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

LUIS ENRIQUE CARDOZO SUAZA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2022

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

LUIS ENRIQUE CARDOZO SUAZA

Documento Técnico para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Nombre
Luis Fernando Zambrano Hernández
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2022

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

1. GLOSARIO

ATAQUES INFORMATICOS: Es la acción de personal que ingresan abruptamente a un sistema de información sin permiso.

BLUE TEAM: área encargada de analizar el comportamiento de los sistemas de información.

CONFIDENCIALIDAD: Es la protección que se le entrega a un dato para que sea accesible únicamente a las personas autorizadas.

CVE: Listado de información de vulnerabilidades ya encontradas y publicadas con su forma de subsanarG

EXPLOIT: Ataque informático que usa vulnerabilidad de un software o equipo de cómputo para causar algún efecto o daño.

FIREWALL: Dispositivo o software el cual filtra y analiza información que ingresa y sale de la conexión a internet.

PENTESTING: Pruebas de ataques amigables con la única razón de encontrar debilidades de seguridad y poder subsanarlas.

RED TEAM: área de profesionales en seguridad los cuales actúan como amenazas buscando superar los controles de seguridad.

VIRTUAL BOX: Software gratuito para el trabajo de máquinas virtuales.

VULNERABILIDADES: Fallo de seguridad en un sistema de información que pone el riesgo de esta misma.

2. RESUMEN

En el curso de seminario especializado - Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team, este es desarrollado en 3 unidades, la primera es el contexto ético, legal Red & Blue Team, el segundo hace referencia a los pasos y procesos Red Team y la tercera unidad es el análisis y contención en Blue Team.

Se realizaron 4 etapas en donde la etapa inicial era identificar conocimientos previos en donde se realizaron varias preguntas de la guía 1 conceptos equipos de seguridad. La segunda etapa fue la actualización ética y legal, en la tercera etapa es la ejecución de pruebas de intrusión y en la última etapa es la contención de ataques informáticos. Estas etapas todas se enfocaron en cómo se debe proteger la información y adicional como se debe contener un ataque informático.

En la última etapa se realiza una socialización de un informe técnico en donde se relacionan los análisis de etapas anteriores en donde se relaciona los aspectos importantes de las anteriores actividades, planteando recomendaciones y conclusiones para un mejoramiento en el sistema de hackers security.

Palabras claves:

Blue Team y Red Team, Ciberseguridad, Equipo de respuestas a incidentes, Estrategias de contención, Seguridad de la información.

ABSTRACT

In the specialized seminar course - Strategic Cybersecurity Teams: Red Team & Blue Team, this is developed in 3 units, the first is the ethical, legal context Red & Blue Team, the second refers to the steps and processes Red Team and the third unit is analysis and containment in Blue Team.

Four stages were carried out where the initial stage was to identify previous knowledge where several questions from the guide 1 concepts of safety equipment were asked. The second stage was the ethical and legal update, in the third stage is the execution of intrusion tests and in the last stage is the containment of computer attacks. These stages all focused on how information should be protected and additionally how a computer attack should be contained.

In the last stage, a socialization of a technical report is carried out, where the analyzes of previous stages are related, where the important aspects of the previous activities are related, proposing recommendations and conclusions for an improvement in the security system of hackers.

3. INTRODUCCIÓN

El presente informe hace referencia a los delitos informáticos y su parte ética de cada uno de ellos en las leyes actuales, es necesario que se vallan realizando pruebas propuestas en los escenarios de esta actividad practica con el fin de hacer una revisión completa entre blue team y red team en donde se debe validar cada una de las vulnerabilidades y fallas dentro de la compañía hackers security, adicional a esto se debe realizar un análisis completo de vulnerabilidades y el cómo se pueden subsanar desde la compañía esto con el fin de entregar un informe completo y concluyente en cada uno de los escenarios propuestos.

Este informe aumentara las capacidades técnicas, éticas y de gestión frente a cada uno de los equipos de Red Team y Blue Team que se encuentran dentro de los escenarios propuestos.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Planificar metodologías de ciberseguridad en la búsqueda de planteamiento en los sistemas información, la ciberseguridad defensivas y ofensivas frente a cada uno de los procesos propuestos en el área paran cada escenario en la infraestructura TI y el área completa.

4.2. OBJETIVOS ESPECÍFICOS

- Analizar y evaluar cada una de las acciones que debe llevar a cabo un equipo de Red Team y Blue Team en la organización en busca de criterios éticos y legales en cada uno de los escenarios propuestos para este informe.

- Detallar cada uno de los escenarios propuestos en busca de vulnerabilidades mostrados en el sistema de información a partir del buen uso de metodologías y técnicas de intrusión esto con el fin de proteger los sistemas de cualquier atacante.

- Realiza la formulación de estrategias para la contención de ataques mediante los análisis de vulnerabilidades y riesgos para la infraestructura de la organización TI todo esto para evitar el robo de información y proteger los sistemas de información.

5. DESARROLLO DEL INFORME

5.1. ETAPA 1 – CONCEPTOS EQUIPOS DE SEGURIDAD

5.1.1. Escenario 1 – Situación Problema

Situación problema: Montaje banco de trabajo

"The Hackers Security requiere previamente una instalación de un banco de trabajo con el cual el personal postulado a hacer parte de la organización deberá utilizar en una serie de escenarios y problemas complejos al interior de The Hackers Security. El banco de trabajo debe estar basado en herramientas software Opensource, la recursividad será vital en este proceso.
De manera simultánea The Hackers Security requiere conocer por medio de una serie de preguntas orientadoras el estado inicial o base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad, al resolver estas preguntas la organización podrá tener una perspectiva global de sus futuros empleados"[1].

5.1.2. Legislación Relacionada con Delitos Informáticos y Protección de Datos Personales en Colombia

Los delitos informáticos son las conductas ilegales, delictivas e ilícitas que usan el internet o dispositivos electrónicos con el fin de dañar y vulnerar los bienes o patrimonios de entidades o terceras personas por ello son castigadas penalmente.

Existen varios tipos de actividades como fraudes, falsificaciones, perjuicios, sabotajes, hurto, entre otras destacándose el uso de equipos de cómputo por lo cual han establecidos unas leyes y normales los cuales buscan minimizar esta serie de delitos informáticos y una seguridad mayor en el país.

Actualmente en la república de Colombia existe la ley 1273 del 2009 la cual busca la protección contra los delitos informáticos y los datos, esta ley actualmente tiene 10 artículos los cuales se especifican a continuación

- ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO
- OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN
- INTERCEPTACIÓN DE DATOS INFORMÁTICOS
- DAÑO INFORMÁTICO
- USO DE SOFTWARE MALICIOSO

[1] UNAD, Anexo 1 – Escenario 1 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2481/mod_folder/content/0/Anexo%201%20-%20Escenario%201.pdf?forcedownload=1

- VIOLACIÓN DE DATOS PERSONALES
- SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES
- CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA
- HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES
- TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

La persona que viole esta **ley 1273 del 2009** ingresará dentro del Código Penal el cual esta conducta está tipificada como acceso abusivo a sistema informático, tendrá de 48 a 96 meses de prisión y de 100 a 1.000 salarios mínimos de sanción. Igualmente, el delito relacionado de interceptación de datos informáticos tendrá una pena de prisión de 36 a 72 meses.

Los datos personales es la información privada de una persona en cual puede interactivas con otras personas o empresas individualizándolo con el resto de sociedad, esto con el fin de la generación de información que no solamente contribuye a la economía de la persona sino también a los servicios y vienes de cada uno.

Actualmente en nuestro país se encuentra en rigor la **ley 1266 del 2008** la cual es aplicada para todos los datos personales financieros, crediticios, comerciales y de servicios que se encuentren registrados en cualquier base de datos.
La **ley 1266 del 2008** o más conocida como habeas data protege la información personal de cada persona de cualquier ámbito y por el mal uso de esta o captar información sin autorización puede enfrentarse a multas hasta los 2000 salarios mínimos mensuales vigentes[2]

5.1.3. Pruebas de penetración o pentesting

El test de penetración es una acción que se acuerda con la empresa o compañía que desea identificar y corregir las vulnerabilidades o peligros que se encuentren asociados a sus sistemas informáticos, esta es una auditoria la cual se logra recolectar bastante información ya que el personal encargado de realizar este test serán personas alejadas de la compañía que trataran de buscar vulnerabilidades para así poder ingresar a los sistemas de información de la compañía[3].

El test de penetración tiene como objetivo intentar ejecutar ataques de ingeniería social, actuar como un atacante interno y comprobar los sistemas físicos de seguridad en la compañía, cualquier test sigue unos pasos determinados para presentar al final resultados que pueden varios dependientes del audito.

---

[2] Congreso de la República, Ley 1273 del 2009. 2020. Disponible en https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[3] Helpsystems, 2021. Las seis fases de pentesting. Disponible en https://www.helpsystems.com/es/blog/las-seis-fases-del-pentesting

1. Preacuerdo
2. Recolección de información
3. Análisis de vulnerabilidades
4. Modelado de amenazas
5. Explotación
6. Post-Explotación
7. Reportes o informes

Estas fases se explicarán a continuación.
La **primera fase** es el contacto en la cual se acuerda con el cliente los formularios que se auditaran, los sistemas, los dominios de la empresa, los costos de la auditoria, en que va a consistir el test de penetración, cuáles son los servicios críticos para la empresa y cuál es el problema más grande en caso de ataque.
Se debe definir las fechas para el reporte final y los tipos de test de penetración como lo son Black Box, Gray Box y White Box.

El **test de caja negra** o también llamado Black Box son las pruebas que se realizan como evaluación de seguridad y pruebas sin conocimiento previo, esto simulando cualquier ataque de hacker malicioso fuera del perímetro de seguridad de la compañía.

El **test de caja gris** también llamado Gray Box son evaluaciones de seguridad y pruebas internas examinando los grados de acceso a la información privilegiada dentro de la red como propósito de simular formas más comunes para ataques que se realicen dentro de la red de la compañía.

El **test de caja blanca** o también llamado White Box implican la evaluación de seguridad y pruebas con el conocimiento completo de la infraestructura de la red también llamados como auditorías internas.

En la **segunda fase** de recolección de información se pueden utilizar varios métodos para realizarlo como Google Hacking, Osint o Doxing. La recolección de información es sumamente importante ya que con esto se conocerá el objetivo en el cual se está trabajando. La idea es sacar la mayor cantidad de información posible como por ejemplo registros de dominios, puertos abiertos, el sitio web corresponde a un cms y la identificación del sistema.

La **tercera fase** es el análisis de vulnerabilidades en donde se empieza a analizar el sistema manualmente o automática para identificar vulnerabilidades para la intrusión, Para esta fase la mejor opción es utilizar Kali Linux el cual ofrece una variedad de herramientas para el análisis de vulnerabilidades y pentesting como lo son Wireshark, Nessus, SQLMap, entre otras pero dentro de este apartado una de las mejores es Nessus por su variedad de opciones y complementos que pueden

hacer que el análisis sea mucho más fácil, adicional el reporte que se extrae arroja la información de cada una de las vulnerabilidades y la mejor manera de solventarla.

En la **cuarta fase** de modelado de amenazas se utiliza la información extraída en el análisis en donde se va a gestionar los perfiles de ataque y se revisara la creación de diccionarios para el ataque de fuerza bruta.

En esta fase se presenta la información estructurada que afecta la seguridad de la aplicación, es una vista de la aplicación su entorno a través de la información. Se busca capturar, organizar y analizar toda la información para la toma de decisiones sobre los riesgos que tiene la aplicación y las amenazas.
La **Quinta fase** o fase de explotación con el modelado de las amenazas se detallará la mejora manera de atacar o que vulnerabilidad se va a explotar para así lograr el objetivo de acceder al sistema de la compañía

En la **sexta fase** de generación de reportes es donde se entrega detalladamente todos los errores de seguridad que se han encontrado y los procesos que se realizaron, adicional se puede indicar cuales son las medidas para solventar estas vulnerabilidades y así tener un sistema con la mayor seguridad posible, se debe indicar que estos testeos deben realizar de manera recurrente ya que es la información de cualquier compañía es preciada.

Actualmente existen dos tipos de reportes el cual es el reporte técnico que es únicamente para los administradores del sistema ya que lleva terminologías propias y se anexan las posibles soluciones que deberían llevar para la implementación. El reporte ejecutivo el cual es para el cliente y la mesa directiva en donde el reporte es con palabras apropiadas para las personas ajenas a la tecnología o la informática y que puedan entender, adicional a esto se debe exponer que se encontró en la auditoria a la persona encargada de la contratación o encargada de la revisión del proyecto.

5.1.4. Herramientas y servicios utilizados en la Ciberseguridad

Las herramientas para la seguridad informática es muy importante ya que ayudan al análisis de vulnerabilidades en los diferentes aplicativos como se describe a continuación

5.1.4.1. Herramientas

5.1.4.1.1. Metasploit

Es una herramienta de prueba para penetración el cual ayuda a descubrir y reforzar las vulnerabilidades en los sistemas de información antes de que sea atacado por hackers o personas inescrupulosas.

Metasploit Framework es un sistema de código abierto basado en Ruby el cual es utilizado por los ingenieros en seguridad informática y ciberdelincuentes ya que ayuda a encontrar, explotar y validar las vulnerabilidades del sistema de información.

Este aplicativo tiene varias funciones desde interfaces, bibliotecas, módulos y complementos.

El software Metasploit tiene varios en las pruebas de penetración los cuales incluyen
- Recopilación de información: mediante el uso de módulos auxiliares: portscan / syn, portscan / tcp, srnb version, db nmap, scanner / ftp / ftp_version y collect / shodan_search.
- Enumeración: utilizando enumshares smb / srnb, enumusers smb / srnb y smb / srnb_login.
- Obtener acceso: mediante el uso de exploits y cargas útiles de Metasploit.
- Escalada de privilegios: mediante el uso de meterpreter-use priv y meterpreter-getsystem.
- Mantener el acceso: mediante meterpreter, ejecuta la persistencia.
- Cubriendo pistas: mediante el uso de módulos anti-forenses posteriores a la explotación.

También tiene varios beneficios al utilizar Metasploit Framework los cuales se describen a continuación.

- Simulación de escenarios del mundo real: los pentesters pueden ver los sistemas de una organización desde la perspectiva de un pirata informático. Esta visibilidad les permite prepararlos para mejorar la seguridad de la red corrigiendo las vulnerabilidades descubiertas y otros vectores de ataque.
- Automatización de tareas: Metasploit permite a los pentesters automatizar muchas de las tediosas tareas involucradas en el proceso de prueba de penetración. Gran parte del código básico de estos comandos se almacena en sus bibliotecas.
- Optimización de casos de negocio: Metasploit proporciona informes claros para los ejecutivos sobre las vulnerabilidades que se deben priorizar. Con una clara evidencia de posibles explotaciones, los equipos de seguridad pueden crear casos comerciales más sólidos para la compra de herramientas de seguridad adicionales que pueden mitigar la superficie de ataque.

5.1.4.1.2. Nmap

Este es un software de código abierto que sirve para escanear la red y los puertos para extraer información para controlar y gestionar su seguridad. Se utiliza bastante para las auditorias de seguridad y monitoreo de redes.

En este software permite diferentes escaneos como el Ping/arp para conocer los hosts que se encuentran dentro de la red, Tpc connect en donde se visualizan todos

los puertos, sondeo de lista el cual muestra los nombre de los dispositivos conectados y fin en donde muestra si el host se encuentra tras un cortafuegos.

El software Nmap sirve principalmente para el mapeo de puertos, pero adicional tiene diferentes funcionalidades que permiten extraer diferente información. Estas son algunas de las funcionalidades que tiene Nmap.

- Mapear una red
- Identificar servicios en ejecución
- Realizar una auditoría de seguridad
- Detectar sistemas operativos

5.1.4.1.3. **Openvas**

Es un software que sirve para encontrar fallas en la seguridad y la información de forma detallada en vulnerabilidades los cuales pueden ser explotadas para poner en riesgo la confidencialidad, disponibilidad y la integridad de la información almacenada y procesos.

Openvas es un software con diferentes funciones en las que se encuentran las pruebas autenticadas, pruebas no autenticadas, cuentas con protocolo industrial y de internet alto o bajo nivel, ajustes personalizados de rendimiento para exploraciones a gran escala, desarrollado en un potente lenguaje de programación interno para implementar cualquier tipo de pruebas de vulnerabilidad.

5.1.4.2. Servicios en línea

5.1.4.2.1. Exploit-DB

Esta es una base de datos de exploits o brechas de seguridad el cual los hackers cuelgan las vulnerabilidades de aplicaciones para aprovecharse de ellas con instrucciones, es un dominio el cual con lleva varios proyectos como lo es Google Hacking Data base el cual funciona igualmente como un exploit tradicional, pero este no usa código en sus servicios u aplicaciones, utiliza la sintaxis de Google para ejecutar comando y así obtener la información necesaria.

Esta es una alternativa de encontrar aplicaciones vulnerables y extraer la información u obtener privilegios.

5.1.4.2.2. CVE

Son los puntos vulnerables y exposiciones en donde se encuentran un listado de fallas de seguridad informática el cual se encuentra disponible para cualquier público.

Los CVE puede reportarlo cualquier persona que descubra una falla y la notifique, muchos proveedores ofrecen recompensas por detectar las fallas de seguridad para ayudar a la divulgación responsable.

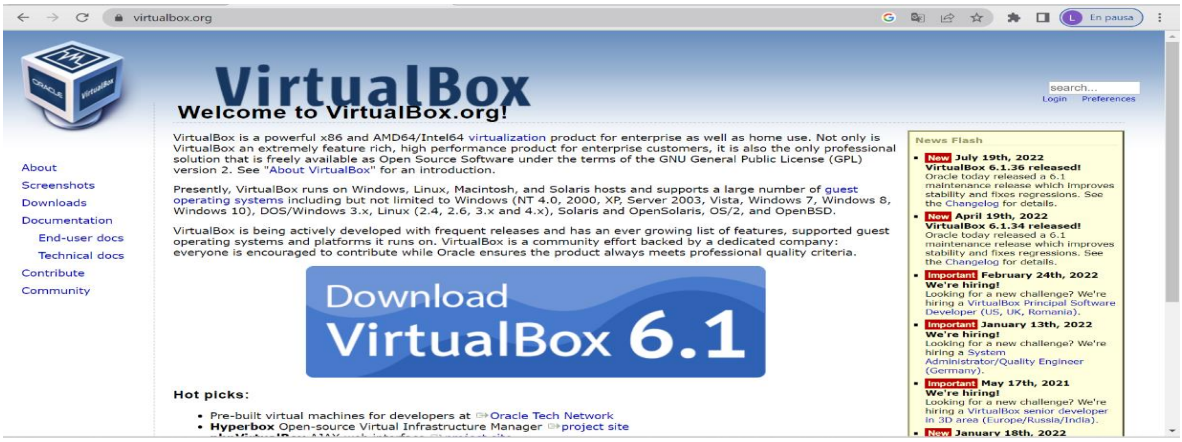
Los números de identificación de CVE se asignan cuando cumplen una serie de criterios.

- Se puede solucionar de forma independiente
- El proveedor afectado las confirma y las documenta
- Afecta una base del código

5.1.5. **Implementación del Banco De Trabajo de forma local**

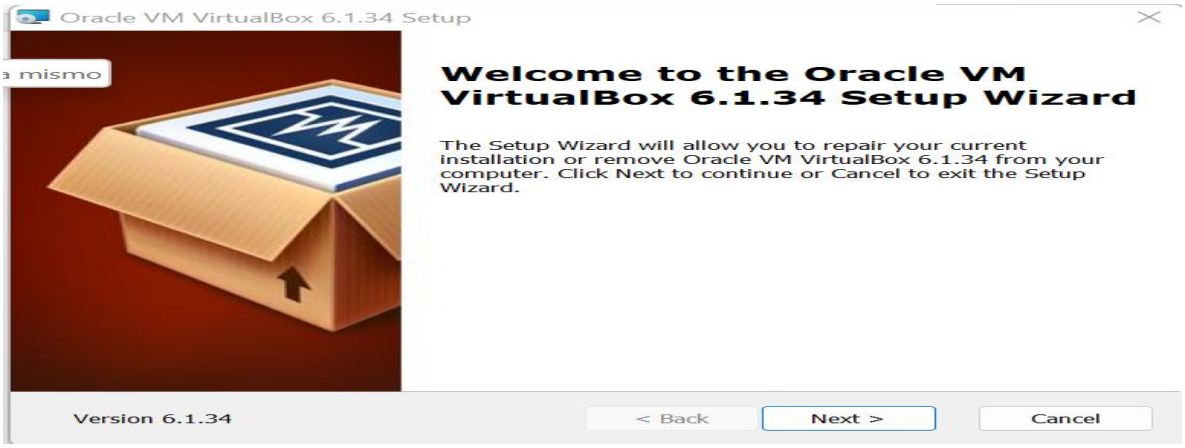
Lo primero que se debe realizar es ingresar a la página de virtual box, descargarlo e instalarlo para poderlo utilizar como lo muestra la figura 1 y 2.

Ilustración 1 Descarga de Virtual Box



Fuente: Luis Cardozo

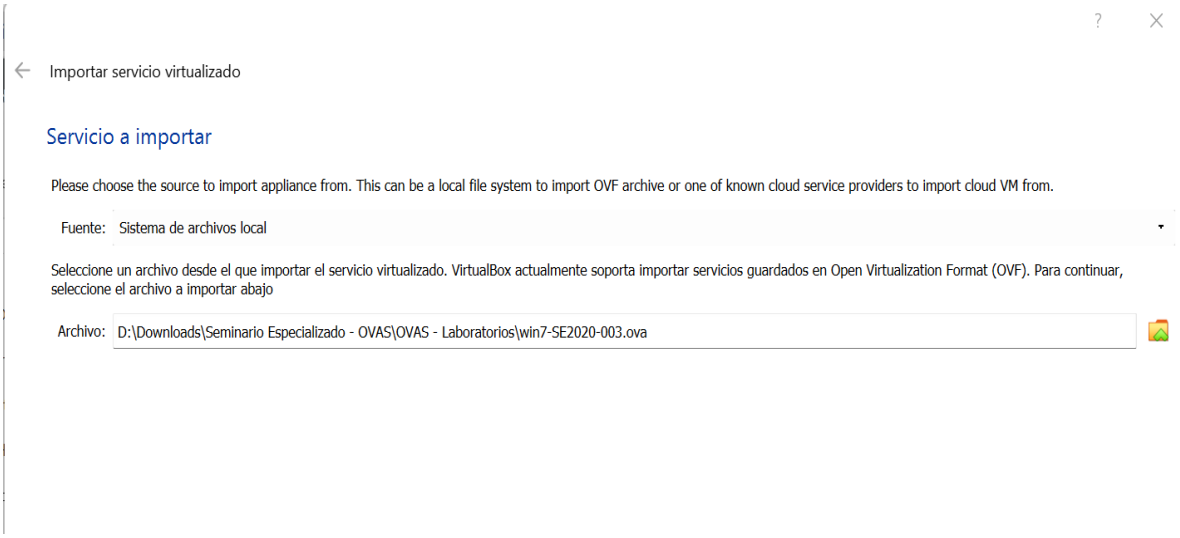
Ilustración 2 Instalación de Virtual Box



Fuente: Luis Cardozo

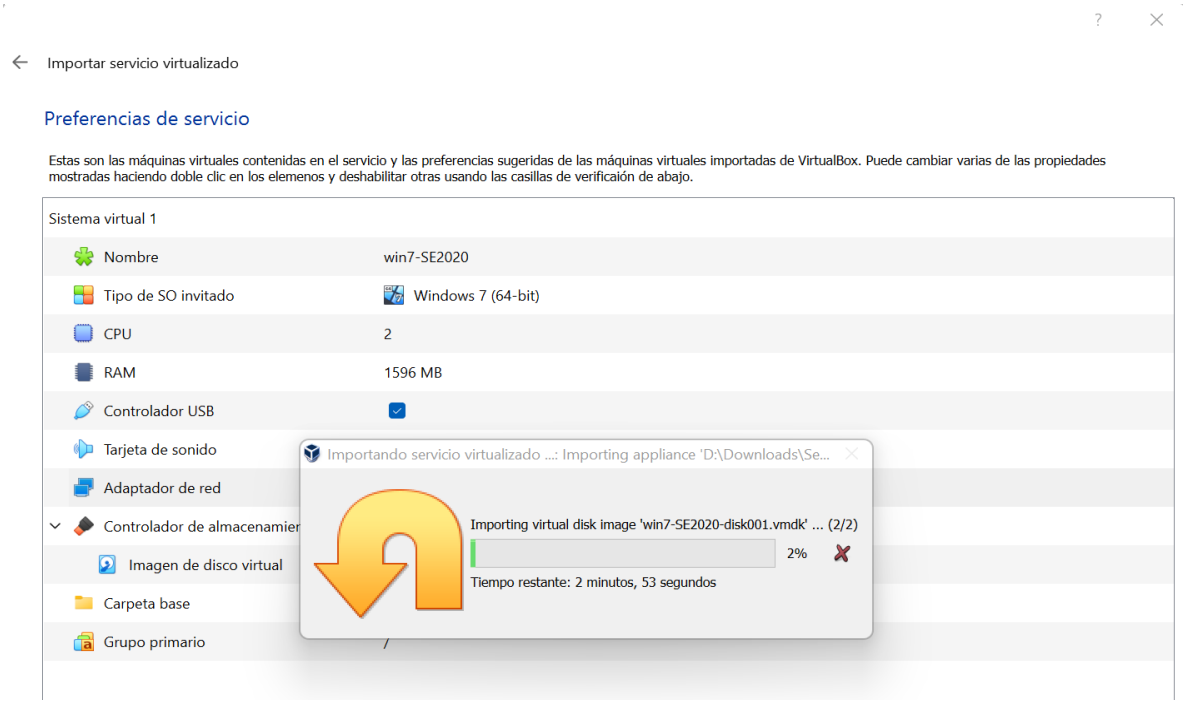
Luego de esto se ejecuta el virtual box y se procede a la importación de la máquina virtual como lo muestra la figura 3 y 4, esto se debe realizar con cada una de las máquinas.

Ilustración 3 Importación de máquina virtual



Fuente: Luis Cardozo

Ilustración 4 Configuración de la máquina virtual

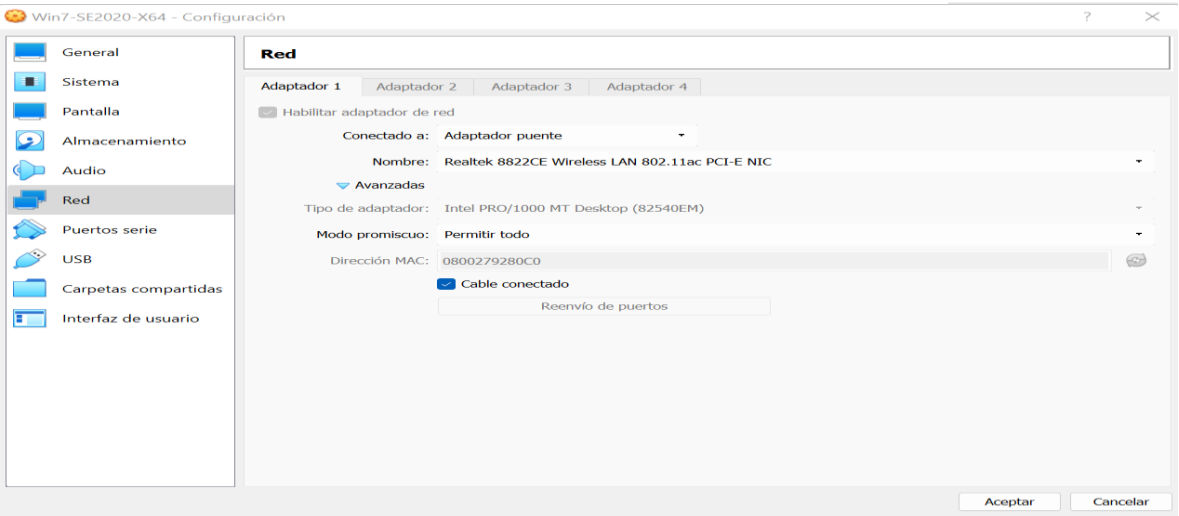


Fuente: Luis Cardozo

Luego de un tiempo que lleva la instalación se realizara el mismo proceso con los dos sistemas operativos que faltan, luego de eso se configurara la red en puente para cada uno de los sistemas operativo se puedan comunicar y se han independientes en la red como se muestra en la imagen 5.

Figura 5. Configuración de red en las máquinas virtuales

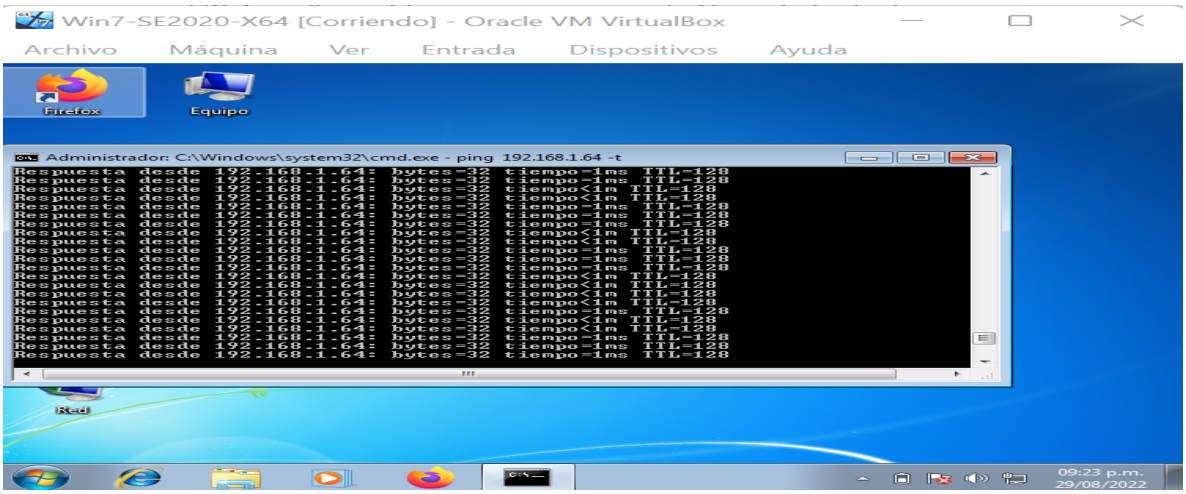
Ilustración 5 Configuración de red en las máquinas virtuales



Fuente: Luis Cardozo

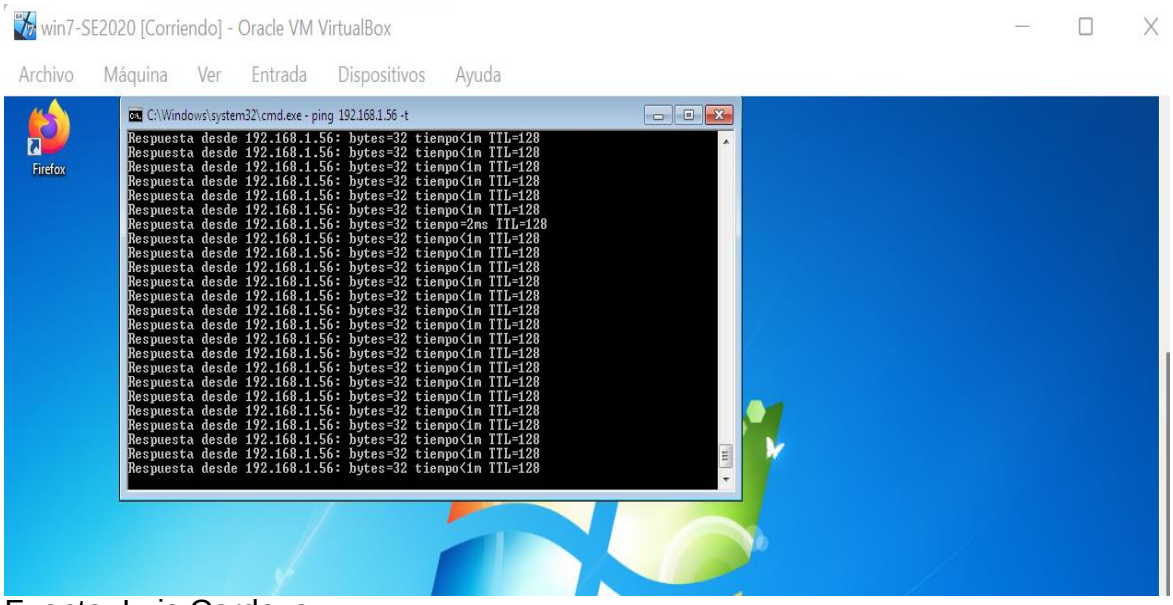
Luego de esto se inicia las máquinas virtuales y se debe ingresar al símbolo de sistema para saber la ip y poder realizar un ping entre los sistemas operativos como se muestra en la figura 6 y 7.

Ilustración 6 Sistema operativo x64 conectado con las demás maquinas



Fuente: Luis Cardozo

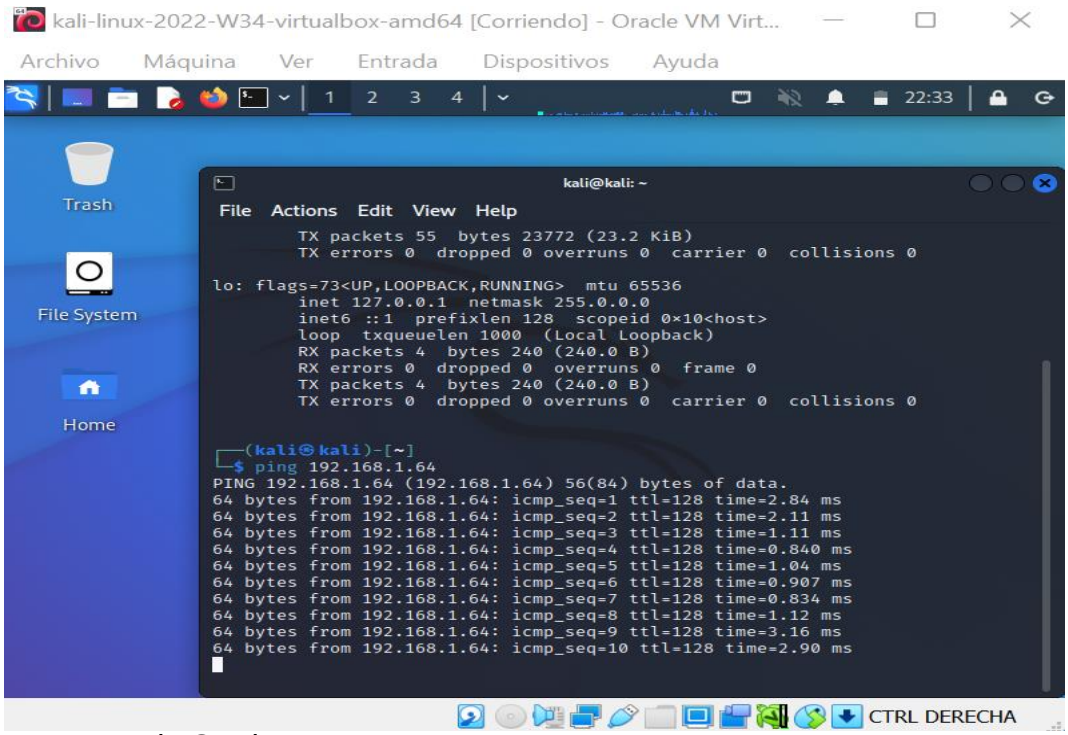
Ilustración 7 Sistema operativo x86 conectado con x64



Fuente: Luis Cardozo

Luego se va a realizar el mismo testeo desde Kali Linux a las máquinas de Windows encontrando la comunicación entre las 3 máquinas virtuales como lo muestra la figura 8.

Ilustración 8 Kali Linux



Fuente: Luis Cardozo

5.2. ETAPA 2: ACTUACIÓN ÉTICA Y LEGAL

5.2.1. Escenario 2

Situación problema: Análisis legal

“La organización Hackers Security es una organización con reconocimiento a nivel mundial por asesorar a grandes Gobiernos en procesos de ciberseguridad y ciberdefensa logrando posicionarse como la organización más importante en el campo de la seguridad informática a nivel mundial, la organización ha decidido que es hora de conformar equipos de Red team y Blue team dentro de su estructura funcional para aumentar los protocolos de seguridad al interior de esta.

Para dar inicio, la organización Hackers Security hace entrega de un contrato para el reclutamiento de sus equipos Red team y Blue team; este contrato fue elaborado por un abogado que ya no labora con la organización y fue despedido por encontrar algunos procesos ilícitos. La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal, por ende, los contratos son entregados sin modificación alguna; ante este evento la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal, sin embargo, la organización aprovecha una serie de problemas que ha identificado en su interior y como prueba de admisión al equipo Red team y Blue team deciden clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión “característica” de estos equipos. También deberá proyectar la instalación de dos máquinas virtuales por medio de virtualbox para poder ejecutar las sesiones de pruebas en las actividades posteriores”[4].

5.2.2. Acuerdo de Confidencialidad

Situación Problema: Análisis Legal

“ACUERDO DE CONFIDENCIALIDAD ENTRE NOMBRE STUDIANTE Y HACKERS SECURITY

Por la parte reveladora
Nombre: Hackers Security
Dirección: EE.UU
Teléfono: 1100011100
E-mail: Info@Thewhitehousesecurity.com

Por la parte receptora de la información

[4] UNAD, Anexo 2 – Escenario 2 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2409/mod_folder/content/0/Anexo%202%20-%20Escenario%202.pdf?forcedownload=1

Nombre: Nombre estudiante
Dirección:
Teléfono:
E-mail:
Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**:

1. Que la información compartida en virtud del presente acuerdo pertenece a Hackers 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 Hackers Security Hackers 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.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proceso de selección de personal, nombre estudiante que, para el presente caso actual como revelador, guarda y administrados de la información de propiedad de Hackers Security.

En consecuencia, las **partes** se suscriben a las siguientes **cláusulas**:

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 Hackers Security no podrán ser divulgados.

Segunda. Definición de información confidencial: se entiende como Información Confidencial, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la parte receptora con ocasión del proceso de selección de personal.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.

parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de esta o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Hackers Security, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

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.

5. Usar la información confidencial que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

6. Mantener la información confidencial en reserva hasta tanto adquiera el carácter de pública.

7. Responder por el mal uso que le den sus representantes a la información confidencial.

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

9. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Hackers Security.

Parágrafo: Cualquier divulgación autorizada de la información confidencial a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente Acuerdo y la parte receptora deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la información confidencial hasta tanto

Sexta. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

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 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 Hackers Security.

Novena. Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

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.

Firman en Bogotá D.C., a los (xxx) días del mes de (xxx) de 201_

Como Parte Receptora:

_____
Nombre del estudiante.

Por la parte reveladora:

_____
Nombre Gerente de la empresa Estudiante UNAD.
Hackers Security
C.C. No. de C.C. No. De"[5]

5.2.3. Análisis de situación problema y el acuerdo de confidencialidad con relación a los artículos vulnerados de la ley 1273 de 2009

Se realizo un análisis con detenimiento al anexo 2 y 3 en donde se evidenciaron bastantes inconsistencias en la empresa Hackers Security y en su contrato por ello a continuación se muestra los párrafos los cuales tienen debilidades al momento de la contratación del personal.

- "Que la información compartida en virtud del presente acuerdo pertenece a Hackers 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."

- "Que la información de propiedad de Hackers Security Hackers 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."

Con la revisión de los anexos se encontraron varias anomalías las cuales no deberían tener una empresa ya que puede estar en riesgo la información y la compañía afectando la confidencialidad, integridad y autenticidad de los datos que maneja la compañía, por ello enumeramos los siguientes hallazgos.

- La gerencia de la compañía Hackers Security no realiza un verdadero análisis a fondo de las personas que ingresan a trabajar para la empresa en donde solo realiza recomendaciones.

- No realiza revisiones periódicamente a los contratos y mas si la persona que los redactaba ya no se encuentra laborando para la compañía.

[5] UNAD, Anexo 3 – Acuerdo PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2409/mod_folder/content/0/Anexo%203%20-%20Acuerdo.pdf?forcedownload=1

- No se resguarda la información de buena manera ya que se la entrega a personas y empresas que no han firmado contrato y no tiene cláusula de confidencialidad.

Luego de estas inconsistencias encontradas esta compañía estaría incurriendo en delitos informáticos dentro de la organización, solamente por dejar en conocimiento y validación de esta información a personal previamente contratado esta vulnerando la información de terceros.

Adicional a eso se encontró que no es la mejor manera de soltarla información de una compañía a un proceso de selección en donde todavía no cuenta con un vínculo laboral con esta, esto con el fin de realizar el proceso de quien va a quedar contratado por esta empresa vulnerando la información de terceros el cual no se sabe cómo la va a manejar y si puede ser publicada o compartida a personas mal intencionadas.

5.2.4. Análisis y revisión de la propuesta laboral con respecto a punto de vista legal y ético

Se evidencian varias inconsistencias en el contrato presentado por la compañía Hackers Security las cuales se muestran a continuación.

- “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 confidéncialo sobre procesos ilegales dentro de Hackers Security no podrán ser divulgados”

En este párrafo que fue señalado del contrato de Hackers Security va contra la ley 1273 del 2009 ya que vulnera la seguridad de la información, materializa lo fraudes tecnológicos y hurtos, el cual puede conllevar a un proceso legal a la compañía y personal implicado directamente.

- “Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos. parte receptora tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados

En este párrafo se evidencia que viola varios de los artículos de la ley 1273 del 2009 los cuales son el artículo 269C – Interceptación de datos informáticos, articulo 269F

– “Violación de datos personales, articulo 269H – circunstancias de agravación punitiva y articulo 269i – hurto por medios informáticos y semejantes. Los cuales pueden acarrear un proceso legal tanto la compañía como el personal que adquirió un contrato con la compañía el cual no especifica en el contrato como se van a trabajar o realizas las actividades”[6].

- “Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.”

Este párrafo vulnerario la seguridad de la información, hurtos y fraudes electrónicos ya que no se especifica las formas o procedimientos para lograr los objetivos esto en contra de la ley 1273 del 2009

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

Este párrafo va en contra de la ética y la moral profesional al encubrir ilegalidades que vulneren los derechos de los terceros y va en contra de la ley 1273 del 2009.

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

Este párrafo va en contra de los controles que se deben realizar ante actos ilícitos que involucren que seguridad de la información haciendo que se dificulte los controles de los entes y violando la ley 1273 del 2009

- “La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de Hackers Security.”

Este párrafo va en contra de la ley 1273 del 2009 porque no puede ser la entidad responsable de investigar y juzgar al mismo tiempo ya que para eso se encuentran constituidas.

[6]Congreso de la República, Ley 1273 del 2009. 2020. Disponible en https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

- “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 Hackers Security”.

Se debe adoptar una responsabilidad compartida en donde la compañía esta en todo el derecho de presentar evidencias legales y no solo recaer en las responsabilidades de los receptores

5.2.5. Análisis y revisión de la propuesta laboral con respeto al punto de vista legal y ético

Como respuesta a esta propuesta seria negativa, aunque el beneficio económico es bastante alto a los que normalmente se ven en el país va en contra de las leyes y normas legales que existen en el país, adicional a esto va en contra de la ética profesional ya que viola los derechos de privacidad de terceros dando libre manipulación de la información en donde se vera afectada la integridad, autenticidad y confiabilidad de la información. En el código de COPNIA el cual es el Consejo Profesional Nacional de ingeniería se muestran los artículos los cuales se infringirían en donde se aceptará el contrato.

Articulo 31 – deberes generales de los profesionales, articulo 35 – derechos de los profesionales para con la dignidad de sus profesionales, articulo 37 – deberes de los profesionales para con sus colegas y demás profesionales, articulo 39 – deberes de los profesionales para con sus clientes y el público en general.

5.2.6. Análisis respecto a la noticia del caso “Operativa Andrómeda Buggly” desde su posición teniendo en cuenta los aspectos legales y éticos

Andromeda Buggly fue una operación legitima y encubierta en la cual el ejercito mediante mentiras atraía a personal civil para que realizara actos ilegales, el tema se desbordo porque no se contaba con una ética clara para el actuar tanto de civiles como de militares. En el caso del ejercito es un actuar fuera de la ética, el usar a civiles mientras bien pudieran emplear los mismos fondos de operaciones de engaño a capacitar a funcionarios militares, es aún más falto de ética atraer y engañar con el fin de obtener datos e información de manera claramente abusiva, poniendo en evidencia a civiles que estaban cometiendo delitos informáticos como son la interceptación y robo de datos, crímenes que ya estaban legislados en su momento bajo la ley 1273 de 2009.

Andromeda buggly se encontraba en el barrio galerías de Bogotá en donde tenía como fachada un restaurante, pero en el segundo piso funcionaba un centro de

hackers en donde se enfocaban en extraer información política y confidencial del estado colombiano.

En el caso del ejército de Colombia actuó con muy poca ética ya que engañaban con el fin de obtener datos e información de manera abusiva, poniendo en evidencias a civiles los cuales cometían delitos de interceptación y robo de datos, crímenes que ya fueron judicializados a trabajes de la ley 1273.

5.3. ETAPA 3 EJECUCIÓN DE PRUEBAS DE INTRUSIÓN

5.3.1. Escenario 3

Situación problema: Análisis Red Team

“La primera misión del equipo Red team es lograr identificar porqué medio o proceso se está generando una serie de fuga de información la cual se presenta al interior de la organización en dos de sus equipos de cómputo en la dependencia. La información con la que cuenta usted como experto de ciberseguridad es la siguiente: Los equipos de cómputo de los cuales se sospecha cuentan con Windows 7 X86 y X64, estos equipos tienen un sistema operativo antiguo dado a una aplicación que sólo funciona en dicho S.O. y no pueden ser reemplazados porque la aplicación no está migrada con compatibilidad a otros sistemas operativos. Los equipos de cómputo cuentan con un SMBv1 activo para compartir impresoras y algunos archivos dentro de la red. Al momento de la fuga de información (10 de junio de 2022) 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, además los equipos de cómputo no tienen instalada la actualización MS17-010.

Para agilizar el proceso de investigación Hackers Security facilitará los dos escenarios controlados idénticos al de los equipos de cómputo sospechosos y un escenario controlado con un S.O orientado al testeto de seguridad para que realice el trabajo de investigación sin alterar la infraestructura de producción de la organización; usted como parte de un equipo Red team deben analizar la información suministrada, y seguir los pasos para encontrar si existe un fallo de seguridad a nivel de S.O, validar que vulnerabilidad podría encontrar y posterior a ello buscar el método de explotación por medio de algún framework o exploit. Hackers Security le recuerda que no tienen conocimiento cuál de los dos equipos de cómputo es el que está generando la fuga de información, y mencionan también, que en ocasiones uno de esos dos equipos de cómputo suele mostrar pantalla azul error de Windows de una manera constante. Recuerde que su misión es confirmar y evidenciar las posibles explotaciones paso a paso, el archivo que contiene la información que han estado extrayendo tiene el nombre de “winse20w0.exe”, si usted logra acceder al equipo de cómputo de manera intrusiva deberá encontrar el archivo mencionado y tomar pantalla de la información allí generada, y además

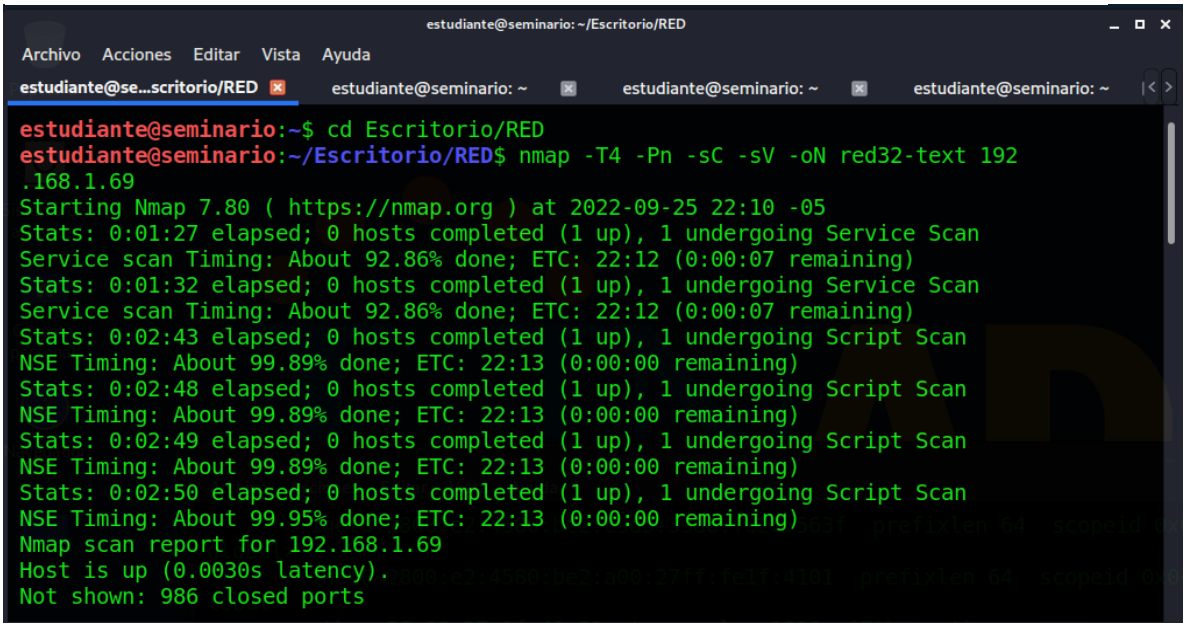
validar por qué uno de esos equipos de cómputo suele mostrar pantalla azul error de windows. Si obtiene esta información podremos decir: BIENVENIDO AL RED TEAM HACKERS SECURITY, este mensaje se destruirá en 3, 2, 1, ... kernel panic....”[7]

El equipo de forense genera una copia del servidor y esta es entregada a usted como experto, debe validar la posible falla de seguridad y si está es explotada debe crear un usuario con su primer nombre y apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC (Prueba de Concepto) ante los altos directivos.

5.3.2. Herramientas y procedimientos utilizados para dar solución al escenario 3 Red Team de acuerdo con los pasos de pentesting

Se realizo un análisis con detenimiento al anexo 4 del escenario 3 en el cual con el uso de la herramienta nmap determinando la ip del equipo en este caso el de 86 bits por ello creamos una carpeta en el escritorio para el guardado del script que arrojara el comando nmap -T4 -Pn -sC -sV -oN red32-text 192.168.1.69 como lo muestra la figura 9, 10 y 11.

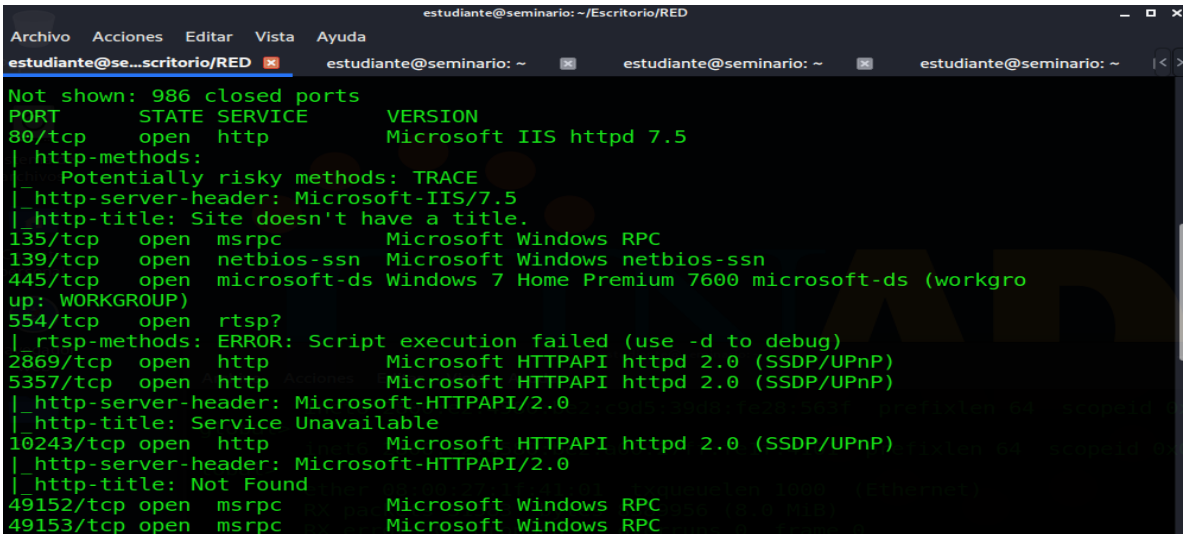
Ilustración 9 Ejecución del comando 1



Fuente: Luis Cardozo

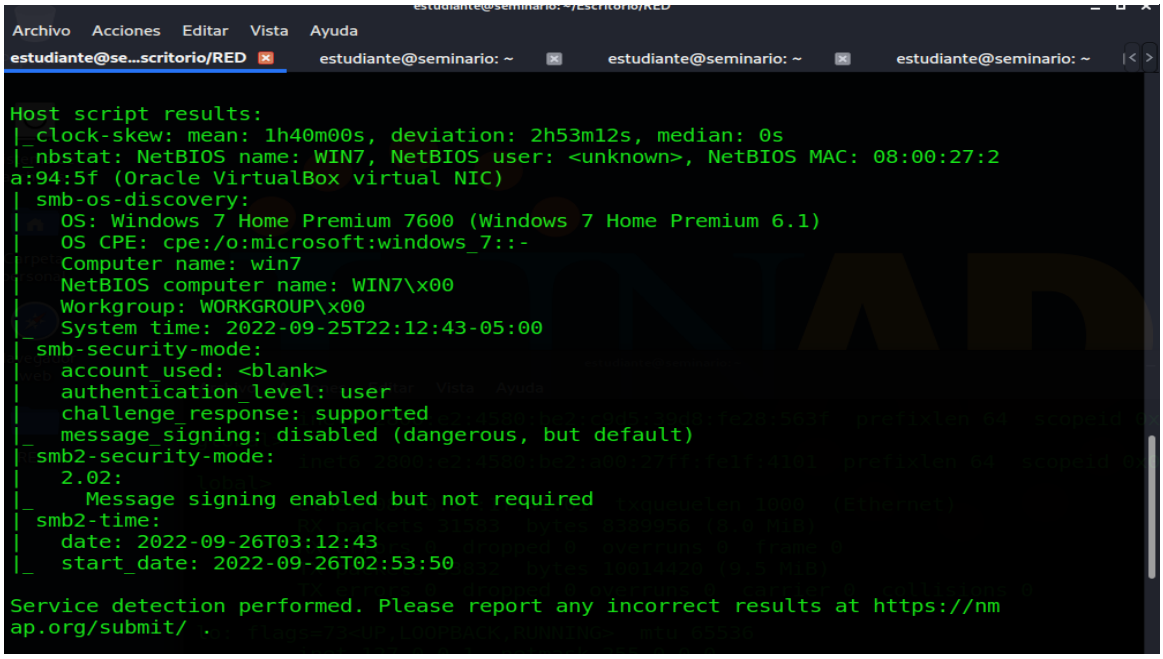
[7] UNAD, Anexo 4 – Escenario 3 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2482/mod_folder/content/0/Anexo%204%20-%20Escenario%203.pdf?forcedownload=1

Ilustración 10 Muestra de puertos abiertos



Fuente: Luis Cardozo

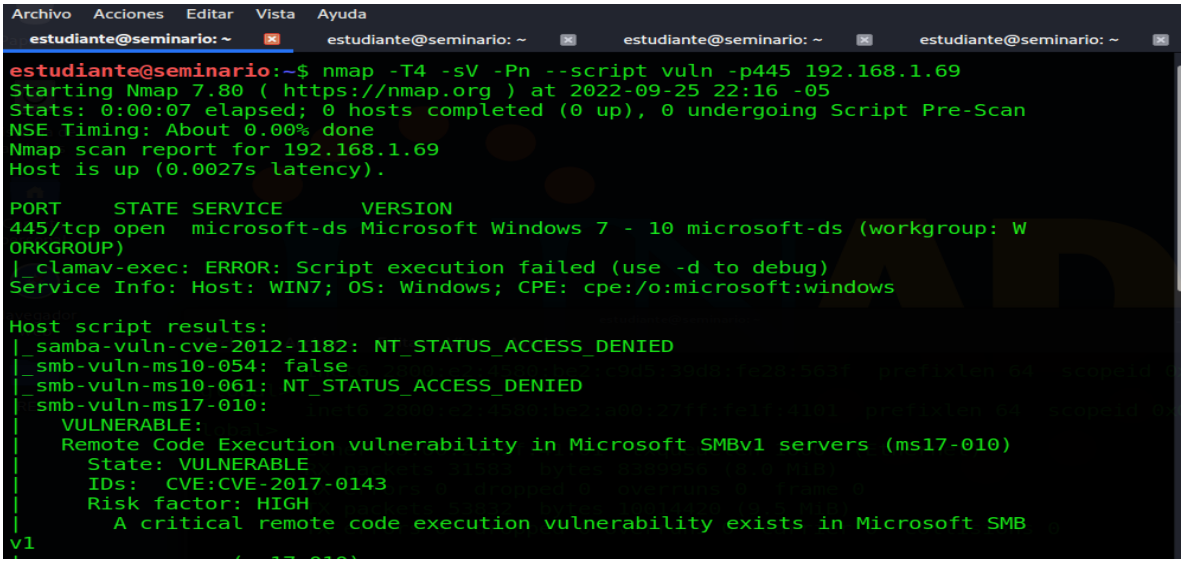
Ilustración 11 Ejecución del comando 3



Fuente: Luis Cardozo

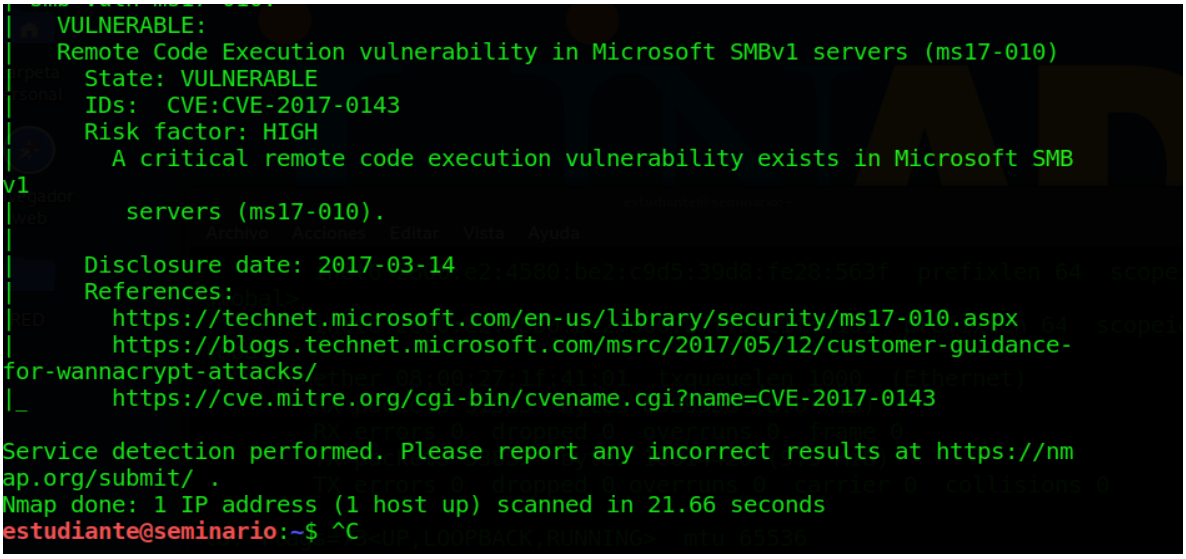
Luego de este comando lo que se realizo es la búsqueda de vulnerabilidades y que quede guardado en un scrip utilizando el software nmap con el siguiente comando nmap -T4 -sV -Pn –script vuln -p445 192.168.1.69, en este comando especificamos el comando 445 el cual es el puerto libre y abierto que vamos a utilizar para hacer el pentesting como lo muestra la figura 12 y 13.

Ilustración 12 Ejecución del comando para vulnerabilidades



Fuente: Luis Cardozo

Ilustración 13 Vulnerabilidades encontradas



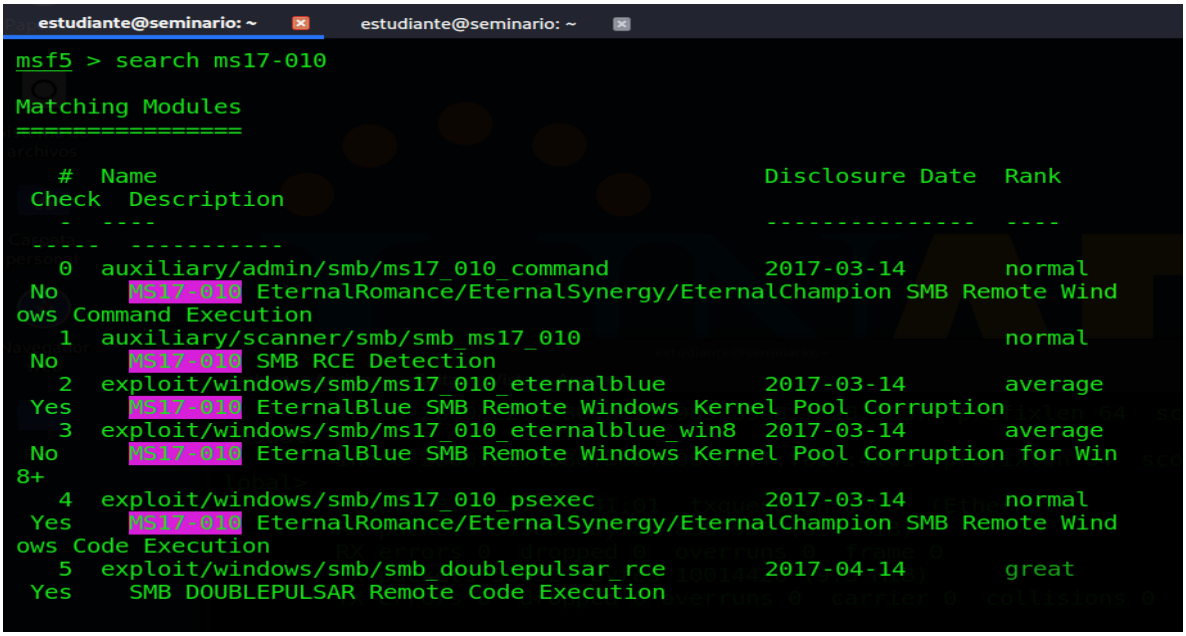
Fuente: Luis Cardozo

Como lo muestra la última imagen encontramos la vulnerabilidad CVE-2017-0143 el cual nos indica el anexo 4 por ello procederemos a iniciar el software metasploit v5.0.94 como lo muestra la figura 14. Luego se procede con la búsqueda del ms17-010 con el comando search, después muestra los exploit que se pueden utilizar para esta vulnerabilidad dependiendo del sistema como lo muestra la figura 15.

Ilustración 14 Inicio de Metasploit

Fuente: Luis Cardozo

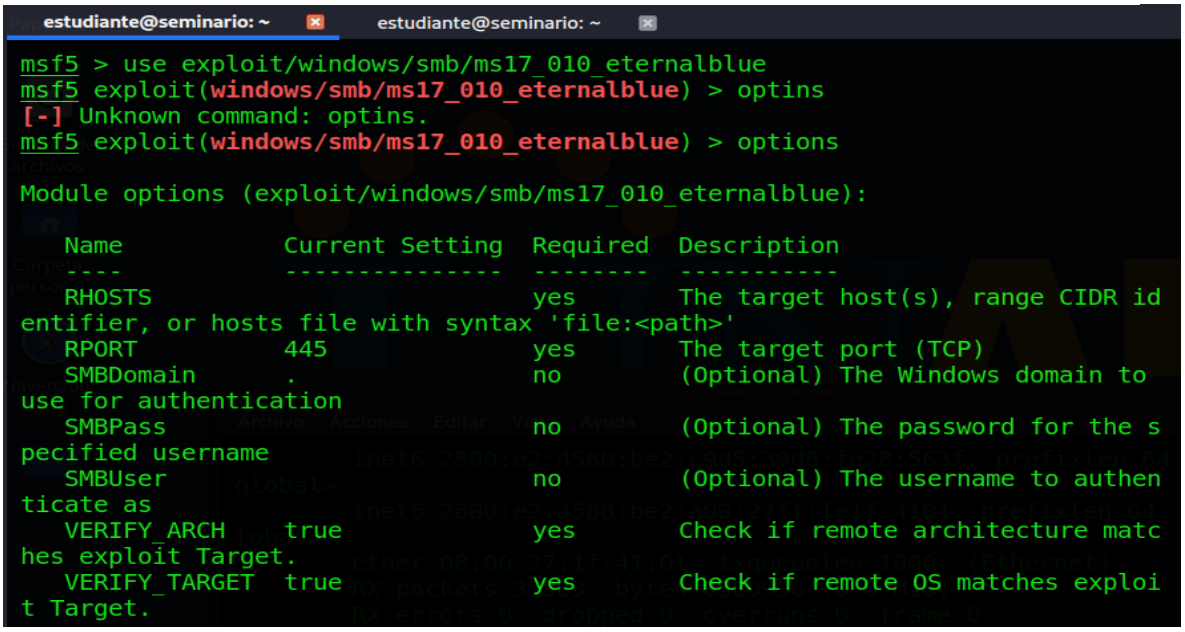
Ilustración 15 Búsqueda del exploit



Fuente: Luis Cardozo

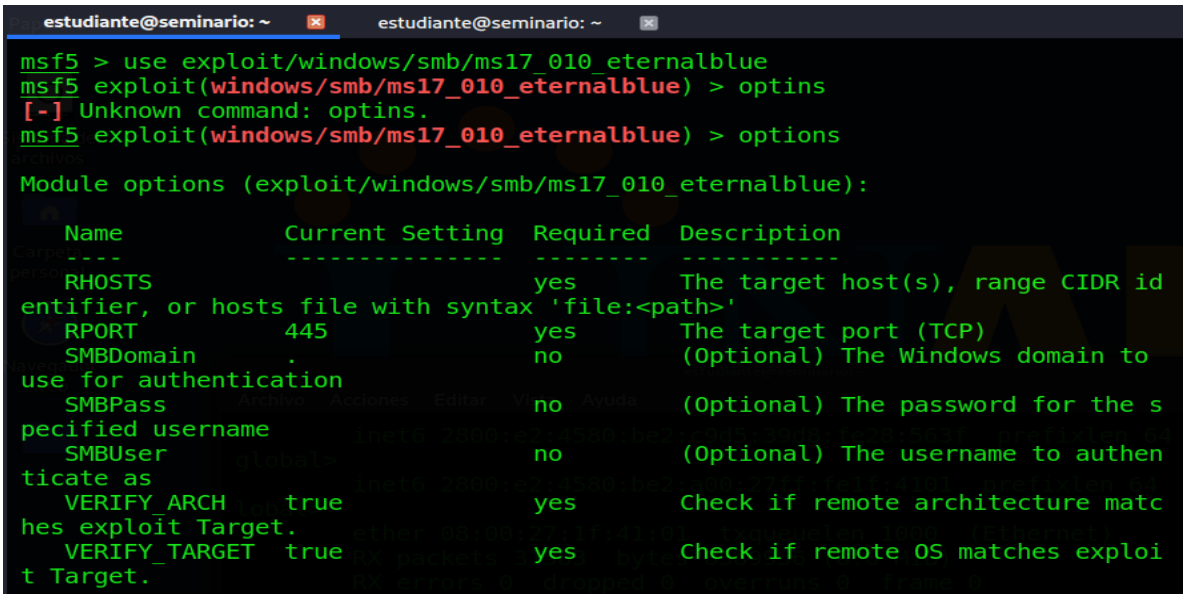
Luego de esto se selecciona el exploit en este caso el eternalblue como lo muestra la figura 16 y se ingresa a las opciones en donde se ingresará el puerto, ip del equipo a atacar, ip del equipo atacante y el payload como lo muestra la figura 17.

Ilustración 16 Selección del exploit



Fuente: Luis Cardozo

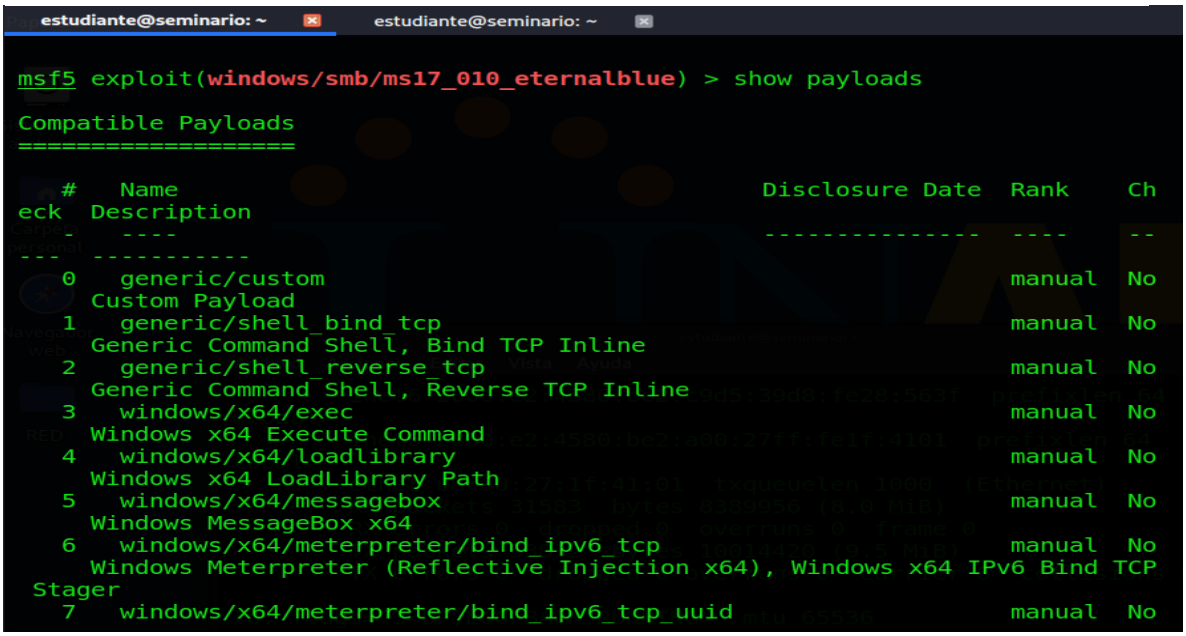
Ilustración 17 Opciones del Exploit



Fuente: Luis Cardozo

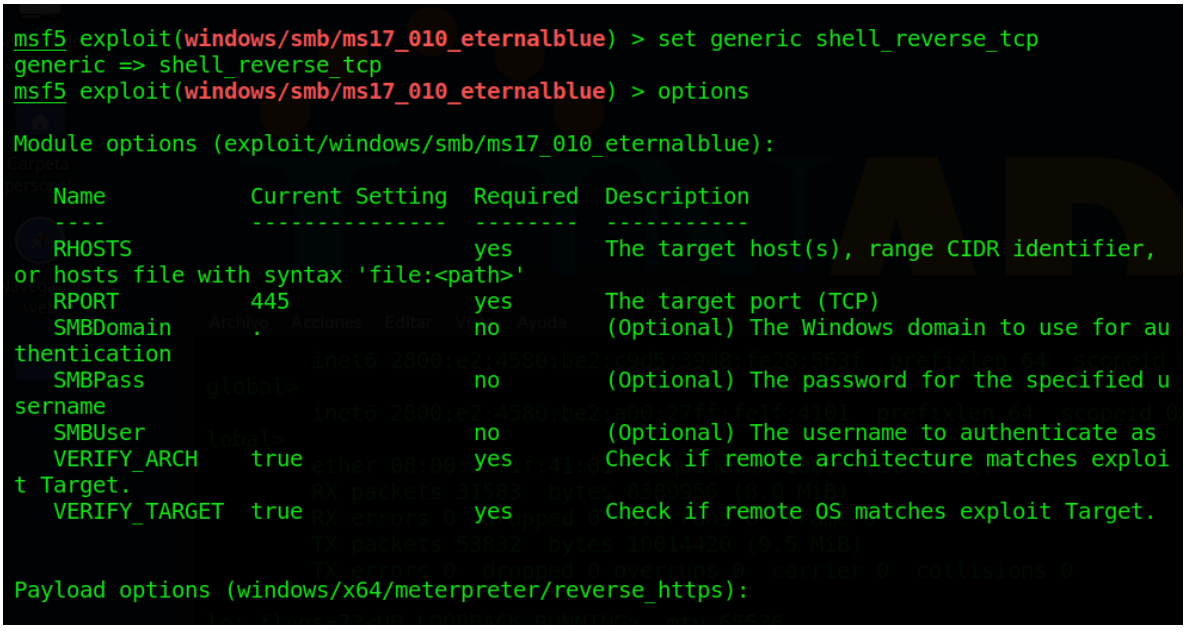
Luego se debe seleccionar el payloads que se va a utilizar, es de recordar que como la maquina es de 86 bits se debe seleccionar uno de acuerdo a su arquitectura como lo muestra la figura 18 y 19

Ilustración 18 Búsqueda de payloads



Fuente: Luis Cardozo

Ilustración 19 Selección de payloads

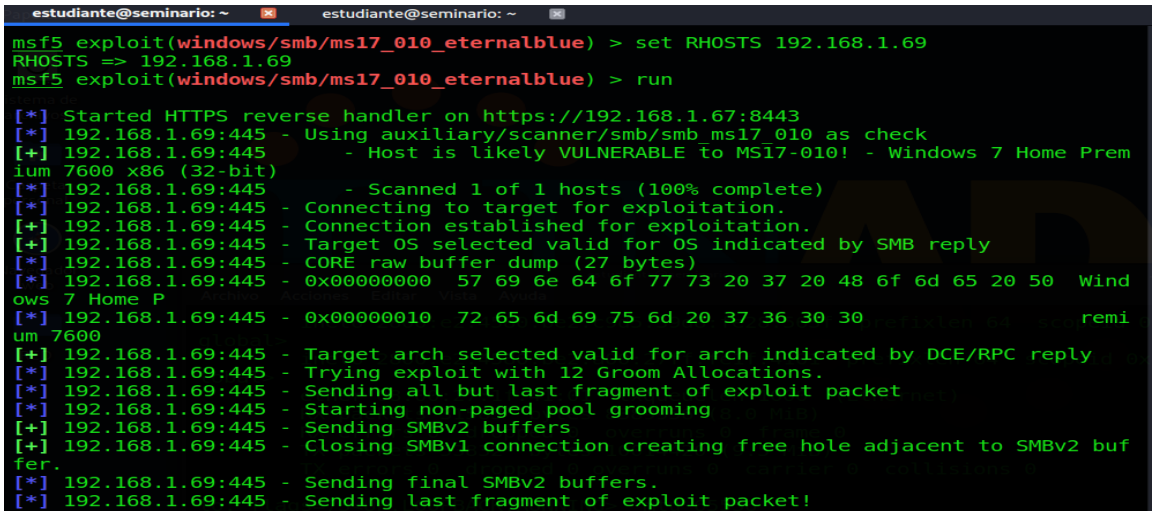


Fuente: Luis Cardozo

Después se inicia el proceso como lo muestra en la figura 20 y después de un tiempo la maquina se reinicia con la pantalla azul como se muestra en al figura 21, esto es porque los payloads que se tienen no son de acuerdos a la arquitectura de 86 bits del sistema operativo por ello nos arroja error failled al momento de realizar la

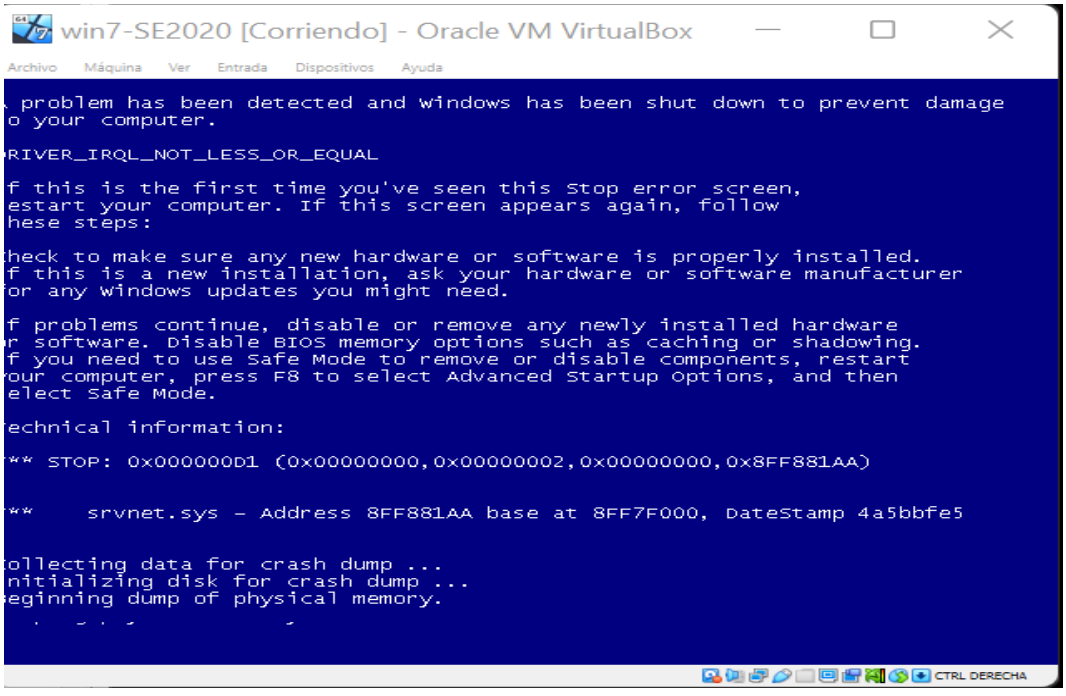
conexión con el atacado como lo muestra la figura 22 y 23 pero comprobamos que si hemos podido ingresar ya que la maquina se realice, por ello es necesario la búsqueda de nuevos payloads para poder comprobar el ataque correctamente.

Ilustración 20 Inicio del proceso



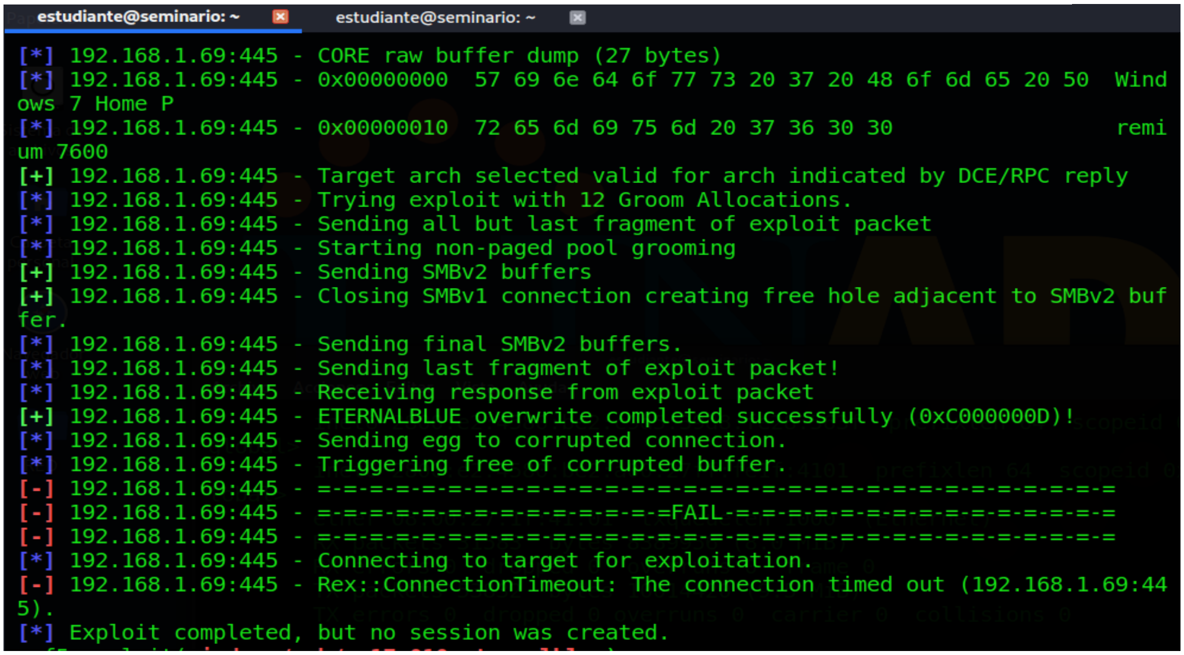
Fuente: Luis Cardozo

Ilustración 21 Pantalla azul equipo atacado



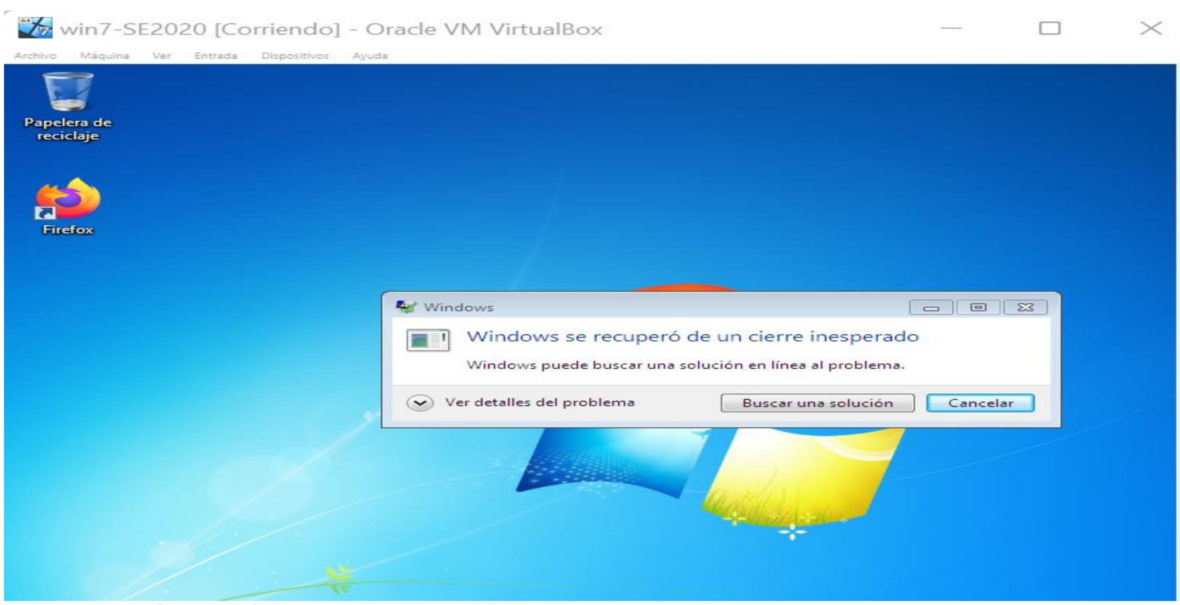
Fuente: Luis Cardozo

Ilustración 22 Ataque Fallido



Fuente: Luis Cardozo

Ilustración 23 Equipo con error de cierre o reinicio

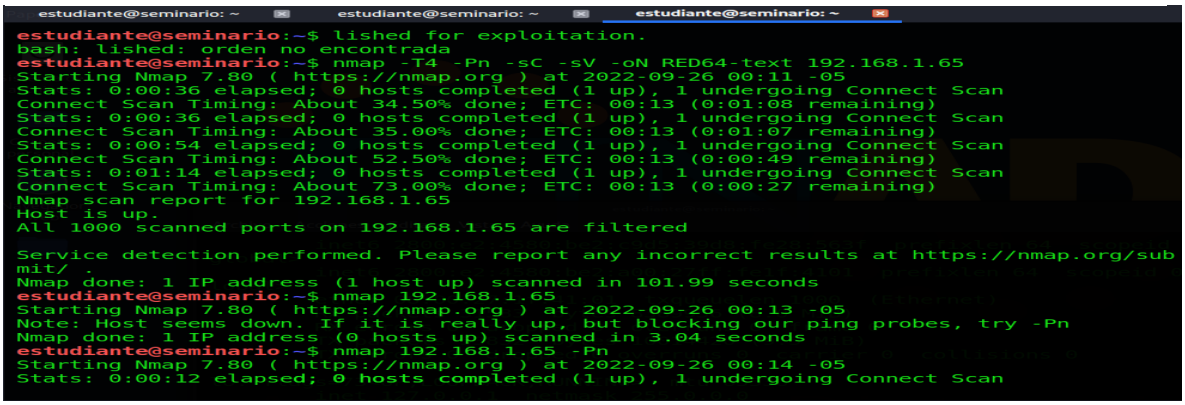


Fuente: Luis Cardozo

5.3.3. Datos e información del escenario 3, utilizados para identificar el fallo de seguridad especifico, el cual ataca a la máquina Windows 7X64

Se realizo el análisis de las vulnerabilidades y puertos abiertos dentro del sistema operativo Windows 7 de 64 bits como lo muestra la figura 24 pero en donde evidenciamos que no se encuentra ninguna vulnerabilidad

Ilustración 24 Análisis de vulnerabilidades Windows 7 64 Bits



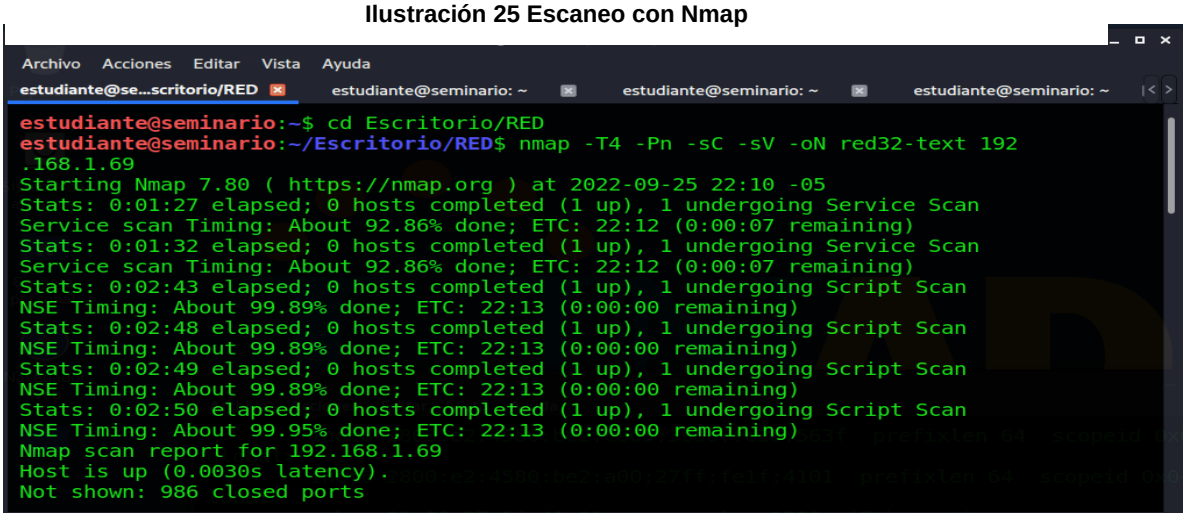
Fuente: Luis Cardozo

Se realizaron diferentes pruebas en donde todas se evidencio de que no se encuentran puertos disponibles con diferente software

5.3.4. Herramienta utilizada para identificar los fallos de seguridad de la maquina Windows 7 86 bits

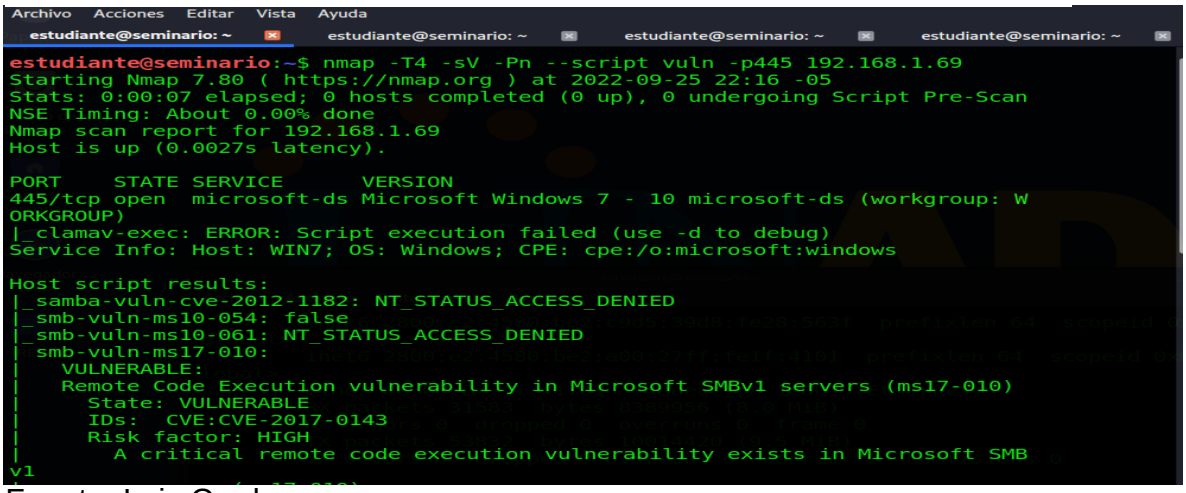
Se utilizo el software nmap para identificar los fallos de seguridad y vulnerabilidades que se encuentran en cada uno de los sistemas operativos como lo muestra en la figura 25 y 26. Adicional a esto se identificó que la vulnerabilidad encontrada en el anexo es la misma del puerto 445 por ello se tomó y se implementó para el pentesting como lo muestra la figura 27

Ilustración 25 Escaneo con Nmap



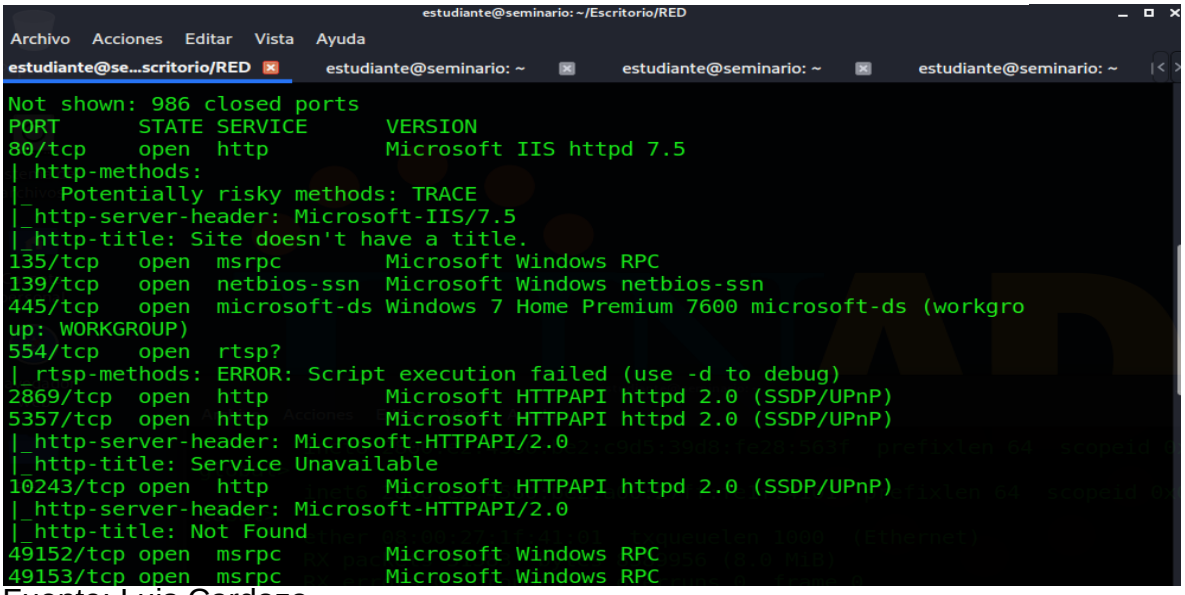
Fuente: Luis Cardozo

Ilustración 26 Vulnerabilidades con Nmap



Fuente: Luis Cardozo

Ilustración 27 Puerto disponible en Nmap

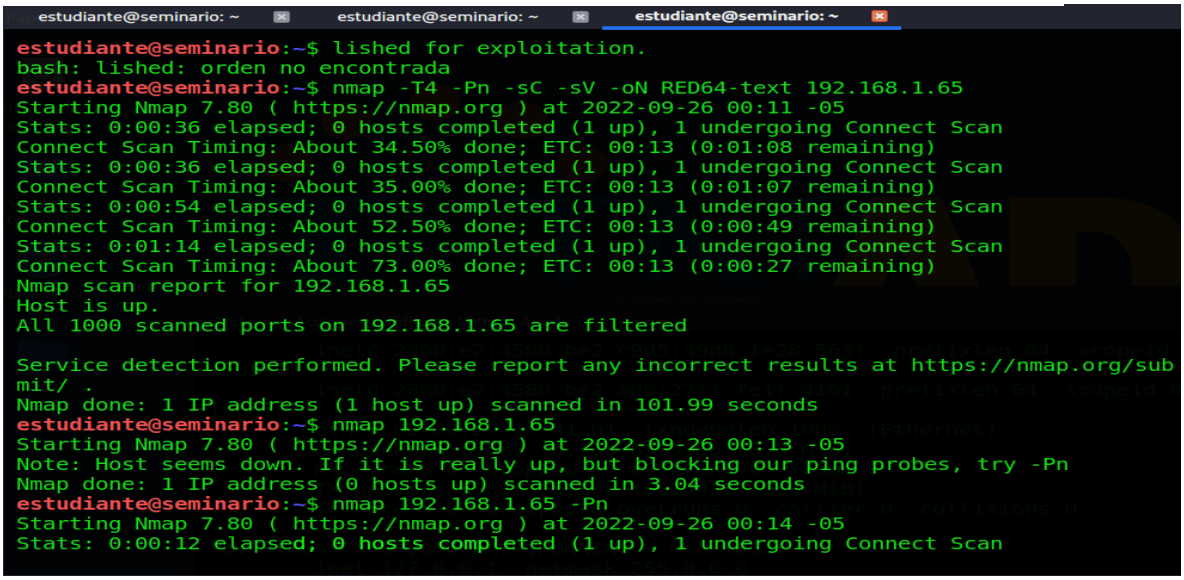


Fuente: Luis Cardozo

5.3.5. Como afecta el ataque a la máquina Windows 7X64

Se realizo el análisis de vulnerabilidades y se evidencio que no tiene ninguna vulnerabilidad ni puerto disponible para poder realizar el pentesting como lo muestra la figura 28.

Ilustración 28 Escaneo de puertos Windows 7 64 Bits



Fuente: Luis Cardozo

5.3.6. Pasos para el explotar la vulnerabilidad

Se realizo los siguientes pasos para explotar la vulnerabilidad de la maquina Windows 7 86 bits.

- Analizar los puertos disponibles
- Analizar las vulnerabilidades
- Búsqueda de la vulnerabilidad y como atacarla
- Iniciar el metasplotable
- Buscar el exploit para atacar la vulnerabilidad
- Seleccionar el payload
- Ingresar la ip del equipo atacado y el atacante
- Seleccionar el puerto
- Iniciar el ataque
- Ataque completado

5.4. ETAPA 4 CONTENCIÓN DE ATAQUES INFORMÁTICOS

5.4.1. Escenario 4

Situación problema: Análisis Blue Team

“Hackers Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel

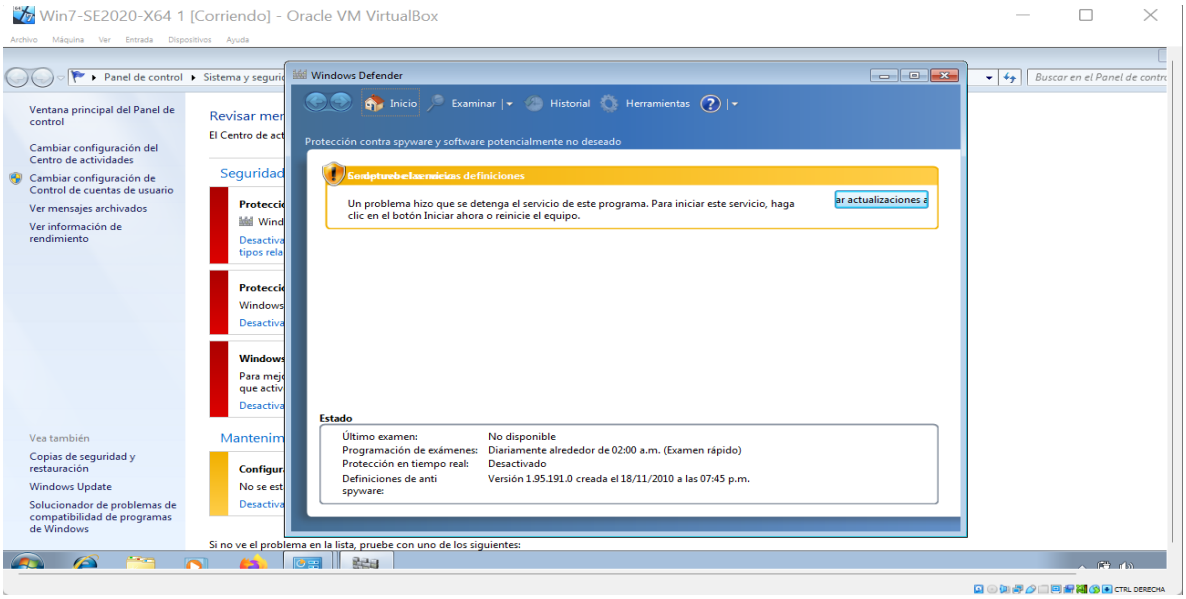
técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. Hackers Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL”[8].

5.4.2. Análisis con acciones necesario para contener un ataque en tiempo real

Como primera medida se debe realizar validaciones con el área de Red Team para validar cuales con las vulnerabilidades que tiene el equipo Windows 7 64 Bits. Después de este análisis junto con Red Team se encontró el firewall y antivirus en estado inactivos como lo muestra la figura 29.

Figura 29. Antivirus desactivado

Ilustración 29 Antivirus desactivado

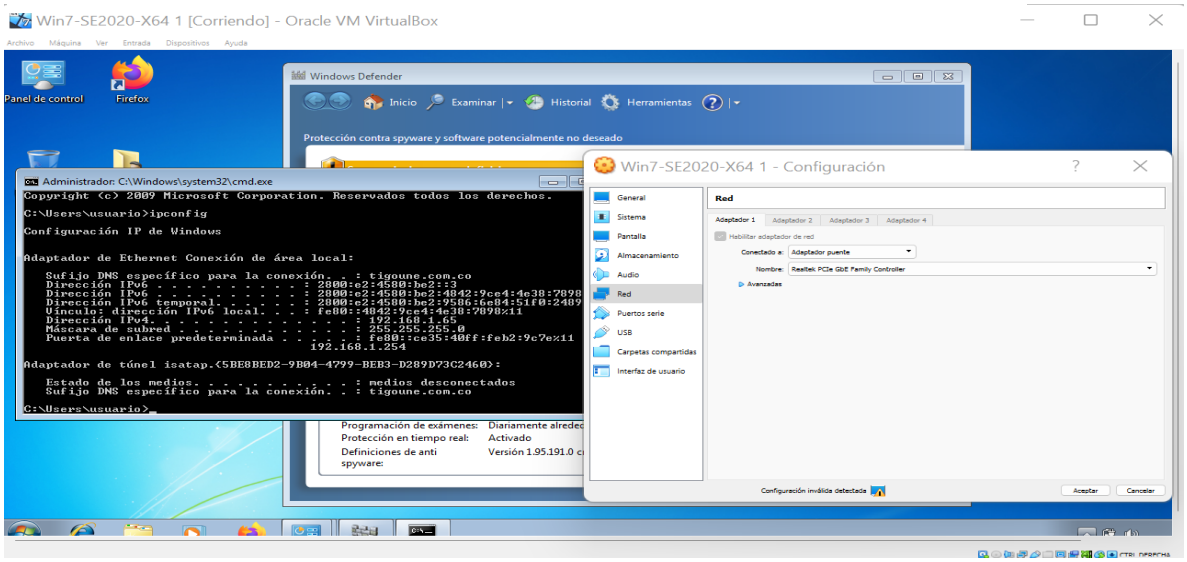


Fuente: Luis Cardozo

Luego se debe validar la red de la maquina windows 7 de 64 Bits en donde encontramos que trabaja como adaptador puente como lo muestra la figura 30.

[8] UNAD, Anexo 5 – Escenario 4 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2411/mod_folder/content/0/Anexo%205%20-%20Escenario%204.pdf?forcedownload=1

Ilustración 30 Estado de red desde equipo



Fuente: Luis Cardozo

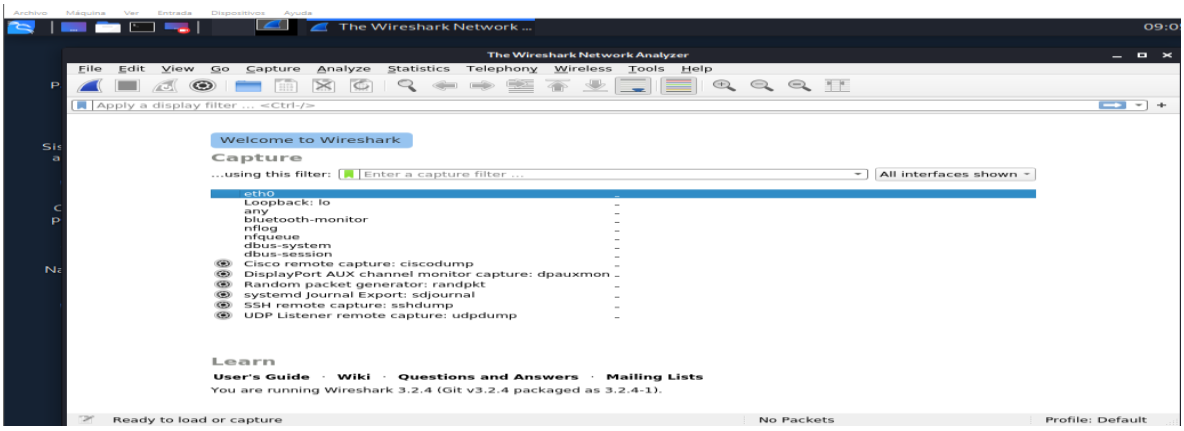
Después de validar el estado de la red la mejor opción es realizar un análisis con un software llamado Wireshark el cual es un snnifer en donde puede capturar datos de paquetes, decodificar y mostrar los cambios de cada paquete, adicional es también usado para validar el estado de ancho de red y las saturaciones de cada una, este software es una herramienta de gran ayuda para analizar problemas en la red, detección de intentos de explotación en donde sirve para alejar los sistemas atacados o explotados y así monitorear el uso de estos sistemas.

En este caso se utilizará el software Wireshark directamente desde el sistema Kali Linux entregado para el desarrollo del proyecto en donde se va a realizar una verificación de la red y los paquetes que hay en el tráfico de esta red, verificar el tipo de ataque que está teniendo el equipo víctima y los datos que tratan de extraer como lo muestra en la figura 31,32 y 33.

Ilustración 31 Kali Linux

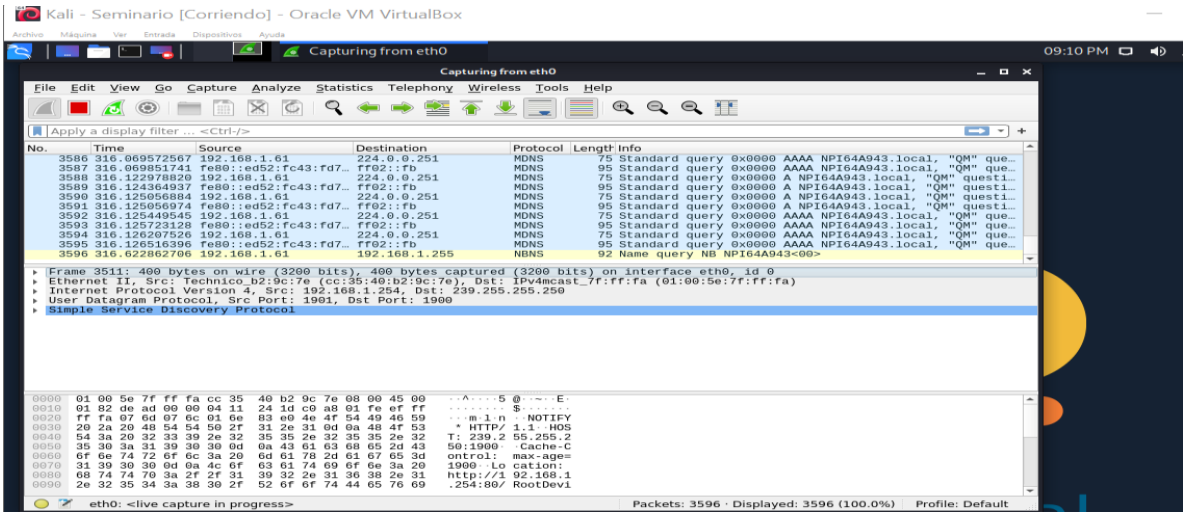
Fuente: Luis Cardozo

Ilustración 32 Wireshark realizando escaneo



Fuente: Luis Cardozo

Ilustración 33 Reporte de Wireshark

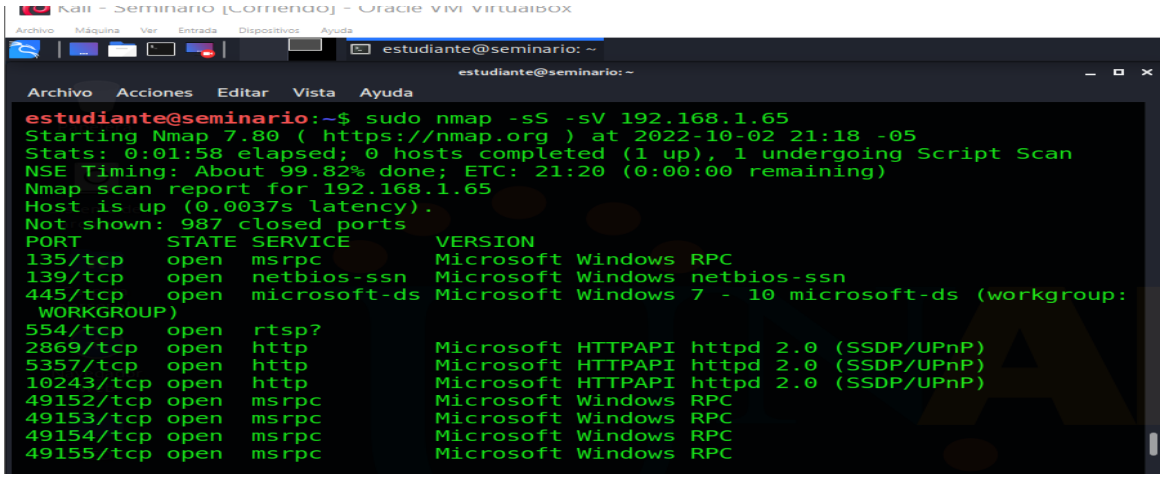


Fuente: Luis Cardozo

Lo más importante es habilitar firewalls y antivirus en todo momento cuando se encuentre en una situación de ataque ya que la idea es resguardar la información e identificar y subsanar la vulnerabilidad por la cual están atacando todo esto actualizando el sistema operativo a su última actualización reduciendo vulnerabilidades y en especial tener el antivirus activo esto con el fin de reducir los riesgos.

Luego de realizar el informe de los puertos y vulnerabilidades el cual realiza el equipo de Red Team, se procede a bloquear esos puertos informados con el software nmap dentro de la maquina Windows 7 64 bits de acuerdo con las vulnerabilidades como lo muestra la figura 34.

Ilustración 34 Análisis con Nmap



Fuente: Luis Cardozo

5.4.3. Acciones de hardenización a implementar para evitar ataques de seguridad informática

De acuerdo con el ejercicio que se ejecutó con el área de Red Team se deben tener en cuenta varios aspectos como tener los sistemas operativos de los equipos completamente actualizados para evitar cualquier vulnerabilidad de estos, antivirus y firewalls activos actualizándose en tiempo real.

Se propone las siguientes medidas en cada sistema operativo como harderización:

- Ingresos de contraseñas caducables, robustas y que tengan sus intentos fallidos de inserción para bloqueo al sistema como para los archivos de información y datos.
- Instalación de sistemas operativos de forma segura con particiones en los discos duros o discos sólidos, esto con fin de separar los archivos de información y datos en otra partición aislándolos del sistema, software y herramientas necesarias para trabajar en el sistema operativo.
- Habilitación de usuarios genéricos en el sistema, adicional se debe renombrar el usuario administrador y eliminar la cuenta local que no se utilicen con el fin de limitar los privilegios de cuentas que estén activas.
- Implementar listas de programas permitidos y no permitidos, restricciones de software, listas negras y blancas.
- Limitación de carpetas compartidas adicional subirles el nivel de complejidad a las contraseñas de accesos a estas redes.
- Realizar bloqueo de puertos que no sean utilizados con el fin de limitar las puertas abiertas para servicios que no se usen.
- Inhabilitar los accesos remotos para todos los equipos que no sea requerido, habilitar los canales cifrados como SSH como el acceso limitado para los usuarios.

- Respaldar la información en unidades físicas fuera de la red de los equipos de información.

5.4.4. Análisis sobre las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos

Los equipos de respuesta para incidentes informáticos o también llamados SCIRT son conformados por personal de la compañía que sufren los incidentes, verifican las vulnerabilidades y los procesos de contención de estas. Tiene como ventajas saber en tiempo real las situaciones que se deben verificar, pero al igual tiene como desventaja que puede filtrar información en donde sería una gran diferente a los diferentes equipos como el Blue Team, que al momento de ser externo la posibilidad de corruptibilidad del proceso es mínima.

Los equipos de Blue Team son agentes externos a la empresa en donde se contratan para funciones básicas de como contener y mantener la ciberseguridad de los sistemas de información de la compañía que contrata al igual trabajan de la mano con el equipo de Red Team los cuales les entregan el insumo que encuentran en los ataques o intrusiones controladas

5.4.5. Análisis sobre las pertinencias de trabar con CIS “Center For Internet Security” como propuesta de aseguramiento por parte de un equipo de Blue Team

El center For Internet Security sería buena opción para el establecimiento de prioridades y actividades a desarrollar en los procesos de contención por ello sería muy buena opción utilizarlo.

Como primera medida para tener en cuenta es que debe ser una organización sin fines de lucro los cuales van encaminado en la ciberseguridad, este tiene el fin de no depender económica ni corporativamente de una empresa o compañía.

Los controles Cis o también llamados Cneter For Internet Securiy permiten crear listas o acciones para realizar en los procesos de contenidos en ataques, al igual recomendaciones en los hardware y software en llegado el caso de desconocimiento, también el aprovechamiento de la comunidad de personas y empresas para la mejora continua de la seguridad, esta se debe usar anónimamente para no hacer pública la información de la compañía que contrata los servicios de Blue Team.

Para la implementación se deben realizar un conjunto de acciones priorizada y en orden cronológicos dado que solamente buscan el conocimiento en común y la protección de los sistemas de información

5.4.6. Análisis sobre las funciones y características principales de un SIEM

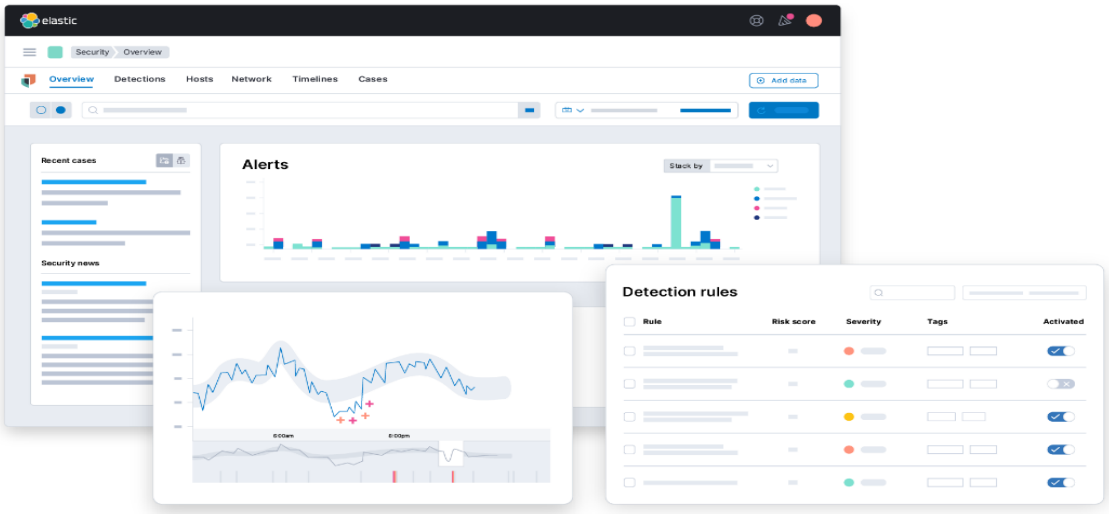
La Gestión de Eventos e Información de Seguridad o SIEM es el conjunto de tecnologías que permiten la gestión de eventos de seguridad y la gestión de información de seguridad.

Es un software de gestión en donde se centraliza la información de las amenazas de ciberseguridad de las redes y equipos de cómputo mediante priorizaciones de amenazas y estándares de datos.

El SIEM busca patrones fuera de lo común del funcionamiento para así encargase en los recursos de seguridad anormal como lo muestra la figura 35. Tiene varias ventajas al momento de la implementación de un programa SIEM las cuales depende de la inversión económica y los alcances[9].

- Automatizar tareas
- Centralizar la información de seguridad
- Disminur tipos de detección de ataques
- Respuesta de manera automática para amenazas o eventos
- Análisis a los logs en tiempo real
- Mejoramiento en el manejo del riesgo
- Detección de activos
- Monitoreo de comportamientos
- Evaluación de vulnerabilidades

Ilustración 35 SIEM



Fuente: Luis Cardozo

[9] Team, Ambit. 2019. Significado de Siem y como funciona. Disponible en https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

5.4.7. Elección de herramientas que permitan contener ataques informáticos

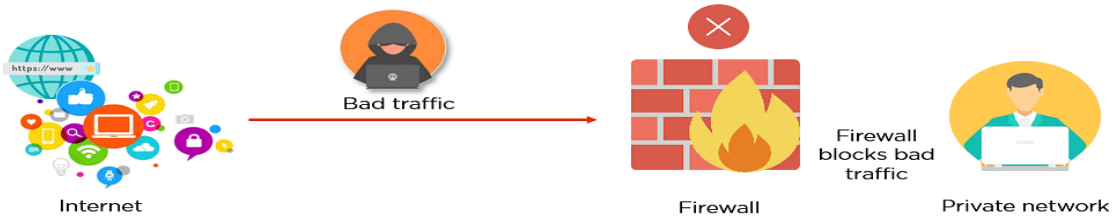
A continuación, se informará 3 herramientas que permite contener los ataques informáticos junto con su descripción y observaciones que se describieron en el escenario propuesto.

5.4.7.1. Firewalls

Una de las principales herramientas es el firewall el cual es primera contención el cual impide el acceso como la salida de la red a diferentes paquetes de datos que no cumplen con las normas de seguridad establecidas en la configuración, el firewall al recibir peticiones no habituales o sospechosas bloquean los puertos como lo muestra en la figura 36 y realizan un aislamiento a los equipos y direcciones ip con una configuración programada o asignada previamente.

Los firewalls normalmente vienen instalados en los router administrables o software que simulan el comportamiento de un firewall de hardware, normalmente estos vienen preconfigurados en los cuales el usuario puede establecer el nivel de dureza para la protección de la red.

Ilustración 36 Firewalls



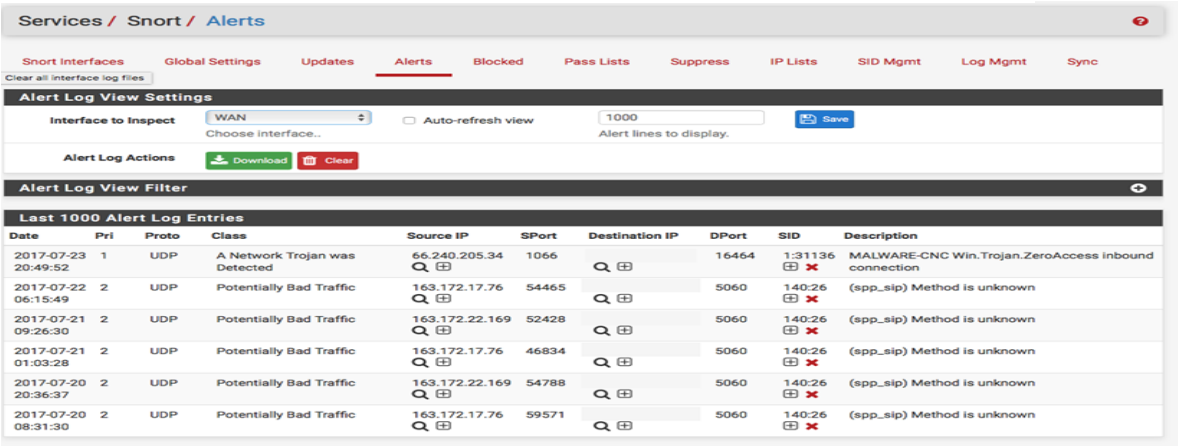
Fuente: Google Imágenes

5.4.7.2. Snort

(Sistema de Detección de Intrusos) el cual es Open Source, este software ayuda al monitoreo y detección de intrusiones a la red el cual utiliza patrones de ciberataques ya conocidos. Este software es muy utilizado con reglas y filtros los cuales se configuran desde la instalación, tiene como ventaja que puede ser utilizado como esnifer para ver el tráfico de los paquetes desde la consola en modo automático o semiautomático. Este software es muy utilizado por los equipos de Blue Team para las contenciones de los ataques como lo muestra la figura 37.

Es un software muy poco pesado y permite el análisis en tiempo real con uso de filtros y detecciones de strings.

Ilustración 37 Snort



Fuente: Luis Cardozo

5.4.7.3. DMZ

La tercera herramienta llamada DMZ es una herramienta muy importante también llamada zonas desmilitarizadas hace parte de una red aislada que se encuentra dentro de la red interna de la compañía, normalmente se encuentran los servicios y recursos que necesitan accesibilidad en internet como los servidores de correos y web.

Los DMZ tienen como características no permitir conexiones que van desde el DMZ local, pero si permite conexiones desde internet, esta busca que los servicios de red los cuales son más susceptibles permitan una mejora en la información, ayuda a la mejora de contención de posibles ataques los cuales no van a ser comprometidos en la red local, tiene como ayuda al igual que los firewalls también pueden ser utilizados desde hardware como software.

5.5. ETAPA 5 SOCIALIZACIÓN DE INFORME TÉCNICO

5.5.1. Escenario 5

Situación problema: Análisis final

“The WhiteHose Security desea un informe técnico donde se plasme el proceso de los escenarios propuestos en cada una de las acciones como Blue team, Red team y aspectos legales que logró usted como experto en Ciberseguridad dentro del período de prueba de la organización. El informe es solicitado para ser analizado por los analistas Seniors en Seguridad con los que cuenta WhiteHouse Security,

esto ayudará al proceso de selección de los expertos que harán parte de esta prestigiosa organización”[10].

[10] UNAD, Anexo 6 – Escenario 5 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2414/mod_folder/content/0/Anexo%206%20-%20Escenario%205.pdf?forcedownload=1

6. CONCLUSIONES

Un profesional en seguridad informática debe estar completamente actualizado, comprender y conocer sobre cada una de las leyes vigentes con sus decretos relacionados con los delitos informáticos y protección de datos personales, así mismo conocer cuáles son los códigos de ética para la entidad COPNIA el cual inspecciona, controla y vigila cada ingeniero.

Con el desarrollo de este informe llevado a cabo a través de la empresa Hackers Security damos como conclusión que el contrato y acuerdo de confidencialidad son ilegales ya que van en contra de los reglamentos legales y éticos para los profesionales de ingeniería, dado que estos documentos muestran la forma inadecuada de la información y el ocultamiento de procesos los cuales van en contra de las leyes y viola el código de COPNIA.

Se realizaron análisis con diferente software de manera gratuita como lo son Nmap, Metasploit y wireshark los cuales fueron de gran ayuda dado la cantidad de opciones que trae cada uno de ellos, es muy importante informar que con la ayuda de estos aplicativos se busca la implementación de un sistema de seguridad informática más eficiente para la compañía analizando cada sistema de información presentado en los escenarios.

7. RECOMENDACIONES

De acuerdo con el informe técnico presentado se realizarán las siguientes recomendaciones con el fin de mejorar cada una de las estrategias de Red Team y Blue Team.

- Se deben realizar continuamente actualizaciones tanto en los sistemas operativos, software, servidores y en los firmwares de los dispositivos de la organización ya que esto ayuda a disminuir los riesgos de seguridad en la compañía.
- Se deben establecer restricciones para la instalación de software sin autorización, ya que esto puede influir en el robo de información a través de programas maliciosos, por ello se recomienda organizar políticas de seguridad.
- Realizar continuamente auditorías internas y análisis de vulnerabilidades para minimizar el riesgo de inseguridad en la red de la compañía
- Obtener asesoría jurídica permanente con el fin de estar relacionados a las nuevas leyes y actualizaciones jurídicas en el campo de la seguridad.
- Establecer manual de políticas de seguridad y buenas prácticas con el fin de restringir cualquier tipo de software mal intencionado y bajar el riesgo de amenazas.

8. BIBLIOGRAFÍA

Congreso de la República, Ley 1273 del 2009. 2020. Disponible en https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

COPNIA, Republica de Colombia, 2020. Disponible en https://www.copnia.gov.co/

Cortes, Sandra. 2021. CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM. Disponible en https://repository.unad.edu.co/jspui/bitstream/10596/50306/1/secortesc.pdf

Helpsystems, 2021. Las seis fases de pentesting. Disponible en https://www.helpsystems.com/es/blog/las-seis-fases-del-pentesting

KeepCoding, 2022. Ciberseguridad. Disponible en https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad

OffSec, services. Kali Linux, Software de testeos. Disponible en https://www.kali.org/gg

ORACOL. Virtual Box. Máquina virtual. Disponible en https://www.virtualbox.org/

UNAD, Anexo 1 – Escenario 1 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2481/mod_folder/content/0/Anexo%201%20-%20Escenario%201.pdf?forcedownload=1

UNAD, Anexo 2 – Escenario 2 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2409/mod_folder/content/0/Anexo%202%20-%20Escenario%202.pdf?forcedownload=1

UNAD, Anexo 3 – Acuerdo PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2409/mod_folder/content/0/Anexo%203%20-%20Acuerdo.pdf?forcedownload=1

UNAD, Anexo 4 – Escenario 3 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2482/mod_folder/content/0/Anexo%204%20-%20Escenario%203.pdf?forcedownload=1

UNAD, Anexo 5 – Escenario 4 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2411/mod_folder/content/0/Anexo%205%20-%20Escenario%204.pdf?forcedownload=1

UNAD, Anexo 6 – Escenario 5 PDF. 2022. Disponible en https://campus112.unad.edu.co/ecbti111/pluginfile.php/2414/mod_folder/content/0/Anexo%206%20-%20Escenario%205.pdf?forcedownload=1

Rodriguez, S. 2009. Ceupe. Disponible en https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html

Security, D. 2013. PowerData. Disponible en https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/234655/la-autenticaci-n-de-usuarios-para-proteger-datos-sensibles

Smith, T. 2021. QuickHash. Disponible en https://www.quickhash-gui.org/

Team, Ambit. 2019. Significado de Siem y como funciona. Disponible en https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

Veritas, Bureau. 2021. Red team y Blue team. Disponible en https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

9. ANEXOS

9.1. Anexo A. Enlace Video

https://www.youtube.com/watch?v=q-Oa7vKzDeA