

Control de Redes II

17/04/2024

Apellido y Nombre: Juri Ignacio

* 1. A que se denomina Honeypots

1. Se denomina honeypot al SW o conjunto de pc cuya intención es atraer atacantes, simulando ser sistemas No vulnerables o fuertes a los ataques
2. **Se denomina honeypot al SW o conjunto de pc cuya intención es atraer atacantes, simulando ser sistemas vulnerables o débiles a los ataques.**
3. Se denomina honeypot al SW o conjunto de pc cuya intención es rechazar atacantes.
   * 2. IPsec en modo túnel es una excelente solución para:
4. Cifrar el tráfico entre 2 equipos de usuario final
5. **Conectar 2 redes completas, cifrando el tráfico entre ellas, a pesar de la desventaja de requerir la instalación de SW en cada equipo de usuario de las respectivas redes.**
6. Conectar 2 redes completas, cifrando el tráfico entre ellas, sin necesidad de instalar SW en cada equipo de usuario de las respectivas redes.
7. Ninguna de las anteriores
   * 3. IPsec tiene como objetivo:
8. **Cifrar tráfico y autentificar los puntos de conexión, para diferentes aplicaciones sin requerir modificación de estas**
9. Implementar cifrado en capa de aplicación permitiendo confidencialidad siempre y cuando la aplicación esté preparada para ello.
10. Solucionar el tráfico a nivel de capa de red cuando se usa firma digital
    * 4. Que es un firewall con conocimiento de estado (stateful):
11. **Firewall capaz de mantener atributos de una conexión en memoria desde comienzo a fin de ella**
12. Firewall capaz de poder implementar NAT
13. Firewall capaz de mantener en memoria un detalle de la estructura de red que protege para mejorar su funcionamiento
    * 5. Desventajas de poseer un IDS:
14. **Pueden generar alertas incorrectas (falsos positivos) o no detectar actividades maliciosas reales (falsos negativos).**
15. **Configurar y mantener un IDS puede requerir un conocimiento técnico significativo.**
16. **Los IDS pueden ser costosos de adquirir, implementar y mantener.**
17. **Un IDS puede afectar el rendimiento de la red al introducir latencia o reducir el ancho de banda.**
    * 6. En los Firewalls la política restrictiva indica que lo que no está expresamente permitido está prohibido (V o F) **Verdadero**.
    * 7. Enuncia ventajas y desventajas de un Honeypots

Ventajas:

1. **Detección temprana de amenazas: Los honeypots pueden detectar actividades maliciosas en una etapa temprana, permitiendo a los administradores de seguridad tomar medidas preventivas antes de que se produzcan daños graves.**
2. **Recopilación de información: Los honeypots pueden recopilar valiosa información sobre tácticas, técnicas y procedimientos (TTP) de atacantes, incluidas las herramientas utilizadas, los vectores de ataque y las vulnerabilidades explotadas**

Desventajas:

1. **Riesgo de compromiso: Si no se configuran adecuadamente y se monitorean de cerca, los honeypots pueden convertirse en un punto débil en la red y ser comprometidos por los atacantes, lo que podría utilizarse para lanzar ataques contra otros sistemas o para obtener información sensible.**
2. **Costo y recursos: Configurar y mantener honeypots puede ser costoso en términos de tiempo, recursos y hardware. Además, se requiere un monitoreo constante para identificar y responder a actividades maliciosas.**
   * 8. Realice un diagrama de una red con un firewall más un IDS
   * 9. Es el tipo de servidor de seguridad que se conecta entre el dispositivo y la red que se conecta a Internet.
3. **Hardware Firewall**
4. Software Firewall
5. Firewall de Estado
   * 10. Un firewall examina cada que está entrando o saliendo.
6. e-mail
7. Actualización
8. **Paquete**
   * 11. ¿En qué capa del modelo OSI funciona un firewall de filtrado de paquetes?
9. Transporte
10. **Red**
11. Aplicación