**Curso: IFCT0109 Seguridad informática**
**Expte.: 29/2020/LJ/0019**
**Evaluación:**
**Acción y grupo:**
**Módulo: MF0488_3 Gestión de incidentes de seguridad informática**

| | |
|---|---|
| Fecha examen: | 20/02/2023 |
| Nombre y apellidos: | |
| NIF: | |
| Docente: | Juan Antonio Ferrández Rodríguez |

| **Tipo de Evaluación** (Señale con una X la que corresponda) | | | |
|---|---|---|---|
| Evaluación 1 | X | Recuperación I | |

**1) El actor de una amenaza quebrantó satisfactoriamente el firewall de la red sin ser detectado por el sistema IDS. ¿Qué condición describe la falta de alerta?**

a) Falso positivo
b) Falso negativo ←
c) Positivo verdadero
d) Negativo verdadero

**2) ¿Cuál de las siguientes herramientas es un sistema de detección de intrusiones basado en host integrado en Security Onion?**

a) OSSEC ←
b) Snort
c) ELK
d) Sguil

**3) ¿Qué uso se le da al valor de hash de archivos en las investigaciones de seguridad de la red?**

a) Ayuda a identificar las firmas de malware. ←
b) Se utiliza como una clave para el cifrado.
c) Se usa para decodificar archivos.
d) Comprueba la confidencialidad de los archivos.

**4) Según el NIST, ¿qué paso en el proceso de análisis forense digital consiste en llegar a conclusiones a partir de los datos?**

a) Elaboración de informes ←
b) Análisis
c) Recopilación
d) Examen

**5) ¿Qué dos fuentes compartidas de información se incluyen en el marco MITRE ATT&CK? (Escoja dos opciones).**

a) Tácticas, técnicas, y procedimientos de atacante ←
b) Recopilación de evidencias de la más volátil a la menos volátil
c) Mapear los pasos de un ataque a una matriz de tácticas generalizadas ←
d) Evidencia de testigos oculares de alguien que observó directamente un comportamiento delictivo
e) Detalles sobre el manejo de la evidencia, incluidos momentos, lugares y personal involucrado.

**6) ¿Por qué los actores de amenazas preferirían usar un ataque de día cero en la fase de armamentización de la cadena de eliminación cibernética?**

a) Para lanzar un ataque DoS hacia el objetivo
b) Para lograr un lanzamiento más rápido del ataque contra el objetivo
c) Para evitar ser detectado por el objetivo ←
d) Para obtener un paquete de malware gratis

**7) ¿Cuál es el objetivo del actor de una amenaza al establecer un canal de comunicación bidireccional entre el sistema objetivo y una infraestructura de CnC?**

a) Robar ancho de banda de la red donde se encuentra el objetivo
b) Lanzar un ataque de desbordamiento del búfer
c) Permitir que al actor de la amenaza emita comandos al software que se instala en el objetivo ←
d) Enviar datos del usuario almacenados en el objetivo del actor de la amenaza

**8) Un analista especializado en ciberseguridad debe acudir a la escena de un crimen que involucra varios elementos de tecnología, incluso una computadora. ¿Qué técnica se utilizará para que la información encontrada en la computadora pueda utilizarse ante el juez?**

a) Recopilación de archivos de registro
b) Imagen de disco sin modificaciones ←
c) Tor
d) Rootkit

**9) El actor de una amenaza recopila información de los servidores web de una organización y busca información de contacto de los empleados. La información recopilada se utiliza para buscar información personal en Internet. ¿A qué fase de ataque pertenecen estas actividades según el modelo de cadena de eliminación cibernética?**

a) Aprovechamiento
b) Acción en objetivos
c) Armamentización
d) Reconocimiento ←

**10) ¿A qué miembro del personal de un SOC se le asigna la tarea de verificar si una alerta activada por un software de monitoreo representa un incidente de seguridad real?**

a) Personal, nivel 1 ←
b) Personal, nivel 3
c) Personal, nivel 2
d) Gerente de SOC

**11) ¿Cuál clasificación indica que una alerta es verificada como un incidente de seguridad real?**

a) Negativo verdadero
b) Falso negativo
c) Falso positivo
d) Positivo verdadero ←

**12) ¿Qué término se utiliza para describir el proceso de conversión de entradas de registros en un formato común?**

a) Estandarización
b) Normalización ←
c) Clasificación
d) Sistematización

**13) ¿Qué herramienta de Windows puede utilizar un administrador de ciberseguridad para asegurar computadoras independientes que no forman parte de un dominio de Active Directory?**

a) PowerShell
b) Política de seguridad local ←
c) Firewall de Windows
d) Windows Defender

**14) Consulte la ilustración. Un analista especializado en seguridad está revisando los registros de un servidor web Apache. ¿Qué medida debería adoptar el analista en función de la salida que se muestra?**

```
HTTP request sent, awaiting response...
  HTTP/1.1 503 Service Unavailable
  Content-Type: text/html; charset=UTF-8
  Content-Length: 904
  Connection: close
  P3P: CP="CAO PSA OUR"
  Expires: Thu, 01 Jan 1970 00:00:00 GMT
  Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-heck=0
  Pragma: no-cache
2021-08-15 16:08:14 ERROR 503: Service Unavailable.
```

a) Ignorar el mensaje.
b) Reiniciar el servidor.
c) Notificar a la administración de seguridad correspondiente del país.
d) Notificar al administrador del servidor. ←

**15) Un profesional de seguridad le hace recomendaciones a una empresa para mejorar la seguridad de los terminales. ¿Qué tecnología de seguridad de terminal se recomendaría como un sistema basado en agentes para brindar protección a hosts contra malware?**

a) IPS
b) HIDS ←
c) Determinación de líneas de base
d) Listas negras

**16) Una el concepto de seguridad con la descripción.**

| | |
|---|---|
| Amenaza | La posibilidad de consecuencias no deseadas |
| Vulnerabilidad | Riesgo |
| Ataque | Un mecanismo utilizado para comprometer a un recurso |
| Riesgo | Ataque |
| | Un punto débil en un sistema |
| | Vulnerabilidad |
| | Un peligro potencial para un recurso |
| | Amenaza |

**17) ¿Qué componente de seguridad de la información se ve comprometido en un ataque DDoS?**

a) Disponibilidad ←
b) Contabilidad
c) Confidencialidad
d) Integridad

**18) ¿Cuál es una característica de IPS?**

a) Se implementa en modo sin conexión.
b) Se centra principalmente en la identificación de posibles incidentes.
c) No afecta la latencia.
d) Puede detener los paquetes maliciosos. ←

**19) Un analista especializado en seguridad usa Tcpdump y Wireshark para obtener un archivo descargado de un archivo pcap. El analista sospecha que el archivo es un virus y quiere saber de qué tipo de archivo se trata para analizarlo en más detalle. ¿Qué comando de Linux puede utilizarse para determinar el tipo de archivo?**

a) file ←
b) tail
c) nano
d) ls -l

**20) ¿Cuál de las siguientes opciones ejemplifica un ataque local?**

a) El actor de una amenaza realiza un ataque de fuerza bruta en un router perimetral empresarial para obtener acceso ilegal.
b) El escaneo de puertos se usa para determinar si el servicio Telnet se está ejecutando en un servidor remoto.
c) El actor de una amenaza intenta obtener la contraseña de usuario de un host remoto mediante el uso de un software de captura de teclado instalado por un troyano. ←
d) Un ataque de desbordamiento del búfer se lanza contra un sitio web de compras en línea y hace que el servidor deje de funcionar.

**21) ¿Qué ataque se integra en los niveles más bajos del sistema operativo de un host e intenta ocultar totalmente las actividades del actor de la amenaza en el sistema local?**

a) Cifrado y tunelizado
b) Inserción de tráfico
c) Rootkit ←
d) Sustitución de tráfico

**22) ¿Qué tipo de técnica de evasión divide las payloads maliciosas en paquetes más pequeños para evitar los sensores de seguridad que no vuelven a ensamblar las cargas antes de escanearlas?**

a) Interpretación errónea a nivel de protocolos
b) Pivoting
c) Inserción de tráfico
d) Fragmentación de tráfico ←

**23) ¿Cuál de las siguientes opciones ejemplifica un ataque de escalamiento de privilegios?**

a) El actor de una amenaza envía un correo electrónico a un administrador de TI para solicitar acceso raíz.
b) Un ataque de escaneo de puertos descubre que el servicio FTP se está ejecutando en un servidor que permite el acceso anónimo.
c) Se lanza ataque DDoS contra un servidor del gobierno y hace que el servidor deje de funcionar.
d) El actor de una amenaza realiza un ataque de acceso y obtiene la contraseña de administrador. ←

**24) ¿Qué herramienta captura paquetes de datos completos con una interfaz de línea de comandos solamente?**

a) Wireshark
b) NBAR2
c) Tcpdump ←
d) nfdump

**25) Un analista de seguridad está revisando la información contenida en una captura de Wireshark creada durante un intento de intrusión. El analista quiere correlacionar la información de Wireshark con los archivos de registro de dos servidores que pueden haber sido comprometidos. ¿Qué tipo de información se puede usar para correlacionar los eventos encontrados en estos múltiples conjuntos de datos?**

a) Cuenta de usuario que ha iniciado sesión
b) Cinco-tuplas IP ←
c) Datos de geolocalización ISP
d) Metadatos de propiedad