

NESSUS PARA EL ESCANEEO DE VULNERABILIDADES

CERTIFICADO DE PROFESIONALIDAD: SEGURIDAD INFORMÁTICA
Examen del módulo formativo: Gestión de servicios en el sistema informático

DIEGO MUCCI

ÍNDICE

| | |
|--|-----------|
| Enunciado | 1 |
| Actividad 1 | 2 |
| Selección y justificación de la herramienta..... | 2 |
| Actividad 2 | 3 |
| Instalación y configuración de la herramienta | 3 |
| En Windows 10..... | 3 |
| En Kali Linux..... | 7 |
| Actividad 3 | 20 |
| Objetivo: Analiza la efectividad de la herramienta. | 20 |

Enunciado

La empresa IRON S.L. desea implementar un sistema de monitorio de redes y sistemas para comprobar su operatividad y analizar su utilidad en la seguridad defensiva de una infraestructura de red.

Alternativamente también está pensando en diseñar un sistema de gestión de identidades.

Nos han pedido desarrollar un proyecto básico basado en la justificación, instalación y configuración de alguno de estos sistemas utilizando alguna de las siguientes herramientas:

- Hobbit-Xymon, Nagios, Cacti, OSSIM, QRADAR, OpenAM, AWS Identity, Microsoft Entra ID, Nessus, o cualquier otra cuya finalidad sea cubrir las necesidades declaradas de la empresa.

Actividad 1 (2,5 puntos)

Objetivo: Selección y justificación de la herramienta.

Tareas:

Redacta un pequeño informe justificando la elección de la herramienta seleccionada, basándose en sus características, ventajas, entorno de desarrollo en el que se va a implementar y cualquiera otra circunstancia que quieras hacer resaltar para determinar tu elección.

Actividad 2 (5 puntos)

Objetivo: Instalación y configuración de la herramienta.

Tareas:

1. Instalar y configura mínimamente la herramienta para comprobar su operatividad en al menos dos equipos o servicios en la red.
2. Describe, justifica, captura y documenta el proceso de instalación y configuración.

Actividad 3 (2,5 puntos)

Objetivo: Analiza la efectividad de la herramienta.

Tareas:

1. Justifica si la herramienta seleccionada cumple con las expectativas que se generaron inicialmente y relata si el coste-beneficio de la implementación es adecuado para su adopción.
2. Ventajas e inconvenientes que aprecies y si recomendarías a una empresa su implementación y los motivos que relatarías.

Actividad 1

Selección y justificación de la herramienta

En el ámbito de la ciberseguridad, la identificación y mitigación de vulnerabilidades en sistemas informáticos es una tarea crítica para proteger la integridad, confidencialidad y disponibilidad de los datos. Una herramienta que ha destacado en este campo es Nessus, un escáner de vulnerabilidades desarrollado por Tenable, Inc. Desde su creación en 1998, Nessus se ha consolidado como uno de los estándares de la industria para la evaluación de vulnerabilidades debido a su eficiencia, precisión y constante actualización.

Se ha elegido la herramienta Nessus ya que es ampliamente utilizada por profesionales de la seguridad, auditores y administradores de sistemas para identificar y evaluar las debilidades en la configuración de sistemas operativos, aplicaciones, dispositivos de red y servicios. Su capacidad para detectar una amplia gama de vulnerabilidades, desde configuraciones incorrectas y parches faltantes hasta vulnerabilidades en aplicaciones web, lo convierte en una herramienta indispensable en cualquier programa de seguridad informática.

El propósito de este trabajo es ofrecer una visión detallada del software Nessus, explorando su funcionalidad, características clave, y el impacto que tiene en la gestión de la seguridad de las redes. Analizaremos su proceso de instalación y configuración, así como los diversos tipos de escaneos que puede realizar. Asimismo, se discutirá cómo interpretar los resultados de los escaneos de Nessus y que soluciones se deberían implementar para remediar esas vulnerabilidades.

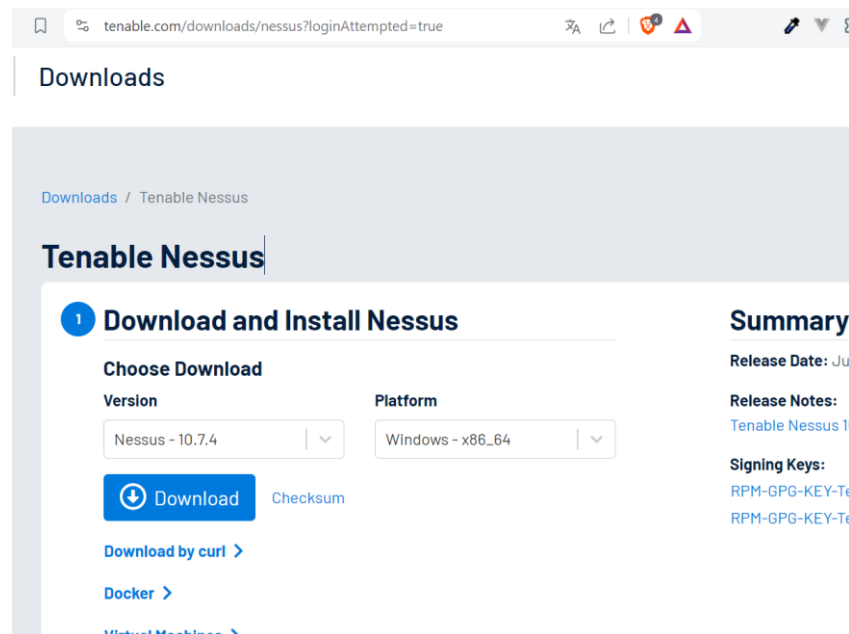
Este trabajo tiene como objetivo no solo familiarizar a los lectores con el uso de Nessus, sino también resaltar su importancia en el fortalecimiento de la postura de seguridad de las organizaciones. A través de un enfoque práctico y teórico, se espera proporcionar una comprensión integral de cómo Nessus contribuye a la protección de los activos digitales en un entorno cada vez más amenazado por ciberataques.

Actividad 2

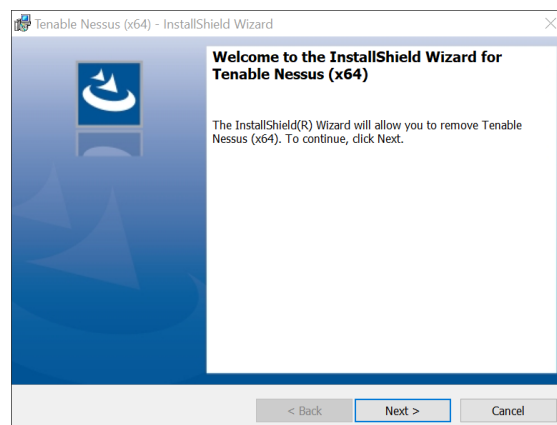
Instalación y configuración de la herramienta

En Windows 10

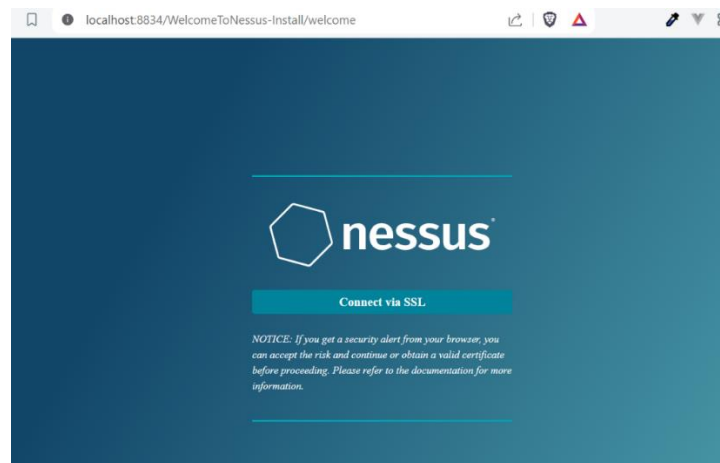
Lo primero de todo será dirigirnos a la web oficial <https://www.tenable.com/downloads/nessus?loginAttempted=true> y seleccionar la versión de Nessus que queremos descargar y el sistema operativo donde se va a instalar:



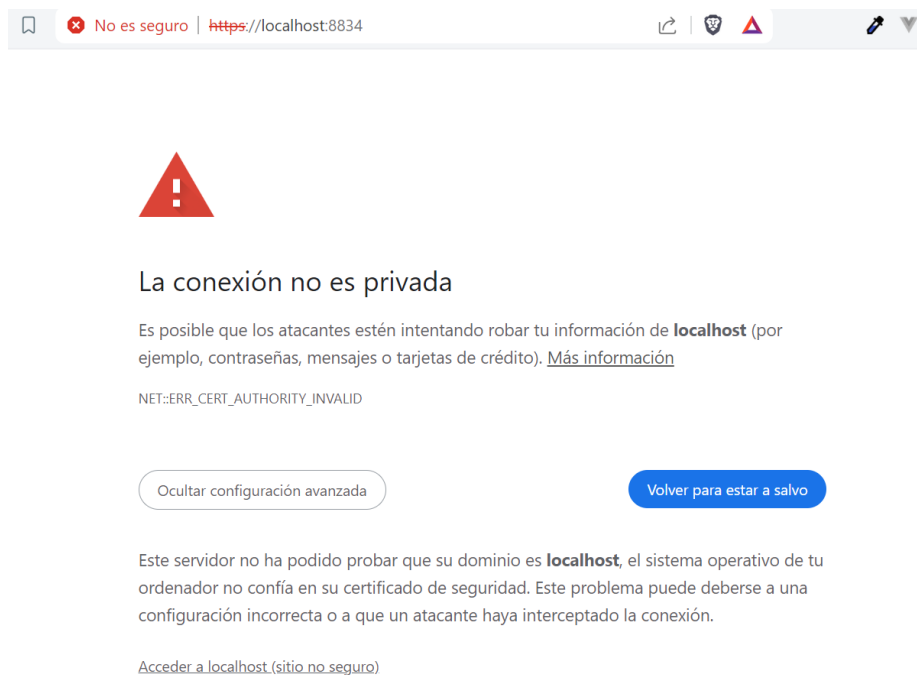
Se nos descargará un archivo con la extensión “.msi” que tendremos que ejecutar y seguir el proceso normal de instalación:



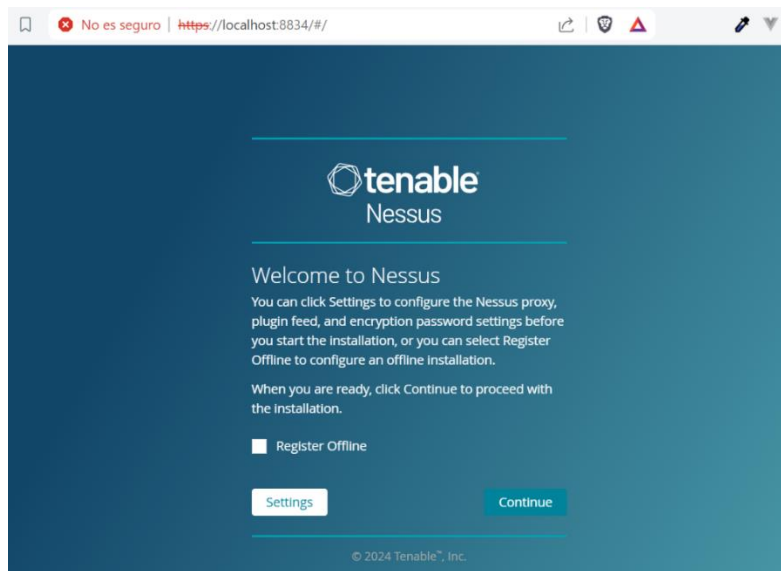
Después de la instalación, nos aparecerá la siguiente ventana en el navegador web. Le damos al botón *Connect via SSL*:



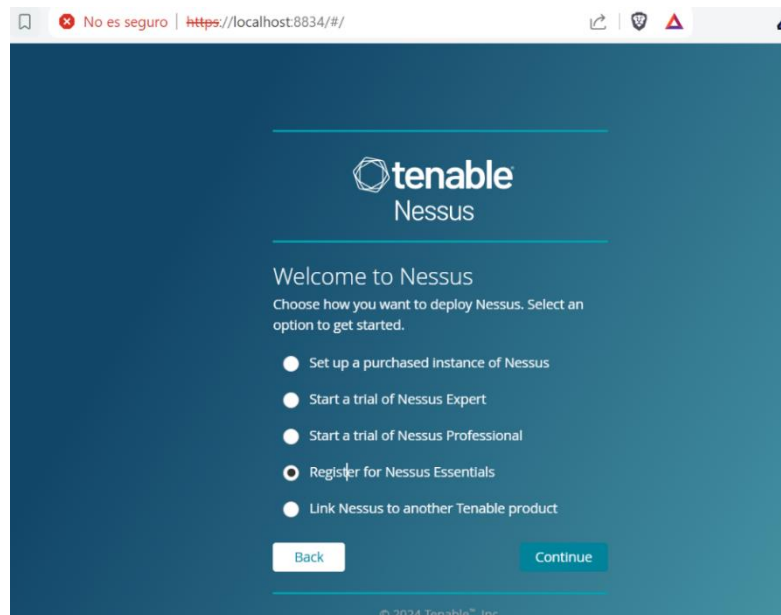
Aparecerá la alerta de que la conexión no es segura, esto es debido a que la conexión es mediante *http* y no *https*. Para poder acceder, clicamos en el enlace de abajo de todo donde dice *Acceder a localhost (sitio no seguro)*:



A continuación, le damos al botón *Continue* sin seleccionar la opción offline porque si no, nos dirá que necesitamos una licencia:



Seleccionamos *Register for Essentials* y le damos a *Continue*:

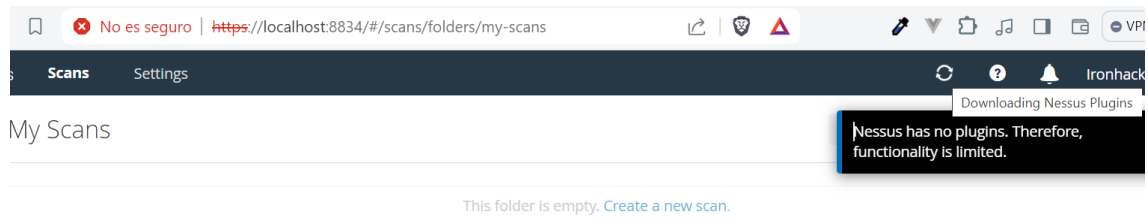


Escribimos nuestros datos, en este caso hemos utilizado una dirección de email temporal y un nombre ficticio:

Escribimos el nombre de usuario y la contraseña para poder acceder a la plataforma:

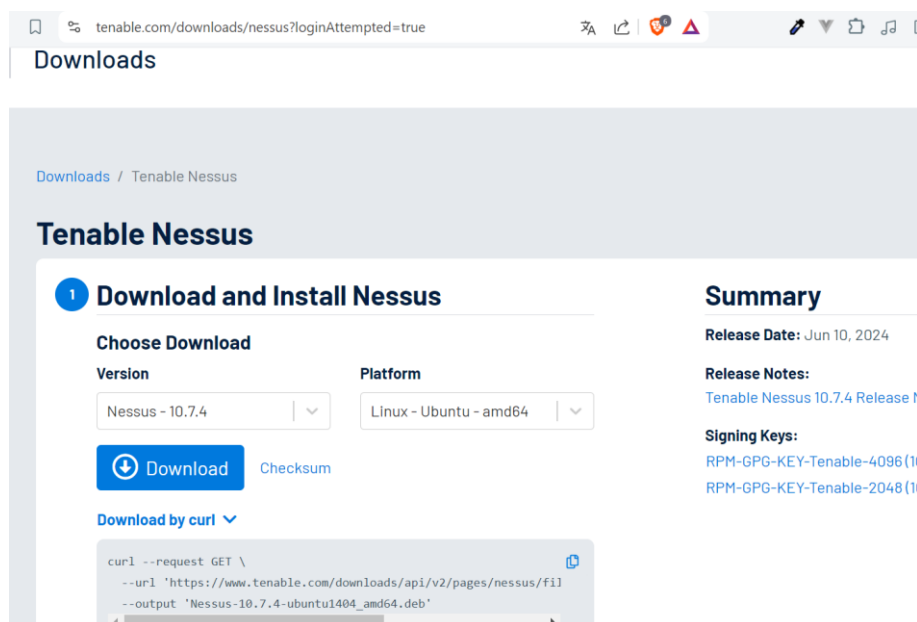
Ahora, empezará con el tema de descarga de *plugins*, esto puede llevar bastante rato ya que son muchos los *plugins* necesarios para su funcionamiento. Es necesario tenerlos actualizados porque si salen nuevas vulnerabilidades, podrían no detectarse.

Después del paso anterior, entraremos a la interface de Nessus, pero seguirá con la descarga de *plugins* y no podremos empezar a escanear hasta que no se descarguen todos.



En Kali Linux

Para instalar Nessus en Kali Linux, deberemos acceder al mismo sitio web que antes y seleccionar la versión de Linux donde queremos que se instale:



A continuación, en la consola de Kali, debemos lanzar los comandos `sudo apt update -y`, y `sudo apt upgrade -y` para la actualización de todos los paquetes. Esto puede llevar más o menos rato, dependiendo de cuando fue la última vez que se realizó dicha actualización.

Después de esto, lanzamos el comando que aparece en *Download by curl*:

```
curl --request GET \  
--url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.7.4-ubuntu1404_amd64.deb' \  
--output 'Nessus-10.7.4-ubuntu1404_amd64.deb'
```

El siguiente comando que debemos lanzar para su instalación es:
sudo dpkg -i Nombredelaversiónnessus

```
(kali@kali)-[~]
└─$ curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.7.4-ubuntu1404_amd64.deb' \
  --output 'Nessus-10.7.4-ubuntu1404_amd64.deb'
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left   Speed
100 66.4M    0 66.4M    0    0  28.4M    0 --:--:--  0:00:02 --:--:-- 28.4M

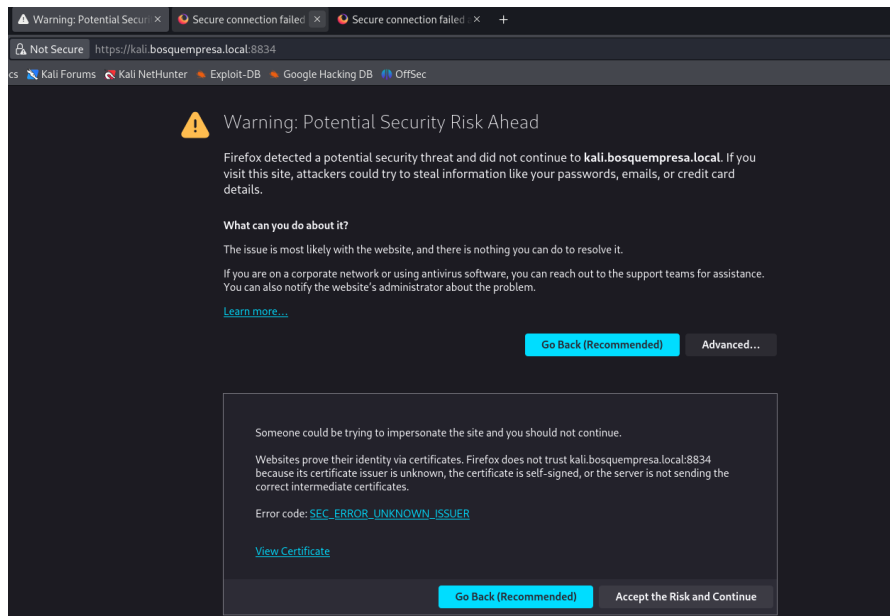
(kali@kali)-[~]
└─$ sudo dpkg -i Nessus-10.7.4-ubuntu1404_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 425341 files and directories currently installed.)
Preparing to unpack Nessus-10.7.4-ubuntu1404_amd64.deb ...
Unpacking nessus (10.7.4) ...
Setting up nessus (10.7.4) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
```

Al finalizar la instalación, nos dará el comando que necesitamos para iniciar el servicio de Nessus, el cual es `/bin/systemctl start nessusd.service` y también la url que deberemos copiar en el navegador para acceder a su interfaz gráfica (en nuestro caso es <https://kali.bosquempresa.local:8834/>):

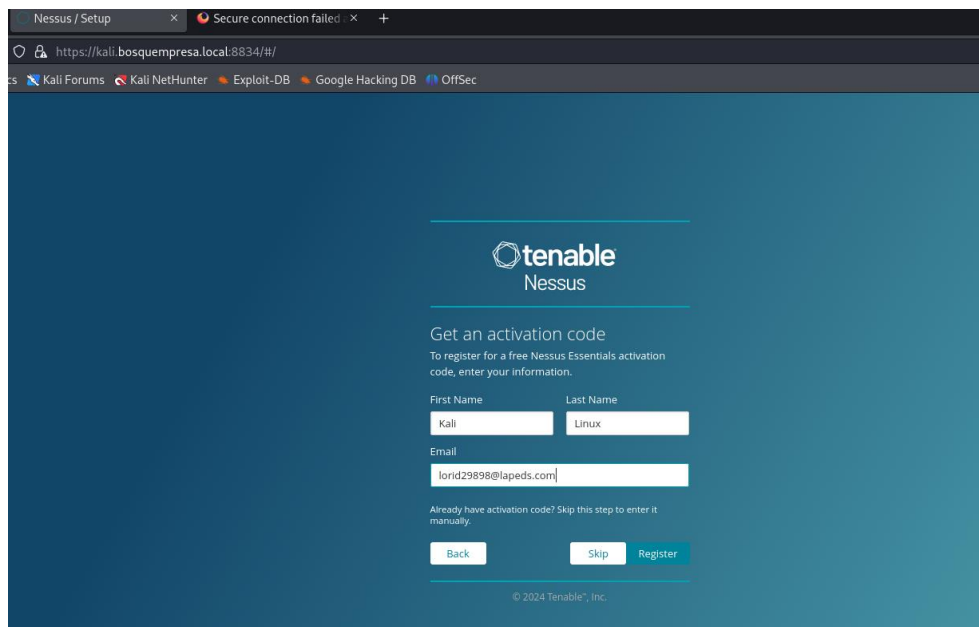
```
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali.bosquempresa.local:8834/ to configure your scanner

(kali@kali)-[~]
└─$ sudo /bin/systemctl start nessusd.service
```

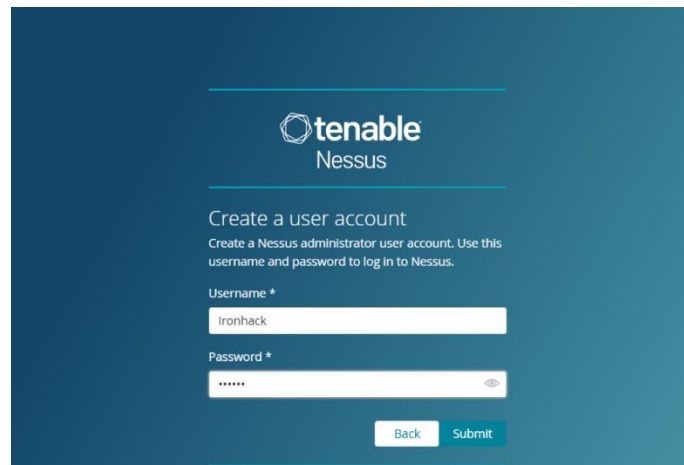
Al igual que en Windows, nos dirá que el sitio web no es seguro. Pero no debemos hacerle caso, así que le damos al botón *Accept the Risk and Continue* para poder entrar:



Una vez dentro, escribimos nuestro nombre y dirección de email para que se genere un código de activación:



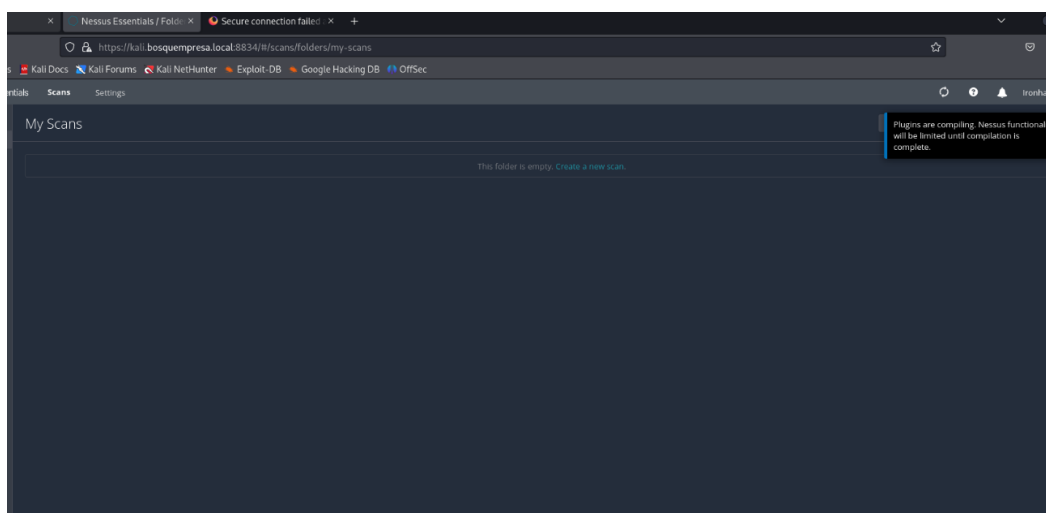
Creamos nuevamente un usuario y contraseña:



Se instalarán todos los *plugins* necesarios:

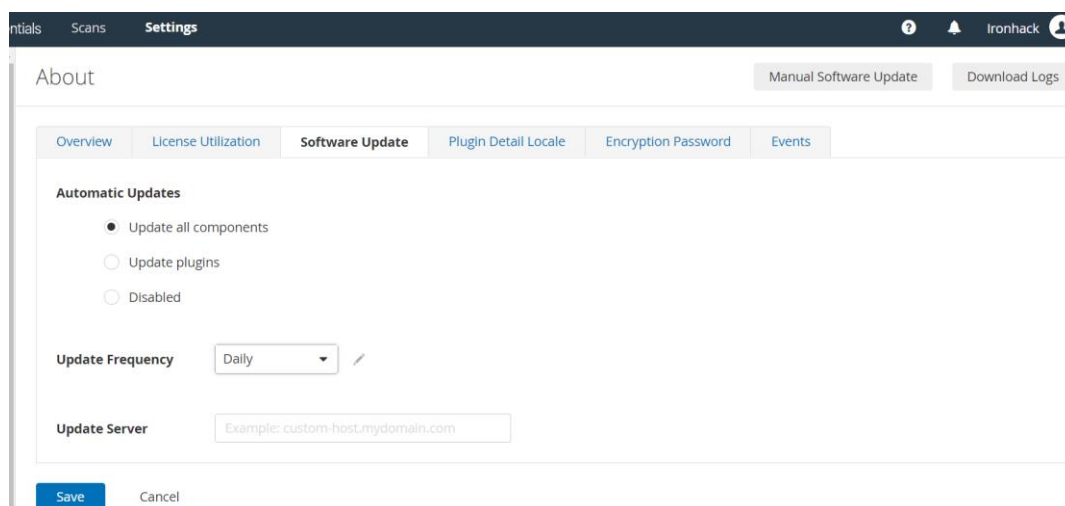


Cuando finalice el paso anterior, continuará la descarga de los *plugins* desde la interfaz gráfica. En nuestro caso no se pudo completar la descarga de *plugins* porque la memoria del disco duro de nuestro Kali Linux se encontraba completamente llena. La idea era poder integrar Metasploit y Nessus, para realizar pruebas de penetración y proporcionar herramientas para la explotación de vulnerabilidades descubiertas. Metasploit Framework incluye una vasta colección de *exploits*, *payloads* y herramientas auxiliares que permiten a los profesionales de seguridad realizar evaluaciones completas de la seguridad de sus sistema.



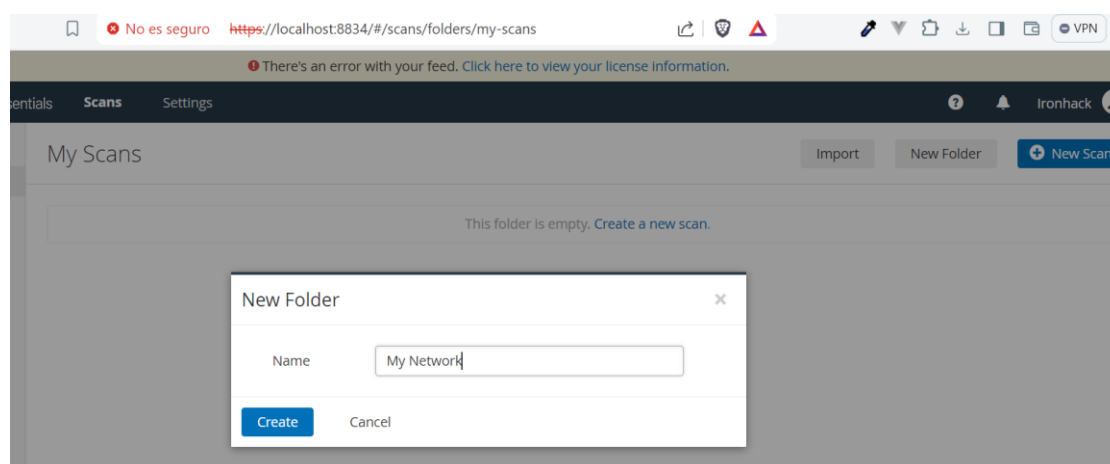
Debido a este inconveniente, configuramos y ejemplificamos algunos usos básicos de esta herramienta únicamente desde Windows 10.

Como toda herramienta de escaneo de vulnerabilidades, deberemos mantener actualizada siempre su base de datos, ya que de lo contrario, si sale una nueva vulnerabilidad, esta no sería detectada. Esto lo configuraremos desde la misma interfaz gráfica, yendo a *Settings* → *Software Update*:

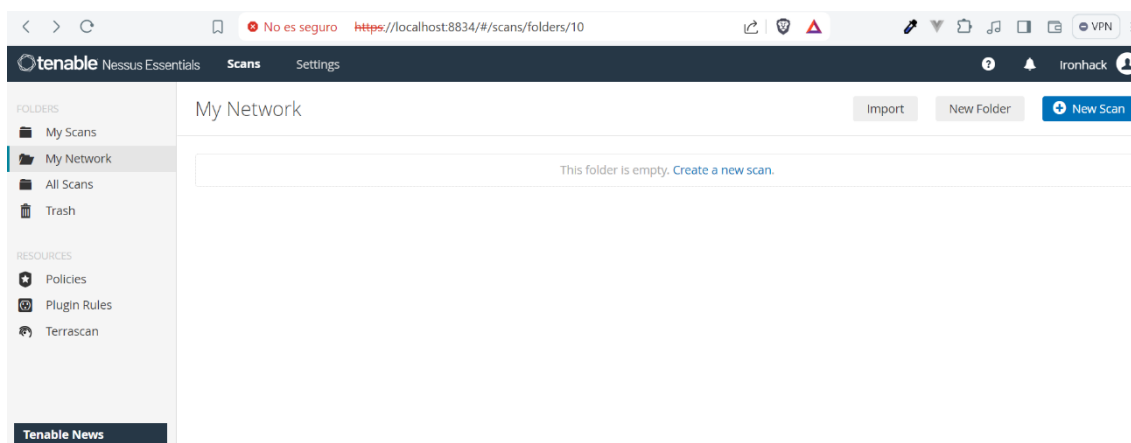


Aquí, seleccionaremos la opción *Update all components* para actualizar todos los componentes y la frecuencia con la que queremos que esto ocurra (diaria, semanal o mensual).

Para realizar un ejemplo de escaneo de vulnerabilidades sobre nuestra red doméstica, primero vamos a crear una carpeta clicando en el botón de arriba a la derecha donde dice *New Folder* y le damos un nombre a esa carpeta:



Seguidamente, le damos al botón de + *New Scan*:



Una vez dentro, veremos tres apartados, uno llamado *Host Discovery*, el cual sirve para ver el número de dispositivos conectados a esa red, otro llamado *Vulnerabilities*, donde veremos muchas opciones de escaneo de vulnerabilidades. Podríamos realizar, por ejemplo, un escaneo básico, un escaneo avanzado (el cual se utilizará la mayoría de las veces), un escaneo de Malware, escaneo para dispositivos móviles (disponible para las versiones de pago únicamente), para aplicaciones web, escaneo de Ransomware, de Log4Shell, etc. Y el tercer apartado, llamado *Compliance*, es utilizado para escanear políticas o auditorías de cumplimiento, también disponible únicamente para las versiones de pago:

tenable Nessus Essentials Scans Settings 2 Ironhack

Scan Templates
[Back to Scans](#)

Scanner Search Library

DISCOVERY

Host Discovery
 A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan
 A full system scan suitable for any host.

Advanced Scan
 Configure a scan without using any recommendations.

Advanced Dynamic Scan
 Configure a dynamic plugin scan without recommendations.

Malware Scan
 Scan for malware on Windows and Unix systems.

Mobile Device Scan
 Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
 Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
 Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
 Remote and local checks for CVE-2017-5689.

Spectre and Meltdown
 Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

WannaCry Ransomware
 Remote and local checks for MS17-010.

Ripple20 Remote Scan
 A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan
 A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solorigate
 Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

ProxyLogon : MS Exchange
 Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

PrintNightmare
 Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter Scan
 Look for misconfigurations in Active Directory.

Log4Shell
 Detection of Apache Log4j CVE-2021-44228.

Log4Shell Remote Checks
 Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks.

Log4Shell Vulnerability Ecosystem
 Detection of Log4Shell Vulnerabilities.

CISA Alerts AA22-011A and AA22-047A
 Detection of vulnerabilities from recent CISA alerts.

ContiLeaks
 Detection of vulnerabilities revealed in the ContiLeaks chats.

Ransomware Ecosystem
 Vulnerabilities used by ransomware groups and affiliates.

2022 Threat Landscape Report (TLR)
 A scan to detect vulnerabilities featured in our End of Year report.

COMPLIANCE

Audit Cloud Infrastructure
 Audit the configuration of third-party cloud services.

Internal PCI Network Scan
 Perform an internal PCI DSS (11.2.1) vulnerability scan.

MDM Config Audit
 Audit the configuration of mobile device managers.

Offline Config Audit
 Audit the configuration of network devices.

PCI Quarterly External Scan
 Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing
 Audit system configurations against a known baseline.

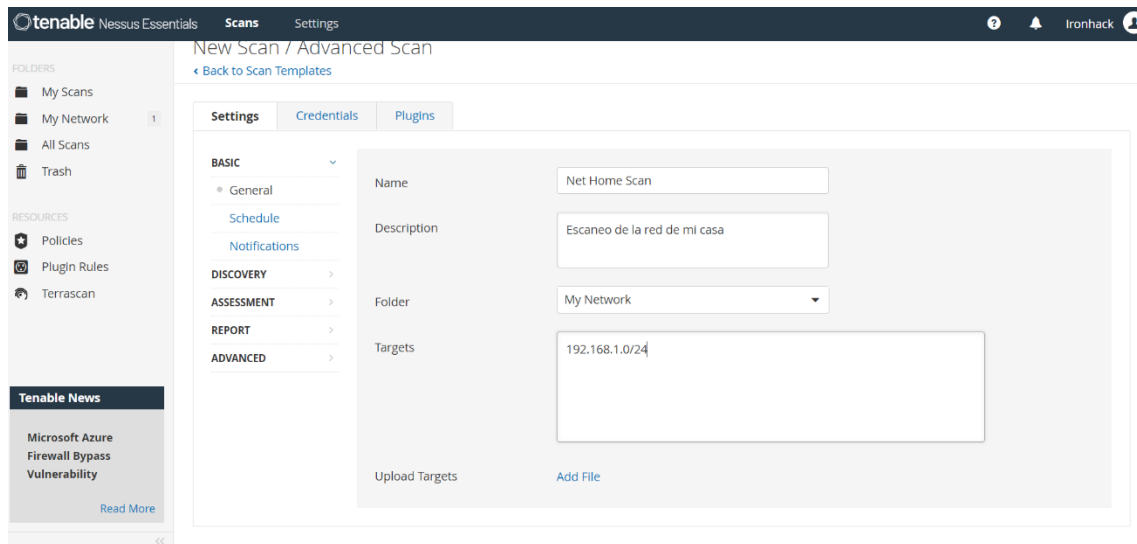
SCAP and OVAL Auditing
 Audit systems using SCAP and OVAL definitions.

Tenable News
 Cloud Workload Protection: The Key to Decreasing C...
 CVE-2024-4577: Proof of Concept Available for PHP...
[Read More](#)

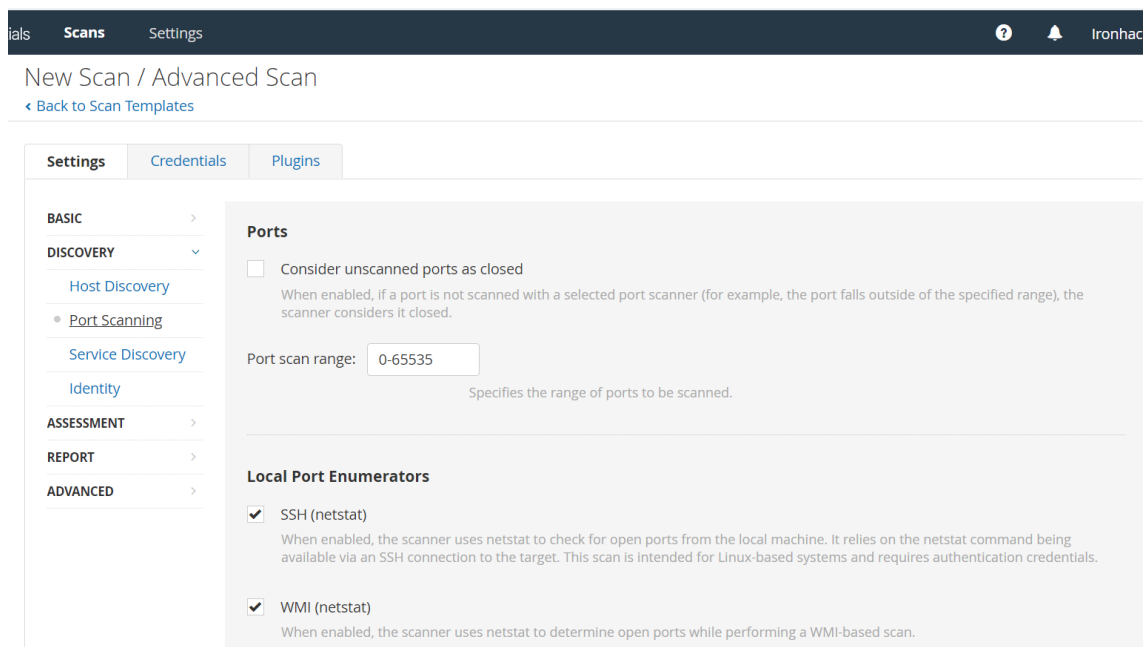
Tenable News
 CVE-2024-4577: Proof of Concept Available for PHP...
[Read More](#)

Tenable News
 CVE-2024-4577: Proof of Concept Available for PHP...
[Read More](#)

Seleccionamos la opción *Advanced Scan* y una vez dentro, le daremos un nombre y una descripción a este escaneo, seleccionaremos la carpeta donde queremos que se guarde (en nuestro caso quedará guardado en la única carpeta que hemos creado, llamada *My Network*). Donde dice *Targets* deberemos escribir la IP del dispositivo que queremos escanear, un rango de IPs, el nombre de un dominio o bien la IP de toda la red que queremos escanear, como en nuestro caso que pusimos la IP 192.168.1.0/24 para así detectar automáticamente todos los *hosts* presentes en esa red:



Si vamos a *Discovery* → *Port Scanning* podremos seleccionar el tipo de puertos y el rango del número de puertos que queremos escanear, en este caso, como queremos escanear todos los puertos, establecemos el rango 0-65535:



Verify open TCP ports found by local port enumerators
When enabled, if a local port enumerator (for example, WMI or netstat) finds a port, the scanner also verifies that the port is open remotely. This approach helps determine if some form of access control is being used (for example, TCP wrappers or a firewall).

Network Port Scanners

☒ SYN

☐ Override automatic firewall detection

☒ Use soft detection

☐ Use aggressive detection

☐ Disable detection

☒ UDP
This option engages the built-in Nessus UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead if possible.

Save **Cancel**

Si quisiéramos escanear algún sitio web, nos dirigimos a *Assessment* → *Web Applications* y escribiríamos la url:

Settings **Credentials** **Plugins**

Web Application Settings

Scan web applications ☒

Web Crawler

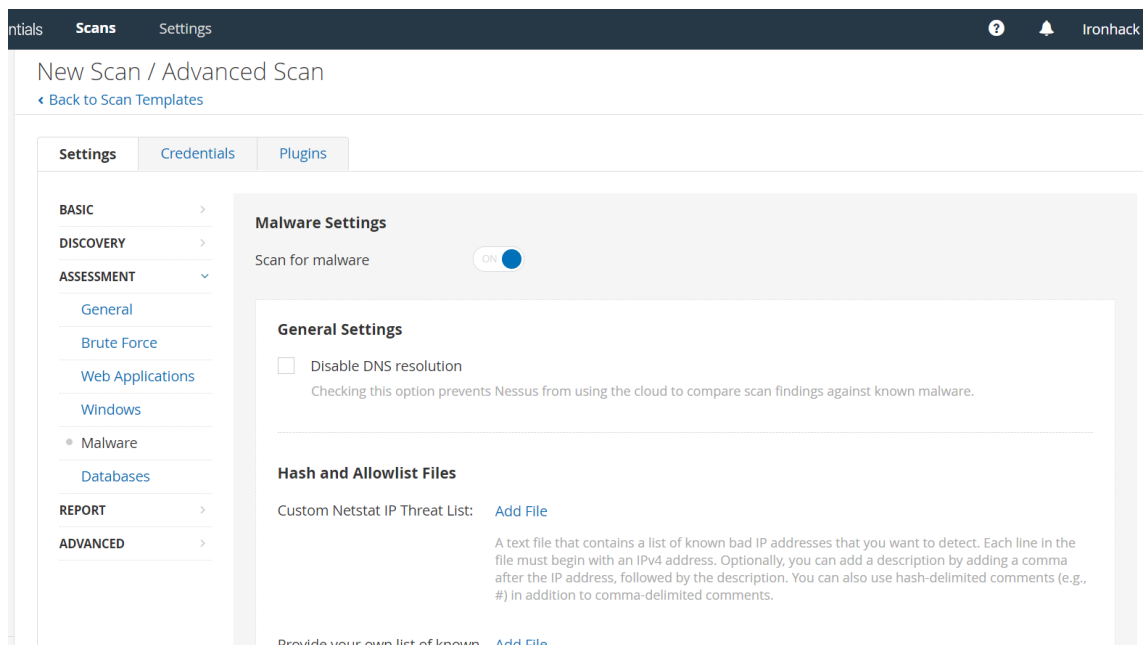
Start crawling from
The URL of the first page that is tested. If multiple pages are required, use a colon delimiter to separate them (e.g., /php4:/base).

Excluded pages (regex)
Specifies portions of the web site to exclude from being crawled. For example, to exclude the /manual directory and all Perl CGI, set this field to: (^/manual) <> (.pl{?.*}?\$).

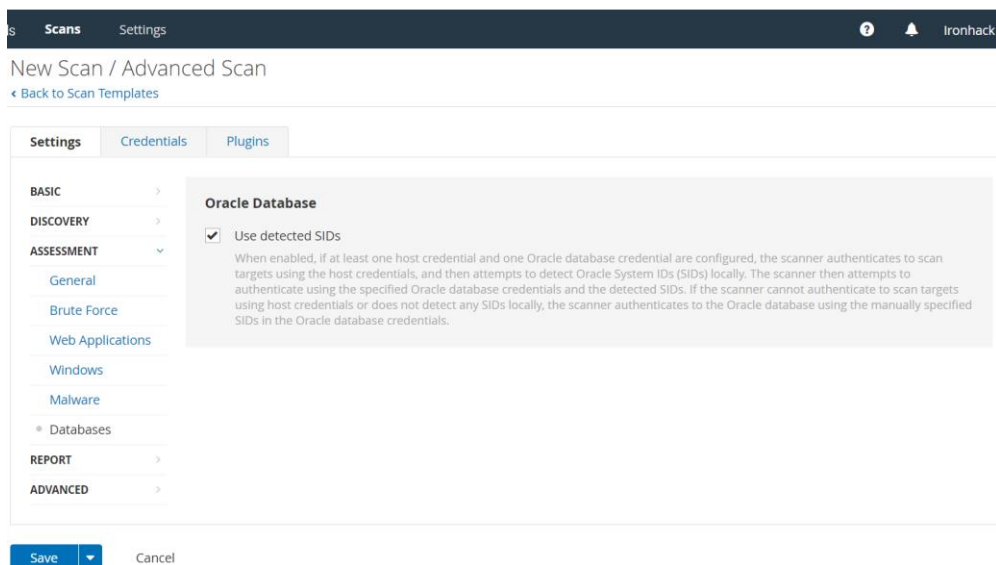
Maximum pages to crawl
The maximum number of pages to crawl.

Maximum depth to crawl

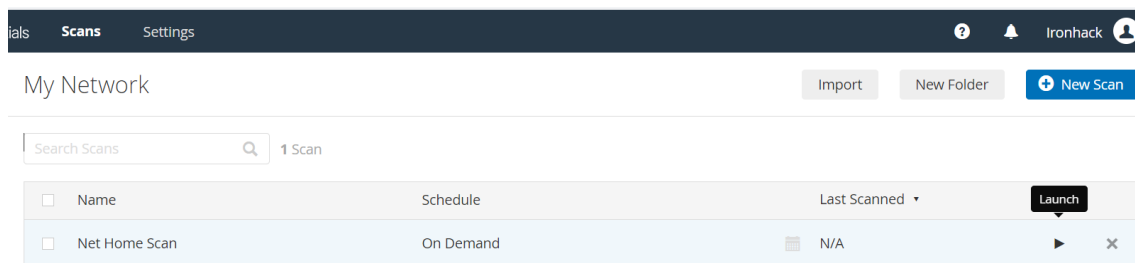
Para detectar si existe algún malware vamos a *Assessment* → *Malware* y seleccionamos la opción *Scan for malware*:



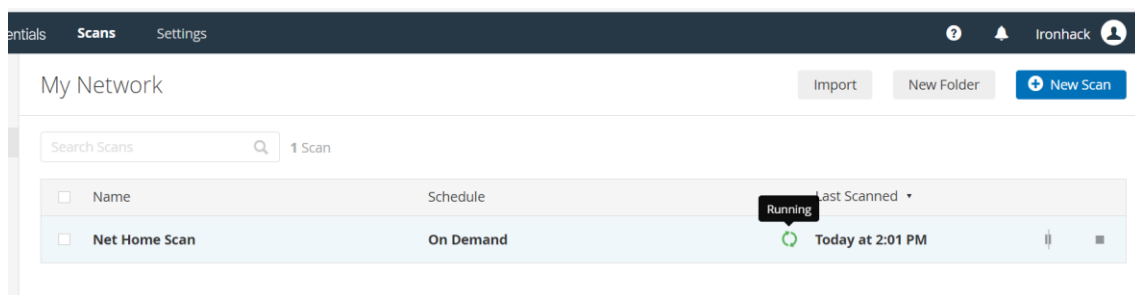
Nessus también puede realizar escaneos de vulnerabilidades en bases de datos Oracle para identificar problemas de seguridad específicos:



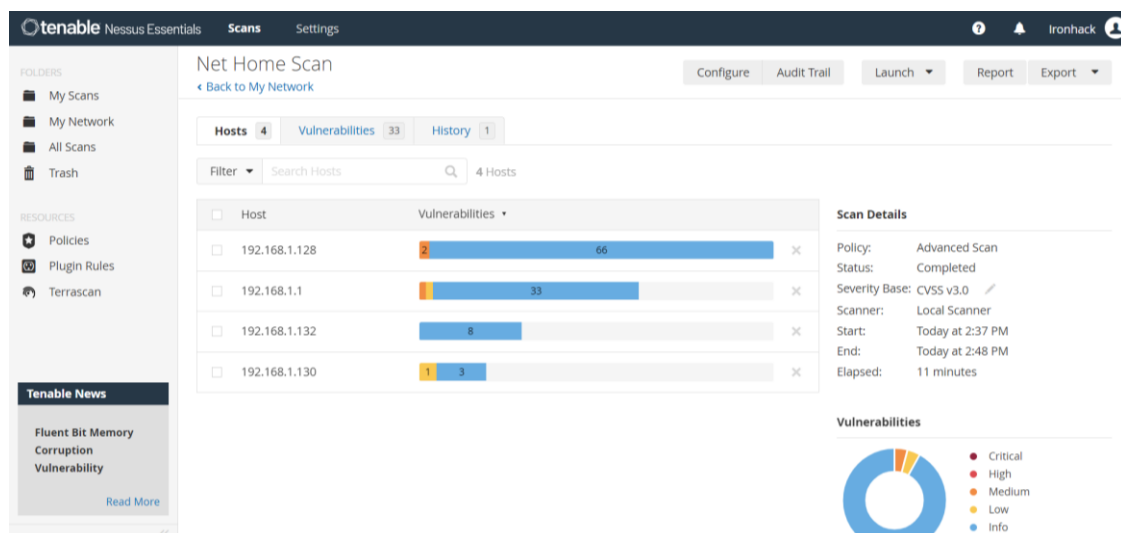
Una vez tengamos configurados todos los parámetros del escaneo, le damos al botón *Save*, después vamos a la carpeta donde se encuentra dicho escaneo y la damos al botón *Launch* para lanzar el escaneo. También, en las configuraciones anteriores, podríamos haberlo programado para que empezara automáticamente en un horario determinado:



Mientras esté en proceso, veremos las dos flechas formando un círculo y la etiqueta de *Running*, este escaneo llevará algunos minutos, el tiempo dependerá de la complejidad del escaneo y de nuestra conexión a internet:



A la que haya finalizado, haremos clic encima de ese escaneo y pasaremos a ver los resultados. Podemos observar que hay tres pestañas, una con todos los hosts que han sido escaneados, otra con todas las vulnerabilidades encontradas y otra con el historial donde simplemente nos dirá la fecha del escaneo. En el gráfico circular de la derecha podemos ver la clasificación de las vulnerabilidades por color y criticidad. Si hacemos clic en alguna de las direcciones IP, veremos más detalladamente esas vulnerabilidades y la posible solución que podemos tomar:



Si entramos en el primer dispositivo, veremos un total de 22 vulnerabilidades, siendo 20 de ellas meramente informativas, una de criticidad variada, ya que se encuentran diferentes vulnerabilidades dentro de ese grupo y otra de criticidad media:

The screenshot shows the Nessus interface for a scan of host 192.168.1.128. The main table lists 22 vulnerabilities. The first few rows show:

| Sev | CVSS | VPR | N... Family | Count |
|--------|------|------|--------------------|-------|
| MEDIUM | 5.3 | S... | Misc. | 1 |
| MIXED | ... | ... | General | 4 |
| INFO | ... | ... | Windows | 6 |
| INFO | ... | ... | Web Servers | 2 |
| INFO | ... | ... | Windows | 2 |
| INFO | ... | ... | Service detection | 2 |
| INFO | ... | ... | N... Port scanners | 24 |
| INFO | ... | ... | D... Windows | 8 |

The right sidebar shows host details for 192.168.1.128, including IP, OS (Windows), start time, and a vulnerability distribution pie chart with categories: Critical, High, and Medium.

Si por ejemplo le damos a la primera vulnerabilidad de todas, la cual es de nivel medio, veremos todos sus detalles:

The screenshot shows the details of a specific vulnerability, 'SMB Signing not required' (Plugin #57608). The page includes a description, solution, and risk information.

Description
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also
<http://www.nessus.org/u?df39b8b3>
<http://technet.microsoft.com/en-us/library/cc731957.aspx>
<http://www.nessus.org/u?74b80723>
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
<http://www.nessus.org/u?a3cac4ea>

Plugin Details
Severity: Medium
ID: 57608
Version: 1.20
Type: remote
Family: Misc.
Published: January 19, 2012
Modified: October 5, 2022

Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.7

En su descripción nos dice que esta vulnerabilidad se relaciona con la configuración de seguridad en servidores SMB (Server Message Block), específicamente con la ausencia de la necesidad de firmar digitalmente las comunicaciones SMB. Esto puede permitir a un atacante sin autenticar realizar ataques de intermediario (*man-in-the-middle*) contra

el servidor SMB. Más abajo también nos da la solución para mitigar las vulnerabilidades, en este caso se recomienda habilitar la firma SMB obligatoria.

Si entramos en la vulnerabilidad que decía *Mixed*, vamos a ver cuatro vulnerabilidades, tres de ellas son informativas y otra es de nivel medio, la cual trata sobre el certificado SSL:

The screenshot shows the Nessus interface for a scan titled 'Net Home Scan / Plugin #51192'. The 'Vulnerabilities' tab is active, showing 22 items. The selected vulnerability is 'SSL Certificate Cannot Be Trusted' (Medium severity). The description explains that the server's X.509 certificate cannot be trusted due to issues with the certificate chain of trust. It lists three potential causes: 1) The top of the chain is not descended from a known public certificate authority. 2) The chain contains a certificate that is not valid at the time of the scan. 3) The chain contains a signature that either didn't match the certificate's information or could not be verified. The solution is to purchase or generate a proper SSL certificate. The 'Output' section shows the details of the certificate found at the top of the chain, signed by an unknown authority.

Vulnerabilities 22

MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

<https://www.itu.int/rec/T-REC-X.509/en>
<https://en.wikipedia.org/wiki/X.509>

Output

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

```
| -Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=LAPTOP-QMORFEER  
| -Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
```

To see debug logs, please visit individual host

| Port | Hosts |
|------------------|---------------|
| 8834 / tcp / www | 192.168.1.128 |

Esta vulnerabilidad indica que hay un problema con el certificado X.509 del servidor, lo cual puede comprometer la seguridad de las conexiones cifradas. Para solucionar esto, se debería obtener un certificado proveniente de una autoridad certificadora (CA) reconocida.

Actividad 3 (2,5 puntos)

Objetivo: Analiza la efectividad de la herramienta.

La relación coste-beneficio de Nessus es ampliamente positiva, ya que en cuanto a su beneficio podemos decir que se trata de una herramienta muy útil para una organización debido a su capacidad de detectar, gestionar vulnerabilidades y reducir significativamente los riesgos de seguridad. También, ayuda a cumplir con normativas de seguridad y estándares de la industria. Además, al identificar y mitigar vulnerabilidades de manera proactiva, se evitan posibles incidentes de seguridad costosos. Y esta detección de vulnerabilidades se puede automatizar, liberando recursos y tiempo para otras tareas críticas de seguridad. Respecto al costo de implementación, no se requieren hardware de alta gama para su implementación y además hay opciones gratuitas de esta herramienta que ofrecen diferentes tipos de licencias, algunas de pago y otras completamente gratuitas como la que hemos usado para la realización de este trabajo, con algunas opciones de escaneo de pago. Respecto al tiempo de implementación es relativamente corto dada su facilidad de instalación y configuración para un uso básico.

De una manera más detallada, podemos enumerar algunas de las ventajas que ofrece Nessus:

1. Amplia Cobertura de Vulnerabilidades:

Nessus tiene una de las bases de datos de *plugins* más grandes y actualizadas, lo que le permite detectar una amplia gama de vulnerabilidades en sistemas operativos, aplicaciones y redes. Esto garantiza que la mayoría de las amenazas conocidas sean identificadas y gestionadas.

2. Facilidad de Uso:

La interfaz web de Nessus es intuitiva y fácil de usar, incluso para usuarios con conocimientos técnicos limitados. Lo cual facilita la adopción y el uso eficiente de la herramienta sin necesidad de una capacitación extensa si se quiere realizar un uso básico.

3. Actualizaciones Frecuentes:

Nessus recibe actualizaciones frecuentes que incluyen nuevos *plugins* y mejoras en el software. Esto mantiene la herramienta actualizada con las últimas amenazas y vulnerabilidades, asegurando una protección continua.

4. **Informes Detallados:**

Genera informes completos que incluyen descripciones de las vulnerabilidades, su severidad y recomendaciones para mitigarlas, y así poder ayudar a los equipos de seguridad a comprender y priorizar las vulnerabilidades, facilitando la toma de decisiones informadas.

5. **Integración con Otras Herramientas:**

Puede integrarse con otras soluciones de seguridad y gestión de TI, permitiendo una gestión centralizada y un flujo de trabajo más eficiente.

6. **Soporte Técnico y Recursos:**

Ofrece un soporte técnico robusto y una amplia gama de recursos, incluyendo documentación y foros de usuarios. Esto puede ayudar a resolver problemas rápidamente y a maximizar el uso de la herramienta.

Aunque la balanza se inclina más hacia sus beneficios, como inconvenientes de Nessus, podríamos hablar de:

1. **Coste:**

Las licencias de Nessus, especialmente las versiones empresariales, pueden ser costosas y esto podría no ser una opción viable para organizaciones con presupuestos limitados. Y también, aunque no se haya percibido para la realización de esta práctica, la herramienta puede requerir recursos de hardware significativos para escaneos grandes o complejos. Pudiendo requerir una inversión adicional en infraestructura.

2. **Curva de Aprendizaje Inicial:**

Aunque es fácil de usar, sacar el máximo provecho de todas las funcionalidades avanzadas puede requerir tiempo y capacitación. Puede haber un período inicial en el que los usuarios necesiten adaptarse y aprender a utilizar la herramienta eficazmente.

3. **Falsos Positivos/Negativos:**

Como con cualquier herramienta de escaneo de vulnerabilidades, pueden ocurrir falsos positivos o negativos. Con lo cual se requiere verificación manual y validación de los resultados para asegurar precisión.

Respondiendo a la pregunta de si recomendaría la implementación de Nessus en una empresa, diría plenamente que sí, ya que se trata de una herramienta de escaneo contra vulnerabilidades que ofrece un amplio abanico de beneficios, siendo algunos de ellos:

- **Protección Proactiva:**
Nessus ayuda a identificar y a remediar vulnerabilidades antes de que puedan ser explotadas por atacantes, proporcionando una capa de seguridad proactiva.
- **Cumplimiento Normativo:**
Ayuda a cumplir con diversas normativas y estándares de seguridad (como PCI-DSS, HIPAA, y otros), lo cual es crucial para muchas industrias.
- **Eficiencia en la Gestión de Vulnerabilidades:**
La capacidad de generar informes detallados y priorizar vulnerabilidades permite a los equipos de seguridad gestionar de manera más eficiente y eficaz los riesgos.
- **Actualizaciones Frecuentes:**
Las actualizaciones regulares aseguran que la herramienta esté siempre al día con las últimas amenazas, proporcionando una protección continua.
- **Flexibilidad y Escalabilidad:**
Nessus se puede escalar y adaptar a las necesidades específicas de la empresa, desde pequeñas organizaciones hasta grandes corporaciones.
- **Soporte y Recursos de Tenable:**
El respaldo de Tenable en términos de soporte técnico y recursos educativos asegura que cualquier problema o duda puede ser resuelto rápidamente, maximizando el retorno de inversión.