WINDOW EXPLOITABLE

CAJA NEGRA TECNICA

CRITICOS :

-----No vulnerable a las criticas de apache por tener instalado el apache tomcat 8.0

# 1.- Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (chequeo increído).

Metasploit (CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Usar después de Gratis)

El huésco remoto se ve afectado por una vulnerabilidad de ejecución de código remoto en el Protocolo de escritorio remoto (RDP). Un atacante remoto no autentictico puede explotar esto, a través de una serie de peticiones especialmente elaboradas, para ejecutar código arbitrario.

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

------No tiene instalado la maquina pHP

# 2.- MS11-030: Vulnerabilidad en la Resolución DNS podría permitir la ejecución del código remoto (2509553) (chequeo remoto)

DNSAPI.dll en el cliente DNS en Microsoft Windows XP SP2 y SP3, Windows Server 2003 SP2, Windows Vista SP1 y SP2, Windows Server 2008 Gold, SP2, R2 y R2 SP1, y Windows 7 Gold y SP1 no procesa adecuadamente las consultas DNS, que permite a los atacantes remotos ejecutar código arbitrario a través de (1) una consulta de emisión LLMNR creada o (2) una aplicación artesanal, alias "DNS Query Vulnerabilidad".

**echa de publicación de parche:** 4/12/2011

**Fecha de publicación de la vulnerabilidad:** 4/12/2011

#### Explotable con

Impacto básico

Metasploit(Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS)

HIGH

# 1.- MS17-010: Actualización de seguridad para Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRcks) (Petya) (chequeo nocreído)

#### Descripción

El host remoto de Windows se ve afectado por las siguientes vulnerabilidades:  
  
- Existen múltiples vulnerabilidades de ejecución de código remoto en Microsoft Server Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autentictico puede explotar estas vulnerabilidades, a través de un paquete especialmente elaborado, 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 Mesage Block 1.0 (SMBv1) debido al manejo inadecuado de ciertas solicitudes. Un atacante remoto no autentictado puede explotar esto, a través de un paquete especialmente elaborado, para revelar información sensible. (CVE-2017-0147)  
  
ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades del Grupo de Ecuación y exploits divulgadas en 2017/04/14 por un grupo conocido como los Shadow Brokers. WannaCry / WannaCrypt es un programa de ransomware que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades del Grupo de Ecuación. Petya es un programa de ransomware que utiliza primero CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.

#### Solución

Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Microsoft también ha lanzado parches de emergencia para sistemas operativos Windows que ya no son compatibles, incluyendo Windows XP, 2003 y 8.  
  
Para sistemas operativos Windows sin soporte, por ejemplo. Windows XP, Microsoft recomienda a los usuarios que dejen de usar SMBv1. SMBv1 carece de características de seguridad que se incluyeron en versiones posteriores de SMB. SMBv1 se puede desactivar siguiendo las instrucciones del proveedor proporcionadas en Microsoft KB2696547. Además, US-CERT recomienda a los usuarios bloquear SMB directamente bloqueando el puerto TCP 445 en todos los dispositivos de límites de red. Para SMB sobre la API de NetBIOS, bloquee los puertos TCP 137 / 139 y UDP puertos 137 / 138 en todos los dispositivos de límites de red.

#### Detalles de Plugin

**Severidad:** alta

**ID:** 97833

**Nombre del archivo:** ms17-010.nasl

**Versión:** 1.30

**Tipo:** remoto

**Agente:** ventanas

**Familia:** [Windows](https://www.tenable.com/plugins/nessus/families/Windows)

**Publicado:** 20/03/2017

**Actualizado:** 5/25/2022

**Sensores apoyados:** Nesso

#### Información de riesgos

##### [VPR](https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss)

**Factor de riesgo:** crítico

**Puntuación:** 9,7

##### [CVSS v2](https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=AV:N/AC:M/Au:N/C:C/I:C/A:C)

**Factor de riesgo:** Alto

**Puntuación de la base:** 9.3

**Puntuación temporal:** 8.1

**Vector:** CVSS2-AV:N/AC:M/Au:N/C:C/I:C/A:C/A:C:C

**Fuente de Puntuación de CVSS:** [CVE-2017-0148](https://www.tenable.com/cve/CVE-2017-0148)

##### [CVSS v3](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C&version=3.0)

**Factor de riesgo:** Alto

**Puntuación de base:** 8.1

**Puntuación temporal:** 7.7

**Vector:** CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/A:H

**Víctor Temporal:** CVSS:3.0/E:H/RL:O/RC:C

#### Información de vulnerabilidad

**CPE:** cpe:/o:microsoft:windows

**Artículos de KB requeridos:** Host/OS, SMB/SMBv1-is-apsoportado

**Exploto Disponible:** verdad

**Exploit Ease:** Los explotas están disponibles

**Fecha de publicación de parche:** 14/03/2017

**Fecha de publicación de vulnerabilidad:** 14/03/2017

**CISA Known Exploited Vulnerability Due Dates:** 15/052022, 27/04/2017, 5/3/2022, 6/14/2022, 8/10/2022

#### Explotable con

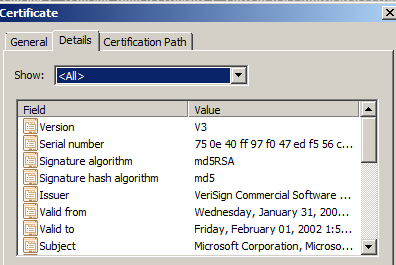
CANVAS(CANVAS)

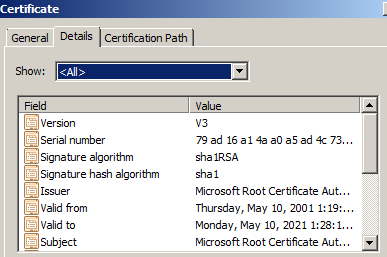
Impacto básico

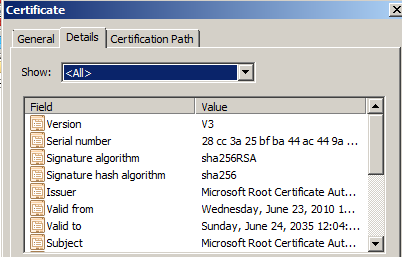
Metasploit(SMB DOBLEPULSAR Remote Code Execution)

# 2.- SSL Certificate Signed Using Weak Hashing Algorithm

El servicio remoto utiliza una cadena de certificados SSL que ha sido firmada usando un algoritmo de hashing criptográficamente débil (por ejemplo. MD2, MD4, MD5, o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, permitiendo a un atacante disfrazarse que el servicio afectado.  
  
Tenga en cuenta que este plugin reporta todas las cadenas de certificados SSL firmadas con SHA-1 que expiran después del 1 de enero de 2017 como vulnerables. Esto está de acuerdo con el arreglo gradual de Google del algoritmo de hash criptacrigráfico SHA-1.  
  
Tenga en cuenta que los certificados en la cadena que están contenidos en la base de datos Nessus CA (conocida-CA.inc) han sido ignorados.







Podemos ver q el sistema es vulnerable sha 1 y md5

El MD5 Message-Digest Algoritm no es resistente a la colisión, lo que facilita que los atacantes dependientes del contexto lleven a cabo ataques de la osto, como lo demuestran los ataques al uso de MD5 en el algoritmo de firma de un certificado X.509.

SHA-1 no es resistente a la colisión, lo que facilita que los atacantes dependientes del contexto lleven a cabo ataques de la suqueta, como lo demuestran los ataques al uso de SHA-1 en TLS 1.2. NOTA: este CVE existe para proporcionar un identificador común para hacer referencia a este número SHA-1; la existencia de un identificador no es, por sí misma, una recomendación de tecnología.

No usar cifrados entre 64 a 112bts, ya que son débiles a los ataques criptográficos sweet32.

**3,. MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)**

Existe una vulnerabilidad arbitraria de código remoto en la aplicación del Protocolo de escritorio remoto (RDP) en el host remoto de Windows. La vulnerabilidad se debe a la forma en que RDP accede a un objeto en memoria que ha sido inicializado incorrectamente o ha sido borrado.   
  
Si se ha habilitado RDP en el sistema afectado, un atacante remoto no autentictico podría aprovechar esta vulnerabilidad para hacer que el sistema ejecute código arbitrario enviándole una secuencia de paquetes RDP especialmente elaborados.   
  
Este plugin también comprueba la vulnerabilidad de denegación de servicio en Microsoft Terminal Server.   
  
Tenga en cuenta que este script no detecta la vulnerabilidad si las 'Pertensión de permitir las conexiones solo desde ordenadores que ejecutan escritorio remoto con la Auténtica de nivel de red' está activada o la capa de seguridad se establece en 'SSL (TLS 1.0)' en el host remoto.

**Exploto Disponible:** verdad

**Exploit Ease:** Los explotas están disponibles

**Fecha de publicación:** 13/03/2012

**Fecha de publicación de la vulnerabilidad:** 13/03/2012

#### Explotable con

CANVAS(Blanco,Phófforo)

Impacto básico

Metasploit(MS12-020 Microsoft Remote Desktop Checker)

#### Información de referencia

**CVE:** [CVE-2012-0002,](https://www.tenable.com/cve/CVE-2012-0002) [CVE-2012-0152](https://www.tenable.com/cve/CVE-2012-0152)

**BID:** [52353,](http://www.securityfocus.com/bid/52353) [52354](http://www.securityfocus.com/bid/52354)

**IAVA:** 2012-A-0039

**MSFT:** MS12-020

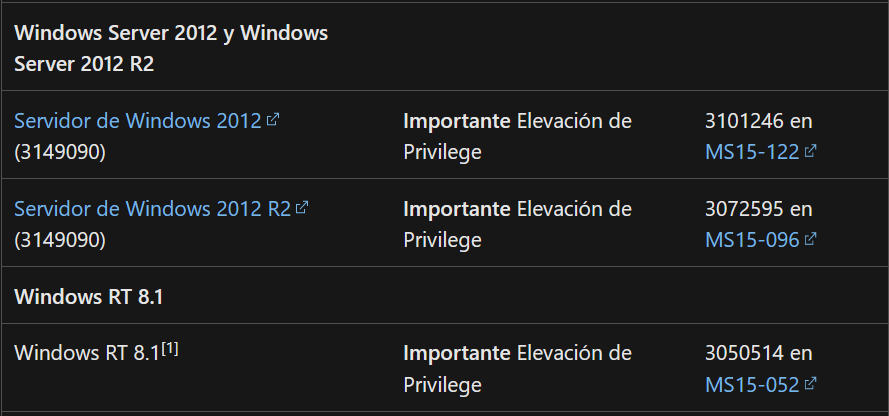
**MSKB:** [2621440](https://support.microsoft.com/kb/2621440), [2667402](https://support.microsoft.com/kb/2667402)

**3.- MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)**

#### Descripción

El huésped remoto de Windows se ve afectado por una elevación de la vulnerabilidad de privilegios en los protocolos de la Autoridad de Seguridad de la Cuenta de Seguridad (SAM) y la Autoridad de Seguridad Local (Política de Dominio) (LSAD) debido a la negociación inadecuada de nivel de autenticación sobre los canales de Llamada de Procedimiento Remoto (RPC). Un atacante hombre en medio capaz de interceptar comunicaciones entre un cliente y un servidor que alojan una base de datos SAM puede explotar esto para forzar el nivel de autenticación a rebajar la calidad, permitiendo al atacante suplantar a un usuario autenticado y acceder a la base de datos SAM.

1. **SAM (Security Account Manager)**:
   * **Función**: El canal SAM se utiliza para acceder y gestionar la base de datos de cuentas de seguridad en un sistema Windows. Esta base de datos contiene información sobre las cuentas de usuario y grupo, incluyendo contraseñas y políticas de seguridad.
   * **Uso**: Es crucial para la autenticación y autorización de usuarios en el sistema. Los administradores y ciertos servicios del sistema utilizan este canal para realizar tareas como la creación, modificación y eliminación de cuentas de usuario.
2. **LSAD (Local Security Authority Database)**:
   * **Función**: El canal LSAD se utiliza para acceder a la base de datos de la Autoridad de Seguridad Local (LSA). Esta base de datos contiene información sobre políticas de seguridad, privilegios de usuario y otros datos relacionados con la seguridad del sistema.
   * **Uso**: Es utilizado por el sistema operativo y aplicaciones para consultar y modificar políticas de seguridad, gestionar privilegios y realizar auditorías de seguridad.



**4.- SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)**.- Esta vulnerabilidad tiene una severidad de 5.3 y una urgencia en resolución de 2.9, a través de la cual, es posible obtener información sensible de un host remoto con servicios habilitados para SSL/TLS, en versiones 3.0 y 1.0, permitiendo ataques de divulgación de información, no siendo afectadas las versiones TLS 1.1, 1.2 y las demás suites que no usen el modo CBC.

Este plugin malicioso funciona intentando establecer conexión remota SSL/TLS, usando las versiones afectadas. Si lo datos son devueltos no fragmentado sen un registro vacio, siendo ésta medida usada por openSSL, como contramedidas menos que se especifique la opción “'SSLOP-DONT-INSERT-EMPTY-FRAGMENTS” cuando se inicializa, siendo contraolable a través de la clave del registro de Windows clave de registro HKEY-LOCAL-MACHINE-System-CurrentControlSet-Control-SecurityProviders-SCHANNEL-SendExtraRecord.

La solución a esta vulnerabilidad es configurar los servidores cpara uso exclusivo con TLS 1.1 o TLS 1.2 p suites que no usen cifrado de bloque, existiendo un parche de seguridad de Windows para su corrección: KB2643584

#### Descripción

El protocolo SSL, tal como se utiliza en ciertas configuraciones en Microsoft Windows y Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, y otros productos, cifra los datos utilizando el modo CBC con vectores de inicialización encadenado, que permite a los atacantes de man-in-the-middle obtener encabezados HTTP de texto a través de un ataque atador elegido en bloque (BCBA) en una sesión HTTPS, en conjunto con el código JavaScript que utiliza (1) la API de entrada web HTML5, (2) el URLC JavaC de URLCAPI deonnection, o (3) la API de Silverlight WebClient, alias un ataque "BEAST".

WEB

<https://www.tenable.com/plugins/nessus/125313>

<https://www.tenable.com/cve/CVE-2019-0708>

<https://www.tenable.com/plugins/nessus/53514>

<https://www.tenable.com/cve/CVE-2011-0657>

<https://www.tenable.com/cve/CVE-2011-3389>

<https://www.tenable.com/plugins/nessus/97833>

<https://www.tenable.com/cve/CVE-2017-0145>

<https://www.tenable.com/cve/CVE-2017-0143>

<https://www.tenable.com/cve/CVE-2017-0144>

<https://www.tenable.com/cve/CVE-2017-0146>

<https://www.tenable.com/cve/CVE-2017-0147>

<https://www.tenable.com/plugins/nessus/97833>

<https://www.tenable.com/plugins/nessus/35291>

<https://www.tenable.com/plugins/nessus/42873>

<https://www.tenable.com/cve/CVE-2016-2183>

<https://www.tenable.com/plugins/nessus/58435>

<https://www.tenable.com/cve/CVE-2012-0002>

<https://www.tenable.com/cve/CVE-2012-0152>

<https://www.tenable.com/plugins/nessus/90510>

<https://www.tenable.com/plugins/nessus/58751>

<https://www.tenable.com/cve/CVE-2016-0128>

<https://msrc.microsoft.com/update-guide/>

este comando genera un certificado autofirmado válido por 365 días.

openssl req -new -x509 -keyout fake\_cert.pem -out fake\_cert.pem -days 365 -nodes