Act.14 – Ingeniería Social (el arte del engaño) – CNO V. Seguridad Informática

Nombre: JUAN ALEJANDRO PÉREZ VENTURA - 180370 **(#23)**
Fecha: 15/04/2026 Calif: _____

1. **¿Cuál fue el principal vector de ataque utilizado por Lam Malone?**
   Ingeniería social.
2. **¿Qué principio psicológico explotó para lograr transferencias millonarias?**
   La urgencia y la confianza.
3. **¿Qué tipo de ataque de ingeniería social se identifica en este caso?**
   Phishing y vishing.
4. **¿Qué debilidad de seguridad informática facilitó el fraude?**
   La exposición de datos críticos.
5. **¿Cómo complementaban Chetal Veer y Serrano Jeandiel el ataque iniciado por Lam?**
   Con llamadas fraudulentas y el acceso remoto.
6. **¿Cuál fue el resultado económico total del esquema fraudulento?**
   4,100 bitcoins (238 millones de dólares).
7. **¿Qué evento marcó el punto de quiebre del caso?**
   La filtración del video, y el despilfarro de Malone visto en redes sociales.
8. **¿Qué evidencia física encontraron las autoridades al detener a Chetal Veer?**
   Coches de lujo, relojes y artículos caros.
9. **¿Qué decisión tomó Chetal Veer frente al proceso judicial?**
   Se declaró culpable de fraude y lavado de dinero.
10. **¿Qué consecuencias legales enfrenta el grupo por estos hechos?**
    Penas de prisión, decomiso de bienes y multas grandes.
11. **¿Qué empresas fueron suplantadas durante el ataque?**
    Google y Gemini.
12. **¿Qué herramienta de acceso remoto fue utilizada para comprometer a la víctima?**
    AnyDesk.
13. **¿Qué acción realizaron inmediatamente después del robo para ocultar los fondos?**
    Movieron el dinero a otras plataformas para lavarlo.
14. **¿Quién contribuyó al rastreo de las transacciones y exposición del caso?**
    ZachXBT.
15. **¿Cuál fue el detallito que tuvo con Skylar Harrison?**
    Un bolso Birkin de Hermes.