

Cuestionario sobre Protocolos de Red: ARP, ICMP y L2TP

Equipo #3: Zenán Fernández, Mathew Verdezoto, Andrés Merino, Josué Palma, Aidan Carrasco

1. ¿Cuál es la función principal del proceso de "Resolución de Direcciones" en el protocolo ARP?

- a) Asignar direcciones IP dinámicas a los hosts de la red.
- b) Asociar una dirección IP lógica con una dirección MAC física.**
- c) Encapsular paquetes de capa 3 en tramas de capa 2.
- d) Establecer túneles seguros entre redes remotas.

Respuesta: b) Asociar una dirección IP lógica con una dirección MAC física.

2. En el contexto de la seguridad en redes, ¿en qué consiste la vulnerabilidad conocida como "ARP Spoofing" o "Poisoning"?

- a) Saturar el ancho de banda con solicitudes de eco ICMP.
- b) Interceptar contraseñas mediante el descifrado de túneles L2TP.
- c) Enviar mensajes ARP falsos para asociar la MAC del atacante con una IP legítima.**
- d) Eliminar las entradas de la caché ARP mediante el proceso de "Aging".

Respuesta: c) Enviar mensajes ARP falsos para asociar la MAC del atacante con una IP legítima.

3. ¿Qué tipo de mensaje de error ICMP se genera cuando un paquete no puede ser entregado a su destino final?

- a) Echo Reply.
- b) Redirect.
- c) Source Quench.
- d) Destination Unreachable.**

Respuesta: d) Destination Unreachable.

4. Observando la estructura de códigos del mensaje ICMP Tipo 3, ¿cuál es el significado específico del Código 1?

- a) Red no disponible.
- b) Host no disponible.**
- c) Protocolo no disponible.
- d) Puerto no disponible.

Respuesta: b) Host no disponible.

5. ¿Cuál es el propósito del mecanismo "ICMP Redirect"?

- a) Sincronizar los relojes de los dispositivos en la red.
- b) Informar a un host de que existe una ruta más corta o eficiente hacia un destino.**
- c) Proveer una dirección MAC de respaldo en caso de falla.
- d) Bloquear el tráfico proveniente de una fuente maliciosa.

Respuesta: b) Informar a un host de que existe una ruta más corta o eficiente hacia un destino.

6. Según la mecánica de la herramienta Traceroute, ¿qué ocurre cuando el TTL de un paquete llega a cero?

- a) El paquete es reenviado automáticamente con un TTL mayor.
- b) El emisor recibe un mensaje de error que permite identificar el salto (router).**
- c) El destino final confirma la recepción exitosa.
- d) Se establece una conexión L2TP inmediata.

Respuesta: b) El emisor recibe un mensaje de error que permite identificar el salto (router).

7. ¿Qué significan las siglas L2TP y en qué nivel opera principalmente?

- a) Layer 2 Tunneling Protocol - Protocolo de túnel de capa 2.**
- b) Level 2 Transport Protocol - Capa de Transporte.
- c) Layer 2 Traffic Protocol - Capa Física.

d) Linked 2 Transmission Protocol - Capa de Aplicación.

Respuesta: a) Layer 2 Tunneling Protocol - Protocolo de túnel de capa 2.

8. En la arquitectura de L2TP, ¿cuáles son los dos componentes fundamentales que establecen el túnel?

a) ARP y Proxy ARP.

b) ICMP Header e IP Header.

c) LAC (L2TP Access Concentrator) y LNS (L2TP Network Server).

d) Host A y Host B.

Respuesta: c) LAC (L2TP Access Concentrator) y LNS (L2TP Network Server).

9. Dentro del protocolo L2TP, ¿qué función cumplen los AVPs (Attribute Value Pairs)?

a) Detectar errores de suma de comprobación en la cabecera Ethernet.

b) Cifrar el contenido de los paquetes IP.

c) Transportar parámetros de configuración y control en el establecimiento del túnel.

d) Limitar el tiempo de vida de una entrada en la tabla ARP.

Respuesta: c) Transportar parámetros de configuración y control en el establecimiento del túnel.

10. ¿Cuál es la utilidad del proceso "PMTU Discovery" basado en ICMP?

a) Encontrar la dirección MAC de un router remoto.

b) Determinar el tamaño máximo de paquete que puede atravesar una ruta sin fragmentarse.

c) Verificar si un puerto TCP específico está abierto.

d) Asignar prioridades de Calidad de Servicio (CoS) al tráfico.

Respuesta: b) Determinar el tamaño máximo de paquete que puede atravesar una ruta sin fragmentarse.