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

CLAUDIA LÓPEZ ARBOLEDA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
POPAYAN CAUCA
2021

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

CLAUDIA LOPEZ ARBOLEDA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

DIRECTOR:
M. SC. JOHN FREDDY QUINTERO

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
POPAYAN CAUCA
2021

RESUMEN

El documento presentado a continuación contiene el informe final realizado para el Seminario Especializado Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team, tomado como opción de grado para la Especialización en Seguridad Informática, de la Universidad Nacional Abierta y a Distancia UNAD.

Este documento tiene por objeto resaltar las diferencias existentes en los equipos Red Team y Blue Team que permitan especificar las responsabilidades y roles que se deben realizar al interior de una organización, esto por medio de estudios de caso solicitados en los anexos con escenarios de la vida diaria referentes a seguridad informática.

Para desarrollar este informe final se tendrán cinco fases:

1. Conceptos de equipos de Seguridad.
2. Actuación ética y legal.
3. Ejecutar pruebas de Pentesting.
4. Contención de ataques informáticos.
5. Socialización de informe técnico.

En la primera fase se identifica el problema a desarrollar y se configura la infraestructura que se va a utilizar en todo el procedimiento. En la segunda fase se desarrolla la propuesta de contrato de confidencialidad de la empresa WhiteHouse Security, bajo criterios legales y éticos. En la fase tres se muestran las posibles vulnerabilidades que puedan estar ocurriendo en los sistemas de información utilizando herramientas y técnicas de Pentesting. Para la cuarta fase se proponen estrategias de contención por medio del análisis de riesgos y vulnerabilidades en la infraestructura TI de la organización. La quinta fase corresponde al 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 se lograron dentro del período de prueba de la organización.

TABLA DE CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

GLOSARIO

ATAQUE INFORMÁTICO: Forma de acceder ilegalmente a un sistema informático, utilizando las debilidades o fallas que se presentan a nivel software, hardware o el componente humano, con el objetivo de extraer información, producir daños o alterar el funcionamiento de un sistema.

BLUE TEAM: Equipo de seguridad caracterizado por brindar proactivamente seguridad a organizaciones frente a ataques informáticos, encargándose de la búsqueda e identificación permanente de vulnerabilidades y fallas de seguridad, y verificar la efectividad de cada medida de seguridad implementada.

CIBERDELINCUENTE: Persona con conocimientos y habilidades técnicas capaz de acceder a sistemas informáticos vulnerables para realizar actividades delictivas como el robo, secuestro y destrucción de información, provocando daño o anulación de los sistemas.

CIBERSEGURIDAD: Conjunto de acciones de carácter preventivo enfocadas a proteger y defender los sistemas informáticos y las redes de datos de los ataques maliciosos que coloquen en riesgo la información.

COPNIA (CONSEJO PROFESIONAL NACIONAL DE INGENIERÍA): Organismo Colombiano de carácter público, encargado de controlar, inspeccionar y vigilar el ejercicio de las actividades de ingeniería.

EXPLOIT: Programa informático o fragmento de software que se utiliza para explotar o aprovechar fallos de seguridad presentes en un sistema o aplicación.

FIREWALL: Herramienta que ayuda a proteger una red interna doméstica o de una organización, contra atacantes o intrusos no autorizados que quieran acceder a ella desde una red externa como Internet.

HARDENING: Proceso de endurecimiento o fortalecimiento de los sistemas para reducir vulnerabilidades y evitar amenazas o ataques.

PARCHE DE SEGURIDAD: Grupo de actualizaciones de software orientadas a la corrección de errores, problemas de seguridad o vulnerabilidades existentes en los sistemas operativos y programas informáticos.

PENTESTING: Pruebas de penetración, método por el cual se evalúa el nivel de seguridad en una red de equipos o sistemas informáticos, usando ataques simulados en ambientes controlados, los cuales buscan detectar las vulnerabilidades que un atacante podría explotar.

RED TEAM: Equipo de seguridad que realiza ataques controlados a objetivos específicos de la infraestructura de una organización con el objetivo de encontrar y explotar vulnerabilidades y fallos de seguridad en los sistemas y equipos.

VULNERABILIDAD: Es el punto débil o fallo existente en un sistema informático, a través del cual un atacante puede comprometer la seguridad del mismo.

INTRODUCCIÓN

A diario en las empresas y organizaciones, la seguridad cobra gran importancia debido a que el uso de las TIC´S en los procesos se hace más amplio, pues sirven para su simplificación y automatización.

De acuerdo con lo anterior es primordial contar con estrategias que ayuden al mejoramiento de ciberseguridad en la organización, éstas se pueden llevar a cabo por parte de equipos red team y blue team, los cuales proporcionan servicios de seguridad desde diversas perspectivas, como el desarrollo de estrategias de contención y defensa por parte de Blue team y en el enfoque de prueba de los controles de seguridad utilizando técnicas de ataque y penetración de sistemas, por parte de Red team.

El Seminario Especializado en Equipos Estratégicos sobre Ciberseguridad, Red-Team y Blue-Team da muchas pautas para poder analizar, conocer e implementar estrategias para pruebas de pentesting y contención de vulnerabilidades que afecten la información de la organización, todo esto enmarcado dentro de lo legal y ético.

En este documento se plasmará los estudios de caso que se desarrollaron durante el seminario Especializado y que fueron requeridos por la organización WhiteHouse Security.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Presentar un Informe Técnico donde se plasme en forma concisa las actividades realizadas por el Estudiante durante el Seminario Especializado y de acuerdo con los requerimientos de la organización WhiteHouse Security.

1.2 OBJETIVOS ESPECIFICOS

- Identificar y analizar la legislación colombiana en lo que respecta a “leyes y decretos” correspondiente a protección de datos personales y delitos informáticos.

- Evaluar las acciones a realizar por parte de los equipos Red Team & Blue Team de la empresa The WhiteHose Security enmarcadas en los aspectos éticos y legales.

- Detallar y desarrollar paso a paso las fases necesarias en un pentesting o pruebas de penetración.

- Mostrar las vulnerabilidades presentes en el sistema informático utilizando técnicas y métodos para Pentesting.

- Definir las herramientas de seguridad a utilizar especialmente las de Opensource de acuerdo con los requerimientos y necesidades de la Empresa.

- Plantear técnicas de contención mediante el análisis de riesgos y vulnerabilidades en la infraestructura TI de la organización The WhiteHose Security.

- Presentar el informe técnico donde se plasme el proceso de los escenarios propuestos en cada una de las actividades como Red Team & Blue Team y plantean conclusiones y recomendaciones para que ayuden al mejoramiento de las estrategias al interior de la organización.

2. DESARROLLO DEL INFORME TÉCNICO

2.1 CONCEPTOS EQUIPOS DE SEGURUDAD

2.1.1 Legislación colombiana para delitos informáticos y protección de datos personales.

Con respecto a la protección de Datos personales y Delitos Informáticos, en Colombia existen entre otras las siguientes Leyes y Decretos:

2.1.1.1 LEY 1273 DE 2009[1] "Con la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - llamado "de la protección de la información y de los datos"- y se preservan de forma integral los sistemas que utilicen las tecnologías de la información y las comunicaciones, y otras disposiciones". (MINTIC, 2009).
Características Principales: Entre los aspectos que se adicionan podemos encontrar:

- Se atenta contra la confidencialidad, integridad y la disponibilidad de los datos y sistemas informáticos.
- Abuso en el acceso a los sistemas de información.
- Obstaculizar de manera ilegal los sistemas informáticos o redes de telecomunicaciones.
- Interceptar datos informáticos
- Daño a la información
- Utilizar software malicioso
- Violar datos personales
- Suplantar sitios web para capturar información.
- Robo por medios informáticos.
- Transferir activos sin consentimiento.

2.1.1.2 LEY ESTATUTARIA 1581 DE 2012 (octubre 17)[2] Esta ley hace referencia a lo concerniente con la protección de los datos personales pudiendo las personas corregir, actualizar y retractarse de la información que de ellas se haya recogido y colocado en archivos o bases de datos.
En el Artículo 2° se establece el ámbito de aplicación, donde se dice que dichas disposiciones de ley serán aplicables a los “datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada”.

2.1.1.3 DECRETO 1377 DE 2013: Realiza la reglamentación parcial de la Ley 1581 de 2012, donde se pueden observar diferentes disposiciones en cuanto a la protección de datos personales.

---

[1] Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC (2009). Ley 1273 2009 [En línea]. [02 de febrero 2021]. p.4 . Disponible en: https://www.mintic.gov.co/portal/604/articles3705_documento.pdf

[2] Ibid., p.11 .

2.1.1.4 Ley 1712 de 2014: Por medio de ésta ley se crea la reglamentación sobre transparencia y los derechos que tenemos los colombianos a acceder a la información pública de carácter nacional.

2.1.1.5 DECRETO 103 DE 2015: Con éste decreto se hace la reglamentación parcial de la Ley 1712 de 2014, aquí se relacionan entre otras cosas el Objeto, el ámbito de aplicación y los estándares necesarios para publicar la Información.

2.1.2 Etapas del pentesting

Un test de penetración o Pentesting, se puede definir como un acuerdo entre un pentester y una persona o empresa que necesita tener su sistema informático en prueba y poder así reconocer y reparar eventuales peligros y vulnerabilidades relacionados con éstas. Una auditoría de éste tipo es una importante fuente de información para el cliente pues el pentester actuará como atacante facilitando información distinta a la que pueda suministrar el equipo de TI de la empresa. Generalmente un test de intrusión debe seguir unos pasos o etapas predeterminadas con el fin de poder presentar buenos resultados al final, estos serían:

2.1.2.1 Etapa de Contacto

Es la etapa inicial en la que se acuerda con el solicitante en qué va a radicar el test, qué finalidad tiene, cuáles los servicios críticos para la empresa entre otros. En esta etapa también se debe concretar de forma escrita las condiciones del pentesting, por ejemplo, el ámbito de aplicación, las IP, servicios y dispositivos que incluye la prueba, en que horarios se ejecutará, y quien será la persona responsable y a contactar para esta labor. Igualmente, en esta etapa se debe adquirir la autorización escrita para el test de penetración, responsabilidades, pagos etc.

2.1.2.2 Etapa de Planificación de las Pruebas

Para esta etapa del pentest se debe dedicar un espacio para adquirir la información disponible usando scanners para tener una idea más concisa del sistema y programas que estén corriendo, es importante revisar también la actividad de los usuarios de las redes sociales de la entidad que nos permiten saber su correo electrónico, sistemas utilizados, y toda la información relevante.
En esta etapa el Experto planifica las pruebas, usando platillas que permitan verificar y planear los requisitos de las pruebas en cuanto a Hardware, software, cronograma, responsabilidades, recursos físicos y humanos etc.

2.1.2.3 Etapa de Diseño o Modelado de las Pruebas

En esta etapa y con la información recogida se diseñará como tal la prueba para realizar el ataque a la maquina víctima.
Para guiar a quienes van a realizar las pruebas se utilizarán listas de chequeo que permitan verificar el cumplimiento del modelo de prueba seleccionado. Las Listas de Chequeo contienen: Ítems a evaluar, descripción, herramienta a utilizar,

resultado real y esperado. Un ejemplo de diseño sería crear un caso de prueba por roles colocando un escenario para cada funcionalidad, con rol sin permiso, rol con permisos mínimos y probar si la función se puede ejecutar ilegalmente por dichos roles.

2.1.2.4 Etapa de Ejecución de las Pruebas o Explotación de vulnerabilidades

Con base en los resultados del trabajo realizado anteriormente, en esta etapa se consigue acceso a los sistemas de la organización. Esta tarea se logra con la ejecución de exploits hacia las vulnerabilidades encontradas o utilizando privilegios adquiridos para tener acceso al sistema. Cuando terminan las pruebas se deben limpiar por completo los posibles falsos positivos encontrados.

2.1.2.5 Etapa de Post-explotación o Mantenimiento de Acceso

En esta etapa, se pretende llegar más lejos dentro del sistema vulnerado, o sea obtener credenciales o permisos de administrador, violentar sistemas más importantes dentro de la empresa por medio de técnicas de pivoting entre otras.

Por ejemplo, la herramienta **ETERNALBLUE** es un exploit desarrollado para aprovechar una vulnerabilidad en la implementación de la primera versión del protocolo conocido como Server Message Block.

2.1.2.6 Etapa de Documentación e Informe de los resultados

Al terminar las fases anteriores, se debe documentar el resultado del proceso realizado en el pentest, las herramientas y técnicas que se utilizaron y las vulnerabilidades encontradas, de tal forma que el cliente entienda la gravedad de los riesgos descubiertos, resaltando los aspectos con buena seguridad y aquellos que se deben corregir y el cómo hacerlo. Esta es la fase más importante para las dos partes. Para mayor comprensión del personal de TI y responsables del área administrativa que no conocen el tema técnico es conveniente separar el informe general que se conoce como informe ejecutivo y el informe técnico. En este Informe se debe incluir el compendio del registro de defectos y dificultades comprendido por las no conformidades o vulnerabilidades detectadas y la etapa donde se detectaron. En esta fase es de gran utilidad el uso de Bitácoras de Registro, Procesador de Texto para elaboración de los Informes entre otras.

2.1.3. Herramientas de ciberseguridad

2.1.3.1 METASPLOIT: Herramienta de código abierto, que permite realizar auditoría de seguridad y pruebas de penetración, que permitan, conocer, explotar y determinar el alcance de las vulnerabilidades de seguridad de los sistemas. El Metasploit más usado es el Framework que permite hacer varias cosas como:

- Identificar y explotar las vulnerabilidades
- Escalar privilegios y robar datos
- Recoger y escanear toda la información de un equipo
- Instalar puertas traseras
- Búsqueda de errores en software de forma aleatoria.
- Evitar el antivirus
- Eliminar registros

2.1.3.2 NMAP (NETWORK MAPPER): Es un software libre, de código abierto, usado para pruebas de intrusión y auditoria en seguridad, esta aplicación permite escanear una red de datos y determinar el número de equipos que la integran, sus características técnicas como sistema operativo, dirección MAC, servicios, puertos en uso, puertos abiertos. Entre las características se tienen:

- Determinar los servicios ejecutados por un equipo.
- Establecer qué sistema operativo y versión utiliza la máquina.
- Conseguir características del hardware de red del equipo víctima.
- Descubrir servidores: Identificar computadores de la red, por ejemplo, cuáles responden a un mensaje ping.
- Reconocer los puertos abiertos en la maquina atacada.

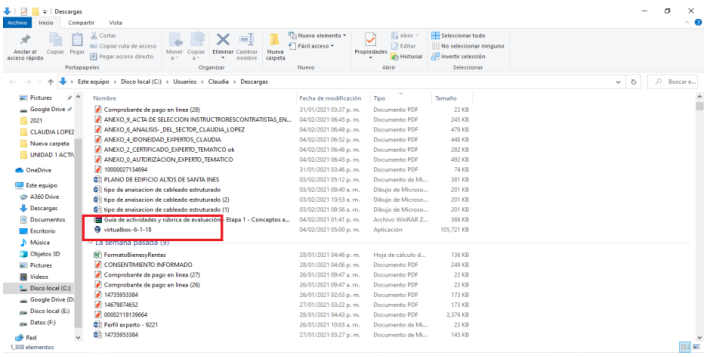
2.1.3.3 OPENVAS: Grupo de herramientas usada para explorar y analizar debilidades de los equipos en la red. Se caracteriza por servir para realizar escaneo simultaneo de varios nodos, tener servidor de correo SSL, puede entregar reportes en diferentes formatos como el HTML y XML.
El resultado mostrado en un reporte de OpenVas contiene la descripción de la vulnerabilidad hallada, los puertos que están abiertos y los servicios que corren allí y la posible solución al problema.

2.1.4. Banco de trabajo

Se realiza el montaje del banco de trabajo solicitado por la organización con el cual el personal que quiere hacer parte de la organización The WhiteHouse Security deberá trabajar y realizar los escenarios y problemas planteados y dar respuesta a las preguntas orientadoras para conocer la base del conocimiento de los aspirantes en cuanto a temas de Ciberseguridad.

Paso A: Se procede a descargar la última versión. (6.1.18) de la aplicación de virtualización “VirtualBox”,

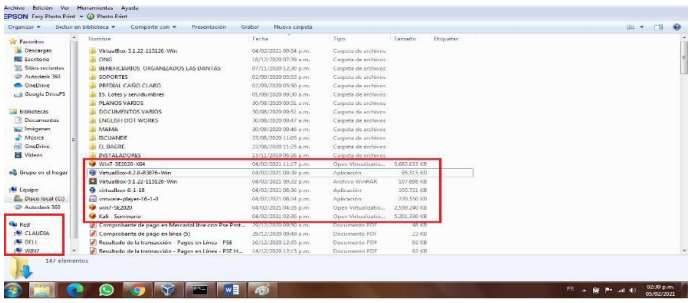
Figura 1 Herramienta Virtual Box descargada



Fuente: Autor

Paso B: Se descarga también las imágenes en OVA que ya están pre configuradas para ser utilizadas en las actividades de carácter técnico. En las imágenes OVA tenemos: Windows7-X86, Windows7-X64, y Kali Linux.

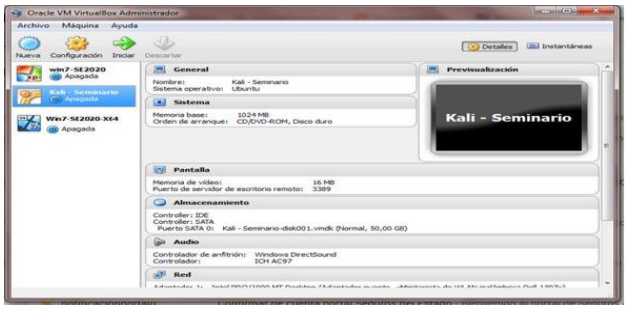
Figura 2 Máquinas virtuales formato .OVA descargadas



Fuente: Autor

Paso C: Validar que existe comunicación entre las máquinas Windows con la máquina de Kali Linux. Se Importaron las tres máquinas, 2 de Windows y la de Kali Linux para verificar la conectividad entre ellas, así:

Figura 3 Máquinas de Windows y Kali Linux Importadas



Fuente: Autor

Prueba de Conexión Maquina Windows 7-X64 y Kali Linux

Maquina Windows 7-X64 y Maquina Kali Linux corriendo

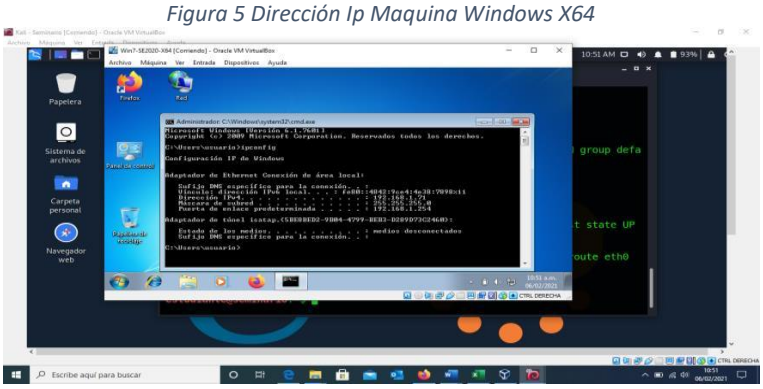
Figura 4 Máquinas Kali Linux y Windows 7 X64 Operando

Fuente: Autor

Comando *ipconfig pa*ra obtener dirección Ip en la maquina Windows 7-X64 obteniendo la dirección 192.168.1.71, cabe resaltar que ambas redes se colocaron

en modo puente, en modo NAT la dirección que nos da es la misma para las dos máquinas, 10.0.2.15.

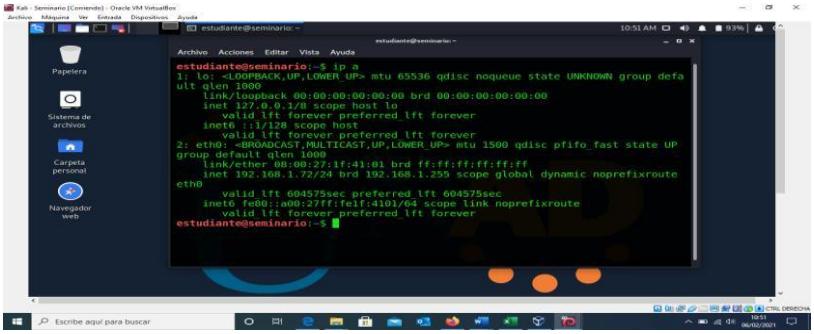
Figura 5 Dirección Ip Maquina Windows X64



Fuente: Autor

Comando *ip a pa*ra obtener dirección Ip en la maquina Kali Linux obteniendo la dirección 192.168.1.72, cabe resaltar que ambas redes se colocaron en modo puente, en modo NAT la dirección que nos da es la misma para las dos máquinas, 10.0.2.15.

Figura 6 Dirección Ip Máquina Kali Linux



Fuente: Autor

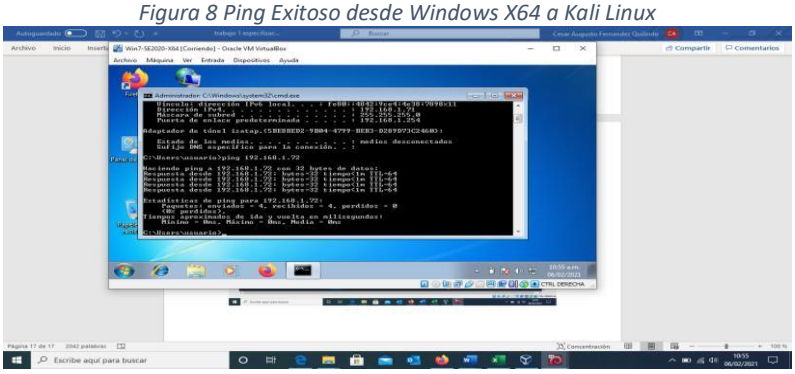
Envío de Ping hacia maquina Windows con ip: 192.168.1.71 para verificar conectividad

Figura 7 Ping Exitoso desde Kali Linux a Windows X64

Fuente: Autor

Envío de Ping hacia maquina Kali Linux con ip: 192.168.1.72 para verificar conectividad

Figura 8 Ping Exitoso desde Windows X64 a Kali Linux



Fuente: Autor

2.2 ACTUACIÓN ETICA Y LEGAL.

2.2.1 Reconocer aspectos éticos y legales

De Acuerdo con el análisis realizado como profesional que soy en cuanto al Acuerdo, voy a resaltar o identificar los apartes que considero vulneran la ética y por tanto se consideran ilegales de acuerdo con los establecido en las leyes colombianas y en especial el Código de ética de COPNIA que es la entidad rectora de nosotros los Ingenieros de Sistemas, estas inconsistencias serían:

*"**Clausula Primera. Objeto**: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima o 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.**"*[3]

En este caso es evidente que la Empresa oculta por medio del acuerdo de confidencialidad en una clausula avalada legalmente que no se puede reportar o denunciar ante las autoridades correspondientes, la información o procedimientos ilegales, esto no es para nada confiable y da mala imagen a la organización y sus posibles empleados.

Segundo aspecto a considerar es acerca de la "***Cláusula segunda: Definición de información confidencial:***

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de

[3] Universidad Nacional Abierta y a Distancia UNAD. *Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team - (202337164A_964)* [En línea]. [9 de febrero 2021]. 6 p. Disponible en: https://campus125.unad.edu.co/ecbti88/mod/folder/view.php?id=5774/Anexo 3 - Acuerdo.pdf/

utilidad, diseños industriales, datos secretos como ***datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'[4].***
Se destaca el cómo han obtenido información ilegalmente infringiendo las leyes colombianas, y resguardándose de nuevo en el acuerdo de confidencialidad. Para este caso tengo la plena seguridad que no firmaría este acuerdo pues va en contra de mi ética y formación en valores que he tenido a lo largo de mi vida tanto personal como profesional.

*"**Cláusula 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."[5]*
Aparentemente pareciera legal, pero siempre es necesario saber la fuente de donde proviene la información para evitar responsabilidades posteriores.

Clausula Cuarta: En las obligaciones establecidas en ésta cláusula, la parte receptora se ve obligada a no realizar la denuncia de actos no éticos o ilegales, como encubrir el espionaje y ser cómplice de dichos actos, esto se puede evidenciar en los siguientes puntos:
"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.
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 Whitehouse Security."[6]

De igual manera el acuerdo señala que la parte receptora responderá por el uso indebido que se le dé a la Información confidencial, igualmente responder legalmente si se le encuentra dicha información, la organización WhiteHouse Security se libra de sus actuaciones ilegales de forma automática y por demás un tanto cínica, para este caso se ve en los siguientes puntos:

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

[4] Ibid, p. 3
[5] Anexo 3-Acuerdo Óp. Cit., P. 3.
[6] Anexo 3-Acuerdo Óp. Cit., P. 4

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."[7]

"Clausula 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 Whitehouse Security."***[8]

Para este caso si el profesional decide firmar estaría totalmente consciente que es una falta grave a la ética y por ende las consecuencias legales que acarrearía este actuar como privación de la libertad, multas y la subsecuente pérdida de la matricula profesional, en realidad ¿es justo sacrificar tanto por tan poco?, creo que no, los valores, la ética y la formación valen más que el dinero.

2.2.2 Análisis de la ley 1273 [9]

Teniendo En cuenta los artículos de ésta Ley y el acuerdo de confidencialidad el análisis de vulnerabilidad de esta ley sería:
*"**Cláusula Primera. Objeto:** en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima o 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."***[10]
Artículos vulnerados:
Art. **269F** La empresa se ampara en el acuerdo de confidencialidad para violar datos personales, e igualmente y de forma directa estaría obligando a ocultar esta información o procesos ilícitos.
Art. **269H** En el que se hace referencia de aprovechar la confianza de quien tiene información o por el hecho de tener un vínculo contractual con este obligar a dar a conocer la información en perjuicio de otra persona, para este caso la empresa obliga a no denunciar estos procesos ilegales.

"Cláusula segunda: Definición de información confidencial:

---

[7] Anexo 3-Acuerdo Óp. Cit., P. 4

[8] Anexo 3-Acuerdo Óp. Cit., P. 5

[9] Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC (2009). Ley 1273 2009 [En línea]. [11 de febrero 2021]. 4 p. Disponible en: https://www.mintic.gov.co/portal/604/articles3705_documento.pdf

[10] Anexo 3-Acuerdo Óp. Cit., P. 2

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".***[11]

Para este caso se incumplen:
Los artículos **269A, 269C y 269H** ya que se evidencia claramente que habrá acceso de forma abusiva al sistema de información, pues se obtiene la información de manera ilegal, sin orden judicial se interceptan datos informáticos y los sistemas de comunicaciones y por estas acciones puede quedar inhabilitado para ejercer la profesión n este campo.

En la tercera cláusula, Tenemos:
*"**Cláusula 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."*[12]

Para este caso hay infracción de los artículos **269I y 239,** relacionados con el robo realizado usando medios informáticos o afines, es claro aquí que esta información se consigue de forma ilegal sobrepasando las normas de seguridad informática o manipulando un sistema de información sin autorización.

"Cláusula Cuarta. Obligaciones de la parte receptora":
"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.
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

[11] Anexo 3-Acuerdo Óp. Cit., P. 3
[12] Anexo 3-Acuerdo Óp. Cit., P. 3

información confidencial o ilegal sin el previo consentimiento por escrito por parte de Whitehouse Security."[13]

Podemos observar infracciones de la Ley en los puntos 3, 4, 7, 8 y 9 enunciados anteriormente y se concluye la vulneración de los siguientes artículos:

269A: Pues se hace referencia al abuso de accesos y espionaje.

269C: De forma clara se evidencia la interceptación de la información.

269F: Se confirma que se violan datos empresariales y personales.

269H en varios de sus numerales así:

1. La organización afirma que trabaja en sistemas informáticos, redes y sistemas de comunicaciones oficiales nacionales y extranjeros.

3. Se ve el abuso de confianza y el haber contratado con alguna de las empresas dio pie para adueñarse de la información.

5. Esta Empresa sigue obteniendo provecho para sí misma de esta información.

8. La Organización continúa con el control de la información.

Ésta cláusula en el numeral 7, indica que se debe responder individualmente si se hace mal uso de información que se considere confidencial. Este actuar se conoce como delito de favorecimiento y vulnera en forma directa el código penal en el artículo 446.

"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 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."***[14]

En éste caso se observa que hay vulneración del artículo **269H** en el enciso 7 donde se está utilizando a un tercero y la empresa se exime de cualquier responsabilidad penal y/o legal en caso de encontrarse información ilegal en manos de sus empleados, aquí habría encubrimiento de estas actividades dada su completa e indudable intervención en todo el proceso de manejo y consecución de la información.

2.2.3. "Aplicación código de ética para ingenieros del COPNIA"

Iniciando con el análisis se observa que el objeto del acuerdo es muy claro en estipular que la parte receptora no podrá divulgar ninguna clase de información concerniente a los procesos ilegales que se realicen en Whitehouse Security, por lo que se puede confirmar una falta contra el Código de Ética **COPNIA** por omitir la

[13] Anexo 3-Acuerdo Óp. Cit., P. 3-4

[14] Anexo 3-Acuerdo Óp. Cit., P. 5

denuncia de los procedimientos ilegales y demás faltas que se cometan y que de hecho van a atentar contra este código.
A pesar de que el sueldo es bastante atractivo y el contrato es vitalicio este acuerdo vulnera en gran medida el Código ético.
El acuerdo establecido por la empresa WhiteHouse Security que pretende se firme claramente presenta vulneración de varios artículos del código de Ética del **COPNIA**, ente regulador para quienes ejercemos la profesión de Ingeniería de Sistemas en Colombia, como se mostrará a continuación:

ART.31: Ocultar o utilizar la información de forma indebida, no denunciar las faltas o delitos que haya en contra del código.
Para este caso está sucediendo todo lo contrario.

ART.32: La organización, a través de este contrato permanente, estaría eligiendo, nombrando, o teniendo a su servicio profesionales que van a ejercer sus funciones de forma ilegal y por ende realizar actos delictivos, por tanto, se verían avocados a sanciones para el ejercicio de la profesión.

ART.34: Se estaría infringiendo por ambas partes, Empresa al ofrecer y el Profesional al aceptar éste trabajo en sin tener en cuenta la normatividad legal que rige en nuestro país.

ART.35. Bajo todo punto de vista no se estaría respetando la normatividad al permitir que se incurran en acciones fraudulentas y aun asi no realizar la denuncia de éstas infracciones.

ART.40: La empresa estaría prestando un servicio cuyo objeto, es de dudosa procedencia.

ART.43: La vulneración se ve al no existir la denuncia ante el organismo profesional correspondiente la existencia de transgresiones contra la ética, con esta situación al ingeniero se le abstiene de licitar, concursar o realizar propuestas de carácter público o privado.

A todas luces este acuerdo infringe el Código de Ética para ejercer la Ingeniería al promover en el Profesional la contravención de sus artículos que en resumen los podemos condensar de la siguiente forma:

- Denunciar los hechos, conductas, y faltas que se conozcan en el ejercicio del quehacer profesional y que vayan en contravía de la Ética.
- No ser un obstáculo para las investigaciones que adelante el Consejo Profesional o las autoridades competentes, en todo momento prestar la colaboración necesaria para el desarrollo de dichas funciones.

- Respetar las disposiciones legales vigentes y no aceptar labores que infrinjan las mismas.
- No realizar actos delictivos que agredan a colegas, autoridades o clientes.
- Cuidar siempre la reputación de la profesión.

De esta manera, el profesional que quiera aplicar al cargo en WhiteHouse Security aprobando dicho acuerdo, no solo será cómplice de conductas anti-éticas e ilegales, sino que obraría en contra de la Ley al permitir la violación de los datos personales y delitos informáticos, que acarrearía tanto multas como privación de la libertad de acuerdo con la Legislación colombiana.
Igualmente, el Profesional podría hacerse acreedor de sanciones por parte del COPNIA al incumplir su código de Ética rector y considerarse como faltas gravísimas.

Con el análisis anterior, además de cumplir las disposiciones de ley colombiana, es de vital importancia acatar lo contenido en el Código de Ética Profesional pues es de obligatorio cumplimiento por ser el órgano rector de la conducta y el accionar del ejercicio profesional nuestro. Bajo mi punto de vista veo totalmente antiético contratar con esta Organización bajo el acuerdo propuesto por ellos.

2.2.4. "Implicaciones legales y éticas en el caso operación andromeda buggly"

De acuerdo con las investigaciones reveladas por el Ejército, la presencia de Andrómeda se hizo totalmente dentro del marco legal. "La creación de la fachada 'Buggly Hacker' fue legal, con base en la Constitución Política de Colombia, directrices, reglamentos y el 'Manual de Manejo de Redes de Informantes', el cual se refiere a la 'fachada' y a la 'historia ficticia', relató en su momento el general Ernesto Maldonado, auditor general de la institución Militar".[15]
Inicialmente la Operación Andrómeda se consideraba legal, el objeto de dicho proceso se alteró por las malas prácticas e inconvenientes de seguridad. A lo largo de todo este proceso no se ve la presencia de un Hacker ético para la supervisión del mismo y que con mucha experiencia y conocimiento de todos los detalles hubiera generado un informe profesional y auditado con los debidos controles de seguridad.

El personal militar incurrió en varios delitos por no contar con el conocimiento técnico ni aplicar la ética profesional en cada una de sus actuaciones. Las actividades de chuzar, hackear y violar sistemas de información, fueron ilegales y por tanto anti-éticas. El Fundamento de la Investigación se basó en la sustracción de las bases de datos de forma ilegal, pagando a personas sin ninguna clase de conocimiento de buenas prácticas éticas, lo que pudo haber ayudado a la fuga de información al interior de organización, revelando secretos políticos y cometer fallas

[15] https://www.eltiempo.com/archivo/documento/CMS-13502795

en su deber como servidores públicos. No se observan parámetros claros, contratos legales ni acuerdos de confidencialidad que conlleven a evidenciar las malas intenciones del procedimiento. La vulneración y ataque a los sistemas informáticos y de comunicación se realizó para lucrarse, y sin tener la suficiente sapiencia para realizarlas de forma directa. Hubo mala organización, ilegalidad total y sin el personal calificado para la operación. La información obtenida por el Señor Sepúlveda, no se puede considerar de un talante Hacker ni tampoco informático al ser proporcionada (vendida) por los titulares de la Fachada, quienes se encargaban de realizar chuzadas y espionaje, actividades éstas que distan mucho de un profesional en el ramo de la seguridad Informática.

2.3 HERRAMIENTAS SOFTWARE UTILIZADAS PARA SOLUCIONAR EL ESCENARIO DE ACUERDO CON LAS FASES DEL PENTESTING

2.3.1 Fases para pentesting

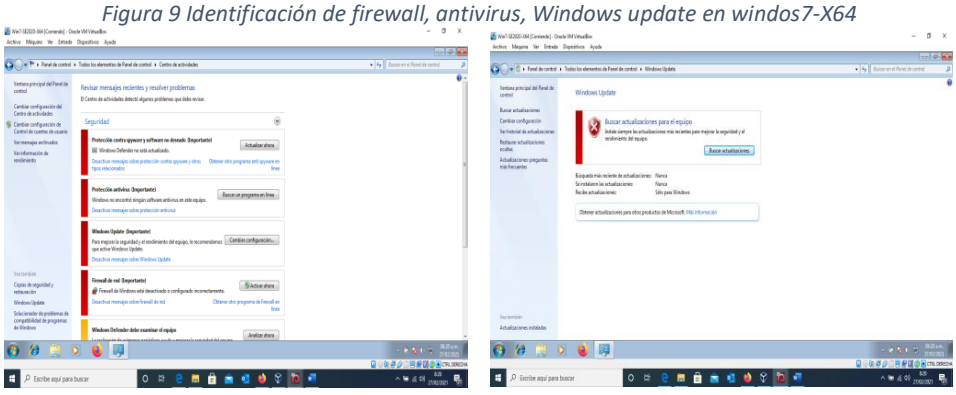
2.3.1.1 Fase para recolección de Información

Se realizó con la herramienta **Nmap** presente en Kali Linux, con ella podemos encontrar vulnerabilidades por ejemplo cuando estamos por puertos abiertos y resultamos atacados, es útil para exploración de la red y verificar su seguridad.

El Objetivo de esta fase es recolectar toda clase de información que permita identificar de la mejor manera al usuario, comprobar la seguridad y explotar las vulnerabilidades halladas. También Red Team escaneara los equipos sospechosos con el fin de obtener información más detallada como el número de puertos que se encuentran abiertos y las posibles vulnerabilidades a que están expuestos.

Debo confirmar que el firewall, antivirus, y update estén desactivados en ambos equipos, si no es así los debo apagar o deshabilitar.

Figura 9 Identificación de firewall, antivirus, Windows update en windos7-X64

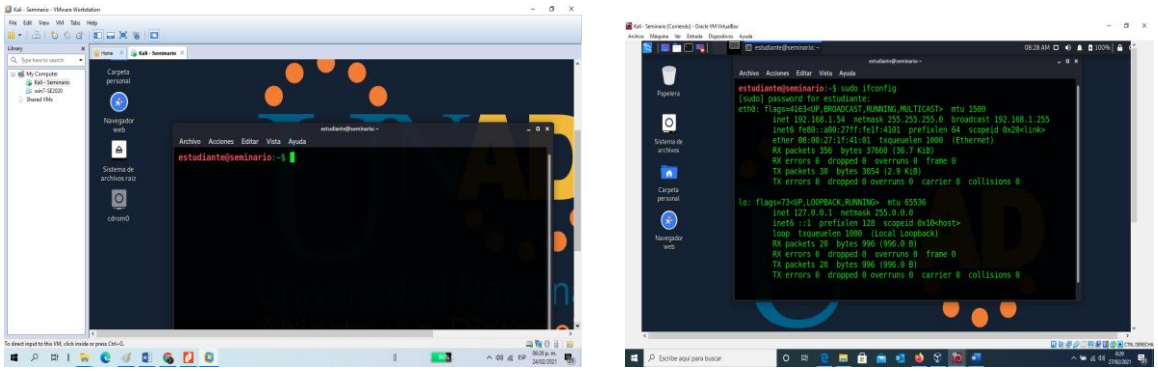


Fuente: Autor

En la máquina Kali busco cuál es la IP y en qué Red estamos con:

sudo ifconfig ó - ***IP route***

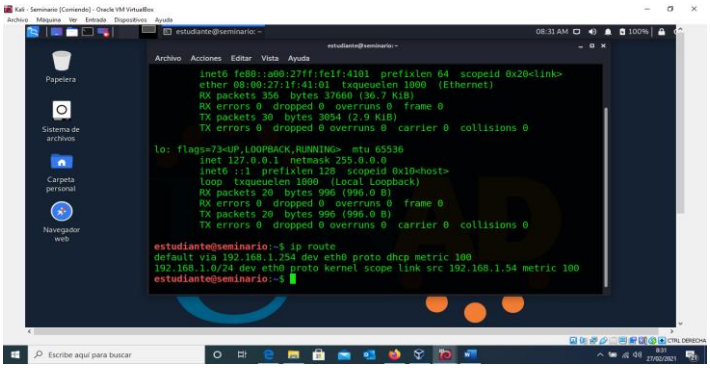
Figura 10 Verificación dirección IP



Fuente: Autor

Ya reconociendo la IP como **192.168.1.54,** también se puede observar que el segmento de red es **192.168.1.0/24**.

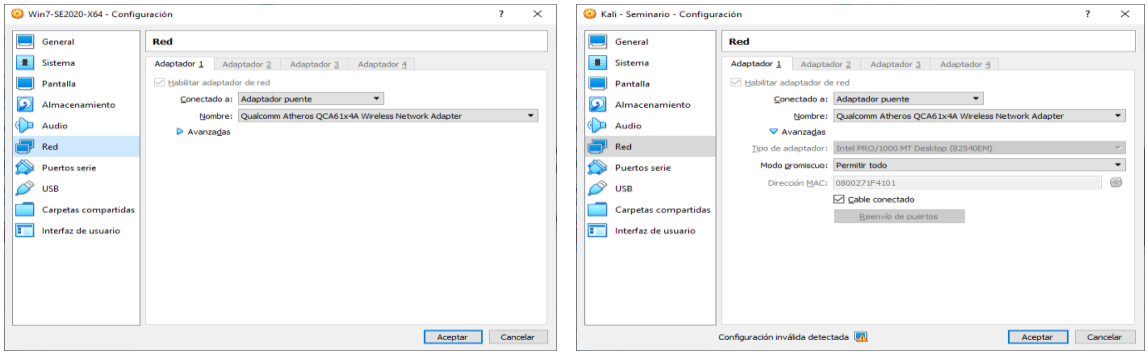
Figura 11 Reconocimiento de Segmento de Red



Fuente: Autor

Para este caso se debe verificar que el modo de configuración del puerto de red sea de Adaptador puente.

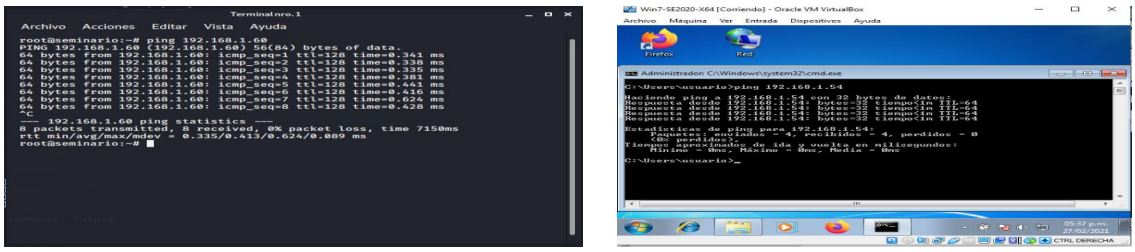
Figura 12 Modo Adaptador Puente Máquinas



Fuente: Autor

Se debe verificar también que las maquinas estén viéndose entre si enviando un ping desde la consola de cada una de ellas

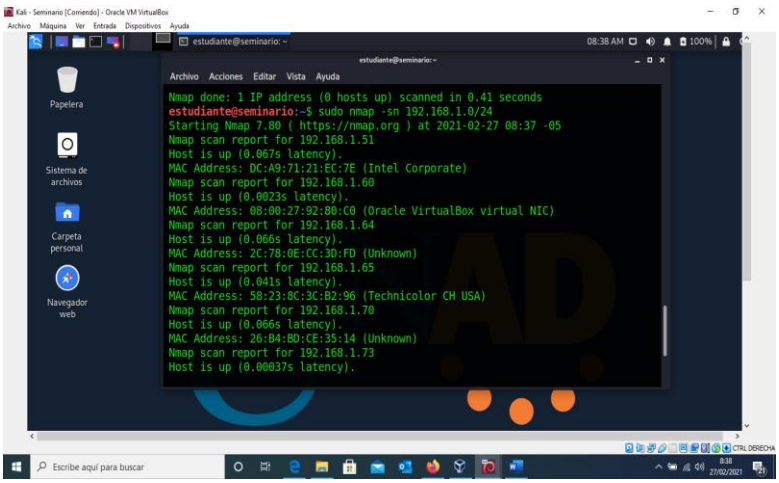
Figura 13 Envío Ping entre Máquinas



Fuente: Autor

Averiguamos los dispositivos que están conectados a la red y se identifica la IP del equipo al cual se le realizará el escaneo y posterior ataque con **Nmap.**
>***sudo nmap –sn 192.168.1.0/24***

Figura 14 Equipos conectados a la Red

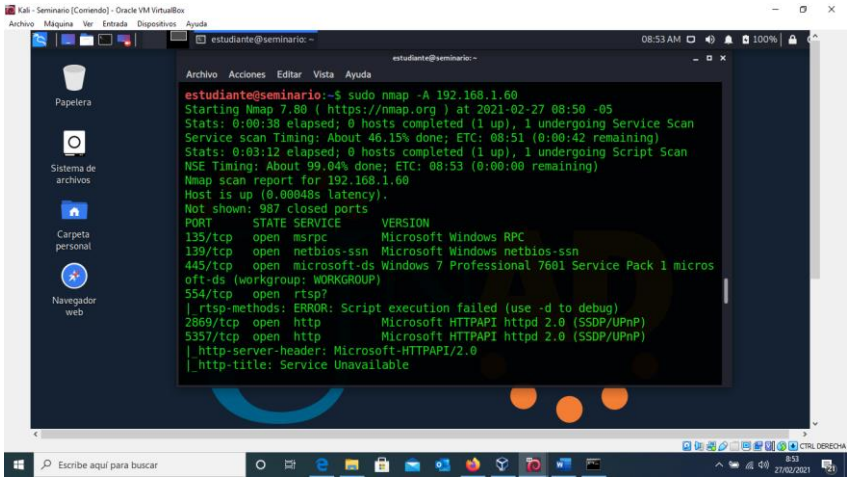


Fuente: Autor

Encontramos 6 hosts, entre ellos **192.168.1.254** Modem Technicolor, **192.168.1.51** el router de internet,**192.168.1.64** el router virtual box, **192.168.1.70** es mi celular Huawei y **192.168.1.54** es la Máquina atacante con Kali Linux, resta indagar e identificar **192.168.1.60**

Se realiza el escaneo de puertos Maquina win7-X64 con dirección **192.168.1.60**

Figura 15 Escaneo puertos Maquina Win7-X64

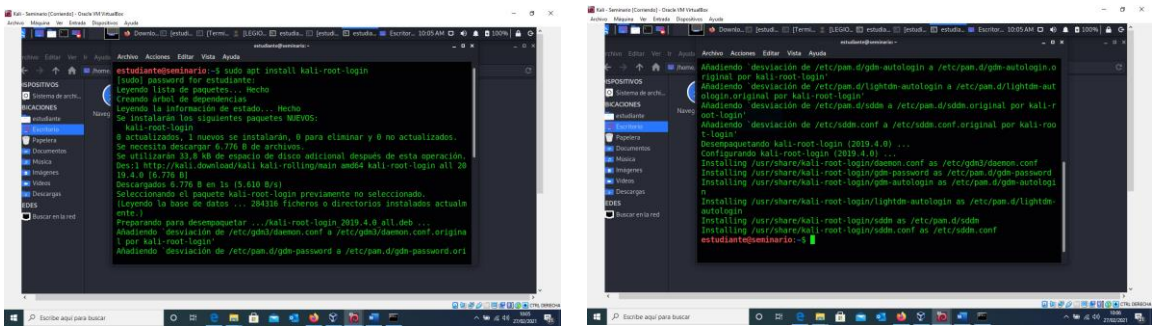


Fuente: Autor

2.3.1.2 Fase de análisis de vulnerabilidades

Después de haber reconocido el ambiente y ver los puertos abiertos para atacar, vamos ahora a analizar qué puntos vulnerables nos permiten realizar un ataque exitoso. Una herramienta útil para explotar estas fallas de seguridad sería **Nessus** que es una estructura de trabajo que ofrece escaneo, búsqueda de vulnerabilidades en la red y posibles soluciones, clasifica los resultados encontrados para la entrega de los informes y **Npam** nos sirve para explorar esas vulnerabilidades y compararlas con las bases de datos. Instalamos ahora Nessus en el equipo atacante con Kali Linux. - La interfaz gráfica realiza todo el proceso. A continuación, se evidencia la instalación de Nessus en la maquina Kali Linux para poder realizar el escaneo de la máquina que posee el fallo de seguridad.

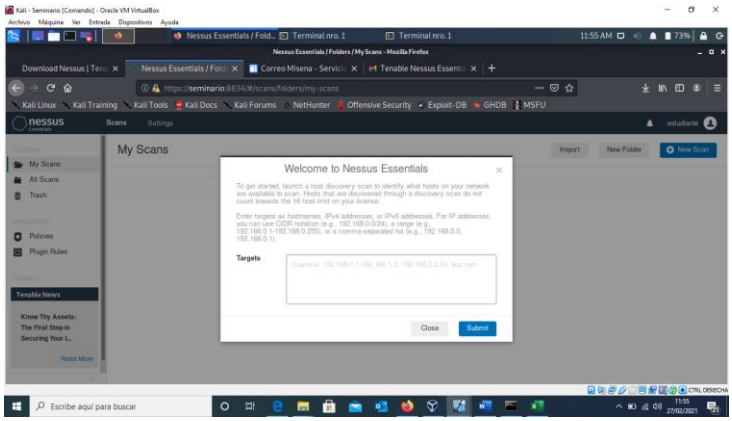
Figura 16 Instalación Nessus en Kali –Linux



Fuente: Autor

Una vez instalada la herramienta se procede a realizar el Escaneo a Win7-X64 utilizando Nessus

Figura 17 Inicio Nessus para escaneo Vulnerabilidades



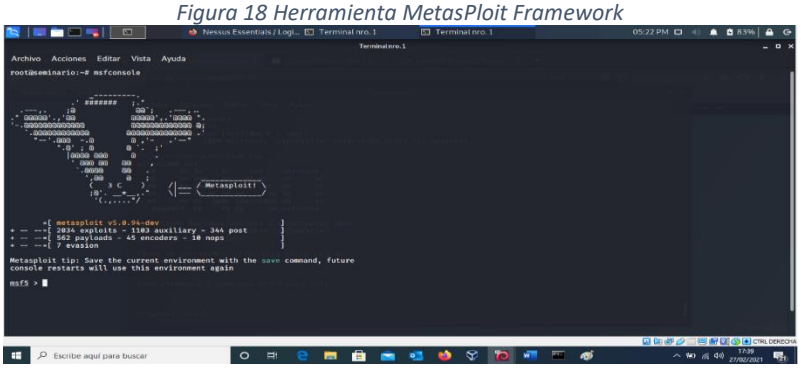
Fuente: Autor

2.3.1.3 Fase de explotación de vulnerabilidades

Para esta Fase se utilizó la herramienta MetasploitFramework es un Proyecto de código abierto el cual da a conocer las debilidades de seguridad en un sistema, sirve también para las etapas de penetración con el fin de protegerlo. Permite utilizar otras herramientas como Nmap y Nessus.
La forma más eficiente y de ayuda es en consola con el comando msfconsole con variantes diferentes como –q entre otras. Desde el terminal de Kali Linux lanzamos la herramienta:

estudiante@seminario:~$ ***msfconsole -q***

Figura 18 Herramienta MetasPloit Framework



Fuente: Autor

2.3.1.4 Fase de Informes o reportes

Es la documentación que especifica el proceso realizado por el equipo Red Team y Blue Team. Las máquinas poseen herramientas que generan reportes que sirven para el informe ejecutivo y técnico que se entregará a la empresa. Por ejemplo, Nessus genera reportes detallados útiles para este fin.

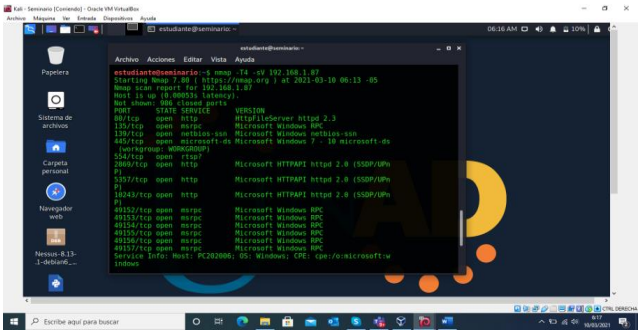
2.3.2 Descripción falla de seguridad

En el anexo 4 – escenario 3 se especifica que la máquina donde se está generando la fuga de información tiene instalada una aplicación llamada rejetto v.2.3 bajo un Windows7 con arquitectura X-64; esta aplicación al parecer tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter, con esta información se pudo identificar la falla de seguridad específica que está corriendo en la máquina con Windows7-X64. El sistema operativo es antiguo y no puede ser reemplazado porque no es compatible con otros sistemas operativos. Al momento de la fuga de información el S.O. no se encontraba actualizado. El equipo de cómputo no tiene instalada la actualización MS17-010.

2.3.2.1 Recopilación de información

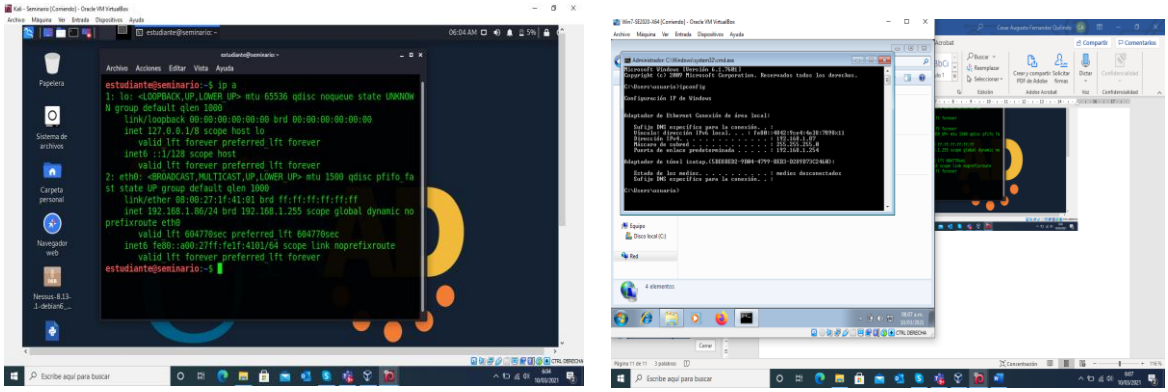
Conocer y disponer de la mayor cantidad de información del sistema que nos permita llevar a cabo nuestro objetivo, en esta etapa utilizaré la herramienta Nmap y así verificar la seguridad por medio de los puertos y los servicios.

Figura 19 Escaneo servicios maquina WIN7-X64



Fuente: Autor

Figura 20 Escaneo Dirección IP ambas máquinas



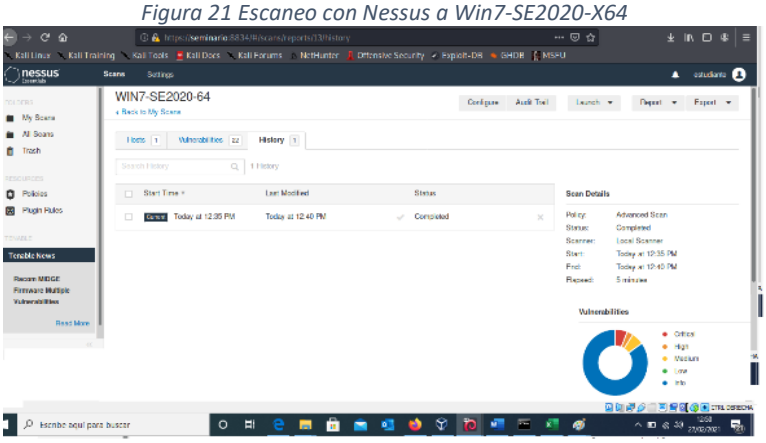
Fuente: Autor

Una vez recopilada la información estamos listos para analizar las vulnerabilidades y realizar la respectiva explotación de las mismas, para el caso específico se solicita también investigar sobre un escalamiento de privilegios por medio de la creación de un usuario tipo administrador del sistema. El equipo de forense facilitó la copia del servidor para validar la posible falla de seguridad y si ésta es explotada se debe crear un usuario con el primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC (Prueba de Concepto) ante los altos directivos.

2.3.3 Herramienta utilizada y fallas de seguridad

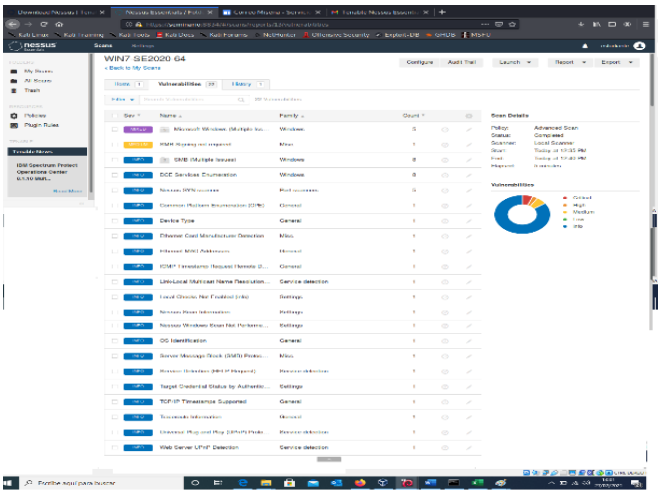
Aquí definimos cual aplicación utilizamos para poder identificar las fallas de la máquina Windows7-X64. Se analiza la información recolectada en búsqueda de amenazas, utilizando la herramienta Nessus.

Figura 21 Escaneo con Nessus a Win7-SE2020-X64



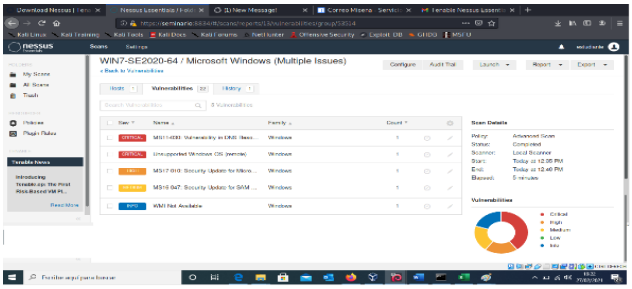
Fuente: Autor

Figura 22 Resultados encontrados en WIN7-X64



Fuente: Autor

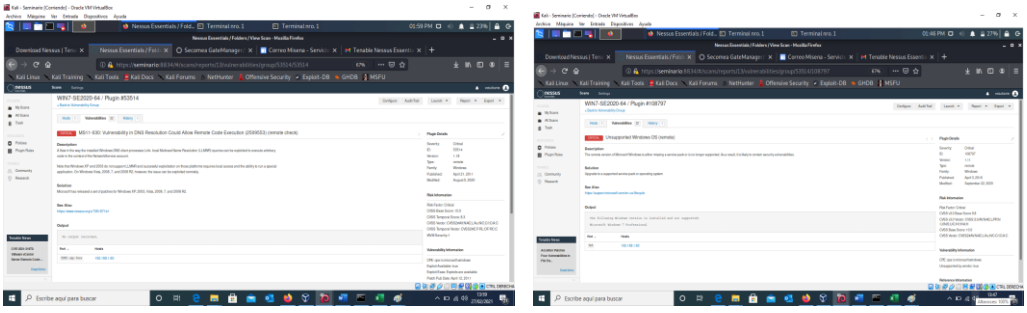
Figura 23 Vulnerabilidades críticas para escoger en el exploit



Fuente: Autor

NIVEL CRÍTICO: MS11-030, UNSUPPORTED WINDOWS OS (REMOTE

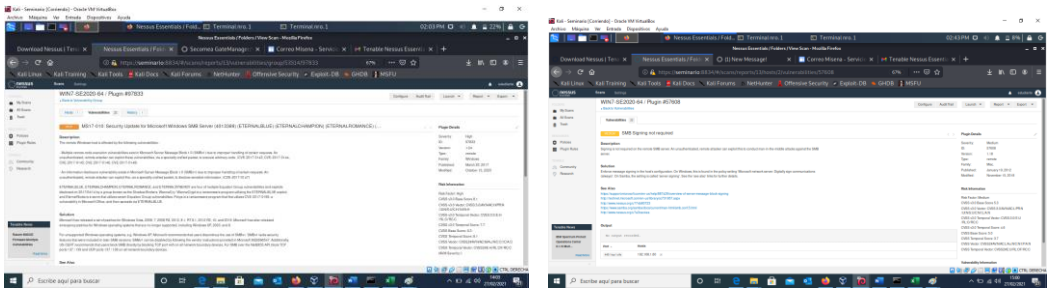
Figura 24 Hallazgos Nivel Crítico



Fuente: Autor

NIVEL ALTO: MS17-010, **NIVEL MEDIO:** MS16-047:

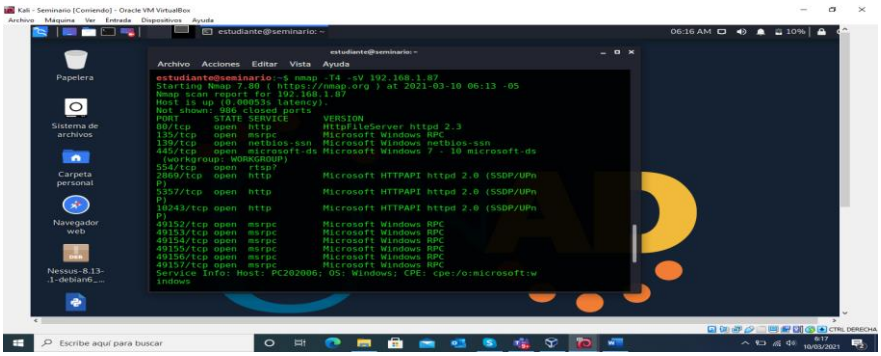
Figura 25 Hallazgos Nivel Alto y Medio



Fuente: Autor

Para este procedimiento se pudo observar que en el informe recibido de Nessus se ven varias vulnerabilidades, pero no se observa la que específicamente solicita le empresa en el anexo referente a la aplicación que está corriendo en esta máquina como es Rejetto v2.3, entonces se procede a solicitar con Nmap la información de los puertos abiertos y servicios que allí se están prestando para así poder tener el insumo para la fase de explotación de dicha vulnerabilidad.

Figura 26 Estado de puertos y servicios WIN7-X64

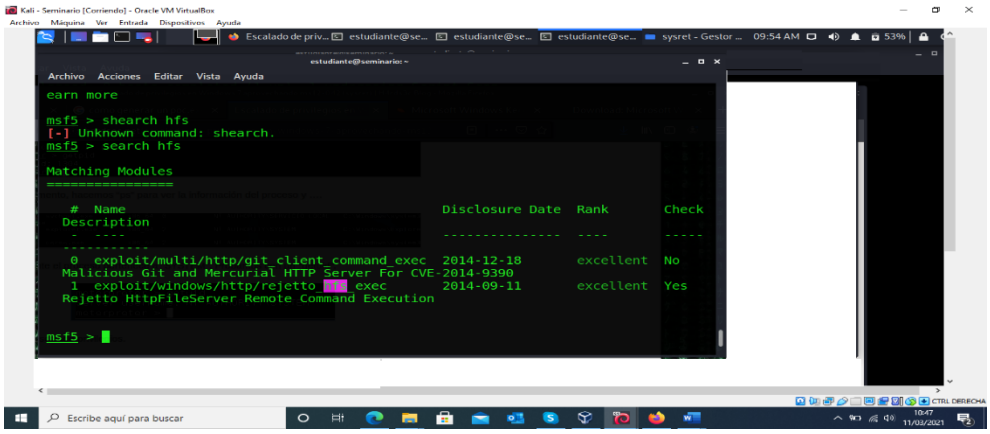


Fuente: Autor

Podemos aquí observar qué puertos están abiertos y cuales servicios o aplicaciones están corriendo allí, para el caso específico nuestro el puerto 80 es el que está dando paso a esta aplicación Rejetto V2.3. Teniendo en cuenta la vulnerabilidad detectada se debe investigar e identificar cuáles son los mejores vectores de ataque para explotarla y así obtener la oportunidad de provecho para introducirnos a la máquina con sistema operativo Windows 7 X64, sacando el mayor provecho de las vulnerabilidades presentes. En esta etapa haremos uso de la herramienta MetasploitFramework para encontrar y ejecutar desde su base de datos la vulnerabilidad para Rejetto V2.3. Una vez identificamos que la vulnerabilidad de rejetto estaba presente y corriendo en el puerto 80 abierto de la máquina de Win7 se procede a realizar una búsqueda por nombre de esta falla y poder así saber el exploit correspondiente y los payloads disponibles y apropiados para verificar la falla, esta es la secuencia:

Msf5>***search hfs***

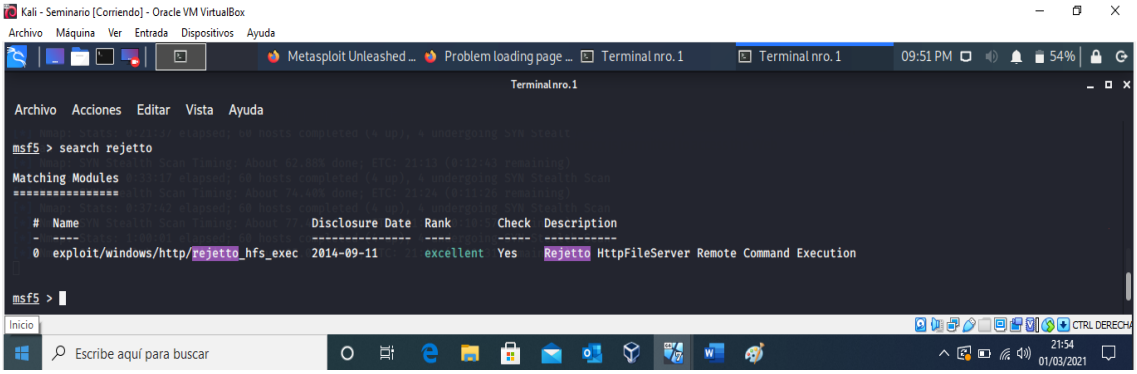
Figura 27 Búsqueda HFS



Fuente: Autor

Msf5>***search rejetto***

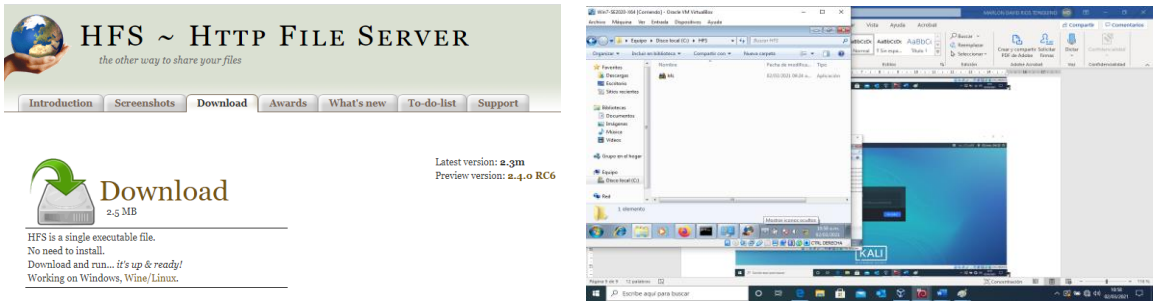
Figura 28 Búsqueda de Rejetto



Fuente: Autor

El servidor de archivos HTTP Rejetto (HFS) es vulnerable al ataque de ejecución de comandos remotos debido a una expresión regular deficiente en el archivo ParserLib. Este módulo explota los comandos de secuencia de comandos HFS para omitir el filtrado. Los sistemas vulnerables son Windows XP-SP3, Windows7- SP1 y Windows 8, para nuestro caso es Windows7- X64 SP1. En la maquina Windows 7 se debe descargar la aplicación Rejetto v2.3 para que se pueda ejecutar la explotación, no es una aplicación, por tanto, no se necesita instalar, solo configurar y ejecutar.

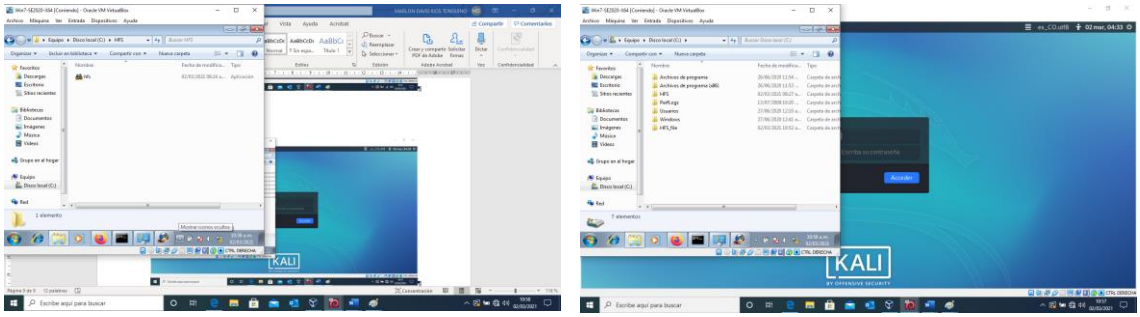
Figura 29 Descarga y Copia de Rejetto V2.3



Fuente: Autor

Para poder identificar los fallos de seguridad de la máquina Windows 7 se utilizó la herramienta Nmap y Metasploit Framework. Con Nmap en sus diferentes variantes se pudo identificar que el puerto 80 abre la aplicación específica en el anexo.

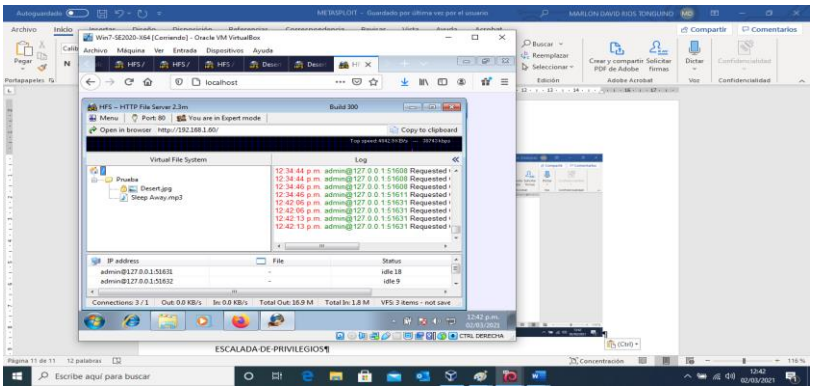
Figura 30 Aplicación HFS y Carpetas para HFS y HFS_Files



Fuente: Autor

En la máquina Windows7-X64 se verifica que los parámetros de configuración de la dirección IP en HFS sean correctos, se cargan automáticamente y se deben seleccionar.

Figura 31 Parámetros configurados HFS



Fuente: Autor

En la Maquina Kali Linux estamos listos para realizar el ataque por medio de la herramienta MetasploitFramework con el comando msfconsole o lanzando la herramienta desde las herramientas de la máquina.

Figura 32 Entorno de Herramienta MetasploitFramework

Fuente: Autor

2.3.4 Descripción ataque a máquina virtual

En este caso vamos a analizar cómo afecta el ataque a la máquina Windows 7 X64). Las debilidades, vulnerabilidades y fallas en sistemas operativos o aplicaciones, se identifican usando las pruebas de penetración. El Pentesting también permite simular métodos que el atacante utiliza para tener acceso a la información de una Empresa. En Windows las vulnerabilidades se explotan por los puertos abiertos, en este caso el 80 siendo fácil de accesar con un exploit y un payload (carga Útil) para abrir una Shell remota conociendo tan solo la IP. Para el ataque se usa MetasploitFramework que proporciona una infraestructura para automatizar tareas rutinarias y complejas permitiendo la identificación de fallas dentro de la máquina. El modo consola de Metasploit Msfconsole posee una base de datos con gran cantidad de exploits permitiéndonos explotar cada una de las vulnerabilidades encontradas

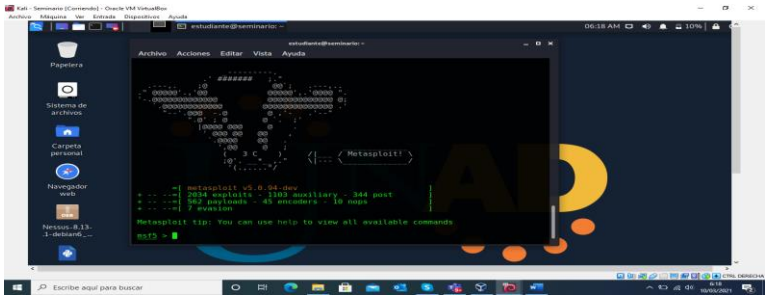
2.3.4.1 Explotación de vulnerabilidades

Ya identificadas las vulnerabilidades definimos cómo aprovecharlas para comprometer el sistema, lo hacemos con MetasploitFramework, utilizando los siguientes comandos:

msfconsole: Da inicio al Metasploit Framework
search: Busca el Exploit
exploit: Lanza ataque, permite tomar ventaja de las fallas en el sistema.
payload: Código o virus que genera un efecto dentro del sistema atacado.
sysinfo: Despliega las características del equipo
getuid: Muestra que nivel de acceso es un usuario
pwd: Ubica el sitio donde se está en el momento
ps: Lista los procesos que están activos

Se Inicia Metasploit Framework con: - ***msfconsole***

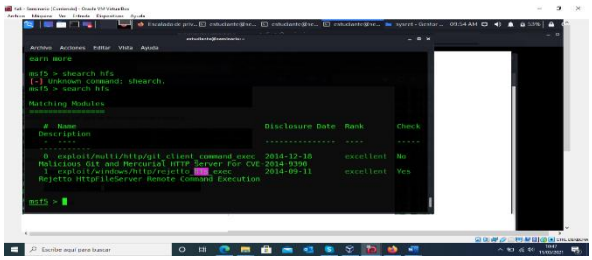
Figura 33 MetasploitFramework Iniciada

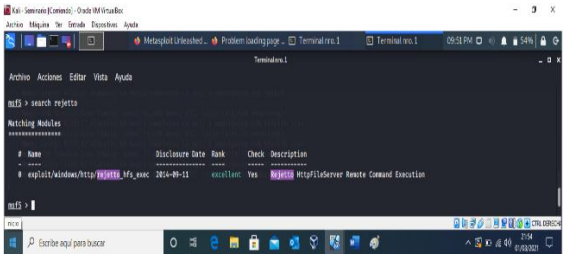


Fuente: Autor

En esta fase conociendo las vulnerabilidades se realiza el ataque directamente y así obtener ingreso al sistema, hacemos uso de los exploits. **Metasploit Framework** tiene una gran base con más de 900 exploits para atacar directamente dispositivos, redes y aplicaciones, el propósito es el acceso al sistema, para nuestro caso la maquina Windows7 X64. Buscamos el Exploit elegido HFS 2.3 server - ***search hfs o rejetto***

Figura 34 HFS y Rejetto encontradas

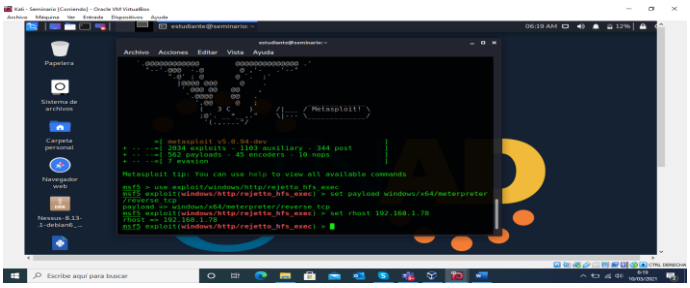




Fuente: Autor

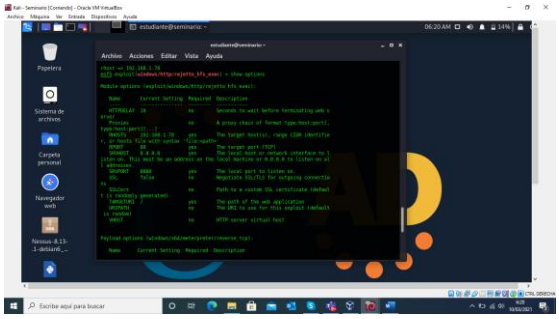
Podemos ver que tenemos el módulo ***exploit / windows / http / rejetto_hfs_exec*** que coincide con el objetivo vulnerable. Cargamos este módulo usando el comando use y configuramos la opción **RHOST** en la dirección IP del objetivo y **RPORT** queda por defecto 8080. También debemos configurar la carga útil o Payload como ***windows / meterpreter / reverse_tcp ,*** el **HOST** local queda en nuestra dirección IP y **LPORT** en los valores por defecto.

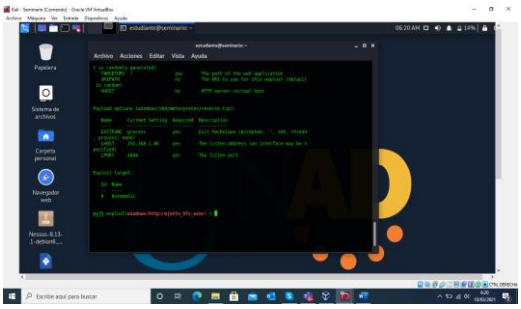
Figura 35 Seteo Opciones del Exploit Rejetto



Una vez que se haya configurado la opción, vemos si todo está configurado correctamente emitiendo el comando show options de la siguiente manera:

Figura 36 Opciones Configuradas en el Exploit

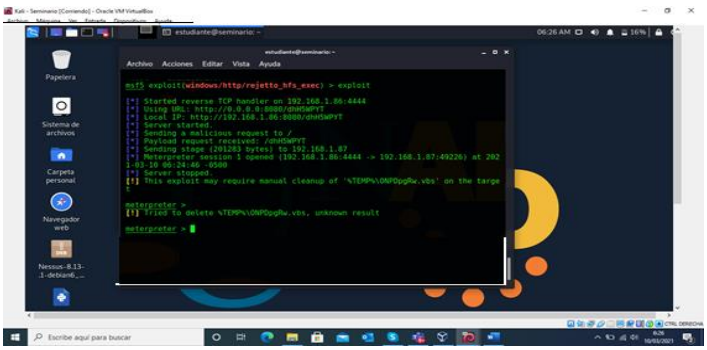




Fuente: Autor

Estando configurado procedemos a atacar el equipo Win7-X64 con el comando: >***exploit***

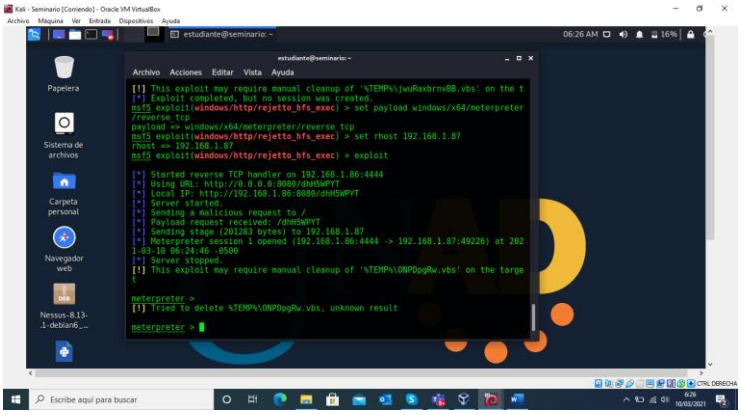
Figura 37 Exploit enviado



Fuente: Autor

Se puede evidenciar que la explotación tuvo éxito y hemos podido ingresar a la herramienta meterpreter que me permitirá tener el control sobre la maquina Windows7-X64 por la respuesta remota que ella nos ha dado por medio del puerto 80 en su estado abierto.

Figura 38 Éxito y sesión meterpreter abierta



Fuente: Autor

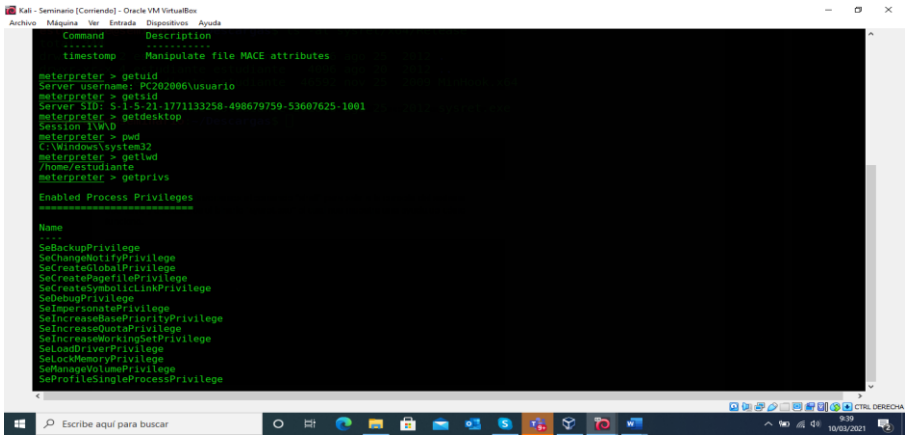
2.3.5 Evidencia intrusión máquina virtual

Se tuvo éxito en la intrusión y con **meterpreter** podemos dar órdenes con comandos y recepcionar más información:

sysinfo Comando para identificar características del equipo en control:

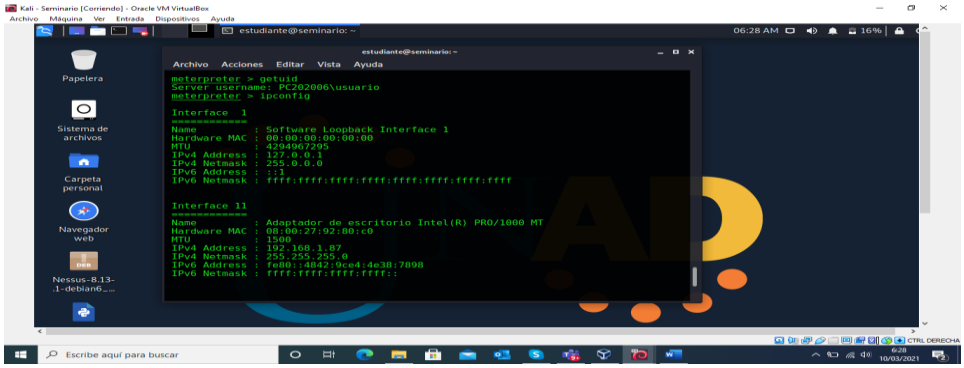
getuid Sabremos cuál es el nivel de acceso que hay en el host.

Figura 39 Comandos de Información del sistema Windows7-X64



Fuente: Autor

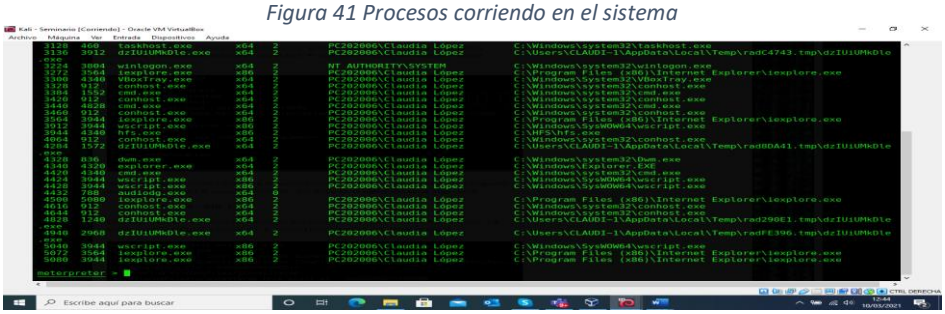
Figura 40 Identificación de Ip máquina atacada



Fuente: Autor

ps Comando para verificar todos los procesos del sistema

Figura 41 Procesos corriendo en el sistema



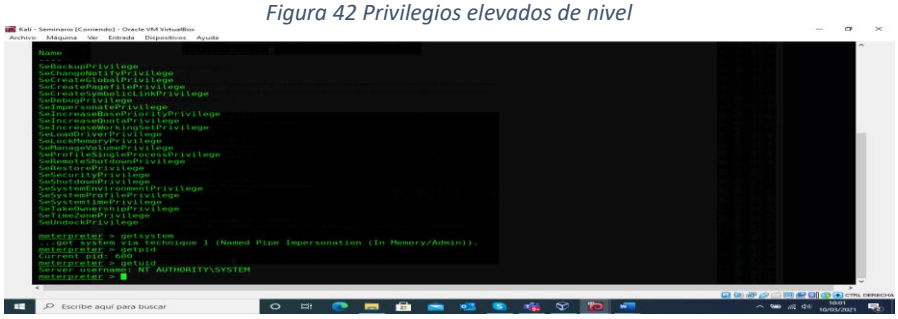
Fuente: Autor

Una vez listados todos los procesos podemos observar el PID ó número identificador del proceso, como la intención es un ataque activo reconocemos el proceso que queremos y lo buscamos para ejecutarlo. En las evidencias anteriores podemos ver que se ha creado y conectado hacia la máquina una sesión en Meterpreter. Al ejecutar e comando ***getsystem*** se elevan privilegios.

meterpreter > ***getsystem***

meterpreter > ***getuid***

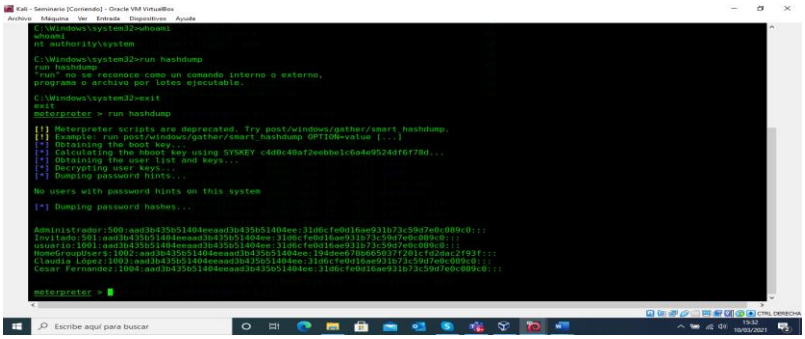
Figura 42 Privilegios elevados de nivel



Fuente: Autor

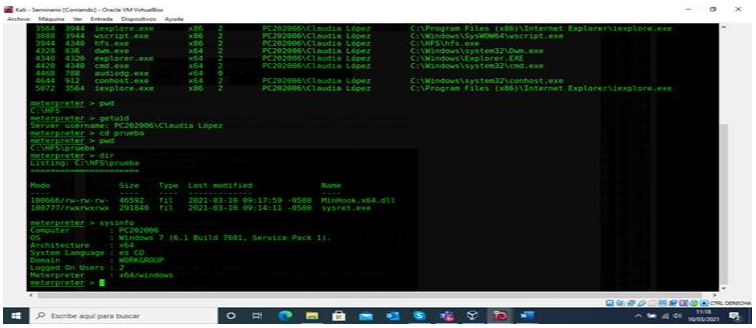
Ahora hay privilegios con nivel de “System” en el sistema Windows. La explotación tuvo éxito y se crea una nueva sesión. Con la cuenta que tenía nivel del usuario “Administrador” hacia la cuenta del nivel “System”, se puede acceder hacia áreas de Windows protegidas. Por ejemplo, podemos visualizar los hashes de las contraseñas del sistema.
meterpreter > ***run post/windows/gather/hashdump***

Figura 43 Contraseñas visualizadas



Fuente: Autor

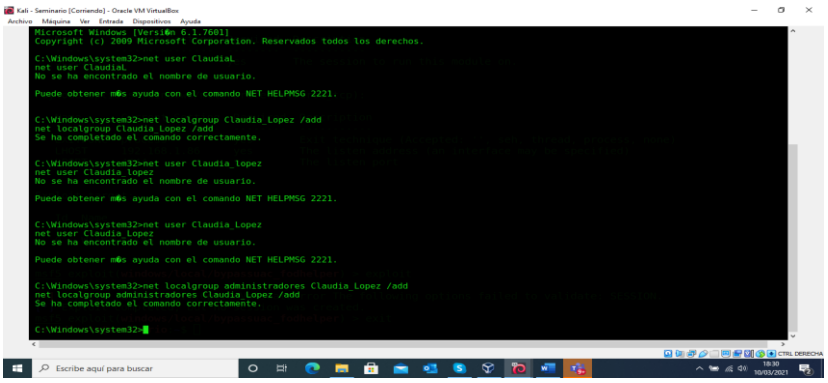
Figura 44 Información obtenida del sistema



Fuente: Autor

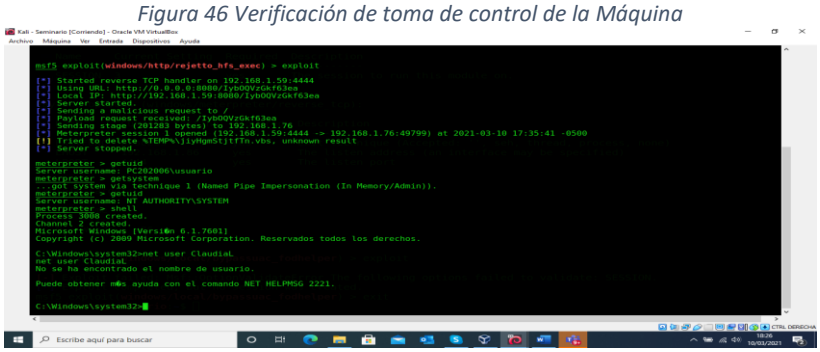
Como el escenario planteado por la empresa en el anexo 4 escenario 3 solicita que se debe crear un usuario con el primer nombre y primer apellido, el usuario debe ser administrador esto con el fin de demostrar una PoC ante los altos directivos, para mi caso he creado el usuario Claudia_Lopez con privilegios de administrador. En la siguiente figura se evidencia el paso a paso de este proceso cuyos comandos son:
Para crear el usuario:
>***net localgroup Claudia_Lopez /add***
Asignar permisos o privilegios de Administrador:
>***net localgroup administradores Claudia_Lopez /add***

Figura 45 Creación de Usuario Administrador



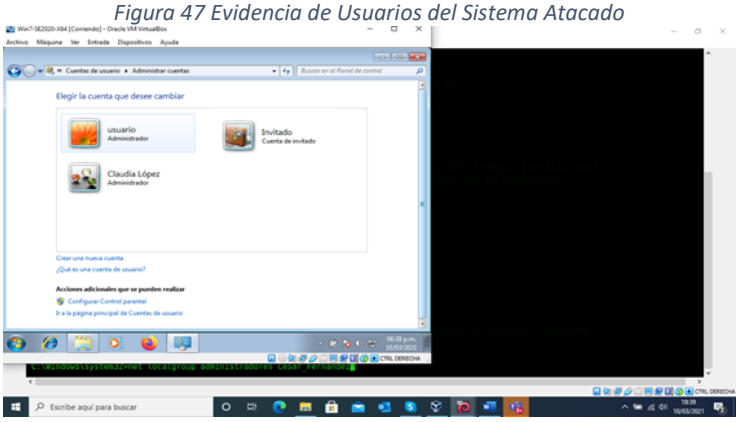
Fuente: Autor

Figura 46 Verificación de toma de control de la Máquina



Fuente: Autor

Figura 47 Evidencia de Usuarios del Sistema Atacado



Fuente: Autor

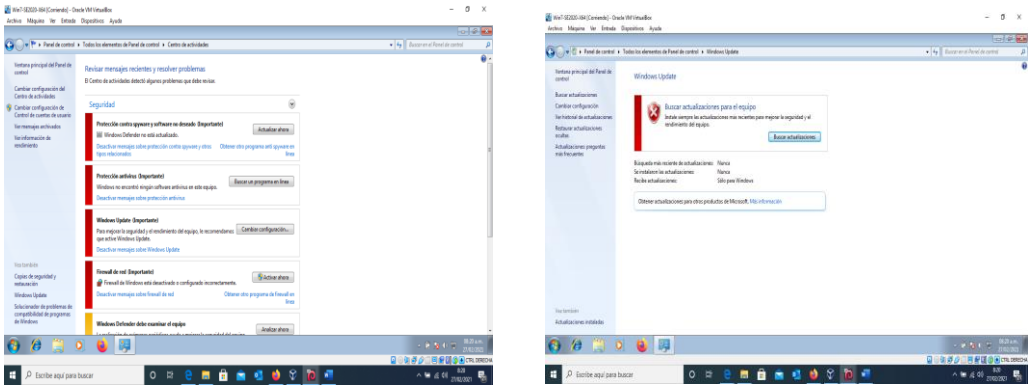
2.4 CONTENCIÓN DE ATAQUES INFORMATICOS

2.4.1 Acciones para un ataque en tiempo real

"¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real?"

2.4.1.1 Validaciones: Primero validar qué tipo de ataque se está presentando, validar con el equipo Red Team cuáles son las vulnerabilidades que tiene el sistema. Según los análisis realizados por el equipo Red Team se evidencian varias fallas entre ellas que los firewalls, el antivirus y Update de los sistemas operativos están desactivados.

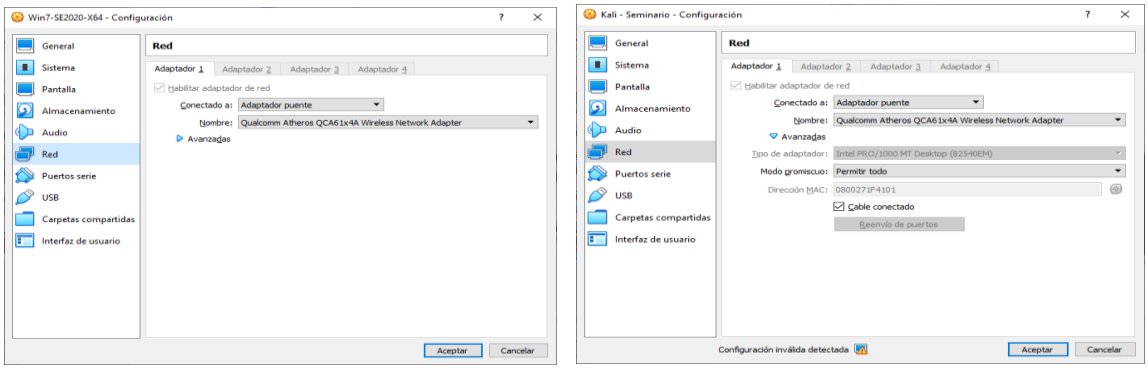
Figura 48.Identificación de firewall, antivirus, Windows update en windos7 x64



Fuente: Autor

Posteriormente se debe validar con el equipo Red Team, el estado de la conexión de red de cada máquina:
Validación de red para las máquinas de Windows7-X64 y Kali Linux.
Para este caso se debe verificar que el modo de configuración del puerto de red sea de Adaptador puente.

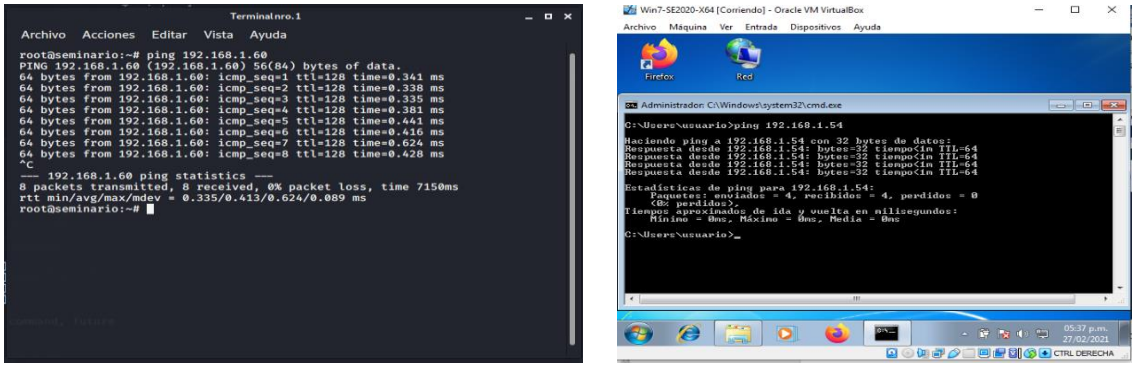
Figura 49 Modo Adaptador Puente Máquinas



Fuente: Autor

Aquí evidenciamos que las maquinas estén viéndose entre sí enviando un ping desde la consola de cada una de ellas

Figura 50 Envío Ping entre Máquinas



Fuente: Autor

2.4.1.2 Fases de Contención: Las acciones básicas para una contención de ataque en tiempo real se pueden definir en 3 fases:

2.4.1.2.1 Prevención:

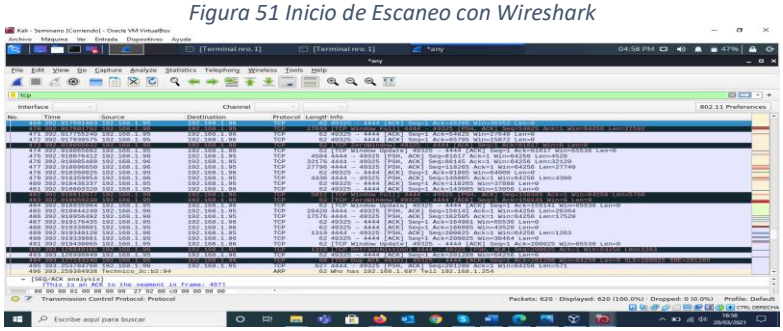
- Establecer procedimientos de prevención, reunir la mayor cantidad de información,
- Comunicarse y concientizar al cliente, esto ayudado con las siguientes medidas:
  - Actualización permanente del software y hardware de los equipos.
  - Instalación, actualización de antivirus y análisis constante de la máquina.
  - Realizar y aislar copias de seguridad.
  - Utilizar contraseñas seguras y robustas para protección del sistema.
  - Ignorar correos desconocidos y evitar descargar archivos sospechosos.
  - Bloquear las direcciones IP no utilizadas.
  - Limitar el acceso a la red.
  - Apagar los servicios no utilizados en la máquina destino para prevenir el escaneo de puertos.

2.4.1.2.2 Detección:

Se debe indagar el tipo de ataque, su alcance mediante monitoreo e incluir a las partes involucradas, esta acción de monitoreo se realiza por medio de un SNIFER (Escaneador o recolector de tráfico) desde la máquina Kali Linux hacia la atacada para verificar el tráfico de paquetes a través de la red. Un Snifer tiene la capacidad de capturar los datos de paquetes, igualmente se puede decodificar y mostrar los campos de uno o varios paquetes de datos. Esta herramienta es útil para analizar problemas en la red, detectar intentos de ataque, vigilar el uso del sistema. Una herramienta seria Wireshark pues es una de las más conocidas, nos permite escanear la red de manera minuciosa, explorar la salida o entrada de paquetes del

ataque o vulneración y está incluida en el sistema Kali Linux cumpliendo así con la recomendación de la empresa que no existe presupuesto para hacer uso de herramientas de pago, esta es open source y no habría erogaciones que realizar.
Desde la máquina Kali Linux se verifica la red y los paquetes incluidos en el tráfico de red y con esto comprobar el tipo de ataque y los datos que quieren extraer. Los tipos de ataques más comunes que podemos encontrar son entre otros, Troyanos, Virus, Phising, Denegación de servicios DoS. En la siguiente figura se evidencia el escaneo de tráfico en la red con Wireshark.

Figura 51 Inicio de Escaneo con Wireshark

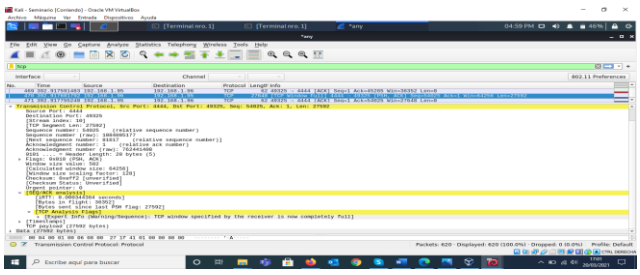


Fuente: Autor

"En la interfaz de usuario (GUI) de la aplicación, cada entrada del resultado del análisis contiene la siguiente información: criticidad, grupo, protocolo y resumen[16], los diferentes niveles y colores usados para diferenciar los estados son los siguientes:

Chat **(gris):** Da información de flujo normal de tráfico.
Nota **(cian):** Se trata de un resultado anormal como el de un código de error.
Advertencia **(amarillo):** Indica alerta, porque puede ser un intento de ataque, se debe prestar cuidado a esta alerta, para nuestro caso particular la aplicación de Rejetto que se está corriendo en la maquina Win7-X64.
Error **(rojo):** Indica que hay graves problemas.

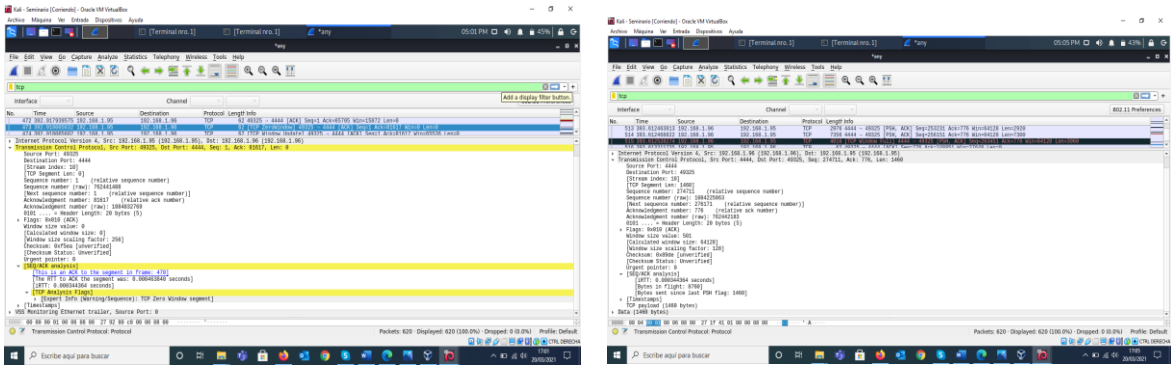
Figura 52 Filtro de Escaneo servicio TCP Maquina Win7-X64



Fuente: Autor

[16] **Expert Infos:** Chapter 7. Advanced Topics
http://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html

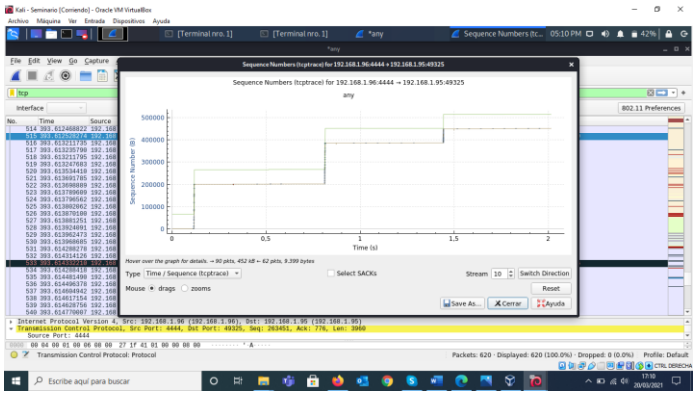
Figura 53 Verificación del Ataque en Win7-X64



Fuente: Autor

Wireshark también nos proporciona muchas formas para evaluar, de manera gráfica, el trabajo en la red, por ejemplo, en nuestro caso hicimos trazabilidad a la sesión TCP.
Se trata de la gráfica *Time Secuencie Graph* (*Steven*) se encuentra en el menú ***Statistics >> TCP Stream Graph*** Para ello hemos seleccionado un paquete de TCP y observamos su gráfica.

Figura 54 Time Secuencie Graph trama TCP seleccionada de la Vulnerabilidad

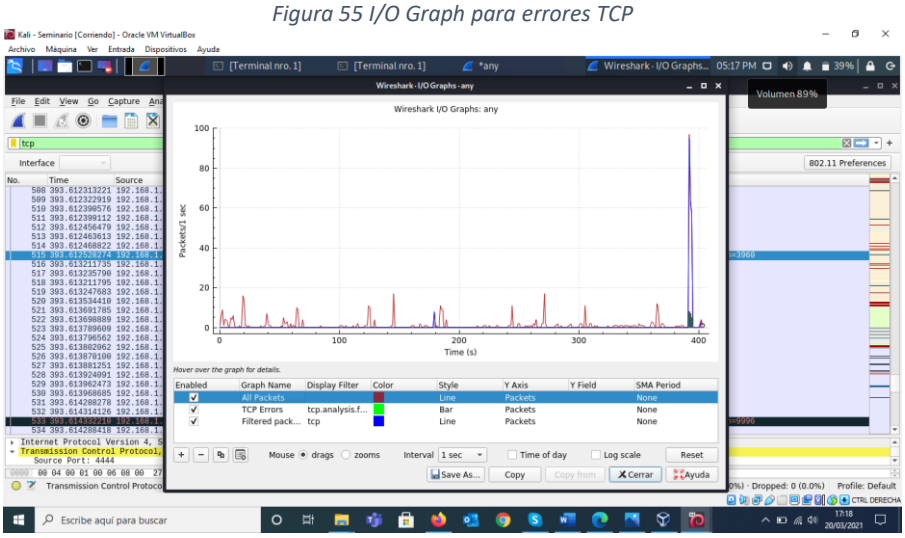


Fuente: Autor

Otra de las gráficas que puede ser útil es la de ***input/output***. Se encuentra en ***Statitics >> I/O Graph***.
Podemos escoger o filtrar las tramas y para nuestro caso también miramos la de TCP que es la que contiene la vulnerabilidad y escoger los colores para su visualización.”

En la Figura 55 - I/O Graph se pueden ver los protocolos separados y observar su proporción respecto al tráfico total escaneado, aquí, se filtró tráfico TCP, de mantenimiento y el tráfico saliente y entrante al servidor.

Figura 55 I/O Graph para errores TCP



Fuente: Autor

2.4.1.2.3 Recuperación: En la recuperación se puede realizar varios objetivos, entre los cuales tenemos: Mitigar las consecuencias del ataque sobre la máquina objetivo utilizando una herramienta de contención apropiada para poder limitar así el impacto y consecuencias del ataque. Utilizar las medidas necesarias para detener el ataque removiendo la amenaza y crear un plan de contingencia que contemple varios aspectos como robo de información, suplantación, bloqueo del sistema y hasta borrado de datos. Regresar al normal funcionamiento de la máquina teniendo en cuenta al detalle el ataque, ajustar las acciones para responder rápidamente a cualquier ataque, con el uso por ejemplo de backups y copias de seguridad.

2.4.1.2.4 Respuesta: Se debe informar el hecho del ataque a los involucrados en toda la organización como son: los clientes, trabajadores y entes gubernamentales para denunciar, explicando las consecuencias del ataque, las acciones tomadas después del daño ocasionado y estar prestos como expertos a responder las inquietudes que se presenten.

2.4.2 Medidas de hardenización

2.4.2.1 "¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team qué medidas de Hardenización propondría para que el ataque no se repita?"

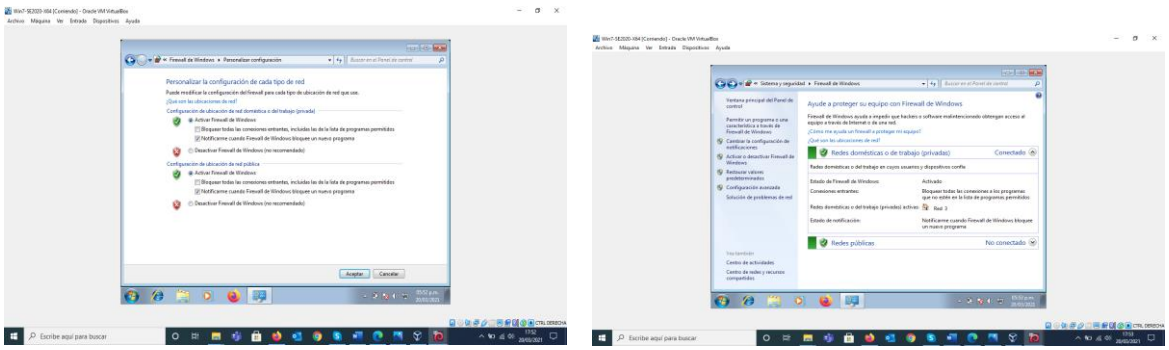
La Hardenización se refiere a configurar una computadora u otros dispositivos de red para resistir ataques, cumpliendo normas de seguridad y analizando las vulnerabilidades. La reducción de ellas se puede lograr mediante la eliminación de servicios, software, usuarios innecesarios en el sistema; también cerrando los

puertos en desuso y otros métodos y técnicas. Para nuestro caso, La máquina virtual Win7-X64, presentó fallas en el sistema operativo y se pudo acceder vía remota, teniendo vía libre a archivos de interés para la empresa. Para proteger la máquina de una nueva intrusión, propongo ejecutar las siguientes actividades en la máquina víctima:

- Actualizar el sistema operativo
- Activar el firewall
- Actualizar o instalar el antivirus
- Bloquear puertos en especial el 80 por donde estaba el rejetto V2.3
- Desactivar el acceso remoto
- Configurar de forma adecuada los permisos de seguridad en carpetas y archivos.

A continuación, se evidencia las acciones de activar el firewall, el antivirus y las actualizaciones del sistema operativo que como se había mencionado anteriormente estaban desactivadas.

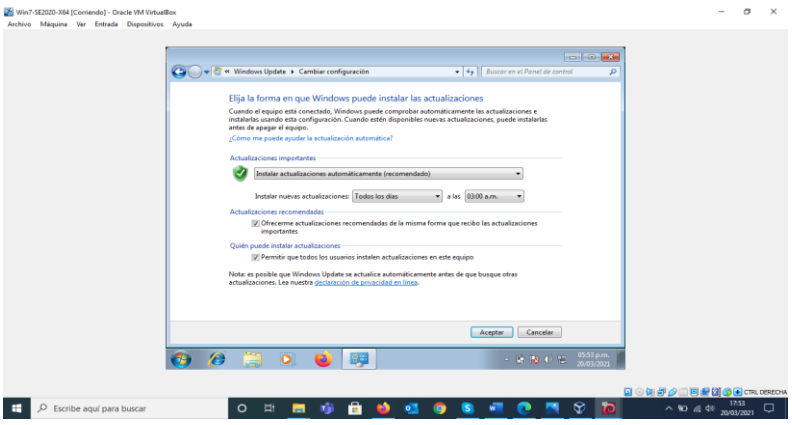
Figura 56 Activación Firewall para todas las redes



Fuente: Autor

También se activó la actualización del sistema operativo

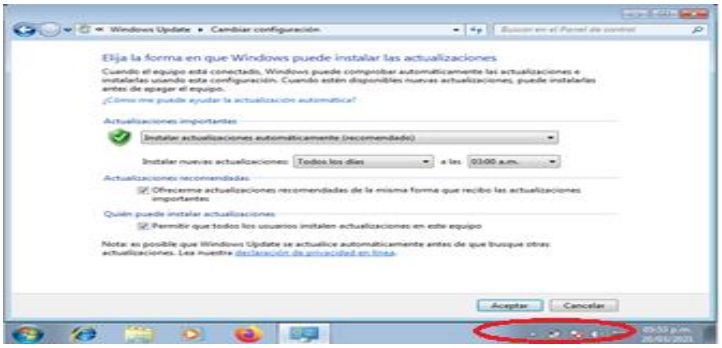
Figura 57 Actualizaciones activadas



Fuente: Autor

Adicionalmente a esas medidas, realizaría en la máquina Windows7-X64, las siguientes acciones de Hardenización:
Instalación segura del sistema operativo, y como principal acción sería realizar las particiones primarias del disco duro, para separar los archivos de datos de las aplicaciones de software que se trabajen en la partición de sistema operativo.
Que las contraseñas sean robustas, con caducidad y se bloqueen con varios intentos fallidos de acceso. Deshabilitar usuarios genéricos, renombrar el usuario administrador y eliminar los usuarios locales que no estén en uso.
Habilitar solo los puertos que se necesiten para servicios específicos y no dejar puertos abiertos.
Una vez realizadas las acciones mencionadas se hizo nuevamente la ejecución del ataque con el exploit, observando que se obtuvo acceso nuevamente a la maquina Windows7-X64, razón por la cual se verificó nuevamente qué acciones pudieron causar de nuevo el ataque, pudiendo evidenciar una señal de alerta en el antivirus, pues no tenía instalado ninguno.

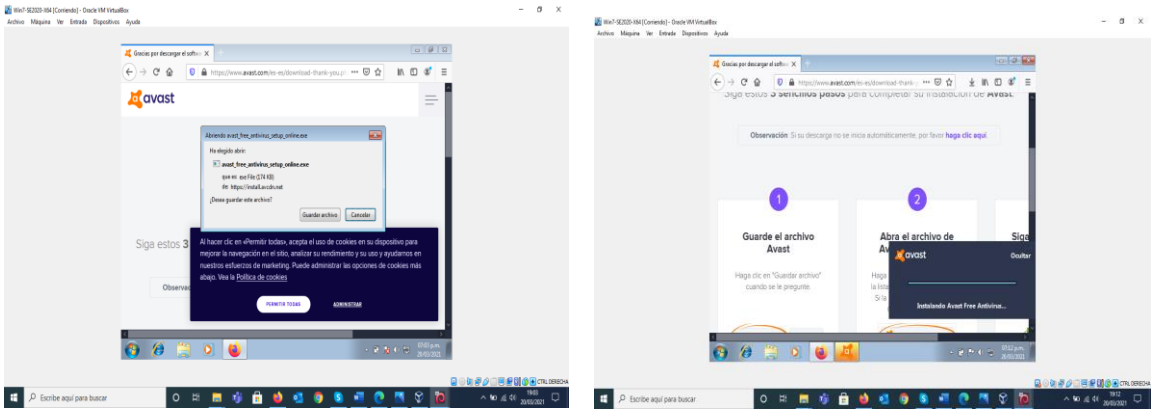
Figura 58 Alerta de Antivirus



Fuente: Autor

Se procede entonces a descargar un antivirus, para realizar su instalación.

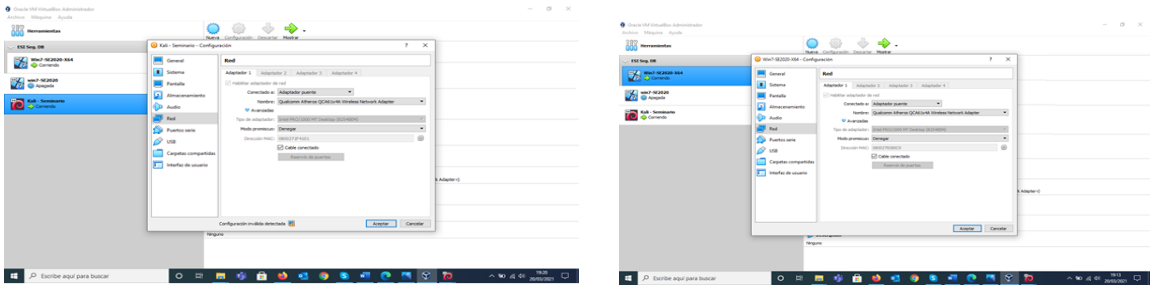
Figura 59 Descarga e Instalación de Antivirus Avast



Fuente: Autor

Igualmente se denegaron los accesos del adaptador puente (modo promiscuo) en ambas máquinas y volver a ejecutar el ataque para verificar que no se pueda acceder nuevamente a la máquina.

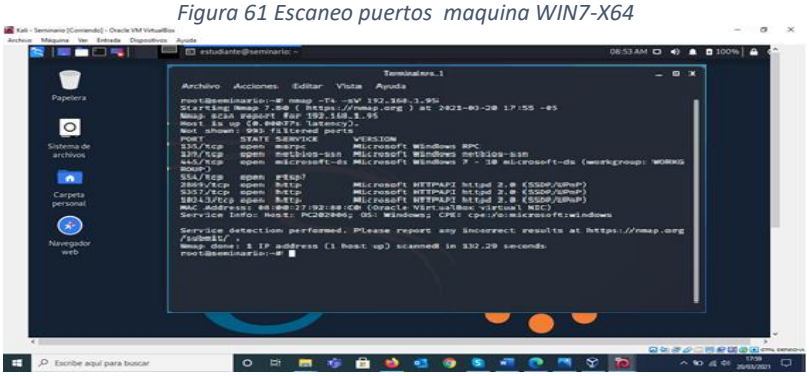
Figura 60 Modo promiscuo denegado



Fuente: Autor

Procedemos a comprobar el estado de los puertos con la herramienta Nmap y así verificar la seguridad por medio de los puertos y los servicios, observando que en el puerto 80 ya no está la aplicación rejjetto y tampoco está abierto.

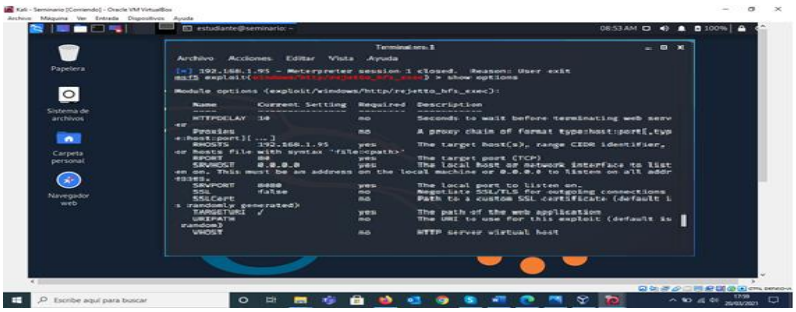
Figura 61 Escaneo puertos maquina WIN7-X64



Fuente: Autor

Se verifica el estado de las opciones del exploit

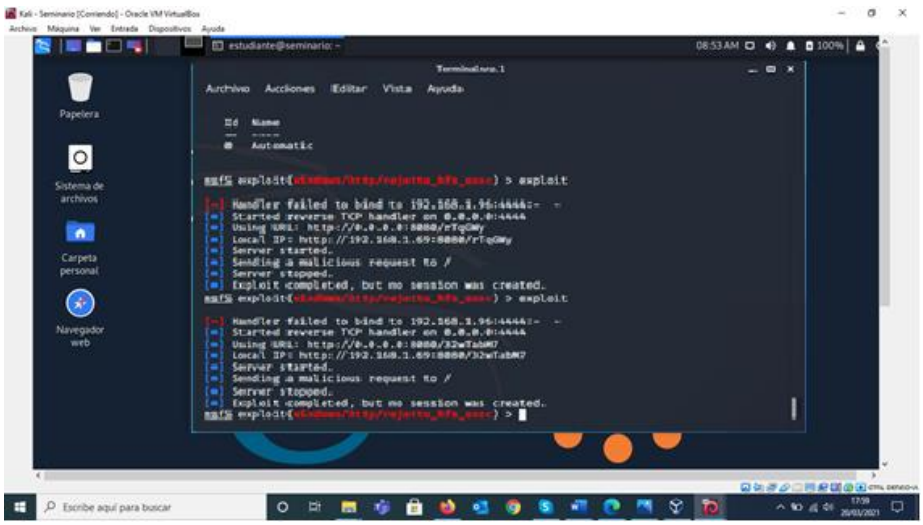
Figura 62 Opciones para exploit Rejetto



Fuente: Autor

Se realiza nuevamente el intento de taque por medio del exploit, verificando que no fue posible abrir la sesión de meterpreter para acceder a la maquina Windows7-X64

Figura 63 Ejecución del exploit sin éxito



Fuente: Autor

2.4.3 Diferencia entre equipo blueteam y equipo de respuesta a incidentes informáticos

2.4.3.1 "Describa con sus palabras las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos."

La tabla siguiente resume las diferencias más relevantes que encontré entre un equipo Blue Team y un equipo CSIRT.

Tabla 1 Diferencias entre Blue Team y CSIRT

Equipo Blue Team	Equipo de respuesta a incidentes informáticos CSIRT
Analiza comportamientos del sistema, aplicaciones y personas	Identifica las causas y consecuencias del incidente por medio de la preservación y documentación de la evidencia
Analiza y evalúa riesgos, auditorias e implementa soluciones SIEM	Analiza las situaciones y responde a los incidentes.
Ataque: riesgo, amenaza.	Incidente: hecho real o sospechoso
Análisis forense de las máquinas afectadas, propone soluciones y establece medidas de detección para casos futuros.	Endurecimiento de infraestructura y software para reducir el número de incidentes a largo plazo.

Equipo Blue Team	Equipo de respuesta a incidentes informáticos CSIRT
Basado en la seguridad defensiva	Enfocado en las incidencias de seguridad informática
Enfocado en la contención de ataques proponiendo mejoras para la Ciberseguridad de una Empresa.	Gestión de incidentes de una organización mayor (Gobierno, Universidad, Institución educativa, Empresa del orden Nacional.)
Rastreo de incidentes de Ciberseguridad	Gestión de incidentes de Ciberseguridad.
Verifica la efectividad de las medidas de seguridad	Respuesta rápida y efectiva a incidentes para que la organización opere con total normalidad
Vigilancia permanente, con un proceso de documentación completa que permite ejecutar procedimientos en beneficio de la organización	Vigilancia periódica pues los objetivos son específicos.

Fuente: Autor

2.4.4 Uso y finalidad de CIS "center for internet security"

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

CIS (Center For Internet Security): El objetivo del CIS es mantener la seguridad de internet, con actividades que permitan identificar, realizar, evaluar y aportar soluciones para los procesos de ciber-defensa. Tiene varios controles y herramientas para la configuración de seguridad de la máquina o sistema elegido, cumpliendo éstos con la normatividad establecida.

Considero que sí se debe utilizar el CIS pues trae beneficios como servir de guía para establecer el listado de prioridades y actividades a desarrollar en cada proceso de contención.
Los CIS son estándares para que así se pueda verificar el cumplimiento de la protección de información. Estos CIS están divididos en 3 grandes grupos que son: Básicos, Fundamentales y Organizativos los cuales se mostrarán en las siguientes tablas, donde NNT NEW NET TECHNOLOGIES Security Trough System Integrity define los siguientes ítems para contencion de ataques así: "**Change Tracker Gen 7 R2** proporciona prevención y detección de ciberseguridad fundamental y crítica, **Fast Cloud** es una tecnología de archivos aprobados y seguros en la nube, **Log Tracker** proporciona una solución SIEM con todas las funciones, **Vulnerability**

Tracker asegurará que cualquier vulnerabilidad conocida pueda identificarse dentro de su infraestructura de TI antes de que sea explotada"[17].

Tabla 2 Controles CIS Básicos

CIS Controles de seguridad críticos asignados a soluciones NNT					
	Control de seguridad crítico CIS	Change Tracker Gen7 R2	Fast Cloud	Log Tracker	Vulnerability Tracker
BÁSICOS	CIS 1: Inventario de Dispositivos permitidos y no permitidos	■			▬
	CIS2: Inventario de Software	▬			▬
	CIS3: Gestión permanente de vulnerabilidades				▬
	CIS4: Control en uso de privilegios administrativos	▬			
	CIS5: Seguridad en configuración para hardware y software en PC móviles, puestos de trabajo, portátiles y servidores.	▬			
	CIS6: Análisis y monitoreo de LOGS de auditoría		▭	▬	

Fuente: NNT NEW NET TECHNOLOGIES Security Trough System Integrity

■ Cobertura Completa ▭ Cobertura Parcial

Tabla 3 Controles CIS Fundamentales

CIS Controles de seguridad críticos asignados a soluciones NNT					
	Control de seguridad crítico CIS	Change Tracker Gen7 R2	Fast Cloud	Log Tracker	Vulnerability Tracker
FUNDAMENTALES	CIS7: Protección de navegadores y correo electrónico	▭			
	CIS8: Defensa contra malware	▭		▬	
	CIS9: Control en protocolos, puertos de red y servicios	▬			▭
	CIS10: Recuperación de datos				
	CIS11: Configuración segura de Firewall, Switches y Routers.	▬			
	CIS12: Defensa de borde	▭			▭
	CIS13: Protección de información	▭	▭		
	CIS14: Control de acceso de conocimiento	▭			
	CIS15: Control de acceso inalámbrico	▭			
	CIS16: Control y monitoreo de cuentas	▬		▬	

Fuente: NNT NEW NET TECHNOLOGIES Security Trough System Integrity

[17]NEW NET TECHNOLOGIES NNT Security Trough System Integrity https://www.newnettechnologies.com/products.html

▬ Cobertura Completa ▭ Cobertura Parcial

Tabla 4 Controles CIS Organizativos

CIS Controles de seguridad críticos asignados a soluciones NNT					
	Control de seguridad crítico CIS	Change Tracker Gen7 R2	Fast Cloud	Log Tracker	Vulnerability Tracker
ORGANIZATIVOS	CIS17: Programa de capacitación y concientización en seguridad				
	CIS18: Seguridad para aplicaciones de software	▭	▭		
	CIS19: Gestión y respuesta de incidentes				
	CIS20: Pruebas de intrusión y ejercicios de Red Team	▭			

Fuente: NNT NEW NET TECHNOLOGIES Security Trough System Integrity

▬ Cobertura Completa ▭ Cobertura Parcial

2.4.5 Funciones y caracteristicas de un SIEM

Explique y redacte las funciones y características principales de lo que es un SIEM. "SIEM significa Security Information and Event Management, se trata de una combinación de dos conceptos: **SIM** (Security Information Management) y **SEM** (Security Event Management). La unión de estos dos conceptos plantea un enfoque basado en software que permite obtener una visión completa de la seguridad informática. Un sistema **SIEM** considera siempre los requisitos específicos de la empresa, teniendo presente que existan definiciones claras e individuales sobre cuales procesos y eventos son relevantes para la seguridad, igualmente de qué forma y con qué prioridad se debe reaccionar ante ellos. El Security Information and Event Management puede entenderse también como un conjunto completo de normas para los estándares de seguridad existentes y de directrices que ayuden a mantener la calidad de las operaciones informáticas de una empresa"[18].

2.4.5.1 Funciones SIEM: Entre las principales funciones de un SIEM se tienen:
Registros: Recolección, análisis, retención, estudio forense de registros
Supervisión de: Registro de la aplicación, actividad de los usuarios, integridad de los archivos.
Alertas: En tiempo real, auditoría de acceso a objetos.
Prioridades: Reportes, cumplimiento de TI, correlación de eventos, cuadros de mando.

[18] ¿Qué es SIEM (Security Information and Event Management)
https://www.ionos.mx/digitalguide/servidores/seguridad/que-es-siem/

2.4.5.2 Características SIEM: Los SIEM poseen entre otras las siguientes características:

- Capacidad de gestionar la información de seguridad, se puede monitorear en tiempo real los eventos, con notificaciones e información de seguridad.
- Almacena los logs de los usuarios, guardando información sobre lo que realizan los usuarios cuando acceden a ciertas zonas. Si alguien entra a una zona restringida se puede observar su actividad, si hace algo anormal, si cambia configuraciones, etc., también almacena información no solo del usuario sino del posible atacante, su IP, por ejemplo.
- Identificar un ataque o amenaza e informar como alerta o notificación, estos avisos nos permitirán estar al día de todos los eventos de seguridad y proteger a tiempo la Información de la Empresa.
- No es limitado solo a un activo, puede proteger todos nuestros activos, desde los computadores de cada trabajador hasta los servidores.
- Centralización de la información y eventos, proporcionando un punto común. La centralización automatiza tareas, ahorra tiempo y dinero, detecta anomalías de seguridad y visualiza datos históricos en una línea de tiempo.

Un SIEM estará caracterizado por los factores anteriores que, en su conjunto, permitirán dar soporte de manera más precisa y eficaz ante los riesgos que podrían poner en peligro a una compañía.

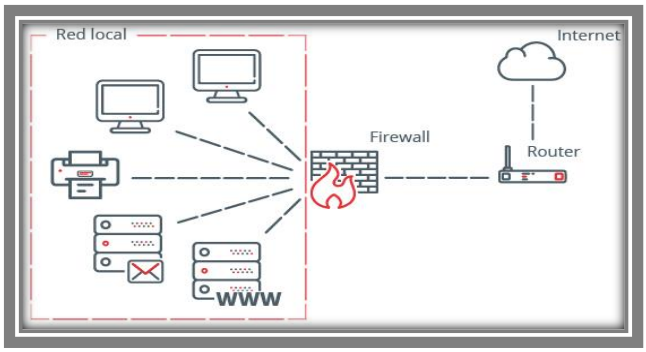
2.4.6 Herramientas de contencion de ataques informáticos

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.
De acuerdo con la observación descrita en el anexo 5 Escenario 4 he seleccionado varias herramientas que permitan contener ataques y que sean de licencia GPL (licencia de derechos de autor ampliamente usada en el mundo del software libre y código abierto).

2.4.6.1 FIREWALL: Considerada como la principal y primera herramienta de contención, impide tanto el acceso como la salida de la red de ciertos paquetes de datos que incumplen las normas de seguridad pre establecidas en la configuración del mismo. Cuando recibe una petición no habitual o sospechosa desde la red bloquea el puerto y aísla el dispositivo o dirección IP.
Los firewalls por hardware vienen instalados casi siempre en los routers administrables, los de software simulan el comportamiento de los firewalls de hardware, vienen pre configurados con soluciones informáticas o sistemas operativos como el firewall de Windows donde el usuario puede establecer el nivel de dureza o de protección de éste.[19]

[19] Protege tu empresa. https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

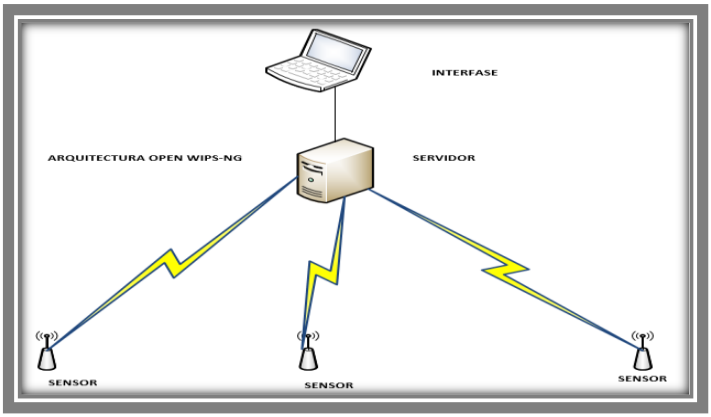
Figura 64 Red de Empresa con Firewall



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

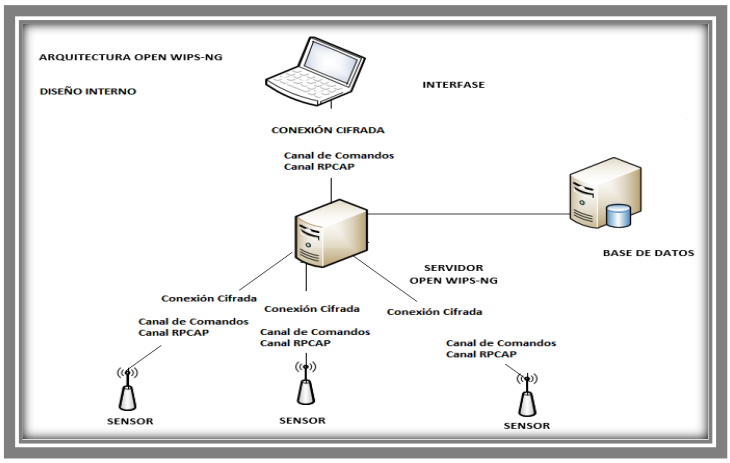
2.4.6.2 OPEN WIPS-NG: Se trata de un sistema de detección y prevención de ataques inalámbricos basados en tres componentes: (Como se muestra en la fig. 65 y 66)
Sensores: Responden a las amenazas, capturan el tráfico enviándolo para su posterior análisis. **Servidores:** Alerta y responde ante amenazas, analizan los datos enviados por los sensores.
Interfaces: Muestra detalles sobre los ataques en las redes inalámbricas.

Figura 65 Arquitectura OPEN WIPS-NG



Fuente: Propia con base en apuntes de Thomas d'Otreppe, autor de Aircrack-ng

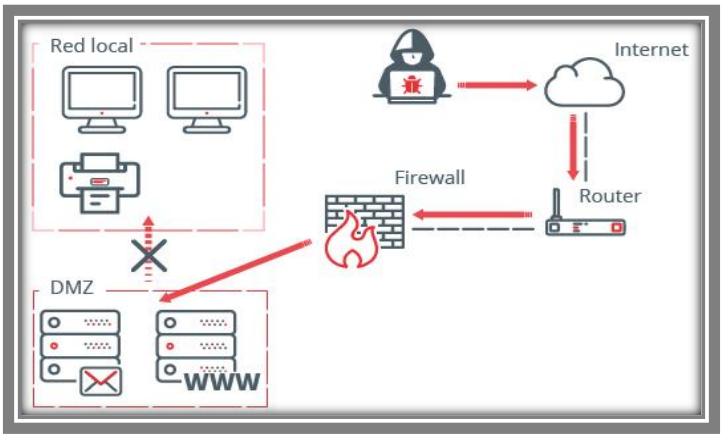
Figura 66 Arquitectura de diseño interno Open WIPS-NG



Fuente: Propia con base en apuntes de Thomas d'Otreppe, autor de Aircrack-ng

2.4.6.3 SNORT: Herramienta de código abierto para análisis y registro de paquetes en tiempo real, puede identificar los ataques DoS y DDoS, útil para la detección de gusanos, exploits y exploración de puertos. Nos permite saber si el tráfico coincide con alguna de las reglas lo cual rechazará dicho tráfico y bloqueará al atacante.
2.4.6.4 DMZ: Zonas desmilitarizadas, forman parte de una red aislada al interior de la red interna de la empresa. En esta zona se ubican los servicios y recursos con acceso desde internet como servidores de correo y servidores web.
La principal característica de una DMZ es no permitir conexiones que van desde la DMZ a la red local, y permitir conexiones procedentes tanto de Internet, como de Intranet de la empresa, como en la siguiente figura.

Figura 67 Configuración DMZ



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

3. CONCLUSIONES

A continuación, se relacionan algunas conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

- Considero que en general todos los actores de la sociedad deberían desarrollar estrategias para adquirir conocimientos en materia de ciberseguridad con el apoyo gubernamental y con políticas claras para que así pueda ser perdurable en el tiempo sin depender de quien esté a la cabeza de la nación, estas políticas deben ser operativas y que ayuden a cambiar el conocimiento implícito por el conocimiento preciso acerca de ciberseguridad.

- Actualmente el enfoque de la ciberseguridad ha cambiado mucho y se debe prestar mayor importancia a gestionar los riesgos en el ciberespacio donde podemos concluir entonces que la ciberseguridad consiste más en aplicar procesos de análisis y gestión de los riesgos que se presentan al usar, procesar, almacenar y transmitir datos o información todo esto basado en estándares internacionales

- Se debería tener como objetivo primordial la gestión del conocimiento sobre ciberseguridad y poder así transferir este saber y la experiencia que hay entre todos los actores y profesionales que tienen la responsabilidad de proteger el ciberespacio, para que asi este conocimiento esté disponible para el resto de personas y la sociedad en general.

- Podría decir sin lugar a equivocarme, tanto mis valores como mi ética Profesional y actuación en el marco de la legalidad no me permiten que por el atractivo dinero que representa el gran salario ofrecido en un acuerdo presentado por una organización realice actos ilegales que vayan en contravía de mi formación personal y profesional, estoy para contribuir al mejoramiento de nuestra sociedad y no para destruirla.

4. RECOMENDACIONES

Dentro del marco de la seguridad informática, se plantean entre otras las siguientes recomendaciones que permitan endurecer los aspectos de seguridad en una Organización:

- Uno de los aspectos a fortalecer debe ser la protección de los datos personales tanto al interior de la empresa como en internet, esta información solo debe ser accedida por el personal autorizado y capacitado y los empleados deben conocer todas estas medidas de seguridad y permitirles únicamente lo necesario y por ende aceptar las restricciones y fines de la recopilación de información.

- Importante también es lo relacionado con los dispositivos de la organización, éstos deben ser muy seguros y encontrarse protegidos en su totalidad, se recomienda que nunca sean sustraídos de la empresa pues se puede presentar allí vulneración de la seguridad, de la misma forma se debe prestar especial cuidado a la red inalámbrica pues muchas intrusiones llegan por este medio, entonces debe tener alta seguridad y no ser visible para personas externas a la organización.

- En la infraestructura física se pueden presentar varios problemas, y para ello es aconsejable crear una política para actuar y seguir en el momento que se presente alguna situación de amenaza a la seguridad como robos, incendio, amenazas contra la integridad del personal, escapes de gas, pérdida de elementos de ingreso (llaves, Tarjetas etc.) y poder asi proteger los activos y medios de información de la empresa.

- Es importante no delegar gran responsabilidad a empleaos recién ingresados pues no tendrían la suficiente confianza y podrían informar a la competencia o a particulares sobre datos de los clientes, estrategias, incluso contraseñas de usuarios y formas de ingreso a la información crítica y confidencial.

- Socializar con los integrantes de la empresa lo importante de las políticas generadas para la seguridad, capacitarlos en la actualización de normatividad y procedimientos requeridos para la seguridad informática, poner en contexto a todo el personal acerca de la necesidad de cumplir el código de ética.

REFERENCIAS BIBLIOGRAFICAS

ALCALDÍA DE BOGOTÁ. (2018). Guardianes de la información Penetration Testing. Alcaldía de Bogotá. {En línea}. {Consultado el 5 de febrero de 2021}. Disponible en: http://ticbogota.gov.co/sites/default/files/seguridad-de-lainformacion/ambito2.pdf

ALLEN, Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD (pp. 33-40). {En línea}. {Consultado el 3 de febrero de 2021}. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf/

ÁLVAREZ, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. (pp. 1-26) {En línea}. {Consultado el 2 de febrero de 2021}. Disponible en: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf/

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29) {En línea}. {Consultado el 3 de febrero de 2021}. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

CIS SECURITY. (2020). CIS Center for Internet Security. CIS Benchmarks. Recuperado de: https://www.cisecurity.org/cis-benchmarks/

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

GAVIRIA, Raúl. (2015). Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira. (pp. 18-61). Recuperado de: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. (2018). (p. 14 - 27) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

INCIBE. (2014). OWASP Testing Guide v4.0. Guía de seguridad en aplicaciones Web. INCIBE-CERT. Recuperado de: https://www.incibe-cert.es/blog/owasp-4

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

MINTIC. (2018). Elaboración de la política general de seguridad y privacidad de la información. Mintic. (pp. 17-24) {En línea}. {Consultado el 3 de febrero de 2021}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf/

MINTIC. (2009). Ley 1273 [LEY_1273_2009].Mintic. (pp. 1-4) {En línea}. {Consultado el 4 de febrero de 2021}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf/.

MINTIC. (2012). Ley 1581 [LEY_1581_2012]. Mintic. (pp. 1-11) {En línea}. {Consultado el 4 de febrero de 2021}. Disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf/

MINTIC. (2018). Guía de aseguramiento del Protocolo IPv6. Mintic. (pp. 21-35) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

MINTIC. (2018). Guía de Auditoria. Mintic. (pp. 12-19) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

MINTIC. (2018). Guía de Transición de IPv4 a IPv6 para Colombia. Mintic. (pp. 46-57) Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

MORENO, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq.(pp. 31-63) Recuperado de: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

OAS. (2018). Convenio Sobre La Ciberdelincuencia. OAS. (pp. 3-26) Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf/

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

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

RAPID7. (2012). Metasploitable 2. (s. f.). Metasploit. Recuperado de: https://metasploit.help.rapid7.com/docs/metasploitable-2

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. Recuperado de: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

ANEXOS

- Link para acceso al video de sustentación del Informe Técnico.
  https://www.youtube.com/watch?v=5kzn66gNI_8

- Link para acceso a la plantilla de sustentación del Informe Técnico.
  https://drive.google.com/drive/u/0/folders/17Fm7J_GSQcUbD77N_o2btOnEZeU_vpwy