Trabajo Práctico 1

Introducción a la seguridad

Grupo: G06

Integrantes:

Nombre	Padrón
Pedro Flynn	105742
Agustina Schmidt	103409
Agustina Fraccaro	103199
Kevin Gadacz	104531
Abraham Osco	102256
Ricardo Luizaga	87528

Lectura del artículo, Análisis de Stuxnet y dimensiones de seguridad

Artículo a leer: Stuxnet explained: The first known cyberweapon

https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

Actividad a Realizar:

1) **Realizar un informe de los eventos, la naturaleza del ataque y las implicaciones de Stuxnet.**

Stuxnet es un “gusano informático” creado por los equipos de inteligencia de EEUU en conjunto con Israel para atacar y retrasar la producción de armas nucleares de Irán, en particular, las centrifugadoras de uranio.

Este virus, una vez dentro de una computadora conectada a una centrifugadora, se encargaba de vulnerar 4 bugs de Windows que aún no habían sido detectados, para aleatorizar los giros de las centrifugadoras, y así deteriorar las máquinas.

A continuación detallamos los eventos claves, la naturaleza del ataque y las implicancias del mismo

Eventos:

1. Desarrollo: Por los gobiernos de los EE.UU. e Israel como parte de la operación “Olympic Games”.
2. El objetivo principal era retrasar el programa iraní de armas nucleares.
3. Detectado en 2010 tras propagarse fuera de su objetivo original, lo que llevó a su análisis por expertos en ciberseguridad.

Naturaleza del Ataque:

1. Explotó múltiples vulnerabilidades de día cero en Windows.
2. Utilizó certificados digitales robados para firmar controladores maliciosos.
3. Diseñado para ser introducido a través de dispositivos USB en sistemas aislados.
4. Dejaba inoperativas las centrifugadoras, causaban su mal funcionamiento mientras enviaba señales falsas de éxito a los operadores.
5. La propagación rápida e indiscriminada de una máquina a otra en una red interna.

Implicancias del ataque:

1. Demostró que el código informático puede causar daños físicos significativos.
2. Logro dañar aproximadamente 2000 centrifugadoras iraníes
3. Se estima que retraso el programa nuclear irani en al menos dos años
4. Aumentó la conciencia sobre la necesidad de proteger sistemas aislados.
5. Impulsó el desarrollo de nuevas herramientas y métodos de detección y análisis de amenazas avanzadas.

2) Elaborar un análisis crítico y reflexivo que integre los conceptos de seguridad vistos en clase con el caso específico de Stuxnet.

a) Analizar el tema presentado en el artículo buscando relaciones con los temas discutidos en la materia. Aplicar por ejemplo las dimensiones de seguridad: confidencialidad, disponibilidad, integridad, autenticación, no repudio y control de acceso, según se presenten en el caso de Stuxnet.

La respuesta a este apartado puede contener párrafos, gráficos o imágenes. Se pide no superar las 400 palabras.

Con la creación del malware Stuxnet se logró reconocer que atacando las dimensiones de la seguridad pueden tener grandes daños en el proyecto.

- **Autenticación:** se viola usando utilizando certificados de clave privados robados
- **Integridad:** se viola dando falsos positivos de que está disponible y el sistema funciona, cuando en realidad las centrífugas se están destruyendo en el proceso.
- **Disponibilidad:** el aumento de los ataques a las centrífugas provocó que haya menor cantidad de centrífugas operantes. Esto afectó gravemente la capacidad operativa de la planta nuclear, un aspecto crítico en cualquier infraestructura.
- **Control de acceso:** se viola debido a la capacidad del rootkit que permite al malware ejecutarse en modo kernel, esto fue posible ya que Stuxnet explotó múltiples ataques de día cero de Windows.
- **No repudio:** aunque no hay un caso claro de no repudio explícito, el uso de certificados robados y la complejidad del código de Stuxnet sugiere que los atacantes intentaron ocultar quién realizó el ataque, lo que indirectamente impacta este principio ya que al no poder identificar fácilmente al autor del ataque, se socava la capacidad de asegurar la responsabilidad y el no repudio de la acción maliciosa.
- **Confidencialidad:** Stuxnet no se centró en robar información, pero si impactó la confidencialidad dado que atacó sistemas industriales críticos que generalmente están aislados de las redes externas, lo que demuestra una vulneración de la confidencialidad de los sistemas que deberían haber sido inaccesibles. Esto quiere decir que en caso de haber querido robar información, podría haberlo hecho sin ser detectado, esto deja en evidencia la falta de controles estrictos en la confidencialidad del sistema.

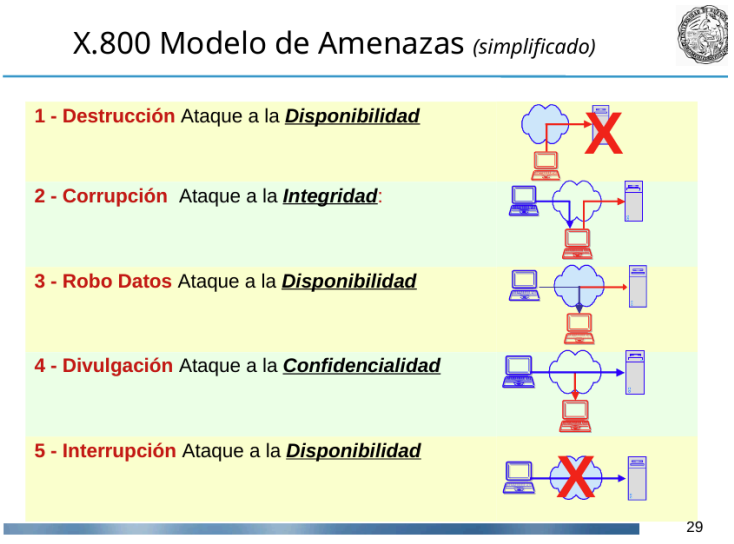
Actividad 2

El artículo elegido es “Cómo robar cuentas de ChatGPT con “Wildcard Web Cache Deception”.

El usuario de github “Nokline”, mediante un programa de recompensas por vulnerabilidades llamado “Bug Bounty”, recibió 6500 USD por encontrar un método para robar cuentas de ChatGPT gracias a un error de Cache del CDN en una feature nueva de OpenAI.

En el post de su blog acerca del ciberataque, explica que la vulnerabilidad se encontraba en un nuevo feature de OpenAI que permite compartir los chats, los cuales se guardaran en el Cache, es decir, que una URL es parseada 2 veces, una por la CDN de Cloudflare y otra por la web server. El atacante descubrió que si bien la web server decodificaba y normalizaba los URLs previniendo un ataque mediante path traversal (un tipo de ataque que, modificando URLs que acceden a una Api, permiten obtener archivos e imágenes privadas de una App). La CDN de Cloudflare no lo hacía, por lo que se podía acceder a data sensible de otros usuarios (como el auth token) mediante este modo.

Según lo visto en la clase de introducción a Seguridad informática, podríamos decir que se vulneran algunas dimensiones de seguridad. Vamos a destacarlas.



- **Autenticación**: El atacante consigue el auth token de otros usuarios, que le permite loguearse como si fueran ellos.
- **Confidencialidad**: Accediendo al Auth token de un usuario, podría acceder a sus chats privados que podrían contener información sensible como datos personales e información bancaria.
- **Control de Acceso** y **Privacidad** por las razones previamente mencionadas.

Además, el próximo diagrama que mostró el propio atacante, lo asociamos al Modelo de Amenazas de ***Divulgación***, que implica un ataque a la ***Confidencialidad.***