

Práctico de Aula N°8: Seguridad en redes

Ejercicio 1: ¿Qué tipos de ataques a la seguridad existen? Explique cada uno.

Ejercicio 2: Explique cada uno de los aspectos de seguridad.

Ejercicio 3: Explique detalladamente los mecanismos de seguridad existentes.

Ejercicio 4: Dadas las siguientes realidades:

- | | |
|---------------------------------|--|
| i) Banco de la Nación Argentina | iv) Tres computadoras de unos Amigos conectadas en red para jugar. |
| ii) Univ. Nac. de San Luis | |
| iii) Negocio de venta de ropa | |

se pide para cada una de las realidades:

- Definir la política de seguridad.
- ¿Qué aspectos de seguridad se consideran en la realidad
- Definir los mecanismos de seguridad a considerar por cada aspecto del ejercicio anterior.

Ejercicio 5: Investigue en Internet sobre estos ataques y clasifíquelos por tipo de ataque (ataque activo o pasivo)

- DDoS
- Sesión hijacking
- Sql injection
- Phishing
- Ingeniería social
- ransomware

Ejercicio 6: Complete el siguiente cuadro:

Amenaza	Tipo de Ataque	Servicio de Seguridad Afectado
Acceso sin autorización		
Observar información sin autorización		
Copiar sin autorización		
Suplantación de usuarios legítimos		
Robo de información quitando el archivo		
Escuchas ocultas en la red		
Destrucción de equipamiento por causa de incendio		
Dificultad en el uso de los datos del recurso requerido		
Llenar el espacio del disco o la memoria		
Falsificación de datos		

Ejercicio 7: Cuáles son las ventajas y desventajas de usar un Firewall

Ejercicio 8: ¿En qué capas de los protocolos ISO/OSI y TCP/IP trabajan los distintos tipos de firewall?

Ejercicio 9: Cuáles son las ventajas y desventajas de usar un Proxy

Bibliografía

1. Redes de Computadoras - Tanenbaum - Capítulo 8
2. Comunicaciones y Redes de Computadoras - Stallings - Capítulo 18
3. Redes de Computadoras un Enfoque Descendente - Kurose - Capítulo 8