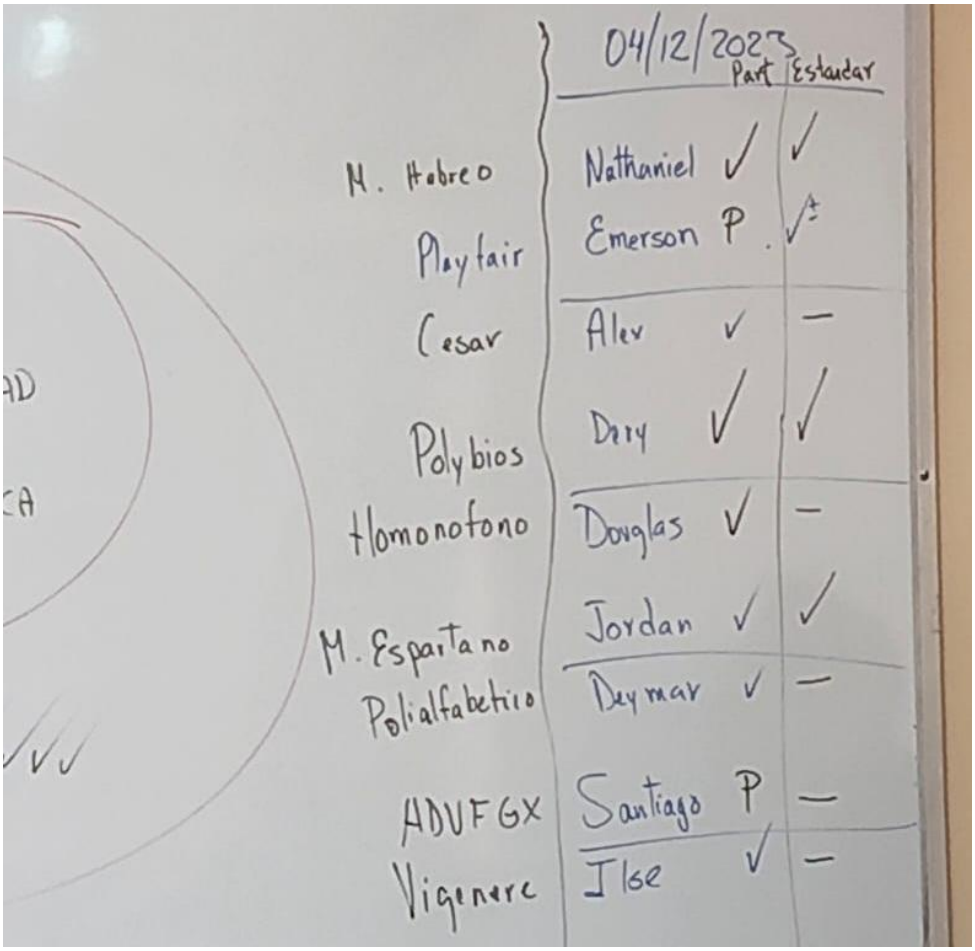
INFORME DE LA ACTIVIDAD

Actividad	Participación semana 2
Nombre del Estudiante	Alex Reynaldo Copa Catari
Nro. de celular	73574893

Lunes 4 de diciembre

Comenzó con un control de lectura de la criptografía clásica, donde los estudiantes fueron asignados para explicar el funcionamiento de un método de cifrado elegido.

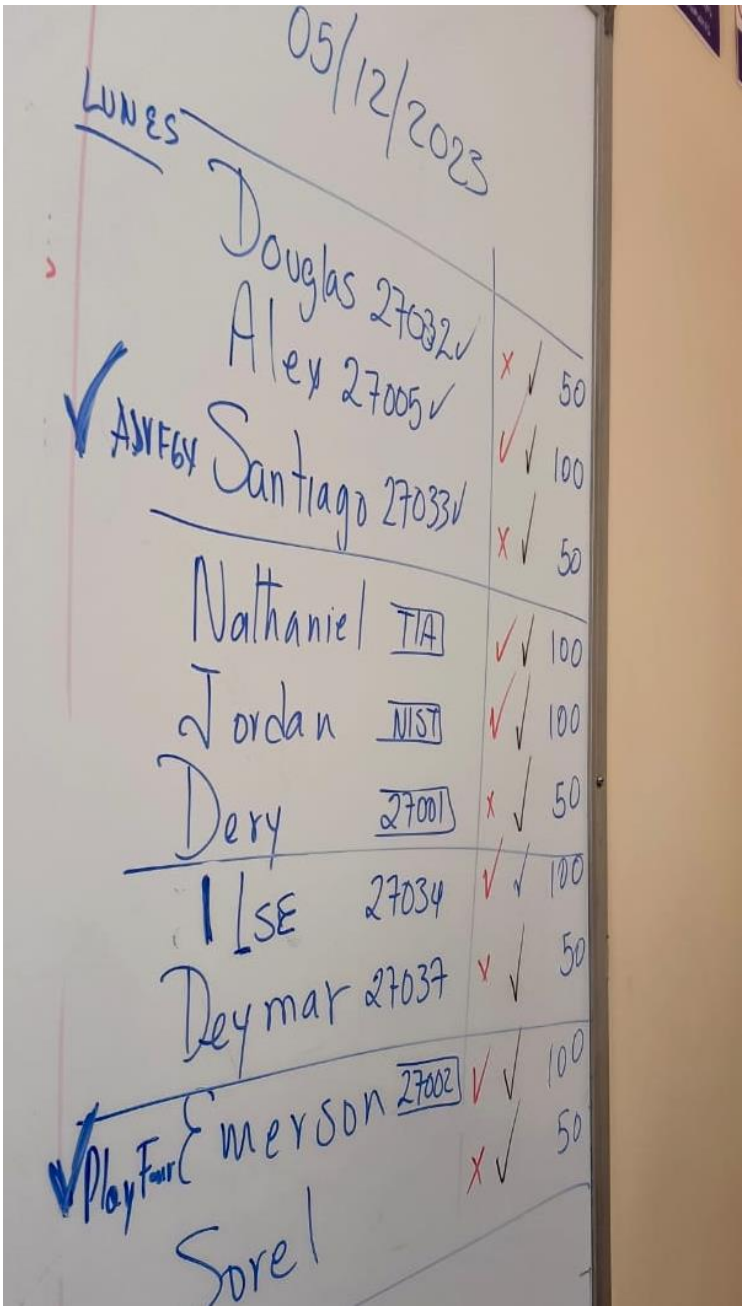
La participación que hice fue explicar el método de cifrado de César, utilizado por el general Julio César para comunicarse con sus tropas. Este método consiste en desplazar cada letra del alfabeto tres posiciones hacia adelante. Por ejemplo, la letra A se convierte en la D, y así sucesivamente. También expliqué las variantes del cifrado de César, que incluyen cifrado con el alfabeto inverso, cifrado circular y cifrado con desplazamiento inverso. Para explicar estas variantes, utilicé mi nombre como ejemplo.



Martes 5 de diciembre

Comenzó con la defensa de las normas asignadas a los estudiantes, seguido por la explicación de tema de las vulnerabilidades. Se elaboró un cuadro comparativo de clasificación de vulnerabilidades

Explique sobre la norma que se me asigno la norma ISO 27005, explicando su propósito y cláusulas. En las investigaciones en grupos de tres, se creó un cuadro comparativo sobre clasificaciones de vulnerabilidades, donde el grupo seleccionado debía responder preguntas relacionadas con su cuadro. En mi caso, mi pregunta fue relacionados con fallos en la gestión de encriptación. La otra investigación fue los tipos de hackers, y me correspondió hablar sobre los "Script kiddies", individuos con conocimientos limitados que buscan herramientas desarrolladas y automatizadas, sin motivaciones serias, realizando sus acciones por diversión.

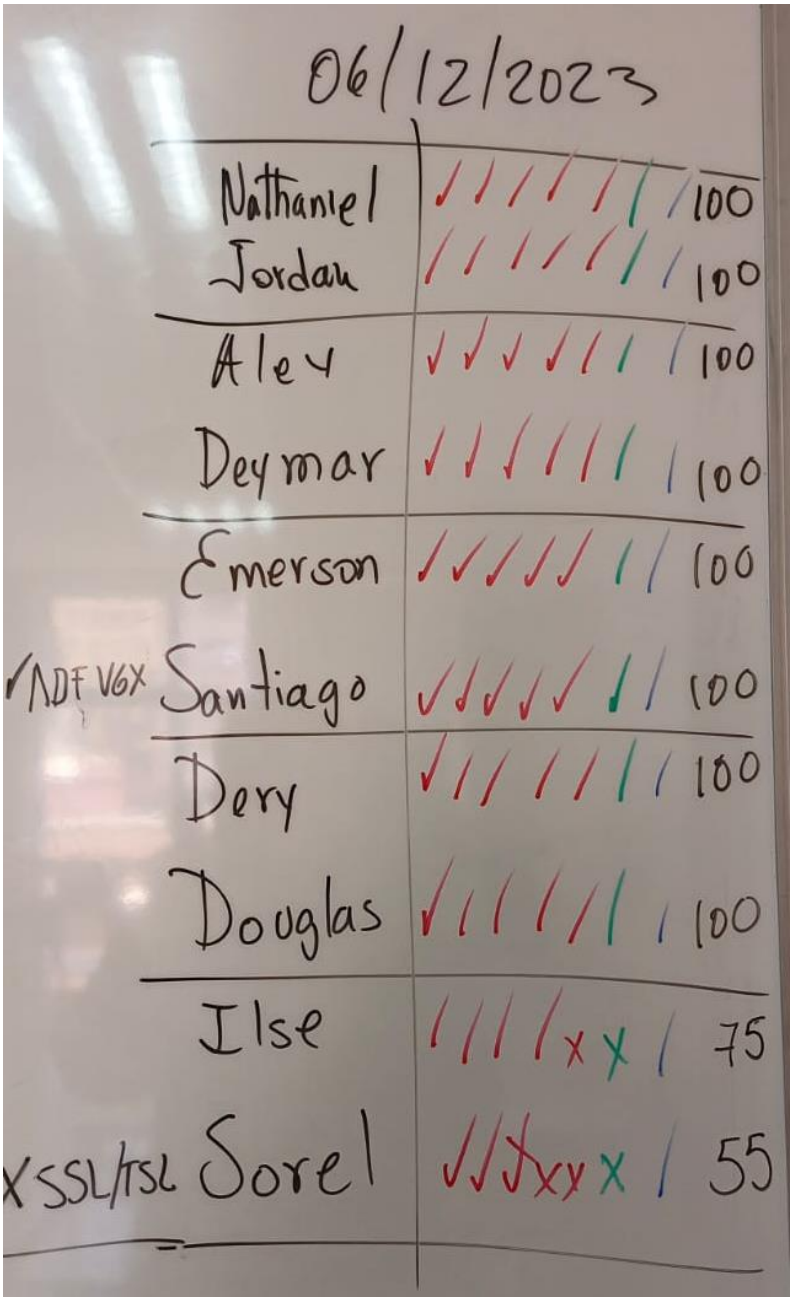


Miércoles 6 de diciembre

Comenzó con 5 ejercicios prácticos con métodos criptográficos realizados en Excel o en hojas de papel, seguidos por la continuación de la explicación del tema 2, que abordó los tipos de virus y las fases de ataque a un sistema.

En parejas, se realizaron ejercicios prácticos de métodos de cifrado, siendo obligatorios los métodos Vigenère, Atbash hebreo y ADFGVX, mientras que los otros dos, en mi grupo, fueron el método de César y Polybios. Estos ejercicios se compartieron en un grupo de WhatsApp y fueron revisados por la docente.

La investigación consistió en la búsqueda de ejemplos de virus en la vida real, donde me centré en el ransomware, destacando el caso conocido de WannaCry que afectó a diversas organizaciones en 2017. Este ransomware explotó una vulnerabilidad en el sistema operativo Windows llamada EternalBlue, cifrando archivos y exigiendo un pago en Bitcoin para la clave de descifrado. Aquellos que no pagaron sufrieron la pérdida permanente de sus datos. La otra investigacion se centró en las fases de ataque, y mi grupo explicó las fases de reconocimiento, entrada, explotación, instalación, elevación de privilegios, movimiento lateral, recopilación de información, encubrimiento y mantenimiento de acceso.



Jueves 7 de diciembre

Mientras se terminaba el tema, se realizaban participaciones sobre ataques informativos, herramientas de protección y explicación acerca de las vulnerabilidades y riesgos.

Participé en la explicación de un ataque específico; en mi caso, fue el ataque global de ransomware Petya. Inicialmente, se disfrazó como un secuestro de archivos con el fin de obtener rescates, pero su verdadero propósito era causar daño y desestabilizar organizaciones en diversas industrias. Afectó a grandes corporaciones y entidades gubernamentales en Europa, Asia y América del Norte.

La segunda participación consistía en nombrar y explicar una herramienta de protección, que en mi caso fue el Nmap. Este es un instrumento de escaneo de red que permite descubrir dispositivos y servicios, así como evaluar la seguridad de una red. La tercera participación se centró en la explicación de la gestión de riesgos. En nuestro grupo, abordamos los conceptos y aspectos relacionados con la planificación y gestión de riesgos, así como técnicas para identificar los riesgos. También discutimos la creación de registros de riesgos, donde se especifican varios campos al identificar un riesgo.