Informe Seguridad e Integridad de Sistemas

Consigna:

El objetivo de este trabajo es realizar una investigación exhaustiva de una entidad o empresa seleccionada, con el fin de recopilar información sensible de acceso público que puedan ser utilizados en potenciales ciberataques.

La semana del 16 al 19 de Octubre deben entregar la primera versión del informe en modalidad **Share via drive**, teniendo en cuenta el **principio de mínimo privilegio**. El docente entregará las correspondientes correcciones en el documento

En la semana del 6 al 9 de noviembre los estudiantes entregarán la segunda versión, con las correcciones ya realizadas.

En la semana del 13 al 16 de noviembre, Si no se cumplió con los requisitos mínimos del informe, además de corregir lo que indique el profesor, deben responder cuestionario en el aula virtual.

Minimos requisitos:

Se cumplen al pie de la letra las entregas

Se respeta el principio de mínimo privilegio

Se aplica metodologia OSINT

Incluir Matriz de Riesgo (3*3 o 5*5)

El trabajo es Grupal(mínimo 3 personas)

Los grupos deben estar deben estar definidos y el objetivo o entidad elegida antes del 28 de septiembre (los grupos y el objetivo o entidad elegida por cada uno estan en la planilla que dejó disponible el ayudante de cátedra, de tener dudas contacto directamente)

Estructura del Informe

- **Introducción:**
  - Breve descripción de lo investigado en el presente trabajo.
  - Propósito de la investigación y su relevancia en el contexto de la seguridad informática.

- **Alcance:**
  - Definición de los límites y alcance de la investigación.

- **Sobre el Objetivo:**
  - Descripción detallada de la entidad o empresa seleccionada.
  - Justificación de la elección del objetivo.

- **Metodología: (OSINT)**
  - Explicación de las herramientas y técnicas utilizadas para la recopilación de datos.
  - Procedimientos seguros y éticos para llevar a cabo la investigación.

- **Recopilación de Datos Sensibles:**
  - Correos electrónicos encontrados.
  - Posibles empleados identificados.
  - Ubicación geográfica de la entidad o empresa.
  - Análisis del dominio y subdominios asociados.
  - Identificación de perfiles de redes sociales relacionados con la entidad.
  - Mención de autoridades de la entidad.
  - Investigación de la metadata de los archivos disponibles en la pagina web
  - Archivos descargables por tipo.
- **Análisis de la Información**
  - Cruzar los datos obtenidos de las distintas herramientas utlizadas para obtener información de calidad que podria representar riesgo para la entidad elegida. Por ejemplo:
    - Personal de la empresa: (Por ejemplo con diferentes enumeradores de perfiles de linkedIn y enumeradores de perfiles de correos electrónicos)
      - Unificar en una sola planilla excel los datos obtenidos con las distintas herramientas para tener al menos:
        - Nombre
        - Apellido
        - Posible correo electrónico
        - RRSS (IG, FB, TW…)
        - GITHUB
        - Cargo
        - Validar si esta su correo corporativo en I have been…
      - Identificar y justificar los perfiles de alto riesgo
    - Software: (por ejemplo con FOCA)
      - Obsolescencia del software identificado
        - Buscar en CVE detalis las vulnerabilidades

            - Verificar si es la última versión o si ya no tiene soporte
        - Unificar los datos en una sola planilla que tenga al menos:
            - Nombre del software
            - Versión
            - Posibles vulnerabilidades asociadas (ver en CVE detalis)
        - Riesgo de fuga de informaciòn
            - por ejemplo si detectan el uso de PDF creator o similar
    - RRSS
        - RRSS sin moderación
        - Sin soporte a los usuarios
    - Entorno geográfico
        - Verificar si hay compartido información que pueda poder en riesgo a la entidad Por ejemplo:
            - accesibilidad
            - informciòn sensible disponible en opiniones de google
    - Información confidencial o sensible
        - Información disponible en internet con datos confidenciales y/o sensibles por ejemplo:
            - Datos personales
            - Datos que puedan identificar a las personas
    - Riesgos reputacionales
        - Información que pueda poner en riesgo la reputación de la empresa o entidad, justificada.
    - Riesgo de las RRSS
        - Falta de moderación de las rrss.
        - No es solo enumerar las redes sociales sino también identificar riesgos asociados y como un ciberdelincuente podría usar esa información en contra de la entidad
    - Análisis del sitio web
        - Validar con sitios como security header o similares la configuración de sitios e identificar sus vulnerabilidades
    - Análisis de los dominios y subdominios
        - De los dominios y subdominios obtenidos, identificar lso riesgos asociado a los mismos y cuales son de mayor riesgo. Justificar

- **Matriz de riesgo**
    - Debe contener de todos los hallazgos encontrados cuales son los riesgos asociados según la probabilidad de ocurrencia y el impacto (utilizar criterio visto en clase y justificar en base a la evidencia encontrada)
- **Recomendaciones:**
    - Sugerencias para mejorar la seguridad de la entidad o empresa basadas en los hallazgos y en lo visto en clase

- **Conclusiones:**
    - Resumen de los resultados y hallazgos más relevantes.
    - Reflexión sobre la importancia de proteger los datos sensibles