Tarea 5 Seguridad Informática Básica – Gpo. 2 Fecha de entrega: 31 /10/ 23

Equipo 4 || Integrantes:

Castelan Ramos Carlos	**317042711**
Martínez González Héctor Eduardo	**316322122**
Martínez Sánchez Berenice Vianney	**317581223**
Pineda González Rodrigo	**317224397**
Vega Alvarez Marcos	**420054432**

10

a) Investigue 20 tipos de atacantes informáticos y describa cada uno.

1. **Hacktivistas:** Un hacktivista puede ser un individuo o un grupo de hackers sin nombre cuya intención es obtener acceso a sitios web y redes gubernamentales. Los datos obtenidos se suelen utilizar para obtener beneficios políticos o sociales.

2. **Phishers:** Estos atacantes suelen utilizar correos electrónicos, mensajes de texto, sitios web falsos y otras técnicas de ingeniería social para lograr que las víctimas revelen sus datos sensibles. El término "phisher" se deriva de "phishing" y se utiliza para describir a quienes llevan a cabo este tipo de actividad maliciosa.

3. **Ransomware Operators:** Es un individuo o grupo de cibercriminales que desarrolla, distribuye y opera ataques de ransomware. Estos operadores suelen utilizar técnicas de criptografía fuerte para cifrar los datos de manera que sea extremadamente difícil o prácticamente imposible recuperarlos sin la clave de descifrado proporcionada por los atacantes. La víctima se enfrenta a la decisión de pagar el rescate o intentar restaurar sus sistemas y datos sin la ayuda de los atacantes.

4. **Spyware Distributors:** Se dedica a la distribución de programas de spyware. Estos distribuidores utilizan diversas técnicas, como anuncios engañosos o descargas de software aparentemente legítimo, para infectar dispositivos y recopilar información confidencial. Su actividad puede ser perjudicial para la privacidad y la seguridad de los usuarios.

5. **Atacantes de día cero:** Son aquellos que explotan vulnerabilidades en software que son desconocidas por el proveedor y, por lo tanto, no tienen solución o parche disponible. Estos ataques se denominan de "día cero" porque una vez que se descubre el fallo, el desarrollador o la organización dispone de "cero días" para dar con una solución.

6. **Malware Developers:** Los desarrolladores de software malicioso analizan, realizan ingeniería inversa y documentan el código fuente del malware para identificar estructuras, funciones y vulnerabilidades. Su objetivo final es explotar las debilidades utilizando sockets de software y técnicas de cifrado y ofuscación. Crean software malicioso, como virus, troyanos y ransomware, para infectar sistemas y robar datos o causar daños.

7. **Ingenieros sociales:** Son personas que manipulan a las personas para que compartan información que no deberían compartir, descarguen software que no deberían descargar, visiten sitios web que no deberían visitar, envíen dinero a delincuentes o cometan otros errores que comprometan su seguridad personal u organizacional. Lo que explota el ingeniero social es la debilidad y el error humano usando la manipulación psicológica.

8. **Hackers de sombrero negro:** Los hackers de sombrero negro, también conocidos como "black hat hackers", son individuos o grupos que utilizan sus habilidades de hacking con intenciones maliciosas y ilegales. Su actividad se centra en violar sistemas, redes y aplicaciones con el propósito de robar información confidencial, causar daño, extorsionar, cometer fraudes o realizar otras actividades ilícitas. A diferencia de los hackers de sombrero blanco que buscan mejorar la seguridad, los hackers de sombrero negro operan de manera ilegal y suelen enfrentar consecuencias legales por sus acciones.

9. **Hackers de sombrero blanco:** Los hackers de sombrero blanco, también conocidos como "ethical hackers" o "hackers éticos", son individuos que utilizan sus habilidades técnicas y conocimientos en seguridad cibernética para identificar y solucionar vulnerabilidades en sistemas, redes o aplicaciones con el permiso del propietario legítimo. Su principal objetivo es mejorar la seguridad informática, ayudando a proteger activos y datos al encontrar debilidades antes de que los ciberdelincuentes puedan explotarlas. Trabajan de manera legal y ética, a menudo como consultores de seguridad o en equipos de seguridad internos, realizando pruebas de penetración, auditorías de seguridad y proporcionando recomendaciones para fortalecer la seguridad.

10. **Hackers de sombrero gris:** Los hackers de sombrero gris, también conocidos como "ethical hackers" en algunos contextos, son expertos en ciberseguridad que utilizan sus habilidades para identificar vulnerabilidades en sistemas, redes o aplicaciones con el permiso del propietario con el fin de mejorar la seguridad. A diferencia de los hackers de sombrero negro (maliciosos) que buscan explotar debilidades, los hackers de sombrero gris trabajan de manera legal y ética para ayudar a proteger activos digitales, detectar posibles amenazas y asegurarse de que las organizaciones estén resistentes a ataques cibernéticos. Su labor incluye pruebas de penetración,

auditorías de seguridad y asesoramiento para fortalecer la defensa de sistemas y datos.

11. **Criminales cibernéticos:** Los criminales cibernéticos son individuos o grupos que utilizan habilidades técnicas y conocimientos informáticos para llevar a cabo actividades ilegales en línea. Sus acciones pueden incluir el robo de datos personales y financieros, la realización de ataques de ransomware para extorsionar a víctimas, la distribución de malware, la suplantación de identidad en línea, el fraude financiero, el espionaje cibernético y la violación de la privacidad. Estos criminales buscan obtener ganancias financieras, dañar la reputación de empresas u organizaciones, o incluso llevar a cabo actividades maliciosas con motivaciones políticas o ideológicas. Sus acciones representan una amenaza para la seguridad de individuos y empresas, y la lucha contra el cibercrimen es una preocupación constante en la era digital.

12. **Script Kiddies:** Los Script Kiddies son individuos con habilidades técnicas limitadas que se dedican a utilizar herramientas y scripts preexistentes para llevar a cabo ataques cibernéticos de bajo nivel, sin una comprensión profunda de cómo funcionan realmente. A menudo, su motivación es ganar notoriedad, causar molestias o, en ocasiones, daño, sin un propósito específico o un objetivo político o financiero. Estos actores suelen carecer de la sofisticación de los ciberdelincuentes más avanzados, pero pueden ser una amenaza para la seguridad en línea y provocar interrupciones y problemas para sitios web y sistemas que no están debidamente protegidos.

13. **Crackers de contraseñas:** Los crackers de contraseñas son individuos o grupos que se dedican a descifrar o romper contraseñas de sistemas o cuentas de forma no autorizada. Utilizan técnicas de fuerza bruta, ataques de diccionario o métodos de ingeniería social para obtener acceso a cuentas y sistemas protegidos por contraseñas. Su objetivo es eludir las medidas de seguridad y obtener información confidencial, como datos personales, credenciales bancarias o secretos comerciales. Las actividades de los crackers de contraseñas son ilegales y constituyen una seria amenaza para la seguridad de la información y la privacidad de los usuarios en línea, lo que subraya la importancia de utilizar contraseñas seguras y técnicas de autenticación robustas para protegerse contra tales ataques.

14. **Hackers éticos:** Los hackers éticos, también conocidos como "hacker ético" o "hacker de sombrero blanco", son profesionales de seguridad cibernética que utilizan sus habilidades técnicas para identificar y resolver vulnerabilidades en sistemas informáticos y redes. Su objetivo es fortalecer la seguridad, proteger la integridad de datos y prevenir ataques cibernéticos. Los hackers éticos trabajan de manera legal y ética, a menudo son

contratados por organizaciones para realizar pruebas de penetración, evaluaciones de seguridad y auditorías para identificar debilidades y ayudar a mejorar la postura de seguridad de una empresa.

15. **State-Sponsored Hackers:** Los hackers respaldados por estados o gobiernos mundiales, también conocidos como actores estatales o APTs (Advanced Persistent Threats), son grupos de ciberdelincuentes que operan con el respaldo y los recursos de un gobierno. Su objetivo principal es llevar a cabo operaciones cibernéticas que benefician a su estado patrocinador, lo que puede incluir actividades como el espionaje cibernético, la infiltración de redes gubernamentales y corporativas, el robo de secretos industriales, la manipulación de la información y la interrupción de infraestructura crítica. Estos grupos suelen ser altamente sofisticados y persistentes, con la capacidad de llevar a cabo ataques sostenidos a largo plazo y a menudo están involucrados en actividades de ciberespionaje y ciberguerra en el ámbito internacional.

16. **Distribuidores de botnets:** Los distribuidores de botnets son individuos o grupos responsables de crear y gestionar redes de bots, conocidas como botnets. Su función implica desarrollar malware para infectar dispositivos y convertirlos en bots, operar servidores de comando y control para coordinar actividades maliciosas, y llevar a cabo una variedad de delitos cibernéticos, como ataques DDoS, distribución de spam y robo de datos. Algunos distribuidores también alquilan o venden acceso a sus botnets a otros ciberdelincuentes. Sus acciones son ilegales y constituyen una seria amenaza para la ciberseguridad y la privacidad en línea. La detección y mitigación de botnets son esenciales para combatir estas amenazas.

17. **Crackers de software:** Los crackers de software son individuos con habilidades técnicas excepcionales que se dedican a romper las protecciones de software, como los sistemas de gestión de derechos digitales (DRM), con el fin de facilitar la distribución ilegal de programas. Entre sus prácticas habituales se encuentra la modificación de programas para sortear restricciones, como alterar fechas de expiración, permitiendo el uso continuado de programas más allá de sus licencias. A pesar de su experiencia técnica, sus acciones se consideran ilegales y éticamente cuestionables, ya que la distribución no autorizada de software pirata puede tener un impacto significativo en los desarrolladores y la seguridad de las aplicaciones.

    Las actividades de los crackers de software plantean desafíos tanto legales como éticos en la industria informática, ya que su enfoque en eludir medidas de protección y redistribuir software sin licencia plantea preocupaciones sobre derechos de autor y seguridad cibernética.

18. **Atacantes de fuerza bruta:** Los atacantes que realizan ataques de fuerza bruta se caracterizan por su enfoque persistente y meticuloso en la búsqueda de credenciales válidas para acceder a sistemas protegidos. Su estrategia se basa en probar exhaustivamente todas las combinaciones posibles de caracteres, desde números y letras hasta símbolos especiales, en lugar de depender de la suerte o la adivinación. Estos ataques suelen ser automatizados y emplean software especializado, lo que permite a los atacantes generar una gran cantidad de posibles contraseñas o credenciales de autenticación.
    La tenacidad y la habilidad técnica son rasgos distintivos de estos atacantes, quienes enfrentan desafíos como bloqueos de cuentas y sistemas de seguridad. A pesar de estos obstáculos, persisten en su búsqueda de la combinación correcta que les otorgará acceso no autorizado a cuentas o sistemas específicos.

19. **Atacantes basados en la web:** Los atacantes basados en la web se enfocan en explotar vulnerabilidades en sitios web y aplicaciones en línea para comprometer sistemas y robar datos sensibles. Utilizan tácticas como la inyección de SQL y el cross-site scripting (XSS) para lograr sus objetivos, lo que les permite acceder a bases de datos, robar información y manipular la salida de sitios web para inyectar scripts maliciosos. Sus motivaciones pueden variar, desde robo de datos personales o financieros hasta causar disrupciones en línea.

20. **Atacantes de redes inalámbricas:** Los atacantes de redes inalámbricas se especializan en explotar vulnerabilidades en redes Wi-Fi y tecnologías inalámbricas con el propósito de acceder a sistemas y datos protegidos. Utilizan diversas técnicas, como ataques de fuerza bruta y ataques de "hombre en el medio" (MITM), para infiltrarse en redes y robar información confidencial. Sus objetivos varían desde redes domésticas hasta empresariales y gubernamentales, y sus motivaciones pueden incluir lucro, espionaje cibernético o causar daño.
    Para protegerse contra estos atacantes, es esencial que los usuarios y organizaciones implementen medidas de seguridad sólidas, como el uso de contraseñas seguras, actualizaciones regulares de dispositivos inalámbricos y la adopción de protocolos de seguridad como WPA3.

b) Investigue 15 nombres de atacantes informáticos famosos/famosas e indique qué ataque fue el que realizaron, dé una breve descripción de dicho ataque.

1. **Kevin Mitnick:** Es un famoso hacker y experto en seguridad informática, conocido por sus actividades en la década de 1990. Uno de los ataques más destacados que realizó fue el acceso no autorizado a numerosos sistemas y la obtención de información confidencial a través de técnicas de ingeniería social y hacking. Uno de sus ataques más notorios fue el hackeo de DEC (Digital Equipment Corporation) en 1982. En ese incidente, Mitnick logró obtener acceso a los sistemas de DEC y copió el código fuente del sistema operativo VMS (Virtual Memory System), que era muy valioso en ese momento. Mitnick utilizó la ingeniería social para engañar a un empleado de DEC para que le proporcionara acceso telefónico a los sistemas de la empresa.
   Posteriormente, Kevin Mitnick fue arrestado y condenado por sus actividades ilegales, y pasó varios años en prisión. Después de cumplir su condena, se convirtió en un consultor de seguridad informática y autor de renombre, ayudando a las organizaciones a protegerse contra ataques cibernéticos y a comprender las técnicas utilizadas por los hackers.

2. **Adrian Lamo:** Adrian Lamo fue un hacker y una figura controvertida en el mundo de la ciberseguridad. Era conocido por sus actividades de hackeo y había realizado acciones de intrusión en sistemas y redes en el pasado, además por vulnerar la seguridad de empresas como The New York Times, Yahoo y Microsoft. Sin embargo, su notoriedad más grande no se debió a sus propios ataques cibernéticos, sino por su papel en la revelación de la fuente de WikiLeaks, Chelsea Manning.Lamo se involucró en una conversación en línea con Manning en la que Manning confesó haber filtrado una gran cantidad de documentos clasificados del gobierno de Estados Unidos a WikiLeaks.
   Adrian Lamo, en lugar de mantener la confidencialidad de esta conversación, decidió informar a las autoridades militares y de inteligencia sobre la revelación de Manning. Esta acción llevó a la detención y posterior enjuiciamiento de Manning, quien fue condenada por la filtración de documentos clasificados. La decisión de Lamo de denunciar a Manning generó un debate ético y moral en la comunidad de hackers y en el ámbito de la seguridad informática. Algunos lo consideraron un héroe por revelar una posible amenaza a la seguridad nacional, mientras que otros lo criticaron por romper la confidencialidad y la ética hacker de proteger a las fuentes.

3. **Albert González:** Es un cibercriminal estadounidense conocido por liderar un ataque de alto perfil contra la cadena de tiendas minoristas TJX Companies. En su ataque más significativo, González y su grupo lograron ingresar a los

sistemas de punto de venta (POS) de TJX Companies explotando vulnerabilidades en la seguridad de estos sistemas. Una vez dentro, instalaron malware en los POS para crear una "puerta trasera", que les permitió recopilar información confidencial, incluyendo datos de tarjetas de crédito de los clientes. Luego, transmitieron los datos a servidores controlados por ellos en ubicaciones remotas y los utilizaron para llevar a cabo transacciones fraudulentas y compras no autorizadas. El ataque resultó en uno de los mayores robos de datos de tarjetas de crédito en la historia, con graves consecuencias financieras. González fue arrestado y condenado por sus actividades delictivas.

4. **Julian Assange:** Es el fundador de WikiLeaks, nacido en Australia en 1971. WikiLeaks, tal y como él lo describe, es “un sistema incensurable que permite la filtración masiva e imposible de rastrear de documentos y su análisis público”. Fue responsable de la publicación de cientos de miles de documentos secretos de Estados Unidos que evidenciaron el abuso que cometió en las guerras de Irak y Afganistán, motivo por el cual, los Estados Unidos acusan a Assange de 18 cargos, incluyendo el *hackeo* de las bases de datos del ejército estadounidense para adquirir información sensible secreta

5. **Edward Snowden:** Es un exanalista de la CIA que recibió asilo político en Rusia en 2013, país donde actualmente radica. En 2013, hizo estallar un escándalo al revelar que el enorme aparato de espionaje estadounidense intervenía comunicaciones y recolectaba datos de personas de todo el mundo, desde simples publicaciones en redes sociales hasta llamadas de la canciller alemana Angela Merkel. Demostró que nadie estaba a salvo de las interceptaciones de la Agencia Nacional de Seguridad (NSA), y mucho menos los estadounidenses, cuyas comunicaciones privadas son supuestamente protegidas por la Constitución.
   También reveló que el servicio de inteligencia británico GCHQ captó, con la ayuda de la NSA, todo el tráfico que circulaba por los mayores cables submarinos de comunicaciones mundiales. La GCHQ además tomó subrepticiamente millones de fotos de las cámaras de ordenadores de gente común mientras estaban en los chats de webcam de Yahoo. El problema, dijo Snowden, no fue la justificación de la lucha contra el terrorismo, si no que había programas secretos virtualmente sin límites.

6. **Chelsea Manning:** Es una tecnóloga, analista y consultora especializada en privacidad, seguridad de redes y optimización de hardware. Fue condenada en 2013 por espionaje después de haber proporcionado más de 700.000 documentos secretos del Departamento de Estado y el Pentágono a WikiLeaks. “Como dijo una vez el ya fallecido Howard Zinn, no existe bandera lo bastante grande como para tapar el asesinato de gente inocente”, escribió

en un comunicado antes de entrar en la cárcel. Los documentos revelaban asesinatos a civiles, abusos de los derechos humanos y corrupción por parte del gobierno de EE UU en las guerras de Iraq y Afganistán.

7. **LulzSec:** LulzSec, abreviatura de "Lulz Security," fue un colectivo de hackers activo durante 2011 que se destacó por llevar a cabo una serie de ataques cibernéticos de alto perfil, incluyendo la infiltración y divulgación de datos confidenciales de organizaciones y gobiernos, como Sony, Nintendo, y el Senado de los Estados Unidos. A menudo afirmaban que sus acciones se realizaban en busca de diversión o "lulz" en lugar de motivaciones políticas o económicas, lo que les ganó notoriedad. Las autoridades arrestaron a varios de sus miembros en 2011, poniendo fin a sus actividades públicas.

8. **Gary McKinnon:** Gary McKinnon es un ciudadano británico conocido por su implicación en uno de los mayores casos de intrusión informática en sistemas gubernamentales de Estados Unidos. Entre 2001 y 2002, McKinnon hackeó computadoras de la NASA y el Departamento de Defensa de los Estados Unidos en busca de evidencia de encubrimiento de tecnología extraterrestre. Sus acciones causaron un gran revuelo y tensión entre el Reino Unido y los Estados Unidos. En 2012, tras años de lucha legal, el gobierno británico decidió no extraditarlo a Estados Unidos debido a preocupaciones sobre su salud mental, lo que puso fin a su caso.

9. **Anonymous:** Anonymous es un grupo o colectivo de hackers y activistas digitales que se originó a principios de la década de 2000. Anonymous ha utilizado los ataques de denegación de servicio como una táctica para expresar su descontento y promover sus agendas. Estos ataques han sido dirigidos a organizaciones, gobiernos, sitios web y servicios en línea en relación con una variedad de temas, como censura en internet, derechos civiles, privacidad y protestas políticas.Por ejemplo, en 2008, manifestó su desacuerdo con la Iglesia de la Cientología y comenzó a inhabilitar sus sitios web, lo que afectó negativamente a su posicionamiento en Google y saturó sus máquinas de fax con imágenes en negro.

10. **Maksym Yastremski:** Maksym Yastremski es un hacker ucraniano conocido por su participación en actividades delictivas en línea, especialmente en la industria del cibercrimen. Yastremski ganó notoriedad por su papel en la creación y distribución de malware, incluyendo el notorio troyano bancario conocido como "Trojan.PWS.Panda." Este malware fue utilizado para robar información financiera y contraseñas de usuarios. Yastremski fue arrestado en 2007 en Turquía y extraditado a los Estados Unidos, donde enfrentó cargos relacionados con sus actividades delictivas en línea. Su arresto representó un paso importante en la lucha contra el cibercrimen y la protección de la seguridad en línea.

11. **Anna Chapman:** Anna Chapman es una exespía rusa que ganó notoriedad internacional en 2010 cuando fue arrestada en los Estados Unidos como parte de un grupo de agentes rusos encubiertos. Chapman y otros miembros del grupo, conocidos como los "espías rusos de la vida real", fueron detenidos por cargos de conspiración y espionaje. Después de su arresto, Chapman fue deportada a Rusia como parte de un intercambio de espías entre Estados Unidos y Rusia. Tras regresar a Rusia, Anna Chapman se convirtió en una figura mediática y empresarial, participando en proyectos relacionados con moda, medios de comunicación y tecnología. Su historia ha sido objeto de gran atención mediática y ha contribuido a la narrativa de las relaciones entre Rusia y los Estados Unidos.

12. **Kim Dotcom:** Kim Dotcom, cuyo nombre real es Kim Schmitz, es un empresario alemán-finlandés conocido por ser el fundador del sitio web Megaupload, que fue uno de los servicios de alojamiento de archivos más grandes del mundo. Dotcom se convirtió en una figura controvertida en 2012 cuando el gobierno de Estados Unidos lo acusó de violación de derechos de autor, fraude y lavado de dinero, lo que llevó al cierre de Megaupload. Actualmente reside en Nueva Zelanda y ha estado involucrado en varios proyectos tecnológicos posteriores, incluyendo el lanzamiento de Mega, un sucesor de Megaupload, y la promoción de servicios de almacenamiento en la nube cifrado. Su caso legal ha generado un debate sobre la propiedad intelectual y la extradición.

13. **The Jester (th3j35t3r):** "The Jester", también conocido como "El Bufón", es un misterioso hacktivista que ha estado operando en el mundo en línea durante más de cinco años. Aunque su identidad real se mantiene en secreto, sus acciones y motivaciones han ganado notoriedad en la comunidad de seguridad informática y más allá.
    Lo que distingue a The Jester de otros hacktivistas es su enfoque en desafiar y desmantelar sitios web que, en su opinión, respaldan la propaganda y el reclutamiento yihadista. A lo largo de su carrera en línea, ha llevado a cabo ataques cibernéticos dirigidos a estos sitios, desplegando tácticas de hacktivismo en un intento por interrumpir y obstaculizar las operaciones de los grupos extremistas en línea.
    Se le atribuye el derribo de docenas de sitios web relacionados con el extremismo yihadista, y su lista de sitios afectados llegó a 179 antes de que dejara de contar. Sus métodos son un tanto controvertidos, ya que a menudo utiliza la fuerza bruta y técnicas de denegación de servicio distribuido (DDoS) para inutilizar temporalmente estos sitios web.

14. **Kevin Poulsen:** Kevin Poulsen, conocido en línea como “Dark Dante”, también fue bastante notorio en la década de 1990 por una serie de hacks que lo llevaron a ser llamado el “Hannibal Lecter de los delitos informáticos”.
    El ataque más notorio de Poulsen fue cuando tomó el control de todas las líneas telefónicas de la estación de radio de Los Ángeles, KIIS-FM, de modo que él fuera la persona que hiciera el llamado número 102 para ganar el valor de un Porsche 944 S2.
    Más tarde empezó a comprometer redes federales, desde donde robó información telefónica grabada, y esto le llevó a encabezar la lista de hackers más buscados del FBI durante un tiempo.
    Después de ser capturado, finalmente Poulsen fue sentenciado a 51 meses de prisión y tuvo que pagar 56.000 dólares.
    Desde entonces ha construido una exitosa carrera como periodista de investigación en seguridad. Actualmente es editor en jefe de Wired News y ha ayudado a hacer cumplir la ley con algunas investigaciones de ciberdelincuentes notables, entre ellos una que dio como resultado la identificación y detención de 744 delincuentes sexuales en la plataforma social MySpace.
    Poulsen y Aaron Swartz co-desarrollaron SecureDrop, el software de código abierto para comunicaciones seguras entre periodistas y fuentes.

15. **Jeanson James Ancheta:** Ancheta asistía a Downey High School en Downey, California hasta 2001, cuando abandonó la escuela. Más tarde ingresó a un programa alternativo para estudiantes con problemas académicos o de conducta. Trabajaba en un cibercafé y, según su familia, quería unirse a las reservas militares. Alrededor de junio de 2004 comenzó a trabajar con botnets después de descubrir rxbot , un gusano informático común que podía propagar su red de computadoras infectadas.
    Jeanson James Ancheta tiene el título de ser la primera persona en ser acusado y condenado por dirigir un ejército de botnets. Ancheta comprometió casi medio millón de computadoras con su ejército de botnets y alquiló publicidad en forma de ventanas emergentes, lo que le valió más de $ 100,000 en el proceso.
    Finalmente fue capturado por el FBI como parte de la Operación: Bot Roast cuando agentes del FBI lo engañaron para que visitara una oficina local para recolectar equipo de cómputo.
    Jeanson James, no se convirtió en uno de los mejores hackers del mundo con la finalidad de conseguir dinero o querer robar tarjetas de crédito. Si no por la curiosidad por los bots y los utilizándolos para llegar a comprometer más de 400.000 ordenadores en el año 2005.
    Jeanson James Ancheta tenía 21 años y organizó un sistema de malware sofisticado que permitía tener el control de sistemas informáticos y poder alquilarlos a otros hackers o a empresas publicitarias. Además, según el

medio Ars Technica, a Jeanson James también le pagaron para la instalación de bots o adware en algunos sistemas para recabar información sobre los mismos.

Referencias.

- Admin. (2021, 11 septiembre). *¿Qué es el crimen cibernético? - Scena criminis. Scena Criminis.* https://www.scenacriminis.com/ciencias-forenses/que-es-crimen-cibernetico/
- buzonuv@uv.mx. (s. f.). Noti_InfoSegura: Siempre tenemos la oportunidad de reivindicarnos, lee esta historia de 5 hackers – seguridad de la información. https://www.uv.mx/infosegura/general/noti_hackers-10/
- Ciberpyme. (2022, 18 enero). *Tipos de ciberataques: ataques a las conexiones*. Revista de Ciberseguridad y Seguridad de la Información para Empresas y Organismos Públicos. https://www.ciberseguridadpyme.es/actualidad/ataques-a-las-conexiones/
- CloudFlare. (2023).¿Qué es un ataque de día cero?. https://www.cloudflare.com/es-es/learning/security/threats/zero-day-exploit/
- Corcuera, L. (2023). Chelsea Manning: “Esta internet que conocemos ahora es la primera de muchas”. Revista El Salto. https://www.elsaltodiario.com/internet/entrevista-chelsea-manning-internet-inteligencia-artificial
- Diez años después de las filtraciones de Snowden, más datos y más controles. (2023). SWI swissinfo.ch - unidad empresarial de la sociedad suiza de radio y televisión SRG SSR. https://www.swissinfo.ch/spa/afp/diez-a%C3%B1os-despu%C3%A9s-de-las-filtraciones-de-snowden--m%C3%A1s-datos-y-m%C3%A1s-controles/48567062
- Elhacker.NET. (n.d.). elhacker.NET. https://www.elhacker.net/hackers-famosos-albert-gonzalez.html
- Español, C. E. (2015, 17 enero). *Conoce al vigilante que hackea a los sitios yihadistas*. CNN. https://cnnespanol.cnn.com/2015/01/17/conoce-al-vigilante-que-hackea-a-los-sitios-yihadistas/
- Equipo editorial de IONOS. (2023, 17 agosto). *Black Hat Hacker: objetivos y modus operandi*. IONOS Digital Guide. https://www.ionos.mx/digitalguide/servidores/seguridad/black-hat-hacker/
- *Hackers de sombrero negro, blanco y gris: definición y explicación*. (2023, 17 agosto). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/hacker-hat-types
- Jaimovich, D. (2019). Quién fue Adrián Lamo, el “hacker vagabundo” que delató a la informante de WikiLeaks, Chelsea Manning. Infobae. https://www.infobae.com/america/tecno/2019/04/23/quien-fue-adrian-lamo-el-hacker-vagabundo-que-delato-al-informante-de-wikileaks-chelsea-manning/
- KeepCoding, R. (2023). 7 tipos de hackers | KeepCoding Bootcamps. https://keepcoding.io/blog/7-tipos-de-hackers-2/#Hacktivistas

- Long, H. (2023). State spyware extensively using ads as distribution channel. RestorePrivacy. https://restoreprivacy.com/state-spyware-extensively-using-ads-as-distribution-channel/
- *Los delitos cibernéticos más recientes*. (2022, 21 julio). Federal Bureau of Investigation. https://www.fbi.gov/news/espanol/los-delitos-ciberneticos-mas-recientes
- Los 10 hackers más infames de todos los tiempos. (2023).Kaspersky LATAM https://latam.kaspersky.com/resource-center/threats/top-ten-greatest-hackers
- Majdalani, J. (2022). Recordando a Kevin Mitnick, uno de los hackers más buscados de la historia. ADSLZone. https://www.adslzone.net/noticias/seguridad/kevin-mitnick-hackers-mas-buscados-historia/
- Marker, G. (2021, 30 noviembre). *¿Qué es un cracker?* Tecnología + Informática. https://www.tecnologia-informatica.com/que-es-un-cracker/
- Perfil, V. (n.d.). *Tipos de atacantes, amenazas y técnicas de ataque*. https://tichoradadams.blogspot.com/2018/12/atacantes.html
- ¿Qué es la Ingeniería Social?. (s.f.). IBM Documentación. https://www.ibm.com/mx-es/topics/social-engineering
- Radware. (s. f.). *7 tipos de ataques más comunes para los que está diseñado el firewall de aplicaciones web (WAF) | Radware*. https://es.radware.com/cyberpedia/application-security/7-most-common-attack-types/
- Rodríguez, J. (2022). ¿Quién es Julian Assange?, te contamos su historia y qué hizo este programador. Expansión. https://expansion.mx/mundo/2022/07/04/julian-assange-que-hizo
- Rudra, A. (2023, 16 mayo). *¿Qué es un ataque de fuerza bruta y cómo funciona?* PowerDMARC. https://powerdmarc.com/es/what-is-a-brute-force-attack/#:~:text=En%20un%20ataque%20de%20fuerza,sistema%20o%20cuenta%20de%20destino.
- Security, P. (2023b, julio 18). *¿Qué es un hacker de sombrero blanco?* Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/hacker-sombrero-blanco/
- What is a Malware Software Developer?. (2022). Business Research Guide. https://www.businessresearchguide.com/faq/what-is-a-malware-software-developer/