

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

### Seguridad informática II.

Ingeniería en Desarrollo de Software.



academiaglobal

TUTOR: Jessica Hernández

ALUMNO: Carlos Ariel Nicolini

FECHA: 21/05/2025

## Índice

<b>Introducción .....</b>	<b>3</b>
<b>Descripción .....</b>	<b>4</b>
<b>Justificación .....</b>	<b>5</b>
<b>Desarrollo.....</b>	<b>6</b>
• <b>Incidencias encontradas .....</b>	<b>6</b>
• <b>Reporte.....</b>	<b>8</b>
• <b>Análisis de identificación de mejoras .....</b>	<b>14</b>
<b>Conclusión.....</b>	<b>17</b>
<b>Referencias.....</b>	<b>18</b>

# Introducción

La detección y prevención de intrusiones son dos términos generales que describen las prácticas de seguridad de aplicaciones que se utilizan para mitigar ataques y bloquear nuevas amenazas.

La primera es una medida reactiva que identifica y mitiga los ataques en curso mediante un sistema de detección de intrusiones. Es capaz de eliminar el malware existente (Troyanos, puertas traseras, etc.) y detectar ataques de ingeniería social (intermediarios, phishing) que manipulan a los usuarios para que revelen información confidencial.

La segunda es una medida de seguridad proactiva que utiliza un sistema de prevención de intrusiones para bloquear preventivamente los ataques a las aplicaciones. Esto incluye la inclusión remota de archivos que facilita la inyección de malware y las inyecciones de SQL utilizadas para acceder a las bases de datos de una empresa.

Un IDS es un dispositivo de hardware o una aplicación de software que utiliza firmas de intrusión conocidas para detectar y analizar el tráfico de red entrante y saliente en busca de actividades anormales.

# Descripción

## **Contextualización:**

Se pretende utilizar algunas técnicas de protección ante ataques de explotación y obtención de accesos a sistemas realizando auditorías a la red mediante herramientas tecnológicas ya sea especializadas o que presenten esta funcionalidad de auditoría.

En este sentido, se requiere analizar los factores que enfatizan la importancia de la seguridad y que se describen a continuación:

- Prevenir los ataques de acceso.
- Prevenir accesos a las redes.
- Monitoreo completo de la red.

## **Actividad:**

Instalar y utilizar un software que permita detectar/prevenir ataques de acceso del sistema y la red.

Auditoria de vulnerabilidades en la red:

- Instalar y analizar el equipo.
- Analizar un equipo en búsqueda de posibles ataques como son virus, accesos o percances en red.
- Adjuntar el reporte generado desde la herramienta o capturar el resultado del análisis.

## Justificación

En esta instalaremos el software de tenable Nessus para realizar una prueba de escaneo en nuestra maquina personal, ejecutaremos un escaneo de red para detectar y revisar el resultado que nos entregue.

En esta oportunidad continuaremos con los temas de seguridad y su importancia que tiene, aprenderemos a realizar escaneos de riesgos o vulnerabilidades, para tal motivo utilizaremos herramientas que son muy conocidas en el mercado y de amplia utilización. No estoy familiarizado con la utilización de tenable Nessus, pero si con los escaneos de seguridad, ya que en la empresa nos toca revisar los escaneos que nos envía el área de seguridad sobre riesgos o vulnerabilidades y como responsables del sistema operativo Windows server nos toca remediarlos o cubrir esas vulnerabilidades.

En nuestro caso dependiendo del riesgo o la vulnerabilidad (critico, moderado, bajo), se tiene cierto tiempo, desde 3 días hasta un mes para su remediación. Hay también un departamento encargado de darle seguimiento a esos casos y se debe dar seguimiento de manera correcta hasta su remediación.

Este trabajo fue subido al siguiente enlace de GitHub

<https://github.com/CarlosNico/Seguridad-inform-tica-II/>

# Desarrollo

## Incidencias encontradas

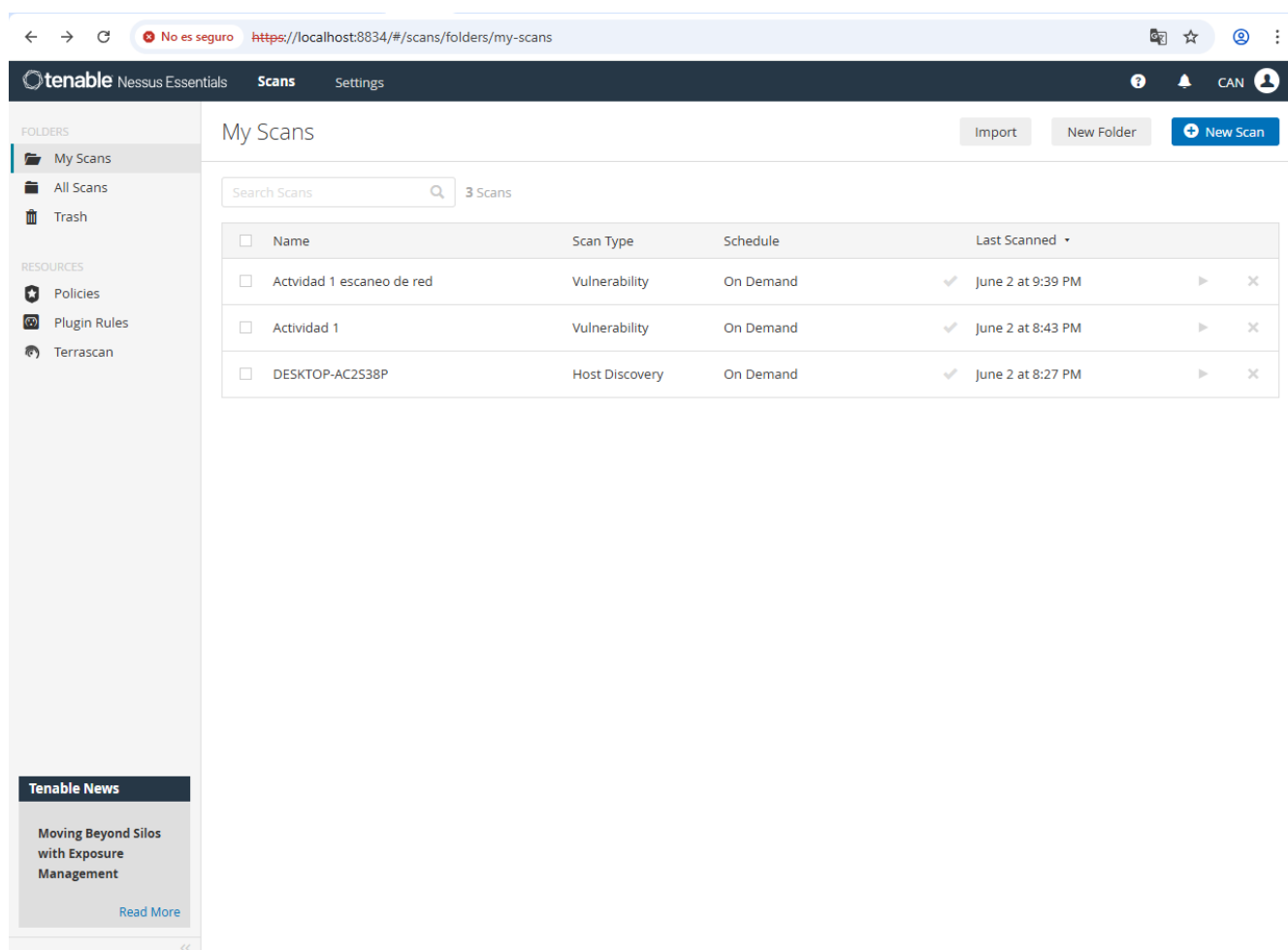
En esta parte del ejercicio realizamos un escaneo de seguridad en la herramienta Nessus Tenable.

Se encontró 3 incidencias de severidad media relacionadas con el certificado SSL que no esta firmado de manera digital y que esta expirado.

- SSL Certificate cannot be trusted
- SSL self-signed certificate
- SSL Certificate expiry

# Reporte

Una vez instalado el software realizamos un Basic Network Scan y obtenemos el resultado. En la imagen se muestra que se realizó el escaneo como se mostraba en el video, aunque también realice un escaneo Host Discovery y un Malware Scan. En el Basic Network Scan se encontraron una vulnerabilidad de certificado como se menciona en el apartado anterior. En los escaneos de Host Discovery y el malware Scan salieron sin ningún riesgo.



The screenshot shows the Tenable Nessus Essentials interface. The top navigation bar includes the Tenable logo, 'Nessus Essentials', and tabs for 'Scans' and 'Settings'. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'My Scans' and features a search bar and a table of scans.

<input type="checkbox"/>	Name	Scan Type	Schedule	Last Scanned		
<input type="checkbox"/>	Actividad 1 escaneo de red	Vulnerability	On Demand	June 2 at 9:39 PM	▶	✕
<input type="checkbox"/>	Actividad 1	Vulnerability	On Demand	June 2 at 8:43 PM	▶	✕
<input type="checkbox"/>	DESKTOP-AC2538P	Host Discovery	On Demand	June 2 at 8:27 PM	▶	✕

Below the table, there is a 'Tenable News' section with the headline 'Moving Beyond Silos with Exposure Management' and a 'Read More' link.

← → ↻ No es seguro https://localhost:8834/#/scans/reports/14/hosts

tenable Nessus Essentials Scans Settings

Actividad 1 escaneo de red

Configure Audit Trail Launch Report Export

Back to My Scans

Hosts 1 Vulnerabilities 23 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.1.8	4 89

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: June 2 at 8:52 PM  
End: June 2 at 9:39 PM  
Elapsed: an hour

Vulnerabilities

4 Critical  
89 High  
23 Medium  
1 Low  
1 Info

Tenable News

Getting Ahead of AI Risk: What Comes Next for Tena...

Read More



tenable

Nessus Essentials

Scans

Settings

?

🔔

CAN

FOLDERS

📁 My Scans

📁 All Scans

🗑️ Trash

RESOURCES

★ Policies

🔧 Plugin Rules

🔍 Terrascan

Tenable News

Getting Ahead of AI Risk: What Comes Next for Tena...

Read More

Actividad 1 escaneo de red / 192.168.1.8 / SSL (Mul...

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities 23

Search Vulnerabilities

8 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	EPSS	Family	Count	
<input type="checkbox"/>	MEDIUM	6.5			General	2	
<input type="checkbox"/>	MEDIUM	6.5			General	1	
<input type="checkbox"/>	MEDIUM	5.3			General	1	
<input type="checkbox"/>	INFO				General	3	
<input type="checkbox"/>	INFO				General	2	
<input type="checkbox"/>	INFO				General	2	
<input type="checkbox"/>	INFO				General	2	
<input type="checkbox"/>	INFO				General	1	

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: June 2 at 8:52 PM

End: June 2 at 9:39 PM

Lapsed: an hour

Vulnerabilities

Critical

High

Medium

Low

Info

Tenable Nessus Essentials Scans Settings

## Actividad 1 escaneo de red / Plugin #51192

[Back to Vulnerability Group](#)

Vulnerabilities 38

### 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 doesn'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.hacktricks.com/TLSSEC-X509/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=Maxima Datacenter Online/CN=Maxima Server/CN=Her York/CN=C/S-HQ/CN=DHS/AC=US
|-Issuer : CN=Maxima Datacenter Online/CN=Maxima Certification Authority/CN=Her York/CN=C/S-HQ/CN=DHS/CN=Maxima Certification Authority

To see debug logs, please visit individual host
```

Host	Port	Hosts
192.168.1.8	443/tcp/www	192.168.1.8

```
The following certificate was part of the certificate chain sent by the remote host, but it has expired :
|-Subject : CN=S/ST=Illinois/CN=Chicago/CN=Daghyrd Studios/CN=WebSocket++/CN=Peter Thorsen/E=peter.thorsen@daghyrd.com
|-Not After : Nov 14 21:00:14 2013 GMT

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=S/ST=Illinois/CN=Chicago/CN=Daghyrd Studios/CN=WebSocket++/CN=Peter Thorsen/E=peter.thorsen@daghyrd.com
|-Issuer : CN=S/ST=Illinois/CN=Chicago/CN=Daghyrd Studios/CN=WebSocket++/CN=Peter Thorsen/E=peter.thorsen@daghyrd.com

To see debug logs, please visit individual host
```

Host	Port	Hosts
192.168.1.8	443/tcp/www	192.168.1.8

No es seguro [https://localhost:8834/#/scans/reports/14/hosts/2/vulnerabilities/group/51192/57582](#)
🔍 ⭐ 🔄

Tenable Nessus Essentials Scans Settings ? 🔔 CAN 👤

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

**Tenable News**

HPE Insight Remote Support Multiple Vulnerabilitie...

[Read More](#)

## Actividad 1 escaneo de red / Plugin #57582

[← Back to Vulnerability Group](#)

Configure Audit Trail Launch ▼ Report Export ▼

Vulnerabilities
23

---

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 : C=US/ST=Illinois/L=Chicago/O=Zaphoyd Studios/OU=WebSocket++/CN=Peter Thorson/E=webmaster@zaphoyd.com
```

To see debug logs, please visit individual host

Port	Hosts
9012 / tcp / www	192.168.1.8

**Plugin Details**

---

Severity: Medium  
ID: 57582  
Version: 1.6  
Type: remote  
Family: General  
Published: January 17, 2012  
Modified: June 14, 2022

**Risk Information**

---

Risk Factor: Medium  
**CVSS v3.0 Base Score: 6.5**  
CVSS v3.0 Vector:  
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N  
CVSS v2.0 Base Score: 6.4  
CVSS v2.0 Vector:  
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

tenable

Nessus Essentials

Scans

Settings

?

🔔

CAN

FOLDERS

📁 My Scans

📁 All Scans

🗑️ Trash

RESOURCES

★ Policies

🔗 Plugin Rules

🔗 Terrascan

Tenable News

Siemens User Management Component V2.15 Multiple V...

Read More

Actividad 1 escaneo de red / Plugin #15901

Configure

Audit Trail

Launch

Report

Export

Back to Vulnerability Group

Vulnerabilities 23

MEDIUM

SSL Certificate Expiry

<

>

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Output

The SSL certificate has already expired :

Subject : C=US, ST=Illinois, L=Chicago, O=Zaphoyd Studios, OU=WebSocket++, CN=Peter Thorson, emailAddress=webmaster@zaphoyd.com

Issuer : C=US, ST=Illinois, L=Chicago, O=Zaphoyd Studios, OU=WebSocket++, CN=Peter Thorson, emailAddress=webmaster@zaphoyd.com

Not valid before : Nov 15 21:20:06 2011 GMT

Not valid after : Nov 14 21:20:06 2012 GMT

To see debug logs, please visit individual host

Port	Hosts
9012 / tcp / www	192.168.1.8

Plugin Details

Severity: Medium

ID: 15901

Version: 1.50

Type: remote

Family: General

Published: December 3, 2004

Modified: February 3, 2021

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 v2.0 Base Score: 5.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

<<

Escaneo de Host Discovery.

tenable

Nessus Essentials

Scans

Settings

?

🔔

CAN

FOLDERS

My Scans

All Scans

Trash

RESOURCES

★ Policies

🔧 Plugin Rules

🔍 Terrascan

Tenable News

Where Capability Meets Opportunity: Introducing th...

Read More

DESKTOP-AC2S38P

Configure

Audit Trail

Launch

Report

Export

Hosts 1

Vulnerabilities 2

History 1

Filter

Search Hosts

1 Host

<input type="checkbox"/>	Host	Ports	
<input type="checkbox"/>	192.168.1.8	135, 139, 445, 49664, 49665, 49666, 49667, 49669, 49670	✕

Scan Details

Policy:

Host Discovery

Status:

Completed

Severity Base:

CVSS v3.0

Scanner:

Local Scanner

Start:

Today at 8:27 PM

End:

Today at 8:27 PM

Elapsed:

a few seconds

Vulnerabilities

Critical

High

Medium

Low

Info

## Escaneos de malware Scan.

The screenshot displays the Tenable Nessus Essentials web interface. The browser address bar shows a local URL: `https://localhost:8834/#/scans/reports/11/hosts`. The interface has a dark blue header with the Tenable logo and navigation tabs for 'Scans' and 'Settings'. On the left, a sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'Actividad 1' and includes tabs for 'Hosts' (1), 'Vulnerabilities' (8), and 'History' (1). Below these tabs is a search bar and a table with one host: 192.168.1.8, which has 35 vulnerabilities. To the right, the 'Scan Details' section shows: Policy: Malware Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: Today at 8:39 PM, End: Today at 8:43 PM, and Elapsed: 5 minutes. Below this is a 'Vulnerabilities' section with a donut chart showing 0 Critical, 0 High, 0 Medium, 0 Low, and 35 Info vulnerabilities. A 'Tenable News' banner at the bottom left promotes 'HPE Insight Remote Support Multiple Vulnerabilitie...'. The bottom of the page shows a double-left arrow navigation control.

tenable Nessus Essentials Scans Settings

Actividad 1

Configure Audit Trail Launch Report Export

Back to My Scans

Hosts 1 Vulnerabilities 8 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.1.8	35

Scan Details

Policy: Malware Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 8:39 PM  
End: Today at 8:43 PM  
Elapsed: 5 minutes

Vulnerabilities

0 Critical  
0 High  
0 Medium  
0 Low  
35 Info

Tenable News

HPE Insight Remote Support Multiple Vulnerabilitie...

Read More

## Análisis e identificación de mejoras

En el análisis de seguridad nos salieron 3 vulnerabilidades derivada de un certificado SSL vencido y que esta parte se analizará el reporte y lo que se debe realizar para cubrir esa vulnerabilidad.

Se necesita crear o comprar un nuevo certificado SSL para este servicio que este firmado por una entidad certificadora que tenga un tiempo de expiración nuevo que Nessus acepte para cubrir ese riesgo de seguridad y aplicarlo en la bóveda de certificados de confianza, luego configurarlo en la página para que lo reconozca como un sitio de confianza.

Se agregan uno sitio y un video donde se revisó como realizarlo.

<https://learn.microsoft.com/en-us/answers/questions/1667447/how-to-fix-51192-ssl-certificate-cannot-be-trusted>

<https://www.youtube.com/watch?v=8-cruG-ZqFc>

## Conclusión

La prevención y detección de ataque de acceso son de vital importancia para la ciberseguridad de una empresa o en nuestra vida personal, ya que nos permitirá proteger información crítica (del negocio en el ámbito empresarial) y mitigar el daño causado por ciberamenazas. La correcta implementación y uso de estos sistemas nos ayudaran a identificar actividades no autorizadas o sospechosas y poder responder de manera rápida para evitar una intrusión y daño.

Pero no solo la implementación de estos sistemas nos va a ayudar a proteger los bienes de la empresa, sino es necesario instruir al personal para su correcto uso y que tengan la responsabilidad de la importancia de su correcta realización, ya que una falla en este proceso puede significar pérdidas económicas para la empresa, daños en su imagen con los clientes o demandas millonarias.

Me a tocado estar en un evento de intromisión y las perdidas en dinero son considerables que hace que las empresas se replanteen los funcionamientos internos de los departamentos y prestar atención a todos los riesgos.

<https://github.com/CarlosNico/Seguridad-inform-tica-II/>

## Referencias

¿Qué es un sistema de prevención de intrusiones (IPS)? (2024, July 16). Ibm.com.  
<https://www.ibm.com/mx-es/topics/intrusion-prevention-system>

TechTalkSecurity [@sumitnick4]. (n.d.). SSL certificate not trusted, even after importing CA cert to trusted root store in Windows machine. Youtube. Retrieved June 8, 2025, from  
<https://www.youtube.com/watch?v=8-cruG-ZqFc>

vinaypamnani-msft. (n.d.). Renovación de certificados. Microsoft.com. Retrieved June 8, 2025, from  
<https://learn.microsoft.com/es-es/windows/client-management/certificate-renewal-windows-mdm>

Wright, M., Ziv Rika, McKeever, G., Hasson, E., Holmes, D., Rika, Z., & Michael Wright.  
(n.d.). Intrusion Detection & prevention. Learning Center; Imperva Inc. Retrieved June 8, 2025, from  
<https://www.imperva.com/learn/application-security/intrusion-detection-prevention/>