Tema: Ciberseguridad
Objetivo: Identificar conceptos propios de la ciberseguridad.

Alumno: Ariadna Abigail Alanis Estrada

CUESTIONARIO

1. **¿Qué es un pirata informático?**

Es una persona que accede sin autorización a sistemas o redes informáticas con el fin de robar información, causar daños o beneficiarse de manera ilegal.

2. **¿Qué es un hacker?**

Es un experto en informática que explora sistemas informáticos y redes. Aunque el término a veces se asocia con delincuentes, no todos los hackers tienen malas intenciones. Existen hackers "éticos" que ayudan a mejorar la seguridad de los sistemas.

3. **¿Qué es un gusano?**

Es un tipo de malware (software malicioso) que se replica automáticamente para propagarse por redes y dispositivos, consumiendo recursos y causando lentitud o fallas en los sistemas.

4. **¿Qué es un ataque DoS?**

Un ataque Denial of Service (DoS) busca saturar un servidor o red con tráfico excesivo para que deje de funcionar correctamente y no pueda atender a los usuarios legítimos.

5. **¿Qué es una botnet?**

Es una red de computadoras infectadas (bots) que son controladas de manera remota por un ciberdelincuente para realizar actividades maliciosas, como enviar spam o ejecutar ataques DoS.

6. **¿Cuáles son los medios por los que se pueden realizar ataques?**

Se pueden realizar mediante correos electrónicos falsos (phishing), enlaces maliciosos, descargas de software infectado, redes Wi-Fi públicas, vulnerabilidades del sistema y dispositivos externos como memorias USB.

7. **¿Como se comporta un troyano?**

Se disfraza de programa legítimo para engañar al usuario e instalarse en el sistema. Una vez dentro, permite el acceso remoto al ciberdelincuente o roba información personal y contraseñas.

8. **¿Qué es el espionaje industrial?**

Es la obtención ilegal de información confidencial de una empresa (como proyectos, fórmulas o estrategias) con el objetivo de obtener ventajas competitivas o perjudicar a la competencia.

9. **¿Qué entiende por ciberdelincuencia?**

Es el conjunto de delitos cometidos mediante el uso de computadoras, redes o Internet, como fraudes, robos de identidad, hackeos, distribución de malware o espionaje digital.

10. **¿Cuáles son las armas que utilizan los ciberdelincuentes?**

Usan virus, troyanos, gusanos, ransomware, keyloggers, phishing, ingeniería social y botnets, entre otras herramientas digitales para atacar o robar información.

11. **¿Dónde se centran los primeros ataques?**

Generalmente se dirigen a los puntos más vulnerables del sistema, como contraseñas débiles, correos

electrónicos, puertos abiertos, cámaras o dispositivos IoT mal configurados.

12. **¿Para qué sirve una puerta trasera?**

Una **"**backdoor" o puerta trasera permite acceder de forma oculta y no autorizada a un sistema, incluso después de que se haya cerrado una vulnerabilidad o instalada seguridad adicional.

13. **¿Qué es un keylogger?**

Es un programa malicioso que registra las pulsaciones del teclado del usuario para capturar contraseñas, mensajes o datos personales sin que este lo note.

14. **De acuerdo a la lectura, ¿Cómo se puede acceder a las cámaras vulnerables?**

Los ciberdelincuentes pueden acceder a cámaras vulnerables mediante contraseñas predeterminadas o débiles, puertos de red abiertos, o mediante malware que explota fallos en el software de las cámaras .

15. **¿Cuál es el objetivo de la ingeniería social en el ciber espionaje?**

Engañar o manipular a las personas para que revelen información confidencial, permitan el acceso a sistemas o descarguen software malicioso sin darse cuenta.

16. **De que se encargan los órganos ISAC's**

Los ISAC's (Information Sharing and Analysis Centers) se encargan de recopilar, analizar y compartir información sobre amenazas cibernéticas entre organizaciones para prevenir y responder de manera coordinada a los ataques.

17. **A que se refiere Cyberwar Playbook**

Hace referencia al conjunto de estrategias, tácticas y procedimientos utilizados por los Estados o grupos organizados en conflictos cibernéticos, es decir, una "guía" de guerra digital.

18. **¿Cuáles son los pasos que se deben realizar al detectar un ataque?**

Detectar y confirmar la amenaza.

Aislar los sistemas afectados para evitar la propagación.

Analizar el tipo y origen del ataque.

Notificar a los responsables de seguridad o autoridades competentes.

Mitigar el daño aplicando parches o restaurando respaldos.

Documentar y prevenir futuros incidentes mejorando la seguridad.

Preguntas de la lectura "EL CIBERESPIONAJE Y LA CIBERSEGURIDAD"