GUÍA DE ESTUDIO PARA SEGURIDAD EN LA RED INFORMÁTICA

1. El mantra de todo ing. De seguridad es que la seguridad no es un producto sino un proceso, quien lo dijo?

Bruce Schneier

2. Es el conjunto d emedidas y proceidmientos, tanto humanos como técnico sque permiten proteger la integridad, confidencialidad y disponibilidad de la información.

Seguridad de la información

3. A que se refiere la integridad?

Asegurar que la información y sus métodos de proceso son exactos y completos.

4. ¿A qué se refiere la confidencialidad?

hacer constar que sólo pueden acceder a la información y modificarla los usuarios autorizados.

5 ¿A qué se refiere la disponibilidad?

Dejar que la información pueda estar disponible cuando los usuarios la requieran.

6. Se considera una rama de la seguridad de la información que intenta proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida.

La seguridad en informática

7. Si hablamos de seguridad informática decimos que se desea proteger?

La seguridad física y seguridad lógica
Activa y pasiva

8. Es un recurso del sistema en el que se consideran trabajadores, sw, datos hw, las comunicaciones que se necesitan para lograr los objetivos de una organización.

Activo

9. Son agujeros de seguridad o debilidad de un activo que puede afectar de alguna forma el correcto funcionamiento del sistema informático.

Vulnerabilidad

10. Cualquier entidad o circunstancia que atenta contra el buen funcionamiento de un sistema informático se llama?

Amenaza

11. Es la acción que intenta aprovechar una vulnerabilidad o debilidad de un sistema informático con el fin d eprovocar un impacto sobr él e incluso tomar el control?

Ataque

12. Son fases por las que pasa un ataque

Reconocimiento
Exploración
Obtención de acceso
Mantener el acceso
Borrar huellas

13. Es una medida d ella probabilidad que se materialice una amenaza

Riesgo

14. Es una forma ordenada y sistemática que nos permitirá conseguir una meta o lograr

Método

15. Es un conjunto de métodos empleados por una disciplina

Metodología

16. Es un conjunto de filosofías, fases, procedimientos, reglas, tecnicas, herramientas, documentación y aspectos de formación par los desarrolladores de SI

Metodología de Desarrollo

17. Generalmente evita que se produzcan errores en los sistemas operativos en donde se realiza el desarrollo, así como en las pruebas del funcionamiento de la aplicación

Seguridad en una aplicación

18. Son ejemplos de metodologías de desarrollo?

OWASP
Microsoft Trustworthy Computing
OSSTMM
OASIS Web Application Security (WAS)

19. Diseñada por MS tiene como objetivo crear y disponer par ala comunidad en general una computación basada en mejores prácticas (best practices) que sea más privada y confiable

Microsoft Iniciativa Trusthorthy Computing

20. La Iniciativa trustworthy computing abarca con conceptos como la estabilidad, la confianza, la seguridad en la plataforma y este ultimo concepto se sustenta de 5 pilares primordiales que no debemos dejar de tomar en cuenta.

Aislamiento y flexibilidad
Calidad
Autenticación
Autorización y control de accesos
Orientación y formación

21. La iniciativa trhust… se basa en seguridad, confiabilidad privacida dy mejores practicas

Verdadero

22. El modelo de amenazas dicta conceptos como ser seguro por defecto, seguro por diseño, seguro por distribución y seguro en las comunicaciones

Verdadero

23. El modelo stride está compuesto d ellas amenazas siguientes: spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privileges

Verdadero

24. Creado por Pete Herzog y desarrollado en ISECOM

La metodología OSSTMM

25. Qué es OSSTMM

Es uno de los estándares más usado en auditorías de seguridad para revisar la seguridad de los sistemas desde Internet.

26. Las fases de OSSTMM referente a la seguridad son?

Seguridad de la información
Seguridad física
Seguridad Inalámbrica
Seguridad en las comunicaciones
Seguridad en tecnologías de internet
Seguridad de los procesos

27. La seguridad de la información abarca?

Revisión d ella inteligencia competitiva
Rev. De la privacidad
Recolección de documentos

28. La seguridad de los procesos refiere que?

Testeo de solicitud
Testeo de sugerencia dirigida
Testeo d ellas personas confiables

29 La seguridad de las tecnologías de Internet abarca algunos conceptos como?

Logística y controles
Exploración de red
Identificación d ellos servicios del sistema
Búsqueda de información competitiva
Revisión de privacidad
Obtención de documentos
Búsqueda y verificación de vulnerabilidades
Testeo de aplicaciones de Internet
Enrutamiento
Testeo de sistemas confiados
Testeo de control de acceso

30. En cuestión de seguridad en las comunicaciones se refiere al testeo de PBX, testeo del correo de voz, revisión del fax, testeo del modem y evaluación de políticas de seguridad.

Falso (las políticas de seguridad no entran)

31. Los conceptos de verificación de radiación electromagnética, verificación de redes inalámbricas, verificación de redes bluetooth, verificación de dispositivos de entrada inalámbricos y verificación de dispositivos d emano inalámbricos pertenecen a?

Seguridad inalámbrica

32. La revisión de perímetro, revisión de monitoreo, la evaluación de controles de acceso, la revisión de respuesta de alarmas y la revisión de ubicación y revisión de entrono son conceptos de?

Seguridad física

33. Tiene como objetivo ofrecer una metodología de libre acceso y utilización, ser utilizada como material de referencia por parte d ellos arquitectos de sw, fabricantes y profesionales de la seguridad

OWASP

34. Son los proyectos mas destacados de OWASP

Webgoat
Webscarab
Top ten

35. Es parte de los principios básicos d ella seguridad de cualquier aplicación o servicio web y se refiere a que los mecanismos de seguridad deben diseñarse para que sean los más sencillos posibles, huyendo de sofisticaciones que compliquen excesivamente la vida a los usuarios

Diseño Simple

36. Son algunos de los elementos de la guía de desarrollo: por ejemplo manejo d epagos, phishing, los serviciow web, autenticación, autorización, etc.

Verdadero

37. Describe un marco de pruebas típico que puede ser desarrollado en una Organización

Framework de pruebas

38. Su uso es para reconocer al usuario en el momento en el que se conecta al servidor, también ofrece personalización

Las cookies

39. ¿El No ser la fuente de robos de identidad, implemente protecciones dentro de su aplicación, monitorice actividad inusual en las cuentas; son pautas para evitar el problema de?

Phishing

40. De cuántas fases consta el framework de pruebas?

5 fases

41. Si se habla d ellas fallas de inyección, como SQL, NoSQL, OS o LFSP que ocurren cuando se envían datos no confiables a un interprete , como parte de un comando o consulta, hablamos de?

A1 Inyección

42. La debilidad más común es simplemente no cifrar datos sensibles

A6 Exposición de datos sensibles

43. Los desarrolladores no conocen todos los componentes que usan y menos sus versiones

A9 Uso de componentes con vulnerabilidades conocidas.

44. Con frecuencia las aplicaciones redirigen a los usuarios a otras páginas

A10. Redirecciones y reenvíos no validos

45. Normalmente las aplicaciones utilizan el nombre o clave actual de un objeto

A4. Referencia directa insegura a objetos

46. Representa una lista concisa y enfocada sobre los diez riesgos más críticos sobre seguridad en aplicaciones y no es un programa de seguridad en aplicaciones

Top Ten

47. Herramienta destinada a la educación y que permite practicar y explotar las vulnerabilidades mas frecuentes en un sitio web, con el fin de poner en práctica una metodología de desarrollo seguro.

Webgoat

48. Es un framework para el análisis de aplicaciones que utilizan como base los protocolos http y https, esta escrito en java y es multiplataforma

WebScarab

49. Los sistemas deben diseñarse para que funcionen con los menos privilegios posibles

Verificación de privilegios

50. ¿Debe evitarse “reinventar la rueda” constantemente, estamos hablando de?

Utilización y reutilización de componentes de confianza.