Universidad Corporativa | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad [1] - [Detección y Prevención de Ataques de Acceso]

[Seguridad Informática II]

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero

Alumno: Carlos Fco Estrada Salazar

Fecha: 27/ene/2025

INDICE

GitHub Link:

INTRODUCCIÓN

En la actualidad, la seguridad informática es una prioridad para cualquier organización, ya que las amenazas cibernéticas están en constante evolución, poniendo en riesgo tanto la integridad de los sistemas como la confidencialidad de los datos. Esta actividad tiene como propósito la detección y prevención de ataques de acceso en sistemas y redes mediante el uso de herramientas tecnológicas especializadas. Este enfoque es crucial para garantizar un entorno seguro y minimizar la exposición a riesgos.

En esta actividad, se llevará a cabo una auditoría de vulnerabilidades para identificar posibles brechas en la seguridad de un equipo y de la red. El objetivo principal es instalar y utilizar un software especializado que permita detectar y prevenir ataques como virus, intentos de acceso no autorizado y otros percances relacionados con la red. A través de este proceso, se busca obtener una visión clara del estado de seguridad del sistema, así como implementar medidas correctivas o preventivas en caso de encontrar debilidades.

Además, se analizarán los factores clave que resaltan la importancia de la seguridad informática, como la prevención de accesos no autorizados, el monitoreo continuo de la red y la protección ante ataques de explotación. Este análisis permitirá comprender las técnicas y herramientas que se pueden emplear para mantener un control proactivo sobre los riesgos de ciberseguridad.

Finalmente, se incluirá un reporte generado por la herramienta seleccionada o capturas de los resultados obtenidos, lo cual respaldará las conclusiones derivadas de la auditoría. Este enfoque práctico no solo fortalece los conocimientos teóricos, sino que también contribuye a desarrollar habilidades esenciales para la protección de sistemas y redes en el ámbito profesional.

DESCRIPCIÓN

La detección y prevención de ataques de acceso en sistemas y redes es una tarea fundamental en el ámbito de la seguridad informática. En el contexto de esta actividad, se enfatiza la necesidad de realizar auditorías de red utilizando herramientas especializadas que permitan identificar vulnerabilidades, analizar posibles brechas de seguridad y prevenir accesos no autorizados. Este enfoque resulta crítico, dado que las amenazas actuales no solo buscan comprometer la disponibilidad de los recursos, sino también la confidencialidad e integridad de la información.

El objetivo principal de esta actividad es garantizar la protección de los sistemas frente a ataques de explotación y obtención de acceso. Esto se logra mediante la implementación de soluciones tecnológicas capaces de realizar auditorías profundas, monitorear constantemente el tráfico en la red y ofrecer alertas en tiempo real ante cualquier anomalía. Estas acciones contribuyen a evitar que actores maliciosos logren infiltrarse en la infraestructura de red o comprometan los equipos conectados a ella.

La instalación y análisis de un equipo mediante herramientas de auditoría permiten observar en detalle su comportamiento, identificando posibles amenazas como virus, malware o accesos no autorizados. Además, al generar reportes o capturas de los resultados obtenidos, se tiene una base sólida para proponer mejoras en las políticas de seguridad.

En esencia, esta actividad fomenta la comprensión de los principios y técnicas necesarias para mantener la seguridad de sistemas y redes en un entorno donde las amenazas evolucionan constantemente. De esta forma, se fortalecen las competencias prácticas y analíticas requeridas para implementar soluciones preventivas y de mitigación frente a riesgos cibernéticos.

JUSTIFICACIÓN

En el contexto actual, donde las amenazas cibernéticas evolucionan constantemente, implementar soluciones de detección y prevención de ataques de acceso se convierte en una necesidad crítica para proteger los sistemas y redes de cualquier organización. Estas soluciones no solo fortalecen la postura de seguridad informática, sino que también ofrecen una respuesta proactiva ante posibles vulnerabilidades que podrían ser explotadas por atacantes.

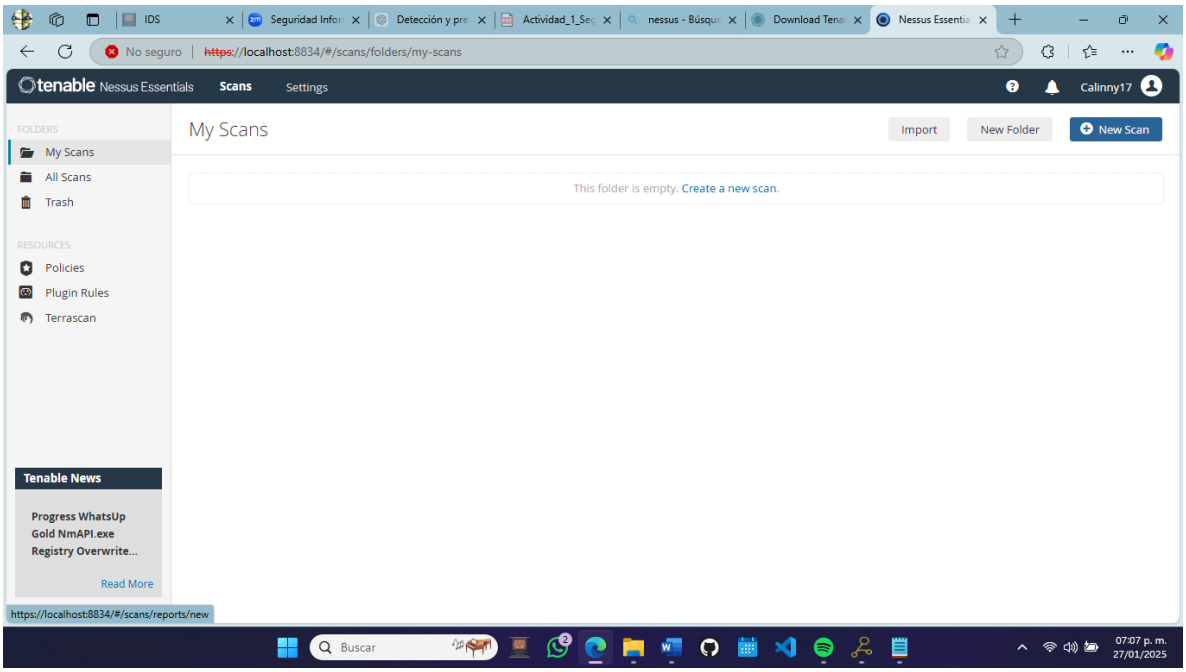
El uso de herramientas tecnológicas especializadas permite realizar auditorías exhaustivas para identificar riesgos como virus, intentos de acceso no autorizado o configuraciones inseguras en la red. Estas auditorías proporcionan datos clave sobre el estado de los sistemas, lo que permite a los administradores tomar decisiones fundamentadas para mitigar riesgos y aplicar medidas preventivas. Además, estas herramientas suelen incluir capacidades de monitoreo en tiempo real, alertas automáticas y generación de reportes detallados, lo que facilita el seguimiento y la documentación de eventos de seguridad.

Otra razón fundamental para emplear estas soluciones es su capacidad de optimizar los recursos y minimizar el impacto de posibles incidentes de seguridad. Al identificar amenazas antes de que se materialicen, se reduce significativamente el tiempo y los costos asociados con la recuperación de sistemas comprometidos. Asimismo, estas herramientas contribuyen al cumplimiento de normativas y estándares de seguridad, asegurando que las redes operen bajo lineamientos adecuados para proteger datos sensibles.

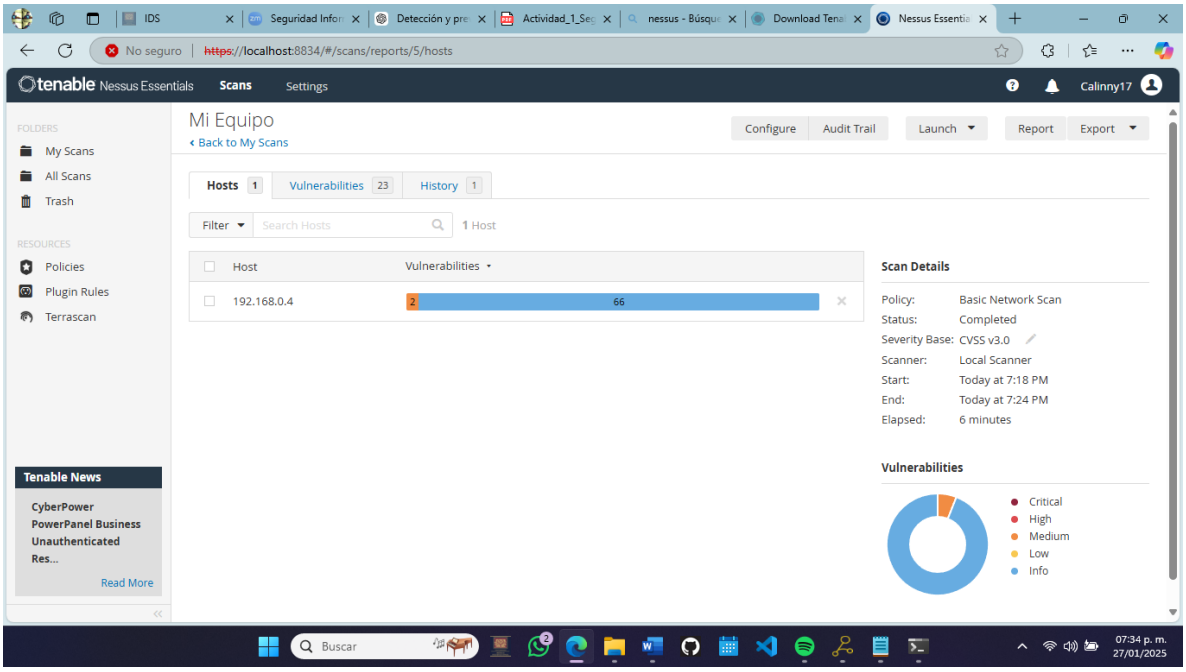
En conclusión, el uso de soluciones de detección y prevención no solo aborda los desafíos técnicos asociados con la seguridad informática, sino que también fortalece la confianza en los sistemas al garantizar la protección continua de los activos digitales. Este enfoque es esencial para construir una infraestructura robusta y resiliente frente a las crecientes amenazas del panorama cibernético.

DESARROLLO

Incidencias encontradas

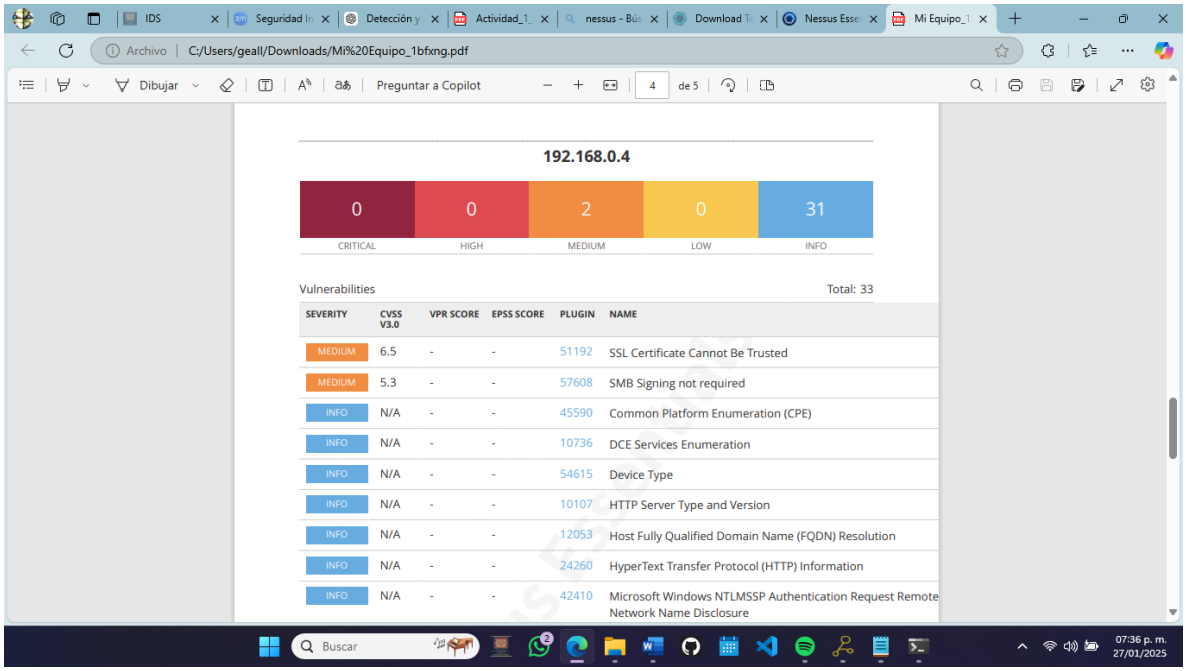


Instalación de Nessus.



Escaneando la IP de mi equipo.

Reporte



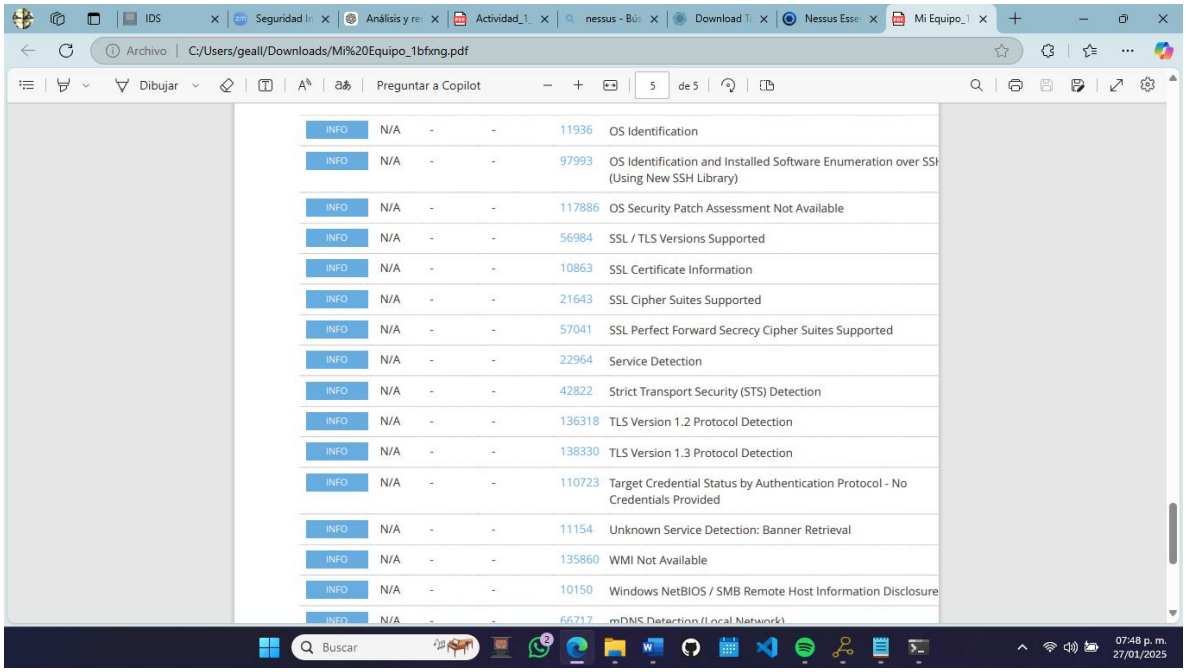
192.168.0.4

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	0	31

Vulnerabilities — Total: 33

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	-	-	57608	SMB Signing not required
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Generando reporte de vulnerabilidades de mi equipo (Adjunto PDF al trabajo).



INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	97993	OS Identification and Installed Software Enumeration over SSH (Using New SSH Library)
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

Análisis e identificación de mejoras

Análisis de Vulnerabilidades

1. **SSL Certificate Cannot Be Trusted (CVSS 6.5, severidad media):**

- Este problema ocurre cuando el certificado SSL utilizado no es confiable, lo que puede comprometer la integridad de las conexiones HTTPS.

2. **SMB Signing not required (CVSS 5.3, severidad media):**

- Indica que el protocolo SMB no requiere firma, lo cual permite que los atacantes realicen ataques de tipo "man-in-the-middle" para interceptar y modificar comunicaciones SMB.

3. **Varios problemas de divulgación de información:**

- Vulnerabilidades de bajo impacto pero informativas incluyen:
- Enumeración de servicios DCE.
- Resolución de nombres FQDN.
- Versiones de SMB soportadas.
- Información del servidor HTTP y SMB.

4. **Vulnerabilidades relacionadas con TLS/SSL:**

- Se detectaron versiones antiguas de TLS/SSL y problemas con las suites de cifrado, lo que puede exponer la conexión a ataques de degradación.

Recomendaciones

1. **SSL Certificate Cannot Be Trusted:**

- Instalar un certificado SSL emitido por una autoridad certificadora confiable.
- Asegurarse de que el nombre común (CN) del certificado coincida con el nombre del host.

2. **SMB Signing not required:**

- Configurar el servidor SMB para requerir firma en todas las conexiones.
- Revisar políticas de seguridad y asegurar el uso de versiones modernas y seguras del protocolo SMB (preferiblemente SMBv3).

3. **Actualización de Protocolos y Cifrado (TLS/SSL):**

- Deshabilitar versiones antiguas de TLS (1.0 y 1.1).
- Configurar el servidor para usar únicamente suites de cifrado que ofrezcan Perfect Forward Secrecy (PFS).

4. **Mitigación de Vulnerabilidades Informativas:**

- Limitar la exposición de información configurando firewalls y reglas para restringir el acceso a servicios innecesarios.
- Deshabilitar servicios de red no utilizados como NetBIOS.

5. **Parcheo y Actualización:**

- Implementar un programa regular de aplicación de parches para asegurar que todas las vulnerabilidades conocidas sean corregidas a tiempo.

6. **Auditorías Recurrentes:**

- Realizar escaneos periódicos con herramientas como Nessus para identificar nuevas vulnerabilidades y evaluar la efectividad de las medidas implementadas.

CONCLUSIÓN

La actividad de detección y prevención de ataques de acceso realizada pone de manifiesto la importancia de implementar prácticas y herramientas de seguridad informática en cualquier ámbito, ya sea profesional o personal. En el entorno laboral, donde los sistemas informáticos y las redes son la columna vertebral de las operaciones diarias, garantizar su protección es esencial para evitar interrupciones, pérdidas de datos o accesos no autorizados que puedan comprometer la información sensible de una organización.

La auditoría de vulnerabilidades es un paso fundamental para identificar posibles riesgos y brechas de seguridad. Esto no solo permite tomar medidas preventivas, como reforzar configuraciones de red o actualizar sistemas, sino que también ofrece una visión clara de las áreas que requieren mejoras. En el ámbito cotidiano, esta práctica resulta igualmente valiosa, ya que los dispositivos personales, como computadoras y teléfonos inteligentes, también son objetivos de ataques cibernéticos, especialmente en un mundo cada vez más conectado.

El uso de herramientas tecnológicas para la detección de amenazas demuestra ser una solución eficiente y accesible para reducir riesgos. Estas herramientas facilitan el monitoreo continuo, la identificación temprana de ataques y la generación de reportes que respaldan la toma de decisiones informadas. Este enfoque fortalece no solo la seguridad de los sistemas, sino también la confianza en el uso de tecnologías digitales.

En conclusión, esta actividad destaca la relevancia de adoptar un enfoque proactivo en seguridad informática, desarrollando habilidades que son indispensables tanto en el campo laboral como en la vida cotidiana para proteger los activos digitales frente a las crecientes amenazas cibernéticas.