CONVOCATORIA DE PRUEBAS SELECTIVAS PARA CUBRIR UNA PLAZA DE PERSONAL LABORAL EN LA COMISIÓN NACIONAL DEL MERCADO DE VALORES. SUBDIRECTOR DE CIBERSEGURIDAD INTERNA PARA EL DEPARTAMENTO DE SISTEMAS DE INFORMACIÓN. 06/21.
FASE DE OPOSICIÓN. SEGUNDA PARTE

Coloque aquí la etiqueta con el código de barras

CUESTIONARIO TIPO TEST

1) **¿Cuál de los siguientes elementos constituye la base de cualquier arquitectura de Seguridad de la Información?**

   a) La estrategia de seguridad de la información
   b) La política de seguridad de la información
   c) Los procedimientos de seguridad de la información
   d) Los controles de seguridad de la información

2) **¿Cómo se solventaría la situación de conflicto de independencia en un área de ciberseguridad que acomete funciones de tercera línea como auditorías de sistemas con ejercicios de Red Team?**

   a) Cancelando los ejercicios de Red Team y limitando los ejercicios a pruebas de intrusión más controladas
   b) Trasladando estos ejercicios a Auditoría Interna o bien asegurando que los equipos de Red Team reportan directamente al CISO
   c) Trasladando los ejercicios al área técnica de Sistemas/Tecnología, con Ciberseguridad como área de control
   d) Asegurando que los equipos de Red Team reportan directamente al CEO y al Comité Ejecutivo

3) ¿Quién está obligado a realizar un registro de actividades del tratamiento?

a) Únicamente el responsable de las actividades de tratamiento efectuadas bajo su responsabilidad
b) Únicamente el responsable y en su caso, su representante, de las actividades de tratamiento efectuadas bajo su responsabilidad
c) El responsable, el encargado y en su caso, sus respectivos representantes de las actividades de tratamiento efectuadas bajo su responsabilidad
d) Solamente los encargados del tratamiento de las actividades de tratamiento efectuadas bajo su responsabilidad

4) ¿En qué línea de defensa debe situarse la gestión de riesgos?

a) Primera línea de defensa
b) Segunda línea de defensa
c) Tercera línea de defensa
d) Entre la segunda y tercera línea

5) ¿Cuál de las siguientes integraciones de la herramienta Grupos Relacionados por el Diagnóstico (GRC) con otras herramientas de seguridad es más prioritaria a fin de consolidar el proceso automático de riesgo?

a) La integración con la herramienta de gestión de identidades
b) La integración con el inventario de activos tecnológico de la entidad
c) La integración con los resultados de los escaneos de vulnerabilidades
d) La integración con los incidentes de seguridad detectados

6) ¿Qué tipo de ataque cibernético involucra a un atacante explotando una vulnerabilidad en un proveedor de servicios en la nube para acceder a los recursos de otros clientes alojados en la misma plataforma?

a) Ataque de denegación de servicio distribuido (DDoS)
b) Ataque de suplantación de identidad
c) Ataque de escalada de privilegios
d) Ataque de hipervisor

7) **¿Qué es el protocolo OAuth y cómo se utiliza en el contexto de la seguridad de aplicaciones?**

a) Un protocolo para cifrar comunicaciones entre dispositivos IoT
b) Una metodología para autenticar usuarios en servidores LDAP
c) Un marco de autorización que permite que las aplicaciones accedan a recursos en nombre de los usuarios
d) Un protocolo de seguridad exclusivo para sistemas operativos móviles

8) **¿Qué control permite aumentar la seguridad en el Secure Software Development Life Cycle (SSLDC) en la fase de diseño?**

a) Análisis estático de código
b) Monitorización de las aplicaciones
c) Modelado de amenazas
d) Análisis de dependencias

9) **Teniendo en cuenta que uno de los métodos más utilizados para explotar una vulnerabilidad con un virus es el buffer overflow, ¿cuál de las siguientes soluciones del sistema operativo protegen al equipo del uso de una dirección de memoria de forma malintencionada?**

a) EDR
b) ASLR
c) DEP
d) B y C son correctas

10) **¿Qué es el "hooking" en el contexto de la detección de código malicioso y cómo podría ser detectado?**

a) El "hooking" es una técnica de ofuscación de código malicioso. Puede ser detectado mediante el análisis de firmas
b) El "hooking" es un tipo de ataque que aprovecha vulnerabilidades en el sistema operativo. Puede ser detectado mediante firewalls
c) El "hooking" es la modificación del flujo de ejecución de una aplicación. Puede ser detectado mediante la monitorización de llamadas al sistema
d) El "hooking" es una técnica de ingeniería social. Puede ser detectado mediante análisis heurístico

11) ¿Cuál de las siguientes respuestas se aproxima más a la siguiente definición?
Su objetivo principal es proporcionar acceso no autorizado y persistente al sistema, lo que permite a los atacantes mantener un control encubierto sobre la máquina infectada.

a) Ransomware
b) Troyano
c) Rootkit
d) Gusano

12) ¿Cuál de las siguientes configuraciones, que por seguridad debe estar deshabilitada, se corresponde con la utilizada por desarrolladores de aplicaciones móviles Android para poder conectarlos vía USB con entornos de desarrollo?

a) USB App Locking
b) USB Tethering
c) Debug USB
d) USB Screen Mirroring

13) ¿Cuál de las siguientes opciones es más segura si queremos proporcionar acceso a la red corporativa a un dispositivo móvil en una ubicación remota?

a) Configurar un APN privado
b) Configurar un APN público
c) Configurar una VPN a través de alguna red WiFi disponible
d) Configurar una VPN a través de la red móvil

14) ¿En qué se diferencian los hipervisores de tipo 1 y de tipo 2?

a) En ambos casos, el hardware es común para los diferentes sistemas operativos Guest OS
b) El hipervisor de tipo 1 se ejecuta directamente en el hardware de la máquina
c) El hipervisor de tipo 2 se ejecuta directamente en el hardware de la máquina
d) En ambos casos, el hipervisor funciona en el sistema operativo de la máquina donde está instalado (host OS)

15) ¿Qué método de cifrado permite realizar operaciones sobre datos cifrados sin la necesidad de descifrarlos?

a) Cifrado Simétrico
b) Cifrado Homomórfico
c) Cifrado Asimétrico
d) Cifrado de Sustitución

16) ¿Cuál de los siguientes protocolos se utiliza para cifrar las comunicaciones web HTTPS?

a) SSL/TLS
b) SSH
c) FTPS
d) HTTP

17) ¿Qué protocolo es usado para el almacenamiento seguro y recuperación de contraseñas en un sistema operativo?

a) PGP (Pretty Good Privacy)
b) OAuth (Open Authorization)
c) TPM (Trusted Platform Module)
d) SSH (Secure Shell)

18) ¿Cuál de los siguientes enfoques proporciona mayor seguridad a la hora de acceder a la red interna de una organización?

a) Implementar una autenticación de doble factor para los usuarios con acceso remoto
b) Hacer uso de una VPN cifrando las comunicaciones de extremo a extremo y autenticar a los usuarios a través de un servidor RADIUS
c) Establecer una red VPN cifrando las comunicaciones de extremo a extremo y realizar la autenticación a través de certificados digitales
d) Segmentar a los usuarios en grupos de IP dinámicos y limitar el acceso mediante un firewall de aplicaciones

19) De las siguientes técnicas, ¿Cuál es la utilizada en una DMZ para permitir el acceso remoto seguro a servicios expuestos en la misma aislándolos de la red interna?

a) Autenticación RADIUS
b) Firewall
c) ACL
d) Proxy inverso

20) En el ámbito de la seguridad en virtualización de aplicaciones y contenedores, ¿Cuál de las siguientes afirmaciones es una ventaja de la tecnología de "sandboxing"?

a) Restringe el acceso a recursos y actividades específicas, limitando así el alcance de los posibles daños
b) Permite que las aplicaciones pueden compartir datos confidenciales de forma segura
c) Aísla por completo los recursos y procesos, disminuyendo la posibilidad de ataques que inunden la red
d) Se encarga de resolver/mitigar las vulnerabilidades en tiempo de ejecución

21) ¿Por qué es recomendable en términos de seguridad deshabilitar la funcionalidad de AutoRun de los sistemas Windows?

a) Puede iniciar de forma automática el proceso de copias de seguridad de datos al conectar un dispositivo de memoria externo
b) Puede consumir una gran cantidad de recursos de memoria durante el inicio del sistema operativo ralentizándolo
c) Bloquea de forma automática la aplicación de actualizaciones de Windows
d) AutoRun podría permitir la ejecución automática de malware desde unidades extraíbles como un USB

22) ¿En un entorno Windows que event id es el que registra la autenticación exitosa de un usuario?

a) 4624
b) 4625
c) 4626
d) 4627

23) ¿Cuál de los siguientes logon type de Windows corresponde con una sesión de escritorio remoto o "RemoteInteractive session"?

a) 2
b) 5
c) 7
d) 10

24) ¿Cuál de las siguientes cadenas de ejecuciones de procesos evidencia más claramente un posible phishing?

a) outlook.exe ->Winword.exe -> cmd.exe -> Powershell.exe
b) Winword.exe -> cmd.exe -> net.exe
c) cmd.exe -> explorer.exe
d) Cmd.exe -> nc.exe

25) ¿Un ataque tipo ARP Poison en que capa del modelo OSI la podemos ver?

a) capa 7 - Aplicación
b) capa 5 - Sesión
c) capa 2 - Enlace de datos
d) Capa 8 – Usuario

26) ¿Cuál de las siguientes soluciones de seguridad tiene como principal función monitorizar una base de datos?

a) WAF
b) DAM
c) DLP
d) DMI

27) ¿Qué elemento se debe tener en cuenta para llevar a cabo un descubrimiento de directorios basado en fuerza bruta?

a) Los métodos HTTP que soporte el servidor
b) El código fuente de la página
c) El nivel de profundidad del árbol HTML de la página
d) Los códigos de respuesta HTTP

28) ¿Cómo se llama el protocolo estándar utilizado por NVD para expresar la información de las vulnerabilidades?

a) CSV
b) XML
c) SCAP
d) OSVML

29) ¿Cuál es el propósito del atributo HTTPOnly en las cookies?

a) Obliga a que las cookies solo sean enviadas a través de HTTP y no HTTPS
b) Hace que las cookies solo sean válidas para la sesión HTTP actual
c) Prohíbe que las cookies sean almacenadas en el lado del cliente
d) Previene que las cookies sean accedidas a través de scripts del lado del cliente, como JavaScript

30) ¿Qué tipo de malware realiza keystrokes?

a) Adware
b) Ransomware
c) Miner
d) Infostealer

Preguntas de reserva

1) ¿Cuál es la primera prioridad para responder a un incidente de seguridad importante tras su declaración oficial?

a) Investigación
b) Contención
c) Recuperación
d) Documentación

2) ¿Qué valor muestra el sitio web del que proviene un usuario?

a) User-agent
b) Referer
c) IP-dst
d) IP-src

PREGUNTAS CORTAS

1. Identifica las 5 dimensiones del ENS y da un ejemplo de medidas para cada tres de ellas.

2. ¿Cómo puedes evidenciar la ejecución de archivos entre los artefactos de Windows? (Log de eventos, prefetch, registros del sistema, Amcache)

3. ¿Qué medidas de contención tomarías al detectar que un usuario comprometido ha accedido desde la VPN a varios servidores de la red interna?

4. ¿Qué fases identificaría para el diseño de un proceso de desarrollo seguro? Describe brevemente cada una de ellas.

5. En una empresa que todavía no tiene implantado un sistema de gestión del riesgo, describe los pasos que se tendrían que dar para desplegar eficazmente un sistema de gestión del riesgo.

6. Desarrolla brevemente las ventajas e inconvenientes de desplegar un modelo operativo basado, de manera pura, en el modelo de las tres líneas de defensa (operaciones – riesgo – auditoría)

7. Indica los derechos que se les reconoce a los interesados (persona física identificada o identificable) según el Reglamento General de Protección de Datos (RGPD)

8. Explica en detalle cómo Threat Intelligence puede ayudar a una organización a fortalecer sus medidas de seguridad y prevenir posibles ataques. Proporciona ejemplos específicos.

9. Describe brevemente la metodología de análisis web.

10. Describe la diferencia entre “Remote File Inclusion” y “File Upload”.