Actividad 13: TCP/IP

Problema 1: Diseño de un sistema de entrega y recuperación de correo electrónico

Objetivos:

1. Diseñar un sistema de correo electrónico robusto utilizando SMTP, IMAP y SSL/TLS.
2. Implementar servidores SMTP e IMAP en Python.
3. Configurar SSL/TLS para encriptar las conexiones.
4. Discutir el manejo de direcciones IP dinámicas y estáticas, DHCP y NAT.

Metodología:

- **Configuración del Servidor SMTP e IMAP:**
  - Implementación de servidores SMTP e IMAP usando librerías en Python.
  - Ejemplo de código para enviar y recibir correos electrónicos.
- **Manejo de SSL/TLS:**
  - Uso de SSL/TLS para garantizar la confidencialidad e integridad de los datos.
  - Ejemplo de implementación con conexiones seguras en Python.
- **Gestión de Certificados X.509:**
  - Importancia de los certificados para SSL/TLS.
  - Ejemplo de carga de certificados en Python.
- **Discusión sobre DHCP y NAT:**
  - Impacto de la asignación dinámica de direcciones IP y la traducción de direcciones en los servidores de correo.
  - Necesidad de configuraciones especiales para garantizar la accesibilidad desde el exterior.

Resultados:

- Ejemplo de correo electrónico enviado y recibido utilizando los servidores SMTP e IMAP implementados.
- Confirmación de la conexión segura mediante SSL/TLS.
- Análisis de cómo DHCP y NAT afectan la configuración y el funcionamiento de los servidores de correo.

Conclusiones:

- La implementación exitosa de servidores SMTP e IMAP demuestra la viabilidad del diseño propuesto.
- SSL/TLS proporciona una capa adicional de seguridad crucial para la transmisión de datos sensibles.
- Se requiere una cuidadosa consideración de DHCP y NAT para garantizar la accesibilidad de los servidores desde el exterior.

Problema 2: Implementación de un protocolo de red personalizado sobre TCP

Objetivos:

1. Definir el formato del mensaje para un protocolo de aplicación personalizado sobre TCP.
2. Desarrollar un esquema de control de flujo para transferencia eficiente de archivos grandes.
3. Implementar funciones de conexión, como el handshake de tres vías de TCP y manejo de retransmisiones.
4. Evaluar el impacto de NAT en la conexión de red y proponer soluciones.

Metodología:

- **Diseño del protocolo:**
  - Especificación del formato del mensaje y cabeceras.
- **Control de flujo:**
  - Implementación de un esquema basado en ventana deslizante para TCP.
- **Implementación de funciones de conexión:**
  - Desarrollo de pseudocódigo para handshake TCP y manejo de retransmisiones.
- **Evaluación de NAT:**
  - Análisis del impacto de NAT en la conexión y propuesta de soluciones.

Resultados:

- Implementación exitosa de un protocolo personalizado sobre TCP.
- Esquema de control de flujo eficiente para la transferencia de archivos grandes.
- Pseudocódigo funcional para conexión TCP y manejo de retransmisiones.
- Propuestas para mitigar el impacto de NAT en la conexión de red.

Conclusiones:

- El protocolo personalizado ofrece una solución eficiente para transferencia de archivos sobre TCP.
- El control de flujo mejora la gestión de grandes volúmenes de datos.

- La consideración de NAT es crucial para garantizar la interoperabilidad en entornos de red.

Problema 3: Creación de un sistema de autenticación segura con LDAP y SSH

Objetivos:

1. Integrar LDAP y SSH para autenticación y autorización seguras.
2. Configurar un túnel SSH para encapsular la comunicación LDAP.
3. Implementar certificados autofirmados y manejo de autenticación LDAP.
4. Analizar el papel de SSL/TLS en la protección de datos en la capa de transporte.

Metodología:

- **Configuración de LDAP y SSH:**
  - Establecimiento de servidor LDAP y túnel SSH.
- **Implementación de seguridad:**
  - Uso de SSL/TLS y certificados autofirmados.
- **Evaluación de seguridad:**
  - Análisis de posibles vulnerabilidades y pruebas de penetración.

Resultados:

- Integración exitosa de LDAP y SSH para autenticación segura.
- Configuración de túnel SSH para comunicación LDAP encapsulada.
- Implementación funcional de certificados autofirmados y autenticación LDAP.
- Análisis de seguridad y mitigación de vulnerabilidades.

Conclusiones:

- La combinación de LDAP y SSH ofrece un sistema de autenticación robusto.
- SSL/TLS proporciona una capa adicional de seguridad para la transmisión de datos.
- La evaluación continua es esencial para mantener la seguridad en el sistema.

Problema 4: Simulación de interoperabilidad de red con múltiples protocolos

Objetivos:

1. Simular la interoperabilidad entre IP, ICMP, IGMP y ARP en una red.
2. Desarrollar un plan de simulación, incluyendo configuración de tabla ARP y manejo de ICMP y IGMP.
3. Probar y validar la interoperabilidad de los protocolos en diferentes segmentos de red.

4. Utilizar utilidades de red para monitorear y resolver problemas en la red simulada.

Metodología:

- **Simulación de protocolos de red en Python:**
    - Generación y manejo de paquetes utilizando scapy.
- **Evaluación de interoperabilidad:**
    - Observación del comportamiento de los protocolos en la red simulada.
- **Uso de utilidades de red:**
    - Implementación de traceroute y ping para diagnóstico de problemas.

Resultados:

- Simulación exitosa de IP, ICMP, IGMP y ARP en una red.
- Identificación y resolución de problemas de interoperabilidad.
- Utilización efectiva de utilidades de red para diagnóstico.

Conclusiones:

- La simulación permite comprender mejor el funcionamiento y la interoperabilidad de los protocolos de red.
- Las utilidades de red son herramientas valiosas para el diagnóstico y resolución de problemas en la red.
- La evaluación continua es necesaria para mantener y mejorar la eficiencia y seguridad de la red.