cuarto, Villa María, San Francisco, Carlos Paz, Jesús María y Villa Dolores.

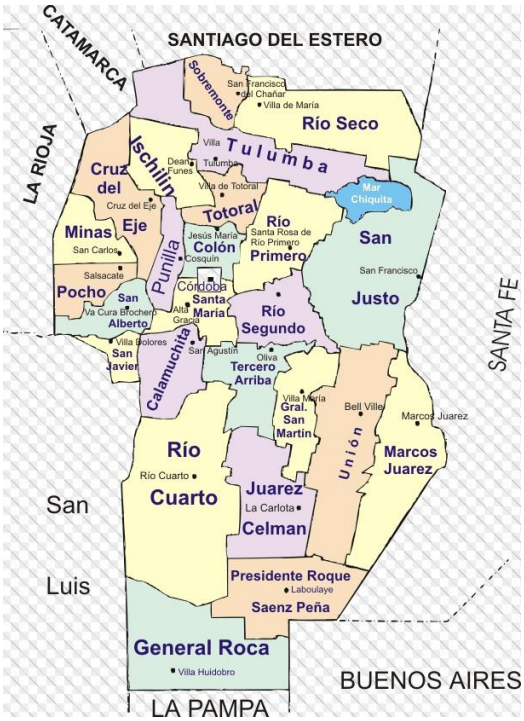


Fig. 11.3. Mapa de la Provincia de Córdoba.

24.3. ANEXO 3: DATOS DEL PERSONAL

11.4.1. FUNCIONES POR ÁREAS GERENCIALES:

Gerencia Administrativa:

- *Finanzas:* Lleva adelante la contabilidad de la empresa y gestiona los recursos económicos de la empresa, además lleva a delante el cobro a los clientes y la facturación de los servicios asociados al cobro.
- *Recursos Humanos y Pagos:* Gestiona el pago a los proveedores y el pago del salario a todos los empleados.
- *Logística de Servicios:* Se encarga de organizar los servicios a los cuales deben presentarse los vigiladores, además de gestionar y controlar la calidad del resto de los servicios.
- *Servicios:* Esta es un área muy importante en la empresa, ya que se llevan a cabo las tareas de control de cámaras y alarmas, a la vez que se gestionan todas las alertas, incluso las de los vigiladores para resolverlas con los clientes o con la policía.
- *Informática y Telecomunicaciones:* Gestiona todas las comunicaciones, ya sean telefónicas, celulares, conectividad de red (equipos informáticos) o radio, como así también, el buen funcionamiento de todos los equipos y su conectividad.

11.4.2. ORGANIGRAMA

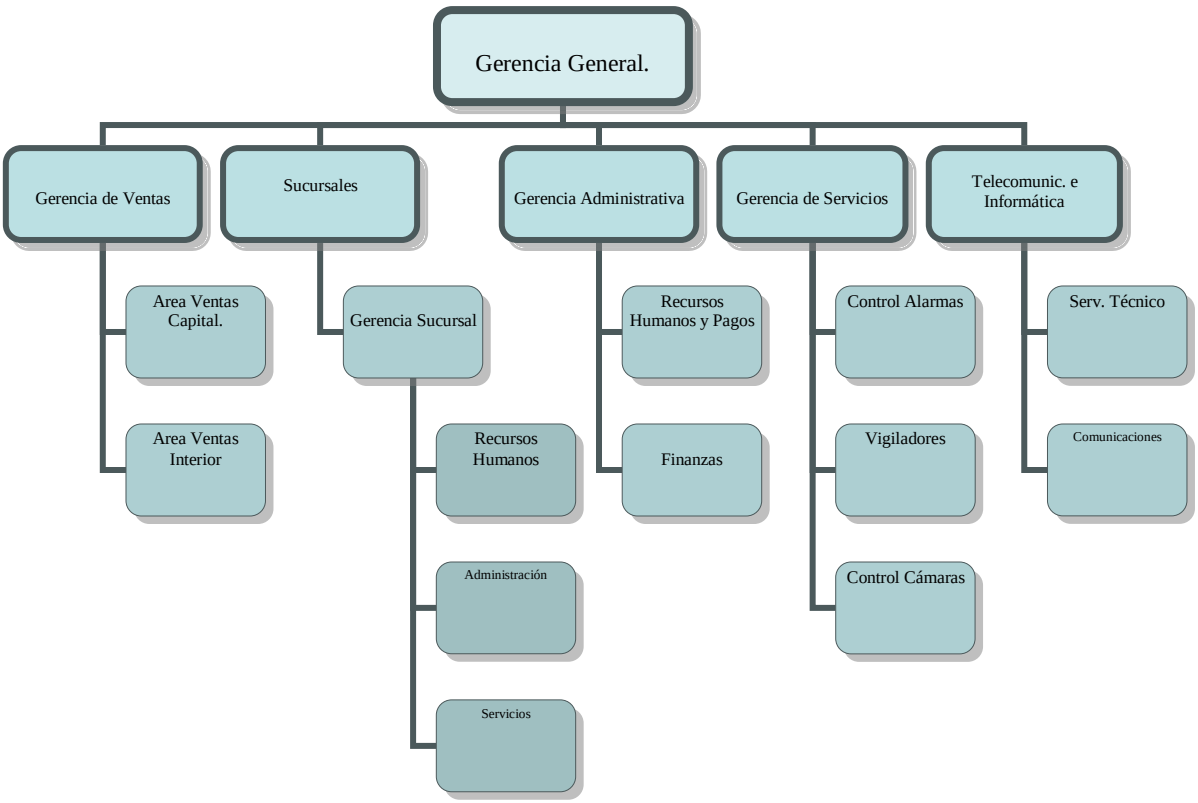


Fig. 11.4.2. Organigrama de MR Seguridad S.A.

11.4.3. DIVISIONES DE SERVICIOS QUE LA INTEGRAN:

- *Control Alarmas*
  - Es un servicio dedicado las 24hs los 365 días del año
  - Se emplea a personal especializado, el cual ante una alerta, intenta comunicarse con el cliente, para así eliminar falsas alarmas. En el caso de que no se pueda comunicar o que la misma sea positiva, el operador se comunica con la policía, y le da un seguimiento acompañando al cliente.
- *Control Cámaras*
  - Es un servicio que varía según el tipo de contrato con el cliente.
  - Se emplea a personal capacitado para la observación de situaciones anómalas en el monitor. Dado el caso de una situación de alerta, se comunica con el cliente o la policía para informar dicho delito.
- *Vigiladores*
  - Es un servicio que varía según el tipo de contrato con el cliente.

- A este servicio lo desarrolla personal capacitado para prevenir cualquier acción que atente o ponga en peligro el bienestar de las personas o bienes del edificio o institución a proteger, como así también la de brindar información y asistir o socorrer en caso de emergencias.

11.4.4. DOTACIÓN

Recursos humanos S.A. cuenta con alrededor de 300 empleados en las todas las sucursales. Los mismos se encuentran distribuidos aproximadamente de la siguiente manera:

- *Planta Baja:*
  - Gerente General. 1
  - Recepción. 1
  - Adm. De Recursos Humanos. 2
  - Logística. 2
  - Taller. 8
  - Adm. Servidores y Redes. 6
  - Coordinador Vigiladores 3
  - Vigiladores 50

- *Primer Piso:*
  - Control de Cámaras. 16
  - Control de Alarmas. 8
  - Logística de Servicios. 3
  - Gerente de Logística 1
  - Gerente de Servicios. 1

- *Sucursales e Interior de Córdoba:*
  - Gerente Sucursal. 8
  - Área administrativa. 25
  - Control de cámaras. 66
  - Control de alamas. 44
  - Recepción. 11
  - Coordinador Vigiladores. 6
  - Vigiladores. 30

Se debe tener en cuenta que muchas veces para cubrir un servicio, se contrata a personal temporal.

24.4. ANEXO 4: DATOS DEL ENTORNO ESPECÍFICO

- *Clientes:* Están conformados por alrededor de 3500 clientes, los cuales se mantienen en un nivel constante durante el año. En su mayoría son clientes hogareños y pequeños comercios.
- *Proveedores:* Son en su mayoría las empresas proveedoras de los elementos necesarios para el desarrollo de la actividad laboral, como por ejemplo: Policía de la Provincia de Córdoba, empresas de insumos de telecomunicaciones e informática, empresas de recursos humanos.

  Existe otro tipo de proveedores que son los impuestos y servicios, alquileres de locales y servicios varios de mantenimiento de las oficinas.
- *Accionistas:* No posee accionistas.
- *Competidores:* Son empresas competidoras, ADT S.A., Alarmix, Securitas S.A., Zeus S.R.L., SPG Seguridad etc.

24.5. ANEXO 5: CAPTURAS DE PANTALLA MICROSOFT BASELINE SECURITY

Fig. 14.3. Etapa 4: Herramientas, Microsoft Baseline Analyzer 2.3.

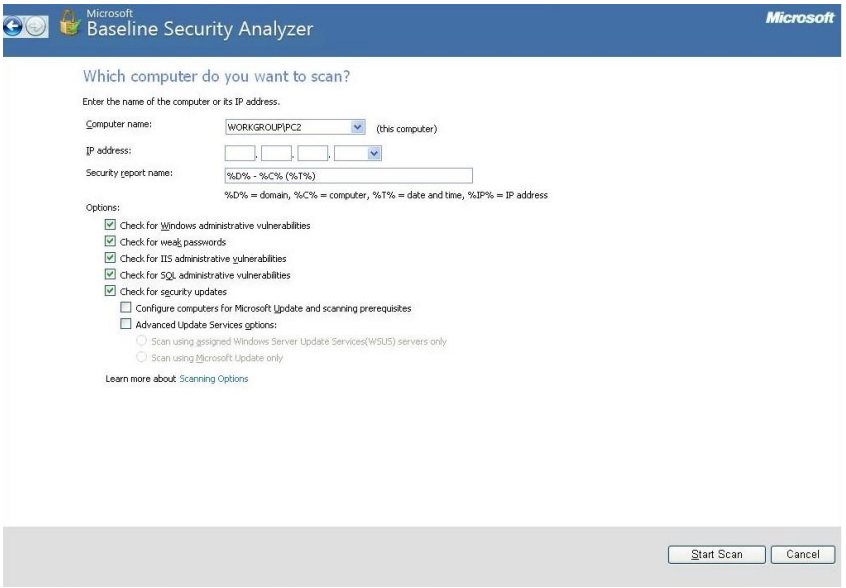


Fig. 14.3. Etapa 4: Herramientas, Microsoft Baseline Analyzer 2.3 – Opciones.

Fig. 14.3. Etapa 4: Herramientas, Microsoft Baseline Analyzer 2.3 – Ejemplo 1.

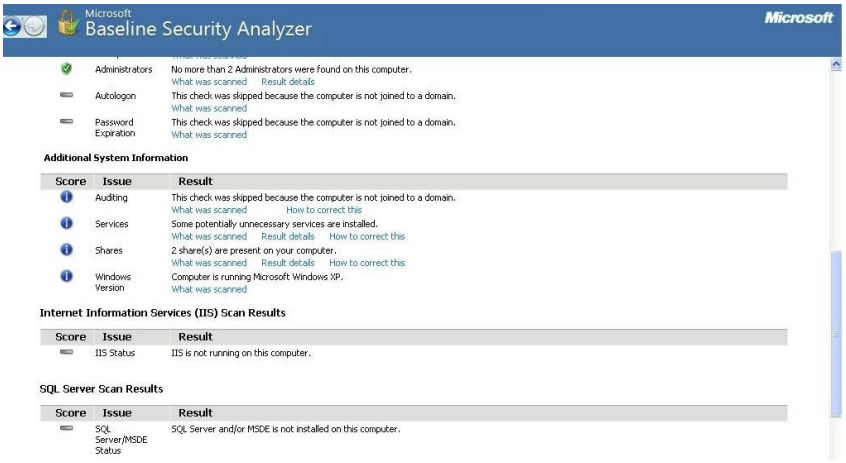


Fig. 14.3. Etapa 4: Herramientas, Microsoft Baseline Analyzer 2.3 – Ejemplo 2.

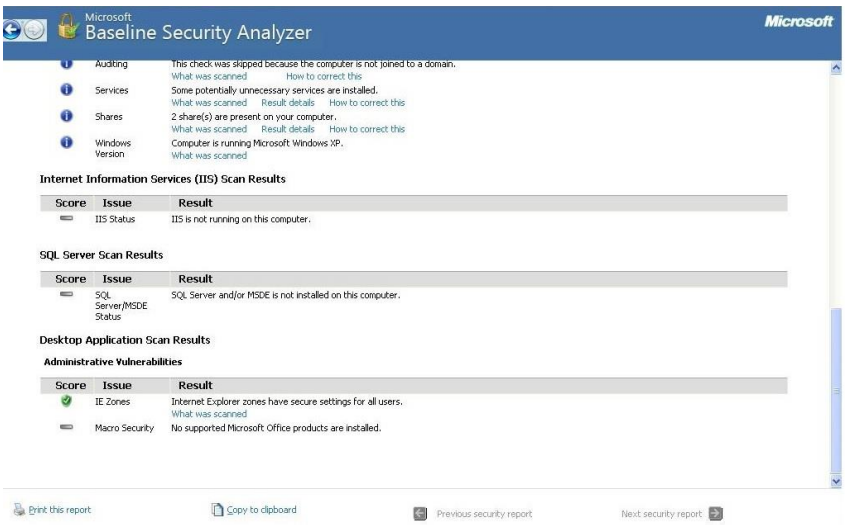


Fig. 14.3. Etapa 4: Herramientas, Microsoft Baseline Analyzer 2.3 – Ejemplo 3.

24.6. ANEXO 6: CAPTURAS DE PANTALLA DE RETINA COMMUNITY

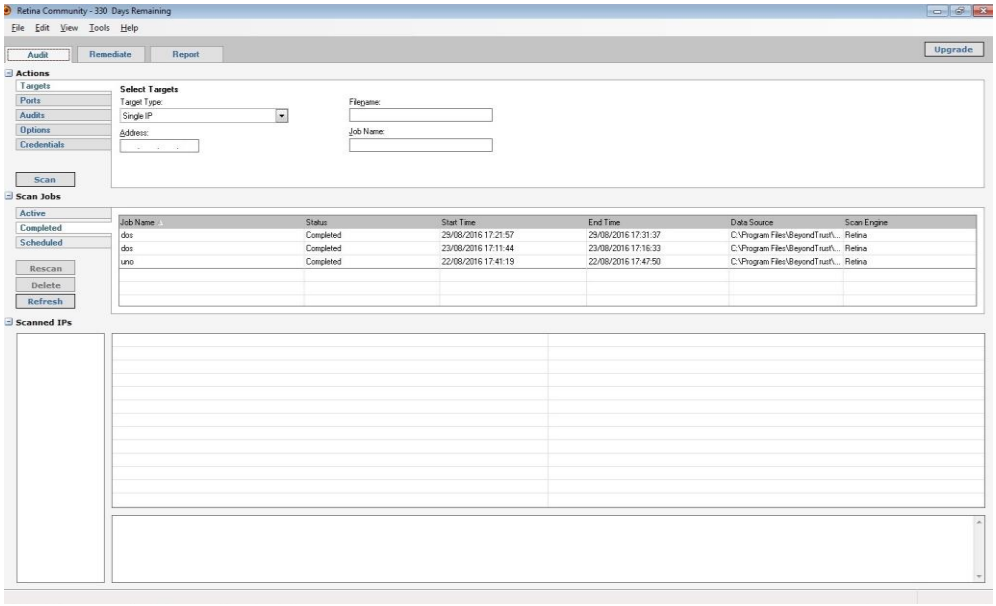


Fig. 14.3. Etapa 4: Herramientas Retina CS.

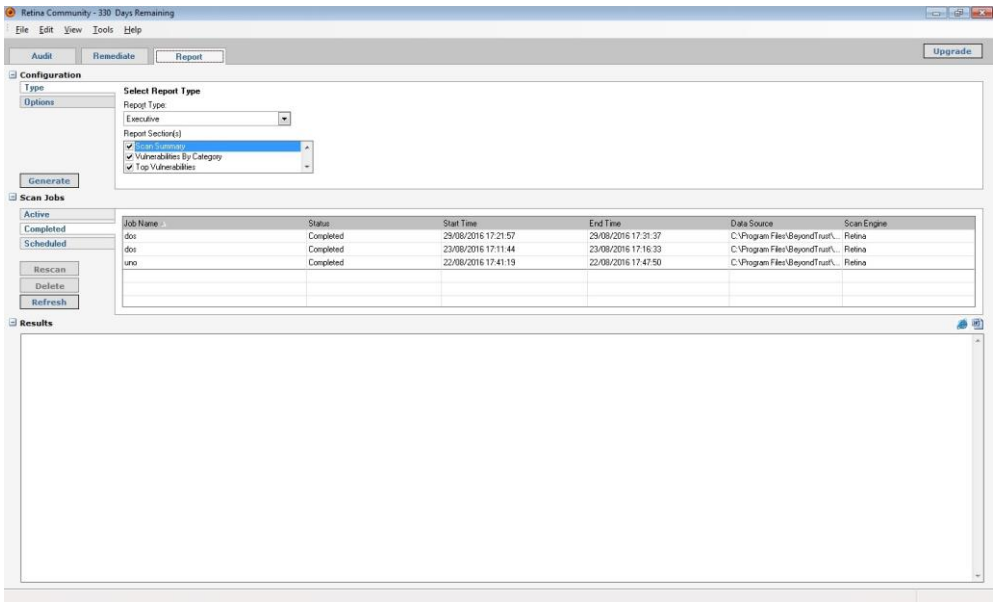
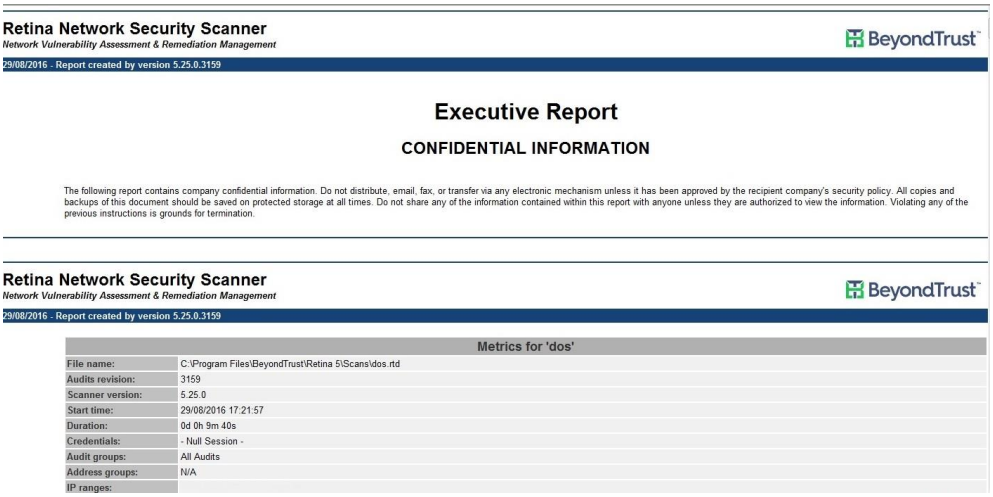


Fig. 14.3. Etapa 4: Herramientas, Retina CS - Ejemplo 1.



Retina Network Security Scanner
Network Vulnerability Assessment & Remediation Management
BeyondTrust
29/08/2016 - Report created by version 5.25.0.3159

Executive Report

CONFIDENTIAL INFORMATION

The following report contains company confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.

Retina Network Security Scanner
Network Vulnerability Assessment & Remediation Management
BeyondTrust
29/08/2016 - Report created by version 5.25.0.3159

Metrics for 'dos'	
File name:	C:\Program Files\BeyondTrust\Retina 5\Scans\dos.rtd
Audits revision:	3159
Scanner version:	5.25.0
Start time:	29/08/2016 17:21:57
Duration:	0d 0h 9m 40s
Credentials:	- Null Session -
Audit groups:	All Audits
Address groups:	N/A
IP ranges:	

Fig. 14.3. Etapa 4: Herramientas, Retina CS – Reporte Ejecutivo 1.

NETWORK ANALYSIS RESULTS

Report Summary			
Scanner Name	Retina	Machines Scanned	2
Scanner Version	5.25.0.3159	Vulnerabilities Total	414
Scan Start Date	29/08/2016	High Risk Vulnerabilities	263
Scan Start Time	17:21:57	Medium Risk Vulnerabilities	119
Scan Duration	0h 9m 40s	Low Risk Vulnerabilities	32
Scan Name	dos	Information Only Audits	46
Scan Status	Completed	Credential Used	
Vulnerable Machines	2		

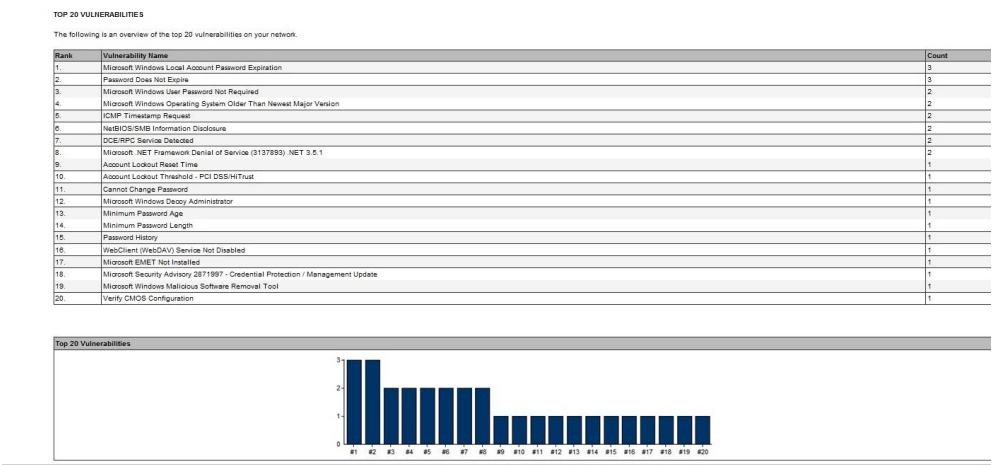
Top 5 Most Vulnerable Hosts

Num. of Vulnerabilities By Risk

% of Vulnerabilities By Risk

Avg. of Vulnerabilities By Risk

Fig. 14.3. Etapa 4: Herramientas, Retina CS – Reporte Ejecutivo 2.



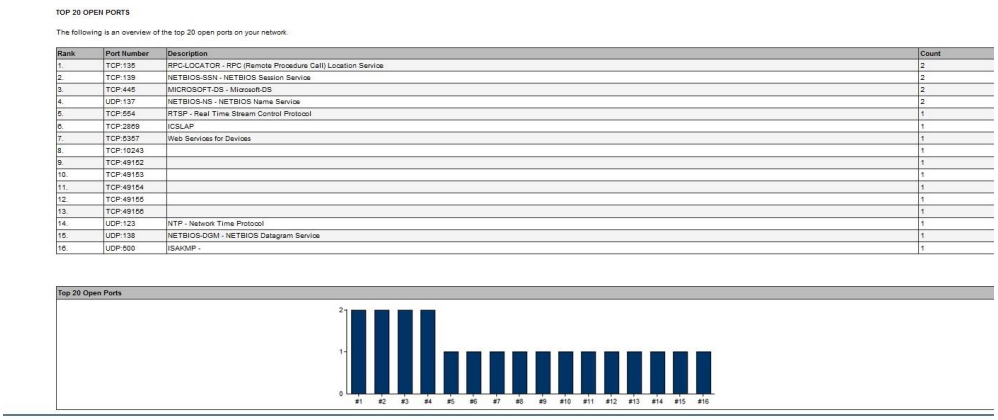
TOP 20 VULNERABILITIES

The following is an overview of the top 20 vulnerabilities on your network.

Rank	Vulnerability Name	Count
1.	Microsoft Windows Local Account Password Expiration	3
2.	Password Does Not Expire	3
3.	Microsoft Windows User Password Not Required	2
4.	Microsoft Windows Operating System Older Than Newest Major Version	2
5.	ICMP Timestamp Request	2
6.	NetBIOS/SMB Information Disclosure	2
7.	DCE/RPC Service Detected	2
8.	Microsoft .NET Framework Denial of Service (3137893) .NET 3.5.1	2
9.	Account Lockout Reset Time	1
10.	Account Lockout Threshold - PCI DSS/HiTrust	1
11.	Cannot Change Password	1
12.	Microsoft Windows Decoy Administrator	1
13.	Minimum Password Age	1
14.	Minimum Password Length	1
15.	Password History	1
16.	WebClient (WebDAV) Service Not Disabled	1
17.	Microsoft EMET Not Installed	1
18.	Microsoft Security Advisory 2871997 - Credential Protection / Management Update	1
19.	Microsoft Windows Malicious Software Removal Tool	1
20.	Verify CMOS Configuration	1

Top 20 Vulnerabilities

Fig. 14.3. Etapa 4: Herramientas, Retina CS – Reporte Ejecutivo 3.



TOP 20 OPEN PORTS

The following is an overview of the top 20 open ports on your network.

Rank	Port Number	Description	Count
1.	TCP:135	RPC-LOCATOR - RPC (Remote Procedure Call) Location Service	2
2.	TCP:139	NETBIOS-SSN - NETBIOS Session Service	2
3.	TCP:445	MICROSOFT-DS - Microsoft-DS	2
4.	UDP:137	NETBIOS-NS - NETBIOS Name Service	2
5.	TCP:554	RTSP - Real Time Stream Control Protocol	1
6.	TCP:2869	ICSLAP	1
7.	TCP:5357	Web Services for Devices	1
8.	TCP:10243		1
9.	TCP:49152		1
10.	TCP:49153		1
11.	TCP:49154		1
12.	TCP:49155		1
13.	TCP:49156		1
14.	UDP:123	NTP - Network Time Protocol	1
15.	UDP:138	NETBIOS-DGM - NETBIOS Datagram Service	1
16.	UDP:500	ISAKMP -	1

Top 20 Open Ports

Fig. 14.3. Etapa 4: Herramientas, Retina CS – Reporte Ejecutivo 4.