Nombre: Torres Trujillo Luis Octavio

Materia: Tópicos Selectos de Seguridad en redes y sistemas de software

Actividad 01 – Cuestionario Introducción al hacking ético

Cuestionario

1. ¿Qué es el hacking ético?

El hacking ético es simular técnicas de los atacantes mediante herramientas, trucos etc para poder saber vulnerabilidades de un sistema y así poder repáralas y asegurar la seguridad del sistema de software.

2. ¿Qué es el hacker ético?

Es un experto en computadoras y redes que atacan a un sistema de software (con permiso de los dueños) para encontrar vulnerabilidades que un hacker malicioso podría utilizar.

3. ¿Qué hacen los hackers éticos con las vulnerabilidades encontradas?

Este las reporta para que la empresa del software pueda arreglarlo, no saca ninguna ventaja de estas vulnerabilidades.

4. ¿Cuáles son los requisitos para ser hacker ético?

Tener habilidades de programación y redes, conocer técnicas de hacking, saber de investigación de vulnerabilidades y seguir un código de conducta.

5. ¿Cuáles son las tres cosas clave que permite el hacker ético?

Prevenir, descubrir y analizar.

6. Describe lo que permite el hacker ético

Prevenir: previene que los hackers maliciosos puedan tener acceso al sistema

Descubrir: descubre vulnerabilidades y analizar su riesgo potencial

Analizar: comprobar y aumentar la seguridad de una organización y de su(s) sistemas de software

7. ¿Qué permite la investigación de vulnerabilidades?

Descubrir debilidades del diseño que puedan permitir acceder a lados que no se deberían y poder darle un mal uso.

8. ¿Cómo pueden ser clasificadas las vulnerabilidades?

Nivel de severidad (bajo, intermedio o alto)

Rango de explotación (local o remoto)

9. ¿Qué son las pruebas de penetración (pentest)?

Son un método de evaluación de la seguridad de un sistema simulando un ataque para encontrar vulnerabilidades que un verdadero atacante puede utilizar.

10. ¿Cuál es el resultado del pentest?

Un reporte en el que se explican las vulnerabilidades y como acceder a ellas el cual es entregado a la empresa para que los equipos técnicos los analicen y les den una solución.

11. ¿Cuáles son los tipos de pruebas de penetración?

Black-box, gray-box y white-box.

12. Describe los tipos de pruebas de penetración

Black-box: no se tiene nada de conocimiento del funcionamiento interno del sistema

Gray-box: se provee algo de información, como ips, urls etc.

White-box: se provee información fuerte del sistema, tales como credenciales, código fuente etc.

13. ¿Cuáles son las fases de las pruebas de penetración?

Preparación, conducción y conclusión.

14. Describe las fases de las pruebas de penetración

Preparación: se firma un contrato que contiene cláusulas de no revelación, así como protecciones al hacker ético y delimitaciones del perímetro, actividades de evaluación etc.

Conducción: Se realizan las simulaciones y se elabora un reporte de lo encontrado

Conclusión: Se entregan los resultados a la empresa y las correcciones que deberían hacer en caso de ser necesario.

15. ¿Cuáles son las fases del hacking ético?

Reconocimiento

Escaneo

Ganar acceso

Mantener el acceso

Borrar huellas