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

ALUMNO:
MAURICIO SÁNCHEZ SABOGAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

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

MAURICIO SANCHEZ SABOGAL

Proyecto de Grado – Seminario Especialización presentado para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMATICA

Tutor de Curso
JOHN FREDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2021

TABLA DE CONTENIDO

LISTA DE FIGURAS

TABLAS

RESUMEN

La continuidad de los negocios no siempre depende solo de un grupo de personas específicas que sacan adelante un negocio, esta continuidad debe estar de la mano de los avances tecnológicos y la forma correcta en que se use la tecnología para dar respuesta a muchos de los cambios estratégicos en las organizaciones. Es por esta razón que los equipos estratégicos tecnológico cobran gran importancia en esta continuidad ya que por medio de estos se hace un uso eficiente y eficaz de la tecnología de seguridad de la información y se hace necesario de igual forma estrategias para salvaguardar los activos de las empresas, es por ello que nacen estos equipos estratégicos tecnológicos para el fortalecimiento en cuanto a la seguridad de la información y la Ciberseguridad.

En primera instancia se describen y se analizan las metodologías de pruebas de penetración, contención y detección que son usadas en la actualidad no solo por organizaciones gubernamentales sino empresas privadas e instituciones académicas en busca de la educación en Ciberseguridad por medio de los equipos de seguridad denominados Blue Team y Red Team.

El seminario cursado da las pautas iniciales para el entendimiento de dichos equipos y sus estrategias tecnológicas en esta búsqueda del equilibrio tecnológico seguro para la preservación de sus activos por medio de Pentesting y estrategias de contención y erradicación.

Palabras Clave:

Equipos Estratégicos, Ciberseguridad, Seguridad de la Información, Ofensiva, Medida Defensiva, Detección. Estrategias de Contención, Equipo de Seguridad, Equipos de Respuesta a Incidentes, Blue Team y Red Team

GLOSARIO

Pruebas de Penetración o Pentest[1]: "Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad."

Red Teams[2]: El día hoy Red teams ha evolucionado bastante y han llegado a convertirse en una fuerza de la seguridad informática. Esta revolución de los equipos rojos se usa por organización gubernamentales y privadas para probar el estado actual de la seguridad física, digital, desafiar las medidas defensivas y conceptos y políticas de seguridad.

Blue Teams: Las funciones de Blue Team son las de analizar sistemas de las organizaciones para poderlos proteger adecuadamente, identificado vulnerabilidades, evaluar efectividad de herramientas y las policitas de seguridad. Este grupo también evalúa la red operativa en búsqueda de vulnerabilidades, proporciona técnicas de mitigación a sus clientes u organizaciones independientemente de su postura de seguridad.

Pentesting[3]: Es un conjunto de ataques que se simulan hacia un sistema informático con el objetivo de detectar vulnerabilidades para que puedan ser corregidas y o pueden ser usadas. Estos procesos usan:

Toma de información, recolección de información
Análisis de vulnerabilidades encontradas
Informe de si los ataques tuvieran o no éxito, y en caso positivo que podrían obtener en el ataque y las posibles respuestas de erradicación para las vulnerabilidades detectadas

Vulnerabilidad[4]: Consiste en una actividad que permite materializarse a una amenaza, esto quiere decir que tener vulnerabilidades es a fin ya que no hay protección para que la amenaza se materialice. Actualmente evidencian ataques

---

[1] INCIBE, Glosario de Seguridad, Pentest [Online, Visitado 20 Septiembre 2021), Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

[2] Que es Red Team , [Online, Visitado 24 Septiembre 2021), Disponible en: https://redteams.net/redteaming/2013/what-is-a-red-team

[3] Que es Pentesting, INCIBE, [Online[, Visitado 25 Septiembre 2021, Disponible en:, https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

[4]BACA Urbina, Introducción a la seguridad informática, Definiciones de Seguridad Informática, Pág. 30

que son intencionados y no intencionados a los cuales las empresas pueden ser vulnerables o no vulnerables.

Exploit: Es un ataque se hace sobre una vulnerabilidad de algún software este puede instalar un malware y dar al atacante control o acceso a algún sistema. Son desarrollados para atacar.

Metasploit: Herramienta software desarrollada que puede ser usada por auditores y equipos estratégicos como BlueTeam y RedTeam y sus derivados para el uso en procesos de investigación de las vulnerabilidades de sistemas con el objeto de determinar los riesgos y amenas expuestas de muchos sistemas.

Herramienta de Seguridad: Tienen como objetivo brindar protección, controlar, proteger información sensible de las organizaciones.

SIEM: Son plataformas de inteligencia de la seguridad para la respuesta, detección y neutralización de las amenazas de seguridad por medio del análisis en tiempo real de las infraestructuras tecnológicas.

CIS: Organizaciones establecidas en controles de CIS Control y CIS Benchmarks más usadas a nivel mundial la cuales se basan en el intercambio de información como recursos confiables para la prevención y protección y recuperación ante las amenazas cibernéticas por medio de mejores prácticas de seguridad.

CVE: La misión del Programa CVE es identificar, definir y catalogar las vulnerabilidades de Ciberseguridad divulgadas públicamente. LAS VULEABILIDADES se registran en un catálogo y publicadas por organizaciones en todo el mundo para su uso sin restricción.

COPNIA: Consejo Profesional Nacional de Ingeniería es una entidad encargada del control y vigilancia del ejercicio de las profesiones de la ingeniería Por medio de las competencias ordenada por la ley en función de la ética profesional.

1. INTRODUCCIÓN

Las formas y métodos para la protección de la información deben ir de la mano con la demanda tecnológica en la búsqueda de ese punto de equilibrio y fortaleza tecnológica y que vayan con el objetivo organizacional, es por ello que el uso de herramientas, metodologías y conociendo el aspecto legal como un enfoque defensivo en contra de las vulnerabilidades, amenazas y los riesgos que implica la aplicación de todos estos aspectos para la protección correcta de los activos de la organización y su infraestructura.

El seminario propuesto y cursado muestra las acciones usadas por equipos estratégicos Blue Team y Red Team como respuesta a incidentes tecnológicos que se pueden dar al interior de las organizaciones.

En el trascurso del proceso de capacitación autónoma se logran evidenciar varios aspectos a lo largo de la interpretación de distintos escenarios propuestos, dentro de estos escenarios se tocan puntos importantes como los aspectos legales y legislación colombiana frente al delito informático, actuaciones éticas como ejemplos de posibles anomalías en contratos mal estructurados, etapas en los proceso de Pentesting usados como la base de laboratorios prácticos para la detección de vulnerabilidades que se logran explotar con la ayuda de las herramientas usadas por los equipos estratégicos Red Team y Blue Team como evidencia de las falencias de seguridad que pueden presentarse en varios escenarios. Por último, se hace el estudio de las estrategias que podrían usarse por el equipo Blue Team en los procesos de contención y corrección de las vulnerabilidades detectadas y las posibles herramientas estandarizadas y tecnológicas para poder hacer frente a las amenazas y vulnerabilidades.

2. DEFINICION DE PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

Las tendencias a nivel mundial debido al aumento de los ataques ofensivos según estudios realizados por organizaciones como la CCN CERT (Centro Criptológico Nacional Computer Emergency Response Team) han ido en aumento por la pandemia de COVID 19, según la revisión del reporte anual en 2020 y 2021 se puedo estimar en los últimos 12 meses el aumento en las operaciones y tecnologías que se usan en las organizaciones para disminuir el impacto de Ciberamenazas, y que según el análisis se logra observar que el uso de las técnicas como las pruebas de penetración con un porcentaje del 53.3% en uso, 34.0% de las organizaciones lo planea usar y el 12.7% no lo tiene planeado usar.

Ilustración 1 Tecnologías usadas y de la gestión de seguridad y previstas para su adquisición

	Currently in use	Planned for acquisition	No plans
Patch management	58.1%	30.3%	11.6%
Advanced security analytics (e.g., with machine learning, AI)	57.1%	35.5%	7.4%
Security configuration management (SCM)	55.4%	32.9%	11.7%
Security information and event management (SIEM)	55.1%	33.3%	11.6%
Vulnerability assessment/management (VA/VM)	55.0%	34.9%	10.1%
Penetration testing / attack simulation software	53.3%	34.0%	12.7%
User and entity behavior analytics (UEBA)	51.8%	36.1%	12.1%
Full-packet capture and analysis	51.0%	36.8%	12.2%
Security orchestration, automation and response (SOAR)	48.6%	37.1%	14.3%
Threat intelligence platform (TIP) or service	48.2%	38.4%	13.4%

Fuente: CYBEREDGE, Cyberthreat Defense Report 2020, Tecnologías operativas y de gestión de la seguridad en uso y previstas para su adquisición, [sitio web]. [Consultado: 10 de Mayo 2022]. Disponible en: https://cyber-edge.com/resources/2020-cyberthreat-defense-report/

Otros estudios y resultados de los grupos de seguridad informática en las organizaciones vienen tomando cada vez más fuerza a nivel regional como Colombia varias organizaciones y empresas particulares hacen esfuerzos para poder poner en desarrollo sus proyectos basados en los equipos de seguridad como Blue Team, Red Team y ahora con más frecuencia el uso de los equipos Purple Team que sería la convergencia entre los dos equipos Blue y Red.

Algunos de los equipos conformados en años anteriores y que han funcionado como plataformas de entrenamiento en Ciberseguridad dan sus primeros avances y pudieron a llegar a ser en el concepto técnico, tecnológico de lo que hoy conocemos como los grupos de seguridad Blue Teams y Red Teams. Dentro de estos primeros grupos tenemos iPhalanx antes denominada ASCET que se enfocaba en 4 tipos de ejercicios la Ciberdefensa enfocada en ejercicios de defensas de los sistemas mediante la automatización, el Ciberataque enfocada en el entrenamiento con objetivos fijos, la Ciberguerra enfocada en la creación de dos grupos que se defienden y atacan mutuamente y el Análisis forense enfocado en el análisis después de un ataque. XNET que fue desarrollada por CERT de la universidad de Carnegie Mellon y se basa en el entrenamiento, simulación y la creación de escenarios como por ejemplo de protección de una red o información clasificada es usada por organizaciones del estado, NATIONAL CYBER RANGE (NCR) desarrollada por el departamento de los estados unidos y las universidades de John Hopkins , Lockedd Martin y supervidada por DARPA se trata de una plataforma de formación para científicos y militares en la búsqueda de perfeccionar las tecnologías de búsqueda de vulnerabilidades por medio de hardware y software por emdio de entornos virtuales.

SANS NETWARS como plataforma privada de aprendizaje y de eventos de seguridad en la que por medio de equipos de seguridad donde se pueden hacer pruebas de evaluación de vulnerabilidades, pruebas de penetración, análisis de Malware, respuesta de incidentes, practicas forenses, está por ser de gran costo solo es accedida pro aquellos que pueden pagar sus costos. SAIC CYBERNEXS desarrollada por SAIC funciona como una plataforma de entrenamiento y competiciones donde los participantes pueden hacer ataques, analizar las redes, defenderse de ataques, hacer análisis forense y hacer pruebas de penetración.[5]

En la universidad Nacional Abierta y Distancia UNAD se han elaborado varios trabajos de grado donde se estudia la temática de las metodologías de pentesting enfocadas al Hacking ético como:

Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, seccional Armenia. “Este trabajo busca evidenciar cómo es posible que, a través de un hacking ético, basado en la metodología abierta de testeo de seguridad – OSSTMM, es posible encontrar vulnerabilidades y

[5] CCN-CERT, INFORMES PUBLICOS, Ciberamenazas y Tendencias. Edición 2015 - 2020 [sitio web]. [consultado: 2 Junio 2021]. Disponible en: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html?limit=100

determinar el nivel de seguridad informática de una organización, como lo es la Dirección Ejecutiva Seccional de Administración Judicial de Armenia, Quindío."[6]

Estudio de las mejores prácticas de Ethical Hacking, para generar un nuevo método que facilité la ejecución de análisis de seguridad enfocados a pruebas de penetración. "El objetivo principal el desarrollo de diferentes simulaciones prácticas acerca una prueba de penetración, dentro dela cual serán mencionadas algunas de las principales metodologías a nivel internacional para la realización de pentesting a redes informáticas, así como la identificación y uso de algunas de las fases que en ellas se expresan, utilizando un entorno de red controlado, donde se explotan varias vulnerabilidades de máquinas virtuales con diferentes sistemas operativos, siguiendo los pasos mencionados."[7]

2.2 FORMULACION DEL PROBLEMA

En las sociedades actuales que basan su funcionamiento en la tecnología en muchos de su aspectos organizacionales y donde mucho de los estudios recientes indican que en los años 2020 y 2021 muchos cambios generados por la pandemia a nivel social y económico donde muchas de las empresas han replanteado su forma de trabajo como la virtualidad, trabajo remoto, compras y ventas online, aumento de transacciones por medios virtuales de la banca y la masificación del uso de internet para toda labor ha producido que se aumente el riesgo de sufrir algún tipo de ataque informático.

De acuerdo con estos cambios las amenazas tecnológicas también han aumentado, los niveles de riesgo y las vulnerabilidades para las empresas que usan las tecnologías de la información y las comunicaciones es por ello por lo que se hace necesario el uso de estrategias tecnológicas que permitan soportar las infraestructuras tecnológicas y salvaguardarlas de una manera eficaz y eficiente ante cualquier incidente de seguridad que surgiera. Es por ello por lo que se plantea el siguiente interrogante.

¿Cómo los equipos estratégicos BlueTeam y RedTeam pueden proporcionar a las organizaciones la seguridad necesaria para el fortalecimiento de su infraestructura tecnológica y bajar el riesgo de un posible ataque informático

---

[6] ZULUAGA Mateus, ALLEN David, Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, UNAD Armenia 2017 [sitio web]. [consultado: 5 de Mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/17410

[7] AVILA GUALDRÓN Miguel Andrés, Estudio de las mejores prácticas de Ethical Hacking, para generar un nuevo método que facilité la ejecución de análisis de seguridad enfocados a pruebas de penetración. UNAD 2018, [sitio web]. [consultado: 5 de Mayo 2022]. Disponible en: https://repository.unad.edu.co/handle/10596/21293

3. JUSTIFICACION

En el entorno de la seguridad informática y de los incidentes de seguridad en Colombia se evidencia un aumento en el número de incidentes del 28 % en promedio de los últimos 10 años , según CCTI “Cámara Colombiana de Informática y Telecomunicaciones” se han presentado más de 45.000 mil casos, con un incremento de 89% frente al año 2019 y 2020, este aumento en época de pandemia entre marzo y diciembre de 2020 reporto un incremento de 101% con unos 37.000 mil reportes, los delitos con mayor incremento son los de suplantaciones de sitios Web, Phising, Spoofing y Pharming y para el robo de datos con un crecimiento exponencial de 303%, además de casos de distribución de malware en las redes organizacionales, otro delito reportado fue el de vulneración y violación a los datos personales con un crecimiento de 174%. Con base a estas evidencias y estudios con datos y eventos el siguiente trabajo radica en la necesidad de proteger los activos de las organizaciones y que mantengan la disponibilidad, integridad y la confidencialidad de la información que manejan

Es por estas razones y con base a las cifras con crecimiento de incidentes de seguridad que la importancia del siguiente trabajo de análisis practico y que por medio de un informe técnico que permita mostrar cómo se puede lograr la conformación de equipos de trabajo Blue Team y Red Team en la necesidad primordial de mantener la integridad, disponibilidad y la confidencialidad de la información en las infraestructuras tecnológicas que manejan, procesan y almacenan la información.

Otra razón importante es que por medio del informe técnico elaborado que se hace necesaria que en las organizaciones se adopten una postura de defensa acorde a las necesidades de seguridad tanto de proceso de gestión, análisis de vulnerabilidades y manejo de los riesgos y que sean capaces de responder ante los incidentes de seguridad, es por ello que la creación de grupos estratégicos como RedTeam Y BlueTeam se hacen necesarios dentro de las organizaciones para poder identificar, tratar y remediar los fallos de seguridad que se posean en la infraestructura organizacional y de esta forma minimizar los riesgos asociados a cada activo.

4. OBJETIVOS

2.1 Objetivo General

Realizar el análisis técnico y documental para determinar que son, para que sirven y porque son usados dentro de las organizaciones los equipos estratégicos RedTeam y BlueTeam

2.2 Objetivos Específicos

Determinar cuál es la legislación colombiana frente al delito informático como base ética para la conformación de equipos estratégicos de Ciberseguridad en la organización The WhiteHose Security.

Usar fases de pentesting como equipo RedTeam en casos específicos de infraestructuras para determinar las vulnerabilidades expuestas.

Usar las vulnerabilidades expuestas y poder hacer explotación de estas por medio de herramientas usadas por el equipo estratégico Redteam

Determinar como equipo BlueTeam las medidas contención y con el uso de herramientas y métodos de hardering para la corrección de las vulnerabilidades expuestas.

Analizar herramientas de contención robustas que permitan tener un control de análisis y respuesta a incidentes por parte de los equipos estratégicos de una forma técnica, centralizada e inmediata ante los incidentes de seguridad de las organizaciones.

Indicar conclusiones y recomendación acerca de los equipos estratégicos en las organizaciones.

5. DISEÑO METODOLÓGICO

El proyecto desarrollado está enmarcado dentro del tipo de autoestudio, indagación y desarrollo de fases:

- Fase de análisis de datos en información de distintas fuentes
- Fase de montaje de Bancos de trabajo
- Fase de desarrollo de laboratorios
- Fase de conclusiones y recomendaciones de desarrollo

6. DESARROLLO

6.1 ETAPA PRIMERA CONCEPTUALIZACION LEGAL Y DE EQUIPOS DE SEGURIDAD

“Leyes, decretos” existen actualmente y las características principales de cada ley.

6.1.1 Reglamentación Legal En Colombia

CONPES 399524 “Se convierte en una política nacional que tiene como objetivo poder establecer las medidas para la confianza digital y poder mejorar la seguridad digital de forma que el país sea una sociedad competitiva en el futuro digital”. Su plan de acción se basa en el fortalecimiento de la capacidad de la seguridad digital de las personas y los sectores públicos y privados para la seguridad digital. Su otro objetivo se centra en el marco de la gobernanza digital y mejorar su seguridad, y adoptar estándares y marcos de seguridad digital de nuevas tecnologías[8]

CONPES 3701 donde se describen los lineamientos para las políticas de Ciberseguridad y Ciberdefensa, describe como desarrollar políticas de prevención y control como parte de planes de desarrollo del país.[9]

CONPES 3854 como política de la seguridad digital donde se indican las condiciones para la gestión del riesgo de la seguridad digital mediante mecanismos de participación, capacitaciones y marco legal basados en la gestión de los riesgos de la seguridad digital.

DECRETO 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Derogado Parcialmente por el Decreto 1081 de 2015. Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma[10]. Este decreto se basa en la posibilidad

---

[8] CONPES 3995, POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL, [sitio web]. [Consultado: 30 de Septiembre 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

[9] CONPES 3701, [sitio web]. [Consultado: 30 de Agosto 2021]. Disponible en: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

[10] PRESIDENCIA DE LA REPUNLICA, DECRETO 1377, [sitio web], [Consultado: 30 de Septiembre 2021]. Disponible en:

de que cada persona como titular autorice o no el uso y tratamiento de sus datos e información de acuerdo a la ley 1581 establecida, se deben manejar aspectos como el aviso de privacidad, dato público, datos sensibles, transferencia y trasmisión.

LEY 1581 2012 Su objeto es el desarrollar el derecho que poseen cada persona de conocer, actualizar y modificar los datos que hayan sido tomados y recolectados de las bases de datos o de archivos, esta ley es aplicable a cualquier dato registrado y almacenado en cualquier base de datos que puede ser usada por entidades públicas y privadas y de los demás derechos que están en el artículo 15 y 20 de la constitución política de Colombia.[11]

Algunas excepciones de esta ley indican bases de datos personales y de ambiente particular. Bases de datos de defensa nacional que se usan por entes del gobierno en contra por ejemplo del terrorismo y lavado de activos. Bases de inteligencia, bases periodísticas y las que están en la ley 1266 de 2008.

DECRETO 1377 2013 este reglamenta la Ley 1581 de 2012. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

DECRETO 1727 2009 que reglamenta y determina de la ley 1266 de 2008 en la cual los bancos de datos de información financiera, crediticia y comercial y de servicios y que provienen de terceros países deben dar información de los titulares de esta información.

LEY 1266 DE 2008 indica las disposiciones generales para la información contenida en bases de datos financieras, de créditos que vienen de terceros países para Habeas Data financiera y de la seguridad en los datos personales**.**

LEY 527 de 1999 indica y reglamenta el acceso y el uso de mensajes de datos de comercios y de las firmas digitales además de establecer cuáles son las entidades de certificación. Indica la aplicación, comunicación y suscriptores de los requisitos jurídicos de los mensajes de datos.[12]

LEY 1621 DE 2013 con esta ley se busca reglamentar las normas que fortalezcan el marco jurídico donde los organizamos que hacen procesos de inteligencia y contrainteligencia puedan cumplir con su misión legal y constitucional en el caso de las medidas de seguridad informática funcionaria como una ley de inteligencia y

---

[Consultado: 30 de Septiembre 2021]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

[11] LEY 1581, LA PROTECCIÓN DE DATOS PERSONALES, [sitio web]. [Consultado: 30 de Septiembre 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[12] LEY 527, [sitio web]. [Consultado: 30 de Septiembre 2021]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

seguridad y que se aplicaran en el ámbito donde sean requeridas y según el caso o medida del gobierno.[13]

LEY 1273 2009 esta ley tipifica los nuevos tipos de penalidades relacionadas con los delitos informáticos y la protección de datos e información, además indican las penas en las que se incurriría por el delito de 120 meses y de las multas de hasta 1500 salarios mínimos legales mensuales.

El Capitulo primero tipifica atentados contra confidencialidad, disponibilidad e integridad de datos y sistemas con los siguientes artículos:

Artículo 269A. Acceso ilegal o abusivo a cualquier tipo de sistema Informático
Artículo 269B. Se refiere a detener o denegar el uso correcto de forma Ilegítima a cualquier tipo de sistema Informático o de sistemas de la red de telecomunicaciones.
Articulo 269C. Se refiere a la apropiación o interceptación de los datos Informáticos por cual quiera medio que se dispongan
Articulo 269D. Daño Informático
Articulo 269E. Uso de Software Malicioso sobre un sistema informático
Articulo 269F. Violación de los Datos Personales
Artículo 269G. Suplantación de sitios web para capturar Datos personales
Articulo 269H. Circunstancias De Agravación Punitiva de los artículos anteriores donde se evidencian aumentos de penas según el tipo de delito.

Las penas por este tipo de delitos se resumen en la imagen teniendo en cuanta el cambio de salario mínimo cambia cada año.

[13] LEY 1621, [sitio web]. [Consultado: 30 de Septiembre 2021]. Disponible en: http://www.dni.gov.co/wp-content/uploads/2018/10/Ley-1621-del-17-de-Abril-de-2013.-Ley-de-Inteligencia-y-Contrainteligencia.pdf

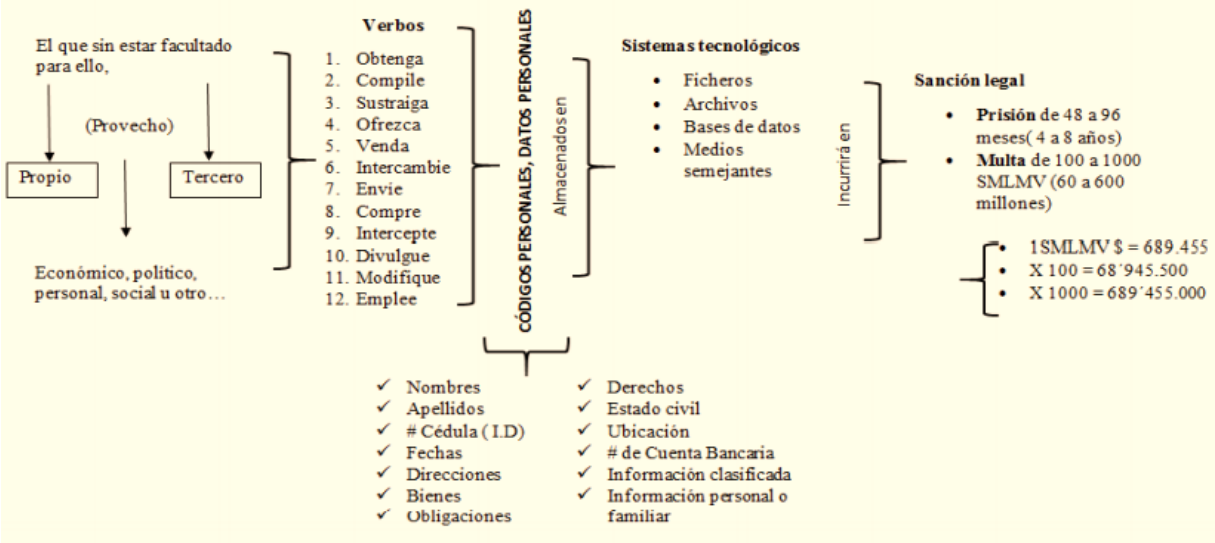


Ilustración 2 Información Punible

Fuente: https://repository.unilibre.edu.co/bitstream/handle/10901/9778/S%C3%A1nchez_Cano_2016.pdf?sequence

El capítulo Segundo habla de los atentados informáticos y otros delitos y se establecen dos artículos:
Artículo 2691 que indica el robo por algún tipo de medio informático
Articulo 269J que indica la transferencia que no es autorizada de activos de cualquier tipo.

6.1.2 Etapas De Pentesting

Las etapas de los proceso de penetración se logran identificar 4 etapas fundamentales que se deben seguir para obtener resultados y objetivos de las mismas

Ilustración 3 Etapas Pentesting

Fuente: Elaboración propia

Etapa de Planificacion y Recoleccion de datos: En esta estapa se obtiene el primer contacto con la infraestrcutura a trabajar y los componentes organzaicionales que la forman, se debe crear una infraestrcutura tecnica para todo el proceso de pentesting. En esta no se usa ninguna herrameinta especifica para escaneo de algo pero si se usan metodos de investigacion para saber que datos e informacion esta disponible de la organización en fuentes como internet o con el uso de herramientas de Google como Google Hacking Database (GHDB) o conocidos como Google Dorks para obtener informacion como Ftp o sistemas de adminstracion Web no configurados, bases de datos expuestas entre otros datos sencibles.

En algunos casos podemos hacer uso de algun software para hacer copias de los sitios web sus enlaces, imágenes y codigos de los objetivos para poder tenerlos y usarlos fuera de linea para posteriores detecciones y obtencio de datos e informacion.

Otra forma de obtencion de datos de la empresa objetivo es por medio de Whois para tener informacion de IPS, DNS, direcciones, o correos entre otros datos.

Etapa Descubrimiento e Identificación de vulnerabilidades

Se puede establecer en esta etapa el tipo de pruebas a realizar si son de tipo pasivas o activas, automáticas o manuales. En esta etapa se hace un proceso de análisis de datos recopilados de la fase anterior y se hace un análisis de las posibles vulnerabilidades. En esta etapa se hace uso de herramientas específicas y según el objetivo de la prueba para el escaneo de vulnerabilidades y teniendo en cuenta si es necesario el ciclo de vida la gestión de las vulnerabilidades que involucre el análisis de las vulnerabilidades y se haga uso de calificaciones de las vulnerabilidades como el uso de métricas CVE

Algunas de las herramientas tipo escáneres usadas de tipo común y globalizado en esta fase son el NMAP para determinar y hacer escaneo de puertos de las infraestructuras, otras más específicas usadas como OpenVas o Nessus que realizan análisis automatizados de vulnerabilidades, otras herramientas usadas en esta fase también son más específicas como escáneres para aplicaciones Web o escáneres de vulnerabilidades de red. Una vez se hace uso de estas herramientas se da un primer indicio de las vulnerabilidades y las posibles consecuencias de estas.

Etapa Ejecución y Explotación de Vulnerabilidades

En esta etapa se realiza el proceso de explotación de las vulnerabilidades descubiertas de la fase anterior, se hace uso de las vulnerabilidades para poder tener acceso a los sistemas ya sean bases de datos, aplicaciones, servicios, servidores, etc. Se debe documentar todo el proceso de explotación para los informes finales.

En esta fase se hace uso de Exploits de tipo cliente, remoto o local para explotar estas vulnerabilidades, estos Exploits son usados en frameworks uno de los más usados es el MetaSploit. Esta etapa requiere una gran cantidad de pruebas de explotación para poder violar los sistemas vulnerables ya que cada sistema posee características que son diferentes y su comportamiento cambia.

En esta fase es importante hacer uso de herramientas que permitan la persistencia de los ataques con el tiempo con el uso de software como Ncat que abra puertas traseras o Backdoors que permitan hacer ataques en el tiempo y evadir algunos sistemas de seguridad.

Etapa de Documentación, Reportes e Informes

Una vez se culminan todas las fases anteriores se debe hacer el proceso de documentar todo lo realizado de una forma coherente y organizada que permita detallar cada etapa y los resultados que se han evidenciado.

Este tipo de informes debe ser lo más explícito posible para que cualquier tipo de persona o la dirección de las organizaciones pueda entenderlos sin dificultades sin dejar de lado el lenguaje técnico propio de cada prueba realizada.

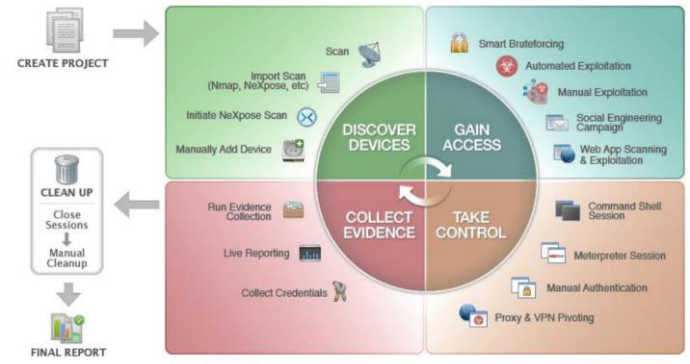
En muchas ocasiones se deben hacer varios tipos de informes separados uno donde se indiquen los aspectos más técnicos y propios del proceso de pentesting y otros informes específicos para la gerencia con resultados más orientados como datos estadísticos, sistemas que se pueden ver afectados, número de usuarios afectados, perdidas, etc.

En los informes finales siempre se deben indicar estrategias que sirvan de mitigación o de corrección de los fallos encontrados o que ayuden a tomar las decisiones adecuadas para evitar las vulnerabilidades expuestas.

6.1.3 Herramientas de Ciberseguridad

Tabla 1 Algunas Herramientas de Ciberseguridad

Nombre	Descripción
Openvas 	"OpenVAS es un escáner de vulnerabilidades automatizado e integrado que originalmente comenzó como una bifurcación del proyecto Nessus." Este software puede detectar distintos tipos de vulnerabilidades según su nivel de criticidad y complejidad tanto de dispositivos de red y otros dispositivos conectados. Este sistema cuenta con sistema operativo GreenBone GOS, GSF, cuenta con una interfaz Web. Posee una base de más de 78.000 pruebas de vulnerabilidad (VT), estas vulnerabilidades que encuentra las clasifica según su gravedad lo que permite su análisis para el tratamiento. Este tipo de software permite el descubrimiento del estado actual el mejoramiento del estado actual y la revisión de las medidas tomadas

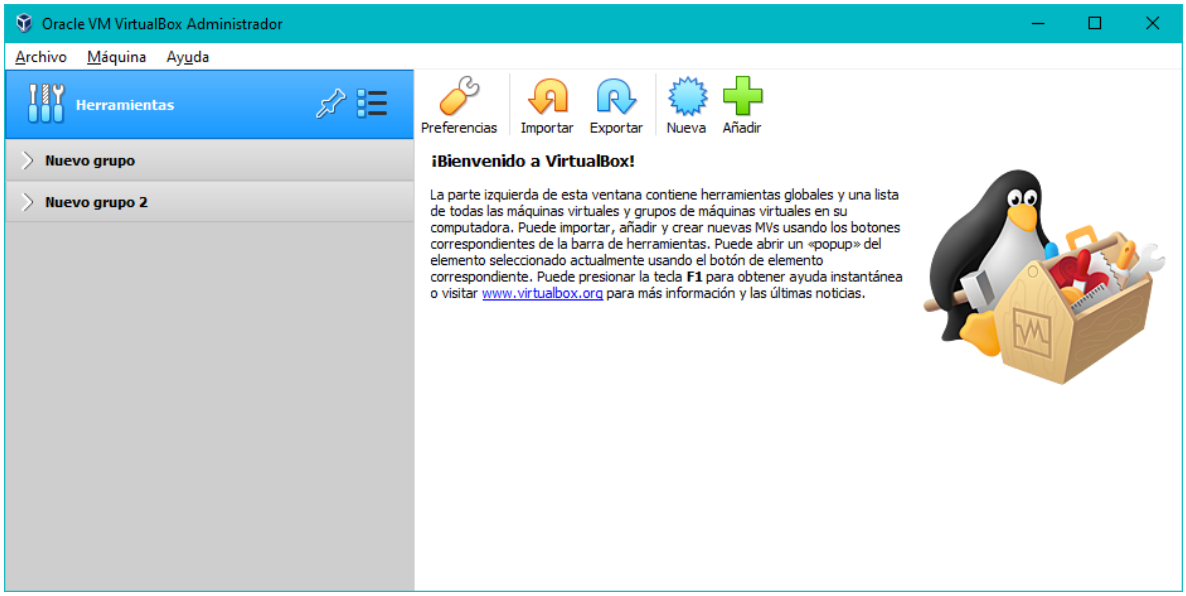
Metasploit	Metasploit se define como una plataforma para las pruebas de penetración que permite a sus analistas encontrar, explotar y validar vulnerabilidades de los sistemas objetivos. Este tipo software actualmente cuenta con la plataforma Metasploit Pro de pago y Metasploit Framework gratuita. Este tipo de sistemas permite la identificación y explotación de vulnerabilidades ayudando a hacer una división de los flujos de trabajo de las pruebas que se realizan y en donde son más fáciles de trabajar. Según la página oficial se puede hacer uso de un flujo guía como indica la imagen.  Este sistema permite la interacción de varias herramientas como Nmap, Nessus entre otras
NMAP	Nmap (Network Mapper) es una herramienta de tipo libre de código abierto que permite el escaneo de redes y de auditoria de seguridad. Su uso varía según las necesidades y de su uso ya que puede ser para monitoreo de las redes de una empresa como para identificar host de red para un ataque premeditado ya que se peude obtener informacio de equipos de la red como su nombre, versionamientos, aplicaciones que corren, puertos abiertos, firewalls entre otros. Este software está disponible para distintas plataformas Linux, Windows, MacOs, puede hacer uso de otros sistemas alidos como Zenmap, Ncat, Nping para facilitar su uso.
	Servicios en Línea
ExploitDB	Es una base de datos de Exploits públicos donde estos Exploits con su software de vulnerabilidad correspondiente esta etiquetado o descrito. Este es usado por personas encargadas de la seguridad o Pentester para poder tener una gran fuente de

	Exploits, ShellCodes y documentos reconocidos de libre acceso y públicos como fuente de información para su trabajo. Algunas de las fuentes o bases reconocidas para encontrar este tipo de información y fuentes son: Exploit DB Rapid7 Vulnerability Lab Google Hacking Database
CVE 	CVE (Common Vulnerabilites abd Exposures) vulnerabilidad comunes y expuestas es un diccionario público de vulnerabilidades que funciona como un listado de entradas con un número de identificación, una descripción de la vulnerabilidad y las referencias públicas de las vulnerabilidades conocidas Los datos de información se toman de fuentes XML de las bases de datos de vulnerabilidades nacional (NVD) proporcionada por el instituto de estándares y tecnología, ademas información como Exploits de www.exploit-db.com y datos e información de fuentes como Metasploit. Otras fuentes como Cvedetails.com las clasifica mediante palabras claves, números cwe. Aunque las fuentes pueden provenir de cualquier usuario que identifique una falla y la reporta ya que muchas veces se paga o se dan dineros por descubrir fallos en sistemas.

6.1.4 Banco de trabajo

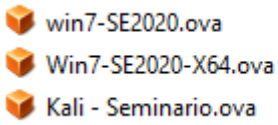
Instalar sistema de virtualización VirtualBox, en mi caso ya está instalada y funcional

Ilustración 4 VirtualBox Home



Una vez descargadas las fuentes entregadas, se procede al cargue de cada una por medio de la herramienta VirtualBox

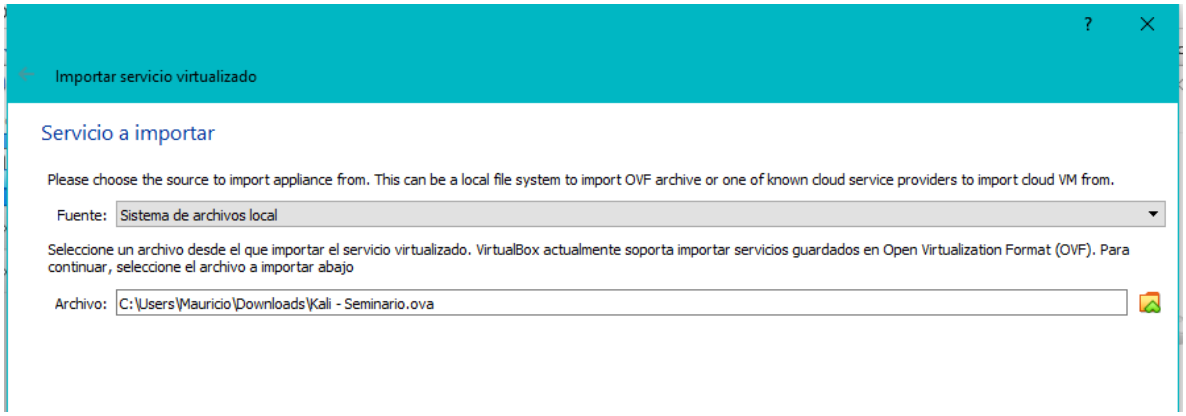
Ilustración 5 Fuentes .ova



Abrir VirtualBox e ir a la opción de herramientas

Allí se debe tomar la opción de importar, esta abrirá una ventana para la búsqueda de la fuente .ova, allí seleccionar la KaliLinux

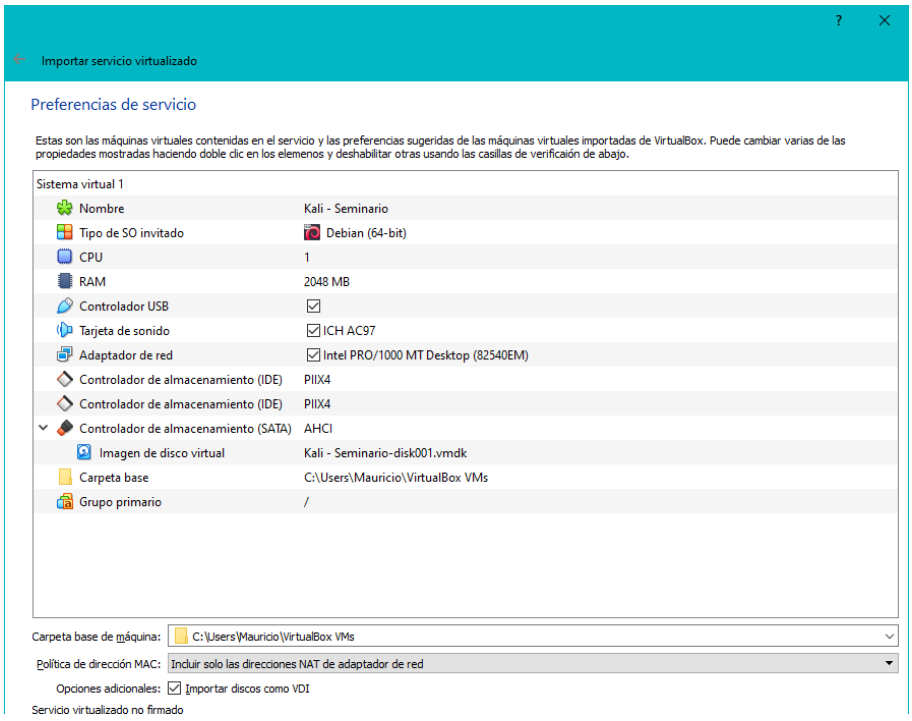
Ilustración 6 Importar KaliLinux



Fuente: Elaboración Propia

Opción siguiente, allí la ventana dará opciones de configuración que son editables más adelante si se requiere.

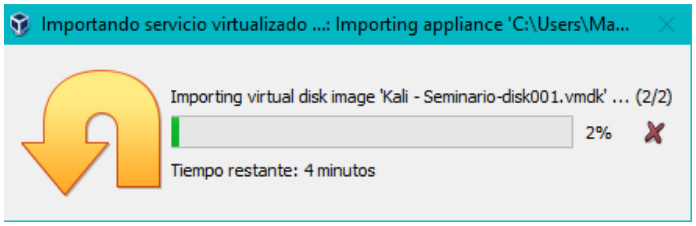
Ilustración 7 Opciones Configuración



Fuente: Elaboración Propia

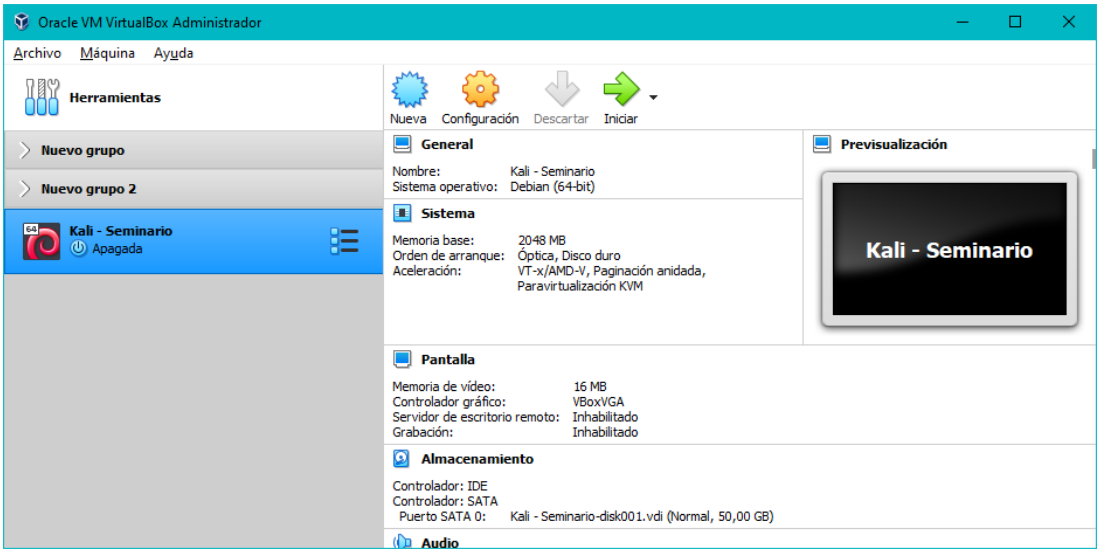
Opción Importar para dar inicio al proceso

Ilustración 8 Proceso Importación KaliLinux



Fuente: Elaboración Propia

Una vez importada esta lista para iniciarla



Fuente: Elaboración Propia

Una vez inicializada se carga el sistema operativo con sistema operativo KaliLinux

Ilustración 9 Máquina Virtual KaliLinux Importada

Fuente: Elaboración Propia

Para las maquinas Windows se debe hacer el mismo proceso de importar para poderlas usar.

Ilustración 10 Importar Maquina Win7 32 Bits

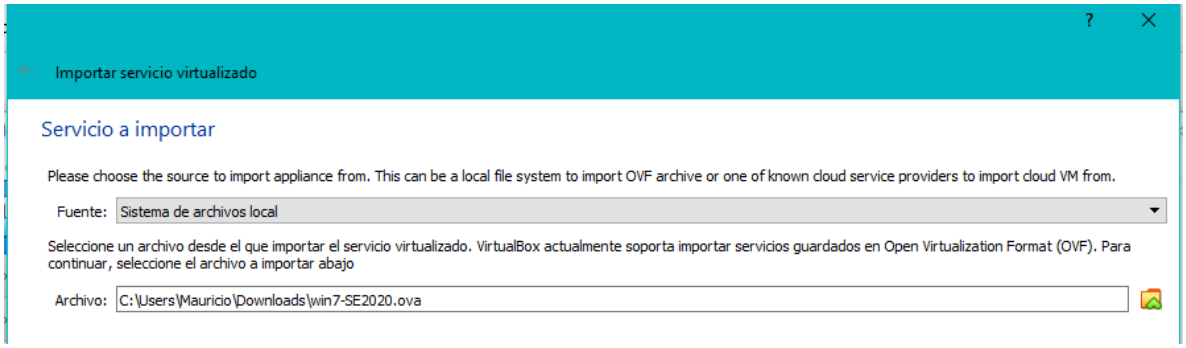
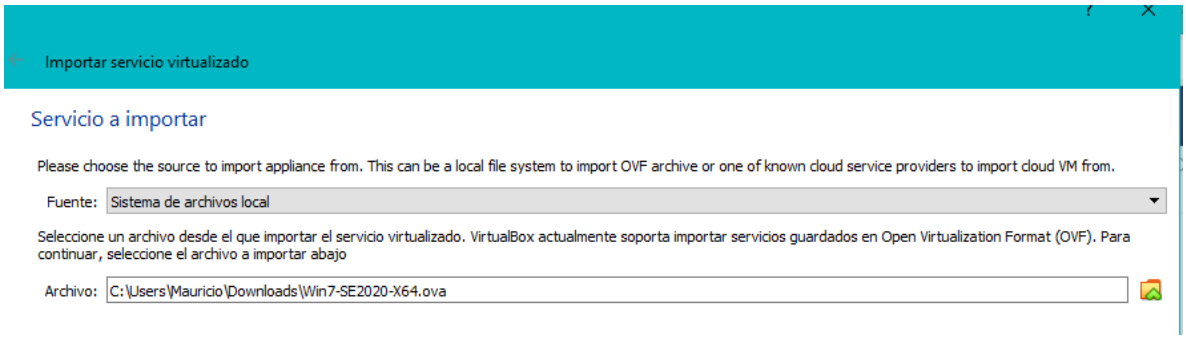
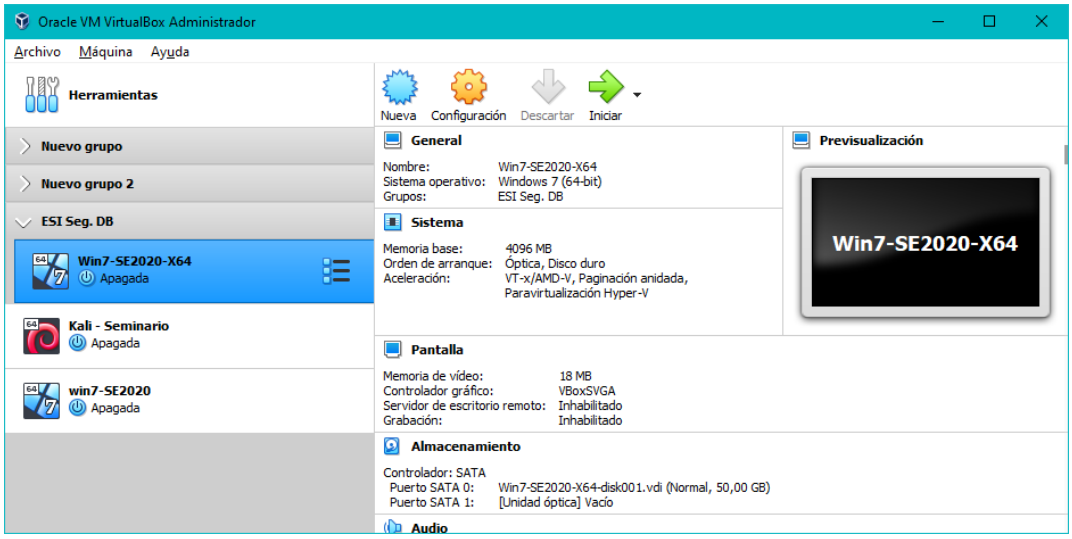


Ilustración 11 Importar Maquina Win7 64 Bits



Una vez importadas se debe iniciar la Windows

Ilustración 12 Máquinas Virtuales



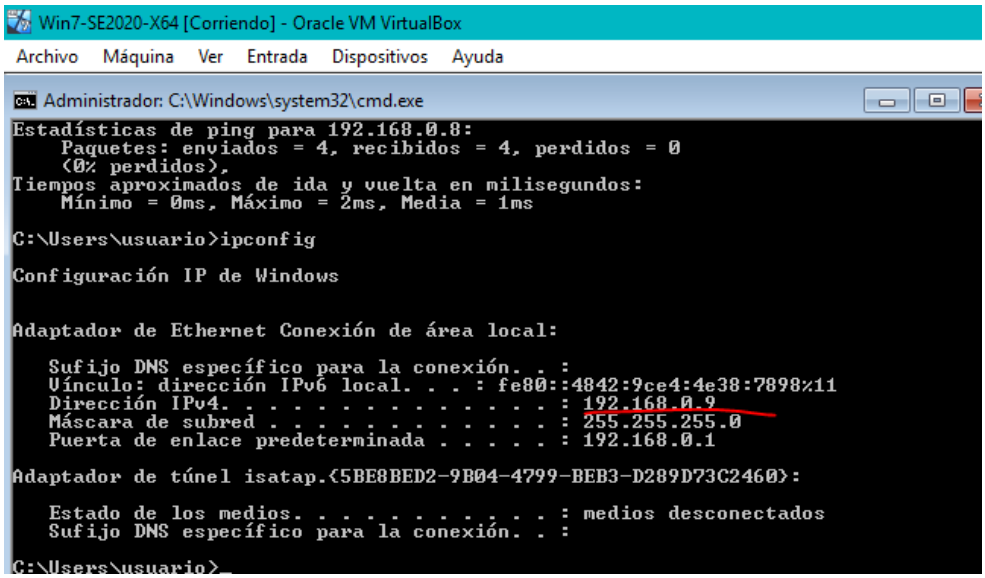
Fuente: Elaboración Propia

Conexión entre las maquinas

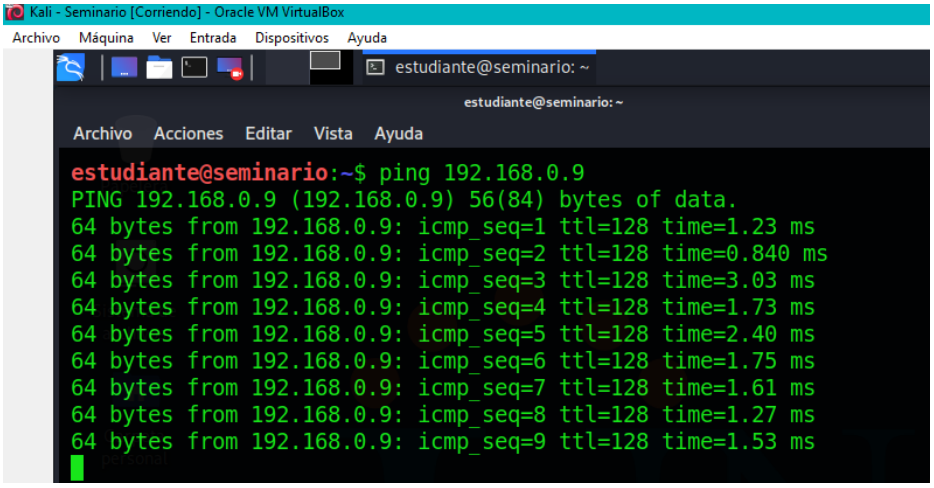
Se inician las maquinas KaliLinux y la maquina Windows 7 64 Bits.

Se hace ping desde maquina KaliLinux hacia Windows

Ilustración 13 Ping de Conexión KaliLinux a Windows 64Bits

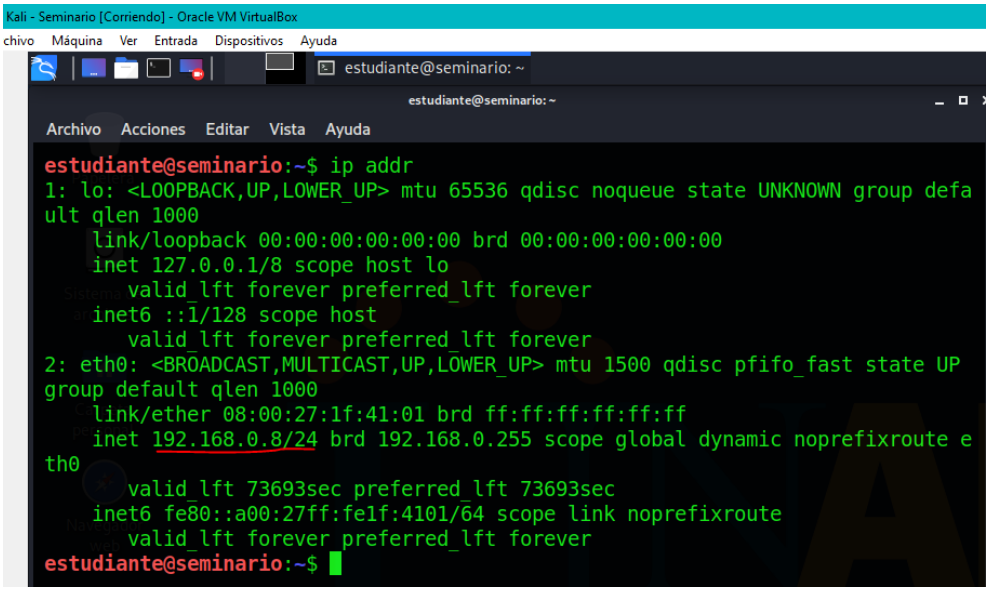


Fuente: Elaboración Propia



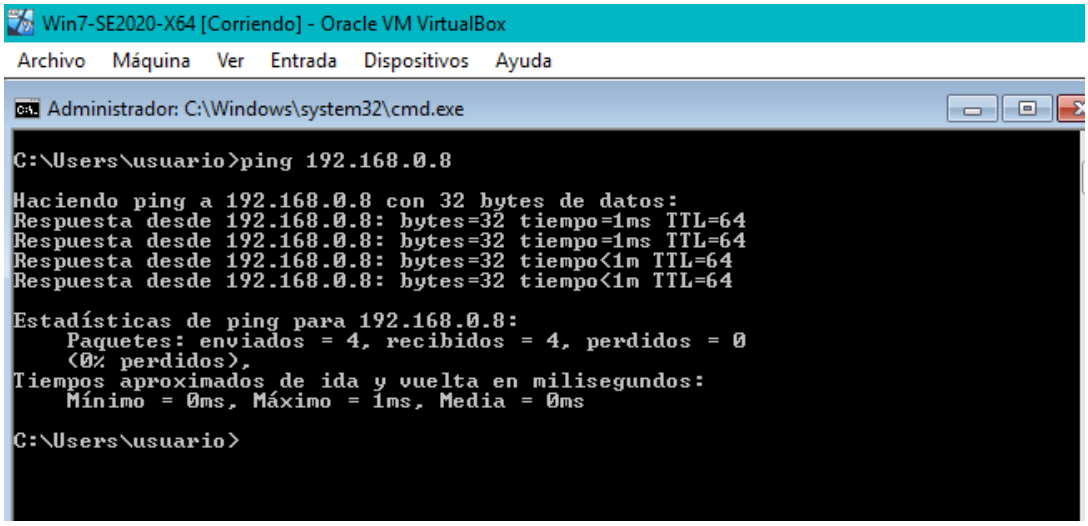
Fuente: Elaboración Propia

Hacer ping desde la maquina Windows 7 a KaliLinux



Fuente: Elaboración Propia

Ilustración 14 Ping de Conexión Windows 64Bits a KaliLinux

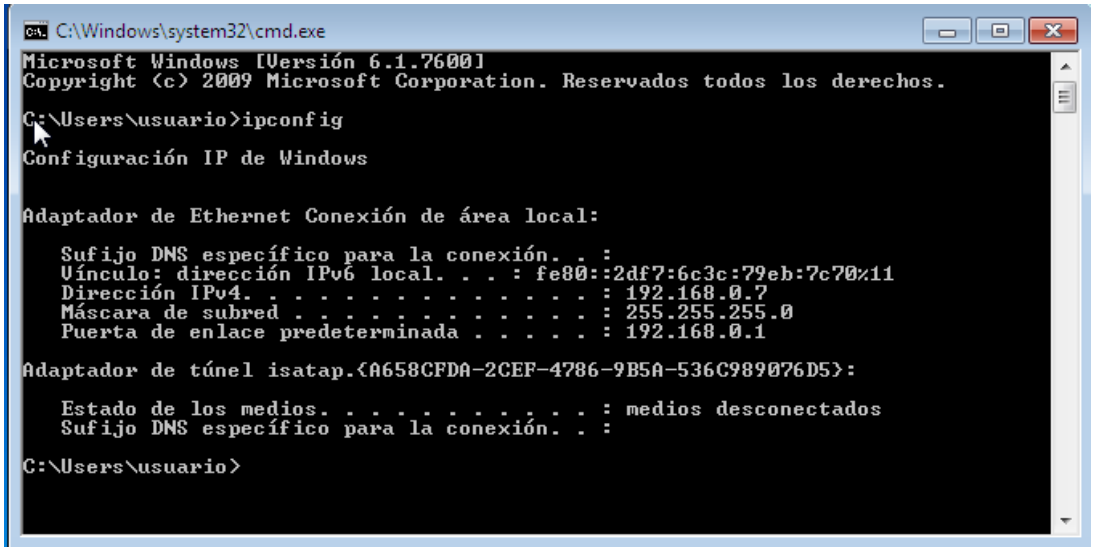


Fuente: Elaboración Propia

Se inician las maquinas KaliLinux y la maquina Windows 7 32 Bits.

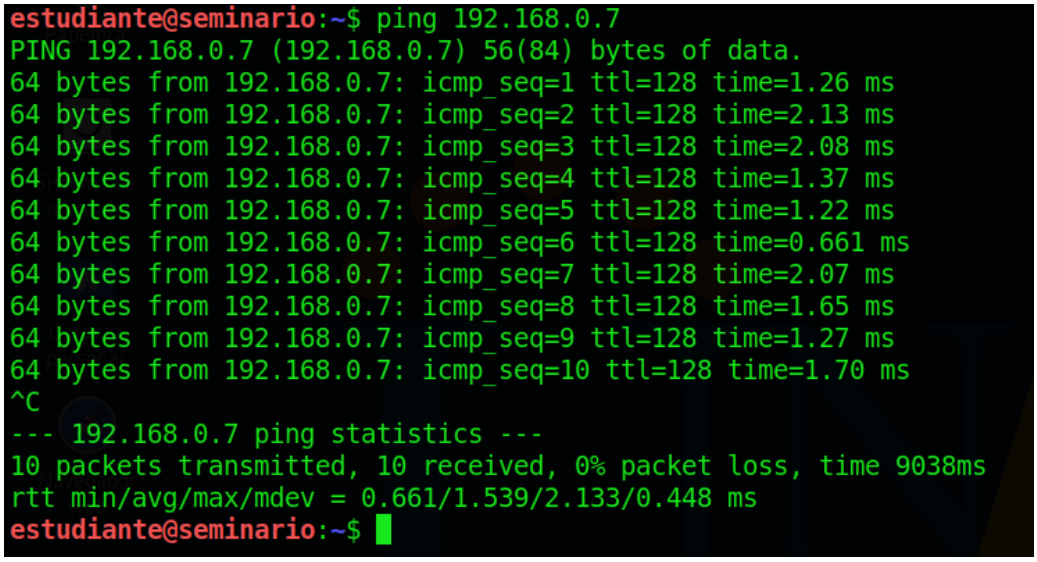
Se realiza ping desde la maquina KaliLinux hacia la maquina Windows

Ilustración 15 Ping de Conexión KaliLinux a Windows 32Bits



Fuente: Elaboración Propia

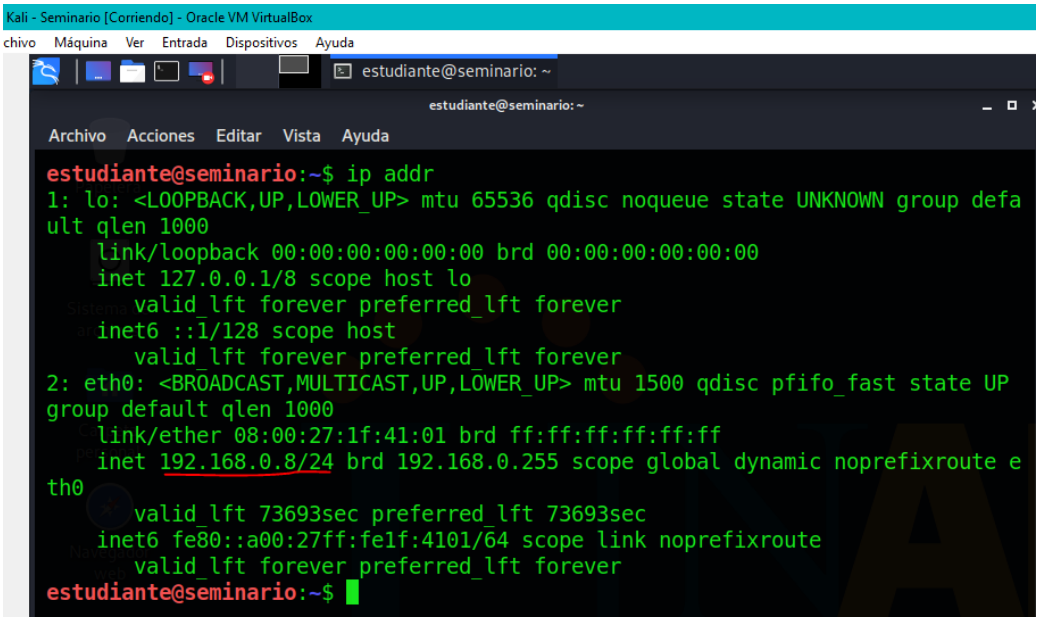
Ilustración 16 Ping de Conexión KaliLinux a Windows 32Bits



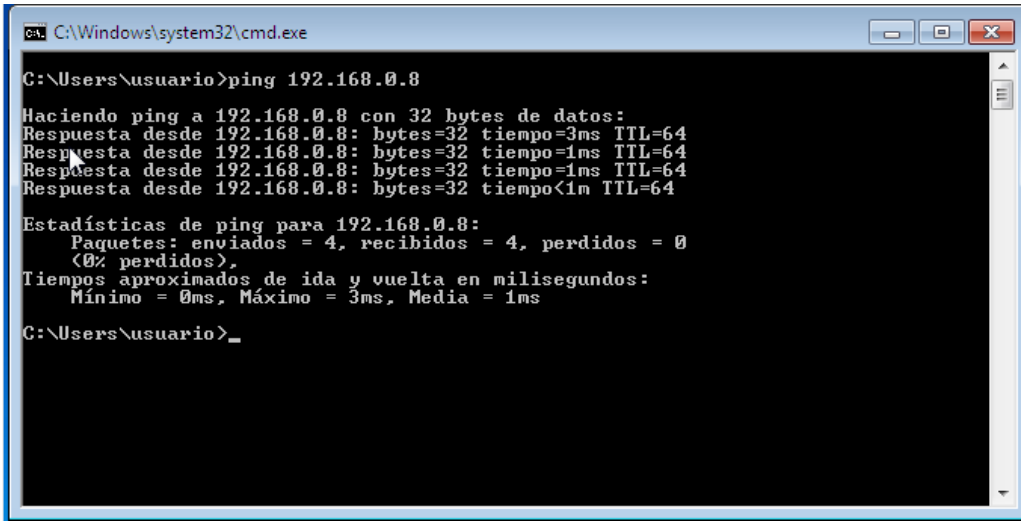
Fuente: Elaboración Propia

Se realiza ping desde la maquia Windows hacia la maquia KaliLinux

Ilustración 17 Ping de Conexión Windows 32Bits a KaliLinux



Fuente: Elaboración Propia

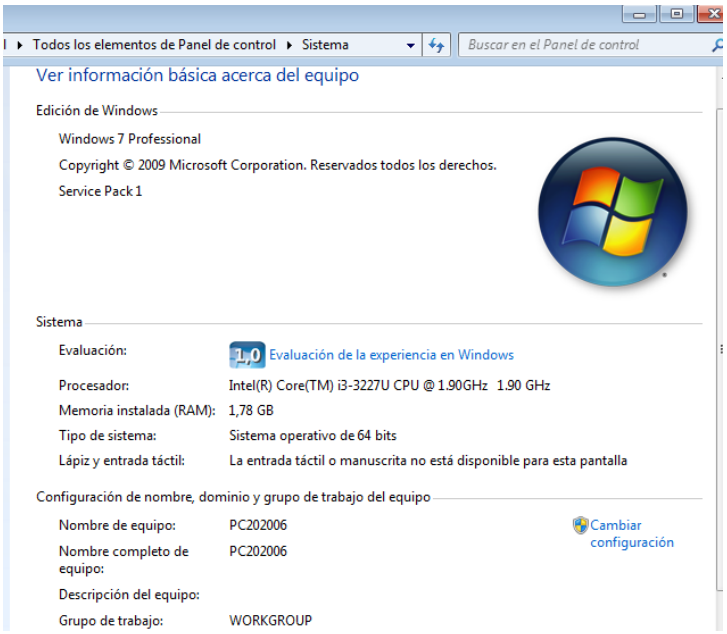


Fuente: Elaboración Propia

Características Técnicas Banco de Trabajo

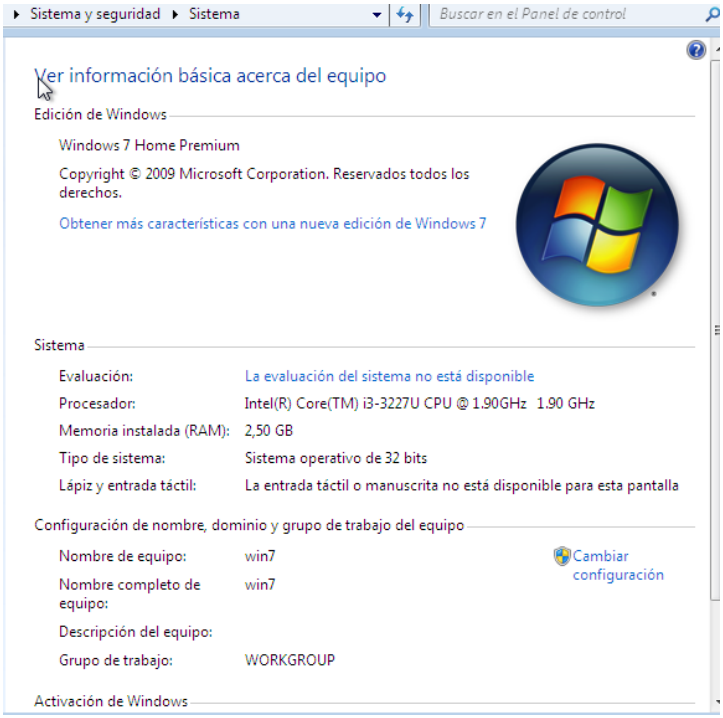
Maquina Windows arquitectura 64 Bits

SO Windows7 Profesional
Arquitectura 64 Bits
RAM 1.78 GB Asignada

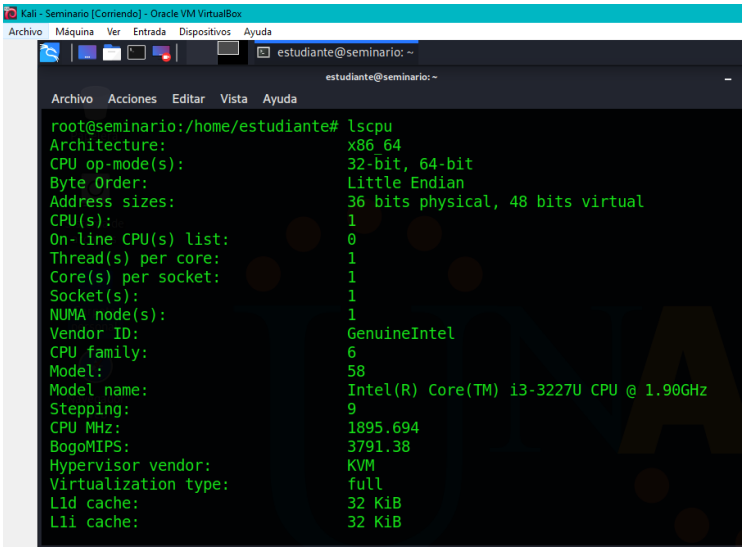


Maquina Windows arquitectura 32 Bits

SO Windows7 Home Premium
Arquitectura 32 Bits
RAM 2.50 GB Asignada

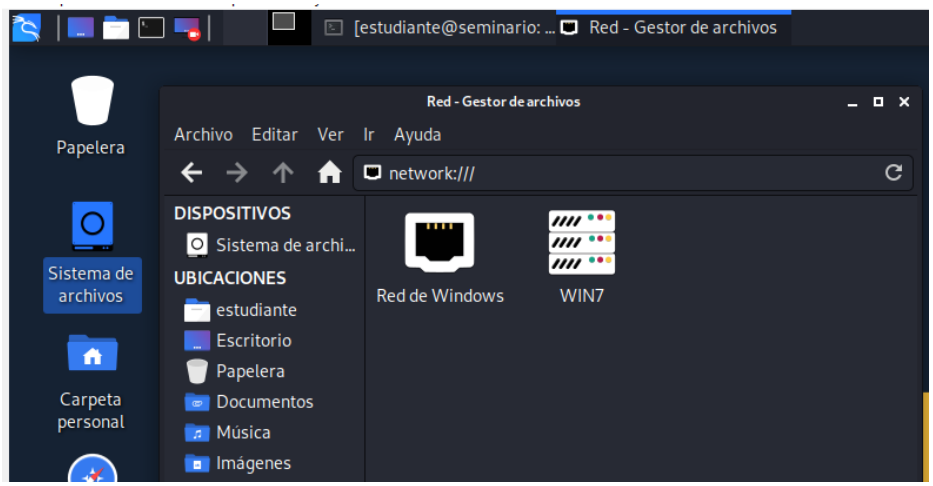


Maquina SO KALILINUX
Arquitectura 64 Bits
RAM 2 GB



Fuente: Elaboración Propia

Se evidencia comunicaciones correctas entre sistema de distintas casas fabricantes y de desarrollo y de distintas arquitecturas.



Fuente: Elaboración Propia

6.2 ETAPA SEGUNDA ANALISIS DE ACTUACION ETICA Y LEGAL

6.2.1 Análisis del contrato "ACUERDO DE CONFIDENCIALIDAD ENTRE MAURICIO SANCHEZ SABOGAL Y WHITEHOUSE SECURITY."

CLAUSULAS:

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

Análisis: Según se evidencia en esta cláusula permite que cualquier aspecto ilegal que se comenta dentro de la organización no pueda ser revelado o divulgado a ningún ente de control o autoridad competente lo que obviamente esta fuera del aspecto ético y legal de las organizaciones ya que crea de inmediato un ambiente de contratación no legal para aquel que se suscriba a este.

Segunda Clausula: "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".*

Análisis: En este párrafo de la segunda cláusula que habla sobre aspectos de la confidencialidad de la información que se pueda llegar a tomar de distintas fuentes y que son de carácter no público para la organización y que serían extraídas de forma ilegal por medio de interceptación, accesos no autorizados y chuzadas lo que se está incurriendo en delito punible para la organización y para las personas que lo lleven a cabo y que atenta contra de la ética y moral de las personas.

Tercera Clausula: "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."*

Análisis: en esta cláusula se refiere al origen de la información que es confidencial y sus fuentes, en él se hace una referencia a que la información puede ser autorizada y manejada desde cualquier fuente de donde provenga lo cual no es acertado y seguro ya que se debe conocer la fuente de toda información que maneje la organización, quien la genero y que la soporta o la soporto en su momento de generación o distribución. Esto se debe a que puede prestarse ya que las fuentes pueden ser ilícitas en la información que suministran.

Cuarta Clausula: "Obligaciones de la parte receptora: Se considerará como parte receptora de la información confidencial a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:"
En el numeral 3 establece". *"No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros"*
En el numeral 4 establece *"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas."*
En el numeral 7 establece *"Responder por el mal uso que le den sus representantes a la información confidencial".*
En el numeral 8 establece *"Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento."*
En el numeral 9 establece *"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."*

Análisis: Esta cláusula habla de las obligaciones de la parte receptora de información, se identificaron las siguientes inconsistencias de los siguientes párrafos, del numeral 3,4,8 y 9 se puede establecer una conducta delictiva ya que hace referencia a que la información que se recibe de cualquier tipo y medio como por ejemplo de espionaje no podrá ser objeto de análisis o de denuncia a las autoridades lo cual no es acorde con unos principios legales y éticos de una organización, se hace referencia que la responsabilidad será mía legalmente en caso de ser develado algún tipo de inconsistencia con cualquier tipo información que se tenga en ese momento y que sea usadas mal por la dirección, librándose de alguna responsabilidad como organización y se hace énfasis en que ningún tipo de datos e información podrá ser revelada así sea de tipo ilegal sin que la organización como tal autorice a ello lo que implica usar la organización completa como cómplice de dichas conductas delictivas.

Octava Clausula*: "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".*

Análisis: En este caso señala que si de alguna forma se encuentra informacion ilegal en mis manos debo acudir a un abogado privado y dejar a la empresa libre de toda culpa, este es un caso grave de hacer el señalamiento a mi como el responsable de todo movimiento de datos e información ilegal en la empresa lo que conllevaría a asumir la responsabilidad legal y ética de mi como profesional y perdiendo de alguna forma la moral que se debe tener en cualquier campo de la vida.

6.2.2 Análisis del contrato según la Ley 1273

Clausula Primera: *Acuerdo de confidencialidad "la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados"* se evidencia que se estaría incurriendo en acción ilegal para el articulo **269F** ya que por medio de la organización se estaría involucrando a terceros en aspectos criminales como fundamento y derecho al manejo correcto de la información que se obtiene de fuentes distintas sin estar facultados para su ocultamiento.

Clausula Segunda: *Definición de información confidencial "datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos".* Se evidencia que la organización obtiene datos de manera ilegal y de forma abusiva a sistemas o los intercepta. En este caso se estaría violando el artículo **269A** donde se accede a cualquier sistema, articulo **269C** donde se hace una interceptación para obtener datos e información

Clausula Tercera: Origen de la información *"independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.".* En este caso se estaría violando el articulo **269I, 269J** se evidencia que se ha violado algún tipo de sistema informático y se ha obtenido algún tipo de datos e información de forma no autorizada.

Clausula Cuarta: 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"
"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas."
"Responder por el mal uso que le den sus representantes a la información confidencial".
"Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento."
"La 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."

En esta cláusula se podría evidenciar la violación a los artículos
Artículo 269A Se realiza o se hace uso de un acceso no autorizado a datos e información, se vale de ellos para obtener información para algún tipo de beneficio
Articulo 269C mucha de la información obtenida por la organización según se evidenció en la cláusula se usa la interceptación para sustraerla.
Articulo 269F se evidencio que se hace uso de datos e información de datos personales de muchas fuentes así no sean legales y sin importar las fuentes y almacenamiento.

Clausula Octava*: "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".*

En este artículo podemos evidenciar que pueden violarse varios los parágrafos del articulo **269H** donde se hace el contrato aprovechándose la organización por medio de un tercero el cual puede firmar el contrato incurriendo en delitos punibles, también se evidencia en el párrafo que indica que puede haber la divulgación de datos e información perjudicando a un tercero en caso de ser descubiertos o hayan investigaciones por parte de autoridades, además de se evidencia que cualquier tipo de falta será responsabilidad en este caso del firmante del contrato ya que se usa como un tercero quitando la responsabilidad de la empresa en cualquier tipo de investigación o disposición legal.

Como conclusión y análisis de la norma se puede evidenciar varias inconsistencias legales que se cometen en el contrato violando varios de los artículos de la ley que estarían de alguna forma involucrando a un tercero en caso de firmar y aceptar dichos términos para el desarrollo de su labor lo cual va en contra de todo principio ético y moral además de las implicaciones legales que esto involucra ,se podría hablar de penas de 3 a 8 años fácilmente incrementándose según lo que explica el articulo 269H donde se evidencias varias circunstancias de agravación cuya pena aumentaría en todos los casos de las clausulas analizadas, es por ellos que para mí como firmante de este no se debería hacer por ningún motivo.

6.2.3 Implicaciones éticas según el código COPNIA

Según el código de ética profesional que está establecido en la ley 842 de 2003 está dividido en los capítulos primero de disposiciones especiales, el segundo capítulo de los deberes y obligaciones y prohibiciones y un tercero que habla de las inhabilidades e incompatibilidades.

El código también señala los tipos de sanciones en caso de que se incumpla la ley como amonestación por faltas leves, suspensión de matrículas profesionales o la cancelación total de esta por faltas muy graves.

En el caso particular de la organización WhiteHouse Security que es reconocida nivel mundial por asesorar a grandes Gobiernos en Ciberseguridad y Ciberdefensa se estaría exponiendo varias faltas a la ética y a sus trabajadores a nivel profesional, esto debido a que hace que sus colaboradores del área que firmen contratos irregulares faltando a varios artículos como:

Capítulo II del Artículo 31 del numeral B donde señala que *"impidiendo o evitando su sustracción, destrucción, ocultamiento o utilización indebidos, de conformidad con los fines a que hayan sido destinados;"* donde en el contrato se hace referencia a que no se puede develar el uso que se le da a la información que usa la empresa. En el numeral *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;"* también se evidencia que puede haber una manipulación para que el contratado en este caso yo no pueda hacer ningún tipo de denuncia así lo sepa y tenga pruebas de ello.

Capítulo II del Artículo 32 en el numeral B que habla de las prohibiciones como profesional específicamente *"Permitir, tolerar o facilitar el ejercicio ilegal de las profesiones reguladas por esta ley"* esta se contradice en las cláusulas del contrato donde se permite por el contrario el ejercicio de la ilegalidad al obtener información de forma y no profesional por parte de los mismos que conforman sus equipos de trabajo.

Capítulo II del Artículo 34 prohibiciones de los profesionales frente a la sociedad en el numeral A *"Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación;"* en este caso se viola este ya que la organización por medio de un contrato está dando indicaciones claras de una intensión ilegal en el manejo y obtención de datos e información y en los hechos que promulgan en las clausulas

Capítulo II del Artículo 39 de los deberes como profesionales para clientes o publico se podría incurrir en que al realizar este tipo de contrato el trabajador tendría que asumir una postura de mantener secreta todo tipo de trabajo que se lleve a cabo y a sabiendas que es ilegal debe mantener esa postura según el acuerdo si se firmara, como indica por ejemplo *"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;*

Capítulo II del Artículo 40 de las prohibiciones profesionales en este caso se estaría evidenciando el incumplimiento de esta ya que la empresa está ofreciendo servicios donde los datos e información son procedentes de fuentes cualesquiera y de forma no legal en su obtención.

Capitulo III se podría dar por entendido y se incumple varios artículos por las faltas que se comenten en dicho contrato y según la ley 842 de 2003 y que acarrearía la cancelación de la matricula profesional por evento como el actuar e incurrir en delitos que atenta en contra de algún cliente en este caso los clientes de la organización que son directamente del estado en temas de Ciberdefensa

En todos los casos y como resumen se podría evidenciar que se incumplen varios de los artículos de ética ya que el documento contrato que expide esta organización WhiteHouse Security implica la violación de estas y de igual forma pone en tela de juicio el buen actuar de los profesionales que lo van a ejecutar ya que serían cómplices de varios delitos punibles , como la obtención de datos de forma ilegal, el no denuncio de delitos que se están realizando al interior de la empresa, el manejo de datos e información con inconsistencias y fuentes. Por esta razón la conducta ética indicaría el no hacer ninguna firma de este tipo de contratos ya que se violan leyes y normas éticas que deben regir el buen actuar como profesional en el área y el campo de la Ciberseguridad.

6.2.4Caso Andrómeda Buggly

El caso específicamente muestra que grupos de inteligencia de Colombia en la ciudad de Bogotá que estarían realizando actividades aparentemente ilegales frente

a un escenario netamente político además de involucrar el nombre de varios presidentes de la república y vicepresidentes. Según se establece y se descubrió que bajo la fachada de una comunidad de denominada Buggy donde su razón aparente era el funcionamiento y la constitución de una comunidad de seguridad informática donde se realizarían sesiones donde se compartían conocimientos en el área de la seguridad y donde ponían algún tipo de reto informativo y de seguridad que se debía superar para poder ir avanzando en dichos temas de la Ciberseguridad, en resumen una comunidad de Hacking Ético

Según evidencio y según las fuentes pudo haber sido el primer paso por parte de organizaciones del estado en este caso el ejército en una forma de reclutamiento de los mejores Hackers para poder de esta forma tener un equipo capaz de servir a sus intereses particulares y según esta políticamente permitido en función de la seguridad nacional se podrían dar este tipo de eventos donde se usa la inteligencia para poder tener información de alguna actividad que le compete a la nación.

Según las evidencias el sitio era muy concurrido por personal del ejército lo que llevaría a pensar que es claramente algo serio y que viene dado por órdenes superiores del estado para realizar este tipo de labores de inteligencia en este caso donde se tendría como objetivo la interceptación de comunicaciones, interceptaciones de correo y la interceptación de todo tipo de medio de comunicación en el proceso de paz realizado para ese tiempo en la Habana cuba con las FARC.

Según la documentación analizada y de las investigaciones que se conocen por medios de comunicación se evidencia que estas entidades del estado al intentar obtener resultados de cualquier forma evaden sus límites éticos y morales de y se valen cualquier tipo de profesión para ellos, pero en este caso se hace por medio de terceros expertos en el tema de Hacking ético para poder de alguna forma manipular su honestidad ofreciendo algunos beneficios económicos.

Según algunas de las investigaciones y en mi concepto la operación Andrómeda como tal es legitima ya que realizaban sus actividades de forma normal, pero según todas las evidencias después de las órdenes dadas se convierte en su propósito ilegal y no actuando en la ética profesional y moral.

Se observa que en ese tipo de interceptaciones o chuzadas como las llaman comúnmente según mi punto de vista y la ley si se estaría afectando directa o indirectamente a alguna persona en su buen nombre. Según se evidencia se pudieron haber cometido varios delitos directos que están en la ley 1273.

Se conocieron por medio de comunicación la condena y como responsable de todo al señor Andrés Sepúlveda por delitos como los indicados en este documento, también se destituyeron algunos oficiales del ejército Nacional, pero en ningún

momento se realiza la revisión del caso para involucrar políticos como se deberían investigar de la misma forma.

Algunos de esos delitos estarían relacionados con el “Acceso abusivo a un sistema informático” del artículo 269”. La “Interceptación de datos informáticos”, al realizar chuzadas a cualquier tipo de sistema como la interceptación de las comunicaciones según el artículo 269C. El “uso de software malicioso“, se pudo haber dado el uso de cualquier tipo de software para las interceptaciones y obtención de correos como indica el articulo 269E. La “Violación de datos personales” también es otro delito en el cual se puedo haber violado ya que al acceder a cuentas de correo, en la interceptación de conversaciones se viola ese derecho, ya que no se respeta la intimidad, perdida de datos, alteración de datos, modificación de los mismos para algún propósito. Además de la violación del código de éticas de COPNIA en su mayoría de las cláusulas que allí exponen, ya que no se evidencia ninguna facultad de moralidad en los hechos.

6.3 ETAPA TERCERA PROCESO DE PRUEBAS DE PENETRACION

6.3.1 Herramientas Software en el Análisis de caso estudio usadas por el Equipo Redteam en fases De Pentesting

Herramientas para el proceso de Pentesting

NMAP[14]: Es una herramienta de licencia gratuita de código abierto que sirve para la gestión de las redes y hacer procesos de auditoria en seguridad informática, inventarios de las redes, gestión de activos, supervisiones de host y servicios. EL sistema usa paquetes IP para determinar equipos de la red, servicios que usan, sistemas operativos que usan, software que pueden estar usando, descubrir firewalls entre otras características importantes. El sistema es multiplataforma Windows, Linux, Mac OS x. Su uso puede ser por línea de comandos o por interfaz gráfica con ayuda de Zenmap y Ncat, en resume una herramienta muy versátil y potente para el uso en distintas área de la informática entre ellas la seguridad.

MASSCAN: Scanner de puertos de la red, Puede escanear todo Internet en menos de 5 minutos, transmitiendo 10 millones de paquetes por segundo, desde una sola máquina.

Se usaran estas herramientas en la *etapa de recopilación de datos e información* de las máquinas de la red para la identificación de puertos, tipos sistemas operativos

[14] NMAP, Nmap Security Scanner - Introduction, [sitio web]. [consultado: 17 de Septiembre de 2021]. Disponible en: https://nmap.org/

y datos de software como si usan firewall, para determinar si es vulnerable a algún tipo de ataque según las características de datos obtenidas en esta recolección.

OPENVAS[15]: "es un escáner de vulnerabilidades automatizado e integrado, este software puede detectar distintos tipos de vulnerabilidades según su nivel de criticidad y complejidad tanto de dispositivos de red y otros dispositivos conectados. Este sistema cuenta con sistema operativo GreenBone GOS, GSF, cuenta con una interfaz Web. Posee una base de más de 78.000 pruebas de vulnerabilidad (VT), estas vulnerabilidades que encuentra las clasifica según su gravedad lo que permite su análisis para el tratamiento. Este tipo de software permite el descubrimiento del estado actual el mejoramiento del estado actual y la revisión de las medidas tomadas."

Este se usara en la *etapa de descubrimiento e identificación de vulnerabilidades* de los sistemas operativos Windows 7 de la red de cualquier tipo de arquitectura 32 o 64 Bits. Permite el escaneo y evidenciar posibles fallos en estos sistemas operativos.

NESSUS: Escáner de vulnerabilidades para distintas plataformas y sistemas operativos de distintas casas y arquitecturas, detecta amenazas en tiempo real gracias a sus exactitud para la prevención de falsos positivos, ayuda en la gestión de seguridad en la detección de las debilidades, errores de configuración que se usan por los atacantes para vulnerar sistemas**.** Su interfaz gráfica ayuda en la interpretación de resultados de vulnerabilidades y además de exponer algunas de las soluciones posibles al fallo encontrado.

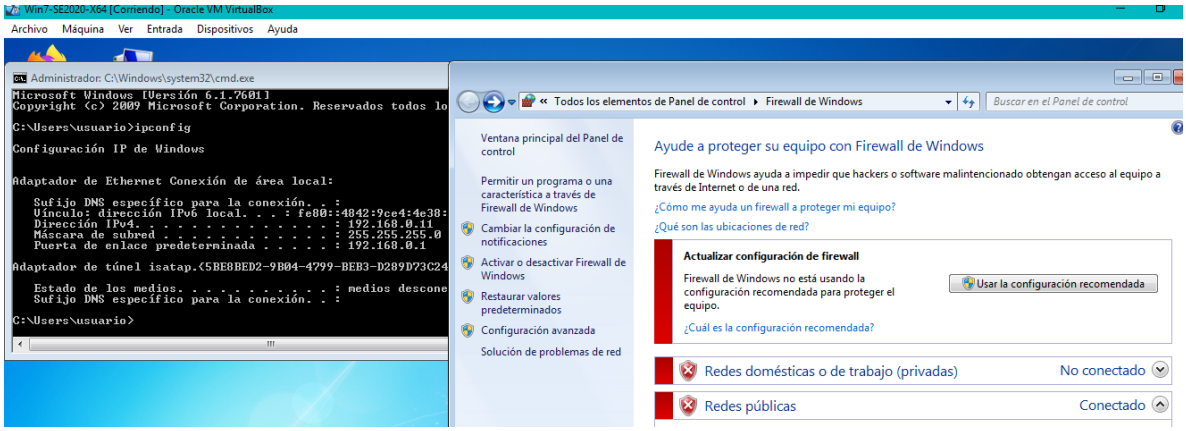
METASPLOIT: "Metasploit se define como una plataforma para las pruebas de penetración que permite a sus analistas encontrar, explotar y validar vulnerabilidades de los sistemas objetivos. Este tipo de sistemas permite la identificación y explotación de vulnerabilidades ayudando a hacer una división de los flujos de trabajo de las pruebas que se realizan y en donde son más fáciles de trabajar."
Se usara en la atapa de explotación de las vulnerabilidades según la descripción de lo que se sabe del caso y de las pruebas obtenidas de las fases anteriores y del escaneo de las vulnerabilidades.

6.3.2 Etapa de Planificación y Recolección de datos

Antes de los procesos de recolecciones datos se quitan todos los sistemas de seguridad de la maquina obtenida y suministrada por la organización en este caso, firewall, actualizaciones, antivirus.

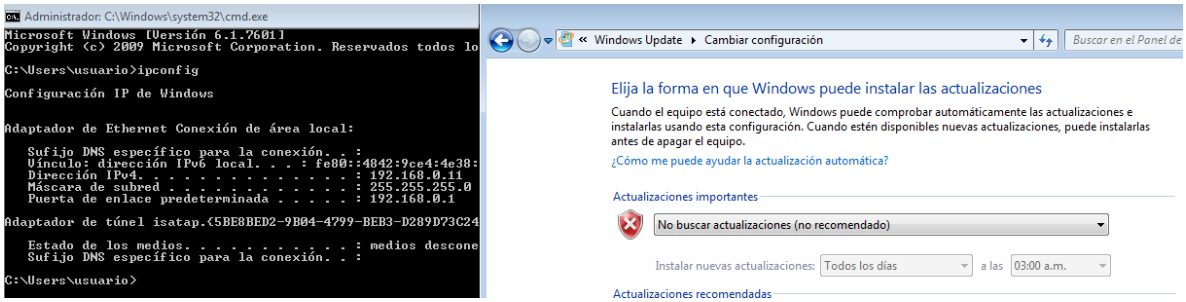
[15] OPENVAS, Open Vulnerability Assessment Scanner, [sitio web]. [consultado: 17 de Septiembre de 2021]. Disponible en: https://openvas.org/

Ilustración 18 Desactivación Firewall Windows



Fuente: Elaboración propia

Ilustración 19 Desactivación Updates Windows



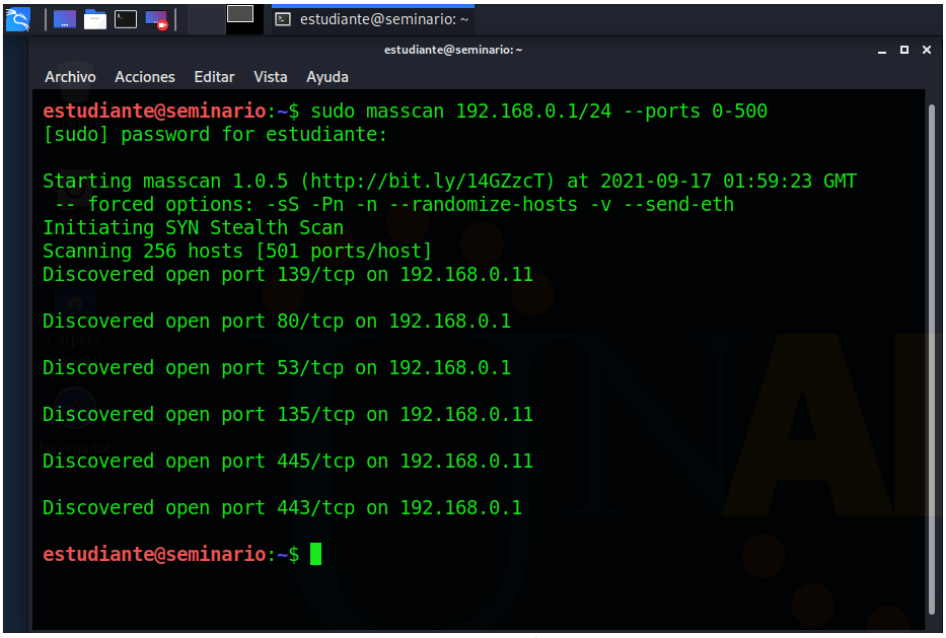
Fuente: Elaboración propia

Para esta etapa se hizo uso de NMAP para la identificación de datos e información de las maquinas objetivo, en este caso maquina Windows 7 64 Bits

Se accede a la maquina KaliLinux y como primera instancia y de manera preliminar se usa la herramienta **masscan** para determinar si tenemos algún tipo de red y puertos.

Se logran identificar algunas máquinas entre ellas la maquina Windows a la cual se le van hacer las pruebas de Testing. La máquina objetivo posee abiertos los puertos 139 TCP, 135 TCP y 445 TCP. En base a esta información se decide usar una herramienta más potente como NMAP.

Ilustración 20 Escanear puerto de red y puertos

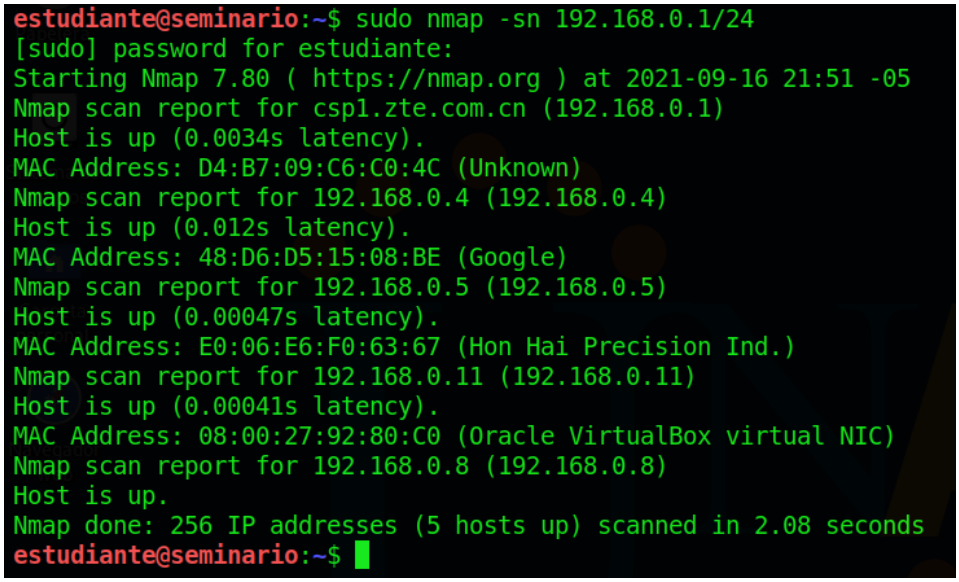


Fuente: Elaboración Propia

Escaneo con la herramienta NMAP para la identificación de puertos, sistemas operativos y servicios.

Identificar equipos de la red y sistemas operativos

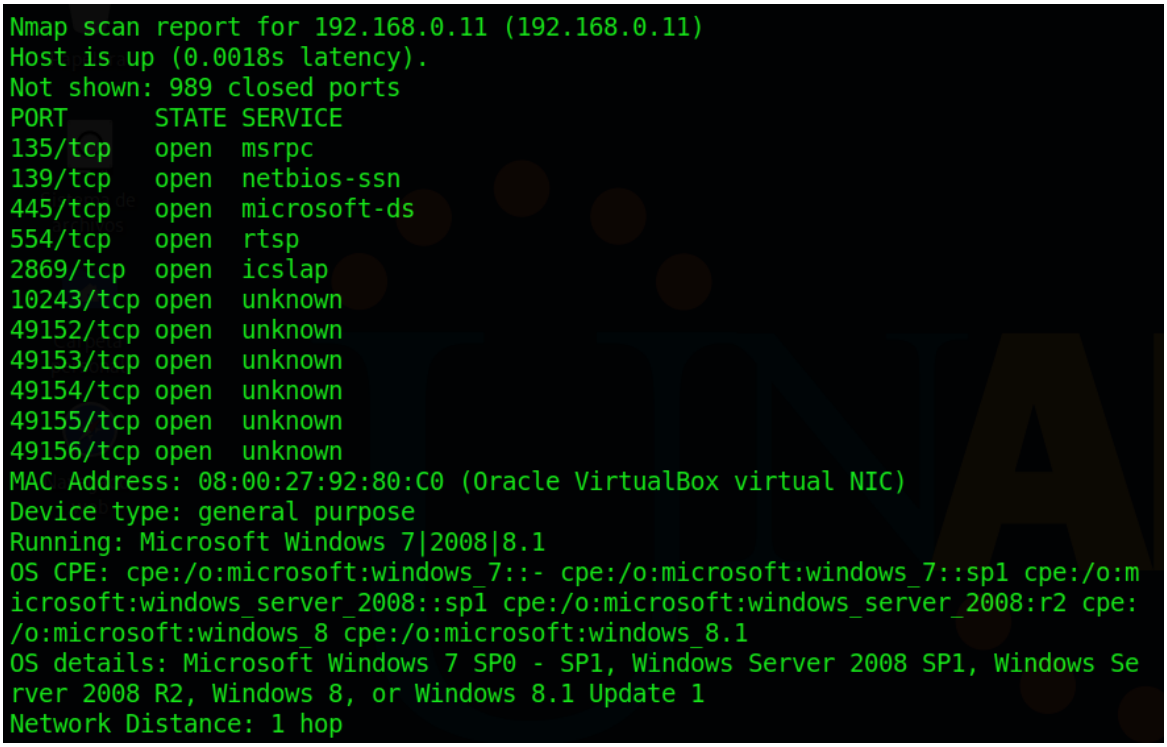
Ilustración 21 Identificación equipos de la red



Fuente: Elaboración propia

Se realiza la identificación de los sistemas operativos de la red entre ellas de la maquina objetivo Windows 7 y puertos abiertos con sus servicios asociados. Además de obtener todos los datos de sus Services Pack instalados.

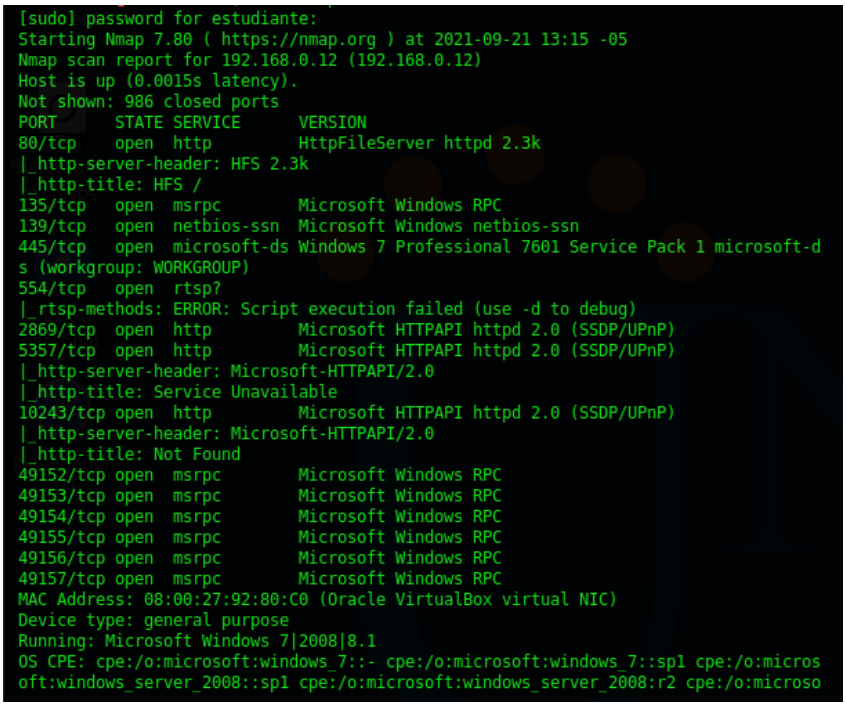
Ilustración 22 Identificación de SO



Fuente: Elaboración propia

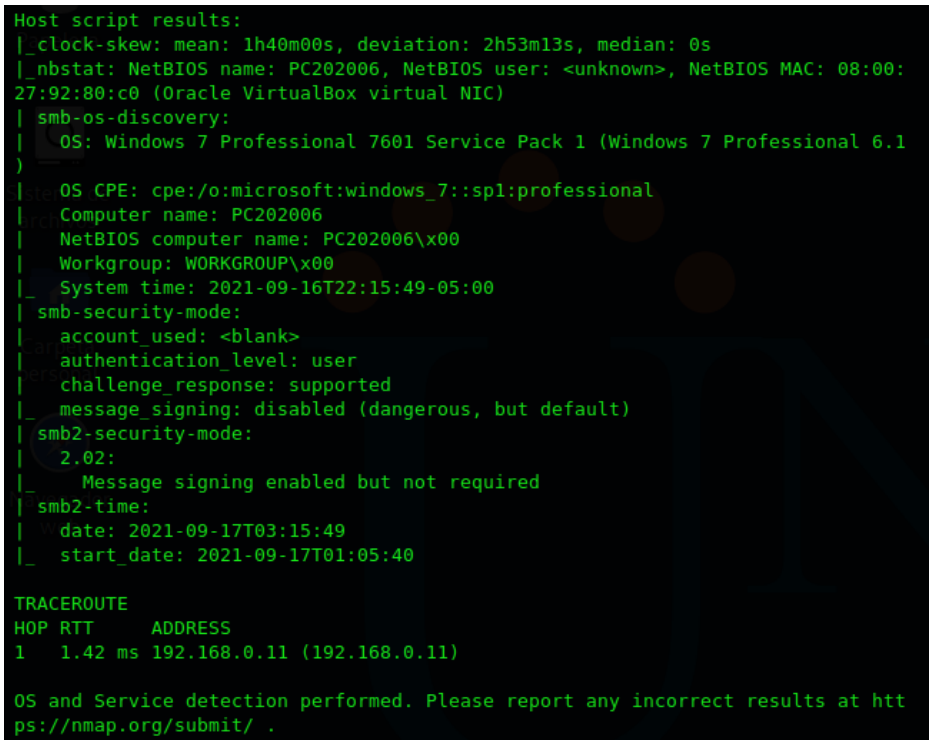
Se realiza la identificación de servicios específicos de la maquina Win7 X64 entre ellos el asociado al aplicativo **rejetto**

Ilustración 23 Identificación de SO



Fuente: Elaboración propia

Ilustración 24 Identificación de SO especifico



Fuente: Elaboración propia

Ilustración 25 Identificación de SO x64

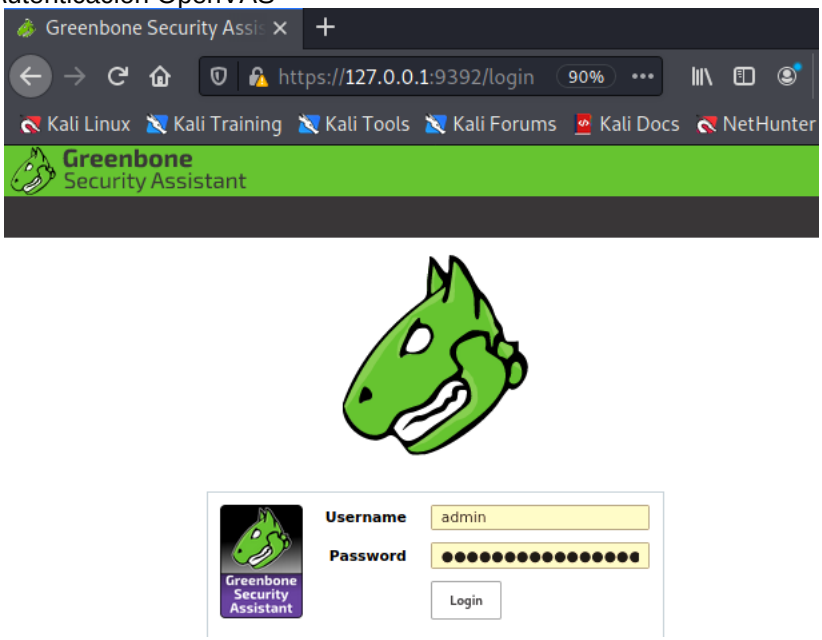
```
estudiante@seminario:~$ sudo nmap -sV --version-intensity 0 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-16 22:46 -05
Nmap scan report for 192.168.0.11 (192.168.0.11)
Host is up (0.00093s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  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  icslap?
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Fuente: Elaboración propia

6.3.3 Etapa de identificación de vulnerabilidades

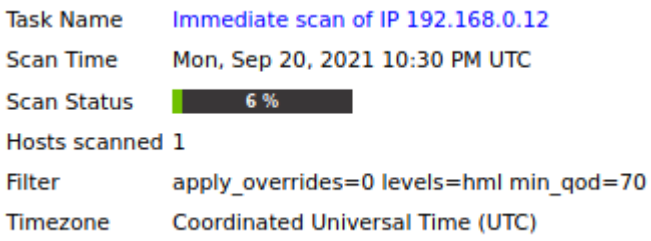
Para poder identificar las vulnerabilidades posibles del sistema Win7 x64 se decide hacer uso de Openvas para este propósito.
Para realizar el proceso desde la maquina Linux se debe ejecutar la herramienta previamente ya instalada y configurada, ingresar el en navegador web y autenticarse en el programa.

Ilustración 26 Autenticación OpenVAS



Fuente: Elaboración propia

Ingresar opciones de tarea y opción, escoger la maquina Windows objetivo y hacer el proceso de escaneo de vulnerabilidades.



Una vez realizo el proceso de escaneo de vulnerabilidades se obtiene los siguientes resultados:

Ilustración 27 Vulnerabilidades SO Win7

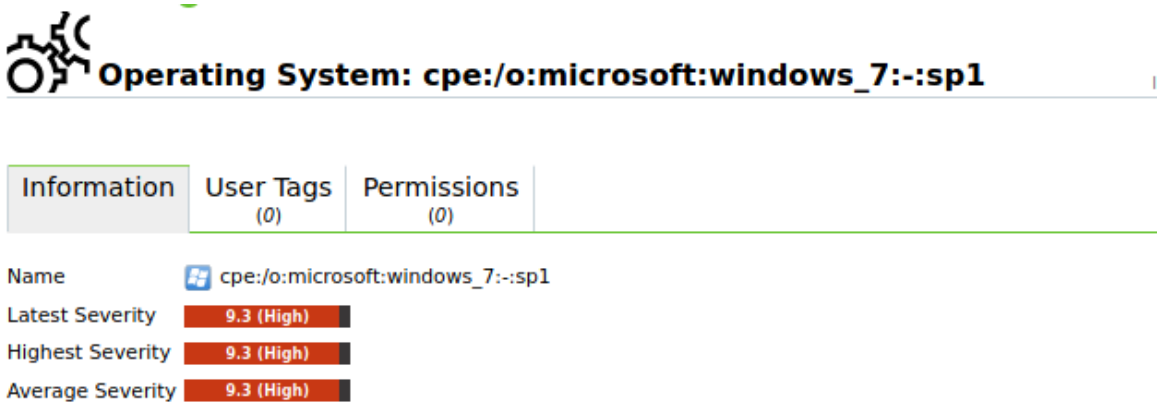
Vulnerability	Severity ▼	QoD
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95 %
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %
TCP timestamps	2.6 (Low)	80 %

Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	Mon, Sep 20, 2021 11:00 PM UTC	Mon, Sep 20, 2021 11:00 PM UTC	9.3 (High)	95 %
DCE/RPC and MSRPC Services Enumeration Reporting	Mon, Sep 20, 2021 10:54 PM UTC	Mon, Sep 20, 2021 10:54 PM UTC	5.0 (Medium)	80 %
Unknown OS and Service Banner Reporting	Mon, Sep 20, 2021 10:45 PM UTC	Mon, Sep 20, 2021 10:45 PM UTC	0.0 (Log)	80 %
Hidden WWW server name	Mon, Sep 20, 2021 10:45 PM UTC	Mon, Sep 20, 2021 10:45 PM UTC	0.0 (Log)	70 %
SMBv1 enabled (Remote Check)	Mon, Sep 20, 2021 10:45 PM UTC	Mon, Sep 20, 2021 10:45 PM UTC	0.0 (Log)	80 %
SMB Remote Version Detection	Mon, Sep 20, 2021 10:39 PM UTC	Mon, Sep 20, 2021 10:39 PM UTC	0.0 (Log)	80 %
Service Detection with 'HELP' Request'	Mon, Sep 20, 2021 10:33 PM UTC	Mon, Sep 20, 2021 10:33 PM UTC	0.0 (Log)	80 %
SMB/CIFS Server Detection	Mon, Sep 20, 2021 10:32 PM UTC	Mon, Sep 20, 2021 10:32 PM UTC	0.0 (Log)	80 %
DCE/RPC and MSRPC Services Enumeration	Mon, Sep 20, 2021 10:32 PM UTC	Mon, Sep 20, 2021 10:32 PM UTC	0.0 (Log)	80 %
SMB NativeLanMan	Mon, Sep 20, 2021 10:32 PM UTC	Mon, Sep 20, 2021 10:32 PM UTC	0.0 (Log)	95 %

Fuente: Elaboración propia

Actualizaciones del sistema operativos SP1

Ilustración 28 Vulnerabilidad SO Actualizaciones



Fuente: Elaboración propia

Vulnerabilidades que permite a los atacantes remotos ejecutar código arbitrario a través de paquetes manipulados,

Ilustración 29 Vulnerabilidad Ejecución Remota Código por actualizaciones SO

Fuente: Elaboración Propia

Insight

Multiple flaws exist due to the way that the
Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Detection Method

Send the crafted SMB transaction request
with fid = 0 and check the response to confirm the vulnerability.
Quality of Detection: remote_active (95%)

Affected Software/OS

- Microsoft Windows 10 x32/x64

- Microsoft Windows Server 2012

- Microsoft Windows Server 2016

- Microsoft Windows 8.1 x32/x64

- Microsoft Windows Server 2012 R2

- Microsoft Windows 7 x32/x64 Service Pack 1

- Microsoft Windows Vista x32/x64 Service Pack 2

- Microsoft Windows Server 2008 R2 x64 Service Pack 1

- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Impact

Successful exploitation will allow remote
attackers to gain the ability to execute code on the target server, also
could lead to information disclosure from the server.

Solution

Solution Type: Vendorfix
The vendor has released updates. Please see the references for more information.

Family

Windows : Microsoft Bulletins

References

CVE CVE-2017-0143
CVE-2017-0144
CVE-2017-0145
CVE-2017-0146
CVE-2017-0147
CVE-2017-0148

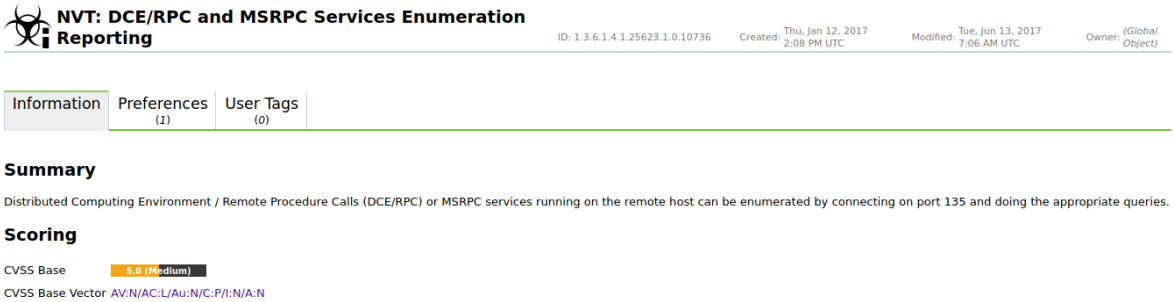
Fuente: Elaboración Propia

Puertos comprometidos

Port	Hosts	Severity ▼
445/tcp	1	9.3 (High)
135/tcp	1	5.0 (Medium)

Vulnerabilidades que afecta la escucha de puertos constantes en la máquina Win7 x64 y se pueden explotar de forma remota

Ilustración 30 Vulnerabilidad de Ejecución Remota de Código



Fuente: Elaboración propia

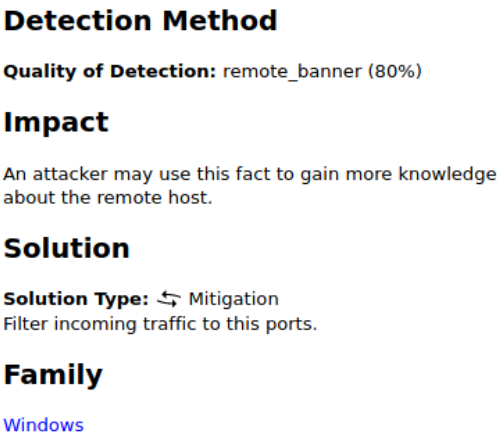
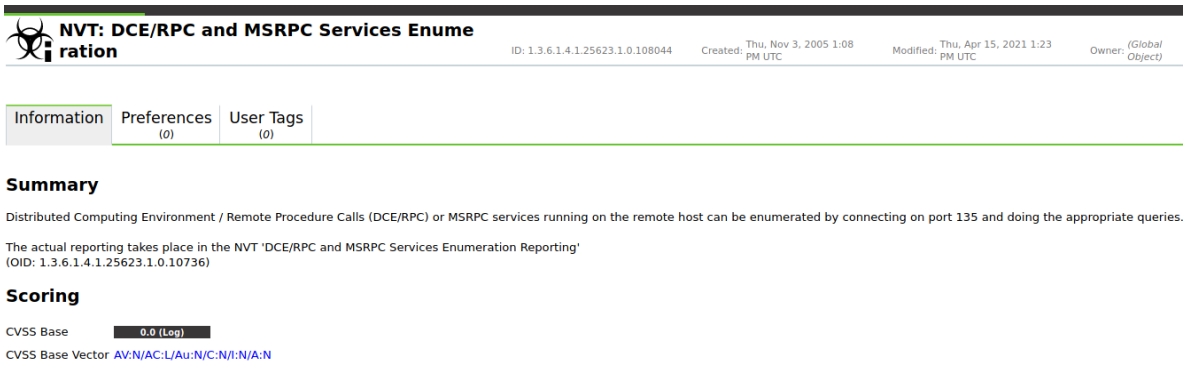


Ilustración 31 Vulnerabilidad de Ejecución Remota de Código



Detection Method

Quality of Detection: remote_banner (80%)

Impact

An attacker may use this fact to gain more knowledge about the remote host.

Solution

Solution Type: Mitigation
Filter incoming traffic to this port.

Family

Service detection

Fuente: Elaboración propia

Ilustración 32 Vulnerabilidad de puertos abiertos identificada para SMB

NVT: SMB/CIFS Server Detection

ID: 1.3

Information | Preferences (0) | User Tags (0)

Summary

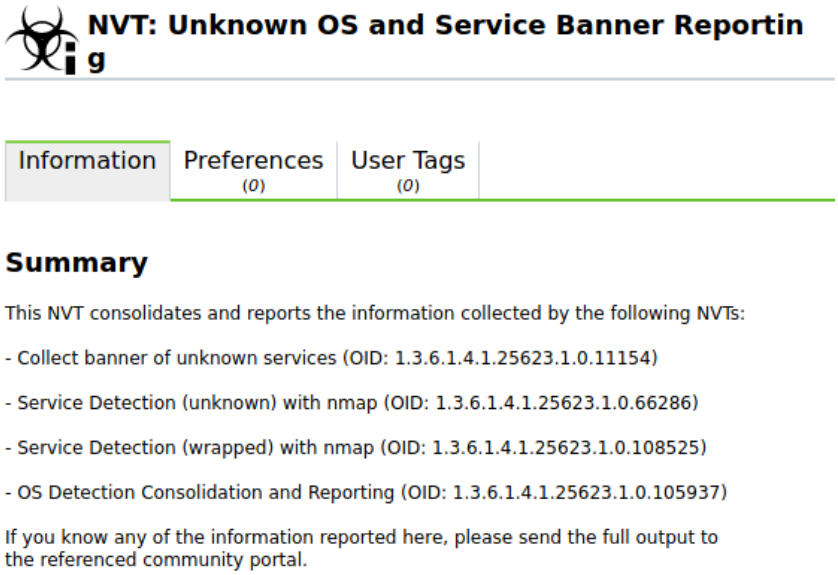
This script detects whether port 445 and 139 are open and if they are running a CIFS/SMB server.

Scoring

CVSS Base 0.0 (Log)

CVSS Base Vector AV:N/AC:L/Au:N/C:N/I:N/A:N

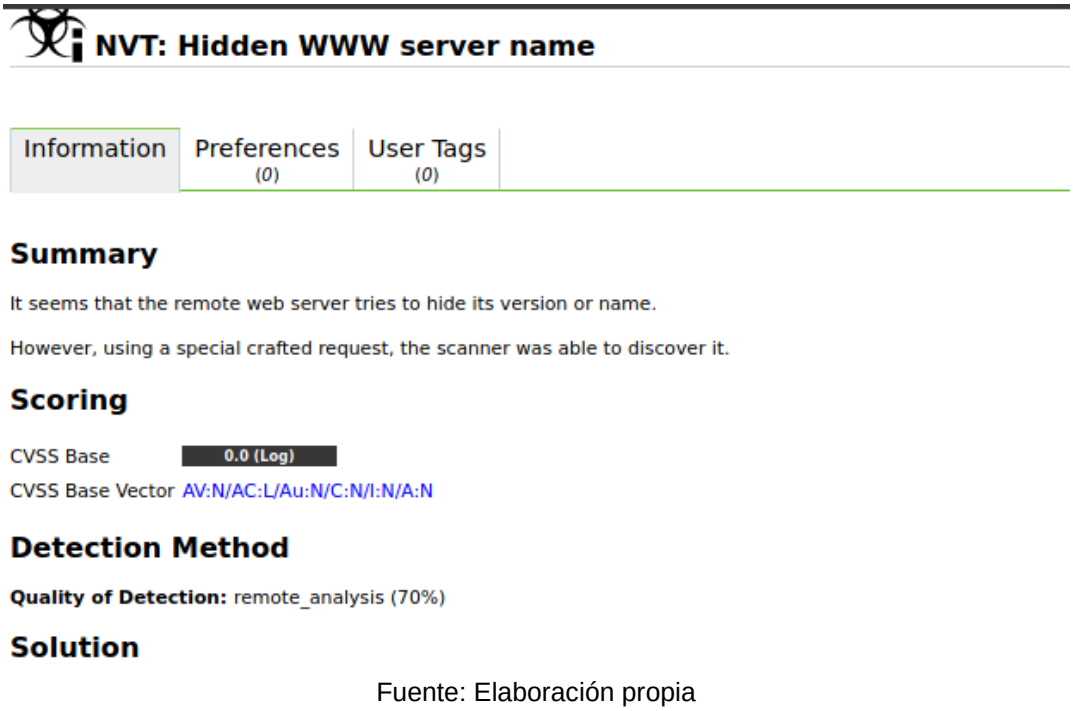
Detection Method



Fuente: Elaboración propia

Se evidencian vulnerabilidades en la cuales se permite obtener datos e información detallada de las máquinas.

Ilustración 33 Vulnerabilidad de revelación de datos del servidor

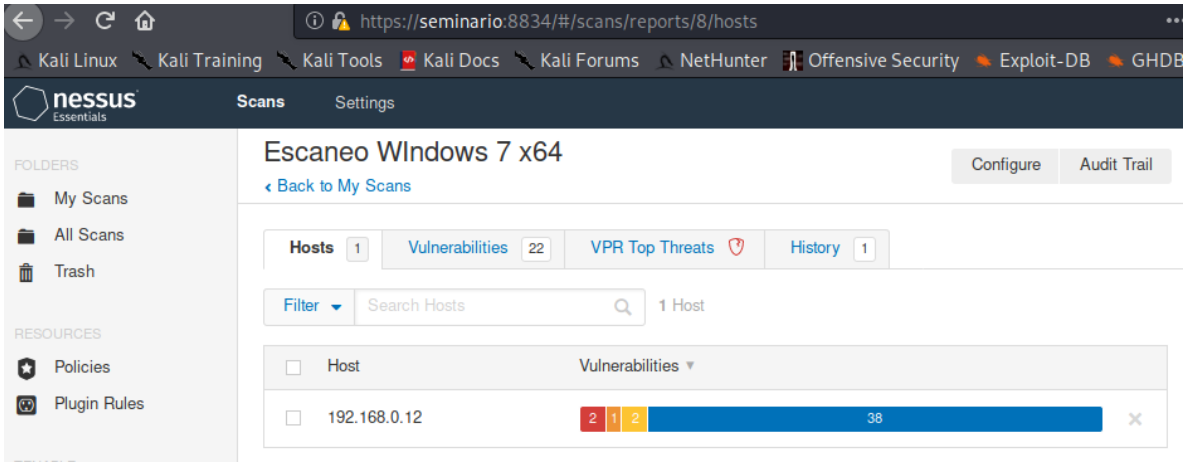


Fuente: Elaboración propia

Escaneo de vulnerabilidades con Nessus

Se realiza el proceso ahora con la herramienta Nessus para verificar que detecta con este sistema obteniendo los resultados siguientes:

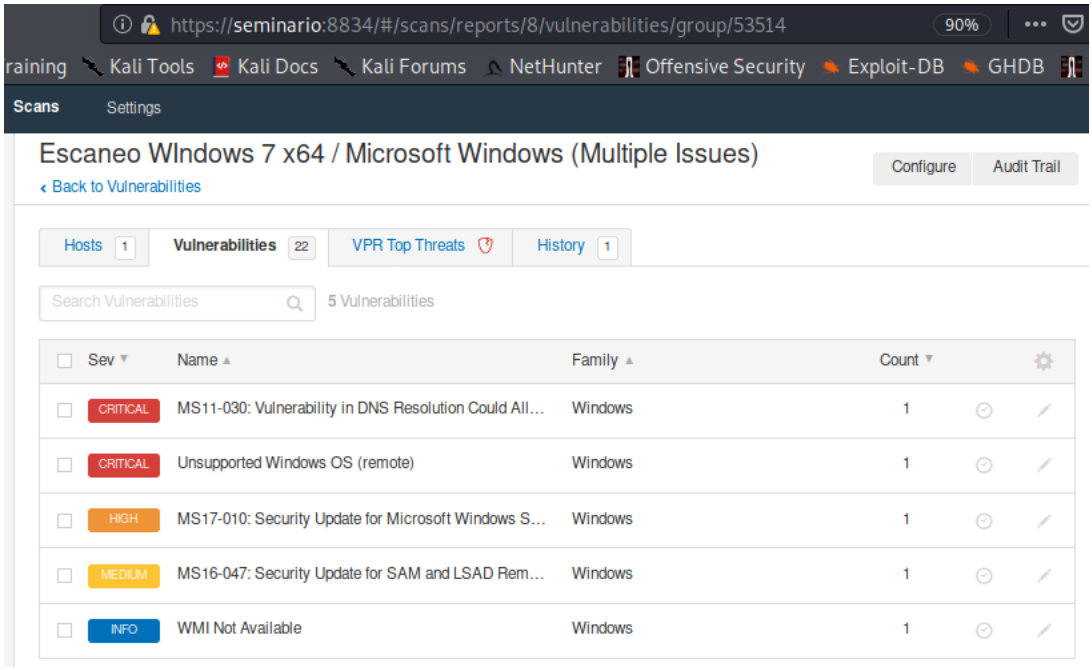
Ilustración 34 Escaneo Win7 Nessus



Sev	Name	Family	Count
MIXED	Microsoft Windows (Multiple Issues)	Windows	5
MEDIUM	Apache Struts 2 s:a / s:url Tag href Element XSS	CGI abuses : XSS	1
MEDIUM	SMB Signing not required	Misc.	1
INFO	DCE Services Enumeration	Windows	8
INFO	SMB (Multiple Issues)	Windows	7
INFO	Nessus SYN scanner	Port scanners	6
INFO	HTTP (Multiple Issues)	Web Servers	2
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1

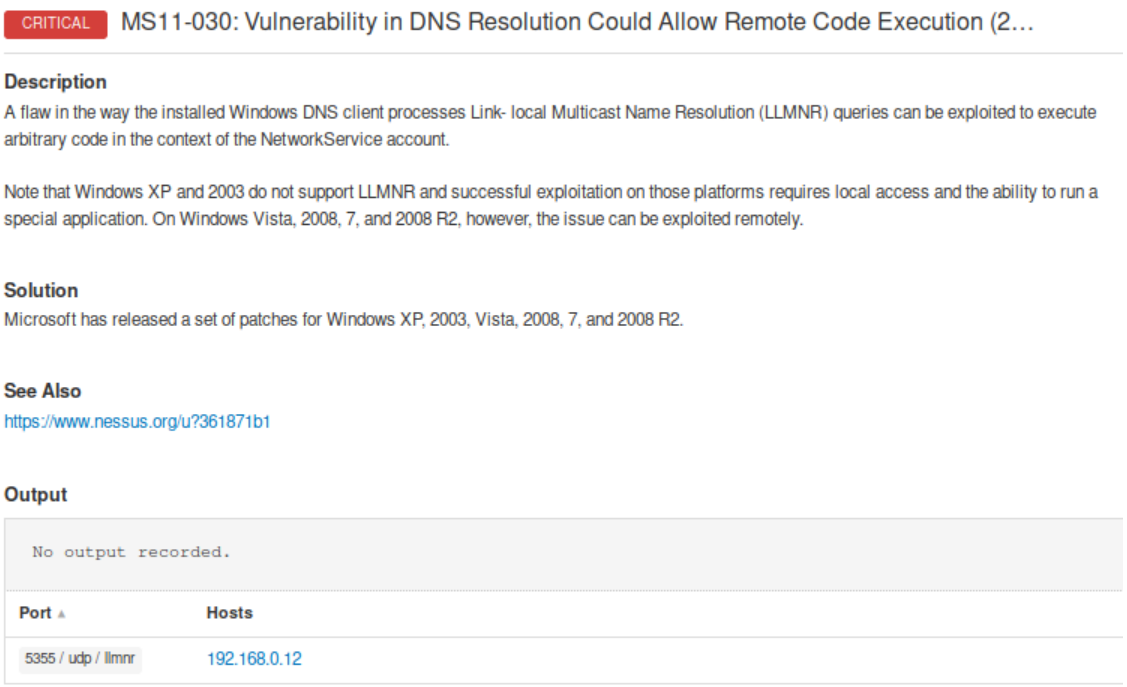
Fuente: Elaboración propia

Ilustración 35 Vulnerabilidades SO



Fuente: Elaboración propia

Ilustración 36 Vulnerabilidad Critica de ejecución remota



Plugin Details

Severity:	Critical
ID:	53514
Version:	1.18
Type:	remote
Family:	Windows
Published:	April 21, 2011
Modified:	August 5, 2020

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 8.3

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C

IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: April 12, 2011

Vulnerability Pub Date: April 12, 2011

Exploitable With

Metasploit (Microsoft Windows DNSAPI.dll LLMNR Buffer Underrun DoS)

Core Impact

Reference Information

MSFT: MS11-030
BID: 47242
IAVA: 2011-A-0039-S
MSKB: 2509553, 2509553
CVE: CVE-2011-0657

Fuente: Elaboración Propia

Ilustración 37 Vulnerabilidad Critica de Service Pack SO

Escaneo WIndows 7 x64 / Plugin #108797

‹ Back to Vulnerability Group

Configure

Vulnerabilities 22

CRITICAL Unsupported Windows OS (remote)

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a supported service pack or operating system

See Also

https://support.microsoft.com/en-us/lifecycle

Output

```
The following Windows version is installed and not supported:
Microsoft Windows 7 Professional
```

Port	Hosts
N/A	192.168.0.12

Plugin Details

Severity:	Critical
ID:	108797
Version:	1.11
Type:	remote
Family:	Windows
Published:	April 3, 2018
Modified:	September 22, 2020

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/o:microsoft:windows

Unsupported by vendor: true

Reference Information

IAVA: 0001-A-0501

Ilustración 38 Vulnerabilidad Alta SO

HIGH MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETER...

Description

The remote Windows host is affected by the following vulnerabilities :

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Plugin Details

Severity:	High
ID:	97833
Version:	1.24
Type:	remote
Family:	Windows
Published:	March 20, 2017
Modified:	October 15, 2020

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 8.1

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C

CVSS v3.0 Temporal Score: 7.7

CVSS v2.0 Base Score: 9.3

CVSS v2.0 Temporal Score: 8.1

CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C

IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: March 14, 2017

Vulnerability Pub Date: March 14, 2017

In the news: true

Exploitable With

Metasploit (MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption)

CANVAS ()

Core Impact

Reference Information

EDB-ID: 41891, 41987

Output

```
Sent:
00000054ff534d4225000000001803c800000000000000000000000000008200a0008000110000000
00ffffffff0000000000000000000000540000005400020023000000110000 5c00500049005000
45005c0000000000

Received:
ff534d4225050200c09803c800000000000000000000000000008200a00080001000000
```

Port ▲	Hosts
445 / tcp / cifs	192.168.0.12

Fuente: Elaboración Propia

Ilustración 39 Vulnerabilidad Control Remoto de Protocolos

MEDIUM MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentia…

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

See Also

http://www.nessus.org/u?52ade1e9
http://badlock.org/

Output

```
No output recorded.
```

Port ▲	Hosts
49156 / tcp / dce-rpc	192.168.0.12

Plugin Details

Severity:	Medium
ID:	90510
Version:	1.9
Type:	remote
Family:	Windows
Published:	April 13, 2016
Modified:	July 23, 2019

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 6.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 5.9

CVSS v2.0 Base Score: 5.8

CVSS v2.0 Temporal Score: 4.3

CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

IAVM Severity: I

Vulnerability Information

CPE: cpe:/o:microsoft:windows

Exploit Available: false

Exploit Ease: No known exploits are available

Patch Pub Date: April 12, 2016

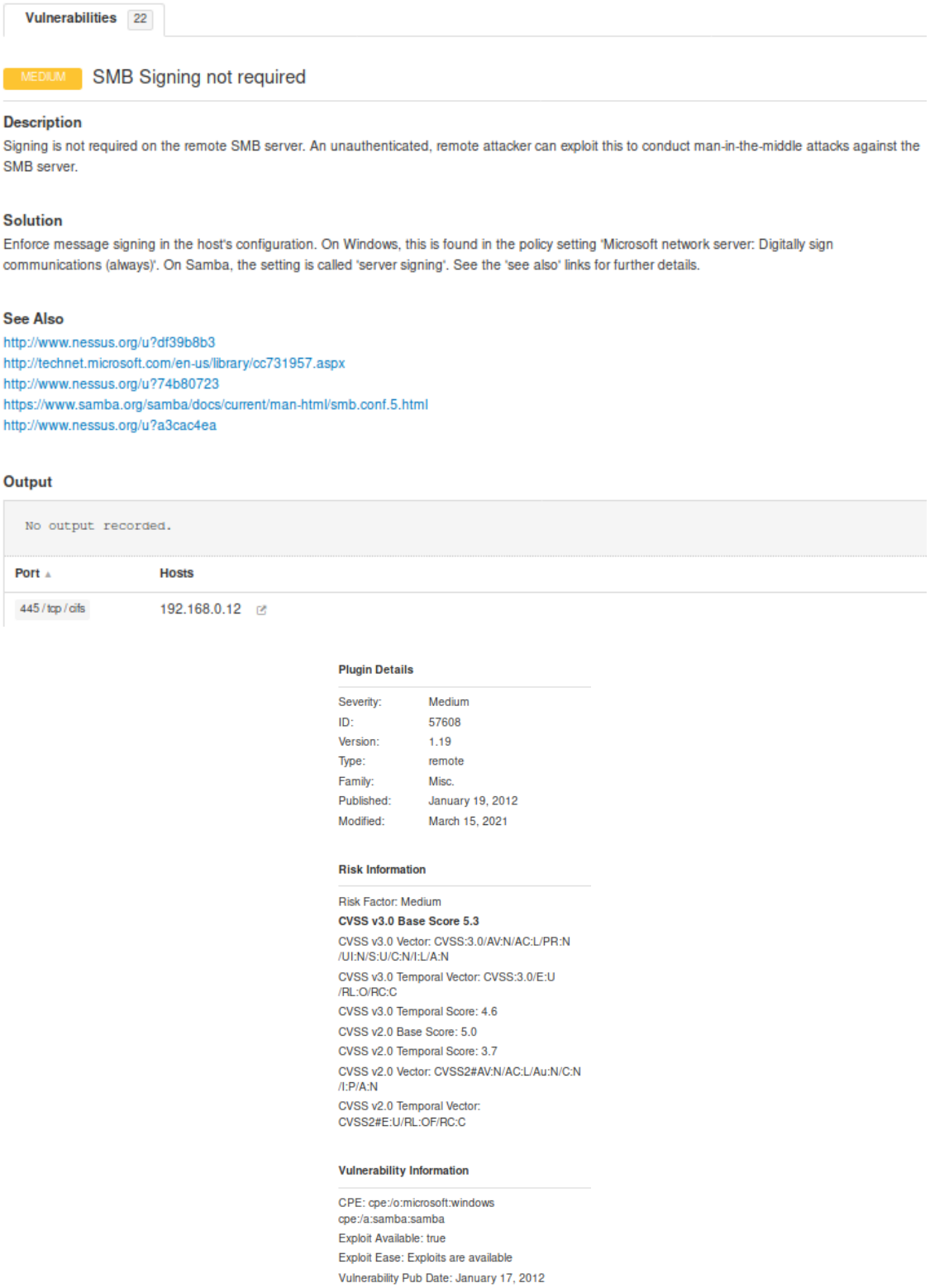
Vulnerability Pub Date: March 23, 2016

In the news: true

Reference Information

CERT: 813296
MSFT: MS16-047
BID: 86002
IAVA: 2016-A-0093
MSKB: 3148527, 3149090, 3147461, 3147458, 3148527, 3149090, 3147461, 3147458
CVE: CVE-2016-0128

Ilustración 40 Vulnerabilidad SMB protocolo



Vulnerabilities 22

MEDIUM SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Output

```
No output recorded.
```

Port	Hosts
445 / tcp / cifs	192.168.0.12

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.19
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	March 15, 2021

Risk Information

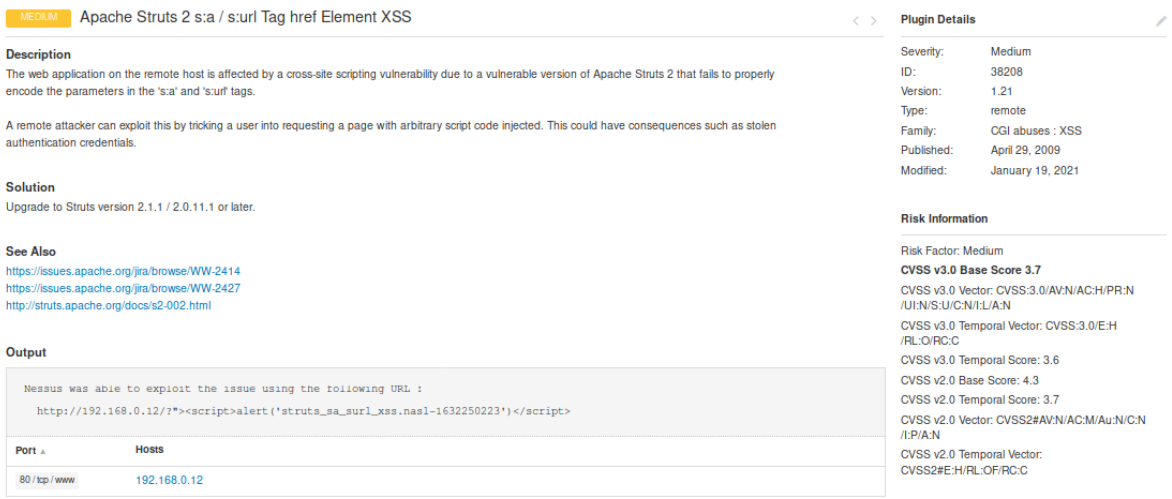
Risk Factor: Medium
CVSS v3.0 Base Score 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

CPE: cpe:/o:microsoft:windows
cpe:/a:samba:samba
Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 17, 2012

Fuente: Elaboración propia

Ilustración 41 Vulnerabilidad Apache Puerto 80



Fuente: Elaboración propia

CRITICAS

MS11-030: Vulnerabilidad de resolución de servicios DNS donde esta se puede usar para la ejecución remota de código si los atacantes logran algún tipo de acceso a las redes comprometidas con la ayuda de programas o Exploits para poder enviar consultas LLMNR para los objetivos vulnerables.

Unsupported windows OS (remote): La versión remota de Windows ya no es compatible actual por ende puede presentar vulnerabilidad de seguridad.

ALTAS

MS17-010: Esta vulnerabilidad sobre el sistema Windows aprovecha la vulnerabilidad de red SMB, permite la ejecución remota de código en las computadoras atacadas lo que permite poder cargar Malware y así poderlo propagar en la red. Permite la divulgación de información Microsoft Server Message Block SMBV1, donde los atacantes no autenticados pueden ejecutarse y revelar información detallada por medio de varios Exploits reconocidos para la ejecución remota de códigos. EternalBlue uno de ellos.

MEDIAS

MS16-047: esta vulnerabilidad permite la elevación de privilegios en un sistema si el atacante lanza ataques de tipo MiTM (Hombre en medio), donde se usan cuentas con privilegio administrativas de seguridad SAM y de tipo local, políticas de dominios

LSAD, esta vulnerabilidad permite pasar un usuario como si estuviese autenticado en el sistema.
Apache Sturts: Esta vulnerabilidad puede hacer que se ejecute código de forma remota con código malicioso enviado que no necesita autenticación de ningún tipo para explotarla la vulnerabilidad que comprometer todo el sistema donde resida.

6.3.4 Explotación de las Vulnerabilidades

Para la fase de explotación de las vulnerabilidades expuestas se hace uso de las herramientas **Metasploit Framework** que permitirá según las evidencias de cada vulnerabilidad hacer uso de esta para poder acceder al sistema objetivo.
Según la evidencia obtenida se puede hacer uso de dos variables de ejecución de intrusión sobre la maquina objetivo:

- Ataque sobre la vulnerabilidad **MS17-010**
- Ataque sobre la vulnerabilidad de servicios ofrecidos por el software de la maquina Windows con sistema en la ejecución de HTTP file Server rejetto 2.3

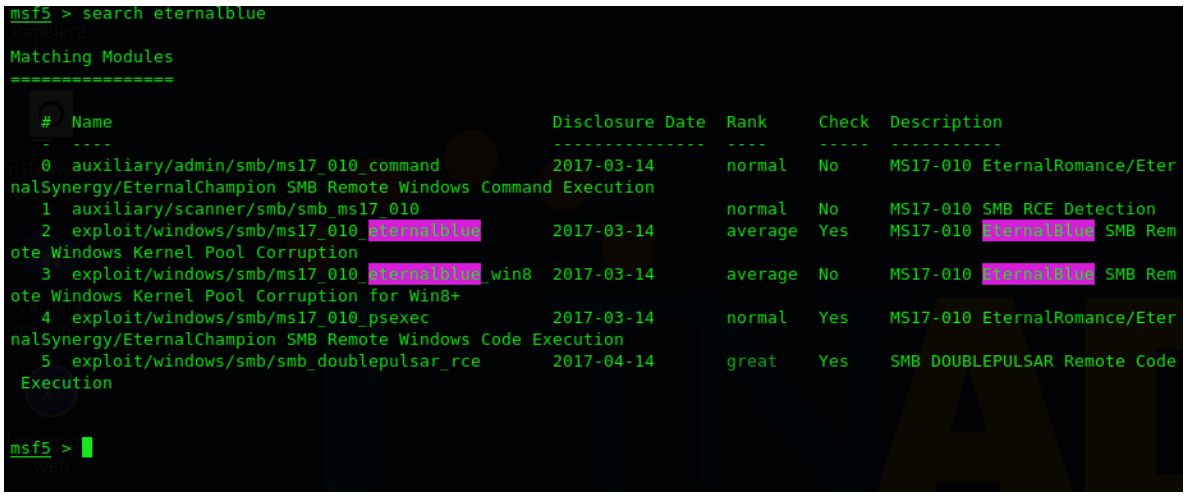
Explotación Vulnerabilidad MS17-010

Ilustración 42 Inicializar Metasploit

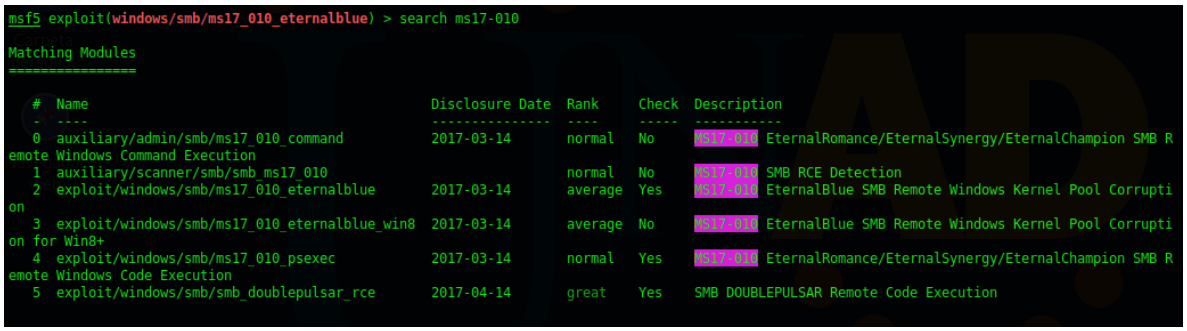
Fuente: Elaboración propia

Se realiza la búsqueda de Exploit EternalBlue el cual está codificado para poder explotar la vulnerabilidad expuesta del sistema.

Ilustración 43 Buscar Exploit

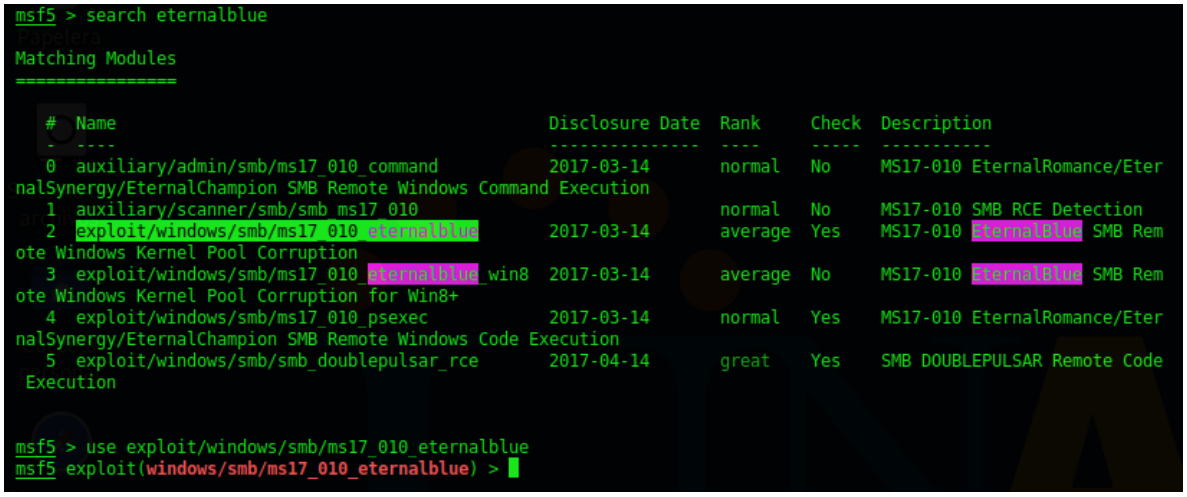


Fuente: Elaboración propia



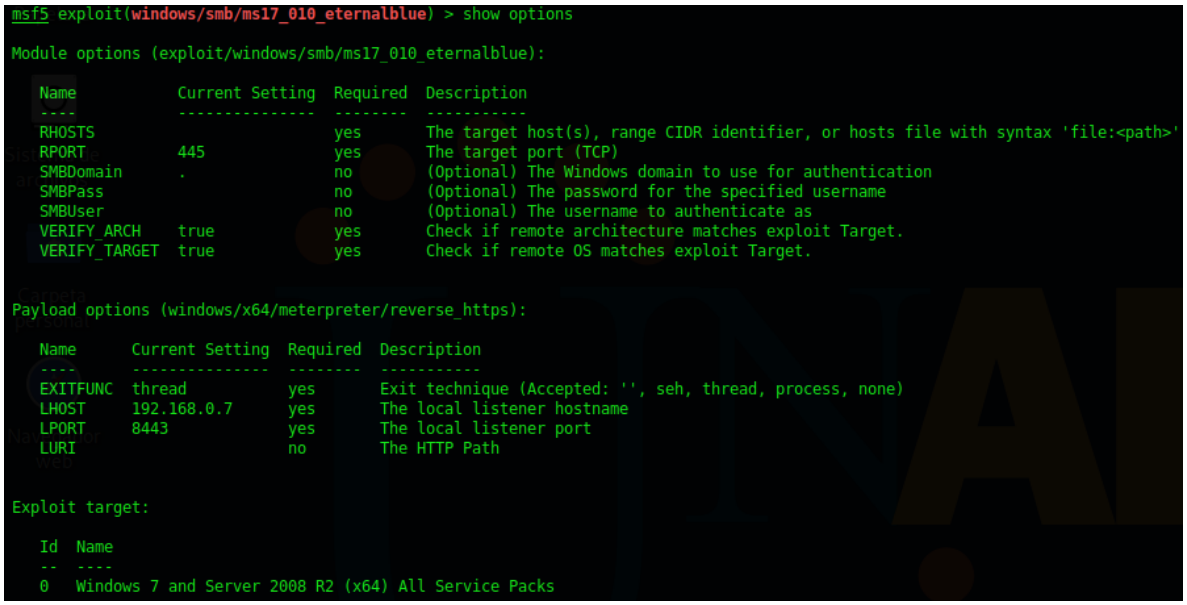
Seleccionar el Exploits para su configuración de ataque

Ilustración 44 Selección de Exploit



Fuente: Elaboración propia

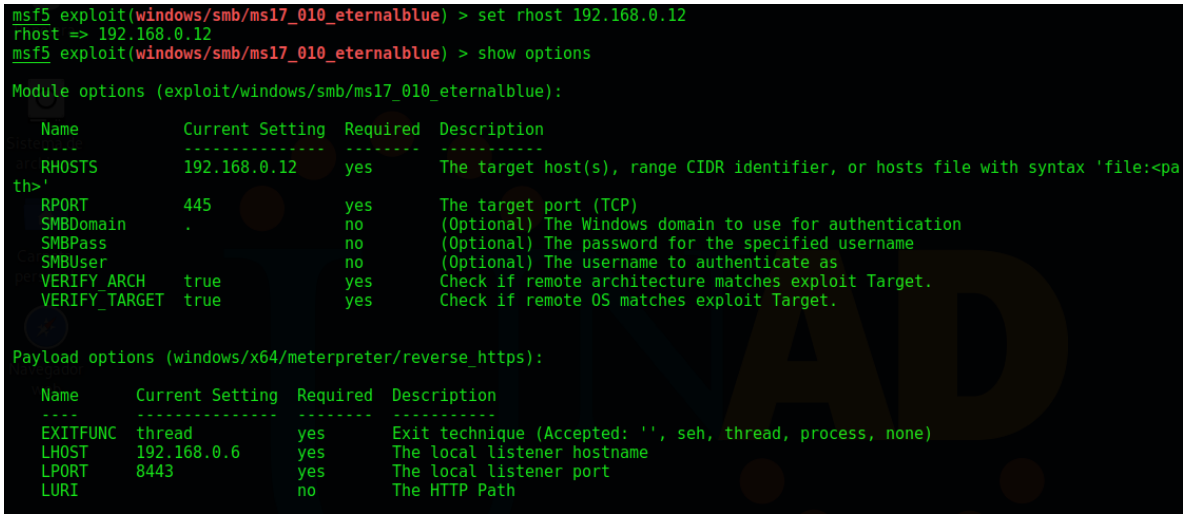
Ilustración 45 Seleccionar la opción de ataque por Host



Fuente: Elaboración propia

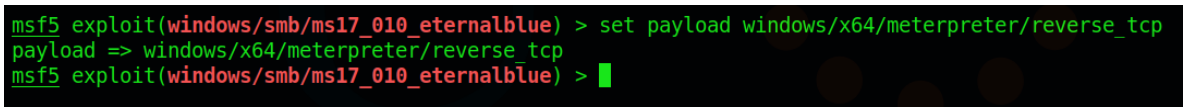
Se selecciona la opción de host remoto RHOST para el ataque sabiendo y conociendo la IP para acceder a la IP objetivo.

Ilustración 46 Seleccionar el Payload



Fuente: Elaboración propia

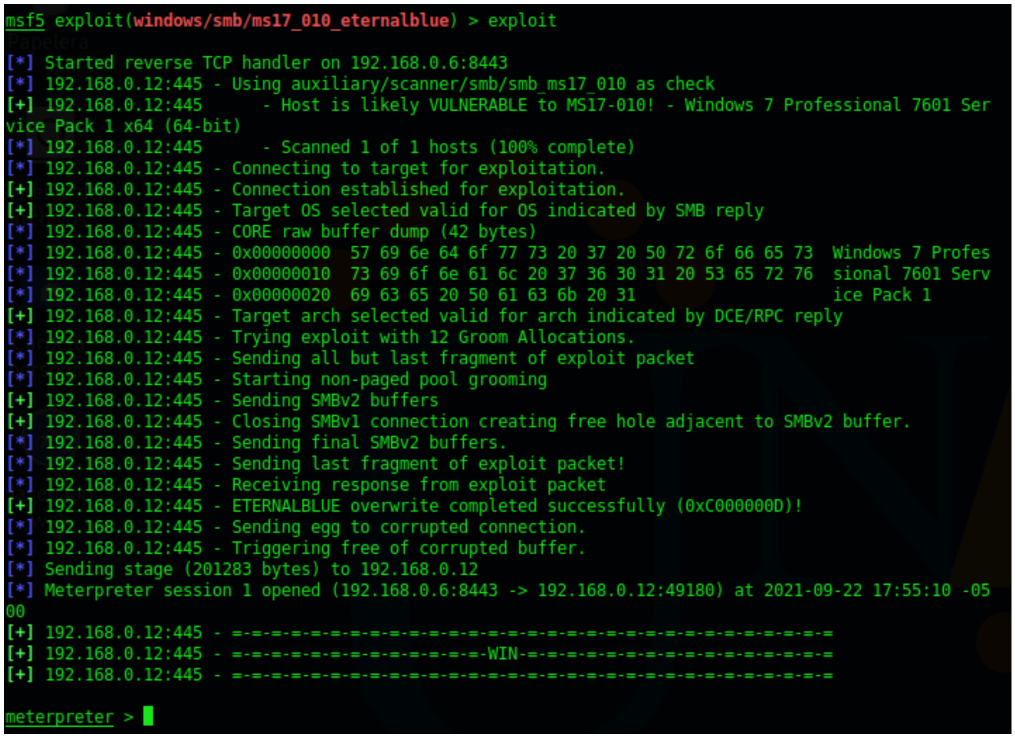
Se selecciona la opción de puerto local LPORT para la escucha por el puerto abierto 8443



Fuente: Elaboración propia

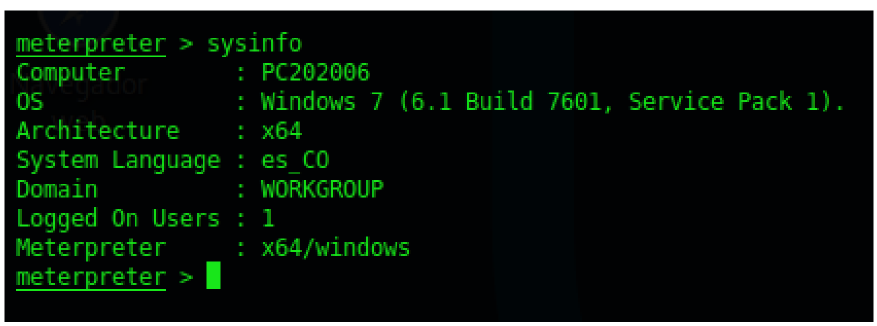
Ejecutar el Exploit para la intrusión a la maquina Windows 7 x64 y se podrá tener control de esta por medio del Meterpreter donde podemos obtener información relevante de la maquina tomada en control.

Ilustración 47 Ejecución Exploit



Fuente: Elaboración propia

Ilustración 48 Obtención de datos

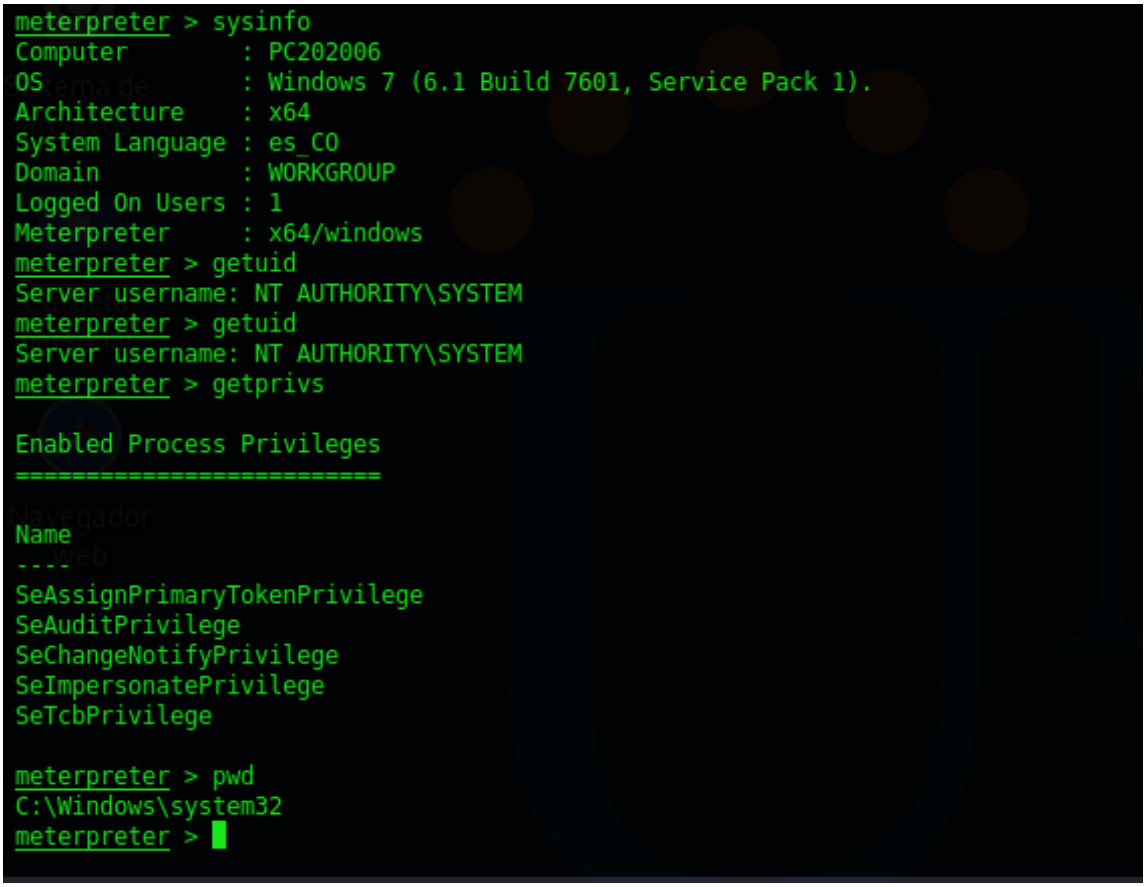


Fuente: Elaboración propia

Ilustración 49 Nivel Autorizado accedido

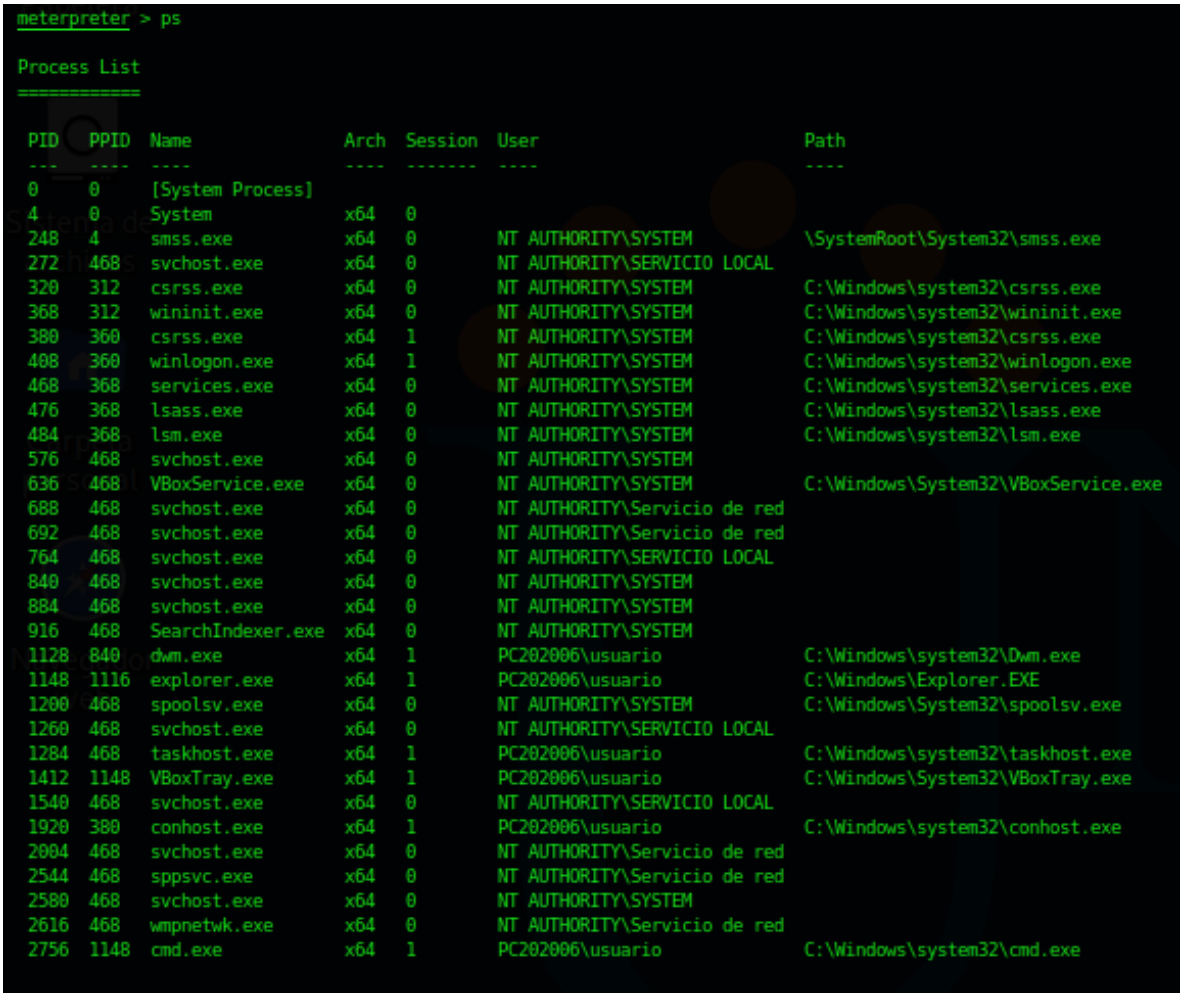
Fuente: Elaboración propia

Ilustración 50 Información del Sistema Relevante



Fuente: Elaboración propia

Se pueden obtener información de los procesos abiertos y en ejecución.

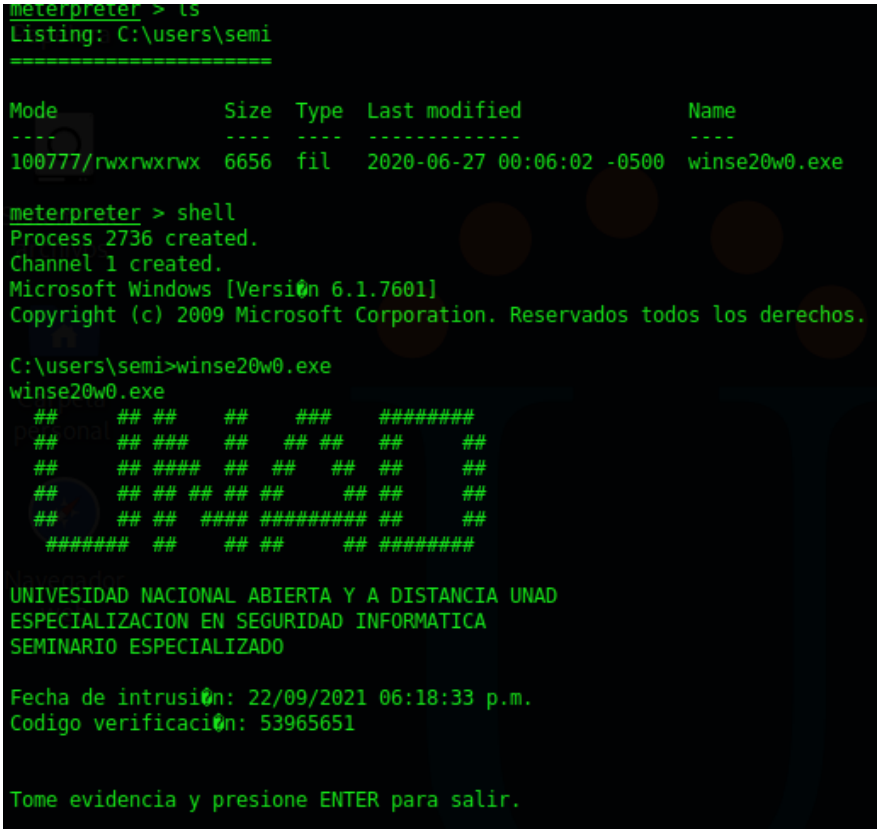


```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x64   0
 248   4     smss.exe          x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 272   468   svchost.exe       x64   0        NT AUTHORITY\SERVICIO LOCAL
 320   312   csrss.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 368   312   wininit.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 380   360   csrss.exe         x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 408   360   winlogon.exe      x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 468   368   services.exe      x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 476   368   lsass.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 484   368   lsm.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 576   468   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 636   468   VBoxService.exe   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxService.exe
 688   468   svchost.exe       x64   0        NT AUTHORITY\Servicio de red
 692   468   svchost.exe       x64   0        NT AUTHORITY\Servicio de red
 764   468   svchost.exe       x64   0        NT AUTHORITY\SERVICIO LOCAL
 840   468   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 884   468   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 916   468   SearchIndexer.exe x64   0        NT AUTHORITY\SYSTEM
 1128  840   dwm.exe           x64   1        PC202006\usuario              C:\Windows\system32\Dwm.exe
 1148  1116  explorer.exe      x64   1        PC202006\usuario              C:\Windows\Explorer.EXE
 1200  468   spoolsv.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1260  468   svchost.exe       x64   0        NT AUTHORITY\SERVICIO LOCAL
 1284  468   taskhost.exe      x64   1        PC202006\usuario              C:\Windows\system32\taskhost.exe
 1412  1148  VBoxTray.exe      x64   1        PC202006\usuario              C:\Windows\System32\VBoxTray.exe
 1540  468   svchost.exe       x64   0        NT AUTHORITY\SERVICIO LOCAL
 1920  380   conhost.exe       x64   1        PC202006\usuario              C:\Windows\system32\conhost.exe
 2004  468   svchost.exe       x64   0        NT AUTHORITY\Servicio de red
 2544  468   sppsvc.exe        x64   0        NT AUTHORITY\Servicio de red
 2580  468   svchost.exe       x64   0        NT AUTHORITY\SYSTEM
 2616  468   wmpnetwk.exe      x64   0        NT AUTHORITY\Servicio de red
 2756  1148  cmd.exe           x64   1        PC202006\usuario              C:\Windows\system32\cmd.exe
```

Fuente: Elaboración propia

En base a estas evidencias podemos hacer la ejecución de un ejecutable que está en esta máquina para corroborar que la maquina está bajo control total de intrusión y por ende hacer cualquier tipo de ataque sobre esta máquina y de la red desde la misma maquina Win7 x64

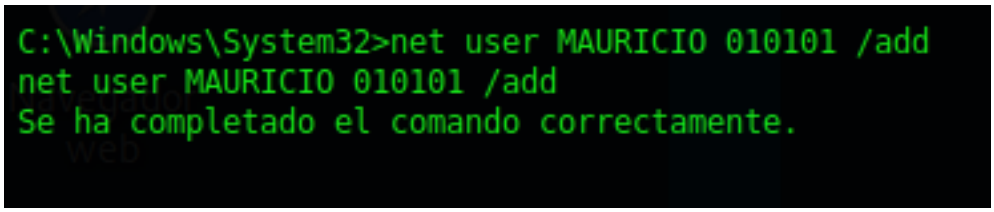
Ilustración 51 Evidencia de Control



Fuente: Elaboración propia

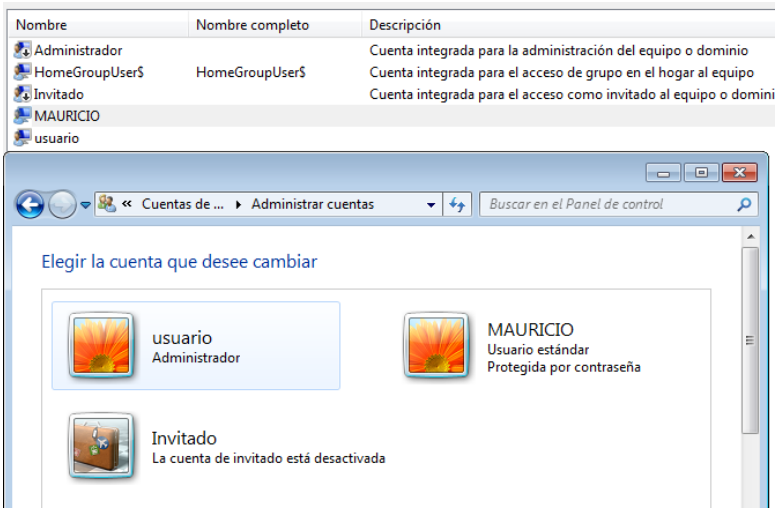
Se realiza la investigación si es posible la creación de un usuario con privilegios después de accedida la maquina por ende se debe usar Shell que permita por consola de comandos cmd crear dicho usuario,

Ilustración 52 Crear usuario con contraseña



Fuente: Elaboración propia

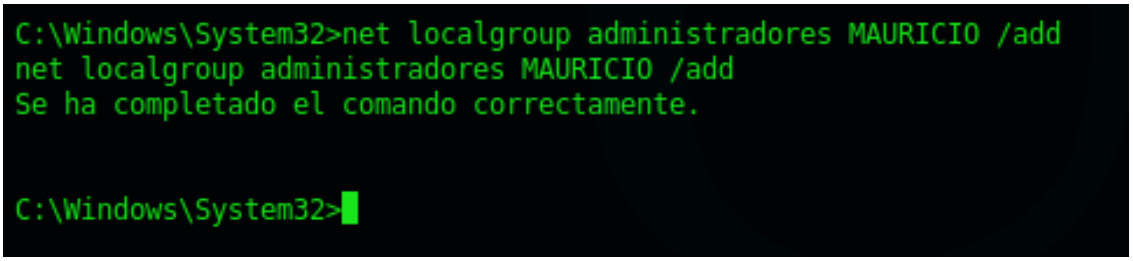
Ilustración 53 Usuario Creado

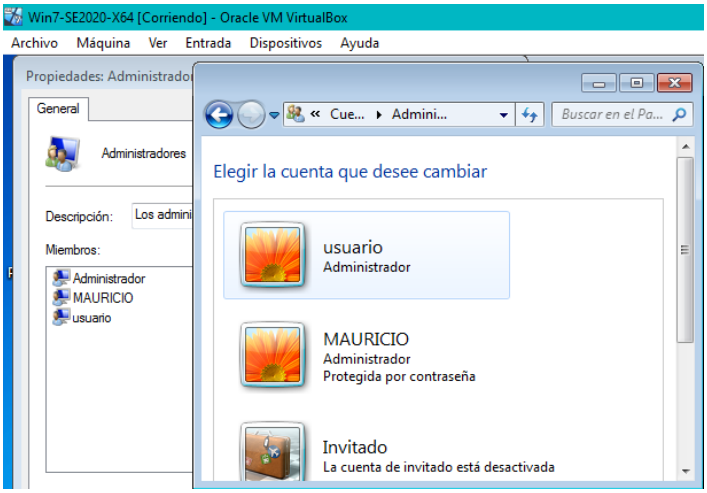


Fuente: Elaboración propia

Dar privilegios de administrador al usuario creado

Ilustración 54 Privilegio Administrador



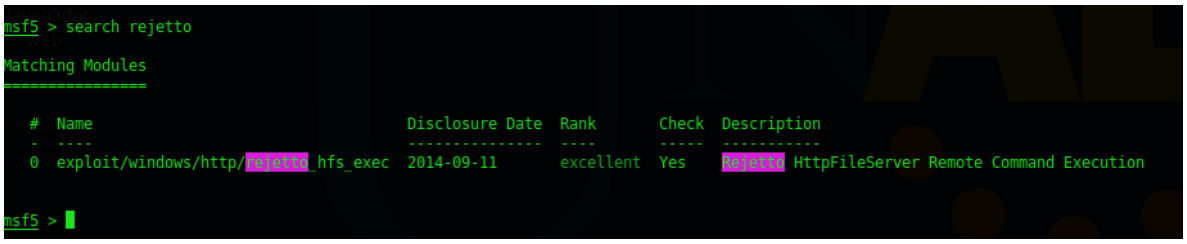


Fuente: Elaboración Propia

Explotación Vulnerabilidad rejetto v. 2.3

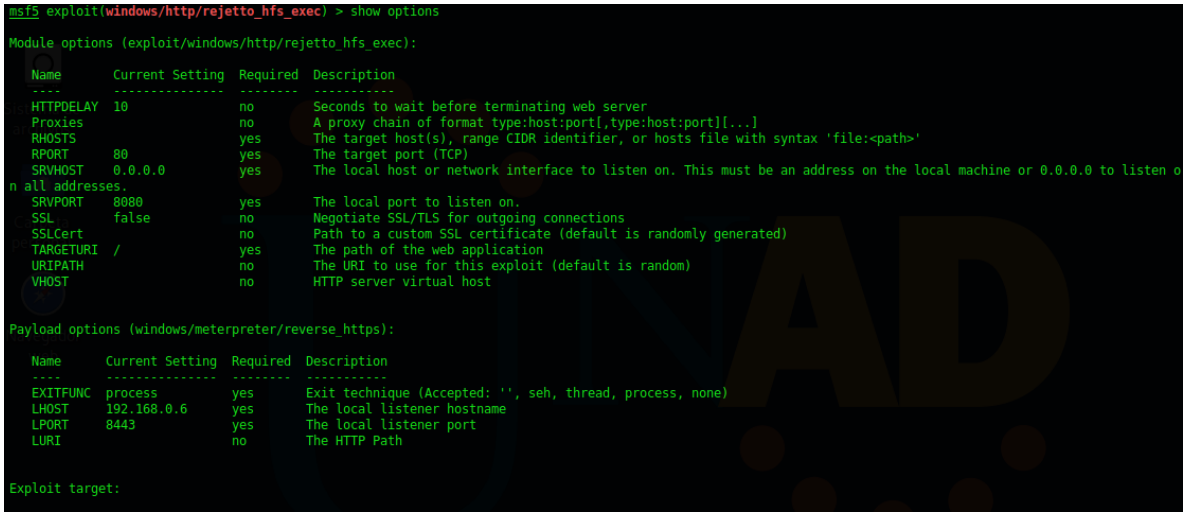
Se realiza otro proceso para explotar dicha vulnerabilidad, una vez se ejecuta la consola de Metasploit se debe buscar el Exploit para dicha vulnerabilidad

Ilustración 55 Buscar Exploit para rejetto



Fuente: Elaboración propia

Ilustración 56 Usar Exploit con Opciones



Fuente: Elaboración Propia

Tomar la opción nuevamente de RHOST y verificar que la opción quede cargada para activar el payload

Ilustración 57 Verificar IP ingresada

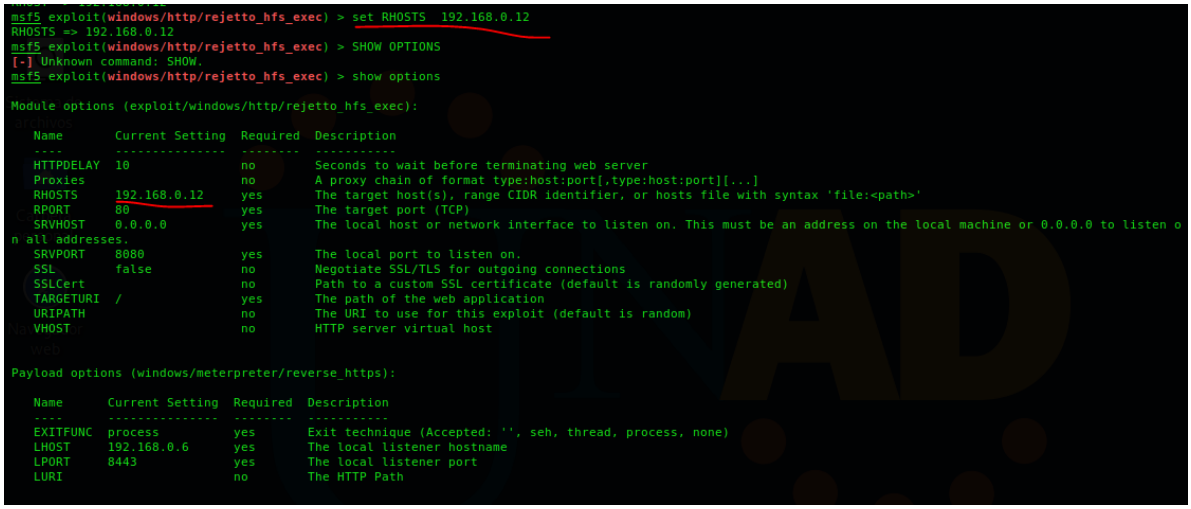
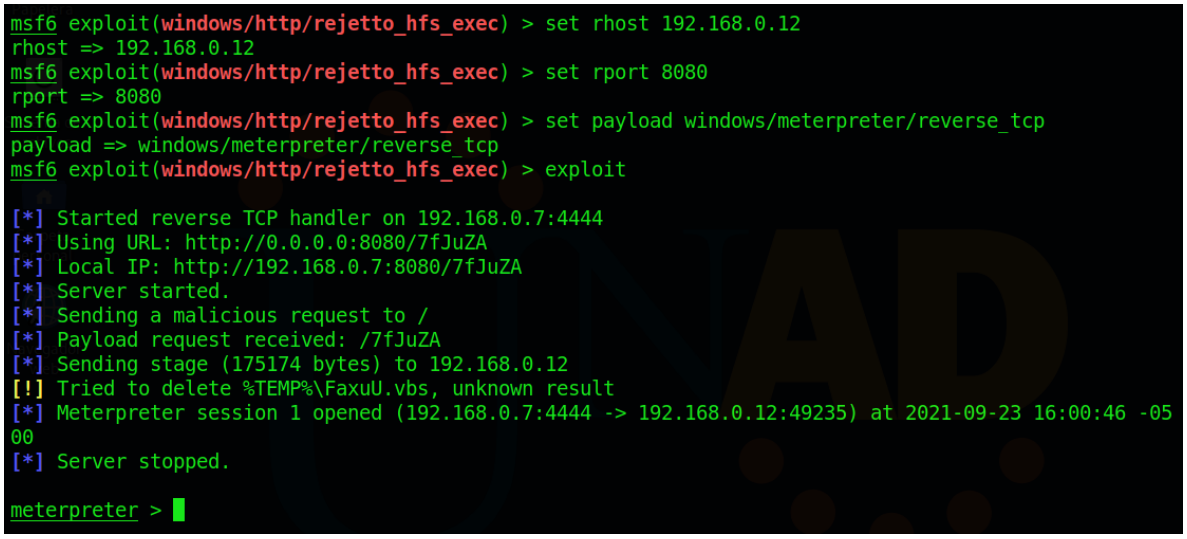


Ilustración 58 Cargar Payload configurado

Ingresar los parametros de ataque y cargar el payload y ejecutar el exploit como se evidencia realiza la conexión meterpreter.

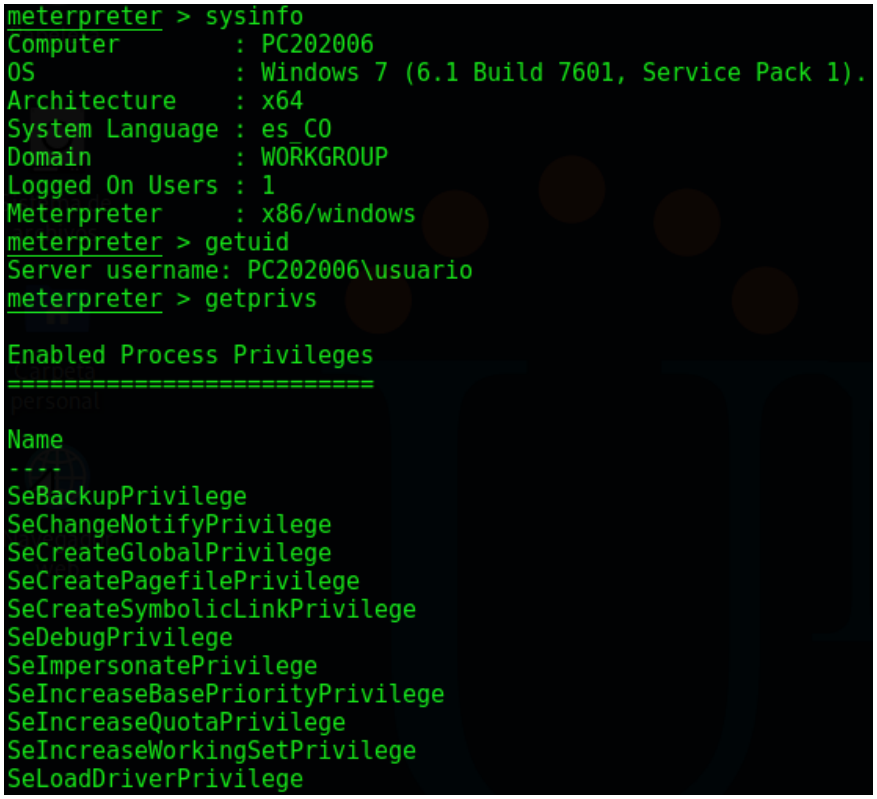


Fuente: Elaboración propia

Se realizan las pruebas de que se posee el control de la máquina y obtención de datos e información por medio de rejetto como enlace de la vulnerabilidad explotada

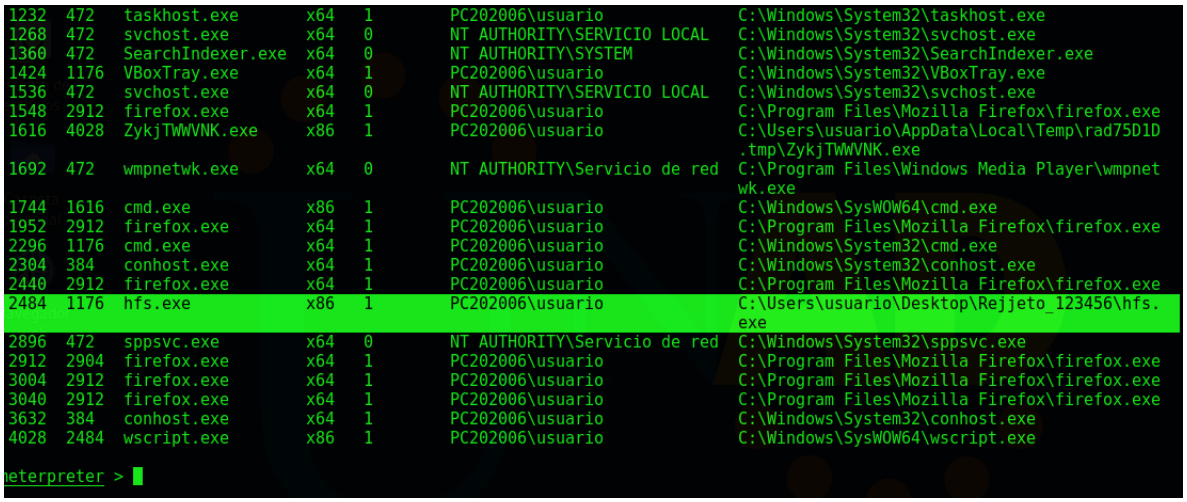
Fuente: Elaboración propia

Ilustración 59 Información del Objetivo Controlado



Fuente: Elaboración propia

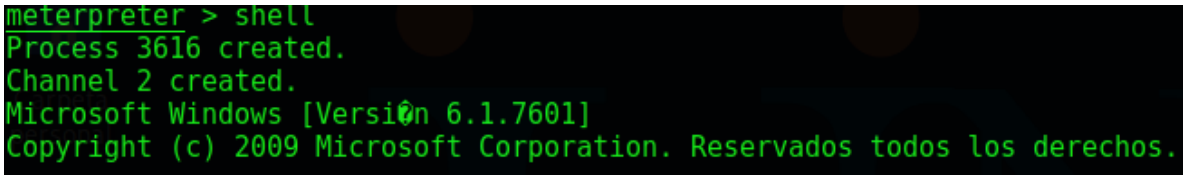
Ilustración 60 Verificación de servicios Corriendo y Rejetto entre ellos



Fuente: Elaboración propia

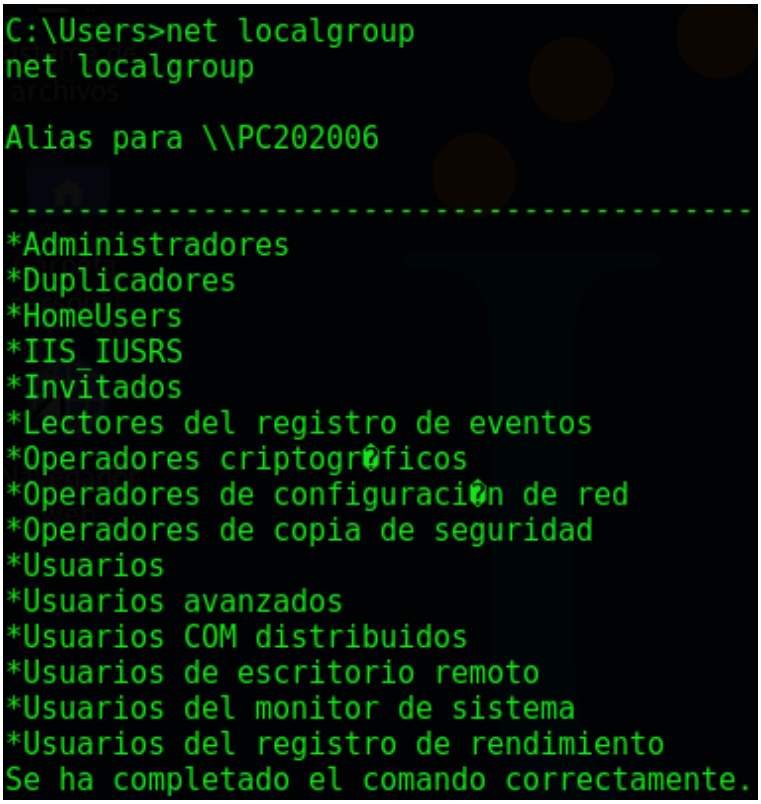
Se realiza la validación de los usuarios creados entre ellos el de MAURICIO el cual se creó ingresando con la vulnerabilidad anterior descrita.

Ilustración 61 Crear la Shell



Fuente: Elaboración propia

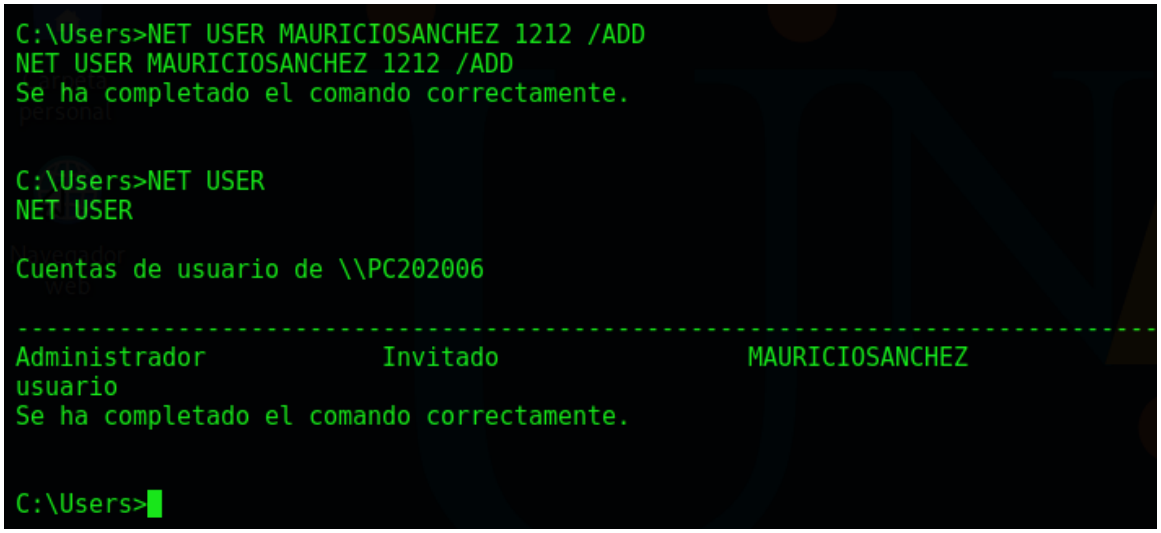
Ilustración 62 Verificación Tipos de Usuarios Win7



Fuente: Elaboración propia

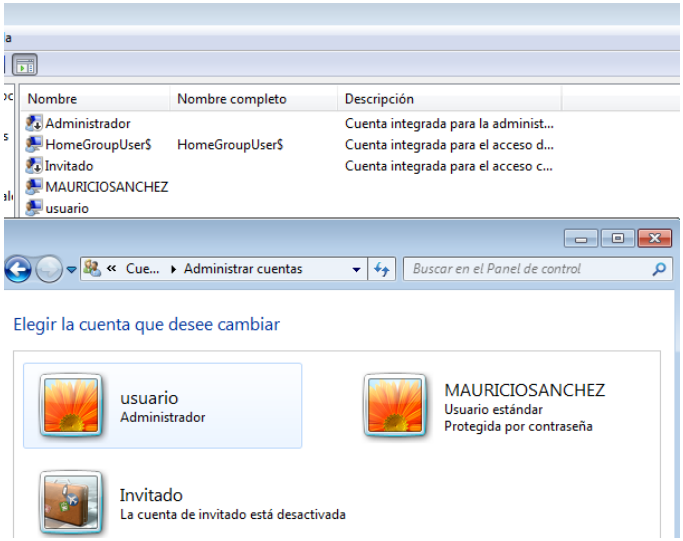
Se procederá con la creación de un usuario y cambio de perfil a administrador

Ilustración 63 Creación Usuario por comandos



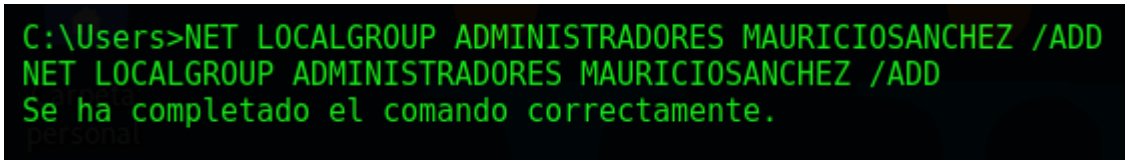
Fuente: Elaboración propia

Ilustración 64 Evidencia Usuario Creado



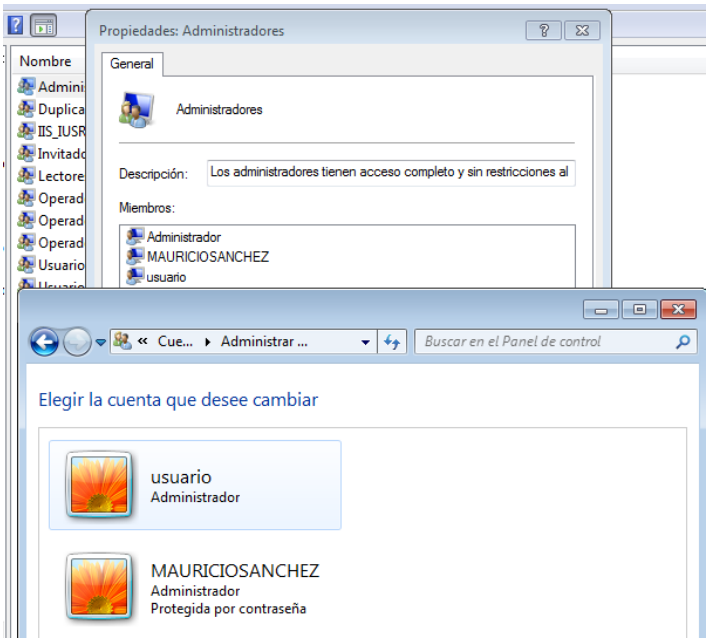
Fuente: Elaboración propia

Ilustración 65 Cambio Perfil Usuario



Fuente: Elaboración propia

Ilustración 66 Evidencia Cambio Perfil Usuario a Administrador



Fuente: Elaboración propia

6.3.5 Informe de Cuestionamientos y respuestas

Identificación de datos e información de evidencias documentales Anexo 4:

Según las evidencias entregadas por la organización fueron de ayuda para tener una base de cual podrían ser las falla de seguridad, en ella se indicaban las fallas de seguridad sobre
Aplicación instalada Software REJETTO VERSION 2.3 HTTP FILE SERVER
Aplicación podría contener vulnerabilidades asociadas a un Exploit que puede acceder con el uso de meterpreter y por medio de un Shell ejecutar comandos en la maquina Windows 7 x64
Con esta información se logra identificar después del proceso de Pentesting corroborar algunas de lo analizado en las fases iniciales y de esta forma usar y buscar el Exploit correcto para cada vulnerabilidad encontrada

Herramientas usadas para la identificación de vulnerabilidades

NMAP y **MASSCAN** para el análisis del objetivo y recaudo de datos en información de los objetivos, puertos abiertos, descripción de sistemas operativos, descripción de servicios asociados a los puertos de comunicación abiertos en la maquina Windows 7 x64.

OPENVAS y **NESSUS** para la identificación de las vulnerabilidades del objetivo, obteniendo datos de fallos de seguridad del sistema operativo y de software que permite la explotación de estas de forma remota, posibles formas de explotación y posibles medidas de Hardering para las correcciones de estas.
Según las evidencias del proceso de análisis inicial y de escaneo de las vulnerabilidades la aplicación File Server abre el puerto 80 8080

Ilustración 67 Puerto Afectado Rejetto

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3k
|_http-server-header: HFS 2.3k
|_http-title: HFS /
```

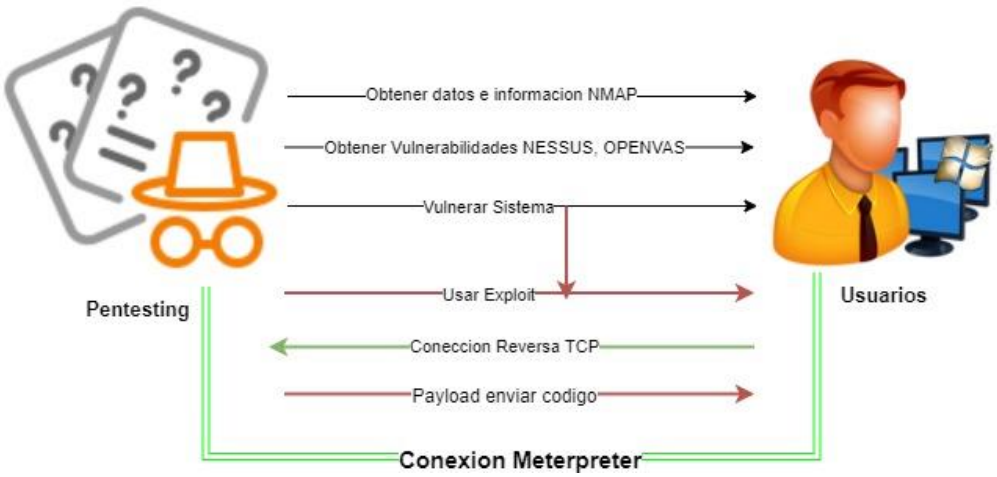
Fuente: Elaboración propia

Como afecta el ataque a la maquina Win7 x64

Este tipo de ataques buscan la forma de valerse de las vulnerabilidades de aplicaciones y sistemas operativos, malas configuraciones, sistemas obsoletos, sistema no actualizados para hacer la intrusión remotamente, de esta forma se da un tipo de ataque de ejecución remota de código que se vale de protocolos de seguridad como SMB y sus puertos de comunicación para poder lograr el objetivo. Una vez se ejecuta el ataque es muy posible que el atacante escale privilegios, cambie información, extraiga información, altere datos o logre infiltrar otras máquinas de la red si ya está dentro de un equipo con los suficientes privilegios que ha podido conseguir. Este tipo de ataque vulnera los principios de confidencialidad, integridad y disponibilidad de la información.

La representación gráfica hace referencia al proceso de ataque

Ilustración 68 Grafica de ataque resumen



6.4 ETAPA CUARTA LAS ESTRATEGIAS DE CONTENCION

Acciones ante de mi parte en un ataque en tiempo real

Según un modelo estandarizado de incidentes se deben seguir unos pasos específicos para tener una respuesta eficaz y eficiente ante cualquier incidente que se presente. Los equipos como Blue Team deben conocer los aspectos de las estrategias, métodos y metodologías como estrategias de contención y defensa.

6.4.1 Preparación de Análisis y Prevención

Establecer procedimientos: Se deben crear los procedimientos donde se especifique que hacer en caso de incidentes de tiempo real con el objeto de saber cómo actuar sin demoras y ordenadamente.
Establecer y usar procedimientos de copias de seguridad y restauración: Se deben poseer copias de seguridad de datos e información actualizada para poder dar solución como contingencia en caso de que el ataque que haya afectado este activo.
Establecer la gestión preventiva de parches de seguridad: Se deben establecer procedimientos de actualización y mantenimiento de parches de seguridad y actualizaciones en SO, Bases de Datos y aplicaciones que use la empresa. Se deben monitorear.
Establecer la seguridad de las redes: Se deben usar y activar sistemas Firewall
Establecer y activar antivirus
Determinar el nivel del riesgo e impacto del incidente: Se debe determinar el impacto de los incidentes según el tipo de incidente y el activo que están siendo afectado por este. Crítico, medio, alto o bajo y escalas de 1 al 10 de impacto.

Tabla 2 Niveles de Riesgo

descripción	nivel
Servicios de la infraestructura tecnológica totalmente afectados y detenidos	Critico
Servicios de la infraestructura afectada no presta algún tipo de servicio especifico	Alto
Servicios se prestan parcialmente con intermitencias y lentitud	Medio
Servicios se prestan con efectos casi nulos en la infraestructura	Bajo

Determinar activos afectados: Se debe hacer un análisis de que activos está siendo impactado y como lo está impactando el ataque.
Determinar la criticidad de los incidentes: Se debe determinar qué tan crítico es el incidente para la empresa para de esta forma determinar el nivel en la respuesta ante este.

Alto: Atension inmediata	Medio: atención inmediata con un tiempo de 4 horas	Bajo: atención se puede dar de 8 a 24 horas

Determinar área de la empresa afectada: Se debe determinar que partes de la empresa han sido afectadas y así mismo informar
Capacitación y entrenamiento: se debe hacer uso de este proceso constantemente al personal en seguridad, concienciación de amenazas y el uso correcto de la tecnología y activos de la información.

6.4.2 Detección de los incidentes

Usar sistemas software: Se debe hacer uso de sistema de detección de eventos ya sea de consolas de antivirus, IDS, IPS, Firewalls u otro tipo de herramienta que permita detectar que está pasando en el momento exacto del ataque en línea.
Verificar el tráfico de red: Se deben hacer escaneos constantes de la red para determinar si hay algo anormal en el tráfico y así hacer una detección efectiva sobre este activo.
Se debe conocer el comportamiento normal de la red
Se debe conocer puertos y servicios en uso
Se deben conocer los horarios de tráfico y utilización de los recursos de red
Se deben conocer y monitorear las IP de la red entendiendo cada activo que la usa.
Identificación del incidente:
Se debe definir el tipo de incidente y cómo está clasificado, esta clasificación ya debe estar diseñada en el modelo y según las evidencias de las vulnerabilidades detectadas se deben ejecutar las acciones de prevención de incidentes.
Determinar el tipo de ataque: Se debe determinar cuál es el tipo de ataque que se ha recibido o está en curso como:
Ataque de denegación de los servicios
Ataque por Malware en todas sus variantes
Ataque inyección SQL
Ataques de fallos por contraseñas
Ataques Phising

6.4.3 Contención, Erradicación y Recuperación:

Su objetivo es el de evitar la propagación del incidente a otras máquinas de la red o dependencias, por ende se deben tomar las medidas inmediatas sobre el activo afectado

Acciones de tipo inmediato de contención:

- Sacar el activo de la red de la organización
- Aislar el activo para posteriores investigaciones
- Quitar los servicios que proporciona el activo para evitar más alteraciones de la seguridad.

- Realizar una copia completa del sistema afectado para hacer la investigación forense y determinar causas, responsables y soluciones.
- Salvaguardar el activo para acciones legales si fuera el caso
- Activar planes de contingencia
- Si se determina la fuente de ataque como correos se deben bloquear los remitentes
- Si se determina la fuente de ataque a nivel de red se debe bloquear tráfico en el firewall y filtrar paquetes.

Realizar copias del sistema afectado cuando ocurre el incidente o ataque para la posterior investigación forense
Usar el software de seguridad: como sistemas contra Malware, antivirus sobre sistemas afectados para erradicar este tipo de amenazas si están presentes tanto en equipos y sistemas de red.

Las estrategias de erradicación y recuperación implican:
Poner en funcionamiento los servicios caídos y afectados después del incidentes con monitoreo constante sobre estos.
Corregir daños en la información y datos por medio de Backups probados y actualizados.
Reinstalación de sistemas como SO o servicios de red.

6.4.4 Actividades Post Incidente

- Esta fase se debe hacer los informes necesarios que documenten todo lo ocurrido con las especificaciones técnicas requeridas su impacto, responsables,
- Levantar un procedimiento para el tipo de ataque específico y documentar las soluciones para este en caso de volver a presentarse.
- Capacitación sobre el incidente para llevar una fuente o base de conocimiento de los mismos por si se vuelve a presentar y con este se tenga la base para solucionarlo en el menor tiempo.
- Determinar que recursos tecnológicos se usaron para analizar, detectar, erradicar, recuperar los sistemas afectados
- Determinar el equipo humano necesario para solventar el incidentes
- Determinar las fallas en la seguridad para las correcciones necesarias

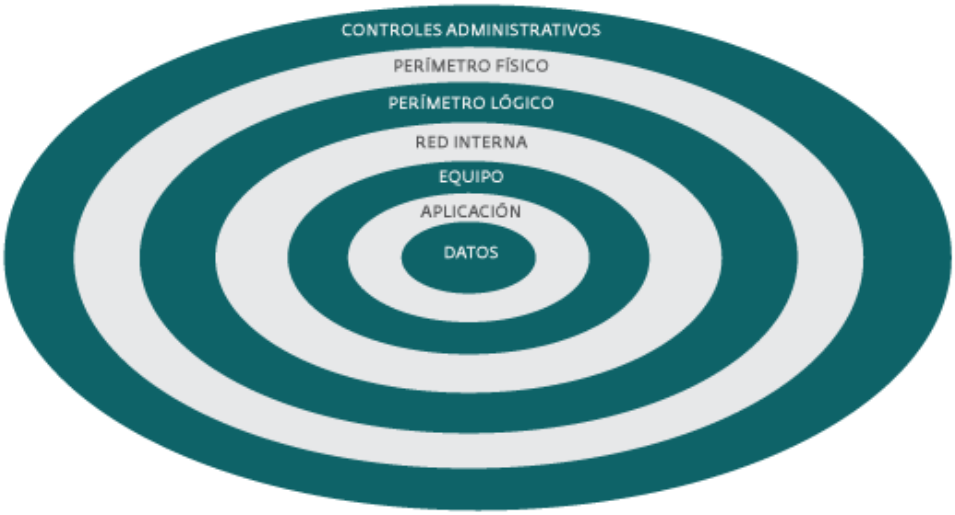
6.5 MEDIDAS DE HARDERING CASO EXPUESTO POR RED TEAMS

Esta técnica hace referencia al endurecimiento de la seguridad en el ajuste de las características correctas de algún tipo de sistema de forma correcta, esto con el objetivo de minimizar las vulnerabilidades sobre activos.

Para el caso expuesto por el equipo Red Team como expertos en seguridad podemos hacer uso de un modelo de “defensa en profundidad” para poder hacer el endurecimiento de forma adecuada de la organización en todos sus niveles de la infraestructura que posean.

El modelo sugerido se refleja en la imagen:

Ilustración 69 Modelo Defensa en Profundidad



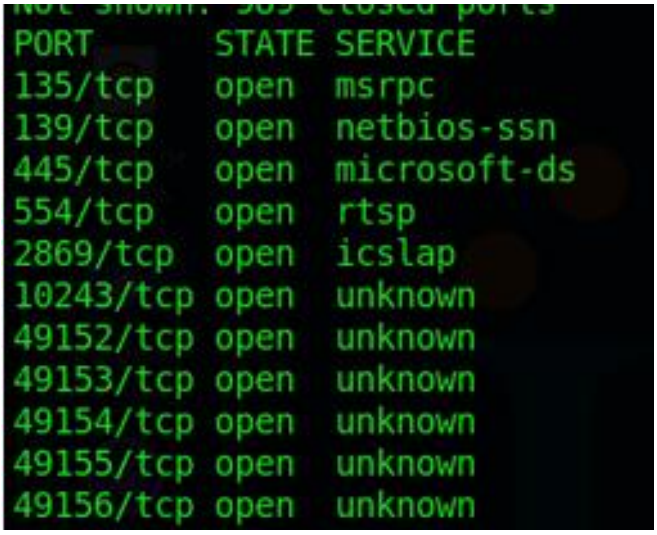
Fuente: https://www.welivesecurity.com/la-es/2010/05/24/defensa-en-profundidad/

Controles Administrativos:
Se deben crear las políticas de seguridad de la información, usar procedimientos y estándares, educar en seguridad a usuarios.
Usar controles específicos para la infraestructura como CIS Benchmarks y NIST

Perímetro Lógico:
Activar e implementar el firewall perimetral para filtrar el tráfico que entre y sale de la red, revisar las reglas sobre los puertos identificados como vulnerables en las escaneos de vulnerabilidades.

Los puertos que se deben configurar y revisar en las reglas son:
135 TCP: Establecer regla para que no se quede expuesto a sistemas externos de la red, de esta forma que no puede ejecutar nada por este de forma remota.

139 TCP: Establecer regla para que no quede expuesto fuera de la red.
445 TCP: Puerto que ejecuta SMB para intercambio de archivos y recursos de red, es la versión mejorada del puerto 139 que si en este caso no se usa se debe desactivar y usar el 445 al cual se le debe establecer reglas de solo uso en la red interna y que no quede expuesto al exterior para evitar los ataques de Eternal Blue y ataques de ejecución remota de código como se evidencio por el equipo Red Teams.
49152, 49153, 49154, 49155, 49156: Se deben deshabilitar son puertos P2P que no están en uso y por ende son vulnerables a un ataque. En caso tal que se haga algún uso o se usa para algún servicio se debe poner una regla de este en el firewall



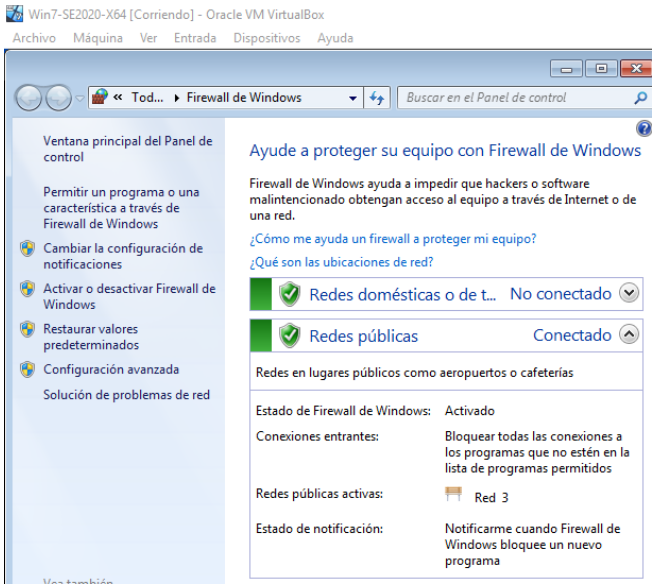
Fuente: Elaboración propia

Implementar algunas herramientas como Honepots que funcionen como señuelos para los atacantes para poder analizar y aprender de ataques que se den.

Red interna:
Se recomienda usar sistemas de detección de intrusos IDS/IPS
Se recomienda usar ACLS para la autenticación correcta de los usuarios
Se recomienda la implementación de servidor de directorio activo para la gestión y control de usuarios y administración de privilegios en la red, para evitar que se escalen o se eleven según las evidencias de los ataques al equipo Windows 7 x64
Segmentar la red Vlans para cada dependencia
Usar sistemas de análisis de trafico como Wireshark para analizar los paquetes que ingresan a la red y así poder descubrir si se está usando algún tipo de Exploit contra alguna IP de la empresa.
Usar y activar los protocolos de seguridad como SSL/TLS

Equipos de cómputo:
Se deben activar los firewall de host de la maquina

Ilustración 70 Activar Firewall Win7 x64

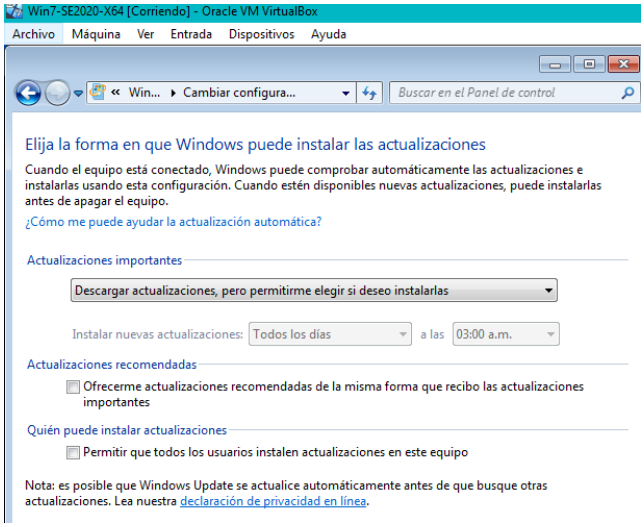


Fuente: Elaboración propia

Activar las actualización automáticas sobre la máquina, si el equipo es ingresado a un sistema de directorio activo se debe hacer la gestión de parches por medio de herramientas como WSUS (Software Update Software)

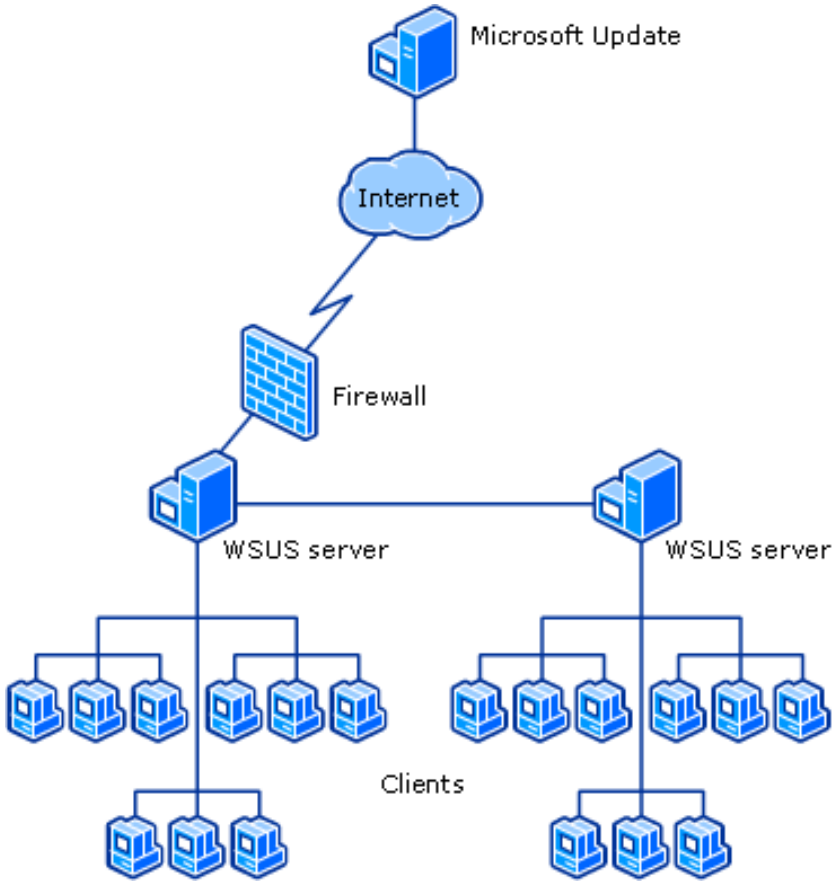
Parchar el sistema operativo, actualizar el sistema operativo con sus últimos Services Pack soluciona muchas de las vulnerabilidades expuestas a la seguridad de del SO como:
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote

Ilustración 71 Activar actualizaciones Automáticas



Fuente: Elaboración propia

Ilustración 72 WSUS



Fuente: https://www.pchardwarepro.com/como-usar-los-servicios-de-actualizacion-de-windows-server-en-el-entorno-empresarial/

Usar un sistema de Antivirus End Point que permitan el monitoreo, actualización y gestión del sistema para la protección en tiempo real de las máquinas de la red.

Deshabilitar cualquier servicio, aplicación y protocolo de red que no se use en las maquinas Windows x64, como uso compartido de recursos, accesos remotos como Telnet, el servicio de directorio LDAP

Realizar escaneo de vulnerabilidades periódicas según un cronograma dispuesto en las políticas y procedimientos.

Gestión de las aplicaciones

Se debe establecer el ciclo de vida para las aplicaciones que están instaladas o se usan para poder determinar su funcionamiento correcto, que implica su documentación, gestión de la configuración, aseguramiento de calidad, que sea

auditable, verificable para poder determinar si posee vulnerabilidades en este caso como el software que genero fallos de seguridad rejetto 2.3

Gestión de contraseñas seguras de longitud, complejidad y de permanencia y límites de intentos para poderlas bloquear si son erradas.
Activar logs de auditoria para todo evento de red y sistemas operativos

Gestión de los datos

Encriptar información sensible
Usar software de encriptación

6.6 DIFERENCIAS ENTRE BLUE TEAMS Y UN EQUIPO DE RESPUESTA A INCIDENTES

Tabla 3 Comparación BlueTeams -CSIRT

Equipos Blue Teams	Equipos Respuesta a Incidentes (CSIRT)
Es el encargado de la defensa de los sistemas de las organizaciones. Pueden hacer uso de ejercicios de simulación de ataques que son objeto de equipos como el Red Team Realizan pruebas de Vulnerabilidades Realizan las técnicas de mitigación de las vulnerabilidades que exponen. Pueden identificar riesgos y amenazas del entorno donde se desenvuelven. Ofrecen recomendaciones de seguridad para la mejorar en Ciberseguridad. Ofrecen acciones de mejora proactivas de detección y respuesta antes incidentes de seguridad. Este tipo de equipos entiende todas las etapas de un incidente de seguridad para dar respuesta ante ellos. Pueden realizar tareas de análisis forenses sobre distintos tipos de	Proveen dentro de las empresas servicios de soporte para la prevención, gestión ante incidentes de seguridad. Posee una estructura de escalamiento de respuestas a incidentes y fallos. Los niveles de respuesta pueden estar en la escala de nivel 1 que sería como la mesa de ayuda o Service desk, nivel 2 técnicos, 3 niveles el especialista de la aplicación, los niveles superiores al 3 serían de tipo coordinación y jefes de áreas. Algunos de sus objetivos se basan en: Verificar un incidente de seguridad se ha materializado. Reducir los impactos de incidentes de seguridad. Prevenir los incidentes de seguridad Restaurar la continuidad de las operaciones del negocio después de un ataque Algunas de sus funciones se basan en: Servicios reactivos que son proceso que se realizan ante un evento de seguridad conocido o detectado como

sistemas para poder dar con las causas de incidentes o ataques. Estos equipos hacen uso de plataformas de la gestión de eventos SIEM, para la detección de fallos en línea y poder clasificar las alarmas en el momento que ocurren. Realizar investigaciones sobre amenazas y vulnerabilidades para poder priorizar acciones. Realizar análisis de tráfico y de datos. Evalúan sistemas para la detección de vulnerabilidades que pueden afectar cualquier sistema que custodian. Buscan la forma de evitar, resistir y responder ante las amenazas de seguridad. Están en la capacidad de desarrollar políticas de seguridad para las organizaciones. En muchas ocasiones se deben considerar como un recurso interno de las empresas ya que son parte de la estructura de seguridad de estas organizaciones. Puede hacer uso de una gran cantidad de herramientas para el análisis, monitoreo y prevención de ataques.	de un virus, una máquina de la red afectada. Son unos componentes de alta importancia para equipos CSIRT. Servicios Proactivos que son servicios de preparación, protección y aseguramiento de los sistemas antes de que puedan ocurrir ataques ya que reducen eventos a futuro. Servicios de la gestión de calidad donde se analizan la gestión del riesgo, planes de continuidad del negocio, educación, capacitación. Estos equipos están en la capacidad de realizar un análisis correcto de los incidentes ya que por medio de la valoración, calificación pueden determinar cómo actuar dependiendo del tipo de incidente. Pueden recolectar evidencia forense con la intensión de reconstruir eventos de ataque. Realizan actividades de seguimiento de los posibles orígenes de intrusos o de los sistemas que fueron violentados. Se pueden integrar con otros Csirts o entes de control como fuerzas del estado, administradores de sistemas para la colaboración en eventos de seguridad. También de apoyo jurídico, legal y financiero. Usan gran cantidad de herramientas para su gestión, indicando un listado, descripción y justificación de las mismas. Es aconsejable que los CSIRTS sean parte de los SGSI para que de forma coordinada se cumplan los lineamientos del SGSI.

Fuente: Elaboración propia

6.7 ANÁLISIS DE TRABAJAR CON CIS “CENTER FOR INTERNET SECURITY” EN EQUIPOS BLUETEAM

En el caso particular de un trabajo conjunto entre los equipos BlueTeam y el uso de CIS sería de gran ventaja ya que estaría dando más valor de conocimiento al equipo y por ende se gana experiencia y actualización de conocimientos en base a estas técnicas de aseguramiento, buenas prácticas y controles que permitirían los fines siguientes:

- Como un conjunto de medidas que son recomendadas y documentadas para poder realizar la protección en Ciberdefensa de la organización a la cual se esté vinculado.
- Como un conjunto de controles CIS ayudan en la priorización de tareas y tácticas que son de alto impacto para la empresa y que dan una mejora en Ciberseguridad en tiempos no muy largos.
- Los controles de CIS puede y están categorizados en pilares de los cuales me valdría según las necesidades de mi seguridad y de mi análisis de requerimientos en cuanto a la seguridad que necesito
- Los CIS controles usan las mejores prácticas de seguridad para mitigar ataques en redes y sistemas.
- Se pueden usar como fuentes de conocimiento ya que se comparten conocimiento sobre ataques, causas y acciones sobre la falla de seguridad.
- Se pueden consultar distintos tipos de herramientas, ayudas y mapas de trabajo para resolver vulnerabilidades.
- Este tipo de controles son de mucha ayuda ya que muchos ataques siguen algún tipo de patrón por lo cual el control lo hace controlable en cierta medida.
- Usaría como controles específicos de CIS 18 Controles, CIS Benchmarks para buenas prácticas como en sistemas operativos, software específico , sistemas de redes, etc., y NIST controles.
- Usarlos y acoplarlos junto a los estándares y marcos regulatorios como NIST, ISO dentro del SGSI.

Ilustración 73 CIS Controls

Fuente: https://www.otechtalks.tv/cloud-security-with-cis-benchmarks/

6.8 FUNCIONES Y CARACTERÍSTICAS PRINCIPALES DE LO QUE ES UN SIEM

Este tipo de necesidades para las organizaciones ha llevado a la necesidad de ejercer control sobre grandes cantidad des de datos e información desde muchos equipos por ende se hace necesario el uso de tecnologías que las puedan manipular y procesar es por ello que los SIEM (Gestor de eventos e información de seguridad) surgen como respuesta a ello.

Los SIEM son plataformas tecnológicas y principales herramientas que usan los centros de operaciones SOC para la detección y respuesta a incidentes que ayudan en la recolección, registro y análisis de los eventos que se van produciendo en las aplicaciones, sistemas y redes. Este tipo de datos y eventos provienen de muchas fuentes como firewalls, antivirus, redes, logs, etc.

Algunas de sus características son:

- Poseen gran capacidad para la administración recibida desde distintas fuentes.
- Procesamiento de datos para transformarlas en información
- Generación de alertas con avisos de seguridad enviadas a los administradores
- Trasforma datos en información en gráficos y tablas
- La información recolectada se trasforma en informes entendibles,
- La información generada es usada en distintos tipos de ingeniería forense.
- Se puede determinar de forma anticipada incidentes que puedan ocurrir y pueden afectar la productividad de las organizaciones
- Gracias a su base centralizada de eventos se puede hacer uso de datos e información relevante a cualquier tipo de investigación.
- El software usado SIEM trabaja sobre inteligencia artificial para que se puedan gestionar potenciales vulnerabilidades y fallos de seguridad.

Componentes de un SIEM

- Sensores: Equipos encargados de recolectar y capturar la información que proviene de los distintos equipos.
- Logs: contiene los registros de los eventos que van ocurriendo y son trasladados al SIEM
- Normalización de logs: este proceso hace que cualquier tipo de datos de logs sea adoptada en un formato estándar para todo el SIEM.
- Reglas de correlación: Son eventos en los cuales se hacen las alertas de los incidentes las cuales deben ser correctamente asociadas para evitar falsos positivos dentro del monitoreo o de las redes.
- Almacenamiento: Son los sistemas de almacenamiento con grandes cantidades de información y con reglas de retención.
- Monitorización: Este proceso hace que sea posible la visualización de toda la información en un único lugar en medio de las conexiones de cada sensor que permitan la gestión de las reglas.

Algunas herramientas SIEM

Fusión SIEM: almacenamiento basado en la Nube, informes detallados y registros e eventos, modelos de detección calificados.
IBM Qradar: Gestión inteligente de incidentes
LogRhythm: Herramienta de estructurada y no estructurada de SOC
SolarWinds: Gestión de eventos de seguridad con herramientas de auditoria
Splunk: Herramienta basada en la Nube para detección, investigación y monitoreo de Ciberamenazas.
Elastic Security: Herramienta gratuita detección y análisis de amenazas.

6.9 HERRAMIENTAS DE CONTENCION EN ATAQUES INFORMATICOS

Tabla 4 Herramientas Contención

WAZUH	Wazuh: Sistema para el monitoreo de la seguridad de código abierto para detectar amenazas, monitorear de la integridad y la respuesta de incidentes, algunas de sus funciones son: Sirve para el análisis de la seguridad Realiza la detección de intrusiones Análisis de datos de registros de los sistemas Detección de las vulnerabilidades Realiza una evaluación de las configuraciones que se realizan. Respuesta a los incidentes que se puedan presentar Cumplimiento normativo acorde a las políticas organizacionales Seguridad en la Nube
Cisco Umbrella	Cisco Umbrella es una aplicación integrada basada en Internet como su infraestructura para poder bloquear y contener destinos y distintos que pueden ser maliciosos antes de que pueda establecer una conexión con la red interna de la organización o endpoints Contención de primera línea de defensa sin importar donde estén los usuarios ya que permite tener visibilidad de lo que ocurre en internet
ARCHERY a security tool	Herramienta de descubrimiento de vulnerabilidades, que permite la administración de muchas de las herramientas DAST más potentes para la detección y contención de las vulnerabilidades. Gestión de vulnerabilidades La evaluación y gestión de las vulnerabilidades de código abierto ayuda a los desarrolladores y pentesters a realizar análisis y gestionar las vulnerabilidades. Panel de múltiples escáneres Gestione la vulnerabilidad desde varios escáneres Escaneo de red

	Todos los datos de los resultados de los análisis de red se visualizan en un panel que le ayuda en la evaluación de riesgos de la red. Administra todos los análisis de forma dinámica y detecta riesgos en las aplicaciones.
Otras Herramientas	Qradar/SIEM: Servicio de monitoreo y gestión de alertas mediante la integración de dispositivos y configuración de casos de uso o políticas. IBM Security SOAR: Sistema que esta diseñado para ayudar a equipos de respuesta a incidentes (o red team) frente a las amenazas cibernéticas. OSSEC: Sistema que permite detección y de la misma forma ayuda a contener riesgos ya que integra análisis de registros, integridad de los archivos, análisis de registros Windows, puede centralizar las políticas de la organización se usa para la detección de rootkits, gestión de alertas en tiempo real y respuesta activa. Multiplataforma para sistemas operativos. Cortafuegos de Perímetro Suites de Antivirus

Fuente: Elaboración propia

7. CONCLUSIONES

En el ámbito de la seguridad informática comprendo que se hace necesario el conocimiento de muchas variables que llevan a que la creación de equipos estratégicos como los de BlueTem y RedTeam tengan éxito en las organizaciones ya que se deben conocer y entender aspectos Éticos, Legales y tecnológicos como el uso de herramientas de penetración y herramientas de contención como medidas ante los incidentes de seguridad que se presenten en las empresas.

Como participante de equipos estratégicos es importante conocer las leyes que promulga el estado en busca de la judicialización de conductas en contra de la seguridad de la información entre las más importantes que se deben manejar encontramos la ley 1273 de 2009 que indica la sanción sobre “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”.

Se realiza una comprensión de las 4 etapas que se deben usar en las pruebas de pentesting para determinar si un sistema posee o no vulnerabilidades expuestas, en el caso de los bancos de trabajos usados sobre la empresa The WhiteHose Security, se evidenciaron varias que comprometían su seguridad por diversas causas como sus sistemas operativos, actualizaciones y el uso de programas software con fallas de seguridad en su desarrollo.

Según evidencia no solo se debería hacer uso de las etapas de pentesting como método de análisis y pruebas de penetración para llevar a cabo una mejor labor de estas etapas se hace necesario el uso de una metodología para pruebas de intrusión que permita a los equipos RedTeam Y BlueTeam la incorporación de una hoja o ruta con ideas practicas probadas para la evaluación ya sea de las redes, aplicaciones o sistemas, estas metodologías ayudarían a los equipos en la forma de hacer la interpretación y gestionar e manea correcta las pruebas que se van realizando.

El uso de herramientas para pruebas de penetración son vital importancia para ambos equipos estratégicos ya que proporcionan el estado de seguridad de los objetivos en las pruebas y en los métodos de contención de la seguridad, es por ellos que se debe estar en constante análisis de estas, versionamientos, funcionamiento y actualizaciones para poder de forma eficaz y eficiente hacer uso de ellas en los equipos.

Puedo determinar que el uso de controles de buenas prácticas junto con herramientas de contención robustas como SIEM crea un ambiente de mayor

protección en cualquier ámbito de seguridad de las empresas que se estén protegiendo de ataques cibernéticos, es el caso y ejemplo del uso de Controles como CIS Control y CIS Beckmark

Resaltó la importancia de articular en las organizaciones el uso de grupos como CSIRT y SOC dentro de las políticas de seguridad de las organizaciones que permitan canalizar la respuesta a incidentes de una forma más acertada de una forma colaborativa que permite una reacción inmediata a los incidentes de seguridad que puedan ocurrir dentro de una empresa. Con estos centros de respuesta podemos lograr la relación de centros nacionales, internacionales e internas de la empresa y el nivel de escalamiento de cada evento que se presente de acuerdo a los procedimientos que se establezcan.

Como conclusión final resaltaría al intensión del diplomado para el entendimiento de distintas formas de protección que se pueden adoptar por distintas empresas en el ámbito tecnológico en la búsqueda de la acciones sobre las amenazas vulnerabilidades y riesgos que implica tener desprotegidos sistemas críticos que manejan datos e información como activo fundamental que da continuidad a los negocios.

8. RECOMENDACIONES

Como recomendación fundamental de seguridad informática se hace necesario la implementación de un SGSI que de soporte a todas las necesidades de la organización partiendo de las policitas hasta las metodologías específicas de contención que permitan el fortalecimiento de la seguridad de las organizaciones.

Para el fortalecimiento de los equipos BlueTeam Y Redteam se hace necesario el uso de metodologías de pruebas de penetración y el estudio actualizado de herramientas para pruebas de pentesting, herramientas de contención y herramientas de detección como mecanismo y estrategia de conocimiento tecnológico que estos equipos deben tener.

Se deben hacer uso de bases como CVE que sirvan como fuente de información y conocimiento de vulnerabilidades de amenazas expuestas que permitan como profesionales en equipos estratégicos dar soluciones a problemas ya documentados y que provisionen la respuesta oportuna ante un incidente de seguridad que se pueda presentar.

Se deben considerar siempre y en la medida de las posibilidades de las empresas la implementación de un SGSI es de vital importancia para las empresas que permiten la gestión de seguridad en todos sus dominios organizacionales como lo son la seguridad organizativa, la seguridad lógica, la seguridad física y la seguridad legal.

Es recomendable adoptar el uso de grupos y equipos de respuesta a incidentes como CSIRT que logren ofrecer más servicios de seguridad a las empresas y equipos estratégicos ya sea como soporte de tipo reactivo o preventivo.

Siempre se deben revisar los contratos de confidencialidad, clausulas y los alcances que son determinantes en un proceso de pentesting para evitar problemas de tipo legal con las organizaciones.

ANEXOS

ANEXO 1. VÍDEO DE SUSTENTACIÓN DEL INFORME TÉCNICO
https://youtu.be/Ngk1_Grxb74

BIBLIOGRAFÍA

NIST, Technical Guide to Information Security Testing and Assessment, [En línea]. (Consultado el 30 Agosto de 2021.), Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

GREENBONE, User Manual Greenbone Security Manager [En línea]. (Consultado el 30 Agosto de 2021.), Disponible en: https://docs.greenbone.net/GSM-Manual/gos-21.04/en/GSM-Manual-GOS-21.04-en.pdf

METASPLOIT, The world's most used penetration testing framework [En línea]. (Consultado el 30 Agosto de 2021.),https://www.metasploit.com/

REDHAT, El concepto de CVE, [En línea]. (Consultado el 30 Agosto de 2021.),https://www.redhat.com/es/topics/security/what-is-cve

EXPLOIT DATABASE, Exploits for Penetration Testers, Researchers, and Ethical Hackers (exploit-db.com) (Consultado el 30 Agosto de 2021.) https://www.exploit-db.com/

Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades, 3 Ciencias, [En línea]. (Revisado 10 Junio 2021.), https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

Norma Técnica Colombiana NTC-ISO-IEC 27001, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI) Requisitos, [En línea]. (Revisado 10 de Junio 2021.), http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

COPNIA, Código de Ética 2015, [En línea]. (Consultado el 7 de Septiembre de 2021.), Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

OAS, OEA, Portal Interamericano de Delitos Cibernéticos, Ley Nro. 1273 del 2009 - De la Protección de la Información y de los Datos [En línea]. (Consultado el 7 de Septiembre de 2021.), Disponible en: http://www.oas.org/es/sla/dlc/cyber-es/paises-pais.asp?c=Colombia

ENTER, Detrás de Buggly: la historia de la fachada Andrómeda, [En línea]. (Consultado el 7 de Septiembre de 2021.), Disponible en: https://www.enter.co/empresas/colombia-digital/detras-de-buggly-la-historia-de-la-fachada-andromeda/

EL TIEMPO, Informe militar sobre el caso Andrómeda, [En línea]. (Consultado el 7 de Septiembre de 2021.), Disponible en: https://www.eltiempo.com/archivo/documento/CMS-15141236is

RCN RADIO, Ejército insiste que operación de Andrómeda fue legal, pero releva del cargo a seis funcionarios, [En línea]. (Consultado el 7 de Septiembre de 2021.), Disponible en: https://www.rcnradio.com/colombia/ejercito-insiste-en-que-operacion-andromeda-es-legal-pero-pidio-relevar-de-sus-cargos-6-de

TRIARIUS, Observatorio Internacional sobre el terrorismo y las nuevas amenazas, [En línea]. (Consultado el 7 de Septiembre de 2021.), Disponible en: https://www.fuerzasmilitares.org/triarius/TRIARIUS-Especial-21.pdf

NIST, NVD - CVE-2020-13432, [En línea]. (Consultado el 20 de Septiembre de 2021.), Disponible en: p_lt_WebPartZone1_zoneCenter_pageplaceholder_p_lt_WebPartZone1_zoneCenter_VulnerabilityDetail_VulnFormView_VulnConfigurationsDiv

NMAP the Network Mapper – Free Security Scanner, [En línea]. (Consultado el 20 de Septiembre de 2021.), Disponible en: https://nmap.org/

OpenVAS - Open Vulnerability Assessment Scanner, [En línea]. (Consultado el 20 de Septiembre de 2021.), Disponible en: https://www.openvas.org/

MS11-030: Una vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código: 12 de abril, 2011 (microsoft.com), [En línea]. (Consultado el 20 de Septiembre de 2021.), Disponible en: https://support.microsoft.com/es-es/topic/ms11-030-una-vulnerabilidad-en-la-resoluci%C3%B3n-dns-podr%C3%ADa-permitir-la-ejecuci%C3%B3n-remota-de-c%C3%B3digo-12-de-abril-2011-98cdc5e4-af92-597a-0a0b-49406f3c4134

KASPERSKY THREATS - Intrusion.Win.MS17-010, [En línea]. (Consultado el 20 de Septiembre de 2021.), Disponible en: https://threats.kaspersky.com/mx/threat/Intrusion.Win.MS17-010.*/

CARNEGIE MELLON UNIVERSITY, Software Engineering Institute, Rejetto HTTP File Server (HFS) search feature fails to handle null bytes, [En línea]. (Consultado el 20 de Septiembre de 2021.), Disponible en: https://www.kb.cert.org/vuls/id/251276

EXPLOIT DATABASE, Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution, [En línea]. (Consultado el 20 de Septiembre de 2021.), Disponible en: https://www.exploit-db.com/exploits/39161

ESCUELA POLITECNICA NACIONAL, MS17-010 EternalBlue SMB Remote Windows, En línea]. (Consultado el 20 de Septiembre de 2021.), Disponible en: https://www.csirt-epn.edu.ec/servicios/vulnerabilidades/58-ms17-010

AVAST, Actualizar Windows para prevenir EternalBlue y DoublePulsar, En línea]. (Consultado el 20 de Septiembre de 2021.), Disponible en: https://support.avast.com/es-co/article/EternalBlue-vulnerability/

INCIBE, Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía, [En línea]. (Consultado el 30 de Septiembre de 2021.), Disponible en: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe-cert_gestion_ciberincidentes_sector_privado.pdf

CSO, Red team versus blue team: How to run an effective simulation, [En línea]. (Consultado el 30 de Septiembre de 2021.), Disponible en: https://www.csoonline.com/article/2122440/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html

Security Art Work, Sandbox evasión: Identificando Blue Teams, [En línea]. (Consultado el 30 de Septiembre de 2021.), Disponible en: https://www.securityartwork.es/2020/10/12/sandbox-evasion-identificando-blue-teams/

CSIRT, Equipo a respuesta de incidentes de seguridad, [En línea]. (Consultado el 30 de Septiembre de 2021.), Disponible en: https://www.csirt.gob.cl/quienes-somos/

UNAM, Universidad Autónoma de México, CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS… ¿PARA QUÉ?, Revista Seguridad, [En línea]. (Consultado el 30 de Septiembre de 2021.), Disponible en: https://revista.seguridad.unam.mx/numero-16/centro-de-respuesta-incidentes-inform%C3%A1ticos-para-qu%C3%A9

INCIBE-CERT, Despliegue de SIEM en entornos TO, En línea]. (Consultado el 30 de Septiembre de 2021.), Disponible en: https://www.incibe-cert.es/blog/despliegue-siem-entornos

SIEM, Gestión de LOGS de eventos de seguridad (SIEM), En línea]. (Consultado el 30 de Septiembre de 2021.), Disponible en: https://ricardo-sb.blogspot.com/2017/04/gestion-de-logs-de-eventos-de-seguridad.html

NIST, NVD - CVE-2020-13432, [En línea]. (Consultado el 30 de Septiembre de 2021.), Disponible en: p_lt_WebPartZone1_zoneCenter_pageplaceholder_p_lt_WebPartZone1_zoneCenter_VulnerabilityDetail_VulnFormView_VulnConfigurationsDiv

ARCHERYSEC, APPLICATION SECURITY POSTURE MANAGEMENT TOOL, [En línea]. (Consultado el 30 de Septiembre de 2021.), Disponible en: https://www.archerysec.com/