CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

EDGAR FERNANDO ARAQUE OROZCO

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

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

EDGAR FERNANDO ARAQUE OROZCO

Curso: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team
Código: 202337164

M.Sc. John F. Quintero
Director de curso.

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

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

Ataque: Se refiere a la acción de acceder de manera no permitida a activos o pasivos informáticos de una persona u organización.

Auditoria de Seguridad:
Estudio técnico y administrativo de carácter independiente de las actividades acontecidas en un sistema de información con el objeto de comprobar la capacidad de control de la estructura de seguridad y los procedimientos definidos para detectar vulnerabilidades y realizar recomendaciones en los procedimientos, controles y estructuras de seguridad.

Confidencialidad:
Acto en el cual se garantiza que la información compartida solo se usara para fines específicos y solo el personal autorizado.

CVE: es el número de identificación que se le asigna a una falla común en sistemas TI, permiten que se aúnen esfuerzos grupales entre organizaciones para resolver y mejorar dichas vulnerabilidades.

Degradación:
Daño parcial o total de un activo motivado por un ataque o vulnerabilidad explotada

Evento de seguridad:
Situación en la que una vulnerabilidad se torna activa y pone en riesgo información o activos de TI.

ExploitDB: Es básicamente una base de datos de vulnerabilidades en donde en comunidad se comparten las vulnerabilidades de aplicaciones, comparten como explotarlas y sacarles provecho.

Gestión de riesgos:
Conjunto de medidas de seguridad para identificar, prevenir, controlar o reducir los riesgos informáticos.

Impacto:
Lo que causa la materialización de una amenaza.

Metasploit: Es una herramienta para auditores de seguridad y equipos red team y blue team tiene más de 1800 exploit o vulnerabilidades conocidas. Permite interactuar con Nmap y Nessus, en la cual se pueden exportar los malwares a UNIX o Windows. Tiene versión gratuita y de pago.

Proyecto de seguridad:
Programa de seguridad cuya envergadura es tal que requiere una planificación específica.

Medida de seguridad:
Procedimiento o mecanismo físico o de software que reduce el riesgo.

Nmap: herramienta que Escanea e informa qué puertos están abiertos y cerrados, se utiliza para auditorías de seguridad, puede realizar inventarios de red, planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

OpenVas: Open Vulnerability Assessment System, sistema abierto de evaluación de vulnerabilidades, corre generalmente sobre Kali Linux, y es un conjunto de herramientas que correo como un framework que tiene un conjunto de herramientas para detectar vulnerabilidades que se actualiza cada semana.

Riesgo:
Es la posibilidad de exposición a amenazas que se pueden presentar en los activos TI a una persona u organización.

Seguridad:
Capacidad de los sistemas TI de mantener los activos libres de amenazas que atenten contra la disponibilidad, autenticidad, integridad y confidencialidad de los activos de información y de los servicios de red de una organización.

Trazabilidad:
Proceso de seguimiento documentado de una situación, vulnerabilidad o riesgo.

Vulnerabilidad:
Posibilidad física, lógica o de software con la cual se pone en riesgo los activos de una persona u organización.

RESUMEN

Este trabajo muestra de manera literal un compendio de evidencias de actividades teórico practicas con las cuales se reafirmaron conocimientos adquiridos durante el desarrollo de cada una de las materias de la especialización en seguridad informática en la Universidad Nacional Abierta y a Distancia UNAD, pero también se evidencian actividades prácticas nuevas y que de manera puntual y directa nos mostró como la seguridad informática paso a ser un pilar en la vida de las personas y organizaciones de nuestra época.

Se inicia con el estudio y de manera particular repaso de la legislación específicamente de la ley 1273 de 2009 que es un la base para conocer que se puede y qué no hacer , según las leyes de nuestro país, seguidamente se procede a explicar el montaje de las máquinas virtuales que nos sirvieron como herramienta práctica para comprobar la efectividad de las actividades de RED TEAM en un ambiente controlado, luego se muestran las actividades realizadas mediante el estudio de caso de caso de un posible contrato como especialista en seguridad informática en el cual vemos ejemplos de situaciones en las que se es posible caer y que si no se sigue el código de ética de nuestra profesión como ingenieros se exponen a la pérdida no solo del título profesional sino de la libertad. En las prácticas de Red Team se realizó un procedimiento de vulneración y explotación de las vulnerabilidades que presentaban las estaciones y de manera real, se evidencio los frágiles que son los sistemas informáticos si no se protegen. seguido a esto se estudiaron y plantearon posibilidades de contención de ataques en caliente como parte del estudio de Blue Team, así como herramientas de que existen en el mercado de carácter GNU para la misma labor.

INTRODUCCIÓN

Como estrategia para optar por el título de especialista en seguridad informática en la UNAD, se plantea la posibilidad de presentar un informe técnico detallado que evidencie cada una de la actividad de tipo cognitivo y practico, desarrolladas durante el curso de seminario especializado en equipos de ciberseguridad Red Team y Blue Team. Para el desarrollo de las competencias y habilidades como parte de un equipo de ciberseguridad se basa en metodologías de ciberseguridad defensivas y ofensivas, que permiten hacer frente a incidentes informáticos en una infraestructura TI en este caso de un entorno controlado de la empresa WhiteHouse Security como parte de estrategia de estudio de caso, teniendo presente el cumplimiento de normas éticas y legales con el fin de mejorar el esquema de ciberseguridad de una organización.

1 OBJETIVOS

1.1 **OBJETIVOS GENERAL**

DESCRIBIR EL DESARROLLO DE ACTIVIDADES TEORICO PRACTICAS BASADO EN UN ESCENARIO CONTROLADO ESTABLECIDO EN EL SEMINARIO DE EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD RED TEAM Y BLUE TEAM.

1.2 **OBJETIVOS ESPECÍFICOS**

- Reconocer las actividades teórico practicas realizadas en el seminario de ciberseguridad en los equipos de Red Team y Blue Team.

- Describir las actividades teórico practicas desarrolladas en el seminario de ciberseguridad en los equipos Red Team y Blue Team.
  .

.

2 DESARROLLO DE LOS OBJETIVOS

2.1 RECONOCER LAS ACTIVIDADES TEÓRICO PRACTICAS REALIZADAS EN EL SEMINARIO DE CIBERSEGURIDAD EN LOS EQUIPOS RED TEAM Y BLUE TEAM.

El conjunto de actividades planteadas en el seminario están enmarcadas en cuatro etapas, las cuales se listan y desarrollan a continuación

2.1.1 Etapa 1: Conceptos equipos de Seguridad

En esta actividad se realiza un análisis de las leyes y jurisprudencia de nuestro país en el tema de delitos informáticos. Así mismo las herramientas de un auditor de seguridad para realizar Pentesting y algunas herramientas de ciberseguridad para realizar nuestro trabajo. Se realiza también la preparación de las máquinas virtuales para realizar las pruebas y prácticas en el curso.[1]

2.1.2 Etapa 2: Actuación ética y legal

En esta actividad se realiza un análisis de caso de un proceso de selección para un cargo de receptor en la empresa WhiteHouse Security, una empresa que realiza un documento de acuerdo, al cual le realice un análisis de posible fallas o incurrencias en delitos o faltas a la ética y la legalidad según la ley 1273 de 2009. Así mismo se evalúa de manera personal si estuviese de acuerdo con aceptar ese contrato dadas una condiciones económicas y contractuales ideales. Una evaluación de las faltas a la ética según el COPNIA y por último un punto de vista del caso" OPERACIÓN ANDROMEDA BUGGLY"

2.1.3 Etapa 3: Ejecución pruebas de intrusión

En esta actividad se realiza un ciberataque de equipo red Team, utilizando herramientas de pentesting como nmap y metaexplot de uso libre y que permiten ver y explotar vulnerabilidades desde un entorno controlado con máquinas virtuales de Windows 7 de 32 y 64 bits, así como la maquina atacante con Kali Linux, configuradas previamente para esta tarea. Se evidencia claramente las vulnerabilidades por no mantener los sistemas operativos actualizados y todo el daño que se puede hacer y recibir si no se controlan las mismas. Se realiza un paso a paso, de todo el proceso y se generan impresiones de pantalla de todo el proceso.

[1] «202337164A_780: Syllabus del curso Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team».

2.1.4 Etapa 4: Contención de ataques informáticos

En esta etapa el estudio de los modelos de contención de ciberataques según el caso planteado en el anexo de la actividad, y se plantean opciones para contener el ataque realizado por el equipo Red en la actividad anterior, seguidamente de alguna paso y herramientas para la harderización de los sistemas de la compañía y el estudio de herramientas como el CIS para los equipo blue de ciberseguridad, así mismo la exploración de las posibilidades de funcionalidad del equipo blue de programas SIEM y algunas herramientas de software hardware para la contención de ataques informáticos.

2.2 DESCRIBIR LAS ACTIVIDADES TEÓRICO PRACTICAS DESARROLLADAS EN EL SEMINARIO DE CIBERSEGURIDAD EN LOS EQUIPOS RED TEAM Y BLUE TEAM.

2.2.1 Etapa 1: Conceptos equipos de Seguridad

La actividad se desarrolló de la siguiente manera:

De individual usted deberá consultar y dar respuesta a las preguntas orientadoras

2.2.1.1 Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación "leyes, decretos" existen actualmente y las características principales de cada ley.

La Ley 1273 de 2009 tipifica la normatividad de delitos informáticos en Colombia en 10 artículos desde el 269A al 269J entre los cuales describe la obstaculización, interceptación, uso de software malicioso, violación de datos personales, suplantación, hurto y transferencia no consentida de información, así como algunas circunstancias punitivas que agravan dichos delitos.[2]

Tabla 1 Resumen delitos informáticos, características y legislación

DELITO INFORMATICO	DESCRIPCIÓN	LEY QUE LO PENALIZA
ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO	Ingresos no autorizados a sistemas de información protegidos o no protegidos	Artículo 269A de la Ley 1273 de 2009, Ley de Delitos Informáticos en Colombia
OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN	Es el ataque con el propósito de colapsar servidores y estaciones de trabajo para impedir el normal funcionamiento de los sistemas de información.	Artículo 269B de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia
INTERCEPTACIÓN DE DATOS INFORMÁTICOS	Es la interceptación de información ya sean datos o voz de comunicaciones sin una orden judicial.	Artículo 269C de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia
DAÑO INFORMÁTICO	Es la destrucción deliberada de un activo informático ya sea sistema de información, a través del borrado, alteración o modificación de código.	Artículo 269D de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia

[2] «ley 1273 del 5 de enero de 2009».

USO DE SOFTWARE MALICIOSO	Es la creación o uso de software mal intencionado ya sean virus, troyanos, etc, cuya finalidad es destruir sistemas de información o robar información de la misma.	Artículo 269E de la ley 1273 de 2009, Ley de Delitos Informáticos en Colombia.
VIOLACIÓN DE DATOS PERSONALES	Es el uso mal intencionado de información de terceros con el propósito de hacer acciones delictivas.	Artículo 269F de la ley 1273, De 2009, Ley de Delitos Informáticos en Colombia
SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES	Es la creación de páginas web fraudulentas que simulan ser originales para obtener información de los usuarios con el propósito de realizar transacciones ilegales.	Artículo 269G de la ley 1273 de 2009, Ley de Delitos informáticos en Colombia
MODIFICACION DEL SISTEMA DE RESOLUCIÓN DE NOMBRES DE DOMINIO	Consiste en la modificación del servidor de nombres de una página web, el cual el usuario cree que accede a la página web solicitada pero su IP ha sido modificada, con el fin de obtener la información del usuario.	Artículo 269G de la ley 1273 de 2009, Ley de Delitos informáticos en Colombia
HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES	Consiste en el robo de información a través del ingreso no autorizado a sistemas de información protegidos.	Artículo 269I de la ley 1273 de 2009, Ley de Delitos informáticos en Colombia.
TRANSFERENCIA NO CONSENTIDA DE ACTIVOS	Consiste en el envío de información de un tercero sin su consentimiento con el fin de realizar actividades ilícitas.	Artículo 269J de la ley 1273 de 2009, Ley de Delitos informáticos en Colombia.

Fuente: propia

El decreto 1377 de 2013 el cual establece las pautas y las responsabilidades de quienes realizan hacking ético o pruebas de penetración en las empresas que lo requieren y debe garantizar las siguientes pautas:
Recolección de datos personales se autorizan los permisos y se establecen los procedimientos para el manejo de la información y los responsables.
Autorización del Tratamiento: es la autorización para recolectar toda la información y la gestión del uso de esta con las respectivas autorizaciones.[3]

La Ley 1581 de 2012: En esta ley se describen las disposiciones de la protección de datos personales. Estas aplican a personas naturales, se autoriza el tratamiento de la información incluyendo el almacenamiento, actualización y rectificación de algún tipo de dato personal. La vemos muy aplicada en el sector bancario y comercial.[4]

[3] «DECRETO 1377 DE 2013».
[4] «Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012]».

2.2.1.2 En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del Pentesting

(OWASP) es un proyecto que ofrece un marco de referencia para llevar a cabo Pentesting alineadas con la metodología PLM ciclo de vida del producto.

Etapa antes del desarrollo: Es la fase donde se establecen las métricas con las que se medirá la efectividad de lo realizado.

Etapa Definición y el diseño: se definen los requisitos de seguridad en los cuales se tienen en cuenta mecanismos de autenticación, autorización, administración, integridad entre otros. Así mismo se define el diseño y la arquitectura del sistema, documentando en texto y en graficas los factores de seguridad de la organización.

Realizar los diagramas UML: Básicos para saber previamente si la aplicación va a funcionar, es en donde los equipos de diseño y desarrollo se sincronizan con esto se realiza el diagrama de amenazas reales para validar el sistema de posibles amenazas que conlleven a mitigar, aceptar o transferir el riesgo.

Implementación: en esta etapa se realizan las pruebas de penetración considerando los aspectos de seguridad definidos en etapa de diseño, se deben realizar pruebas adicionales en configuraciones y servicios en la infraestructura también.

Mantenimiento y operaciones: Se establece el procedimiento para realizar la evaluación periódica de los sistemas y aplicaciones, en el cual se describa las actividades de verificación después de realizar la implementación de un cambio.

En las pruebas de seguridad en este modelo se dividen en activas y pasivas, las pasivas son las que explican la lógica, las entradas y las salidas de la aplicación, es donde se recolecta la información del sistema.

Para las pruebas activas se realizan los intentos de vulneración de la aplicación, para esto OWASP propone once (9) categorías y noventa y un (91) controles.[5]

[5] «GUÍA DE PRUEBAS OWASP 2008 V3.0».

2.2.1.3 Las herramientas de ciberseguridad son de vital importancia, además, que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas: Herramientas:

• Metasploit: Es una herramienta para auditores de seguridad y equipos red team y blue team tiene más de 1800 exploit o vulnerabilidades conocidas. Permite interactuar con Nmap y Nessus, en la cual se pueden exportar los malwares a UNIX o Windows. Tiene versión gratuita y de pago.

• Nmap: herramienta que Escanea e informa qué puertos están abiertos y cerrados, se utiliza para auditorías de seguridad, puede realizar inventarios de red, planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos

• OpenVas: Open Vulnerability Assessment System, sistema abierto de evaluación de vulnerabilidades, corre generalmente sobre Kali Linux, y es un conjunto de herramientas que correo como un framework que tiene un conjunto de herramientas para detectar vulnerabilidades que se actualiza cada semana.

• ExploitDB: Es básicamente una base de datos de vulnerabilidades en donde en comunidad se comparten las vulnerabilidades de aplicaciones, comparten como explotarlas y sacarles provecho.

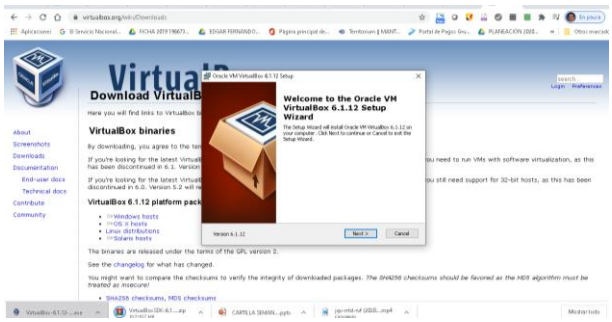
• CVE: es el número de identificación que se le asigna a una falla común en sistemas TI, permiten que se aúnen esfuerzos grupales entre organizaciones para resolver y mejorar dichas vulnerabilidades.

2.2.1.4 Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

Paso A: Descargar la herramienta virtualiza dora “VirtualBox” en su última versión.[6]

[6] Oracle VM VirtualBox ®, «Oracle VM VirtualBox ®¨».

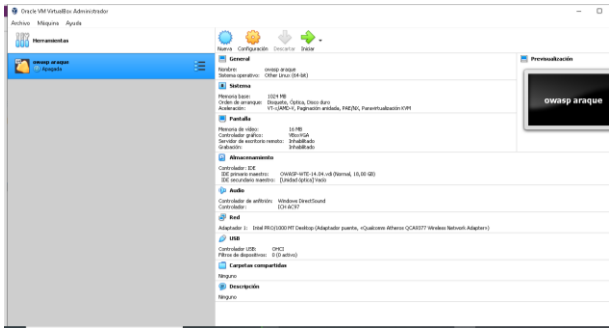
ilustración 1 Descarga de VirtualBox



Fuente: propia

En el siguiente paso se evidencia la instalación de la primera máquina virtual

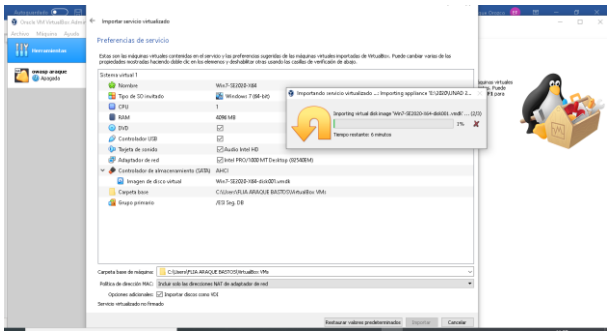
ilustración 2 VirtualBox instalado en mi maquina



Fuente: propia

Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

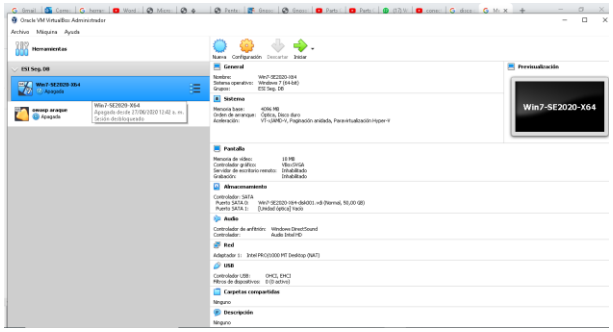
ilustración 3 Importando la máquina virtual de win7 de 64 Bits



Fuente: propia

En el siguiente paso se evidencia la instalación de la máquina virtual para 32 bits

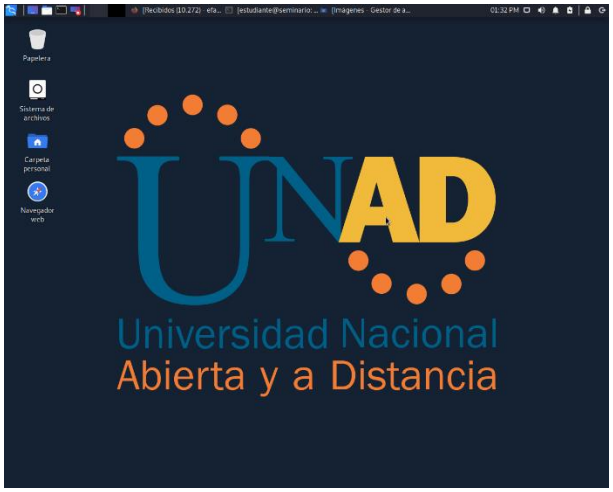
ilustración 4 Importando la máquina virtual de win7 de 32 Bits



Fuente: propia

Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda.

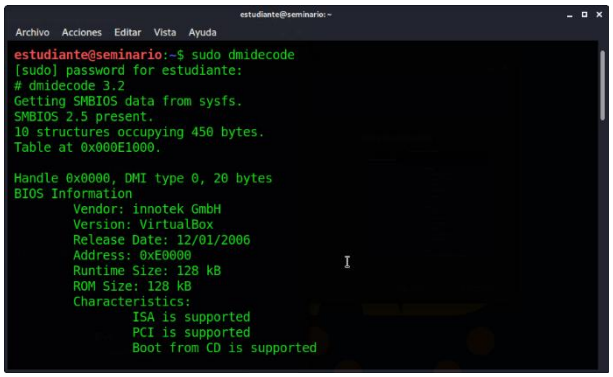
ilustración 5 Máquina Virtual de Kali con perfil de estudiante



Fuente: propia

En el siguiente paso se evidencia la identificación de la máquina virtual por consola

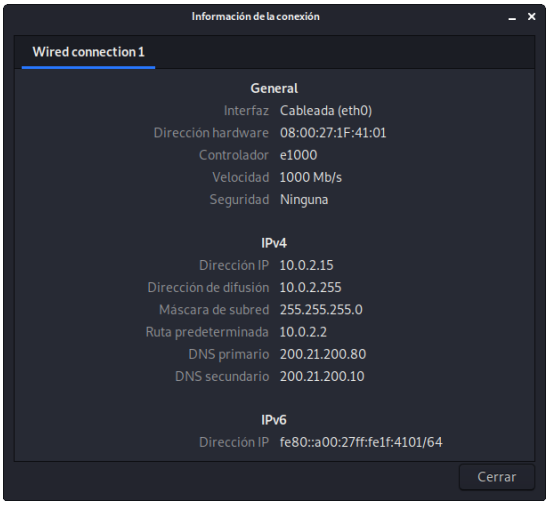
ilustración 6 Identificación de la máquina virtual por consola



Fuente: propia

En el siguiente paso se evidencia la verificación de la ip de la máquina de Kali linux

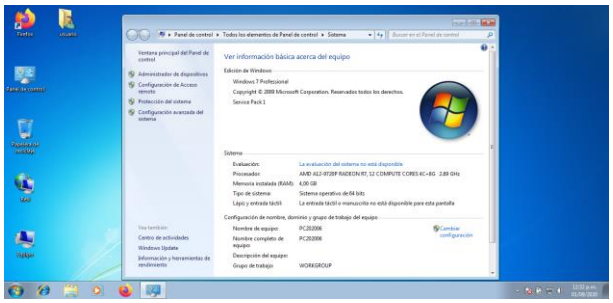
ilustración 7 Ip de Kali



Fuente: propia

En el siguiente paso se evidencian las características de la máquina virtual Windows 7 de 64 bits.

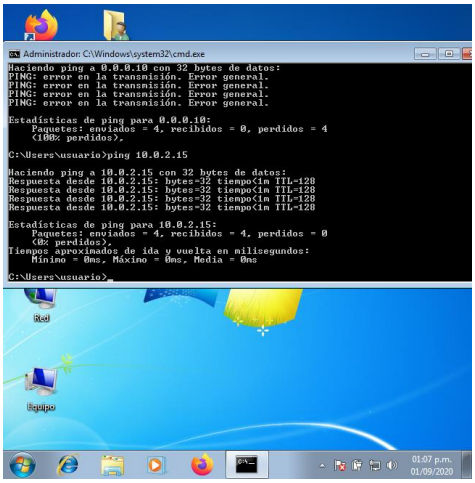
ilustración 8 Máquina virtual de Windows 7 de 64 bits



Fuente: propia

En el siguiente paso se evidencian las características de red de la máquina virtual Windows 7 de 64 bits.

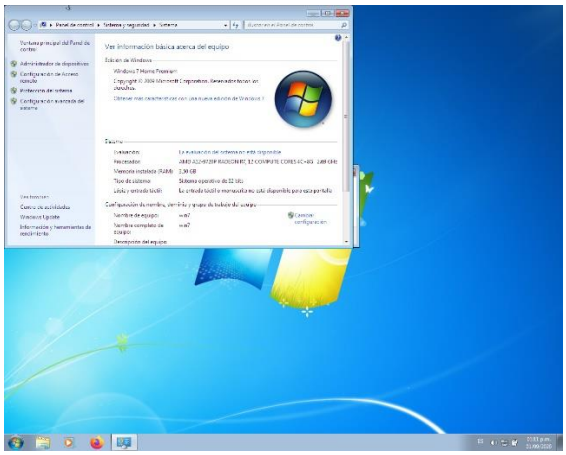
ilustración 9 Comunicación de Máquina virtual de Windows 7 de 64 bits a máquina virtual de Kali



Fuente: propia

En el siguiente paso se evidencian las características de la máquina virtual Windows 7 de 32 bits.

ilustración 10 Máquina virtual de Windows 7 de 32 bits

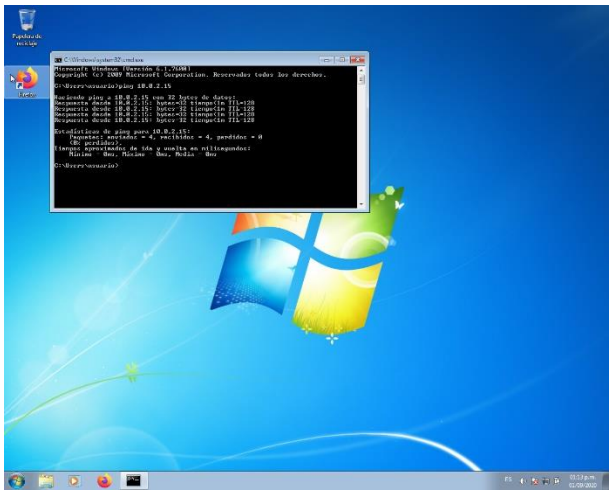


Fuente: propia

En el siguiente paso se evidencian las características de red de la máquina virtual Windows 7 de 32 bits.

.

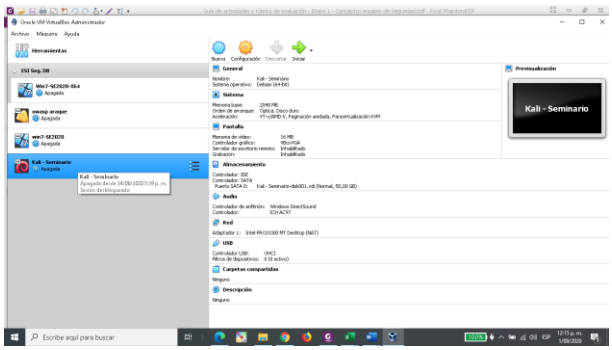
ilustración 11 Comunicación de Máquina virtual de Windows 7 de 32 bits a máquina virtual de Kali



Fuente: propia

Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”

ilustración 12 Banco de trabajo



Fuente: propia

2.2.2 Etapa 2: Actuación ética y legal

Esta actividad de tipo teórica y de análisis se desarrolló de la siguiente manera:

2.2.3 De manera individual usted deberá leer el problema que se encuentra en el anexo 2 – Escenario 2, además deberá leer y analizar el anexo 3 – Acuerdo para generar la solución a las siguientes preguntas orientadoras

2.2.3.1 ¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Con respecto al anexo2.
Como primera medida, se evidencia que la gerencia de la organización WhiteHouse Security, no realiza un análisis exhaustivo del personal que va a trabajar para ellos y por el contrario solo hace recomendaciones y deja un contrato sin revisar de una persona que ya no trabaja para ellos en una labor tan delicada como la información de otras personas y compañías que contratan sus servicios. En mi criterio la empresa puede estar incurriendo sin preverlo en delitos informáticos al interior de su organización, por el simple hecho de dejar una labor tan delicada como el conocimiento y validación de la información del personal contratado está dejando vulnerable la información de terceros.
Así mismo me parece que es inapropiado “aprovecharse “ y soltar la información de una empresa en un proceso selección en donde son se tiene ningún vínculo laboral

definido aún con quien va a realizar un proceso tan delicado como el del manejo de la información de terceros a nombre de la empresa WhiteHouse Security
Con respecto al anexo 3.
Las consideraciones del contrato:
1. Que la información compartida en virtud del presente acuerdo pertenece a Whitehouse Security, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del proceso de selección de personal
2. Que la información de propiedad de Whitehouse Security Whitehouse Security ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

2.2.3.2 Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal, EDGAR FERNANDO ARAQUE OROZCO que para el presente caso actúa como revelador, guarda y administrador de la información de propiedad de Whitehouse Security.

Está delimitando el manejo de la información. Se ampara en protección de la propiedad industrial en Colombia que está regulada con la Decisión 486 de 2000 de la Comunidad Andina de Naciones, que consagra el "Régimen Común sobre Propiedad Industrial".
Las Cláusulas del acuerdo:
En la cláusula Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.

Me genera duda que en un contrato uno pueda estar de acuerdo en ocultar información de procesos ilegales de una empresa. Me parece un hecho no ético firmar estar de acuerdo con esta cláusula.

En la cláusula Cuarta. Obligaciones de la parte receptora, en el ítem 3 y 4:

3. *No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.*

4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

Esto debería estar soportado y aclarado en el inicio del contrato que la empresa Whitehouse Security, procederá en donde acontezca realizar dichas denuncias y publicaciones como empresa y no de manera particular.

En el ítem 8 de esta cláusula:

Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento.

La empresa aclara que, en caso de ser encontrado con información ilegal o delictiva, responde personalmente el receptor, el cual está oficiando en nombre de Whitehouse Security, lo cual no es ético. Así mismo en la cláusula octava Solución de controversias: Las partes (nombre estudiante – nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security. Lo que deja claro aún más todas las responsabilidades recaen de manera particular en el receptor lo cual sigue sin ser ético.

En la Clausula 5ta Quinta.
Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:
1. Mantener la reserva de la información confidencial hasta tanto…. queda inconcluso y no tiene argumentos concluyentes.
En la cláusula Décima.
Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente Acuerdo y por tanto manifiestan estar conformes y aceptan todas las condiciones.
Se presenta la posibilidad para aceptar participar en un proceso de selección el cual a su vez es un contrato que a todas luces está responsabilizando de cualquier situación adversa a el aceptante del acuerdo, sin ser este aun empleado, lo cual no me parece de ningún modo legal y mucho menos ni ético.

2.2.3.3 Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 - Acuerdo deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

Lo primero es dejar claro que se evidencia explotación laboral por parte de la empresa Whitehouse Security pues en nuestro país para elaborar este tipo de contratos o actividades se deben establecer responsabilidades contractuales y extracontractuales, las cuales están siendo delegadas directamente sobre el aspirante al cargo, el cual no tiene ningún tipo de vinculación, pero si todo tipo de responsabilidades sobre lo que va a realizar.

En la cláusula Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados.

En la cláusula Cuarta. Obligaciones de la parte receptora, en el ítem 3 y 4:

3. No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

4. Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

En mi concepto si se habla de no divulgar procesos ilegales dentro de la empresa Whitehouse Security se puede estar incurriendo y aceptando cualquier delito informático que este tipificado en la ley1273 de 2009 pero particularmente las más asequibles por el tipo de actividad serian:
El delito de Acceso abusivo a un sistema informático. Que está tipificado den el artículo 269A de la ley 1273 que reza “El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo”[7]. Se presta para realizar acciones delictivas, consentidas en el acuerdo con la empresa Whitehouse Security.
Así mismo pudiese está violando el articulo 269C al poder estar realizando interceptaciones ilegales y no denunciarlas, por un acuerdo de confidencialidad que acepta procesos ilegales en la empresa Whitehouse Security
Pudiese incurrir en el delito de Violación de datos personales tipificado el articulo 269F, que le permitiría violar los datos personales de terceros para conseguir los fines de la empresa Whitehouse Security

[7] «ley 1273 del 5 de enero de 2009».

En la Clausula 5ta Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora: Mantener la reserva de la información confidencial hasta tanto….

Al quedar inconclusa la cláusula queda abierta a que se pueda inferir cualquier situación que se quiera y haberla aceptado. Permitiendo con esto poder realizar acciones que estén en contra de la ley 1273 de 2009 por no haberlas definido de manera clara.

2.2.3.4 ¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿usted cómo experto en ciberseguridad aplicaría a este trabajo en The WhiteHouse, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio?

Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros. "**NO APLICARIA**"

Motivos:
1 Al actuar y permitir actuaciones ilegales seria participe de los mismos y por tanto corresponsable, aunque las cláusulas en el acuerdo hablan claramente de que estaría por cuenta propia.
2 Ese tipo de empresas no duran mucho.
3 No arriesgaría mi carrera profesional por algo que permite lo ilegal.
Sustento con el código de ética del COPNIA.
El inciso b del artículo 31. deberes generales de los profesionales del Código de ética para ingenieros del COPNIA, reza: Custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados[8]; claramente estaría violando este principio, que resultaría en la cancelación de mi matricula profesional y el fin de mi carrera como ingeniero.
Así mismo el inciso F que reza: Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder; teniendo en cuenta que una de las cláusulas dice que no podría denunciar actos ilegales dentro dela empresa, estaría violando es inciso.

[8] «Código de ética para ingenieros».

El artículo 32. De prohibiciones generales a los profesionales. Estaría violando el inciso b, que reza Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley;

En el artículo 34. prohibiciones especiales a los profesionales respecto de la sociedad. Estaría violando del inciso a, que reza:) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación;

En el artículo 40. prohibiciones a los profesionales respecto de sus clientes y el público en general. Estaría violando el inciso a) Ofrecer la prestación de servicios cuyo objeto, por cualquier razón de orden técnico, jurídico, reglamentario, económico o social, sea de dudoso o imposible cumplimiento, o los que, por circunstancias de idoneidad personal, no pudiere satisfacer;

2.2.3.5 Deberá buscar la noticia del caso “OPERACIÓN ANDROMEDA BUGGLY” en la ciudad de Bogotá, y redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar

Al ver este tipo de noticias y recordar el código de ética como ingeniero y los delitos informáticos que se pueden cometer al aceptar o consentir acuerdos si analizar bien la situación, se observa que en este caso muchos profesionales del área cayeron de manera desprevenida y pudieron ser utilizados para fines particulares sean del estado o de privados para demostrar sus capacidades.
Claramente fue una estrategia de cazar talentos muy atractiva que dio sus frutos y estos produjeron resultados tangibles para unos y otros. Desafortunadamente la estrategia estaba enfocada en realizar una selección de personal capacitado y apto para fines con oscuros intereses y conllevo a cometer delitos informáticos y esto afecto la reputación de muchos de quienes trabajamos en esta área. Pero en mi labor soy consciente que las comunidades de desarrolladores como OWASP, Kali Linux entre muchas, producen muy buenos resultados y aportan al mejoramiento de las funciones que realizamos.
La ingenuidad y desconocimiento legal y ético de muchos ingenieros dedicados a la seguridad informática, en esa época, permitieron que grupos de delincuentes con fines económicos y de poder se aprovechan de esto y difamaran en parte la labor.
Actualmente y gracias programas de educación como el que cursamos y a ejercicios como el que estoamos realizando nos ponen sobre aviso y nos permiten ir un paso adelante para no caer en manos de explotadores que solo les importan sus fines.[9]

[9] «Detrás de Buggly: la historia de la fachada Andrómeda • ENTER.CO».

2.2.4 Etapa 3: Ejecución pruebas de intrusión

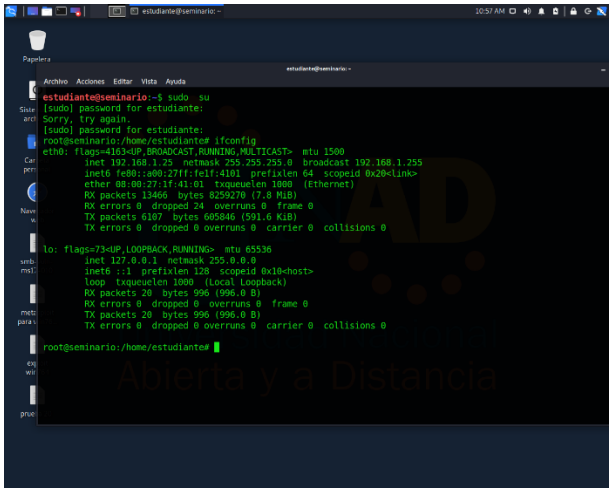
Esta actividad de tipo practico y analítico se desarrolló de la siguiente manera:

De manera individual usted deberá leer el problema que se encuentra en el anexo 4 – escenario 3 referente a equipo Redteam y por medio del banco de trabajo configurado previamente deberá dar respuesta a las siguientes preguntas orientadoras:

2.2.4.1 Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Red Team. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un Pentesting.

Según la recomendación de correo deje la configuración de red NAT, pero al validar, no me dio las conexiones de red, lo que me obligo a cambiar el adaptador de red en las máquinas de cada sistema operativo y validar nuevamente las direcciones ip quedando de con las direcciones: 192.168.1.25, para el equipo de Kali Linux.

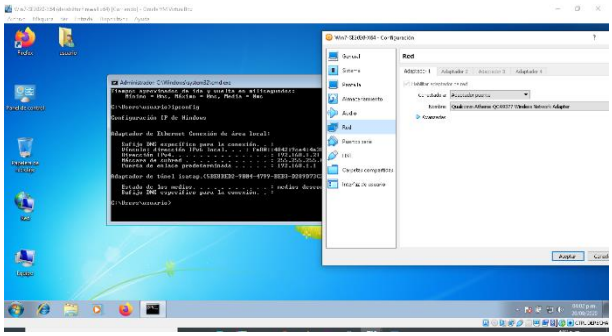
ilustración 13 Ajuste de las configuraciones red de la máquina de Kali Linux



Fuente: propia

Así mismo se realizó para las máquinas de Windows 7 de 64 bits: 192.168.1.21

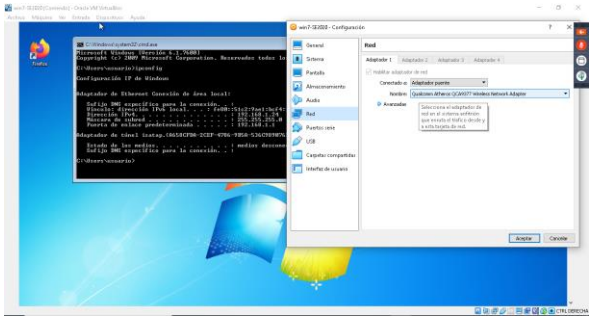
ilustración 14 Ajuste de las configuraciones red de la máquina de Win 7 64 Bits



Fuente: propia

Así mismo se realizó para las máquinas de Windows 7 de 32 bits: 191.168.1.24

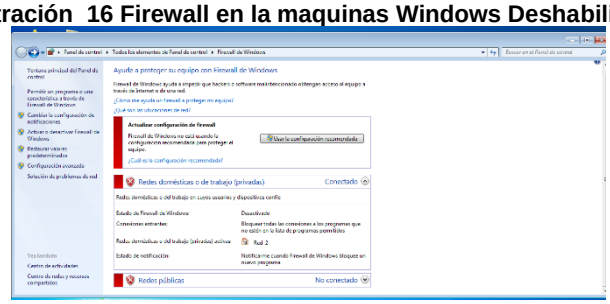
ilustración 15 Ajuste de las configuraciones red de la máquina de Win 7 32 Bits



Fuente: propia

Luego de esto se validó el estado del firewall en la maquinas Windows:

ilustración 16 Firewall en la maquinas Windows Deshabilitado



Fuente: propia

Teniendo esto listo procedí a seguir los pasos del Pentesting para el punto 1 de la actividad:

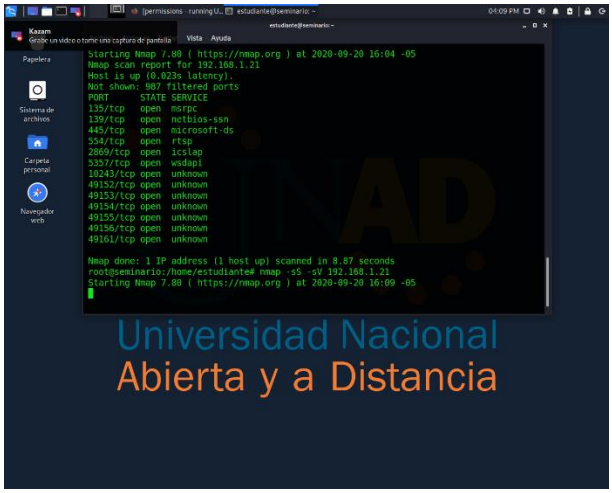
Fase de recolección de información:
Según el anexo 4, Los equipos que posiblemente fueron víctimas cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Nos indican que los equipos estaban desactualizados y que su última actualización fue en febrero de 2017 y que la posible falla de seguridad puede estar relacionado con el identificador CVE-2017-0144, así mismo nos dice que no tienen instalada la actualización MS17-010.

Fase de búsqueda de vulnerabilidades:
La herramienta que utilice para realizar el Pentesting fue:

NMAP: esta herramienta me permitió escanear e informa qué puertos están abiertos y cerrados, se utiliza para auditorías de seguridad, puede realizar inventarios de red, planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

Existen algunos scripts ya diseñados para escanear vulnerabilidades, que permiten de manera específica correrlo para ejecutar los escaneos de vulnerabilidades específicas. En este caso corrimos la citada por nmap en su página web https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html. En este caso para la vulnerabilidad ms17-010. Se puede descargar en Kali desde https://svn.nmap.org/nmap/scripts/smb-vuln-ms17-010.nse y ejecutar como se realizó en este caso.
Lo primero que realice fue la validación de la ip, y luego la búsqueda de la vulnerabilidad, Como no fue muy especifica la respuesta procedí a realizar una búsqueda más detallada en donde evidencio el puerto 445 que está abierto y es utilizado en el workgrup que permite hacer lo que nos indican en el anexo 4 que manejan archivo de red e impresoras en Windows 7en este caso de 64 bits:

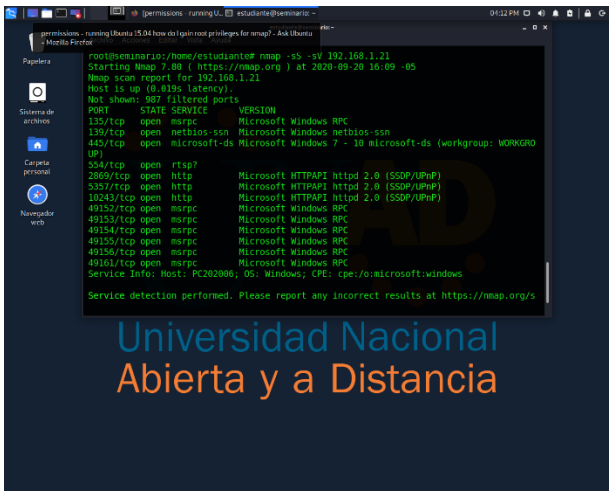
ilustración 17 Ejecución de comando Nmap



Fuente: propia

Descripción detallada de puertos y servicios arrojados por Nmap

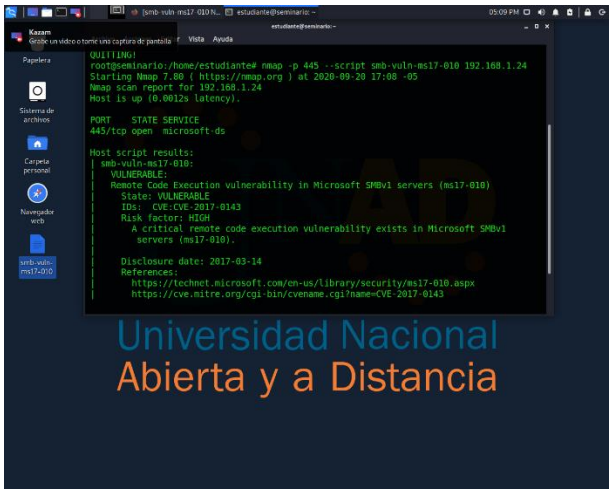
ilustración 18 búsqueda más detallada de puertos abiertos



Fuente: propia

Ahora ejecuto el script para la vulnerabilidad ms17-010 para la posible vulnerabilidad mencionada en el anexo 4, acá evidencio claramente que efectivamente el puerto 445 está abierto y la vulnerabilidad está presente en esta máquina de windows7 de 32 bits:

ilustración 19 ejecución del script para la vulnerabilidad ms17-010

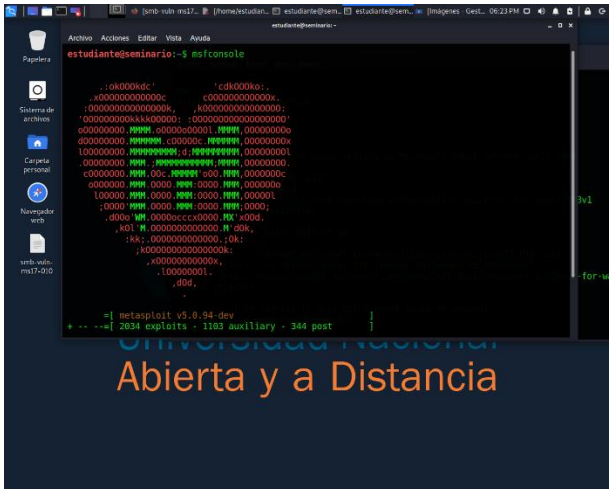


Fuente: propia

En la siguiente fase del pentesting seguiría la explotación de vulnerabilidades la cual realice haciendo una validación especifica utilizando la herramienta **Metaexploit**[10] que específicamente es una base de datos de vulnerabilidades en donde en comunidad se comparten las vulnerabilidades de aplicaciones, comparten como explotarlas y sacarles provecho.

Ejecuto el comando de cargar el Metaexploit y su base de datos msfconsole:

ilustración 20 Ejecución del comando msfconsole

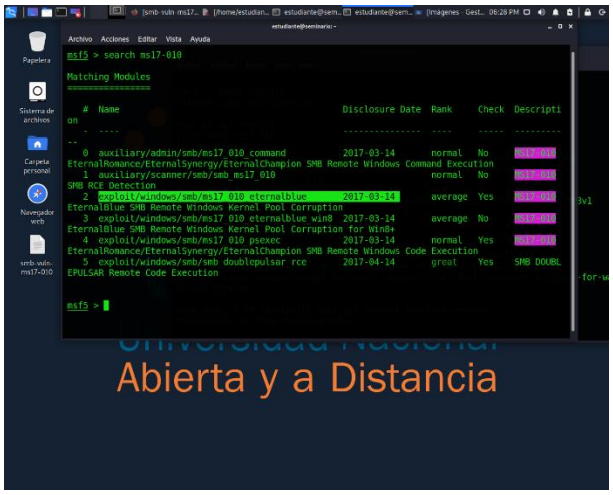


Fuente: propia

[10] «HACKING 4 BAD PENTESTERS: [STEP-BY-STEP] Eternalblue desde Metasploit - Hacking Windows 7».

Realizo la busque de la vulnerabilidad mencionada en el anexo 4, y encuentro la misma y con el exploit eternalblue, confirmando con esto que la máquina que estoy aplicando el pentesting si tiene esta vulnerabilidad, tanto en el sistema de 32bits como en el de 64bits:

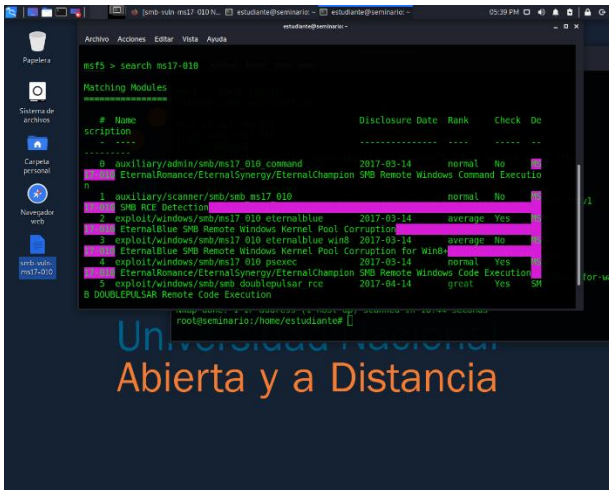
ilustración 21 Vulnerabilidad eternalblue



Fuente: propia

En el siguiente paso se evidencian las características de la vulnerabilidad eternalblue

ilustración 22 Vulnerabilidad eternalblue



Fuente: propia

2.2.4.2 A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca constantemente las dos máquinas con Windows 7 X86 y Windows 7 X64**.**

SMBv1:
Cuando en el anexo 4 nos dicen que "*Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red"* lo relacionamos al protocolo SMB, utilizado para la transmisión de datos entre maquinas Windows y Windows- Linux o viceversa. Este protocolo permite acceder y modificar de manera remota archivos y gestionar periféricos como impresoras, lo que implica puertos abiertos y posibles vulnerabilidades.

CVE-2017-0144:
Cuando en el anexo 4 nos dicen que: "*los S.O. no se encontraban actualizados, y su última actualización fue el 05 de febrero de 2017 preocupando a la organización, porque pueden estar relacionados al fallo de seguridad con identificador CVE-2017-0144"* lo relaciono con el identificador en la base de datos de vulnerabilidades que de Microsoft Windows CVE-2017-0144, el cual está relacionado con el fallo SMBv1 que se tiene en varias versiones del sistema operativo.

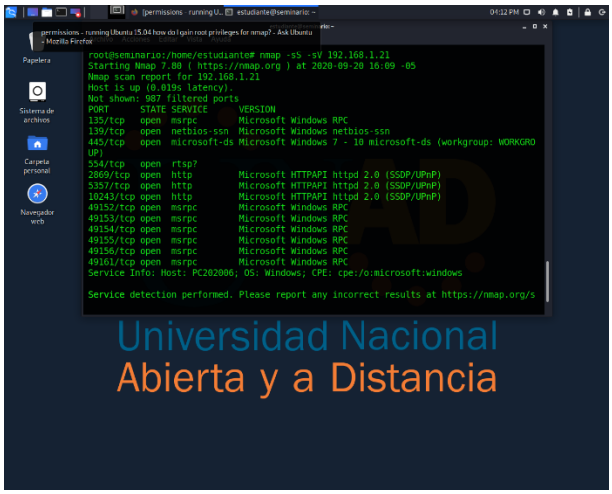
MS17-010:
Cuando en el anexo 4 nos dicen que: *"además los equipos de cómputo no tienen instalada la actualización MS17-010"*
Lo relacionamos a que no tiene instalada esta actualización de seguridad que corrige la vulnerabilidad SMBv1 y está relacionado al eternalblue, el cual es un exploit que lanza la pantalla azul en el equipo que es vulnerado. Así mismo lo relaciono con el ultimo párrafo que dice: "*validar por qué uno de esos equipos de cómputo suele mostrar pantalla azul error de windows".*

2.2.4.3 ¿Qué herramienta utilizó para poder identificar los fallos a nivel de sistema operativo "máquinas Windows 7"? incorpore en una tabla los fallos encontrados, categoría, y descripción general.

La herramienta que se utilice en este caso fue NMAP la cual me permitió escanear qué puertos están abiertos y cerrados, y cuales presentaban vulnerabilidades en las maquinas win7

En este caso utilice el comando nmap (-sS) que realiza un escaneo de mediante TCP Connect, la cual realiza una verificación completa via TCP, así mismo lo convine con un escaneo de puertos estándar, para no demorar mucho el escaneo (-sV).[11]
Luego el comando que use fue: *nmap -sS -sV192.168.1.21* para el win7 de 64 bits y *nmap -sS -sV192.168.1.24* para el win7 de 32 bits

Pantalla de ilustración 23 Tabla de fallos



Fuente: propia

2.2.4.4 Explique con sus palabras y de manera específica cómo afecta el ataque a cada una de las máquinas (Windows 7 X86 y Windows 7 X64), haga uso de gráficos para explicar el ataque.

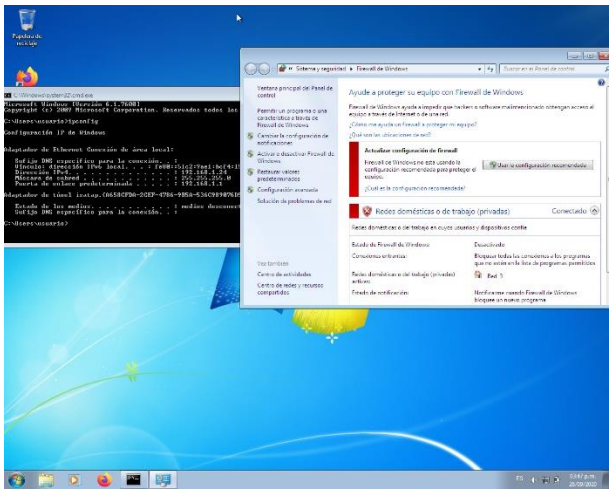
El ataque afecta directamente todo lo que se maneje en esa quina y con lo que tenga contacto a través de red o cualquier puerto de la maquina atacada en este caso win7x86 y win7x64, particularmente se pueden realizar cualquier tipo de delito informático , pues al hacer el meterpreter se tiene el dominio de la maquina en general, pudiendo desde simplemente desactivar la máquina, sacar o extraer información y hasta dañar el dispositivo comprometiendo la información contenida y los equipos que con el conecten en red.

Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en las máquinas Windows 7.

Win7X86:

[11] «smb-vuln-ms17-010 NSE Script».

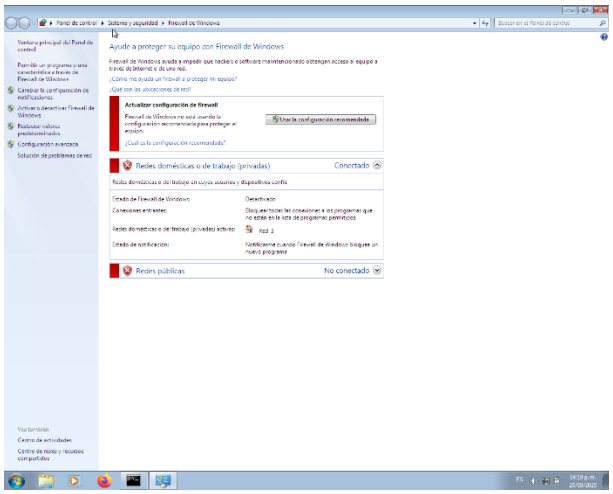
ilustración 24 Verificación de la ip de la maquina



Fuente: propia

Verificando el estado del firewall parala ejecución de las pruebas de pentesting:

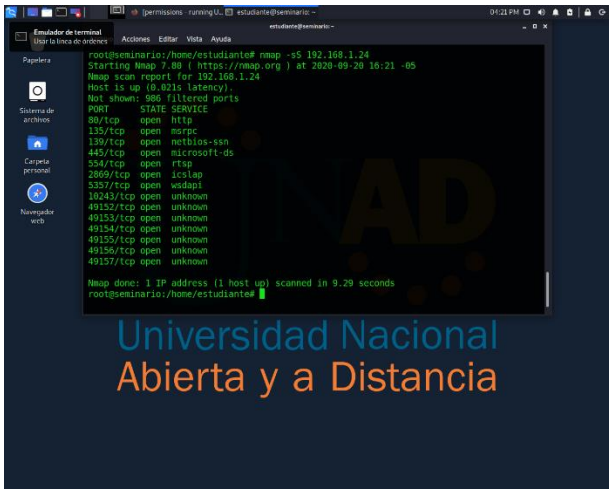
ilustración 25 verificación del estado de firewall del dispositivo



Fuente: propia

Validación de ip y puertos vulnerables con comando nmap:

ilustración 26 Validación de ip y puertos vulnerables con comando nmap



Fuente: propia

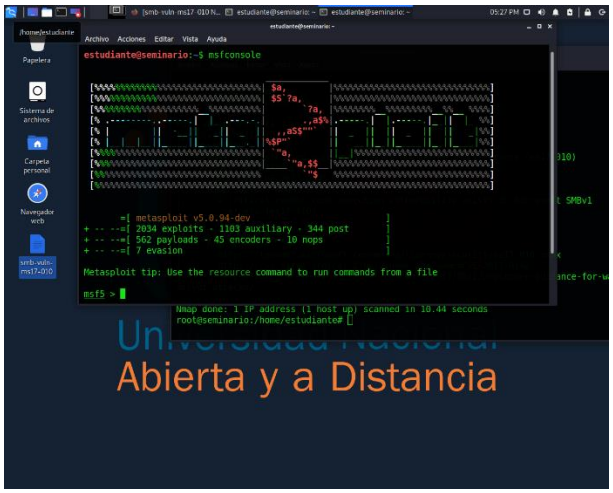
En el siguiente paso se evidencian el detalle de puertos y servicios abiertos arrojados por Nmap.

ilustración 27 Detalle de puertos y servicios abiertos

Fuente: propia

En el siguiente paso se evidencia la ejecución del metasploit:

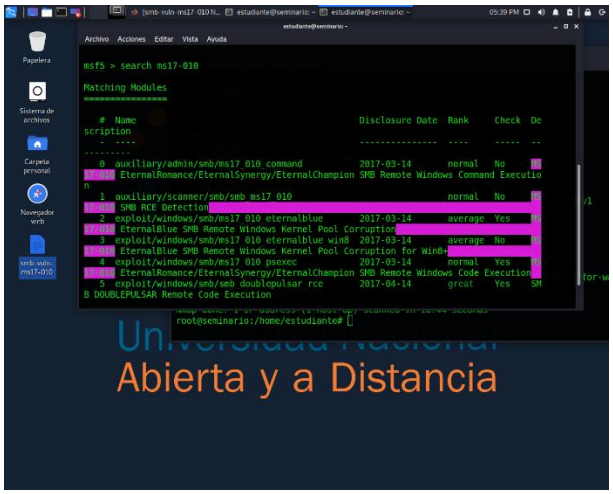
ilustración 28 Ejecución del metasploit



Fuente: propia

Búsqueda de la vulnerabilidad ms17-017

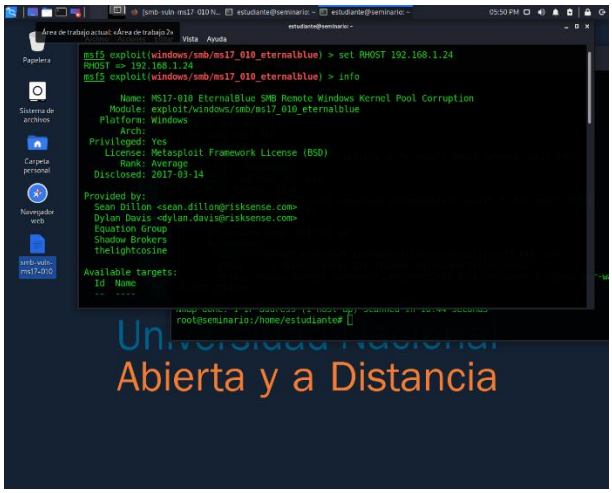
ilustración 29 visibilizando la vulnerabilidad ms17-017



Fuente: propia

Seteo del puerto remoto e información de la vulnerabilidad:

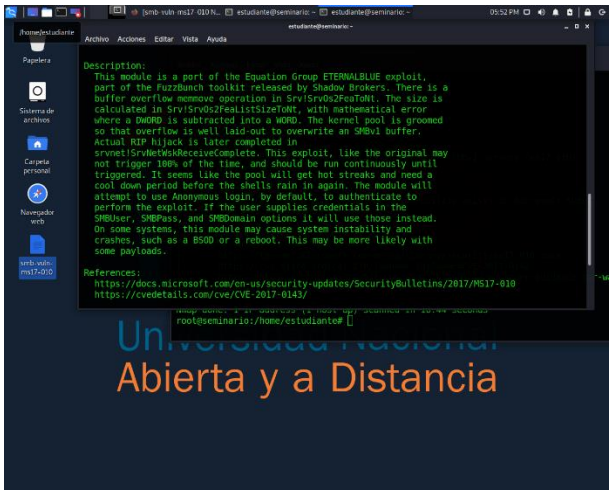
ilustración 30 Descripción detallada del eternalblue



Fuente: propia

Información de la vulnerabilidad encontrada y el desarrollador del exploit :

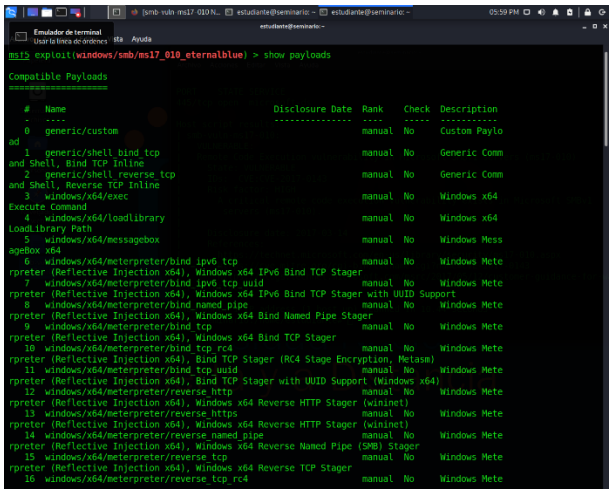
ilustración 31 Descripción detallada del eternalblue



Fuente: propia

Muestra de los payload disponibles para el exploit:

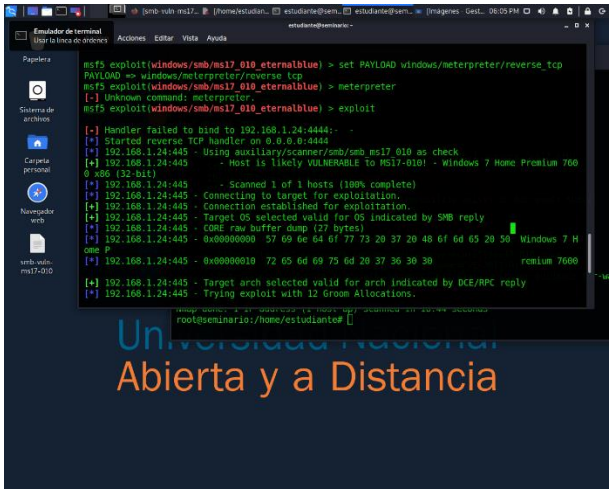
ilustración 32 Detalle de los payloads disponibles



Fuente: propia

Carga del payload meterpreter para explotar la vulnerabilidad

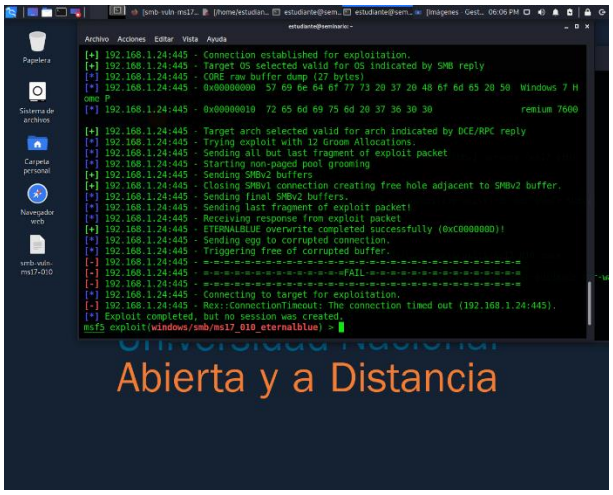
ilustración 33 Explotando el meterpreter



Fuente: propia

Resultados del exploit, en donde se evidencia que se explotó la vulnerabilidad eternalblue, pero no fue posible acceder al equipo

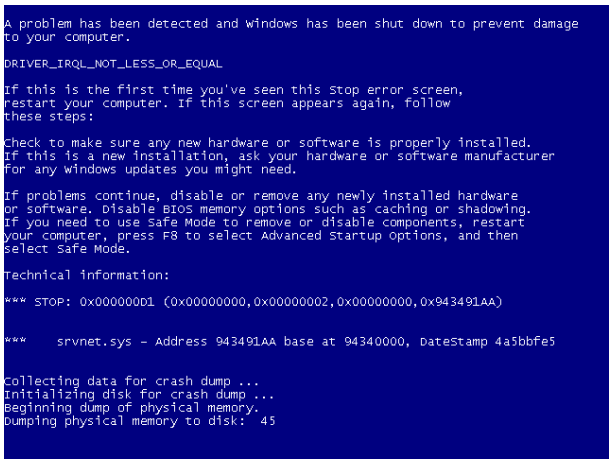
Ilustración 34 Se explota la vulnerabilidad, pero hay una falla



Fuente: propia

Motivo por el que no se pudo acceder al equipo, pantalla azul:

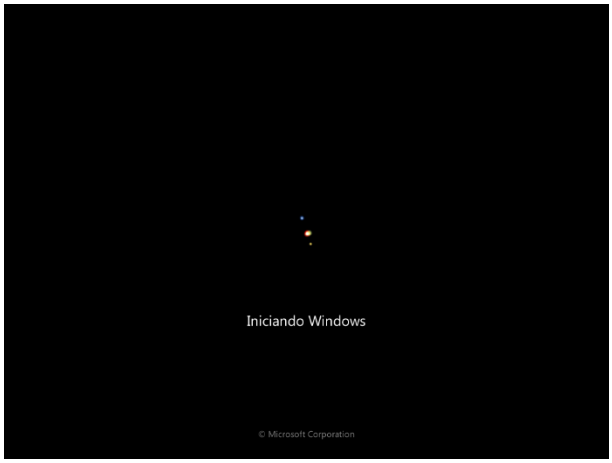
Ilustración 35 Vulnerabilidad encontrada pantalla azul



Fuente: propia

Windows reiniciando luego de ejecutar el exploit:

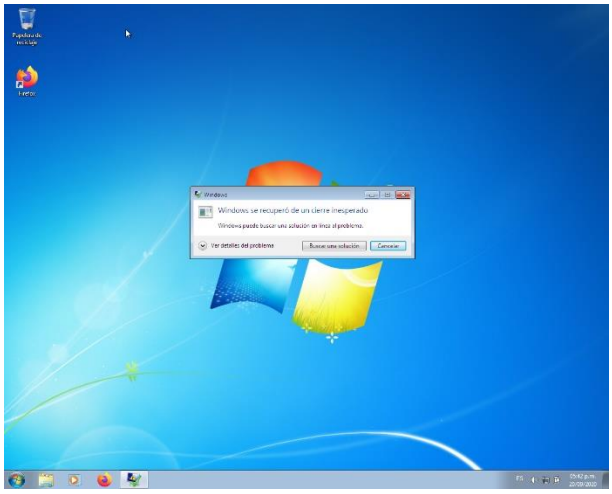
ilustración 36 Reinicio de la máquina virtual luego del ataque



Fuente: propia

Una vez el equipo se reinicio arrojo la siguiente ilustración en donde se evidencia haberse recuperado de una falla en le sistema operativo, ocasionada por el exploit.

ilustración 37 Mensaje de Windows luego del reinicio

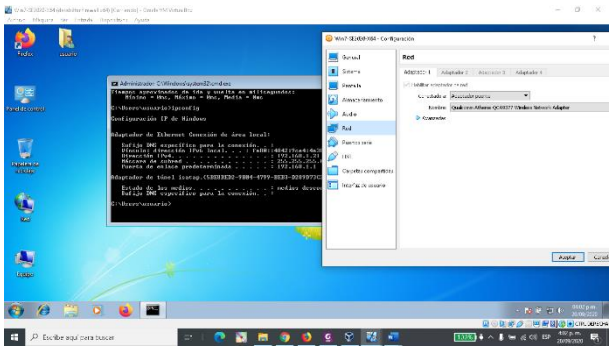


Fuente: propia

Win7x64

Ip de la máquina:

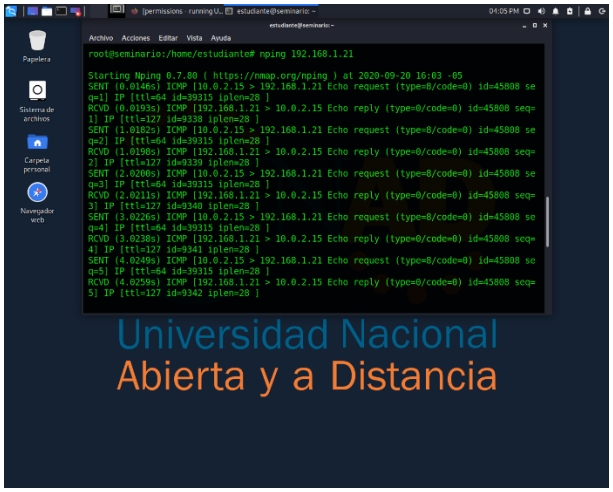
ilustración 38 Verificación de ip y protocolo de red



Fuente: propia

Nping a la ip de la maquina con sistema operativo win7 de 64 bits:

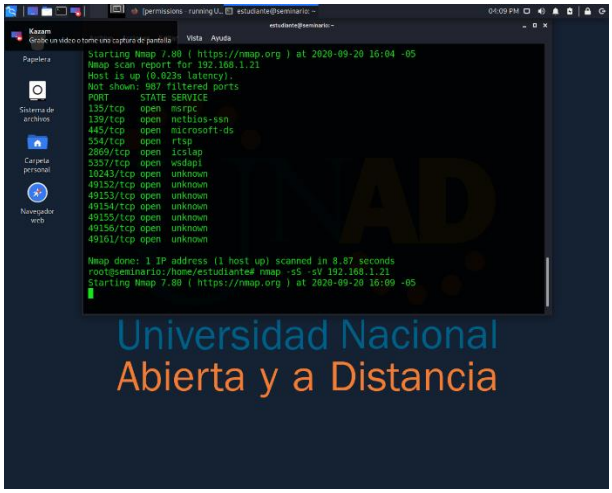
ilustración 39 verificación de que el equipo está en red



Fuente: propia

Nmap para ver puertos vulnerables de la maquina:

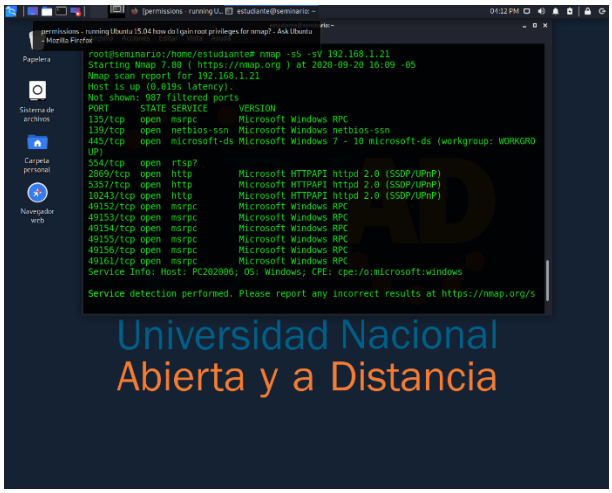
Pantalla de ilustración 40 ejecucion del nmap



Fuente: propia

Identificación de la vulnerabilidad con los puertos con nmap:

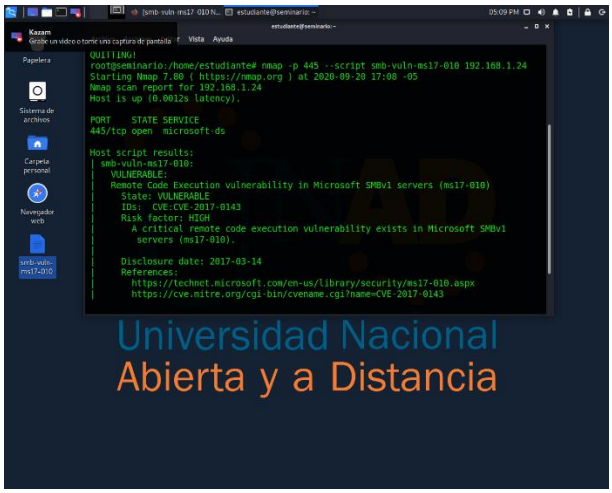
ilustración 41 Identificando puertos y servicios abiertos



Fuente: propia

Información del script de la vulnerabilidad:

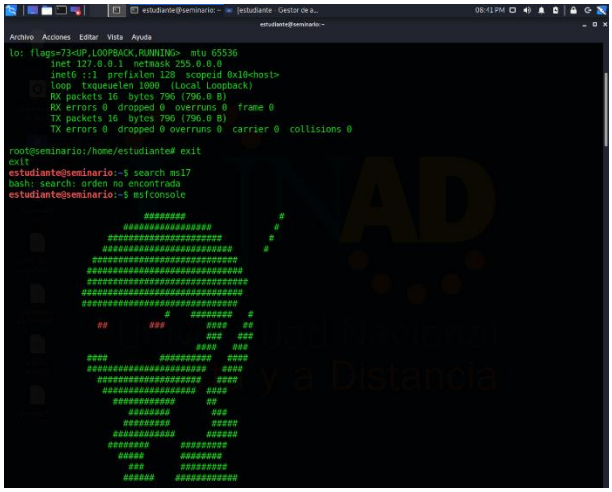
ilustración 42 información del script de la vulnerabilidad ms17-010



Fuente: propia

Ejecutando el metaesploit:

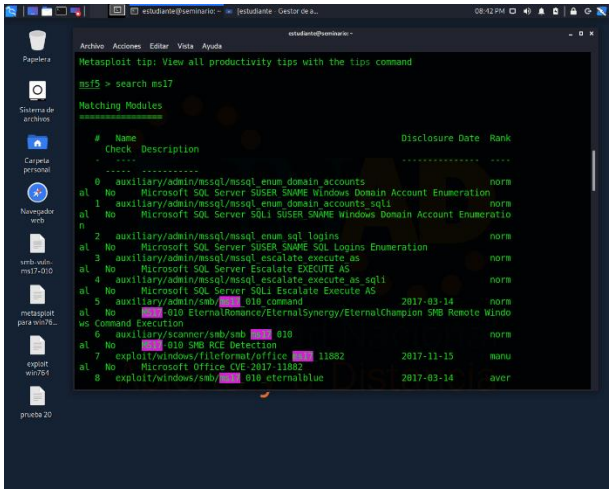
ilustración 43 información del script de la vulnerabilidad ms17-010



Fuente: propia

Búsqueda de la vulnerabilidad encontrada con el nmap:

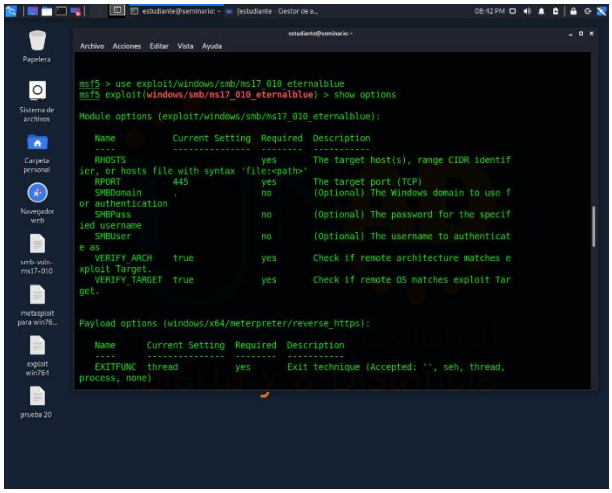
Ilustración 44 Vulnerabilidad eternalblue encontrada



Fuente: propia

Explotando la vulnerabilidad ms17-010:

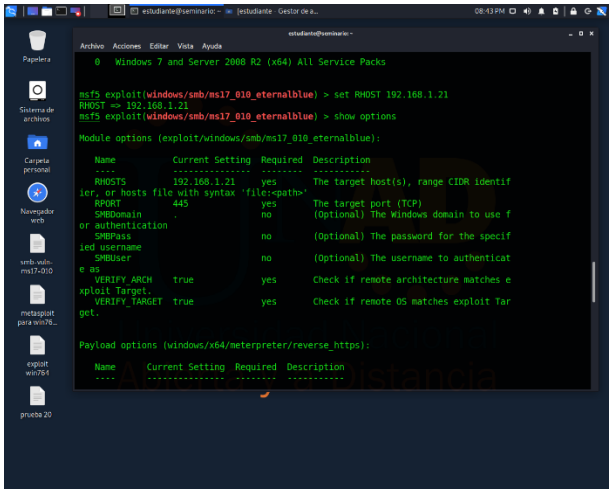
Ilustración 45 Explotando la vulnerabilidad y verificando puertos



Fuente: propia

Configurando la ip del equipo remoto en el exploit:

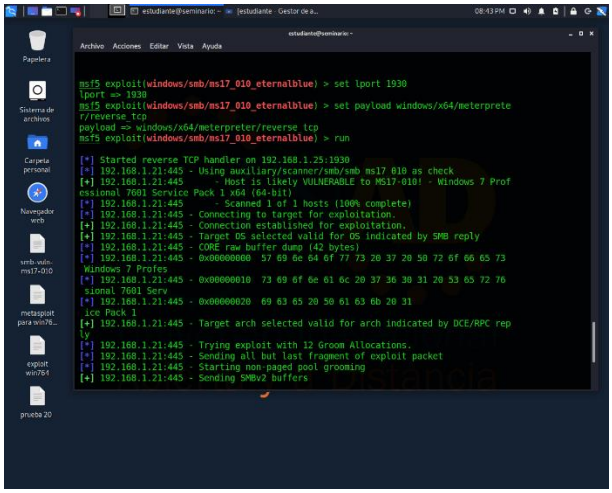
ilustración 46 Seteo de la ip del equipo remoto



Fuente: propia

Configurando el puerto del equipo remoto, cargando el payload y corriendo el exploit:

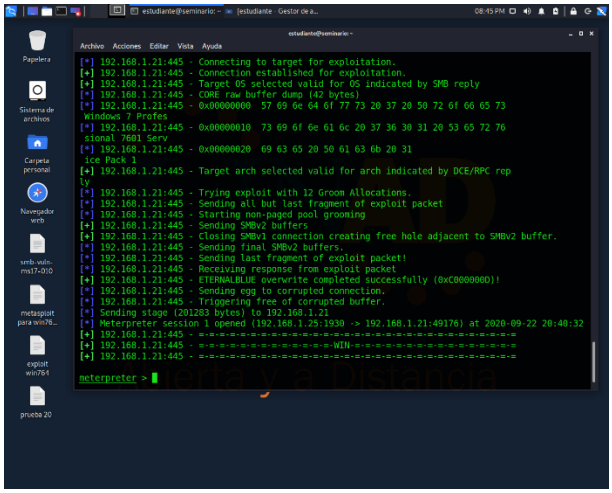
ilustración 47 Cargando el payload de meterpreter



Fuente: propia

Equipo vulnerado con exploit y utilizando el meterpreter**:**

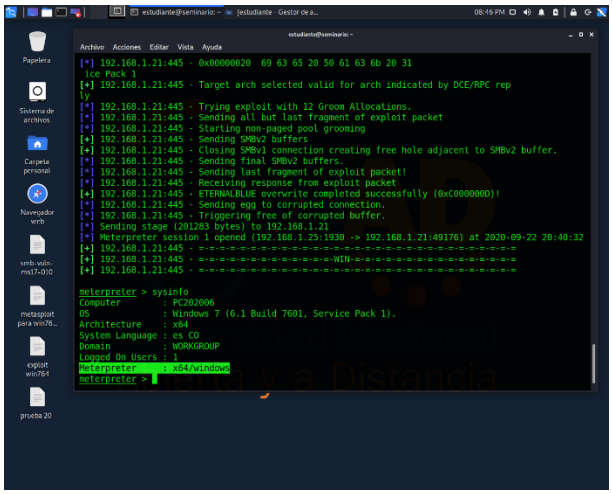
ilustración 48 evidencia de equipo vulnerado



Fuente: propia

Identificación del equipo vulnerado:

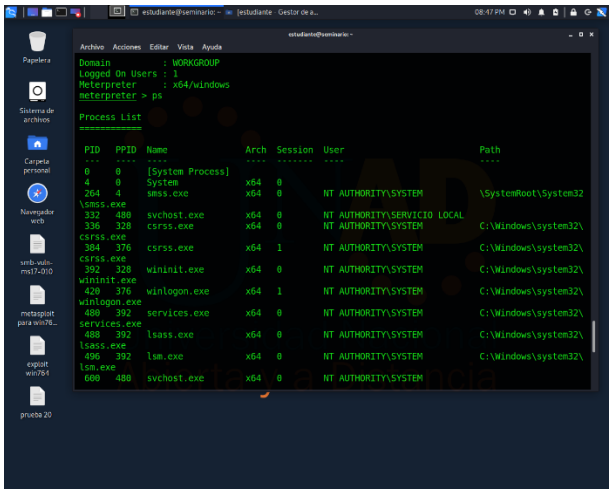
ilustración 49 datos de la maquina vulnerada remotamente



Fuente: propia

Listado de procesos en ejecución y los puertos por los que está ejecutando cada uno, de la maquina vulnerada:

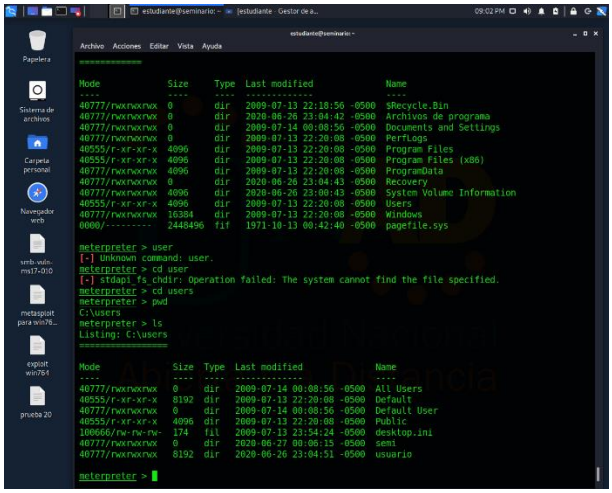
ilustración 46 procesos en ejecución de la máquina vulnerada



Fuente: propia

Búsqueda de archivos y ubicación en cada directorio, ingreso a la carpeta de usuarios:

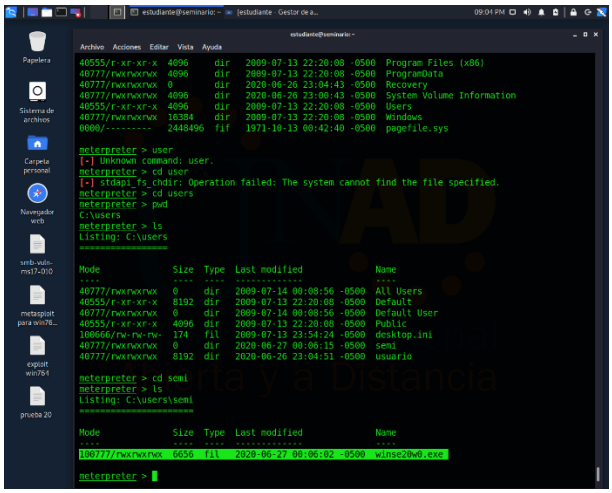
ilustración 47 navegación remota por consola de loe la máquina vulnerada



Fuente: propia

Archivo winse20w0.exe encontrado en la carpeta semi de la sesión de user:

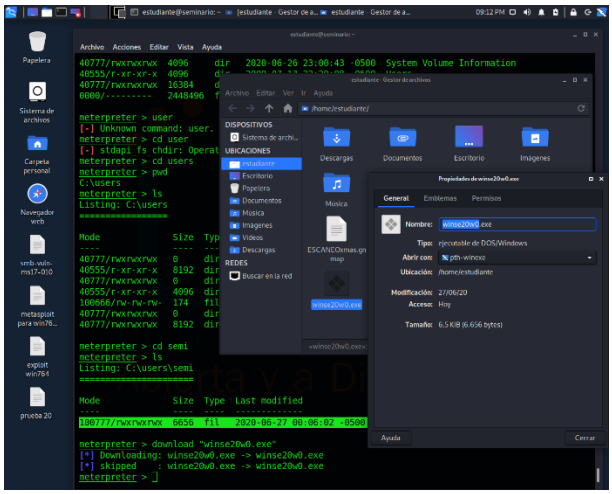
ilustración 482 archivo buscado, localizado



Fuente: propia

Descarga del archivo al equipo Kali atacante red team.

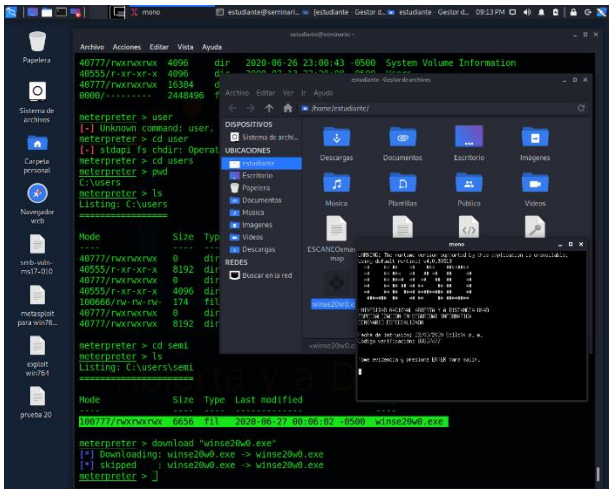
ilustración 49 Descarga del archivo buscado a la máquina de Kali



Fuente: propia

Ejecución del archivo desde Kali linux del equipo red team:

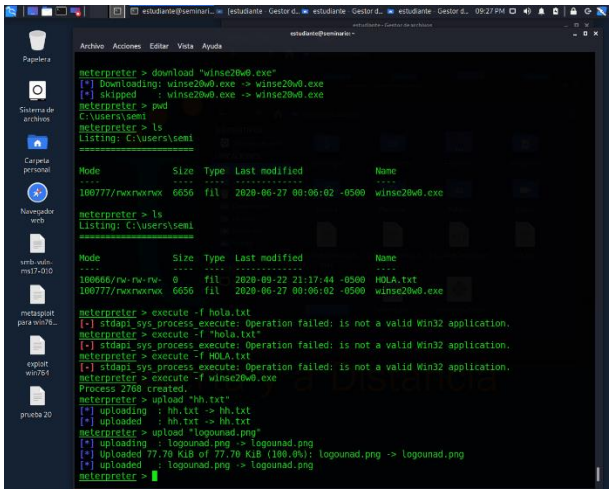
ilustración 54 Ejecución del archivo winse20w0.exe en kali Linux



Fuente: propia

Pruebas adicionales de archivos creados desde la maquina red team:

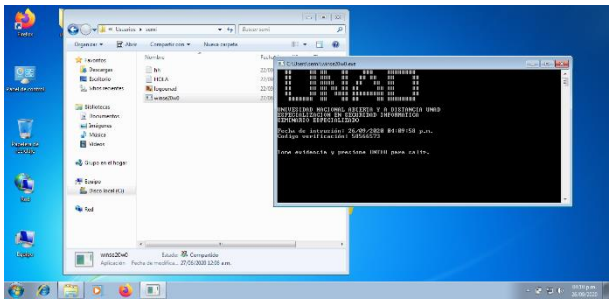
ilustración 50 Ejecución de prueba de subir un archivo remotamente



Fuente: propia

Se evidencia el archivo ejecutado desde Kali pero en el equipo Windows

ilustración 516 Archivo de Windows ejecutado remotamente

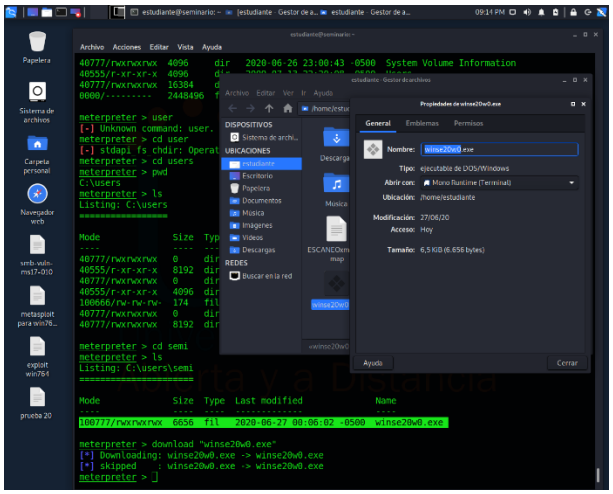


Fuente: propia

2.2.4.5 Adjunte un printscreen con la evidencia generada por el archivo winse20w0.exe el cual podrá ejecutar y visualizar una vez irrumpa en la máquina víctima.

Para ejecutar la aplicación instale la aplicación wine y las librerías de mono runtime desde la consola y al dar click derecho se ejecuta y muestra los siguiente:

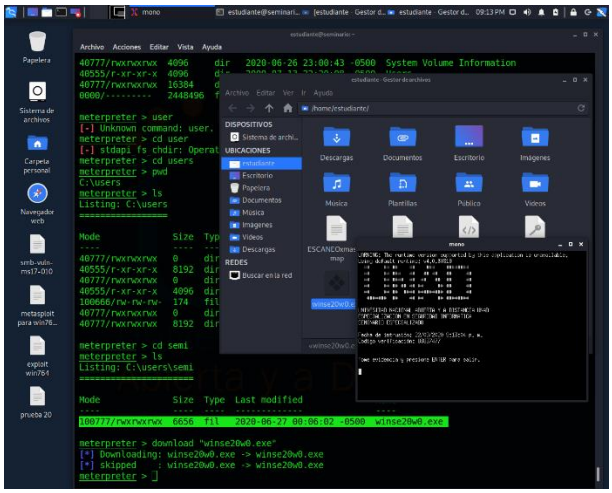
ilustración 527 archivo winse20w0.exe en la maquina atacante



Fuente: propia

Archivo ejecutado desde Kali Linux

ilustración 58 Ejecución del archivo winse20w0.exe en la maquina atacante



Fuente: propia

2.2.5 Etapa 4: Contención de ataques informáticos

Esta etapa es una etapa analítica en donde buscamos herramientas de contención y modos en que podemos proteger de manera activa los activos de información de la empresa.

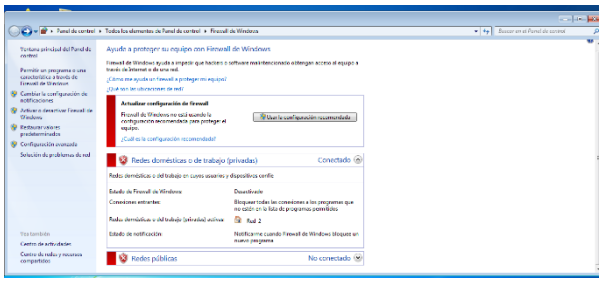
De manera individual usted deberá leer el problema que se encuentra en el anexo 5 – escenario 4 referente a equipo Blue Team y por medio del banco de trabajo configurado en la actividad anterior deberá dar respuesta a las siguientes preguntas orientadoras:

2.2.5.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Primero validar que tipo de ataque se está presentando, validar con el equipo Red Team cuales son las vulnerabilidades que tiene mi sistema.

Luego según los análisis realizados por el equipo Red Team se evidencian varias fallas entre ellas que los firewalls y el antivirus están desactivados.

ilustración 59 Maquina de Windows sin firewall activos

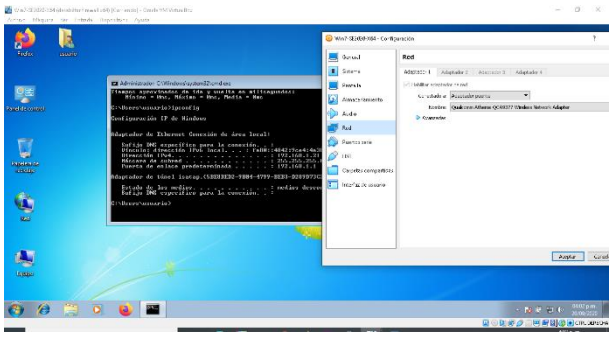


Fuente: propia

Seguido validar con el equipo Red Team, el estado de la conexión de red de cada máquina:

Validación de red para las máquinas de Windows 7 de 64 bits: 192.168.1.21

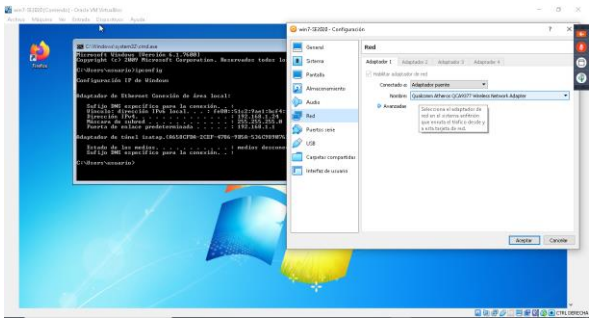
ilustración 53 validación de configuración de red



Fuente: propia

Validación de red para la máquina de Windows 7 de 32 bits: 191.168.1.24

ilustración 541 validación de configuración de red



Fuente: propia

Seguido a esto correría un snifer desde cada máquina atacada para verificar el flujo o tráfico de información a través de la red,

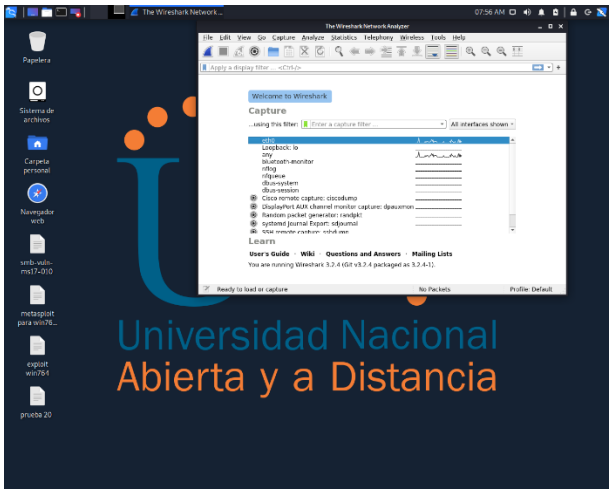
Un esnifer puede capturar los datos de paquetes, así mismo se puede decodificar y mostrar los diversos campos de uno o varios paquetes de datos. Estas herramientas nos pueden ayudar a analizar problemas de red, detectar intentos de explotación aislando los sistemas explotados, vigilar el uso de los sistemas.

Una herramienta podría ser Wireshark[12] que es una de las más conocidas y permite esnifar la red a nivel muy minucioso y poder explorar la salida o entrada de paquetes de un posible ataque o vulneración.

En este caso puedo desde mi estación de Kali, hacer una verificación de red y los paquetes que están siendo traficados en red y con esto verificar de qué tipo de ataque estoy siendo víctima y que tipo de datos me están tratando de extraer.

[12] «Wireshark User's Guide».

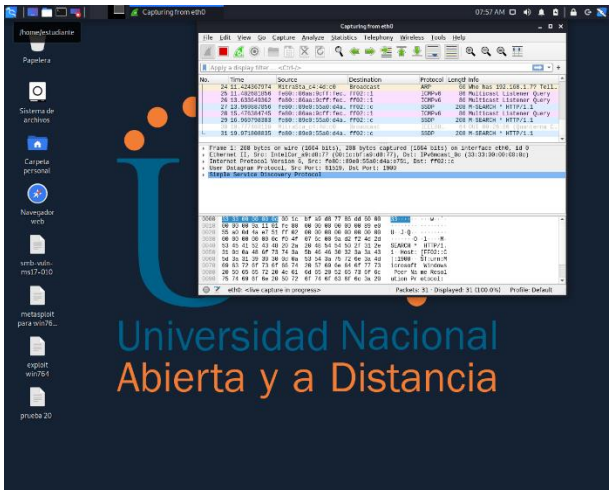
lustración 552 snifer wireshark llamado



Fuente: propia

En esta pantalla se observa el sniffer en ejecución:

ilustración 563 snifer wireshark ejecutando

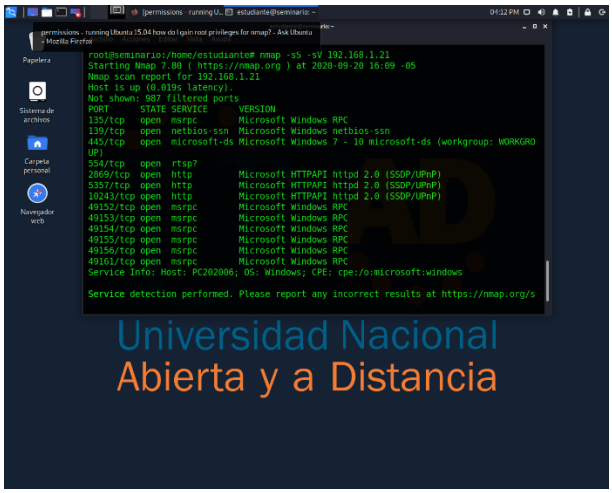


Fuente: propia

Debido a todo esto lo primero sería habilitar los firewalls y el antivirus de cada máquina, así como realizar la actualización de sistema operativo, con las cuales pueda reducir las vulnerabilidades encontradas por el equipo red.

Seguido a esto de acuerdo con el informe de puertos vulnerables, realizado por el Red Team, bloquearía los puertos encontrados con la herramienta Nmap sobre cada máquina de Windows 7 y de acuerdo con las vulnerabilidades.

ilustración 574 búsqueda de vulnerabilidades con nmap



Fuente: propia

2.2.5.2 ¿TENIENDO EN CUENTA EL ATAQUE EJECUTADO DESDE EL EJERCICIO DE RED TEAM QUÉ MEDIDAS DE HARDERIZACIÓN PROPONDRÍA PARA QUE EL ATAQUE NO SE REPITA?

Lo primero es mantener los sistemas operativos actualizados, seguidamente activar tanto el firewall como el antivirus local de las maquinas.

Adicionalmente a esas medidas, realizaría dentro de cada sistema operativo de Windows 7 en este caso, las siguientes acciones de harderización:

Propondría la Instalación segura de los sistemas operativos, en la que la principal acción seria realizar las particiones primarias del disco duro, separando los archivos de datos en otra partición y dejando solo las herramientas de software específicamente necesarias para trabajar en la partición de sistema operativo.

Colocaría contraseñas robustas, caducables y que se bloqueen con intentos fallidos de inserción tanto en acceso al sistema como a los sistemas de archivos de datos.

Des habilitación de usuarios genéricos del sistema, renombraría el usuario administrador y eliminaría las cuentas locales que se no se estén utilizando, limitando los privilegios de las cuentas que queden activas. [13]

Limitaría las carpetas de acceso compartido y subiría el nivel de las contraseñas de acceso a estas en red.

Implementaría las restricciones de software no funcional, implementando listas de software permitido y no permitido, listas blancas y listas negras, para generar cultura de uso en los usuarios.

Según el uso de cada máquina, se habilitarían los puertos necesarios según los servicios que cada uno use, no se dejarían puertos o servicios abiertos, limitando las puertas traseras abiertas por servicios que no se usen.

Se recomendaría el uso de red en NAT y se limitarían los servicios de TCP/IP en lo posible, ya que allí se habilitan muchas vulnerabilidades de seguridad.

Se deshabilitaría el acceso remoto a los equipos que no lo requieran, y si es específicamente necesario, propondrá el uso de canales de comunicación cifrados como SSH, así como el acceso limitado a usuarios específicos.

Propondría el uso de correo electrónico y mensajería instantánea cifrada.

Y en cuanto al respaldo de la información, propondría los respaldos en unidades físicas que no estén ligadas por red del equipo que genera la información. [14]

2.2.5.3 ¿Describa con sus palabras las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos?

[13] JAISON DUVANY FACHE MONTAÑA, «ESTUDIO SOBRE LA APLICACIÓN DE HARDENING PARA MEJORAR LA SEGURIDAD INFORMÁTICA EN EL CENTRO TECNICO LABORAL DE TUNJA – COTEL».
[14] «7 TÁCTICAS EFICACES PARA ROMPER LA CADENA DE ATAQUE / CYBER KILL CHAIN DE LOCKHEED MARTIN».

Los equipos Blue Team, son equipos externos a la compañía que se contratan para la función específica de buscar desde un punto de vista externo las mejores maneras de contener y mantener la ciberseguridad activa de los sistemas informáticos de la empresa contratante y dependen directamente de los que los equipos Red Team entreguen como insumo encontrado con sus ataques o intrusiones controladas. [15]

Los equipos de respuesta a incidentes informáticos SCIRT son equipos de respuesta a incidentes que son conformados básicamente por personal de la compañía que está sufriendo los incidentes, son recurso humano de la empresa, lo siguiente seria que ese equipo realiza el mismo, la verificación de vulnerabilidades y todos los procesos de contención y eliminación de vulnerabilidades, básicamente haría todo el proceso en un solo equipo , tiene la ventaja de cómo es personal interno de la empresa que lo usa, saber en tiempo real que situaciones pueden ser objeto de verificación, pero esta ventaja se convierte en desventaja al tiempo, pues al ser de la misma compañía puede ser infiltrado o manejado por el personal que puede estar filtrando información y allí radica la principal diferencia, con el Blue Team, que al ser externo la posibilidad de corruptibilidad del proceso es mínima. [16]

2.2.5.4 ¿Si dentro de un equipo Blue Team le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

Si lo utilizaría, como una guía para establecer un listado de prioridades y actividades a desarrollar en cada proceso de contención.

Lo primero que tendría en cuenta para esta decisión es que es una organización sinfines de lucro, lo cual está encaminado con un de los pilares de la ciberseguridad en mi concepto, que es sin costo o para no depender en lo posible, ni económica ni corporativamente de ninguna empresa.

Lo segundo es que es los controles CIS me permitirían crear una lista de cosas o acciones a realizar para hacer en el proceso de contención de ataques, así como usar las recomendaciones de software y hardware que en algún caso de desconocimiento amerite, aprovechando la experiencia de una comunidad de personas y empresas para realizar mejoras de seguridad mediante el intercambio

[15] «Red Team, Blue Team y Purple Team: funciones y diferencias».
[16] «Crear un csirt by DragoN JAR - issuu».

de ideas y la acción colectiva, pero en este último ítem es donde se torna delicado el asunto, pues se tendría que usar con Taltal anonimato para no hacer pública la información de la empresa contratante de los servicios de Blue Team.

Al implementar este tipo de herramientas tendría un conjunto de acciones priorizadas y en orden cronológico, basadas en la experiencia de personas del medio que solo tiene el fin de buscar el conocimiento común y la mejor protección de los sistemas que ellos protegen. [17]

2.2.5.5 Explique y redacte las funciones y características principales de lo que es un SIEM.

SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management)

SIEM es la unión de dos tecnologías que permitían una, la gestión de eventos de seguridad SEM y la otra la gestión de la información de seguridad SIM.

Se puede catalogar como un software de gestión en donde se centraliza la información sobre potenciales amenazas de ciberseguridad en las redes y equipos de la empresa, mediante la estandarización de datos y priorización de amenazas.

Se basa en el principio de buscar patrones y encontrar situaciones fuera de lo común del funcionamiento y al hacer esto se enfoca los recursos de seguridad en lo anormal.

Las principales ventajas que se podrían obtener al implementar un programa SIEM pueden ser las siguientes dependiendo de los alcances e inversión económica en el mismo: [18]

- Centralización de la información de seguridad.
- Automatización de tareas.
- Respuesta automática a eventos y amenazas.
- Disminución del tiempo de detección de ataques.
- Información rápida y eficiente para realizar análisis forense.
- Alertas de seguridades eficientes.
- Análisis y correlación de logs en tiempo real.
- Seguimiento de eventos.
- Mejor manejo del riesgo.
- Manejo de métricas de seguridad.
- Detección de activos.

[17] «CIS Controls Spanish Translation».
[18] Camila Pachón, «¿Qué es SIEM y cómo funciona? Alcance e implementación | Nsit».

- Evaluación de vulnerabilidades.
- Detección de violaciones de seguridad.
- Monitoreo de comportamiento.

Funciones principales de un programa SIEM:

- Recopilación de registros y datos de contexto: Esta función recoge los datos de registro de las máquinas de la empresa, los datos que maneja cada usuario, las vulnerabilidades de cada máquina, así como los datos de identidad de cada usuario.
- Clasificación y normalización: Esta función, comprende el paso en donde se unifica el formato de almacenamiento de registros de todos los usuarios y se establece que es normal y que no, para que el programa SIEM los gestione.

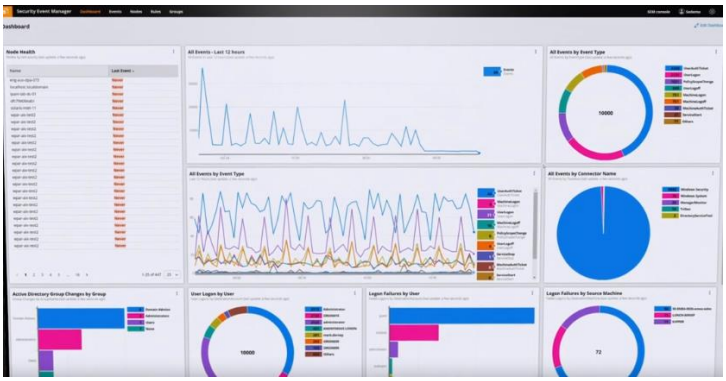
- Correlación: en esta función, se realiza el proceso de correlacionar las reglas, mediante procesos estadísticos y de algoritmia, se relacionan los datos de contexto, esta correlación se realiza en general en tiempo real pero también hay datos que no tiene posibilidad de usarse así, por lo que se correlaciona con las bases de datos de eventos ya ocurridos.

- Alertas y notificaciones: Esta función es relevante para los administradores del programa y/o gerentes de TI, las principales alertas se centran en los servicios de mensajería y los SNMP (protocolos de administración de red).

- Establecimiento de prioridades: Esta función permite valorar la prioridad de eventos importante de seguridad de aquellos que no lo son, luego hace que las alarmas se den solo cuando sea verdaderamente relevante. Esto lo logran utilizando la correlación de datos de vulnerabilidades cruzadas con la información de activos de la compañía.

- Visitas en tiempo real: se realiza en la mayoría de los casos utilizando un gestor de eventos, que puede ser manejado por programas como SolarWinds. La desventaja de este producto es que es de pago, pero bien vale la utilidad. Es muy versátil y no solo permite ver los eventos en tiempo real, sino que también permite observar los eventos de datos históricos.

ilustración 585 Gestor de vulnerabilidades Solarwinds



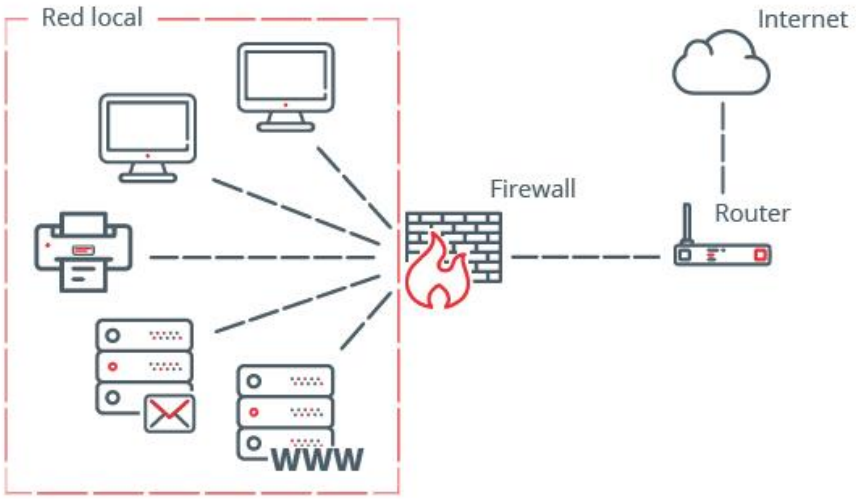
Fuente: https://www.solarwinds.com/es/network-performance-monitor

- Flujos de trabajo con seguridad: es parte de las funciones que permite hacer el proceso de gestión de incidentes de manera automática o semiautomática, así mismo permite abrir nuevos casos de incidentes o realizar procesos de investigación de incidentes. [19]

2.2.5.6 Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Firewalls:

ilustración 596 topología de firewall



Fuente: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

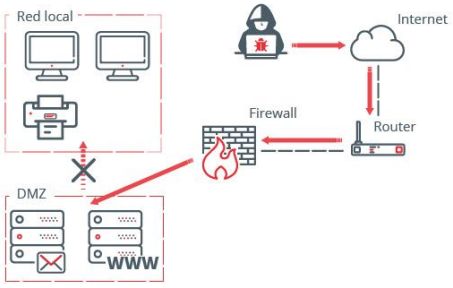
[19] «SIEM: herramientas de registro y gestión de eventos».

Se constituyen como la principal y primera herramienta de contención, estos impiden tanto el acceso como la salida de la red de determinados paquetes de datos que no cumplen con una serie de normas de seguridad previamente establecidas en la configuración del cortafuegos. Los firewalls al recibir una petición no habitual o sospechosa desde la red bloquean el puerto y aíslan ese equipo o dirección ip, según la configuración preasignada o programada,

Los firewalls los hay por hardware, instalados casi siempre en los routers administrables o por software que emulan el comportamiento de los firewalls de hardware, generalmente vienen preconfigurados con soluciones informáticas como el caso de los firewalls de Windows en los cuales el usuario puede establecer el nivel de dureza o de protección de este.

DMZ o zonas desmilitarizadas:

ilustración 607 Topología de DMZ



Fuente: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Las zonas desmilitarizadas hacen parte de una red aislada que se encuentra dentro de la red interna de la organización. Generalmente se ubica en esta zona de la red, los servicios y recursos que necesitan accesibilidad desde internet como los servidores de correo y los servidores web.

La principal característica de una DMZ es no permitir las conexiones que van desde la DMZ a la red local, pero si permite las conexiones procedentes tanto de Internet, como de la red local de la empresa donde están los equipos de trabajo de los empleados, lo que busca básicamente es que los servicios de red que son susceptibles desde internet son más propensos de vulnerabilidades permiten mayor

posibilidad de pérdidas de información, al realizarla implementación de esta solución de contención los posibles atacantes, atacaran en la primera línea a servicios que no estén comprometidos en la red local, ya que las conexiones procedentes de la DMZ se encuentran bloqueadas.

Al igual que los firewalls también pueden ser de hardware o de software. [20]

Snort

Es un IDS Sistema de Detección de Intrusos basado en red (IDSN) open source.
Es programa de monitoreo y detección de intrusiones por red que utiliza bases de datos y patrones de ciberataque conocidos, está basado en la creación de reglas que conforman patrones de monitoreo de red. El programa bien con reglas y filtros que se configuran desde la instalación inicial para adaptar el proceso de monitoreo a lo que requerimos. Tiene la ventaja de funcionar como un esnifer es decir que podemos ver el tráfico en paquetes desde consola o como un IDS (sistema de detección de intrusos) en modo automático o semiautomático. Cuando un patron de los ya prestablecidos coincide con un paquete de datos se loguea, de esta manera se saben las características básicas del ataque, tales como el cuándo , el como y el donde, permitiendo la respuesta activa del Blue Team en la contención del ataque.

Como características relevantes tiene que es de distribución gratuita, es poco pesado, permite el análisis en tiempo real, el uso de filtros y la detección de strings. [21]

[20] «Qué es una DMZ y cómo te puede ayudar a proteger tu empresa | INCIBE».
[21] «Snort - Network Intrusion Detection & Prevention System».

3 CONCLUSIONES

Se desarrollo un proceso de estudio de la ley 1273 de 2009 en la cual se planteó un resumen practico de vulnerabilidades y jurisprudencia que aplica en cada caso genérico.

Se desarrollo la práctica de alistamiento de un ambiente de trabajo controlado para la implementación de prácticas de los equipos red y Blue en el seminario de ciberseguridad que permitió en un ambiente controlado realizar la practicas de ataque y contención.

Mediante el análisis de un caso tangible de selección laboral, se plantearon escenarios hipotéticos en los que se pueden ver inmersos los especialistas en seguridad informática en los cuales se pueden violar varias leyes e incurrir por desconocimiento en delitos informáticos, así como faltar al código de ética que nos rige como ingenieros según el COPNIA.

En la actividad de Red Team, se aprendió el manejo practico de herramientas GNU para la realización de los pentesting en este caso en un ambiente controlado pero que nos mostro de manera real lo que se puede hacer como atacante a una o varias máquinas u organizaciones, si no se toman las medidas de seguridad necesarias para mantener los sistemas actualizados y libres de amenazas.

Se reconocieron y plantearon estrategias de contención de ataque en caliente, planteando alternativas para disminuir los riesgos y limitar las amenazas.

Se estudiaron medidas de harderización como una estrategia Blue Team para la contención de amenazas, así mismo herramientas de software como CIS ó SIEM y hardware como los firewalls y las zonas desmilitarizadas para realizar contenciones a posibles ataques.

4 RECOMENDACIONES

Como aspirante a especialista en seguridad informática puedo decir primero que todo que este tipo de seminarios nos abren una visión aún mas clara de una realidad laboral a la que nos enfrentamos en nuestro desarrollo profesional.

Las actividades de Red Team y Blue Team entiendo son más difíciles de realizar en ambientes virtuales, pero se deberían tener algún tipo de ambiente de desarrollo practico en físico, para ejemplificar y profundizar aún más las practicas reales.

Desde el punto de vista ético y legal, recomiendo el acompañamiento de alguna autoridad en alguna charla o encuentro virtual, para aclarar algunas dudas de carácter procedimental que se pueden presentar y que la bibliografía no alcanza a abarcar.

En cuanto a los equipos Red Team Y Blue Team, se debe dar a conocer mediante la socialización y profundización en seminarios como este, a la comunidad de TI las posibilidades que ofrecen en el mercado nacional, pues por desconocimiento casi no se tienen en cuanta sobre todo en el sector corporativo.

Las herramientas de harderización aún son poco conocidas y se implementan no como un conjunto sino como usos puntuales para casos específicos de control de algunas vulnerabilidades.

BIBLIOGRAFÍA

«7 TÁCTICAS EFICACES PARA ROMPER LA CADENA DE ATAQUE / CYBER KILL CHAIN DE LOCKHEED MARTIN». Accedido 15 de octubre de 2020. https://blog.smartekh.com/tacticas-eficaces-para-romper-la-cadena-de-ataque-cyber-kill-chain-de-lockheed-martin.

«202337164A_780: Syllabus del curso Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team». Accedido 13 de octubre de 2020. https://campus102.unad.edu.co/ecbti81/mod/folder/view.php?id=1669.

Camila Pachón. «¿Qué es SIEM y cómo funciona? Alcance e implementación | Nsit». Accedido 15 de octubre de 2020. https://www.nsit.com.co/que-es-siem-en-seguridad-informatica-alcance-e-implementacion/.

«CIS Controls Spanish Translation», s. f.

«Código de ética para ingenieros». Accedido 15 de octubre de 2020. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf.

«Crear un csirt by DragoN JAR - issuu». Accedido 15 de octubre de 2020. https://issuu.com/dragonjar/docs/crear_un_csirt.

«DECRETO 1377 DE 2013». Accedido 15 de octubre de 2020. http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081.

«Detrás de Buggly: la historia de la fachada Andrómeda • ENTER.CO». Accedido 15 de octubre de 2020. https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/.

«GUÍA DE PRUEBAS OWASP 2008 V3.0», 2002.

«HACKING 4 BAD PENTESTERS: [STEP-BY-STEP] Eternalblue desde Metasploit - Hacking Windows 7». Accedido 15 de octubre de 2020. https://www.hacking4badpentesters.com/2017/04/step-by-step-eternalblue-desde.html.

JAISON DUVANY FACHE MONTAÑA. «ESTUDIO SOBRE LA APLICACIÓN DE HARDENING PARA MEJORAR LA SEGURIDAD INFORMÁTICA EN EL CENTRO TECNICO LABORAL DE TUNJA – COTEL». Accedido 15 de octubre de 2020.

https://repository.unad.edu.co/bitstream/handle/10596/11908/1049612360.pdf?sequence=1&isAllowed=y.

«ley 1273 del 5 de enero de 2009». Accedido 15 de octubre de 2020. https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

«Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1581_2012]». Accedido 15 de octubre de 2020. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

Oracle VM VirtualBox ®. «Oracle VM VirtualBox ®¨», 2012, 1-362.

«Qué es una DMZ y cómo te puede ayudar a proteger tu empresa | INCIBE». Accedido 15 de octubre de 2020. https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa.

«Red Team, Blue Team y Purple Team: funciones y diferencias». Accedido 15 de octubre de 2020. https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/.

«SIEM: herramientas de registro y gestión de eventos». Accedido 15 de octubre de 2020. https://www.softhoy.com/conoce-puedes-hacer-herramientas-registro-gestion-eventos.html.

«smb-vuln-ms17-010 NSE Script». Accedido 15 de octubre de 2020. https://nmap.org/nsedoc/scripts/smb-vuln-ms17-010.html.

«Snort - Network Intrusion Detection & Prevention System». Accedido 15 de octubre de 2020. https://www.snort.org/#get-started.

«Wireshark User’s Guide». Accedido 15 de octubre de 2020. https://www.wireshark.org/docs/wsug_html_chunked/.