Test Tema 125 #2

Actualizado el 13/04/2025

1. En el protocolo IPSEC, una asociación de seguridad (SA) queda unívocamente identificada por medio de:

a) Una dirección IP.

b) Un índice de parámetro de seguridad (SPI).

c) Un índice de parámetro de seguridad (SPI) y un puerto de comunicación TCP.

d) Una dirección IP y un Índice de Parámetro de Seguridad (SPI).

2. ¿Cuál de los siguientes conceptos NO aporta seguridad a una intranet?

a) Spoofing

b) Firewalls

c) NAT

d) Proxy

3. El programa dañino "WannaCry" es un ejemplo de "malware" del tipo:

a) Spoofing.

b) Rootkit.

c) Ransomware.

d) Spyware.

4. El ataque a SSL/TLS que permite extraer información sobre los tokens de login, email, etc en 30 segundos se llama:

a) Beast Attack

b) Crime

c) Breach

d) No existe dicho ataque

5. ¿Qué tipo de ataque es un "ataque smurf"?

a) Denegación de servicio.

b) Hombre en el medio.

c) Fuerza Bruta.

d) Ingeniería social.

6. En el ámbito de la seguridad de redes, cuál de las siguientes afirmaciones es falsa:

a) Los ataques de "buffer overflow" son posibles debido a fallos de programación

b) Los ataques mediante "spoofing" se basan en la generación de paquetes de información falsa

c) NIS, NFS, DNS o SMTP son protocolos de aplicación inseguros

d) Los ataques mediante "secuestro de sesión" no pueden prevenirse en la labor de administración

7. En una conexión IPsec en modo túnel entre dos cortafuegos usando Internet, debemos escoger cuál es la mejor implementación teniendo en cuenta que nuestro proveedor de Internet bloquea el protocolo IP 51 y que tenemos como requisitos que la información que viaje por el túnel esté cifrada. Indique cuál de las siguientes opciones es correcta para la configuración de dicho túnel.

a) ESP

b) TLS

c) AH

d) SSTP

8. Un ataque Port Stealing es

a) Un tipo de ataque DoS (Denial of Service)

b) Un tipo de ataque DDoS (Distributed Denial of Service).

c) Un tipo de ataque MitM (Man in the Middle)

d) Un tipo de ataque XSS (Cross Site Scripting)

9. ¿Para qué utilizamos un honeypot?

a) Para hacer una suplantación de identidad y obtener credenciales de acceso a un sistema.

b) Como señuelo ante posibles atacantes, pudiendo detectar y/o desviar los ataques recibidos.

c) Para ocultar información confidencial dentro de sus metadatos y poder enviarla sin riesgo.

d) -

10. Indique cuál es el número de protocolo ESP (Encapsulating Security Payload):

a) 51

b) 50

c) 49

d) Ninguno de los anteriores

11. Las fases básicas del protocolo TLS son:

a) Negociado de algoritmos, intercambio de claves con autenticación y cifrado simétrico de los mensajes.

b) Intercambio de certificados cliente y servidor, validación de certificados y cifrado de mensajes con clave privada.

c) Autenticación de cliente y servidor, establecimiento del túnel y cifrado de los mensajes con protocolo ESP (Encapsulating Security Payload).

d) Autenticación, generación del token y trasmisión, consumo del token.

12. Del protocolo IKE de IPSec podemos decir…

a) que su componente OAKLEY usa el método de Diffie-Helman modificado para la generación e intercambio de claves

b) que tiene 3 componentes: ISAKMP, SA y OAKLEY

c) que sólo se usa en modo túnel, ya que el modo transporte no cifra la cabecera IP original

d) nada de lo anterior es cierto

13. El ataque consistente en provocar una sobrecarga de los recursos de un sistema informático utilizando múltiples equipos contra un único sistema se denomina:

a) Ransomware

b) Desbordamiento de buffer (Buffer Overflow)

c) Denegación de servicio distribuido (DDoS)

d) Sniffing

14. En el ámbito de la seguridad, existe una gran cantidad de tipos de ataques a las redes. Entre ellos está el Spoofing, que consiste en:

a) La captura y lectura del tráfico y datos que son transmitidos en la red.

b) La suplantación de la identidad mediante medios técnicos.

c) La suplantación de la identidad mediante ingeniería social.

d) La captura del tráfico entre dos sistemas con posibilidad de modificar e inyectar su propio tráfico.

15. ¿Cuál de los siguientes puertos es el puerto estándar de POP3 sobre SSL?

a) 995
b) 993
c) 220
d) 465

16. El estándar WPA3 ofrece dos variantes:

a) WPA3-Personal y WPA3-Enterprise
b) WPA3-Home y WPA3-Business
c) WPA3-Standard y WPA3-Pro
d) WPA3-In y WPA3-Out

17. ¿Qué protocolo se puede utilizar para encapsular el tráfico que atraviesa el túnel de VPN?

a) IPX
b) MPLS
c) PPTP
d) ATM

18. Para establecer una conexión segura de manera remota entre un usuario y un servidor corporativo, se utilizan tecnologías VPN. ¿Cuál de las siguientes NO es una tecnología existente válida para ello?

a) IPsec VPN.
b) Open VPN.
c) SSL/TLS.
d) GNU-VPNv2.

19. En el contexto de seguridad en redes, que se entiende por cortafuegos:

a) Un sistema que separa, en cuanto a seguridad se refiere, una máquina o subred del resto.

b) Es un programa que se instala en un anfitrión de la red interna para proteger los accesos a la misma.

c) Es un sistema que se instala en la red externa para controlar los accesos a la red interna.

d) Es software o dispositivo que realiza una acción en representación de otro, garantizado as! su seguridad.

20. Cuál de las siguientes afirmaciones es FALSA:

a) IPSEC es utilizada para el establecimiento de túneles seguros a través de Internet
b) IPSEC se comporta igual con Ipv4 que con Ipv6
c) Con IPSEC se garantiza la integridad y la autenticidad, siendo la confidencialidad opcional

d) Cada conexión con IPSEC requiere de dos SA para que sea bidireccional

21. ¿Cómo se denomina la debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información?

a) Ingeniería social
b) Phising
c) Vulnerabilidad
d) Amenaza

22. La cabecera de autenticación (AH) de IPSec:

a) Proporciona integridad, no repudio en origen y protección contra replay.

b) Proporciona confidencialidad, autenticidad de origen e integridad.

c) Crea la asociación de seguridad.

d) Ninguna de las anteriores.

23. ¿Se puede filtrar el tráfico, mediante un firewall de nivel 3, entre dos máquinas situadas en la misma LAN?

a) Si

b) No

c) Depende de la configuración del FW

d) Depende de la configuración de la LAN

24. WPS (Wifi Protected Setup) define los mecanismos a través de los que los diferentes dispositivos de la red obtienen las credenciales (SSID y PSK), necesarias para iniciar el proceso de autenticación. ¿Cuál de las siguientes configuraciones WPS para el intercambio de credenciales es FALSA?

a) RADIUS

b) PBC

c) NFC

d) USB

25. ¿Cuál de las siguientes es una definición acertada del concepto “vigilancia digital”?

a) La vigilancia digital consiste en encontrar, analizar y rastrear cualquier información perjudicial para evitar que la amenaza se convierta en un problema real y de ese modo minimizar el impacto sobre la reputación corporativa.

b) La vigilancia digital consiste en obtener secretos sin el permiso del poseedor de la información (personal, sensible, propietaria o de naturaleza clasificada), de individuos, competidores, rivales, grupos, gobiernos y enemigos para ventaja personal, económica, política o militar a través del hackeo de redes privadas

c) La vigilancia digital consiste en la búsqueda continua de productos, servicios, marcas y conceptos que estén creando tendencia en redes sociales de mercados extranjeros, con el fin de su análisis y posible réplica en el mercado local

d) La vigilancia digital consiste en el conjunto de sistemas de vigilancia de una instalación que emiten sus datos a través de una conexión de internet/intranet a una plataforma de ciberseguridad centralizada

26. ¿Cuál de las siguientes funciones de seguridad no ofrece SSL?

a) No repudio.

b) Confidencialidad.

c) Integridad.

d) Ofrece todas las anteriores.

27. Un servidor "proxy":

a) Sirve para traducir direcciones IP

b) Actúa de intermediario, para acceder a determinados servicios de forma indirecta

c) Permite acceder a cualquier servicio de internet, actuando de intermediario

d) Sirve para realizar pagos on-line

28. Existen distintos formatos de firma que van incrementando la calidad de la misma hasta conseguir una firma que pueda ser verificada a largo plazo (de forma indefinida) con plenas garantías jurídicas, ¿cuáles son?

a) B-B;B-T;B-LT;B-LTA

b) B-B;B-T;B-C;B-LTA

c) B-B;B-T;B-X;B-LTA

d) B-B;B-T;B-C;B-XL

29. De los siguientes, cuál es un protocolo diseñado para suministrar un marco de trabajo que ofrezca servicios AAA (Authentication, Authorization, Accounting) para aplicaciones que involucran acceso a redes o aplicaciones IP móvil:

a) DIAMETER.
b) ENUM.
c) RTCP.
d) H.323.

30. Los cortafuegos de filtrado de paquetes:

a) Analizan el tráfico de la red fundamentalmente en la capa 3
b) Generalmente se usan formando 2 listas de reglas: una con acciones permitidas y otra con acciones denegadas
c) Son útiles contra ataques de denegación de servicio, y destacan por su rapidez transparencia y flexibilidad
d) Todas las respuestas anteriores son correctas

31. ¿Qué son los IDS?

a) Sistemas que permiten a los hackers rastrear puertos
b) Sistemas que permiten detectar actividad inadecuada, incorrecta o anómala en un sistema
c) Sistemas que simulan uno o más sistemas fáciles de atacar con el fin de tentar a los intrusos
d) Ninguno de los anteriores

32. ¿Qué afirmación respecto al protocolo SSL NO es cierta?

a) Responde por Secure Socket Layer.
b) Es un estándar de facto propuesto por Netscape, ampliamente disponible en servidores y navegadores web.
c) En su funcionamiento se establece primeramente una clave de sesión para conseguir el cifrado del canal. (confidencialidad).
d) Es un protocolo cliente-servidor que requiere la autenticación de ambas partes.

33. Cuando un atacante accede a una videoconferencia haciéndose pasar por un usuario legítimo, estaríamos hablando de un ataque de tipo:

a) Man in the midle
b) Bombing
c) Sunburst
d) Spear-phising

34. Los sistemas de recuperación de fallos hardware se basan siempre en:

a) La redundancia del equipo o empleo de equipos fault-tolerant
b) El establecimiento de una política de respaldo rigurosa
c) Una política de mantenimiento de equipos adecuada
d) Evitar manipulaciones indebidas en la instalación informática

35. La arquitectura de cortafuegos que combina un router con un host bastión y donde el principal nivel de seguridad proviene del filtrado de paquetes se denomina:

a) Screened Subnet.
b) Dual-Homed Host.
c) Router-Homed Host.
d) Screened Host.

36. En el ámbito de IPsec, ¿qué proporciona a la vez confidencialidad de los datos y la autenticación de paquetes IP?

a) AH

b) RSA

c) IKE

d) ESP

37. Indique cuál de las siguientes expresiones no es correcta para Kerberos:

a) Se basa en criptografía de clave asimétrica y requiere un tercero de confianza

b) Es un protocolo de autenticación por red que permite que dos entidades de la misma se demuestren su identidad de manera segura

c) Se basa en el intercambio de tickets de servicio

d) Puede implementarse tanto en entornos Linux como en entornos Windows

38. En relación a las técnicas de control de acceso:

a) DAC permite a los propietarios de los datos elegir los sujetos que tienen acceso a los mismos

b) MAC usa un sistema de etiquetado

c) El control de acceso no discrecional usa un método basado en roles para determinar los permisos

d) Todas las respuestas anteriores son correctas

39. ¿Qué es un honeypot?

a) Un tipo de malware que explota vulnerabilidades 0day.

b) Un ramsomware bancario.

c) Un sistema hardware o herramientas software que simulan ser equipos vulnerables para poder exponerlos sin ningún riesgo y permitir el análisis de todos los ataques efectuados sobre ellos.

d) Un ataque sofisticado de phishing.

40. ¿Qué afirmación describe una característica de IPsec?

a) IPsec puede proteger el tráfico en las capas 1 a 3.

b) IPsec funciona independiente del protocolo de capa 2.

c) El cifrado puede causar problemas con el enrutamiento.

d) Se trata de una suite propietaria.

41. Refiriéndonos a medidas de protección ante malware avanzado, si necesitamos en nuestra organización una herramienta que se pueda aplicar a los puestos cliente y que nos permita realizar un análisis forense, nos permita detectar ataques en tiempo real y responder de manera rápida y efectiva a esos ataques, qué tipo de herramienta deberá implementar:

a) EPP.

b) EDR.

c) Antivirus tradicional.

d) Sandbox.

42. Los routers para filtrado de paquetes ("packet filtering"):

a) Son cortafuegos (firewalls) que operan en el nivel de aplicación en su modalidad "stateful inspection".

b) Son firewalls que operan en el nivel de aplicación en su modalidad "stateless inspection".

c) No son firewalls, sino dispositivos de encaminamiento ("routing") que se pueden conectar a un cortafuegos como complemento de éste.

d) Son firewalls que operan en el nivel de red.

43. En una organización que dispone de múltiples elementos de seguridad que generan eventos propios como pueden ser firewalls, IPS, proxy, antivirus o servidores, que herramienta podemos implementar que nos recopile toda la información de forma centralizada para poder realizar un análisis profundo y poder correlar alertas provenientes de distintos sistemas:

a) SIEM.

b) WAF.

c) Antispam.

d) Escáner de vulnerabilidades.

44. El ataque conocido como "ARP Spoofing":

a) Se impide con el uso de conmutadores (switches) en vez de concentradores (hubs).

b) Se efectúa en el nivel 3 de OSI ya que falsifica direcciones IPs.

c) Sirve para interceptar tráfico en una red de área local (LAN), pero no para modificarlo.

d) Puede impedirse mediante DHCP snooping.

45. Dentro del ámbito de Kerberos, ¿cuál de las siguientes afirmaciones es INCORRECTA?

a) Es un protocolo de autenticación de usuarios dentro de una red.

b) Está basado en el Protocolo de Needham-Schroeder.

c) Mantiene una base de datos de claves secretas de todos los usuarios.

d) El envío de las contraseñas desde el Centro de Distribución de Claves (KDC) y el Servidor de Autenticación (AS) se hace de manera no encriptada.

46. Una organización necesita desplegar una red privada sobre líneas de datos alquiladas a un operador de telecomunicaciones que no permite implementar redes VPN de capa dos sobre su infraestructura. De las siguientes tecnologías, ¿cuál deberá utilizar para implementar dicha VPN?

a) PPTP

b) L2TP

c) TDEA

d) IPSec

47. Los cortafuegos de filtrado de paquetes:

a) Funcionan a nivel de red

b) Funcionan a nivel de aplicación

c) Funcionan a nivel de enlace

d) Funcionan a nivel de sesión

48. En la implantación de una Extranet, en lo relativo a la seguridad de la misma, ¿cuál de los siguientes aspectos NO es fundamental?

a) Definir las tecnologías de conexión que serán permitidas a los usuarios

b) Definir un sistema de asignación de credenciales

c) Definir que equipos formarán parte de la zona desmilitarizada

d) Definir filtros de aplicaciones, direcciones IP y direcciones MAC

49. ¿Cómo se denominan los sistemas que tienen como función principal detectar indicios de ataque o compromiso hacia elementos de la infraestructura, de los sistemas o redes?

a) Concentradores VPN

b) IDS

c) IPS

d) Cortafuegos

50. Indique cuál de las siguientes afirmaciones relacionadas con IPsec es FALSA:

a) IPv6 incluye explícitamente la posibilidad de utilizarlo.

b) Puede operar en modo túnel o en modo transporte.

c) El protocolo AH proporciona confidencialidad.

d) El protocolo ESP proporciona autenticación.

51. ¿cuál es una característica de los ataques DoS?

a) Siempre preceden a ataques de acceso

b) Intentan comprometer la disponibilidad de un equipo, red, o aplicación

c) Un ejemplo de ellos es el escaneo de puertos

d) Un ejemplo de ellos es el "barrido de ping"

52. La gestión de claves en IPsec se realiza a través del protocolo:

a) IKE

b) AH

c) ESP

d) A través de los protocolos AH y ESP.

53. El sistema Kerberos de autenticación y de distribución de claves de sesión requiere:

a) La existencia de una tercera entidad de confianza centralizada.

b) Que cada usuario tenga un par de claves reconocidas: la pública y la privada.

c) La existencia de una red de conexión interna total mente segura.

d) Que cada servidor de aplicaciones mantenga claves secretas compartidas con todos los usuarios que le puedan solicitar servicios.

54. Entre las mejores prácticas de seguridad propuestas por el CCNCERT para dispositivos móviles (CCN_CERT_BP/03 Dispositivos móviles) NO se encuentra:

a) Deshabilitar la gestión remota del dispositivo móvil.

b) Limitar y minimizar lo máximo posible la funcionalidad disponible en la pantalla de bloqueo si no se introduce el código de acceso.

c) Deshabilitar todos los servicios y funcionalidades del dispositivo móvil que no vayan a ser utilizados de forma permanente por parte del usuario.

d) Usar las capacidades nativas de cifrado del dispositivo móvil con el objetivo de proteger todos los datos e información asociadas al usuario, u organización, almacenados en el mismo.

55. En un cortafuegos en modo SPI (Stateful Packet Inspection), señale la opción verdadera:

a) Trabaja exclusivamente en el nivel 3 de OSI.

b) Permitirá el paso de un paquete solo si se dirige al puerto 80 de nuestro servidor.

c) Tiene en cuenta la negociación en 3 pasos (3 way handshake) del protocolo TCP/IP.

d) No permite la conexión SSH ya que está cifrada.

56. Por IP-SPOOFING entendemos:

a) Captura de passwords.

b) Uso fraudulento de direcciones de enlace.

c) Suplantación de direcciones de red.

d) Propagación de virus.

57. ¿A qué tipo de ataque nos referimos cuando se suplanta la identidad de una dirección IP origen?

a) DoS

b) Phishing

c) Sniffing

d) Spoofing

58. En el contexto de la seguridad lógica, si hablamos de una bomba lógica ¿cuál de las siguientes afirmaciones es verdadera?

a) El código se replica al activarse.

b) Su efecto es retardado.

c) No se activan por eventos.

d) Es otra manera de referirse a los troyanos.