CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

NILDA BECERRA FLOREZ

TUTOR:
MSc: JOHN FREDDY QUINTERO TAMAYO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
LETICIA
2020

RESUMEN

La ciberdelincuencia es una las actividades que se ha incrementado con el paso del tiempo aún más en tiempos de crisis, ya que por la problemática que estamos viviendo a nivel mundial casi todas las diligencias se deben realiza vía on line donde la gran mayoría de las personas no conocen muy bien los procedimientos que se deben tener en cuenta con respecto a la seguridad de la información y de datos, donde en un instante pueden ser víctimas de este tipo de delincuencia cibernética. Las organizaciones a pesar de tener seguridad en su infraestructura tecnológica también han sido víctimas de ataques, suplantaciones etc, los cuales en algunos casos no saben cómo manejar la situación en la brevedad posible, y esto hace que su sistema se convierta en vulnerable y corra riesgos, para lo cual es importante tener un recurso humano capacitado que implemente y ejecute mecanismos de ciberseguridad para la identificación de vulnerabilidades o fallos aplicando técnicas de ataques y contención de ataques fundamentados en una metodología con la finalidad de buscar una mejora continua con respecto a la ciberseguridad de una organización.

ÍNDICE

TABLA DE ILUSTRACIONES

GLOSARIO

BACKUS DE INFORMACIÓN: Es un respaldo de información o datos, copia que se considere importante no perder en caso de que la información original sufra algún error o daño, no se pierda toda la información, el cual se guarda en un dispositivo de almacenamiento.

CVE: lista de información registrada sobre las vulnerabilidades registradas con números de identificación las cuales son de carácter público donde se puede tener acceso, cuando se escucha hablar de un CVE, hace mención al número de identificación de una falla de seguridad

ERI: Equipo de Respuesta a Incidentes, este equipo desarrolla medidas de prevención y reactivos que ayudan a controlar y minimizar cualquier tipo de daño que se pueda presentar en sistema de información.

FIREWALL: También llamado cortafuegos, una de sus principales funciones es la del bloqueo de acceso no autorizados.

HARDENING: Proceso de aseguramiento de un sistema para reducir las vulnerabilidades.

METERPRETER: Es el intérprete de comandos que permite la interacción entre ambas máquinas, el cual se da una manera creíble que no se deja detectar fácilmente por herramientas como los antivirus.

METASPLOIT: programa informático, de tipo libre el cual nos ayuda a la verificación de vulnerabilidades de tipo de redes, aplicaciones y dispositivos implementadas en pruebas de penetración

PENTESTING: El Pentesting o también llamado test de penetración es una serie o pasos de procedimientos mediante el cual se pretenden detectar vulnerabilidades de un sistema informático, para ello existen diferentes herramientas que se pueden utilizar para lograr detectar la vulnerabilidad existente y dar soluciones a los mismos.

SIEM: Es un sistema de gestión de información y de eventos que ayuda a un sistema informático, alarmando sobre posibles amenazas que puede sufrir el sistema de una organización, que, por la integración de su tecnología y la combinación de sus funciones de seguridad ayudan a la protección de un sistema.

NMAP: es una de las herramientas utilizadas para el escaneo de puertos, también de código abierto

INTRODUCCIÓN

Los equipos Blue Team y Red Team juegan un papel importante dentro de la siberseguridad de una organización, ya que las personas que forman parte de los mencionados grupos poseen conocimientos técnicos sobre las actividades o procesos a realizar con el fin de establecer controles que permitan reforzar la seguridad cibernética de una organización, teniendo en cuenta que los activos más preciados de una organización es la información y los datos.

En el presente informe se muestra las fases implementadas en cada proceso partiendo desde la identificación y análisis de la normatividad colombiana y el código de ética desde la ingeniería y sus profesiones afines en virtud de lo contemplado en la Ley colombiana, hasta la obtención de resultados de un caso de estudio analizado mediante el cual se fundamenta en una metodología, ataque, y formulación de contención de ataque mediante el análisis de riesgos y vulnerabilidades en un sistema informático con la finalidad de buscar una mejora continua con respecto a la ciberseguridad de una organización.

OBJETIVOS

Objetivo General

Dar a conocer los mecanismos, procesos, herramientas, y acciones para la identificación de vulnerabilidades o fallos a los que se encuentra expuesta una organización, e implementación técnica para la contención de ataques informáticos en pro de mejorar la ciberseguridad en una organización.

Objetivos Específicos

1. Identificar las leyes y decretos que se rigen y que amparan los comportamientos éticos y legales en Colombia.

2. Evaluar las acciones de los equipos Red Team & Blue Team a partir de la normatividad colombiana, Ley 1273 de 2009.

3. Documentar las etapas del Pentesting para la identificación de vulnerabilidades, fallas que se presentan en un sistema informático a partir de un caso de estudio implementando metodologías y técnicas de intrusión.

4. proponer mecanismos y herramientas de contención mediante el análisis de riesgo y vulnerabilidades de una infraestructura TI.

DESARROLLO DEL INFORME

Conceptos equipos de Seguridad.

El resultado de esta primera etapa se fundamenta en la investigación sobre el Análisis de la legislación relacionada con delitos informáticos, teniendo en cuenta las actividades u oficio que desarrollemos desde nuestra profesión. Por ende, en necesario verificar, identificar, y analizar las, Leyes, normas, artículos mediante el cual la Ley colombiana nos ampara siempre y cuando seamos víctimas, en caso de ser lo contrario, estaríamos siendo juzgados por la misma Ley. En Colombia el auge de la delincuencia en el ámbito cibernético es cada vez más notorio, el cual es muy preocupante y surge la necesidad de reforzar la seguridad interna, y porque no, la externa en convenios con otros países que pueden ayudarnos a combatir este tipo de delitos que se presentan en la actualidad. En los artículos de la Ley 1273 de 2009[1] se puede identificar que cualquier tipo de actividad, acción voluntaria de una persona con fines de apropiarse de información ajena, modificar, distribuir, intercambiar y así mismo distribuir la información a través de diferentes dispositivos electrónicos esta faltado a uno de los artículos que concierne a la Ley 1273.

En Colombia se creó la Ley 1273 de 2009, el cual se denomina “De la protección de la información y de los datos” (Mintic, 2009), mediante el cual se modificó el código Penal y se crea un sistema legal a fin de proteger y preservar los sistemas que utilicen las tecnologías y las comunicaciones, donde se aplica una penalización y multas para los delitos que incurran con esta ley.
Dentro del margen legal en Colombia, los delitos informáticos son considerados actividades delictivas según la Ley 1273 de 2009, actividades de alteración, modificación o de cualquier uso indebido de los sistemas informáticos, se está incurriendo en una falta grave según la Ley en Colombia, el cual afecta la seguridad informática y la protección de la información y de datos, el cual tiene una pena de prisión de hasta 120 meses y multas de hasta de 1500 salarios mínimos legales mensuales vigentes, según la gravedad del delito, el cual están relacionados a unos artículos donde especifican los delitos para ser penalizados.

De acuerdo a la Ley mencionada anteriormente aprobada por el congreso de la república de Colombia en enero de 2009 se relacionan de la siguiente manera:

[1] Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Con respecto a la protección de datos personales en Colombia se rige mediante la Ley 1581 de 2012[2] decreto 1377 de 2013[3], es la que faculta y otorga a los individuos colombianos para que, como dueños de los datos personales decidamos a quien proporcionar la información teniendo en cuenta para qué y cómo se van a utilizar, al mismo tiempo nos permite acceder, cancelar y/o a la oposición al tratamiento de los datos personales. Se evidencia los tipos de datos según la aceptabilidad de la divulgación de la información, el cual debemos conocerlos al momento de compartir la información personal para la protección de datos personales que son: Aviso de privacidad; se debe brindar información escrita o verbal del tratamiento de los datos teniendo en cuenta la finalidad.

También están los datos públicos: son datos establecidos por la Constitución política ya sean públicos o privados, datos sensibles: vienen siendo aquellos que afecta al titular o dueño de la información, Datos Semiprivados; son aquellos que no son reservados ni públicos pero que puede ser de interés a ciertos grupos de personas,

En artículo 2 de la Ley 1581 de 2012 hay unas excepciones en el ámbito personal o doméstico, mediante el cual se exceptúan de la aplicación de dicha Ley y del presente Decreto las actividades que se inscriban en el marco de la vida privada o familiar de las personas naturales, dichos artículos aplican las informaciones de ámbito periodístico, investigaciones de inteligencia y contrainteligencia, censos poblaciones, entre otras.

Actuación ética y legal.

Se fundamenta en evaluar las acciones de los quipos Red Team & Blue Team[4] de una organización partiendo en el marco de los criterios éticos y legales según las leyes y normas que se rigen por la Constitución Política de Colombia. Se realiza un análisis en el ámbito Legal y Ético en el ejercicio de la Profesión como ingenieros, y dentro de la Ley 1273 de 2009 que ampara la Protección de la Información y de los Datos y que presentan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, como también está el código de ética Profesional regido por el Concejo Profesional Nacional de Ingeniería[5], la cual constituyen los

[2] Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

[3] Decreto 1377 de 2013 - EVA - Función Pública. (2017. Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

[4] Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. Recuperado de: https://repository.unad.edu.co/handle/10596/35497

[5] Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

“comportamientos éticos y legales en Colombia para el ejercicio de la profesión de la Ingeniería en General y sus profesiones afines y auxiliares” (Copnia, 2015).

Partiendo de un caso de estudio, identificado como escenario 2 situación problema – Análisis Legal que presenta la organización **WhiteHouse Security,** empresa reconocida mundialmente por su amplia experiencia en procesos de ciberseguridad y ciberdefensa, pero que, presenta una situación problemática no agradable desde el punto de vista ético Legal, Donde en el anexo 3 contiene un **ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE ESTUDIANTE Y WHITEHOUSE SECURITY,** el cual se da con fines de reclutamiento para sus equipos Red Team y Blue Team.

Al analizar el acuerdo de confidencialidad se evidencia una seria de irregularidades que terminarían percudido al estudiante, teniendo en cuenta la Ley colombiana 1273 de 2009 que la regula y el código de ética en ejercicio de la profesión. Para ello es importante conocer de las Leyes que nos amparan, cualquier actividad que valla en contra de lo legal está faltando a una Ley, artículo al que dicha actividad se encuentra relacionada como no permitida, en el ámbito del código ético profesional existen unas reglas que debemos obedecer al momento de ejercer una profesión. Tanto en la ingeniería, como en otras profesiones también existe el catálogo de conductas profesionales las cuales exigen, prohíben o, a bien inhabilitarlos de sus profesiones, cualquier profesional debe regirse por un código de ética, donde estipula lo que se puede o no hacer.

Los errores en el caso de estudio, se enfatiza en lo ético como falta a la ley 1273 de 2009 artículo 269 F, y también la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, el acuerdo de confidencialidad que se establece en el contrato o acuerdo van en contra de las leyes mencionadas anteriormente, que, en caso de firmarlo estaría expuesta a una serie de investigaciones e imputación de cargos de delitos, porque soy consciente de las actividades que voy a realizar, y así mismo conocedora de las consecuencias que pueden traer mis acciones. La empresa como contratante debe cerciorarse de lo estipulado en el acuerdo de confidencialidad, y se ve el obrar de mala fe en dejar desamparado a la parte receptora, donde, como trabajador no tiene garantías, ya que lo responsabilizan ante las autoridades competentes de todas las actividades a realizar que se ejecuta a favor de la empresa. Ejemplo, de uno de los acuerdos estipulado en el contrato (anexo 3 – fase 2) al momento que indican que no se pueden divulgar informaciones ilegales ante las autoridades competentes, como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos, actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros en otras actividades ilícitas y otras que allí pretendan realizar”, están violando la Ley 1273, está vulnerando Artículo 269H (Mintic, 2009) “Circunstancias de agravación punitiva, más exacto en el numeral: más exacto en el numeral 5. Obteniendo provecho para

sí o para un tercero, 7. Utilizando como instrumento a un tercero de buena fe, 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales" (P. 2)

Artículo 269 F. "Violación de datos personales. Esto aplica para el que no tiene la facultad de acceder, sustraiga, ofrezca, venda, intercambie, envié, intercepte, o modifique los datos o información personal, infringe este artículo, ya que falta a la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos" (Mintic, 2009) . Lo anterior a pesar de que la empresa lo está permitiendo como confidencial, pero al ser una actividad donde se va llevar procesos ilícitos, va en contra de una ley establecida en la Constitución Colombiana, por tal motivo se aplicaría la sanción penal y económica que estipule este artículo.

En la actualidad y con el auge de las tecnologías los delitos informáticos se dan muy frecuentes en diferentes partes del mundo, cabe aclarar que las personas que realizan este tipo de actividades tienen conocimientos y están a la vanguardia tecnológica, buscando herramientas que le ayuden a facilitar su objetivo delictivo, y al encontrarnos en un País de pocas oportunidades, existen profesionales que se le miden a realizar este tipo de actividades, muchas veces por necesidad, otras veces por ganar dinero rápido, en algunos casos por curiosidad y enriquecer sus conocimientos, el cual, sí lo hace dentro del hacking ético no hay problemas siempre cuando tenga autorización.

Para el caso de la empresa **WHITEHOUSE SECURITY** ofrece un salario bastante apetecido, pero, muy delicado en el ámbito ético legal. Como profesional, ante todo se hizo un juramento donde implica el tipo de conducta que debemos asumir a partir del ejercicio de la profesión como ingeniero, y como persona honrada, honesta y de buenos valores, No firmaría un contrato o acuerdo de confiabilidad, sabiendo de las vulneraciones o atropellos que se están cometiendo, y en lo profesional me vería perjudicada; y aún más, desprotegida por parte de la empresa, ya que están siendo muy claros y específicos en cada una de las clausulas, donde se evidencia que no se tiene garantías, ni respaldo de parte de la empresa. Por ende, si no se entiende o conoce lo estipulado en un contrato es mejor asesorarse.

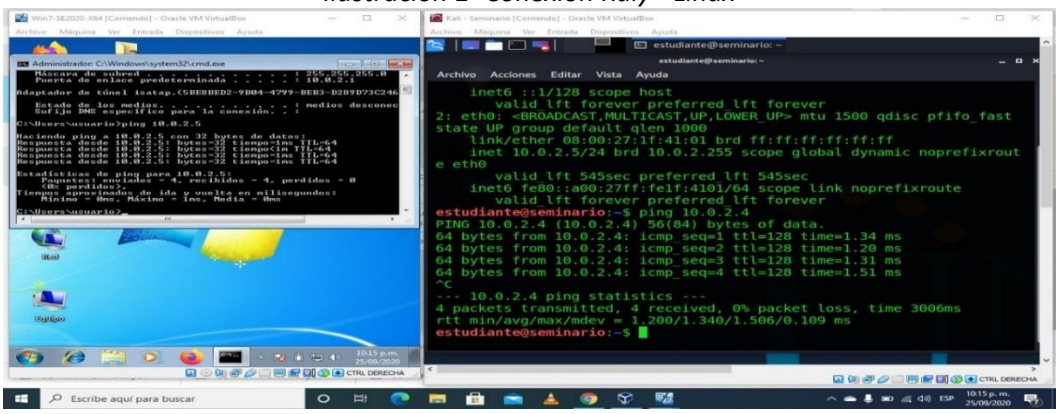
Ejecución pruebas de intrusión.

Esta etapa comprende la parte práctica de la ejecución de pruebas de intrusión utilizando herramientas pre configuradas con una situación problemica a desarrollar en aras de demostrar vulnerabilidades en un sistema informático teniendo en cuenta la metodología y técnicas.

Se trabajó con máquinas virtuales, utilizando Virtualbox versión 6.1.14, S.O Windows 7 x86, Windows 7 x64 y Kali. Es importante mencionar que, antes de dar inicio a la ejecución del pentesting[6] es importante desactivar el Firewall, Windows defender y Windows Update.

Los softwares que se llevaron a cabo para el desarrollo de la actividad fueron; Nmap, Metasploit [7], exploit eternalblue, Se configuran las máquinas en red nat para que funcionen, en la siguiente imagen se puede evidenciar la conexión de maquina win 7 x64 y la máquina de Kali seminario, al hacer ping podemos identificar la comunicación existente.

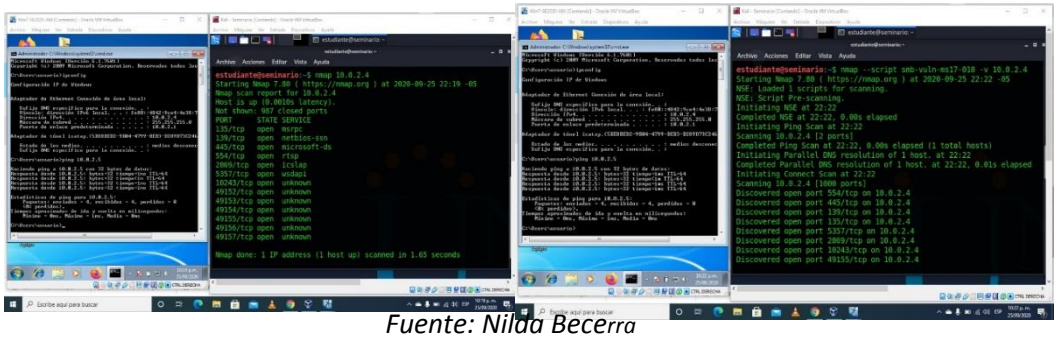
Ilustración 1- Conexión Kaly - Linux



Fuente: Nilda Becerra

Con la herramienta nmap, comando implementado; nmap --script smb-vuln -ms17-010 -v 10.0.2.4, verificamos si esta ip es vulnerable a ms17-010, en las siguientes imágenes se puede el resultado del comando ejecutado, el cual muestra el estado vulnerable del sistema.

Ilustración 2- Verificación IP.

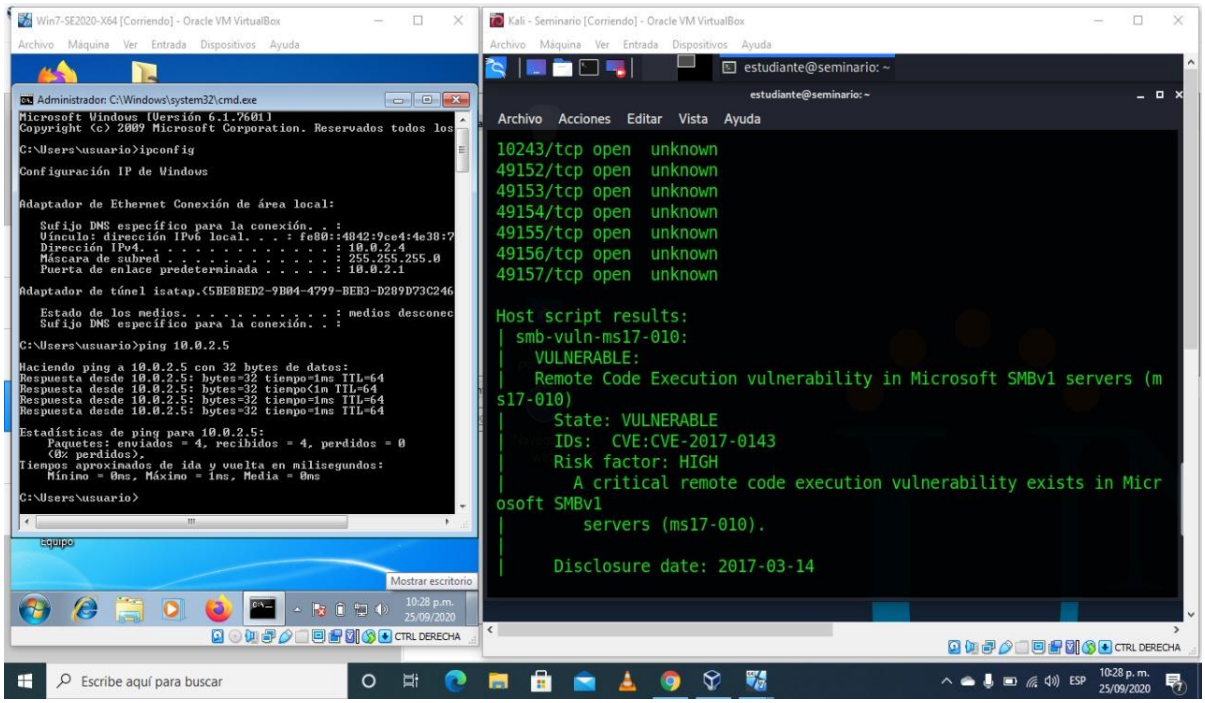


Fuente: Nilda Becerra

---

[6] Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Recuperado de: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Ilustración 3-Sistema vulnerable



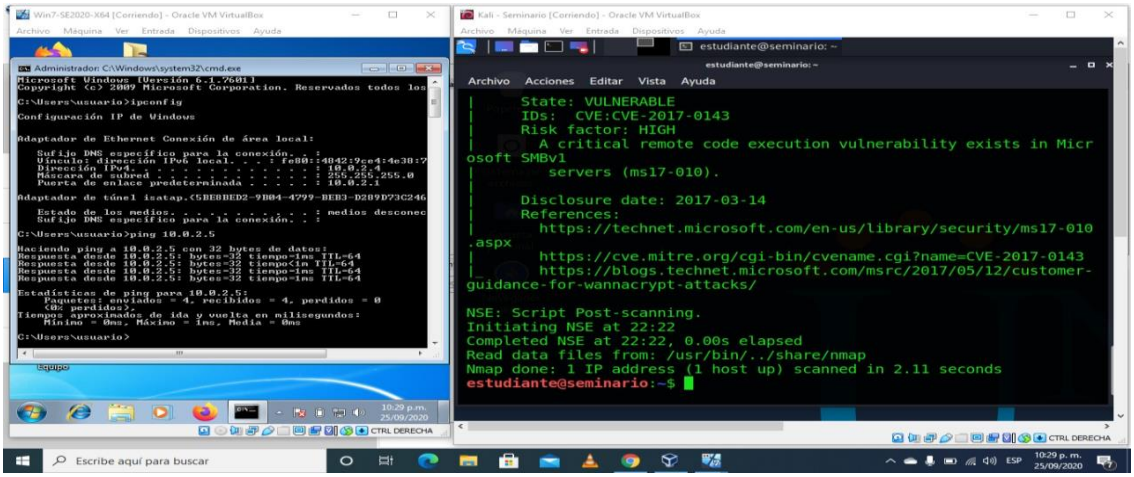
Fuente: Nilda Becerra

El fallo identificado en la siguiente imagen es un CVE-2017-0143.
El servidor SMBv1 en “Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario a través de paquetes diseñados, también conocidos como "Vulnerabilidad de ejecución remota de código SMB de Windows". Esta vulnerabilidad es diferente de las descritas en CVE-2017-0144, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148”[8].

Este fallo está relacionado a un fallo en la vulnerabilidad en el servicio de uso compartido en S.O Windows, por tal motivo permite al atacante ingresar de forma remota.

[8] hreat Landscape Dashboard | McAfee. (2020). from https://www.mcafee.com/enterprise/es-es/threat-center/threat-landscape-dashboard/vulnerabilities-details.cve-2017-0143.html

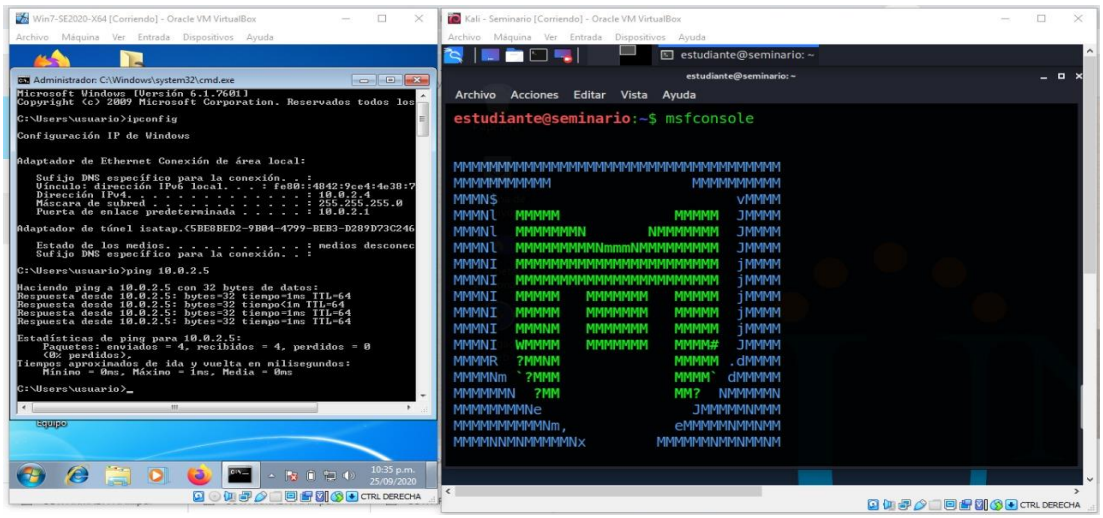
Ilustración 4-Vulnerabiliad



Fuente: Nilda Becerra

En la fase de **búsqueda de vulnerabilidades** se realizó con Franework del metasploit, payload de x64, Se inició mestasploit con el comando msfconsole desde la maquina Linux.

Ilustración 5- comando msconsole

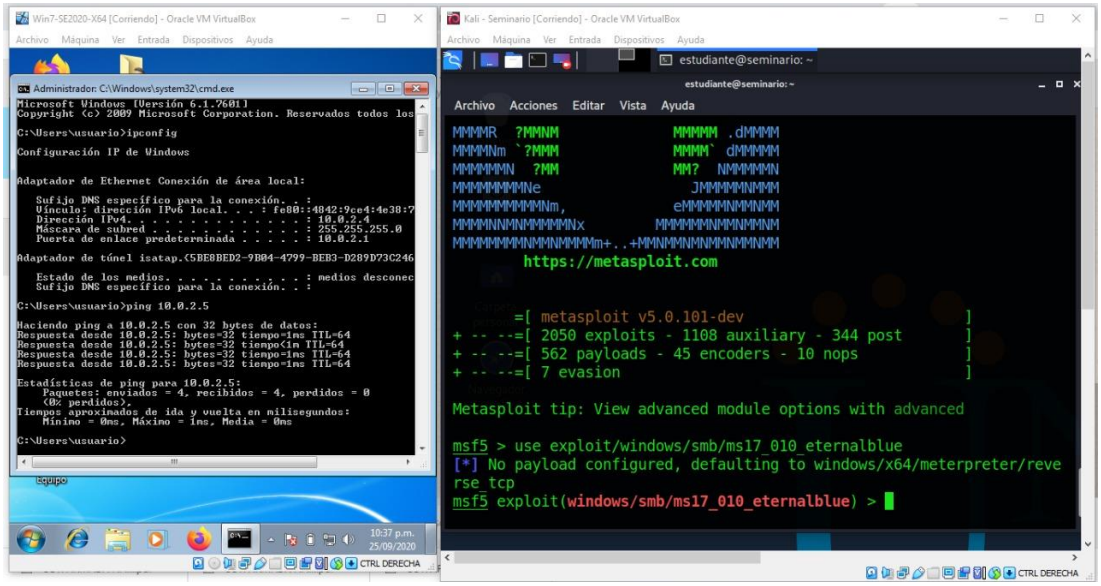


Fuente: Nilda Becerra

Al utilizar el siguiente fremwork: use exploit/windows/smb/ms17_010_eternalblue, el cual es para **explotar la vulnerabilidad** identificada.

En la siguiente imagen se puede evidenciar que el Payload no está configurado para la maquina windows 7 x64.

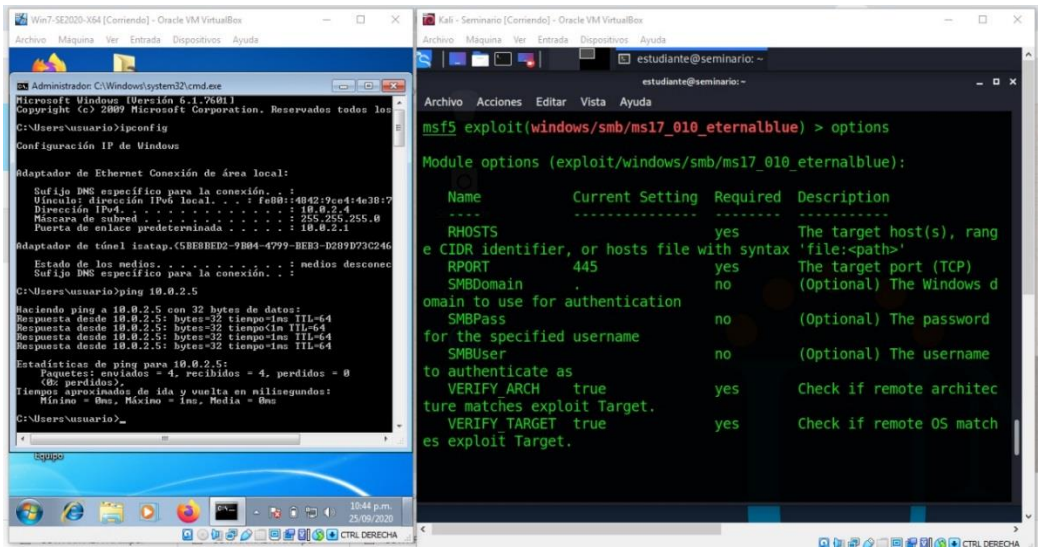
Ilustración 6-Payload wix 7x64



Fuente: Nilda Becerra

Utilizando el comando Options, se procede hacer la verificación del framwork para poder identificar el Payload que se va implementar en este proceso, también nos muestra el error de; no está configurada la ip.

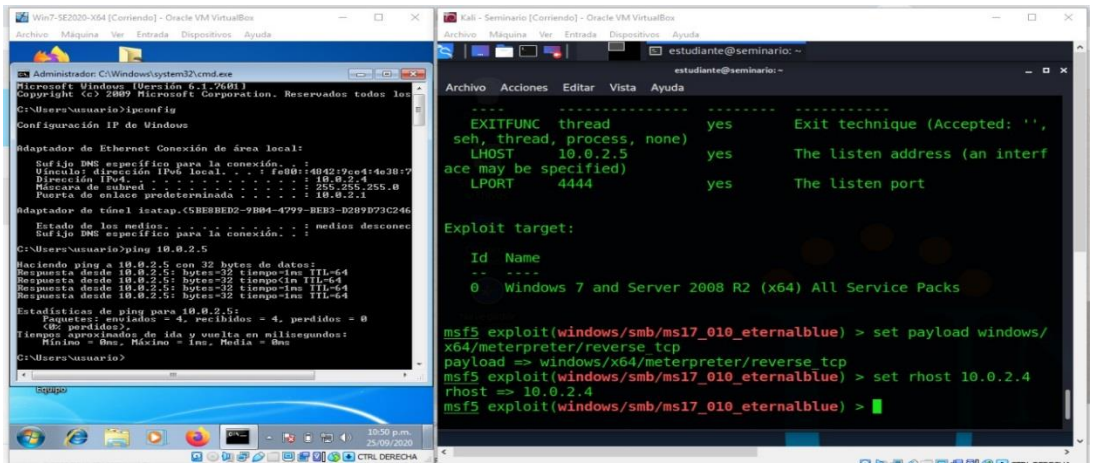
Ilustración 7-verificación del sistema



Fuente: Nilda Becerra

En la siguiente imagen nos muestra la opción del Payload a utilizar. Se procede a utilizar el payload con el comando: set payload indows/x64/meterpreter/reverse_tcp.

Ilustración 8-ejecución del Payload

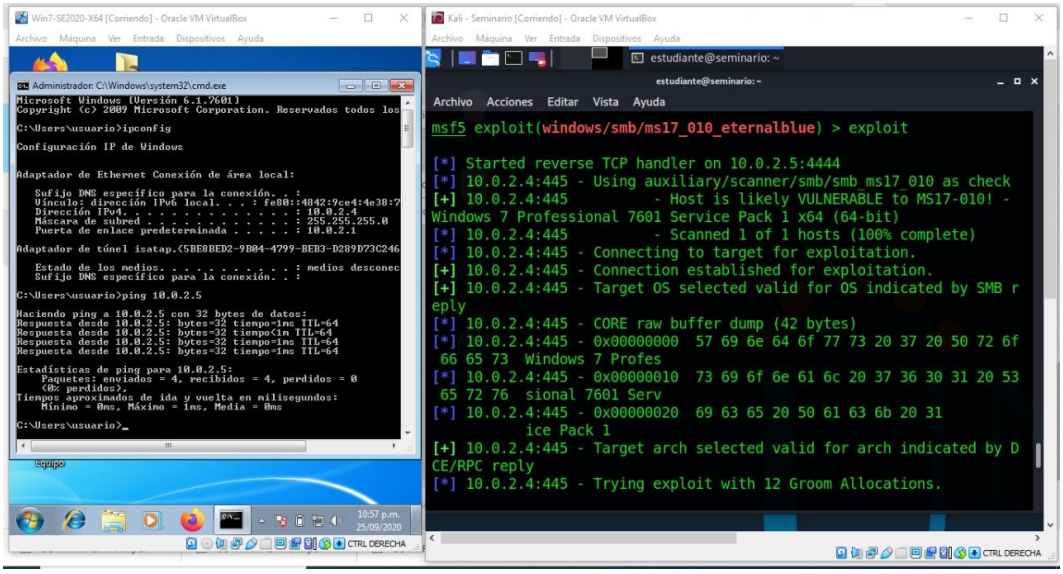


Fuente: Nilda Becerra

Procedemos a verificar haciendo uso del comando options, para ver si quedo la ip de la maquina víctima y el payload que se va usar.

Para iniciar la **fase de explotación** iniciamos el comando exploit.

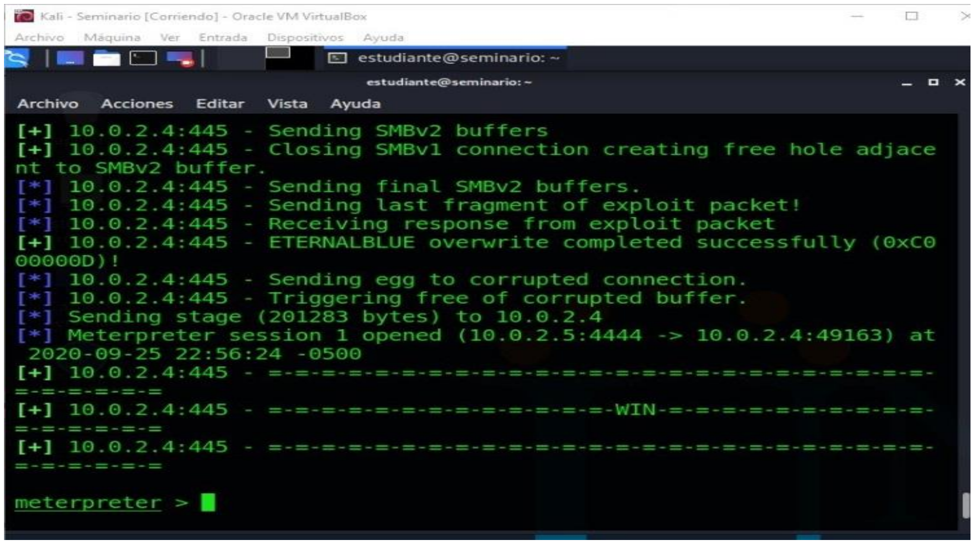
Ilustración 9-explotación



Fuente: Nilda Becerra

En la siguiente imagen nos dice que se inició una sesión en la máquina victima

Ilustración 10- Resultado ingreso a la máquina víctima

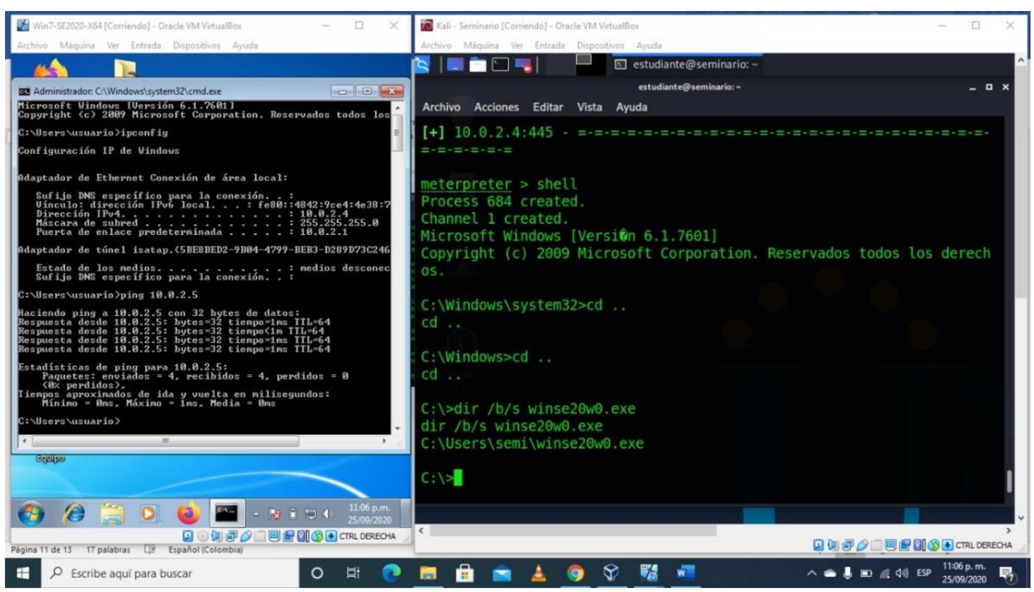


Fuente: Nilda Becerra

El meterpreter es como el intérprete de ambas máquinas. Con el comando Shell nos dirigimos al cmd o consola de comandos del Windows. Procedamos a buscar el archivo de la guía, winse20w0.exe para eso nos vamos a la raíz del sistema, saliendo de cada directorio con cd .., cd ..

Con el comando: dir /b/s winse20w0.exe nos busca la ruta dónde está el archivo ejecutable.

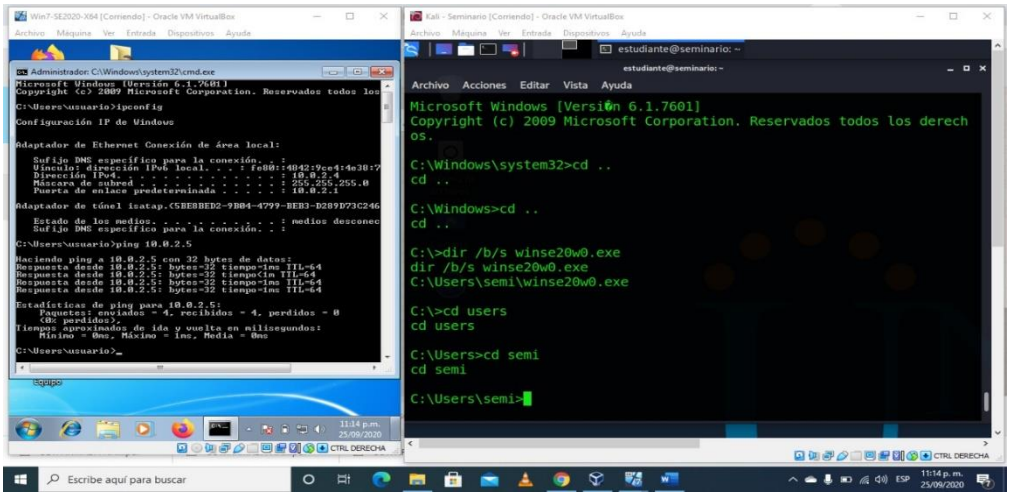
Ilustración 11-Raíz del sistema Windows



Fuente: Nilda Becerra

Procedemos a dirigimos a la ruta que nos arroja utilizando el comando cd users, cd semi, y Con dir para confirmar que en esa ruta está el archivo ejecutable semi20w20.exe

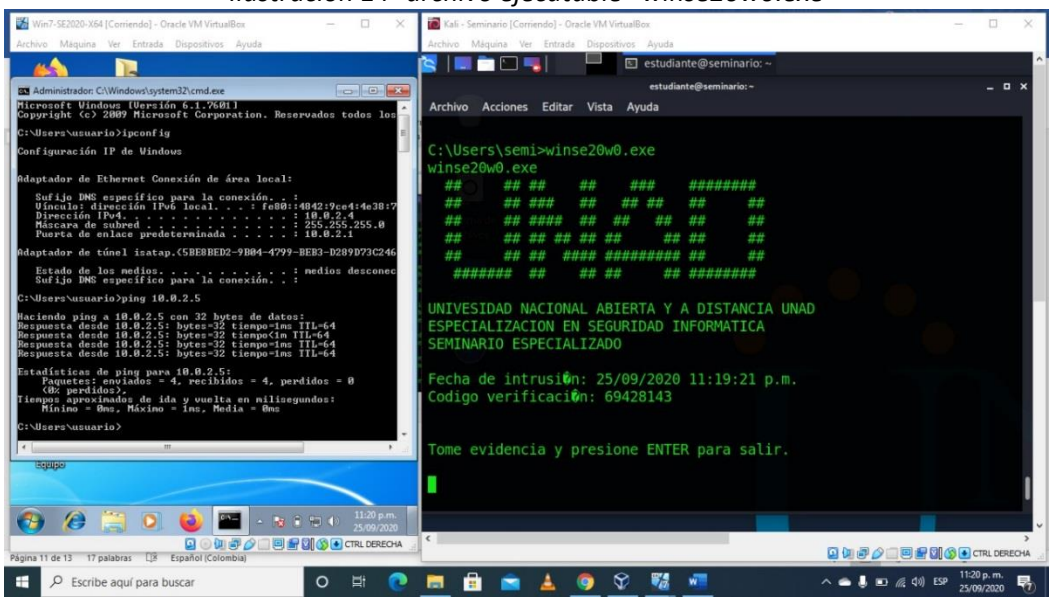
Ilustración 12-Direccionamiento ruta del archivo



Fuente: Nilda Becerra

Procedemos a ejecutar el archivo, digitando el nombre del mismo y enter, el nombre de archivo se puede verificar en la siguiente imagen.

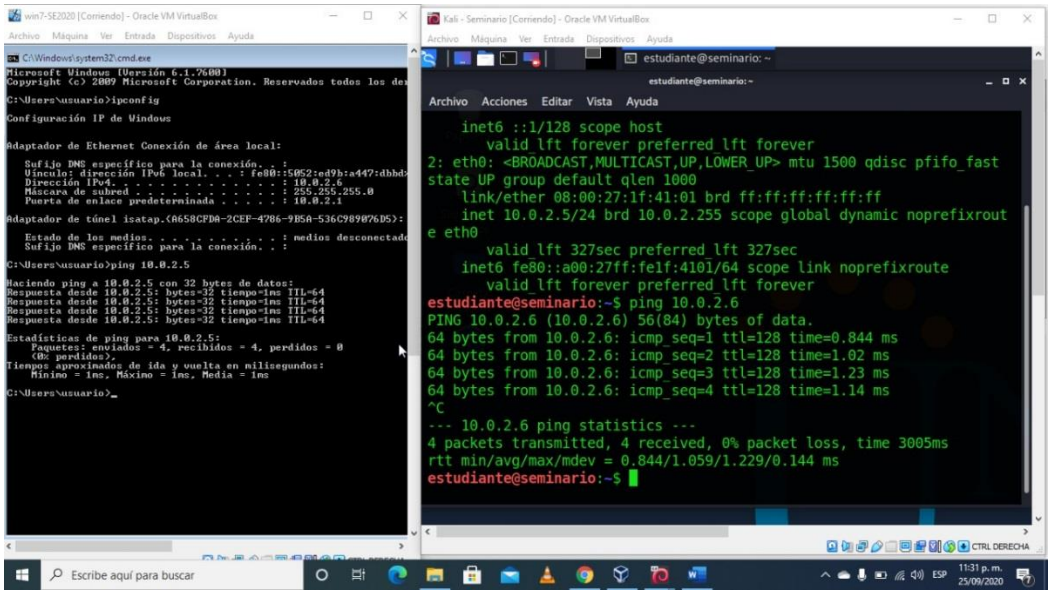
Ilustración 14- archivo ejecutable "winse20w0.exe



Fuente: Nilda Becerra

Con la segunda máquina, se realiza el mismo procedimiento, hacemos ping en amabas para ver que están en funcionamiento. En la siguiente imagen se identifica claramente las ip de ambas maquinas win7 x86 tiene la 10.0.2.6 y la kali tiene la 10.0.2.5

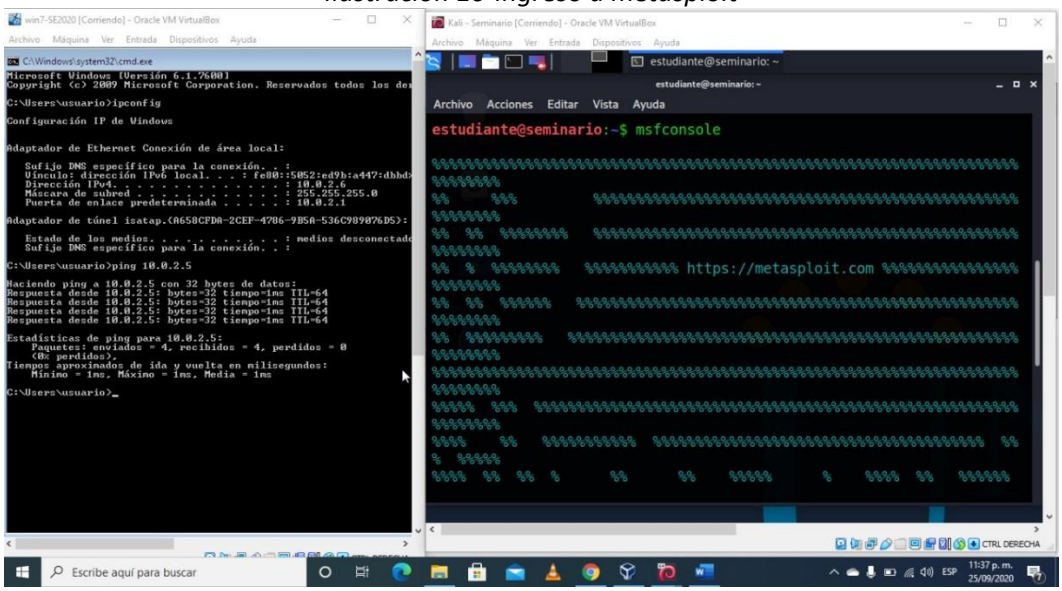
Ilustración 15-ping maquina win7 x 86



Fuente: Nilda Becerra

Con el comando msfconsole se ingresa al metasploit

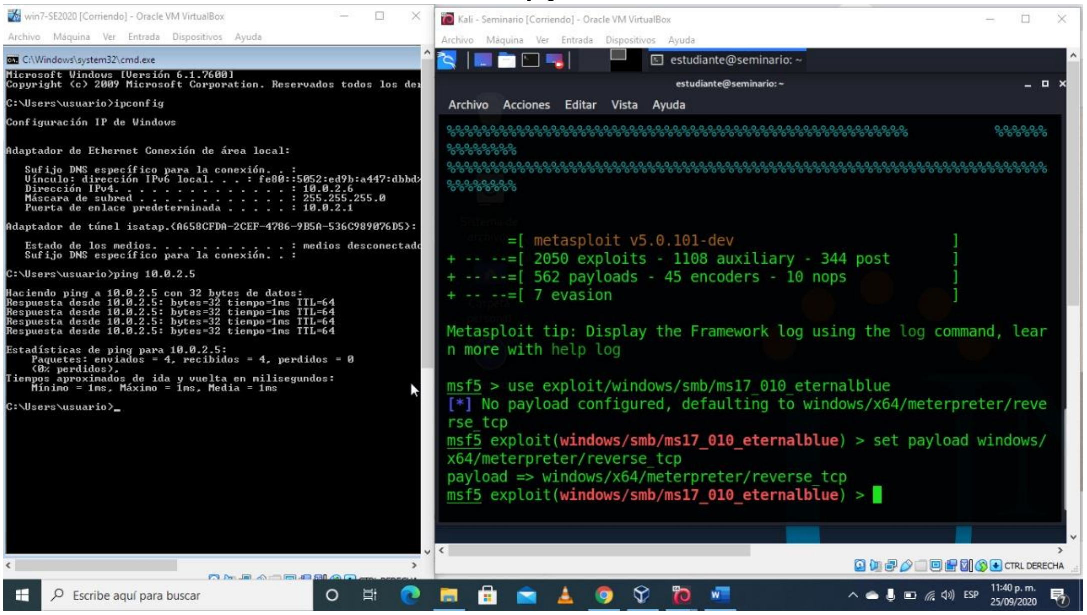
Ilustración 16-Ingreso a metasploit



Fuente: Nilda Becerra

En este lapso se utiliza los mismos comandos del anterior (fremwork y el payload), y luego procedemos a configurar la ip victima con rhost 10.0.2.6

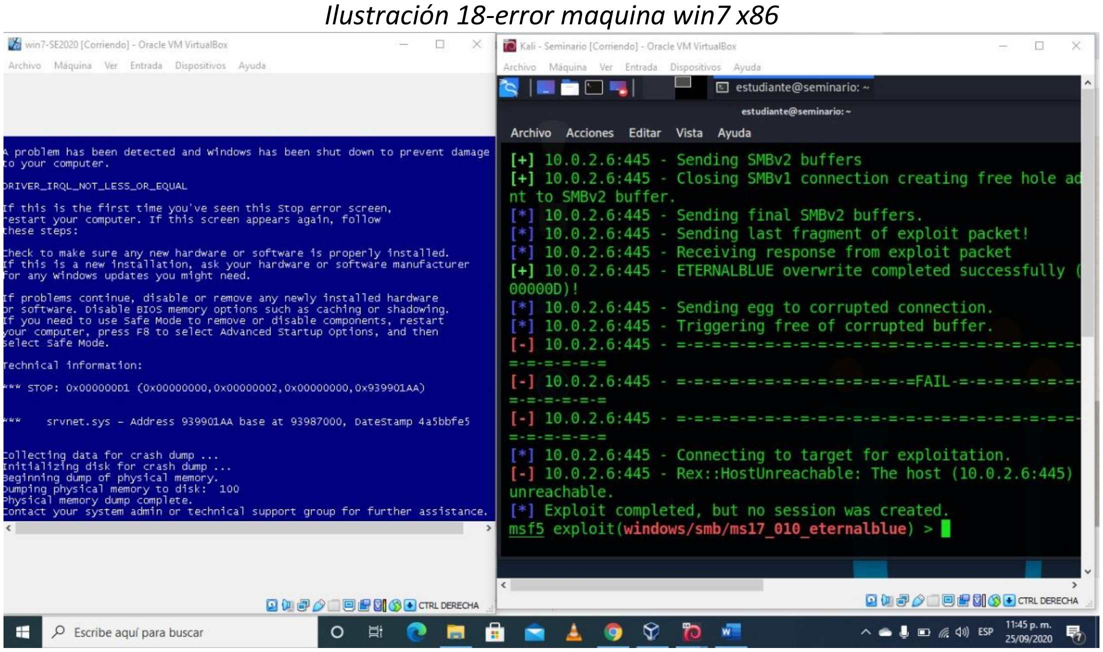
Ilustración 17-Configuración IP víctima



Fuente: Nilda Becerra

De acuerdo a la configuración anterior arroja el siguiente error.

Ilustración 18-error maquina win7 x86



Fuente: Nilda Becerra

En la segunda maquina win 7 x32 bits, arroja pantalla azul, motivo por la cual el exploit inicialmente funciona para un sistema operativo win 7 x64 bits.

Esta etapa se concluye con los soportes de las pruebas de ejecución correspondiente a la fase 3, donde se aborda las fases que tiene un pentesting[9], basado en un caso de estudio con la finalidad de identificar posibles vulnerabilidades al que se encuentra un sistema en el ámbito real.

Contención de Ataques Informáticos

El equipo Blueteam como la seguridad defensiva, aquel equipo que defiende a las organizaciones de ataques de manera proactiva. (UNIR, 2020)
Con base a lo anterior podemos definirlo como un equipo de profesionales en ciberseguridad con la capacidad de ayudar a prevenir e identificar riesgos a partir de las detecciones tempranas de las vulnerabilidades existentes en una organización, los cuales llevan el control del sistema a través de análisis e identificación de comportamientos maliciosos en pro de mejorar los controles de seguridad de una organización.

SIEM (Security Information and Event Management), solución dedicada y capaz de detectar, responder y neutralizar las amenazas informáticas. Su objetivo principal es proporcionar una visión global de la seguridad de las tecnologías de la información". (Pachon, 2020). Esta herramienta también nos facilita a la identificación de vulnerabilidades y gestión de controlar la acción del delincuente.

"La revista Owas define un Equipo de Respuesta a Incidentes (ERI) provee servicios y da soporte para prevenir, gestionar y responder ante los incidentes de Seguridad de la información*"* (OWAS, s.f.).
Al igual que el equipo BluTeam, también son equipos de profesionales con experiencias en el campo de resolución de problemas en el campo de seguridad, los cuales lo conforman de acuerdo a la experiencia y profesión, como desarrolladores, auditores, consultorías en equipo de seguridad, entre otros, de gran importancia para la conformación del equipo de respuestas a incidentes de seguridad, todos trabajan en conjunto, cooperan para brindar una solución a la organización, este equipo desarrolla medidas de prevención y reactivos que ayudan a controlar y minimizar cualquier tipo de daño que se pueda presentar.

---

[9] Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. Recuperado de: https://repository.unad.edu.co/handle/10596/35497

La contención se basa en contener una determinada actividad para evitar su propagación, en este caso nos basados en campo informático, los cuales nos ayudan a prevenir perdidas de datos, información y también daños materiales, las cuales se pueden llevar a cabo con estragáis, hardware y Software que ayuden la detención de un incidente.

Una de las herramientas identificadas a nivel general en la contención de ataques son; Backus de información, ISO o imágenes de los servidores, una buena implementación de los firewall, existen herramientas automatizadas como los son Cisco FireSIGHT y Cisco FirePOWER[10] que se encargan de la detección precoz y contención de amenazas en rede de organizaciones, **Cisco FireSIGHT se encarga "**escanea la actividad de la red con sensores cuya inteligencia es actualizada constantemente con las últimas alertas. Estos sensores buscan en los sistemas corporativos código malicioso o prohibido por las políticas de seguridad. También monitorizan las conexiones de usuarios y dispositivos para detectar si se conectan a dominios peligrosos, como podrían ser los de una botnet" (Dacom.global, 2016). Cisco también tiene la plataforma denominada "**Contención Rápida de Amenazas de Cisco**" [11] el cual contiene una serie de controles, mecanismos, herramientas que facilitan dicha operación. También existe la herramienta "Panda Security es una empresa especializada en la creación de productos de seguridad para endpoints que son parte del portfolio de soluciones de seguridad IT de WatchGuard. Centrada inicialmente en la creación de software antivirus, la compañía ha ampliado sus objetivos expandiendo su línea de negocio hacia los servicios de ciberseguridad avanzada con tecnologías para la prevención del cibercrimen" (PandaSecurity, 2018).

[10] *Datacom.Global*. Datacom.Global. (2016) *cisco Seguridad: Detección de amenazas en las organizaciones*. Recuperado de: https://datacom.global/cisco-seguridad-deteccion-de-amenazas-en-las-organizaciones/

[11] Cisco. (2020). ebook Guía de Detección y Contención Rápida de Amenazas de Recuperado de: http://info.datacom.global/hubfs/eBooks/ebook-seguridad2.pdf

CONCLUSIONES

Los equipos Blue Team y Red Team conforman un equipo capaz de llevar soluciones estratégicas en pro de la ciberseguridad de una organización, cada uno aportando desde en un enfoque metodológico y técnico para reforzar los controles de seguridad de cualquier organización. Dentro de la seguridad informática es importante contar con equipos estratégicos que ayuden a brindar soluciones e identificar fallos a partir de técnicas de ataques como los equipos anteriormente mencionados, teniendo en cuenta que ambos desarrollan actividades independientes con diferentes propósitos pero que trabajan conjuntamente, en pro de la seguridad de la infraestructura tecnológica de cualquier organización.

Con base al caso de estudio se identificó vulnerabilidades y fallos en un sistema operativo, donde al simular ser un externo y realizar un Pentesting se identificaron las vulnerabilidades y fallos muy comunes con respecto a la seguridad de los sistemas operativos.

RECOMENDACIONES

Ante el auge del avance de las tecnologías es indispensable la seguridad de la infraestructura tecnología para evitar ser víctimas de la ciberdelincuencia, para ello es importante cumplir a cabalidad con los protocolos de seguridad establecidos por los responsables de la seguridad de TI en una organización, y entender que la seguridad parte de la responsabilidad de todos los que hacen parte de ella, los protocolos se deben verificar y actualizar de acuerdo las amenazas, riesgos, y vulnerabilidades o fallos encontrados en una infraestructura TI. Así mismo implementar técnicas desde un enfoque metodológico que ayuden a identificar de maneta temprana o en la contención de conductas delictivas en este campo de la informática.

FUENTES DOCUMENTALES

Mintic. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4) Recuperado de: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Mintic. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) Recuperado de: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

Decreto 1377 de 2013 - EVA - Función Pública. (2017. Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. Recuperado de: https://repository.unad.edu.co/handle/10596/35497

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Recuperado de: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf

Allen, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

hreat Landscape Dashboard | McAfee. (2020). from https://www.mcafee.com/enterprise/es-es/threat-center/threat-landscape-dashboard/vulnerabilities-details.cve-2017-0143.html

Rapid7. (2012). Metasploitable 2. (s. f.). Metasploit. Recuperado de: https://metasploit.help.rapid7.com/docs/metasploitable-2

UNIR. (2020). Red Team, Blue Team y Purple Team: funciones y diferencias. Recuperado de: https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/.

Pachón, C. (2020). *¿Qué es SIEM y cómo funciona? Alcance e implementación. Recuperado de:* https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/.

OWASPSpain8_secicat_equipo_de_respuestas_a_incidentes. Recuperado de: https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf

Cisco. (2020). ebook Guía de Detección y Contención Rápida de Amenazas de Recuperado de: http://info.datacom.global/hubfs/eBooks/ebook-seguridad2.pdf

Pachón, C. (2020). *¿Qué es SIEM y cómo funciona? Alcance e implementación. Recuperado de:* https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/.

OWASPSpain8_secicat_equipo_de_respuestas_a_incidentes. Recuperado de: https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. Recuperado de: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

Anexa: Video https://www.youtube.com/watch?v=ChzvagW0NJ0