Examen ciberseguridad

Ramírez Fuentes Edgar Alejandro

Escriba qué es un hacker

En el ámbito de la ciberseguridad es aquella persona que se encarga de estudiar y conocer profundamente para ser capaz de modificarlo o alterarlo con buenas o malas intenciones (depende del tipo de hacker).

Escriba qué es un ciberdelincuente?

Basado en la respuesta anterior, el ciberdelincuente es aquel que toma ventaja del conocimiento para generar un daño a un sistema informático, en algunas ocasiones es para beneficio propio.

¿Qué es un ciberataque?

Es toda aquella acción que se realiza contra sistemas informáticos con el objetivo de impedir su correcto funcionamiento o extraer información de los mismos. Los ciberataques afectan tanto a los sistemas informáticos como a la información, y sus consecuencias pueden ser de extrema gravedad.

¿Qué es el malware y qué tipos hay?

Malware es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Algunos tipos de malware son: - Ransomware - Virus - Gusanos - Troyanos - Spyware - Scareware - Adware

Diferencia entre el virus y el gusano

Existen varias diferencias entre estos tipos de malware, pero las más significativas son las siguientes: - Los gusanos se propagan por medio de redes informáticas, mientras que los virus lo hacen por medio de archivos ejecutables. - Los gusanos dañan los recursos, mientras que los virus destruyen los archivos del ordenador. - Los virus no necesitan la intervención de ningún ser humano, los gusanos sí.

¿Qué tipo de hacker son?

- Richard Stallman:
  - White hat
- Captain Crunch:
  - Black hat
- Kevin Mitnick :
  - Antes Black hat
  - Actualidad White hat
- Linus Torvalds

  - White hat
- George Hotz
  - Antes Black hat
  - Actualidad Lo pondría como un Gray hat porque debido a sus acciones realizadas con productos Sony y Apple, colaboró en Project Zero de Google para encontrar vulnerabilidades en Internet, pero no estoy seguro de que sus acciones sean bien intencionadas.
- Tim Berners-Lee
  - White hat
- Kevin Poulsen
  - Black hat
- Tsutomu Shimura
  - White hat

Investigue los hechos ocurridos respectos a los casos

- STUXNET
  - Este evento es uno de los grandes, esto debido a que nos mostró lo peligroso que puede llegar a ser un ciberataque bien organizado. Los hackers creadores de este malware (que se tiene cree que fue producto de estados unidos e israel) lograron infectar máquinas de la central nuclear Natanz, en irán, para hacer que estas se sabotearan solas para retrasar el programa nuclear iraní. En este caso se logró que se sabotearan las centrifugadoras de esta planta, pero debemos de estar conscientes de que eso pudo llegar más lejos, y lo más impresionante es que logró infectar máquinas.
- WannaCry
  - Este evento me dejó muchos aprendizajes y cosas en las cuales pensar. Una de las principales es que el gobierno, en especial de los Estados Unidos, siempre tiene recursos para poder investigar a la sociedad, y un ejemplo de esos recursos es la base de datos de vulnerabilides dentro de sistemas informáticos que fue protagonista en la realización de este malware. Este suceso nos permitió al mundo saber que tan vulnerables estamos ante una falla de seguridad informática llegando a afectar a hospitales con pocos recursos para invertir en seguridad informática y así no poderse defender ante este malware. Un caso muy conocido, y aún así en la sociedad seguimos sin prestar atención ante este tipo de vulnerabilidades que nos pueden afectar a todos.
- SolarWinds:
  - Este tema me intrigó por lo comentado en clase, debido a que este tipo de ataque tiene el objetivo principal del desprestigio hacia una empresa lider. Obviamente hubieron más objetivos implícitos, pero como se mencionó en clase uno de los objetivos era el desprestigio y me pone a pensar que nosotros como usuarios comunes debemos de tomar muchas precauciones en cuanto a nuestra seguridad de la información y seguridad informática para en la medida de lo posible

decrementar la posibilidad de ser vulnerados.

Investigue y clasifique

- MEMZ
  - Troyano
- RYUK
  - Ramsomware
- BonziBuddy
  - Spyware y Adware
- ILOVEYOU
  - Gusano

¿Qué es una botnet?

Una botnet es una red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques de denegación de servicio distribuido (DDoS) sin el conocimiento o el consentimiento de los propietarios reales de los equipos.

¿Qué medidas piensa tomar para mejorar su ciberseguridad o la de su familia?

- Verificar la fuente de los documentos que me sean enviados por correo
- Evitar aquellos enlaces maliciosos que posiblemente sean Phishing para la obtención de información personal.
- Evitar descargar software de sitios no seguros para evitar obtener cualquier tipo de malware.
- Informar a mis seres queridos de las técnicas que los podrían compremeter para que no sean víctimas de ciberdelitos.
- Informarme más con respecto al tema y aplicar esos conocimientos a mis desarrollos y a mi vida diaria.
- Activar el Multifactor authorization en mis cuentas para mantener una barrera más en ellas.
- Escoger contraseñas seguras y cambiarlas cada dos meses para asegurar mis cuentas
- No compartir información crítica en redes sociales que puedan comprometer mi seguridad y la de mi familia.

Diferencias entre seguridad de la información y ciberseguridad

La seguridad de la información se encarga de utilizar diferentes técnicas (no exclusivamente informáticas) para la protección de información, mientras que la ciberseguridad está enfocada a técnicas de protección de sistemas informáticos y la información que es alojada en estos.

Mencione 5 métodos de cifrado aún en vigencia (no vulnerados)

- AES
- RSA
- Diffie-Hellman key exchange
- SHA512
- ThreeFish