SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE MINATITLÁN

INGENIERÍA EN SISTEMAS COMPUTACIONALES

"MANUAL DE PRÁCTICAS "

MATERIA

ADMINISTRACION DE REDES

MINATITLÁN, VER. JUNIO DEL 2023

3.2 ÍNDICE DEL MANUAL DE PRÁCTICAS

3.1 INTRODUCCIÓN

El presente manual de prácticas de la materia "Administración de Redes" se ha elaborado con el propósito de proporcionar a los estudiantes una guía detallada y estructurada que les permitirá adquirir un sólido entendimiento de los conceptos fundamentales, las técnicas y las habilidades necesarias para administrar redes de manera efectiva y segura. La administración de redes desempeña un papel crítico en el mundo de la tecnología de la información, donde la conectividad y la seguridad son esenciales para el funcionamiento de organizaciones y sistemas a nivel global.

Este manual está diseñado para acompañar el curso teórico y proporcionar a los estudiantes una plataforma para la aplicación práctica de los conocimientos adquiridos. Las prácticas contenidas en este documento abarcan una amplia gama de temas, desde la configuración de dispositivos de red hasta la implementación de medidas de seguridad, pasando por el análisis y monitoreo del desempeño de la red. Cada práctica se ha estructurado cuidadosamente para garantizar que los estudiantes adquieran competencias prácticas valiosas.

El manual está organizado en secciones temáticas, de acuerdo con el temario de la materia, que abarcan aspectos clave de la administración de redes, tales como la configuración, la seguridad, el análisis y el monitoreo. Cada sección contiene prácticas específicas que permiten a los estudiantes aplicar los conceptos teóricos en situaciones prácticas y reales.

Además de las instrucciones detalladas para llevar a cabo cada práctica, este manual proporciona información de fondo, conceptos clave, objetivos de aprendizaje y sugerencias adicionales para fomentar la comprensión y el desarrollo de habilidades. Los ejercicios prácticos se basan en escenarios reales de administración de redes, lo que brinda a los estudiantes la oportunidad de enfrentarse a desafíos y situaciones que podrían encontrar en sus futuras carreras.

Es importante destacar que este manual de prácticas es una herramienta dinámica que puede adaptarse a las necesidades específicas de su curso. Se

alienta a los instructores y estudiantes a utilizarlo como punto de partida y a complementarlo con ejercicios adicionales, discusiones en clase y proyectos prácticos para profundizar en el conocimiento y la experiencia.

La administración de redes es un campo en constante evolución, y adquirir habilidades sólidas en este ámbito es esencial para aquellos que buscan carreras en tecnología de la información. Este manual de prácticas es un recurso valioso que pretende facilitar el proceso de aprendizaje y preparar a los estudiantes para enfrentar los desafíos de administrar redes en un mundo cada vez más conectado.

3.2 JUSTIFICACIÓN

1. Aplicación Práctica del Conocimiento: La administración de redes es un campo altamente técnico y práctico. Los estudiantes necesitan la oportunidad de aplicar los conceptos teóricos aprendidos en el aula a situaciones reales. Este manual proporciona un conjunto de prácticas que les permiten experimentar de primera mano la configuración, el mantenimiento y la seguridad de redes.

2. Preparación para el Mundo Laboral: En un entorno laboral cada vez más dependiente de la tecnología, los profesionales de TI con habilidades sólidas en administración de redes son altamente demandados. Este manual prepara a los estudiantes para carreras en las que deberán administrar y mantener redes de manera efectiva, lo que les da una ventaja competitiva en el mercado laboral.

3. Complemento a la Teoría: El manual complementa las clases teóricas al proporcionar una dimensión práctica que ayuda a los estudiantes a comprender y consolidar los conceptos enseñados en el aula. Les brinda la oportunidad de ver cómo funcionan las redes en la vida real y cómo se aplican los principios teóricos en la práctica.

4. Desarrollo de Habilidades Técnicas: Las prácticas en este manual permiten a los estudiantes desarrollar habilidades técnicas esenciales, como la configuración de dispositivos de red, la solución de problemas, el monitoreo

del rendimiento y la implementación de medidas de seguridad. Estas habilidades son transferibles y valiosas en una variedad de entornos profesionales.

5. Conciencia de la Seguridad: En un mundo digital donde la seguridad de la información es fundamental, este manual incluye prácticas relacionadas con la seguridad de la red, lo que ayuda a sensibilizar a los estudiantes sobre las amenazas y las medidas necesarias para proteger las redes y los datos.
6. Flexibilidad en el Aprendizaje: El manual es un recurso versátil que puede ser utilizado por instituciones educativas y profesionales de TI. Puede adaptarse a las necesidades y los niveles de experiencia de los estudiantes, lo que lo convierte en una herramienta de aprendizaje flexible.
7. Enfoque en la Resolución de Problemas: Las prácticas fomentan la resolución de problemas, una habilidad crítica en el campo de la administración de redes. Los estudiantes aprenderán a abordar desafíos de manera efectiva y a tomar decisiones informadas.
8. Preparación para Certificaciones: La experiencia adquirida a través de las prácticas en este manual puede ser valiosa para aquellos que buscan obtener certificaciones de administración de redes, ya que les brinda un entorno de aprendizaje práctico.
9. Fomento de la Colaboración: Algunas prácticas pueden realizarse en equipo, lo que promueve la colaboración y la comunicación entre los estudiantes, habilidades esenciales en el lugar de trabajo.

3.3 OBJETIVO GENERAL DEL MANUAL DE PRÁCTICAS

El objetivo general de un manual de prácticas para la materia de Administración de Redes es proporcionar a los estudiantes una guía estructurada y detallada que les permita adquirir un sólido entendimiento de los conceptos, técnicas y habilidades necesarios para administrar redes de manera efectiva y segura.

3.4 DESARROLLO

3.4.1 Práctica 1 Verificar el estado de dispositivos de red usando protocolos de administración

3.4.1.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran la capacidad de verificar el estado de dispositivos de red utilizando protocolos de administración, lo que les permitirá comprender cómo se realizan operaciones básicas de supervisión y gestión de dispositivos en una red.

3.4.1.2 Introducción

La administración de redes implica una serie de tareas fundamentales para garantizar el funcionamiento óptimo de una infraestructura de red. Una de las actividades clave en la administración de redes es la verificación del estado de los dispositivos de red. Esto implica la capacidad de monitorear y evaluar dispositivos como routers, switches, servidores y otros componentes para asegurarse de que funcionen correctamente y estén disponibles para los usuarios.

En esta práctica, los estudiantes aprenderán a utilizar protocolos de administración para verificar el estado de dispositivos de red. La habilidad para acceder y verificar dispositivos es esencial para la resolución de problemas, la optimización del rendimiento y la garantía de la disponibilidad de servicios de red.

3.4.1.3 Correlación Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde al subtema 3.1 Protocolos de administración de red.

3.4.1.4 Material Y Equipo Necesario

1. Dispositivos de red, como routers, switches o servidores (se pueden simular en un entorno de laboratorio si no se dispone de hardware real).

2. Computadoras con acceso a la red para configurar y ejecutar protocolos de administración.
3. Software de emulación de red (si se utiliza un entorno de laboratorio virtual).
4. Documentación de referencia sobre los protocolos de administración utilizados.
5. Acceso a una red de prueba o laboratorio para realizar las verificaciones.

3.4.1.5 Metodología

Preparación del entorno:

- Configurar una red de laboratorio con dispositivos de red (reales o simulados) que se utilizarán en la práctica.
- Asegurarse de que los equipos de los estudiantes tengan acceso a esta red de laboratorio.

Selección de protocolos de administración:

- Elegir los protocolos de administración que se utilizarán en la práctica (por ejemplo, SNMP, SSH, Telnet, ICMP).
- Asegurarse de que los estudiantes tengan acceso a las herramientas necesarias para utilizar estos protocolos en sus equipos (por ejemplo, un cliente SSH).

Ejecución de verificaciones:

- Los estudiantes deben acceder a los dispositivos de red seleccionados y utilizar los protocolos de administración para verificar su estado. Esto puede incluir la obtención de información de hardware, la revisión de registros de eventos, la medición del rendimiento, etc.

Análisis y documentación:

- Los estudiantes deben registrar los resultados de sus verificaciones, incluyendo cualquier problema o anomalía detectada.

- Deben comparar los resultados con las expectativas y discutir posibles implicaciones para la operación de la red.

Presentación y discusión:

- Los estudiantes deben presentar sus hallazgos en el aula y participar en una discusión sobre las prácticas y los desafíos encontrados durante la verificación de dispositivos de red.

3.4.1.6 Sugerencias Didácticas

4 Enfocarse en la documentación: Anima a los estudiantes a llevar un registro detallado de todas las acciones realizadas durante la práctica, incluyendo comandos utilizados, resultados obtenidos y cualquier problema encontrado. La documentación es esencial en la administración de redes.

5 Fomentar la resolución de problemas: Pide a los estudiantes que intenten identificar y resolver problemas durante la práctica. Esto ayudará a desarrollar sus habilidades de solución de problemas, un aspecto crucial de la administración de redes.

6 Promover la colaboración: Anima a los estudiantes a trabajar en parejas o en grupos pequeños. La colaboración puede enriquecer la experiencia de aprendizaje y permitir que los estudiantes compartan conocimientos y enfoques.

7 Realizar análisis crítico: Después de realizar las verificaciones, pide a los estudiantes que analicen los resultados y consideren el impacto de los hallazgos en la red. Esto fomenta la comprensión crítica y el pensamiento analítico.

8 Conexión con escenarios reales: Relaciona la práctica con situaciones de administración de redes del mundo real. Discute casos en los que la verificación de dispositivos es esencial para mantener la operación de la red.

3.4.1.6 Reporte Del Alumno

1. Título: Práctica 1: Verificación del Estado de Dispositivos de Red.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para verificar el estado de los dispositivos de red, incluyendo los protocolos de administración utilizados.
5. Resultados: Muestra los resultados de las verificaciones, incluyendo cualquier problema o anomalía detectada.
6. Análisis: Analiza los resultados y discute sus implicaciones para la operación de la red.
7. Conclusiones: Resume las conclusiones principales de la práctica.
8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado.

3.4.2 Práctica 2 Crear cuentas y perfiles de acceso

3.4.2.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para crear cuentas de usuario y perfiles de acceso en una red, lo que les permitirá entender cómo se gestionan las identidades y los niveles de acceso en un entorno de red.

3.4.2.2 Introducción

La administración de identidades y perfiles de acceso es una parte fundamental de la administración de redes. En una red, es esencial gestionar quién tiene acceso a los recursos y qué privilegios se les otorgan. Esta práctica se enfoca en enseñar a los estudiantes cómo crear cuentas de usuario y perfiles de acceso para garantizar que los usuarios tengan acceso a los recursos adecuados y se cumplan las políticas de seguridad.

En esta práctica, los estudiantes aprenderán cómo crear cuentas de usuario, establecer contraseñas, asignar permisos y configurar perfiles de acceso en un entorno de red. Estas habilidades son cruciales para la seguridad, la gestión de recursos y la optimización de la red.

3.4.2.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde al subtema 4.3: Políticas de seguridad.

3.4.2.4 Material Y Equipo Necesario

1. Servidores de autenticación, como servidores LDAP o Active Directory (pueden ser emulados en un entorno de laboratorio si no se dispone de hardware real).
2. Computadoras cliente con acceso a la red.

3. Software de administración de usuarios y perfiles (puede incluir herramientas de administración de dominio, como "Active Directory Users and Computers" en el caso de Active Directory).
4. Documentación de referencia sobre políticas de seguridad y procedimientos de creación de cuentas de usuario.

3.4.2.5 Metodología

Configuración del Entorno: Configura un entorno de laboratorio con servidores de autenticación y computadoras cliente. Esto puede incluir servidores LDAP, Active Directory u otras soluciones de autenticación, según la infraestructura disponible.

Creación de Cuentas de Usuario: Los estudiantes deben crear cuentas de usuario en el servidor de autenticación. Esto incluye establecer nombres de usuario, contraseñas seguras y, en algunos casos, información adicional sobre los usuarios.

Asignación de Permisos y Perfiles de Acceso: Los estudiantes deben asignar permisos y configurar perfiles de acceso para las cuentas de usuario creadas. Esto puede incluir la asignación de roles, grupos o políticas de seguridad.

Prueba de Acceso: Los estudiantes deben verificar que las cuentas de usuario creadas puedan acceder a los recursos de la red de acuerdo con los permisos y políticas configurados.

Análisis y Documentación: Los estudiantes deben documentar las cuentas de usuario creadas, los perfiles de acceso y cualquier problema encontrado durante la práctica.

Presentación y Discusión: Los estudiantes deben presentar y discutir sus hallazgos en el aula, incluyendo los desafíos enfrentados y las soluciones implementadas.

3.4.2.6 Sugerencias Didácticas

- Enfocarse en la Seguridad: Subraya la importancia de establecer contraseñas seguras y aplicar políticas de seguridad al crear cuentas de usuario. Esto ayudará a los estudiantes a comprender la relevancia de la seguridad en la administración de identidades.
- Simulación de Escenarios Reales: Proporciona a los estudiantes escenarios de usuario reales en los que deben crear cuentas y perfiles de acceso. Esto les dará la oportunidad de aplicar sus habilidades en situaciones prácticas.
- Prueba y Verificación: Anima a los estudiantes a probar y verificar las cuentas de usuario creadas para asegurarse de que tengan acceso a los recursos apropiados. Esto les ayudará a comprender la importancia de la configuración correcta.
- Políticas y Cumplimiento: Destaca la importancia de cumplir con las políticas de seguridad y las regulaciones de privacidad al crear cuentas de usuario. Esto fomentará la comprensión de las implicaciones legales y éticas de la administración de identidades.
- Colaboración y Comunicación: Fomenta la colaboración entre los estudiantes al crear cuentas y perfiles de acceso. La comunicación efectiva es esencial en la administración de identidades, especialmente en entornos empresariales.

3.4.2.7 Reporte Del Alumno

1. Título: Práctica 2: Creación de Cuentas y Perfiles de Acceso.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para crear cuentas de usuario y perfiles de acceso.

5. Resultados: Muestra los resultados de las configuraciones, incluyendo las cuentas de usuario creadas y los perfiles de acceso configurados.
6. Análisis: Analiza las implicaciones de las configuraciones en términos de seguridad y acceso a recursos.
7. Conclusiones: Resume las conclusiones principales de la práctica.
8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado.

3.4.3 Práctica 3 Configurar bitácoras de acceso y uso de recursos en diferentes elementos de red.

3.4.3.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para configurar y gestionar bitácoras de acceso y uso de recursos en diversos elementos de red, lo que les permitirá supervisar y auditar el acceso a la red y garantizar la seguridad y el cumplimiento normativo.

3.4.3.2 Introducción

La implementación de registros o bitácoras de acceso y uso de recursos en elementos de red es un componente crucial de la administración de redes y la seguridad cibernética. Las bitácoras permiten llevar un registro de las actividades realizadas en la red, lo que es esencial para la detección de intrusiones, la solución de problemas y el cumplimiento de políticas de seguridad.

En esta práctica, los estudiantes aprenderán a configurar y gestionar bitácoras de acceso en diferentes elementos de red, como routers, switches, servidores y firewalls. La capacidad de registrar eventos y actividades en la red es fundamental para la administración efectiva y la respuesta a incidentes de seguridad.

3.4.3.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde al subtema 3.2: Bitácoras.

3.4.3.4 Material Y Equipo Necesario

1. Dispositivos de red, incluyendo routers, switches, servidores y firewalls.
2. Computadoras con acceso a los dispositivos de red para configuración y administración.
3. Software de configuración de dispositivos de red (por ejemplo, interfaces de línea de comandos para routers y switches).

4. Documentación de referencia sobre la configuración de bitácoras y registros de eventos en dispositivos de red.

3.4.3.5 Metodología

Configuración del Entorno: Prepara un entorno de laboratorio con dispositivos de red, como routers, switches, servidores y firewalls, donde los estudiantes puedan configurar las bitácoras de acceso y uso de recursos.

Selección de Dispositivos: Los estudiantes deben seleccionar uno o varios dispositivos de red en los que configurarán las bitácoras de acceso y uso de recursos. Pueden elegir diferentes tipos de dispositivos para comprender su configuración específica.

Configuración de Bitácoras: Los estudiantes deberán acceder a los dispositivos de red y configurar las bitácoras de acceso y uso de recursos de acuerdo con las necesidades de supervisión y auditoría.

Generación de Eventos: Realiza acciones que generen eventos en los dispositivos, como intentos de acceso, transferencias de datos o cambios en la configuración, para que los estudiantes puedan observar cómo funcionan las bitácoras.

Análisis y Documentación: Los estudiantes deberán revisar las bitácoras generadas, identificar eventos relevantes y documentar sus hallazgos.

Presentación y Discusión: En el aula, los estudiantes presentarán sus configuraciones de bitácoras y discutirán los eventos observados y su importancia para la seguridad y el monitoreo de la red.

3.4.3.6 Sugerencias Didácticas

- Variabilidad de Dispositivos: Anima a los estudiantes a configurar bitácoras en diferentes tipos de dispositivos de red, como routers, switches y servidores, para comprender las diferencias en la configuración.

- Escenarios de Seguridad: Proporciona a los estudiantes escenarios de seguridad realistas que puedan simular al generar eventos en las bitácoras. Esto les permitirá comprender cómo se utilizan las bitácoras en la detección de amenazas.
- Interpretación de Eventos: Pide a los estudiantes que interpreten los eventos registrados en las bitácoras y evalúen su relevancia para la seguridad y el funcionamiento de la red.
- Políticas de Retención de Datos: Discute las políticas de retención de datos y cómo afectan a las bitácoras. Esto es importante para comprender cuánto tiempo se deben mantener los registros.
- Comparación de Configuraciones: Compara y contrasta las configuraciones de bitácoras de acceso en diferentes dispositivos y discute las mejores prácticas para la administración de bitácoras.

3.4.3.7 Reporte Del Alumno

1. Título: Práctica 3: Configuración de Bitácoras de Acceso y Uso de Recursos.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para configurar las bitácoras de acceso y uso de recursos en los dispositivos de red seleccionados.
5. Resultados: Muestra los registros y eventos generados en las bitácoras.
6. Análisis: Analiza los eventos registrados y su relevancia para la seguridad y el monitoreo de la red.
7. Conclusiones: Resume las conclusiones principales de la práctica.

8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado.

3.4.4 Práctica 4 Utilizar un analizador de protocolos para verificar el estado del tráfico de una red en funcionamiento.

3.4.4.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para utilizar un analizador de protocolos en una red en funcionamiento, lo que les permitirá comprender y verificar el estado del tráfico de la red, identificar problemas, y realizar análisis de desempeño y seguridad.

3.4.4.2 Introducción

Un analizador de protocolos, también conocido como "sniffer," es una herramienta esencial en la administración de redes. Permite a los administradores de red supervisar y analizar el tráfico de la red en tiempo real. Esta práctica se enfoca en enseñar a los estudiantes cómo utilizar un analizador de protocolos para obtener información detallada sobre el tráfico de una red en funcionamiento.

En esta práctica, los estudiantes aprenderán a capturar y analizar paquetes de red, a identificar problemas de tráfico, a evaluar el rendimiento de la red y a detectar posibles amenazas de seguridad. El uso de un analizador de protocolos es fundamental para el diagnóstico y la optimización de redes en tiempo real.

3.4.4.3 Especificar La Correlación Con El O Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde al subtema 3.3: Analizadores de protocolos (scanners y sniffers).

3.4.4.4 Material Y Equipo Necesario

1. Computadoras con acceso a la red.
2. Software de analizador de protocolos (puede incluir herramientas como Wireshark, tcpdump u otros).
3. Documentación de referencia sobre el uso de analizadores de protocolos y la interpretación de paquetes de red.

4. Acceso a una red en funcionamiento para realizar la captura de paquetes y el análisis

3.4.4.5 Metodología

1. Configuración del Entorno: Prepara un entorno de laboratorio con computadoras y acceso a una red en funcionamiento. Asegúrate de que el software del analizador de protocolos esté instalado en las computadoras de los estudiantes.
2. Captura de Paquetes en la Red en Funcionamiento: Los estudiantes deben utilizar el analizador de protocolos para capturar paquetes de la red en funcionamiento. Pueden seleccionar segmentos de la red o dispositivos específicos para la captura.
3. Análisis de Paquetes: Los estudiantes deberán analizar los paquetes capturados para identificar diferentes tipos de tráfico, entender las conversaciones entre dispositivos y detectar problemas o anomalías en el tráfico.
4. Identificación de Problemas y Amenazas: Pide a los estudiantes que identifiquen problemas de tráfico, como congestión, latencia excesiva o paquetes perdidos. Además, anímales a detectar posibles amenazas de seguridad, como intentos de intrusión.
5. Documentación y Presentación: Los estudiantes deben documentar sus hallazgos y presentarlos en el aula, discutiendo los problemas identificados, sus causas y posibles soluciones.

3.4.4.6 Sugerencias Didácticas

- Casos de Uso Reales: Proporciona a los estudiantes casos de uso reales de problemas de red y amenazas de seguridad para que los busquen durante la captura de paquetes. Esto les ayudará a aplicar su conocimiento en situaciones prácticas.

- Escenarios de Seguridad: Incluye escenarios de seguridad específicos en los cuales los estudiantes deben detectar intentos de intrusión o actividades maliciosas en el tráfico de la red.
- Comparación con el Estado Deseado: Anima a los estudiantes a comparar el estado actual del tráfico con el estado deseado o óptimo de la red. Esto les ayudará a identificar áreas de mejora.
- Uso de Filtros: Enséñales a usar filtros en el analizador de protocolos para enfocarse en tipos específicos de tráfico, lo que facilita la identificación de problemas y amenazas.
- Discusión de Soluciones: Fomenta la discusión en el aula sobre posibles soluciones a los problemas y amenazas detectados. Esto promueve el pensamiento crítico y la resolución de problemas.

3.4.4.7 Reporte Del Alumno

1. Título: Práctica 4: Análisis de Tráfico de Red con un Analizador de Protocolos.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para capturar y analizar paquetes de red utilizando el analizador de protocolos.
5. Resultados: Muestra los problemas de tráfico y las amenazas de seguridad detectadas durante el análisis de paquetes.
6. Análisis: Discute las causas de los problemas y las implicaciones de las amenazas de seguridad identificadas.
7. Conclusiones: Resume las conclusiones principales de la práctica y las recomendaciones para mejorar el estado de la red.

8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados, incluyendo posibles soluciones a los problemas detectados.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado durante la práctica.

3.4.5 Práctica 5 Instalar un sistema de monitoreo basado en un protocolo de administración de red

3.4.5.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para instalar y configurar un sistema de monitoreo de red basado en un protocolo de administración de red, lo que les permitirá supervisar el rendimiento, la disponibilidad y la seguridad de una red de manera efectiva.

3.4.5.2 Introducción

El monitoreo de red es una parte esencial de la administración de redes. Permite a los administradores de red supervisar el estado y el rendimiento de los dispositivos y servicios de la red, identificar problemas y tomar medidas proactivas para mantener la red funcionando de manera eficiente y segura. En esta práctica, los estudiantes aprenderán cómo instalar y configurar un sistema de monitoreo de red basado en un protocolo de administración, lo que les proporcionará una herramienta poderosa para la administración y el mantenimiento de la red.

El monitoreo de red ayuda a garantizar la disponibilidad de servicios críticos, a detectar y resolver problemas de red, y a evaluar el rendimiento y la seguridad de la red. Al utilizar un protocolo de administración de red, los estudiantes podrán recopilar datos valiosos y tomar decisiones informadas para mejorar la infraestructura de la red.

3.4.5.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde al subtema 3.1 Protocolos de administración de red.

3.4.5.4 Material Y Equipo Necesario

1. Servidor o computadora que actuará como servidor de monitoreo.
2. Dispositivos de red (routers, switches, servidores) que se monitorearán.
3. Software de monitoreo de red (puede incluir soluciones como Nagios, Zabbix, PRTG, entre otros).
4. Documentación de referencia sobre la instalación y configuración del sistema de monitoreo y el protocolo de administración de red seleccionado.

3.4.5.5 Metodología

1. Planificación y Diseño: Los estudiantes deben planificar y diseñar la implementación del sistema de monitoreo de red. Esto incluye la selección del software de monitoreo, la identificación de los dispositivos a monitorear y la elección del protocolo de administración.
2. Instalación y Configuración: Los estudiantes instalarán el software de monitoreo en el servidor designado y configurarán los dispositivos de red para que sean monitoreados. Esto implica la configuración de alertas, umbrales de rendimiento y otros parámetros relevantes.
3. Recopilación de Datos: El sistema de monitoreo comenzará a recopilar datos sobre el rendimiento y la disponibilidad de la red. Los estudiantes

deben supervisar la recopilación de datos y asegurarse de que se están recopilando adecuadamente.

4. Análisis de Datos y Resolución de Problemas: Los estudiantes deben analizar los datos recopilados y utilizarlos para identificar problemas de rendimiento o disponibilidad en la red. Deben tomar medidas para resolver problemas según sea necesario.

5. Documentación y Presentación: Los estudiantes deben documentar la implementación del sistema de monitoreo, los problemas identificados y las soluciones aplicadas. Luego, presentarán sus hallazgos en el aula y discutirán las lecciones aprendidas.

3.4.5.6 Sugerencias Didácticas

- Selección de Software de Monitoreo: Anima a los estudiantes a investigar y seleccionar software de monitoreo de red basado en protocolos de administración de red adecuados para el entorno de la práctica.

- Configuración de Alertas: Enfatiza la importancia de configurar alertas adecuadas en el sistema de monitoreo para que los estudiantes sean notificados en tiempo real de problemas de red.

- Escenarios de Problemas: Proporciona a los estudiantes escenarios de problemas de red simulados que deben identificar y resolver utilizando el sistema de monitoreo.

- Documentación Efectiva: Enseña a los estudiantes la importancia de documentar adecuadamente la configuración y los procedimientos de monitoreo para futuras referencias y auditorías.

- Interpretación de Datos: Ayuda a los estudiantes a comprender cómo interpretar los datos recopilados y a tomar decisiones informadas en función de esos datos.

3.4.5.7 Reporte Del Alumno

1. Título: Práctica 5: Implementación de un Sistema de Monitoreo de Red.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para seleccionar, instalar, configurar y utilizar el sistema de monitoreo de red.
5. Resultados: Muestra los resultados del monitoreo, incluyendo problemas de red identificados y resueltos.
6. Análisis: Discute los problemas identificados, las soluciones aplicadas y la eficacia del sistema de monitoreo.
7. Conclusiones: Resume las conclusiones principales de la práctica y las lecciones aprendidas.
8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados, así como sugerencias para mejorar el sistema de monitoreo.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado durante la práctica.

3.4.5 Práctica 6 Habilitar un programador de tareas para generar avisos ante eventos predefinidos

3.4.6.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para habilitar un programador de tareas en un sistema informático con el fin de generar avisos o notificaciones automáticas ante eventos predefinidos, lo que les permitirá automatizar tareas de supervisión y administración de la red.

3.4.6.2 Introducción

La automatización de tareas es esencial en la administración de redes y sistemas informáticos. Un programador de tareas permite programar acciones específicas que se deben ejecutar de forma regular o en respuesta a eventos predefinidos. En esta práctica, los estudiantes aprenderán cómo habilitar un programador de tareas para generar avisos automáticos ante eventos específicos, como caídas de servicio, cambios en la configuración de red o superación de umbrales de rendimiento.

La capacidad de generar avisos automatizados es fundamental para la administración proactiva de la red, la resolución rápida de problemas y la supervisión continua del estado de la red.

3.4.6.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde al subtema 4.4 Mecanismos de seguridad física y lógica.

3.4.6.4 Material Y Equipo Necesario

1. Un sistema informático con un sistema operativo compatible con programadores de tareas (por ejemplo, Windows Task Scheduler en sistemas Windows o cron en sistemas Unix/Linux).

2. Acceso a dispositivos de red o servicios que generen eventos predefinidos que requieran notificación.
3. Documentación de referencia sobre la configuración y el uso del programador de tareas específico para el sistema operativo utilizado.

3.4.6.5 Metodología

1. Identificación de Eventos Predefinidos: Los estudiantes deben identificar los eventos predefinidos que requieren notificación, como caídas de servicio, cambios en la configuración de red o superación de umbrales de rendimiento.
2. Selección del Programador de Tareas: Los estudiantes deben seleccionar un programador de tareas adecuado para el sistema operativo utilizado. Pueden optar por utilizar el programador de tareas del sistema operativo o uno de terceros si es necesario.
3. Programación de Tareas: Los estudiantes deben programar tareas específicas en el programador de tareas para que generen avisos automáticos en respuesta a los eventos predefinidos.
4. Verificación y Pruebas: Los estudiantes deben verificar la configuración y realizar pruebas para asegurarse de que las notificaciones se generen correctamente en respuesta a los eventos predefinidos.
5. Documentación y Presentación: Los estudiantes deben documentar la configuración del programador de tareas y presentar sus resultados en el aula, discutiendo la funcionalidad de notificación y cómo esta automatización puede mejorar la administración de la red.

3.4.6.6 Sugerencias Didácticas

- Escenarios de Eventos: Proporciona a los estudiantes escenarios de eventos predefinidos realistas que deben abordar en la programación de tareas. Esto les ayudará a comprender cómo automatizar respuestas a situaciones específicas.

- Seguridad y Autenticación: Enseña a los estudiantes cómo configurar adecuadamente la seguridad y la autenticación en el programador de tareas para garantizar que solo personas autorizadas puedan modificar las tareas programadas.
- Control de Acceso: Anima a los estudiantes a considerar las políticas de control de acceso al programador de tareas para evitar modificaciones no autorizadas.
- Notificaciones Multicanal: Explora con los estudiantes la posibilidad de configurar notificaciones multicanal, como correos electrónicos, mensajes de texto o integraciones con sistemas de administración de incidentes, para aumentar la efectividad de las alertas.
- Documentación Clara: Destaca la importancia de documentar claramente las tareas programadas, los eventos predefinidos y las acciones de notificación para futuras referencias y auditorías.

3.4.6.7 Reporte Del Alumno

1. Título: Práctica 6: Automatización de Avisos mediante Programador de Tareas.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para identificar eventos predefinidos, seleccionar un programador de tareas, programar tareas de notificación y verificar su funcionamiento.
5. Resultados: Muestra los resultados de la configuración del programador de tareas, incluyendo ejemplos de notificaciones generadas.
6. Análisis: Discute la importancia de la automatización de avisos y cómo esta práctica contribuye a la administración de la red.

7. Conclusiones: Resume las conclusiones principales de la práctica y las lecciones aprendidas sobre la automatización de tareas de notificación.
8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados, así como sugerencias para mejorar la configuración de notificaciones.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado durante la práctica.

3.4.7 Práctica 7 El estudiante instalará un sistema operativo de red configurando su conectividad TCP/IP, así como los servicios que este provea como por ejemplo, el servicio Web, correo electrónico, conexión remota, transferencia de archivos, sistemas de archivos en red, DHCP.

3.4.7.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para instalar un sistema operativo de red en un servidor o máquina virtual y configurar su conectividad TCP/IP, así como los servicios esenciales, como servidor web, correo electrónico, conexión remota, transferencia de archivos, sistemas de archivos en red y DHCP, para proporcionar una infraestructura de red funcional.

3.4.7.2 Introducción

La instalación y configuración de un sistema operativo de red es un paso fundamental en la administración de redes. En esta práctica, los estudiantes aprenderán a instalar un sistema operativo de red en un servidor o máquina virtual y configurar la conectividad TCP/IP. Además, configurarán servicios esenciales que permiten el funcionamiento de la red, como un servidor web para hospedar sitios, servicios de correo electrónico para la comunicación, conexiones remotas para la administración y transferencia de archivos.

La configuración de servicios TCP/IP y la implementación de servicios de red son competencias esenciales para administradores de redes, ya que garantizan la disponibilidad y la funcionalidad de la infraestructura de red.

3.4.7.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde a los subtemas 2.1 DHCP y 2.2 DNS

3.4.7.4 Material Y Equipo Necesario

1. Servidor físico o máquina virtual para la instalación del sistema operativo de red.

2. ISO o medios de instalación del sistema operativo de red (por ejemplo, una imagen de un sistema operativo Linux).
3. Conectividad de red (cables, switch, enrutador) para la máquina virtual o el servidor físico.
4. Documentación de referencia sobre la configuración de servicios TCP/IP, incluyendo DHCP, DNS, servidor web, correo electrónico, conexiones remotas y transferencia de archivos.

3.4.7.5 Metodología

1. Selección del Sistema Operativo de Red: Los estudiantes deben seleccionar el sistema operativo de red que se utilizará en la práctica, como una distribución de Linux o una versión de Windows Server. Esta elección debe estar en línea con los objetivos de aprendizaje de la práctica.
2. Instalación del Sistema Operativo: Los estudiantes deben instalar el sistema operativo de red en una máquina virtual o un servidor físico. Esto incluye la configuración de las opciones de red y la creación de cuentas de usuario.
3. Configuración de la Conectividad TCP/IP: Los estudiantes deben configurar la conectividad TCP/IP, incluyendo la asignación de direcciones IP, la configuración del enrutamiento (si es necesario) y la resolución de nombres.
4. Configuración de Servicios TCP/IP: Los estudiantes deben configurar servicios esenciales como servidor web, servidor de correo electrónico, conexiones remotas (SSH, RDP), transferencia de archivos (FTP) y un servidor DHCP, según sea necesario.
5. Verificación y Pruebas: Los estudiantes deben verificar la conectividad de red y probar el funcionamiento de los servicios configurados, asegurándose de que todo esté operativo.
6. Documentación y Presentación: Los estudiantes deben documentar la instalación y configuración del sistema operativo, así como la configuración de los servicios. Además, presentarán sus resultados en el aula,

discutiendo los servicios implementados y su importancia en la administración de redes.

3.4.7.6 Sugerencias Didácticas

- Entornos Virtuales: Si es posible, fomenta el uso de máquinas virtuales para que los estudiantes practiquen sin necesidad de hardware físico, lo que les brinda flexibilidad y facilidad para cometer errores sin consecuencias graves.
- Escenarios de Uso Real: Proporciona a los estudiantes escenarios de uso real en los que deben configurar servicios, como la creación de un sitio web, la configuración de una cuenta de correo electrónico o la implementación de un servidor DHCP en una red empresarial simulada.
- Enfoque en la Seguridad: Enfatiza la importancia de configurar adecuadamente la seguridad en los servicios, como la aplicación de cortafuegos, políticas de acceso y cifrado de comunicaciones.
- Resolución de Problemas: Proporciona a los estudiantes problemas simulados que deben resolver, lo que les ayudará a desarrollar habilidades de diagnóstico y solución de problemas.
- Escalabilidad y Rendimiento: Discute con los estudiantes cómo la configuración de servicios debe ser escalable y eficiente en función de las necesidades de la red y del tráfico esperado.

3.4.7.7 Reporte Del Alumno

1. Título: Práctica 7: Instalación y Configuración de un Sistema Operativo de Red.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.

4. Procedimiento: Describe los pasos seguidos para seleccionar, instalar y configurar el sistema operativo de red, así como la configuración de los servicios TCP/IP.
5. Resultados: Muestra los resultados de la configuración, incluyendo ejemplos de servicios configurados y su funcionamiento.
6. Análisis: Discute la importancia de la configuración de servicios en la administración de redes y cómo esta práctica contribuye al funcionamiento de la infraestructura de red.
7. Conclusiones: Resume las conclusiones principales de la práctica y las lecciones aprendidas sobre la instalación y configuración de sistemas de red.
8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados, así como sugerencias para mejorar la configuración de servicios.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado durante la práctica.

3.4.5 Práctica 8 Instalación de una entidad emisora de certificados, creación de firmas digitales.

3.4.8.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para instalar y configurar una entidad emisora de certificados (CA) en una infraestructura de red, así como para crear firmas digitales, lo que les permitirá comprender el funcionamiento de la infraestructura de clave pública y su importancia en la seguridad de la comunicación y la autenticación en redes.

3.4.8.2 Introducción

La seguridad de la comunicación y la autenticación de usuarios y dispositivos son aspectos críticos en la administración de redes. Las entidades emisoras de certificados (CA) desempeñan un papel fundamental al emitir certificados digitales que garantizan la autenticidad e integridad de la información transmitida. En esta práctica, los estudiantes aprenderán cómo instalar y configurar una CA y cómo utilizarla para crear firmas digitales.

La infraestructura de clave pública (PKI) es esencial en la seguridad de la comunicación en redes, y la creación de firmas digitales es una competencia clave en la administración de redes seguras.

3.4.8.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde a los subtemas 4.1 Elementos de la seguridad y 4.3 Políticas de seguridad.

3.4.8.4 Material Y Equipo Necesario

1. Servidor dedicado o máquina virtual para alojar la entidad emisora de certificados.

2. Software de CA, como Microsoft Certificate Services o OpenSSL (dependiendo de las preferencias del instructor y del entorno).
3. Documentación de referencia sobre la instalación y configuración de una entidad emisora de certificados y la creación de firmas digitales.

3.4.8.5 Metodología

1. Selección del Software de CA: Los estudiantes deben seleccionar el software de entidad emisora de certificados (CA) que utilizarán en la práctica, como Microsoft Certificate Services o OpenSSL. La elección debe basarse en los objetivos de aprendizaje y los recursos disponibles.
2. Instalación de la CA: Los estudiantes instalarán y configurarán la CA en un servidor dedicado o una máquina virtual. Esto implica definir la jerarquía de certificados, generar claves maestras y configurar políticas de emisión.
3. Creación de Certificados Digitales: Los estudiantes crearán certificados digitales utilizando la CA. Esto incluye la emisión de certificados de usuario y servidor, así como la generación de firmas digitales.
4. Configuración de Servicios de Red: Los estudiantes aplicarán los certificados digitales a servicios de red, como servidores web, correos electrónicos seguros y conexiones VPN. Esto garantizará la autenticación y la seguridad de la comunicación.
5. Pruebas y Verificación: Los estudiantes verificarán el funcionamiento de la CA y los certificados digitales mediante pruebas de autenticación y firma digital en servicios de red.
6. Documentación y Presentación: Los estudiantes documentarán el proceso de instalación de la CA, la creación de certificados y su aplicación a servicios de red. Además, presentarán sus resultados en el aula, destacando la importancia de la PKI en la seguridad de la red.

3.4.8.6 Sugerencias Didácticas

- Casos de Uso Reales: Proporciona ejemplos de casos de uso reales en los que la PKI y las firmas digitales son esenciales, como la autenticación en una red empresarial o la seguridad de las transacciones en línea.
- Seguridad y Políticas: Enseña a los estudiantes la importancia de configurar políticas de seguridad y definir roles y responsabilidades para garantizar una emisión segura de certificados.
- Pruebas de Seguridad: Proporciona ejercicios de prueba de seguridad en los que los estudiantes intenten falsificar firmas digitales o realizar ataques de intermediario (man-in-the-middle) para comprender las amenazas a la seguridad.
- Caso de Estudio: Presenta un caso de estudio en el que los estudiantes deben diseñar una infraestructura de PKI desde cero, lo que les ayudará a aplicar los conocimientos adquiridos en la práctica.
- Resolución de Problemas: Proporciona situaciones problemáticas en las que los estudiantes deben resolver problemas relacionados con certificados digitales y firmas, lo que fortalecerá sus habilidades de resolución de problemas.

3.4.8.7 Reporte Del Alumno

1. Título: Práctica 8: Instalación de una Entidad Emisora de Certificados y Creación de Firmas Digitales.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para seleccionar, instalar y configurar el software de CA, así como la creación de certificados digitales y su aplicación a servicios de red.

5. Resultados: Muestra los resultados de la instalación de la CA, ejemplos de certificados digitales creados y su uso en servicios de red.
6. Análisis: Discute la importancia de la PKI y las firmas digitales en la seguridad de la red y cómo esta práctica contribuye a la administración segura de redes.
7. Conclusiones: Resume las conclusiones principales de la práctica y las lecciones aprendidas sobre la instalación de una entidad emisora de certificados y la creación de firmas digitales.
8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados, así como sugerencias para mejorar la seguridad de la red.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado durante la práctica.

3.4.9 Práctica 9 Instalación de firewalls, proxys, filtros de contenido.

3.4.9.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para instalar y configurar soluciones de seguridad, como firewalls, proxies y filtros de contenido, en una red, lo que les permitirá proteger la red de amenazas externas, controlar el acceso a recursos y garantizar la seguridad de los usuarios.

3.4.9.2 Introducción

La seguridad de la red es una prioridad fundamental en la administración de redes. Los firewalls, proxies y filtros de contenido son componentes esenciales para garantizar la seguridad y el control en una infraestructura de red. En esta práctica, los estudiantes aprenderán a instalar y configurar estas soluciones de seguridad para proteger la red contra amenazas externas y controlar el acceso a recursos y contenido.

La implementación adecuada de firewalls, proxies y filtros de contenido es esencial para la seguridad y el cumplimiento de políticas en la administración de redes.

3.4.9.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde a los subtemas 4.1 Elementos de la seguridad y 4.2 Tipos de riesgos y amenazas.

3.4.9.4 Material Y Equipo Necesario

1. Hardware o servidores dedicados para alojar las soluciones de seguridad (firewalls y proxies).
2. Software de firewall, como pfSense o iptables (dependiendo de las preferencias del instructor y del entorno).

3. Software de proxy, como Squid, y software de filtro de contenido, como DansGuardian o SquidGuard (según sea necesario).
4. Documentación de referencia sobre la configuración y administración de firewalls, proxies y filtros de contenido.

3.4.9.5 Metodología

1. Selección de Soluciones de Seguridad: Los estudiantes deben seleccionar las soluciones de seguridad que utilizarán en la práctica, como firewalls, proxies y filtros de contenido. La elección debe basarse en los objetivos de aprendizaje y los recursos disponibles.
2. Instalación de las Soluciones de Seguridad: Los estudiantes instalarán y configurarán las soluciones de seguridad en servidores dedicados o máquinas virtuales. Esto incluye definir reglas de firewall, configurar el proxy y establecer filtros de contenido.
3. Definición de Políticas de Seguridad: Los estudiantes deben definir políticas de seguridad que determinen qué tráfico se permitirá o bloqueará, qué sitios web se pueden acceder y cómo se filtrará el contenido.
4. Pruebas y Verificación: Los estudiantes verificarán el funcionamiento de las soluciones de seguridad mediante pruebas de acceso y tráfico de red. Deben asegurarse de que las políticas se apliquen correctamente.
5. Documentación y Presentación: Los estudiantes deben documentar el proceso de instalación, configuración y definición de políticas de seguridad. Además, presentarán sus resultados en el aula, destacando la importancia de las soluciones de seguridad en la administración de redes.

3.4.9.6 Sugerencias Didácticas

- Políticas de Seguridad: Enfatiza la importancia de definir políticas de seguridad sólidas que reflejen las necesidades y requisitos de la organización. Explora diferentes escenarios y casos de uso para definir políticas eficaces.

- Escenarios de Ataque: Proporciona a los estudiantes ejemplos de escenarios de ataque en los que deben utilizar las soluciones de seguridad para mitigar amenazas, como ataques de denegación de servicio (DDoS) o ataques de phishing.
- Auditorías de Seguridad: Anima a los estudiantes a realizar auditorías de seguridad para evaluar la efectividad de las soluciones implementadas. Esto les ayudará a identificar posibles vulnerabilidades.
- Evaluación de Rendimiento: Explora la importancia de evaluar el rendimiento de las soluciones de seguridad y cómo estas pueden afectar el rendimiento de la red. Los estudiantes deben considerar el equilibrio entre seguridad y rendimiento.
- Resolución de Problemas: Proporciona situaciones problemáticas en las que los estudiantes deben resolver problemas relacionados con la configuración de soluciones de seguridad, lo que fortalecerá sus habilidades de diagnóstico y solución de problemas.

3.4.9.7 Reporte Del Alumno

1. Título: Práctica 9: Instalación de Firewalls, Proxies y Filtros de Contenido.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para seleccionar, instalar y configurar las soluciones de seguridad, así como la definición de políticas de seguridad.
5. Resultados: Muestra los resultados de la configuración, ejemplos de políticas de seguridad definidas y su impacto en el tráfico de red.

6. Análisis: Discute la importancia de las soluciones de seguridad en la protección de la red y el control de acceso, así como cómo esta práctica contribuye a la administración segura de redes.
7. Conclusiones: Resume las conclusiones principales de la práctica y las lecciones aprendidas sobre la instalación de firewalls, proxies y filtros de contenido.
8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados, así como sugerencias para mejorar la seguridad de la red.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado durante la práctica.

3.4.10 Práctica 10 El estudiante configurará un sistema de cuotas que administre el uso de espacio en disco por parte de los usuarios que en el sistema él haya creado.

3.4.10.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para configurar y administrar un sistema de cuotas que limite y controle el uso de espacio en disco por parte de los usuarios en un sistema, lo que les permitirá garantizar la eficiencia en el uso de recursos de almacenamiento y prevenir problemas de agotamiento de espacio.

3.4.10.2 Introducción

El uso eficiente de recursos, como el espacio en disco, es esencial en la administración de sistemas y redes. Un sistema de cuotas permite controlar y limitar la cantidad de espacio en disco que los usuarios pueden utilizar, lo que evita el agotamiento de recursos y garantiza un funcionamiento óptimo del sistema. En esta práctica, los estudiantes aprenderán a configurar y administrar un sistema de cuotas para el uso de espacio en disco por parte de los usuarios.

La implementación de cuotas es fundamental para la gestión de recursos en entornos de red y sistemas.

3.4.10.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde al subtema 3.4 Análisis de Desempeño de la Red: Tráfico y Servicios.

3.4.10.4 Material Y Equipo Necesario

1. Servidor o sistema en el que se configurará el sistema de cuotas.
2. Sistema operativo compatible con la implementación de cuotas, como Linux (ext3, ext4, XFS) o Windows Server.

3. Documentación de referencia sobre la configuración de cuotas en el sistema operativo utilizado.

3.4.10.5 Metodología

1. Selección del Sistema Operativo y Sistema de Archivos: Los estudiantes deben seleccionar el sistema operativo y el sistema de archivos en el que configurarán las cuotas. Esta elección debe estar en línea con los objetivos de aprendizaje y las preferencias del instructor.
2. Configuración del Sistema de Cuotas: Los estudiantes configurarán las cuotas en el sistema seleccionado, definiendo límites de espacio en disco por usuario o grupo. Esto puede implicar el uso de herramientas específicas del sistema operativo o software adicional.
3. Creación de Usuarios y Grupos: Los estudiantes crearán usuarios y grupos en el sistema, asignando usuarios a grupos apropiados si es necesario. Esto les permitirá aplicar cuotas de manera efectiva.
4. Asignación de Cuotas: Los estudiantes asignarán cuotas a usuarios o grupos específicos, definiendo límites de espacio en disco que se aplicarán a cada entidad. Deben entender cómo se aplican las cuotas de manera efectiva.
5. Monitoreo y Pruebas: Los estudiantes supervisarán el uso de espacio en disco y realizarán pruebas para asegurarse de que las cuotas se apliquen correctamente. Deben abordar cualquier problema o infracción de cuotas.
6. Documentación y Presentación: Los estudiantes documentarán el proceso de configuración de cuotas, incluyendo la asignación de cuotas a usuarios y grupos. Además, presentarán sus resultados en el aula, resaltando la importancia de la gestión de recursos de almacenamiento.

3.4.10.6 Sugerencias Didácticas

- Escenarios de Uso Real: Proporciona escenarios de uso real en los que los estudiantes deben configurar cuotas para abordar problemas de

agotamiento de espacio en disco, como en un servidor de archivos compartidos.

- Simulación de Problemas: Crea situaciones problemáticas en las que los estudiantes deben resolver problemas relacionados con cuotas, como usuarios que superan los límites asignados.
- Monitorización Continua: Enfatiza la importancia de la monitorización continua de las cuotas y el uso de espacio en disco para garantizar el cumplimiento y prevenir problemas.
- Resolución de Problemas: Proporciona escenarios en los que los estudiantes deben solucionar problemas relacionados con cuotas, lo que fortalecerá sus habilidades de diagnóstico y solución de problemas.
- Estudio de Casos: Presenta un caso de estudio en el que los estudiantes deben diseñar un sistema de cuotas para una organización con necesidades específicas, lo que les permitirá aplicar los conocimientos adquiridos en la práctica.

3.4.10.7 Reporte Del Alumno

1. Título: Práctica 10: Configuración de un Sistema de Cuotas para el Uso de Espacio en Disco.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para seleccionar el sistema operativo, configurar las cuotas, crear usuarios y grupos, asignar cuotas y supervisar su uso.
5. Resultados: Muestra ejemplos de cuotas configuradas, cómo se aplican y ejemplos de uso de espacio en disco por usuarios o grupos.

6. Análisis: Discute la importancia de la configuración de cuotas para el control de recursos de almacenamiento y cómo esta práctica contribuye a la administración eficiente de sistemas.
7. Conclusiones: Resume las conclusiones principales de la práctica y las lecciones aprendidas sobre la gestión de cuotas.
8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados, así como sugerencias para mejorar la gestión de recursos de almacenamiento.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado durante la práctica.

3.4.11 Práctica 11 Utilizar algoritmos para cálculo de ancho de banda.

3.4.11.1 Objetivo

El objetivo general de esta práctica es que los estudiantes adquieran las habilidades necesarias para utilizar algoritmos y herramientas para calcular el ancho de banda en una red, lo que les permitirá comprender y gestionar eficazmente el rendimiento de la red y optimizar su utilización.

3.4.11.2 Introducción

El ancho de banda es un recurso crítico en la administración de redes, y su correcta gestión es esencial para garantizar un rendimiento óptimo de la red. Los algoritmos y herramientas de cálculo de ancho de banda permiten a los administradores de redes medir y evaluar la capacidad de la red y su utilización.

En esta práctica, los estudiantes aprenderán a utilizar algoritmos y herramientas para calcular el ancho de banda de una red, lo que les ayudará a tomar decisiones informadas sobre la asignación de recursos y la optimización de la red.

3.4.11.3 Correlación Con Los Temas Y Subtemas Del Programa De Estudio Vigente.

Esta actividad corresponde al subtema 3.4 Análisis de Desempeño de la Red: Tráfico y Servicios.

3.4.11.4 Material Y Equipo Necesario

1. Computadoras o servidores de prueba en la red que se utilizarán para realizar mediciones de ancho de banda.
2. Herramientas y software de medición de ancho de banda, como iperf, Wireshark, o herramientas de monitoreo de red.
3. Documentación de referencia sobre el uso de las herramientas y los algoritmos de cálculo de ancho de banda.

3.4.11.5 Metodología

1. Selección de Herramientas de Medición: Los estudiantes deben seleccionar las herramientas y algoritmos de medición de ancho de banda que utilizarán en la práctica. Esto puede incluir la elección de software de medición, como iperf o Wireshark.
2. Configuración de Escenarios de Prueba: Los estudiantes deben configurar escenarios de prueba en la red utilizando computadoras o servidores de prueba. Deben definir las condiciones y parámetros de prueba.
3. Realización de Mediciones de Ancho de Banda: Los estudiantes llevarán a cabo mediciones de ancho de banda en los escenarios de prueba utilizando las herramientas seleccionadas. Registrarán los resultados de las mediciones.
4. Análisis de Resultados: Los estudiantes analizarán los resultados de las mediciones para evaluar el ancho de banda disponible, identificar posibles cuellos de botella y comprender el rendimiento de la red.
5. Documentación y Presentación: Los estudiantes documentarán el proceso de medición, los resultados obtenidos y las conclusiones. Presentarán sus hallazgos en el aula, destacando la importancia de la medición del ancho de banda en la administración de redes.

3.4.11.6 Sugerencias Didácticas

- Escenarios de Prueba Reales: Proporciona a los estudiantes escenarios de prueba basados en situaciones reales, como medir el ancho de banda en una red empresarial o en un entorno de servidor de aplicaciones.
- Variación de Parámetros: Anima a los estudiantes a variar los parámetros de prueba, como el tamaño de los paquetes, la dirección de tráfico o la carga de la red, para comprender cómo afectan al ancho de banda.

- Comparación de Herramientas: Pide a los estudiantes que comparen diferentes herramientas de medición de ancho de banda para comprender sus ventajas y limitaciones.
- Escenarios de Escalamiento: Desafía a los estudiantes a diseñar escenarios de prueba que representen situaciones de escalamiento, como un aumento en el número de usuarios o la implementación de servicios adicionales.
- Resolución de Problemas: Proporciona situaciones problemáticas en las que los estudiantes deben resolver problemas relacionados con el rendimiento de la red basados en los resultados de las mediciones.

3.4.11.7 Reporte Del Alumno

1. Título: Práctica 11: Utilización de Algoritmos para el Cálculo de Ancho de Banda.
2. Objetivos: Enumera los objetivos de la práctica.
3. Materiales y Equipo: Enumera los materiales y el equipo utilizados en la práctica.
4. Procedimiento: Describe los pasos seguidos para seleccionar las herramientas, configurar escenarios de prueba, realizar mediciones y analizar los resultados.
5. Resultados: Muestra ejemplos de mediciones de ancho de banda realizadas, los parámetros de prueba y los resultados obtenidos.
6. Análisis: Discute los resultados de las mediciones, identifica cuellos de botella o problemas de rendimiento y destaca la importancia de la medición del ancho de banda en la administración de redes.
7. Conclusiones: Resume las conclusiones principales de la práctica y las lecciones aprendidas sobre la medición del ancho de banda.

8. Recomendaciones: Proporciona recomendaciones basadas en los hallazgos y desafíos encontrados, así como sugerencias para mejorar el rendimiento de la red.
9. Bibliografía: Incluye cualquier referencia o recurso utilizado durante la práctica.

FUENTES DE INFORMACIÓN

Impresas:

1. Tanenbaum, A. S. (2011). Redes de Computadoras (Quinta ed.). Pearson.
2. Olifer, N. (2009). Redes de Computadoras (Primera ed.). Mc.Graw-Hill.
3. Anderson, R. J. (2008). Security Engineering (Primera ed.). Wiley.
4. Bejtlich, R. (2005). El tao de la monitorización (Primera ed.). Pearson.
5. CISCO Systems. (2004). Guía del Primer año CCNA 1 y 2, Academia de Networking de Cisco Systems (Tercera ed.). Pearson/Cisco Press.
6. CISCO Systems. (2004). Guía del Segundo año CCNA 3 y 4, Academia de Networking de Cisco Systems (Tercera ed.). Pearson/Cisco Press.
7. Flickenger, R. (2003). Linux Server Hacks (Primera ed.). O'Reilly.
8. Hagen, W., & Jones, B. (2005). Linux Server Hacks Volume Two (Primera ed.). O'Reilly.
9. Maxwell, S. (2001). RedHat Linux, Herramientas para la administración de redes, (Primera ed.). Mc Graw Hill.
10. Ockhart, A. (2006). Network Security Hacks (Primera ed.). O'Reilly.
11. Peterson, E. T. (2005). Web Site Measurement Hacks (Primera ed.). O'Reilly.
12. Tanenbaum, A. S. (2003). Redes de Computadoras (Cuarta ed.). Pearson / Prentice-Hall.

Electrónicas:

13. CISCO Systems. (2014). The Internet Protocol Journal. Obtenido de http://www.cisco.com/web/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

14. COFETEL (Comisión Federal de Telecomunicaciones). (2014). Industria. Obtenido de http://www.cft.gob.mx:8080/portal/industria-2/industria-intermedia-nv/

15. Corning Incorporated. (2014). Corning Telecommunications. Obtenido de http://www.corning.com/products_services/telecommunications/index.aspx

16. Corning Incorporated. (2014). CorningIncorporated. Obtenido de http://www.youtube.com/user/CorningIncorporated

17. IEEE. (2014). IEEE Standards Association. Obtenido de http://www.youtube.com/user/IEEESA

18. IEEE. (2014). Technology Standards & Resources. Obtenido de http://standards.ieee.org/findstds/index.html

19. TED. (2014). TED Topics Internet. Obtenido de http://www.ted.cnom/topics/Internet

20. The Siemon Company. (2014). Siemon Company Videos. Obtenido de http://www.youtube.com/user/SiemonNetworkCabling

21. The Siemon Company. (2014). Siemon Network Cabling Solutions. Obtenido de http://www.siemon.com/la/