PRUEBA TEORICA UNIFICADA - Profesional de Tecnología en Seguridad Informática

Duración total sugerida: 90 minutos

Puntaje total: 100 puntos

Nivel exigido para aprobación: 80 puntos

Modalidad: Escrita, sin acceso a internet ni ayuda externa

Sección 1: Fundamentos de Seguridad (30 puntos)

1. Explica los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Respuesta sugerida: Confidencialidad: evita accesos no autorizados. Integridad: evita alteraciones no autorizadas. Disponibilidad: asegura acceso cuando se necesita.

2. Diferencia entre ataque activo y pasivo, con ejemplo.

Respuesta sugerida: Activo: modifica sistemas (ej: DoS). Pasivo: escucha sin alterar (ej: sniffing).

3. ¿Qué es el principio de mínimo privilegio y cómo se aplica?

Respuesta sugerida: Otorgar solo los permisos estrictamente necesarios a usuarios/sistemas.

4. ¿Qué es un SIEM y para qué se usa? Menciona dos ejemplos.

Respuesta sugerida: Herramienta que centraliza y analiza logs. Ej: Splunk, QRadar.

5. ¿Qué es Zero Trust y por qué es útil?

Respuesta sugerida: Modelo que no confía en nadie por defecto. Se basa en validación continua y segmentación.

Sección 2: Redes de Datos (30 puntos)

6. Diferencia entre switch y router, y capa OSI de cada uno.

Respuesta sugerida: Switch: capa 2, conecta dispositivos en red local. Router: capa 3, conecta diferentes redes.

7. ¿Qué es una VLAN y para qué sirve?

Respuesta sugerida: Red lógica que segmenta tráfico dentro de una red física para mejorar seguridad.

8. Menciona 3 protocolos de seguridad de red y su función.

Respuesta sugerida: IPSec (cifrado IP), 802.1X (control de acceso), SSH (conexión segura).

9. ¿Qué es DNS y cómo se puede atacar?

Respuesta sugerida: Sistema que traduce nombres de dominio. Vulnerable a spoofing, tunneling.

10. ¿Qué es una VPN y diferencias entre IPSec y SSL?

Respuesta sugerida: VPN: túnel cifrado. IPSec: red. SSL: aplicación. SSL es más flexible.

Sección 3: Arquitectura, Riesgo y Cumplimiento (20 puntos)

11. Explica controles técnicos, administrativos y físicos con ejemplos.

Respuesta sugerida: Técnico: firewall. Administrativo: políticas. Físico: cerraduras biométricas.

12. ¿Qué es un análisis de riesgos y qué se evalúa?

Respuesta sugerida: Amenazas, vulnerabilidades, impacto, controles existentes.

13. Cita 2 normas de seguridad internacionales y su objetivo.

Respuesta sugerida: ISO 27001 (SGSI), NIST CSF (gestión de ciberseguridad).

Sección 4: Criterio y Resolución de Problemas (20 + 30 puntos)

14. Detectas múltiples intentos fallidos desde una IP externa. ¿Qué haces?

Respuesta sugerida: Bloquear IP, revisar logs, notificar, habilitar MFA si no hay.

15. Un usuario abre un archivo sospechoso. ¿Procedimiento?

Respuesta sugerida: Aislar el equipo, alertar a seguridad, analizar, cambiar contraseñas, remediar.

16. Un directivo exige acceso remoto al core sin autorización. ¿Qué haces?

Respuesta sugerida: Propuesta controlada, escalamiento, justificación documentada.

17. Hay fuga de datos. ¿Cómo actúas?

Respuesta sugerida: Aislar, activar plan IR, recolectar evidencia, notificar a legal y mitigar.

18. Detectas servidor sin parches. ¿Qué haces?

Respuesta sugerida: Reportar, evaluar criticidad, agendar parcheo o aplicar controles temporales.

19. Un usuario accede archivos indebidos. ¿Qué haces?

Respuesta sugerida: Verificar logs, suspender acceso, entrevistar, escalar si procede.

20. Un proveedor necesita acceso a red interna. ¿Qué medidas tomas?

Respuesta sugerida: Acceso segmentado, temporal, con MFA y monitoreo activo.