## **1. ¿Cuál es el objetivo de la seguridad activa?**

Proteger y evitar daños a los sistemas informáticos.

## **2. En IPS, ¿qué método produce más falsos positivos?**

Detección por anomalías.

## **3. Enumera las motivaciones de los atacantes.**

* Dinero
* Ideología
* Compromiso
* Autorrealización

## **4. ¿Cuál es la principal diferencia entre IDS e IPS?**

* **IDS (Sistema de detección de intrusos)**: Notifica los ataques.
* **IPS (Sistema de prevención de intrusos)**: Notifica y elimina el ataque.

## **5. ¿Por qué los ataques pasivos son muy difíciles de detectar?**

Porque no provocan ninguna alteración de los datos.

## **6. ¿Qué es un Host IDS?**

Un programa instalado en los hosts, que comprueba los paquetes de datos entrantes y salientes.

## **7. ¿Qué tipo de ataque activo es el phishing?**

Suplantación de identidad.

## **8. ¿Cuál es la diferencia entre las herramientas preventivas y las paliativas?**

* **Preventivas**: Intentan evitar los ataques.
* **Paliativas**: Intentan evitar los daños si el ataque se produce.

## **9. ¿En qué tipo de ataque la atención se centra en la detección?**

Ataque activo.

## **10. ¿En qué tipo de dispositivos debemos evitar la reproducción/ejecución automática?**

En los dispositivos extraíbles.

## **11. ¿Cuál es el método más fácil de usar para combatir un malware?**

Eliminación una vez instalado el malware.

## **12. No acceder desde conexiones públicas pertenece al tipo de seguridad…**

Mensajería instantánea.

## **13. Define malware.**

Programa que se ejecuta sin conocimiento ni autorización del usuario, realizando funciones perjudiciales para el usuario o el sistema.

## **14. Si ignoramos mensajes poco éticos e inmorales, ¿qué estamos protegiendo?**

Nuestra seguridad en las redes sociales.

## **15. ¿Cuál es un típico ataque de gusano?**

Los DoS o DDoS.

## **16. ¿Los protectores de pantalla tienen algún riesgo?**

Sí, hay que evitar descargarlos en la navegación web.

## **17. ¿Cómo suelen descargarse los fantasmas?**

Al visitar sitios web, revisar correo electrónico y por ventanas emergentes.

## **18. ¿Cuál es uno de los servicios más usados para distribuir malware?**

El correo electrónico.

## **19. ¿Qué tipo de malware se orienta hacia el robo de datos bancarios?**

Troyano.

## **20. Con respecto al hardening y los USB, ¿qué debemos hacer?**

Debemos deshabilitar la ejecución automática de dispositivos USB.

## **21. ¿Por qué la detección de rootkits es muy difícil?**

Porque es capaz de corromper el programa que debería detectarlo.

## **22. ¿Por qué debemos mantener actualizados el sistema operativo y las aplicaciones?**

Porque el malware busca sus vulnerabilidades para entrar en nuestros equipos.

## **23. ¿Cuál es la diferencia entre keyloggers y stealers?**

* **Keyloggers**: Envían las pulsaciones del teclado.
* **Stealers**: Envían la información almacenada en el equipo.

## **24. ¿Cuáles son las contramedidas más comunes para evitar el reconocimiento y las vulnerabilidades?**

Restringir la información a través de los DNS y filtrar los paquetes de datos.

## **25. ¿Cuál es el objetivo de los ataques distribuidos?**

Crear un conjunto de equipos usados para actividades dañinas sin conocimiento de sus propietarios.

## **26. Instalar cortafuegos hardware y software, ¿qué evita?**

Que el atacante obtenga acceso al sistema.

## **27. Enumera las fases de un ataque.**

* Reconocimiento
* Vulnerabilidades
* Obtener acceso
* Mantener acceso
* Borrado de huellas

## **28. ¿Cuáles son los objetivos del malware?**

* Robo
* Secuestro
* Redes de bots

## **29. Password filtering, ¿en qué fase del ataque se usa?**

Obtener acceso.

## **30. ¿Qué incorporan también muchos gusanos?**

Puertas traseras.

## **31. La creación de cuentas con privilegios administrativos, ¿en qué fase del ataque se usa?**

Mantener acceso.

## **32. ¿Qué tipo de malware tiene apariencia de ser inofensivo?**

Troyano.

## **33. ¿Cuáles son las contramedidas para evitar el borrado de huellas?**

Guardar los archivos log en lugar distinto a su generación y la gestión de históricos y monitorización.

## **34. ¿Qué hacen los rootkits?**

Modifican el sistema operativo para permanecer oculto al usuario.

## **35. ¿Cuál es el objetivo de las herramientas preventivas?**

Evitar que el malware se instale en el sistema informático.

## **36. ¿Cómo se llama el malware que muestra publicidad de forma intrusiva?**

Adware.

## **37. ¿Cuál es la mejor forma de descargar actualizaciones?**

A través de los mecanismos ofrecidos por el propio fabricante del software.

## **38. Si deshabilitamos las carpetas compartidas, ¿qué evitamos?**

La propagación de gusanos.

## **39. ¿En qué consiste el hardening?**

En configurar el sistema operativo para hacerlo más seguro.

## **40. Bloquear las imágenes es una buena práctica en…**

Protección del correo electrónico.

## **41. ¿Qué sucede si respondemos al correo spam?**

Confirmamos que la dirección de correo se encuentra activa.

## **42. Impedir la ejecución automática de archivos es buena práctica en…**

Seguridad en la navegación web.

## **43. ¿Cuándo es imprescindible verificar el hash?**

Cuando descargamos software de seguridad.

## **44. Cambiar periódicamente las contraseñas y no repetirlas es buena práctica en…**

Seguridad en las redes sociales.

## **45. Explorar con un antivirus todos los archivos descargados es buena práctica en …**

Seguridad en las redes P2P y en la mensajería instantánea.

## **46. No compartir información confidencial es buena práctica en…**

Seguridad en la mensajería instantánea.

## **47. ¿Podemos transportar información confidencial en un dispositivo extraíble?**

Sí, pero tiene que estar cifrada.

## **48. ¿A qué apelan las herramientas preventivas?**

Al sentido común del administrador del sistema y a los usuarios en general.

## **49. Enumera las herramientas paliativas más comunes.**

* Encriptación
* Antimalware
* Firewall
* IDS
* IPS

## **50. ¿Qué herramienta paliativa no elimina las instrucciones?**

IDS.

## **51. ¿Cuál es la diferencia entre HIDS y NIDS?**

* **HIDS**: Monitoriza solo hosts.
* **NIDS**: Supervisa la red entera.

## **52. ¿Qué herramientas concretas suelen utilizarse en los HIDS?**

Tripwire y Aide.

## **53. ¿Qué tipos de redes son supervisadas por los Network IDS?**

Tanto las externas (Internet) como las locales (LAN).

## **54. ¿Qué función realizan los IPS?**

Las mismas que los IDS, añadiendo la capacidad de eliminar intrusiones.

## **55. ¿Qué significan las siglas IDPS?**

Sistema de detección y prevención de intrusos.

## **56. Indica los tres métodos de detección IPS.**

* Basado en firmas
* Análisis de protocolos
* Basado en anomalías

## 

## **57. En un ataque activo, ¿cuál es el daño al sistema?**

Daño permanente.

## **58. Indica las vulnerabilidades utilizadas por los backdoors.**

Puertos abiertos, contraseñas y cortafuegos débiles.

## **59. El malware capaz de modificar la redirección de servidores DNS se llama…**

Hijacking.

## **60. ¿Qué nos permite aprender a pensar como los atacantes y a no subestimar su mentalidad?**

Conocer las etapas de un ataque informático.

## **61. No almacenar información confidencial y sensible en el mismo equipo incrementa la seguridad en…**

Redes P2P.

## **62. Reinstalar el sistema operativo es muchas veces la única solución para los…**

Rootkits.

## **63. ¿Qué pretende el intruso mediante un ataque activo?**

Abrirse paso a través de las defensas de la red para entrar en el sistema

## **64. ¿El criptominado se basa en?**

Botnets o redes zombies.

## **65. ¿Qué tipo de ataque utiliza la información recopilada en el ataque pasivo?**

Ataque activo.

## **66. ¿Qué tipo de ataque activo impide el uso normal de recursos informáticos y de comunicaciones?**

Denegación de servicios.

## **67. Completa la siguiente frase: “El ataque activo representa…”**

Una amenaza para la integridad y la disponibilidad.

## **68. ¿Cuál es el objetivo de los virus?**

Provocar el mal funcionamiento del ordenador.

## **69. Escribe los malwares que suelen ser instalados como troyanos.**

Spyware, adware y hijacking.

## **70. Explica la detección basada en firmas.**

Supervisa el tráfico de red en busca de ataques y lo compara con patrones predefinidos.

## **71. Usar perfiles de usuarios con los menores privilegios posibles, pertenece a…**

Endurecimiento del sistema operativo.

## **72. ¿Cuál es una herramienta típica de NIDS?**

SmoothSec.

## **73. En las herramientas preventivas, ¿qué deben hacer los usuarios?**

Incorporar buenas prácticas para proteger y prevenir.

## **74. ¿Cuáles son los sistemas IDS más usados?**

HOST IDS y NETWORK IDS.

## **75. Las botnets son usadas en…**

Envío de spam, denegación de servicios y criptominado.