ANÁLISIS DE AMENAZAS PRESENTES EN LOS ENTORNOS COMPUTACIONALES, VINCULANDO SISTEMAS OPERATIVOS, REDES Y BASES DE DATOS COMO ESTRATEGIA DEFENSIVA ANTE CIBER-ATAQUES SOBRE PLATAFORMA WINDOWS

GERMAN ARLEY PORTILLA GONZÁLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PAMPLONA, COLOMBIA
2020

ANÁLISIS DE AMENAZAS PRESENTES EN LOS ENTORNOS COMPUTACIONALES, VINCULANDO SISTEMAS OPERATIVOS, REDES Y BASES DE DATOS COMO ESTRATEGIA DEFENSIVA ANTE CIBER-ATAQUES SOBRE PLATAFORMA WINDOWS.

GERMAN ARLEY PORTILLA GONZÁLEZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Tutora de Curso
YENNY STELLA NUÑEZ
Asesora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PAMPLONA, COLOMBIA
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Pamplona., 29 de Abril del 2021

DEDICATORIA

Con aprecio dedico este trabajo a mi familia, amigos y demás personas que contribuyen para que cada día mejore en mis habilidades y capacidades.

AGRADECIMIENTOS

Agradezco a Kevin Tocora, Marleny Fernández, Gustavo Quijada, Omar Portilla, Camilo Suarez, además de mi directora de trabajo de grado por su paciencia y dedicación en todo este proceso académico que contribuyeron a culminarlo de la mejor manera.

INTRODUCCIÓN

En la actualidad el aumento de información ha cambiado de forma visible respecto a las décadas anteriores, del mismo modo como la migración de la mayoría de los datos que se tenían por escrito ahora hacen parte de organizaciones y sistema de cómputo, el área de la investigación ha evolucionado para ofrecer las defensas necesarias junto con la información y los datos que hoy en día están en cualquier espacio computacional, los bancos protegen su información basados en este concepto pero además empresas como Facebook twitter y WhatsApp usan estas herramientas para ofrecer grados de confidencialidad a los usuarios[1], donde se evita que sean víctimas de algún intruso que pueda afectar de forma negativa sus vidas negocios o cualquier otra actividad que desempeña, ciertas herramientas como la criptografía, la seguridad en bases de datos y la seguridad en sistemas operativos son observadas o se rigen mediante organizaciones las cuales entregan todo lo relacionado con la aplicación o implementación de estos métodos sobre los datos haciendo que exista un estándar en cuando a la codificación y decodificación de la información se refiere entre las organizaciones que están presenten dentro de esta área se tiene NIST, IEFT ISO entre otras que al final buscan un estándar que sea practico y posible entre los usuarios, de este modo tener grados de favorabilidad con la protección de los datos y la información con los estándares suministrados por las organizaciones nombradas con anterioridad [2].

[1] GONZÁLEZ, Diego. Diseño de Un Plan Estratégico de Seguridad de La Información, Mediante La Aplicación de Análisis de Riesgos Con La Norma ISO/IEC 27005. Caso de Estudio INAMHI. Revista INNOVA. 2018, vol. 3, no. 2, pp. 84-91. ISSN 2477-9024

[2] GUZMÁN PACHECO, Goyo Francisco . Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica Ortega. Tesis de postgrado 2015. Universidad Nacional del Centro de Perú

CONTENIDO

pág.

INTRODUCCIÓN *13*

1. DEFINICIÓN DEL PROBLEMA *14*

1.1 ANTECEDENTES DEL PROBLEMA 14

1.2 FORMULACIÓN DEL PROBLEMA 14

2 JUSTIFICACIÓN *16*

3 OBJETIVOS *17*

3.1 OBJETIVOS GENERAL 17

3.2 OBJETIVOS ESPECÍFICOS 17

4 MARCO REFERNCIAL *18*

4.1 MARCO TEÓRICO 18

4.1.1 INGENIERÍA SOCIAL 19

4.1.2 TROYANO 20

4.1.3 MAN IN THE MIDDLE 21

4.1.4 BOTNETS 23

4.1.5 DEFACEMENT 25

4.1.6 PHISING 26

4.1.7 VISHING 28

4.1.8 PHARMING 28

4.1.9 DOS 30

4.1.10 ESCALADO DE PRIVILEGIOS 30

4.1.11 SNIFFING 30

4.1.12 MALWARE 31

4.1.13 DESBORDAMIENTO DE BUFFER 33

5 análisis de la seguridad en el entorno presente de la plataforma de windows 33

5.1 ESTRATEGIAS Y PATRONES QUE SUMINISTRAN UN ANÁLISIS SOBRE LAS VULNERABILIDADES PRESENTES EN WINDOWS 34

5.2 planes de seguridad 34

5.3 desarrolla en buenas prácticas de servicios en vulnerabilidades sobre el sistema operativo 36

5.3.1 ACTUALIZACIÓN DEL SOFTWARE 36

5.3.2 SEGURIDAD EN SISTEMA OPERATIVO 37

5.3.3 SEGURIDAD EN CORREO ELECTRÓNICO WINDOWS O LINUX 37

5.3.4 SEGURIDAD EN NAVEGADORES 38

5.3.5 SEGURIDAD P2P 39

5.3.6 SEGURIDAD EN SISTEMAS REMOVIBLES 39

5.3.7 COPIAS DE SEGURIDAD 39
5.3.8 SEGURIDAD DE LA MENSAJERIA 40
5.3.9 ANÁLISIS DE AMENAZAS 2019 DE SOPHOSLABS 40
5.3.10 ESTADÍSTICAS DE SEGURIDAD INFORMÁTICA QUE IMPORTAN EN WINDOWS 41
5.3.11 ESTADÍSTICA DE CIBER AMENAZAS EN TIEMPO REAL DE KASPERSKY EN SISTEMAS DE WINDOWS 42

6 aPLICACIÓN DE LA METODOLOGÍA SOBRE LA VULNERABILIDAD EN EL SISTEMA OPERATIVO 47

6.1 aLCANCE DEL PLAN DE SEGURIDAD INFORMÁTICA 47

6.2 CARACTERIZACIÓN DEL SISTEMA INFORMÁTICO 48

6.3 RESULTADO DEL ANALISIS DE RIESGO 48

6.4 POLÍTICAS DE SEGURIDAD INFORMÁTICA 49

6.5 PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA 49

6.6 estrategias para la solución de problemas de las vulnerabilidades presentes en las redes y bases de datos 50
6.6.1 PLAN DE SEGURIDAD INFORMÁTICA 50
6.6.2 SENTIDO COMÚN 50
6.6.3 UTILIZAR SOLUCIONES DE SEGURIDAD 51
6.6.4 ACTUALIZAR EL SISTEMA OPERATIVO Y APLICACIONES 51
6.6.5 REALIZAR COPIAS DE SEGURIDAD 51
6.6.6 PRECAUCIONES CON LAS REDES WIFI PÚBLICAS 51

6.7 ALTERNATIVAS ANTE LA APARICIÓN DE VULNERABILIDADES EN LA PLATAFORMA WINDOWS 52
6.7.1 NESSUS 52
6.7.2 ACUNETIX 54
6.7.3 SUITE AIRCRACK-NG 56
6.7.4 OPENVAS 56
6.7.5 OWASP ZAN ATTACK PROXY ZAP 57
6.7.6 VEGA 57

6.8 PLANEACIÓN 58

6.9 DESCUBRIMIENTO 59

6.10 ATAQUE 62

6.11 REPORTE 63

7 RESULTADOS 65

7.1 análisis bibliográfico de los ataques cibernéticos actuales en las redes de datos, bases de datos sobre la plataforma Windows 65
7.1.1 RANSONWARE 65
7.1.2 SQL INJECTION 67

7.2 herramientas, estrategias o patrones que suministren la capacidad de formular un análisis completo sobre las vulnerabilidades presentes en los entornos de plataforma Windows 69

7.2.1 GFI LANGUARD 70
7.2.2 NEXPOSE 71

7.3 estrategias que puedan dar solución a la problemática de las vulnerabilidades presentes en las redes y bases de datos 72
7.3.1 ESCANEAR EL SISTEMA OPERATIVO PARA DETECTAR VULNERABILIDADES 73
7.3.2 IDENTIFICAR LAS VULNERABILIDADES 73
7.3.3 PRIORIZAR LOS RIESGOS 74

7.4 infraestructura capaz de brindar una alternativa ante la aparición de vulnerabilidades a nivel de software y hardware 74
7.4.1 SOFTWARE 74
7.4.1.1 ACTUALIZACIÓN DE SOFTWARE: SISTEMA OPERATIVO Y APLICACIONES 74
7.4.1.2 SEGURIDAD EN EL SISTEMA OPERATIVO 75
7.4.1.3 SEGURIDAD EN REDES PEER - TO – PEER 75
7.4.1.4 ZONA DESMILITARIZADA (DMZ) 76
7.4.2 HARDWARE 77
7.4.2.1 DISPOSITIVOS UMT 77
7.4.2.2 HONEY POTS 79

8 CONCLUSIONES 80

9 BIBLIOGRAFÍA 82

FIGURAS

Figura 1 Ejemplo de Man in the Middle 22
Figura 2 Nivel de conocimiento declarado sobre términos relacionados con el fraude online. (%) 29
Figura 3 Sniffing 31
Figura 4 Desbordamiento de Buffer 33
Figura 5 Tipos de archivo de riesgo 41
Figura 6 Infecciones locales en el mes de noviembre del 2020 43
Figura 7 Lista de las infecciones locales en el mes de noviembre del 2020 43
Figura 8 Amenazas web 43
Figura 9 Lista de las Amenazas Web 44
Figura 10 Ataque a redes 44
Figura 11 Lista de los ataques de redes 44
Figura 12 Vulnerabilidades 45
Figura 13 Lista de las Vulnerabilidades 45
Figura 14 Correo infectado 45
Figura 15 Lista de los correos infectados 46
Figura 16 Botnet 46
Figura 17 Metodología 47
Figura 18 Análisis de Riesgo 49
Figura 19 Nessus 53
Figura 20 Versiones de Nessus 53
Figura 21 Acunetix 55
Figura 22 Tipos de escaneo de Acunetix 55
Figura 23 OpenVas 57
Figura 24 Interfaz Gráfica Vega 58
Figura 25 Pagina de la Herramienta GFI Languard 70
Figura 26 Nexpose 72

RESUMEN

La presente propuesta monográfica dentro del área de estudio de seguridad informática parte de la necesidad que existe en el entorno computacional, de las empresas y organizaciones gubernamentales de ofrecer una descripción completa de las amenazas más importantes que atentan contra los conjuntos de datos, de redes y sistemas operativos. Los cuales se encuentran en varios documentos de forma particular enfatizando en muchos casos fenómenos aislados sin sus posibles estrategias de escudo ante cada una de las eventualidades que puedan llegar a presentarse, es labor del especialista en seguridad informática tener un repositorio con las herramientas necesarias ante los ataques o posibles casos de violación de la seguridad de cada uno de los entornos trabajados, en el mayor de los casos la información que se trabaja a través de estas plataformas tienen un valor no calculable debido a que la información personal que no se puede cualificar pero si establecer su grado de importancia. Este tipo de amenazas diferentes para cada uno de los entornos es una desventaja notable, debido a que en el mayor de los casos existe un atraso significativo en el control, lo que genera demoras y hasta la perdida de estos datos. Las vulnerabilidades presentes en las bases de datos son tan importantes como las presentes en los sistemas operativo, pero con la diferencia notable que en las bases de datos la inyección SQL ha estado presente desde hace mucho tiempo con estrategias que se han establecido pero que de una u otra forma no se implementan.

Palabras clave: Alertas, amenazas, defensa, entornos computacionales, plataforma, redes, sistemas, virus, vulnerable.

ABSTRACT

This proposal for undergraduate work within the IT security project area starts from the need that exists in the computational environment, to provide a full description of the most important threats to data sets, networks and operating systems. Which are found in several documents in a particular way emphasizing in many cases isolated phenomena without their possible strategies of shield before each of the eventualities that may arise, it is the job of the IT security specialist to have a repository with the necessary tools to deal with attacks or possible cases of security breaches in each of the working environments, in the greatest of cases the information that is worked through these platforms has a value not calculable because the personal information cannot be qualified but rather establish their degree of importance. This type of different threats for each of the environments is a notable disadvantage, because in the greatest of cases there is a significant delay in control, which generates delays and even the loss of this data. The vulnerabilities present in the databases are as important as those present in the operating systems, but with the notable difference that in the databases SQL injection has been present for a long time with strategies that have been established but that in one way or another are not implemented.

Keywords: Alerts, computational environments, Defense, networks, platform, systems, Threats, Virus, Vulnerable.

INTRODUCCIÓN

En la actualidad el aumento de información ha cambiado de forma visible respecto a las décadas anteriores, del mismo modo como la migración de la mayoría de los datos que se tenían por escrito ahora hacen parte de organizaciones y sistema de cómputo, el área de la investigación ha evolucionado para ofrecer las defensas necesarias junto con la información y los datos que hoy en día están en cualquier espacio computacional, los bancos protegen su información basados en este concepto pero además empresas como Facebook twitter y WhatsApp usan estas herramientas para ofrecer grados de confidencialidad a los usuarios[3], donde se evita que sean víctimas de algún intruso que pueda afectar de forma negativa sus vidas negocios o cualquier otra actividad que desempeña, ciertas herramientas como la criptografía, la seguridad en bases de datos y la seguridad en sistemas operativos son observadas o se rigen mediante organizaciones las cuales entregan todo lo relacionado con la aplicación o implementación de estos métodos sobre los datos haciendo que exista un estándar en cuando a la codificación y decodificación de la información se refiere entre las organizaciones que están presenten dentro de esta área se tiene NIST, IEFT ISO entre otras que al final buscan un estándar que sea practico y posible entre los usuarios, de este modo tener grados de favorabilidad con la protección de los datos y la información con los estándares suministrados por las organizaciones nombradas con anterioridad [4].

[3] YAMPOLSKIYA, Mark, KINGB, Wayne, GATLINA, Jacob, BELIKOVETSKYC, Sofia, BROWNA, Adam, SKJELLUMD, Anthony y ELOVICIC, Yuval. Security of additive manufacturing: Attack taxonomy and survey. Additive Manufacturing. 2018. 21, 431–457. https://doi.org/10.1016/j.addma.2018.03.015

[4] RIXOM, Jessica, y MISHRA, Himanshu. Ethical ends: Effect of abstract mindsets in ethical decisions for the greater social good. Organizational Behavior and Human Decision Processes. 2014, 124, 110–121. https://doi.org/10.1016/j.obhdp.2014.02.00.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Desde la aparición de los entornos de datos y la migración de toda la información a servicios de nube o de sistemas de administración de información las amenazas han estado presentes debido a que la mayoría de atacantes busca de una u otra forma afectar el correcto funcionamiento de las mismas, es importante resaltar que los especialistas en seguridad informática o los encargados de proteger la información presente en los sistemas, están alertas ante la aparición de estos sucesos, facilitando las tareas de control, a partir de métodos preventivos paliativos y correctivos que fortalecen todos estos procesos. Si ejecutamos la búsqueda de todas las amenazas más importantes o relevantes dentro de los sistemas de información no se muestran trabajos notables que enfaticen en el conjunto completo, sino que son parciales y dan algunas estrategias de contención, en muchos casos se preguntan si usar las estrategias preventivas ante los ataques es algo importante o algo que se debe tener en un grado relativo de importancia, y la respuesta es muy concreta es que la búsqueda de estrategias que fomenten el descubrimiento y la corrección de amenazas no fuese importante de nada serviría tener los datos de importancia en los sistemas, sino que sería mejor tenerlos de forma física sin tener la preocupación que existan procesos de vulneración, pero debido a que los volúmenes de información cada vez son más grandes que de una u otra forma se dificulta buscar como almacenarlos, es por esta razón que las empresas o usuarios buscan que su información se encuentre en un formato digital. Según estadísticas, cerca del 91% de los computadores tienen spyware pirata de acuerdo con un reporte de la firma Earthlink, en una revisión cerca de 1 millón de computadores en internet.

1.2 FORMULACIÓN DEL PROBLEMA

Según datos de proveedores de servicios de protección de información y antivirus de tiene que en los sistemas operativos de Windows se neutralizaron alrededor de 284.489 ataques de cifradores y 243.604 usuarios a los cuales se les neutralizo la ejecución de programas todo esto para el primer trimestre de 2019.

Con el transcurso de los años cada una de las amenazas han mutado y adaptado a los nuevos cambios de protección que se ejecuten por esta razón se hace indispensable tener un documento actualizado que entregue las estrategias referentes a cada una de estas amenazas. Además de ser un punto de partida ante la actualización de las mismas que evite el dispendioso trabajo, el cual puede ser tardío de realizar cada vez que se genera un nuevo ataque una búsqueda de las estrategias de contención, en este año vemos la mutación del ransonware el cual se mostraba como un virus o amenaza de fácil eliminación pero con el pasar de los días se hace más peligroso debido a que aplican las ecuaciones de encriptación

manejadas para atacar directamente los datos de los ordenadores. En muchos de esos casos obligando a los usuarios o empresas a entregar dineros, con cada cambio de este ransonware debe tener un historial de trabajo donde su forma de ejecución sean las alternativas de contención para que los datos que sean afectados por el mismo sean protegidos, esta amenaza se está tornando más peligrosa que la inyección SQL debido a que el nivel de daño es completo para las víctimas que no tienen las alternativas necesarias para la contención[5].

¿Cómo establecer un análisis de amenazas presentes en entornos computacionales como estrategia de defensa ante los ciber-ataques haciendo uso de herramientas e investigaciones dispuestas sobre el área de vulnerabilidades?

[5] GÓMEZ VIEITES, Álvaro La importancia del factor humano en la seguridad informática. 2017 [consultado 30 de junio 2020]. Artículo publicado por EDISA. Compañía de software en Madrid, España.

2 JUSTIFICACIÓN

Según los datos de los virus informáticos siguen siendo una de las principales fuentes de perdida financieras en las organizaciones, seguidos de impactos derivados en accesos no autorizados de los sistemas, el robo de información de propiedad industrial y la perdida de computadores personales. Estas son las causas que generan más del 74% del total de las pérdidas financieras y de información privada por parte de los usuarios de Windows. En la actualidad las plataformas como Windows siempre están trabajando en evitar ataques cibernéticos con actualizaciones que disponen a sus usuarios, pero esto no es suficiente ya que hay que determinar el modo de operación su origen y búsqueda del método con el cual el atacante implanto algún virus causando la extracción de información y la pérdida total de ella. Por lo tanto, en el siguiente proyecto de investigación se busca profundizar los conocimientos relacionados con los ciber ataques para prevenir algún robo de información. Cuando se refiere a las amenazas las fuentes son diversas las investigaciones que se presentan son particulares y es importante tomar las investigaciones que presenten importancia significativa, que permitan unificar los conceptos y tener a disposición un conjunto de pautas ejemplos, además de estrategias técnicas que logren que un entorno computacional se desarrolle de forma idónea ejecutando tareas preventivas o correctivas con el fin de proteger la información o los datos que en el mundo actual se presenta en volúmenes que son difíciles de cuantificar [6].

[6] DAVILA VILLANUEVA, Miguel Augusto y SUXE RAMÍREZ, María Alicia, MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. Tesis para optar el título profesional de ingeniero de sistemas. Chimbote, Perú Universidad Católica los Ángeles de Chimbote. Junio de 2018.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Realizar un análisis de las amenazas presentes en los entornos computacionales como estrategia defensiva ante ciber-ataques presentes de la plataforma Windows.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar análisis a bibliográfico de los ataques cibernéticos actuales en las redes de datos, bases de datos sobre la plataforma Windows.
- Identificar las herramientas, estrategias o patrones que suministren la capacidad de formular un análisis completo sobre las vulnerabilidades presentes en los entornos de plataforma Windows.
- Proponer las estrategias que puedan dar solución a la problemática de las vulnerabilidades presentes en las redes y bases de datos.
- Proponer un tipo de infraestructura capaz de brindar una alternativa ante la aparición de vulnerabilidades a nivel de software y hardware.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Hablar de fundamentos de la ciberseguridad, mecanismos preventivos, correctivos y detectivos de seguridad informática, evaluación de riesgos, amenazas y vulnerabilidades. La seguridad informática es uno de los aspectos más importantes para las organizaciones, pues todos los esfuerzos que se emplean son en busca de proteger los activos principales con los que cuenta un sistema informático, con el pasar del tiempo se han desarrollado cualquier tipo de herramientas ya sea de hardware o de software que han permitido que muchos de los aspectos que conforman las redes se encuentren salvo contando con integridad, disponibilidad y confiabilidad, este desarrollo tecnológico en pro de la seguridad surge de que día a día se generan diferentes tipos de ataques o sucesos que dejan al descubierto las vulnerabilidades de las empresas y esto los mueve a crear las solucionen que aseguren sus empresas [7].

En los sistemas computacionales actuales es común apreciar un conjunto de fallos presentes en los sistemas informáticos como las bases de datos o los sistemas operativos todo debido que hace algunos años el uso de plataformas de bases de datos relacionales y no relacionales no eran tan usadas, además de que los servicios de internet eran deficientes con anchos de banda que limitaban dichas tareas, las páginas web y demás entornos donde el usuario podía interactuar eran diferentes a los vistos en la actualidad, los ataques en esa época eran mínimos junto con las herramientas para los mismos, en los años actuales las estrategias junto con las herramientas para vulnerar los sistemas son múltiples puesto que el auge de las redes de internet y se portales de comunicación buscan que las personas tengan conceptos más avanzados de esta temática [8], dentro del espacio de los ataques no solo se presentan en una fracción del sistema sino que todo el sistema sufre de lo mismo por una infinita de algoritmos maliciosos que cambian con el pasar de las horas y los días con el fin de obtener datos tanto de los usuarios como de la empresa, a continuación se hará una descripción de las posibles amenazas a las cuales son sometidas los sistemas informáticos, bases de datos, sistemas operativos y en general las redes que son el soporte de los sistemas de cómputo actuales [9].

---

[7] FERRER, Jorge y FERNÁNDEZ-SANGUINO, Javier. Seguridad informática y software libre. 2007, 1–11.

[8] GIMÉNEZ ALBACETE, Jose Francisco. Seguridad en equipos informaticos. Antequera, Malaga. 2014

[9] KANAT ALEXANDER, Max. Code simplicity: the science of software development., 2012. [en línea]

4.1.1 INGENIERÍA SOCIAL

La ingeniería social no es más que la manipulación de las víctimas para que están proporcionen información para realizar accesos no autorizados a sus equipos o aplicaciones [10], algunas de las formas que emplean los ciber atacantes para obtener esta información es:

- Por correo electrónico, empleando ataques tipos phishing.
- Por teléfono, empleando la técnica llamada vishing, que es una técnica para obtener información engañando a personas o compañías por llamadas telefónicas.
- A través de las redes sociales, un canal muy empleado por los delincuentes para extorsionar a los usuarios.
- Por medio de USB, empleando malware para infectar equipos de las instalaciones de las compañías, usando la técnica conocida como baiting.
- Por mensaje de texto, empleando la técnica llamada smishing, con este método los delincuentes suplantan a identidad de una compañía, mostrando confianza en el mensaje de texto para que las personas respondan a este llamado.

Sabiendo las técnicas empleadas es preciso saber que existen formas de contrarrestar la ingeniería social [11], estando alerta y ser cautelosos a la hora de usar dispositivos o equipos.

- No revelar información personal ni datos confidenciales: los datos como credenciales, números de tarjetas de crédito, cuentas bancarias, los números de identificación, etc. son información que a menudo se solicita, es importante tener en cuenta que este tipo de datos no pueden ser revelados mediante teléfono, email u otras aplicaciones que incluyan mensajería.
- No publicar información personal en internet: las redes sociales son uno de los principales objetivos de los delincuentes de la red, allí se encuentra todo tipo de información como número de teléfono o dirección, por esto es importante no dejar al descubierto ningún tipo de información que pueda ser empleado en un delito informático.

[10] KRAUS, Rob, BARBER , Brian, BORKIN, Mike y ALPERN, Naomi. CHAPTER 1 – Windows Operating System – Password Attacks. Seven Deadliest Microsoft Attacks, 2010. 1–23. https://doi.org/10.1016/B978-1-59749-551-6.00001-7

[11] KRAUS, Rob, BARBER , Brian, BORKIN, Mike y ALPERN, Naomi. SQL Server – Stored Procedure Attacks. Seven Deadliest Microsoft Attacks. November 2009, 49–69. https://doi.org/10.1016/B978-1-59749-551-6.00003-0.

- Verificar ficheros adjuntos: los archivos deben ser examinados antes de descargarlos, con el objetivo de no verse afectado por un virus, un gusano, spam, etc.
- Instalar y actualizar el antivirus y/o cortafuegos: esta es una protección que ayuda en caso de ataques de este tipo, pero que si no cuenta con una actualización adecuada pueda que n identifique muchas amenazas que llegan al dispositivo.

Precaución: es la última recomendación: pues ante los engaños empleados en la ingeniería social, esta es la mejor herramienta con la que se puede contar para tener seguridad en internet.

4.1.2 TROYANO

El troyano es un programa ilegitimo que este contenido dentro un programa legítimo que fue colocado por acción no autorizada y que este programa malicioso hace operaciones que pasan inadvertidas. Los troyanos específicamente de las bases de datos son un ataque más elaborado pues se divide en dos partes, la inyección del código malicioso y la llamada del código malicioso, como están separados en dos fases es más difícil de rastrear. Por lo tanto, es una tarea que posee gran dificultad relacionar los dos eventos, que ocurren en momentos distintos, con diferentes conexiones y con diferentes IP pertenezcan al mismo ataque [12] .

Este es un malware que pasa desapercibido normalmente pero que oculta un software malicioso dentro de un archivo que parece normal, y es en ese momento donde los delincuentes informáticos aprovechan para acceder ilegalmente a los sistemas de los usuarios, robar información confidencial y obtener acceso por la puerta trasera al sistemas, otras de las consecuencias que puede tener la infección con un troyano es la eliminación, modificación, bloqueo o copia de la información, además que puede interferir con el funcionamiento de los equipos [13]. Este tipo de ataque se divide en cuatro categorías:

- Un ataque que inyecta el troyano y lo llama
- Un ataque que emplea un intermediario para inyectar el troyano y luego realiza una acción para llamarlo y extraer la información, o realizar una acción dentro de la base de datos.

---

[12] LÓPEZ MATACHANA. . Los virus informáticos : una amenaza para la sociedad. Retrieved. [en línea].2020 [consultado 01 de Diciembre 2020]. Disponible en http://bibliotecavirtual.unad.edu.co:2139/eds/detail/detail?vid=9&sid=e2e23ef1-fcc3-4a6e aa8342fcae585cac%40sessionmgr104&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZQ%3D%3D#A

[13] MANSFIELD-DEVINE, Steve. The malware arms race. Computer Fraud and Security, 2018, 15–20. GIMÉNEZ ALBACETE, Jose Francisco. Seguridad en equipos informaticos. Antequera, Malaga. 2014.

- Un ataque que emplea un usuario para infectarlo con el troyano y otro para llamarlo.
- Un ataque que emplea un usuario y un proceso ajeno para inyectarlo y un usuario y un proceso para llamarlo.

Para la protección contra los troyanos es necesario adquirir un software con buenas características antimalware, hacer un análisis con aplicaciones de seguridad en internet periódicamente, obtener las actualizaciones tanto del SO como de otras aplicaciones que usen los equipos, procurar visitar sitios seguros, n descargar archivos o acceder a enlaces que parezcan sospechosos, hacer una elección de contraseñas complejas para las cuentas y finalmente se recomienda usar firewall para la protección de la información.

2011 fue un año en el que más empresas nacionales se convirtieron en blanco de ciberataques, especialmente por los caballos de Troya [14]. Informe de seguridad de ESET el software antivirus muestra que, en México, el 82.5% de las empresas encuestadas dijeron tener Infectados en un año, este es el país con mayor número de incidentes a través de programas maliciosos en Latinoamérica. En segundo lugar, está Ecuador 77,88%, Perú ocupó el tercer lugar con 56,02%

Actualmente, existen varias formas de detectar y clasificar programas malware, como caballos de Troya y gusanos; no obstante, la cantidad de dispositivos a nivel mundial, el número de productos electrónicos infectados sigue siendo elevado de problemas que deben resolverse, el rostro de las empresas antivirus también está en alza, algunas de las cuales son principalmente:

- Miles o incluso millones de muestras que su laboratorio recibe todos los días análisis.
- Las técnicas utilizadas por los creadores de códigos maliciosos dificultan Verifique su programa, por ejemplo: modifique el código, use Compresor o empaquetador, ofuscación, algoritmo de cifrado, etc.

Programas maliciosos complejos desarrollados por el gobierno para los siguientes propósitos espía y sabotaje.

4.1.3 MAN IN THE MIDDLE

Este consiste en establecer una conexión con las víctimas y controlar la conversación que establecen, interceptando los mensajes que envían e inyectar

[14] GÓMEZ VIEITES, Álvaro La importancia del factor humano en la seguridad informática. 2017 [consultado 30 de junio 2020]. Artículo publicado por EDISA. Compañía de software en Madrid, España.

nuevos, este ataque es exitoso solo si el atacante suplanta cada punto final correctamente, lo cual es un ataque de autenticación mutua [15].

Para prevenir los ataques MITM la autenticación de extremos es una solución con la que la mayoría de los protocolos criptográficos cuenta y un ejemplo de ello es que SSL realiza una autenticación del servidor implementando una autoridad de certificación de confianza mutua[16].

Démosle un ejemplo simple para ilustrar la composición de este ataque:
Supongamos que tenemos 3 hosts en la red, a saber, host A, host B y host C. El anfitrión A quiere intercambiar Información sobre el host B (este host puede o no estar en la misma red), para esto, el paquete debe enviarse a Dirigiéndolos al enrutador de B. Ahora, si el host C tiene la intención de "escuchar" los mensajes enviados por A B, solo necesita actuar como puente entre A y el enrutador.

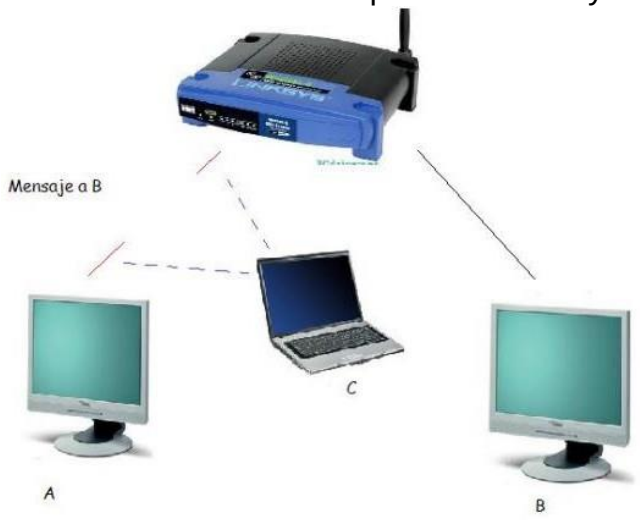

Figura 1 Ejemplo de Man in the Middle

Como ataque pasivo, la víctima no encontrará nada extraño, por lo que es difícil lidiar con este ataque. En resumen, este ataque permite monitorear el tráfico malicioso desde la red al host enrutador, por ejemplo, de enrutador a host.

Detección de los Ataques más relevantes de Man in the Middle en la plataforma de Windows

[15] KANAT ALEXANDER, Max. Code simplicity: the science of software development., 2012. [en línea] Editorial O´reilly media Inc. Estados Unidos de América.
[16] ORDUZ BARRERA, Diana. Análisis de Emergencias Cibernéticas Que Se Presentan En Las Ciudades de Tunja, Duitama y Sogamoso Con Respecto Al País En Los Últimos Dos Años [en línea]. Monografía de posgrado. Universidad Nacional Abierta y a Distancia, 2019 [consultado 11 Noviembre 2020].Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31410/dmorduzb.pdf?sequence=1&isAllowed=y

Es difícil detectar este tipo de aplicaciones (Wireshark o Cain) porque son por decir lo menos, casi sin huella. Mucha de la información difundida en Internet texto sin formato, capaz de acceder a esta información confidencial desde cualquier computadora en la misma red que utilice un rastreador simple, como hemos visto en esta guía. A continuación, se mostrarán algunas técnicas para intentar detectar ataques "man in the middle", pero no son mutuamente excluyentes, por lo que es posible fusionarlos según sea necesario.

1. **Entrar en la maquina:** Por decir lo menos, esto es lo más improbable. Si se puede acceder físicamente a la máquina formada como parte de la red, podemos ver una lista de cada aplicación y proceso activo, podemos verificar si algunos procesos pueden ser rastreadores. A veces, estos programas se ejecutan al iniciar la computadora o tienen una entrada en el registro del sistema. Por ejemplo, Wireshark, si no se está ejecutando, pero está instalado, podemos Registro de Windows, en la siguiente ruta: HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Uninstall \ Wireshark.

2. **Prueba de ICMP:** Se realiza ping a la dirección IP donde se quiere analizar el retraso del paquete. Una vez que se vea como resultado, se crea una conexión TCP falsa en la red durante un período de tiempo y luego se espera un tiempo posible. El rastreador procesa estos paquetes, lo que aumenta el tiempo de espera. Si se vuelve a analizar el retraso del ping, se encuentra que el tiempo en milisegundos ha aumentado significativamente, lo que se olfatea la red.

3. **Prueba de ARP:** La prueba se basa en enviar una solicitud de eco (ping) ICMP a la dirección IP que se quiere, pero utilizando la MAC error. Para ello podemos agregar la dirección que queramos a la tabla ARP, es decir, incluir la dirección el comando MAC proporcionado por ARP es incorrecto.

Protección frente a SNIFFERS: La mejor forma de protegerse contra los rastreadores es proteger la información que enviamos mediante algún tipo de cifrado. La tecnología de cifrado para cifrar y descifrar información permite intercambiar información. Una forma segura para que solo el destinatario de la información pueda identificar la información.

4.1.4 BOTNETS

Esta es una red de bots o equipos zombis que han sido infectados por algún malware y estas a disposición del atacante. Al tener estos equipos a su disposición

se emplean para enviar spam, virus, ataques DDoS o para robar información confidencial [17].

Algunas acciones que se puede implementar en una organización para no quedar expuesto ante una red botnets es:

- Contar con un antivirus de buena reputación y confianza.
- Contar con los softwares actualizados.
- Procurar no abrir ni descargar archivos que sean sospechosos.

Cuando surgen negocios de spam y problemas relacionados (como distribución de malware y phishing), trate de lograr un nivel suficiente de rentabilidad para los ciberdelincuentes actuales, ellos han un problema mayor. Hasta ahora, los servidores vulnerables han sido secuestrados y los servidores descubiertos todos los días ya no lo son suficientes para el propósito de estas personas. Entonces el problema es lograr que se distribuya más correos electrónicos para llegar a más usuarios, maximizando así sus ganancias. La solución viene de la mano de la potencia informática distribuida. Las botnets representan la principal amenaza de impacto de las Organizaciones y usuarios de hoy día. A través de ellos los ciberdelincuentes intentan comprometerse, el propietario sin el consentimiento del propietario, Para utilizarlos como "trampolín" se utiliza para iniciar diferentes tipos de atacar a un tercero, por ejemplo, Denegación de servicio, fraude y robo Identidad, etc.

Hoy, los ataques de Internet han sufrido una profunda transformación, hace un tiempo centrarse en afectar la usabilidad Infraestructura y servicios hoy también contra Personas y organizaciones, detrás de estos nuevos ataques existen en el host comprometidos, ubicados en la casa, escuelas, organizaciones privadas y Gobierno; infectado computadoras llamadas robot Controladores y otros robots compuestos por robots que es una red de computadoras que normalmente se llama botnet o Ejército de zombies. Esta es una existencia canal de comunicación Controlador, diferente de otros tipos de ataques de botnet [18].

Como primer paso para solucionar este problema el tema es esencial son las características de la botnet: Componentes, arquitectura existente y su funcionamiento. El análisis de comportamiento puede usar desde red en ejecución o simulado entorno de diferentes botnets. Cuando se trata de pruebas, hay muchas tecnologías y diferentes clasificaciones, la tecnología pasiva y tecnología activa.

[17] VENOSA, Lina Paula y DÍAZ, Javier. Detección de botnets utilizando herramientas Opensource Resumen Introducción. Workshop de Investigadores en Ciencias de la Computación. Enero, 2014, pp. 832–836.

[18] NGO, Quoc-Dung, NGUYEN, Huy-Trung, NGUYEN , Le-Cuong y NGUYEN, Doan-Hieu. A survey of IoT malware and detection methods based on static features. ICT Express, 2020, no. xxxx, doi: 10.1016/j.icte.2020.04.005.

Habilidades pasivas Incluida la obtención de datos de vigilancia sin interferencias, medio ambiente o evidencia de cambio, y las personas activas incluyen recursos Supervisado.

- **FUNCIONAMIENTO DE LOS BOTNETS**

Esta distribución se realiza a través de una gran cantidad de mensajes (por ejemplo, a mediados de enero, muchos usuarios fueron engañados. Títulos como "La muerte de Fidel", desafortunadamente, "mató una tormenta que arrasó Europa", "La vida de Saddam Hussein" Atención suficiente a que miles de ordenadores se infectaron y empezaron a actuar la base de una nueva ola de ataques. Una vez que la red está configurada correctamente (usando 10 o miles de computadoras), botmaster (responsable) porque puede tomar decisiones con total libertad, ya sea de forma remota o en cualquier parte del mundo cómo afrontarlo, por ejemplo:

- Enviar Spam
- Realizar un ataque distribuido de denegación de servicio
- Crear un servidor para alojar software warez, programas de craqueo, números de serie, etc
- Implementar un servidor web para alojar material pornográfico y pedófilo
- Colocar un servidor web para ataques de phishing.

El control de la red se puede realizar de muchas formas: puede controlar la red por completo o puede controlar la red de las siguientes formas: Segmente a través de canales de IRC y confíe en DNS gratuito para garantizar su cifre permanentemente el canal para evitar que personas ajenas lo rastreen, lo identifiquen o lo interfieran El método más común es controlar uno o más servidores IRC para enviar el orden de otros nodos de la red. El servidor llamado Command and Control (C&C) es el punto más débil de la red, porque si se identifica que puede darse de baja, el botmaster puede ser aislado de tu red.

4.1.5 DEFACEMENT

Consiste en un ataque que se encarga de la desfiguración del sitio web, es decir modificar características de la misma sin la autorización del administrado. Esto es posible lograrlo si son hallados errores de código o Bugs, que permite que el atacante acceda como usuario roo. Algunas técnicas que son empleadas son: XSS, HTML injection, SQl injection, RFI, Backdoors y Rookit y Mass Defacement entre las más conocidas.

Algunas acciones que se pueden implementar para proteger un sitio Web de un ataque Defacement son:

- Realizar auditorias

- Emplear medidas de protección contra inyección de código.
- Agregar medidas de prevención contra XSS y RFI
- Contar con un plan de seguridad que permita actuar en caso de que se presente el incidente.

Los ataques cibernéticos en el sitio web continúan afectando la integridad y disponibilidad de la información, esto hace que sea necesario implementar o reducir el riesgo a un nivel aceptable. Los incidentes informáticos tienen un impacto económico y la reputación de diferentes organizaciones. Ha habido un aumento en los ataques informáticos en diferentes organizaciones, uno de los cuales son los ataques de daño a la reputación, que incluyen modificaciones no autorizadas. Cambios en el sitio web que afectan a la integridad del sitio web. Este artículo describe el desarrollo del modelo para establecer controles de seguridad para limitar y reportar este ataque, actualmente centrarse en sitios web de entidades gubernamentales. El método utilizado para hacer prueba desarrolladas en dos páginas web real. Durante la prueba, los dos tienen diferentes atributos de cantidad (HREF, SRC) y complejidad (en cuanto a recursos, enlaces, infraestructura, etc.). Primero, se usa una página web desarrollado con PHP con 415 atributos, en segundo lugar, Se evaluó otra página web con menos atributos (149). de La segunda actividad del control incluye descargar todos los recursos web que se probará. La tercera actividad evalúa la eficiencia del control en base a su funcionamiento en dos páginas web. En particular, se definieron 15 muestras y se registró el tiempo de generación. En proceso de calcular el valor del cheque.

4.1.6 PHISING

Es una técnica de ingeniería social, que es empleada por los delincuentes para adquirir información confidencial de sus víctimas. Este se hace pasar por una persona o empresa de confianza a la cual imitan, para hacer creer que es legítima la conversación en una comunicación electrónica, por sitio web, por correo u otro sistema de mensajería instantánea [19].
Algunas medidas preventivas a tener en cuenta son:

- No enviar datos personales o financieros por ningún medio electrónico.
- Verificar que el correo es legítimo, sin duda del mismo no acceda a lo que le está demando.
- Procurar utilizar las direcciones correctas de entidades financiera u otras, pues existen variedad de páginas engañosas que se hacen pasar por estas.
- Proteger sus contraseñas y no revelarlas

[19] VRBANĆIĆ, Grega, FISTER, Iztok y PODGORELEC, Vili. Datasets for phishing websites detection. Data Br., 2020, vol. 33, p. 106438, doi: 10.1016/j.dib.2020.106438

- Mantener actualizado el navegador y aplicar parches de seguridad.

"Los ataques de suplantación de identidad adoptan la forma de ingeniería social y medios técnicos robar datos de identificación personal y credenciales de los consumidores cuentas financieras. Plan de ingeniería social basado en correo electrónico engañar a los consumidores haciéndoles hacerse pasar por sitios web diseñados para defraudar. Los destinatarios divulgan datos financieros como números de tarjetas de crédito, nombre de usuario de la cuenta, contraseña y número de seguro social. Nombres comerciales de bancos, emisores y compañías de tarjetas adecuados los phishers suelen persuadir al destinatario para que responda. Los medios técnicos implican la instalación de software criminal en computadoras personales, robar credenciales directamente, generalmente utilizando troyanos capturados con pulsación de tecla ".

El phishing es un tipo de técnica presente dentro de la ingeniería social donde se busca obtener información relevante del usuario, pero suminisrada por el mismo, existen varios procesos uno de ellos es el de solicitar el acceso a portales mediante correos electrónicos donde el usuario o victima entrega sus credenciales que serán tomadas por el atacante dentro de esta modalidad, pueden ser enlaces vínculos entre otros. El usuario responde al correo electrónico con sus datos personales, creyéndolo legítimo pregúntele a su proveedor o entidad [20].

Los usuarios desconfían gradualmente de este tipo de correo electrónico, por lo que los ciberdelincuentes fueron más allá al introducir enlaces a sitios web sospechosos. Entidad, en realidad es una página fraudulenta, imitando la página original, y se utiliza para capturar datos de usuarios, contraseñas, etc. La perfección de estos la página está en curso. Use un nombre similar o incluso el mismo que el nombre original, pero con contenido falso de otros servidores. "Windows Ventana emergente "en la que no aparece ninguna dirección visible.

FASE DE ATAQUE

- Actualmente, fraude que implica una participación "moderada" o "alta" La víctima necesita participar en la competencia, porque como abrir un correo electrónico, Visite la web o realice una búsqueda de El ataque es perfecto.

En lo que a tareas se refiere, no hay tareas comunes, depende de su tipo Phishing seleccionado. Por lo tanto, en el primer caso, el foco del ataque está en el servidor

[20] NGO, Quoc-Dung, NGUYEN, Huy-Trung, NGUYEN , Le-Cuong y NGUYEN, Doan-Hieu. A survey of IoT malware and detection methods based on static features. ICT Express, 2020, no. xxxx, doi: 10.1016/j.icte.2020.04.005.

Compañía o institución objetivo, mientras que los otros dos tipos son de comunicación o Prepare trampas para las víctimas de diferentes formas.

4.1.7 VISHING

Es un Phishing por voz, es decir una estrategia de fraude electrónico en el que el atacante engaña a su víctima para que le revele información confidencial, esta táctica no siempre requiere del internet para efectuarse pues se realiza mediante tecnología de voz, ya sea correo electrónico de voz, VoIP o por celular o teléfono fijo. En general se emplea para delitos financieros, es decir obtener números de cuenta y otros datos confidenciales. Para su ejecución muchas veces se emplea una técnica de falsificación de identificador de llamadas lo que les permite que las llamadas que se emplean para el ataque parezcan legitimas o de una fuente confiable [21].

Para prevenir ataques de vishing es recomendable tener las siguientes recomendaciones:

- Procurar no responder a números desconocidos
- Si la llamada es tomada, no entregar información confidencial
- Emplear una aplicación de identificación de llamadas
- Si es una entidad conocida la que le realiza la llamada, cerciorarse acudiendo a la misma.

El vishing usa el teléfono como herramienta. Se basa en el uso de Software llamado "War Dialer" cuya función es realizar llamadas desde la computadora usando tecnología de teléfono IP. Una vez él después de que el usuario atacado descuelgue, se activará una grabación para intentar convencerlo o visita el sitio web para proporcionar sus datos personales o usted directamente "Confirma" tus datos en la misma llamada. Problemas reales de este tipo el ataque es la confianza de la gente en el teléfono y el uso del teléfono. Las empresas tradicionalmente legales lo han hecho. El término "phishing" afirma ser conocido España tiene el 41,2% de los usuarios de Internet, pero hay pocos otros tipos de fraude Identificado. Así, por ejemplo, el 21,6% de los usuarios de Internet afirman saber ¿Qué es "estafa" y "engaño" (8,1%), "esperanza" (4,1%) y "esperanza"? (3,7%) de uso frecuente red [22].

4.1.8 PHARMING

[21] ASHVINI, Dheshmukh, PARIKSHIT, Mahalle. Survey on Linux Security and Vulnerabilities. Maharashtra, India.: Department of Computer Engineering , Smt. Kashibai Navale college of Engineering, University of Pune, Ijecs.In, 2014. 3, 8265–8269. Retrieved from http://www.ijecs.in/issue/v3-i9/58 ijecs.pdf

Este es un ataque que se encarga de dirigir usuarios de un sitio Web legítimo y confiable a un sitio malicioso, empleando la estrategia de DNS cache envenenamiento, el sitio web falso les permite a los estafadores obtener información importante de sus víctimas para acceder a sus finanzas, una de las formas de ejecutar el ataque es modificando el archivo Host, el atacante secuestra la computadora y lleva al usuario a un sitio falsificado.
Precauciones para prevenir Pharming.

- Emplear un proveedor de servicios de internet confiable y legítimo.
- Contar con un software robusto de antivirus
- Tener actualización de los programas de los equipos que se empleen.
- Utilizar la URL correcta de los sitios web visitados
- Verificar el certificado
- Verificar la dirección HTTP
- Buscar icono de candado bloqueado o una llave que indica una conexión segura.

El título incluye todas las formas de phishing basadas en: Interferencia con el proceso de búsqueda de nombres de dominio (traducción de nombres de dominio) Dirección IP ingresada en el navegador). No hay duda de que los productos farmacéuticos se supone que este nombre habitual para cometer este delito es más peligroso que algunas otras variantes que se han analizado, porque la cooperación de la víctima es menor y el disfraz que usa la víctima el criminal parece más real.

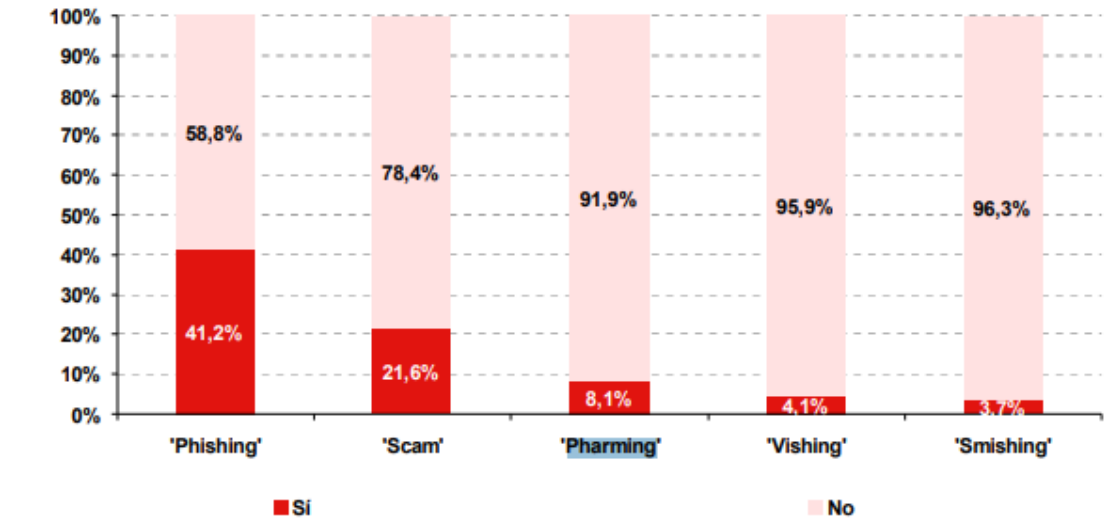

Figura 2 Nivel de conocimiento declarado sobre términos relacionados con el fraude online. (%)

4.1.9 DOS

Los ataques de denegación de servicio se basan en agotar los recursos del cliente para que se posible atender una solicitud de un usuario legítimo, el atacante mediante internet al ancho de banda y la conectividad, el delincuente toman los puntos y los inunda con una gran cantidad de paquetes de manera que este se sature y se bloquee al intentar atender todas las solicitudes que le llegan. Estos ataques son a nivel de red, a nivel de aplicación, a nivel de sistema operativo y a nivel de datos que en este caso es el que se quiere tratar. El problema de este ataque es que la preocupación principal no son precisamente el contenido de los paquetes sino más bien la cantidad, y que significa que los protocolos de red normales como se van a degradar. Una evolución de este ataque es el ataque DDoS el cual emplea varios puntos que atacar y enviar paquetes desde distintas maquinas con el mismo propósito que la primera víctima sean los servidores al saturarse, y posteriormente cuando se instala un software algunas computadoras procede a comprometer otros sistemas vulnerables instalando además un software de ataque, los sistemas que el atacante controla se denominan bost, y cuando una red completa es infectada se llama botnet, estos agentes son los que realizan el trabajo de enviar gran cantidad de paquetes al servidor por orden del delincuente informático, y este agota sus recursos rápidamente.

4.1.10 ESCALADO DE PRIVILEGIOS

El escalado de privilegios es un ataque que se basa en la explotación de una vulnerabilidad, falla o mala configuración de alguna aplicación se emplea para obtener acceso a recursos del sistema que usualmente tiene protección, al obtener más privilegios el atacante lleva a cabo acciones malintencionadas que ponen en peligro la seguridad de los sistemas.

Cada sistema cuenta con usuarios a los que se les atribuye ciertos privilegios, esos determinan que acciones pueden tomar o que puede llevar a cabo dentro del sistema.
Los atacantes además de intentar obtener privilegios físicamente también lo pueden realizar remotamente. A través de aplicaciones con consultas que les permiten a los atacantes tener más permisos de los que deberían tener al momento de hacer uso de ellas, el escalado de privilegios puede traer grandes consecuencias que pueden involucrar perdida de información, daño en los sistemas, configuración de los sistemas, daño en lo equipos, etc.

4.1.11 SNIFFING

El sniffing es una técnica empleada para escuchar el tráfico de la red, y captura la información, de donde se saca provecho como contraseñas, información confidencial entre otras cosas, esta información es capturada por el delincuente, se

puede realizar físicamente por medio de un hardware o mediante un software, cuando esta técnica alcanza al servidor de base de datos podría extraer cualquier tipo de información, por tal razón se recomienda emplear técnicas criptográficas para él envió de información [23].

Como los circuitos telefónicos, también lo son las redes informáticas canales de comunicación compartidos, simplemente son demasiado costosos. El conmutador (concentrador) de cada par de computadoras involucradas en la comunicación. Indica que la computadora puede recibir información enviada a otras máquinas. La captura de información que pasa a través de la red se denomina rastreo. Por lo general, el método para conectar varias computadoras es a través de Ethernet. El protocolo Ethernet funciona enviando información de paquetes a todos los hosts en el mismo circuito, el encabezado del paquete contiene la dirección apropiada la máquina objetivo. Solo las máquinas con direcciones de cabecera pueden debería aceptar el paquete. Una máquina que acepta todos los paquetes. No importa lo que ponga en el encabezado del paquete, se llama modo promiscuo[24].
La siguiente figura muestra el proceso de diálogo entre dos máquinas de ubicación remota, pases de identificación de usuario máquina a otra. Este ejemplo es la transferencia de archivos a través de FTP: (Máquina A Inicie la conexión con la máquina B y solicite el ID de usuario. A Para autenticarse en la computadora remota B, el rastreador capturará la clave.)

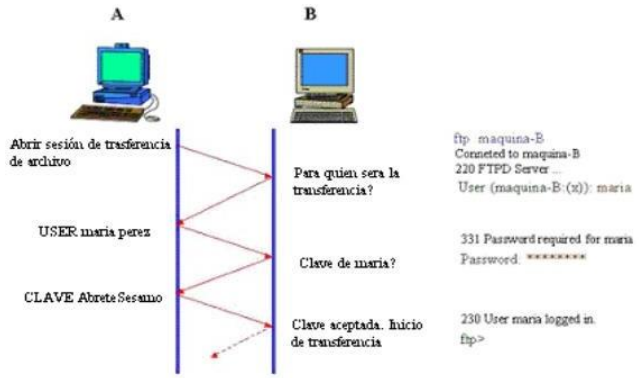

Figura 3 Sniffing

4.1.12 MALWARE

Son programas informáticos malicioso que son diseñados por delincuentes para causar algún tipo de daño ya sea sobre la información, en el sistema operativo o en

[23] MORA RODRÍGUEZ, David, y MUÑOZ, Mario. Memory Corruption Failures Attack and Defense Techniques. Revista Ingenierías Universidad de Medellín. 2011. 10, 149–158. ISSN 1692-3324.
[24] KIGERL, Alex. Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories [en línea]. Washington: Social Science Computer Review, 2017. [Fecha de

las aplicaciones e inclusive apoderase de los equipos, los malware pueden ser detectados si se usa las herramientas adecuadas, normalmente estos códigos maliciosos pasan inadvertidos. Existen formas de evitar los malware y son dos sencillas acciones estar atento a actividades sospechosas y contar con una buena seguridad para los equipos, los servidores y la red [25].

Malware o software malicioso (malware), se refiere a cualquier programa o aplicación, que después de infectar el sistema informático víctima, con el objetivo de destruir diferentes formas de sistemas informáticos (El malware afecta a diferentes sistemas según el tipo de malware) sin la intención del usuario. Según su comportamiento, el malware se puede dividir en gusanos, software espía, caballos de Troya, Ransomware y otro software que se describe a continuación; de lo anterior, se puede decir que el malware se refiere a Cualquier tipo de código malicioso o amenaza Cálculo del tipo de lógica, incluso si solo se llama virus[26].

Principales Clases de Malware

Virus: si se ha desarrollado una aplicación o un programa para causar un mal funcionamiento Sistema operativo, archivos del sistema de ataque (generalmente Aplicaciones), modificarlas o eliminarlas; requisitos para su activación y propagación ejecute la aplicación infectada[27].

Gusano: esta Incrustado en los archivos propios del sistema, apunta a ejecutar y Difundir sin intervención usuario.

Spyware: se refiere a un archivo instalado en el sistema, generalmente con propósito de recopilar información del usuario almacenado en el sistema informático sin autorización; esta información se envía a los desarrolladores de software espía suelen utilizar publicidad.

Troyanos: Están diseñados para permitir secretamente e Instale gusanos o software espía de forma remota; estos suelen estar alojados en el programa. Aplicación, la simulación es legal, entonces permanecerá en silencio cuando se ejecute.

Adware: estos están alrededor de los anuncios y se pueden generar automáticamente una ventana con anuncios que dirige a los usuarios a sitios de

[25] BREWER, Ross. Advanced persistent threats: Minimising the damage. Network Security, 2014, 5–9. https://doi.org/10.1016/S1353-485870040-6

[26] CRISTIAN LUGA, Jason y EROLA, Arnau. Baiting the Hook: Factors Impacting Susceptibility to Phishing Attacks [en línea]. Oxford: Human-Centric Computing and Information Sciences, 2016.

[27] FREIRE FAJARDO, Franklin. Plan de Contingencia Ante Ciberataques [en línea]. Tesis de Maestría. Escuela Superior Politécnica del Litoral, 2017 [consultado 11 mayo 2020]. Disponible en https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf FREIRE FAJARDO.FREIRE FAJARDO.FREIRE FAJARDO, “Plan de Contingencia Ante Ciberataques.”

publicidad, en algunos casos, también recopilan información sobre hábitos Las visitas del usuario (el tiempo que se conectó en un día, Quién visitará, etc.).

4.1.13 DESBORDAMIENTO DE BUFFER

Este se trata una gran cantidad de información que se envía por medio de formularios, y la aplicación recibe mucha más información de la que es capaz de soportar, esto genera un error en de software y puede generar que el programa realice acciones no previstas, este es un fallo de programación.

El desbordamiento de búfer ocurre cuando el programador no controla el espacio que Memorice el programa, y luego alguien puede ingresar su propio código en este espacio de memoria, la máquina lo ejecutará antes de realizar cualquier operación. Por ejemplo, otra tarea suele ocurrir con frecuencia en la carga útil Inyecte una cierta cantidad de memoria, incluso dentro de la puerta trasera, inyecte una cierta cantidad o una cierta cantidad en la memoria RAM Code, incluso inicia toda la parte del sistema antes de que comience operación o ciertos archivos en el mismo sistema de inicio normal. La ***figura 4*** muestra un ejemplo de desbordamiento buffer.

Figura 4 Desbordamiento de Buffer[28]

5 ANÁLISIS DE LA SEGURIDAD EN EL ENTORNO PRESENTE DE LA PLATAFORMA DE WINDOWS

Análisis de amenazas presentes en los entornos computacionales, vinculando sistemas operativos, redes y bases de datos como estrategia defensiva ante ciber-ataques sobre la plataforma Windows.

[28] FAJARDO DIAZ, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el Mercado colombiano. Tesis de pregrado, 2017. Instituto Universitario Politécnico GranColombia.

Aquí se debe describir las vulnerabilidades físicas, lógicas, tipos de vulnerabilidades como desbordamiento de buffer, errores de configuración, errores web, errores de protocolo, entre otros. También hablar sobre la detección de vulnerabilidades, métodos de escaneo. Muchas de estas vulnerabilidades mencionadas generan problemas de seguridad ya que llegan a través del sistema operativo, donde los ciber-atacantes logran explotar la información de los usuarios y comprometen totalmente su privacidad y seguridad. En Windows los fabricantes lanzan parches de seguridad, pero estos no siempre están disponibles y no se instalan correctamente [29].

En Windows nuevas variantes de ciber-ataques son conocidas como vulnerabilidades de canal lateral de ejecución especulativa y a estas se les han asignado los siguientes CVE:

- CVE-2018-11091- “Memoria no almacenable en cache de muestreo de datos de microarquitectura”.
- CVE-2018-12126- “Muestreo de datos de búfer de almacén de microarquitectura (MSBDS)”.
- CVE-2018-12127- “Muestreo de datos de búfer de relleno de microarquitectura (MFBDS)”.
- CVE-2018-12130- “Muestreo de datos de puerto de carga de microarquitectura (MLPDS)”.

El tratamiento para mitigar las amenazas puede ayudar a identificar los sistemas afectados por las vulnerabilidades CVE. Entre las acciones determinantes se encuentra el impacto de rendimiento potencial el cual puede variar según el hardware del equipo y según se ejecuten cargas en el sistema. La configuración más común es tener la tecnología Hyper-Threading habilitada.

5.1 ESTRATEGIAS Y PATRONES QUE SUMINISTRAN UN ANÁLISIS SOBRE LAS VULNERABILIDADES PRESENTES EN WINDOWS

Se describen las estrategias que permitirán tener un análisis sobre las vulnerabilidades en la plataforma de Windows, dando soporte a planes de seguridad en Windows. También se hace una descripción de las vulnerabilidades más importantes en este sistema operativo y de cómo estar al tanto de cualquier ciber ataque.

5.2 PLANES DE SEGURIDAD

Es un planteamiento de unas medidas de seguridad que sirven de guía a las empresas para la reducción de los riesgos, es un plan que le precede al análisis de

[29] MEADOWS, Oliver. Window Safety Devices. J. Pediatr. Heal. Care, 2010, vol. 24, no. 3, pp. 199–202, doi: 10.1016/j.pedhc.2009.12.002

riesgos, en este plan la prioridad es la seguridad de la información por lo tanto todos los esfuerzos están dirigidos a salvaguardar los recursos que están relacionados directa o indirectamente con esta y solventar situaciones que pongan en riesgo la estabilidad, confiabilidad, integridad y disponibilidad del sistema de información [30].

Para la realización de este plan es necesario tener en cuenta en un primer momento los objetivos estratégicos organizacionales, y en una alineación con estos mismos contribuir en su cumplimiento, integrando la seguridad como obligación y de esta manera integrar nuevas prácticas para la modernización del manejo organizacional de cada proceso y función que tiene el personal a cargo.

Las acciones que le preceden a un plan director se encuentran a continuación y constituyen lo que se debe lograr a partir de un estudio estructurado de la situación de la organización:

- Cuantización y valoración de los riesgos de la organización, cada uno de los riesgos obtenidos en el análisis de riesgos deben ser estudiados y relacionados con cada una de las áreas para determinar las acciones a seguir para controlarlas y eliminar las situaciones de amenaza.
- Las acciones estratégicas que debe establecer el plan director son pre diseñadas para contrarrestar el impacto que los incidentes de seguridad pueden tener sobre el sistema de información, y además prever futuras situaciones que sean riesgosas.
- La estructura organizacional se modifica a manera que apoye las mejoras del plan director, con un marco de trabajo que opere de acuerdo con las necesidades de seguridad global.
- Establecer una métrica de la seguridad, que sean fácil de controlar y realizar un seguimiento, así como dar prioridad a las acciones de mejora que se requieran de forma inmediata para disminuir el nivel de riesgo.
- Incorporación de métodos, mecanismos y procesos de seguridad dentro de la operatividad normal de las empresas, con soporte de la dirección que avala cada una de las acciones en pro de mejora.
- Establecer tácticas de progreso y evolución de los sistemas, teniendo en cuenta la seguridad parte fundamental de los mismos, yendo a la par con los avances tecnológicos.

Para llevar a cabo los planes de seguridad es recomendable implementar estrategias que permitan una protección de los datos y cuentas sobre los equipos

[30] ÁLVAREZ, G., & Pérez, P. Seguridad informática para empresas y particulares. 2004. https://doi.org/978-84-481-4008-3

que manejan el sistema operativo de Windows. En estas estrategias tenemos las siguientes:

1. **Ofrecer formación:** Donde mantener a los empleados de la empresa mejora la concienciación sobre la seguridad. Debe de ser un tipo de formación continuo, para que tengan precaución de las amenazas cibernéticas que normalmente están al asecho.
2. **Tener cuidado con las contraseñas:** Hay que asegurarse de seguir las reglas básicas para no tener ningún tipo de robo de esta información en las cuales están: cambiar la contraseña predeterminada, utilizar contraseñas diferentes para cada cuenta, crear contraseñas seguras que contengan letras, números y símbolos.
3. **Mantener actualizada la tecnología:** Se debe asegurar que las aplicaciones y el sistema operativo siempre se encuentre actualizado, lo cual permite la instalación de parches de seguridad para los equipos.
4. **Consigue una EPS:** La EPS (solución de seguridad de endpoints) protege todos los endpoints de diferentes dispositivos como portátiles y móviles para evitar malware que cause daños como robo de datos.

5.3 DESARROLLA EN BUENAS PRÁCTICAS DE SERVICIOS EN VULNERABILIDADES SOBRE EL SISTEMA OPERATIVO

Las buenas prácticas, se refieren a recomendaciones orientadas al manejo de los recursos involucrando la seguridad de la información en todos y cada uno de los procesos y los procedimientos organizacionales [31], el documento de buenas prácticas engloba un grupo de normas básicas que deben ser de conocimiento general en las empresas para que con un esfuerzo conjunto se factible incluirlas dentro del actuar cotidiano de la empresa [32].

5.3.1 ACTUALIZACIÓN DEL SOFTWARE

- La actualización del software se debe realizar mediante sitio de confianza que no implique riesgo para el sistema, la mejor opción para actualización es emplear un sitio oficial ofrecido por el fabricante.
- Para las organizaciones es necesario disponer de políticas que involucren las actualizaciones como una obligación corporativa, que les atribuya una

[31] DHESHMUKH, A., & Mahalle, P. Survey on Linux Security and Vulnerabilities. *Ijecs.In*, 2014. *3*8265, 8265–8269. Retrieved from http://www.ijecs.in/issue/v3-i9/58 ijecs.pdf

[32] BASHAH, A., Ali, M., Yaseen, A., Shakhatreh, I., & Syazwan, M.. Procedia Computer SQL-injection vulnerability scanning tool for automatic creation of SQL-injection attacks. *Procedia Computer Science*, 2011. *3*, 453–458. https://doi.org/10.1016/j.procs.2010.12.076.

responsabilidad a la empresa sobre la gestión y administración de parches de seguridad sobre los sistemas operativos y las aplicaciones

5.3.2 SEGURIDAD EN SISTEMA OPERATIVO

- La configuración del sistema operativo para prevenir posibles situaciones de riesgo se describe a continuación:
- Desactivar las carpetas compartidas para evitar la infiltración de posibles ataques por medio de este segmento.
- Hacer uso de contraseñas lo sumamente robustas, que impidan la fácil detección pro medio de herramientas de fuerza bruta.
- El perfil que sea designado para el usuario, no debe tener privilegios elevado, esto aumenta la vulnerabilidad sobre el sistema, en un inicio las cuentas de usuario poseen privilegios administrativos que deben ser modificado para elevar la seguridad.
- Contar con una plataforma moderna que cuente con actualizaciones y soporte técnico.
- Impedir la ejecución automática de los medios extraíbles como medios USB, pues son de los medios utilizados para propagar un ataque.
- Configurar las características para los archivos ocultos, pues son comunes archivos maliciosos con atributos de esta índole.

Verificar que las extensiones de los archivos se mantengan visibles, de esta manera será posible identificar cuando una extensión no corresponde al archivo que se encuentra allí, y podría significar una alerta de ataque.

5.3.3 SEGURIDAD EN CORREO ELECTRÓNICO WINDOWS O LINUX

- El correo electrónico es uno de los medios más empleados por el cual se propagan de mayor forma los malware actualmente, por tal razón es uno de los medios de comunicación en el cual se debe orientar los esfuerzos para que este no represente una debilidad o vulnerabilidad para los sistemas de información.
- El spam es una de las principales estrategias para filtrar códigos maliciosos, por tal razón es indispensable realizar un examen exhaustivo al archivo adjunto que contiene el spam antes de aplicar cualquier acción sobre el mismo.
- Verificar los archivos adjuntos pues puede estar sujetos a duplicación de extensión.

- No hacer de conocimiento público en la red la cuenta de correo electrónico en especial en sitios de poca confianza, esto evitara que esta cuenta de conocimiento de los spammers.
- Emplear filtro anti-spam que hagan efectivo la depuración de correo no deseado.
- La contestación a un spam, implica colocar aún más en riesgo lo cuenta por lo tanto es mejor no hacer uso de estos mensajes y eliminarlos sin darles contestación.
- Emplear una cuenta alternativa que no deje expuesta la cuenta de correo electrónico personal.
- Usar claves seguras, y además que sean cambiadas en un pequeño lapso de tiempo.
- Emplear otra forma de seguridad habilitando una pregunta secreta, le dará un nivel más alto de seguridad.
- La cuenta de correo electrónico debe ser debidamente configurada para que ningún documento de cualquier formato sea descargado antes de ser examinado, y dado el caso de que contenga un código malicioso bloquearlos por completo [33].

5.3.4 SEGURIDAD EN NAVEGADORES

- Examinar detenidamente el contenido que se desea descarga en especial cuando son aplicaciones que van a ser ejecutadas, y tener en cuenta las políticas de seguridad que estas mismas puedan tener para verificar su integridad.
- Realizar las configuraciones pertinentes sobre el navegador para disminuir el nivel de riesgo y exposición al navegar en internet.
- La implementación de antivirus y firewall resultan ser dos soluciones que aportan en gran manera a la detección de códigos maliciosos, así como permite también bloquear comunicaciones de entrada y de salida.
- Es preciso eliminar cada vez que se haya terminado la navegación cualquier información que sea vulnerables como cache, direcciones URL, cookies, contraseñas, archivos temporales o formularios, que dejan al descubierto información confidencial.
- Los sitios que no representan ninguna confiabilidad deben ser bloqueados totalmente del navegador de esta manera s evitar cualquier riesgo de propagarse un ataque teniendo como fuente el navegador.

[33] ÁLVAREZ, G., & Pérez, P. Seguridad informática para empresas y particulares. 2004. https://doi.org/978-84-481-4008-3

5.3.5 SEGURIDAD P2P

- Además de la implantación de un antivirus muy efectivo, es preciso tomar medidas con respecto al almacenamiento de información, cualquier información de tipo confidencial no debe almacenarse en el equipo que pertenece a la red p2p y por la cual se comparte otro tipo de información.
- Tomar medidas para lograr comprobar la integridad de los archivos descargados, verificar tamaño de la información entre otras características.
- La carpeta de intercambio por red debe contener únicamente los archivos que se desean compartir, y la configuración del programa cliente debe estar debidamente configurada para mejorar la seguridad en la comunicación [34].

5.3.6 SEGURIDAD EN SISTEMAS REMOVIBLES

- Desarrollo de políticas de seguridad que involucren el buen manejo de los sistemas extraíbles como memorias USB, discos duros, CD, DVD, SD, etc, que involucren los efectos del mal manejo de estos y el riesgo que implican para los sistemas de información.
- Asignar un acceso limitado los usuarios que haga manejo de estos dispositivos, habilitando y deshabilitando los puertos, dependiendo de la amenaza que representen.
- Para ciertas áreas de las organizaciones es necesario inclusive prohibir el uso de estos mismos con el fin de salvaguardar su integridad.
- Cuando estos sistemas son los que se emplean para hacer el transporte de la información confidencial se deben aplicar técnicas de seguridad sobre las mismas para que la información se encuentre protegida en todo momento, por medio de cifrado o estenografía.
- Emplear un antivirus que permita examinar unidades extraíbles.
- Realizar una configuración correcta en lo que concierne a la ejecución de los dispositivos extraíbles en los sistemas operativos, deshabilitando esta función para poder analizar el sistema detectado.

5.3.7 COPIAS DE SEGURIDAD

Como buena práctica de seguridad es preciso realizar copias de seguridad de cualquier información como software, imágenes y sistemas y almacenarla en una ubicación distinta de manera que se evite la perdida de información dado el caso de un incidente. Es necesario llevar a cabo algunas recomendaciones que contribuyan a realizar correctamente las copias de seguridad de un sistema de información:

[34] MIRA ALFARO José, y MONTAÑA, Rogelio. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Tesis. 2002. 1, 1–142.

- Llevar un control sobre las copias de seguridad que se realizan, por lo tanto, se generara un registro por cada vez que se efectúe esta opción y se documentara la restauración del sistema a partir de la copia de seguridad.
- Definir un alcance, sobre que método es más favorable según las necesidades de restauración.
- Determinar el sitio de almacenamiento de las copias de seguridad en un área remota
- Ejecutar el cifrado de la información para salvaguardar su confidencialidad en caso de ser extraída por un atacante.

5.3.8 SEGURIDAD DE LA MENSAJERIA

Es indispensable evitar el uso de estos dos tipos de comunicación dentro de la organización, pues son métodos altamente vulnerables a ataques, y generan un vector por el cual los atacantes pueden acceder a la red local.

5.3.9 ANÁLISIS DE AMENAZAS 2019 DE SOPHOSLABS

Hay una clase de vulnerabilidad en el editor de fórmulas (componente de Excel) Está instalado de forma predeterminada, simplemente abra la hoja de trabajo para llamarlo Las piedras te hacen vulnerable a las infecciones. No es necesario habilitar ningún script de macro; El ataque ya está en curso y normalmente termina en menos tiempo del que se tarda en completarlo. Lee esta frase.

Microsoft es consciente de estas vulnerabilidades (les dio el nombre de código CVE-2017- 11882 y CVE-2018-0802) y lanzó varias actualizaciones a mediados de 2017 Productos de la suite de Office para evitar su uso, pero no todo el mundo recibe todas las actualizaciones, incluso si hay actualizaciones, algunas empresas pospusieron el lanzamiento de actualizaciones con fines de prueba, ya qué ha sucedido desde el error (incluso el error de prueba de concepto) que se convirtiese en dominio público, generalmente porque ***Microsoft*** ha lanzado uno o más. Actualice los parches hasta que las víctimas potenciales los reciban. Realmente peligroso[35].

Entre los documentos maliciosos analizados por SophosLabs en pruebas recientes, hay tres cuartas partes que son creadas por herramientas de tres generaciones. Parece que Cada generador tiene varios clientes principales (editores de malware) en la lista Cliente: Threadkit es el generador preferido de malware Trickbot y Los

[35] SOPHOS. Informe de Amenazas 2019 de SOPHOSLABS. Sophos, p. 27, 2019, [En linea]. Disponible en: https://www.sophos.com/es-es/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf.

distribuidores de FareIt y LokiBot utilizan principalmente lo que llamamos generadores EQN_kit.

Extensión de archivo	Detalles del tipo de archivo	Componente de Windows
.CHM	Ayuda HTML compilada	Archivo ejecutable de ayuda HTML (hh.exe)
.CMD	Archivo de comandos de Microsoft	Shell
.CPL	Panel de control	Shell
.DOTM	Plantilla de documento habilitado para macros	Word.exe
.HTA	Aplicación HTML	Windows Script Host (wscript.exe)
.JAR	Aplicación Java	java.exe
.JS	Javascript	Windows Script Host (wscript.exe)
.LNK	Acceso directo de Windows	Shell
.PIF	Archivo PIF	Shell
.PS1	Script de PowerShell	powershell.exe
.SCF	Archivo de comandos de Shell	Shell
.VBS	Script de Visual Basic	Windows Script Host (wscript.exe)
.WSF	Archivo de script de Windows	Windows Script Host (wscript.exe)

Figura 5 Tipos de archivo de riesgo

Durante este período, la gama de documentos que pueden considerarse peligrosos se ha ampliado. Cubre una variedad de tipos de archivos de ***Windows*** en los últimos dos años, no todos los archivos ejecutables. Esta es una breve lista de algunos tipos de archivos Además de las aplicaciones .exe tradicionales (estamos en una gran cantidad de malware y otros ciberataques contra computadoras con ***Windows***.

Cuando estos tipos de archivos se utilizan como correo electrónico, los archivos maliciosos, generalmente están en formato de archivo comprimido (p. Ej. Zip, rar, ace, y .gz, también se pueden proteger con contraseña para omitir Detección automática más eficaz.

5.3.10 ESTADÍSTICAS DE SEGURIDAD INFORMÁTICA QUE IMPORTAN EN WINDOWS

Los ataques cibernéticos y las brechas de seguridad son cada vez más comunes, por lo que proteger la computadora de sus intereses académicos y su propia computadora es más importante que nunca. Así como algunos hogares tienen sistemas de alarma para prevenir intrusos, un hogar debe tener el mismo nivel de seguridad para evitar ataques virtuales[36].

[36] TOVAR VALENCIA, Orlando. Inyección De Sql , Tipos De Ataques Y Prevención En Asp . Net - C#. Universidad Piloto de Colombia. 2014, pp. 1–9.

Claramente, la mayor amenaza radica en los piratas informáticos de sombrero negro. No solo obtienen acceso no autorizado a redes y sistemas, sino que también realizan ataques de phishing, ransomware y cryptojack con fines de lucro. El mundo de la seguridad digital está en constante evolución, por lo que es importante comprender la última tecnología para proteger su equipo. Para ilustrar el estado actual de la seguridad informática, compartiremos estadísticas sobre este tema, que son fundamentales para entender los diferentes ataques en los sistemas de ***Windows***:

SEGURIDAD INFORMÁTICA

- El 70% de las organizaciones cree que sus riesgos de seguridad han aumentado drásticamente en 2017.
- Se estima que para 2020, la cantidad de contraseñas utilizadas crecerá a 300 mil millones.
- Windows es el sistema operativo más atacado, seguido de Android.
- El número de variantes de malware cryptojack aumentó de 8 en 2017 a 25 en mayo de 2018.
- El costo total de un ciberataque exitoso es de más de $ 5 millones, o $ 301 por empleado.
- Los dos ataques más comunes son el malware y los ataques basados en web. El gasto de la empresa en defensa se estima en 2,4 millones de dólares.
- Cada día se producen más de 4000 ataques de ransomware.
- El 91% de los ataques comienzan con técnicas de spear phishing, que están diseñadas para invadir correos electrónicos e infectar organizaciones.
- Una encuesta a más de 1300 profesionales de TI encontró que el 56% de las organizaciones consideran el phishing como el mayor riesgo de seguridad de TI.
- Kaspersky detectó 246,231,645 intentos de phishing en 2017, un aumento de 91 millones en comparación con 2016.

5.3.11 ESTADÍSTICA DE CIBER AMENAZAS EN TIEMPO REAL DE KASPERSKY EN SISTEMAS DE WINDOWS

Kaspersky es uno de los antivirus más usados en la plataforma de Windows ya que su programa provee diferentes tipos de seguridad que permiten a los usuarios navegar con más tranquilidad por los sitios web. En la ***Figura 6 y 7*** se observa la cantidad de infecciones locales en el mes de noviembre del 2020 en Colombia estas graficas están soportadas en la página web de Kaspersky de ciber amenazas en tiempo real, la ***Figura 8 y 9*** se evidencia la cantidad de amenazas web y su listado de ataques, en la ***Figura 10 y 11*** se observa la gráfica de ataques a redes en Colombia con sus respectivos listados de ataques todo esto en la plataforma de Windows, la ***Figura 12 y 13*** muestra la gráfica de vulnerabilidades, la ***Figura 14 y 15*** representa la gráfica de correo infectado y su lista de ataques más frecuentes y

por último la ***Figura 16*** es la gráfica de Botnet la cual se mantiene en un estado neutro en el mes de noviembre del 2020 en el país de Colombia[37].

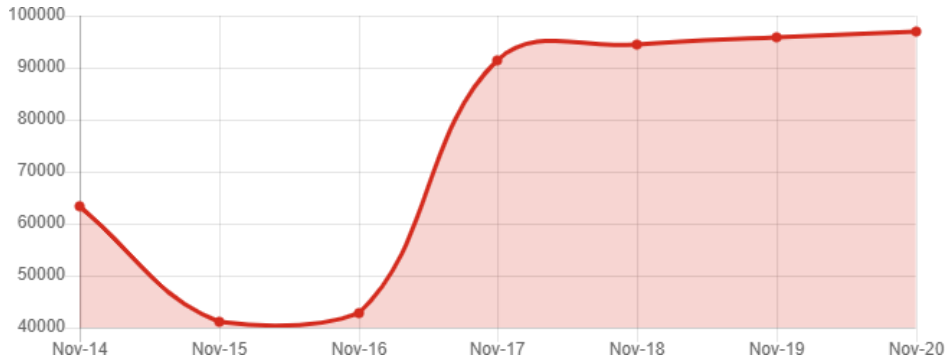

Figura 6 Infecciones locales en el mes de noviembre del 2020

Arriba - Infecciones locales EN EL ÚLTIMO SEMANA		
1	HackTool.Win32.KMSAuto.gen	10.71%
2	DangerousObject.Multi.Generic	6.81%
3	Virus.Win32.Renamer.j	6.64%
4	HackTool.MSIL.KMSAuto.dh	6.49%
5	HackTool.MSIL.KMSAuto.di	5.54%
6	HackTool.MSIL.HackKMS.d	4.49%
7	HackTool.MSIL.HackKMS.a	4%
8	HackTool.Win32.KMSAuto.om	3.46%
9	HackTool.MSIL.HackKMS.aj	2.72%
10	Worm.Win32.WBVB	2.66%

Figura 7 Lista de las infecciones locales en el mes de noviembre del 2020

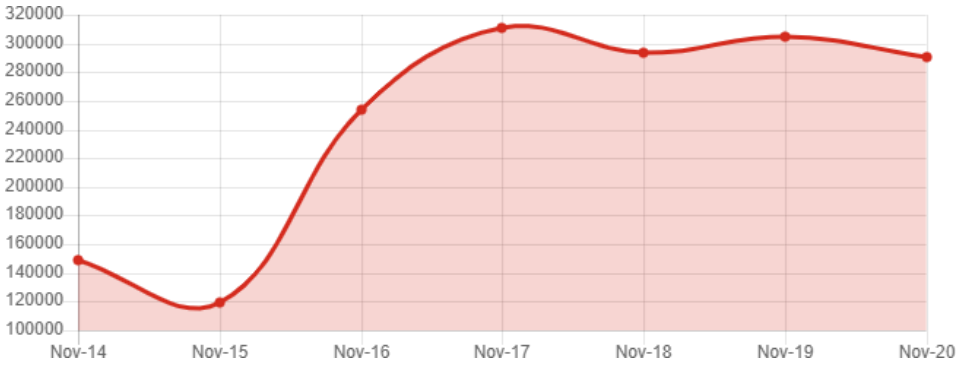

Figura 8 Amenazas web

[37] RUTKIN, Aviva. The health hackers. New Scientist. 2015. 2273028, 18–19. https://doi.org/10.1016/S0262-407930690-4.

Arriba - Amenazas web EN EL ÚLTIMO SEMANA		
1	Trojan.PDF.Badur.gen	24.49%
2	Trojan.Script.Generic	16.78%
3	Trojan.Script.Miner.gen	16.62%
4	Trojan-Downloader.Win32.Cabby.cgnu	9.47%
5	Exploit.Win32.CVE-2011-3402.a	9.04%
6	Trojan.Win32.Nion.gen	6.2%
7	Trojan-Downloader.Win32.Cabby.cdrg	4.24%
8	Trojan.Script.Redirector.gen	3%
9	Trojan.Multi.Preqw.gen	2.92%
10	Trojan.Win32.Vebzenpak	2.17%

Figura 9 Lista de las Amenazas Web

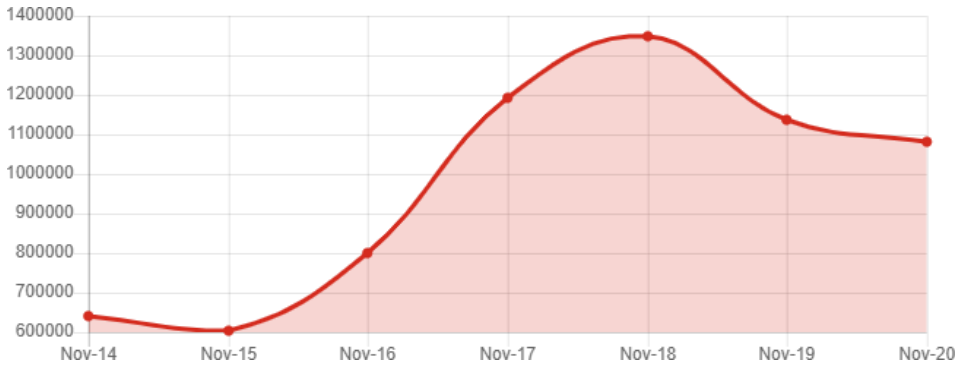

Figura 10 Ataque a redes

Arriba - Ataque a redes EN EL ÚLTIMO SEMANA		
1	Bruteforce.Generic.Rdp.d	74.44%
2	Bruteforce.Generic.Rdp.a	8.78%
3	Intrusion.Win.MS17-010.o	8.22%
4	Scan.Generic.PortScan.UDP	2.63%
5	Scan.Generic.PortScan.TCP	2.5%
6	Bruteforce.Generic.RDP	1.08%
7	Intrusion.Win.MS17-010.p	1.03%
8	DoS.Generic.Flood.ICMP	0.33%
9	Bruteforce.Generic.Rdp.c	0.29%
10	DoS.Generic.Flood.TCPSYN	0.29%

Figura 11 Lista de los ataques de redes

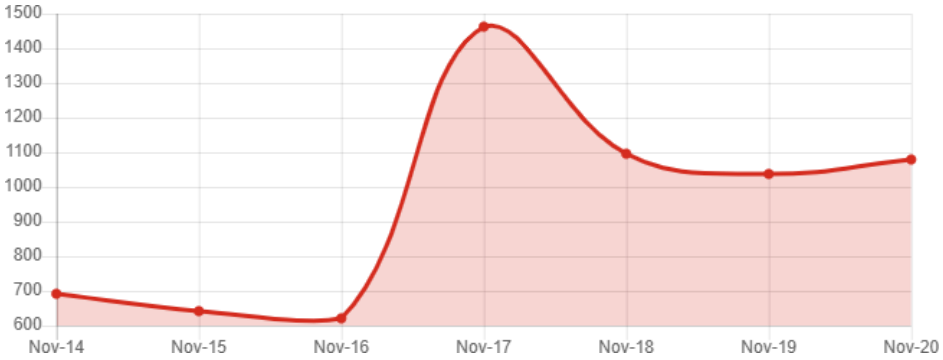

Figura 12 Vulnerabilidades

Arriba - Vulnerabilidades EN EL ÚLTIMO SEMANA		
1	Exploit.Win32.CVE-2011-3402.a	86.58%
2	Exploit.Win32.Generic	1.88%
3	Exploit.Win64.ShadowBrokers.d	1.51%
4	Exploit.Win32.CVE-2015-1701.gen	1.29%
5	Exploit.Win32.MS17-010.shc	1.16%
6	Exploit.Win64.ShadowBrokers.c	0.85%
7	Exploit.Win32.ShadowBrokers.z	0.77%
8	Exploit.MSIL.ShellCode.gen	0.57%
9	Exploit.Win32.ShellCode.gen	0.5%
10	VHO:Exploit.Win32.Generic	0.35%

Figura 13 Lista de las Vulnerabilidades

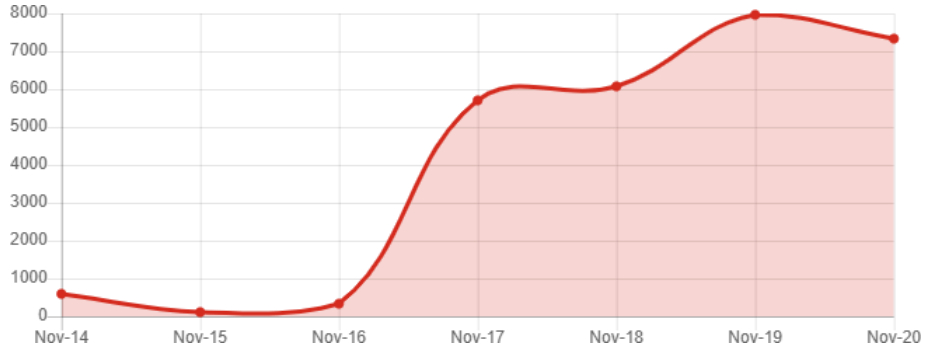

Figura 14 Correo infectado

Arriba - Correo Infectado EN EL ÚLTIMO SEMANA		
1	Backdoor.MSIL.Remcos.gen	28.93%
2	Trojan-Spy.MSIL.Noon.gen	13.83%
3	Trojan.Win32.ISO.gen	9.46%
4	Trojan.Win32.Delikle.vho	9.13%
5	Trojan-PSW.MSIL.Agensla.gen	8.17%
6	Trojan.PDF.Badur.gen	4.26%
7	Trojan-Downloader.PowerShell.Small.gen	3.02%
8	Trojan.Script.Generic	2.96%
9	Hoax.Script.Scaremail.gen	2.65%
10	Trojan.MSOffice.SAgent.gen	1.42%

Figura 15 Lista de los correos infectados

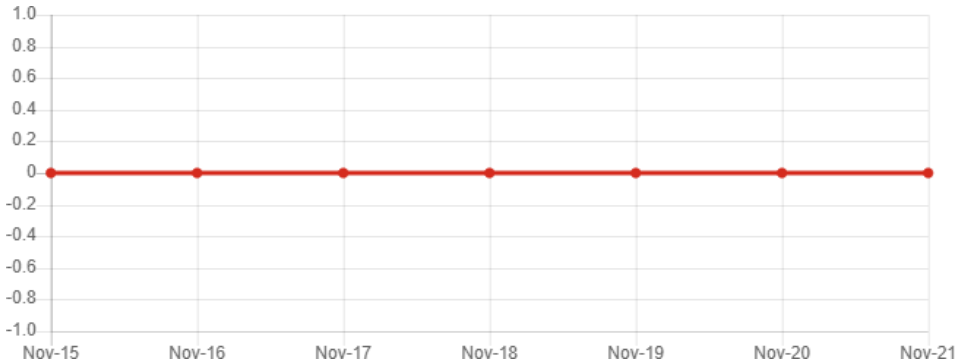

Figura 16 Botnet

6 APLICACIÓN DE LA METODOLOGÍA SOBRE LA VULNERABILIDAD EN EL SISTEMA OPERATIVO

Figura 17 Metodología

6.1 ALCANCE DEL PLAN DE SEGURIDAD INFORMÁTICA

El alcance de seguridad informática abarcará un radio de acción en el cual se ejecutará el plan, de acuerdo a los sistemas informáticos con objeto de protección, donde fueron determinados los riesgos del sistema de seguridad. Lo importante es dejar definido claramente el alcance para tener a priori una idea precisa de la extensión y los límites de vigencia [38].

.

- Evaluación de riesgos de seguridad a los que está expuesta la información.
- Selección de controles y objetivos de control para reducir, eliminar o evitar los riesgos identificados, indicando las razones de su inclusión o exclusión.
- Definición de política de seguridad.

[38] GARCÍA MONJE, Robert Alexander, Seguridad Informática Y El Malware. 2017, p. 11, Tesis de Licenciatura. Universidad Piloto de Colombia [en linea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2641

Durante la revisión del alcance del sistema de seguridad informática se deben de tener en cuenta etapas muy importantes:

1. Determinar las necesidades de protección del sistema informático objeto de análisis, como la caracterización del sistema, identificación de los atacantes y estimación de esos riesgos.
2. Implementar y ejecutar acciones de seguridad que garanticen minimizar los riesgos identificados en la primera etapa, se deben definir las políticas de seguridad.
3. Evaluar el sistema de seguridad informático diseñado.

6.2 CARACTERIZACIÓN DEL SISTEMA INFORMÁTICO

En esta se describirá de forma detallada el sistema informático, precisando los elementos que permitan identificar las particularidades en el sistema operativo de Windows [39], sus principales componentes, información y tecnologías de información, considerando entre otros:

1. Bienes informáticos, su destinación e importancia.
2. Servicios informáticos y de comunicaciones disponibles
3. Características del procesamiento, transmisión y conservación de la información, teniendo en cuenta el flujo inter y externo y los elementos de clasificación de la misma.
4. Utilización de tareas puntuales y muy acotadas, sistemas de uso general y manejo amplio de la información.
5. Volumen en el procesamiento en las estaciones de trabajo (workstations) capacidad limitada.
6. Propósito del sistema básico de la información, apoyo en la toma de decisiones y sistemas basados en técnicas Web

6.3 RESULTADO DEL ANALISIS DE RIESGO

Para las vulnerabilidades en los sistemas operativos de Windows los primeros pasos en la gestión de riesgo es el análisis de los riesgos que tienen como propósito atacar el sistema dejándolo vulnerable. Sus vulnerabilidades los dejan debilitados y las amenazas los ponen en peligro, en la figura 2 se evidencia la magnitud del riesgo [40].

[39] GIMÉNEZ ALBACETE, Jose Francisco. Seguridad en equipos informaticos. Antequera, Malaga. 2014.

[40] MONDRAGÓN MACA, Oscar Eduardo, MERA ARCOS, Andrés Felipe, URCUQUI, Christian y NAVARRO CADAVID, Andrés. Security control for website defacement, Sist. y Telemática. 2017, vol. 15, no. 41, pp. 45–55, doi: 10.18046/syt.v15i41.2442

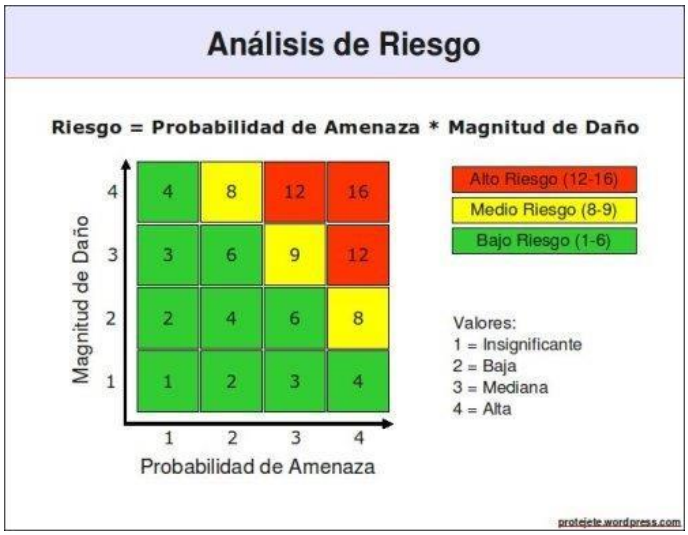

Figura 18 Análisis de Riesgo

El método con el cual se valora el riesgo es basado en una fórmula matemática

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

También es muy importante analizar un riesgo y reconocer que cada uno es diferente y cuenta con características las cuales son:

- Cambiante y dinámico (vulnerabilidad e interacción de amenazas)
- No siempre es percibido entre los miembros de la institución o usuarios que participan en el sistema
- Diferenciado con los caracteres de vulnerabilidad

6.4 POLÍTICAS DE SEGURIDAD INFORMÁTICA

Los aspectos que conforman la estrategia se definen en políticas de seguridad informativa, donde se establecen normas generales para cumplir con los requisitos de seguridad. Las políticas se describen como toda organización, que cumple en cualquier área que requieran, razón por la que son suficientes y flexibles para poder implementarse, en cualquier caso, mediante las medidas y procedimientos que demanden diferentes características específicas[41].

6.5 PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA

Las medidas para los procedimientos de seguridad informática no deben confundirse con declaraciones o intenciones de línea de deseos, por lo que con su

[41] OCAMPO, Carlos Alberto, CASTRO BERMÚDEZ, Yanci Viviana y SOLARTE MARTÍNEZ, Guillermo Roberto Sistema de detección de intrusos en redes corporativas *Intrusion Detection System in Corporate Networks*. Pereira, Risaralda. Universidad Tecnológica de Pereira. 2017, Vol. 22, No. 1

descripción se especifican controles implementados. Las acciones que garantizan una óptima seguridad informática están clasificadas por diferentes áreas.

1. **Clasificación y control de bienes informáticos:** son métodos de control y supervisión que utilizan personas encargadas para ejecutarlos. Garantizando el control de movimiento en los bienes informáticos.
2. **Seguridad física:** son medidas que tienen como objetivo evitar los procesos físicos no autorizados, daños e interferencias contra las instalaciones.Esta protección se alcanza por medio de barreras físicas alrededor de áreas de procesamiento de la información.

6.6 ESTRATEGIAS PARA LA SOLUCIÓN DE PROBLEMAS DE LAS VULNERABILIDADES PRESENTES EN LAS REDES Y BASES DE DATOS

Se proponen unas estrategias óptimas para evitar problemas de vulnerabilidades presentes en la plataforma de Windows, esto con el fin de estar preparados para cualquier ciber ataque y dar su respectiva solución.

6.6.1 PLAN DE SEGURIDAD INFORMÁTICA

Las amenazas a la ciberseguridad continúan aumentando y se han convertido en un problema importante en todo el sector de la tecnología, desde un joven con un teléfono inteligente hasta Internet y sistemas operativos como los son Windows. En los últimos años siempre ha existido la introducción de malware en diversos tipos de plataformas, el robo de datos, los ataques de privacidad o DDoS a servicios comerciales, y el uso de estrategias de ciberespionaje en ataques contra empresas estratégicas[42]. Y obligando a usuarios de Windows a tomar medidas activas de control. Hay que tener en cuenta algunas medidas para la protección de los datos cuando se navega por la red y proteger todos los datos personales y mitigar cualquier tipo de riesgo, entre esas medidas tenemos las siguientes:

6.6.2 SENTIDO COMÚN

La precaución es la mejor barrera contra el malware. Preste especial atención a la sección sobre descarga e instalación de aplicaciones de sitios inseguros; navegación por ciertas páginas de Internet; apertura de mensajes o correos electrónicos no solicitados o archivos adjuntos de remitentes desconocidos o de redes sociales o aplicaciones de mensajería. La apertura de correos electrónicos o

[42] ROMERO CASTRO, Martha Irene, FIGUEROA MORÀN, Grace Liliana, VERA NAVARRETE, Denisse Soraya, ÁLAVA CRUZATTY, José Efraín, PARRALES ANZÚLES, Galo Roberto, ÁLAVA MERO, Christian José, MURILLO QUIMIZ, Ángel Leonardo y CASTILLO MERINO, Miriam Adriana, Introducción a la seguridad informática y el análisis de vulnerabilidades. Ingenieria y Tecnología. 2018. ISBN: 978-84-949306-1-4

archivos adjuntos que contienen vulnerabilidades en actividades de software malicioso que los ciberdelincuentes pueden aprovechar.

6.6.3 UTILIZAR SOLUCIONES DE SEGURIDAD

Hay muchos proveedores de soluciones de seguridad comercial y gratuita, y su uso debe evaluarse. Lo mismo se aplica a las aplicaciones anti-malware nativas incluidas en determinados sistemas operativos. Los profesionales de negocios móviles deben considerar el uso de paquetes de seguridad comerciales integrales y otras herramientas de seguridad, como firewalls o sistemas de encriptación de datos[43].

6.6.4 ACTUALIZAR EL SISTEMA OPERATIVO Y APLICACIONES

Todos los sistemas operativos tienen herramientas para mantener su computadora actualizada. Y son necesarios porque incluyen actualizaciones de seguridad contra amenazas conocidas. En comparación con las aplicaciones instaladas, es muy importante actualizar las aplicaciones actualizadas a la última versión, ya que generalmente contienen parches de seguridad. Cuando la versión es más antigua, es más probable que sean atacados por ciberdelincuentes y encontrarán lagunas en el programa, especialmente en algunos casos, como Java, Adobe Flash o Reader.

6.6.5 REALIZAR COPIAS DE SEGURIDAD

No hay seguridad al 100% en el mundo conectado, no solo por virus, porque los errores de hardware pueden causar la pérdida de valiosa información personal y / o profesional. Por tanto, se recomienda encarecidamente realizar copias de seguridad para los usuarios o profesionales que pretendan proteger la información personal y de la empresa en los equipos informáticos. Además de las tareas de mantenimiento que contribuyen a la salud del hardware. La copia de seguridad debe almacenarse en un dispositivo de almacenamiento externo a nuestro equipo o en un servicio de almacenamiento en la nube.

6.6.6 PRECAUCIONES CON LAS REDES WIFI PÚBLICAS

Los puntos de acceso inalámbrico y gratuito a Internet se han extendido a múltiples áreas en ciudades, restaurantes, aeropuertos, estaciones de tren o metro, hoteles y todo tipo de negocios. Resulta que son muy inseguros y se pueden usar para una navegación intrascendente, manteniendo las precauciones adecuadas, pero no se pueden usar para requerir la visualización de sus datos, derechos de acceso y derechos de acceso de contraseña. Los usuarios de servicios móviles no deben

[43] SMITH, Craig. The Car Hacker's Handbook. Network Security, 2016, 4. https://doi.org/10.1016/S1353-485830034-4

confiar en ellos para realizar sus actividades profesionales, sino elegir una red de banda ancha móvil dedicada más segura.

6.7 ALTERNATIVAS ANTE LA APARICIÓN DE VULNERABILIDADES EN LA PLATAFORMA WINDOWS

Estas están vinculadas a la aparición de cualquier ciber ataque que pueda generar una vulnerabilidad en la plataforma de Windows ocasionando la perdida y robo de datos. En los siguientes índices se explican de manera adecuada las herramientas más importantes en Windows para la detección de vulnerabilidades y su respectiva protección.

6.7.1 NESSUS

Nessus es un escáner de vulnerabilidades para todos los sistemas operativos. Consiste en un demonio nessusd (que realiza un escaneo del sistema operativo de destino) y un cliente nessus (que muestra el progreso e informa todo lo encontrado en diferentes escaneos). Nessus se puede ejecutar mediante comandos en el nivel de consola o mediante una interfaz gráfica de usuario. Nessus comienza primero realizando un escaneo de puertos, porque esto suele ser lo primero que se hace en una prueba de penetración, por lo que Nessus aprovecha al máximo las capacidades de Nmap, aunque también tiene su propio programa de escaneo de puertos abiertos. La herramienta te permite exportar los resultados del escaneo en diferentes formatos, como texto plano, XML, HTML y LaTeX, además toda la información se guarda en la base de datos de "conocimiento" para su posterior revisión. En la actualidad, Nessus tiene una versión gratuita muy limitada, y luego brinda una versión paga más completa con el apoyo de la empresa que la respalda. Algunas características muy importantes de Nessus son que casi no tiene falsos positivos, alta cobertura de vulnerabilidad y es ampliamente utilizado por toda la industria de la seguridad, por lo que se actualiza casi constantemente para incorporar la última tecnología y fallas de seguridad solicitud[44] .

[44] ÁLAVA MERO, Christian José, MURILLO QUIMIZ, Ángel Leonardo y CASTILLO MERINO, Miriam Adriana, Introducción a la seguridad informática y el análisis de vulnerabilidades. Ingenieria y Tecnología. 2018. ISBN: 978-84-949306-1-4.

Figura 19 Nessus

Una versión más completa del centro de seguridad de Nessus se centra en La monitorización continua, este paquete le permite monitorizar de forma continua La infraestructura permite la recopilación de datos de múltiples sensores Apoyará el análisis de vulnerabilidades, monitoreo de amenazas. La diferencia en los servicios mencionados permitirá la exploración activos, lo que permite el uso de conectores inteligentes e incluso la exploración agente. También se pueden manejar:

- Si cumple con los estándares.
- Detección de malware y otras utilidades.
- Escáner de vulnerabilidad.
-

El escáner de vulnerabilidades se divide en 3 partes, como se muestra en la ***Figura 20***.

Figura 20 Versiones de Nessus

Nessus Cloud le permite realizar análisis internos y externos y realizar múltiples escaneos para personalizar políticas y delegación de resultados a posibles gestores de la infraestructura o desarrollo, también apoya el cumplimiento de estándares

internacionales, una de sus principales ventajas es que puede escanear proxies, reduciendo el tiempo, costos y riesgos.

Nessus Manager, esta versión permite escanear, administrar políticas Informes y estadísticas sobre vulnerabilidades detectadas organización e infraestructura. La herramienta se actualiza constantemente al hacer frente a amenazas avanzadas, vulnerabilidades de día cero y nuevas amenazas cumplir con los requisitos de la norma. Permitiendo pasar algunos datos de infraestructura de seguridad periférica en el medio de su Api, por ejemplo, Cortafuegos, sistema de virtualización.

Nessus Professional Esta versión permite escanear múltiples sistemas operativos tanto las bases de datos físicas como virtuales y pueden ser este tipo de escaneado y muchas infraestructuras. El escaneo es con o sin credenciales de acceso, se puede realizar de varias formas. exploración con las credenciales de acceso, podrá comprender mejor evaluando los estándares de cumplimiento, puede manejar política interna y puede administrar si realmente tiene requisitos de acceso escanear. Por ejemplo, puede comprobar la complejidad de la contraseña, si tienen una longitud mínima, alguna fecha de vencimiento, etc., son de varias letras[45].

6.7.2 ACUNETIX

Ahora la herramienta de análisis se llama Acunetix, que es un escáner principalmente para las diez vulnerabilidades web de OWASP donde los principales defectos o deficiencias, este es un desarrollo y Apoye las investigaciones y comience a publicar exploits en sus herramientas desde allí.

Acunetix también puede manejar vulnerabilidades que pueden tener un impacto muy alto grandes herramientas integradas en su escáner se puede utilizar, se puede instalar y trabajar localmente, o realice un escaneo en línea. Según Tovar Valencia esta aplicación es muy versátil una herramienta con interfaz gráfica a través de la red diseñada para encontrar huecos seguridad para todas las aplicaciones de Internet o implementadas localmente en organizaciones que pretenden descubrir estas vulnerabilidades, el atacante no entrará al sistema y robará información de él. En estos Las vulnerabilidades se pueden encontrar en ataques de inyección SQL, secuencias de comandos entre sitios, contraseña insuficiente.

Para descargar la herramienta, debe visitar el sitio web https: // www. Puede descargar una versión de demostración en acunetix.com/ o comprar una Licencia de aplicación para análisis de vulnerabilidades. La ***figura 47*** muestra La página principal de descarga de esta aplicación.

[45] VERMA, Vinita, MUTTOO, Sunil y SINGH V.B. Multiclass malware classification via first- and second-order texture statistics. Computers & Security. 2020, vol. 97, p. 101895, doi: 10.1016/j.cose.2020.101895

Figura 21 Acunetix

En esta herramienta, puede seleccionar objetivos de una manera muy general con esta herramienta, puede realizar escaneos para detectar vulnerabilidades, puede seleccionar un cierto rango de direcciones IP y comenzar a descubrir Posibles fallas dentro de la empresa. Entre diferentes tipos de escaneos los métodos de escaneo más comunes que se pueden aplicar dentro de la organizaciónse toma completo o personalizado, como se muestra en la ***Figura 22***.

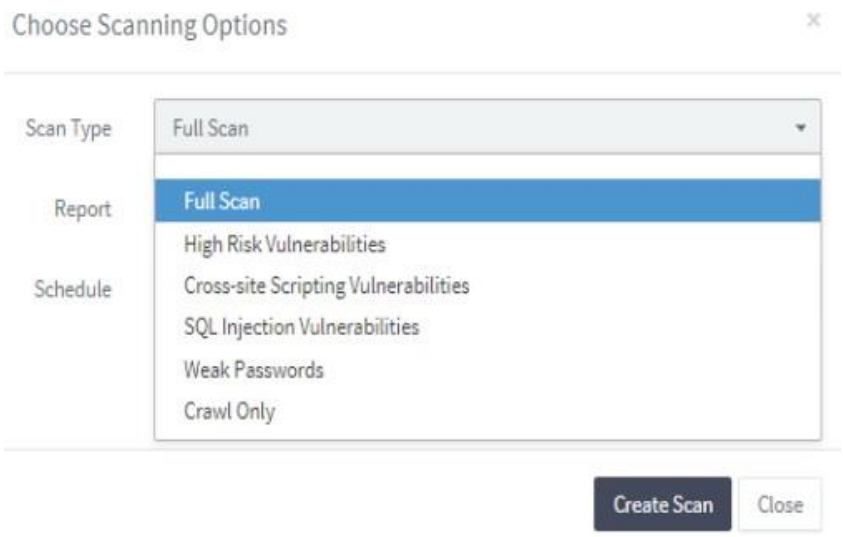

Figura 22 Tipos de escaneo de Acunetix

Con Acunetix, puede definir algunos puertos para buscar localmente, A través de los puertos más comunes (por ejemplo, HTTP o, Sin embargo, para definirlo, Acunetix recomienda configurarlo en los puertos 80 y 443 Suele tener un servicio

web service, también puedes trabajar Utilizado directamente con la parte SSL y TLS [46].

6.7.3 SUITE AIRCRACK-NG

La red Wi-Fi es uno de los enlaces más débiles de Windows, por lo que es una de las áreas a las que más debemos prestar atención. En este punto, Aircrack-ng es sin duda la mejor herramienta para probar la seguridad de cualquier red Wi-Fi y encontrar cualquier laguna que pueda permitir que cualquier usuario no autorizado obtenga nuestra contraseña de red. Aircrack-ng no es realmente una herramienta única, sino que consta de varias herramientas dedicadas a diferentes tareas:

- Airmon-ng: Responsable de poner la tarjeta de red Wi-Fi en modo de monitoreo para permitir que Airodump-ng capture toda la información.
- Airodump-ng: puede capturar datos y exportar toda la información para su uso posterior de herramientas de terceros o incluso otras herramientas de la suite.
- Aircrack-ng. Aireplay-ng: esta herramienta se utiliza para realizar ataques de reproducción, des autenticación de clientes, creación de AP maliciosos y otros tipos de inyección de paquetes. Un detalle importante es que la tarjeta Wi-Fi que usemos debe ser compatible con la inyección de paquetes, porque muchas no son compatibles.
- Aircrack-ng: Este programa se encarga de descifrar las claves WEP, WPA y WPA2 de la red Wi-Fi y obtener toda la información obtenida por el resto de programas de la suite.

6.7.4 OPENVAS

OpenVAS es un escáner de vulnerabilidades en el que podemos ingresar la dirección IP y encomendar el análisis del dispositivo para recopilar información sobre servicios en ejecución, puertos abiertos, errores de configuración, vulnerabilidades conocidas que puedan existir en el dispositivo o software del servidor. El programa se puede ejecutar desde dentro de la red o desde un servidor externo, simulando así un ataque real. Al final, generará un informe completo que contendrá todas las debilidades que pueden representar una amenaza para nuestra seguridad. Además, podemos configurarlo en modo de monitoreo continuo para establecer una alarma, y la alarma saltará cuando se detecte la más mínima falla.

[46] YORK, Dan. Identity, Spoofing, and Vishing. Seven Deadliest Unified Commun. Attacks, 2010, pp. 117–136, doi: 10.1016/b978-1-59749-547-9.00006-5.

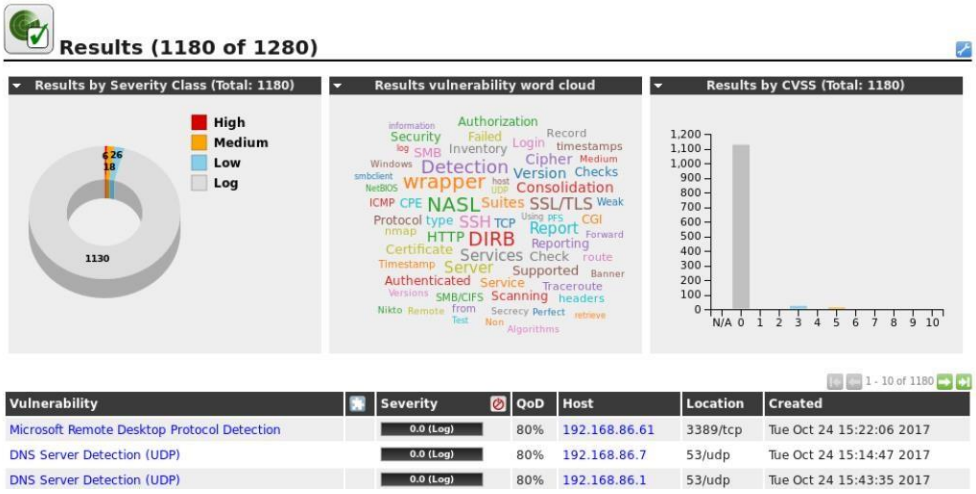

Figura 23 OpenVas

OpenVAS es una herramienta gratuita que permitirá realizar una gran cantidad de pruebas de vulnerabilidad en servidores web. Además, existe una gran comunidad detrás de OpenVAS para apoyarlo e incorporar nuevas funciones para aprovechar al máximo su potencial.

6.7.5 OWASP ZAN ATTACK PROXY ZAP

El proyecto OWASP (Open Web Application Security Project) es un proyecto abierto sin fines de lucro destinado a mejorar la seguridad de las redes, servidores, computadoras y aplicaciones y servicios para hacer que Internet sea más seguro. Zed Attack Proxy (Zed Attack Proxy) ZAP es una de las herramientas gratuitas del proyecto, su principal objetivo es monitorear la seguridad de la red y las aplicaciones web para encontrar fallas de seguridad, errores de configuración o incluso incógnitas que puedan causar problemas de seguridad o lagunas de red. Finalmente, ZAP tiene una biblioteca de complementos para aumentar las funciones predeterminadas de la herramienta, y estos complementos son desarrollados por la comunidad detrás del proyecto.

6.7.6 VEGA

Vega es una alternativa perfecta a Burp Suite, pero es completamente gratuito y de código abierto. La herramienta se puede utilizar como un proxy gratuito, además, también cuenta con un motor para buscar vulnerabilidades y otras vulnerabilidades de seguridad en cualquier sistema o red. La principal ventaja de Vega es que es una herramienta muy flexible que puede encontrar versiones para Linux, macOS y Windows, aunque para este último solo podemos encontrarlo a través de la interfaz gráfica GUI. Esta herramienta es una de las herramientas básicas para realizar pruebas de penetración y escanear vulnerabilidades web.

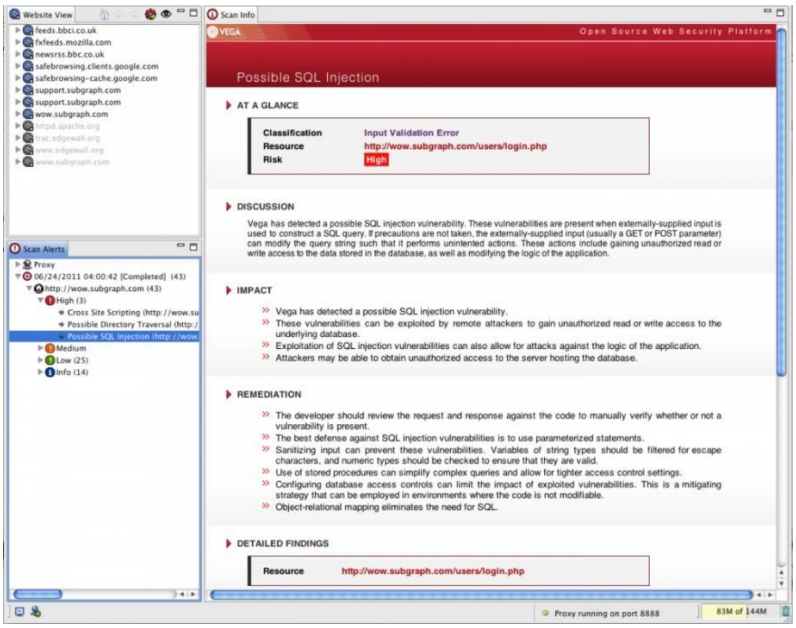

Figura 24 Interfaz Gráfica Vega

6.8 PLANEACIÓN

Aplicando el análisis correspondiente a la empresa es importante aclarar que no se tiene una distribución exacta de la misma por lo que se debe suponer el modelo a explorar siendo un tanto puntuales un escenario de mediana empresa que cuentan con servicios de email servidores, hub de conexión entre otros, que logran ejemplificar el diseño que se dispondrá a analizar adicionando que le componente de topología se basa en una tipo mixta debido a que los servicios que se ofrecen son solventados por esta, en la fase de planeación se dispone de determinar el alcance de la prueba donde se deben encontrar aquellos activos que se evalúan dentro del experimento, se debe tener especial cuidado con el manejo de la información siendo el paso más importante tener los permisos por parte del cliente necesarios para desarrollar la metodología dispuesta en el párrafo anterior, con este debido permiso por parte del cliente tendremos una información no sesgada además de no incurrir sobre problemas legales como los delitos informáticos penados por la actual ley Colombiana dispuesta en la ley 1273 del 2009 donde se dispone la protección de la información y de los datos [47].

Luego de tener dicha aprobación se deben incluir ciertos aspectos que permitan que la metodología CEH se desarrolle de la manera esperada.

[47] ARANO CHÁVEZ, Raúl Manuel, ESPINOSA MEJÍA, Francisco y ARROYO GRANT, Georgina. El rol de la dirección estratégica en las empresas. *Académicos de la Facultad de Ciencias Administrativas y Sociales de la Universidad Veracruzana*. 2000. 29–31.

Estos items comienzan desde seleccionar los sistemas que se desean atacar incluyendo aquellos que lleven procesos con nivel de criticidad elevada puesto que pueden ser vulnerables, luego se debe realizar una evaluación del riesgo presente donde se deben usar planes de choque en caso que no se tenga previsto algunos cambios en muchos caso llamado respaldo de emergencia que permita tener un soporte de datos en caso de pérdida de la información por aplicar dicha herramienta, este proceso se observa en casi todas las empresas para proteger su información y la de sus clientes.

Para que el proceso pueda ser efectuado es importante relacionar los tiempos de ejecución de cada una de las pruebas, para que no interfieran con el acceso de clientes o de los administradores del entorno logrando que las pérdidas en caso de que existan serian consideradas como mínimas. Cuando estos ataques deseen realizarse es importante que se tenga un estudio previo del funcionamiento de cada una de las etapas conociendo los conceptos de cajas blancas o cajas negras interactuando con el tipo de prueba que el usuario o cliente desee implementar, cuando se detectan un grupo de vulnerabilidades se sigue aplicando dicho ataque hasta lograr determinar los puntos críticos hasta dónde puede llegar el mismo, sin afectar la integridad de todo el sistema y consignando sobre un reporte dichos valores, solo en la fase de planeación donde se dispone lo que se va a realizar conforme la implementación de la prueba con la metodología CEH de hacking ético. En el alcance de la prueba se debe definir cuáles son los pasos a seguir con la culminación de cada ataque o paso de la metodología aplicada, haciendo una planeación de los eventos presentes y eventos futuros con cada situación de penetración o pen testing, estos reportes o alcances son relacionados directamente con los objetivos secundarios de la prueba pero se deben contemplar en esta fase los posibles cambios o resultados inesperados que puedan darse, siempre en la aplicación de esta metodología es importante revisar los procesos críticos y sus alcances críticos y no críticos con el fin de clasificar el comportamiento del sistema ante la implementación de la metodología planteada.

6.9 DESCUBRIMIENTO

En este apartado ya se tiene una descripción y alcances de aplicar dicha metodología al entorno con lo cual el profesional encargado debe tener una serie de pasos estratégicos de recolección de información que le permitan obtener los datos necesarios para un futuro ataque, esta es una de las fases más importantes de toda la metodología puesto que mediante el uso de herramientas otorgadas por la misma metodología se junta la información necesaria basando su fuerza en el manejo de la red de internet, para esta fase se tienen dos tipos de reconocimiento el activo y el pasivo [48].

[48] SMITH, Craig. The Car Hacker's Handbook. Network Security, 2016, 4. https://doi.org/10.1016/S1353-485830034-4

El descubrimiento o reconocimiento le da facultades al profesional en seguridad información de host se servidores, direccionamiento y toda la distribución de la red, en este tipo de reconocimiento el profesional puede ser detectado fácilmente debido al uso de herramientas que lo ponen al descubierto debido a su manejo de la red; por el contrario tenemos al reconocimiento pasivo el cual consiste en buscar información datos y demás aspectos relevantes para el proceso de implementación de la metodología CEH pero de forma sigilosa para no ser detectado fácilmente a este tipo de descubrimiento o reconocimiento se le atribuye el concepto de ingeniería social aunque en muchos casos se usan distintas herramientas que se tocaron dentro del trabajo practico del curso como lo son los sniffers en modo detección para observar cual es el comportamiento que circula en la red [49].

Para lograr esta fase de descubrimiento se usan herramientas previamente desarrolladas por fabricantes y otras otorgadas por los dueños de las metodologías del hacking ético entre las más importantes podemos denotar las siguientes:

- ARIN
- Maltego
- Traceroute
- Smart-Whois

Existe un sinnúmero de aplicaciones para esta fase, aunque no lo es todo, en este apartado es importante tocar los temas de ingeniería social y el mapeo los cuales dan todo el soporte necesario para que el sistema operativo tomado como referencia tenga la mejor implementación de hacking ético sobre la metodología CEH.

En el paso de recolección de información es importante el concepto de ingeniería social, puesto que no se trata directamente de una carrera ingenieril sino que es un conjunto de pasos o métodos que se aplican sobre los usuarios con el fin de obtener información de ellos mismos, bajo el criterio de que los usuarios son el punto más débil dentro de un complejo productivo o sistemático, la ingeniería social tiene ciertas herramientas que tratan de convencer al usuario de que algo está siendo efectuado de la mejor manera en pocas palabras ganarse su confianza mediante el dialogo la insistencia con el fin de obtener los datos posibles y reforzarlos en esta etapa donde ya se pueden considerar como los blancos vulnerables, las herramientas dentro de este ámbito son varias aunque solo se mostraran las más usadas [50].

[49] ALEXANDER, Bryce, HASEEB, Sohaib y BARANCHUK, Adrian. Are implanted electronic devices hackable?. Ontario, Canadá. Division of Cardiology, Queen's University, Trends in Cardiovascular Medicine. 2018. https://doi.org/10.1016/j.tcm.2018.11.011.

[50] ROESSING, Rolf Von. Highwaymen to hackers. Computer Fraud and Security, 2016, 13–15. https://doi.org/10.1016/S1361-372330026-4

- Phishing
- Duplicación de identidad
- Supervisión o vigilancia

Otro apartado en esta fase corresponde al poco conocido mapeo o escaneo cuya herramienta fue trabajada previamente en esta asignatura y consiste en el uso de herramientas digitales algunas más robustas que otras para obtener un mapa de la red o distribución de la misma, con el fin de hallar IP, puertos cerrados puertos abiertos servicios y todo aquello que esté presente en la red, mediante envió y recepción de paquetes de información que el mismo ´programa ejecuta para obtener un reporte, este mapeo permite detectar cuáles son las vulnerabilidades o espacios por donde los intrusos pueden ingresar y afectar el sistema de forma negativa, puesto que en la mayoría de los casos estas vulnerabilidades o espacio s no reforzados no son penetrados por especialistas buenos que van a mejorar sino que buscan la afectación del sistema, los sistemas que son actualizados constantemente son víctimas de estos ataques debido a que los especialistas que están fortaleciendo hacen ataques controlados con el fin de generar lo que se llaman parches o actualizaciones capaces de tapar este tipo de bugs o fallos que permitan la intrusión, en muchos casos las pruebas se hacen de forma externa para determinar los cambios presentes en cada uno de los escenarios pero también es cierto que dentro de la empresa o espacio se hacen este tipo de pruebas de carácter interno y son comparadas, el problema más grande dentro del mapeo de vulnerabilidades es que la empresa o entorno debe cerrar sus puertos de comunicación externo con el fin de reforzar la entrada de intrusos, si solo se permiten ataquen o falencias desde adentro es mucho más sencillo efectuar correcciones y ajustes de actualización dentro de la plataforma.

Las herramientas usadas en el mapeado de vulnerabilidades entregan ventajas respecto a la ingeniería social puesto que dan un detallado de toda la red donde puede ser generado el ataque o la aplicación de la metodología dispuesta entre los más importantes tenemos los siguientes.

- Nessus
- Qualys
- Acunetrix
- Microsoft Baseline Security
- Saint

Luego de que estos programas tracen un mapa de aquellas vulnerabilidades presentes en el sistema de debe efectuar un proceso de recolección de datos utilizando herramientas descritas anteriormente que fortalezcan esta fase de la metodología CEH, aunque los pasos o las herramientas pueden variar se debe manejar un plan ordenado que entregue resultados parciales en cada etapa que se adapten a los requerimientos esperados con la empresa con el fin de tener los

soportes de mejoras o parches dentro de la empresa que facilite la seguridad en los administradores del servicio y el cuerpo técnico además de dar una satisfacción al cliente final.

En el desarrollo del componente practico dispuesto sobre sistemas operativos se ejecutaron dichos procesos con las herramientas más comunes en plataformas Linux pero es posible implementarlas en Windows bajo el uso de algunos paquetes que facilitan las tareas de reconocimiento de alcance y de ataque luego de usar Nessus se obtiene un detallado de mapa que relaciona los puertos abiertos los cerrados y aquellos servicios que poder ser vulnerados mediante las herramientas que se dispondrán más adelante en este proyecto.

6.10 ATAQUE

En esta fase se disponen de las herramientas que logran entregar el acceso al sistema de información o al sistema de redes el cual fue detallado en los pasos anteriores, desde el descubrimiento o reconocimiento y la fase de planeación en esta etapa se colocan en marca una serie de actividades que se van acoplando para generar el resultado esperado, las etapas en la explotación son pocas puesto que las fases anteriores tienen el mayor peso técnico puesto que dan todas las pautas requerimientos usos y posibles eventualidades que puedan presentarse, en la fase de ataque o para otros llamada explotación no es más que el uso de herramientas computaciones o herramientas de software que permitan hacer pruebas sobre las vulnerabilidades que se encuentren en cada uno de los componentes del sistema como sus entornos web sus bases de datos o sus redes de datos, en esta fase es importante aclarar que en el apartado de planeación el experto ya define el alcance de cada prueba de intrusión que dará como resultado un análisis de vulnerabilidad acertada o rechazada, el concepto más usado en este apartado es el exploit el cual no es más que una sentencia de algoritmos que se aprovechan de los espacios débiles o vulnerabilidades del sistema alterando su funcionamiento, es un proceso que demora más tiempo que las anteriores etapas puesto que el algoritmo debe hacer el ataque de forma repetida hasta que el sistema muestre la vulnerabilidad y decaiga en este aparto seguidamente del ataque o vulnerabilidad se busca que escalar privilegios lo cual dará como ventaja al atacante tener el control sobre los medios del sistema como estaciones de servicios y demás obtenido licencias o permisos de administrador que le darán todas las facultades del ataque logrando ejecutar sentencias y algoritmos que crea convenientes dentro de los programas o herramientas más usadas para la explotación o ataque en la metodología CEH se tienen las siguientes [51].

[51] GUERRERO-HIGUERAS, Ángel Manuel, DECASTRO-GARCÍA, Noemí y MATELLÁN Vicente. Detection of Cyber-attacks to indoor real time localization systems for autonomous robots. Robotics and Autonomous Systems.[En línea] 2018. 99, 75–83. https://doi.org/10.1016/j.robot.2017.10.006 Disponible en: http://bibliotecavirtual.unad.edu.co:2139/eds/detail/detail?vid=9&sid=e2e23ef1-fcc3-4a6e-aa83-

- SVScanner
- DVWA(Damn Vulnerable Web Aplication)
- Sploitus

Existen otras herramientas capaces de explotar los resultados obtenidos en la fase anterior, pero todo depende del tipo de ataque que desee realizar basando dicho ataque en la estructura de la empresa y sus servicios de seguridad estas herramientas en su mayoría son gratuitas y se encuentran en sistemas operativos de testeo de redes como Kali Linux mediante líneas de comando se pueden establecer las interfaces y dar inicio al ataque con solo una línea de código y la tecla enter [52].

6.11 REPORTE

Al finalizar las fases anteriores es el reporte o la documentación la más importante de todo el proceso puesto que se consigna dentro de un archivo todos los hallazgos encontrados en la ejecución de la metodología de hacking ético para determinar las vulnerabilidades sobre el sistema operativo seleccionado como trabajo, el reporte de esta información se debe socializar o dar a conocer por todos los grupos que hacen parte del sistema con el fin de mostrar cuales deben ser las pautas o los pasos que se deben tomar para mitigar dichas eventualidades arrojadas desde el inicio de la metodología, este reporte debe ser avalado por los expertos en el campo que detallaran la información en la fase de planeación descubrimiento y ataque con el fin se mejorar los servicios y no se sometidos por ninguna eventualidad externa, en muchas ocasiones este tipo de ataques presentados en la fase anterior son robustos y de largo tiempo en pocas ocasiones se ven ataques externos tan fuertes como en las pruebas de fortalecimiento del sistema de la empresa, pero mediante la aplicación de esta metodología la empresa debe estar preparada para las eventualidades, respecto a las actualizaciones del sistema pueden presentarse antes o después de aplicar el componente metodológico pero al mismo tiempo dan al grupo directivo la faculta de realizar los cambios en el momento que sea necesario de este modo proteger en primera medida al usuario y por consiguiente a la empresa, dado que en el reporte se consigna todo, esta fase da la facilidad de que el trabajo sobre la metodología planteada (CEH) sea trabajada más adelante sin tener que realizar las fases iniciales si no es necesario puesto que quedaría consignado un estudio que puede ser continuado, logrando vincular el reporte al trabajo desempeñado en la asignatura se puede relacionar con los resultados obtenido y entregados en un informe escrito que da las pautas del trabajo realizado además de observaciones características tipos de intrusión explotación y las conclusiones necesarias para la ejecución de la propuesta de proyecto en seguridad

---

42fcae585cac%40sessionmgr104&bdata=Jmxhbmc9ZXMmc2l0ZT1lZHMtbGl2ZQ%3D%3D#AN=edselb.10357400&db=edselb.

informática sobre un sistema operativo puede emplearse sobre otros de la misma forma sin denotar que uno es mejor que el otro, la cual debe demostrar que está a la altura de muchas otras haciendo una protección de los datos con un uso de la información que este dentro de las normativas técnicas y judiciales sin incurrir en delitos o en posteriores demandas por su mal uso.

7 RESULTADOS

7.1 ANÁLISIS BIBLIOGRÁFICO DE LOS ATAQUES CIBERNÉTICOS ACTUALES EN LAS REDES DE DATOS, BASES DE DATOS SOBRE LA PLATAFORMA WINDOWS

En las siguientes definiciones se hizo un estudio y análisis bibliográfico de los ataques cibernéticos más relevantes en la plataforma de Windows. Estos ataques cuentan con descripciones y características importantes para entender cómo funcionan y quienes los generan, estos ataques cibernéticos están ligados a diferentes entornos en los cuales están las redes de datos, bases de datos y vulnerabilidades. Este capítulo analizará los conceptos relacionados con la seguridad informática, la base principal, sus componentes, la terminología empleada, las correcciones de seguridad informática, y también hablará de los problemas relacionados con los diferentes mecanismos de autenticación de usuarios.

La seguridad busca la gestión de riesgos, lo que significa que tiene siempre la forma de evitarlo o prevenirlo, y se pueden realizar determinadas acciones (evite estas situaciones de la mejor manera). Definir la seguridad puede ser Clasificado como libre de riesgo, la definición del término implica cuatro Operaciones que siempre están inmersas en cualquier problema de seguridad, como:

- Prevención de riesgos
- Riesgo de transferencia
- Mitigar los riesgos
- Toma riesgos

7.1.1 RANSONWARE

Con el desarrollo de Internet, equipos y tecnología Los teléfonos móviles, la computación en la nube y, más recientemente, el Internet de las cosas (IoT) son realmente dispositivos, redes y aplicaciones invasoras en todas las áreas de la empresa. Como era de esperar, este impulso no es Sin riesgo, por inmediatez, miniaturización, Liquidez, conveniencia de pago, comunicación, etc. Empresas, gobiernos y usuarios también Participar en actividades maliciosas[53]. El ransomware afecta cualquier posibilidad Pague a cambio de su información. El malware está afectando a usuarios domésticos, empresas, gobiernos e incluso servicios críticos. Como hospitales o plantas de energía, causando pérdidas temporales o La

[53] INSTITUTO NACIONAL DE CIBERSEGURIDAD, Ransomware : una guía de aproximación para el empresario Índice. 2017. [En linea]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

información permanente interrumpe las actividades normales, provoca pérdidas económicas para restaurar sistemas y archivos, y en algunos casos daña la reputación. En esta guía, recomendamos actuar Conozca, prevenga y mitigue esta amenaza [54].

Este consiste en el secuestro digital de datos, donde un software malicioso infecta la computadora y realiza un cifrado de la información, posteriormente el atacante solicita una suma de dinero en Bitcoins para rescatar su información algunos producen un bloqueo de pantalla del equipo y otro tipo de ransomware encripta la información.

Existen algunas recomendaciones para prevenir este tipo de ataque y se presentan a continuación:

Realización de copias de seguridad de ficheros y archivos

- La utilización de software de seguridad y hardware para la detección de los ataques son una gran herramienta, así como la capacitación del personal para identificar e-mail y páginas web que generen riesgo.

- Establecer barreras para el acceso de la información.

- Verificar que se encuentre instalada la versión más actualizada de las herramientas con las que cuenta la empresa como solución de seguridad.

- Instaurar un sistema de seguridad que incluya varias capas, así como otras protecciones contra amenazas avanzadas.

Discutir que el malware que cifra archivos en Windows es cada vez más común. Sean Williams es el director y desarrollador del proyecto Cryptostalker, que fue diseñado originalmente para controlar el sistema de archivos, es decir, la lectura y escritura de archivos. Sin embargo, considerando que el tipo de amenaza con la que nos enfrentamos es la escritura aleatoria de datos para lograr el cifrado de archivos, la utilidad se ha modificado para poder advertir a los usuarios. Teniendo en cuenta que esta amenaza también afectará a los sistemas operativos actualmente disponibles, y que la utilidad se desarrolló utilizando Python, se le preguntó al desarrollador si la herramienta podría llegar al sistema operativo de escritorio del sistema operativo. Cupertino. La respuesta es clara, y no se descarta

[54] ESTRADA COLA, Carlos y GARCÍA VALDÉS, Angela Maria y GARCÍA FONT, Victor. Estudio sobre el malware Ransomware. 2019, p. 117, [En linea]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89025/6/cestradacolTFM0119memoria.pdf

la posibilidad, pero primero debemos asegurarnos de que después de desarrollar para Linux, el próximo objetivo será Windows [55].

- **Hay variedades de Ransomware**

El ransomware es una actividad delictiva en muchas formas. Desde su nacimiento, este malware es más complejo y más destructivo. Algunos relacionados con otros este tipo de malware roba información (cuenta bancaria, credenciales de acceso ...), abre una puerta trasera o instala una botnet. También personalizan sus mensajes en función del idioma de la víctima. Inicialmente, bloquearon el acceso al sistema operativo o al navegador. El rescate no fue muy alto envíe SMS a un número corto (p. Ej. Compañía telefónica o actividades de desastre) o transferir a billetera electrónica. ser policía canceló esta forma de pago[56].

7.1.2 SQL INJECTION

Este es un ataque que se basa en la inserción de un código SQL o la adición de este a los parámetros de entrada de la aplicación que pasan posteriormente al servidor que alberga la base de datos para su análisis y ejecución y este se encargara de controlar el servidor de la base de datos, dado que las bases de datos relacionales se construyen a partir del código SQL son potencialmente vulnerables, pues este tipo de código cuenta con diversas opciones de codificación[57]. El ataque se ejecuta principalmente cuando se realiza la inyección de código sobre parámetros que son concatenados a los comandos SQL de la base de datos y por esta razón son ejecutados, otra forma de este ataque podría ser cuando las cadenas que contienen el código malicioso son almacenadas en una tabla o como metadatos y posteriormente se concatenan con las instrucciones SQL dinámicas para ser ejecutadas[58]. Cuando el atacante accede a la base de datos es posible que pueda configurar las sentencias que posee el código antes de ser detectado, y si esto sucede este podrá ejecutarse como si fuera un usuario privilegiado, esta a su vez puede interactuar con otros componentes de un sistema como servidor web, el sistema operativo, el servidor de aplicaciones y de la misma manera podrá infectar lo que encuentre a su paso[59].

---

[55] MATA VILLALPANDO- BECERRA, Isaac, y GUEVARA-JUÁREZ, Oscar Antonio. Virus informáticos, todo un caso, pero no perdido. CienciaUAT, 2010, vol. 4, no. 4, pp. 56–61. ISSN: 2007-7521

[56] INSTITUTO NACIONAL DE CIBERSEGURIDAD, Ransomware : una guía de aproximación para el empresario Índice. 2017. [En linea]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

[57] MCWHIRTER, Paul, KIFAYAT, Kashif, SHI ,Qi , y ASKWITH, Bob. SQL Injection Attack classification through the feature extraction of SQL query strings using a Gap-Weighted String Subsequence Kernel. Journal of Information Security and Applications. 2018, vol. 40, pp. 199–216, doi: 10.1016/j.jisa.2018.04.001.

[58] MOYLE, Steve. The blackhat ' s toolbox : SQL injections, Network security. 2007 vol. 2007, no 11, p. 12-14.

[59] LEE, Inyong, JEONG , Soonki, YEO, Sangsoo y MOON, Jongsub. A novel method for SQL,2010.

Existe infinidad de maneras de explotar las vulnerabilidades de los sistemas para realizar un ataque de inyección de código, todo esto depende de la base de datos a la que vaya dirigido el ataque al igual que los sistemas que están interconectados a ella. La forma en que sucede usualmente es mediante una aplicación web interactúa con una base de datos, de manera que esta permite que existan maneras a base de código para conectarse con una de ellas [60]. La mayor vulnerabilidad se encuentra cuando el desarrollador web no plasma en el código una validación de los valores de entrada antes de que estos pasen a las consultas SQL que son las que irán dirigidas a ejecutarse en el servidor de la base de datos, es ahí cuando es aprovechada esta oportunidad para lograr que la interpretación de estas sentencias no sean de datos sino de un código para que pueda ejecutarse allí. Por tal razón el problema yace en la programación ya que se generan problemas de seguridad en los códigos que se desarrollan para las aplicaciones y estas vienen siendo vulnerables a este tipo de ataque [61].

Muchas de las bases de datos que son reconocidas hoy en día manejan el lenguaje estándar SQL como forma de acceso, algunos ejemplos son: Oracle, MySQL, Sybase, Microsoft SQL Server [62].Todas las consecuencias que trae una inyección SQL pueden ser mitigadas de varias maneras, es posible verificar el código de la aplicación sin olvidar la base de datos, las bases de datos cuentas con una cuentas preestablecidas que poseen privilegios de administrador para algunas bases de datos conocidas como Microsoft SQL Server la cuenta de administrador es “sa”, que son creadas de forma automática cuando se crea una base de datos, pero existen muchas más cuentas que poseen contraseñas predeterminadas y conocidas. Los administradores se encargan de instalar los servidores de bases de datos que se ejecutan con una cuenta de usuario que posee privilegios de administrador, y es ahí donde existe la vulnerabilidad pues es más beneficioso ejecutarse como un usuario sin privilegios evitando que en caso de un ataque pueda acceder a la red completa y causar un daño considerable. Igualmente, cada tipo de servidor de base de datos se encarga de imponer control sobre las cuentas que manejan el acceso o no de los datos, así como también determinan que sentencias se pueden ejecutar y cuáles no [63] .

---

[60] MCWHIRTER, Paul, KIFAYAT, Kashif, SHI ,Qi , y ASKWITH, Bob. SQL Injection Attack classification through the feature extraction of SQL query strings using a Gap-Weighted String Subsequence Kernel. Journal of Information Security and Applications. 2018, vol. 40, pp. 199–216, doi: 10.1016/j.jisa.2018.04.001.

[61] GARDOKI, Cardenal. Ataques de inyección SQL Qué son y cómo protegerse. Bilbao, Vizcaya. 2013.

[62] MOHAMED, Gori y VISUMATHI. A predictive model of machine learning against phishing attacks and effective defense mechanisms. Materials Today: Proceedings c. 2020, no:1225, doi: 10.1016/j.matpr.2020.09.612.

[63] KRAUS, Rob, BARBER , Brian, BORKIN, Mike y ALPERN, Naomi. SQL Server – Stored Procedure Attacks. Seven Deadliest Microsoft Attacks. November 2009, 49–69. https://doi.org/10.1016/B978-1-59749-551-6.00003-0.

En cuanto a las aplicaciones también posee cuentas privilegiadas que le permiten realizar una gran cantidad de acciones que nada tiene que ver con el propósito de la aplicación, por tanto, en vez de esto se debería emplear cuentas de usuario específicas que no permitan el fácil acceso de los atacantes a la base de datos [64].

Con una inyección SQL el atacante podría omitir el mecanismo de autorización y autenticación de una aplicación web y obtener la información completa de una base de datos, o bien para violentar la información agregando, modificando y eliminando registro [65].

Este tipo de ataque es posible prevenirlo por medio de las siguientes acciones:

- Escapar los caracteres especiales empleados en las consultas SQL, esto hace referencia a agregar una barra invertida delante de las cadenas que se emplean en las consultas para evitar que estas puedan afectar y corromper la consulta.

- Delimitar valores de las consultas, es preciso asignar un límite entero entre comillas simples.

- Es necesario verificar la información que introduce el usuario y el tamaño de esa información, para determinar si es la información que se está solicitando o si es algún tipo de ataque.

El acceso que se tiene desde el código a la base de datos debe contar con privilegios no tan extendido, pues en caso de un ataque se daría acceso a toda la información.

7.2 HERRAMIENTAS, ESTRATEGIAS O PATRONES QUE SUMINISTREN LA CAPACIDAD DE FORMULAR UN ANÁLISIS COMPLETO SOBRE LAS VULNERABILIDADES PRESENTES EN LOS ENTORNOS DE PLATAFORMA WINDOWS

El objetivo principal de este proyecto es diseñar un enfoque técnico para la detección y evaluación de las vulnerabilidades en sistemas operativos de Windows mediante la identificación de todos los tipos de malware en este servicio. Este

[64] TURGEMAN, Avi. BioCatch and CyberLink tackle security risk. Biometric Technol. Today, vol. 2019, no. 2, p. 2, doi: 10.1016/s0969-476530015-3.

[65] PING-CHEN, Xue. SQL injection attack and guard technical research. Advanced in Control Engineeringand Information Science. 2011. 15, 4131–4135. https://doi.org/10.1016/j.proeng.2011.08.775

enfoque consiste en determinar algunos nombres y versiones de las herramientas para la protección en servicios de Windows y así dar seguridad a las bases de datos que se encuentran alojadas en estos equipos. A continuación, se mencionan las herramientas más usadas para la detección de vulnerabilidades en Windows.

7.2.1 GFI LANGUARD

Languard es un escáner de vulnerabilidades con algunas otras ventajas Herramienta porque permite el escaneo local y el escaneo en red Es posible que se requieran algunos datos, como las credenciales de usuario Puede ser administrador local o administrador de dominio estándar El análisis se puede realizar desde allí. Entre las muchas ventajas Herramientas que se pueden mencionar:

- Actualización automatizada de múltiples sistemas operativos
- Encuentra vulnerabilidades
- Auditoría de hardware y software
- Realizar informes de cumplimiento

El sitio web principal de la herramienta se puede encontrar en Visite https: //www.gfihispana.com/products-and-solutions/network-securitysolutions/gfi-languard, la ***Figura 26*** muestra la página de inicio de esta herramienta.

Figura 25 Pagina de la Herramienta GFI Languard

Esta herramienta se basa en la automatización actualizada Independientemente del tipo de sistema operativo, las vulnerabilidades de seguridad de la red son generalmente causado por falta de actualizaciones, generalmente actualizaciones regulares o de seguridad y LanGuard analiza y detecta estos, antes de exponer

vulnerabilidades en la red según la política Miembros de cada organización, lo que ayuda a reducir el tiempo de actualización de equipos. Cuando detecta que el sistema operativo no está actualizado, puede Enviar alerta.

También busca ***vulnerabilidades en más de 60.000 evaluaciones*** de vulnerabilidades para ejecutar a través de la red LanGuard, incluido el entorno virtual, Dispositivos móviles y datos de red, incluidos CISCO, TRICOM, datos de sistemas operativos como Windows. Generalmente escanea el sistema operativo y las aplicaciones instaladas en el entorno virtual utilizando una base de datos de verificación, como OVAL (abrir Vulnerabilidades y lenguaje de evaluación. A diferencia de otras herramientas Acunetix y Nessus no tienen el top ten de OWASP porque no lo hicieron. Sin embargo, existen otros tipos de cumplimiento con las páginas escaneadas.

La herramienta también realiza auditorías de hardware y software, proporcionando un análisis detallado del estado de la red, que incluye; aplicación o configuración (por defecto), y pueden suponer riesgos para la seguridad de la organización, también proporciona aplicaciones instaladas, imágenes completas del hardware de red, dispositivos móviles conectados al servidor, etc. Si algunas aplicaciones instaladas por el usuario están ubicadas o no en autorizar la organización puede generar informes desde allí.

7.2.2 NEXPOSE

Esta aplicación fue creada por rapid7.com, ellos son los creadores de la herramienta Metasploit, la cual aprovecha las vulnerabilidades, estas vulnerabilidades funcionarán en la Web y en las partes de la red. La ventaja de esta aplicación en comparación con otras aplicaciones es que puede interactuar. La vulnerabilidad se puede explotar directamente a través de Metasploit, y la herramienta se puede descargar directamente de www.rapid7.com. La ***Figura 26*** muestra la página principal de descarga de esta herramienta.

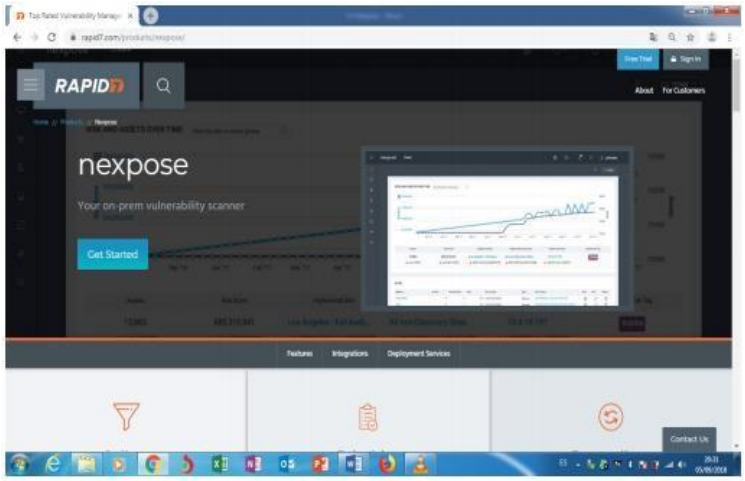

Figura 26 Nexpose

La herramienta funciona directamente en la consola web y se ha iniciado el servicio. Una vez que este seguro Vulnerabilidades, la herramienta indicará si existen exploits Solo Metasploit, o descargue algún código directamente desde la página La Internet. En esta aplicación, puede generar algunos informes, Informe de ejecución de procesos o informe técnico.

Hay varias versiones, como la versión comunitaria, la versión expresa, la versión de consultor, la versión empresarial Y Ultimate, en este caso, lo único que cambiará es la opción, pero hay una La versión gratuita se llama comunidad y se puede utilizar sola y Permitir escanear hasta 32 IP como máximo, en esta versión, también verificada Detección de vulnerabilidades, actualizaciones de gestión de anomalías, etc. Otras cosas [66].

7.3 ESTRATEGIAS QUE PUEDAN DAR SOLUCIÓN A LA PROBLEMÁTICA DE LAS VULNERABILIDADES PRESENTES EN LAS REDES Y BASES DE DATOS

Se pueden utilizar herramientas de detección para detectar vulnerabilidades presentes en las redes y bases de datos, donde se realiza un escaneo de puertos para verificar qué puertos están abiertos intentando obtener información sobre el servicio que se ejecuta en él. Tomando el tiempo que utilice esta información para encontrar vulnerabilidades relacionadas con las siguientes vulnerabilidades: Hay tres métodos de detección.

A través del ***escáner de vulnerabilidades***, se pueden utilizar herramientas como Nikto la cual trabaja buscando errores basados en el servidor, Nessus, Nmap, etc.

[66] VERMA, Vinita, MUTTOO, Sunil y SINGH V.B. Multiclass malware classification via first- and second-order texture statistics. Computers & Security. 2020, vol. 97, p. 101895, doi: 10.1016/j.cose.2020.101895

Una de las ventajas en lo que respecta a los escáneres de vulnerabilidades, pueden ejecutarse automáticamente, encontrando un cierto rango de direcciones IP y comenzando a escanear, la máquina ejecuta todo el proceso de casi una persona.

En el ***análisis manual***, el análisis es muy importante porque todo el escaneo automático no detecta automáticamente todas las vulnerabilidades. Puede tener en un sistema, entonces también es necesario realizar algunos. Analizando manualmente las vulnerabilidades encontradas para evitar y así poder escapar o irte.

La otra parte es ***información de consulta*** y otra parte es ***información oculta***. La cual tiene algún tipo de información pirateada de Google, por lo que puedes mencionarla o algo similar, usando un servicio simple, es decir, busca información en las siguientes ubicaciones, red para construir o encontrar información útil para la organización, donde identifica ciertas vulnerabilidades que pueden tener todos los servicios.

7.3.1 ESCANEAR EL SISTEMA OPERATIVO PARA DETECTAR VULNERABILIDADES

Otra parte fundamental del ciclo de corrección de errores, es parte del sistema de escaneo para detectar fallas. En este paso, el escáner por lo general, verifica el software, la configuración o el equipo que tiene cada dirección IP y determina si se han reportado vulnerabilidades en el servicio o software o de alguna configuración. Del mismo modo, si se realiza un escaneo de cumplimiento, el escáner verificará la máquina que detecta configuraciones inseguras. Tenga en cuenta que el escáner requiere acceso de administrador a las siguientes computadoras: Serán escaneados, y al final de dicho escaneo, producirá un listado de todas las vulnerabilidades detectadas.

7.3.2 IDENTIFICAR LAS VULNERABILIDADES

En otra parte del ciclo de reparación, las vulnerabilidades se comprueban en lagunas listas. Lo importante es escanear el sistema en busca de vulnerabilidades, etc. La diferencia es que para verificar las vulnerabilidades en la lista activos de la empresa. Esto incluye la identificación de vulnerabilidades con las siguientes vulnerabilidades: Detectados por el escáner, primero, están relacionados, generalmente si un escáner produce demasiados errores, el escáner puede producir falsas alarmas Las falsas alarmas tardarán mucho en solucionarse, La cuenta no es innecesaria.

7.3.3 PRIORIZAR LOS RIESGOS

No se pueden reparar todas las vulnerabilidades detectadas, por eso, es necesario categorizar los riesgos, y lo más importante es imponer riesgos a organización. No puede resolver todas las fallas encontradas porque casi no tiene tiempo, pocos empleados y, lo más importante, muy poco dinero. Para ello, la organización debe en primer lugar, céntrese en solucionar las vulnerabilidades más graves en los sistemas críticos, pero para ello, se debe diseñar un plan de prioridades para La gravedad de la vulnerabilidad y la importancia del sistema para la empresa.

7.4 INFRAESTRUCTURA CAPAZ DE BRINDAR UNA ALTERNATIVA ANTE LA APARICIÓN DE VULNERABILIDADES A NIVEL DE SOFTWARE Y HARDWARE

Ante la aparición de vulnerabilidades en el sistema operativo de Windows se plantean dos niveles de infraestructura uno que es la parte del software y el otro que es el hardware, con el fin de brindar alternativas ante la aparición de las vulnerabilidades más importantes las cuales son:

7.4.1 SOFTWARE

Las vulnerabilidades en el software por lo general son una debilidad o fallo en el sistema operativo que pone en riesgo la seguridad de la información en el equipo. Permitiendo que el atacante pueda comprometer los datos y la integridad de un usuario, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estas pueden tener distintos orígenes, por ejemplo; errores de configuración, diseño o carencia de procedimientos.

7.4.1.1 ACTUALIZACIÓN DE SOFTWARE: SISTEMA OPERATIVO Y APLICACIONES

La actualización del software se debe realizar mediante sitio de confianza que no implique riesgo para el sistema, la mejor opción para actualización es emplear un sitio oficial ofrecido por el fabricante.

Para las organizaciones es necesario disponer de políticas que involucren las actualizaciones como una obligación corporativa, que les atribuya una responsabilidad a la empresa sobre la gestión y administración de parches de seguridad sobre los sistemas operativos y las aplicaciones.
.

7.4.1.2 SEGURIDAD EN EL SISTEMA OPERATIVO

Las configuraciones del sistema operativo para prevenir posibles situaciones de riesgo se describen a continuación:

Desactivar las carpetas compartidas para evitar la infiltración de posibles ataques por medio de este segmento.

Hacer uso de contraseñas lo sumamente robustas, que impidan la fácil detección pro medio de herramientas de fuerza bruta.

El perfil que sea designado para el usuario, no debe tener privilegios elevado, esto aumenta la vulnerabilidad sobre el sistema, en un inicio las cuentas de usuario poseen privilegios administrativos que deben ser modificado para elevar la seguridad.
Contar con una plataforma moderna que cuente con actualizaciones y soporte técnico.

Impedir la ejecución automática de los medios extraíbles como medios USB, pues son de los medios utilizados para propagar un ataque.

Configurar las características para los archivos ocultos, pues son comunes archivos maliciosos con atributos de esta índole.

Verificar que las extensiones de los archivos se mantengan visibles, de esta manera será posible identificar cuando una extensión no corresponde al archivo que se encuentra allí, y podría significar una alerta de ataque.

7.4.1.3 SEGURIDAD EN REDES PEER - TO – PEER

Además de la implantación de un antivirus muy efectivo, es preciso tomar medidas con respecto al almacenamiento de información, cualquier información de tipo confidencial no debe almacenarse en el equipo que pertenece a la red p2p y por la cual se comparte otro tipo de información.

Tomar medidas para lograr comprobar la integridad de los archivos descargados, verificar tamaño de la información entre otras características.

La carpeta de intercambio por red debe contener únicamente los archivos que se desean compartir, y la configuración del programa cliente debe estar debidamente configurada para mejorar la seguridad en la comunicación.
.

7.4.1.4 ZONA DESMILITARIZADA (DMZ)

Generalmente se describe a una zona desmilitarizada (DMZ) cono una configuración de la red apartada de la red de área local (LAN), en donde se interponen los servicios, con direcciones ip privadas apartadas de la LAN, con la finalidad de proteger los equipos terminales de la red local. Ambas secciones estarán separadas por un cortafuego, en algunas redes más seguras se suelen hacer arreglos de cortafuegos para permitir una mayor seguridad dentro de la red, estableciendo diferentes topologías lógicas.

Si las estructuras se conectan juntas a una misma red, conformando un bastión, se corre el riesgo de que uno de los servidores esté infectado y ponga en riesgo al resto de la red, cabe aclarar que la mayoría de los ataques son dirigidos a los servidores. De manera resumida, una DMZ debe estar compuesta por un router frontera, y un firewall, para separar adecuadamente las dos redes, la de servicios y la local. En algunos casos con el ánimo de proteger la red interna, se suele emplear un segundo cortafuego entre la DMZ y la red LAN, lo que posibilita la configuración de rutas estáticas, que regulen el tráfico circundante entre ambas redes.

Por lo general, los equipos conectados a la DMZ no tienen acceso a la LAN, a menos que el administrador de las mismas, le haya otorgado ese permiso. A continuación, se muestra un ejemplo de una red simulada donde se establece una DMZ en apoyo a los argumentos anteriores.

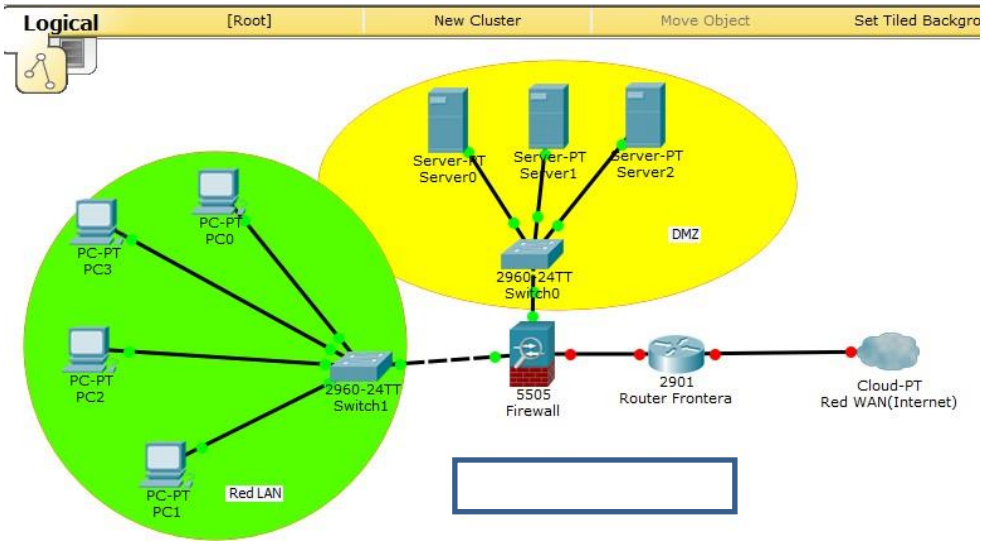

Figura 27: DMZ estrategia

7.4.2 HARDWARE

En cuanto a seguridad a nivel de hardware, existen muchos dispositivos que permitan realizar acciones de protección supervisada y no supervisada dentro de una red computarizada. Sin embargo, para esta propuesta, como se ilustra en la figura anterior, se pueden emplear enrutadores y firewalls que cumplan con las funciones de aislar las conexiones no deseadas. Tal es el caso de los equipos de tecnología UMT.

7.4.2.1 DISPOSITIVOS UMT

En la actualidad, debido a la innumerable cantidad de amenazas cibernéticas, y a la fusión de algunas de ellas, ha surgido una tecnología que ha venido cobrando fuerza debido a la naturaleza de los problemas que afrontan las redes. Ésta tecnología es la UTM, gestión unificada de amenazas de sus siglas en inglés, es una única solución de seguridad que integra diversos esquemas de seguridad, como la detección de virus, spam, malware, algunos traen integrada la opción de configuración de firewall, traducción de direcciones con el protocolo NAT (network address translation), entre otras funcionalidades.

Lo atractivo de este tipo de sistemas de seguridad, es su sencillez en la implementación e instalación, sin embargo, trae consigo una gran desventaja, al ser el único punto de seguridad en las redes, pues son el punto más vulnerable a ataques, una vez sobrepasado este limitador, la red entera estaría en riesgo, inclusive, por un mal funcionamiento del equipo ya sea por software o por daño físico, se comprometería la integridad de la red.

En vista de ese problema que posee la tecnología antes mencionada, se suele emplear software o hardware secundario, como sistema de seguridad de respaldo, en caso de que la UTM llegase a fallar, unos ejemplos son firewalls físicos y de software, aunado con sistemas de antivirus licenciados.

Una UTM conocida en el mercado por su relación costo beneficio es la Zyxel Zywall (usg) Utm Firewall, Blocks Ransomware, Pu W2, con un costo promedio de 2.00.00 COP.

Figura 29: UMT Zyxel Zywal

Adicionalmente, en las configuraciones de la red, deberán configurarse algunos puertos de salida para establecer protocolos de comunicaciones seguros, a continuación, se listan algunos:

Tabla 1. Lista principal de puertos a configurar, para asegurar las conexiones I/O.

PUERTO	SERVICIO	DESCRIPCIÓN
22	SSH	Secure shell remote login protocol
23	Telnet	Acceso a terminal remoto
25	SMTP	Simple mail transfer protocol
109	POP2	Post office protocol
115	SFTP	Simple file transfer protocol
161	SNMP	Simple network management protocol
197	DLS	Directory location service
443	HTTP	Hyper text transfer protocol
546	DHCP	Dynamic host configuration protocol
631	UDP	User datagram protocol

Se deberá configurar la red para asegurar el log de sus empleados y las conexiones cliente que ingresan a la red, de manera tal que se ajustan las certificaciones digitales que permean el flujo de clientes, cada certificado digital está compuesto por llaves públicas y privadas, para que la autoridad de certificación avale la conexión, dentro de los certificados necesarios para asegurar las conexiones están:

1) Certificado Wilcard: Proporciona protección SSL para un número indeterminado de sub-dominios, conocido con el nombre que aparece en su CSR (solicitud de firma de certificado)
2) Certificado SSL escalable: proveen niveles de cifrado de hasta 2048 bits. Ofrece la máxima protección que puede darse.
3) Certificado de firma de código: utilizados para firmar digitalmente una fuente, para demostrar que no ha sido alterada ni modificada.
4) Sello de sitio: Proporciona certificación de legitimidad al sitio web.
5) SSH: se implementa principalmente para proveer un certificado de conexión remota.
6) TLS: Integra un estilo SSL de cifrado al sistema, permite que el mecanismo de acción de los puertos del protocolo TCP/IP a nivel del túnel funcionen de manera segura.

7.4.2.2 HONEY POTS

Una alternativa adicional, que no se contempla en el diseño original, es la configuración de HoneyPots, para enmascarar el ataque externo o al menos otorgarle un señuelo alos atacantes. Una HoneyPot generalmente se define como un recurso computacional que simula ser un objetivo abierto para ser acatado, su principal objetivo es distraer a los atacantes para obtener información del ataque y el atacante. El valor real que se le da a este tipo de recursos, es que puedan ser escaneados, atacados o comprometidos, para obtener información esencial de las intrusiones a los sistemas. La principal ventaja de este tipo de recursos, es que todo el tráfico se considera sospechoso, es decir, no se contempla un tráfico normal, a pesar de que no es un mecanismo de defensa como tal, puede detener al atacante hasta ser descubierto, sin embargo, el costo de mantenimiento es muy alto. Pueden categorizarse por el nivel de interacción:

- Bajo nivel de interacción: fáciles de instalar y mantener, solo proveen servicios emulados, distractores para el atacante, no posee ningún sistema operativo sobre el cual el atacante pueda operar
- Nivel medio de interacción: opera con niveles más avanzados de interacciones con el atacante, a pesar de tampoco poseer sistema operativo, provee una ilusión mayor de objetivo para el atacante
- Alto nivel de interacción: Se convierten en objetos de ataque mucho más atractivos para los atacantes, pues poseen un sistema operativo sobre el cual pueda ejercerse una mayor presión, dan indicadores mucho más reales de las intenciones del atacante.

8 CONCLUSIONES

A partir de las diferentes metodologías que se ven en la seguridad informática es posible establecer un conjunto de amenazas junto con sus posibles formas de defendernos ante las eventualidades presentes en los sistemas operativos, para ser enfáticos sobre Windows aunque las demás plataformas de sistemas operativos no son ajenos al caso, la mayoría de amenazas presentes en estas interfaces surgen de las problemática de que existe entre los hackers de sombrero blanco o los de sombrero negro que luchan por atacar y otros defender ocasionando que los usuarios que son los directamente implicados sufran de todos estos cambios, las herramientas para contener cada una de las amenazas radica en el sistema operativo junto con la disponibilidad monetaria que aunque no fue definida dentro del texto corresponde a grandes suma, debido a que el manejo de datos está presente en cualquier tipo de sistema, más si es un entorno de información de bases de datos o centro de respuestas, la mayoría de estrategias para contener los ataques se basan exclusivamente en el uso de metodologías que deben estar encaminadas a la solución de las operaciones dentro de las normativas de la empresa.

Cuando hablamos de definir un tipo de infraestructura debemos tener en cuenta el ámbito donde debe ser aplicado, la infraestructura tanto física como lógica no es igual para todo los escenarios de un sistema ni resistente a todas las amenazas, el plantear una infraestructura es un trabajo arduo y extenso que contempla el tipo de datos que se manejan el volumen de datos, la capacidad de información, los escudos los sistemas operativos, la importancia de la información a partir de estos criterios que se consideran como básicos prima algo mucho más importante, que es el factor de implantación el cual tiene un costo que en la mayoría de situaciones es difícil de prever debido a que no podemos partir de unos supuestos si no conocemos directamente las necesidades que tiene una empresa de la implantación de un sistema tanto en hardware como en software que pueda contener los ataques , solo podemos prever y tratar de contenerlos.

El desarrollo de una caracterización de amenazas puede lograrse en un ámbito investigativo donde se tengan en cuenta todas las variables que compone un sistema, para este caso particular un entorno Windows en el cual se presentan varios ataques que son posibles de contener siempre y cuando las necesidades de la empresa estén debidamente enmarcadas sobre metodologías de ethical hacking que dan la robustez esperada a la implementación de topologías, algoritmos y estrategias criptografías que sean necesarias para las eventualidades específicas.

Los trabajos de construcción de análisis de vulnerabilidades presentes en la plataforma Windows obedecen a múltiples aspectos y características que se deben tener en cuenta para establecer un conjunto de metodologías que se adapten a este

tipo de afectaciones, dentro de las nuevas estrategias que no se contemplan en el documento son las basadas en inteligencia artificial IA las cuales poseen núcleos de aprendizaje basados en las separaciones optimas a los hyperplano y la categorización por etiquetas donde es posible parametrizar a nivel de software y hardware debido a la vinculación del software, las amenazas sobre la plataforma Windows pueden ser soportadas mediante estas estructuras de machine learning, deep learning o cualquier tipo de IA´s que darían un soporte optimo a todas estas problemáticas que afectan al sistema operativo Windows, en el momento los desarrollos son muy nuevos por lo que tener porcentaje de eficiencia y efectividad no serían claros, o les faltaría soporte o rigor científico pero es una realidad que en algunos años la detección, acción y protección se harán con este tipo de estrategias que se basan en un aprendizaje secuencial de relaciones que favorece los sistemas operativos, para este caso puntual Windows que es el sistema operativo más usado en el mundo pero al mismo tiempo es el sistema más vulnerable.

9 BIBLIOGRAFÍA

ÁLAVA MERO, Christian José, MURILLO QUIMIZ, Ángel Leonardo y CASTILLO ALEXANDER, Bryce, HASEEB, Sohaib y BARANCHUK, Adrian. Are implanted electronic devices hackable. Ontario, Canadá. Division of Cardiology, Queen's University, Trends in Cardiovascular Medicine. 2018. https://doi.org/10.1016/j.tcm.2018.11.011.

ÁLVAREZ, G., & Pérez, P. Seguridad informática para empresas y particulares. 2004. https://doi.org/978-84-481-4008-3

ARANO CHÁVEZ, Raúl Manuel, ESPINOSA MEJÍA, Francisco y ARROYO GRANT, Georgina. El rol de la dirección estratégica en las empresas. Académicos de la Facultad de Ciencias Administrativas y Sociales de la Universidad Veracruzana. 2000. 29–31.

ASHVINI, Dheshmukh, PARIKSHIT, Mahalle. Survey on Linux Security and Vulnerabilities. Maharashtra, India.: Department of Computer Engineering, Smt. Kashibai Navale college of Engineering, University of Pune, Ijecs.In, 2014. 3, 8265–8269. Retrieved from http://www.ijecs.in/issue/v3-i9/58 ijecs.pdf

ASHVINI, Dheshmukh, PARIKSHIT, Mahalle. Survey on Linux Security and Vulnerabilities. Maharashtra, India.: Department of Computer Engineering, Smt. Kashibai Navale college of Engineering, University of Pune, Ijecs.In, 2014. 3, 8265–8269. Retrieved from http://www.ijecs.in/issue/v3-i9/58 ijecs.pdf

BASHAH, A., Ali, M., Yaseen, A., Shakhatreh, I., & Syazwan, M. Procedia Computer SQL-injection vulnerability scanning tool for automatic creation of SQL-injection attacks. Procedia Computer Science,2011. 3, 453–458. https://doi.org/10.1016/j.procs.2010.12.076.

BREWER, Ross. Advaxnced persistent threats: Minimising the damage. Network Security, 2014, 5–9. https://doi.org/10.1016/S1353-485870040-6

CRISTIAN LUGA, Jason y EROLA, Arnau. Baiting the Hook: Factors Impacting Susceptibility to Phishing Attacks [en línea]. Oxford: Human-Centric Computing and Information Sciences, 2016.

DAVILA VILLANUEVA, Miguel Augusto y SUXE RAMÍREZ, María Alicia, MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. Tesis para optar el título profesional de ingeniero de sistemas. Chimbote, Perú Universidad Católica los Ángeles de Chimbote. Junio de 2018.

ESTRADA COLA, Carlos y GARCÍA VALDÉS, Angela Maria y GARCÍA FONT, Victor. Estudio sobre el malware Ransomware. 2019, p. 117, [En linea]. Disponible en:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89025/6/cestradacolTFM0119memoria.pdf

FAJARDO DIAZ, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el Mercado colombiano. Tesis de pregrado, 2017. Instituto Universitario Politécnico GranColombia.

FERRER, Jorge y FERNÁNDEZ-SANGUINO, Javier. Seguridad informática y software libre. 2007, 1–11.

FREIRE FAJARDO, Franklin. Plan de Contingencia Ante Ciberataques [en línea]. Tesis de Maestría. Escuela Superior Politécnica del Litoral, 2017 [consultado 11 mayo 2020]. Disponible en https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf FREIRE FAJARDO.FREIRE FAJARDO.FREIRE FAJARDO, “Plan de Contingencia Ante Ciberataques.”

GARCÍA MONJE, Robert Alexander, Seguridad Informática Y El Malware. 2017, p. 11, Tesis de Licenciatura. Universidad Piloto de Colombia [en linea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2641

GARDOKI, Cardenal. Ataques de inyección SQL Qué son y cómo protegerse. Bilbao, Vizcaya. 2013.

GIMÉNEZ ALBACETE, Jose Francisco. Seguridad en equipos informaticos. Antequera, Malaga. 2014

GÓMEZ VIEITES, Álvaro La importancia del factor humano en la seguridad informática. 2017 [consultado 30 de junio 2020]. Artículo publicado por EDISA. Compañía de software en Madrid, España.

GONZÁLEZ, Diego. Diseño de Un Plan Estratégico de Seguridad de La Información, Mediante La Aplicación de Análisis de Riesgos Con La Norma ISO/IEC 27005. Caso de Estudio INAMHI. Revista INNOVA. 2018, vol. 3, no. 2, pp. 84-91. ISSN 2477-9024

GUERRERO-HIGUERAS, Ángel Manuel, DECASTRO-GARCÍA, Noemí y MATELLÁN Vicente. Detection of Cyber-attacks to indoor real time localization systems for autonomous robots. Robotics and Autonomous Systems. [En línea] 2018. 99, 75–83. https://doi.org/10.1016/j.robot.2017.10.006

GUZMÁN PACHECO, Goyo Francisco. Metodología para la seguridad de tecnologías de información y comunicaciones en la clínica Ortega. Tesis de postgrado 2015. Universidad Nacional del Centro de Perú

INSTITUTO NACIONAL DE CIBERSEGURIDAD, Ransomware : una guía de aproximación para el empresario Índice. 2017. [En linea]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

KANAT ALEXANDER, Max. Code simplicity: the science of software development., 2012. [en línea] Editorial O´reilly media Inc. Estados Unidos de América.

KIGERL, Alex. Profiling Cybercriminals: Topic Model Clustering of Carding Forum Member Comment Histories [en línea]. Washington: Social Science Computer Review, 2017.

KRAUS, Rob, BARBER, Brian, BORKIN, Mike y ALPERN, Naomi. CHAPTER 1 – Windows Operating System – Password Attacks. Seven Deadliest Microsoft Attacks, 2010. 1–23. https://doi.org/10.1016/B978-1-59749-551-6.00001-7

KRAUS, Rob, BARBER, Brian, BORKIN, Mike y ALPERN, Naomi. SQL Server – Stored Procedure Attacks. Seven Deadliest Microsoft Attacks. November 2009, 49–69. https://doi.org/10.1016/B978-1-59749-551-6.00003-0.

LEE, Inyong, JEONG, Soonki, YEO, Sangsoo y MOON, Jongsub. A novel method for SQL,2010.

LÓPEZ MATACHANA. Los virus informáticos : una amenaza para la sociedad. Retrieved. [en línea].2020 [consultado 01 de Diciembre 2020]. Disponible en http://bibliotecavirtual.unad.edu.co:2139/eds/detail/detail?vid=9&sid=e2e23ef1

MANSFIELD-DEVINE, Steve. The malware arms race. Computer Fraud and Security, 2018, 15–20. GIMÉNEZ ALBACETE, Jose Francisco. Seguridad en equipos informaticos. Antequera, Malaga. 2014.

MATA VILLALPANDO- BECERRA, Isaac, y GUEVARA-JUÁREZ, Oscar Antonio. Virus informáticos, todo un caso, pero no perdido. CienciaUAT, 2010, vol. 4, no. 4, pp. 56–61. ISSN: 2007-7521

MCWHIRTER, Paul, KIFAYAT, Kashif, SHI, Qi, y ASKWITH, Bob. SQL Injection Attack classification through the feature extraction of SQL query strings using a Gap-Weighted String Subsequence Kernel. Journal of Information Security and Applications. 2018, vol. 40, pp. 199–216, doi: 10.1016/j.jisa.2018.04.001.

MCWHIRTER, Paul, KIFAYAT, Kashif, SHI, Qi, y ASKWITH, Bob. SQL Injection Attack classification through the feature extraction of SQL query strings using a Gap-Weighted String Subsequence Kernel. Journal of Information Security and Applications. 2018, vol. 40, pp. 199–216, doi: 10.1016/j.jisa.2018.04.001.

MEADOWS, Oliver. Window Safety Devices. J. Pediatr. Heal. Care, 2010, vol. 24, no. 3, pp. 199–202, doi: 10.1016/j.pedhc.2009.12.002
MERINO, Miriam Adriana, Introducción a la seguridad informática y el análisis de vulnerabilidades. Ingenieria y Tecnología. 2018. ISBN: 978-84-949306-1-4.
MIRA ALFARO José, y MONTAÑA, Rogelio. Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia. Tesis. 2002. 1, 1–142.

MOHAMED, Gori y VISUMATHI. A predictive model of machine learning against phishing attacks and effective defense mechanisms. Materials Today: Proceedings c. 2020, no:1225, doi: 10.1016/j.matpr.2020.09.612.

MONDRAGÓN MACA, Oscar Eduardo, MERA ARCOS, Andrés Felipe, URCUQUI, Christian y NAVARRO CADAVID, Andrés. Security control for website defacement, Sist. y Telemática. 2017, vol. 15, no. 41, pp. 45–55, doi: 10.18046/syt.v15i41.2442

MORA RODRÍGUEZ, David, y MUÑOZ, Mario. Memory Corruption Failures Attack and Defense Techniques. Revista Ingenierías Universidad de Medellín. 2011. 10, 149–158. ISSN 1692-3324.

MOYLE, Steve. The blackhat ' s toolbox : SQL injections, Network security. 2007 vol. 2007, no 11, p. 12-14.

NGO, Quoc-Dung, NGUYEN, Huy-Trung, NGUYEN, Le-Cuong y NGUYEN, Doan-Hieu. A survey of IoT malware and detection methods based on static features. ICT Express, 2020, doi: 10.1016/j.icte.2020.04.005.

OCAMPO, Carlos Alberto, CASTRO BERMÚDEZ, Yanci Viviana y SOLARTE MARTÍNEZ, Guillermo Roberto Sistema de detección de intrusos en redes corporativas Intrusion Detection System in Corporate Networks. Pereira, Risaralda. Universidad Tecnológica de Pereira. 2017, Vol. 22, No. 1

ORDUZ BARRERA, Diana. Análisis de Emergencias Cibernéticas Que Se Presentan En Las Ciudades de Tunja, Duitama y Sogamoso Con Respecto Al País En Los Últimos Dos Años [en línea]. Monografía de posgrado. Universidad Nacional Abierta y a Distancia, 2019 [consultado 11 Noviembre 2020].Disponible en https://repository.unad.edu.co/bitstream/handle/10596/31410/dmorduzb.pdf?sequence=1&isAllowed=y

PING-CHEN, Xue. SQL injection attack and guard technical research. Advanced in Control Engineeringand Information Science. 2011. 15, 4131–4135. https://doi.org/10.1016/j.proeng.2011.08.775

RIXOM, Jessica, y MISHRA, Himanshu. Ethical ends: Effect of abstract mindsets in ethical decisions for the greater social good. Organizational Behavior and Human Decision Processes. 2014, 124, 110–121. https://doi.org/10.1016/j.obhdp.2014.02.00.

ROESSING, Rolf Von. Highwaymen to hackers. Computer Fraud and Security, 2016, 13–15. https://doi.org/10.1016/S1361-372330026-4

ROMERO CASTRO, Martha Irene, FIGUEROA MORÀN, Grace Liliana, VERA NAVARRETE, Denisse Soraya, ÁLAVA CRUZATTY, José Efraín, PARRALES ANZÚLES, Galo Roberto, ÁLAVA MERO, Christian José, MURILLO QUIMIZ, Ángel Leonardo y CASTILLO MERINO, Miriam Adriana, Introducción a la seguridad informática y el análisis de vulnerabilidades. Ingenieria y Tecnología. 2018. ISBN: 978-84-949306-1-4

RUTKIN, Aviva. The health hackers. New Scientist. 2015. 2273028, 18–19. https://doi.org/10.1016/S0262-407930690-4.

SMITH, Craig. The Car Hacker’s Handbook. Network Security, 2016, 4. https://doi.org/10.1016/S1353-485830034-4

SOPHOS. Informe de Amenazas 2019 de SOPHOSLABS. Sophos, p. 27, 2019, [En linea]. Disponible en: https://www.sophos.com/es-es/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf.

TOVAR VALENCIA, Orlando. Inyección De Sql , Tipos De Ataques Y Prevención En Asp . Net - C#. Universidad Piloto de Colombia. 2014, pp. 1–9.

TURGEMAN, Avi. BioCatch and CyberLink tackle security risk. Biometric Technol. Today, vol. 2019, no. 2, p. 2, doi: 10.1016/s0969-476530015-3.

VENOSA, Lina Paula y DÍAZ, Javier. Detección de botnets utilizando herramientas Opensource Resumen Introducción. Workshop de Investigadores en Ciencias de la Computación. Enero, 2014, pp. 832–836.

VERMA, Vinita, MUTTOO, Sunil y SINGH V.B. Multiclass malware classification via first- and second-order texture statistics. Computers & Security. 2020, vol. 97, p. 101895, doi: 10.1016/j.cose.2020.101895

VERMA, Vinita, MUTTOO, Sunil y SINGH V.B. Multiclass malware classification via first- and second-order texture statistics. Computers & Security. 2020, vol. 97, p. 101895, doi: 10.1016/j.cose.2020.101895

VRBANĆIĆ, Grega, FISTER, Iztok y PODGORELEC, Vili. Datasets for phishing websites detection. Data Br., 2020, vol. 33, p. 106438, doi: 10.1016/j.dib.2020.106438

YAMPOLSKIYA, Mark, KINGB, Wayne, GATLINA, Jacob, BELIKOVETSKYC, Sofia, BROWNA, Adam, SKJELLUMD, Anthony y ELOVICIC, Yuval. Security of additive manufacturing: Attack taxonomy and survey. Additive Manufacturing. 2018. 21, 431–457. https://doi.org/10.1016/j.addma.2018.03.015

YORK, Dan. Identity, Spoofing, and Vishing. Seven Deadliest Unified Commun. Attacks, 2010, pp. 117–136, doi: 10.1016/b978-1-59749-547-9.00006-5.