



Rivadeneyraj

www.wuolah.com/student/Rivadeneyraj



Resumen TAI.pdf

Resumen de los términos más preguntados



3º Tecnologías Avanzadas de la Información



Grado en Ingeniería Informática - Tecnologías Informáticas



Escuela Técnica Superior de Ingeniería Informática

Universidad de Sevilla

Como aún estás en la portada, es
momento de redes sociales.
Cotilleáanos y luego a estudiar.



Wuolah



Wuolah



Wuolah_apuntes

WUOLAH

- Ataques en función del objetivo (adi)
- Confidencialidad → Obtener info privilegiada → Gi Nmap, Sniffing
 - Autenticidad → Engaña a un sistema haciéndole pensar que alguien de confianza → Gi spoofing, Ing. Soc., hijacking
 - Disponibilidad → Inhabilitar el acceso al sistema víctima o a los servicios que → Gi DDOS, flooding ofrece
 - Integridad → Modificar o destruir info → Gi Exploit, Bugs y/o aplicaciones

- Métricas más utilizadas
- Retraso :
 - Jitter : Variación en el tiempo de entrega de dos paquetes consecutivos
 - Pérdida de paquetes : Consideramos que se ha perdido cuando no llega al destino
 - Ancho de banda } - Cap. Transporte → Capacidad de transferencia entre el origen y el destino. (Es un promedio)
 - Cap. Ruta → Correspondiente a la mínima capacidad de enlace existente entre dos nodos de la ruta
 - Orden de entrega
 - Disponibilidad de red y servicio
 - Experiencia de calidad.

- Spoofing
- El atacante pretende hacerse pasar por otra persona, para realizar alguna acción maliciosa.
 - Tipos
 - IP: Usurpar la IP de alguien
 - DNS: Manipula los paquetes UDP para comprometer el serv. DNS
 - ARP: Se redirige el tráfico de una máquina de la red hacia el atacante. El atacante vincula su MAC con la IP de un equipo
 - Mail/Web: Correos o web falsas (Phising)

Arquitecturas QoS

Intserv: Las aplicaciones solicitan a la red una reserva de recursos explícita. Los dispositivos de red comprobarán si los paquetes pertenecen a un flujo existente y si hay recursos de red disponibles para aceptar el paquete. Para ello se usa el protocolo RSVP

Diffserv: Permite la clasificación de paquetes en clases de tráfico, las cuales tendrán un tratamiento diferente en función de a la clase que pertenezcan. El encarcado de paquetes consiste en la alteración del campo (TOS), para que sean procesados posteriormente en función de la marca

Ambas arquitecturas pretenden garantizar limitar el nº de paquetes y establecer una prioridad.

Mientras que en intserv es la aplicación quien solicita los recursos de conexión explícita, en diffserv los recursos van en función de las clases.



Definición de términos.

- **Túnel de red:** Canal de comunicación en el que se encapsula un protocolo dentro de otro. Se usa en las VPN para establecer una comunicación privada dentro de una red, o para que usuarios remotos puedan acceder a recursos compartidos.
- **Hash:** Función que dada una cadena de bits variable, devuelve otra cadena de bits fijos. Sirve para garantizar la integridad.
- **Cifrado simétrico:** Tanto emisor como receptor utilizan la misma clave.
- **IPSec:** Es un método para implementar VPN de acceso remoto. Son un conjunto de protocolos que se encargan de la autenticación y encriptación de cada paquete IP en una sesión de comunicación.
- **Cifrado Asimétrico:** Utiliza diferentes claves para el cifrado y el descifrado.
- **Certificado digital:** Archivo firmado con la clave privada de una autoridad de certificación.
- **Autoridad de Certificación:** Con su firma acredita que alguien es quien dice ser. Sirve para evitar la suplantación.
- **Firma electrónica:** Se cifra (con la clave privada) el hash de un contenido. De este modo nos aseguramos de que el documento no sufre cambios y podemos verificar quién es el autor.
- **SLA:** Acuerdo a nivel de servicio. Contrato entre un proveedor de servicios y un cliente, para garantizar la calidad en dicho servicio.
- **Ingeniería Social:** Engañar o mentir para que otra persona haga lo que la parte atacante quiere.