

Actividad |1| Detección y Prevención de Ataques de Acceso.

Seguridad Informática II.

Ingeniería en Desarrollo de Software.



TUTOR: Jessica Hernández Romero.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 28/05/2025.

Introducción.	3
Descripción.	3
Justificación.	4
Desarrollo:	5
Instalación y configuración	5
Incidencias encontradas.	9
Reporte.	14
Análisis e Identificación de mejoras.	17
Conclusion.	19
Referencias.	20

Introducción.

En esta primera actividad de la materia de Seguridad Informática II, En el panorama digital actual, la protección contra ataques de explotación y el acceso no autorizado a sistemas es crucial de las empresas o personales. Este documento aborda la implementación de técnicas de auditoría de red utilizando herramientas tecnológicas especializadas para reforzar la seguridad y la prevención de ataques. Nos centraremos en la importancia de la seguridad cibernética, destacando tres factores clave: la prevención de ataques de acceso, la protección de las redes y el monitoreo integral. Nuestra actividad principal será la instalación, el uso de software diseñado para detectar y prevenir ataques tanto a nivel de sistema como de red. Posteriormente, realizaremos una auditoría de vulnerabilidades exhaustiva. Esto incluirá como actividades la instalación, el análisis de un equipo específico, buscando activamente amenazas como virus, intentos de acceso no autorizado y percances de red. Los hallazgos se documentaron a través de reportes generados por la herramienta o capturas de pantalla de los resultados del análisis, proporcionando una visión clara del estado de seguridad.

Descripción.

En esta primera actividad de la materia de Seguridad Informática II. En el panorama digital actual, protegerse de ciberataques y accesos no autorizados es vital para empresas y usuarios individuales. Esta actividad se enfoca en fortalecer la seguridad mediante la implementación de técnicas de auditoría de red con herramientas especializadas. Nos centraremos en la importancia de la ciberseguridad, destacando tres pilares: la prevención de ataques de acceso, la protección de redes y el monitoreo integral.

Nuestra tarea principal será instalar y utilizar software diseñado para detectar y prevenir ataques tanto a nivel de sistema como de red. Posteriormente, realizaremos una auditoría de vulnerabilidades exhaustiva en un equipo específico. Esto implica buscar activamente amenazas como virus, intentos de acceso no

autorizado y percances de red. Los resultados se documentarán mediante el informe o informes generados por la herramienta o capturas de pantalla, ofreciendo una visión clara del estado de seguridad. Esta metodología busca asegurar la integridad y confidencialidad de la información, reforzando la postura defensiva contra futuras amenazas.

Justificación.

Esta actividad de la materia Seguridad Informática II es fundamental para comprender y aplicar las defensas necesarias en el entorno digital actual. La creciente sofisticación de los ataques de explotación y los accesos no autorizados exige que los profesionales de TI dominen las técnicas de auditoría de red. Al utilizar herramientas tecnológicas especializadas, no sólo reforzamos la seguridad de la infraestructura, sino que también desarrollamos habilidades prácticas cruciales.

La justificación radica en la necesidad de prevenir ataques de acceso, proteger integralmente las redes y garantizar un monitoreo constante de la actividad. La instalación, el uso de software de detección y prevención de ataques nos permite experimentar de primera mano la importancia de estas herramientas. Realizar una auditoría de vulnerabilidades exhaustiva en un equipo real, identificando virus, intentos de acceso y percances de red, nos proporciona una visión práctica de las amenazas y la capacidad de generar reportes detallados, preparando a los estudiantes para los desafíos de seguridad del mundo real.

Estos puntos adicionales a utilizar en la justificación para la realización de la documentación de esta actividad que son los siguientes:

- PDF de esta actividad en el portafolio GitHub.
- Anexa link de GitHub en documento.
- Utilizar la herramienta Nessus Essential.
- Comprimir en la actividad 1 el reporte de la herramienta de nesus en el sitio de GitHub.

- Toma de pantallas de la instalación y configuración de la herramienta Nessus Essencial.

Desarrollo:

En estas la Actividad 1: Detección y Prevención de Ataques de Acceso, nos enfocaremos en una serie de pasos clave para fortalecer nuestras habilidades en seguridad informática. Iniciaremos con la instalación de la herramienta Nessus Essencial designada como una de las herramientas a escoger para esta actividad. Luego, documentamos las incidencias encontradas, generando un reporte detallado de las mismas. Y finalmente, analizaremos e identificamos las soluciones para cada una. Este proceso no solo nos permitirá mejorar la seguridad de nuestra infraestructura, sino que también nos brindará habilidades prácticas esenciales para el manejo de amenazas cibernéticas.

Link: GitHub

Link: Reporter Nessus

Instalación y configuración

En este punto de la actividad mostraremos la evidencia de la instalación y configuración de la herramienta de Nessus Essencial que será utilizada para la detección de vulnerabilidades.

The image shows two screenshots of the Tenable website. The top screenshot is the Tenable Nessus Essentials landing page, and the bottom screenshot is the Tenable Nessus Downloads page.

Tenable Nessus® Essentials

Nessus Essentials es un producto gratuito de Tenable que proporciona escaneo de vulnerabilidades a profundidad y de alta velocidad para hasta 16 direcciones IP por escáner.

Limitaciones: Nessus Essentials no admite escaneo ilimitado, verificaciones de cumplimiento, auditorías de cumplimiento, Live Results, informes configurables ni el dispositivo virtual de Nessus. Para obtener acceso a estas funcionalidades y más, [actualice a Nessus Professional](#).

Para estudiantes y profesores: si emplea Nessus Essentials para labores educativas, regístrese mediante el programa [Tenable for Education](#) para iniciar.

Aprenda a usar Nessus: nuestro [curso bajo demanda Nessus Fundamental](#) cubre todo, desde la detección de activos hasta el cumplimiento, ayudándole a dominar Nessus para obtener una evaluación de vulnerabilidades eficaz en diversos casos de uso de negocios.

Regístrese para obtener un código de activación

Se está registrando para una licencia de 1 año para Nessus Essentials.

Nombre: Apellido:

Correo electrónico laboral:

☐ Quiero recibir actualizaciones de Tenable

Tenable solo procesará sus datos personales como se describe en su Política de privacidad.

[Empezar](#)

Tenable Downloads

Tenable Nessus

Download and Install Nessus

Choose Download

Getting Started

Check out our [documentation for Nessus](#)

Summary

Release Date: Apr 17, 2025

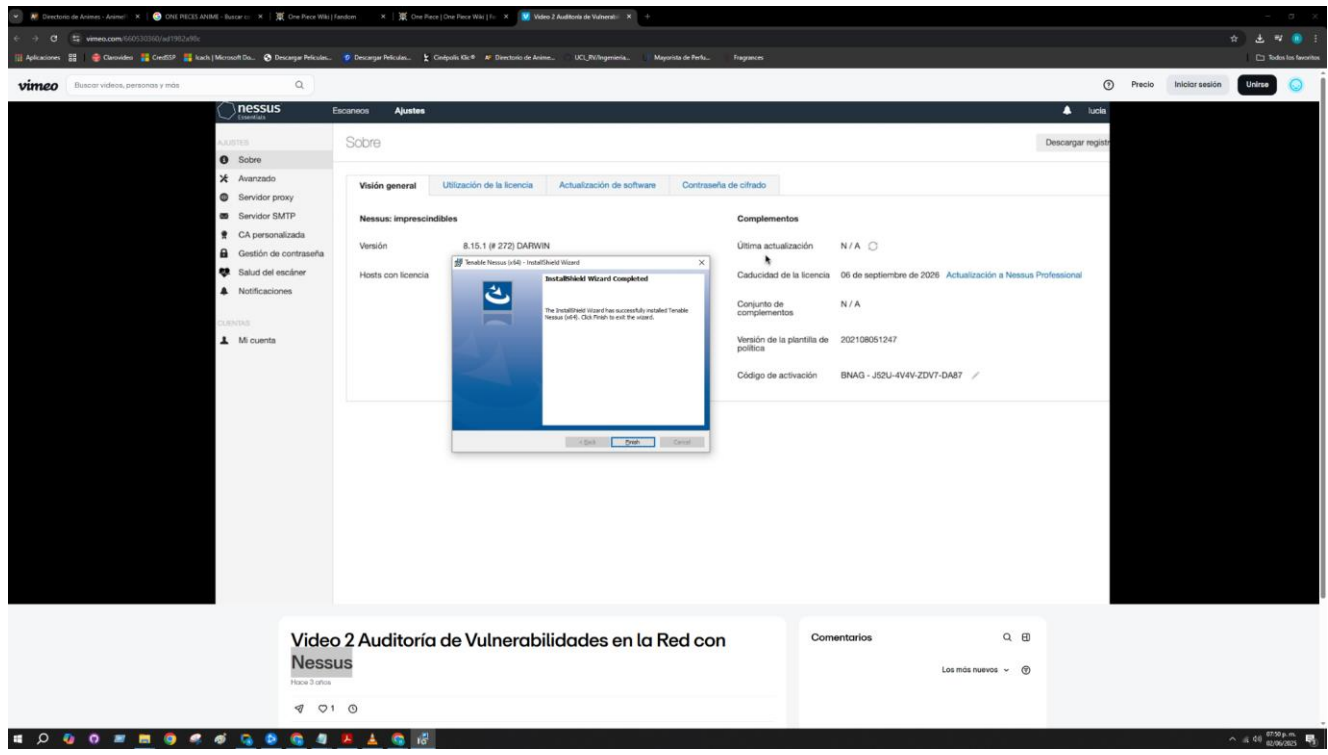
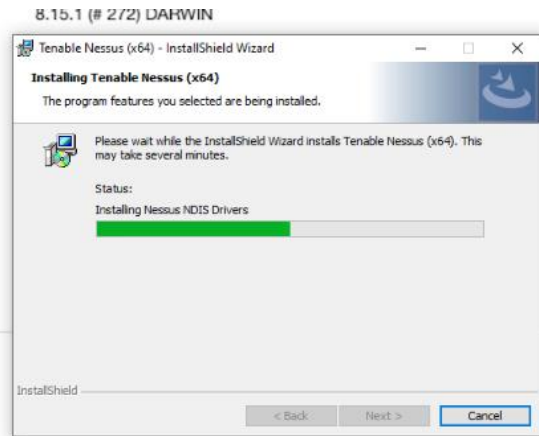
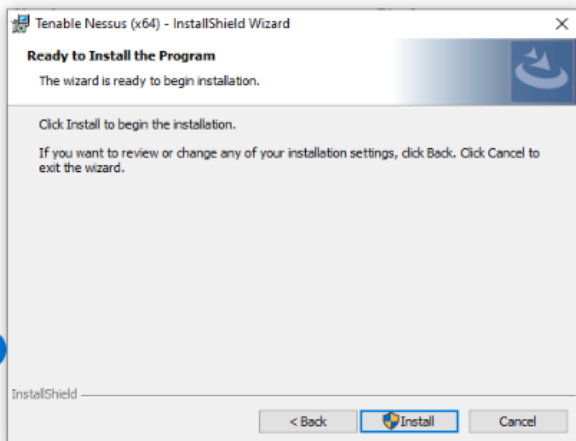
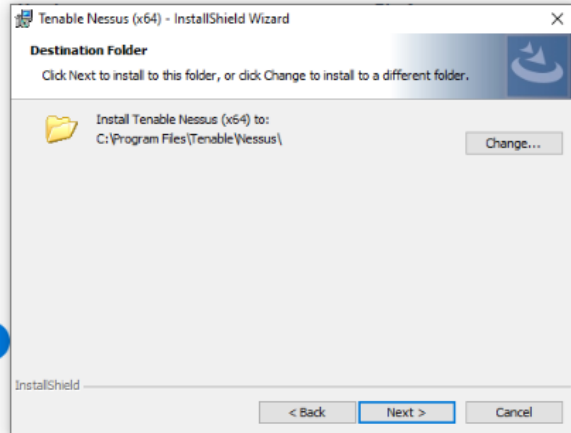
Release Notes:
[Tenable Nessus 10.8.4 Release Notes](#)

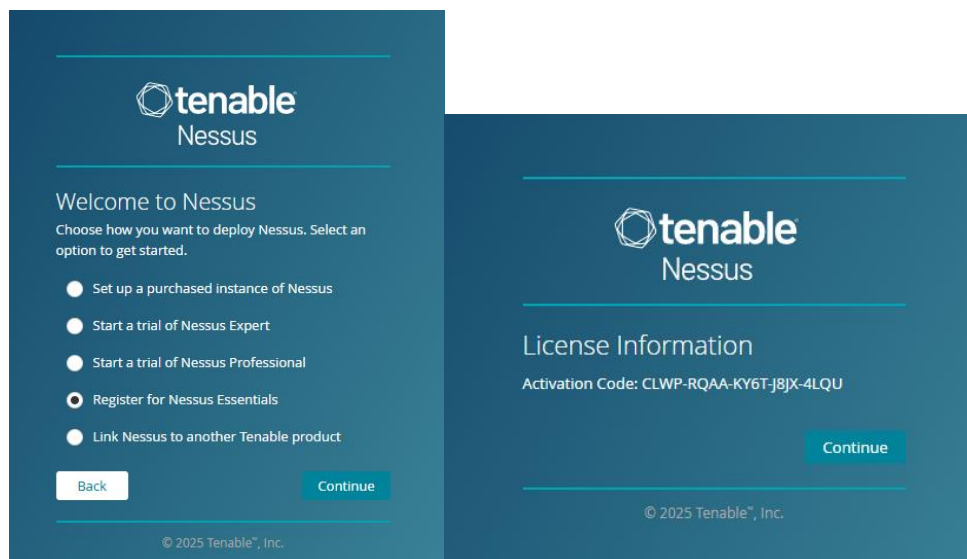
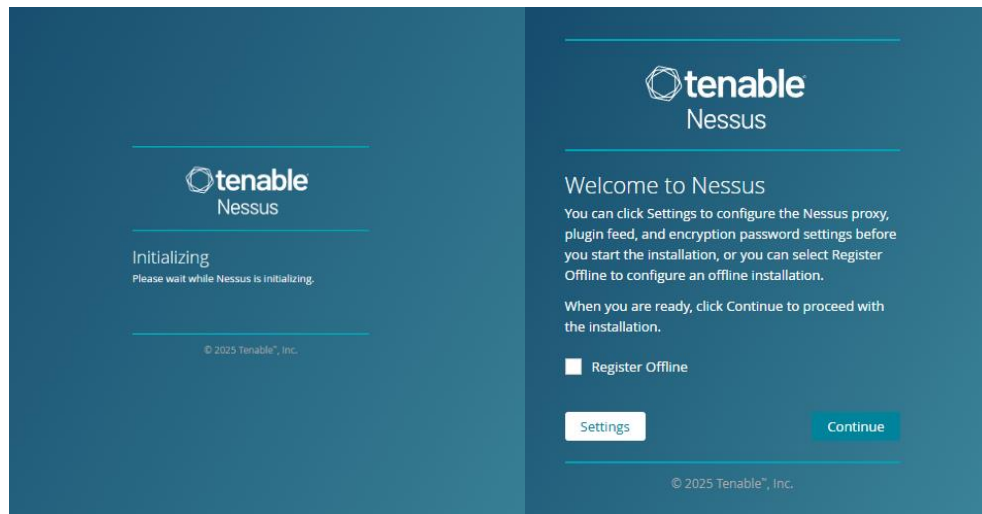
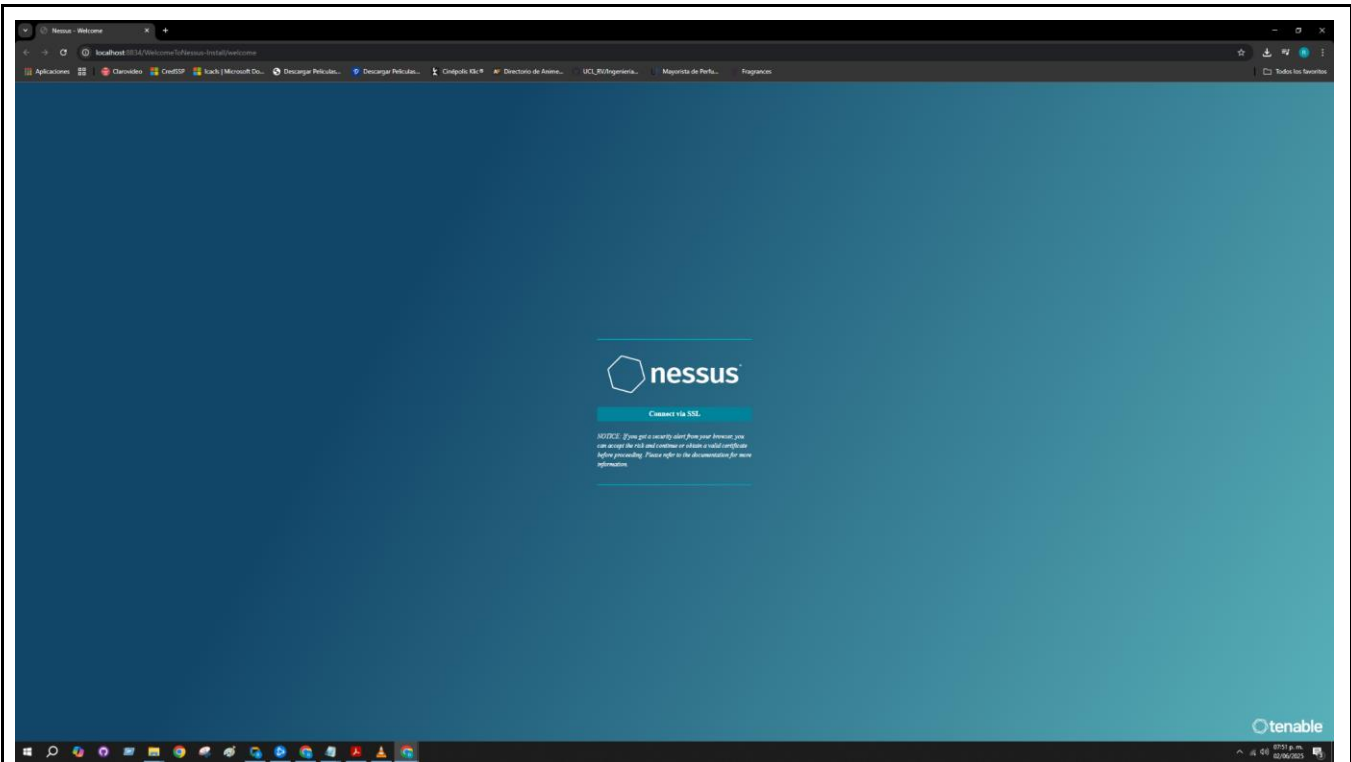
Signing Keys:
 RPH-GPG-KEY-Tenable-4086 (10.4 & above)
 RPH-GPG-KEY-Tenable-2048 (10.3 & below)


Footer:

Tenable.com Community & Support Documentation Education

© 2025 Tenable®, Inc. All Rights Reserved Privacy Policy Legal SDR Compliance







Create a user account


Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Password *

[Back](#) [Submit](#)

© 2025 Tenable™, Inc.

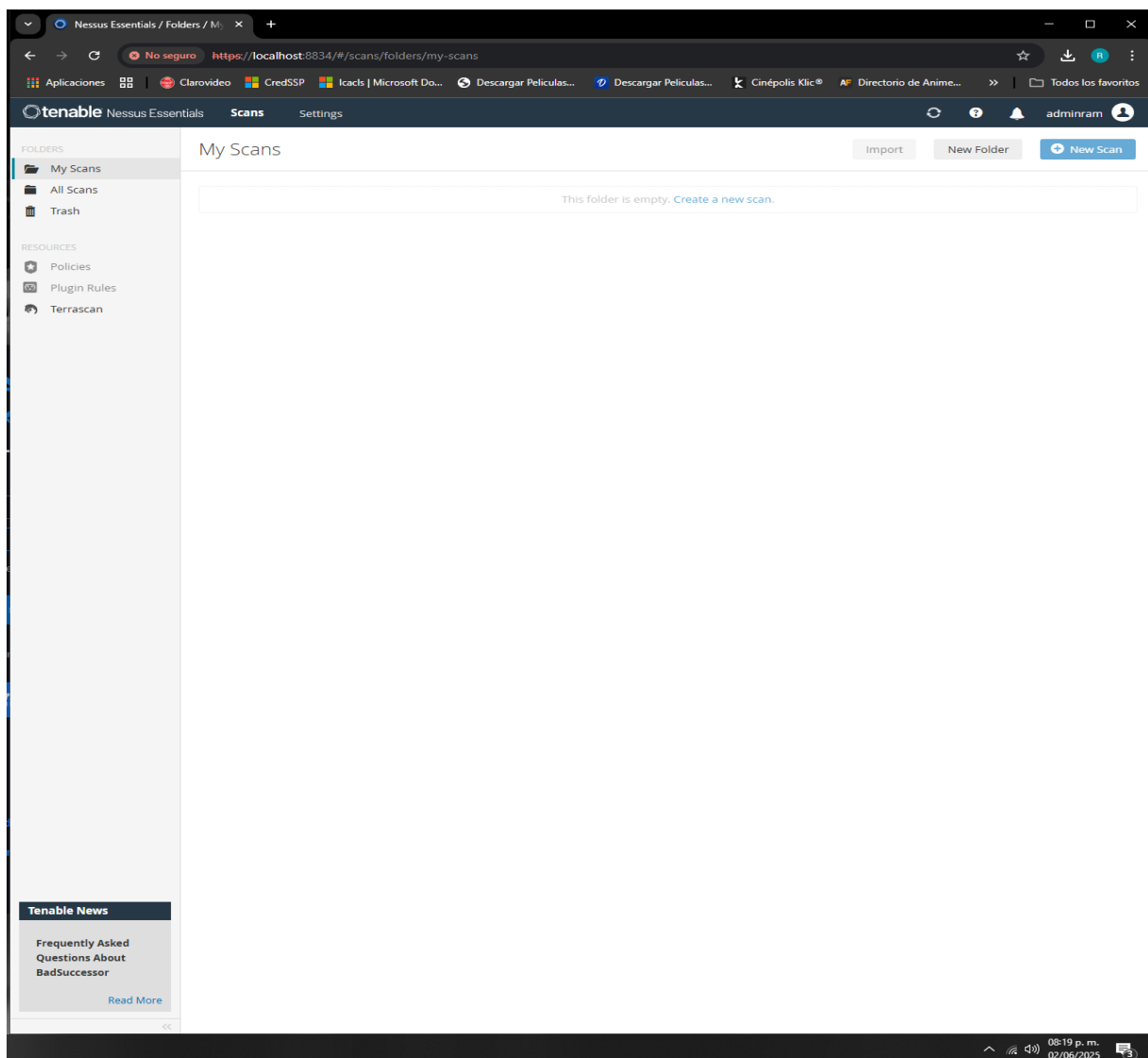


Initializing

Please wait while Nessus is initializing.

Downloading plugins...

© 2025 Tenable™, Inc.



Incidencias encontradas.

En este punto de la actividad se detectaron 7 incidencias en el equipo de cómputo personal de las cuales la clasificó de severidad alta y 6 de severidad media, indicando la herramienta de Nessus Escencial que se tienen vulnerabilidades que solucionar.

My Basic Network Scan / Plugin #42873

[Back to Vulnerability Group](#)

Vulnerabilities 22

HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

<http://www.nessus.org/u?df555f5>

<https://sweet32.info>

Output

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

Name	Code	KEX	Auth	Encryption	MAC
DES-CBC3-SHA	0x00, 0x0A	RSA	RSA	3DES-CBC (168)	SHA1

The fields above are :

```
{Tenable ciphername}
{Cipher ID code}
Kex={key exchange}
Auth={authentication}
Encrypt={symmetric encryption method}
MAC={message authentication code}
{export flag}
```

To see debug logs, please visit individual host

Port	Hosts
1433 / tcp / mssql	192.168.100.22

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 : CN=SSL_Self_Signed_Fallback
| -Issuer  : CN=SSL_Self_Signed_Fallback
```

To see debug logs, please visit individual host

Port	Hosts
------	-------

1433 / tcp / mssql	192.168.100.22 
--------------------	--

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=DESKTOP-S36GML9
| -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	192.168.100.22 
------------------	--

Vulnerabilities 22

MEDIUM SSL Self-Signed Certificate

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Output

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :
```

```
| -Subject : CN=SSL_Self_Signed_Fallback
```

To see debug logs, please visit individual host

Port	Hosts
1433 / tcp / mssql	192.168.100.22 

Vulnerabilities 22

MEDIUM TLS Version 1.0 Protocol Detection

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

See Also

<https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00>

Output

```
TLSv1 is enabled and the server supports at least one cipher.
```

To see debug logs, please visit individual host

Port	Hosts
1433 / tcp / mssql	192.168.100.22 

Vulnerabilities 22

MEDIUM TLS Version 1.1 Deprecated Protocol**Description**

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

See Also

<https://datatracker.ietf.org/doc/html/rfc8996>

<http://www.nessus.org/u?c8ae820d>

Output

TLSv1.1 is enabled and the server supports at least one cipher.

To see debug logs, please visit individual host

Port	Hosts
1433 / tcp / mssql	192.168.100.22

192.168.100.22

Vulnerabilities 22

MEDIUM SMB Signing not required**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>

Output

No output recorded.

To see debug logs, please visit individual host

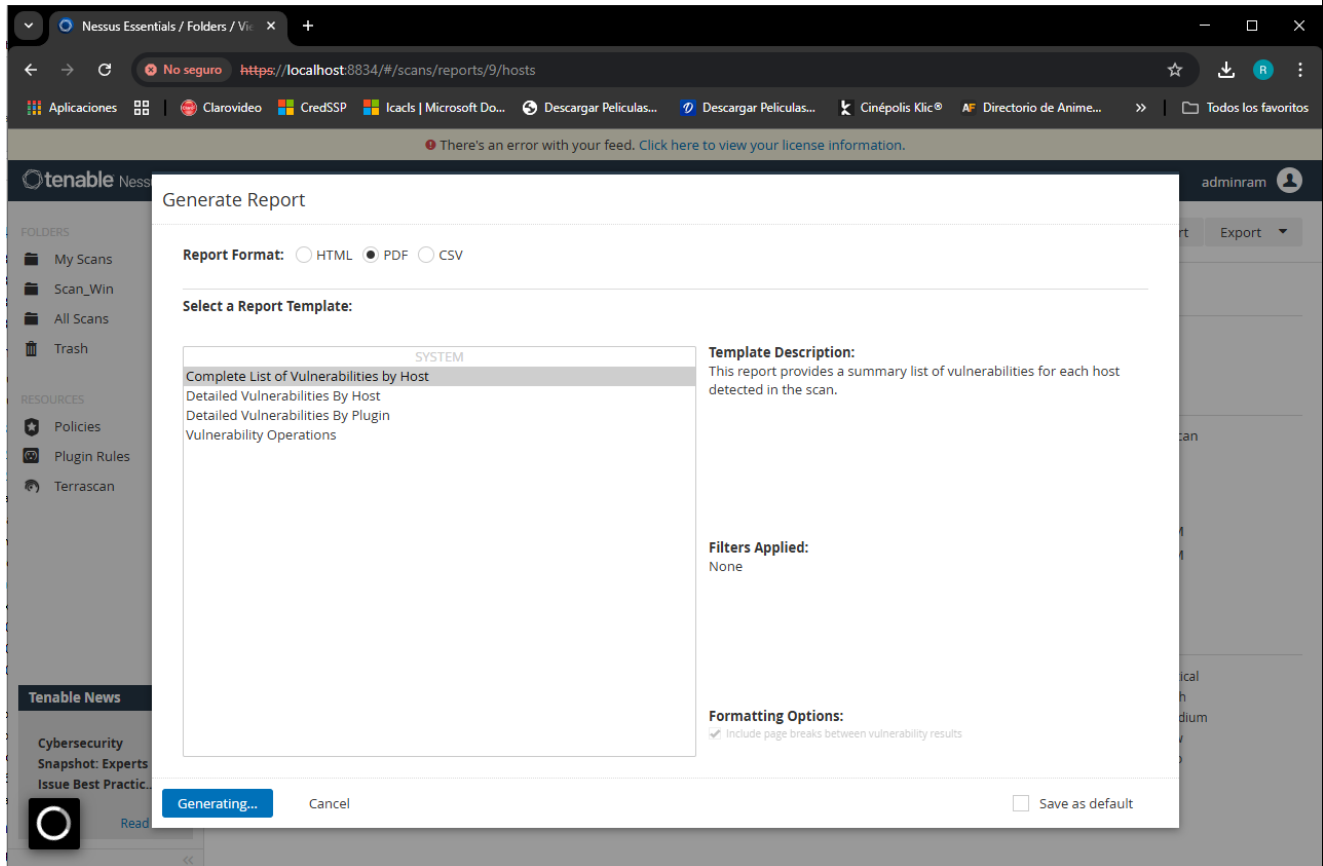
Port	Hosts
445 / tcp / cifs	192.168.100.22

192.168.100.22

The screenshot displays the Tenable Nessus Essentials web interface. The browser address bar shows the URL `https://localhost:8834/#/scans/reports/9/hosts`. The interface includes a sidebar with 'FOLDERS' (My Scans, Scan_Win, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'My Basic Network Scan' and includes tabs for 'Hosts' (1), 'Vulnerabilities' (26), and 'History' (2). A table lists the scanned host: 192.168.100.22, showing 6 vulnerabilities. To the right, 'Scan Details' are provided: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: June 6 at 5:57 PM, End: June 6 at 6:15 PM, Elapsed: 18 minutes. A 'Vulnerabilities' donut chart shows the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (blue), and Info (light blue).

Reporte.

En este punto de la actividad realizaremos la generación del reporte o reportes con las incidencias detectadas en la herramienta de tenable Nessus. realizaremos dos reportes: El primero donde se nos muestre el listado de las vulnerabilidades y su severidad, el segundo donde la información sea más detallada como se nos muestra en incidencias encontradas severidad, vulnerabilidad y su solución en un reporte facilitará a cualquier persona entender la situación que se nos está presentando en nuestra infraestructura.



192.168.100.22



Vulnerabilities

Total: 44

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5	6.1	0.5478	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.3	-	-	57608	SMB Signing not required

Nessus Essentials / Folders / Vulnerabilities

https://localhost:8834/#/scans/reports/9/hosts

There's an error with your feed. [Click here to view your license information.](#)

adminram

Generate Report

Report Format: ☐ HTML ☒ PDF ☐ CSV

Select a Report Template:

- SYSTEM
- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host**
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

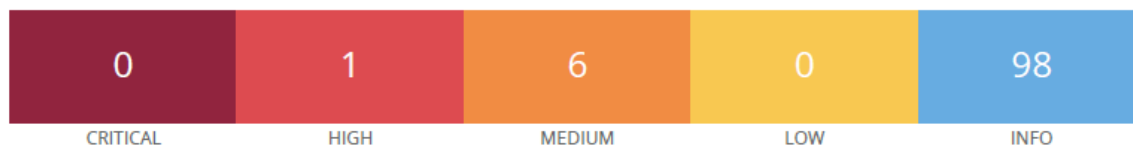
Template Description:
This report presents detailed vulnerabilities by host.

Filters Applied:
None

Formatting Options:
☒ Include page breaks between vulnerability results

Generating... Cancel ☐ Save as default

192.168.100.22



Host Information

Netbios Name: DESKTOP-S36GML9
IP: 192.168.100.22
OS: Microsoft Windows

The screenshot displays the Tenable Nessus Essentials web interface. The browser address bar shows the URL `https://localhost:8834/#/scans/reports/9/hosts`. The interface has a dark header with the Tenable logo and navigation tabs for Scans and Settings. A sidebar on the left contains 'FOLDERS' (My Scans, Scan_Win, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main area is titled 'My Basic Network Scan' and includes buttons for Configure, Audit Trail, Launch, Report, and Export. Below the title are tabs for Hosts (1), Vulnerabilities (26), and History (2). A search bar and a table of hosts are visible. The table lists one host, 192.168.100.22, with 6 vulnerabilities. To the right, the 'Scan Details' panel shows: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: June 6 at 5:57 PM, End: June 6 at 6:15 PM, and Elapsed: 18 minutes. Below this is a 'Vulnerabilities' donut chart showing a distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Análisis e Identificación de mejoras.

En este punto de la actividad realizaremos el análisis de la detección e identificamos que requerimos para realizar la solución de mejora para nuestro equipo y nuestra infraestructura.

HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

No dice que el método de encriptación que sea mayor que 64 bit y menor a 112 bit en una llave que usa 3DES encryption suite es vulnerable con un score de 7.5 siendo catalogado como severidad alta.

La solución o mejora que se identifica es no utilizar este tipo de encriptado y deshabilitar esta funcionalidad para evitar su uso por algún error o que sea blanco de algún ataque.

<p>MEDIUM SSL Certificate Cannot Be Trusted</p>	<p>Me indica que no tengo un certificado válido para</p>
<p>MEDIUM SSL Self-Signed Certificate</p>	<p>utilizar la herramienta de tenable nessus que genere un certificado válido para poder utilizar de manera segura y correcta ya que la herramienta lo ve las dos detecciones vulnerables con un score de 6.5 siendo catalogado como severidad media.</p> <p>La solución o mejora que se identifica es obtener un certificado de una entidad certificadora válida para poder proteger el usos de la herramienta y no sea un blanco de ataques.</p> <p>Nota: existe una tercera vulnerabilidad que se duplica y se homologa con la primera vulnerabilidad.</p>
<p>MEDIUM TLS Version 1.0 Protocol Detection</p>	<p>Aquí indica el servicio remotos con acceso a el protocolo TLS 1.0 ya no se debe de utilizar ya que es una tecnología ya obsoleta y vulnerable con un score de 6.5 siendo catalogado como severidad media.</p> <p>La solución o mejora que se identifica es utilizar el protocolo TLS 1.2 o 1.3 ya que estos son métodos seguros de conexión para los servicio remotos por tal motivo se procede con la deshabilitación del protocolo 1.0.</p>
<p>MEDIUM TLS Version 1.1 Deprecated Protocol</p>	<p>Aquí indica el servicio remotos con acceso a el protocolo TLS 1.1 ya no se debe de utilizar ya que es una</p>

	<p>tecnología ya obsoleta y vulnerable con un score de 6.5 siendo catalogado como severidad media.</p> <p>La solución o mejora que se identifica es utilizar el protocolo TLS 1.2 o 1.3 ya que estos son métodos seguros de conexión para los servicio remotos por tal motivo se procede con la deshabilitación del protocolo 1.1.</p>
<p>MEDIUM SMB Signing not required</p>	<p>Nos indica que el protocolo SMB es vulnerable con un score de 5.3 siendo catalogado como severidad media.</p> <p>La solución o mejora que se identifica es el deshabilitar el SMB para evitar qué sea blanco de algún ataque.</p>

Conclusion.

En conclusión: En mi día a día, ya sea como profesional de TI o simplemente como usuario de internet, la detección y prevención de ataques de acceso es fundamental. Constantemente interactuamos con sistemas que almacenan información sensible, desde datos bancarios hasta historiales médicos o en el campo laboral, propiedad intelectual y diseños críticos. Un ataque de acceso exitoso puede resultar en robo de identidad, fraude financiero, interrupción de servicios o, para una empresa, pérdidas millonarias y daño reputacional irreparable.

La clave no es sólo reaccionar ante una brecha, sino establecer defensas proactivas. Capacitar a los usuarios sobre prácticas seguras, como el uso de contraseñas robustas y la identificación de intentos de phishing. La vigilancia continua, la actualización de software y la respuesta rápida ante cualquier anomalía son esenciales. En un mundo cada vez más conectado, la seguridad no es una opción, sino una necesidad imperante para proteger nuestra información y mantener la confianza en los sistemas digitales.

Referencias.

Gemini - chat to supercharge your ideas. (n.d.). Gemini. Retrieved January 9, 2025, from <https://gemini.google.com/>

Ingeniería en desarrollo de software. (n.d.). Edu.Mx. Retrieved January 9, 2025, from <https://umi.edu.mx/coppel/IDS/login/index.php>

SSL medium strength cipher suites supported (SWEET32). (n.d.). Tenable.com. Retrieved June 8, 2025, from <https://www.tenable.com/plugins/nessus/42873>

NVD - CVSS v2.0 calculator. (n.d.). Nist.gov. Retrieved June 8, 2025, from <https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=AV:N/AC:L/Au:N/C:P/I:N/A:N>

Tai, W. (2020, April 16). *What is VPR and how is it different from CVSS?* Tenable®. <https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss>