Test Tema 125 #1

Actualizado el 13/04/2025

1. En el ámbito de las amenazas a la seguridad, la interrupción afecta a la disponibilidad. De forma similar:

a) La interceptación afecta a la integridad

b) La modificación afecta a la confidencialidad

c) La fabricación afecta a la integridad

d) La fabricación afecta a la confidencialidad

2. ¿Cuál de los siguientes tipos de ataque vulnera la integridad de la información?

a) Interrupción.

b) Modificación.

c) Fabricación.

d) Intercepción.

3. ¿Qué es PAT?

a) Port Address Translation

b) Protocol Access Translation

c) Port Acknowledge Timeout

d) PDU access token

4. La siguiente instrucción “iptables -L”:

a) Habilita el firewall de un equipo basado en iptables.

b) Habilita el interface loopback a través del firewall iptables.

c) Habilita el paso de paquetes de retorno a través del firewall iptables.

d) Muestra la lista de reglas del firewall basado en iptables.

5. La seguridad en red en las organizaciones se basa en la implementación de múltiples barreras de seguridad. Los cortafuegos son una de las principales barreras utilizadas, ¿cuál de las siguientes características NO le aplica a los cortafuegos?

a) Filtrado de paquete.

b) NAT - Network Address Traslation.

c) VPN - Virtual Private Network.

d) NAC - Network Access Control.

6. ¿Cuál es el método de autenticación mejor?

a) Algo que alguien sabe

b) Algo que alguien es

c) Algo que alguien tiene

d) Lo que una persona sabe y es

7. Seleccione cuál de las siguientes es una característica básica de un Firewall o Cortafuegos de seguridad perimetral:

a) Ofrecer funcionalidades de servidor de DNS (Domain Name System)

b) La inspección de estado de paquetes (stateful inspection), en la que el firewall inspecciona cada paquete individual y su colocación dentro de una serie de paquetes.

c) Una latencia de transporte menor que 100 ms.

d) El soporte de conexiones inalámbricas.

8. ¿Cómo se utiliza un protocolo reto/respuesta con una implementación con un dispositivo de tokens?

a) Este protocolo no se usa, se usa la criptografía

b) El servicio de autenticación genera un reto y el dispositivo inteligente genera una respuesta basado en el reto

c) El dispositivo pide el usuario y la contraseña

d) El dispositivo compara la contraseña del usuario contra una base de datos de credenciales

9. Procedimiento para generar de forma dinámica dominios donde se alojarán los servidores de Comando y Control, técnica usada en redes Botnet para dificultar su detención:

a) AXFR.

b) DGA.

c) Ataque POODLE.

d) CSFR.

10. El protocolo de comunicaciones seguras en que el cliente genera aleatoriamente una clave simétrica, y la cifra con la clave pública del servidor receptor de la información, enviándosela cifrada a éste, y posteriormente el servidor la descifra, con lo cual ambas partes ya poseen la clave simétrica y se pueden comunicar con confidencialidad, es:

a) IPSec (IP Security).

b) SSL/TLS (Secure sockets Layer/Transport Layer Security).

c) RSA (Rivest-Shamir-Adleman).

d) WEP (Wired Equivalent Privacy).

11. ¿Cuál de las siguientes opciones es la más adecuada?

a) Las listas de control de acceso (ACL) se deben colocar cerca del destino si son extendidas y cerca del origen si son estándar.

b) Tanto las listas de control de acceso (ACL) estándar como extendidas se deben colocar cerca del origen.

c) Tanto las listas de control de acceso (ACL) estándar como extendidas se deben colocar cerca del destino.

d) Las listas de control de acceso (ACL) se deben colocar cerca del destino si son estándar.

12. Una organización que desea proporcionar un servicio Telnet a un conjunto restringido de usuarios autenticados previamente, necesita disponer de un cortafuegos basado en:

a) Filtros de paquetes tradicionales.

b) Combinación de filtros de paquetes tradicionales con filtros con memoria de estado.

c) Filtros con memoria de estado.

d) Combinación de filtros de paquetes con pasarelas de aplicación.

13. ¿Qué norma comunitaria creó la Red de Equipos de Respuesta a Incidentes de Seguridad Informática o Red de CSIRT, por sus siglas en inglés de "Computer Security Incident Response Teams"?

a) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

b) Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

c) Directiva (UE) 2018/1972 del Parlamento y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas

d) Directiva 2013/40/UE del Parlamento Europea y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información

14. La monitorización del estado y comportamiento de la red se convierte en una necesidad que tiene por objeto la detección de posibles ataques y vulnerabilidades. Indique cuál de los sistemas que a continuación se citan NO es un ejemplo de solución tecnológica que permite detectar o controlar las intrusiones en sistemas y redes:

a) HIDS (Host-based intrusion detection system)

b) IPS (Intrusion Prevention System)

c) RTDS (Root of Trust Detection System)

d) SIEM (Security Information and Event Management)

15. ¿A qué tipo de ataque pertenece el denominado ping de la muerte?

a) Spoofing.

b) Man in the middle.

c) Denial of Service.

d) Flooding.

16. En el establecimiento de una comunicación mediante SSL, ¿cuál es el protocolo que especifica la forma de encapsular los datos que se van a intercambiar?:

a) Cipher Secure Layer.

b) SSL Handshake.

c) SSL Record.

d) Secure Socker Layer.

17. En el enfoque clásico de la seguridad en las redes de comunicación se hablaba de las cuatro dimensiones de la seguridad. ¿Cuál de las siguientes NO es una de ellas?

a) Autenticidad.

b) Confidencialidad.

c) Integridad.

d) Decisión.

18. Revisar los logs de seguridad es un tipo de seguridad:

a) Preventiva

b) De detección

c) Disuasoria

d) Correctiva

19. Starvation es:

a) un ataque al servidor DHCP consistente en inundar con peticiones DHCP REQUEST, con direcciones MAC falseadas con el objetivo de agotar su espacio de direcciones asignables.

b) un ataque al servidor DNS donde el atacante logra alterar los servidores DNS para que las consultas de resolución de nombres se resuelvan incorrectamente y redirijan a los usuarios a sitios maliciosos.

c) un ataque que consiste en suplantar al servidor de DHCP de una red y modificar los parámetros de red que reciben los equipos conectados al renovar o solicitar una nueva IP.

d) un ataque al servidor DHCP consistente en inundar con peticiones DHCPOFFER, con direcciones MAC falseadas con el objetivo de agotar su espacio de direcciones asignables.

20. Pedro es administrador corporativo de seguridad. Para él, la Intranet y la DMZ son:

a) El conjunto de aplicaciones que son de uso interno del personal del Organismo.

b) El conjunto de servicios y personal que no son directamente accedidos desde el exterior.

c) Dominios de seguridad, entendidos como el conjunto de máquinas cuya configuración es responsabilidad de un departamento interno.

d) El conjunto de ordenadores que no tienen acceso directo al exterior.

21. Señale la norma que NO está asociada correctamente a su contenido:

a) ISO 15408 - Common criteria

b) RFC 2527 - DPC (Declaración de Prácticas de Certificación)

c) CWA 14890 - Protocolo de autenticación mutua, usado para el certificado de componente del DNI

d) RFC 5246 - IPSEC

22. ¿Cuál de las siguientes es una tecnología relacionada con el establecimiento de Redes Privadas Virtuales (VPN)?

a) H.323.

b) MPLS.

c) LTE.

d) FTTH.

23. Existen diversas técnicas para garantizar la seguridad en una red TCP/IP. ¿Cuál es la diferencia fundamental entre utilizar la técnica IPSEC u otras tales como SSL, TSL o SSH?

a) SSL es una técnica más segura al utilizar certificados de 256 bits.

b) SSL, TSL y SSH precisan de una conexión IPSEC subyacente.

c) IPSEC funciona en el nivel de red de la pila TCP/IP mientras que las otras lo hacen en el nivel de aplicación.

d) IPSEC no funciona a través de routers y las demás sí.

24. En el ámbito de la seguridad, ¿a qué atienden las siglas AAA?

a) Authentication, Authorization and Accounting

b) Acknowledge, Authorization and Accounting

c) Authentication, Authorization and Access

d) Authentication, Approval and Accounting

25. ¿Cuál de los siguientes es un protocolo de autenticación PPP (Point to Point)?

a) RADIUS - Remote Authentication Dial In User Service

b) Kerberos

c) CHAP Challenge Handshake Authentication Protocol

d) Todos los anteriores

26. Los productos asociados a la familia Cortafuegos puede ofrecer protección a diferentes niveles dentro de las capas definidas por el modelo de interconexión de sistemas abiertos que se corresponde con la norma ISO/IEC:

a) ISO/IEC 9126-1.

b) ISO/IEC 15504.

c) ISO/IEC 25101.

d) ISO/IEC 7498-1.

27. ¿Qué método de acceso es utilizado para establecer conexiones remotas de línea de comandos, manteniendo el ID de usuario, la contraseña y los contenidos de la sesión de manera privada?

a) Telnet

b) Consola

c) Puerto auxiliar

d) SSH

28. En relación a IPSec señale la opción INCORRECTA:

a) Se definió originariamente en las RFCs 1825 y 1829.

b) Tanto AH (Authentication Header) como ESP (Encapsulating Security Payload) proporcionan integridad y autenticación en la comunicación.

c) En modo transporte con AH no es posible traducir direcciones mediante NAT transversal.

d) ESP debe implementar obligatoriamente el algoritmo AES-CBC con claves de 128 bits.

29. ¿Cómo se denomina a la aplicación, fragmento de software o archivo de secuencia de comandos (script) diseñado para aprovechar una determinada brecha de seguridad o vulnerabilidad de un sistema informático?

a) Adware

b) Exploit

c) Ramsomware

d) Backdoors

30. De acuerdo con el Reglamento eIDAS, ASiC, ¿qué especifica?:

a) Circuito integrado de aplicación específica.

b) El uso de estructuras contenedoras para unir uno o más objetos firmados con firmas electrónicas avanzadas o tokens de sellos de tiempo en un único contenedor digital.

c) El intercambio seguro de claves.

d) Ninguna de las anteriores.

31. El 12 de mayo de 2017 se registró un ataque a escala mundial con un programa dañino tipo ransomware llamado WannaCry. El ataque aprovechaba la vulnerabilidad de un protocolo de red que permite compartir archivos e impresoras, a través del puerto 445, en ordenadores con sistema operativo Microsoft Windows que no tuvieran la actualización de seguridad correspondiente. ¿Cuál es este protocolo de red para compartir archivos?

a) SAFP

b) SMB

c) SNMP

d) ARP

32. En IPSec, el modo de funcionamiento en el que sólo los datos son cifrados o autenticados, y el enrutamiento permanece intacto por lo que asegura la comunicación extremo a extremo, se denomina:

a) Modo túnel.

b) Modo transporte.

c) Modo encapsulado.

d) Modo transparente.

33. Existen varios procedimientos de ataques en internet, como el "hijacking". ¿En qué consiste éste?

a) Suplantación de la dirección IP origen.

b) Repudiación de la auditoría del mensaje.

c) Secuestro de una conexión TCP/IP por ejemplo durante una sesión Telnet permitiendo a un atacante inyectar comandos o realizar un DoS durante dicha sesión.

d) Escucha de una comunicación y grabación de su contenido.

34. ¿Qué es un Servidor de Comando y Control (C&C)?

a) Es un dispositivo que da órdenes a dispositivos infectados con malware.

b) Componente del plano de control de kubernetes que está pendiente de los Pods que no tienen ningún nodo asignado y selecciona uno donde ejecutarlo.

c) Es el software de gestión de dispositivos móviles que permite asegurar, monitorizar y administrar dispositivos móviles independientemente del operador de telefonía o proveedor de servicio.

d) Dispositivo de la Fog Computing capaz de enviar comandos a los dispositivos IoT bajo su cobertura.

35. En una VPN (Virtual Private Network) de acceso remoto:

a) Al tratarse de una red privada, no es necesario ningún tipo de encapsulamiento de los paquetes de datos para protegerlos de posibles ataques.

b) No es necesario verificar la identidad de los usuarios.

c) No permite cifrado de datos.

d) Los paquetes de datos viajan por un túnel definido en la red pública.

36. Señale la afirmación CORRECTA respecto a los sistemas IDS (Intrusion Detection System) e IPS (Intrusion Prevention System):

a) Un IDS es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.

b) Un IPS cuenta con una actuación reactiva, ya que no trata de mitigar una intrusión.

c) Un IDS es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva

d) Un IDS no es vulnerable a los ataques DDoS.

37. En el protocolo SSL, el paso "Server Key Exchange" o Intercambio de clave del servidor es:

a) Obligatorio

b) Opcional, únicamente cuando no existe certificado

c) Nunca es necesario

d) Ninguna de las anteriores

38. Diferencia entre un virus y un “Caballo de Troya”:

a) El virus suele utilizar canales encubiertos.

b) El virus presenta un mecanismo de replicación.

c) El “Caballo de Troya” advierte de su presencia.

d) El “Caballo de Troya” no esconde funciones potencialmente maliciosas.

39. Los cortafuegos de filtrado de paquetes ¿en qué capa TCP/IP actúan?

a) Capa IP

b) Capa de Aplicación

c) Capa de Sesión

d) Capa de Transporte

40. ¿Qué respuesta es INCORRECTA respecto a SAML?:

a) Es un estándar abierto basado en XML desarrollado por OASIS.

b) Al ser un producto propietario, no tiene versiones open source.

c) Define una infraestructura para intercambio de credenciales entre distintos dominios de seguridad.

d) Se integra con XML Encryption y XML Signature.

41. ¿Cuál de las siguientes características es INCORRECTA sobre el protocolo RADIUS (Remote Authentication Dial In User Service)?

a) Es un protocolo cliente/servidor que utiliza el protocolo de transporte fiable TCP y el puerto 1813

b) Utiliza el protocolo de nivel de enlace PPP (Point to Point Protocol) para el envío de las credenciales de usuario

c) El sucesor de RADIUS es el protocolo DIAMETER

d) Es utilizado a menudo para facilitar itinerancia (roaming) entre proveedores de servicio de internet (ISP)

42. Los IDS, (Sistemas de Detección de Intrusos), pueden clasificarse:

a) Solamente en función de los sistemas que monitorizan.

b) En función de los sistemas que monitorizan y en función de cómo operan los Sistemas de Detección de Intrusos.

c) Solamente en función de cómo operan los Sistemas de Detección de Intrusos.

d) Estos sistemas es imposible clasificarlos.

43. Indique dentro de qué tipo puede categorizarse un ataque "Port Stealing":

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

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

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

d) Un tipo de ataque DDoS (Distributed Denial of Service)

44. ¿Cuál es el método que se recomienda para proteger los datos en una WLAN?

a) Utilizar el cifrado.

b) Utilizar el SSID de no difusión.

c) Establecer la energía transmitida al ajuste más sólido.

d) Utilizar el canal 7 en lugar de cualquier otro canal en los espectros de 2,4 GHz.

45. Un ataque Zero-day:

a) aprovecha una vulnerabilidad de un software antes de que se publiquen y apliquen los parches que la corrigen

b) intercepta mensajes entre dos victimas poniéndose el atacante en medio de la comunicación

c) es el uso de la línea telefónica convencional y de la ingeniería social para engañar personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad

d) es un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar

46. La diferencia entre un IDS y un IPS es:

a) Los IDS se pueden instalar en un servidor y los IPS solo pueden ser un equipo hardware.

b) Los IPS detectan un ataque, generan una alerta, actúan e intentan neutralizar el ataque.

c) Los IDS detectan un ataque, generan una alerta, actúan e intentan neutralizar el ataque.

d) -

47. Se entiende como spoofing:

a) Envío de correos no deseados

b) Suplantación de identidad

c) Envío de ventanas de publicidad a la pantalla del usuario

d) Inyección de código malicioso

48. ¿Cuál de las siguientes es una herramienta IDS?

a) Nessus

b) Snort

c) Nagios

d) NetSaint

49. La red aislada que se encuentra dentro de la red interna de la organización donde se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo se denomina...

a) DMZ

b) Back-end

c) Front-end

d) -

50. ¿Para qué me sirve un honeypot?

a) No existe ese concepto

b) Para devolver el ataque

c) Para detectar actividades anormales o sospechosas en la red

d) Para penetrar en un sistema

51. ¿En qué se basa el sistema de navegación anónima TOR?

a) Se trata de una red que funciona sobre Internet; los mensajes viajan a través de una serie de nodos intermedios con el objetivo de ocultar la dirección IP origen del usuario al servidor de destino.

b) TOR es una red privada, aislada de Internet a nivel físico, con protocolos de encriptación no públicos para impedir que sean vulnerados.

c) Se trata de una red que funciona sobre Internet, a la que se accede a través de un navegador especial que utiliza un direccionamiento IP privado no estándar, de forma que la IP origen nunca sale del navegador.

d) Se trata de una red que funciona sobre Internet, que utiliza el protocolo “https” para cifrar la dirección IP origen del usuario, que de esta forma queda oculta al servidor de destino.

52. Referente a las radiaciones electromagnéticas espurias emitidas por los equipos basados en tecnologías de la información:

a) TEMPEST es el acrónimo de Telecommunications Electronics Material Protected from Emanating Spurious Transmissions.

b) En el ámbito del Ministerio de Defensa la certificación TEMPEST es emitida por el CCN (Centro Criptológico Nacional).

c) El nivel 3 de certificación TEMPEST corresponde a equipos cuyas radiaciones son imperceptibles a distancias superiores a los 15 metros.

d) Se pueden prevenir apantallando los equipos mediante una jaula de Faraday.

53. El protocolo SSL v.3:

a) Trabaja tanto sobre TCP como sobre UDP.

b) Hasta hace pocos años los navegadores que incorporaban SSL tenían su exportación desde EE UU limitada a claves de 128 bits.

c) Es idéntico al protocolo TLS, aunque este último está normalizado por el IETF mediante un RFC.

d) Intercambia las claves secretas mediante el ensobrado digital (digital envelopment) o mediante Diffie-Hellman.

54. ¿Qué método de control de acceso está dirigida al usuario?

a) No discrecional

b) MAC

c) Basado en identidades

d) DAC

55. Entre los diferentes tipos de servidores que existen, indique en cuál de ellos es correcto que se realicen las funciones de un servicio de cortafuegos:

a) Servidor de acceso remoto
b) Servidor web
c) Servidor de red
d) Servidor de comunicaciones

56. Los sistemas de gestión de información y eventos de seguridad (Security Information and Event Management -SIEM) funcionan:

a) Necesariamente con agentes instalados en los sistemas monitorizados.
b) Necesariamente sin agentes.
c) Pueden funcionar con y sin agentes.
d) Necesariamente han de realizar la recolección de eventos por interfaces Out of band.

57. ¿Cómo se denominan los 2 modos de utilización de IPSec?

a) balanceado y no balanceado.
b) túnel y abierto.
c) datagrama y transporte.
d) transporte y túnel.

58. Los denominados cortafuegos o firewalls de filtrado de paquetes, se caracterizan porque:

a) Analizan únicamente la información incluida en la cabecera TCP/IP de cada paquete.
b) Analizan la carga útil de datos de cada paquete.
c) Autentifican los usuarios que acceden a la red.
d) No permiten filtrar paquetes en función del puerto destino de la comunicación saliente.

59. Un ejemplo de ataque al control de acceso es:

a) Denegación de servicio
b) Spoofing
c) Ataques de diccionario
d) Todas las respuestas anteriores son correctas

60. Qué dos algoritmos de cifrado se utilizan en IPsec VPN:

a) 3DES y AES
b) AES y DH
c) 3DES y PSK
d) IKE y PSK

61. Los cortafuegos a nivel de aplicación:

a) suelen prestar servicios de tipo proxy
b) son generalistas, no basándose en ningún protocolo en concreto
c) no pueden prestar en ningún caso servicios de autenticación de usuarios
d) Ninguna de las respuestas anteriores es correcta

62. En un firewall de paquetes IP, los paquetes entrantes:

a) Primero se filtran, luego se hace el NAT
b) Primero se hace NAT y luego se filtran
c) Es igual que para los paquetes salientes
d) Depende de la interfaz

63. ¿Cómo se conoce al hecho de que un adulto se haga pasar por un menor en Internet para intentar establecer contacto con adolescentes y conseguir una relación de confianza a partir de la cual obtenga su control emocional y pueda realizar un chantaje con fines sexuales?

a) Grooming

b) Sexting

c) Doxing

d) Smishing

64. En el contexto de NAT IP, ¿qué dirección se usa para representar equipos internos en el exterior?

a) Local interna

b) Global interna

c) Local externa

d) Global externa

65. ¿Qué funcionalidad incorporan los cortafuegos de próxima generación (next-generation firewalls NGFWs) frente a los cortafuegos tradicionales?

a) Traslación de direcciones de red (Network Address Translation NAT).

b) Inspección profunda de paquetes (Deep Packet Inspection DPI).

c) Soporte a redes privadas virtuales VPN.

d) Filtrado de paquetes.

66. ¿Qué se entiende por NGFW (Next-Generation Firewall)?:

a) Es una gama de firewall de la compañía Barracuda.

b) Es un tipo de firewall empleado en entornos “cloud” como AWS.

c) Es un tipo de firewall específico para las redes 5G de comunicaciones móviles.

d) Es un tipo de firewall con capacidades de inspección en la capa 7 del modelo OSI.

67. ¿Qué es el spyware?

a) SW de alto secreto usado por los servicios de inteligencia de cada país

b) SW que diversas compañías introducen en tu ordenador cuando te descargas algo de internet, para ver tus programas y tus usos y sacar estudios de mercado

c) Es otro nombre de las conocidas cookies

d) La denominación es errónea, no se refiere a nada

68. Las VPNs utilizan mecanismos basados en túneles para:

a) Habilitar la navegación por Internet.

b) Encapsular paquetes de un protocolo dentro de otros paquetes pudiendo acomodar así protocolos incompatibles.

c) Efectuar una tarificación a la corporación que habilita acceso VPN.

d) Deshabilitar la seguridad del acceso VPN una vez autenticado el cliente VPN.

69. En el campo de la ciberseguridad, ¿qué es Ryuk?

a) Un virus que manipula la información para evitar el acceso a la misma y así poder obtener beneficios a cambio del antivirus.

b) Un ransomware que cifra la información para evitar el acceso a la misma y así poder obtener beneficios a cambio de la herramienta de descifrado.

c) Un ataque por denegación de servicio DDoS que impide el acceso de los organismos atacados a la misma.

d) Un rootkit para obtener el control de los equipos de usuario de los organismos atacados.

70. Para detectar vulnerabilidades en una red en la que trabajan distintos servidores y ordenadores pueden utilizarse herramientas de:

a) Software de monitorización de servidores.

b) Gestión de la configuración.

c) Soporte a usuarios y gestión de contraseñas.

d) Descubrimiento de puertos activos como, por ejemplo, el programa "Nmap".

71. ¿Qué no puede hacer un sistema de detección de intrusos?

a) Controlar el tráfico de red dentro y fuera de los firewall

b) Evitar que salten alarmas falsas

c) Detectar tiempos de acceso anormales

d) Guardar logs de los accesos

72. De los protocolos para proporcionar seguridad en internet es cierto que:

a) IPSec no es transparente a las aplicaciones

b) PPP asegura sólo un enlace, pero no la conexión completa

c) WTLS es más complejo que TLS ya que se adapta al entorno inalámbrico

d) Los protocolos a nivel de aplicación son comunes a grupos de aplicaciones según su funcionalidad

73. En relación con los servidores proxy y cortafuegos, señale la opción CORRECTA:

a) La función Network Address Translation (NAT) no puede ser realizada por un cortafuegos.

b) Un cortafuegos de aplicación opera sobre la capa 7 del modelo OSI, pudiendo filtrar protocolos como DNS, DHCP o HTTP.

c) Los servidores proxy abiertos no se pueden utilizar para prácticas como spam.

d) La utilización de soluciones Firewall-as-a-Service (FWaaS) alojadas en la nube no aumenta debido a la ausencia de oferta por parte de los fabricantes.

74. ¿Cuál de los siguientes NO es un tipo de ataque activo?

a) Interrupción.

b) Interceptación.

c) Modificación.

d) Generación.

75. ¿Cuál de los siguientes elementos de seguridad opera en el nivel 3 del modelo OSI?

a) Proxy

b) Firewall de filtrado de paquetes

c) Antivirus

d) Filtro anti-SPAM

76. ¿Cuál es una característica de los Caballos de Troya?

a) Un caballo de troya proxy abre el puerto 21 en el sistema objetivo.

b) Un caballo de troya es difícil de detectar, porque detiene su ejecución cuando la aplicación que lo ejecutó se cierra.

c) Un caballo de Troya puede cargarse en un virus o un gusano.

d) Un caballo de Troya FTP compromete el funcionamiento de cortafuegos.

77. De acuerdo con el modelo de arquitectura de seguridad de OSI, definido en la norma ISO/IEC 7498-2, indique cuál de las siguientes afirmaciones es correcta:

a) Un mecanismo de seguridad puede ser suministrado por varios servicios de seguridad

b) Cada servicio de seguridad debe ser suministrado por el mecanismo correspondiente

c) Todos los mecanismos de seguridad que se definen en el modelo se basan en algoritmos criptográficos

d) Un mismo servicio de seguridad puede ser suministrado por varios mecanismos de seguridad

78. Protegería un CPD de los ataques Tempest mediante:

a) Sistemas biométricos.

b) Jaulas de Faraday.

c) Cifrados asimétricos.

d) Antivirus.

79. El ataque que suplanta la identidad de un servidor DNS entregando direcciones IP falsas se denomina:

a) DoS.

b) Hijacking.

c) Spoofing.

d) Phishing.

80. En la arquitectura de cortafuegos "screened subnet" o subred apantallada:

a) se dispone de un único router, estando el bastión y los demás componentes en la red interna

b) se dispone de 2 routers, interno y externo, y tanto el bastión como los demás componentes están en la red interna

c) se dispone de 2 routers, interno y externo, y el bastión está en una red intermedia desmilitarizada o DMZ

d) no se dispone de ningún router, sino de un bastión con funciones de proxy que apantalla la red interna y alberga los servidores públicos

81. Señale cuales de las siguiente afirmaciones NO es una característica del protocolo EAP-TTLS:

a) En la creación del túnel TLS el servidor se autentica mediante certificado.

b) El cliente puede usar un método de autenticación distinto a EAP.

c) Está soportado de forma nativa en sistemas operativos Windows 7.

d) Los mensajes de autenticación del cliente son enviados cifrados al servidor.

82. Señale cuál de las siguientes opciones es CORRECTA respecto al control de acceso y la seguridad:

a) El spoofing se produce cuando alguien intenta utilizar la identidad de un usuario válido para acceder a información sensible.

b) El NAC (Network Access Control) es un dispositivo que permite asegurar la identidad con doble factor de autenticación.

c) En seguridad, un SIEM son las siglas de System Information Encryption Manager, que es un sistema que cifra la información para evitar ataques de ransomware.

d) -

83. Indique cuál es el comando correcto para realizar una captura con tcpdump sobre el fichero de salida output.pcap:

a) tcpdump - i eth0 - vv - F output.pcap

b) tcpdump - i eth0 - vv - o output .pcap

c) tcpdump - i eth0 - vv - f output.pcap

d) tcpdump - i eth0 - vv - w output.pcap

84. Los productos asociados a la familia Web Application Firewall (WAF) son capaces de utilizar, entre otras, las siguientes técnicas de protección (señale la respuesta INCORRECTA):

a) Basadas en firmas (signature-based).

b) Modelos de seguridad positiva/negativa.

c) Control de acceso seguro basado en certificado electrónico.

d) Detección de anomalías.

85. Si se desea implantar un sistema de filtrado de red con capacidad para establecer políticas de filtrado a nivel de aplicaciones en general (a nivel de la capa 7 de OSI) deberemos utilizar:

a) IP ACL del router

b) Cortafuegos con inspección de estado de paquetes (stateful inspection)

c) Firewall de aplicación web (web application firewall)

d) Firewall de nueva generación (Next Generation Firewall)

86. Meltdown y Spectre son dos tipos de:

a) Sistemas operativos de software libre.

b) Vulnerabilidades críticas que afectan a procesadores Intel, entre otros.

c) Ransomware que afectan a la criptomoneda.

d) Phishing que afectan a aplicaciones como Netflix y Paypal.

87. ¿Cuál de las siguientes afirmaciones sobre el virus Blaster es correcta?

a) Es un gusano que inspecciona la agenda de direcciones y envía un mensaje replicado a todas ellas

b) Es un gusano que usa una vulnerabilidad de Windows por la que el atacante puede tener permisos de ejecución locales

c) Es un gusano que se propaga a través del correo electrónico en un mensaje escrito en inglés de características variables, así como a través de los programas de intercambio de ficheros punto a punto

d) Es un gusano que busca en todas las unidades de disco direcciones de correo electrónico y se autoenvía a ellas utilizando su propio motor SMTP

88. ¿Cuál de las siguientes afirmaciones sobre el Protocolo SSL («Secure Socket Layer») es correcta?

a) Solo proporciona servicios de seguridad para el protocolo HTTP («HyperText Transfer Protocol»).

b) Utiliza mecanismos de criptografía asimétrica para garantizar la confidencialidad de los datos a transmitir.

c) El protocolo se implementa entre los niveles de Transporte y de Red.

d) Los servicios de seguridad que proporciona son transparentes al usuario y a la aplicación.

89. Al instalar un cortafuegos (firewall) para la protección de un servidor web, añadimos un mecanismo de salvaguarda que incrementa los niveles de:

a) La dimensión de confidencialidad de la información

b) La dimensión de disponibilidad de la información

c) La dimensión de integridad de la información

d) Todas las anteriores

90. ¿Cuál de los siguientes protocolos NO se utiliza para la constitución de Redes Privadas Virtuales (VPNs)?

a) L2TP

b) TLS

c) IPSEC

d) RTCP

91. El ataque de denegación de servicio llamado Smurf consiste en:

a) Dejar una conexión en estado semiabierto y no llegar a realizarse el paso final para establecer una conexión

b) Se trata de mandar a un puerto abierto del servidor un paquete hecho con la dirección y puerto origen igual que la dirección y puerto destino

c) Consiste en recolectar direcciones BroadCast para después mandar una petición ICMP cada una de ellas, falsificando la dirección IP de origen

d) Se trata de saturar la red mediante una cantidad repetitiva y enorme de peticiones de conexión

92. Kerberos es un protocolo de autenticación de redes de ordenador que:

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

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

c) Se basa en criptografía de clave asimétrica y no requiere un tercero de confianza

d) Se basa en criptografía de clave simétrica y no requiere un tercero de confianza

93. ¿Cuál de las siguientes NO es una característica de las amenazas APT?

a) Avanzada

b) Puntual

c) Dirigida

d) Persistente

94. ¿Cuál de las siguientes NO es una herramienta de VPN?:

a) NordVPN.

b) ExpressVPN.

c) CitosVPN.

d) PrivateVPN.

95. ¿Qué política de control aplica cuando la infraestructura usa un modelo no discrecional?

a) Basado en reglas

b) Basado en roles

c) Basado en identidades

d) MAC

96. Indique cuál de éstos no es un método EAP:

a) PEAP

b) EAP-SIM

c) EAP-PAP

d) EAP-TTLS

97. Se puede definir la técnica de ataque spoofing como:

a) La que captura el tráfico existente en una red y lo analiza.

b) La que suplanta la identidad mediante medios técnicos.

c) La que suplanta la identidad mediante ingeniería social.

d) Aquella en la que el atacante captura el tráfico entre dos sistemas con posibilidad de modificar e inyectar su propio tráfico.

98. Los cortafuegos de nivel 7 de la capa OSI, esto es, nivel de aplicación:

a) No existen

b) Tratan con números de secuencias de paquetes TCP/IP

c) Pueden ser considerados como filtros de paquetes

d) Actúan a modo de proxy para las distintas aplicaciones que van a controlar

99. Opción dentro de la herramienta NMAP que permite la detección del sistema operativo del objetivo a analizar:

a) —sN

b) —F

c) —O

d) —D

100. La diferencia entre un IDS y un IPS es:

a) los IDS detectan un ataque, generan una alerta, actúan e intentan neutralizar el ataque.

b) los IDS se pueden instalar en un servidor y los IPS solo pueden ser un equipo hardware.

c) los IDS y los IPS funcionan exactamente igual.

d) los IPS detectan un ataque, generan una alerta, actúan e intentan neutralizar el ataque.

101. ¿Qué diferencia, entre otras, hay entre S-HTTP y SSL?

a) El protocolo SSL fue desarrollado por Enterprise Integration Technologies (EIT) y el S-HTTP por Netscape

b) S-HTTP permite el cifrado pero no la autenticación digital, SSL permite tanto el cifrado como la autenticación digital

c) S-HTTP funciona entre la capa TCP y la capa de aplicación, SSL funciona en la de aplicación

d) S-HTTP solamente sirve para la navegación web, mientras que SSL sirve para cualquier comunicación

102. El protocolo L2TP es comúnmente utilizado por las VPN (Redes Privadas Virtuales) para:

a) Efectuar el proceso de encriptado de los datos transmitidos a través de la red pública.

b) Efectuar la autentificación de los usuarios.

c) Crear túneles de nivel OSI 2 que encapsulan los datagramas IP transmitidos a través de la red pública.

d) Filtrar los datos recibidos por cada usuario.

103. En un entorno de red, un pinchado de línea puede causar:

a) Uso excesivo de CPU

b) Acceso no autorizado a datos

c) a) y b)

d) Ninguna de las anteriores

104. SSL (Secure Socket Layer) y TLS (Transport Layer Security) son protocolos de cifrado con las siguientes características. Señale la opción INCORRECTA.

a) Ambos operan en la capa de transporte de internet

b) Su función es cifrar el tráfico de datos entre el cliente y el servidor

c) SSL es el protocolo sucesor de TLS

d) Cuando la comunicación tiene lugar en esta capa de transporte cifrada, se añade una “s” al nombre del protocolo: por ejemplo, http pasa a ser https

105. Un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información o controlar remotamente a la máquina anfitriona, se denomina:

a) Un caballo de Troya.

b) Un virus.

c) Un gusano.

d) El talón de Aquiles.

106. ¿Quién elaboró la especificación Transport Layer Security (TLS)?

a) UIT (Unión Internacional de Telecomunicaciones).
b) IETF (Internet Engineering Task Force).
c) Netscape Communications.
d) ETSI (European Telecommunications Standards Institute).

107. En qué consiste el mecanismo de Sobrecarga NAT:

a) En la utilización de puertos para traducir una dirección interna local en una dirección interna global.

b) En la utilización de puertos para traducir direcciones internas locales en una o más direcciones globales internas.

c) Traduce una dirección local interna en una global interna.
d) Traduce una dirección local interna en otra dirección local interna.

108. El protocolo Secure Shell, definido en la RFC (IETF Request for Comment) 4251:

a) Permite la negociación de los algoritmos criptográficos a usar
b) Proporciona, entre otros, los servicios de confidencialidad, no repudio e integridad
c) Opcionalmente admite compresión, que en este caso debe aplicarse tras el cifrado del paquete

d) Trabaja tanto sobre TCP como sobre UDP

109. Indique la respuesta FALSA, respecto al protocolo IPSEC:

a) El protocolo IPSEC AH garantiza integridad y autenticación, pero no confidencialidad.
b) El protocolo IPSEC ESP utiliza el número de protocolo 50 en la cabecera IP.
c) IPSEC utiliza IKE como protocolo de intercambio de claves.
d) IPSEC ESP es incompatible con el modo transporte, sólo se puede utilizar en modo túnel.

110. En el protocolo Secure Socket Layer (SSL) el subprotocolo de negociación (handshake) negocia las claves de sesión mediante el esquema de Diffie-Hellman (D-H) o RSA. Indique la respuesta correcta:

a) D-H anónimo es susceptible de ataques por hombre en medio.
b) D-H efímero no requiere certificado del servidor ni del cliente.
c) D-H constante no precisa certificado del cliente.
d) RSA necesita la generación de un número aleatorio por el servidor que es enviado al cliente cifrado con la clave pública de éste.

111. ¿Cuáles de las siguientes NO es una característica de un cortafuegos de nivel de aplicación?

a) Realizan control del estado de la comunicación (stateful inspection).
b) Tiene mejor rendimiento que un cortafuegos “stateless” (con hardware equivalente).
c) Inspeccionan el contenido.
d) -

112. La información puede obtenerse a través de señales eléctricas en las ondas. Una forma de combatirlo es a través de:

a) Tempest
b) Ruido Blanco
c) Zonas de control
d) Todas las respuestas anteriores son correctas

113. De los siguientes ¿Cuál es un componente básico de un cortafuegos?

a) El balanceador de carga (o asignador de tareas) que permite la ampliación horizontal del "bastión" mediante la asignación de tramas IP entre varias subredes o máquinas configuradas en forma idéntica.

b) Los servicios proxy, entendidos como aplicaciones SW para reenviar o bloquear conexiones a servicios como finger, telnet o ftp.

c) el sistema operativo LINUX en sus distribuciones seguras.

d) La monitorización de servicios de red tipo SMTP, POP3, HTTP, NNTP, PING… a efectos de disponibilidad y rendimiento (performance).

114. En relación al ámbito de seguridad de la red de una organización, podríamos afirmar que:

a) IDS (Intrusion Detection System) es un servidor en la red que bloquea los accesos no autorizados.

b) IPS (Intrusion Prevention System) es un software que se utiliza para proteger a los sistemas de ataques y accesos no autorizados.

c) SIEM (Security Information and Event Management) es la figura responsable encargada de atender las peticiones de acceso a los recursos de la organización.

d) IGS (Intrusion Gateway System) combina las tareas de un IDS y un IPS, proporcionando un análisis en tiempo real de las alertas de seguridad generadas por los distintos dispositivos hardware y software de la red.

115. Si estamos recibiendo un ataque basado en HTTP Flood que intenta inundar de peticiones HTTP (GET y POST) nuestras aplicaciones web, que tipo de sistema es el más adecuado para protegernos y parar este tipo de ataques:

a) Sistemas antivirus.

b) Sistemas antispam.

c) Sistemas de detección de intrusiones (IDS).

d) Sistemas anti-DDoS.

116. ¿Cuál de los siguientes sistemas correspondería con un sistema de autenticación fuerte?

a) Un sistema que utilice usuario y contraseña.

b) Un sistema que utilice usuario, contraseña y token digital.

c) Un sistema que utilice identificación biométrica.

d) Un sistema que utilice usuario y código numérico.

117. Señale la opción correcta sobre la criptografía simétrica de bloque:

a) El uso del algoritmo DES resulta más seguro que el de AES.

b) SNOW 3G es un algoritmo de este tipo de criptografía utilizado en UMTS/LTE.

c) 64 Kbits y 128 Kbits son longitudes típicas de los bloques empleadas en sus algoritmos.

d) Son algoritmos de este tipo de criptografía Camellia y AES/Rijndael.

118. ¿Cuál de las siguiente definiciones se corresponde con la vulnerabilidad DDoS que puede producirse sobre nuestros sistemas?

a) Suplantación de la dirección IP

b) Escuchas en red

c) Denegación de servicio Distribuido

d) Ataques de desbordamiento de buffer

119. En relación con los algoritmos de cifrado, señale cuál de las siguientes afirmaciones es CORRECTA:

a) El protocolo TLS 1.3 definido en la rfc 8446 de la IETF utiliza algoritmos de cifrado simétrico y asimétrico.

b) El protocolo TLS 1.4 se utiliza en navegadores obsoletos con algoritmos simétricos y se recomienda su sustitución por SSL 2.1 definido en la rfc 8543 de la IETF.

c) Los protocolos TLS y PGP utilizan solo algoritmos de certificado público.

d) -

120. ¿Cuál de los siguientes elementos, de resultar inadecuado, podría facilitar un ataque de denegación de servicio en un sistema de información?

a) La configuración del router y reglas aplicadas.
b) El diseño de la red interna.
c) Las técnicas de revisión de auditoria.
d) Las técnicas de prueba de auditoria.

121. Si queremos configurar un servidor web Apache para permitir únicamente tráfico TLSv1.2, indique la directiva donde se realiza dicha configuración:

a) SSLCipherSuite
b) SSLProtocol
c) TLSRequire
d) TLSProtocol

122. Señale la opción correcta respecto al protocolo Transport Layer Security (TLS):

a) Está en proceso de sustitución por el protocolo Secure Sockets Layer (SSL)
b) Emplea criptografía simétrica para autenticar a las partes, y criptografía asimétrica para el flujo de datos entre ellas
c) Utiliza el protocolo IPSec para el intercambio de información en el nivel de red
d) Se emplea sobre la capa de transporte para cifrar los datos de protocolos del nivel de aplicación

123. Respecto a la seguridad en redes, indique qué es un exploit:

a) Es un malware diseñado para aprovechar la vulnerabilidad de un software.
b) Persona que accede a datos no autorizados.
c) Adware que modifica la página de inicio de los navegadores de Internet sin el consentimiento del usuario.
d) Software utilizado para la suplantación de la identidad de un usuario de la red.

124. Cuál de los siguientes sistemas está colocado tradicionalmente en la DMZ de una red:

a) Servidor de aplicaciones
b) Proxy
c) Servidor LDAP
d) Servidor de base de datos

125. El estándar XMLDSig, en relación con la situación de los datos que se van a firmar con respecto a su firma, ¿cuál es la clasificación correcta?

a) Enveloped Signature
b) Detached Signature
c) Enveloping Signature
d) Todas las anteriores

126. Respecto al protocolo de seguridad IKE, cuál de las siguientes respuestas es falsa:

a) recrea las claves cada cierto tiempo.
b) permite utilizar certificados digitales.
c) se necesita una asociación de seguridad IKE para cada conexión IPSEC.
d) está basado en Oakley.

127. En ciberseguridad, ¿qué se entiende por “honeypot”?:

a) Es una funcionalidad de los “firewalls” web para bloquear “ransomware”.

b) Es un sistema que actúa de señuelo ante ciberataques.

c) Es una arquitectura de red mallada específicamente diseñada para proteger determinados activos.

d) Es un tipo de ataque del tipo “man-in-the-middle”.

128. Cuando multitud de sistemas atacan un único sistema provocando su caída, estamos ante:

a) Un ataque de denegación de servicio (DoS)

b) Echelon, una red global de espías

c) Un ataque distribuido de denegación de servicio (DDoS)

d) Un ataque de ingeniería social

129. ¿Qué se entiende por IP Spoofing?

a) Es un ataque que se basa en la ejecución de código "Script" arbitrario en un navegador.

b) Es un ataque que pretende provocar un direccionamiento erróneo en los equipos afectados, mediante la traducción errónea de los nombres de dominio a direcciones IP.

c) Es un ataque que consiste en modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los originó.

d) Es un ataque que se compone de un conjunto de actuaciones que persiguen colapsar determinados equipos o redes informáticas, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios.

130. ¿Qué protocolo emplea el sistema Cl@ve entre los Proveedores de Identidad (IdP) y las aplicaciones (SP, Proveedores de Servicio) que solicitan la autenticación de un ciudadano?:

a) OAuth 2.0 (RFC 6749).

b) SAML 2.0 (RFC 7522).

c) Microsoft AD LDAP.

d) OpenID 1.1.