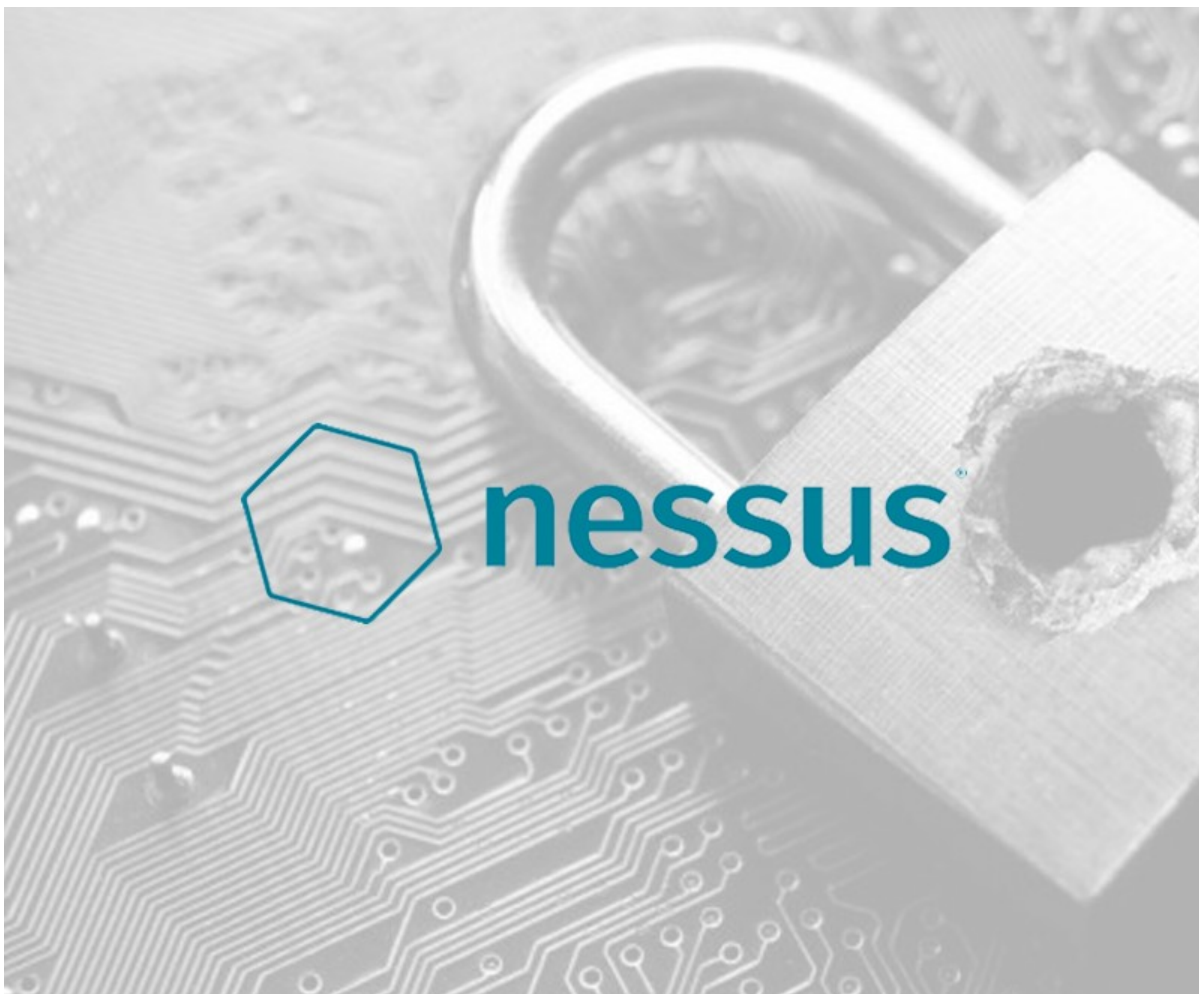


securitytwins.com

Detectando vulnerabilidades con Nessus - Security Twins

6-7 minutos



Hola

En esta ocasión os voy a hablar de una herramienta, muy completa y muy útil para la localización de vulnerabilidades, vamos a ver como se instala, configura y se usa, así que vamos al lío.

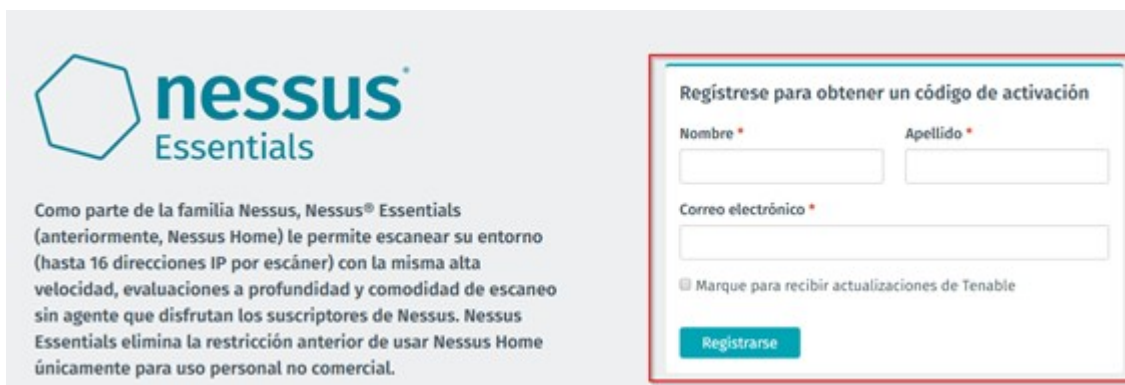
- [Preparación](#)
- [Instalación](#)
- [Configuración](#)
- [Detección de Vulnerabilidades](#)

Preparación

Pasos instalación, configuración y uso de Nessus.

Primero debemos obtener la clave de activación de nessus, en este caso usaremos nessus essentials ya que es gratuito, pero nos servirá para poder ver como es esta herramienta y probarla.

Enlace de registro: [Registro Nessus](#)



nessus[®] Essentials

Como parte de la familia Nessus, Nessus[®] Essentials (anteriormente, Nessus Home) le permite escanear su entorno (hasta 16 direcciones IP por escáner) con la misma alta velocidad, evaluaciones a profundidad y comodidad de escaneo sin agente que disfrutaron los suscriptores de Nessus. Nessus Essentials elimina la restricción anterior de usar Nessus Home únicamente para uso personal no comercial.

Regístrese para obtener un código de activación

Nombre * Apellido *

Correo electrónico *

☐ Marque para recibir actualizaciones de Tenable

Registrarse

Activating Your Nessus Essentials Subscription

Your activation code for Nessus Essentials is:

1134-1004-1011-1011-1011

This is a one time code. If you uninstall and then reinstall you will need to register the scanner again and receive another activation code.

After initial installation of Nessus you will be prompted to set up and activate your scanner. For further details on activating your subscription review the [installation guide](#).

Una vez que hemos obtenido nuestro código de activación ya solo







debemos descargar la versión correspondiente.

En mi caso al poseer un Windows 10 x64 yo descargaré la segunda opción.

Enlace de descarga: [Descargar Nessus](#)

 Nessus-8.6.0-Win32.msi	Windows 7, 8, 10 (32-bit)	89.7 MB	Aug 13, 2019	Checksum
 Nessus-8.6.0-x64.msi	Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016 (64-bit)	95.1 MB	Aug 13, 2019	Checksum
 Nessus-8.6.0.dmg	macOS (10.8 - 10.14)	84.6 MB	Aug 13, 2019	Checksum

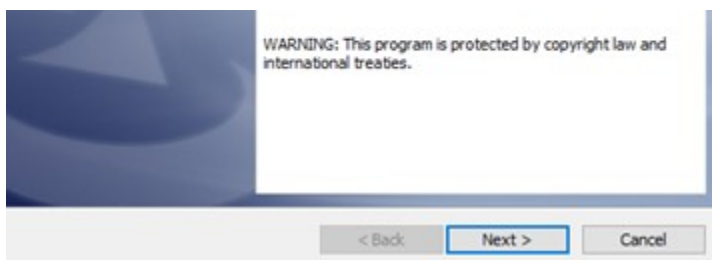
Si por lo contrario posee otra opción u otro sistema como Linux o Windows tan solo debemos descargar la versión correcta.

 Nessus-8.6.0-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09	78 MB	Aug 13, 2019	Checksum
 Nessus-8.6.0-debian6_amd64.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 AMD64	77.7 MB	Aug 13, 2019	Checksum
 Nessus-8.6.0-debian6_i386.deb	Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3 i386(32-bit)	75.7 MB	Aug 13, 2019	Checksum
 Nessus-8.6.0-es5.x86_64.rpm	Red Hat ES 5 (64-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	77.8 MB	Aug 13, 2019	Checksum
 Nessus-8.6.0-es5.i386.rpm	Red Hat ES 5 i386(32-bit) / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel)	75.6 MB	Aug 13, 2019	Checksum
 Nessus-8.6.0-es6.x86_64.rpm	Red Hat ES 6 (64-bit) / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise	77.8 MB	Aug 13, 2019	Checksum

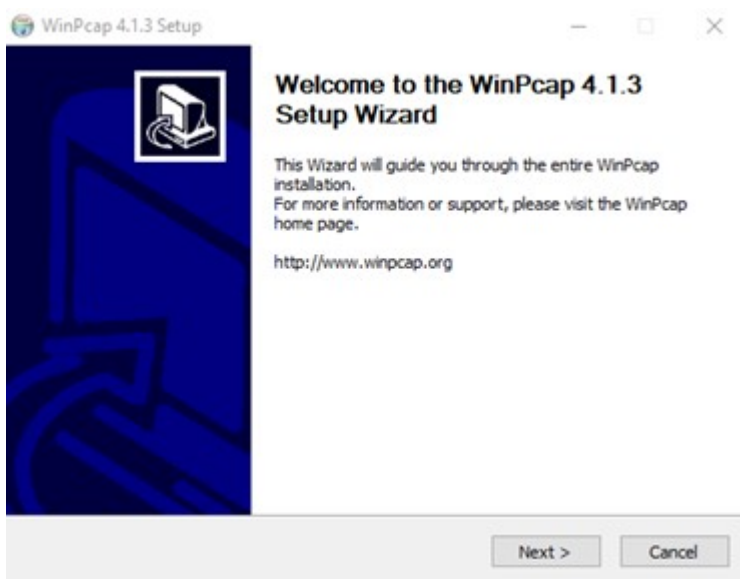
Instalación

Una vez que hemos descargado el instalador lo ejecutamos y procedemos a su instalación.





Durante la instalación de nessus, nos saltará el instalador para WinCap para proceder con su instalación, si ya lo tienes instalado no hace falta que lo instales.

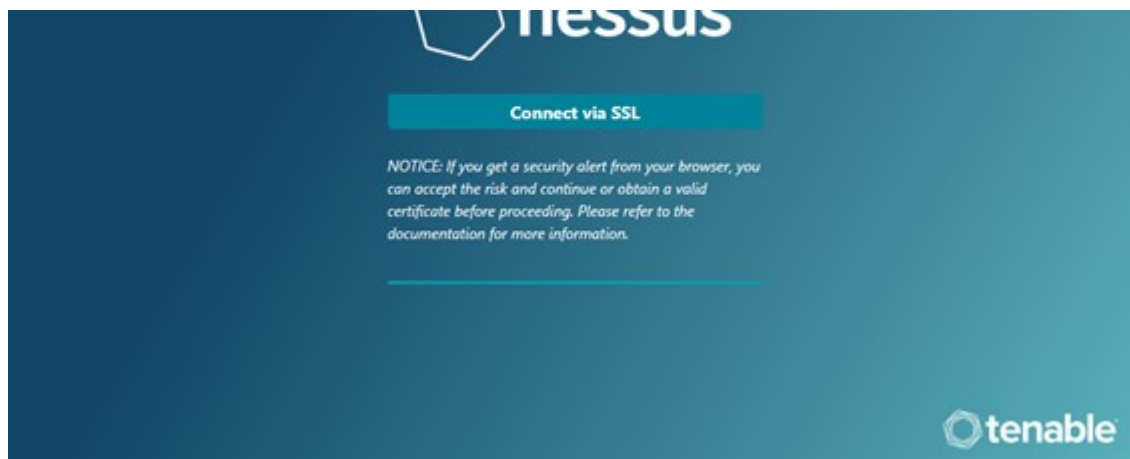


Una vez que se haya finalizado con la instalación, se nos abrirá el navegador web para proseguir con la configuración.

Wincap: Es la herramienta estándar de la industria para acceder a la conexión entre capas de red en entornos Windows. Permite a las aplicaciones capturar y transmitir los paquetes de red puenteando la pila de protocolos.

Configuración





Hacemos clic en *Connect via SSL*

Si nos sale una advertencia indicándonos de que este sitio no es seguro, no te preocupes, Accedemos a él.

Este sitio no es seguro.

Es posible que haya una persona que intenta engañarte o robar la información que envíes al servidor. Deberías cerrar este sitio inmediatamente.

[Ir a la página Inicio](#)

Detalles

Tu equipo no confía en el certificado de seguridad de este sitio web.

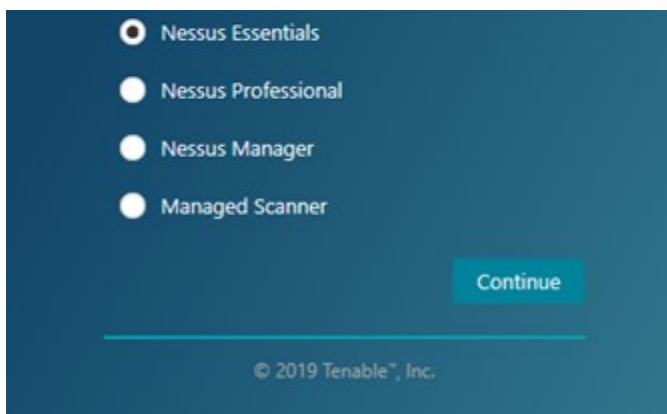
El nombre de host del certificado de seguridad del sitio web es distinto del sitio web que intentas visitar.

Código de error: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

[Acceder a la página web \(No recomendado\)](#)

Elegimos la versión que vamos a instalar, en nuestro caso Nessus Essentials.



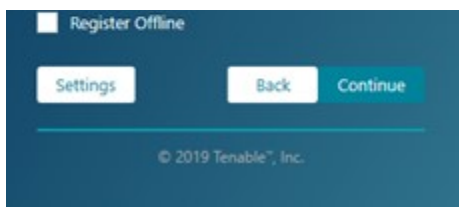


Una vez que hacemos clic en continuar nos mostrará un formulario para introducir nuestros datos, para obtener un código de activación, si ya tienes el código de activación hacemos clic en skip, si no introduces tus datos y haz clic en email para obtenerlo.

A screenshot of the Nessus Essentials registration form. The header shows the 'nessus Essentials' logo. Below it, the text 'Get an activation code' is followed by instructions: 'To receive an email with a free Nessus Essentials activation code, enter your information.' and 'If you already have an activation code, skip this step.' The form includes input fields for 'First *' (containing 'John'), 'Last *' (containing 'Smith'), and 'Email *' (containing 'user@example.com'). At the bottom, there are three buttons: 'Skip' (highlighted with a red rectangle), 'Back', and 'Email'. The copyright notice '© 2019 Tenable®, Inc.' is at the very bottom.

Introducimos nuestro código de activación y hacemos clic en Continuar.

A screenshot of the Nessus Essentials registration form, showing the 'Register Nessus' section. It prompts the user to 'Enter your activation code.' and features an input field labeled 'Activation Code *'. The input field contains a blurred, illegible string of characters. The background is dark blue with the 'nessus Essentials' logo at the top.



NOTA: Si tienes configurado algún proxy en la red te recomiendo que le eches un vistazo la opción de *Settings*, para configurarlo.



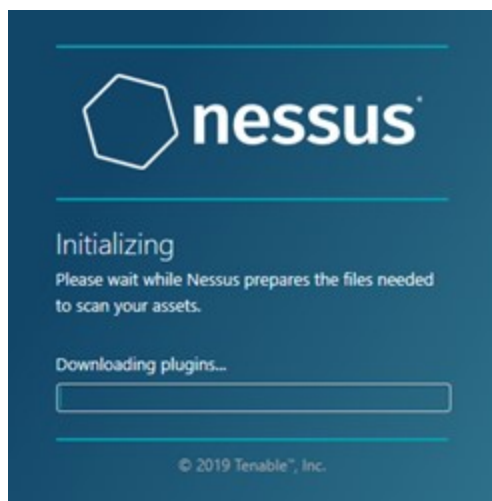
Se nos pide que creamos una cuenta de administración proporcionando nombre de usuario y contraseña.

NOTA: El uso de nombres de usuario como *admin* o contraseñas como *123456789*, no son para nada recomendables, ya que usando herramientas de fuerza bruta como **John The Ripper** o **Hydra** (Las veremos en un futuro artículo) se podrían obtener estas credenciales.

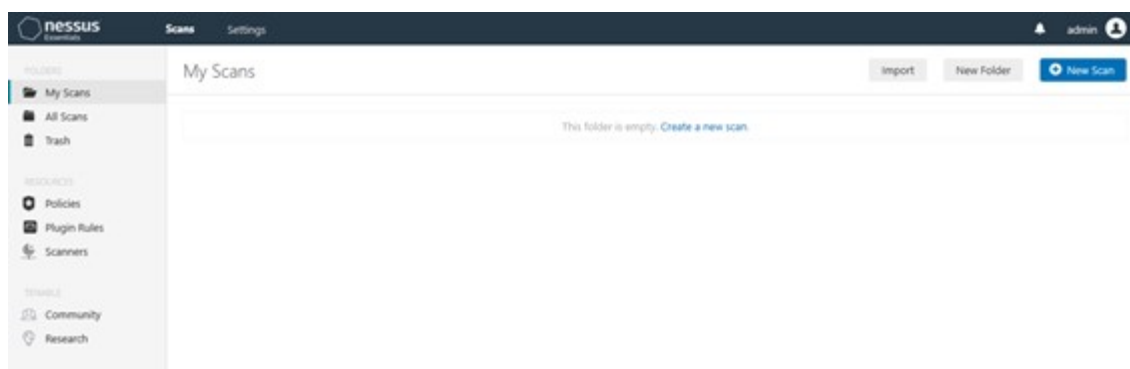
He usado estas credenciales solo y exclusivamente para la realización de este tutorial.

Ahora solo debemos esperar finalice la inicialización, tendremos

que tener paciencia ya que se demora mucho.



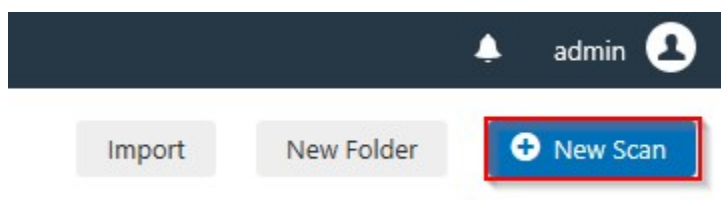
Una vez finalizada la instalación, podremos ver la interfaz.



Detección de vulnerabilidades

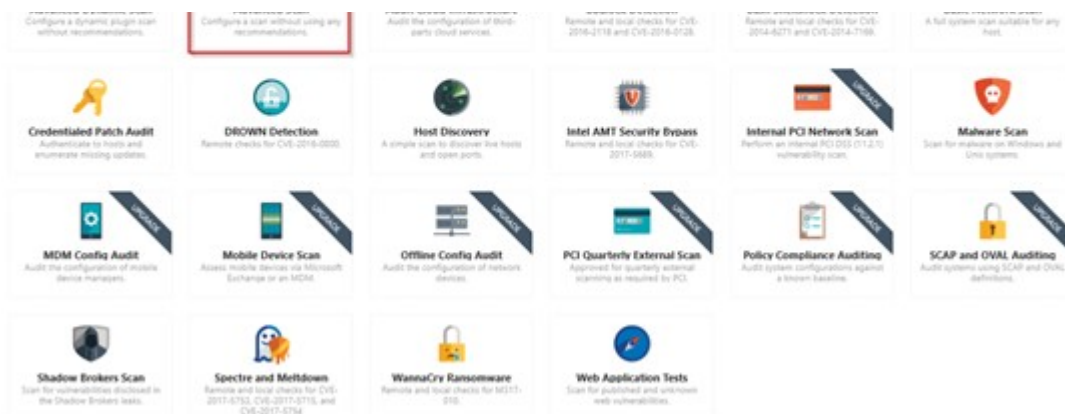
Una vez que ya está todo listo, ya podemos empezar, para ello debemos seguir los siguientes pasos.

Hacemos clic en *New Scan*.



Hacemos clic en Advanced Scan.





NOTA: Como podemos observar existen otras muchas opciones, estas las veremos en otro artículo, ahora nos enfocaremos en la búsqueda de vulnerabilidades.

Ahora simplemente vamos configurando nuestro escaner.

The image shows the Nessus configuration interface for a new scan. The 'Settings' tab is active, and the 'BASIC' section is expanded. The 'General' sub-section is selected. The 'Name' field is 'Prueba', the 'Description' is 'Esto es una prueba', the 'Folder' is 'My Scans', and the 'Targets' field contains '192.168.1.186'. There are 'Upload Targets' and 'Add File' buttons at the bottom. 'Save' and 'Cancel' buttons are at the very bottom.

Existen otras formas de añadir objetivos como:

Por rangos:

The image shows the 'Targets' field in the Nessus configuration interface. The text '192.168.1.186-192.168.1.190' is entered, representing an IP range.

Red:

Targets

192.168.1.0/24

Dominio:

Targets

prueba.com

Marcamos, las opciones que veamos oportunas, pero debemos hacerlo con cuidado ya que a más opciones marcadas más información y eso equivale a más tiempo.

BASIC

DISCOVERY

Host Discovery

Port Scanning

Service Discovery

ASSESSMENT

REPORT

ADVANCED

Remote Host Ping

Ping the remote host ☒

General Settings

☒ Test the local Nessus host
This setting specifies whether the local Nessus host should be scanned when it falls within the target range specified for the scan.

☐ Use fast network discovery
If a host responds to ping, Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. Fast network discovery bypasses those additional tests.

Ping Methods

☒ ARP

☒ TCP

Destination ports

☒ ICMP

☐ Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries

☒ UDP

BASIC

DISCOVERY

Host Discovery

Port Scanning

Service Discovery

ASSESSMENT

REPORT

ADVANCED

Ports

☐ Consider unscanned ports as closed

Port scan range:

Local Port Enumerators

☒ SSH (netstat)

☒ WMI (netstat)

☒ SNMP

☒ Only run network port scanners if local port enumeration failed

☐ Verify open TCP ports found by local port enumerators

Network Port Scanners

☒ SYN

☐ Override automatic firewall detection

The image displays four screenshots of the Nessus configuration interface, showing various settings for Discovery, Assessment, and Reporting. The interface is organized into a sidebar on the left with categories: BASIC, DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The main content area shows the configuration for the selected category.

Screenshot 1: General Settings (Discovery)

- ☒ Probe all ports to find services
Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.
- Search for SSL/TLS services: ☒
- Search for SSL/TLS on:
- Identify certificates expiring within x days:
- ☒ Enumerate all SSL/TLS ciphers
When selected, Nessus ignores the list of ciphers advertised by SSL/TLS services, and enumerates them by attempting to establish connections using all possible ciphers.
- ☐ Enable CRL checking (connects to the Internet)

Screenshot 2: Accuracy and Antivirus (Assessment)

- Accuracy**
 - ☐ Override normal accuracy
 - ☒ Avoid potential false alarms
 - ☐ Show potential false alarms
 - ☐ Perform thorough tests (may disrupt your network or impact scan speed)
- Antivirus**
 - Antivirus definition grace period (in days):

Screenshot 3: SMTP (Reporting)

- SMTP**
 - Third party domain:
This domain must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test might be aborted by the SMTP server.
 - From address:
 - To address:

Screenshot 4: General Settings (Assessment)

- General Settings**
 - ☒ Only use credentials provided by the user
Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.
- Oracle Database**
 - ☐ Test default accounts (slow)

Screenshot 5: User Enumeration Methods (Assessment)

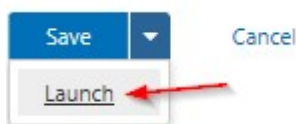
- User Enumeration Methods**
 - ☒ SAM Registry
 - ☒ ADSI Query
 - ☒ WMI Query
 - RID Brute Forcing: ☐

Como se ha podido observar no se han activado todas las opciones, solo se activaron aquellas que sean necesarias, para no alargar el análisis, pero entre las opciones disponibles, existen otras como la búsqueda de malware o el escaneo de aplicaciones web.

Existen otras dos opciones principales que son:

- **Credentials:** En esta opción añadiremos las credenciales en el caso en el que fuera necesario, por ejemplo, usuario y contraseña de Windows.
- **Plugins:** Aquí podremos ver todos los plugins que necesita nessus para realizar sus escáneres, podemos activarlos o desactivarlos a nuestro gusto.

Una vez que se ha terminado podemos guardarlo para lanzarlo posteriormente o lanzarlo inmediatamente.

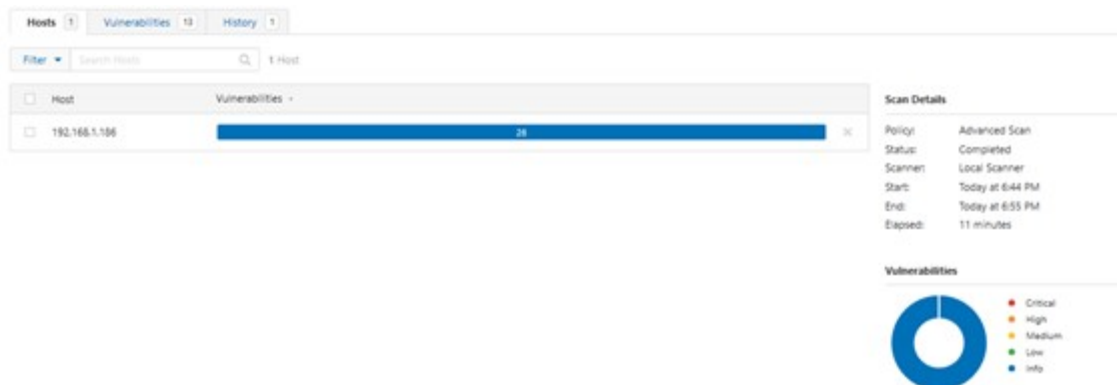


En nuestro caso lo lanzamos.

Ahora solo debemos tener un poco de paciencia.



Una vez que haya finalizado hacemos clic en el escáner para ver los resultados.



Podemos ver todo tipo de información como hosts, vulnerabilidades y un historial que indica las distintas ejecuciones

de este escáner.

Si hacemos clic en vulnerabilidades podemos verlas.

Sev	Name	Family	Count
Info	DCE Services Enumeration	Windows	8
Info	SMB (Multiple Issues)	Windows	7
Info	Common Platform Enumeration (CPE)	General	1
Info	Device Type	General	1
Info	Dropbox Software Detection (unauthenticated check)	General	1
Info	Ethernet Card Manufacturer Detection	Misc.	1
Info	Ethernet MAC Addresses	General	1
Info	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
Info	Local Checks Not Enabled (Info)	Settings	1
Info	Nessus Scan Information	Settings	1
Info	No Credentials Provided	Settings	1

Scan Details

Policy: Advanced Scan
 Status: Completed
 Scanner: Local Scanner
 Start: Today at 6:44 PM
 End: Today at 6:55 PM
 Elapsed: 11 minutes

Vulnerabilities

Donut chart showing 100% Info level results.

Como podemos ver no se han localizado vulnerabilidades, solo es información.

Vamos a repetir este análisis para en vez de una maquina en concreto toda la red, para que de esta manera asegurarme de que veáis vulnerabilidades.

¿Cómo se hace?

Hacemos clic en *configure*.

Configure | Audit Trail | Launch | Report | Export

Hosts | Vulnerabilities | History

Host | Vulnerabilities

192.168.1.186 | 26

Scan Details

Policy: Advanced Scan
 Status: Completed
 Scanner: Local Scanner
 Start: Today at 6:44 PM
 End: Today at 6:55 PM
 Elapsed: 11 minutes

Settings | Credentials | Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

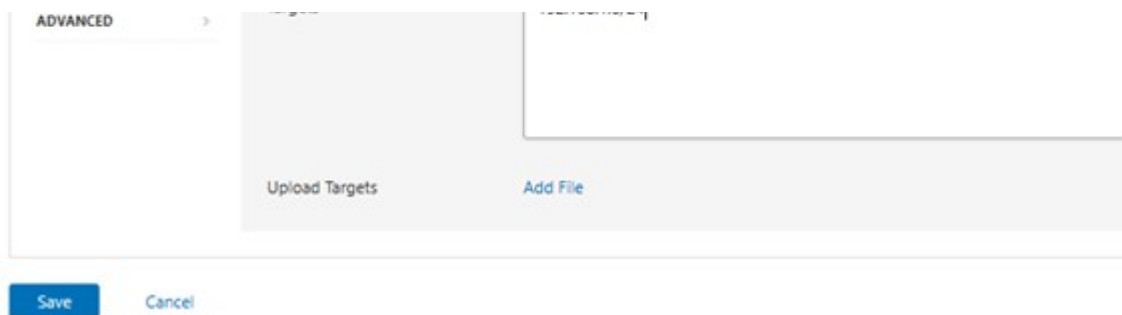
REPORT

Name: Prueba

Description: Esto es una prueba

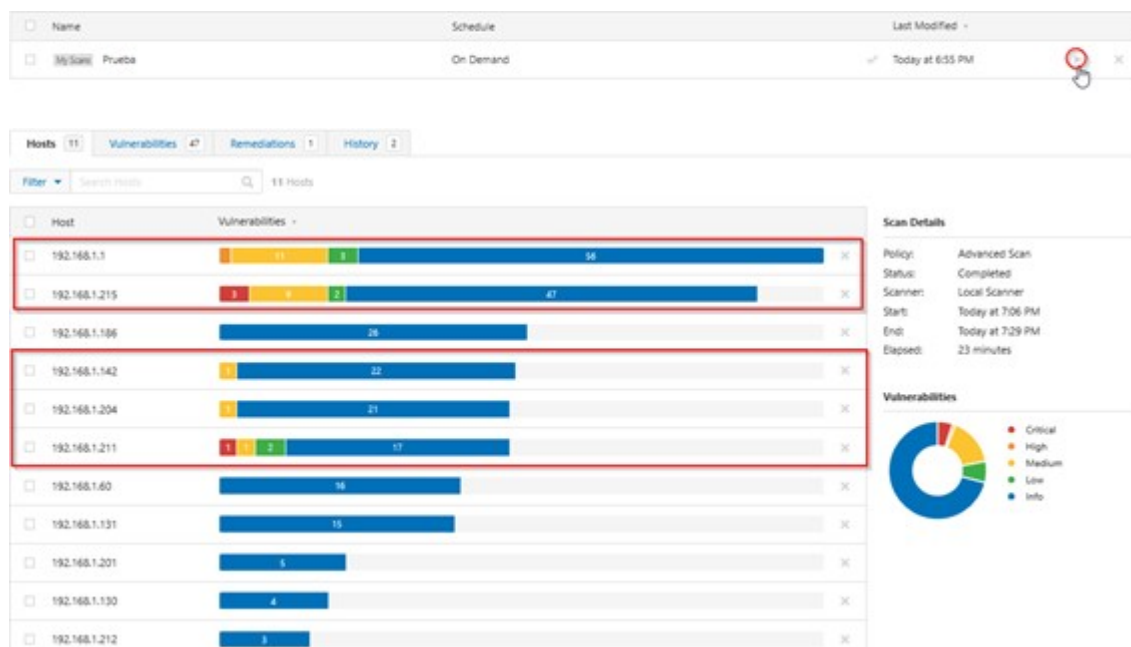
Folder: My Scans

Targets: 192.168.1.0/24



En vez de indicar la dirección IP indicamos la red entera y hacemos clic en *save*.

Luego en el menú lateral izquierdo nos dirigimos a *All Scans* y volvemos a lanzar nuestro escáner y ya simplemente esperamos.



Al repetir el análisis podemos ver en distintos equipos de la red existen vulnerabilidades, en dos de ellos críticos, para ver las vulnerabilidades de un equipo en concreto hacemos clic en el.

Como podemos ver se nos muestran las distintas vulnerabilidades y cada una por su nombre, para saber aún más información de una vulnerabilidad en concreto hacemos clic en ella.



<input type="checkbox"/>	MED	Microsoft Windows (Multiple Issues)	Misc.	4			DNS: WIN-JT968P5J49 MAC: 000C29D4543F OS: Microsoft Windows 7 Professional Start: Today at 7:21 PM End: Today at 7:25 PM Elapsed: 4 minutes KB: Download
<input type="checkbox"/>	MED	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows	1			Vulnerabilities Critical High Medium Low Info
<input type="checkbox"/>	MED	SSL Certificate Signed Using Weak Hashing Algorithm	General	1			
<input type="checkbox"/>	LOW	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	1			
<input type="checkbox"/>	INFO	SMB (Multiple Issues)	Windows	8			
<input type="checkbox"/>	INFO	DCE Services Enumeration	Windows	8			
<input type="checkbox"/>	INFO	Nessus SYN scanner	Port scanners	4			
<input type="checkbox"/>	INFO	TLS (Multiple Issues)	Service detection	2			
<input type="checkbox"/>	INFO	Common Platform Enumeration (CPE)	General	1			

Podemos ver que entre toda la información se nos proporciona una descripción de la vulnerabilidad y una posible solución.

Si nos fijamos en la parte derecha de la pantalla se nos ofrece más información como información del riesgo, sobre la vulnerabilidad, etc.

Vulnerabilities 29

Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MITM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MITM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstscapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

Solution

- Force the use of SSL as a transport layer for this service if supported, or/and
- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

See Also

<http://www.cisid.it/downloads/http-gbv.pdf>
<http://www.nessus.org/u/9033ba0f>
<http://technet.microsoft.com/en-us/library/cc782610.aspx>

Output

No output recorded.

Port	Hosts
3389/tcp/mrdp	192.168.1.215 0/

Plugin Details

Severity: Medium

ID: 18405

Version: 1.31

Type: remote

Family: Windows

Published: June 1, 2005

Modified: August 1, 2018

Risk Information

Risk Factor: Medium

CVSS Base Score: 5.1

CVSS Temporal Score: 3.8

CVSS Vector: CVSS2#AV/N/A/C/H/Au/N/C/R/I/R/A/P

CVSS Temporal Vector: CVSS2#E/U/R/L/D/R/R/C

Vulnerability Information

CPE: cpe:/o:microsoft/remote_desktop_connection

cpe:/o:microsoft/windows_terminal_services_using_rdp

Exploit Available: false

Exploit Ease: No known exploits are available

Vulnerability Pub Date: May 28, 2005

Reference Information

BID: 13818

CVE: CVE-2005-1754

Sé que este tutorial puede haber sido un poco largo, pero espero que os haya servido para conocer esta herramienta y ver qué podemos hacer con ella.

¿Se os ocurre alguna otra cosa que podemos hacer con nessus? ¿Cuántas vulnerabilidades habéis localizado? Dejadmelo en los comentarios 😊 .

Sed buenos.

15 de 15

30/11/2020 1:27