

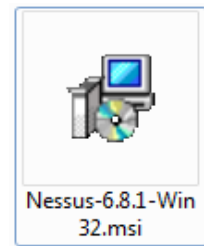
Uso de herramienta Nessus

MF0487_3: Auditoría de Seguridad Informática

1ª Parte: Nessus

Versión Instalada: Nessus-6.8.1-Win32 (Home)

Acceso por el navegador: <https://localhost:8834/>

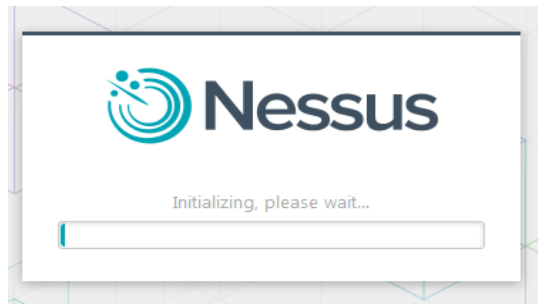


Todos los programas -> Tenable Network Security -> Nessus -> Nessus Web Client

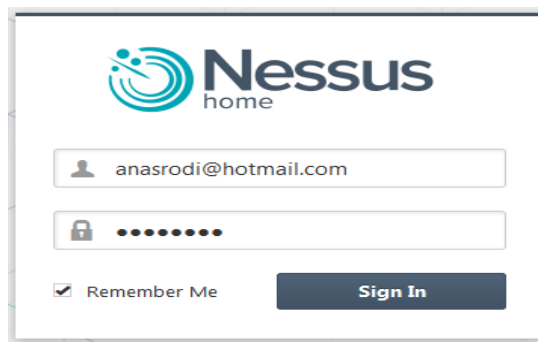
(Hay que añadirlo como excepción para poder utilizarlo)

Notas

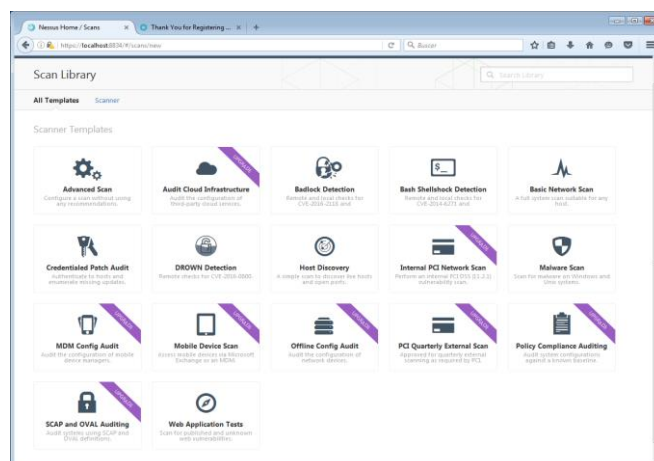
- Hay que registrarse para que nos den un código de activación.
- Si tienes instalada alguna versión es mejor desinstalarla e instalar la nueva.
- Esta es la pantalla que sale después de haberlo activado y de descargar los plugins que necesita.



Página de inicio



Nessus escanea de acuerdo a unas plantillas o templates, según la versión que tengamos instalada. Elegiremos dependiendo de lo que queramos escanear.



Podemos hacer varios tipos de escaneo, desde uno básico a un “The Badlock vulnerability (CVE-2016-2118 and CVE-2016-0128)”. Depende de la versión de Nessus que tengamos instalada.

En este caso elegimos un escaneo básico.

Settings / Basic / General

Name	<input type="text" value="Escaneo Basico"/>
Description	<input type="text" value="Escaneo Basico"/>
Folder	<input type="text" value="My Scans"/>
Targets	<div>192.168.1.0/24</div>

[Upload Targets](#) [Add File](#)

Lo podemos configurar cuando hacerlo y que nos envíe un mensaje con los resultados.

Settings / Basic / Schedule

Enable Schedule ☒

Launch	<input type="text" value="Once"/>
Starts On	<input type="text" value="08/07/2016"/> <input type="text" value="20:30"/>
Timezone	<input type="text" value="(UTC) Casablanca"/>
Summary	Once on Sunday, August 7th, 2016 at 8:30 PM

Filtrando incluso por tipo de vulnerabilidad.

Settings / Basic / Notifications

Notifications will not be sent until your SMTP Server is configured.

Email Recipient(s)

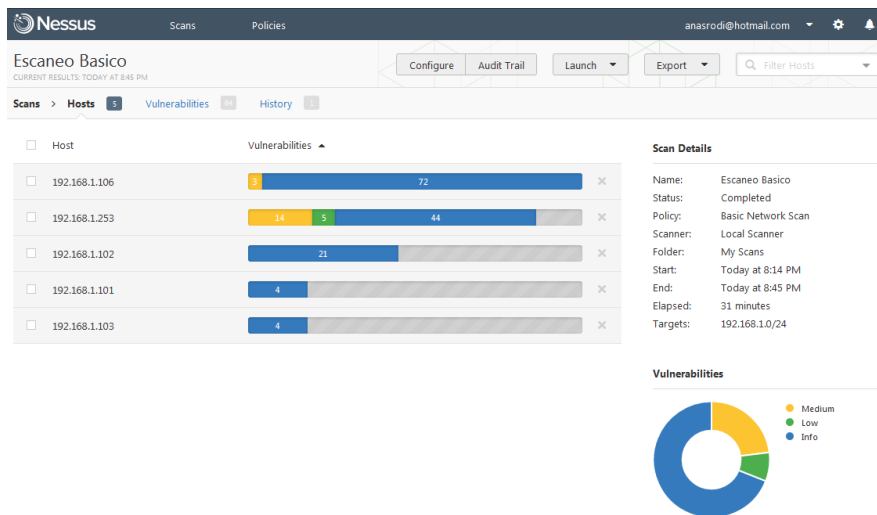
Result Filters

Match of the following:

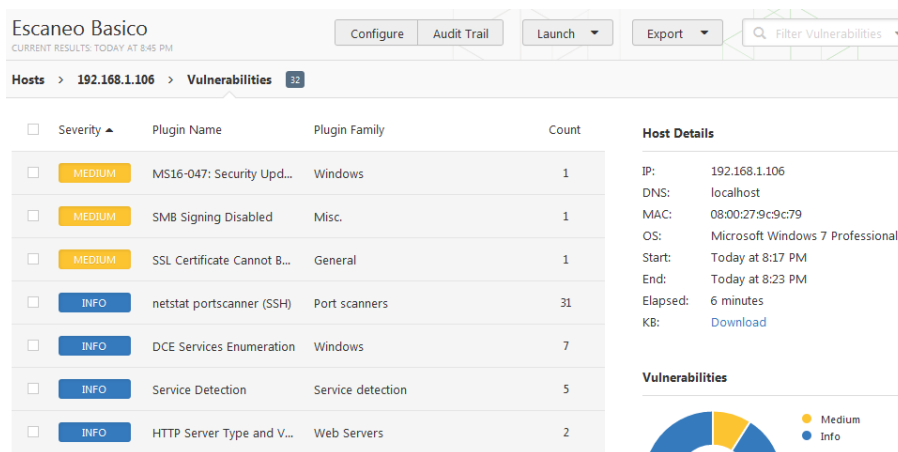
<input type="text" value="CVSS v3.0 Vector"/>	<input type="text" value="is equal to"/>	<input type="text" value="TEXT"/>	<input type="text" value="X"/>
<input type="text" value="Bugtraq ID"/>	<input type="text" value="is equal to"/>	<input type="text" value="NUMBER"/>	<input type="text" value="X"/>
<input type="text" value="Malware"/>	<input type="text" value="is equal to"/>	<input type="text" value="true"/>	<input type="text" value="X"/>

[Add Filter](#)

Proceso de escaneo – Equipos que ha encontrado con sus vulnerabilidades

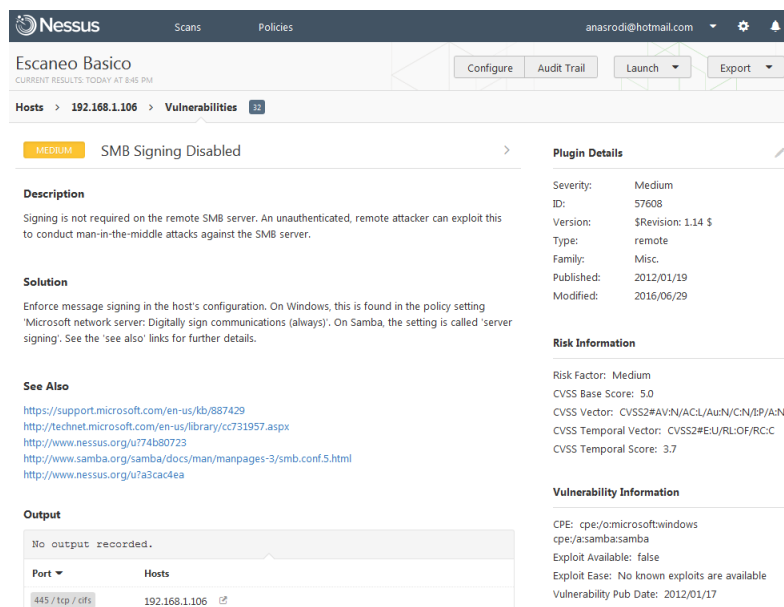


Detalle de uno de los equipos



Ha detectado tres niveles de vulnerabilidad.

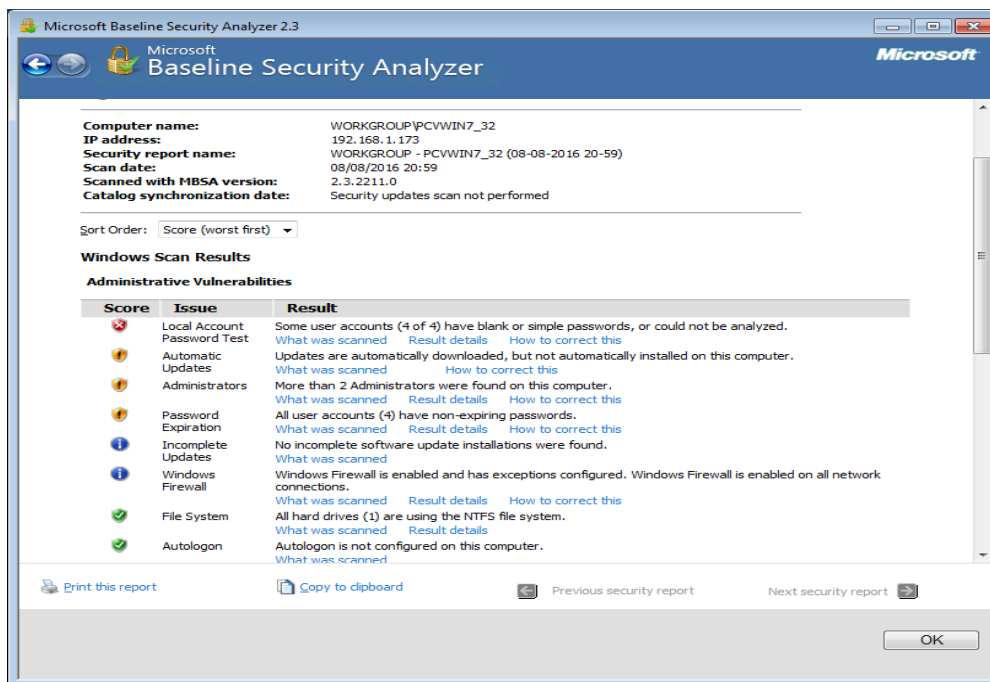
Detalle de una de las vulnerabilidades. Con su descripción y posible solución.



Microsoft Baseline Security Analyzer

Una sencilla herramienta con la que puedes realizar un análisis automático de tu sistema en busca de posibles vulnerabilidades y fallos de seguridad.

Encuentra errores de administración y fallos de seguridad comunes, pero no por ello menos importantes, tales como falta de actualizaciones del sistema, contraseñas caducadas, existencia de más de una cuenta de administrador o de una cuenta de invitado, qué directorios se comparten y con quién, posibles fallos en Internet Explorer, Office, SQL Server, Internet Information Server, etc.



Pulsando sobre el resultado nos da el detalle de la vulnerabilidad.

Microsoft Baseline Security Analyzer

Local Account Passwords

Check Description

This check identifies any blank or simple passwords for each local user account on the computer. This check is not performed on domain controllers.

Microsoft® Windows® Server 2008, Microsoft® Windows® Server 2003, Windows Vista, Windows XP, and Windows 2000 operating systems all require user authentication through passwords. In general, users are permitted to choose their own passwords. The security of their account depends on the choice of the password. This check enumerates all user accounts and checks for the following password conditions:

- Password is blank.
- Password is the same as the user account name.
- Password is the same as the computer name.
- Password uses the word "password."
- Password uses the word "admin" or "administrator."

This check also notifies you of any accounts that have been disabled or are currently locked out.

For Windows XP computers that use simple file sharing (includes Windows XP Home Edition and Windows XP Professional computers not joined to a domain), MBSA will not flag local accounts with blank passwords. To help protect users who do not password-protect their accounts, Windows XP Professional accounts without passwords can only be used to log on at the physical computer console. By default, accounts with blank passwords can no longer be used to log on to the computer remotely over the network, or for any other logon activity except at the main physical console logon screen.

Notes

- Microsoft Baseline Security Analyzer does not attempt to crack passwords during this check, and instead attempts a password change request using each condition in the preceding list. Account lockout policy counts will be reset if in effect on the scanned computer.

Additional Resources

[What's New in Security for Windows XP Professional and Windows XP Home Edition](#)

[Creating Strong Passwords](#)

Ejemplo de Vulnerabilidad 12 de abril de 2016

<http://www.redeszone.net/2016/04/12/desvelan-la-informacion-tecnica-badlock-la-vulnerabilidad-samba/>

“Hace 3 semanas, uno de los responsables del desarrollo de Samba, protocolo de intercambio de archivos multiplataforma desarrollado para facilitar la comunicación entre Windows, Linux y Mac OS X, informaba de la existencia de una vulnerabilidad crítica en el protocolo SMB/CIFS, denominada como **Badlock**.

Esta vulnerabilidad podía comprometer la seguridad de las conexiones que se realizaran a través de él y, por motivos de seguridad, ni los responsables de Samba ni Microsoft han dado ninguna información sobre la vulnerabilidad, la cual ha permanecido totalmente en secreto, hasta hoy. – Ver mas en:

<http://www.redeszone.net/2016/04/12/desvelan-la-informacion-tecnica-badlock-la-vulnerabilidad-samba/#sthash.13ytmaBr.dpuf>

El uso conjunto de estas vulnerabilidades puede permitir a un atacante **realizar ataques MITM** para capturar el tráfico entre el cliente y el servidor o **ataques DoS** para dejar sin servicio a los usuarios.

Las versiones afectadas (prácticamente todas) son: 3.6.x, 4.0.x, 4.1.x, desde la 4.2.0 a la 4.2.9, desde la 4.3.0 a la 4.3.6 y la 4.4.0. Según **CVSS**, la vulnerabilidad ha sido considerada como de **gravedad alta**, con una nota de **7.1 sobre 10.**”

2ª Parte:

Escaneo de un Linux Ubuntu Virtualizado.

The screenshot shows the Nessus web interface for creating a new scan. The breadcrumb trail is 'New Scan / Basic Network Scan'. The left sidebar has tabs for 'Scan Library', 'Settings', and 'Credentials'. Under 'Settings', there are sub-tabs for 'BASIC', 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'BASIC' tab is selected, and within it, the 'General' sub-tab is active. The main form area is titled 'Settings / Basic / General' and contains the following fields:

- Name:** Linux Ubuntu Escaneo Básico
- Description:** Linux Ubuntu Escaneo Básico
- Folder:** My Scans (dropdown menu)
- Targets:** 192.168.1.72

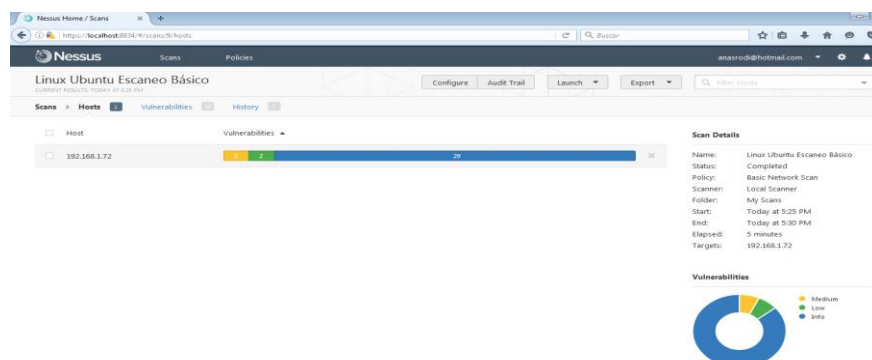
Preparamos el escaneo que queremos realizar: tipo, nombre, descripción, donde se guarda, objetivo del escaneo.

The screenshot shows the Nessus web interface for the 'Scans / My Scans' page. The table lists the following scans:

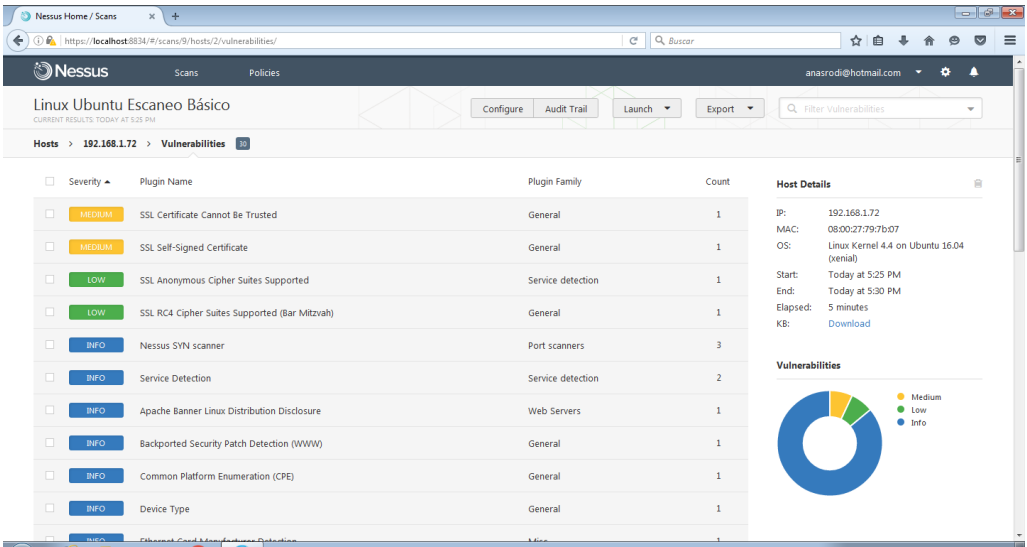
Name	Schedule	Last Modified
Red ICSE	On Demand	August 29
Damn Vulnerable Linux	On Demand	August 29
Linux Ubuntu Escaneo Avanzado	On Demand	August 26
Linux Ubuntu Escaneo Básico	On Demand	August 26
Escaneo Basico	On Demand	August 7

Dicho escaneo lo podemos programar o iniciarlo manualmente.

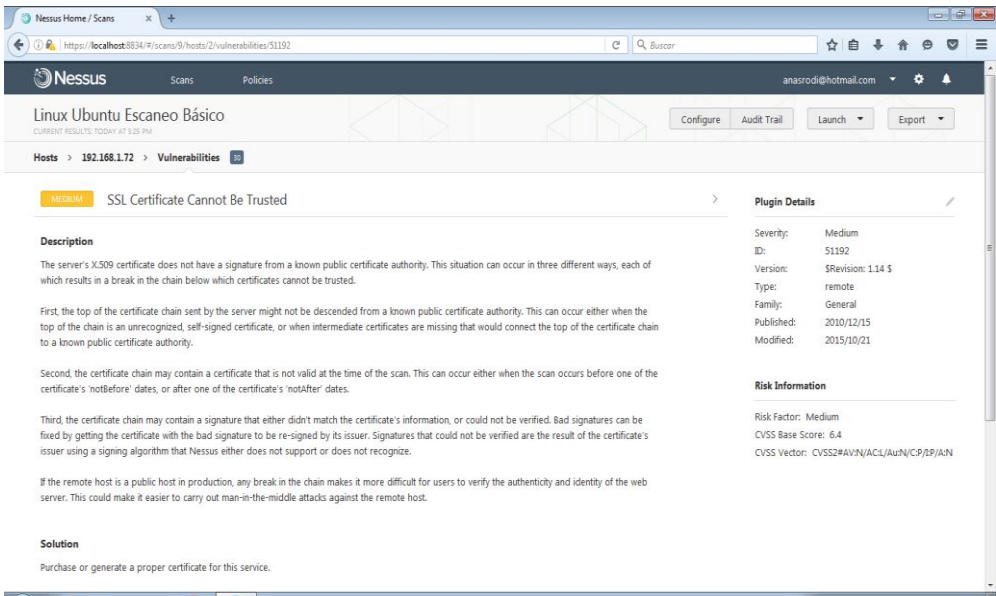
Resultado del Escaneo Básico de la máquina con Ubuntu.



1er Detalle del Escaneo



2º Detalle de una de las vulnerabilidades de tipos medio detectado por Nessus.



Solution

Purchase or generate a proper certificate for this service.

Output

The following certificate was at the top of the certificate chain sent by the remote host, but is signed by an unknown certificate authority :

|-Subject : CN=ubuntu
|-Issuer : CN=ubuntu

Port	Hosts
25 / tcp / smtp	192.168.1.72

Informe

1º Vulnerabilidad. Tipo Medio.

Certificado SSL no se puede verificar.

Descripción

El certificado X.509 del servidor no tiene una firma de una autoridad de certificación pública conocida. Esta situación puede ocurrir de tres maneras diferentes, cada una de las cuales produce una ruptura en la cadena de certificados por debajo del cual no se puede confiar.

En primer lugar, la parte superior de la cadena de certificados enviados por el servidor no podría ser descendiente de una autoridad de certificación pública conocida. Esto puede ocurrir ya sea cuando la parte superior de la cadena es un certificado reconocido, con firma, o cuando los certificados intermedios faltan que conectaría la parte superior de la cadena de certificados de una entidad de certificación pública conocida.

En segundo lugar, la cadena de certificados puede contener un certificado que no es válido en el momento de la exploración. Esto puede ocurrir ya sea cuando se produce la exploración antes de una de las fechas del certificado 'NotBefore', o después de una de las fechas del certificado 'notAfter'.

En tercer lugar, la cadena de certificados puede contener una firma que, o bien no se ha encontrado la información del certificado, o no pudo ser verificada. Malas firmas pueden ser fijados por conseguir el certificado con la firma defectuosa que ser re-firmado por su emisor. Las firmas que no pudieron ser verificados son el resultado del emisor del certificado utilizando un algoritmo de firma que Nessus no es compatible o no reconoce.

Si el host remoto es un sistema público de producción, cualquier ruptura en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría hacer que sea más fácil de llevar a cabo ataques man-in-the-middle contra el host remoto.

Solución

Adquirir o generar un certificado adecuado para este servicio.

2ª Vulnerabilidad

También relacionada con la CA.

SSL Self-Signed Certificate

Descripción

La cadena de certificados X.509 para este servicio, no está firmado por una autoridad de certificación reconocida. Si el cliente remoto es un sistema público, anula el uso de SSL. Cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

Tenga en cuenta que este plugin no comprueba cadenas de certificados que terminan en un certificado que no es auto-firmado, pero está firmado por una autoridad de certificación reconocida.

Solución Adquirir o generar un certificado adecuado para este servicio.

<https://documentation.cpanel.net/pages/viewpage.action?pagelid=6455789#Preguntasfrecuentesydiagn%C3%B3sticodeproblemasobreSSL-Laverificaci%C3%B3ndeidentidad>

3ª Vulnerabilidad

Linux Ubuntu Escaneo Básico

CURRENT RESULTS: TODAY AT 5:25 PM

Hosts > 192.168.1.72 > Vulnerabilities 30

LOW SSL Anonymous Cipher Suites Supported

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Errores comunes de seguridad en Apache

A continuación se describen soluciones para algunas de las notificaciones más comunes al realizar escaneos con herramientas VRA (Nessus, ScanAlert, etc) y/o Web-Servers Scanners.

1) SSL Anonymous Cipher Suites Supported

- Synopsis: The remote service supports the use of anonymous SSL ciphers.
- Description: El cliente remoto soporta The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.
- See also: <http://www.openssl.org/docs/apps/ciphers.html>

* Solución implementada:

Se agregó la directiva "SSLCipherSuite !ADH:HIGH:MEDIUM" en el file /etc/apache2/sites-available/ssl

4ª Vulnerabilidad

Nessus

Scans Policies

anasrodi@hotmail.com

Linux Ubuntu Escaneo Básico

CURRENT RESULTS: TODAY AT 5:30 PM

Hosts > 192.168.1.72 > Vulnerabilities 30

LOW SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

See Also

<http://www.nessus.org/u?217a3666>
<http://cr.jp.to/talks/2013.03.12/slides.pdf>

Plugin Details

Severity:	Low
ID:	65821
Version:	\$Revision: 1.9 \$
Type:	remote
Family:	General
Published:	2013/04/05
Modified:	2016/06/16

Risk Information

Risk Factor:	Low
CVSS Base Score:	2.6
CVSS Vector:	CVSS2#AV:N/AC:H/Au:N/C:P/IN/A:N
CVSS Temporal Vector:	CVSS2#E:ND/RL:OF/RC:C
CVSS Temporal Score:	2.3

Protocolos y cyphers vulnerables

Aplique los pasos detallados a continuación cuando en la lista de protocolos y cyphers soportados por un servidor que se realiza durante la prueba aparezca SSL 2.0, SSL 3.0, RC4, DES y ADH.

1. Añada (**o modifique**) las siguientes opciones mod_ssl a la configuración SSL/TLS del servidor web Apache
2. SSLProtocol all -SSLv2 -SSLv3
3. SSLHonorCipherOrder on
4. SSLCipherSuite
EECDH+AES:EDH+AES:RSA+AES:3DES:!RC4:!aNULL:!eNULL:!EXP:!MEDIUM:!LOW:!MD5
5. Vuelva a cargar la configuración de Apache

La tabla que se muestra a continuación contiene los nombres de los archivos de configuración correctos y los comandos de recarga en función del tipo de servidor que está utilizando.

<http://blog.cryptographyengineering.com/2013/03/attack-of-week-rc4-is-kind-of-broken-in.html>

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

5º Resto de las vulnerabilidades: informativas.

Por ejemplo

The screenshot shows the Nessus interface with the following details:

- Header:** Nessus Scans Policies
- Section:** Linux Ubuntu Escaneo Básico
- Sub-section:** Hosts > 192.168.1.72 > Vulnerabilities (30)
- Tab:** INFO Service Detection
- Description:** Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.
- Output:**
 - An SMTP server is running on this port.**

Port	Hosts
25 / tcp / smtp	192.168.1.72
 - A web server is running on this port.**

Port	Hosts
80 / tcp / www	192.168.1.72

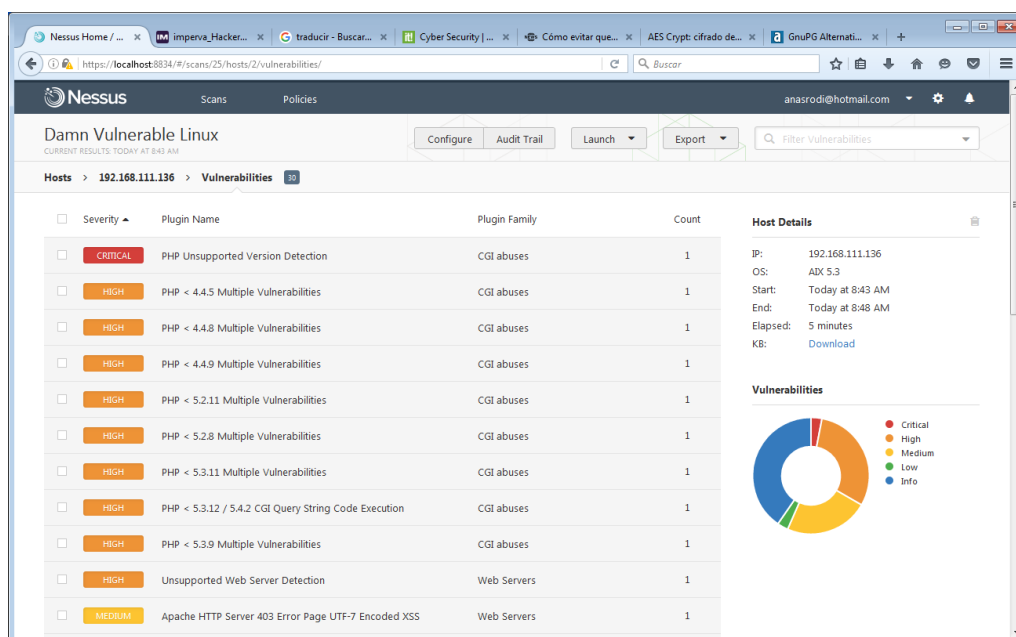
Nos dice que el puerto 25 y el puerto 80 están en funcionamiento.

25	SMTP	TELEcommunication NETwork, usado para envío de correo electrónico. Un puerto muy escaneado para aprovechar vulnerabilidades para el envío de SPAM. Asegúrate de validar usuarios para el envío de correo.
80	HTTP	Servidor Web. Utilizado para navegación web. Este servicio por si solo ya supone un riesgo. Suele ser escaneado y se las ingenian para encontrar nuevas entradas.

Prueba en Damn Vulnevable Linux



Hemos iniciado los servicios SSH y PHP, para ver si Nessus reconoce alguna vulnerabilidad en éstos.



Vemos que ha encontrado unas cuantas vulnerabilidades relacionadas con dichos servicios, aparte de otras vulnerabilidades tal como:

Damn Vulnerable Linux
CURRENT RESULTS TODAY AT 8:43 AM

Configure Audit Trail Launch Export

Hosts > 192.168.111.136 > Vulnerabilities 30

LOW X Server Detection

Description

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Output

Port	Hosts
6000 /tcp /x11	192.168.111.136

Plugin Details

Severity: Low
ID: 10407
Version: \$Revision: 1.37 \$
Type: remote
Family: Service detection
Published: 2000/05/12
Modified: 2013/01/25

Risk Information

Risk Factor: Low
CVSS Base Score: 2.6
CVSS Vector: CVSS2#AV:N/AC:H/Au:N/C:P/IN:A/N

Vulnerabilidad contemplada en la página del CCN.

<https://www.ccn-cert.cni.es/component/vulnerabilidades/view/242.html>

DEFENSA FRENTE A LAS CIBERAMENAZAS

Bienvenido Su búsqueda Abrir sesión

Inicio Sobre nosotros Gestión de incidentes Formación Guías Informes Herramientas ENS Empresas Seguridad al día Registro

ÚLTIMA HORA 29/08/2016 08:45
Primera botnet para Android controlada a través de Twitter

NIVEL DE ALERTA
MUY ALTO

Boletines de Vulnerabilidades

Vulnerabilidad en X server de Open Unix y UnixWare

Clasificación de la vulnerabilidad

Propiedad	Valor
Nivel de Confianza	Oficial
Impacto	Confidencialidad
Dificultad	Experto
Requerimientos del atacante	Acceso remoto con cuenta

Información sobre el sistema

Propiedad	Valor
Fabricante afectado	GNU/Linux
Software afectado	SCO Open Unix 8.0.0 SCO UnixWare 7.1.1& 7.1.3

Descripción

Se ha descubierto una vulnerabilidad en el X server (X11 server) en Open Unix 8.0.0 y UnixWare 7.1.1 y 7.1.3. El directorio "/dev/x" y todos los ficheros que contiene tienen permisos de escritura y lectura. Esto puede permitir a un usuario local realizar una denegación de servicio u obtener información a la que no está autorizado. Se desconocen más detalles sobre esta vulnerabilidad.

Solución

Actualización de software
Aplique el parche proporcionado por el fabricante
<ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.4>

Identificadores estándar

Hay otras vulnerabilidades críticas como la primera. Podemos ver la descripción y la solución que da el propio Nessus.

Nessus Scans Policies anasrodi@hotmail.com

Configure Audit Trail Launch Export

Hosts > 192.168.111.136 > Vulnerabilities 30

CRITICAL PHP Unsupported Version Detection

Description

According to its version, the installation of PHP on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of PHP that is currently supported.

See Also

<http://php.net/eol.php>
<https://wiki.php.net/rfc/releaseprocess>

Output

Port	Hosts
80 /tcp /www	192.168.111.136

Plugin Details

Severity: Critical
ID: 58987
Version: \$Revision: 1.13 \$
Type: remote
Family: CGI abuses
Published: 2012/05/04
Modified: 2015/10/06

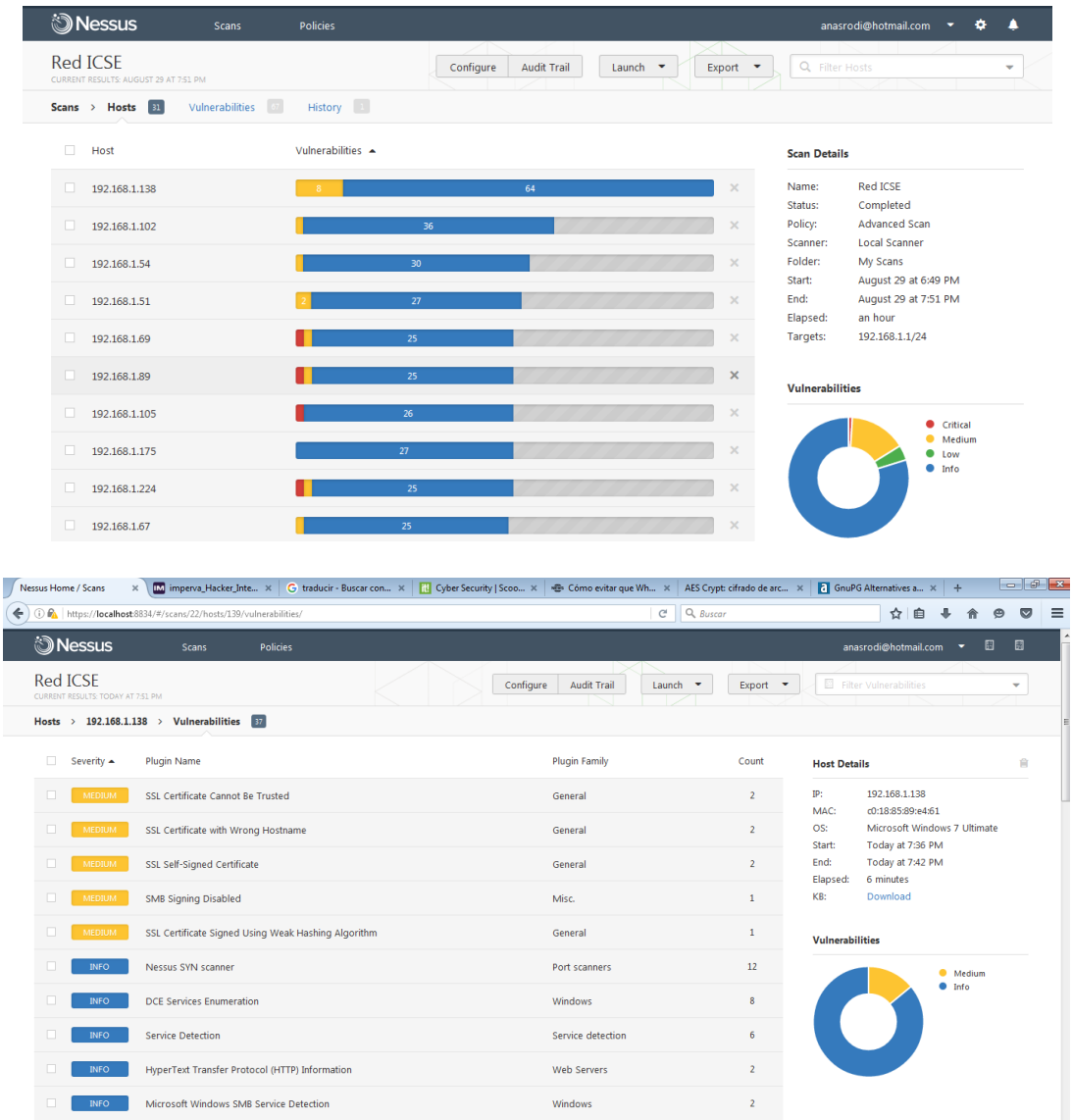
Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/IC:A/C

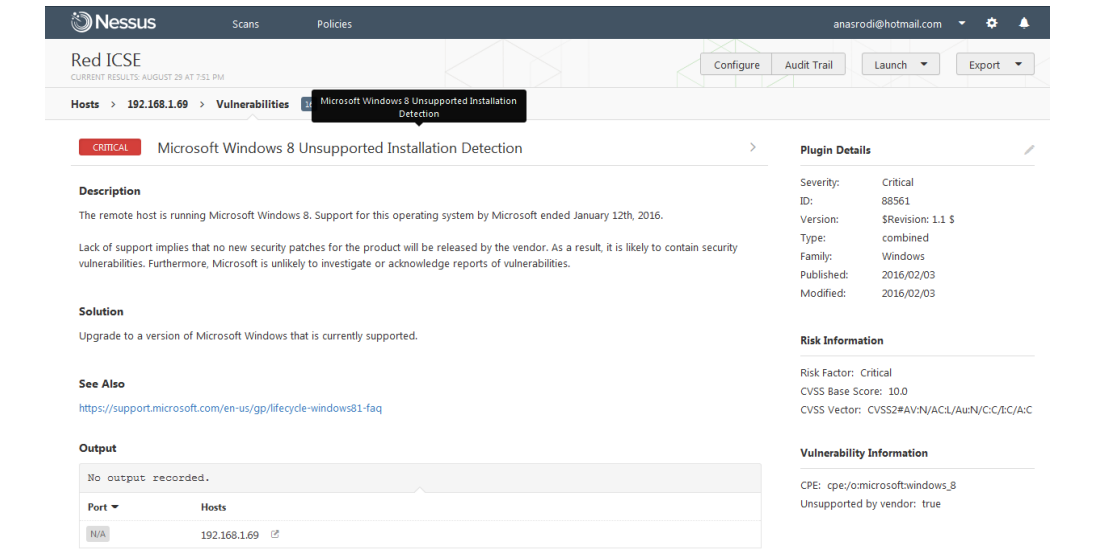
Vulnerability Information

CPE: cpe:/a:php:php
Unsupported by vendor: true

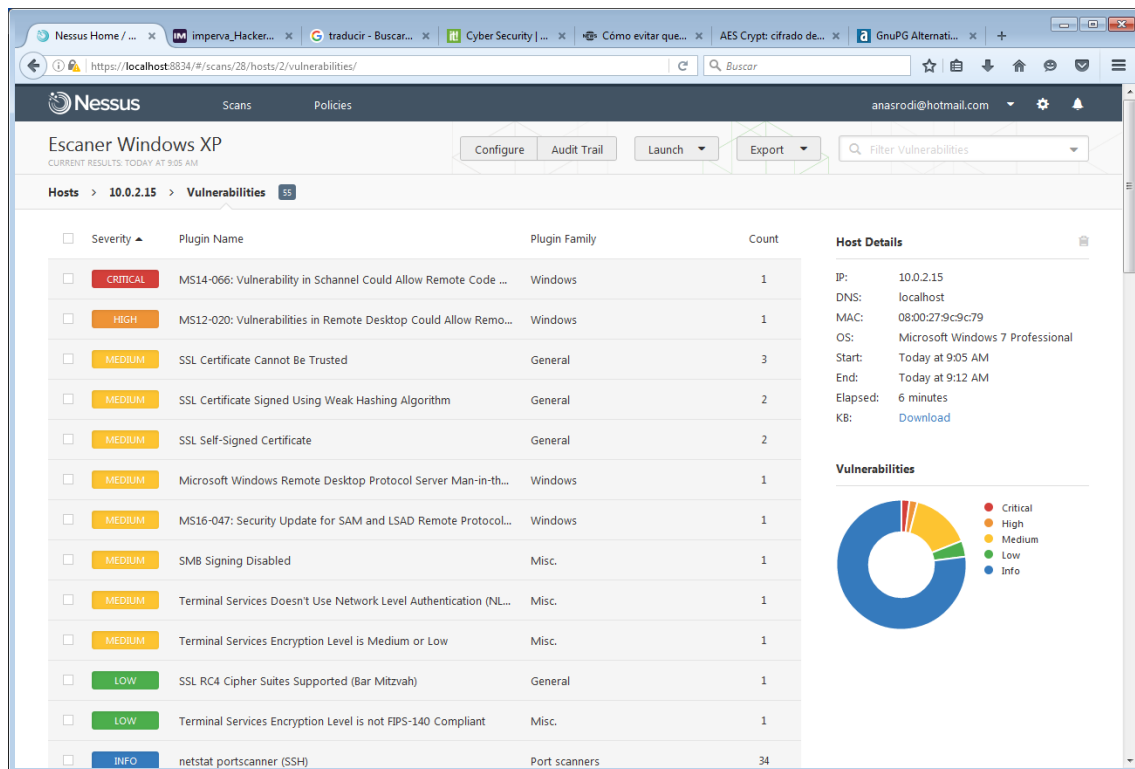
Escaneo Red ICSE



Vemos que existen varias vulnerabilidades críticas.



Escaneo de un sistema con Windows XP



Vemos que es un sistema con muchas vulnerabilidades.

Escaner Windows XP
CURRENT RESULTS: TODAY AT 9:05 AM

Hosts > 10.0.2.15 > Vulnerabilities

CRITICAL MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992...

Description

The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.

Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.

Solution

Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.

See Also

<https://technet.microsoft.com/library/security/ms14-066>

Output

No output recorded.

Port	Hosts
3389 / tcp / msrdp	10.0.2.15

Plugin Details

- Severity: Critical
- ID: 79638
- Version: \$Revision: 1.33 \$
- Type: remote
- Family: Windows
- Published: 2014/12/01
- Modified: 2016/08/15

Risk Information

- Risk Factor: Critical
- CVSS Base Score: 10.0
- CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
- CVSS Temporal Vector: CVSS2#E:ND/RL:OF/RC:C
- CVSS Temporal Score: 8.7

Vulnerability Information

- CPE: cpe:/o:microsoft:windows
- Exploit Available: true
- Exploit Ease: Exploits are available
- Patch Pub Date: 2014/11/11
- Vulnerability Pub Date: 2014/11/11

Microsoft ha descubierto una **vulnerabilidad grave** en su sistema que afecta a **todas las versiones de Windows**. Permite ejecutar códigos en los ordenadores afectados y acceder a los sistemas.

El parche dependiendo de la versión de vuestro sistema operativo. Disponible para **Win Server 2003, 2008, 2008 R2, 2012, 2012 R2, Win Vista, Win 7, Win RT, Win RT 8.1, Win 8 y Win 8.1**.

Sólo hay que acceder al enlace que os indicamos, **seleccionar el parche** que corresponde a **nuestro sistema operativo** y tras seleccionar el **idioma** de nuestro Windows (normalmente español) clic en **Descargar**. [Descargar parche MS14-066](#)

Description

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.

This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.

Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host.

Solution

Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2.

Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000.

See Also

<http://technet.microsoft.com/en-us/security/bulletin/ms12-020>

Output

No output recorded.

Port ▾	Hosts
3389 / tcp / msrdp	10.0.2.15 

Plugin Details

Severity: High
ID: 58435
Version: \$Revision: 1.27 \$
Type: remote
Family: Windows
Published: 2012/03/22
Modified: 2016/07/19

Risk Information

Risk Factor: High
CVSS Base Score: 9.3
CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C
CVSS Temporal Vector:
CVSS2#E:POC/RL:OF/RC:C
CVSS Temporal Score: 7.3
IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:remote_desktop_protocol
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: 2012/03/13
Vulnerability Pub Date: 2012/03/13

Exploitable With

Metasploit (MS12-020 Microsoft Remote Desktop Checker)
CANVAS (White_Phosphorus)
Core Impact

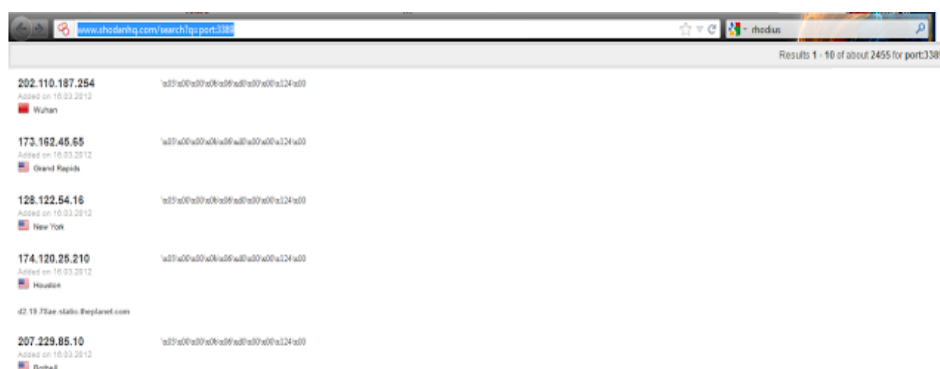
ANTECEDENTES

El 13 de marzo 2012, Microsoft hacia público en su boletín de seguridad, la detección de múltiples vulnerabilidades, de entre ellas destaca:

MS12-020: Boletín "crítico" que resuelve dos vulnerabilidades (CVE-2012-0002 y CVE-2012-0152) localizadas en el protocolo de Escritorio remoto (RDP), que no está habilitado por defecto en ningún sistema operativo Windows. El más grave de los problemas puede permitir la ejecución remota de código. Afecta a toda las familias de Windows. [[Hispacec](#)]

El RDP, permite a un usuario remoto tomar el control total del ordenador. Este servicio se encuentra activado por defecto en todos los Sistemas Operativos de Windows.

La importancia de esta vulnerabilidad, se debe sobre todo al gran número de usuarios / equipos que se encuentra afectados. Una búsqueda de equipos que tiene el puerto 3389 disponible (open) en Internet utilizando el servicio [SHODAN](#), refleja que existe al menos más de 2000 equipos conectados directamente a Internet, y por tanto expuesto a cualquier ataque.



En vista de los resultados, se necesita "tomar" una serie de medidas de protección para evitar que "alguien" pueda atacar nuestro equipo.

MEDIDAS DE PROTECCIÓN

Aunque todavía no se conoce exploit, si que están apareciendo las primeras pruebas de concepto sobre la vulnerabilidad (MS12-020), por ello se os recomienda realizar las siguientes acciones, lo más pronto posible:

1. Mantener actualizado el Sistema Operativo Windows, al día | Aplicar el parche ([aquí](#)).
2. **Deshabilitar** el servicio de RDP, si no lo usáis.

¿Cómo se deshabilita el servicio RDP?

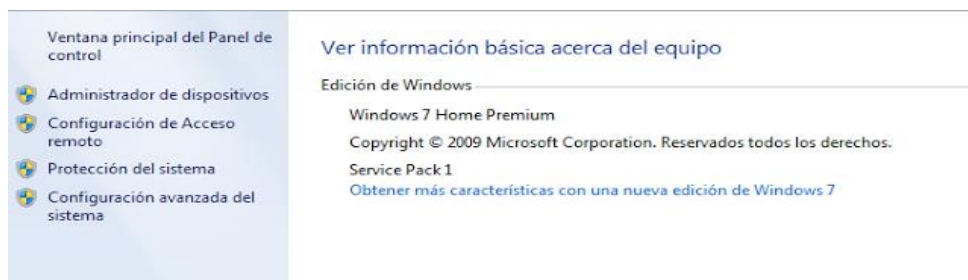
La mejor manera de hacerlo es seguir las [instrucciones de Microsoft](#), no obstante aquí os dejo un resumen:

Para Windows XP:

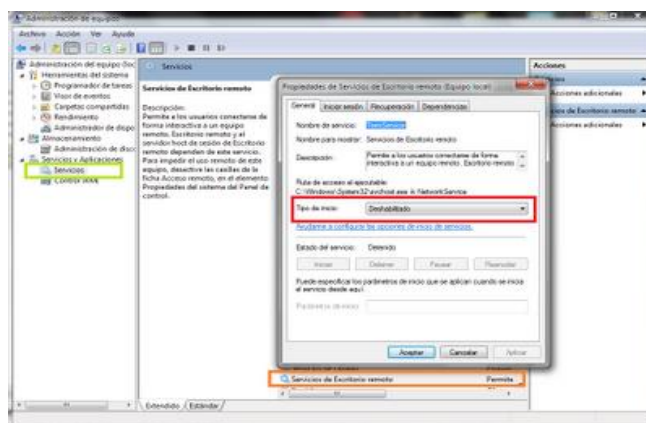
1. Haga clic en **Inicio**, haga clic en **Ejecutar**, escriba **gpedit.msc** y, a continuación, haga clic en **Aceptar**.
2. En el editor de Directiva de grupo, haga clic para expandir **Configuración del equipo**, **Plantillas administrativas**, **Componentes de Windows y Servicios de Terminal Server**.
3. Haga doble clic en la directiva **No permitir conexiones de clientes nuevos**.
4. Establezca la directiva como **Habilitada** y haga clic en **Aceptar**.

Para Windows Vista/7:

1. Acceder al **Panel de control**, Todos los elementos de Panel de control, y luego en **Sistema**.
2. Hacer clic en "**Configuración de Acceso Remoto**".
3. Una vez en el Menú, No permitir ninguna conexión remota.



O bien ir directamente a la lista de Servicios de Windows, y Deshabilitar el RDP.

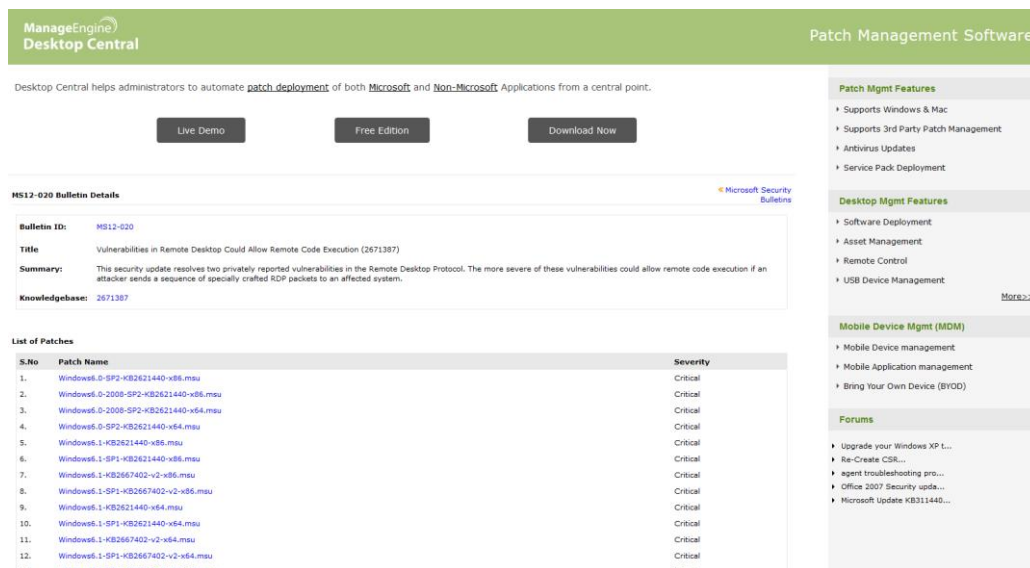


Otras opciones, si por necesidad se debe de seguir utilizando el servicio de escritorio remoto, se pueden minimizar los riesgos, aplicando el [parche](#), configurando adecuadamente el cortafuegos (bloqueando cualquier IP, que no sea la autorizada), o incluso realizando una configuración segura del servicio como se "indica" en este [artículo de Microsoft](#).

<http://www.seguridadparatodos.es/2012/03/ms12-020-el-escritorio-remoto-rdp-ha.html>

Hay páginas como ManageEngine que nos orientar para parchear estas vulnerabilidades.

<https://www.manageengine.com/products/desktop-central/patch-management/MS12-020.html>



ManageEngine Desktop Central Patch Management Software

Desktop Central helps administrators to automate patch deployment of both **Microsoft** and **Non-Microsoft** Applications from a central point.

[Live Demo](#) [Free Edition](#) [Download Now](#)

MS12-020 Bulletin Details

Bulletin ID: MS12-020

Title: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)

Summary: This security update resolves two privately reported vulnerabilities in the Remote Desktop Protocol. The more severe of these vulnerabilities could allow remote code execution if an attacker sends a sequence of specially crafted RDP packets to an affected system.

Knowledgebase: 2671387

List of Patches

S.No	Patch Name	Severity
1.	Windows6.0-SP2-KB2621440-x86.msu	Critical
2.	Windows6.0-SP2-KB2621440-x86.msu	Critical
3.	Windows6.0-SP2-KB2621440-x64.msu	Critical
4.	Windows6.0-SP2-KB2621440-x64.msu	Critical
5.	Windows6.1-KB2621440-x86.msu	Critical
6.	Windows6.1-KB2621440-x86.msu	Critical
7.	Windows6.1-KB2667402-v2-x86.msu	Critical
8.	Windows6.1-KB2667402-v2-x86.msu	Critical
9.	Windows6.1-KB2621440-x64.msu	Critical
10.	Windows6.1-KB2621440-x64.msu	Critical
11.	Windows6.1-KB2667402-v2-x64.msu	Critical
12.	Windows6.1-KB2667402-v2-x64.msu	Critical

Patch Mgmt Features

- Supports Windows & Mac
- Supports 3rd Party Patch Management
- Antivirus Updates
- Service Pack Deployment

Desktop Mgmt Features

- Software Deployment
- Asset Management
- Remote Control
- USB Device Management

Mobile Device Mgmt (MDM)

- Mobile Device management
- Mobile Application management
- Bring Your Own Device (BYOD)

Forums

- Upgrade your Windows XP L...
- Re-Create CSR...
- agent troubleshooting pro...
- Office 2007 Security upda...
- Microsoft Update KB311440...

Otros escaneos con Nessus

http://www.computersecuritystudent.com/SECURITY_TOOLS/NESSUS/lesson1/