Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team

Edwin Andrés Jimenez García

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

Dedico este proyecto a mi abuela que me acompaña desde el cielo, por ser un gran ejemplo de vida y aunque entendía muy poco de mi profesión, formo parte fundamental de mis pilares como persona que aplico en cada aspecto de mi vida.

Resumen

La transformación digital de las empresas, presenta diferentes retos a nivel de tecnología y ciberseguridad, por lo cual surge la necesidad de robustecer su nivel de madurez para poder prepararse frente a los ataques que cada día son más sofisticados, volviendo prioritario aumentar las capacidades técnicas de los equipos de ciberseguridad, basados en los ejercicios de Red Team para aumentar la proteger de las brechas de seguridad junto con la respuesta ante eventos o incidentes de ciberseguridad, Blue Team para endurecer la defensa y aplicar diferentes tácticas que puedan desviar la atención el atacante para proteger los activos de la información.

Palabras clave: Blue Team, capacidades, ciberseguridad, Red Team, visibilidad

Abstract

The digital transformation of companies presents different challenges at the level of technology and cybersecurity, which creates the need to strengthen their level of maturity in order to prepare for attacks that are increasingly sophisticated. This makes it a priority to enhance the technical capabilities of cybersecurity teams, based on Red Team exercises to improve protection against security breaches, along with response to cybersecurity events or incidents, and Blue Team strategies to harden defense and apply different tactics that can divert the attacker's attention to protect information assets.

Keywords: Blue Team, capabilities, cybersecurity, Red Team, visibility

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

Es el equipo de seguridad defensiva (escudo), encargados de fortalecer los sistemas, redes e infraestructura de la organización contra diferentes vectores de ataque que pueden comprometer la seguridad de la información.

Ciberataque:

Es un ataque intencionado por parte de un tercero para generar acceso no autorizado a un sistema de información con fines ilícitos.

Cracker:

Es un experto que se caracteriza por romper o vulnerar sistemas de seguridad, actuando para beneficio propio de forma ilícita.

CVE:

Vulnerabilidades y exposiciones comunes, es un identificador único y estandarizado para vulnerabilidades de seguridad conocidas, lo cual nos ayuda a aislar la falla especifica acorde al software o hardware identificado en la misma.

Defensa en profundidad:

Es un modelo de ciberseguridad caracterizado por utilizar múltiples capas de controles y herramientas de seguridad, bajo el principio básico de tener diferentes controles en cada una de las capas para asegurar la infraestructura de la organización.

Equipo pivote:

Es un equipo dentro de la red sobre el cual se obtiene acceso inicial y es utilizado como plataforma para moverse a través de la red.

Escalar privilegios:

Es una técnica utilizada para que un usuario obtenga privilegios en un sistema, para poder ejecutar acciones sin ninguna restricción.

Explotación (Exploit):

Programa diseñado para aprovechar una vulnerabilidad en un sistema de información, para ejecutar acciones no autorizadas.

ExploitDB:

Es repositorio web donde se almacena una lista de exploits gratuitos para realizar laboratorio o pruebas de vulnerabilidades.

Hacker:

Es un experto con diferentes capacidades a nivel informático que le permite encontrar vulnerabilidades en diferentes sistemas de información.

Matasploit:

Es una herramienta open source, diseñada para para el desarrollo y ejecución de exploit, la cual tiene una gran comunidad que alimenta continuamente la base de datos lo cual sirve dentro de la ejecución de prueba de seguridad.

Movimiento lateral:

Es una técnica utilizada para moverse a través de una red comprometida y acceder a diferentes equipos dentro de un sistema.

Nmap:

Es una herramienta Open Source utilizada para el escaneo, explotación y gestión de redes, es muy utilizada en las fases de descubrimiento en pruebas de seguridad.

Open Source:

Es un software que está disponible públicamente, lo cual permite su uso de forma abierta.

OpenVas:

Herramienta open source conocida también como Greenbone, es un sistema de automatización para la identificación de vulnerabilidades mediante el escaneo de la red, basado en los repositorios internos de vulnerabilidades identificadas dependiendo el sistema auditado.

Red Team:

Es el equipo de seguridad ofensiva (espada), encargados de verificar la seguridad de los sistemas, mediante ejercicios controlados que simulan ciberataques para evaluar el correcto funcionamiento de la seguridad de la organización.

Vulnerabilidad:

Es una debilidad en un sistema que puede estar a nivel físico o lógico y que puede ser explotada para obtener acceso no autorizado al sistema, información o frenar su producción.

Introducción

El mundo actual ha sufrido grandes transformaciones y una de las más importantes es la digital, la cual, fue impulsada de forma positiva por el paradigma de la pandemia mundial que cambio los modelos convencionales de trabajo presencial, adoptando modelos de trabajo hibrido y teletrabajo, las organizaciones transformaron su forma de trabajar, aumentando la cantidad de gestión realizada de forma presencial y migrando varios procesos fundamentales a infraestructura a servicios en la nube, por lo que, se han generado brechas de seguridad que no estaban contempladas bajo los esquemas de ciberseguridad para muchas áreas de tecnología con arquitecturas en las instalaciones. Dentro de la problemática que presenta la ciberseguridad en una organización, los integrantes del área de tecnología han mejorado sus capacidades para adaptarse a los cambios planteados y proteger sus activos de información. Trabajando de forma conjunta con grupos dedicados a la ciberseguridad desde el punto de vista del ataque en pruebas de penetración dirigida por los Red Team y desde la posición de endurecimiento de defensa con el Blue Team, en cada una de estas pruebas es necesario pensar fuera de los esquemas actuales y posicionarnos tanto en la defensa como en el ataque para robustecer nuestro perfil profesional.

Justificación

Dentro de una organización sin importar el tamaño o razón social presentan diferentes necesidades en temas de ciberseguridad para resguardar sus activos de información y garantizar la continuidad del negocio, es así como, el área de tecnología basa sus esfuerzos en auditorias de seguridad enfocadas en el descubrimiento de vulnerabilidades y endurecimiento de las salvaguardas o controles aplicados para su seguridad. Dentro de las pruebas planteadas se utilizan diferentes auditorias de seguridad perimetral, interna y test de intrusión, con las cuales la organización podrá evaluar, crear y ajustar sus políticas de seguridad informática. Como paso inicial se plantea ejecutar una prueba de pentesting para identificar las posibles vulnerabilidades que serán utilizadas como el insumo inicial para validar el cumplimiento de las medidas de seguridad implementadas en la organización. La ejecución de esta prueba permite a la organización identificar y generar un plan de trabajo que busca mitigar las vulnerabilidades presentes en sus sistemas. Para cerrar los posibles vectores de ataque que puede ser aprovechado por un cracker para afectar la organización.

Aunque los hackers existen desde la década de los sesenta, su cultura fue creciendo desde la creación de ARPANET como la primera red intercontinental de alta velocidad y la creciente popularidad del ordenador personal en los setenta, esto, por otra parte, fue aumentando los grupos dedicados a explotar en sus inicios las vulnerabilidades presentadas en los sistemas interconectados. Mencionada evolución, ha permitido robustecer las leyes, desde el primer arresto realizado por abuso informático en 1984, pasando por la implementación de la primera ley de fraude y abusos informático, hasta la creación de compañías dedicadas a los sistemas de seguridad informática.

Es así como, en 1995 – Dan Farmer y Wietse Venema presentan SATAN, un escáner automático de vulnerabilidades, que se convierte en una popular herramienta de hacking.[1]

El desarrollo de SATAN fue el inicio del aumento exponencial de ciberdelitos que para el año 2020 su valor podría estar cerca de un billón de dólares.

Los incidentes de delitos cibernéticos alrededor del mundo presentaron un valor arriba de un trillón de dólares en 2020. [2]

En los diferentes escenarios y eventos donde una de las grandes constantes es la capacidad de los delincuentes para adaptarse al cambio, innovar sus modos de ataque y dedicación para obtener sus objetivos manteniendo la eficacia en sus actividades. El comienzo de la pandemia como la tormenta perfecta no solo presento retos en la compañía enfocados a la trasformación digital para continuar con sus actividades, impulso la búsqueda de alternativas para el trabajo sincrónico y la mejora de controles para mitigar los vectores de ataque que no fueron contemplados en un inicio al tener sus empleados en modalidad de teletrabajo.

Es importante realizar pruebas de penetración a las infraestructuras actualmente para conocer las brechas de seguridad que se encuentran vigentes en la infraestructura y no tener una falsa sensación se seguridad lo cual puede ser peligroso frente a la incursión de un ciberdelincuente en la infraestructura de la empresa, gracias a la realización de prueba, identificación y mitigación oportuna de las vulnerabilidades, manteniendo una infraestructura segura que salvaguarde loa activos de información y no generar incumplimientos de la normativa nacional que pueden acarrear medidas legales y sanciones.

[1] Kaspersky Labs. (2021, enero), una breve historia sobre el hackeo
[2] McAfee (2021, Enero) Cybercrime could cost the world almost $1 trillion in 2020

Objetivos

Objetivo General

Aplicar las habilidades adquiridas como especialista en ciberseguridad para desarrollar los escenarios prácticos de estrategia de los equipos Red Team y Blue Team.

Objetivos Específicos

Identificar las implicaciones éticas y legales sobre el uso inadecuado del conocimiento adquirido en el escenario profesional.

Aplicar marco de referencia de la legislación Colombia actual al escenario propuesto sobre delitos informáticos.

Implementar herramientas de software libre para realizar pentesting alineados a los escenarios plateados durante el seminario.

Implementar un plan de atención de incidentes de un ataque activo, para detener el avance del hacker dentro de la red.

DESARROLLO DEL INFORME, INTEGRANDO

Situación problema: Marco legal delitos informáticos Colombia

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

Ley 1273 de 2009

Dentro del marco legislativo nacional Colombiano, se tiene la ley 1273 de 2009, donde se redactan diferentes artículos orientados a la protección de la información y de los datos, abordando diferentes sanciones aplicadas dependiendo de la naturaleza del delito como son topes de multas en salarios mínimos y tiempo de prisión aplicable.[3]

A continuación, se adjunta una tabla de apoyo con los artículos, estipulados en la 1273 con las definiciones establecidas.

Tabla 1

Artículos Ley 1273 de 2009

Articulo	Delito informático	Descripción
269ª	Acceso abusivo a un sistema informático	El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho

[3] (CONGRESO DE LA REPÚBLICA, 2009 Ley 1273 de 2009)

		(48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
269B	Obstaculización ilegítima de sistema informático o red de telecomunicación	El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.
269C	Interceptación de datos informáticos	El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
269D	Daño Informático	El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

269E	Uso de software malicioso	El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes
269F	Violación de datos personales	El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
269G	Suplantación de sitios web	para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

269H	Circunstancias de agravación punitiva	Las penas imponibles de acuerdo con los artículos descritos en este título se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

269I	Hurto por medios informáticos y semejantes	El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.
269J	Transferencia no consentida de activos	El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Nota. La tabla es adaptación de los artículos de la ley 1273 de 2009 del Congreso de la república

Ley 1581 de 2012

Es la ley que establece los parámetros generales de la protección de datos personales, como derecho constitucional en Colombia es necesario proteger los datos sensibles de las personas cuando son ingresados a una base de datos privada o pública.[4]

En la cual se aplicarán los siguientes principios básicos:

Legalidad: Acorde a lo estipulado en la ley es de estricto cumplimiento bajo el territorio nacional de Colombia.

Finalidad: Se debe informar al titular de la información el fin sobre el cual se utilizarán los datos proporcionados y dar claridad frente a cualquier cambio posterior a la recepción de la información.

Libertad: El titular de la información debe expresar su consentimiento, expreso e informado y los datos no podrán ser obtenidos o divulgados sin una autorización previa o que por proceso de terceros se genere una orden o mandato judicial.

Veracidad o calidad: La información suministrada al titular no puede ser parcial o incompleta, ya que debe tener pleno conocimiento sobre las acciones tomadas con la información y también debe ser clara.

Transparencia: En caso de ser requerido el titular de la información, tiene derecho a solicitar información de los datos contenidos y el uso de estos.

Acceso y circulación restringida: La utilización de los datos sólo podrá hacerse por personas autorizadas por el titular o por las personas previstas por la ley

[4] (CONGRESO DE LA REPÚBLICA, 2009 Ley 1581 de 2012)

Ley 1266 de 2008

El alcance de esta ley se limita al sector financiero, en la cual se establecen diferentes normas de cumplimiento por las entidades financieras, asegurados y del mercado de valores, donde regula el uso y la administración de las bases de datos, más conocida como Habeas Data busca proteger el buen nombre de las empresas y/o personas a nivel comercial y crediticio.[5]

Situación problema: Escenario base

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

Tipos de escenarios para pentesting

Caja blanca: Es la prueba de instrucción en el cual se conocen todas las características del sistema a auditar, como son aplicaciones, arquitectura, sistemas operativos y controles aplicados. Está catalogado como la prueba de pentesting más completa. Se recomienda ser desarrollada por un miembro del equipo de TI de la compañía.

Caja negra: Es la prueba de instrucción en la cual no se conoce ningún tipo de información del sistema, esta moldeada para ser una replicada de un ataque externo y se recomienda ser desarrollada por un tercero.

Caja gris: Es la prueba de instrucción en la cual se mezcla el escenario caja blanca y negra, ya que la persona que realiza la prueba tiene un objetivo definido por la organización, este

[5] (CONGRESO DE LA REPÚBLICA, 2008 Ley 1266 de 2008)

escenario recrea una prueba basada en la posibilidad que algún trabajador o antiguo colaborador compartiera información privilegiada con el atacante.

Caja roja: En este escenario la organización tiene constituido un equipo de red team el cual utiliza técnicas de seguridad ofensiva basadas en objetivos específicos, estos equipos manejan el escenario progresivo, actualizando sus técnicas de ataque y verificando brechas de seguridad relacionadas con vulnerabilidades no parchadas o de día cero.

Caja azul: En este escenario la organización tiene constituido un equipo de blue team, los cuales realizan procesos de defensa contra los ataques de red team, su seguridad avanzada gira en torno a los registros de seguridad, capturas de tráfico, caza de amenazas desplegadas en un centro de operaciones de seguridad.

Caja purpura: En este escenario se mezclan dentro de la organización la red team y el blue team, mediante el trabajo en equipo purpura, colaboradores de los diferentes grupos evalúan las capacidades de detección, respuesta a incidentes frente a amenazas se comparte documentación y recomendaciones que fortalecen la seguridad de la organización.

Fases para pentesting

Fase de reconocimiento: Acorde al escenario de pentesting a trabajar en el alcance de las pruebas y el conocimiento del entorno se definen los objetivos de la prueba, con lo cual esta etapa es fundamental para iniciar utilizando diferentes hermanastras de reconocimiento para escanear la red, levantar información de fuentes abiertas e identificar los dominios, direcciones IP, puertos y toda la información que genera valor de cara al inicio de escaneo de vulnerabilidades.[6]

[6] (Dragon Jar, Manual de la Metodología Abierta de Testeo de Seguridad)

Se recomienda utilizar un reconocimiento pasivo en producción con una intensidad baja para no generar alertas o saturación en la red.

Fase de escaneo de vulnerabilidades: Durante esta fase se utilizará el informe de reconocimiento y se implementaran nuevas herramientas para validar las posibles vulnerabilidades que pueden llegar a hacer mach con las tecnologías identificadas, puertos, equipos y configuraciones base. Las herramientas que se utilizan en esta fase son Nmap. Tenable (Nessus), OpenVas, Legion entre otras herramientas del mercado.

Acorde al inventario de software, puertos y direcciones IP encontrado se puede abordar cada posible vulnerabilidad dentro de los siguientes tipos:

Vulnerabilidades de diseño: Fallas en la arquitectura basa de software que le puede permitir al atacante generar un funcionamiento anómalo para su explotación

Software con versiones desactualizadas u obsoletas: Software con versiones desactualizadas, sin parches de seguridad u obsoletas con vulnerabilidades identificadas.

Fallas en autenticación: Procesos de autenticación débiles o con fallas que pueden ser aprovechadas para acceder al sistema.

Carga de archivos maliciosos: permite carga de archivos maliciosos sobre las aplicaciones para permitir acceso o funcionamiento anómalo.

Fase de explotación: Es la fase del reto, donde se busca explotar cada uno de los sistemas identificados, así poder catalogar las vulnerabilidades y su riesgo dentro de la compañía. Cuando la vulnerabilidad identificada es explotable y se evidencia su aplicabilidad se realiza un análisis basado en la criticidad del activo, la dificultas de explotación, la red sobre la cual está el activo y el impacto dentro de la organización.[7]

[7] ánchez-García, I.D., Feliu, T.S., Calvo-Manzano, J.A. 2022 Unraveling the establishment of residual risk in cybersecurity

Fase de reporte y mitigaciones: Una vez terminada la explotación es necesario generar un informe detallado técnico y un gerenciales los cuales deben los fallos de seguridad, su priorización, posibles mitigaciones y alternativas para mejorar la seguridad.

Las recomendaciones y los ajustes sugeridos deben ser claros, enfocándolos a las necesidades de cada compañía acorde a su arquitectura, tamaño y su capacidad financiera.

Montaje banco de trabajo

Software utilizado

VirtualBox: Es un software de virtualización gratuito, permite a los usuarios crear y ejecutar máquinas virtuales en su propio sistema operativo. Esto permite ejecutar múltiples sistemas operativos de forma simultánea en una sola máquina física y crear entornos aislados y seguros.

Figura 1

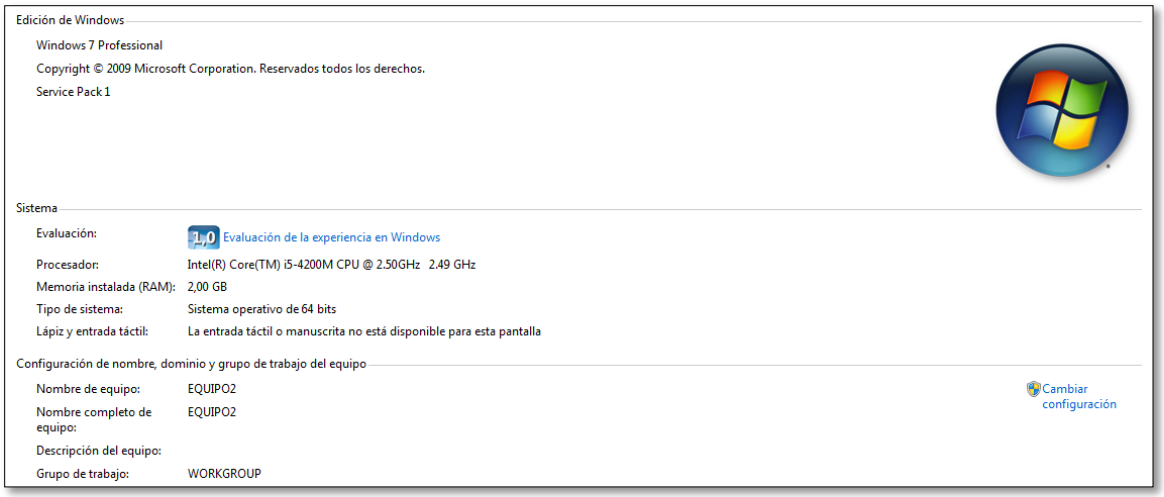
VirtualBox versión utilizada

Nota. Herramienta virtual box versión 7.1.4, utilizada para la virtualización del laboratorio.

Windows 7: Sistema operativo de Microsoft estrenado en el 2009 y finalizo soporte en 2020. Controla el hardware y el software de una computadora, considerado una versión muy estable y amigable con los usuarios finales.

Figura 2

Equipo Windows 7 utilizado

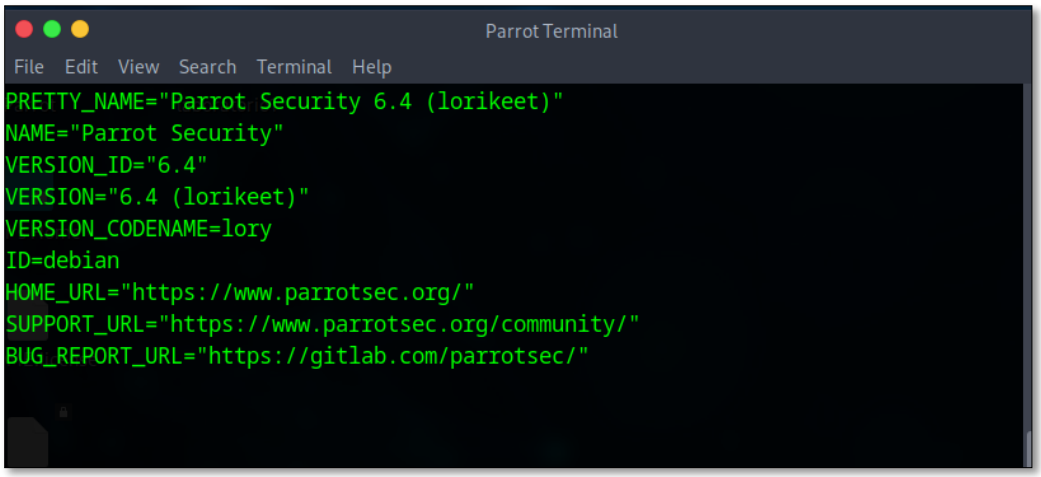


Nota. Sistema operativo Windows 7 profesional service pack 1

Parrot Linux: Con su base binaria basada en Debian, está diseñada para realizar pruebas de penetración, análisis forense, criptografía y navegación segura.

Figura 3

Parrot versión 6.4

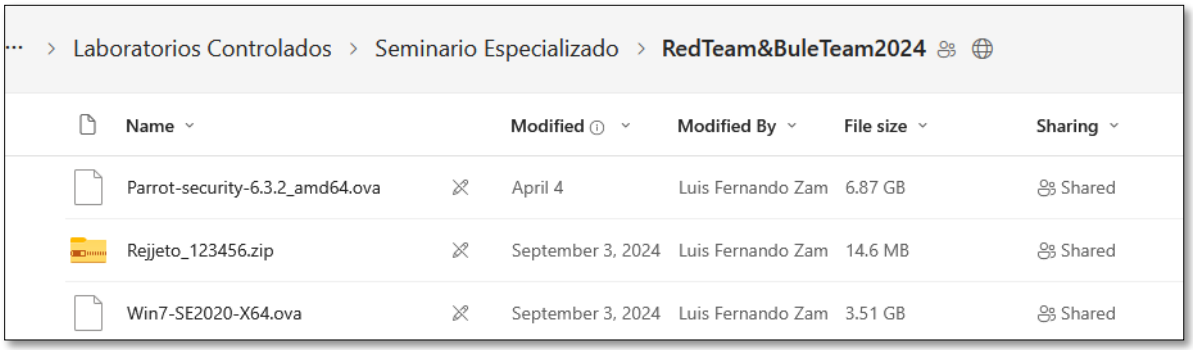


Nota. Sistema operativo Parrot security versión 6.4

Se utilizará las ovas compartidas para el desarrollo de la actividad, las cuales se descargan del SharePoint de la universidad.

Figura 4

Ovas Laboratorio UNAD

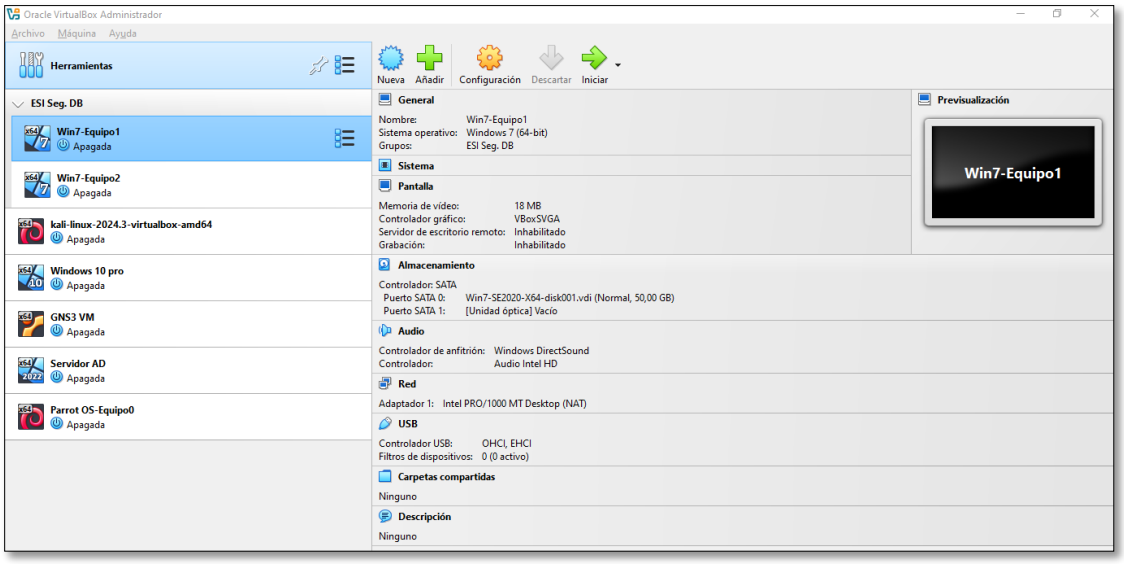


Nota. Repositorio en el cual se almaceno para compartir las máquinas virtuales en formato ova.

Se descargaron las imágenes del laboratorio y se importaron al virtualizador, tienen por nombre Win7-Equipo1, Win7-Equipo2, Parrot OS-Equipo0.

Figura 5

Entorno de máquinas virtuales utilizado

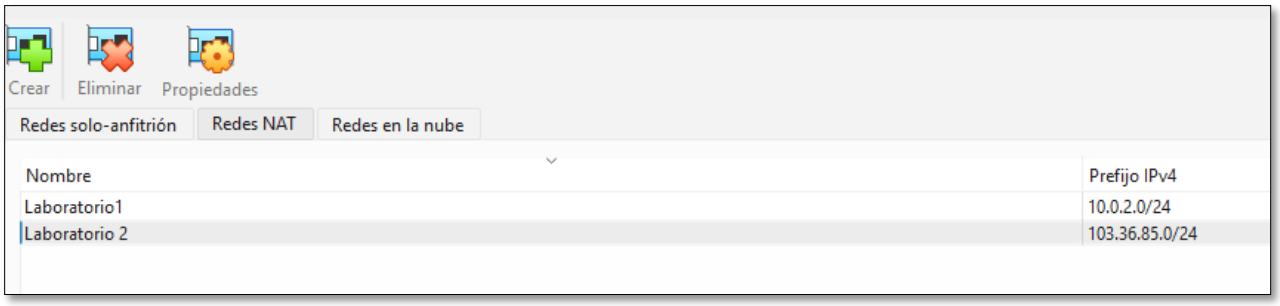


Nota. Herramienta virtualbox con las maquinas ya previamente virtualizas para iniciar el laboratorio.

Para la comunicación entre las redes utilizaremos dos Redes NAT del virtualizador para no consumir más recursos de los necesarios en el equipo del laboratorio, en los casos con un host para laboratorio más robusto sugiero utilizar GNS3 donde se puede ver la arquitectura generada y su interacción.

Figura 6

Redes NAT configuradas

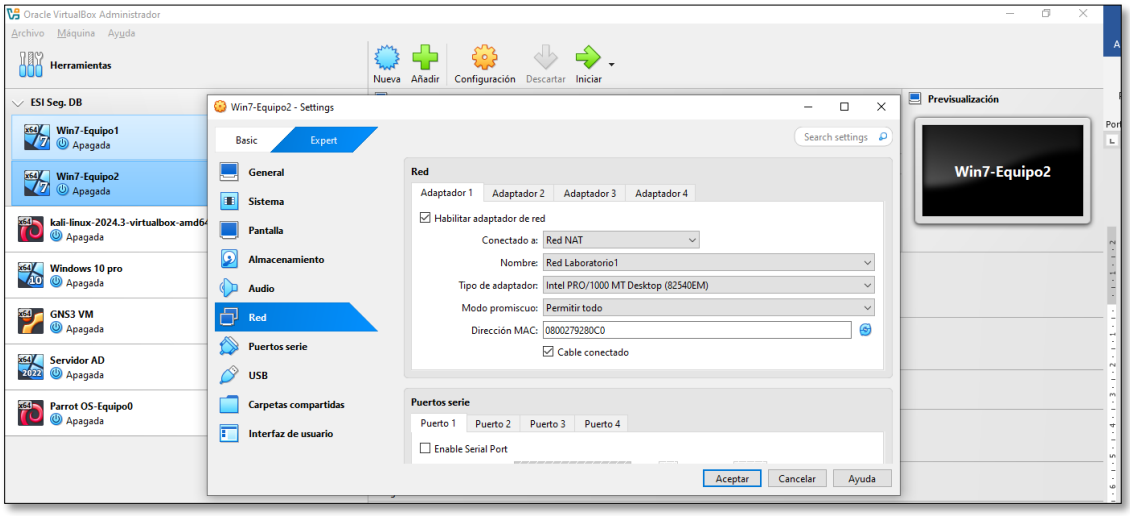


Nota. Redes virtualizadas configuradas en la herramienta VirtualBox en protocolo IPv4

Se configura en la tarjeta de red de los equipos Windows 7 la red NAT que tiene por nombre “Red Laboratorio1”

Figura 7

Configuración tarjeta de red equipo Win7

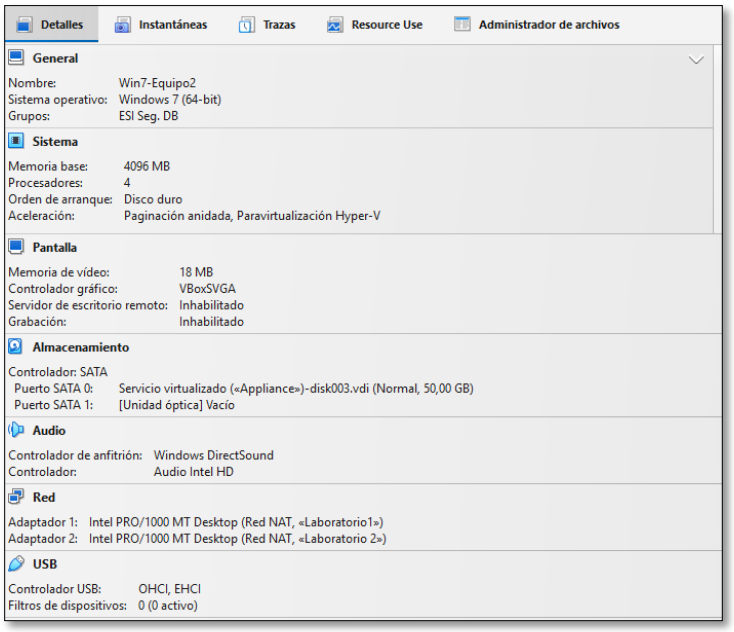


Nota. Configuración adaptador de red 1, con la red virtualizada 1

Para la segunda maquina se utilizará la red NAT del primero, pero adicional configuraremos una segunda con la red NAT “Laboratorio 2”

Figura 8

Segunda tarjeta de red como red NAT "Laboratorio 2"

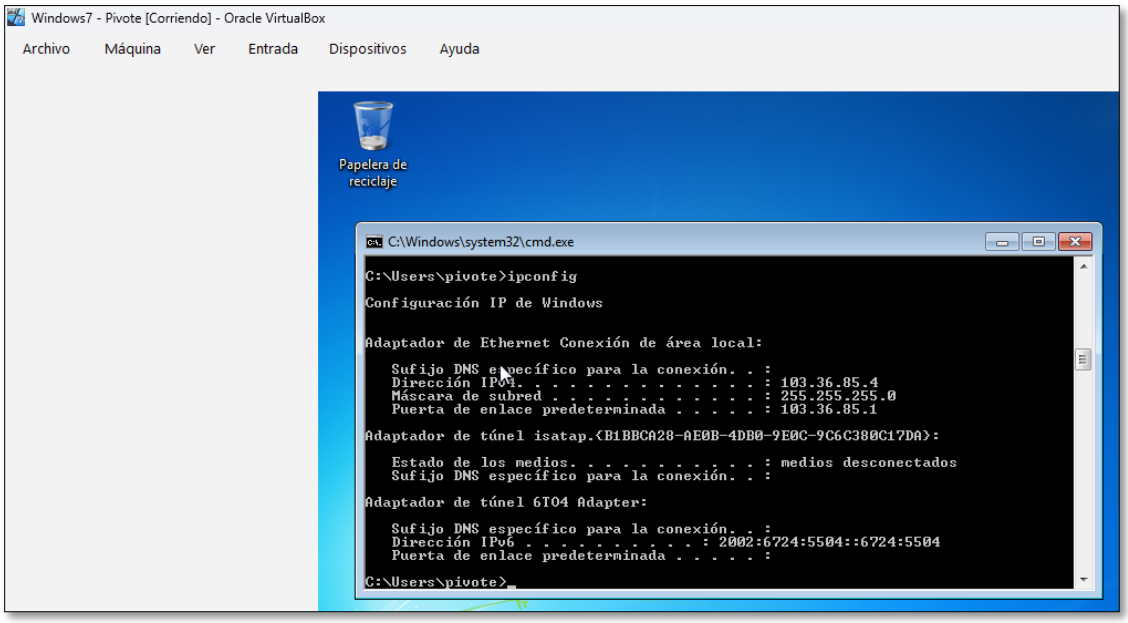


Nota. Configuración adaptador de red 2, con la red virtualizada 2

Se verifica la dirección IP asignada para el equipo1, el cual tiene solo una tarjeta de red y seria nuestro objetivo en el laboratorio. Dirección asignada 103.36.85.4

Figura 9

Verificación dirección IP Equipo1

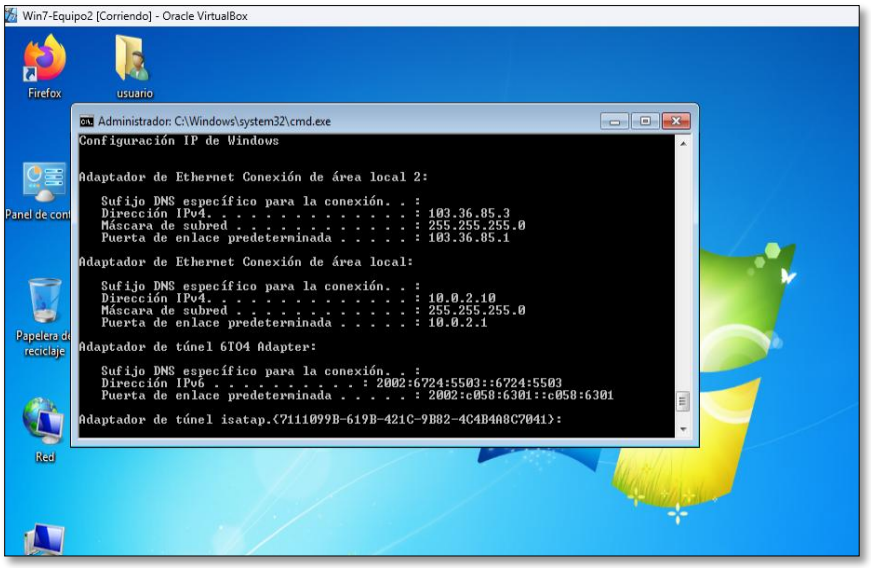


Nota. Verificación de direccionamiento registrado por la tarjeta de red.

Se verifica las direcciones IP asignadas para el equipo2, el cual tiene una tarjeta de red interna y otra para la red externa, ese será nuestro equipo pivote. Dirección asignada 10.0.2.10 y 103.36.85.3

Figura 10

Verificación dirección IP Equipo2

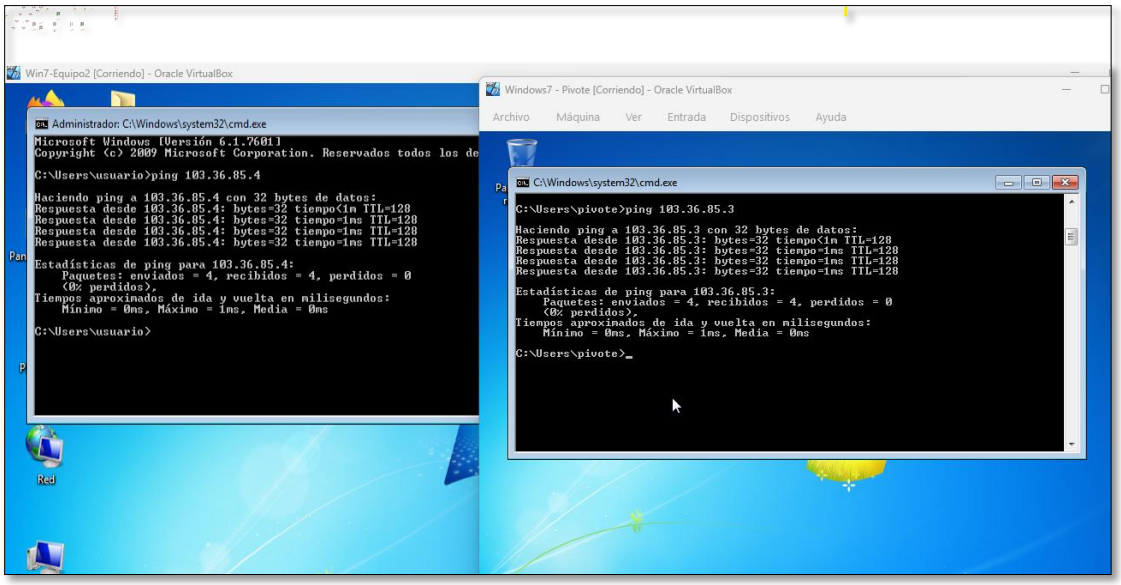


Nota. Verificación de direccionamiento registrado por la tarjeta de red.

Se valida conexión entre los dos equipos, tener presente que al ser la misma imagen se debe cambiar hostname y Mac de las tarjetas de red.

Figura 11

Prueba conectividad equipo 1 y 2

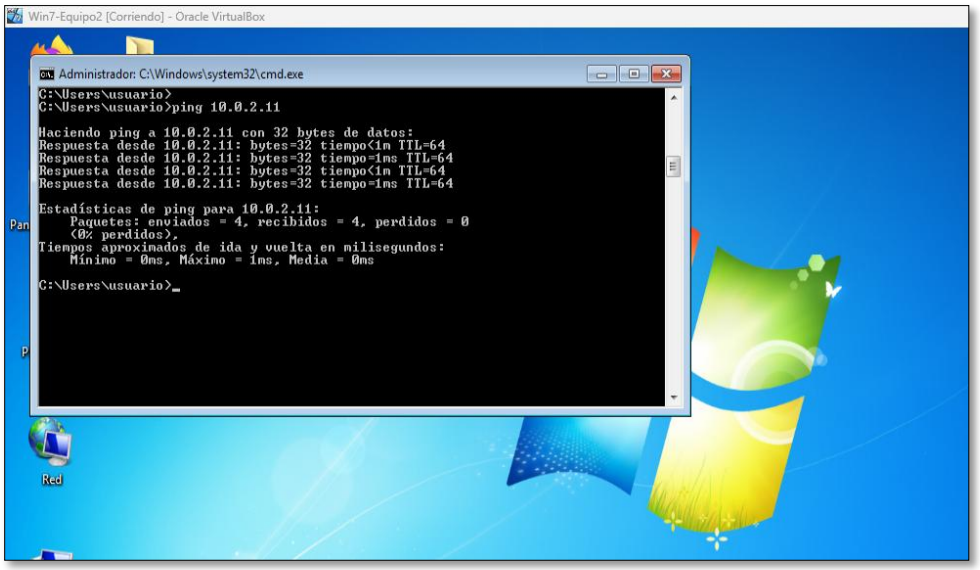


Nota. Prueba de conexión mediante herramienta ping entre la red 1

Se valida direccionamiento IP desde el equipo Parrot que sería el equipo atacante y también que alcance la dirección IP 10.0.2.10 del equipo objetivo.

Figura 12

Verificación IP equipo atacante

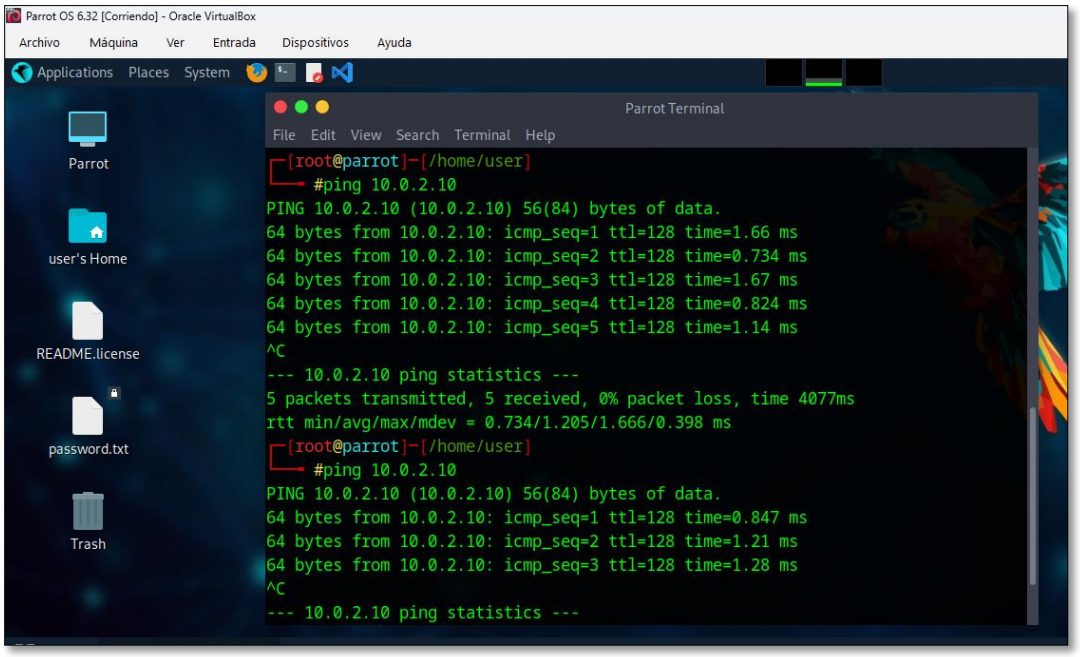


Nota. Prueba de conexión mediante herramienta ping entre la red 2

Verificación de conexión entre el equipo atacante y el equipo Pivote.

Figura 13

Conexión entre equipo atacante y Pívot



Nota. Prueba de conexión mediante herramienta ping entre la red 1 y la red 2

Situación problema: marco legal y ético

Dentro del escenario propuesto se evidencian varias irregularidades.

"Contrato y acuerdo de confidencialidad, genera riesgos de incluir cláusulas con procesos ilícitos o contrarios a la ética profesional"

Aunque puede ser un practica legal aceptada en Colombia diligenciar un NDA es necesario que tenga algunos ítems como son (Actividad especifica, periodo de duración, tipo de dato sensible), igualmente al ser un aspirante a un cargo no debería entregarse el contrato hasta que el proceso de selección finalice y se le otorgue la vacante.

Como profesionales en ciberseguridad debemos tener la capacidad de identificar procesos ilícitos o no éticos que afecten la prestación de un servicio o cumplimiento de un contrato, siendo personas éticas e integras prevaleciendo nuestro estatus como profesionales en Colombia.

Acuerdo de confidencialidad

Dentro del acuerdo de confidencialidad evidencie varias irregularidades.

"datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"

Para el caso específico de realizar interceptaciones ilegales de información o ingresar a sistemas sin autorización previa, se debe tener una orden judicial emitida por una autoridad legal competente Juez o tribunal, de lo contrario será un acto ilegal bajo la ley 1273 de 2009 – 269B acceso abusivo a un sistema informático y 269C interceptación de datos informáticos.

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

Igual que el punto anterior es nuestra obligación como profesionales denunciar cualquier delito del cual se tenga conocimiento como ejercicio de la profesión. Será un acto ilegal bajo la ley 1273 de 2009 – obstaculización ilegitima de sistema informático.

"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"

Como empleados o en este caso aspirante se puede responder o aceptar una culpa por una falla de conducta o procedimiento durante el desarrollo de una actividad, pero nunca se debería responder por el mal uso que genere un tercero fuera de nuestro alcance o función.

"Solución de controversias: Las partes se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de que la información ilegal o

confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs"

Bajo ninguna circunstancia de debe aceptar la culpa por actividades realizadas en misión de un cargo asignadas por la empresa contratante, debemos velar por que la documentación con la solicitud necesaria de acuerdos para pruebas esté en regla antes de iniciar alguna actividad.

Revisión propuesta laboral

En la revisión del escenario se identificó que el abogado que redacto el contrato fue despedido por la organización por posibles irregularidades en su gestión, lo cual puede llegar a ser causal de que el contrato sea viciado y generar la nulidad del mismo, por lo cual debe ser analizado por un profesional en esta rama.

Como profesional no optaría por un trabajo en una empresa con este tipo de antecedentes con un acuerdo de confidencialidad y un contrato que puede ser nocivo en mi carrera profesional

Ciberespionaje y ética en Securenova Labs

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Partiendo del principio de mínimo privilegio las empresas que prestan servicios como terceros en temas de auditoría, deben implementar medidas de seguridad solidad, desde el marco legal al funcional como son:

- Contrato de confidencialidad
- Cifrado de información (VPN, equipos, correo y herramientas ofimáticas)
- Alcance definido de auditoria (Activos alcanzados)
- Logs de seguridad, sobre acciones ejecutadas en los sistemas.
- Gobierno de gestión de accesos definido para cada rol.

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Se debe tener sistema de control de modificación potencialmente no deseada (PUM) con el cual se puede auditar el ingreso, registro de actividad y grabaciones a las máquinas que tienen instaladas las herramientas de análisis forense avanzado. Cuando las herramientas son externas a un sistema se debe manejar una cadena de custodia de información y del equipo entregado para realizar actividades específicas con un numero de caso actividad que demuestra la legitimidad de su uso.

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente?

Cuando una empresa realiza ciberespionaje se debe denunciar directamente ante los entes gubernamentales correspondientes, con lo cual se levantarán los cargos necesarios en función a los delitos cometidos durante el desarrollo de las actividades y se debe vetar a la empresa de participación en contratación pública.

Situación problema: Análisis red team escenario 2

SecureNova Labs detectó fugas de información desde una estación de trabajo Windows (Host-A). La imagen forense indica que la máquina ejecutaba una aplicación vulnerable probablemente explotada para obtener shell y escalar privilegios, además de evidencias de la creación no autorizada de un usuario con permisos administrativos. Los registros sugieren movimientos laterales desde Host-A hacia un servidor secundario (Host-B), como un servidor de archivos o base de datos, desde donde se habría obtenido información sensible. En este contexto,

la misión del equipo Red Team consiste en determinar el vector de fuga en Host-A, validar si la vulnerabilidad fue efectivamente explotada y si existió escalamiento de privilegios, reproducir en un laboratorio aislado el pivoting Host-A → Host-B y, como prueba de concepto controlada, crear en la imagen clonada de Host-B una cuenta administrativa con el formato "primerNombre+primerApellido" de carácter efímero y documentado, para finalmente entregar la evidencia técnica, un timeline forense completo y un plan de remediación integral.

Pentesting

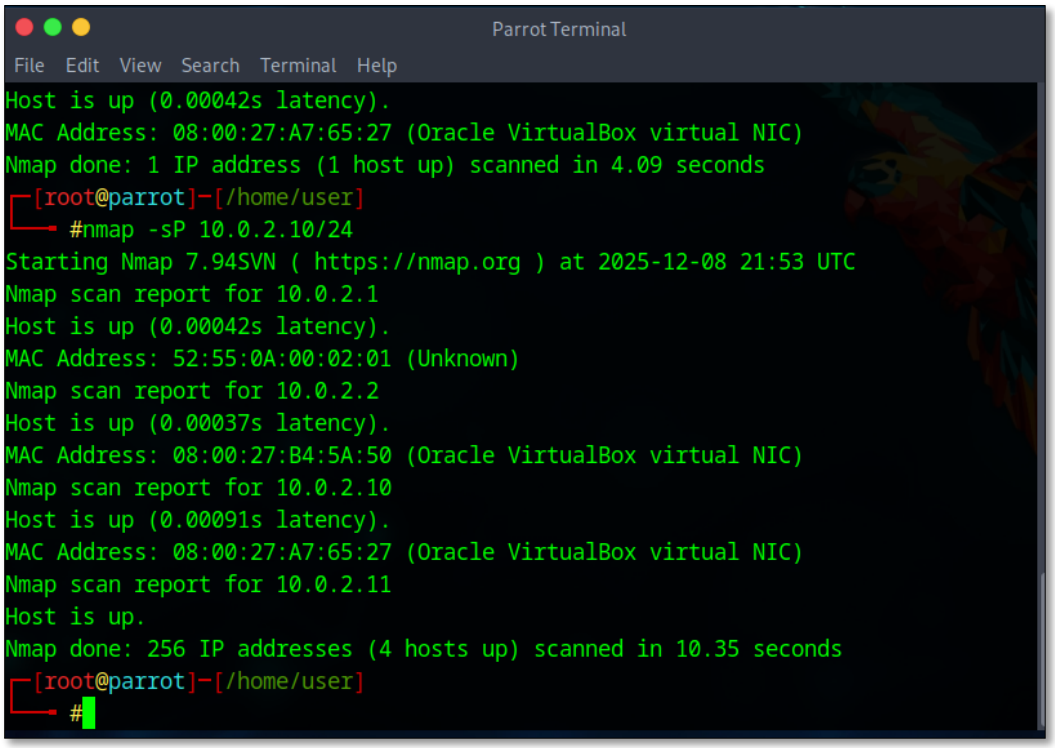
Reconocimiento

Es la primera fase del pentesting en la cual se verifica el entorno de la prueba, validando diferentes segmentos de red para encontrar el objetivo a analizar.

Dentro de las herramientas más populares y con una gran tasa de efectividad esta nmap. Dónde utilizaremos el siguiente comando para hacer descubrimiento "nmap -sP 10.0.2.10/24"

Figura 14

Descubrimiento de red local

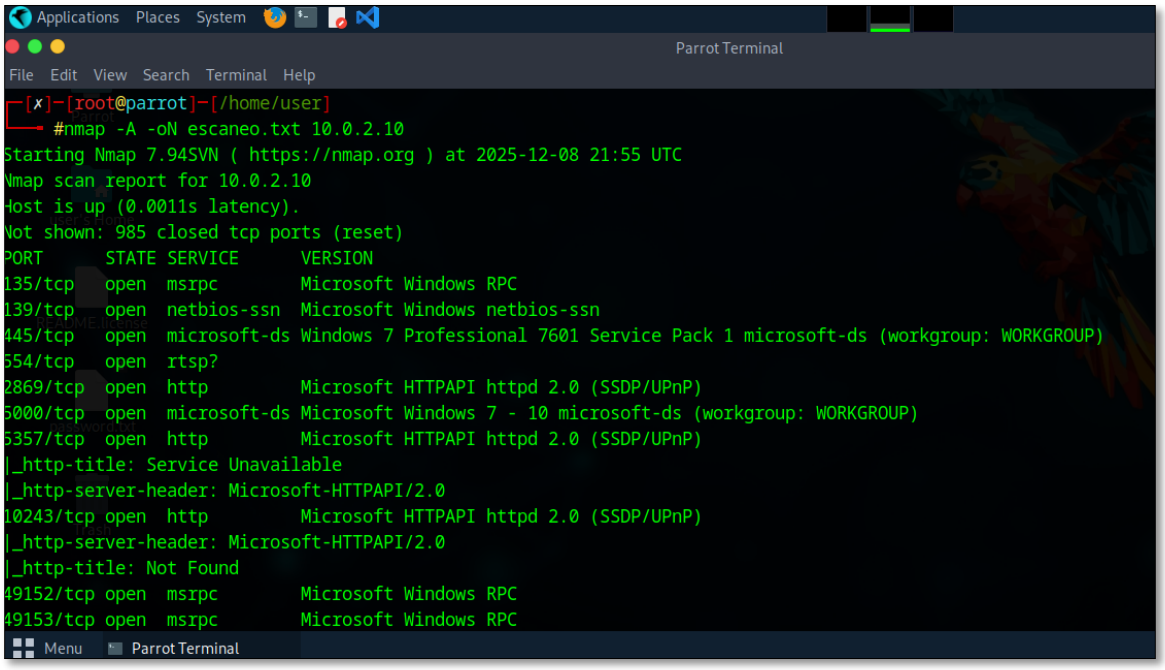


Nota. Herramienta nmap utilizada para el descubrimiento de red.

Mediante el reconocimiento se encontraron diferentes hosts conectados a la red, donde identificamos el 10.0.2.10 como el equipo con Windows 7 sobre el cual realizaremos la explotación.

Figura 15

Ejecución nmap



Nota. Resultado de la herramienta nmap utilizada durante el descubrimiento de red.

Realizamos un escaneo agresivo con Nmap y guardamos los datos en un archivo con nombre “escaneo.txt” utilizando el comando “nmap -A -oN escaneo.txt 10.0.2.10” el resultado completo se deja como evidencia en el Anexo1.

Tabla 2

Lista de puertos abiertos

PORT	STATE SERVICE	VERSION
135/tcp	open msrpc	Microsoft Windows RPC
139/tcp	open netbios-ssn	Windows netbios-ssn
	Microsoft	

445/tcp	open	microsoft-ds	Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
554/tcp	open	rtsp?	
2869/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Nota. Se recopila la información obtenida durante el escaneo de la herramienta nmap.

Escaneo de vulnerabilidades

En la segunda fase se inicia con los datos obtenidos durante el reconocimiento realizando investigación de posibles vulnerabilidades y validando el host objetivo los puertos encontrados.

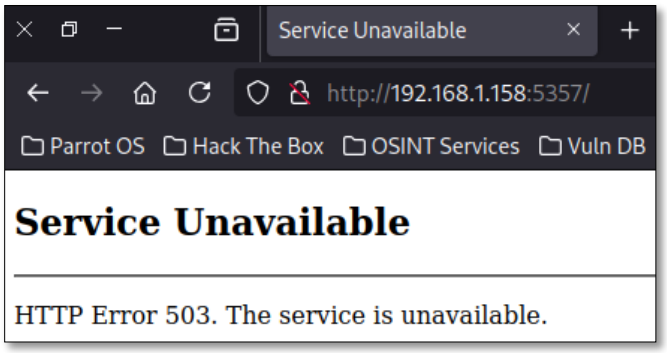
Durante esta fase revisamos los puertos que tienen protocolo http y su respuesta. A continuación, se encontraron los errores 503 y 404.

Error 503: El servidor no puede procesar la solicitud porque está temporalmente inaccesible, ya sea por mantenimiento, sobrecarga o un problema técnico

Error 404: la página web solicitada no fue encontrada por el servidor

Figura 16

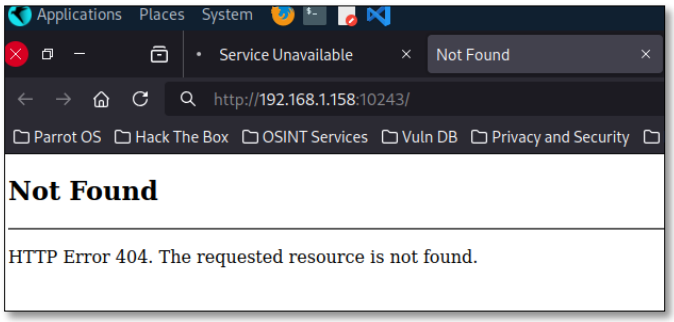
Error 503



Nota. Mensaje de error del servidor https

Figura 17

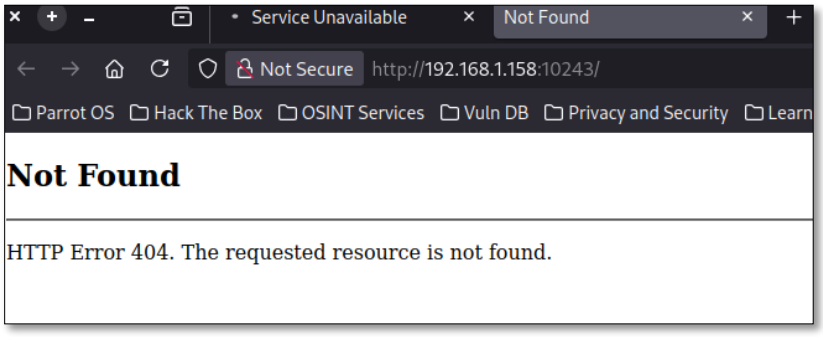
Error 404



Nota. Mensaje de error del servidor https

Figura 18

Error 404



Nota. Mensaje de error del servidor https

Tabla 3

Posibles vulnerabilidades x puerto

PORT	Posibles vulnerabilidades
135/tcp	Puerto de red 135 queda expuesto: ataques como WannaCry y Blaster Worm[8]
139/tcp	Puerto 139 está asociado con SMBv1, vulnerable a ataques como EternalBlue y WannaCry.
445/tcp	Puerto 445, es un protocolo de archivos de intercambio de Microsoft Windows vulnerable Wannacry. SambaCry
554/tcp	No tiene vulnerabilidades conocidas
2869/tcp	Ejecución remota de código ICS (CVE-2013-5065) permite ejecutar código en un sistema con solo enviar un paquete al puerto 2869, se puede tomar control total del sistema.[9]
5357/tcp	Vulnerabilidad de ejecución remota de código debido a la API de Servicios Web para Dispositivos (WSDAPI).[10]
10243/tcp	No es un Puerto estándar, asi que se debe validar que aplicación se está ejecutando en él.

Nota. Recopilación de la investigación realizada por los puertos y protocolos identificados.

Explotación vulnerabilidades

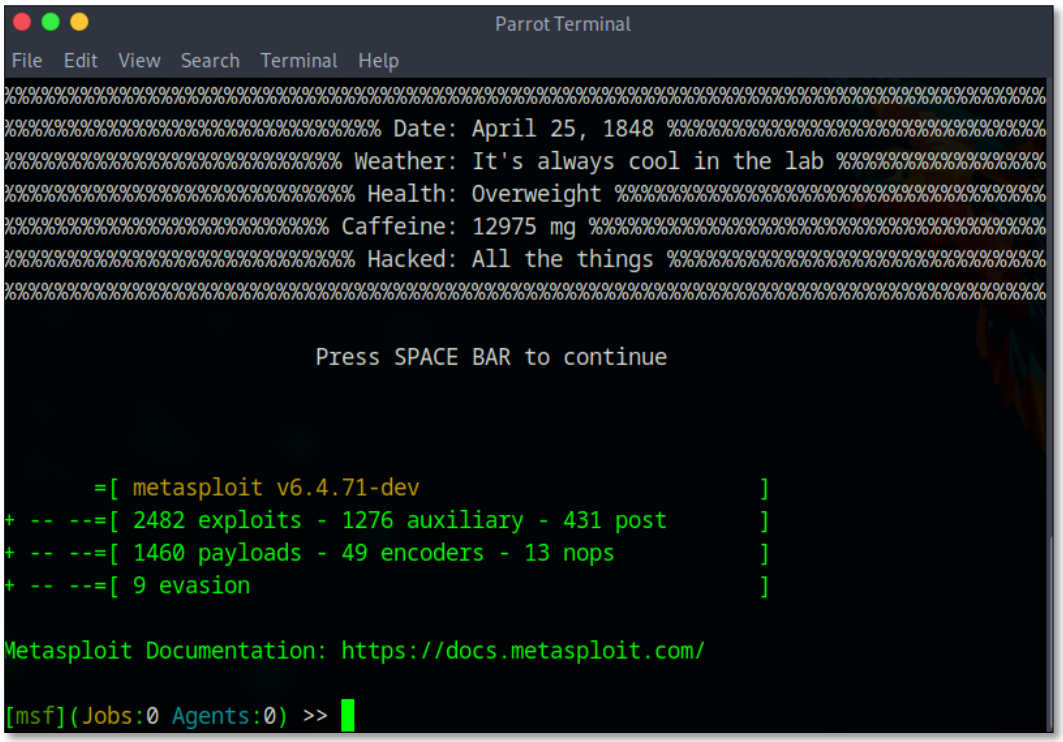
La fase de explotación se pone a prueba todas las hipótesis de posibles vulnerabilidades encontradas para determinar si suponen una amenaza real y son explotables.

[8] Kaspersky Labs. (2017, junio) ¿Qué es el ransomware WannaCry?
[9] Instituto nacional de ciberseguridad (2013) Vulnerabilidad en Microsoft Windows (CVE-2013-5065)
[10] Entel digital (2025) CVE-2025-24813 de Apache Tomcat, explotado activamente en ataques RCE

Para la explotación utilizaremos Metasploit y probaremos diferentes vectores identificados en la fase anterior.

Figura 19

Herramienta Metasploit

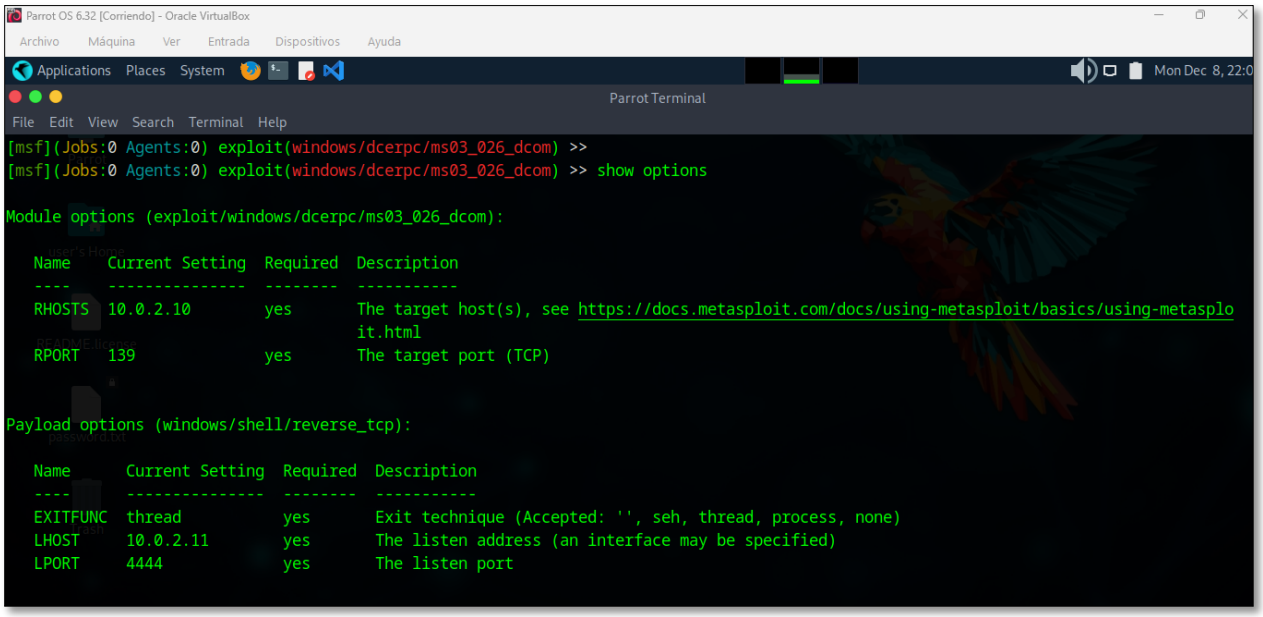


Nota. Herramienta metrasploit en su versión 6.4.71

Iniciaremos intentando explotar la posible vulnerabilidad asociada al puerto 139, utilizando el siguiente exploit de Windows “use exploit/windows/dcerpc/ms03_026_dcom” durante la revisión se evidencia que fallaba el exploit en el puerto.

Figura 20

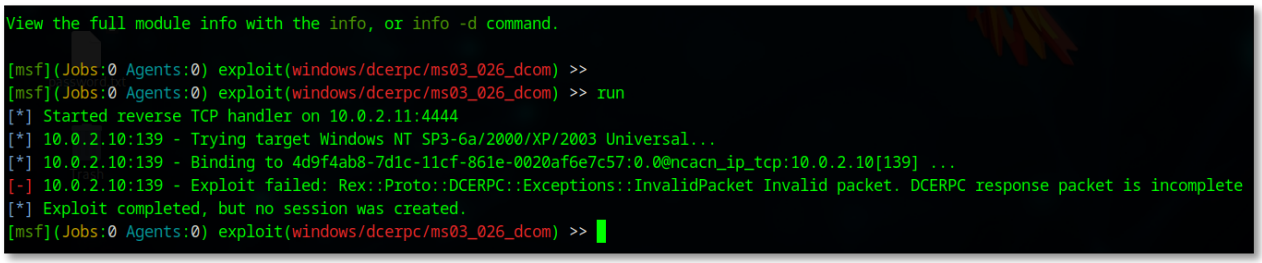
Evidencia Configuración



Nota. Configuración de exploit para ejecución en la máquina atacada.

Figura 21

Evidencia falla exploit

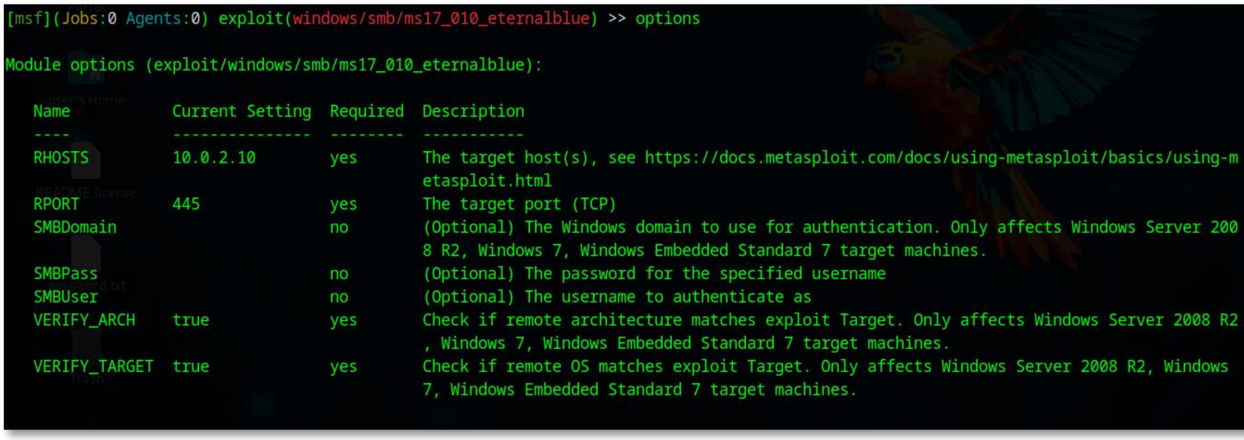


Nota. Ejecución del exploit en la maquina atacada

Iniciaremos intentando explotar la posible vulnerabilidad asociada al puerto 445, asociado a eternal blue con el siguiente comando “auxiliary/scanner/smn/smb_ms17_010” para validar si el host es vulnerable.

Figura 22

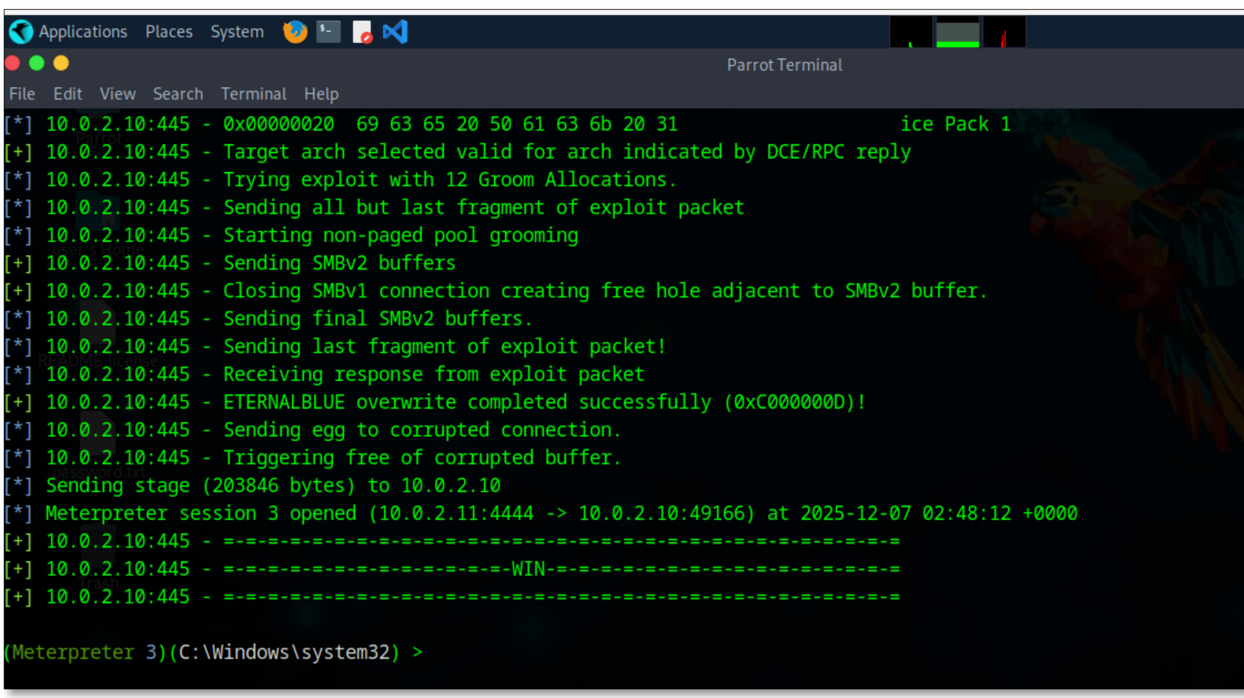
Evidencia ejecución comando



Nota. Revisión de la configuración realizada en el exploit con el comando options.

Figura 23

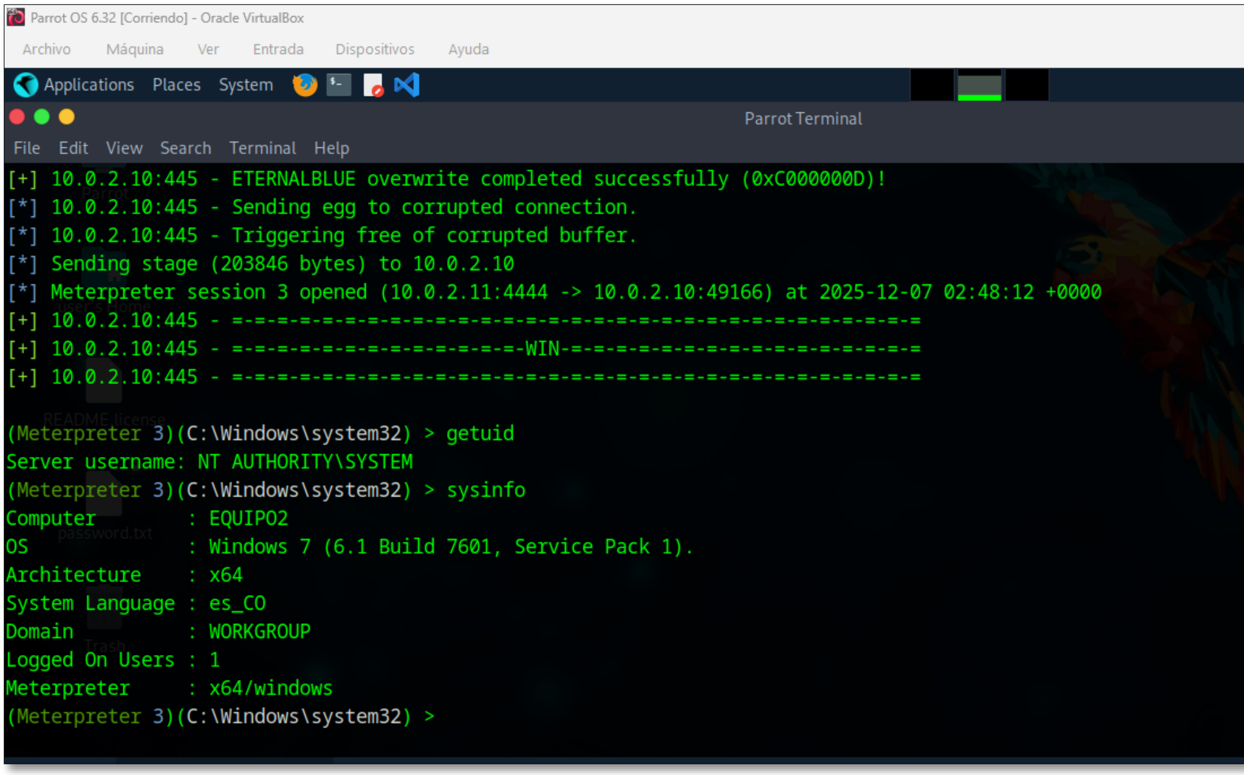
Explotación EternalBlue



Nota. Resultado de la ejecución del exploit, con conexión exitosa a la maquina atacada.

Figura 24

Verificación de ingreso Equipo2



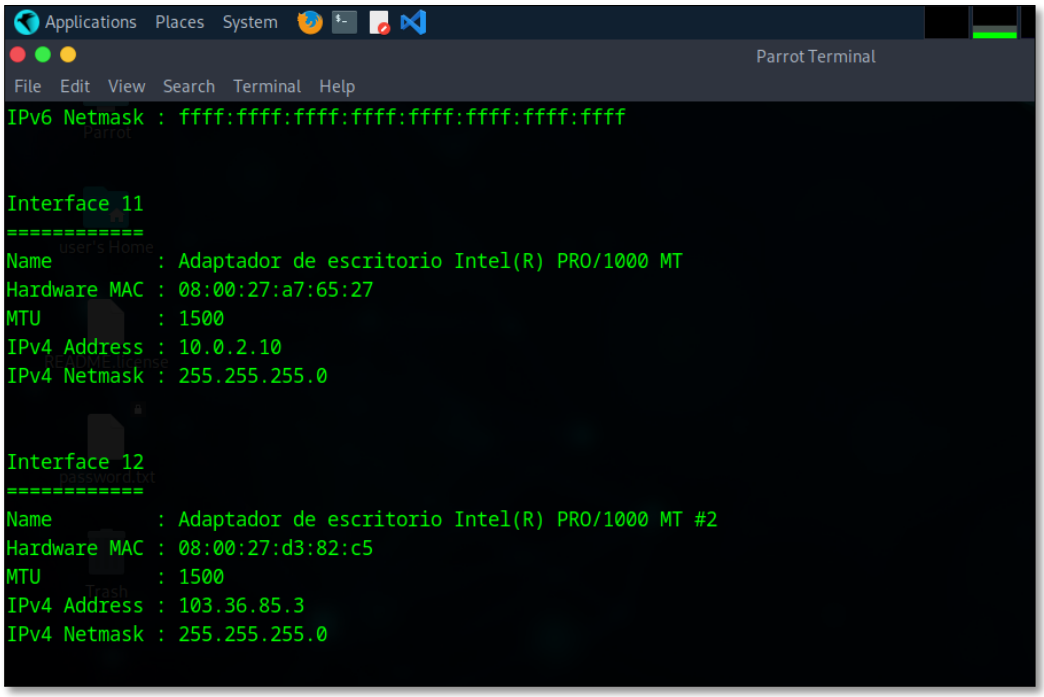
Nota. Verificación del nombre de la maquina atacada "EQUIPO2"

Ahora que ingresamos al equipo de pivote, vamos a iniciar la fase de pivoting, en la cual configuraremos la sesión actual establecida con Meterpreter para poder saltar a la máquina de la red interna la cual atacaremos.

Iniciamos por utilizar el comando "ipconfig" para validar si se tiene otra tarjeta de red y cuál es la IP.

Figura 25

Meterpreter ipconfig

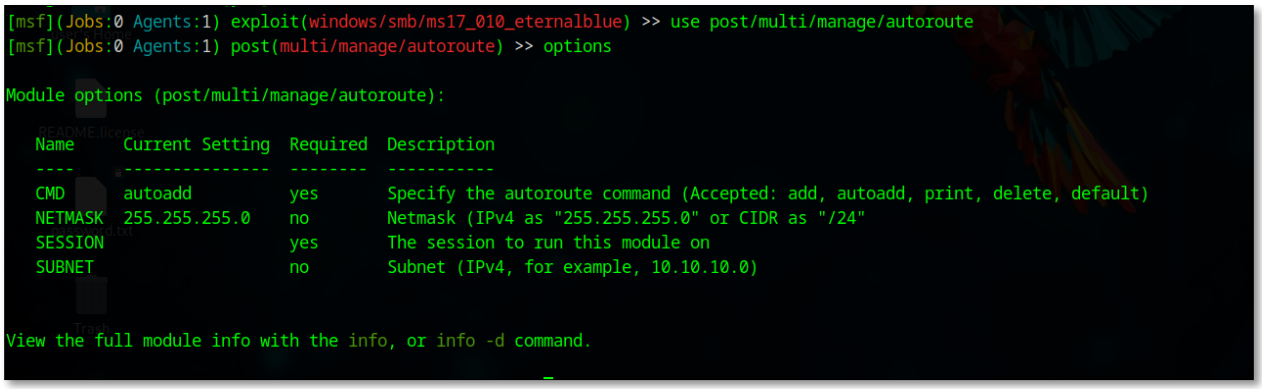


Nota. Verificación del direccionamiento IP de la maquina atacada, para validar la segunda tarjeta de red.

Para el pivoting vamos a utilizar el autoroute con la finalidad de enrutar el tráfico interno desde el equipo al cual ya tenemos acceso “use post/multi/manage/autoroute”

Figura 26

Autoroute

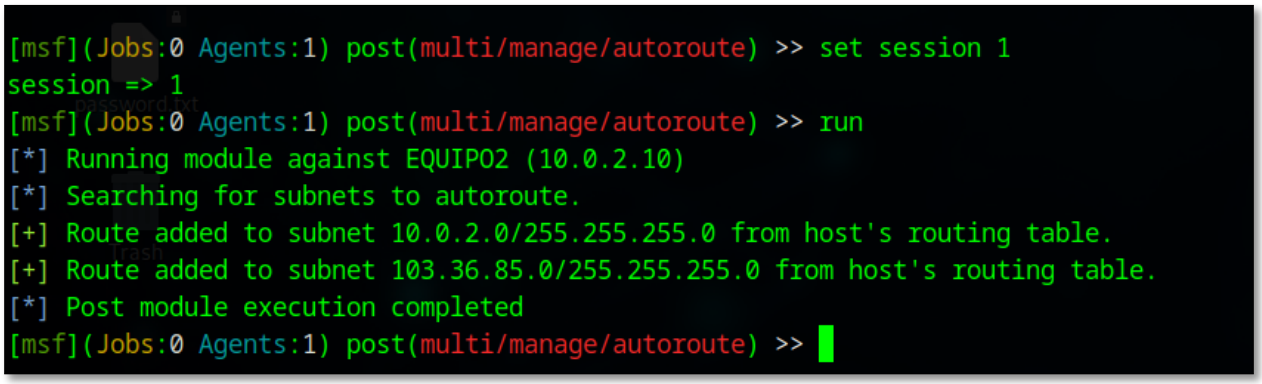


Nota. Configuración del exploit autorote para bypass entre redes

Se enruta el tráfico por la sesión con la configuración de autorote, indicándole la sesión que se encuentra activa, para este caso la sesión 1 que validamos con el comando “sessions -l”

Figura 27

Trafico enrutado

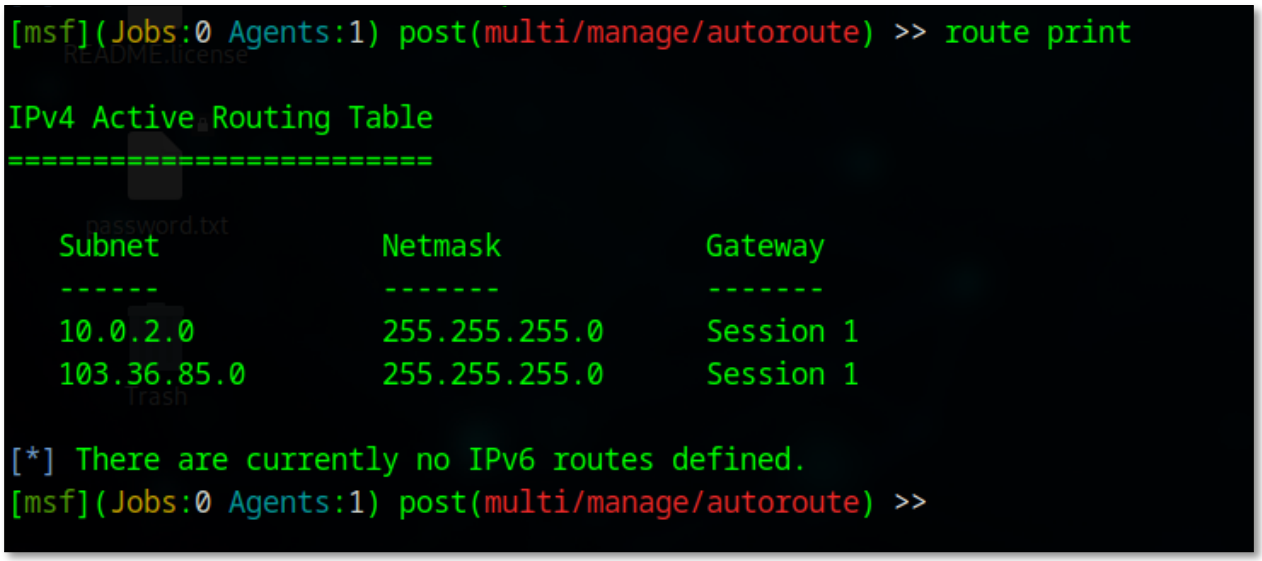


Nota. Verificación de enrutamiento de tráfico en la red

A continuación de evidencia enrutamiento realizado a nivel del equipo pivote.

Figura 28

Configuración route

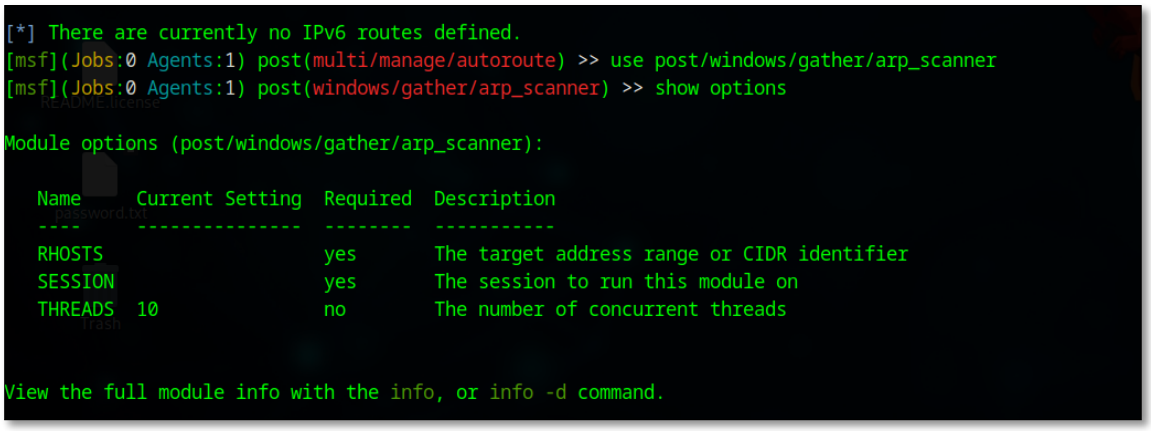


Nota. Validación del resultado de enrutamiento del tráfico.

Procedemos a validar si dentro de la nueva red alcanzada se tienen equipos objetivos para poder hacer la explotación, esto lo hacemos con arp_scanner de la siguiente forma

Figura 29

Opciones arp_scanner

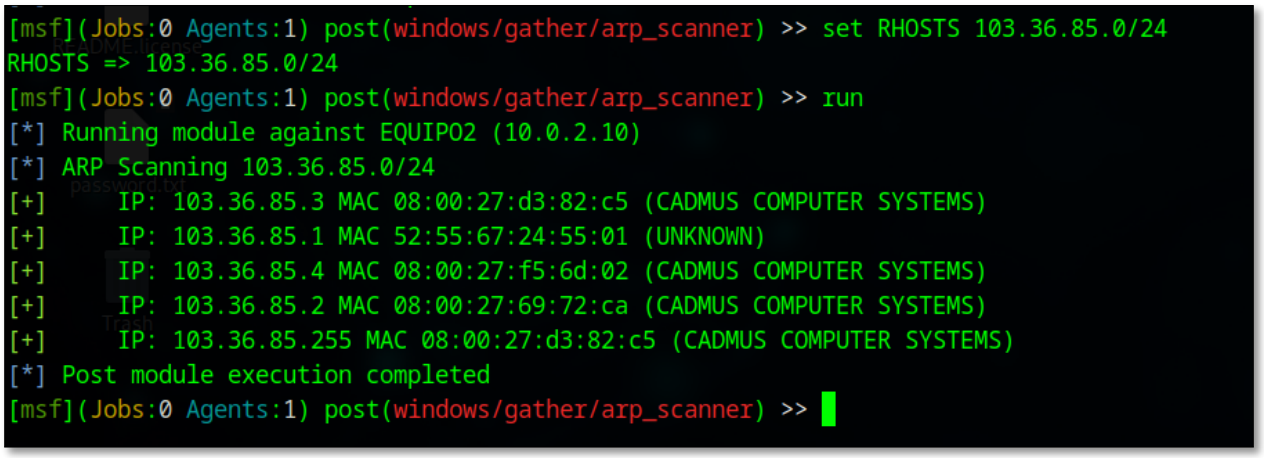


Nota. Ejecución del exploit arp scaner para escanear la red

Como se evidencia el resultado del escaneo de la red nos muestra los diferentes equipos entre ellos el identificado con la IP 103.36.85.4 el cual sería nuestro equipo objetivo final

Figura 30

Resultado arp_scanner

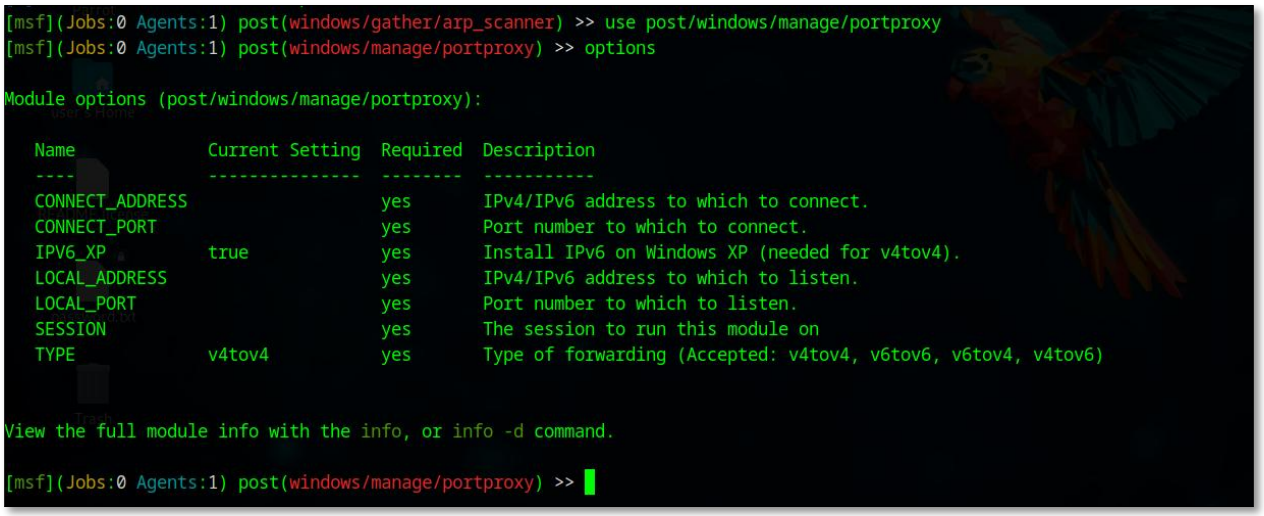


Nota. Resultado ejecución del exploit arp scaner

Ahora utilizaremos una función “use post/Windows/manage/portproxy” para enrutar el tráfico de un puerto especifico por proxy a la maquina pivote a la maquina objetivo final, para poder generar la explotación de la vulnerabilidad.

Figura 31

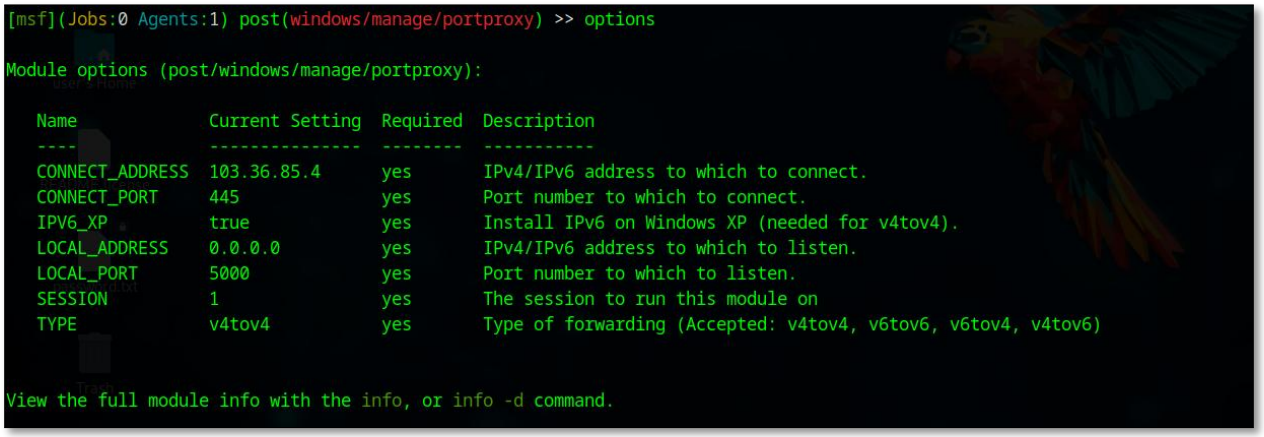
Parámetros de configuración portproxy



Nota. Configuración de exploit portproxy para enturar puerto especifico.

Figura 32

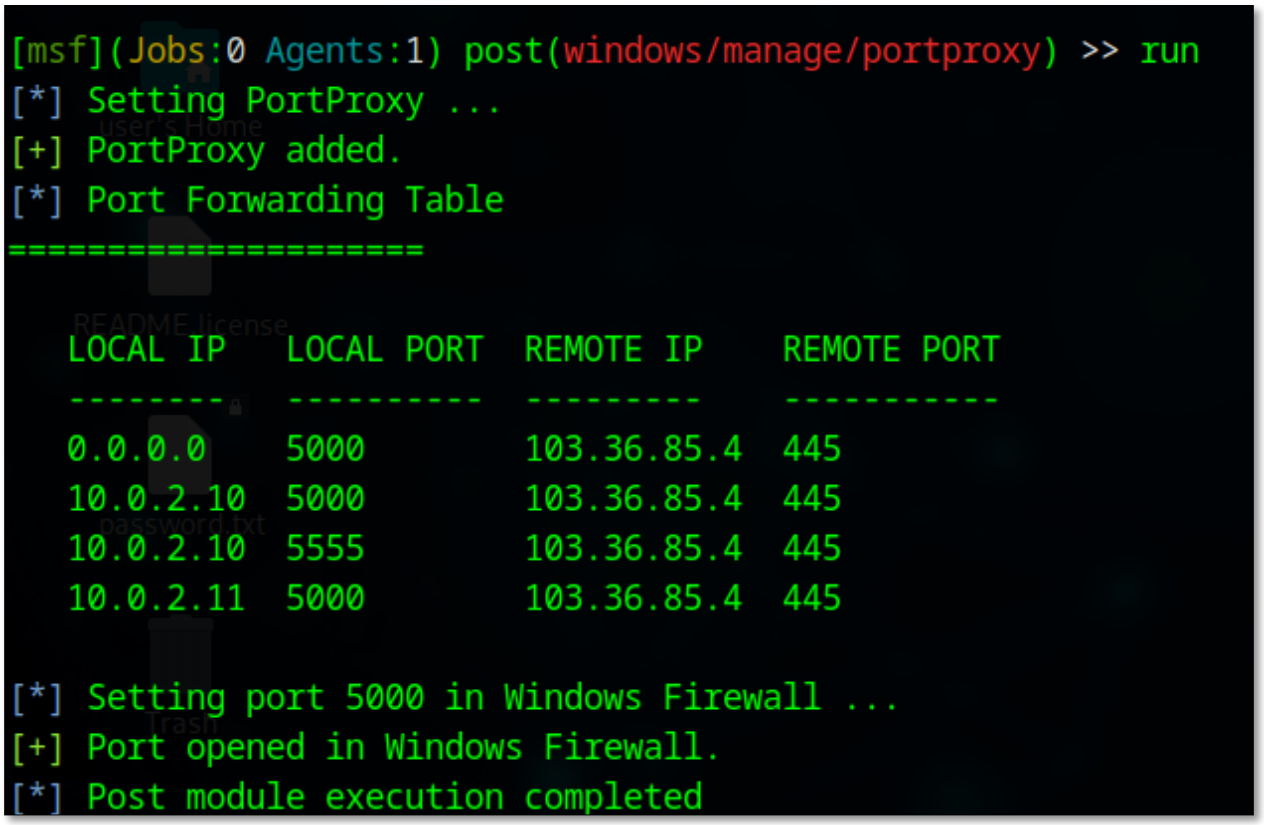
Configuración portproxy



Nota. Verificación de configuración realizada exploit portproxy.

Figura 33

Evidencia de la configuración de forma correcta

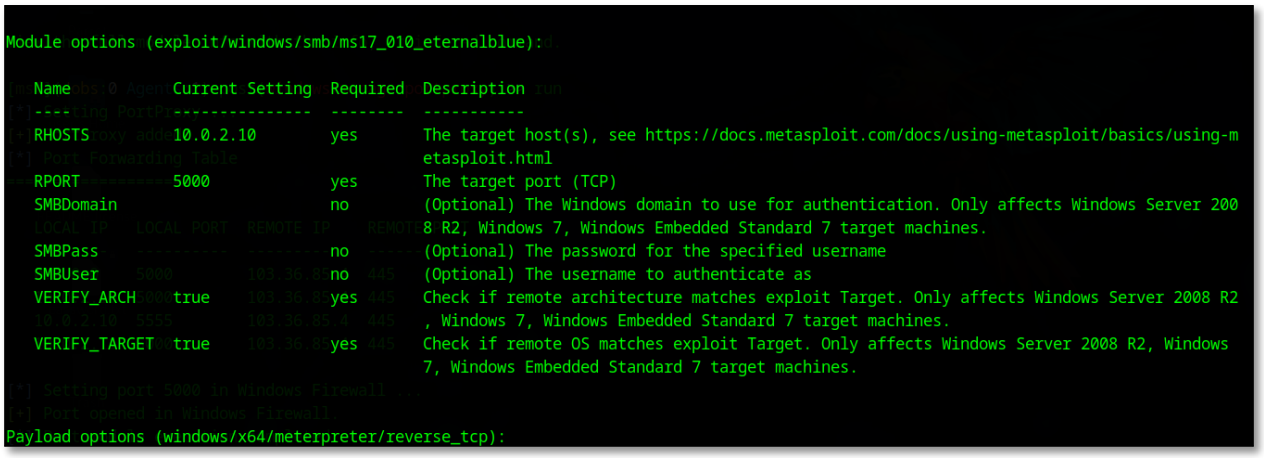


Nota. Se verifica resultado de la ejecución del enrutamiento del puerto por el exploit proxy.

Se abre una nueva terminal y se ejecuta nuevamente la vulnerabilidad de EternalBlue esta vez atacamos el puerto 5000 ya que fue el configurado en la maquina pivote que realmente está conectado al equipo final que atacaremos al puerto 445.

Figura 34

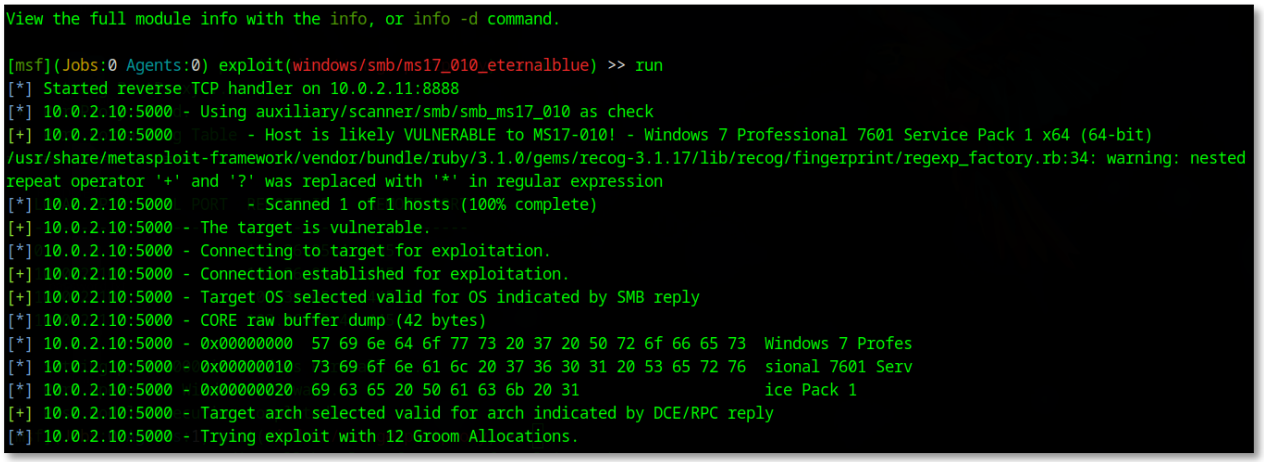
Configuración vulnerabilidad bajo puerto 5000



Nota. Configuración exploit eternablue

Figura 35

Explotación al Equipo 1

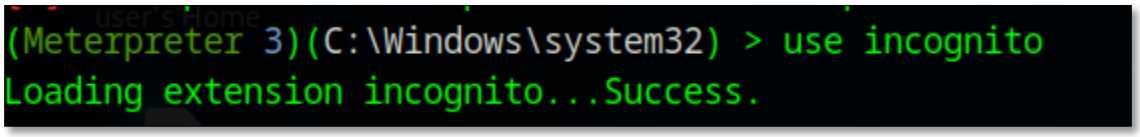


Nota. Ejecución del exploit eternalblue

Ya dentro del Equipo 1 vamos a ejecutar los siguientes comandos para crear un usuario y asignarlo al equipo de administradores. Primero usamos comando “use incognito” para escalar privilegios como administrador en la sesión establecida.

Figura 36

Comando incognito

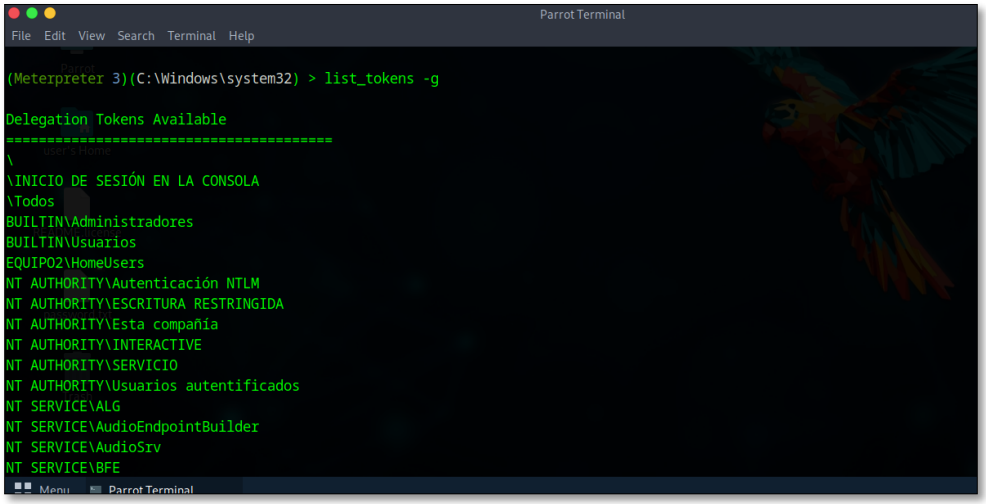


Nota. Ejecución comando incognito en meterpreter

Procedemos a ejecutar el comando “list_tokens - g” para descubrir los grupos del sistema.

Figura 37

Lista de grupos sistema



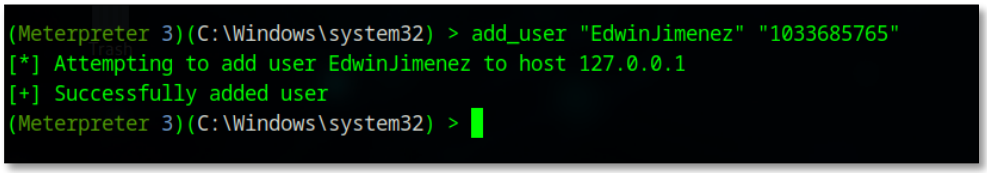
Nota. Verificación de lista de grupo de seguridad en el sistema operativo víctima.

Ahora procedemos a crear el usuario con el siguiente comando “add_user

“EdwinJimenez” “1033685765”

Figura 38

Creación usuario



Nota. Elevación de privilegios, creación de usuario y contraseña.

Después elevar permisos como administrador local Add_localgroup_user "Administradores" "EdwinJimenez"

Figura 39

Agregar al usuario como administrador

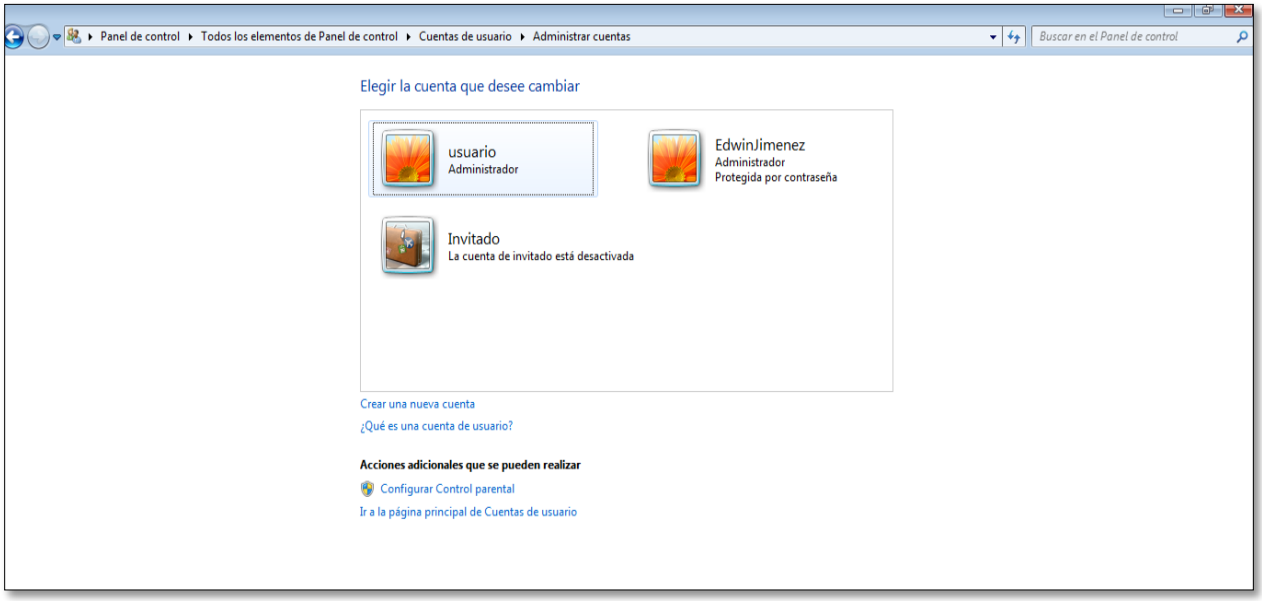
```
(Meterpreter 3)(C:\Windows\system32) > add_localgroup_user "Administradores" "EdwinJimenez"
[*] Attempting to add user EdwinJimenez to localgroup Administradores on host 127.0.0.1
[+] Successfully added user to local group
```

Nota. Elevación de privilegios como usuario miembro del grupo administrador.

Ahora se evidencia usuario creado como administrador en el sistema atacado.

Figura 40

Evidencia conexión con el exploit

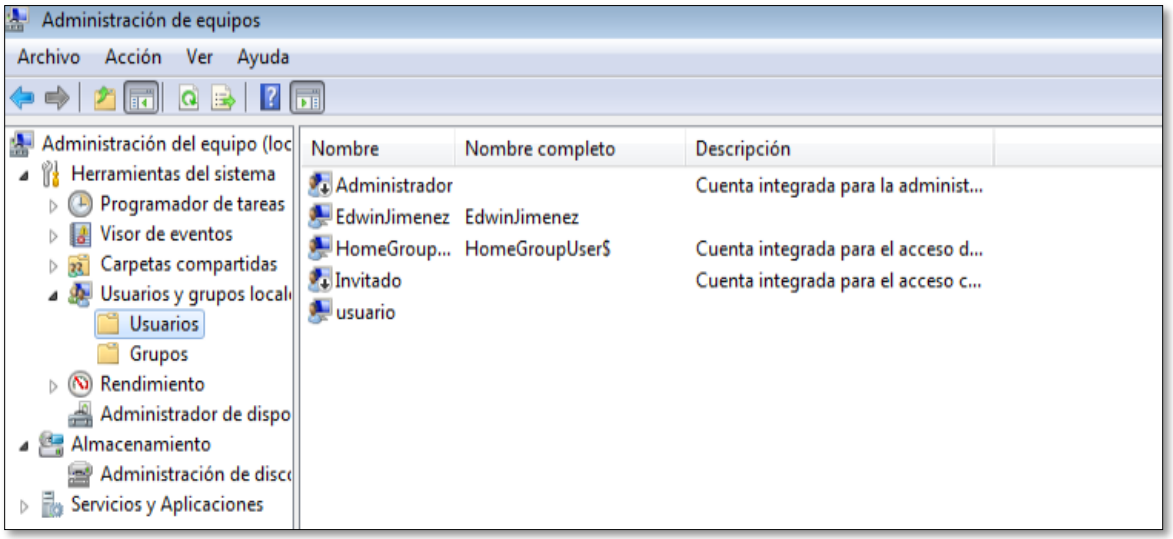


Nota. Verificación de usuario creado en la maquina atacada

Ahora en el equipo con Windows 7 x64 se comprueba la creación del usuario EdwinJimenez y asignación al grupo de Administradores

Figura 41

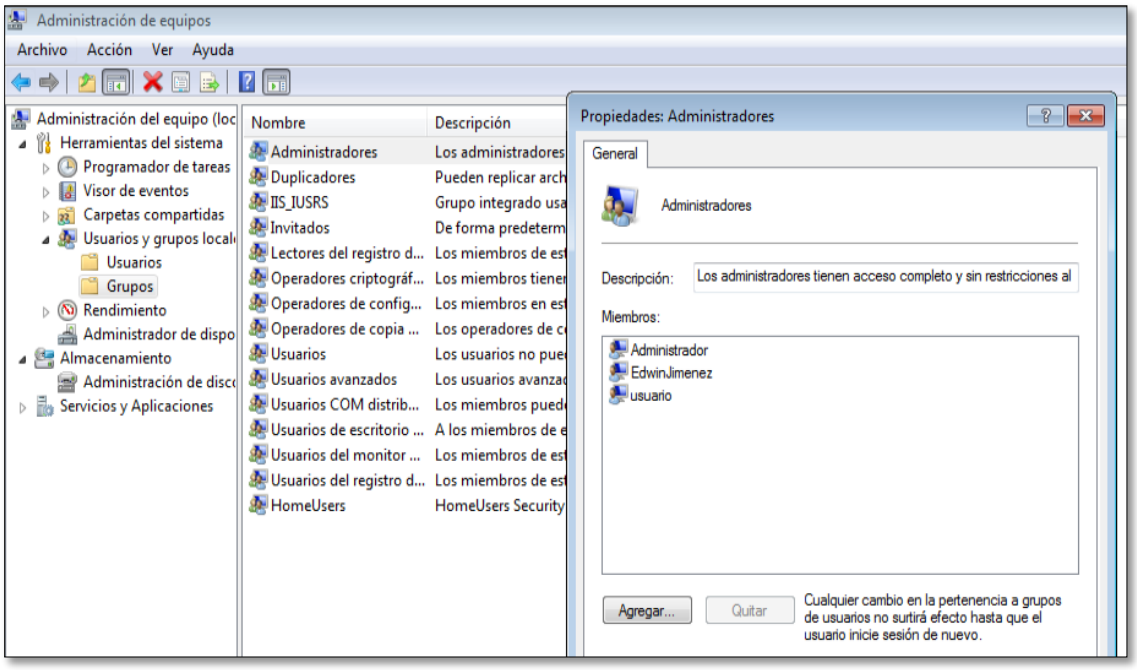
Usuarios del equipo



Nota. Verificación de los usuarios creados en el sistema atacado.

Figura 42

Administradores del equipo



Nota. Verificación del grupo local de administradores.

Análisis escenario 4 – Respuesta y contención ante incidentes de ciberseguridad

Situación problema: Análisis Blue team SecureNova Labs solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. SecureNova Labs le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

Análisis escenario: Blue team

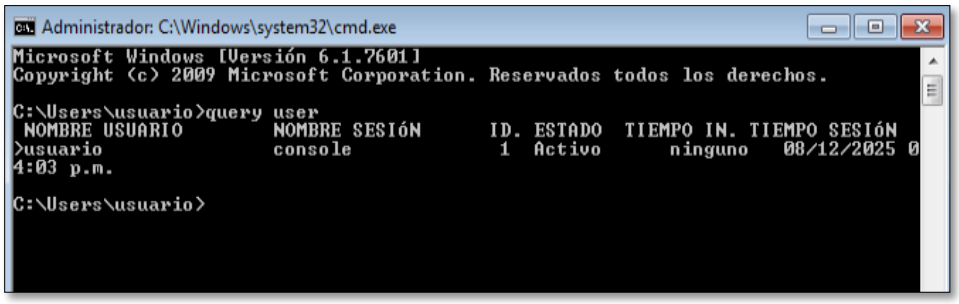
¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Inicialmente como parte del equipo Blueteam iniciaría por la validación del plan de repuesta y los procedimientos diseñados para contener un incidente, en caso de no contar con un plan diseñado realizaría los siguientes pasos.

Primer paso identificaría si el equipo atacado tiene sesiones remotas activas, si tenemos acceso físico a la maquina procederemos a utilizar la línea de comandos de sistema para ejecutar los comandos "query user" con el cual podemos ver si se tiene una sesión activa.

Figura 43

Ejecución comando "query user"

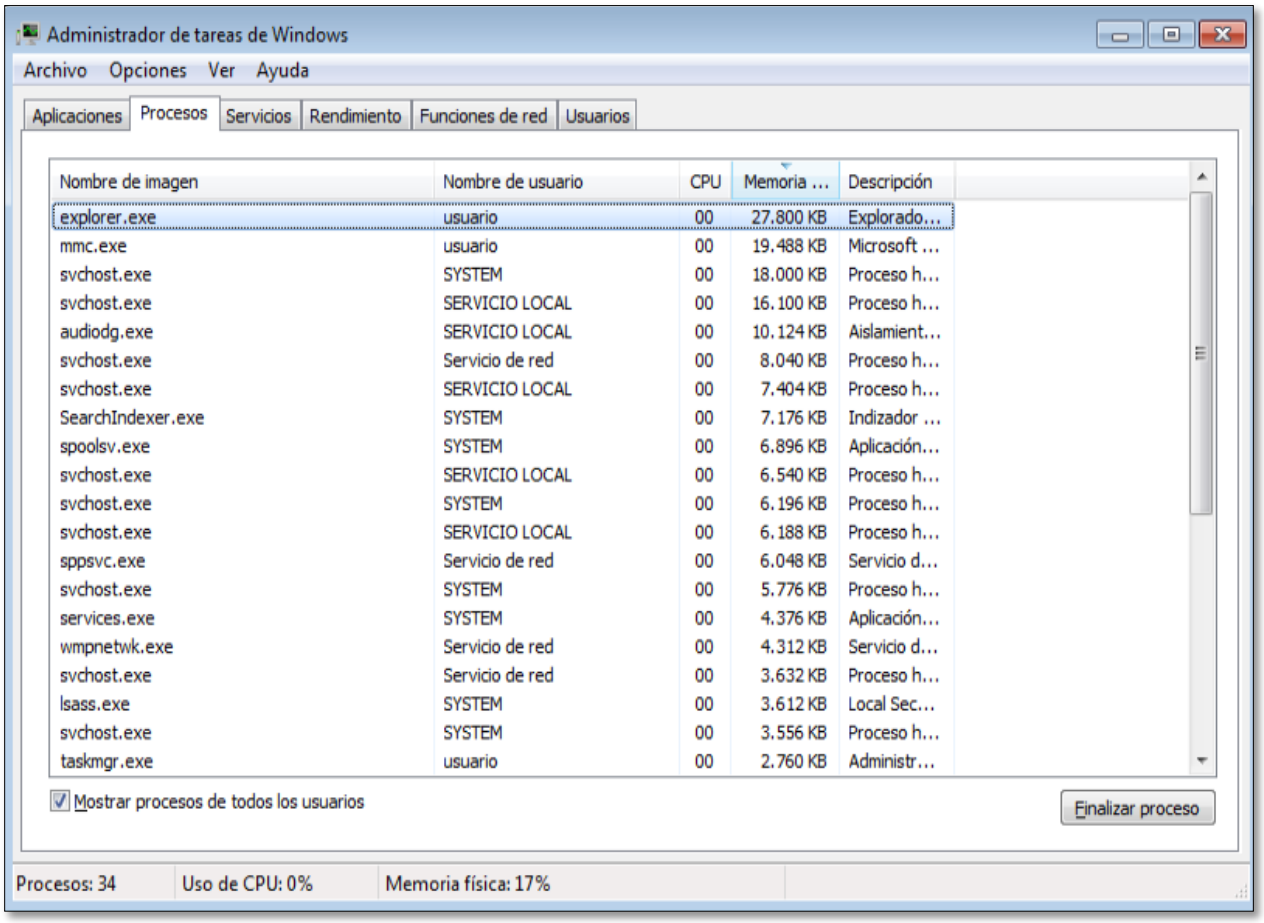


Nota. Verificación usuarios con sesiones activos.

También podemos validar procesos anómalos desde el administrador de tareas, donde buscaremos tareas con alto consumo de recursos o que no están dentro de la lista de aplicaciones instaladas, frente a cualquier amenaza poder ver los procesos y servicios del equipo puede ser fundamental en el análisis del ataque,

Figura 44

Administrador de tareas equipo atacado

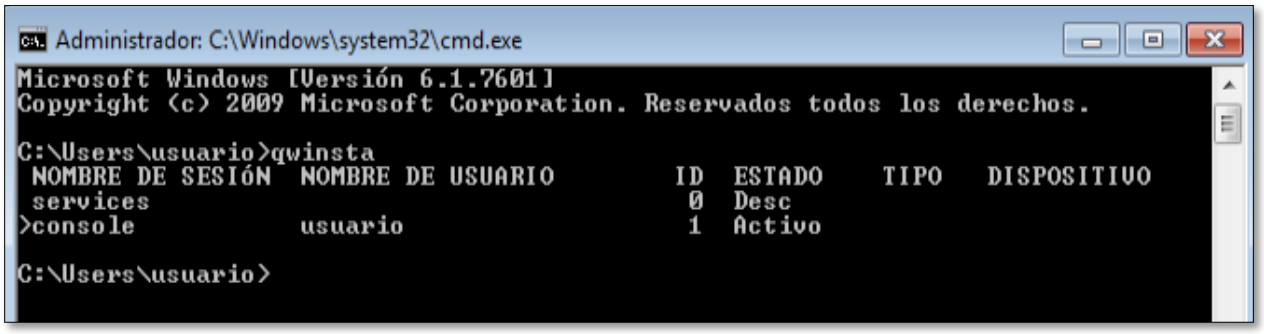


Nota. Verificación del consumo de servicios mediante el administrador de tareas.

Al identificar una sesión anómala, procedemos a utilizar la línea de comandos para cerrar la sesión, inicialmente con el comando “qwinsta” para validar las sesiones activas y posteriormente el comando “rwinsta”, para cerrar la sesión desconocida.

Figura 45

Sesiones activas



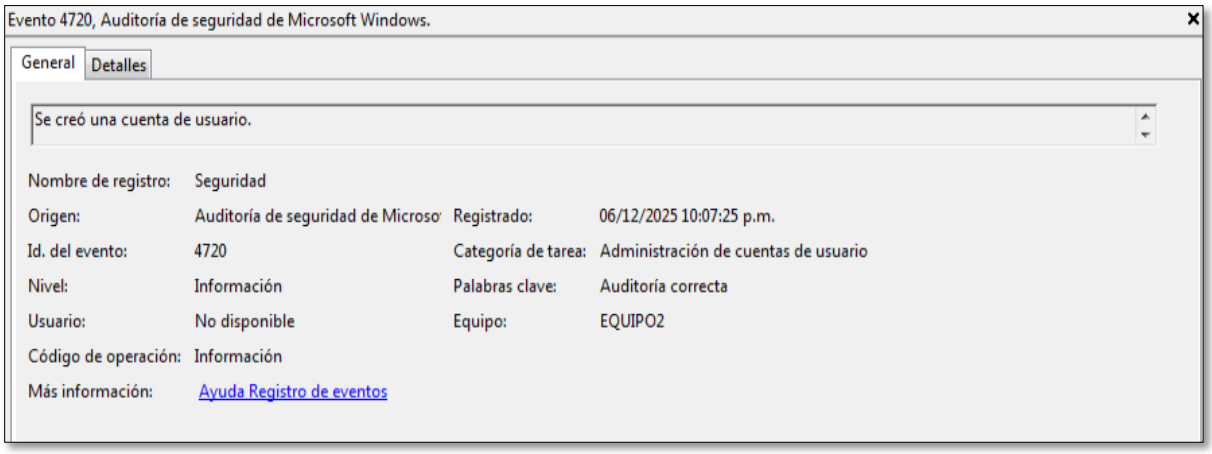
Nota. Verificación de sesiones activas mediante la línea de consola.

Una vez se cierra la sesión del atacante, procedemos a revisar la hora del sistema, ya que los atacantes cambian la hora del sistema para cubrir sus huellas y que no se pueda rastrear de forma efectiva la línea de tiempo del ataque generado.

En caso de que la hora corresponda con la hora loca, procedemos a verificar los registros del sistema mediante el visor de eventos con el comando “eventvwr.msc”, los primeros eventos que se deberían revisar son los relacionados con creación y modificación de cuentas de usuario evento 4738, inicios de sesión exitosos 4624 y fallidos 4625. Se evidencia en el evento 4722 la creación de una cuenta “EdwinJimenez” la cual no es conocida en el sistema.

Figura 46

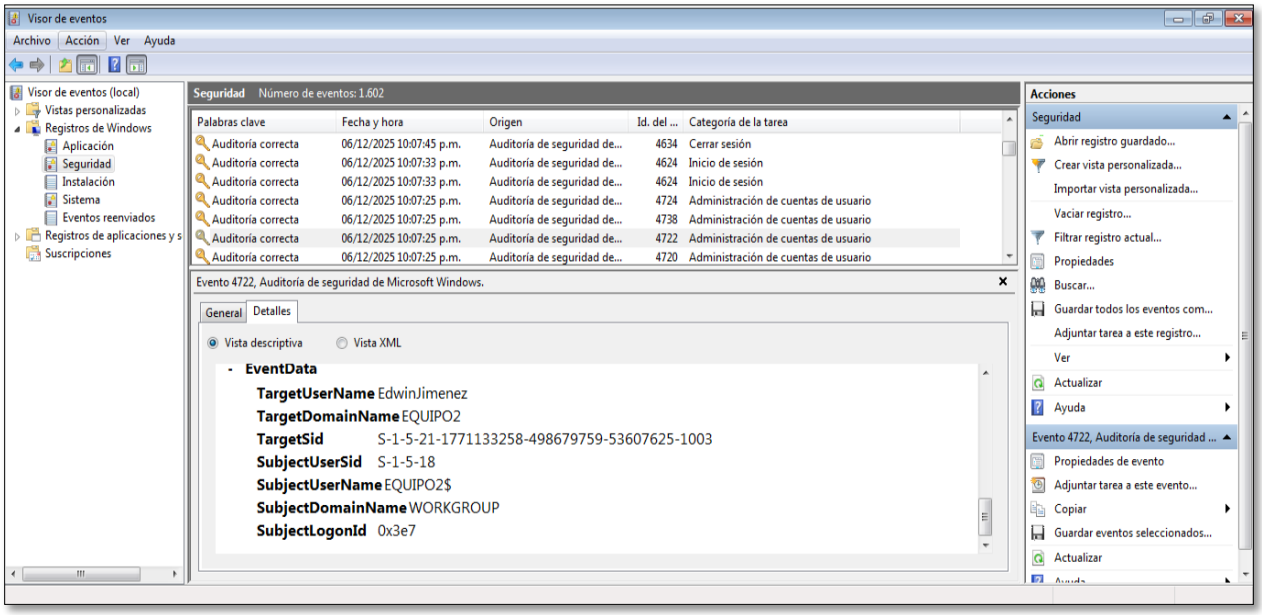
Auditoria creación de cuenta



Nota. Verificación de registros de auditoría, para la creación de usuarios.

Figura 47

Nombre de la cuenta anómala creada

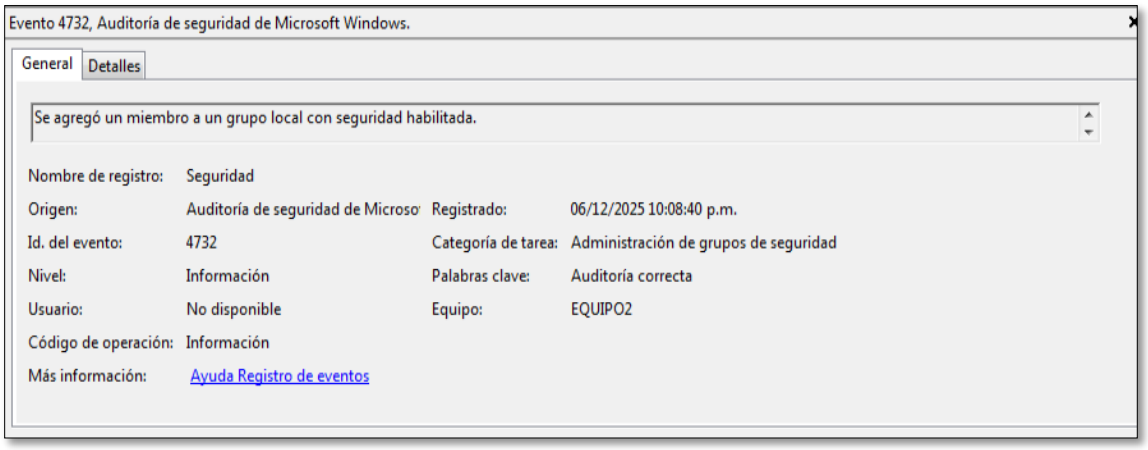


Nota. Verificación de los detalles de auditoría.

Se evidencia en el evento 4732 la elevación de privilegios de la cuenta anómala.

Figura 48

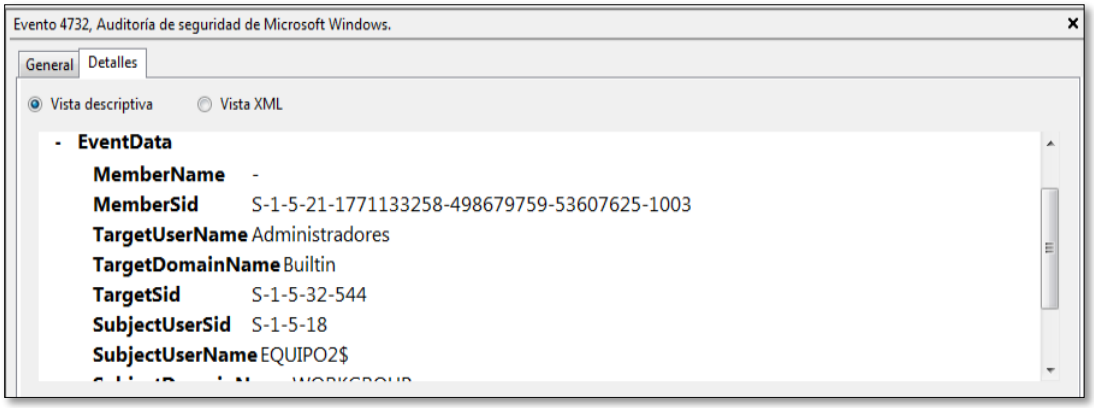
Cambio al grupo cuenta anómala



Nota. Verificación detalles auditoria escalada de privilegios.

Figura 49

Cuenta ingresa a grupo "Administradores"

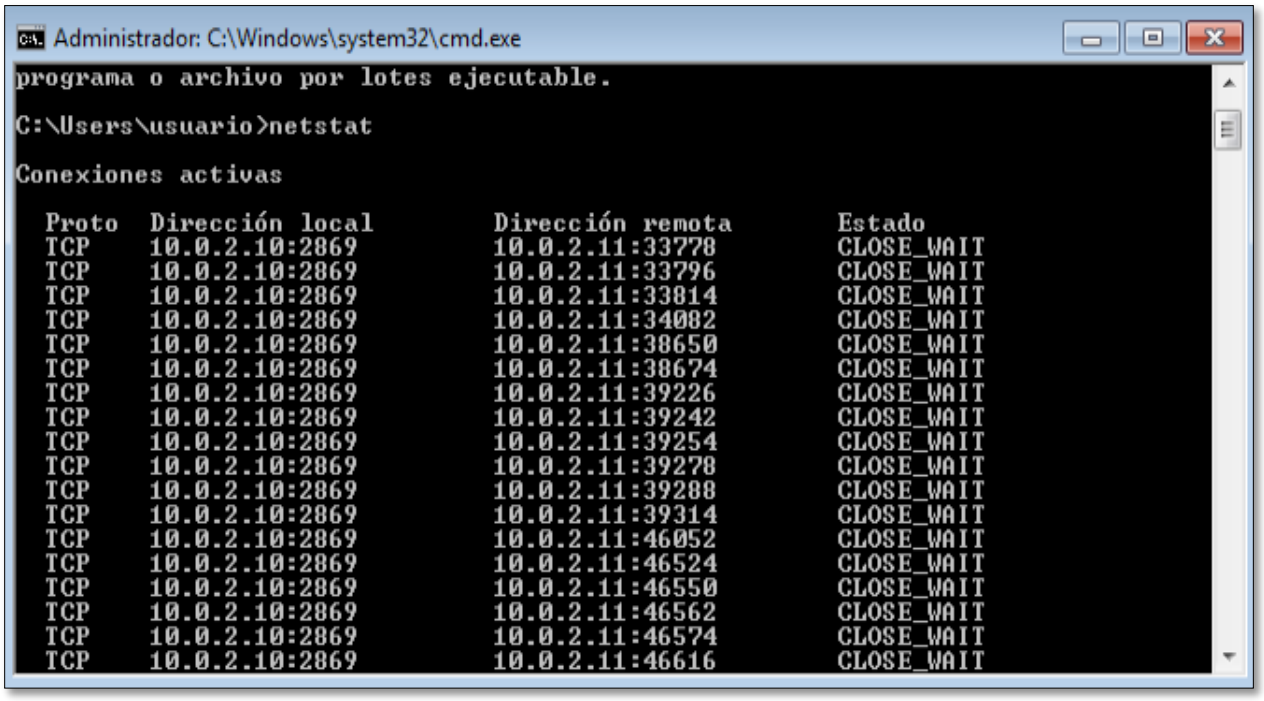


Nota. Verificación detalles auditoria escalada de privilegios.

Se verifica conexiones establecidas, para analizar estatus del equipo y si actualmente se encuentra algún equipo conectado.

Figura 50

Ejecución netstat

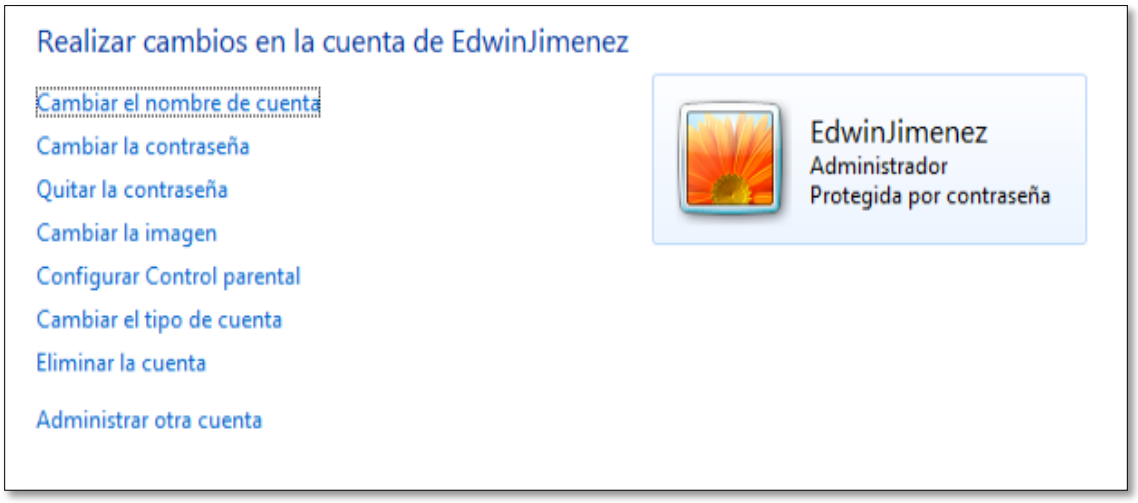


Nota. Verificación de conexiones activas a nivel de la tarjeta de red.

Se evidencia interacción con un equipo que no es conocido en la red, con múltiples conexiones a diferentes puertos, aunque algunas están abajo otras están establecidas.

Figura 51

Se desactiva la cuenta



Nota. Desactivación de la cuenta administrador anómala creada.

Durante la revisión se evidencia que se encuentra un usuario desconocido como, por lo cual procedemos a deshabilitar el usuario correspondiente el cual se puede realizar mediante el panel de control en administrar cuentas y deshabilitar la cuenta seleccionada.

Se procede a aislar la máquina, para frenar la amenaza activa y pasamos a generar la validación del vector de ataque.

Se validaría el direccionamiento IP desde el cual se conectaron a realizar la creación del usuario, por lo cual utilizaría los logs del firewall en caso de no tener firewall, revisaría los eventos del sistema del equipo atacado, en caso de no tener eventos identificados instalaría una wireshark para validar el tráfico o los intentos de conexión al equipo.

Una vez identifica la dirección IP del equipo que utilizo como pivote el atacante, volvería a realizar los pasos anteriores y una vez identificado la dirección IP externa del atacante procedería a bloquearla en el firewall interno del equipo.

También es importante iniciar una validación de la arquitectura correspondiente a la infraestructura atacada, identificar las vlan´s que actualmente se partiendo del equipo Windows identificado como paciente cero.

Una vez identificada en la arquitectura las vlan´s que, interactuando con el equipo atacado, se debe proceder con la realización del hardening correspondiente e iniciar un esquema de defensa en profundidad diseñado para proteger los activos de información.

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team, qué medidas de hardenización propondría para que el ataque no se repita?

Teniendo presente la utilización de herramientas sin pago, comenzaría utilizando Microsoft Security Compliance Tolkit para testear el estado actual de los equipos Windows de la infraestructura basándome en las platillas del CIS Benchmark y generando un plan de remediación para las diferencias evidenciadas. Para la ejecución del plan de remediación abarcaría actualización de sistemas operativos a una versión superior, en caso de no poder actualizar los sistemas por temas de licenciamiento o por un software core de la compañía que no funciona en versiones superiores, aislaría los equipos que se encuentran fuera de soporte en una vlan sin internet y permitiría el acceso solo bajo condiciones seguras como acceso físico. Generaría un plan de hardenización semestral para que se valide que las condiciones iniciales no cambien en los equipos y generaría una hoja de vida para los cambios realizados en los equipos.

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

El Blueteam es el equipo que salvaguarda la infraestructura de la compañía, son los encargados en trabajar proactivamente en el aseguramiento de cada activo de información y generar planes de mejora frente a posibles amenazas, cargando indicadores de compromiso en las herramientas de seguridad para amenazas de día cero. El equipo de respuesta a incidentes se

encarga de la respuesta activa frente a un incidente de ciberseguridad, trabajando en identificar los vectores de ataque para solicitar su remediación o listando diferentes indicadores de compromiso que puedan ser utilizados para explotar el software instalado en la compañía.

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

Cuando se trabaja con el CIS, es utilizado principalmente por sus plantillas para realizar hardenización en los sistemas, ya que abarca un gran número de plantillas que pueden ser utilizadas para una auditoria de políticas a nivel del sistema, pero también tiene un compendio de guías para diferentes sistemas operativos, bases de datos de diferentes fabricantes que contiene diferentes prácticas de la industria que se pueden aplicar para mejorar procesos y tener una infraestructura más segura.

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

Un SIEM es un gestor de información y eventos de seguridad, también podemos decir que es un correlacionador de eventos de seguridad cuando hablamos de un correlacionador decimos que es un sistema que recopila datos de diferentes herramientas de seguridad (firewall, directorio activo, antivirus, bases de datos, endpoint etc) con la finalizada de analizar y detectar eventos anómalos dentro de los sistemas para generar alertas de seguridad. Aunque en teoría es solamente un esquema básico la idea general de un SIEM debería ser mucho más que alarmas que se reporten como eventos de seguridad, debería tener configuraciones de respuestas automática configuradas en eventos específicos para poder conectarse con otras herramientas como el firewall y poder bloquear direcciones IP sospechosas, aislar equipos en la red interna frente a un ataque, también debería tener capacidades de análisis de comportamiento de usuarios y entidades con lo cual poder generar nuevas alertas basados en los comportamientos inusuales de la red o los sistemas.

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

Implementación de una solución de EDR para la red.

La implementación de esta solución tiene como objetivo la detección, análisis y respuesta en tiempo real de amenazas que afecten puntos finales críticos como servidores, estaciones de trabajo, dispositivos de red.

Esta solución debe ser desplegada en los servidores críticos como Active Directory y los equipos finales. Se sugiere generar la integración con un SIEM para lograr con el ello la correlación de eventos y la elaboración de respuesta automática.

Los beneficios que tiene la implementación de este tipo de solución está el análisis de comportamiento para la detección del malware avanzado como Ransomware, APT. La respuesta automatizada del aislamiento de los puntos finales, la eliminación de archivos maliciosos. La posibilidad de la trazabilidad forense post incidente.

Implementación de una DMZ

Conocida como la zona desmilitarizada es un tipo de subred aislada, que actúa como un puente o capa de protección entre la red interna y redes externas como internet. Su funcionalidad principal es alojar equipos que necesitan estar expuestos al público o conectados a internet como (Servidores de correo, FTP, DNS) para el caso de estudio también pueden alojar un honeypot.

Aunque la DMZ tienes diferentes arquitecturas dependiendo los equipos que se conectan, su estructura básica es mediante un firewall que contiene como mínimo dos interfaces, una para un WAN (Externa) y una LAN (Interna) con el cual las políticas de la red y en la mitad aislado se ubica el DMZ y se configura el acceso a un equipo especifico por su función o necesidad.

Implementación de una Honey Pot (Trampa de Atacante)

El objetivo de este elemento es que detecte, analice y contenga amenazas externas mediante la simulación de servicios vulnerables, para lograr identificar comportamientos y técnicos de ataque, desviar la atención de los atacantes de activos reales y para generar alertar tempranas. La aplicación del elemento debe ser desplegada en la DMZ por lo cual se sugiere como complementario a la aplicación anterior, simulando un servidor vulnerable como SSH, Web o FTP. Debe instalarse en la red productiva, herramientas posibles idónea, T-Pot, Cowrie, Honeyd. Los beneficios es no afectar el rendimiento del sistema real, mejora la detección de ataques internos o persistentes (APT), aporta inteligencia de amenazas local.

Evidencias de Sustentación

En cumplimiento de los requisitos de la Etapa 5 del Seminario Especializado, se presenta el video de sustentación disponible en el siguiente enlace:

Video de sustentación del informe final: https://youtu.be/9qdUIN0Ceic

Conclusiones

Las herramientas o ejercicios de escritorio, nos ayuda a conocer nuestras debilidades con una mirada crítica desde el interior con la finalidad de apoyarnos con expertos en el área, que busquen brechas de seguridad y eviten que lleguemos a un estado de falsa sensación de seguridad, durante los ejercicios realizados logramos manejar diferentes aspectos desde el punto legal con un análisis profundo de la legislación en Colombia y las leyes establecidas.

El plan de mejora continua y endurecimiento de nuestra infraestructura es una actividad del blue team el cual es nuestro escudo con el cual buscamos mejores alternativas para endurecer la seguridad, con la implementación de herramientas y hardenización de los sistemas.

Durante el desarrollo del laboratorio practico desde el punto de vista del red team se evidencio las diferentes vulnerabilidades en el sistema objetivo el cual ya es un sistema obsoleto sin actualizaciones de seguridad que no permitió explotar diferentes vulnerabilidades, realizar movimiento lateral mediante un equipo pivote, escalamiento de privilegios y creación de usuarios no autorizados.

Como profesionales en ciberseguridad debemos tener un amplio conocimiento de las herramientas de seguridad con las que podemos interactuar en la infraestructura de las empresas, pero también es necesario conocer los planes de respuesta y contención de incidentes de seguridad, por lo cual nos preparamos con diferentes laboratorios y casos de estudia, para pensar fuera de la infraestructura conocida para poder generar esquemas de aseguramiento técnico. Aunque el avance tecnológico es exponencial durante los años de experiencia y estudio encuentro de gran valor poder tener alternativas frente a cualquier escenario para poder actuar

bajo presión basados en nuestro aprendizaje continuo y la evolución de los procesos de aseguramiento de la infraestructura.[11]

Cada uno de los procesos desarrollados durante las actividades cubren cada uno de los aspectos integrales de la carrera lo cual apoya en gran medida nuestras habilidades de cara a los proyectos y proyección en el ámbito laboral en Colombia.

[11] Guohong, Z., Zhongwei, X., Feng, H., Zhongyi, X. The audit committee's IT expertise and its impact on the disclosure of cybersecurity risk (2025)

Recomendaciones

Cada uno de los escenarios trabajados, nos muestra diferentes puntos de vista desde los equipos de blue team y red team, es necesario como profesional entender las implicaciones de cada uno y acorde a los problemas plateados se abren diferentes alternativas para poder proteger una red y para ser explotadas.

Aunque desde mi punto de vista es más interesante estar del red team, para poder hace investigación sobre la evolución de las diferentes vulnerabilidades crear scripts para explotar fallas en diseño y trabajar entornos robustos, es importante conocer cada uno de los procesos de aseguramiento desde el punto de vista de blue team, la ejecución de controles compensatorios, la integración de nuevas herramientas de seguridad y la hardenización.

Los aspectos éticos son lo que nos forma como profesionales, lo cual nos indica que debemos utilizar nuestros conocimiento de una forma responsable y tener un amplio conocimiento de la legislación para no generar actividades que no estén debidamente soportadas y puedan generar sanciones legales porque la empresa en la cual trabajamos no se hace responsable de las actividades que solicita.

Aunque se puede llegar a evidenciar un ataque en curso, es necesario tener un conocimiento integral de las herramientas de seguridad para robustecer la seguridad de la empresa y en caso de ser necesario poder actual en un escenario de compromiso como un equipo de respuesta a incidentes que logre contener un ataque.

Cada día avanza más la tecnología y nos estamos encaminando en una carrera de automatización con nuevas tecnologías, la creación de robots autónomos con capacidad avanzadas y los diferente4s bloques de decisión que conforman maquina con inteligencia artificial que pueden simular un atacante o ser utilizadas en los nuevos ataques avanzados.

Aunque no está en la dedicatoria, creo que el cambio de ritmo y enfoque suministrado durante el seminario nos llevó a explorar diferentes alternativas, me parece de gran valor las propuestas de mejora encaminadas a un aprendizaje más robusto.[12]

[12] Ramírez, D.M.R., Garcés-Giraldo, L.F., Doria-Orozco, T., Franco-Castaño, S., Valencia-Arias, A., Rodríguez-Correa, P.A., Román, J.E. Bibliometric analysis on the use of Machine Learning in cybersecurity

Referencias Bibliográficas

Congreso de la república. *ley 1273 de 2009*

http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso de la república. *ley 1581 de 2012*

http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Congreso de la república. *ley 1266 de 2008*

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Dragonjar. (2021, febrero) *osstmm, manual de la metodología abierta de testeo de seguridad*

https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de seguridad.xhtml

Entel digital (2025) *CVE-2025-24813 de Apache Tomcat, explotado activamente en ataques*

RCE, https://portal.cci-entel.cl/Threat_Intelligence/Boletines/2175

Fiscalía general de la nación. (2021, enero), *delitos informáticos archives.*

https://www.fiscalia.gov.co/colombia/tag/delitos-informaticos/

Instituto nacional de ciberseguridad (2013) *Vulnerabilidad en Microsoft Windows (CVE-2013-5065)*, https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2013-5065

Kaspersky Labs. (2021, enero), *una breve historia sobre el hackeo*

https://encyclopedia.kaspersky.es/knowledge/a-brief-history-of-hacking/

Kaspersky Labs. (2017, junio) *¿Qué es el ransomware WannaCry?*

https://www.kaspersky.es/resource-center/threats/ransomware-wannacry

Ministerio de comercio, industria y turismo (2013) *decreto 1377 de 2013* http://wsp.presidencia.gov.co/normativa/decretos/2013/documents/junio/27/decreto%201377%20del%2027%20de%20junio%20de%202013.pdf

(n.d.). (2021, Enero) *Cybercrime could cost the world almost $1 trillion in 2020, McAfee says - The Hindu*. from https://www.thehindu.com/sci-tech/technology/cybercrime-could-cost the-world-almost-1-trillion/article33269047.ece

(n.d.). (2021, enero) *The 2020 Official Annual Cybercrime Report - Herjavec Group.* https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

Apéndices

Apéndice A

Resultado de revisión en Turnitin

El resultado demuestra una similitud de un 35% compuesta de un 29% del trabajo enviado por mí en otra materia, esto es debido a que también curso la materia Trabajo de Grado II en el grupo 219024_3 con el director de curso Christian Obando y el trabajo de grado fue basado en el seminario que estoy cursando. Adjunto evidencias.

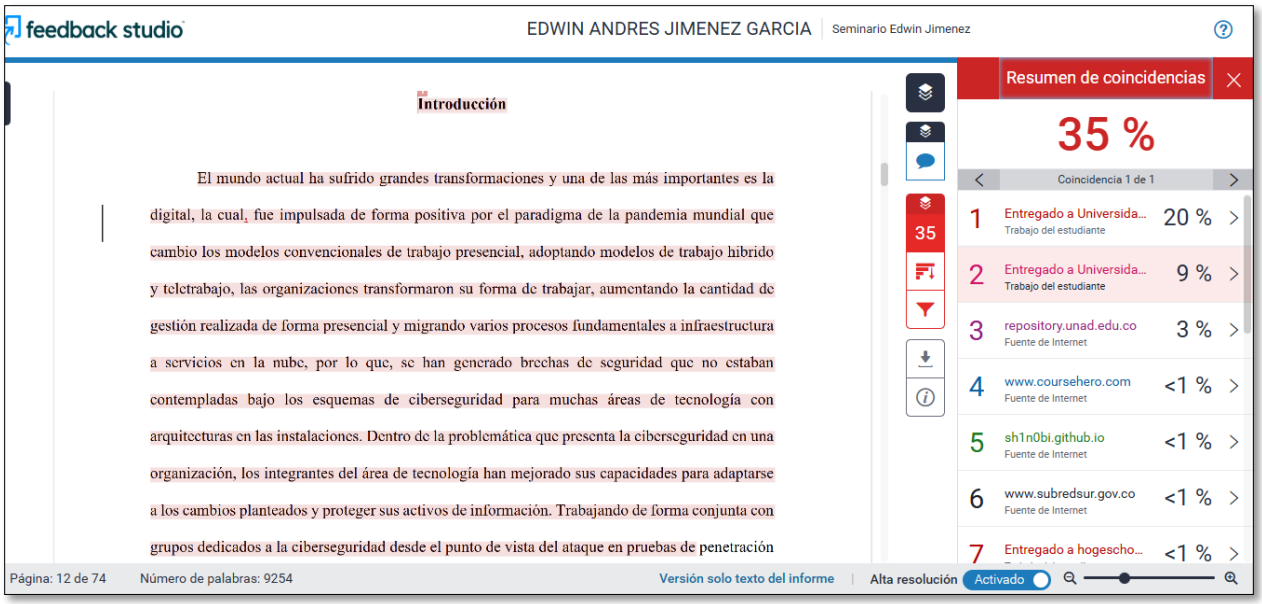
turnitin

Recibo digital

Este recibo confirma que Turnitin ha recibido tu trabajo. A continuación, encontrarás la información del recibo perteneciente a tu entrega.

Autor del envío	EDWIN ANDRES JIMENEZ GARCIA
Identificador del trabajo de Turnitin (Identificador de referencia)	2840590165
Título del Envío	Seminario Edwin Jimenez
Título de Tarea	ECBTI - Draftbank 2
Fecha del envío	08/12/25, 20:10

Imprimir


feedback studio
EDWIN ANDRES JIMENEZ GARCIA
Seminario Edwin Jimenez
Introducción
El mundo actual ha sufrido grandes transformaciones y una de las más importantes es la digital, la cual, fue impulsada de forma positiva por el paradigma de la pandemia mundial que cambio los modelos convencionales de trabajo presencial, adoptando modelos de trabajo hibrido y teletrabajo, las organizaciones transformaron su forma de trabajar, aumentando la cantidad de gestión realizada de forma presencial y migrando varios procesos fundamentales a infraestructura a servicios en la nube, por lo que, se han generado brechas de seguridad que no estaban contempladas bajo los esquemas de ciberseguridad para muchas áreas de tecnología con arquitecturas en las instalaciones. Dentro de la problemática que presenta la ciberseguridad en una organización, los integrantes del área de tecnología han mejorado sus capacidades para adaptarse a los cambios planteados y proteger sus activos de información. Trabajando de forma conjunta con grupos dedicados a la ciberseguridad desde el punto de vista del ataque en pruebas de penetración
Resumen de coincidencias
35 %
Coincidencia 1 de 1
1 Entregado a Universida... 20 %
Trabajo del estudiante
2 Entregado a Universida... 9 %
Trabajo del estudiante
3 repository.unad.edu.co 3 %
Fuente de Internet
4 www.coursehero.com <1 %
Fuente de Internet
5 sh1n0bi.github.io <1 %
Fuente de Internet
6 www.subredsur.gov.co <1 %
Fuente de Internet
7 Entregado a hogescho... <1 %
Página: 12 de 74
Número de palabras: 9254
Versión solo texto del informe
Alta resolución
Activado


SES40
Español - Internacional (es)
Menú de Accesibilidad
Gestión Administrativa
Gestión Académica
Mis cursos
Página Principal / Páginas del sitio / Mis cursos
Agenda del curso
Escuchar
Calendario
Vista general de curso
Todos
Buscar
Ordenar por nombre del curso
Tarjeta
TRABAJO DE GRADO II - (219024A_2034)
Category 1
100% completado