Test:

¿Qué medidas de seguridad se deben implementar en el diseño de una red segura?  
A. Segmentación, redundancia y minimización de los puntos de acceso  
B. Únicamente cortafuegos  
C. Únicamente cortafuegos de nueva generación  
D. Usar solo encriptación para los datos

¿Qué herramientas pueden ayudar a proteger las redes contra el phishing?  
A. Sistemas de detección de correos electrónicos fraudulentos y formación de usuarios  
B. Cortafuegos sólo  
C. Únicamente el uso de cifrado en todos los correos  
D. Desactivar la recepción de correos de fuera de la red interna

¿Cuáles son las mejores prácticas para proteger los puntos de acceso Wi-Fi?  
A. Usar contraseñas fáciles de recordar  
B. Desactivar toda seguridad en redes públicas  
C. Utilizar WPA3 e implementar redes de invitados para separar los dispositivos  
D. Permitir acceso solo por cable

¿Cuáles son las características de los protocolos de seguridad inalámbrica como WPA3?  
A. No ofrecen cifrado  
B. Sólo protegen las conexiones Ethernet  
C. Son sólo utilizados en redes privadas  
D. Ofrecen encriptación mejorada para proteger las conexiones Wi-Fi contra ataques de fuerza bruta

¿Cuál es la diferencia entre un IDS y un IPS?  
A. Un IDS puede prevenir intrusiones de manera activa  
B. Un IDS no puede detectar tráfico sospechoso  
C. Un IPS solo se utiliza en redes privadas  
D. Un IPS puede prevenir intrusiones en tiempo real, bloqueando tráfico sospechoso

¿Cuál es la diferencia entre las amenazas que afectan a redes cableadas y sin hilos?  
A. Las redes inalámbricas no tienen ninguna amenaza de seguridad  
B. Las redes inalámbricas son más vulnerables al sniffing y al cracking de claves  
C. Las redes inalámbricas solo son vulnerables a ataques de denegación de servicio (DoS)  
D. Las redes cableadas no sufren amenazas como el phishing

¿Qué medidas de seguridad se deben implementar en el diseño de una red segura?  
A. Segmentación, redundancia y minimización de los puntos de acceso  
B. Únicamente cortafuegos  
C. Únicamente cortafuegos de nueva generación  
D. Usar solo encriptación para los datos

¿Cuál es la importancia de la seguridad en redes en entornos modernos?  
A. Es fundamental para proteger los datos y garantizar la confianza en las comunicaciones de redes globales  
B. Es solo una preocupación para empresas grandes  
C. Únicamente para evitar la pérdida de datos personales  
D. Sólo es importante para las redes inalámbricas

¿Cómo puede ayudar la segmentación de redes en la seguridad?  
A. Reduce la latencia de la red  
B. Aísla las diferentes partes de la red para limitar los daños en caso de ataque  
C. Mejora la velocidad de la red  
D. Permite la conexión de más dispositivos

¿Qué es un IDS (Sistema de Detección de Intrusiones)?  
A. Un dispositivo para crear copias de seguridad  
B. Un sistema que monitorea el tráfico de red para identificar actividades sospechosas y generar alertas  
C. Un sistema de protección contra virus  
D. Un sistema para optimizar el tráfico de red

¿Qué protocolos se utilizan para proteger las redes inalámbricas?  
A. WPA3 y autenticación 802.1X  
B. Wi-Fi Directo y Bluetooth  
C. TCP/IP e IPsec  
D. NAT y DNS

¿Qué significa el término ARP spoofing?  
A. Falsificación de direcciones IP para realizar ataques DDoS  
B. Ataques de fuerza bruta para obtener contraseñas  
C. Un tipo de phishing para robar información  
D. Falsificación de direcciones MAC para interceptar el tráfico de la red

¿Qué estrategia ayuda a proteger los datos en tránsito?  
A. Crear redes inalámbricas públicas  
B. Cifrado de datos durante la comunicación para evitar que sean interceptadas  
C. Uso de contraseñas fáciles  
D. Desactivar la conexión a redes externas

¿Qué es un IDS (Sistema de Detección de Intrusiones)?  
A. Un dispositivo para crear copias de seguridad  
B. Un sistema que monitorea el tráfico de red para identificar actividades sospechosas y generar alertas  
C. Un sistema de protección contra virus  
D. Un sistema para optimizar el tráfico de red

¿Cuál de las siguientes amenazas puede afectar las redes cableadas?  
A. Ataques DDoS solo  
B. Ataques de phishing exclusivamente  
C. Sniffing y ARP spoofing  
D. Únicamente ataques de fuerza bruta a contraseñas

¿Cuál es la diferencia entre un IDS y un IPS?  
A. Un IDS puede prevenir intrusiones de manera activa  
B. Un IDS no puede detectar tráfico sospechoso  
C. Un IPS solo se utiliza en redes privadas  
D. Un IPS puede prevenir intrusiones en tiempo real, bloqueando tráfico sospechoso

¿Cuáles son las características de los protocolos de seguridad inalámbrica como WPA3?  
A. No ofrecen cifrado  
B. Sólo protegen las conexiones Ethernet  
C. Son sólo utilizados en redes privadas  
D. Ofrecen encriptación mejorada para proteger las conexiones Wi-Fi contra ataques de fuerza bruta

¿Qué herramientas pueden ayudar a proteger las redes contra el phishing?  
A. Sistemas de detección de correos electrónicos fraudulentos y formación de usuarios  
B. Cortafuegos solo  
C. Únicamente el uso de cifrado en todos los correos  
D. Desactivar la recepción de correos de fuera de la red interna

¿Cuáles son las mejores prácticas para proteger los puntos de acceso Wi-Fi?  
A. Usar contraseñas fáciles de recordar  
B. Desactivar toda seguridad en redes públicas  
C. Utilizar WPA3 e implementar redes de invitados para separar los dispositivos  
D. Permitir acceso solo por cable

¿Cuál es la importancia de la seguridad en redes en entornos modernos?  
A. Es fundamental para proteger los datos y garantizar la confianza en las comunicaciones de redes globales  
B. Es solo una preocupación para empresas grandes  
C. Únicamente para evitar la pérdida de datos personales  
D. Sólo es importante para las redes inalámbricas

Test Respuestas correctas:

****¿Qué medidas de seguridad se deben implementar en el diseño de una red segura?****  
****Respuesta: A. Segmentación, redundancia y minimización de los puntos de acceso****

****¿Qué herramientas pueden ayudar a proteger las redes contra el phishing?****  
****Respuesta: A. Sistemas de detección de correos electrónicos fraudulentos y formación de usuarios****

****¿Cuáles son las mejores prácticas para proteger los puntos de acceso Wi-Fi?****  
****Respuesta: C. Utilizar WPA3 e implementar redes de invitados para separar los dispositivos****

****¿Cuáles son las características de los protocolos de seguridad inalámbrica como WPA3?****  
****Respuesta: D. Ofrecen encriptación mejorada para proteger las conexiones Wi-Fi contra ataques de fuerza bruta****

****¿Cuál es la diferencia entre un IDS y un IPS?****  
****Respuesta: D. Un IPS puede prevenir intrusiones en tiempo real, bloqueando tráfico sospechoso****

****¿Cuál es la diferencia entre las amenazas que afectan a redes cableadas y sin hilos?****  
****Respuesta: B. Las redes inalámbricas son más vulnerables al sniffing y al cracking de claves****

****¿Qué medidas de seguridad se deben implementar en el diseño de una red segura?****  
****Respuesta: A. Segmentación, redundancia y minimización de los puntos de acceso****

****¿Cuál es la importancia de la seguridad en redes en entornos modernos?****  
****Respuesta: A. Es fundamental para proteger los datos y garantizar la confianza en las comunicaciones de redes globales****

****¿Cómo puede ayudar la segmentación de redes en la seguridad?****  
****Respuesta: B. Aísla las diferentes partes de la red para limitar los daños en caso de ataque****

****¿Qué es un IDS (Sistema de Detección de Intrusiones)?****  
****Respuesta: B. Un sistema que monitorea el tráfico de red para identificar actividades sospechosas y generar alertas****

****¿Qué protocolos se utilizan para proteger las redes inalámbricas?****  
****Respuesta: A. WPA3 y autenticación 802.1X****

****¿Qué significa el término ARP spoofing?****  
****Respuesta: D. Falsificación de direcciones MAC para interceptar el tráfico de la red****

****¿Qué estrategia ayuda a proteger los datos en tránsito?****  
****Respuesta: B. Cifrado de datos durante la comunicación para evitar que sean interceptadas****

****¿Qué es un IDS (Sistema de Detección de Intrusiones)?****  
****Respuesta: B. Un sistema que monitorea el tráfico de red para identificar actividades sospechosas y generar alertas****

****¿Cuál de las siguientes amenazas puede afectar las redes cableadas?****  
****Respuesta: C. Sniffing y ARP spoofing****

****¿Cuál es la diferencia entre un IDS y un IPS?****  
****Respuesta: D. Un IPS puede prevenir intrusiones en tiempo real, bloqueando tráfico sospechoso****

****¿Cuáles son las características de los protocolos de seguridad inalámbrica como WPA3?****  
****Respuesta: D. Ofrecen encriptación mejorada para proteger las conexiones Wi-Fi contra ataques de fuerza bruta****

****¿Qué herramientas pueden ayudar a proteger las redes contra el phishing?****  
****Respuesta: A. Sistemas de detección de correos electrónicos fraudulentos y formación de usuarios****

****¿Cuáles son las mejores prácticas para proteger los puntos de acceso Wi-Fi?****  
****Respuesta: C. Utilizar WPA3 e implementar redes de invitados para separar los dispositivos****

****¿Cuál es la importancia de la seguridad en redes en entornos modernos?****  
****Respuesta: A. Es fundamental para proteger los datos y garantizar la confianza en las comunicaciones de redes globales****