Arquitectura y S.O.

CLASE 8

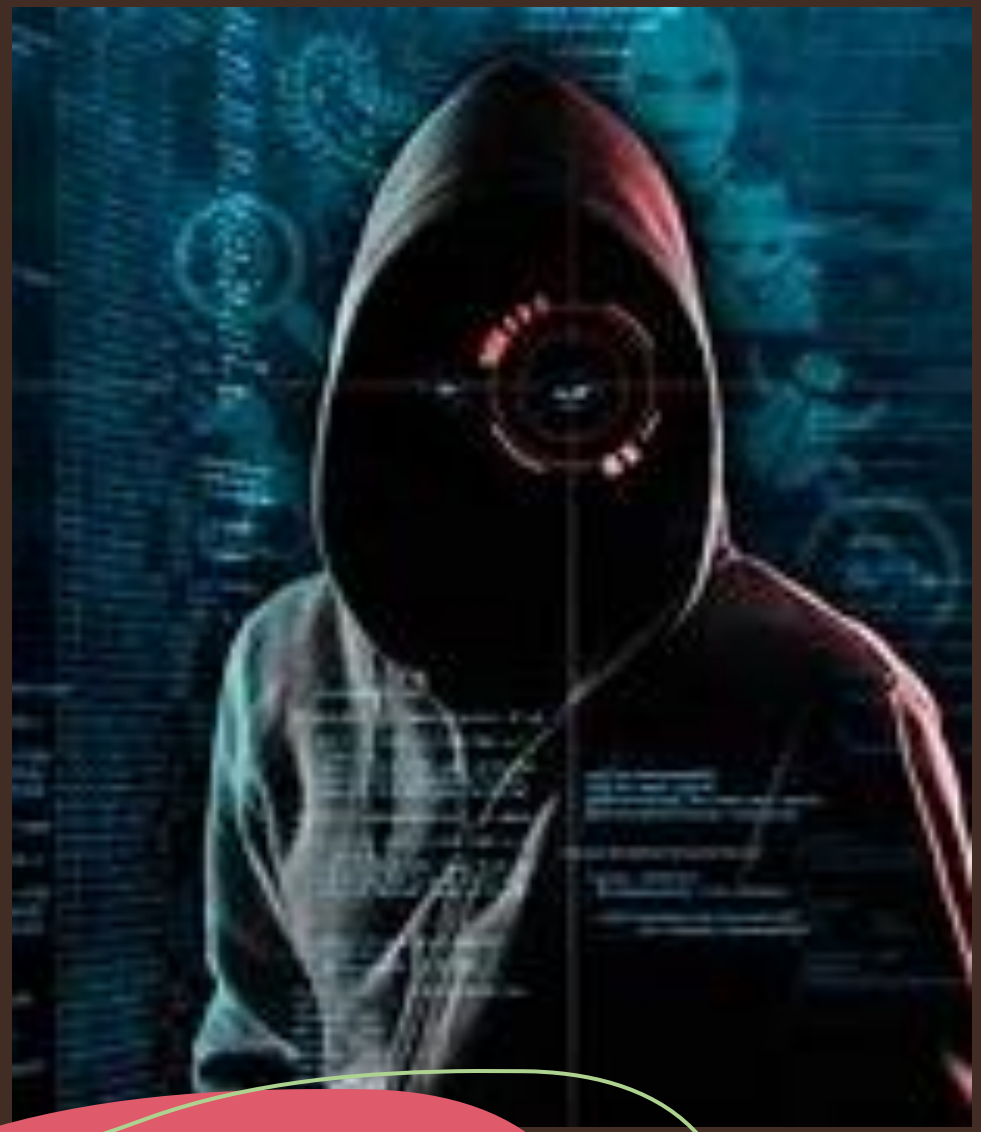
PROF. Natalia Lucero

CiberSeguridad

- Amenazas cibernéticas comunes

Ataques de intermediario

- Los ataques de intermediario son ataques de espionaje, en los que un ciberdelincuente intercepta y transmite mensajes entre dos partes para robar datos. Por ejemplo, en una red Wi-Fi no segura, un atacante puede interceptar los datos que se transmiten entre el dispositivo del invitado y la red.

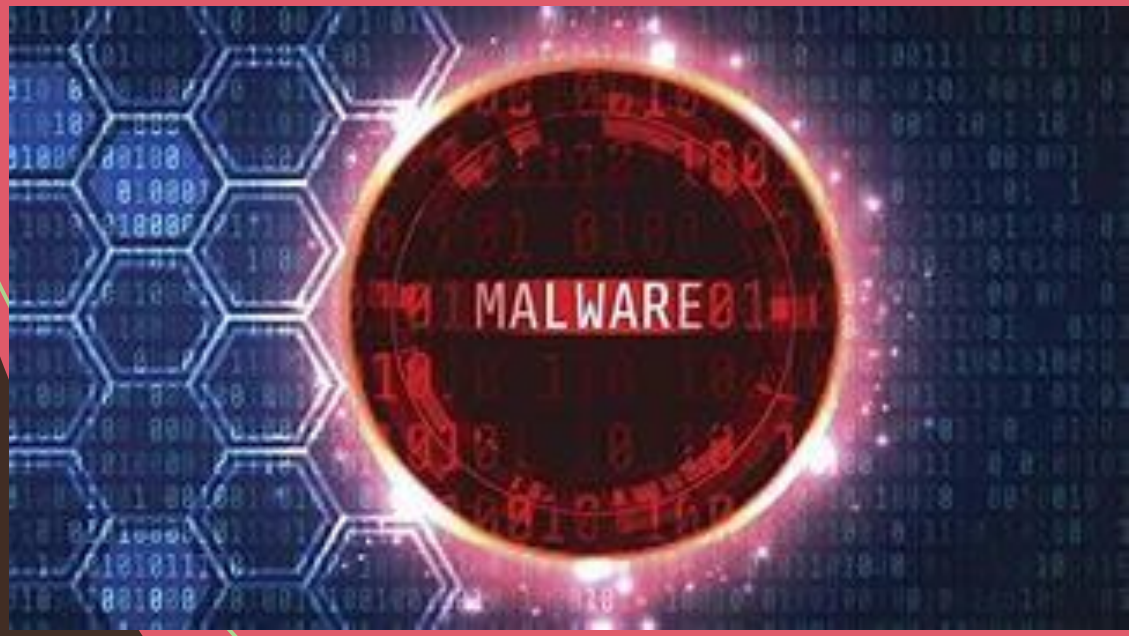


Soluciones de IA para la ciberseguridad

- A medida que los ciberataques crecen en volumen y complejidad, la inteligencia artificial (IA) está ayudando a los analistas de operaciones de seguridad con recursos insuficientes a anticiparse a las amenazas. Las tecnologías de inteligencia artificial, como el machine learning y el procesamiento del lenguaje natural, seleccionan la inteligencia de amenazas de millones de artículos de investigación, blogs y noticias, y brindan insights rápidos para deshacerse del ruido de las alertas diarias, lo que reduce drásticamente los tiempos de respuesta.
-

Malware

- El término "malware" se refiere a variantes de software malicioso, como gusanos informáticos, virus, troyanos y programas espía, que brindan acceso no autorizado o causan daños a una computadora. Los ataques de malware son cada vez más "sin archivos" y están diseñados para evadir métodos de detección familiares, como herramientas antivirus, que escanean archivos adjuntos maliciosos.



Ransomware

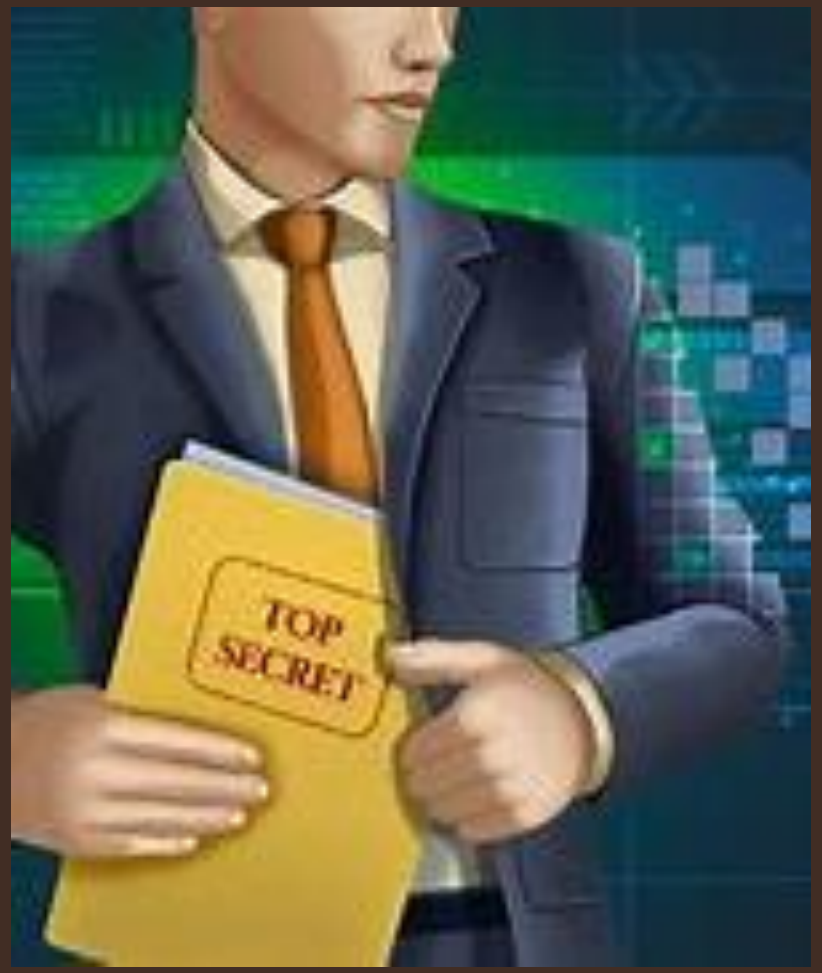
- Es un tipo de malware que bloquea archivos, datos o sistemas y amenaza con borrar o destruir los datos, o hacer que los datos sean privados o confidenciales al público, a menos que se pague un rescate a los ciberdelincuentes que lanzaron el ataque.
- Los recientes ataques de ransomware se han dirigido a los gobiernos estatales y locales, que son más fáciles de vulnerar que las empresas y están bajo presión para pagar rescates con el fin de restaurar aplicaciones y sitios web de los que dependen los ciudadanos.

Estafas por correo electrónico / ingeniería social

- Las estafas por correo electrónico son una forma de ingeniería social que engaña a los usuarios para que proporcionen su propia PII o información confidencial. En este tipo de estafa, los correos electrónicos o mensajes de texto parecen provenir de una empresa legítima que solicita información confidencial, como datos de tarjetas de crédito o información de inicio de sesión. El FBI ha notado un aumento en las estafas por correo electrónico relacionadas con la pandemia, vinculado al crecimiento del trabajo remoto.

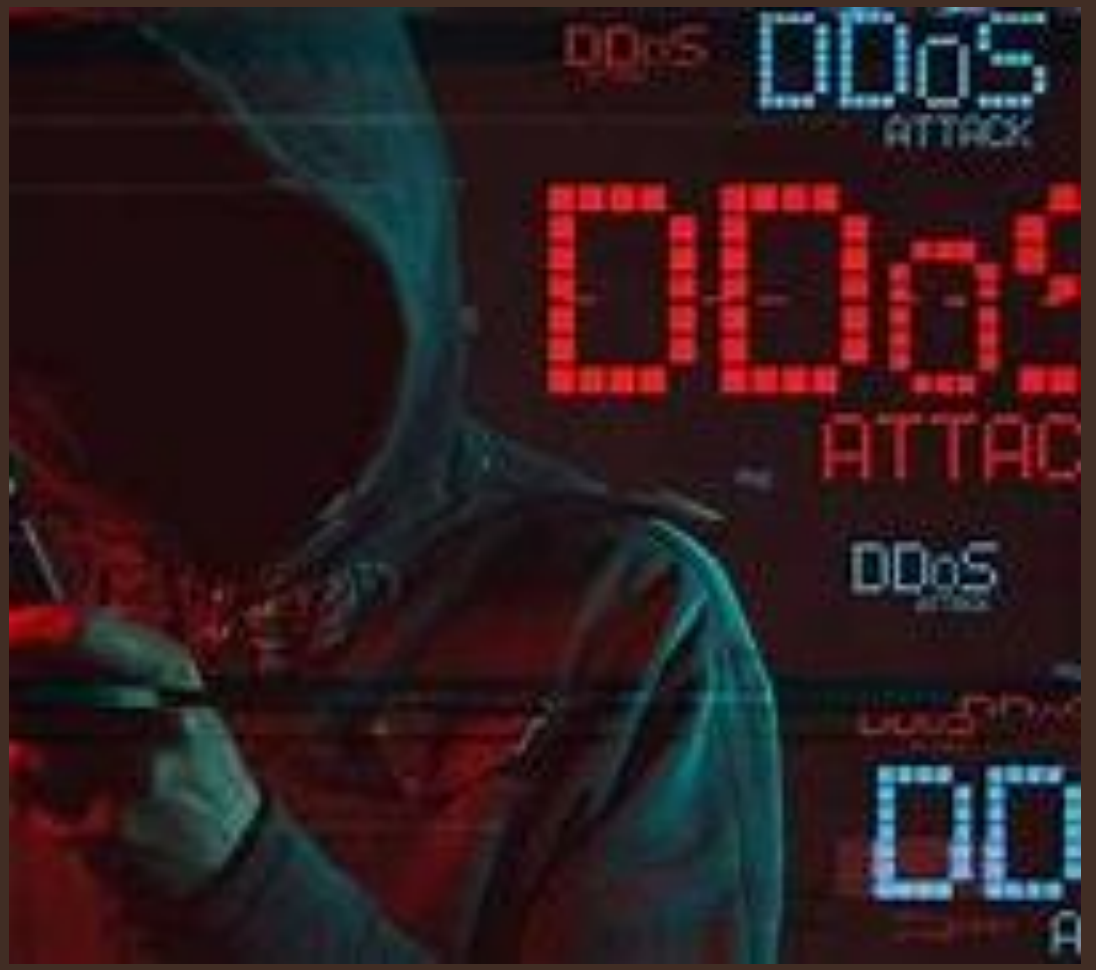
Amenazas internas

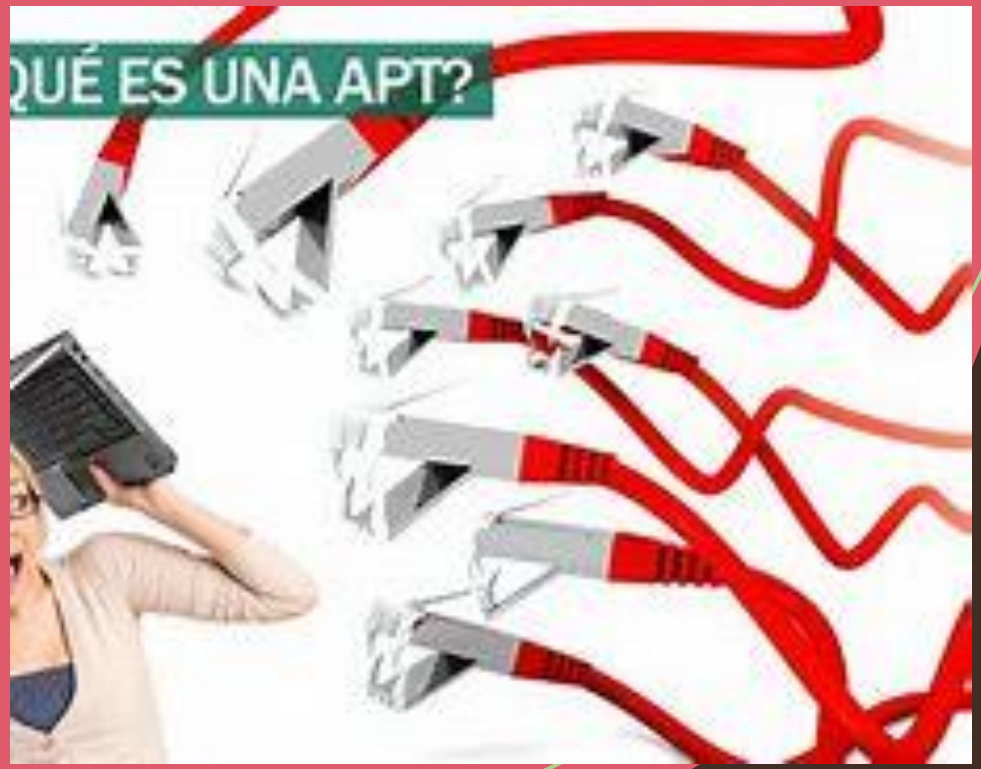
- Los empleados actuales o anteriores, socios comerciales, contratistas o cualquier persona que haya tenido acceso a sistemas o redes en el pasado se pueden considerar una amenaza interna si abusan de sus permisos de acceso. Las amenazas internas pueden ser invisibles para las soluciones de seguridad tradicionales como firewalls y sistemas de detección de intrusos, que se enfocan en amenazas externas.



Ataques de denegación de servicios distribuidos (DDoS)

- Un ataque DDoS intenta bloquear un servidor, sitio web o red sobrecargándolo con tráfico, generalmente de múltiples sistemas coordinados. Los ataques DDoS abruman las redes empresariales a través del protocolo simple de administración de red (SNMP), que se utiliza para módems, impresoras, conmutadores, routers y servidores.





Amenazas persistentes avanzadas (APT)

- En una APT, un intruso o un grupo de intrusos se infiltra en un sistema y permanece sin ser detectado durante un período prolongado. El intruso deja las redes y los sistemas intactos para poder espiar la actividad empresarial y robar datos confidenciales mientras evita la activación de respuestas defensivas. La reciente brecha de seguridad de Solar Winds de los sistemas del gobierno de los Estados Unidos es un ejemplo de una APT.

Tecnologías clave y mejores prácticas de ciberseguridad

- La Gestión de identidad y acceso (IAM)
- Una plataforma de seguridad de datos integral
- La gestión de eventos e información de seguridad (SIEM)

La Gestión de identidad y acceso (IAM)

- Define los roles y privilegios de acceso para cada usuario, así como las condiciones bajo las cuales se le otorgan o niegan sus privilegios. Las metodologías IAM incluyen el inicio de sesión único, que permite a un usuario iniciar sesión en una red una vez sin volver a ingresar las credenciales durante la misma sesión; autenticación multifactor, que requiere dos o más credenciales de acceso; cuentas de usuario privilegiadas, que otorgan privilegios administrativos solo a ciertos usuarios; y gestión del ciclo de vida del usuario, que gestiona la identidad y los privilegios de acceso de cada usuario desde el registro inicial hasta el término. Las herramientas de IAM también pueden brindar a sus profesionales de ciberseguridad una visibilidad más completa de la actividad sospechosa en los dispositivos de los usuarios finales, incluidos los puntos finales a los que no pueden acceder físicamente. Esto ayuda a acelerar los tiempos de investigación y respuesta para aislar y contener el daño de una brecha de seguridad.

Una plataforma de seguridad de datos integral

- Protege la información confidencial en varios entornos, incluidos los entornos multinube híbridos. Las mejores plataformas de seguridad de datos brindan visibilidad automatizada y en tiempo real de las vulnerabilidades de los datos, así como supervisión continua que alerta sobre las vulnerabilidades y los riesgos de los datos antes de que se conviertan en brechas de seguridad; también deben simplificar la conformidad regulatoria de la privacidad de datos del gobierno y de la industria. Las copias de seguridad y el cifrado también son vitales para mantener los datos seguros.

La gestión de eventos e información de seguridad (SIEM)

- Agrega y analiza datos de eventos de seguridad para detectar automáticamente las actividades sospechosas de los usuarios y desencadenar una respuesta preventiva o correctiva. Actualmente, las soluciones SIEM incluyen métodos de detección avanzados como la analítica del comportamiento del usuario y la inteligencia artificial (IA). La SIEM puede priorizar automáticamente la respuesta a las amenazas cibernéticas de acuerdo con los objetivos de gestión de riesgos de su empresa. Y muchas organizaciones están integrando sus herramientas SIEM con plataformas de orquestación, automatización y respuesta de seguridad (SOAR) que automatizan y aceleran aún más la respuesta a incidentes de ciberseguridad y resuelven muchos sin intervención humana.

Actividad:

- 1- Realizar cuestionario para la asistencia en el campus
- 2-Solo leer el material y ver videos