# SEGURIDAD EN REDES DE COMPUTADORAS

Ingeniería en Computación

## UNIVERSIDAD AUTÓNOMA DE ZACATECAS

## UNIDAD ACADÉMICA DE INGENIERÍA ELÉCTRICA

## INGENIERÍA EN COMPUTACIÓN

**Tarea 1**

Cuestionario

**Docente**

Carlos Héctor Castañeda Ramírez

**Alumna**

Jessica Vanegas López

**Grado**

8° “B”

Zacatecas, Zacatecas 31/01/2023

1. **Menciona los tres tipos de protección de datos.**

   Criptografía, bóvedas y protección contra escritura.

2. **¿Cuál es el objetivo de la ciberseguridad?**

   Reducir el riesgo de ciberataques y proteger contra la explotación no autorizada de sistemas, redes y tecnologías.

3. **¿Qué significa CID?**

   Confidencialidad, Integridad y Disponibilidad

4. **¿Cuáles son los tipos de riesgo en la ciberseguridad?**

   Activo, vulnerabilidad, amenaza, salvaguarda (control, contramedida), impacto, riesgo e incidente (breacha, ataque).

5. **¿Qué tipo de amenaza se utiliza para robar datos y se instala en el sistema cuando el usuario hace clic en un enlace en un correo?**

   Malware

6. **¿Cómo es el método de infección de Ransomware?**

   Es a través de un anexo en un correo electrónico enviado al usuario mediante phising.

7. **¿Qué hace la amenaza de Social Engineering?**

   Manipula a las personas para que realicen acciones, cometan errores de seguridad o divulguen información confidencial. También aprovecha de la disponibilidad de las personas de ayudar pretendiendo ser otra persona: una autoridad, un empleado, solicitando información de forma inusual o desesperada donde puede falsificarse gafetes para acceder a espacios restringidos o entrar detrás de alguien que tiene ese acceso.

8. **¿Cuál es la amenaza que engaña al usuario para que comparta información personal, y es muy difícil de detectar?**

   Phising

Zacatecas, Zacatecas 31/01/2023

9. **¿Existe algún parche de seguridad en la amenaza de Zero-day Exploit y como suelen ofrecerse?**

   No existe aún un parche de seguridad o actualización que la mitigue por parte del fabricante o desarrollador. Y suelen ofrecerse como servicio (software as a service) donde el creador recibe parte del beneficio una vez efectuado el ataque, ya sea por la venta o por comisión del pago de rescate en el caso de ransomware.

10. **¿Qué diferencias existen entre las amenazas de Denial of Service Attack (DoS), Man in the midle, Password cracking y Covert Hardware?**

| Denial of Service Attack (DoS) | Man in the midle | Password cracking | Covert Hardware |
|---|---|---|---|
| • Inunda los sistemas, redes o servidores con tráfico masivo.<br>• Puede agotar los recursos de un sistema como memoria, espacio en disco duro.<br>• Se pueden utilizar varios dispositivos infectados para lanzar un ataque en el sistema, generando una de denegación de servicio distribuida (DDoS). | • Comunicación entre dos partes. Escucha y captura paquetes enviados por la red, teniendo acceso a datos confidenciales, o incluso modificar la respuesta al usuario.<br>• Si los datos no viajan cifrados (texto plano) son fácilmente interceptados.<br>• En algunos casos es posible interceptar datos cifrados y aplicar técnicas de cracking para obtener contraseñas en texto plano (wifi cracking). | • Se hacen pruebas para diversas contraseñas posibles hasta adivinar la correcta (guessing).<br>• Se prueban combinaciones numéricas o alfabéticas.<br>• Se prueban palabras en un diccionario como contraseñas.<br>• Se prueban combinaciones de palabras de diccionario con frases al inicio o al final.<br>• Se van combinando todos los caracteres posibles en todas las posiciones. | • El atacante puede uKlizar diferentes disposiKvos de hardware que le faciliten la infiltración encubierta en las redes y sistemas. |

11. **¿Cuáles son las dos principales características de la fuente de amenaza de Hackers?**

    Black Hat Hackers y White Hat Hackers.

12. **¿Como se lleva a cabo la fuente de amenaza del Terrorist Groups?**

Zacatecas, Zacatecas 31/01/2023

Se llevan a cabo con ataques cibernéticos para destruir, infiltrarse o explotar la infraestructura crítica para amenazar la seguridad nacional, comprometer el equipo militar, perturbar la economía y causar bajas masivas.

13. **¿A que se le puede tener acceso con base a la amenaza de Malicious Insiders y cómo atacan?**

    Al acceso legítimo a los activos de la empresa, pero hacen un mal uso para robar o destruir información con fines de lucro personal o financiero. Y atacan por venganza al no ser promocionados, o infiltrados a propósito para filtrar secretos comerciales.

14. **Menciona a los dos hackers más importantes.**

    Jonathan James y Albert González.

15. **Menciona al menos dos ataques recientes del año 2021 que hayan sido más relevantes para ti.**

- 2 de junio de 2021 Ciberataque por ransomware a JBS USA el mayor distribuidor de carne en el mundo, afectando la distribución y precios de la carn, pago de 11m de dólares por el rescate de la información.
- 5 de marzo de 2021, Ciberataque por explotación de vulnerabilidades en Microsoft Exchange, el software de correo más usado en el mundo, afecto a empresas en todo el mundo.

16. **¿Qué riesgo puede haber en la ciberseguridad?**

    El riesgo de ciberseguridad es la posibilidad de que una amenaza explote una vulnerabilidad en un control de seguridad dando pie a un ciberataque, que afecta los activos de información de una organización y puede generar un impacto negativo.

Zacatecas, Zacatecas 31/01/2023