Servicios de consultoría en TI

Preparado para:

XXXXXXXXXXXX

Preparado Por:

Departamento de Consultoría.

Fecha:

06 de Noviembre de 2014.

Tabla de contenidos

1. Introducción

La seguridad informática se ha vuelto cada día más compleja para las empresas. Cada año se contabilizan perdidas millonarias en las compañías debido a la gran cantidad de ataques de virus y violaciones a la seguridad informática.

Hoy en día las empresas deben enfocar parte de su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos; para evitar pérdidas cuantiosas de dinero. Consecuentemente, se debe tener claro que no se trata solo de comprar el equipo más caro disponible en el mercado sino, saber aplicar las soluciones y medidas que se encuentran en todos departamentos y sobretodo en el personal de la empresa.

Constantemente, los intrusos informáticos aprovechan la mala cultura e inocencia de los usuarios para obtener información confidencial de las entidades; inclusive teniendo una barrera de alta tecnología, la fuga de información no se puede evitar al 100%, esta ha sido la clave para muchos atacantes en la actualidad y es un asunto que involucra tanto a los colaboradores como a las mismas empresas.

Preocuparse por la seguridad en los momentos en los que pasan los desastres es un lujo que pocas empresas se pueden permitir.

La seguridad es un factor muy importante en las empresas que no se debe dejar de lado ni restarle importancia porque en la actualidad cada vez son más los riesgos que hay, lo cual puede llegar a afectar tanto a las empresas como a sus clientes.

2. Resumen

El presente documento es un análisis realizado por YYYYYYYYYYYYYYYYY para la empresa XXXXXXXXXXX, este informe presenta un análisis de las vulnerabilidades encontradas en el edificio central de XXXXXXXXXXX y en algunas de sus agencias, en el cual se realiza un descubrimiento de equipos para hacerles un análisis de riegos con respecto a las vulnerabilidades encontradas en los mismos.

3. Definición del Problema

El análisis de vulnerabilidades es un componente crítico de cualquier infraestructura de seguridad, ya que permite la detección proactiva y remediación de vulnerabilidades de seguridad.

El análisis de vulnerabilidades le presenta a TI una amplia vista del estado y seguridad de la red (LAN/WAN); esto es lo mismo que un intruso puede ver desde internet o desde su red interna, más que un simple escaneo de puertos, este Análisis de Vulnerabilidades presentará las debilidades de los sistemas que de ser explotadas por hackers, puede poner su información en riesgo.

4. Definición del Proyecto

Objetivos del proyecto:

- Proveer a la empresa un conocimiento real en cuanto al nivel de seguridad en que se encuentran sus equipos informáticos.
- Brindarles una guía para solucionar las vulnerabilidades que tienen los equipos y así reducir el riesgo tanto local como en general.
- Dar a conocer medidas que se pueden tomar para mejorar la cultura actual de los usuarios.
- Medir el nivel de riesgo de las vulnerabilidades encontradas en la red de XXXXXXXXXXX.
- Brindarles el material necesario al personal para corregir las vulnerabilidades que presentan los equipos.

5. Definición de actividades

A continuación se detallan las actividades propuestas para llevar a cabo los objetivos establecidos.

Para cumplir los objetivos propuestos se definió el siguiente plan de trabajo:

Solicitud de información acerca del direccionamiento IP y requerimientos para el ingreso del equipo a las oficinas de XXXXXXXXXXXX:

- Dirección estática para asignarla al equipo 10.30.30.236
- Se solicita la posibilidad de sesiones remotas.

Instalación y configuración del software en el equipo:

- Se instala el sistema operativo Windows 2003 server con sus debidas actualizaciones.
- El equipo cuenta con dos tarjetas de red, una se configura con la información de la red de YYYYYYYYYYYYYYYYY y la otra con la dirección brindada por el cliente.
- Descarga e instalación de McAfee Vulnerability Manager 7.0.
- Se actualiza dicha aplicación.
- Se configura la aplicación y además se hace la solicitud de la licencia a McAfee de acuerdo a la configuración de la NIC del equipo que en su caso tenía asignada la ip 10.30.30.236.

Visita a XXXXXXXXXXXX

En las instalaciones del cliente se llevan a cabo las siguientes actividades:

1. Se agrega el equipo a la red configurando las siguientes funciones:

    - Escaneo para descubrir los equipos en las siguientes subredes y direcciones ip:
        - Estaciones de trabajo oficinas centrales
        - Servidores en oficinas centrales
        - Servidores Agencias
        - Equipos de Comunicaciones Oficinas Centrales
        - Equipos de Comunicaciones Agencias
        - Escaneo Wireless

    - Escaneo completo intrusivo en las siguientes subredes
        - Servidores en oficinas centrales
        - Servidores Agencias
        - Equipos de Comunicaciones Oficinas Centrales
        - Equipos de Comunicaciones Agencias

    - La aplicación se configura para que se genere un reporte para cada uno de los escaneos mencionados.

2. Programación de horario en coordinación con el departamento de Informática para asegurar que los escaneos fueran realizados cuando los equipos estuvieran encendidos.
3. Programación de sesiones remotas con el departamento para monitorear y revisar el avance del proceso.
4. Toma de datos de los escaneos realizados.
5. Retiro del equipo de Edificio de XXXXXXXXXXXX.

Elaboración del Informe

Con base a los datos recolectados por el equipo durante el proceso de escaneo se estudiaran para realizar un documento donde se le informara al cliente los riesgos y recomendaciones a tomar para sus plataformas.

6. Nivel de Riesgo

A continuación se hará un análisis del nivel de riesgo presente en cada uno de los segmentos de red analizados.

6.1 Servidores Oficinas Centrales

Los servidores analizados tienen el siguiente rango de direccionamiento: **10.30.30.0 / 24**

El nivel de Riesgo de la institución en sus servidores de oficinas centrales de XXXXXXXXXXXX es de un 70%; porcentaje que ubica al riesgo por debajo del promedio aceptable, esto se detalla en el siguiente gráfico:

FOUNDSCORE SUMMARY >> Detailed Report

Low Risk  High Risk 30 / 100

Click here for a Detailed Explanation of the FoundScore Risk Rating System.

DISCOVERED HOSTS SUMMARY >> Detailed Report

Top Ten Networks by Active System Count

Network Name	Active IP Addresses	Total IP Addresses Scanned
10.30.30.226 - 10.30.33.255	18	798
10.30.30.1 - 10.30.30.224	80	224
Total	**98**	**1022**

Total Active Systems	**89**

6.2 Servidores Agencias

Direcciones Escaneadas:

10.200.102.25, 10.200.104.25, 10.200.106.25, 10.200.109.25, 10.200.110.25, 10.200.111.25, 10.200.112.25, 10.200.113.25, 10.200.114.25, 10.200.115.25, 10.200.116.25, 10.200.117.25, 10.200.118.25, 10.200.119.25, 10.200.120.25, 10.200.121.25, 10.200.122.25, 10.200.123.25, 10.200.124.25, 10.200.125.25, 10.200.126.25, 10.200.127.25, 10.200.128.25, 10.200.129.25, 10.200.130.25, 10.200.131.25, 10.200.132.25, 10.200.133.25, 10.200.134.25, 10.200.135.25, 10.200.136.25.

De acuerdo con la información recopilada los servidores de las agencias de XXXXXXXXXXX se encuentran en un nivel de riesgo nulo (0%), como se puede observar en el siguiente gráfico de algunos de los servidores escaneados:

FOUNDSCORE SUMMARY >> Detailed Report

Low Risk  High Risk 100 / 100

Click here for a Detailed Explanation of the FoundScore Risk Rating System.

DISCOVERED HOSTS SUMMARY >> Detailed Report

Top Ten Networks by Active System Count

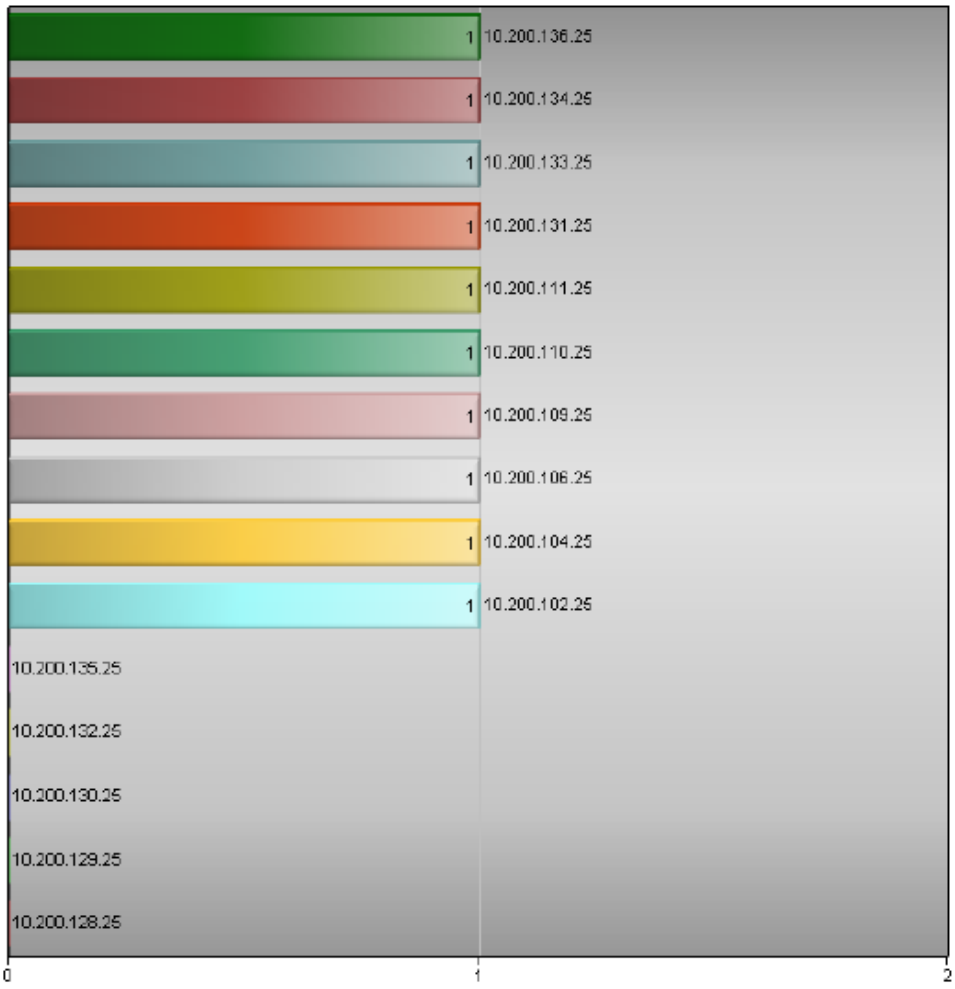
Network Name	Active IP Addresses	Total IP Addresses Scanned
10.200.102.25	1	1
10.200.104.25	1	1
10.200.106.25	1	1
10.200.109.25	1	1
10.200.110.25	1	1
10.200.111.25	1	1
10.200.131.25	1	1
10.200.133.25	1	1
10.200.134.25	1	1
10.200.136.25	1	1
Total	**10**	**10**

Total Active Systems	**10**

Hosts Report

Discovered Addresses By Range(s) Scanned

McAfee Vulnerability Manager uses a combination of ICMP, UDP, and TCP "pings" to discover hosts. The graph and tables below contain the results of McAfee Vulnerability Manager's thorough host discovery process, displaying active and total potential hosts for the IP address ranges provided.



6.3 Equipos de Comunicación Oficina Central

Direcciones: 10.0.0.0 /24

Los equipos de comunicación de las oficinas centrales se encuentran sin un nivel de riesgo promedio como vemos en el siguiente gráfico:

FOUNDSCORE SUMMARY >> Detailed Report

Low Risk  High Risk 69 / 100

Click here for a Detailed Explanation of the FoundScore Risk Rating System.

DISCOVERED HOSTS SUMMARY >> Detailed Report

Top Ten Networks by Active System Count

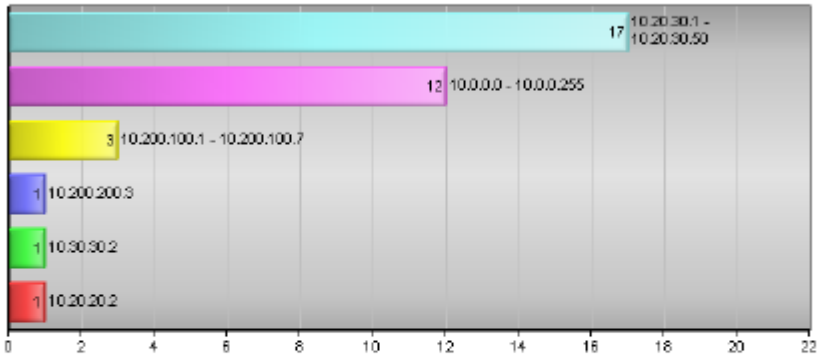
Network Name	Active IP Addresses	Total IP Addresses Scanned
10.20.20.2	1	1
10.30.30.2	1	1
10.200.200.3	1	1
10.200.100.1 - 10.200.100.7	3	7
10.0.0.0 - 10.0.0.255	12	256
10.20.30.1 - 10.20.30.50	17	50
Total	**35**	**316**

Total Active Systems	**34**

Note: McAfee Vulnerability Manager uses a customizable rule-based system to track individual assets, hence it is possible that multiple discovered hosts match a single asset based on currently configured rules. For this reason, the number of Active Systems (assets) displayed in the Discovered Hosts or Assets Summary section can be less than the total number of Hosts Found in the scan status page.

Discovered Addresses By Range(s) Scanned

McAfee Vulnerability Manager uses a combination of ICMP, UDP, and TCP "pings" to discover hosts. The graph and tables below contain the results of McAfee Vulnerability Manager's thorough host discovery process, displaying active and total potential hosts for the IP address ranges provided.



Summary of Discovered Addresses

Network Name	Active IP Addresses	Total IP Addresses Scanned
10.0.0.0 - 10.0.0.255	12	256
10.20.20.2	1	1
10.20.30.1 - 10.20.30.50	17	50
10.30.30.2	1	1
10.200.100.1 - 10.200.100.7	3	7
10.200.200.3	1	1
Total	**35**	**316**

6.4 Equipos de Comunicación de Agencias

Direcciones:

100.200.102.1 - 100.200.102.2
100.200.103.1 - 100.200.103.2
100.200.104.1 - 100.200.104.2
100.200.105.1 - 100.200.105.2
100.200.106.1 - 100.200.106.2
100.200.107.1 - 100.200.107.2
100.200.108.1 - 100.200.108.2
100.200.109.1 - 100.200.109.2
100.200.110.1 - 100.200.110.2
100.200.111.1 - 100.200.111.2
100.200.112.1 - 100.200.112.2
100.200.113.1 - 100.200.113.2
100.200.114.1 - 100.200.114.2
100.200.115.1 - 100.200.115.2
100.200.116.1 - 100.200.116.2
100.200.117.1 - 100.200.117.2
100.200.118.1 - 100.200.118.2
100.200.119.1 - 100.200.119.2
100.200.120.1 - 100.200.120.2
100.200.121.1 - 100.200.121.2
100.200.122.1 - 100.200.122.2
100.200.123.1 - 100.200.123.2
100.200.124.1 - 100.200.124.2
100.200.125.1 - 100.200.125.2
100.200.126.1 - 100.200.126.2
100.200.127.1 - 100.200.127.2
100.200.128.1 - 100.200.128.2
100.200.129.1 - 100.200.129.2
100.200.130.1 - 100.200.130.2
100.200.130.1 - 100.200.130.2
100.200.131.1 - 100.200.131.2
100.200.132.1 - 100.200.132.2
100.200.133.1 - 100.200.133.2
100.200.134.1 - 100.200.134.2
100.200.135.1 - 100.200.135.2
100.200.136.1 - 100.200.136.2
100.200.137.1 - 100.200.137.2
100.200.138.1 - 100.200.138.2
100.200.139.1 - 100.200.139.2
100.200.140.1 - 100.200.140.2

Los equipos de comunicación se encuentran sin nivel de riesgo relevante como se muestra en los gráficos siguientes:

DISCOVERED HOSTS SUMMARY >> Detailed Report

Top Ten Networks by Active System Count

Network Name	Active IP Addresses	Total IP Addresses Scanned
10.200.132.1 - 10.200.132.2	2	2
10.200.133.1 - 10.200.133.2	2	2
10.200.134.1 - 10.200.134.2	2	2
10.200.135.1 - 10.200.135.2	2	2
10.200.136.1 - 10.200.136.2	2	2
10.200.137.1 - 10.200.137.2	2	2
10.200.138.1 - 10.200.138.2	2	2
10.200.139.1 - 10.200.139.2	2	2
10.200.140.1 - 10.200.140.2	2	2
10.200.121.1 - 10.200.122.2	5	258
Total	**23**	**276**

Total Active Systems	**75**

6.5 Wireless

Rango: 10.200.100.0 - 10.200.100.24

El nivel de riesgo de wireless como se puede observar es de un 0%, se muestra en gráfico adjunto:

FOUNDSCORE SUMMARY >> Detailed Report

Low Risk  High Risk

100
100

Click here for a Detailed Explanation of the FoundScore Risk Rating System.

DISCOVERED HOSTS SUMMARY >> Detailed Report

Top Ten Networks by Active System Count

Network Name	Active IP Addresses	Total IP Addresses Scanned
10.200.100.1 - 10.200.100.24	6	24
Total	**6**	**24**

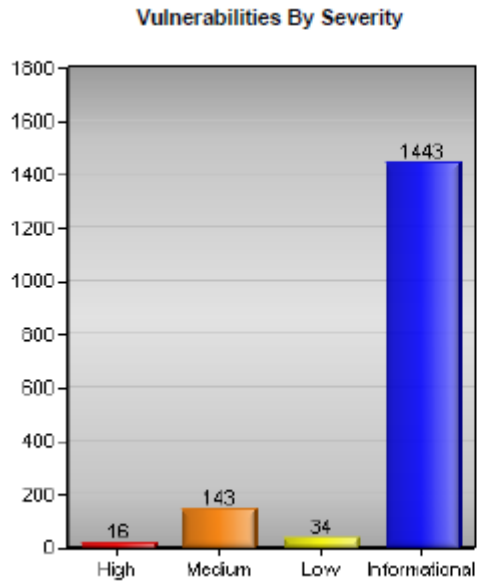
Total Active Systems	**6**

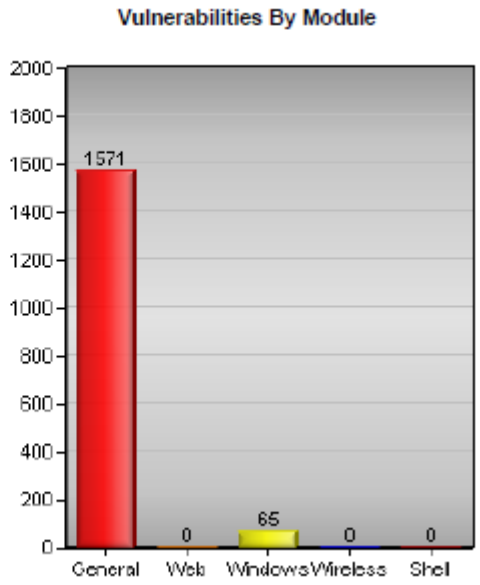
7. DETALLE DE NIVELES DE RIESGO

Cantidad de vulnerabilidades por severidad y tipo de modulo del segmento de red.

7.1 SERVIDORES DE OFICINA CENTRAL

Segmento analizado 10.30.30.0…10.30.30.255

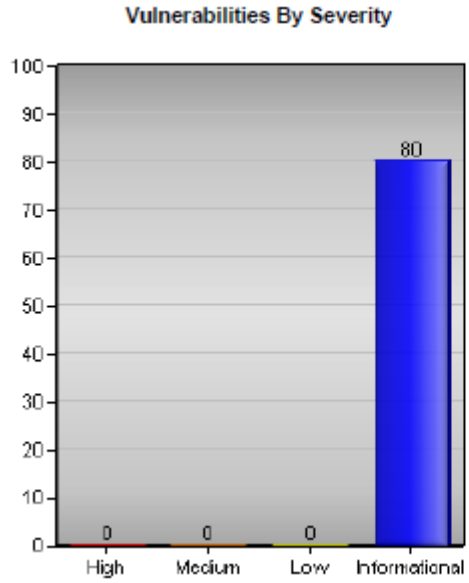


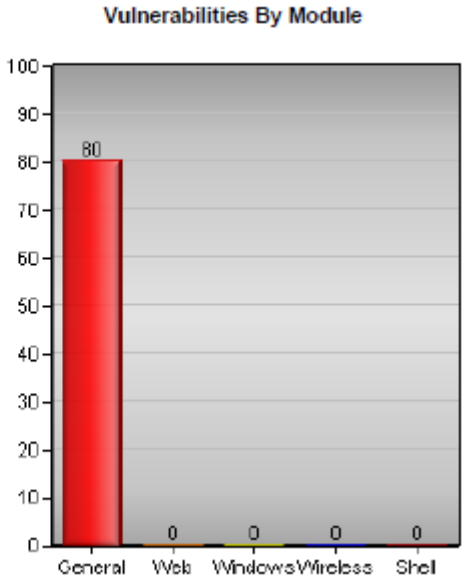


7.2 SERVIDORES AGENCIAS

Direcciones Escaneadas:

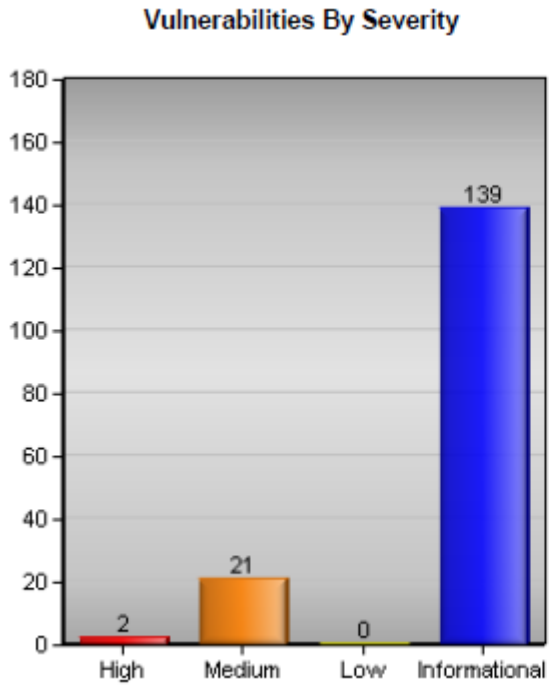
10.200.102.25, 10.200.104.25, 10.200.106.25, 10.200.109.25, 10.200.110.25, 10.200.111.25, 10.200.112.25, 10.200.113.25, 10.200.114.25, 10.200.115.25, 10.200.116.25, 10.200.117.25, 10.200.118.25, 10.200.119.25, 10.200.120.25, 10.200.121.25, 10.200.122.25, 10.200.123.25, 10.200.124.25, 10.200.125.25, 10.200.126.25, 10.200.127.25, 10.200.128.25, 10.200.129.25, 10.200.130.25, 10.200.131.25, 10.200.132.25, 10.200.133.25, 10.200.134.25, 10.200.135.25, 10.200.136.25.

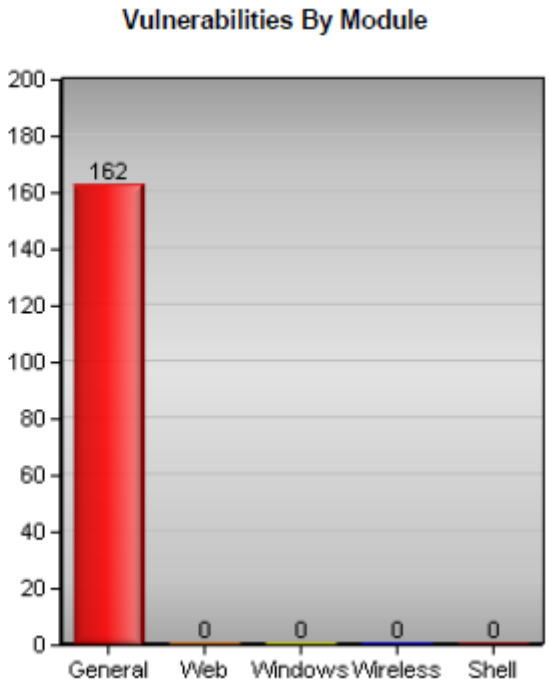




7.3 EQUIPOS DE COMUNICACION OFICINA CENTRAL

Segmento analizado: 10.0.0.0 /24



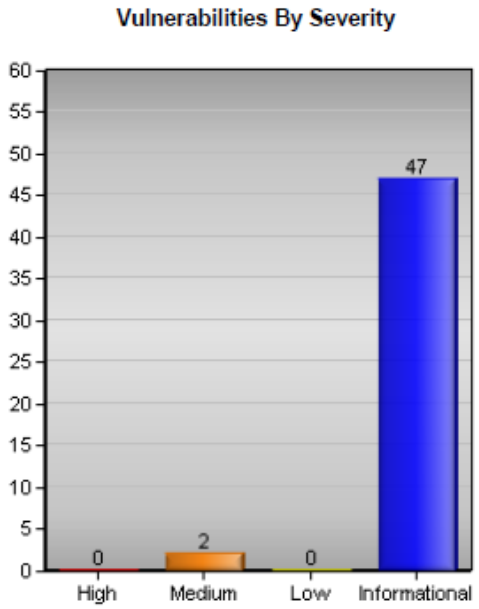


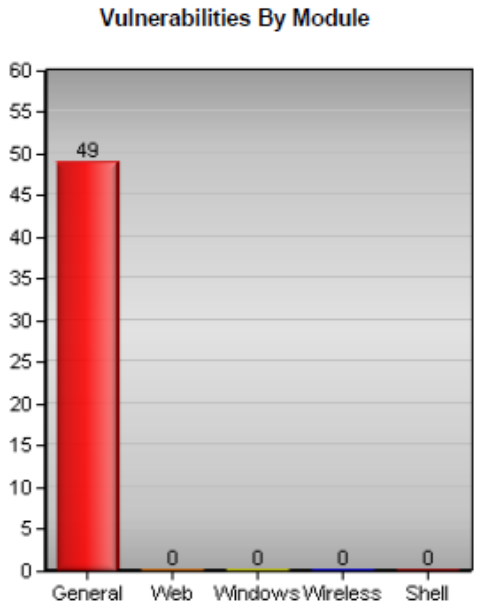
7.4 EQUIPOS DE COMUNICACIÓN AGENCIAS

Direcciones:

100.200.102.1 - 100.200.102.2
100.200.103.1 - 100.200.103.2
100.200.104.1 - 100.200.104.2
100.200.105.1 - 100.200.105.2
100.200.106.1 - 100.200.106.2
100.200.107.1 - 100.200.107.2
100.200.108.1 - 100.200.108.2
100.200.109.1 - 100.200.109.2
100.200.110.1 - 100.200.110.2
100.200.111.1 - 100.200.111.2
100.200.112.1 - 100.200.112.2
100.200.113.1 - 100.200.113.2
100.200.114.1 - 100.200.114.2
100.200.115.1 - 100.200.115.2
100.200.116.1 - 100.200.116.2
100.200.117.1 - 100.200.117.2
100.200.118.1 - 100.200.118.2
100.200.119.1 - 100.200.119.2
100.200.120.1 - 100.200.120.2
100.200.121.1 - 100.200.121.2
100.200.122.1 - 100.200.122.2
100.200.123.1 - 100.200.123.2
100.200.124.1 - 100.200.124.2
100.200.125.1 - 100.200.125.2
100.200.126.1 - 100.200.126.2
100.200.127.1 - 100.200.127.2
100.200.128.1 - 100.200.128.2
100.200.129.1 - 100.200.129.2
100.200.130.1 - 100.200.130.2
100.200.130.1 - 100.200.130.2
100.200.131.1 - 100.200.131.2
100.200.132.1 - 100.200.132.2
100.200.133.1 - 100.200.133.2
100.200.134.1 - 100.200.134.2

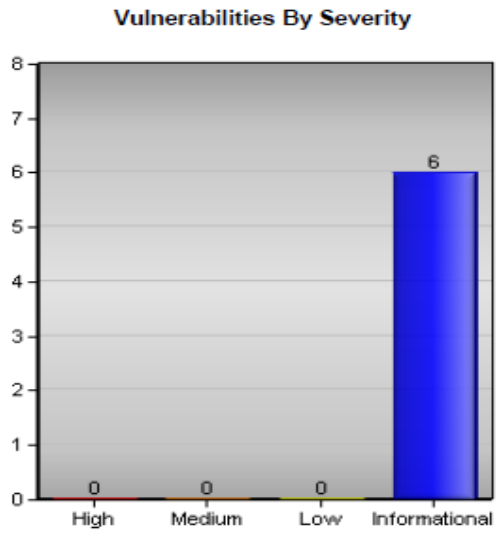
100.200.135.1 - 100.200.135.2
100.200.136.1 - 100.200.136.2
100.200.137.1 - 100.200.137.2
100.200.138.1 - 100.200.138.2
100.200.139.1 - 100.200.139.2
100.200.140.1 - 100.200.140.2

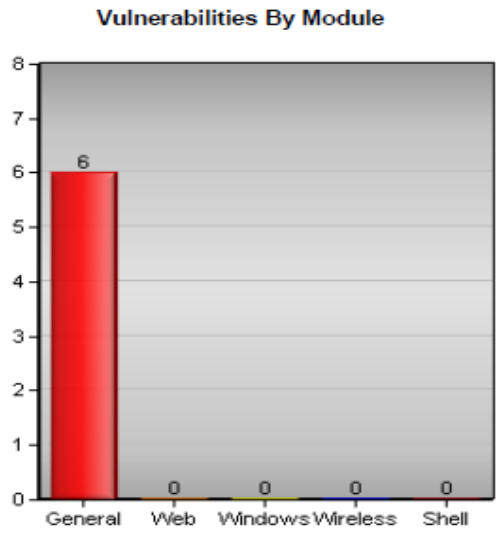




7.5 WIRELESS

La red wireless no presenta vulnerabilidades significativas, como se muestra en la siguiente figura.





8. VULNERABILIDADES

8.1 VULNERABILIDADES DE ALTO RIESGO SERVIDORES OFICINA CENTRAL

Nivel de Riesgo	Nombre Vulnerabilidad	Equipos Afectados	Descripción	Recomendaciones
ALTO	(CVE-2007-2897) Microsoft Internet Information Services Remote DoS	CEFEO, 10.30.30.20	Microsoft Internet Information Services contiene una vulnerabilidad que podría permitir ataques remotos de denegación de servicio.	McAfee es actualmente consciente de un parche suministrado por el proveedor o actualización (07/28/2014) Para mitigar el impacto de esta vulnerabilidad, URLScan se puede configurar para filtrar las solicitudes de URL que causan la denegación de servicio. http://www.iis.net/downloads/microsoft/urlscan
ALTO	ISC BIND DNS out-of-bailiwick Data Information Disclosure Vulnerability	10.30.30.47	Una vulnerabilidad de divulgación de información está presente en algunas versiones de ISC BIND.	Descargue la versión más reciente de ISC BIND desde la siguiente ubicación: https://www.isc.org/downloadables/11

ALTO	ISC BIND inet_network Libbind Denial Of Service Vulnerability	10.30.30.47	ISC BIND inet_network Libbind vulnerabilidad de denegación de servicio	Descargue la versión más reciente de ISC BIND desde la siguiente ubicación: https://www.isc.org/downloadables/11
ALTO	Apache httpd Ranges Header Field Memory Exhaustion	bity.XXXXXXXXXXXXficr.local, 10.30.30.55	Una vulnerabilidad de denegación de servicio está presente en algunas versiones de Apache Software Foundation HTTP Server.	El vendedor ha publicado una actualización para resolver el problema: https://www.apache.org/dist/httpd/Announcement2.2.html http://h20565.www2.hp.com/portal/site/hpsc/public/kb/secBullArchive/?ac.admitted=1337001371440.876444892.492883150#MU
ALTO	Samsung Printer SNMP Backdoor	thot.XXXXXXXXXXXXficr.local, THOT, 10.30.30.57	Una vulnerabilidad de puerta trasera está presente en algunas versiones de las impresoras Samsung.	El vendedor ha publicado un aviso para abordar el tema: http://www.kb.cert.org/vuls/id/281284

ALTO	OpenSSL TLS DTLS Heartbeat Extension Packets Information Disclosure	osiris.XXXXXXXXXXXficr.local, OSIRIS, 10.30.30.22 hadar.XXXXXXXXXXXficr.local, HADAR, 10.30.30.239 druso.XXXXXXXXXXXficr.local, DRUSO, 10.30.30.53	Una vulnerabilidad en algunas versiones de OpenSSL podría llevar a la divulgación de información.	El vendedor ha publicado una actualización para resolver el problema: http://www.openssl.org/news/secadv_20140407.txt Los detalles adicionales con respecto a la mitigación del producto McAfee y remediación se pueden encontrar en: https://kc.mcafee.com/corporate/index?page=content&id=SB10071
A;TO	OpenSSL SSL/TLS Man-In-The-Middle Injection Attack	osiris.XXXXXXXXXXXficr.local, OSIRIS, 10.30.30.22 hadar.XXXXXXXXXXXficr.local, HADAR, 10.30.30.239 tau.XXXXXXXXXXXficr.local, TAU, 10.30.30.24 hefesto.XXXXXXXXXXXficr.local, HEFESTO, 10.30.30.30 druso.XXXXXXXXXXXficr.local, DRUSO, 10.30.30.53 proteo.XXXXXXXXXXXficr.local, PROTEO, 10.30.30.77 turin.XXXXXXXXXXXficr.local, 10.30.30.89	Una vulnerabilidad en algunas versiones de OpenSSL podría conducir a un ataque de inyección.	El vendedor ha publicado una actualización para resolver el problema: http://www.openssl.org/news/secadv_20140605.txt
ALTO	Apache Tomcat Malicious JSP Remote Code Execution	infooc44.XXXXXXXXXXXficr.local, TECNOC57, 10.30.30.108	Una vulnerabilidad en algunas versiones de Apache Tomcat podría provocar la ejecución remota de código.	El vendedor ha publicado una actualización para resolver el problema: http://tomcat.apache.org/security-7.html#Fixed_in_Apache_Tomcat_7.0.40 Nota: Si el entorno no cumple los requisitos de este ataque, el objetivo es segura y este informe vulnerabilidad puede ser ignorada. Pero es mejor para

				actualizar a la última versión de Tomcat versión.

Todas las vulnerabilidades encontradas en este banco de servidores se pueden consultadas en los documentos adjuntos denominados:

Servidores Oficinas Centrales.pdf

8.2 VULNERABILIDADES DE ALTO RIESGO SERVIDORES AGENCIAS

Los servidores de las agencias de XXXXXXXXXXXX en este punto de análisis se encuentran muy bien protegidos, ya que no presentan vulnerabilidades de alto riesgo.

FoundScore: Vulnerabilities	Your Results	Deductions	Running Score
High Risk Vulnerabilities	0	0	100
Medium Risk Vulnerabilities	0	0	100
Low Risk Vulnerabilities	0	0	100
Informational Risk Vulnerabilities	80	0	100
	Score after Vulnerability Deductions:		100

8.3 VULNERABILIDADES DE ALTO RIESGO EQUIPOS DE COMUNICACIÓN OFICINA CENTRAL

ALTO	Samsung Printer SNMP Backdoor	10.20.30.23 10.20.30.24	Una vulnerabilidad de puerta trasera está presente en algunas versiones de	El vendedor ha publicado un aviso para abordar el tema: http://www.kb.cert.org/vuls/id/281284

las impresoras
Samsung.

8.4 VULNERABILIDADES DE ALTO RIESGO EQUIPOS DE COMUNICACIÓN AGENCIAS

Los equipos de comunicación de las agencias de XXXXXXXXXXXX no presentan riesgo alto con respecto a las vulnerabilidades.

FoundScore: Vulnerabilities	Your Results	Deductions	Running Score
High Risk Vulnerabilities	0	0	100
Medium Risk Vulnerabilities	2	1	99
Low Risk Vulnerabilities	0	0	99
Informational Risk Vulnerabilities	47	0	99
	Score after Vulnerability Deductions:		99

8.5 VULNERABILIDADES DE ALTO RIESGO WIRELESS

Los equipos Wireless de las agencias de XXXXXXXXXXXX no presentan riesgo alto con respecto a las vulnerabilidades.

FoundScore: Vulnerabilities	Your Results	Deductions	Running Score
High Risk Vulnerabilities	0	0	100
Medium Risk Vulnerabilities	0	0	100
Low Risk Vulnerabilities	0	0	100
Informational Risk Vulnerabilities	6	0	100
	Score after Vulnerability Deductions:		100

9. Recomendaciones

- Instalar parches y actualizaciones tanto para sistemas operativos como aplicaciones.

- Implementar un sistema de administración de actualizaciones para la mayoría de las aplicaciones como por ejemplo Windows Server Update Services (WSUS) donde los administradores pueden manejar centralmente la distribución de parches a través de actualizaciones automáticas a todos los computadores de la red corporativa.
- Mantener las aplicaciones de seguridad para Endpoint con las últimas versiones y actualizaciones. Además asegurarnos de que cada aplicación tenga su correcta configuración.
- Si se cuenta con una consola centralizada para el antivirus hacer reportes para visualizar el estado de las actualizaciones, versiones y además ver si hay equipos que han sido infectados con mucha frecuencia.
- Revisar en cada equipo si hay servicios innecesarios en ejecución ya que estos podrían ser explotados por alguna vulnerabilidad.
- En caso de transportar información de un lugar a otro se recomienda el uso de un sistema para encriptar la información ya sea en dispositivos extraíbles o equipos portátiles y así disminuir el riesgo de fuga de información en caso de extravió, robo o cualquier otra situación similar.
- Recomendamos el uso de un sistema de prevención de intrusiones perimetral (IPS) y de Endpoint (HIPS) debido a que este nos ayudaría a prevenir ataques, a proteger sistemas no parcheados y ayudaría a optimizar el rendimiento de la red.
- Se recomienda usar un sistema de control de dispositivos para controlar el uso por ejemplo de unidades extraíbles con esto se controla el riesgo que estos dispositivos pueden resultar para la empresa.
- Para los sistemas operativos o aplicaciones no Windows se recomienda revisar las guías de mejores prácticas en cuanto a seguridad y aplicar las mismas según la necesidad de la organización para proteger dichos sistemas.
- En relación a los sistemas operativos o aplicaciones no Windows se debe de aplicar los parches encontrados o recomendaciones del fabricante para mejorar la seguridad de los mimos.

10. Conclusión

Se logra observar un gran avance en cuanto al tema de vulnerabilidades, ya que estas aunque están presentes se han logrado reducir. Se debe seguir prestando atención a este tema, y a las herramientas de seguridad con las que cuentan para así reducir o minimizar los ataques informáticos, para poder evitar pérdidas cuantiosas de dinero o de la información.

Se debe continuar con las mismas ideas y políticas, crear una cultura sana dentro de los usuarios para que los intrusos informáticos tengan una barrera, no lograremos evitar la fuga de información en un 100% pero si estar atentos, y preparados para cualquier tipo de ataque. Seguir con la misma preocupación por la seguridad informática, es un gran habito que no se puede dejar pasar.

Recordar que, la seguridad es un factor muy importante en las empresas que no se debe dejar de lado ni restarle importancia porque en la actualidad cada vez son más los riesgos que hay, lo cual puede llegar a afectar tanto a las empresas como a sus clientes.

En general, siempre existirá algún tema por perfeccionar pero si debemos prestar más atención a mejorar principalmente la aplicación de parches y actualizaciones de las aplicaciones instaladas en los equipos para tratar de no dar lugar a vulnerabilidades que pueden ser explotas y traer serias consecuencias a la institución.

11. Anexos

ANEXO 1

ESCANEO NO INTRUSIVO

DESCRIPCION

General Vulnerabilities

BruteForce

FTP Brute Force

IMAP Brute Force

Microsoft Windows LDAP Bind Request Information Disclosure Vulnerability

POP Brute Force

SSH Brute Force

Telnet Brute Force

Miscellaneous

AnalogX SimpleServer:Shout Server Buffer Overflow

AppleFileServer Buffer Overflow

Atrium Software Mercur Mailserver IMAP Service Buffer Overflow

Blue Coat Systems WinProxy Host Header Overflow Intrusive

CA iGateway Content-Length Buffer Overflow Vulnerability

Computer Associates BrightStor ARCserve Backup Agents Buffer Overflow

Computer Associates Message Queuing (CAM/CAFT) Multiple Vulnerabilities

eIQnetworks Enterprise Security Analyzer Monitoring Agent Buffer Overflow Vulnerabilities

FreeBSD NFS Server Remote Denial of Service Vulnerability

freeFTPd PORT Command Denial Of Service Vulnerability

FTP Server Allows CHMOD Command

Helix Universal Server\RealServer View Source Remote Code Execution

HP OpenView Network Node Manager ovalarmsrv Integer Overflow Vulnerability

HP Printer FTP Denial-of-Service

IBM DB2 Denial-of-Service

IBM Informix JDBC Connection Long Password Denial Of Service Vulnerability

IBM Informix Multiple Vulnerabilities

Icecast Appended Character Denial-of-Service

Kyocera 3830 Printer Unauthorized Access Vulnerability

MailEnable HTTPMail Authorization Buffer Overflow

MailEnable SMTP NTLM Authentication Buffer Overflow

MySQL Database COM_TABLE_DUMP Buffer Overflow

NetWin Dmail Dlist.exe Authentication Bypass

NIPrint LPD Buffer Overflow

Novell Border Manager Audit Trail Proxy DoS

Novell FTP Denial-of-Service

Novell NetMail IMAPD Command Continuation Heap Overflow

Novell Netware FTP Null Value Denial-of-Service

Oracle 8i/9i TNS Listener SERVICE_CURLOAD Denial-of-Service

Oracle Database Server Default Credentials

Oracle8i TNS Listener dbsnmp Denial-of-Service

PHP Zend Multiple Vulnerabilities

PlatinumFTPserver Denial-of-Service

SNMP Writable Community Strings

Sun Java System Directory Server LDAP Search Request Denial Of Service Vulnerability

- Symantec Antivirus Remote Code Execution
- Symantec pcAnywhere Pre-Authentication Heap Overflow Vulnerability
- Symantec Veritas Backup Exec Authentication Overflow
- Symantec Veritas Backup Exec Status Denial Of Service
- Symantec Veritas NetBackup Remote Code Execution
- Symantec Veritas NetBackup vmd Shared Library Buffer Overflow
- Telnet Daemon AYT Memory Overwrite
- TFTP File Disclosure
- TFTP Server Long Filename Buffer Overflow Vulnerability
- Trend Micro OfficeScan Denial-of-Service

Network

- 3com OfficeConnect DSL Router Denial-of-Service
- Asterisk SDP Excessive RTP Payloads Overflow
- Asterisk SIP Channel Driver Pedantic Mode Remote Denial-of-Service Vulnerability
- Asterisk Skinny Channel Driver Remote Denial-of-Service Vulnerability
- Asterisk Stack Buffer Overflows in SIP Channel's T.38 SDP Parsing Code
- Check Point VPN-1 ASN.1 Decoding Heap Overflow Vulnerability
- Cisco CatOS Telnet AYT Memory Overwrite
- Cisco HTTP Question Mark Denial-of-Service
- Cisco IOS SNMP Denial-of-Service
- Cisco ONS FTP/Telnet Denial-of-Service
- Cisco Secure ACS web server arbitrary code execution
- Cisco VoIP Phone Stream Request Denial-of-Service
- SNMPv1 Long Community Name Buffer Overflow
- VxWorks FTP Denial-of-Service

Raw Socket

- Raw Socket Test Host Name Not Available
- Raw Socket Test ICMP Replies Received
- Raw Socket Test ICMP Timestamp Request
- Raw Socket Test IP Identification Value Randomness
- Raw Socket Test Many Open TCP Ports Detected
- Raw Socket Test Others Flag Detected

UNIX

- BSD FTP Glob Expansion Buffer Overflow
- BSD Line Printer Daemon Vulnerability
- CDE DTLogin X-Windows XDMCP Double Free
- CDE dtspcd Buffer Overflow
- GAMSoft TelSrv Long Username Denial of Service
- Gnome libgtop_daemon Vulnerability
- Hewlett Packard HP-UX ftpd PASS Vulnerability
- Hewlett Packard HP-UX ftpd REST Memory Disclosure
- Hewlett Packard HP-UX XFS Buffer Overrun
- ISC BIND 8.x OPT Denial-of-Service
- knfsd NFS server Negative Size Denial of Service
- Linux NFS xlog Off By One
- LPRng Format String
- NTPD Buffer Overflow
- Pluggable Authentication Modules Long User Vulnerability
- Postfix Address Resolver Parsing Denial-of-Service
- ProFTPD MKDIR Remote Buffer Overflow
- QPOP Buffer Overflow
- SGI IRIX 6.x ttdbserverd Buffer Overflow
- SGI IRIX Default Accounts Without a Password
- Sun KCMS Profiles Directory Traversal
- Sun Solaris /bin/login Authentication Bypass
- Sun Solaris cachefsd Memory Overwrite
- Sun Solaris Calendar Manager rpc.cmsd Buffer Overflow
- Sun Solaris fs.auto Buffer Overflow
- Sun Solaris nisd Buffer Overflow
- Sun Solaris RPC sadmind Buffer Overflow
- Sun Solaris RPC snmpXdmid Remote Overflow
- Sun Solaris RPC ttdbserverd Buffer Overflow
- Sun Solaris RPC XDR Library Routines Integer Overflow
- Sun Solaris RPC xdr_array cmsd Buffer Overflow

- Sun Solaris RPC xdr_array dmispd Buffer Overflow
- Sun Solaris SNMP Subagent Vulnerability
- Sun Solaris snmpdx Buffer Overflow
- Sun Solaris Telnet Login Buffer Overflow
- Sun Solaris ToolTalk Server Heap Corruption
- Sun Solaris X Font Server (xfs) Buffer Overflow Vulnerabilities
- Sun Solaris ypbind Buffer Overflow
- Sun Solaris yppasswd Buffer Overflow
- SuSE Linux in.identd Denial of Service
- SuSE Linux rpc.kstatd Vulnerability
- ToolTalk RPC Service Denial-of-Service Vulnerability
- University of Washington (UW) IMAP Buffer Overflow
- WU-FTPD Buffer Overflow
- WU-FTPD File Globbing Heap Corruption

Web

Windows

- (MS02-006) Microsoft Windows NT 4.0 SNMP Buffer Overflow (314147)
- (MS02-018) Microsoft IIS 5.0 FTP Denial-of-Service (Q319733)
- (MS02-018) Microsoft Windows 2000 MSDTC Denial Of Service (Q319733)
- (MS02-056) Microsoft SQL Server Hello Buffer Overflow (Q316333)
- (MS03-026) Microsoft Windows RPC DCOM Buffer Overflow (Intrusive)
- (MS03-049) Microsoft Windows 2000 Workstation Service Buffer Overflow (Intrusive)
- (MS03-049) Microsoft Windows XP Workstation Service Buffer Overflow (Intrusive)
- (MS99-003) Microsoft IIS 3.0 and 4.0 FTP NLST Overflow
- Windows DNS Server Service RPC Vulnerability (Intrusive)

Wireless Vulnerabilities

Wireless

Cisco Aironet Wireless Access Point Telnet Denial of Service

Windows Vulnerabilities

Baseline

- Windows Policy Baselining

Windows

(MS06-070) Microsoft Workstation Service Memory Corruption Vulnerability (924270)

(MS08-067) Microsoft Windows Server Service Vulnerability Intrusive (958644)

Microsoft Windows SMB2.0 Negotiate Protocol Request Out-Of-Bounds Dereference Vulnerability

Microsoft Windows spoolss Remote Denial of Service

Shell Vulnerabilities

Baseline

Unix Policy Baselining

Red Hat Enterprise Linux Security Policy/Options

Red Hat Enterprise Linux AT Subsystem Access

Red Hat Enterprise Linux Cron Access

Red Hat Enterprise Linux Crontab Referenced File Permissions

Red Hat Enterprise Linux Current Directory Entry In Path Environment Variable

Red Hat Enterprise Linux Current Directory Entry Not At End Of Path Environment Variable

Red Hat Enterprise Linux Device Files Found

Red Hat Enterprise Linux Device Files In Home Directories

Red Hat Enterprise Linux Expired Password

Red Hat Enterprise Linux Exported NFS Directory Secure Option Policy

Red Hat Enterprise Linux File ACL Policy

Red Hat Enterprise Linux File Content Search

Red Hat Enterprise Linux File Group Ownership

Red Hat Enterprise Linux Files Or Directories With No Owner

Red Hat Enterprise Linux Files Owned By Disallowed Groups

Red Hat Enterprise Linux Files Owned By Disallowed Users

Red Hat Enterprise Linux Files With Sticky Bit Set

Red Hat Enterprise Linux Files With Uneven Permissions

Red Hat Enterprise Linux GECOS Field Password Disclosure

Red Hat Enterprise Linux Group Writable Directories In Path Environment Variable

Red Hat Enterprise Linux Group writable files

Red Hat Enterprise Linux Group Writable User Files

Red Hat Enterprise Linux Hidden Directories

- Red Hat Enterprise Linux MD5 Hash Value Mismatch
- Red Hat Enterprise Linux Minimum Umask Policy
- Red Hat Enterprise Linux NFS Exported Directory Unrestricted Root Access
- Red Hat Enterprise Linux Prohibited Files
- Red Hat Enterprise Linux Report Remote Account Access
- Red Hat Enterprise Linux Sendmail Restricted Shell
- Red Hat Enterprise Linux Setgid Files
- Red Hat Enterprise Linux Setuid Files
- Red Hat Enterprise Linux Startup File Contents
- Red Hat Enterprise Linux Startup File Permissions
- Red Hat Enterprise Linux Suspicious File Names
- Red Hat Enterprise Linux Unsuccessful Su Attempts Not Logged
- Red Hat Enterprise Linux User Account Password Match
- Red Hat Enterprise Linux User Account Password Matches User Account Name
- Red Hat Enterprise Linux User Directories Before System Directories In Path Environment Variable
- Red Hat Enterprise Linux User Setuid/Setgid Files
- Red Hat Enterprise Linux Username/Password Match
- Red Hat Enterprise Linux World Writable Directories in PATH
- Red Hat Enterprise Linux World Writable Directories Without Sticky Bit
- Red Hat Enterprise Linux World Writable Files
- Red Hat Enterprise Linux World Writable User Files

Solaris Security Policy/Options

- Sun Solaris AT Subsystem Access
- Sun Solaris Cron Access
- Sun Solaris Crontab Referenced File Permissions
- Sun Solaris Current Directory Entry In Path Environment Variable
- Sun Solaris Current Directory Entry Not At End Of Path Environment Variable
- Sun Solaris Device Files In Home Directories
- Sun Solaris Device Files Not In /dev Directory
- Sun Solaris Expired Password
- Sun Solaris File ACL Policy

Sun Solaris File Content Search

Sun Solaris Files Not Listed in Template

Sun Solaris GECOS Field Password Disclosure

Sun Solaris Group owners disallowed

Sun Solaris Group Ownership

Sun Solaris Group Writable Directories In Path Environment Variable

Sun Solaris Group Writable Files

Sun Solaris Group Writable User Files

Sun Solaris Hidden Directories

Sun Solaris Idle Accounts

Sun Solaris Invalid Home Directory

Sun Solaris MD5 Hash Value Mismatch

Sun Solaris Minimum Umask Policy

Sun Solaris Owners Disallowed

Sun Solaris RBAC Based Access

Sun Solaris Remote Only Accounts

Sun Solaris Sendmail Restricted Shell

Sun Solaris Setgid files

Sun Solaris Setuid files

Sun Solaris Startup File Contents

Sun Solaris Startup File Permissions

Sun Solaris Sticky Files

Sun Solaris Suspicious File Names

Sun Solaris Uneven File Permissions

Sun Solaris Unowned Directories/Files

Sun Solaris Unused Accounts

Sun Solaris User Account Password Match

Sun Solaris User Account Password Matches User Account Name

Sun Solaris User Accounts Login Without Password

Sun Solaris User Directories Before System Directories In Path Environment Variable

Sun Solaris User Password Equals Username

Sun Solaris User Setuid/Setgid Files

- Sun Solaris World Writable Directories In Path Environment Variable
- Sun Solaris World Writable Directories Without Sticky Bit
- Sun Solaris World Writable Files
- Sun Solaris World Writable User Files

Web Vulnerabilities

Authentication

- Cross-Site Request Forgery (CSRF) Potentially Insecure Prevention Measure
- Cross-Site Request Forgery (CSRF)
- Possible Authentication bypass via Forced Browsing
- Sensitive Form Begins at an Unencrypted Page
- Unencrypted Login Information Disclosure

CGI attacks

- Multiple Vendor Phf Cgi Arbitrary Command Execution

Cross Site Scripting

- Fusebox Index.CFM Cross-Site Scripting Vulnerability
- Persistent Web Application Cross Site Scripting
- phpinfo() XSS Vulnerability
- Web Application Cross Site Scripting

Database

Potentially Exploitable Database Error Message

Directory Traversal

HTTP Header

- HTTP Response Splitting

Information Leakage

- AutoComplete attribute is missing
- Database Error Disclosure
- DB2 Database Error Disclosure Vulnerability
- File Downloads Over Non-HTTPS link
- Http Trace / Track Methods Allowed
- Improper Error Handling
- MS Access Database Error Disclosure Vulnerability
- MS SQL Database Error Disclosure Vulnerability

- MySQL Database Error Disclosure Vulnerability
- Oracle Database Error Disclosure Vulnerability
- Possible SQL Injection Vulnerability (Generic Database Error Disclosure)
- Sensitive information possibly sent via HTTP GET Method
- VBScript Error Disclosure Vulnerability

Multiple Vulnerabilities

- User specified URL redirection (Open Redirect)

PHP Attacks

- PHP Directive 'allow_url_fopen' is Enabled
- PHP Directive 'register_globals' is Enabled
- PHP Remote File Inclusion Vulnerabilities (RFI)
- Web Server Info.php / Phpinfo.php Detection

Server Attacks

- Apache Multiviews Feature Arbitrary Directory Listing
- IIS .ida ISAPI Filter Enabled
- OS Command Injection

Server Side Code Injection

SQL Injection

- Blind MS SQL Injection Vulnerability
- MarketLive - SQL Injection - (display.do?ruleID)
- MarketLive - SQL Injection - (display.do?ruleID) - Encoded
- MarketLive - SQL Injection - (display.do?ruleID) - Filtered
- Potentially Exploitable SQL Blind Injection
- SQL Injection Vulnerability in MySQL Database
- SQL Injection Vulnerability in Oracle Database
- SQL Injection Vulnerability in SQL Server
- SQL Query Found

WebServer

- Base_path Parameter Remote File Include Vulnerability
- Local File Include Vulnerability
- Microsoft Iis Webdav Unicode Request Directory Security Bypass
- WebDAV Detection

Anexo 2

Servicios encontrados en la red con algunas definiciones y recomendaciones:

Nombre del servicio	Puerto Estándar	Descripción
File Transfer Protocol Control	21 - tcp	El FTP (File Transfer Protocol) se utiliza para transferir archivos entre ordenadores a través de una red. Muchos servidores FTP son vulnerables a los ataques que podría permitirle a un usuario remoto con acceso de administrador. Ejecute el servicio FTP con el uso de envolturas TCP para controlar el acceso al FTP.
Secure Shell	22 –tcp	El SSH es utilizado como un sustituto seguro de texto plano y servicios de inicio de sesión interactivos como rlogin, rsh y telnet. SSH utiliza múltiples algoritmos de cifrado para garantizar la integridad de los datos y la seguridad. Le recomendamos que ssh sea utilizado como un reemplazo de cualquier servicio de acceso sin cifrar. También le recomendamos que utilice las envolturas TCP para restringir quién puede conectarse a su servidor SSH. Las envolturas TCP son típicamente un paquete estándar en la mayoría de Unix.
Hyper Text Transfer Protocol	80 - tcp	La WWW (World Wide Web) permite la transferencia de páginas web de marcado de hipertexto lenguaje (HTML) para ser interpretado por un navegador web. Hay muchas vulnerabilidades de seguridad en aplicaciones web y servidores que pueden permitir a un usuario acceso remoto al sistema de alguna manera. La mejor recomendación es auditar el código de la aplicación web, la búsqueda de debilidades en el diseño de la seguridad. Además, debe eliminar cualquier programa innecesario y archivos del servidor para reducir su vulnerabilidad.
Windows RPC service	135 - tcp	El puertoTCP135, similar al puertoUDP135, permite a un atacante ver información del sistema sin autenticar. La información como los servicios instalados internamente, el direccionamiento IP puede ser descubierto y aprovechado para ganar más acceso. Si es un servicio esencial en su organización(es decir, -MSExchange requiere ella), debe restringir la fuente de la que se puede conectar al puerto a través de un mecanismo de filtrado de puertos tales como un firewall.
NETBIOS NameService	137 - udp	PuertoUDP137le permite a un atacante consultar el servicio de nombres de Windows. Con esta información, un atacante puede aprender acerca de los nombres de sistema de Windows y aprovechar la información para nuevos ataques
NETBIOS SessionService	139 - tcp	Le permite a un atacante conectarse remotamente a los sistemas .Netbioses sin duda la amenaza más grande en la existencia de Windows. Debe restringir el acceso a este puerto siempre que sea posible. Para restringir el acceso a este

		puerto se puede 1) Inhabilitar el servicio WINS TCP / IP, 2) Activar un dispositivo de filtrado de paquetes, o 3) Activar un firewall.
Simple Network Management Protocol	161 - udp	Se utiliza para administrar y controlar dispositivos en una red. Se recomienda usar la versión 3 por la criptografía que ofrece y así asegurar la comunicación.
HTTP over SSL	443 - tcp	Es un protocolo de seguridad que proporciona privacidad en las comunicación es a través de Internet.
Win2k Server Message Block	445 - tcp	ServicioasociadoconWindows2000SMB. Almacena y mantiene toda la información relacionada de los sistemas de usuarios, grupos, permisos, etc., así como permitir a un usuario asignar compartidos, cuotas y otras funciones
Spooler	515 - tcp	La cola de impresión en línea permite a los usuarios remotos para utilizarlos recursos de impresión. Una vulnerabilidad fue recientemente descubierta en algunas implementaciones de la cola de impresión en línea en los sistemas Linux. Las Listas de control de acceso son la mejor línea de defensa contra los ataques. Asegúrese de mantener el software actual y sólo se ejecuta este servicio si es necesario.
VMwareAuthenticationDaemon	912 - tcp	VMware servicio de autenticación
H323 Host CallSetup	1720 - tcp	h323hostcall
RemotelyAnywhere	2000 - tcp	Servicio de administración, acceso y control remoto
Microsoft Terminal Services	3389 - tcp	Se recomienda que limite el acceso a este servicio a través de filtrado de paquetes de routers y firewalls
PossibleTrojan - NetBus	12345 - tcp	NetBus es un troyano de puerta trasera. Permite a un atacante remoto tomar el control completo del sistema donde se está ejecutando. Un atacante puede ver el escritorio, tomar el control del teclado y el ratón, de los programas que se ejecutan en el sistema de troyanos, etc