

INFORME DE VULNERABILIDADES OPENVAS
INFORME TÉCNICO OPENVAS
INFORME EJECUTIVO OPENVAS

JUAN CARLOS RODRÍGUEZ CAMPO

Instructor
MAURICIO ORTIZ

Centro de Servicios y Gestión Empresarial
Tecnología en Gestión de Redes de Datos

Ficha: 1438055
SENA – ANTIOQUIA

Medellín 2018

INTRODUCCIÓN

Durante la ejecución de esta actividad, se dará a conocer el funcionamiento de software de análisis de vulnerabilidades, la herramienta que usaremos se llama OPENVAS, un software multiplataforma, el cual será instalado en el sistema operativo Kali Linux y analizará dos servidores, un CentOS 7 y un Windows Server 2012.

Se explicará la instalación y configuración de OPENVAS, demostrando de forma detallada el paso a paso, desde la agregación de repositorios, pasando por los comandos utilizados y finalmente haciendo una demostración de como se escanean los servidores.

Objetivo: aprender a utilizar y configurar software para el análisis de vulnerabilidades de servidores empresariales.

Objetivo específico: escanear posibles vulnerabilidades de servidores utilizando software apropiado para ello, así como entender e interpretar los resultados numéricos y gráficos que nos provee OPENVAS.

INSTALACIÓN DE OPENVAS

Primero agregamos los repositorios a Kali Linux en `/etc/apt/source.list`

```
# deb cdrom:[Debian GNU/Linux 2017.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20170416-02:08]/ kali-rolling contrib main non-free
```

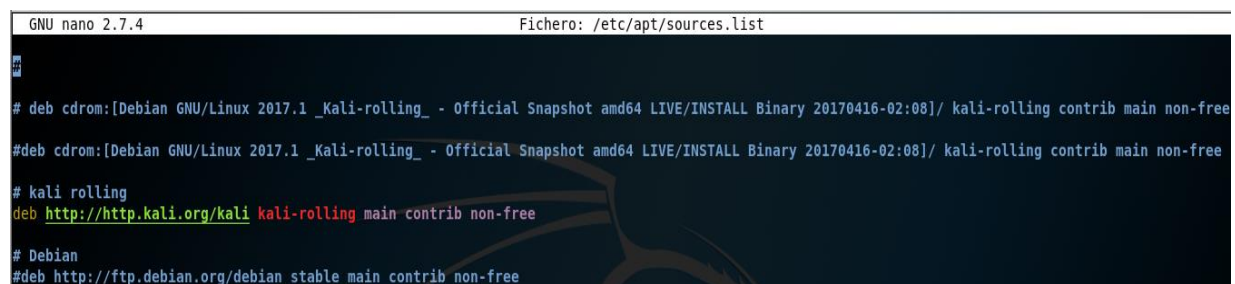
```
#deb cdrom:[Debian GNU/Linux 2017.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20170416-02:08]/ kali-rolling contrib main non-free
```

```
# kali rolling
```

```
deb http://http.kali.org/kali kali-rolling main contrib non-free
```

```
# Debian
```

```
#deb http://ftp.debian.org/debian stable main contrib non-free
```



```
GNU nano 2.7.4                                Fichero: /etc/apt/sources.list

# deb cdrom:[Debian GNU/Linux 2017.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20170416-02:08]/ kali-rolling contrib main non-free
#deb cdrom:[Debian GNU/Linux 2017.1 _Kali-rolling_ - Official Snapshot amd64 LIVE/INSTALL Binary 20170416-02:08]/ kali-rolling contrib main non-free
# kali rolling
deb http://http.kali.org/kali kali-rolling main contrib non-free
# Debian
#deb http://ftp.debian.org/debian stable main contrib non-free
```

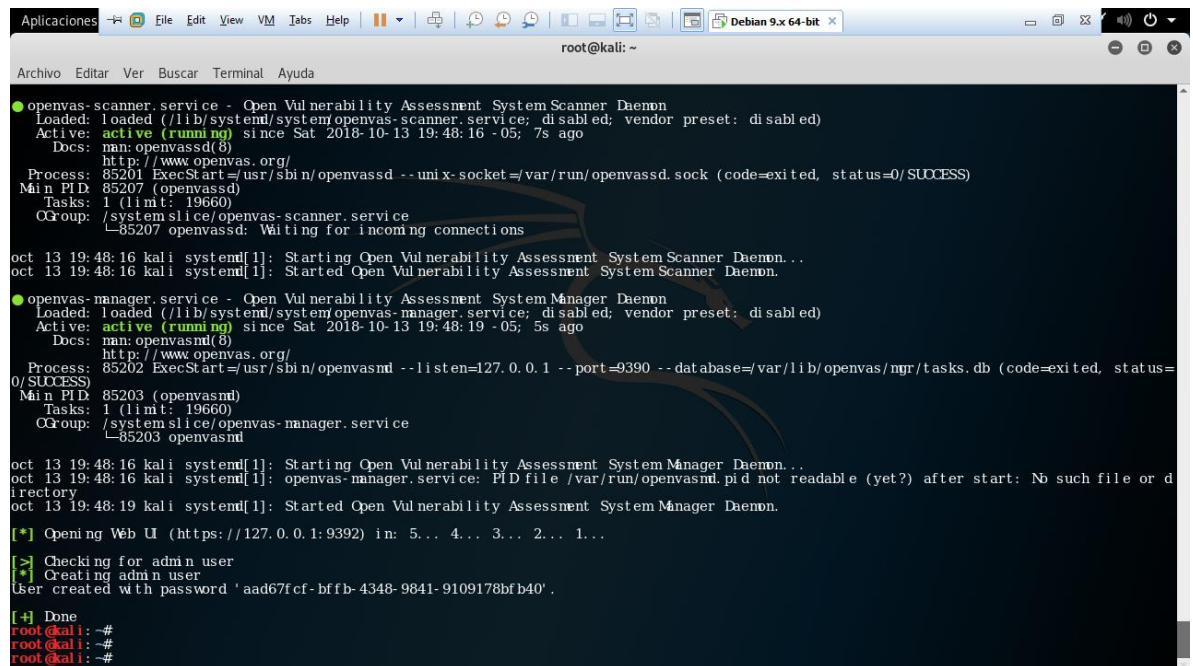

Abrimos openvas con el siguiente comando.

openvas-setup

```
Aplicaciones  File Edit View VM Tabs Help  Debian 9.x 64-bit x
root@kali: ~
root@kali: ~# openvas-setup
[+] Updating OpenVAS feeds
[1/3] Updating: NVT
-- 2018-10-13 19:02:47-- http://dl.greenbone.net/community-nvt-feed-current.tar.bz2
Resolviendo dl.greenbone.net (dl.greenbone.net)... 89.146.224.58, 2a01:130:2000:127::d1
Conectando con dl.greenbone.net (dl.greenbone.net)[89.146.224.58]:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 30236027 (29M) [application/octet-stream]
Grabando a: "/tmp/greenbone-nvt-sync.iEOqghzGCM/openvas-feed-2018-10-13-84709.tar.bz2"
enbone-nvt-sync.iEOqghzGCM/openvas 9% ==> ] 2,68M 525KB/s eta 54s
```

```
Aplicaciones  File Edit View VM Tabs Help  Debian 9.x 64-bit x
root@kali: ~
root@kali: ~# openvas-setup
2009/sepod_tpmiotus_notes_mim_lig_vuln_lin.nasl
2009/gb_apache_struts_dir_traversal_vuln.nasl.asc
2009/gb_adobe_pdrts_mult_vuln_dec09_win.nasl
2009/gb_maxthon_addr_bar_spoofing_vuln.nasl
2009/gb_xerxes_http_server_dir_traversal_vuln.nasl
2009/sepod_firefox_url_spoof_vuln_win.nasl
2009/gb_dovecot_base_dir_sec_bypass_vuln.nasl
2009/finnyWebGallery_34892.nasl
2009/sepod_apache_tiles_xss_vuln.nasl.asc
2009/moodle_cms_file_disclosure.nasl
2009/gb_sun_java_sys_web_serv_bof_vuln_lin.nasl.asc
2009/gb_mysql_auth_bypass_vuln_lin.nasl
2009/sepod_openfire_mult_vuln_mar09.nasl
2009/gb_google_chrome_js_uri_xss_vuln_sep09.nasl
2009/gb_ms_ie_null_ptr_dos_vuln.nasl
2009/gb_thunderbird_mult_vuln_mar09_lin.nasl.asc
2009/sepod_innraieplugh_activate_ctrl_vuln.nasl
2009/finnyXQ_36391.nasl.asc
2009/gb_titan_ftp_server_dos_vuln.nasl
2009/gb_opera_xml_dos_vuln_win.nasl
2009/phpgroupware_35761.nasl
2009/sepod_php_unserialize_dos_vuln.nasl.asc
2009/gb_alleycode_html_editor_bof_vuln.nasl.asc
2009/sepod_ms_ie_dos_vuln_nov09.nasl.asc
2009/openssh_32319_remote.nasl.asc
2009/DHCart_multiple_xss.nasl
2009/gb_novell_groupwise_client_activex_bof_vuln.nasl.asc
2009/sepod_foxit_wac_server_bof_vuln.nasl.asc
2009/demum_cms_multiple_vulnerabilities.nasl
2009/sepod_pi_dgin_mult_bof_vuln_lin.nasl
2009/sepod_ms_ie_unicode_str_dos_vuln.nasl
2009/sepod_ms09-006.nasl
2009/gb_cscope_mult_bof_vuln.nasl
2009/gb_firefox_ssl_spoof_vuln_win.nasl.asc
2009/gb_pi_dgin_oscar_dos_vuln_lin.nasl
2009/eliteCMS_multiple.nasl.asc
2009/sepod_f_prot_av_sec_bypass_vuln_lin.nasl.asc
2009/net2ftp_34440.nasl
2009/deluxeBB_1.3.nasl
2009/cs_whois_34700.nasl
2009/gb_apple_safari_dos_vuln_jul09.nasl.asc
2009/bind_37118.nasl.asc
2009/gb_pi_dgin_oscar_dos_vuln_oct09_lin.nasl
```

Después de que termina la iniciación de openvas



```
Aplicaciones File Edit View VM Tabs Help Debian 9.x 64-bit x root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda

● openvas-scanner.service - Open Vulnerability Assessment System Scanner Daemon
  Loaded: loaded (/lib/systemd/system/openvas-scanner.service; disabled; vendor preset: disabled)
  Active: active (running) since Sat 2018-10-13 19:48:16 -05; 7s ago
  Docs: http://www.openvas.org/
        man: openvassd(8)
  Process: 85201 ExecStart=/usr/sbin/openvassd --unix-socket=/var/run/openvassd.sock (code=exited, status=0/SUCCESS)
  Main PID: 85207 (openvassd)
  Tasks: 1 (limit: 19660)
  OGroup: /system.slice/openvas-scanner.service
         └─85207 openvassd: Waiting for incoming connections

oct 13 19:48:16 kali systemd[1]: Starting Open Vulnerability Assessment System Scanner Daemon...
oct 13 19:48:16 kali systemd[1]: Started Open Vulnerability Assessment System Scanner Daemon.

● openvas-manager.service - Open Vulnerability Assessment System Manager Daemon
  Loaded: loaded (/lib/systemd/system/openvas-manager.service; disabled; vendor preset: disabled)
  Active: active (running) since Sat 2018-10-13 19:48:19 -05; 5s ago
  Docs: http://www.openvas.org/
        man: openvasmd(8)
  Process: 85202 ExecStart=/usr/sbin/openvasmd --listen=127.0.0.1 --port=9390 --database=/var/lib/openvas/mgr/tasks.db (code=exited, status=0/SUCCESS)
  Main PID: 85203 (openvasmd)
  Tasks: 1 (limit: 19660)
  OGroup: /system.slice/openvas-manager.service
         └─85203 openvasmd

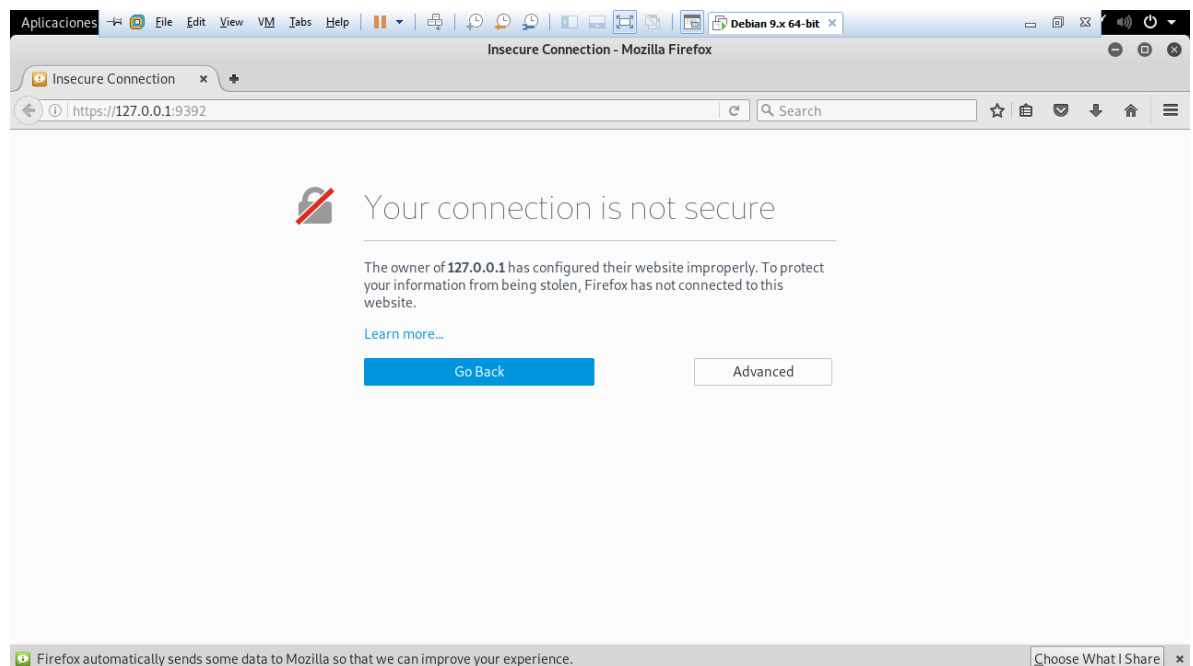
oct 13 19:48:16 kali systemd[1]: Starting Open Vulnerability Assessment System Manager Daemon...
oct 13 19:48:16 kali systemd[1]: openvas-manager.service: PID file /var/run/openvasmd.pid not readable (yet?) after start: No such file or directory
oct 13 19:48:19 kali systemd[1]: Started Open Vulnerability Assessment System Manager Daemon.

[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...

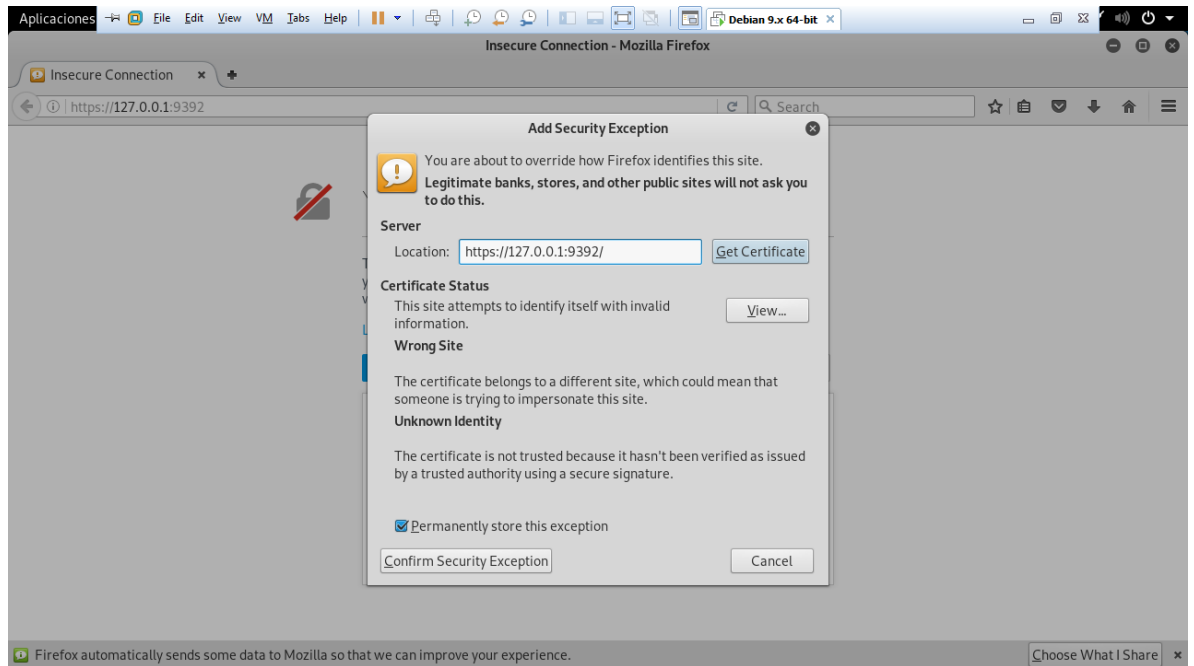
[+] Checking for admin user
[+] Creating admin user
User created with password 'aad67fcf-bffb-4348-9841-9109178bfb40'.

[+] Done
root@kali: ~#
root@kali: ~#
root@kali: ~#
```

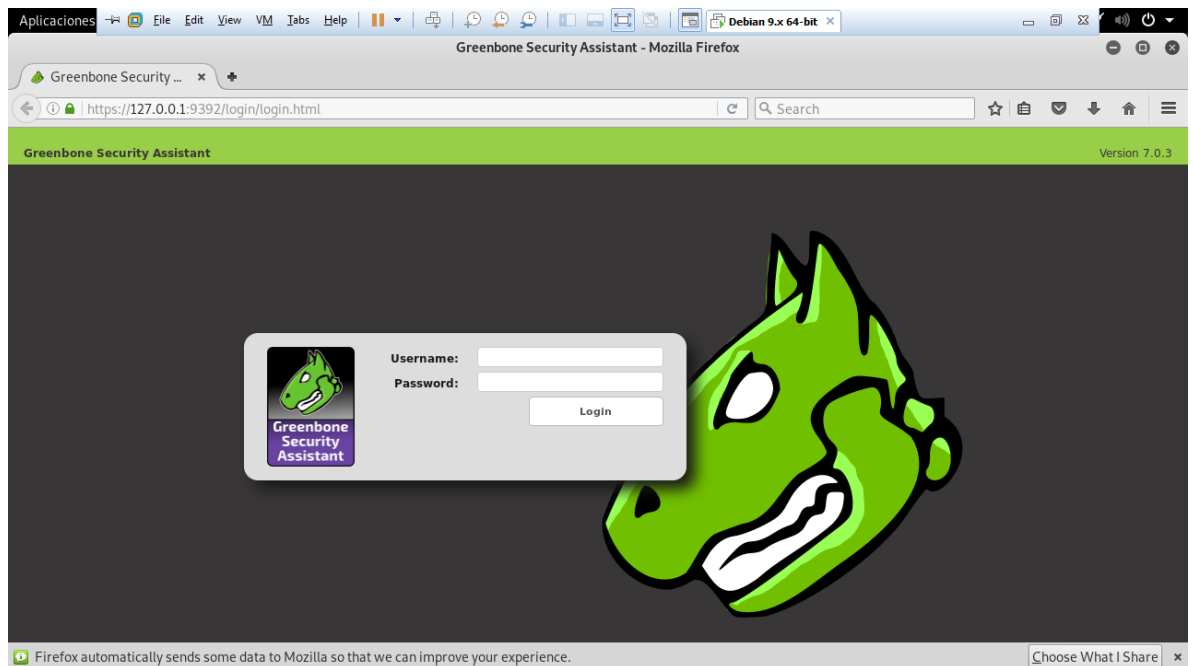
Se nos abre automáticamente el navegador web con openvas.



Acá elegimos opción avanzada y agregamos la excepción.



Y ya estamos en openvas



Para cambiar el usuario y contraseña del openvas ingresamos la siguiente línea.

```
root@kali:~# openvasmd --create-user=root --role=Admin && openvasmd --user=root --new-password=Sena2018
```

Nota: como medida de rapidez en procesos futuros vamos a detener el

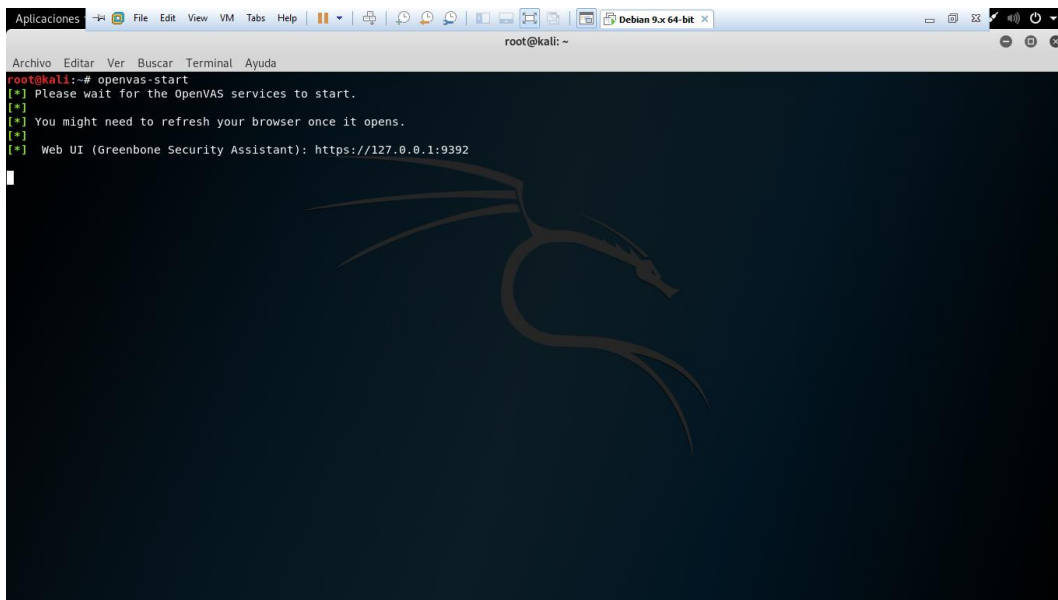
firewall de nuestro servidor openvas.

Para hacer instalamos ufw y luego hacemos ufw disable para deshabilitar el firewall

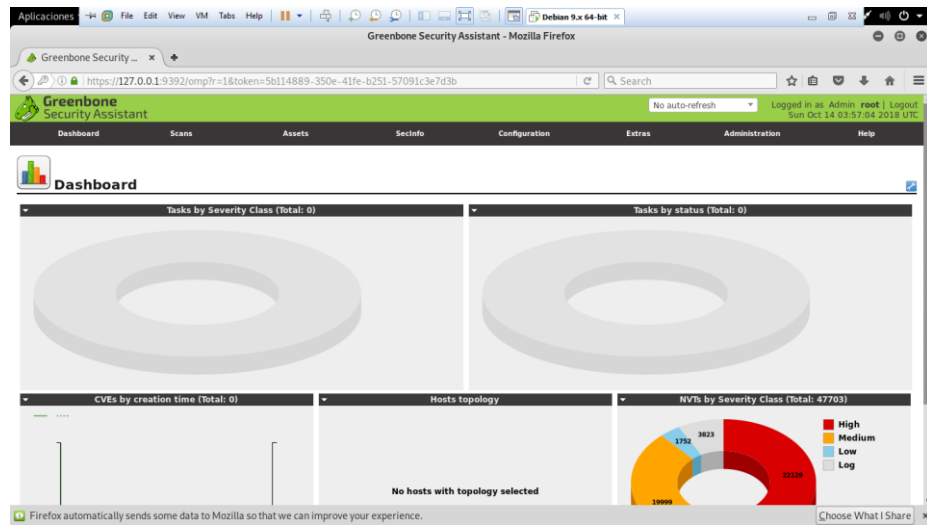
```
root@kali:~# apt-get install ufw
```

```
root@kali:~# ufw disable
```

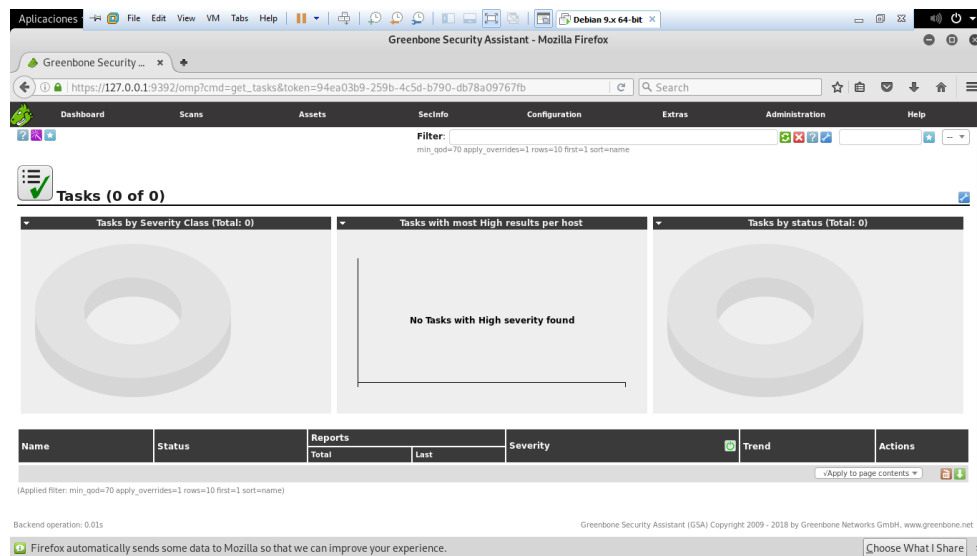
Nota: debido a que la cesión de openvas caduca relativamente rápido, se debe ingresar por la terminal con el comando: “openvas-start



Y esta es la interfaz web de openvas, desde donde realizaremos el análisis de vulnerabilidades de nuestra red.



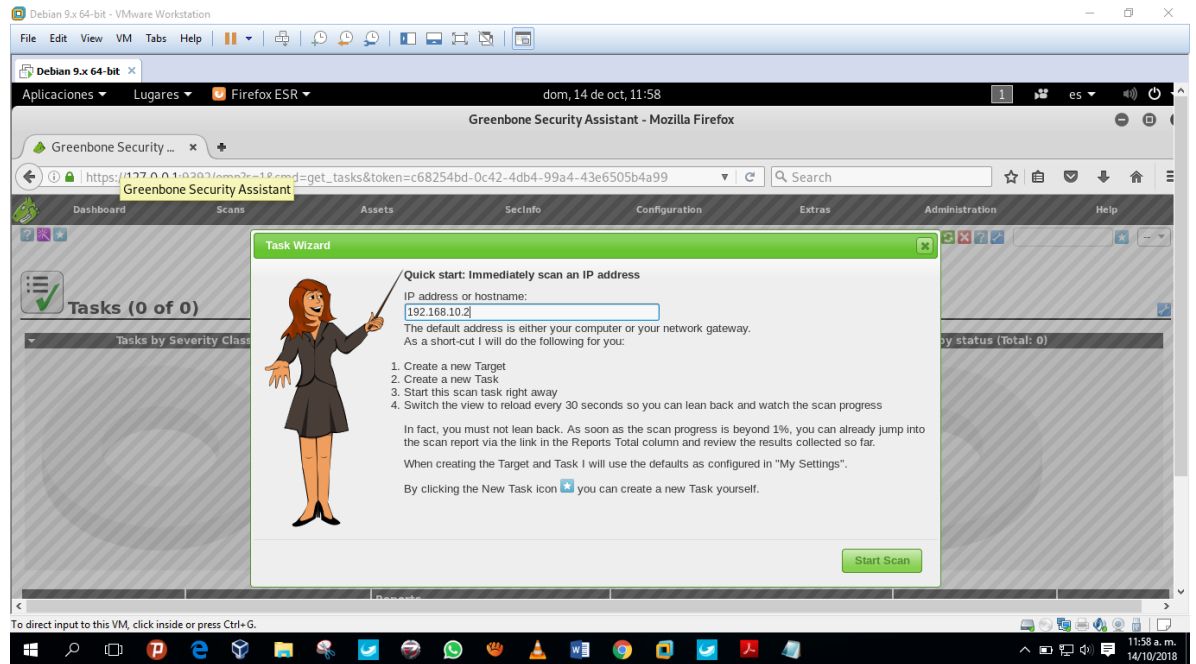
Para empezar el escaneo damos en “scans” y luego “tasks”



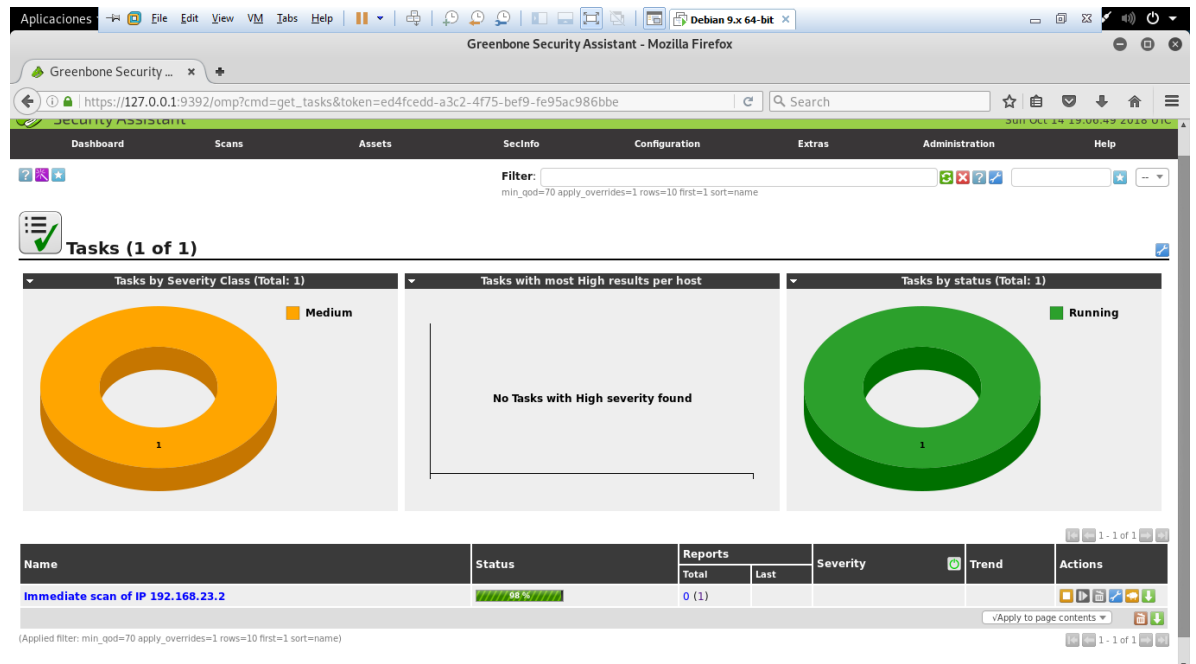
Nos ubicamos en la barita y damos clic en Task Wizard



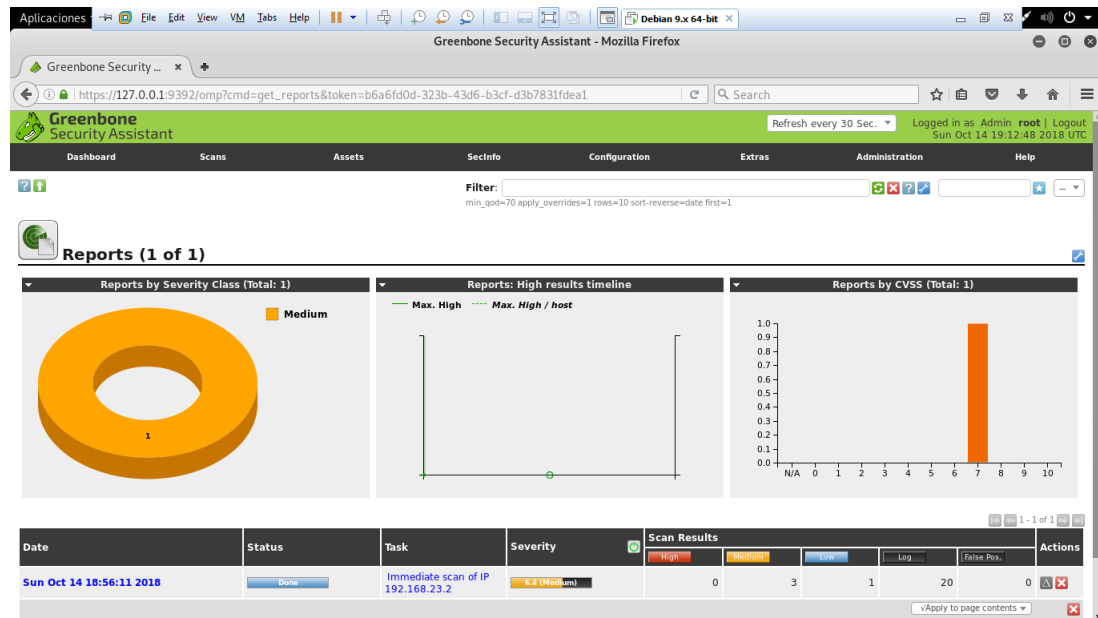
Ingresamos la IP del servidor de CentOS 7



Esperamos a que cargue.



Al terminar el escaneo, se nos genera un reporte diciendo que nuestro servidor de CentOS 7 tiene vulnerabilidades de nivel medio.



Luego damos clic en la fecha y nos aparecerá el resultado de todo el escaneo.

Date

[Sun Oct 14 18:56:11 2018](#)

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant

Filter: sort=auto apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=html min_god=70

Report: Results (4 of 61)

Vulnerability	Severity	QoD	Host	Location	Actions
Check for Anonymous FTP Login	6.4 (Medium)	80%	192.168.23.2	21/tcp	Details Fix
HTTP Debugging Methods (TRACE/TRACE) Enabled	5.8 (Medium)	99%	192.168.23.2	80/tcp	Details Fix
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.23.2	22/tcp	Details Fix
TCP timestamps	2.0 (Low)	80%	192.168.23.2	general/tcp	Details Fix

Backend operation: 4.49s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

Para descargar el reporte en algún formato lo ubicamos en esta parte.

Greenbone Security Assistant - Mozilla Firefox

Greenbone Security Assistant

Logged in as Admin root | Logout
Sun Oct 14 19:16:57 2018 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML [Icons] [Buttons] [Filter]

Filter: autofs=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70

Report: Results (4 of 61)

ID: 256d4ec0-26b2-4374-b036-f763896976eb
Modified: Sun Oct 14 19:10:08 2018
Created: Sun Oct 14 18:56:26 2018
Owner: root

Vulnerability	Severity	QoD	Host	Location	Actions
Check for Anonymous FTP Login	6.4 (Medium)	80%	192.168.23.2	21/tcp	[Icons]
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.9 (Medium)	99%	192.168.23.2	80/tcp	[Icons]
SSH Weak Encryption Algorithms Supported	4.9 (Medium)	95%	192.168.23.2	22/tcp	[Icons]
TCP timestamps	2.6 (Low)	80%	192.168.23.2	general/tcp	[Icons]

(Applied filter: autofs=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)

Backend operation: 4.49s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

INFORME TÉCNICO DE VULNERABILIDADES SERVIDOR CENTOS 7

HOST Y SISTEMA OPERATIVO

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Host: 192.168.23.2

ID: 10b70bf3-dc3d-463f-8975-10ae81bce017
Created: Mon Oct 15 20:46:19 2018
Modified: Mon Oct 15 20:46:19 2018
Owner: root

Comment:

Hostname:

IP: 192.168.23.2

OS: Red Hat Linux (cpe:/o:redhat:linux:7)

Route: 192.168.23.20 ▶ 192.168.23.2

Severity: 6.4 (Medium)

El análisis encontró 61 vulnerabilidades, de las cuales se destacan 4, 3 de tipo medio y una de tipo bajo, los puertos que se vieron comprometidos con vulnerabilidades fueron el puerto 21 en nivel medio, 22 en nivel medio y 80 en nivel medio por la capa de transporte TCP. También se encontró un puerto general por TCP.

Nota: el informe encontró una vulnerabilidad en el servicio FTP, que es el usuario anónimo habilitado, como previamente se sabía esto, esta vulnerabilidad se considera un falso positivo.

- Vulnerabilidad Servicio HTTP

Nivel

Medio (CVSS:5.8)

Tipo de vulnerabilidad

NVT: Métodos de depuración HTTP (TRACE / TRACK) habilitados

Puerto

80/TCP

Resumen

Las funciones de depuración están habilitadas en el servidor web remoto.

El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar las conexiones del servidor web.

Resultado de detección de vulnerabilidad

El servidor web tiene habilitados los siguientes métodos HTTP: TRACE

Impacto

Un atacante puede usar esta falla para engañar a sus usuarios legítimos de la red para que le den sus credenciales.

Solución

Tipo de solución: Mitigación

Desactive los métodos TRACE y TRACK en la configuración de su servidor web.

Consulte el manual de su servidor web o las referencias para obtener más

Software / OS afectado

Servidores web con métodos TRACE y / o TRACK habilitados.

Perspectiva de la vulnerabilidad

Se ha demostrado que los servidores web que admiten estos métodos están sujetos a ataques de scripts entre sitios, llamados XST para el rastreo de sitios cruzados, cuando se usan junto con varias debilidades en los navegadores.

Método de detección de vulnerabilidad

Detalles: Métodos de depuración HTTP (TRACE / TRACK) habilitados (OID: 1.3.6.1.4.1.25623.1.0.11213)

Versión utilizada: \$ Revisión: 10828 \$

Referencias

CVE: CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE-2014-7883

BID: 9506, 9561, 11604, 15222, 19915, 24456, 33374, 36956, 36990, 37995

CERT: CB-K14 / 0981, DFN-CERT-2014-1018, DFN-CERT-2010-0020

Otras referencias

<http://www.kb.cert.org/vuls/id/288308>

<http://www.kb.cert.org/vuls/id/867593>

<http://httpd.apache.org/docs/current/de/mod/core.html#traceenable>

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

- Vulnerabilidad Servicio SSH

Nivel

Medio (CVSS:4.3)

Tipo de vulnerabilidad

NVT: Algoritmos de encriptación débil SSH compatibles

Puerto

22/TCP

Resumen

El servidor SSH remoto está configurado para permitir algoritmos de cifrado débiles.

Resultado de detección de vulnerabilidad

El servicio remoto admite los siguientes algoritmos débiles de cifrado de cliente a servidor:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
pez volador-cbc
cast128-cbc

El servicio remoto admite los siguientes algoritmos débiles de encriptación de servidor a cliente:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
pez volador-cbc
cast128-cbc

Solución

Tipo de solución: Mitigación

Desactivar los algoritmos de cifrado débiles.

Perspectiva de la vulnerabilidad

El cifrado `arcfour` es el cifrado de flujo de Arcfour con claves de 128 bits. Se cree que el cifrado Arcfour es compatible con el cifrado RC4 [SCHNEIER]. Arcfour (y RC4) tiene problemas con las teclas débiles y no debe usarse más.

El algoritmo `none` especifica que no se debe realizar ningún cifrado. Tenga en cuenta que este método no proporciona protección de confidencialidad y NO SE RECOMIENDA su uso.

Existe una vulnerabilidad en los mensajes SSH que emplean el modo CBC que puede permitir que un atacante recupere texto sin formato de un bloque de texto cifrado.

Método de detección de vulnerabilidad

Compruebe si el servicio ssh remoto es compatible con Arcfour, ninguno o cifrados CBC.

Detalles: algoritmos de encriptación débil SSH compatibles (OID: 1.3.6.1.4.1.25623.1.0.105611)

Referencias

Otro:

<https://tools.ietf.org/html/rfc4253#section-6.3>
<https://www.kb.cert.org/vuls/id/958563>

- Vulnerabilidad General

Nivel

Bajo (CVSS:2.6)

Tipo de vulnerabilidad

NVT: TCP timestamps (marcas de tiempo)

Resumen

El host remoto implementa marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad.

Resultado de detección de vulnerabilidad

Se detectó que el host implementa RFC1323.

Las siguientes marcas de tiempo se recuperaron con un retraso de 1 segundo entre:

Paquete 1: 11947328

Paquete 2: 11948343

Impacto

Un efecto secundario de esta característica es que el tiempo de actividad del host remoto a veces se puede calcular.

Solución

Tipo de solución: Mitigación

Para deshabilitar las marcas de tiempo TCP en Linux, agregue la línea 'net.ipv4.tcp_timestamps = 0' a /etc/sysctl.conf. Ejecute 'sysctl -p' para aplicar la configuración en tiempo de ejecución.

Para deshabilitar las marcas de tiempo TCP en Windows ejecute 'netsh int tcp set global timestamps = disabled'

A partir de Windows Server 2008 y Vista, la marca de tiempo no se puede desactivar por completo.

El comportamiento predeterminado de la pila TCP / IP en este sistema es no usar las opciones de marca de hora al iniciar conexiones TCP, sino usarlas si el par TCP que está iniciando la comunicación las incluye en su segmento de sincronización (SYN).

Consulte también: <http://www.microsoft.com/en-us/download/details.aspx?id=9152>

Software / OS afectado

Implementaciones TCP / IPv4 que implementan RFC1323

Perspectiva de la vulnerabilidad

El host remoto implementa marcas de tiempo TCP, como se define en RFC1323.

Método de detección de vulnerabilidad

Los paquetes de IP especiales se falsifican y se envían con un pequeño retraso entre la IP de destino. Las respuestas se buscan por una marca de tiempo. Si se encuentran, se informan las marcas de tiempo.

Detalles: marcas de tiempo TCP (OID: 1.3.6.1.4.1.25623.1.0.80091)

Versión utilizada: \$ Revisión: 10411 \$

Referencias

Otro:

<http://www.ietf.org/rfc/rfc1323.txt>

LISTA DE SERVICIOS Y DISPOSITIVOS VULNERABLES

Servicio FTP (falso positivo)

Servicio HTTP

Servicio SSH

Software / OS afectado

Servidores web con métodos TRACE y / o TRACK habilitados.

Servicio SSH

Software / OS afectado

Implementaciones TCP / IPv4 que implementan RFC1323

Nota: al hacer nuevos escaneos de vulnerabilidades con openvas, con el SELinux deshabilitado y el firewall detenido, siguieron estando las mismas 4 vulnerabilidades, 3 de nivel medio y 1 de nivel bajo.

Glosario

Falso positivo: hablamos de falso positivo cuando un hecho que se presume como cierto o verdadero, resulta no ser tal.

FTP: (File Transfer Protocol) Es el Protocolo de Transferencia de Archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo.

Servicio FTP: un servicio FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet. Su función es

permitir el intercambio de datos entre diferentes servidores/computadores.

Usuario FTP Anónimo: característica de ciertos servidores FTP que le permiten al usuario ingresar al servicio FTP sin un nombre de usuario y contraseña que lo identifiquen.

Archivo sensible: archivo sensible o información sensible es el nombre que recibe la información personal privada de un individuo, por ejemplo, ciertos datos personales y bancarios, contraseñas de correo electrónico e incluso el domicilio en algunos casos. Aunque lo más común es usar este término para designar datos privados relacionados con Internet o la informática, sobre todo contraseñas, tanto de correo electrónico, conexión a Internet, IP privada, sesiones del PC, etc. Los crackers utilizan la llamada ingeniería social para intentar hacerse con este tipo de información.

Host: Un host o anfitrión es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio web. Un host de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o nombre de host.

Servicio HTTP: (Hypertext Transfer Protocol o HTTP) es un protocolo de transferencia de hipertexto, el protocolo de transferencia de hipertexto (HTTP) es un nivel de aplicación. Protocolo de información distribuida, colaborativa, hipermedia.

Métodos de depuración HTTP (TRACE / TRACK) habilitados: el servidor web remoto es compatible con los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para la depuración de las entradas de los usuarios. En este caso se debe desactivar ya que mediante él se puede ejecutar un ataque web del tipo XSS: Cross-site scripting, un tipo de vulnerabilidad comúnmente encontrada en Servidores Web (Tomcat, Apache, etc.).

Servidor web remoto: servidor de acceso remoto (Remote Access Server/Services) es una combinación de hardware y software que permite el acceso remoto a herramientas o información que generalmente residen en una red de dispositivos.

Hablando de un servidor como un equipo, son las computadoras que se usan para tener a su vez programas servidores. Son mucho más grandes y poseen mayores características que los equipos normales. Estos equipos son los que nos dan un espacio para almacenar nuestro sitio web,

es decir, nos permiten tener lo que llamamos un Hosting, además de éste se necesita un nombre para el sitio web; es decir, un Dominio, por medio del cual cualquier persona podrá acceder a nuestro sitio web a través de la red.

Método Trace HTTP: El método TRACE realiza una prueba de bucle de retorno de mensaje a lo largo de la ruta al recurso de destino.

Ataques de scripts XST: XSS ocurre cuando un atacante es capaz de inyectar un script, normalmente Javascript, en el output de una aplicación web de forma que se ejecuta en el navegador del cliente. Los ataques se producen principalmente por validar incorrectamente datos de usuario, y se suelen inyectar mediante un formulario web o mediante un enlace alterado.

Servicio SSH: SSH o Secure Shell, es un protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores remotos a través de Internet.

Algoritmo: en Matemática, ciencias de la Computación y disciplinas relacionadas, un algoritmo (del latín, dixit algorithmus y éste a su vez del matemático persa Al Juarismi) es un conjunto reescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien lo ejecute. Dados un estado inicial y una entrada, siguiendo los pasos sucesivos se llega a un estado final y se obtiene una solución. Los algoritmos son objeto de estudio de la algoritmia.

Algoritmos de encriptación: el método de encriptación y desencriptación es llamado Cifrado. Algunos métodos criptográficos se basan en el anonimato de los algoritmos de encriptación; tales algoritmos son de interés histórico y no son adecuados para las necesidades del mundo real. En lugar de anonimato de los algoritmos por si solos, todos los algoritmos modernos basan su seguridad en la utilización Llaves; y un mensaje solo puede ser desencriptado si la llave utilizada para desencriptar coincide con la utilizada para encriptar.

Cifrado: el cifrado es la práctica de codificar y decodificar datos. Cuando los datos están cifrados, se les ha aplicado un algoritmo para codificarlos, de manera que dejan de estar en su formato original y, por consiguiente, no se pueden leer. Los datos solo se pueden decodificar a su forma original aplicando una determinada clave de descifrado. Las técnicas de codificación son una parte importante de la seguridad de los datos, ya que protegen la información sensible contra amenazas como la explotación

mediante malware y el acceso no autorizado de terceros. El cifrado de datos es una solución de seguridad versátil: puede aplicarse a datos como una contraseña, o de forma más amplia, a datos de un archivo o incluso a datos contenidos en medios de almacenamiento.

Encriptación: es una manera de codificar la información para protegerla frente a terceros.

Servidor: un servidor es un ordenador u otro tipo de equipo informático encargado de suministrar información a una serie de clientes, que pueden ser tanto personas como otros dispositivos conectados a él. La información que puede transmitir es múltiple y variada: desde archivos de texto, imagen o vídeo y hasta programas informáticos, bases de datos, etc.

Arquitectura Cliente/Servidor: esta arquitectura consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta. Aunque esta idea se puede aplicar a programas que se ejecutan sobre una sola computadora es más ventajosa en un sistema operativo multiusuario distribuido a través de una red de computadoras. La interacción cliente-servidor es el soporte de la mayor parte de la comunicación por redes. Ayuda a comprender las bases sobre las que están contruidos los algoritmos distribuidos.

Algoritmo débil: modalidad de secuencia, un método de cifrado en el que se cifra cada byte individualmente. Se considera generalmente una forma de cifrado débil.

Arcfour o RC4: en criptografía RC4 es el cifrado de flujo software más utilizado y se utiliza en los protocolos populares como Secure Sockets Layer y WEP. Mientras que destaca por su sencillez y rapidez en el software, RC4 tiene debilidades que argumentan en contra de su uso en los nuevos sistemas. Es especialmente vulnerables cuando el comienzo de la secuencia de claves de salida no se descarta, o cuando no aleatoria o claves relacionadas se utilizan; algunas maneras de utilizar RC4 puede conducir a criptosistemas muy inseguros tales como WEP.

Cifrado CBC: en el modo cipher-block chaining (CBC), a cada bloque de texto plano se le aplica la operación XOR con el bloque cifrado anterior antes de ser cifrado. De esta forma, cada bloque de texto cifrado depende de todo el texto en claro procesado hasta este punto. Para hacer cada mensaje único se utiliza asimismo un vector de inicialización.

TCP timestamps (marcas de tiempo): las marcas de tiempo TCP se utilizan para proporcionar protección contra los números de secuencia envueltos. Es posible calcular el tiempo de funcionamiento del sistema (y el tiempo de arranque) mediante el análisis de las marcas de tiempo de TCP (ver más abajo).

Estos tiempos de funcionamiento calculados (y los tiempos de inicio) pueden ayudar a detectar sistemas operativos ocultos habilitados para la red (ver TrueCrypt), vincular direcciones IP y MAC falsificadas, vincular direcciones IP con puntos de acceso inalámbricos Ad-Hoc, etc.

INFORME EJECUTIVO SERVIDOR CENTOS 7

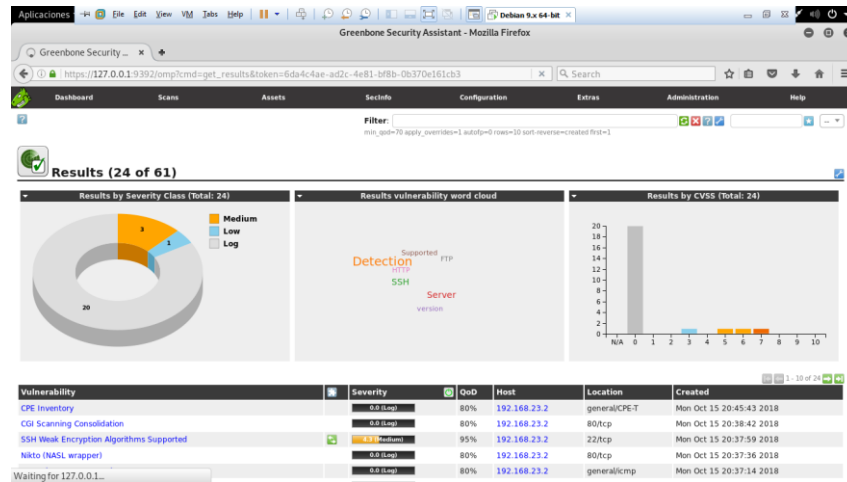
RESUMEN DEL ANÁLISIS DE VULNERABILIDADES:

Durante el análisis del servidor CentOS 7, con la ayuda del software de escaneo de redes openvas, se pudieron detectar 61 reportes y 61 vulnerabilidades, de las cuales solo 4 se destacaban, 3 de nivel medio y 1 de nivel bajo.

Se intento generar reportes y vulnerabilidades de nivel alto y crítico, deteniendo el firewall y deshabilitando el SELinux, pero el resultado fue el mismo.

El reporte mostró falencias en los servicios de la empresa, HTTP y SSH, sin mencionar el servicio FTP puesto que es un falso positivo, debido a que se sabe con antelación que se tiene el usuario anónimo habilitado del servicio FTP.

ANÁLISIS GRÁFICO CON CLASIFICACIÓN DE VULNERABILIDADES Y LOS ACTIVOS QUE AFECTA.



SISTEMA OPERATIVO CENTOS 7



HTTP

Clasificación: media

Impacto

Un atacante puede usar esta falla para engañar a sus usuarios legítimos de la red para que le den sus credenciales.

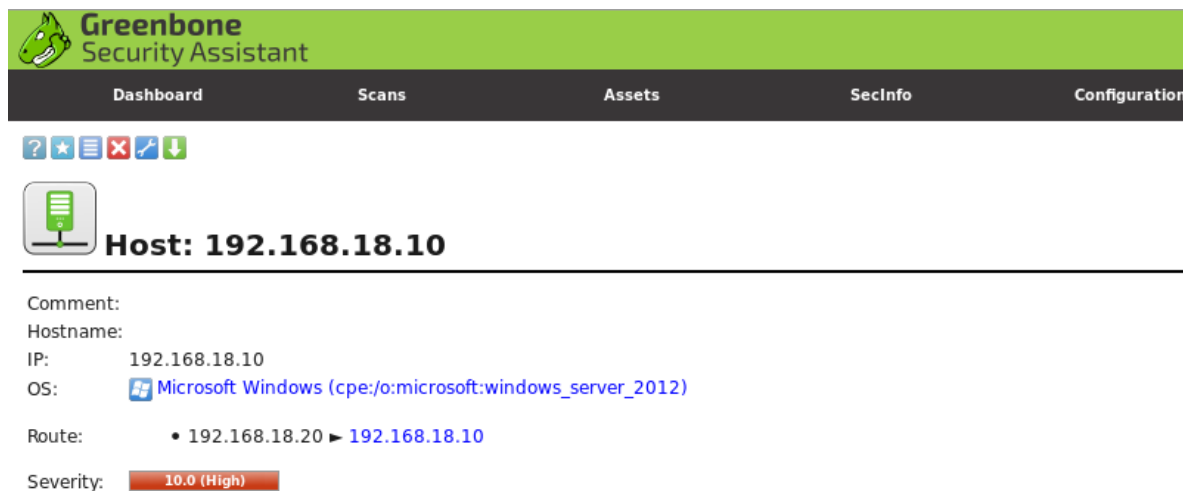
Software / OS afectado

Servidores web con métodos TRACE y / o TRACK habilitados.


INFORME TÉCNICO DE VULNERABILIDADES WINDOWS SERVER 2012

El análisis encontró 207 vulnerabilidades de las cuales se destacan 4 en nivel alto, los puertos que se vieron comprometidos con vulnerabilidades fueron el puerto 443 en nivel alto, 444 en nivel alto y 444 en nivel alto por la capa de transporte TCP.

HOST Y SISTEMA OPERATIVO



The screenshot shows the Greenbone Security Assistant interface. At the top is a green header with the logo and name. Below it is a dark navigation bar with tabs: Dashboard, Scans, Assets, SecInfo, and Configuration. Under the Dashboard tab, there are several icons. Below the icons, a host icon is shown next to the text "Host: 192.168.18.10". Below this, the following details are listed:

- Comment:
- Hostname:
- IP: 192.168.18.10
- OS:  Microsoft Windows (cpe:/o:microsoft:windows_server_2012)
- Route: • 192.168.18.20 ► 192.168.18.10
- Severity: 10.0 (High)

Vulnerabilidades de tipo alto

Vulnerabilidad Servicio HTTP

Nivel

Alto (CVSS:10.0)

Tipo de vulnerabilidad

NVT: MS15-034 Vulnerabilidad de ejecución remota de código HTTP.sys (verificación remota)

Puerto

444/TCP

Resumen

A este host le falta una actualización de seguridad importante según Microsoft Bulletin MS15-034.

Resultado de detección de vulnerabilidad

La vulnerabilidad se detectó de acuerdo con el método de detección de vulnerabilidad.

Impacto

La explotación exitosa permitirá a los atacantes remotos ejecutar código arbitrario en el contexto del usuario actual y realizar acciones en el contexto de seguridad del usuario actual.

Solución

Tipo de solución: VendorFix VendorFix

Ejecute Windows Update y actualice las revisiones enumeradas o descargue y actualice las revisiones mencionadas en el aviso del siguiente enlace:

<https://technet.microsoft.com/library/security/MS15-034>

Software / OS afectado

Microsoft Windows 8 x32/x64

Microsoft Windows 8.1 x32/x64

Microsoft Windows Server 2012

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior

Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Perspectiva de la vulnerabilidad

La falla existe debido a la pila de protocolo HTTP 'HTTP.sys' que se activa al analizar las solicitudes HTTP.

Método de detección de vulnerabilidad

Envíe una solicitud GET HTTP especialmente diseñada y verifique la respuesta

Detalles: MS15-034 Vulnerabilidad de ejecución remota de código en HTTP.sys (verificación remota) (OID: 1.3.6.1.4.1.25623.1.0.105257)
Versión utilizada: \$ Revisión: 10724 \$

Referencias

CVE: CVE-2015-1635
CERT: CB-K15 / 0527, DFN-CERT-2015-0545
Otro: <https://support.microsoft.com/kb/3042553>
<https://technet.microsoft.com/library/security/MS15-034>
<http://pastebin.com/ypURDPc4>

Vulnerabilidad Servicio HTTP

Nivel

Alto (CVSS:10.0)

Tipo de vulnerabilidad

NVT: MS15-034 Vulnerabilidad de ejecución remota de código HTTP.sys (verificación remota)

Puerto

443/TCP

Resumen

A este host le falta una actualización de seguridad importante según Microsoft Bulletin MS15-034.

Resultado de detección de vulnerabilidad

La vulnerabilidad se detectó de acuerdo con el método de detección de vulnerabilidad

Impacto

La explotación exitosa permitirá a los atacantes remotos ejecutar código arbitrario en el contexto del usuario actual y realizar acciones en el contexto de seguridad del usuario actual.

Solución

Tipo de solución: VendorFix VendorFix

Ejecute Windows Update y actualice las revisiones enumeradas o descargue y actualice las revisiones mencionadas en el aviso del siguiente enlace:

<https://technet.microsoft.com/library/security/MS15-034>

Software / OS afectado

Microsoft Windows 8 x32 / x64

Microsoft Windows 8.1 x32 / x64

Microsoft Windows Server 2012

Microsoft Windows Server 2012 R2

Microsoft Windows Server 2008 x32 / x64 Service Pack 2 y anteriores

Microsoft Windows 7 x32 / x64 Service Pack 1 y anteriores

Perspectiva de la vulnerabilidad

La falla existe debido a la pila de protocolo HTTP 'HTTP.sys' que se activa al analizar las solicitudes HTTP.

Método de detección de vulnerabilidad

Envíe una solicitud GET HTTP especialmente diseñada y verifique la respuesta

Detalles: MS15-034 Vulnerabilidad de ejecución remota de código en HTTP.sys (verificación remota) (OID: 1.3.6.1.4.1.25623.1.0.105257)

Versión utilizada: \$ Revisión: 10724 \$

Referencias

CVE: CVE-2015-1635

CERT: CB-K15 / 0527, DFN-CERT-2015-0545

Otro: <https://support.microsoft.com/kb/3042553>

<https://technet.microsoft.com/library/security/MS15-034>

<http://pastebin.com/ypURDPc4>

Vulnerabilidad Servicio HTTP

Nivel

Alto (CVSS:9.3)

Tipo de vulnerabilidad

NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Puerto

445/TCP

Resumen

A este host le falta una actualización de seguridad crítica según Microsoft Bulletin MS17-010

Resultado de detección de vulnerabilidad

La vulnerabilidad se detectó de acuerdo con el método de detección de vulnerabilidad.

Impacto

La explotación exitosa permitirá a los atacantes remotos obtener la capacidad de ejecutar código en el servidor de destino, también podría llevar a la divulgación de información desde el servidor.

Nivel de impacto: Sistema

Tipo de solución: VendorFix VendorFix

Ejecute Windows Update y actualice las revisiones enumeradas o descargue y actualice las revisiones mencionadas en el aviso del siguiente enlace, <https://technet.microsoft.com/library/security/MS17-010>.

Software / OS afectado

Microsoft Windows 10 x32/x64 Edition
Microsoft Windows Server 2012 Edition
Microsoft Windows Server 2016
Microsoft Windows 8.1 x32/x64 Edition

Microsoft Windows Server 2012 R2 Edition
Microsoft Windows 7 x32/x64 Edition Service Pack 1
Microsoft Windows Vista x32/x64 Edition Service Pack 2
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2.

Perspectiva de la vulnerabilidad

Existen múltiples fallas debido a la forma en que el servidor Microsoft Server Message Block 1.0 (SMBv1) maneja ciertas solicitudes.

Método de detección de vulnerabilidad

Envíe la solicitud de transacción SMB diseñada con fid = 0 y verifique la respuesta para confirmar la vulnerabilidad.

Detalles: Vulnerabilidades múltiples remotas del servidor Microsoft Windows SMB (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)

Versión utilizada: \$ Revisión: 7543 \$

Referencias

CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

BID: 96703, 96704, 96705, 96707, 96709, 96706

CERT: CB-K17 / 0435, DFN-CERT-2017-0448

Otro: <https://support.microsoft.com/en-in/kb/4013078>

<https://technet.microsoft.com/library/security/MS17-010>

<https://github.com/rapid7/metasploit-framework/pull/8167/files>

GLOSARIO

MS15-034 Vulnerabilidad de ejecución remota de código HTTP.sys (verificación remota): esta actualización de seguridad resuelve una vulnerabilidad en Microsoft Windows. La vulnerabilidad podría permitir la ejecución remota de código si un atacante enviara una solicitud HTTP especialmente diseñada a un sistema de Windows afectado. La actualización de seguridad corrige la vulnerabilidad al modificar la manera en la que la pila de HTTP de Windows administra las solicitudes.

Explotación: la explotación de software se refiere a los ataques lanzados contra las aplicaciones y servicios de alto nivel. Ellos incluyen el acceso a los

datos utilizando debilidades en los objetos de acceso a datos de una base de datos o un defecto en un servicio o aplicación.

TCP: TCP (que significa Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

Microsoft Bulletin MS15-034: esta actualización de seguridad resuelve una vulnerabilidad en Microsoft Windows. La vulnerabilidad podría permitir la ejecución remota de código si un atacante envía una solicitud HTTP especialmente diseñada a un sistema Windows afectado.

Actualización de seguridad (Parche): en informática, un parche consta de cambios que se aplican a un programa, para corregir errores, agregarle funcionalidad, actualizarlo, etc.

Código: en el caso de la informática, se conoce como código fuente al texto desarrollado en un lenguaje de programación y que debe ser compilado o interpretado para poder ejecutarse en un ordenador, también llamado computadora.

Ataque informático: es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un **sistema informático o red**.

Sistema operativo: un sistema operativo puede ser definido como un conjunto de programas especialmente hechos para la ejecución de varias tareas, en las que sirve de intermediario entre el usuario y la computadora.

Seguridad informática: la Seguridad de la Información consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

Vendor Fix o Vendor Patch: un parche de proveedor es una actualización de un programa proporcionado por un proveedor de software para solucionar algún tipo de problema con el software. Un parche suele ser una pequeña

actualización que no cambia significativamente la funcionalidad. Los parches se implementan normalmente para corregir errores que se han descubierto en un programa, especialmente las vulnerabilidades de seguridad. El término distingue los parches del proveedor de los parches no oficiales de los usuarios.

Windows Update: Windows Update es un servicio gratuito de Microsoft que se utiliza para proporcionar actualizaciones como paquetes de servicio y parches para el sistema operativo Windows y otro software de Microsoft.

Windows Update también se puede utilizar para actualizar controladores para dispositivos de hardware populares.

Los parches y otras actualizaciones de seguridad se lanzan de manera rutinaria a través de Windows Update el segundo martes de cada mes, se llama Patch Tuesday. Sin embargo, Microsoft también publica actualizaciones en otros días, como para soluciones urgentes.

Pila de protocolo: es una colección ordenada de protocolos organizados en capas que se ponen unas encima de otras y en donde cada protocolo implementa una abstracción encuadrada en la abstracción que proporciona la capa sobre la que está encuadrada. Los protocolos encuadrados en la capa inferior proporcionan sus servicios a los protocolos de la capa superior para que estos puedan realizar su propia funcionalidad.

HTTP.sys: HTTP.sys es un servidor web para ASP.NET Core que solo se ejecuta en Windows. HTTP.sys es una alternativa a Kestrel y ofrece algunas características que Kestrel no proporciona.

Solicitud HTTP: una solicitud HTTP es un conjunto de líneas que el navegador envía al servidor. Comprende:

Una línea de solicitud: una línea que especifica el tipo de documento solicitado, el método que se aplicará y la versión del protocolo utilizada. La línea está formada por tres elementos que deben estar separados por un espacio: el método, la dirección URL y la versión del protocolo utilizada por el cliente (por lo general, HTTP/1.0)

Los campos del encabezado de solicitud: un conjunto de líneas opcionales que permiten aportar información adicional sobre la solicitud y/o el cliente (navegador, sistema operativo, etc.). Cada una de estas líneas está formada por un nombre que describe el tipo de encabezado, seguido de dos puntos (:) y el valor del encabezado.

El cuerpo de la solicitud: un conjunto de líneas opcionales que deben estar separadas de las líneas precedentes por una línea en blanco y, por ejemplo, permiten que se envíen datos por un comando POST durante la transmisión de datos al servidor utilizando un formulario.

Solicitud GET HTTP: el método GET solicita una representación de un recurso específico. Las peticiones que usan el método GET sólo deben recuperar datos.

Código arbitrario: el término ejecución arbitraria de código (del inglés arbitrary code execution), hace referencia -en el campo de la Seguridad informática- a la capacidad de un atacante para ejecutar comandos o inyectar código en una aplicación a su antojo, generalmente aprovechando alguna vulnerabilidad (por ejemplo, un desbordamiento de búfer).

Actualización de seguridad: las actualizaciones tienen como objetivo reparar problemas específicos de vulnerabilidades que se presentan en un programa. Algunas veces, en lugar de liberar un sólo parche o actualización, los distribuidores publican una versión actualizada de su software, aunque podrían referirse a ésta como un parche.

Servidor: un servidor es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

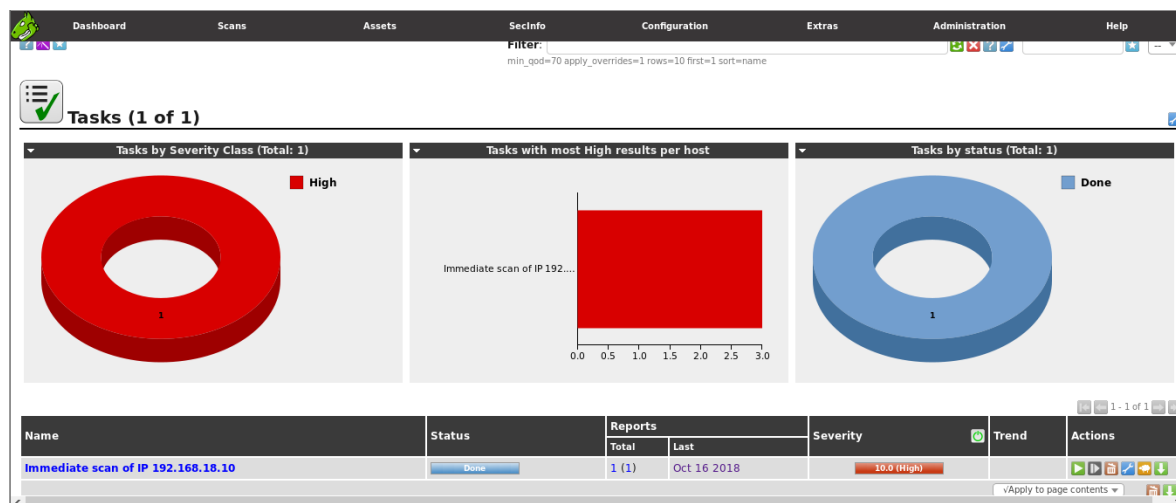
INFORME EJECUTIVO WINDOWS SERVER 2012

RESUMEN DEL ANÁLISIS DE VULNERABILIDADES:

Durante el análisis del servidor Windows Server 2012, en donde se conocía de antemano, que tenía los siguientes servicios configurados; DNS, HTTP, Active Directory y Servidor de Correo Exchange, con la ayuda del software de escaneo de redes openvas, se pudieron detectar 207 reportes y 2017 vulnerabilidades, de las cuales solo 4 se detectaron en nivel alto.

El reporte mostró fallas en los servicios de la empresa, en los servicios de HTTP asociados a los puertos 443/TCP, 444/TCP y 445/TCP, por lo que la empresa debe aplicar las soluciones dadas por el software de vulnerabilidades openvas, entre esas medidas están las de actualizar software, parchar sistemas, ejecutar las actualizaciones brindadas por Windows Update y consultar las referencias basadas en CERT y otras referencias captadas durante el análisis de vulnerabilidades.

ANÁLISIS GRÁFICO CON CLASIFICACIÓN DE VULNERABILIDADES Y LOS ACTIVOS QUE AFECTA.



Clasificación: alta.

Impacto

Delincuentes informáticos pueden aprovecharse de estas vulnerabilidades para ejecutar códigos arbitrarios de forma remota sin que la empresa lo autorice, las faltas de actualizaciones seguras pueden dar lugar para la explotación de códigos que pueden interrumpir la actividad normal de la empresa desde el área que depende de sistemas informáticos, que por lo general son casi todas las dependencias.

Todos aquellos equipos que tengan sistemas operativos

Windows 7
Windows 8,
Microsoft Windows 10 x32/x64 Edition
Microsoft Windows Server 2012 Edition
Microsoft Windows Server 2016
Microsoft Windows 8.1 x32/x64 Edition
Microsoft Windows Server 2012 R2 Edition
Microsoft Windows 7 x32/x64 Edition Service Pack 1
Microsoft Windows Vista x32/x64 Edition Service Pack 2
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Se ven altamente afectados por estas vulnerabilidades encontradas.

FUENTES Y/O REFERENCIAS

<https://randed.com/falso-positivo-y-falso-negativo/>

<https://www.internetya.co/que-es-el-servicio-ftp-file-transfer-protocol/>

http://www.alegsa.com.ar/Dic/ftp_anonimo.php

https://es.wikipedia.org/wiki/Informaci%C3%B3n_sensible

<https://tools.ietf.org/html/rfc2616>

<https://shieldnow.co/2013/03/01/http-trace-track-methods-allowed/>

<http://aprendeenlinea.udea.edu.co/lms/moodle/mod/page/view.php?id=73890>

<https://developer.mozilla.org/es/docs/Web/HTTP/Methods>

<https://diego.com.es/ataques-xss-cross-site-scripting-en-php>

<https://www.hostinger.es/tutoriales/que-es-ssh#gref>

<https://www.ecured.cu/Algoritmo>

https://www.segu-info.com.ar/proyectos/p1_algoritmos-basicos.htm

<https://latam.kaspersky.com/resource-center/definitions/encryption>

<https://infortelecom.es/blog/que-es-un-servidor-y-para-que-sirve/>

https://www.ecured.cu/Arquitectura_Cliente_Servidor

https://www.ibm.com/support/knowledgecenter/es/SSGU8G_12.1.0/com.ibm.sec.doc/ids_en_010.htm

<https://www.ecured.cu/RC4>

[https://es.wikipedia.org/wiki/Cifrado_por_bloques#Cipher-block_chaining_\(CBC\)](https://es.wikipedia.org/wiki/Cifrado_por_bloques#Cipher-block_chaining_(CBC))

<https://support.microsoft.com/es-uy/help/3042553/ms15-034-vulnerability-in-http-sys-could-allow-remote-code-execution-a>

<https://es.ccm.net/contents/281-protocolo-tcp>

<https://01seguridad.wordpress.com/2013/10/18/entender-la-explotacion-software/>

<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-034>

[https://es.wikipedia.org/wiki/Parche_\(inform%C3%A1tica\)](https://es.wikipedia.org/wiki/Parche_(inform%C3%A1tica))

<https://definicion.de/codigo/>

https://www.ecured.cu/Ataque_inform%C3%A1tico

<https://tecnologia-informatica.com/el-sistema-operativo/>

<https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/>

<https://www.techopedia.com/definition/32180/vendor-patch>

<https://www.lifewire.com/what-is-windows-update-2624597>

https://es.wikipedia.org/wiki/Pila_de_protocolos

<https://docs.microsoft.com/en-us/aspnet/core/fundamentals/servers/httpsys?view=aspnetcore-2.1>

<https://es.ccm.net/contents/264-el-protocolo-http#solicitud-http>

<https://developer.mozilla.org/es/docs/Web/HTTP/Methods>

https://es.wikipedia.org/wiki/Ejecuci%C3%B3n_arbitraria_de_c%C3%B3digo

<https://www.cert.org.mx/historico/documento/index.html-id=27>

<http://www.onyxsystems.es/que-es-un-servidor.html>

