**SEGURIDAD EN REDES:** TRABAJO DE INVESTIGACIÓN

1. Define RIESGO y SEGURIDAD
2. ¿Qué es un firewall y cuál es su función?
3. ¿Qué es un firewall por software?
4. ¿es lo mismo firewall que antivirus?
5. ¿Qué es un puerto y cuáles son los más usados en redes?
6. ¿Qué es un firewall por hardware?
7. ¿Qué es un honeypots? ¿cuál es su función?
8. ¿Qué es el DNS spoofing?
9. ¿Cómo actúa un SNIFFER en la red?
10. ¿Qué es un adware y cuál es su función en la red?
11. ¿Qué es el protocolo HTTPS y cómo funciona?
12. ¿Qué es el ETHICAL HACKING?
13. ¿Cuáles son las fases de ataques a una red informática?
14. ¿Cuáles son algunas de las medidas preventivas que se deben tomar para evitar acceso a los sistemas informáticos?

**Respuestas:**

1. El riesgo es el problema potencial que puede ocurrir en un procesador segmentado. La seguridad es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos.
2. Un firewall o cortafuegos es un elemento informático que controla el tráfico entrante y saliente de un dispositivo o una red privada con la finalidad de bloquear la entrada de datos que no cumplan con algunos criterios de seguridad.
3. Los firewalls por software son aquellos que pueden instalarse en cualquier dispositivo electrónico para darle protección adicional.
4. No son lo mismo porque un antivirus es un software que se encarga de escanear, localizar, detectar y eliminar programas maliciosos, virus y otros códigos perjudiciales para la salud de un equipo. Y un firewall es un elemento informático que controla el tráfico entrante y saliente de un dispositivo o una red privada
5. Se refiere a un punto de conexión específico en un dispositivo, como un router, que se utiliza para dirigir el tráfico de red entrante y saliente. Los puertos de red más usados son: 20, 21, 22, 23, 25, 53, 80, 110, 143, 443, 3389, 445, 3306, 5432, 6379, 27017.
6. Un firewall de hardware es un dispositivo físico similar a un servidor que filtra el tráfico dirigido a una computadora.
7. Un honeypot está ubicado en una red o sistema informático para que su objetivo sea evitar un posible ataque al sistema informático. La función principal de esta herramienta es detectar y obtener información del ataque informático, y, sobre todo, de dónde procede, para posteriormente tomar las medidas de seguridad necesarias.
8. El DNS spoofing, es el proceso de alterar entradas en un servidor de DNS para redirigir a un usuario específico a una web malintencionada que está bajo control del atacante.
9. Es un software o hardware que se utiliza para monitorizar, capturar y analizar en tiempo real los paquetes de datos que pasan por una red, sin redirigirlos ni alterarlos.
10. Un adware es un tipo de programa publicitario malicioso. El adware genera beneficios a su programador desplegando automáticamente anuncios en la interfaz de usuario del software o en la pantalla emergente que salta durante el proceso de instalación.
11. El protocolo de transferencia de hipertexto seguro (HTTPS) es la versión segura de HTTP, que es el principal protocolo utilizado para enviar datos entre un navegador web y un sitio web.
12. El ETHICAL HACKING es el proceso de identificar y resolver vulnerabilidades en sistemas informáticos de manera legal y ética.
13. Las fases son:
    1. Reconocimiento
    2. Exploración
    3. Obtener Acceso
    4. Mantener Acceso
    5. Borrar Huellas
14. Algunas medidas son:
    1. Controles de acceso a los datos más estrictos
    2. Realizar copias de seguridad
    3. Utilizar contraseñas seguras
    4. Proteger el correo electrónico
    5. Contratar un software integral de seguridad
    6. Utilizar software DLP
    7. Trabajar en la nube
    8. Involucrar a toda la empresa en la seguridad
    9. Monitorización continua y respuesta inmediata