CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA LOS EQUIPOS REDTEAM Y BLUETEAM EN COLOMBIA

GUSTAVO ADOLFO GAMBOA GONZALEZ

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

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA LOS EQUIPOS REDTEAM Y BLUETEAM EN COLOMBIA

GUSTAVO ADOLFO GAMBOA GONZALEZ

Proyecto de Grado – Seminario Especializado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Yenny Stella Núñez
Directora de Curso

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

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, octubre 31 de 2021

CONTENIDO

pág.

INTRODUCCIÓN 11

1. DEFINICIÓN DEL PROBLEMA 12

1.1 ANTECEDENTES DEL PROBLEMA 12

1.2 FORMULACIÓN DEL PROBLEMA 12

2 JUSTIFICACIÓN 13

3 OBJETIVOS 14

3.1 OBJETIVOS GENERAL 14

3.2 OBJETIVOS ESPECÍFICOS 14

4 MARCO REFERENCIAL 15

4.1 MARCO TEÓRICO 15

4.2.1 RedTeam 15

4.2.2 Blueteam 15

4.2 MARCO CONCEPTUAL 16

4.3 MARCO HISTÓRICO 17

4.4 ANTECEDENTES O ESTADO ACTUAL 20

4.5 MARCO CIENTÍFICO O TECNOLÓGICO 20

4.6 MARCO LEGAL 20

5 DISEÑO METODOLÓGICO 22

6 DESARROLLO DE LOS OBJETIVOS 23

6.1 NORMATIVIDAD SOBRE DELITOS INFORMÁTICOS 23

6.2.1 Ley 1273 de 2009 23

6.2.2 Ley 1928 de 2018 25

6.2 EJECUCION DE PRUEBAS PESTESTING – RED TEAM 26

6.2.1 Fases de la prueba de la pluma 27

6.2.2 Componente practico 28

6.2.3 Wireshark 35

6.2.4 Suplantación de identidad – Spoofing 38

6.2.5 Prueba de Spoofing 39

6.2.6 Protocolos FTP / SFTP 44

6.3 PLAN DE CONTENCION – BLUE TEAM 60

6.2.1 Situación problema: Análisis Blue team 61

6.2.2 Acciones iniciales 61
6.2.3 Logs de eventos 62
6.2.4 Medidas de hardenización para que el ataque no se repita 65
6.2.5 CIS - Centro para la Seguridad de Internet 66
6.2.6 SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) 67
6.2.7 Acciones para contención de ataques informáticos:..... 68
7 CONCLUSIONES 71
8 RECOMENDACIONES 72
9 BIBLIOGRAFÍA 74
ANEXOS ..... *¡Error! Marcador no definido.*

TABLA DE FIGURAS

Figura 1 - Configuración MV Win7 28
Figura 2 - Configuración MV Kali Linux 29
Figura 3 - Configuración de red 30
Figura 4 - XAMPP Configuración Puerto 30
Figura 5 - XAMPP File config.txt 31
Figura 6 - XAMPP DB Server 31
Figura 7 - XAMPP File my.ini 32
Figura 8 - Kali Linux dirección IP 32
Figura 9 - Kali Linux Nmap Escaneo 33
Figura 10 - Kali Linux Escaneo puertos, servicios y versiones 33
Figura 11 - Kali Linux Version DB Server 34
Figura 12 - Kali Linux Puerto específico DB Server 34
Figura 13 - Wireshark Inicio ..... **¡Error! Marcador no definido.**
Figura 14 - Wireshark Interfaz 35
Figura 15 - Wireshark Campos 36
Figura 16 - Wireshark Dirección IP Web Server 37
Figura 17 - Wireshark Bytes 38
Figura 18 - Tomado de Imperva. Suplantación de DNS 38
Figura 19 - Actores Ataque 39
Figura 20 - Kali Linux Identificar direcciones IP atacante y víctima 39
Figura 21 - Ataque Spoofing DNS File Index 40
Figura 22 – Inicio Servicio Apache 40
Figura 23 - Evidencia Ataque 40
Figura 24 - File etter.dns 40
Figura 25 - Parametrización file etter 41
Figura 26 - Ettercap ejecución 41
Figura 27 - Ettercap Interfaz 41
Figura 28 - Ettercap listado hosts 42
Figura 29 – Ettercap target 42
Figura 30 - Ettercap ARP Poisoning 43
Figura 31 – Ettercap dns_spoof 43
Figura 32 - Spoofing evidencia ataque 44
Figura 33 - FTP Server Configuración 44
Figura 34 - FTP Permisos 45
Figura 35 - FTP Configuración Server 45
Figura 36 – Filezilla Cargue file 46
Figura 37 - Wireshark Análisis de trafico 46
Figura 38 - Pruebas Protocolo SFTP Terminal 47
Figura 39 - Pruebas Protocolo SFTP Openssh-server 47
Figura 40 - Pruebas Protocolo SFTP Creación grupo 47
Figura 41 - Pruebas Protocolo SFTP ID 48

Figura 42- Pruebas Protocolo SFTP Creacion User 48
Figura 43 - Pruebas Protocolo SFTP Copia fichero 48
Figura 44 - Pruebas Protocolo SFTP Modificación archivo 48
Figura 45 - Pruebas Protocolo SFTP Creacion directorio 49
Figura 46- Pruebas Protocolo SFTP Restart servicio 49
Figura 47- Pruebas Protocolo SFTP Dirección IP 49
Figura 48 - Filezilla Conexion SFTP 49
Figura 49 - Aceptar la conexion 50
Figura 50 - Filezilla configuramos sitio 50
Figura 51 - Análisis de tráfico wireshark 51

GLOSARIO

- VULNERABILIDAD: Es una debilidad que existe en el sistema de información, que pone en riesgo el activo más valioso de las organizaciones, permitiendo que un atacante afecte la integridad, disponibilidad o confidencialidad de esta.

- AMENAZA: Corresponde a un hecho, persona o incidente que podría generar daños a un sistema.

- RIESGO: Grado de presentación de un beneficio que permite la aparición de un peligro.

- BLUE TEAM: Equipo de seguridad informática que que tiene la misión de proteger y defender la empresa, realizando una vigilancia constante de los comportamientos fuera de lo común que se den día a día, tanto a nivel de usuario como a nivel de redes y sistemas de información. También establecen las respuestas en caso de incidentes.

- RED TEAM: Es el equipo encargado de simular a los atacantes, haciendo uso de las mismas herramientas o similares a la de los atacantes con el fin de explotar las vulnerabilidades de seguridad informática, con el fin de dar las bases de información al equipo de blue team para que este sepa cómo defenderse ante posibles ataques

- PENTESTING: se refiere a un ejercicio de ataque sobre un sistema informático con el propósito de hallar las vulnerabilidades de seguridad y tener acceso a ella.

- KALI LINUX: es una distribución de Linux cuyo propósito fundamental es la auditoría de sistemas informáticos.

- CIBERSEGURIDAD: es el grupo de procedimientos y herramientas que se concentran para brindar protección a la información que se genera y procesa a través de diferentes recursos informáticos.

RESUMEN

Muchas tácticas de ciberseguridad están inspiradas en los juegos de guerra militares, pero ninguna más que el redteam y blueteam. Una forma de piratería ética, equipos rojos y equipos azules implican que las empresas contraten a expertos en ciberseguridad altamente capacitados para infiltrarse en sus sistemas informáticos, redes y servidores. El objetivo de contratar a un pirata informático ético es fortalecer las defensas de ciberseguridad de la organización al encontrar y remediar las debilidades durante un ataque simulado y crear planes de respuesta a incidentes que se alineen con las condiciones del mundo real.

La formación de equipos rojos es un método desarrollado por el ejército alemán en el siglo XIX. Inicialmente, los oficiales militares usaban un juego de mesa que consistía en piezas de terreno y fichas de batalla para simular secuencias de batalla. La idea era dominar mejor los eventos impredecibles (conocidos como "fricciones") en los conflictos militares. En la ciberseguridad moderna, la formación de equipos rojos es una simulación de ataque de múltiples capas en toda regla diseñada para medir qué tan bien las redes de computadoras, las aplicaciones de software y los controles de seguridad física de una organización pueden resistir un ataque de un ciberdelincuente real.

ABSTRACT

This report sets out the techniques carried out by the DE RedTeam and BlueTeam teams to measure the security of an organization. In order to achieve the objectives, tasks were carried out based on the consultation of different repositories. Firstly, the RedTeam teams, their techniques to perform attacks seeking to exploit, compromise and circumvent the security of the system. In the case of the BlueTeam teams, techniques were used to detect and prevent different types of attacks, as well as to execute reactive or preventive actions.

Taking into account that a real company was not approached in the field, a controlled environment was enabled to simulate, in a real scenario, the techniques and behaviors of attackers that could occur through virtual machines in Linux and MS Windows in a didactic way and with evidence that allows us to test the maturity of the security of an organizational system, as well as its ability to detect and respond to an attack.

Currently there are many low-cost and even free tools to monitor our systems. Kali is a Linux OS distribution used for pentesting and ethical hacking, it is made up of security-related tools and focused on network and computer security professionals.

INTRODUCCIÓN

Este informe establece las técnicas llevadas a cabo por los equipos RedTeam y BlueTeam para medir la seguridad de una organización. Para la consecución de los objetivos se llevaron a cabo unas tareas basadas en la consulta de diferentes repositorios. En primer lugar, los equipos RedTeam, sus técnicas para realizar ataques buscando explotar, comprometer y eludir la seguridad del sistema. En el caso de los equipos BlueTeam se utilizaron técnicas que permitieron detectar y prevenir los diferentes tipos de ataques, así mismo ejecutar acciones reactivas ó preventivas.

Teniendo en cuenta que no se abordó una compañía real en campo, si se habilitó un entorno controlado para simular, en un escenario real, las técnicas y los comportamientos de atacantes que podrían darse a través de máquinas virtuales en Linux y MS Windows de una manera didáctica y con evidencias que nos permiten probar la madurez de la seguridad de un sistema organizacional, así como su capacidad para detectar y responder a un ataque.

Actualmente existen muchas herramientas de bajo costo e incluso gratuitas para monitorear nuestros sistemas. Kali es una distribución de Sistema Operativo Linux utilizada para pentesting y hacking ético, está conformada por herramientas ligadas con la seguridad y enfocada a profesionales en redes y seguridad informática.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El riesgo de ciberseguridad es la probabilidad de exposición o pérdida resultante de un ciberataque o violación de datos en su organización. Una definición mejor y más abarcadora es la pérdida o daño potencial relacionado con la infraestructura técnica, el uso de la tecnología o la reputación de una organización.

Las organizaciones se están volviendo más vulnerables a las amenazas cibernéticas debido a la creciente dependencia de computadoras, redes, programas, redes sociales y datos a nivel mundial. Las violaciones de datos, un ciberataque común, tienen un impacto comercial negativo masivo y, a menudo, surgen de datos insuficientemente protegidos. La conectividad global y el uso creciente de servicios en la nube con parámetros de seguridad predeterminados deficientes significan que el riesgo de ataques cibernéticos desde fuera de su organización está aumentando.

Ya no es suficiente depender de los Ingenieros de la tecnología de la información y los controles de seguridad tradicionales para la seguridad de la información. Hay una clara necesidad de herramientas de inteligencia de amenazas y programas de seguridad para reducir el riesgo cibernético de su organización y resaltar las posibles superficies de ataque.

Los encargados de la toma de decisiones deben realizar evaluaciones de riesgos al priorizar a los proveedores externos y tener una estrategia de mitigación de riesgos y un plan de respuesta a incidentes cibernéticos para cuando ocurra una infracción.

1.2 FORMULACIÓN DEL PROBLEMA

Aunque los controles generales de seguridad de TI son útiles, son insuficientes para brindar protección contra ataques cibernéticos frente a ataques sofisticados y una configuración deficiente.

¿Cómo se puede identificar y mitigar los riesgos asociados a la ciberseguridad en una organización?

2 JUSTIFICACIÓN

A continuación, indicaremos la justificación de las pruebas ejecutadas sobre equipos RedTeam y BlueTeam tomando como referencia las vulnerabilidades identificadas:

En primer lugar, se debe recurrir a una solución SFTP porque mantiene seguras las contraseñas y otra información confidencial, ya que esos datos se transfieren a través del canal seguro SSH. La seguridad de datos mejorada es el mayor beneficio de elegir el alojamiento SFTP como opción para compartir archivos. FTP por sí solo no proporciona ningún cifrado, por lo que los datos transferidos son tan fáciles de interceptar.

Las actualizaciones de software ofrecen muchos beneficios. Es absolutamente necesario instalar parches cuando estén disponibles, se trata de revisiones. Estos pueden incluir la reparación de los agujeros de seguridad que se han descubierto y la reparación o eliminación de errores informático. Los parches de seguridad evitan que los piratas informáticos y los ciberdelincuentes aprovechen las vulnerabilidades que podrían detener las operaciones.

El uso de contraseñas débiles, cambiar las contraseñas débiles con regularidad y usar una herramienta de administración de contraseñas. Implementar el bloqueo de intrusos después de un número definido de intentos fallidos de inicio de sesión. Desafortunadamente, un atacante también puede obtener la contraseña de usuario a través de ingeniería social, phishing o malware, por lo tanto, se debe asegurar de que los usuarios siempre utilicen contraseñas seguras. Esto se reduce a dos actividades: usar mecanismos de seguridad de contraseñas en su aplicación y probar contraseñas débiles.

Un firewall juega un papel vital en la seguridad de la red y debe configurarse correctamente para mantener a las organizaciones protegidas contra la fuga de datos y los ataques cibernéticos. La configuración incorrecta del firewall puede hacer que los atacantes obtengan acceso no autorizado a redes y recursos internos protegidos. Como resultado, los ciberdelincuentes buscan constantemente redes que tengan software o servidores obsoletos y que no estén protegidas.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Elaborar un informe técnico abordando los aspectos más relevantes de las capacidades técnicas, legales y de gestión para los equipos RedTeam y BlueTeam como estrategia a la seguridad de la información en Colombia.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar las leyes y códigos que apliquen a los delitos informáticos y al ejercicio de la profesión relacionada con la seguridad de la información.

- Ejecutar las pruebas pestesting bajo un escenario controlado para identificar las vulnerabilidades de un sistema.

- Establecer un plan de contención ante un ataque informático ejecutado en tiempo real por medio de herramientas que apoyen el proceso de contención y análisis de impacto.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.2.1 RedTeam

El equipo rojo usa una métodos y herramientas para ayudar a encontrar vulnerabilidades y debilidades en un sistema. Estos ejercicios incluyen simulación de adversarios, pruebas de penetración de caja negra y supuestos escenarios de infracción para generar recomendaciones para los hallazgos de vulnerabilidad. Los equipos rojos buscan explotar los controles de seguridad cibernética y los entornos corporativos por cualquier medio necesario, incluidos:

- Pruebas de penetración. Esto también se conoce como piratería ética e involucra a un evaluador que intenta obtener acceso a un sistema utilizando herramientas de software.
- Violación de seguridad física. Se trata de un pirata informático que intenta obtener acceso físico a una computadora o sistema, en persona.
- Acceso inalámbrico. El acceso inalámbrico implica a los equipos rojos que intentan acceder a un sistema de forma remota.
- Explotaciones de Active Directory. Un exploit del directorio activo es cuando un equipo rojo utiliza el directorio para obtener acceso a los derechos de dominio.
- Explotaciones de correo electrónico y phishing. Estas tácticas se utilizan para intentar que los miembros de la empresa inicien sesión en sitios web de spam, proporcionen sus credenciales y más.
- Servidores de archivos vulnerables. Los equipos rojos encontrarán servidores de archivos vulnerables e intentarán explotarlos para obtener acceso a todo el sistema.
- Puntos finales vulnerables. Los equipos rojos pueden utilizar puntos finales vulnerables para trabajar en su camino de regreso a través de un sistema.
- Técnicas apropiadas de ingeniería social para el acceso. Esto involucra a un equipo rojo que usa amenazas, recompensas atractivas, alarmas y más para intentar obtener acceso.
- Vulnerabilidades conocidas (conocimiento común). Los equipos rojos pueden usar vulnerabilidades conocidas en una organización para ingresar o explotar a los miembros del equipo para obtener acceso.

4.2.2 Blueteam

Los equipos azules en ciberseguridad evalúan y analizan constantemente los sistemas de seguridad para aplicar parches, identificar fallas de seguridad,

problemas de configuración relevantes para la seguridad y verificar el impacto de los controles de seguridad

Los equipos azules realizan todas las funciones del SOC (centro de operaciones de seguridad) y generalmente son responsables de la gestión de eventos, seguimiento de incidentes, inteligencia de amenazas, captura y análisis de paquetes y automatización de la seguridad.

- Protección de endpoints
- Registro (recopilación, análisis y normalización)
- NSM por capa de red
- Conceptos de monitoreo continuo de seguridad (CSM)
- Colección de eventos CSM
- Centralización de datos
- Eventos, alertas, anomalías e incidentes
- Sistemas de gestión de incidentes
- Plataformas de inteligencia de amenazas
- Triaje y análisis
- Sintonización de alertas
- Automatización de seguridad

4.2 MARCO CONCEPTUAL

Un ejercicio de equipo rojo es un esfuerzo “total” para penetrar las defensas de seguridad de una organización. El objetivo es obtener acceso a los sistemas a través de violaciones físicas, redes informáticas, sistemas telefónicos, sistemas de RF (radiofrecuencia) y manipulación de los empleados. El equipo rojo está confirmado por profesionales de hacking éticos cualificados donde su trabajo es lanzar ataques controlados en las áreas de seguridad física y cibernética del objetivo. Los miembros del equipo son contratados externamente y no están conectados a la organización objetivo. El objetivo del equipo rojo es montar un ataque muy realista contra la organización objetivo. Los ataques pueden ocurrir de forma rápida e inesperada, lo que hace que sea muy difícil para el equipo azul neutralizar la amenaza antes de que el equipo rojo logre su objetivo. Aprovecharán fácilmente las debilidades y los errores. En los sistemas de su objetivo para mostrar brechas en su infraestructura técnica. En última instancia, estas brechas pueden subsanarse para mejorar la postura de seguridad general de la organización.

El equipo azul está formado por el personal de seguridad interno de la empresa, a menudo desde su Centro de Operaciones de Seguridad (SOC). El SOC está conformado por profesionales muy bien preparados cuyo trabajo es mejorar las defensas de su organización, trabajando 24 horas al día, 7 días a la semana.

El objetivo del equipo azul es detectar, contrarrestar y debilitar al equipo rojo. El equipo azul identificará y neutralizará ataques más sofisticados. Supervisarán cuidadosamente las amenazas identificadas y emergentes para defender su organización de forma preventiva. El equipo azul debe comprender cada fase de un incidente, incluidos los patrones de tráfico sospechosos y otros indicadores de compromiso. Deben responder en consecuencia, cerrando rápidamente cualquier amenaza. Deben identificar los servidores de comando y control del actor de la amenaza (equipo rojo) y bloquear su conectividad con el objetivo. El equipo azul realizará pruebas y análisis forenses de los diversos sistemas operativos de su organización, incluidos los sistemas de terceros. Realizarán análisis de tráfico y flujo de datos mediante la revisión de los datos de registro.

Ejecutar pruebas de redteam y blueteam es una manera segura de robustecer la seguridad de TI de una compañia y ciberseguridad con sus las defensas. Cuando estas pruebas se ejecutan de manera correcta, es posible que no exista mejor forma de emular las amenazas que sufren las organizaciones diariamente.

4.3 MARCO HISTÓRICO

Los ejercicios del equipo rojo-azul toman su nombre de sus antecedentes militares. La idea es simple: un grupo de profesionales de seguridad, un equipo rojo, ataca algo y un grupo contrario, el equipo azul, lo defiende. Originalmente, los ejercicios fueron utilizados por los militares para probar la preparación de la fuerza. También se han utilizado para probar la seguridad física de sitios sensibles como instalaciones nucleares y los Laboratorios y Centros Tecnológicos Nacionales del Departamento de Energía. En los años 90, los expertos comenzaron a usar ejercicios de equipo rojo-azul para realizar pruebas sobre los sistemas de seguridad de informática.

"Realmente, esta es una capacidad y experiencia que se desarrolló naturalmente aquí a partir de la misión del laboratorio como uno de los laboratorios de la agencia nacional de seguridad nuclear", dice John Clem, gerente de programa del Equipo Rojo de Garantía de Diseño de Información en el Laboratorio Nacional Sandia del DoE. Los expertos de Sandia ayudaron a asesorar a la Comisión Presidencial sobre Protección de Infraestructuras Críticas en la década de 1990, lo que llevó al grupo actual a centrarse en la seguridad de la información. El equipo de Clem ha "unido" la infraestructura de Sandia y ha trabajado con otras agencias federales y, como parte de la misión de protección de la infraestructura del laboratorio, el equipo también trabaja con empresas del sector privado. Clem destaca la opinión generalizada de que el 85 por ciento de la infraestructura crítica de Estados Unidos es propiedad de empresas privadas. Estas empresas mantienen refinerías de petróleo, plantas de energía nuclear y proveedores de telecomunicaciones funcionando de forma segura. Los investigadores del Laboratorio Nacional de Idaho ofrecen un servicio similar al de Sandia, a veces construyen bancos de pruebas modelo para imitar la red de una empresa.

Sin embargo, las empresas de cualquier industria pueden beneficiarse de un ejercicio de equipo rojo-azul. SANS organizó un evento de guerra cibernética en sus entrenamientos de Las Vegas de 2007 en el que un equipo rojo atacó a una empresa falsa a la que llamó GIAC Enterprises, supuestamente el mayor proveedor mundial de fortunas para galletas de la fortuna. En febrero de este año, eBay realizó un ejercicio de equipo rojo con varios CISO y proveedores invitados. Para aquellos que se perdieron el ataque de la galleta de la fortuna o la confabulación de eBay, hemos recopilado consejos sobre cómo aprovechar al máximo su propia simulación de equipo rojo-azul de seguridad de la información.

"Empiezo por reunir al personal de administración y seguridad en la misma sala", dice Michael Assante, estratega de protección de infraestructura del Laboratorio Nacional de Idaho (INL). "Pido al equipo de seguridad que haga un análisis exhaustivo de lo que tenemos en marcha". Esta es una de las formas más fáciles de identificar vulnerabilidades de seguridad y también ayuda con un problema clave para cualquier ejercicio exitoso de equipo rojo-azul: compre. Sí, es una de las frases más usadas en el vocabulario de un consultor, pero la aprobación de la gerencia y los empleados es esencial cuando se prueban los sistemas de seguridad de la información.

El objetivo de un ejercicio de equipo rojo-azul no es solo identificar los agujeros en la seguridad, sino capacitar al personal y la gerencia de seguridad. Si no todo el mundo está de acuerdo con el valor del ejercicio, rápidamente puede convertirse en una postura defensiva y una pérdida de tiempo. Después de todo, es posible que esté pidiendo a los superiores el tiempo y el presupuesto necesarios para corregir los defectos que descubra el ejercicio. Una evaluación inicial puede identificar cambios que deben realizarse. Entonces, es hora de empezar.

La versión más simple de un ejercicio de equipo rojo-azul requiere poco más que una mesa de conferencias. Divida a su personal de seguridad en equipos y pase una tarde hablando de posibles escenarios de ataque y defensa. El elemento clave para el éxito es un equipo rojo que pueda adoptar la mentalidad de un atacante.

"La formación de equipos rojos es un proceso de pensamiento", explica Tom Anderson de INL. "El problema de que las personas que construyeron [el sistema de seguridad] lo hagan es que tienen interés en protegerlo". Para combatir el interés personal y la homogeneidad, Anderson y Assante crean equipos diversificados donde los expertos de INL trabajan junto con el personal de la empresa a la que asisten.
Eso no quiere decir que no pueda hacerlo por su cuenta, pero es importante al menos tratar de pensar como un extraño. "Muchas veces, cuando desarrollamos sistemas de seguridad, es para que la persona honesta sea honesta", explica Assante. Un atacante ignorará más que las reglas; él o ella ignorará las normas de la empresa. Considere quiénes pueden ser sus atacantes. Las centrales eléctricas pueden ser blanco de terroristas. Bancos por delincuentes. Cualquiera por un ex empleado descontento. Puede llevar tiempo y esfuerzo dar un paso atrás y ver el sistema como un extraño, o incluso un interno que tiene la intención de hacer daño.

Uno de los valores de un ejercicio de mesa es que permite a los jugadores considerar el sistema como un todo. Es poco probable que la gran parte de las empresas que no albergan materiales nucleares realicen ejercicios físicos a gran escala con las fuerzas armadas asaltando su edificio, pero es importante tener en cuenta la seguridad física al desarrollar ataques de pizarra.

"Los sistemas físicos tienen que proteger los cibersistemas, y los cibersistemas tienen que proteger los sistemas físicos", dice Ray Parks, líder del Sandia Red Team. "Lo primero que me dicen los chicos que diseñan sistemas de seguridad física es, por lo general, que la columna vertebral de nuestra seguridad es un gigabit Ethernet". Elimine eso (mediante un ataque cibernético o físico) y, de repente, el sistema de control de acceso físico está fuera de servicio. El ejercicio de la sala de conferencias es especialmente importante para las empresas que nunca antes han intentado un ejercicio de equipo rojo-azul. "Con solo hacer un ejercicio de mesa, puede aprender mucho sobre su riesgo", dice Assante.

Y, por extraño que parezca, mantener las cosas hipotéticas brinda una oportunidad de aprendizaje que un ataque cibernético real por parte de profesionales de alto nivel puede no tener. En un artículo reciente, Greg B. White, director del Center for Infrastructure Assurance and Security, calificó los ataques del equipo rojo contra objetivos verdaderamente no preparados como "aproximadamente equivalentes a los reclutas del ejército que intentan defender una instalación de un grupo de fuerzas paramilitares de élite". , los reclutas se darían cuenta de que no estaban preparados, pero el ejercicio no les proporcionaría ningún entrenamiento para prepararlos ".

Un ejercicio de mesa brinda la oportunidad de reflexionar y evaluar las opciones de respuesta, así como los ataques. Y luego piense en lo que podrían significar las posibles infracciones. Sin embargo, una vez que haya arreglado los agujeros que identificaron sus ejercicios de pizarra, un ejercicio de ataque y defensa en vivo puede proporcionar un nivel completamente nuevo de conocimiento, pero no es una actividad que debamos tomar a la ligera. En algunos casos, las vulnerabilidades se pueden demostrar de forma segura en una red corporativa activa, pero no es aconsejable lanzar un ataque real contra sus sistemas de producción.
Assante dice que en Idaho National Labs, su equipo ha construido bancos de prueba específicos para el cliente que imitan la red real de la empresa para ofrecer lo que él llama "capacitación inmersiva facilitada". Algunos miembros del personal de seguridad y de red intentan defender la red, mientras que otros se unen a los compañeros del equipo rojo de Assante para atacarla.

"Esto le da confianza al equipo azul, a los defensores", dice Assante. "También es muy útil para el equipo rojo. Ves las vulnerabilidades bajo una luz completamente nueva. Y ellos traen esa capacitación" a sus compañeros de trabajo.

4.4 ANTECEDENTES O ESTADO ACTUAL

Teniendo en cuenta que no se aborda una organización real, se considera que el escenario controlado cuenta con los equipos, recursos, condiciones para llevar a cabo las pruebas por el equipo rojo y la capacidad de contener y elaborar un plan de acción por parte del equipo azul.

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

Los equipos rojos comienzan recopilando información sobre la pila de tecnología del objetivo. Comenzarán por descubrir qué sistemas operativos están en uso (por ejemplo: Windows, macOS o Linux), cada uno de los cuales tiene sus propias debilidades, identificando la marca y el modelo del equipo de red. Si planean perpetrar un ataque físico en persona, como robar un disco duro, en lugar de montar un ataque remoto, también investigarán qué controles físicos existen, como puertas, cerraduras, cámaras y personal de seguridad.

- Pruebas de penetración: ciberataques simulados configurados en torno a un conjunto de objetivos de prueba.
- Ingeniería social: manipular psicológicamente a alguien para que divulgue información confidencial.
- Phishing: ponerse en contacto con una víctima por teléfono, correo electrónico o mensaje de texto mientras pretende representar a una organización legítima.
- Interceptar herramientas de software de comunicación: Interceptar correos electrónicos, llamadas telefónicas y otras comunicaciones electrónicas para ver su contenido.
- Clonación de tarjetas: robar datos de tarjetas de pago con chips EMV y usarlos para crear tarjetas de banda magnética.

Los equipos azules suelen estar formados por consultores de respuesta a incidentes que asesoran a los equipos de TI sobre cómo responder a los ciberataques. Antes de un ataque, el equipo azul reúne datos, define cuales sistemas deben protegerse y ejecutar una evaluación de riesgos. Una evaluación de riesgos es el proceso de identificar y analizar amenazas potenciales. Luego trabajan para establecer medidas de seguridad para proteger los activos clave de la organización.

4.6 MARCO LEGAL

Antes de analizar la legislación y normativa de seguridad informática que aplica al problema seleccionado vamos primero a tener claridad sobre el perfil de un ciberdelincuente. Los ciberdelincuentes cuentan con habilidades que los delincuentes tradicionales no tienen, es decir, cuentan con altas competencias en el manejo de

sistemas informáticos y usualmente tienen fácil acceso a información sensible y clasificada.

Al leer las fuentes disponibles se identifican estudios realizados los cuales afirman que los ciberdelincuentes no actúan solos, sino que en muchos casos operan para organizaciones criminales en todo el mundo que especialmente atacan al sector financiero y a los gobiernos, como dato estadístico se tiene que Norteamérica y Sudamérica suman el 19% del total de ataques a escala mundial.

RICSH afirma: “Cualquier persona con conocimientos suficientes de seguridad informática e impulsado por ansias económicas puede prestar su labor a empresas de seguridad o usarlo para su propio beneficio. Estas personas se sienten orgullosas cuando demuestran sus habilidades, de modo que su grado de autorrealización es más elevado cuando mayor es el impacto del perjuicio provocado”.

Cada una de las leyes las abordaremos más adelante en el desarrollo del objetivo 1.

5 DISEÑO METODOLÓGICO

Para la consecución de los objetivos se llevaron a cabo unas tareas basadas en la consulta de diferentes repositorios. En primer lugar, los equipos RedTeam, sus técnicas para realizar ataques buscando explotar, comprometer y eludir la seguridad del sistema. En el caso de los equipos BlueTeam se utilizaron técnicas que permitieron detectar y prevenir los diferentes tipos de ataques, así mismo ejecutar acciones reactivas ó preventivas.

Teniendo en cuenta que no se abordó una compañía real en campo, si se habilitó un entorno controlado para simular, en un escenario real, las técnicas y los comportamientos de atacantes que podrían darse a través de máquinas virtuales en Linux y MS Windows de una manera didáctica y con evidencias que nos permiten probar la madurez de la seguridad de un sistema organizacional, así como su capacidad para detectar y responder a un ataque.

6 DESARROLLO DE LOS OBJETIVOS

6.1 NORMATIVIDAD SOBRE DELITOS INFORMÁTICOS

6.2.1 Ley 1273 de 2009

En relación a los delitos informáticos y su regulación, Colombia dio un gran paso con la creación de la ley 1273 del 2009. Con esta norma se amplía el código penal para la protección de la información y de los datos, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones. A continuación, los artículos que la conforman y su interpretación:

- *Artículo 269A*. Complementa el acceso abusivo a un sistema informático, que se manifiesta cuando el pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de la información.

- *Artículo 269B*. Hace referencia como delito la obstaculización ilegítima del sistema informático o red de telecomunicación, y se origina cuando el hacker informático bloquea en forma ilegal un sistema o impide su ingreso por un tiempo, hasta cuando obtiene un beneficio por lo general económico. Aquí también se enmarca el acceso a cuentas de correo electrónico sin el debido consentimiento de sus propietarios y el manejo o bloqueo de las claves obtenidas de distinta forma.

- *Artículo 269C.* Aborda la interceptación ilícita de datos informáticos, Se origina cuando una persona, valiéndose de los recursos tecnológicos, obstruye datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático, o de emisiones electromagnéticas de un sistema electromagnético que los transporte.

- *Artículo 269D.* Se refiere al delito relacionado con los daños informáticos el cual se comete cuando una persona que, sin estar autorizada, modifica, altera, daña, borra, destruye o suprime datos del programa o de documentos electrónicos.

- *Artículo 269E.* En los recursos de las TIC, contempla el delito vinculado con el uso de software malicioso técnicamente denominado malware, ya generalizado en internet. Se presenta cuando se producen, adquieren,

venden, distribuyen, envían, introducen o extraen del país software o programas de computador que causen daños en los recursos de las TIC.

- *Artículo 269F.* El delito sobre violación de datos personales y está orientado a proteger los derechos fundamentales de la persona como dignidad humana y libertad ideológica. Se presenta cuando un individuo sin estar facultado, sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en ficheros, archivos, bases de datos o medios similares con el fin de lograr utilidad personal o para otros.

- *Artículo 269G.* Trata de la suplantación de sitios web para capturar datos personales. Sucede cuando el suplantador (phisher)8 o delincuente informático crea una página y un dominio similar al de la entidad a la cual desea abordar, lo ubica en un hosting (espacio en un servidor) desde donde envía correos spam9 o engañosos. Al no distinguir la página original de la falsa, las personas inocentemente suministran información personal y claves bancarias que el suplantador almacena en una base de datos y luego ordena la transferencia del dinero de la víctima a cuentas de terceros quienes prestan sus cuentas o servicios (testaferros), que luego reclama o distribuye.

- *Artículo 269H.* Circunstancias de agravación punitiva, las penas imponibles de acuerdo con los artículos descritos en esta ley, se aumentarán de la mitad a las tres cuartas partes.

- *Artículo 269I.* Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta 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.

- *Artículo 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.

6.2.2 Ley 1928 de 2018

En noviembre de 2001 Colombia empezó a formar parte del Convenio De Budapest, el cual fue el primer tratado internacional en la historia de la humanidad sobre ciberdelincuencia, actualmente está confirmado por 41 países más. El objetivo que buscan los países con este acuerdo está basado en la necesidad de "prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos". De la ley 1928 de 2018 vamos a destacar estos artículos:

- *Artículo 3. Interceptación Ilícita.*
  Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

- *Artículo 4. Interferencia En Los Datos.*
  Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

- *Artículo 5. Interferencia En El Sistema.*
  Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

- *Artículo 7. Falsificación Informática.*
  Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención

fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

- *Artículo 8. Fraude Informático.*
  Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:
  a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;
  b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

6.2 EJECUCION DE PRUEBAS PESTESTING – RED TEAM

Una prueba de penetración es un ataque simulado autorizado que se realiza en un sistema informático para evaluar su seguridad. Los probadores de penetración utilizan las mismas herramientas, técnicas y procesos que los atacantes para encontrar y demostrar los impactos comerciales de las debilidades de sus sistemas.

Las pruebas de penetración generalmente simulan una variedad de ataques diferentes que podrían amenazar su negocio. Una prueba de penetración podría examinar si un sistema es lo suficientemente robusto para resistir ataques desde posiciones autenticadas y no autenticadas, así como una variedad de funciones del sistema. Con el alcance adecuado, una prueba de lápiz puede sumergirse en cualquier aspecto de un sistema que necesite evaluar.

El equipo rojo usa una métodos y herramientas para ayudar a encontrar vulnerabilidades y debilidades en un sistema. Estos ejercicios incluyen simulación de adversarios, pruebas de penetración de caja negra y supuestos escenarios de infracción para generar recomendaciones para los hallazgos de vulnerabilidad. Los equipos rojos buscan explotar los controles de seguridad cibernética y los entornos corporativos por cualquier medio necesario, incluidos:

- Pruebas de penetración. Esto también se conoce como piratería ética e involucra a un evaluador que intenta obtener acceso a un sistema utilizando herramientas de software.
- Violación de seguridad física. Se trata de un pirata informático que intenta obtener acceso físico a una computadora o sistema, en persona.
- Acceso inalámbrico. El acceso inalámbrico implica a los equipos rojos que intentan acceder a un sistema de forma remota.

- Explotaciones de Active Directory. Un exploit del directorio activo es cuando un equipo rojo utiliza el directorio para obtener acceso a los derechos de dominio.
- Explotaciones de correo electrónico y phishing. Estas tácticas se utilizan para intentar que los miembros de la empresa inicien sesión en sitios web de spam, proporcionen sus credenciales y más.
- Servidores de archivos vulnerables. Los equipos rojos encontrarán servidores de archivos vulnerables e intentarán explotarlos para obtener acceso a todo el sistema.
- Puntos finales vulnerables. Los equipos rojos pueden utilizar puntos finales vulnerables para trabajar en su camino de regreso a través de un sistema.
- Técnicas apropiadas de ingeniería social para el acceso. Esto involucra a un equipo rojo que usa amenazas, recompensas atractivas, alarmas y más para intentar obtener acceso.
- Vulnerabilidades conocidas (conocimiento común). Los equipos rojos pueden usar vulnerabilidades conocidas en una organización para ingresar o explotar a los miembros del equipo para obtener acceso.

6.2.1 Fases de la prueba de la pluma

Los probadores de lápiz tienen como objetivo simular ataques llevados a cabo por adversarios motivados. Para hacerlo, normalmente siguen un plan que incluye los siguientes pasos:

- Reconocimiento. Reúna tanta información sobre el objetivo como sea posible de fuentes públicas y privadas para informar la estrategia de ataque. Las fuentes incluyen búsquedas en Internet, recuperación de información de registro de dominio, ingeniería social, escaneo de red no intrusivo y, a veces, incluso inspección en la basura.
- Exploración. El probador de lápiz utiliza herramientas para examinar el sitio web o el sistema de destino en busca de debilidades, incluidos servicios abiertos, problemas de seguridad de las aplicaciones y vulnerabilidades de código abierto. Los probadores de lápiz utilizan una variedad de herramientas basadas en lo que encuentran durante el reconocimiento y durante la prueba.
- Ganando acceso. Las motivaciones de los atacantes varían desde robar, cambiar o eliminar datos hasta mover fondos o simplemente dañar su reputación. Para realizar cada caso de prueba, los probadores de lápiz deben decidir las mejores herramientas y técnicas para obtener acceso a su sistema, ya sea a través de una debilidad, como la inyección SQL, o mediante malware, ingeniería social u otra cosa.
- Mantener el acceso. Una vez que los probadores de penetración obtienen acceso al objetivo, su ataque simulado debe permanecer conectado el

tiempo suficiente para lograr sus objetivos: extraer datos, modificarlos o abusar de la funcionalidad. Se trata de demostrar el impacto potencial.

6.2.2 Componente practico

Un servidor web y base de datos:

Windows 7 – MV_GUSTAVO_GAMBOA_WIN7

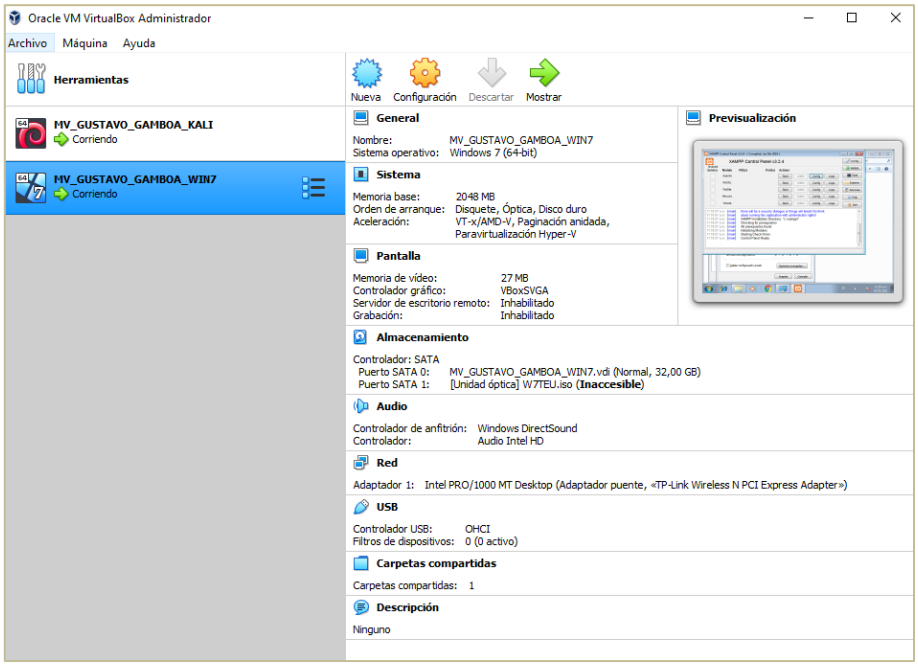


Figura 1 - Configuración MV Win7

Una maquina Kali Linux que se encarga de revisar el comportamiento de la red en los momentos de los ataques:

Mv_Gustavo_Gamboa_Kali

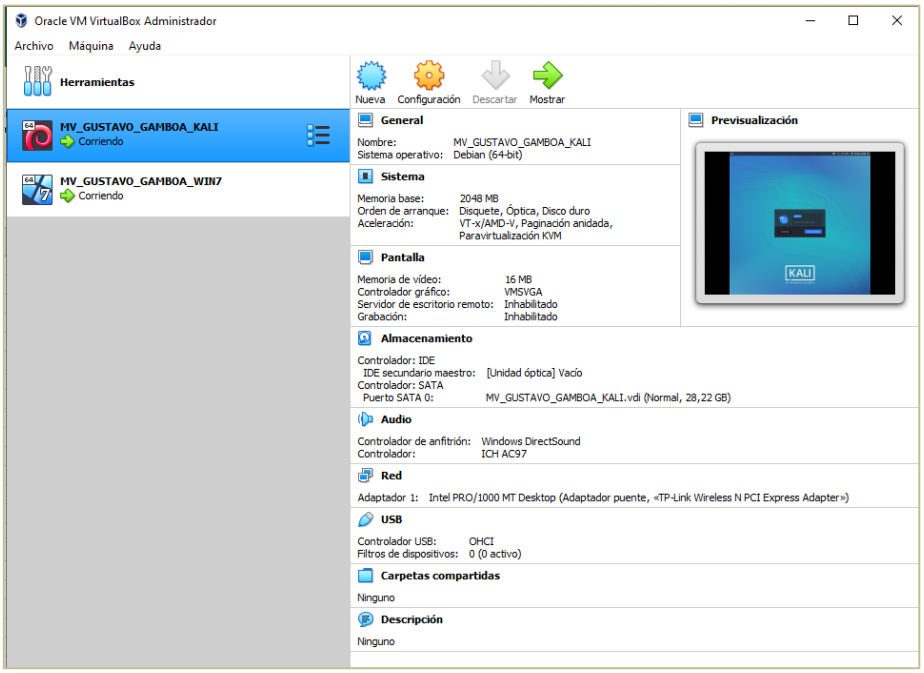


Figura 2 - Configuración MV Kali Linux

Configuración de red:

Nombre Maquina Virtual	Rol	SO	Direccion IP
MV_GUSTAVO_GAMBOA_WIN7	Servidor Web y Base de datos	Windows 7	192.168.0.3
MV_GUSTAVO_GAMBOA_KALI	Revisar el comportamiento de la red en los momentos de los ataques	Kali Linux	192.168.0.16

Configurar los servidores web y de bases de datos, con los parámetros de IP y puerto indicados en la tabla 1 y grafica 1.

Asignacion IP servidor web con ID (ultimo digito de mi cedula **3**):

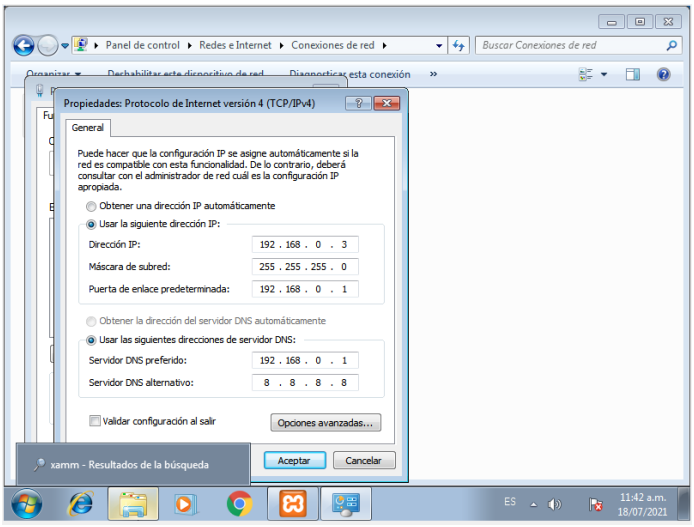


Figura 3 - Configuración de red

Configuración puerto servidor web, a pesar de que la guía define una estructura para el puerto 80_ID, sería 80_3, sin embargo, no corresponde a un puerto valido por lo que trabajaremos con el puerto 80:

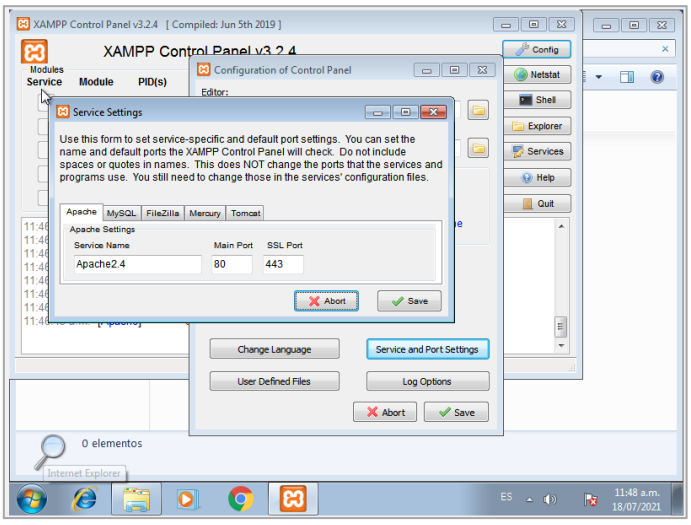


Figura 4 - XAMPP Configuración Puerto

También debemos abrir el archivo httpd.conf y validar el puerto:

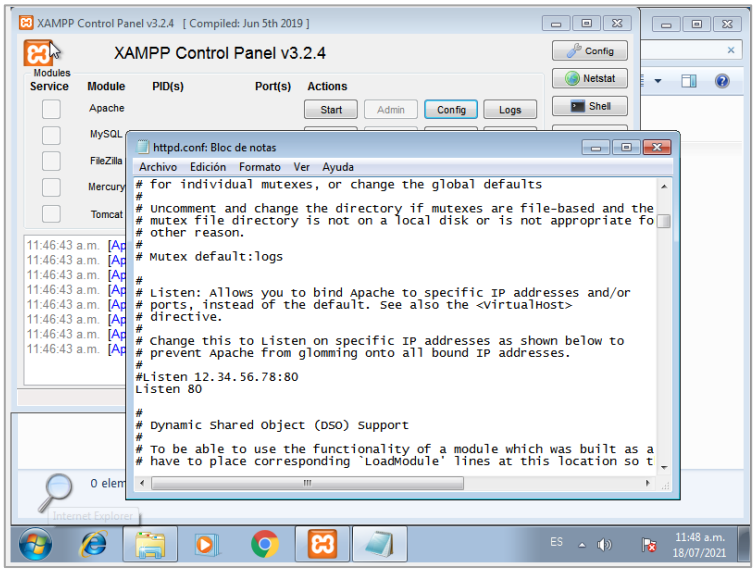


Figura 5 - XAMPP File config.txt

Configuración puerto servidor base de datos, trabajaremos con el puerto 3306:

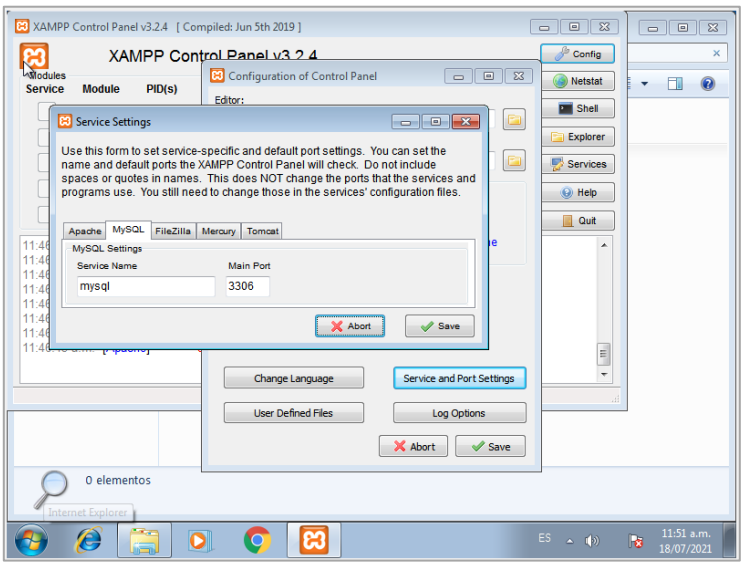


Figura 6 - XAMPP DB Server

También debemos abrir el archivo my.ini y validar el puerto:

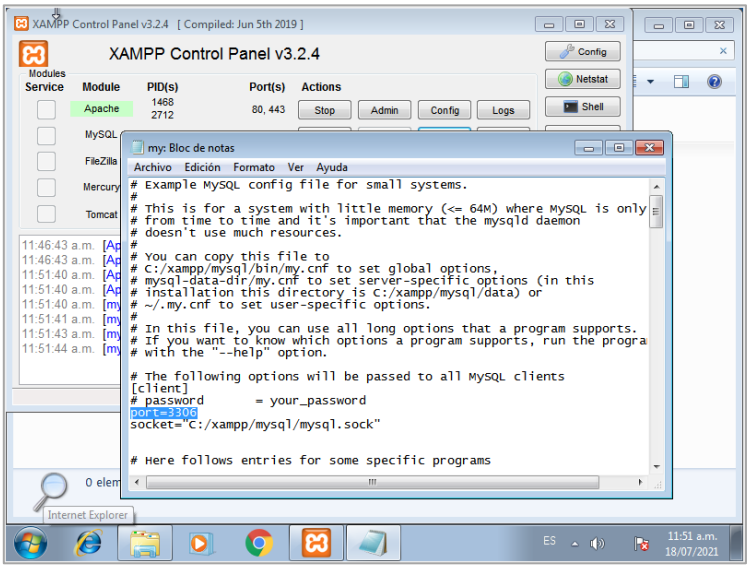


Figura 7 - XAMPP File my.ini

Describir la forma en que NMAP averigua IP, puerto y la versión del servidor web (por ejemplo, Apache).

Ejecutamos nuestra MV en Kali Linux y confirmamos nuestra dirección IP:

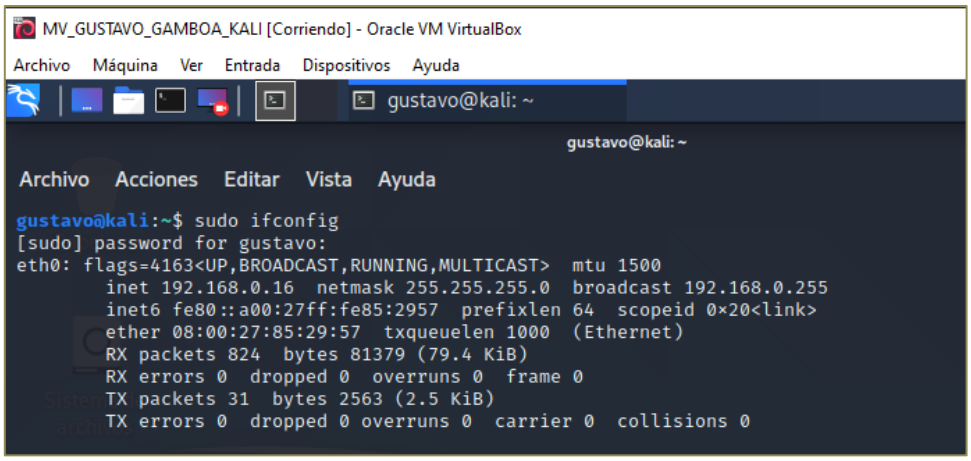


Figura 8 - Kali Linux dirección IP

Ahora realizamos un escaneo de los dispositivos conectados a la red:

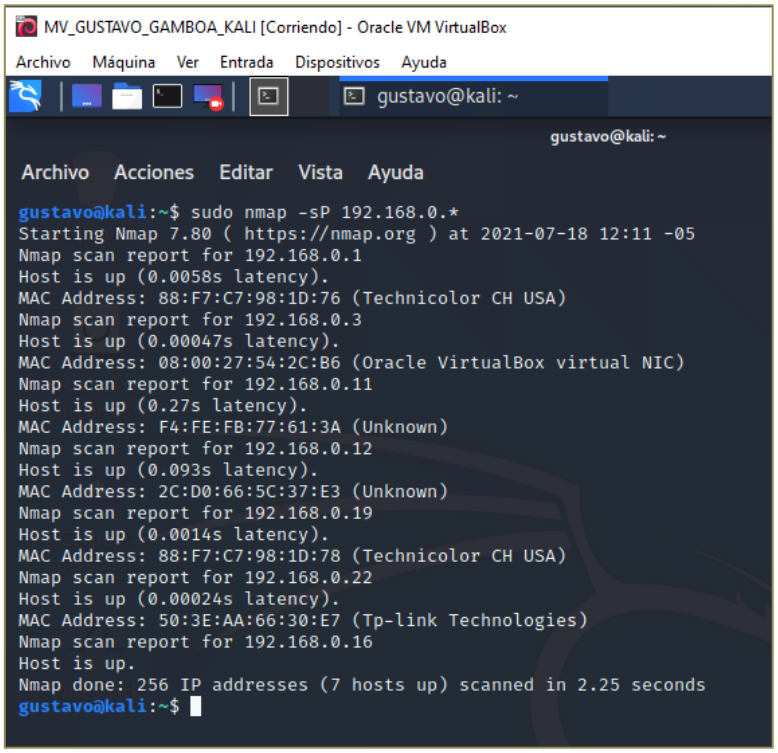


Figura 9 - Kali Linux Nmap Escaneo

Con el comando nmap -O -sV 192.168.10.3, vamos a detectar puertos, estado, servicio y versión de nuestro servidor web:

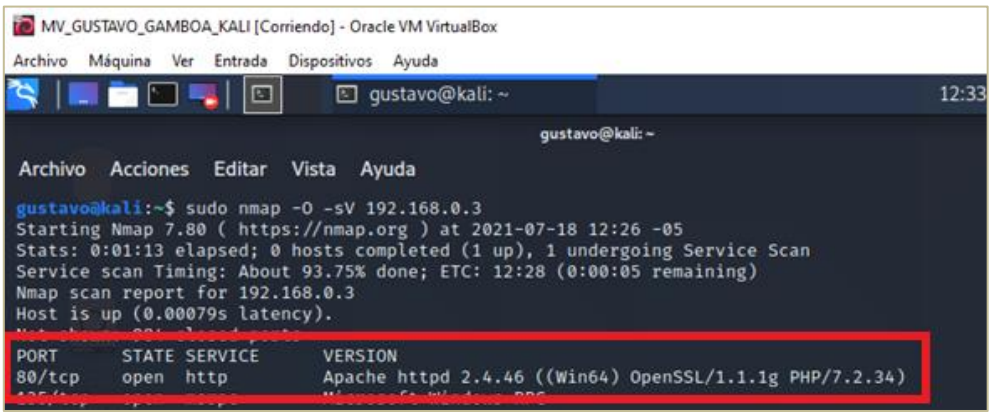


Figura 10 - Kali Linux Escaneo puertos, servicios y versiones

Describir la forma en que NMAP averigua IP, puerto y la versión usada en el servidor de bases de datos (por ejemplo, MySQL). Con el comando nmap -O -sV 192.168.10.3, vamos a detectar puertos, estado, servicio y versión de nuestro servidor de base de datos:

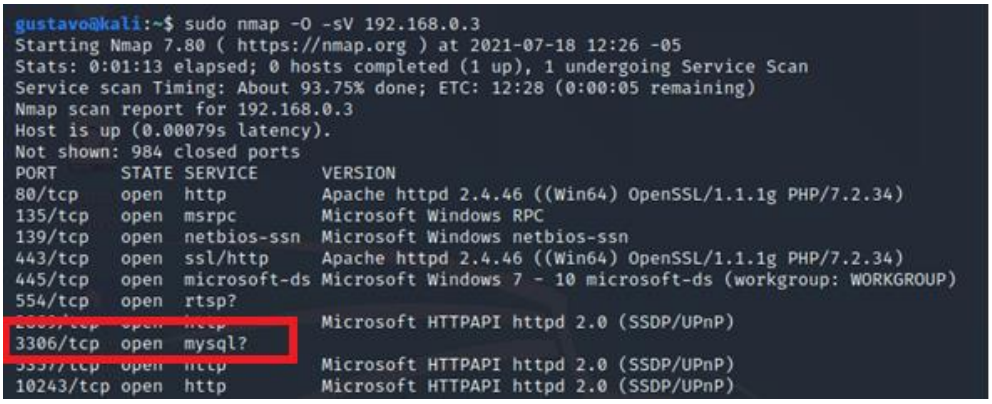


Figura 11 - Kali Linux Version DB Server

También podemos ejecutar el comando nmap -sV -n -p 33606 192.168.10.3, para en el puerto especifico, estado, servicio y versión de nuestro servidor de base de datos:

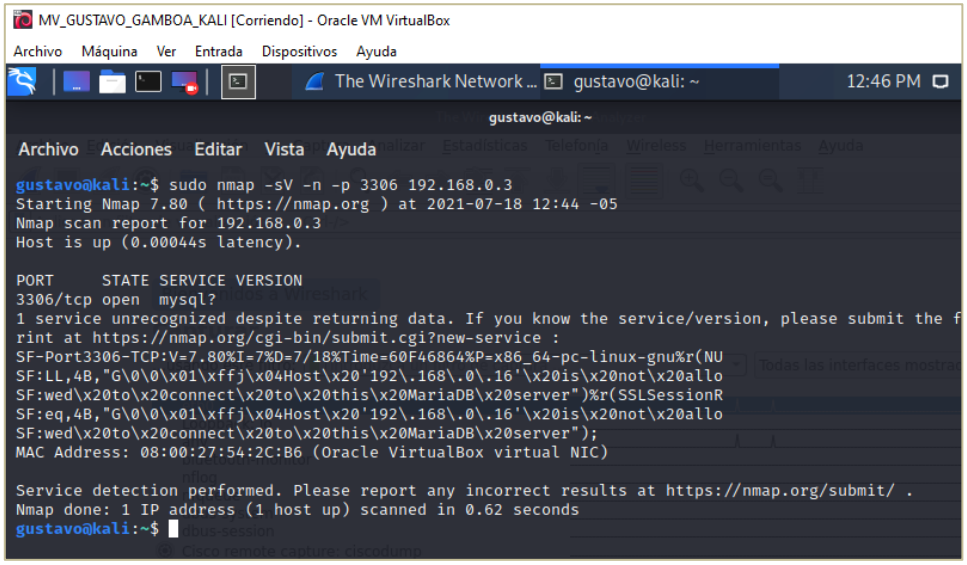


Figura 12 - Kali Linux Puerto específico DB Server

6.2.3 Wireshark

Wireshark viene incluido en la distribución de Kali Linux, iniciamos de nuestra máquina virtual y los buscamos en el inicio y ejecutamos:

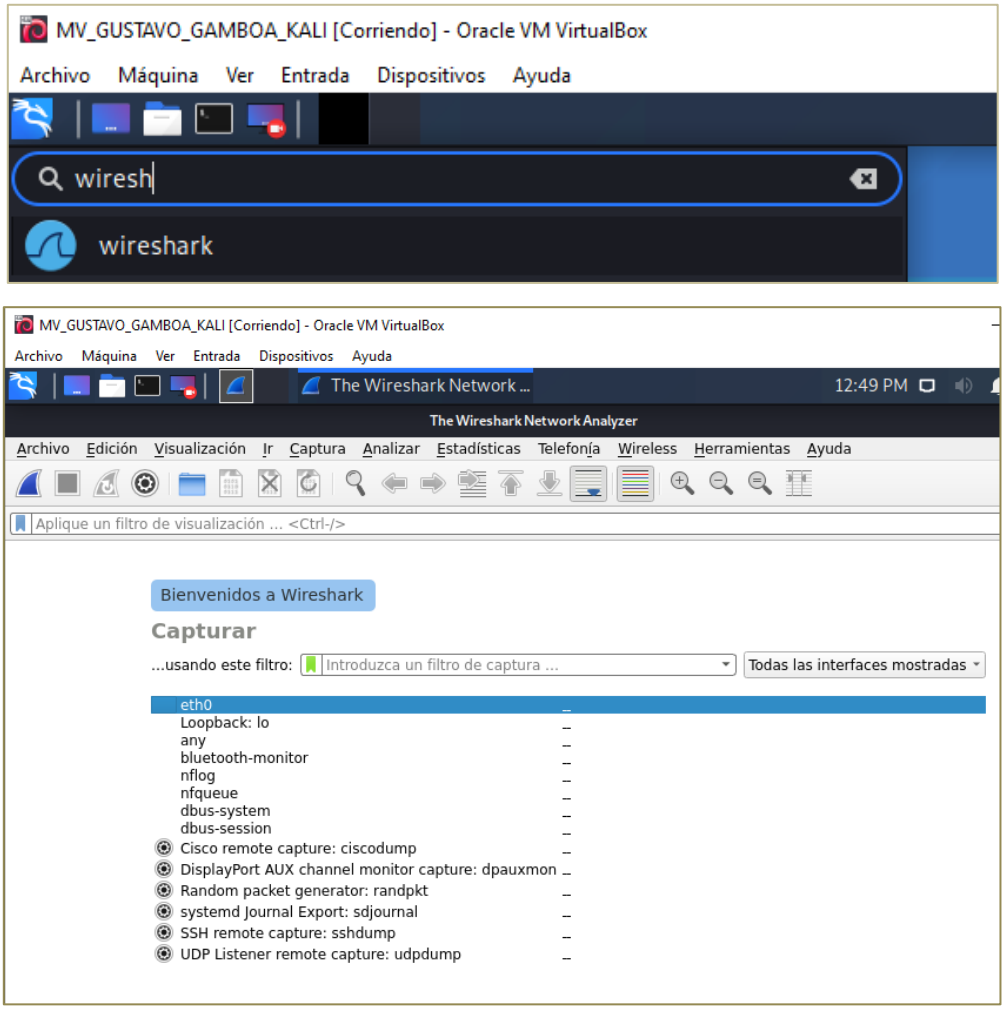


Figura 13 - Wireshark Interfaz

Inspeccionamos todo el tráfico donde podemos apreciar las direcciones IPs de nuestras máquinas virtuales e incluso otros dispositivos conectados a la misma red. La interfaz de datos capturados contiene tres secciones principales:

a. El panel de la lista de paquetes (la sección superior)
b. El panel de detalles del paquete (la sección central)
c. El panel de bytes del paquete (la sección inferior)

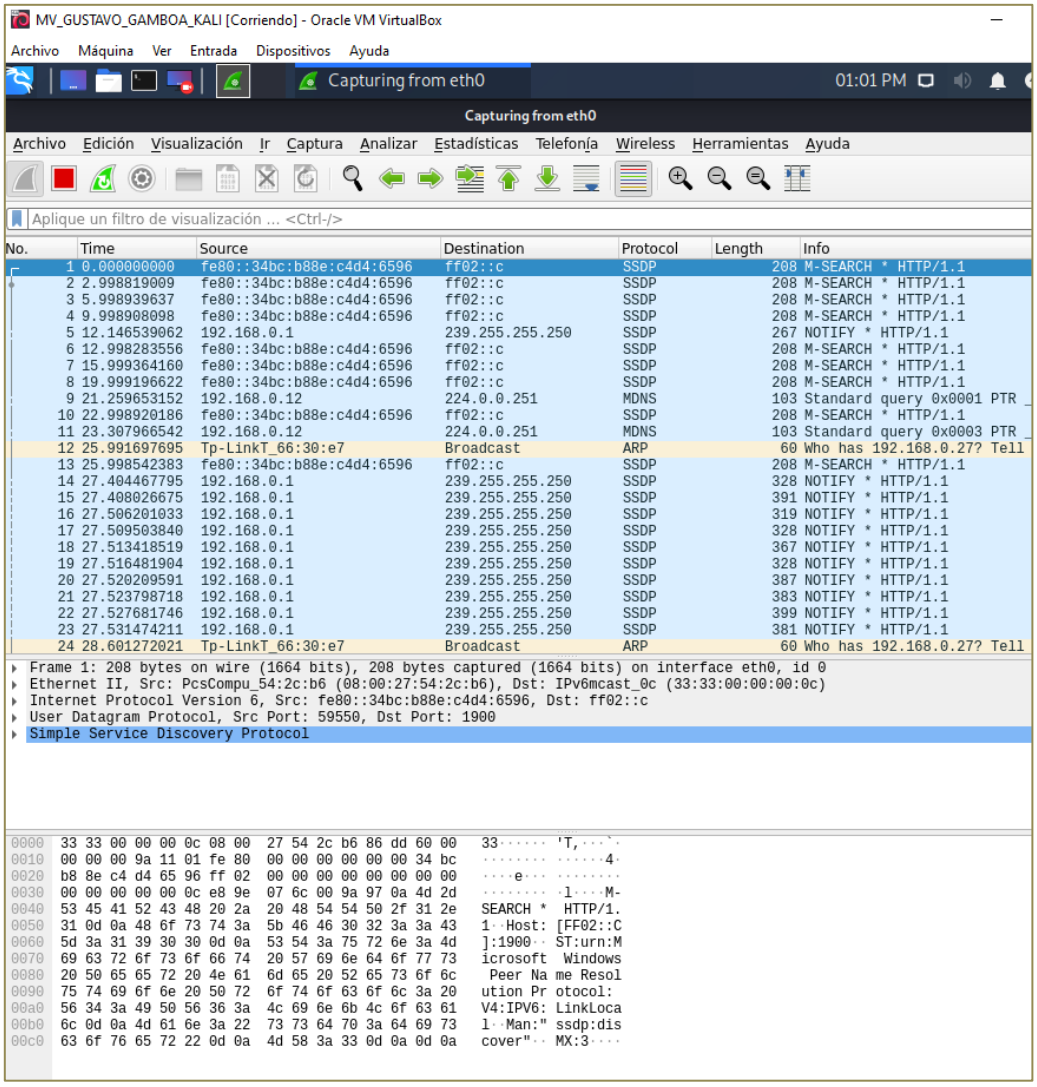


Figura 14 - Wireshark Campos

El panel de la lista de paquetes, ubicado en la parte superior de la ventana, muestra todos los paquetes encontrados en el archivo de captura activo. Cada paquete tiene su propia fila y el número correspondiente asignado, junto con cada uno de estos puntos de datos:

No: este campo indica qué paquetes forman parte de la misma conversación. Permanece en blanco hasta que seleccione un paquete.

Hora: La marca de tiempo de cuando se capturó el paquete se muestra en esta columna. El formato predeterminado es el número de segundos o segundos parciales desde que se creó por primera vez este archivo de captura específico.

- **Fuente**: esta columna contiene la dirección (IP u otra) donde se originó el paquete.
- **Destino**: esta columna contiene la dirección a la que se envía el paquete.
- **Protocolo**: el nombre del protocolo del paquete, como TCP, se puede encontrar en esta columna.
- **Longitud**: la longitud del paquete, en bytes, se muestra en esta columna.
- **Información**: Aquí se presentan detalles adicionales sobre el paquete. El contenido de esta columna puede variar mucho según el contenido del paquete.

Podemos observar la dirección IP de nuestro servidor web: 192.168.0.3:

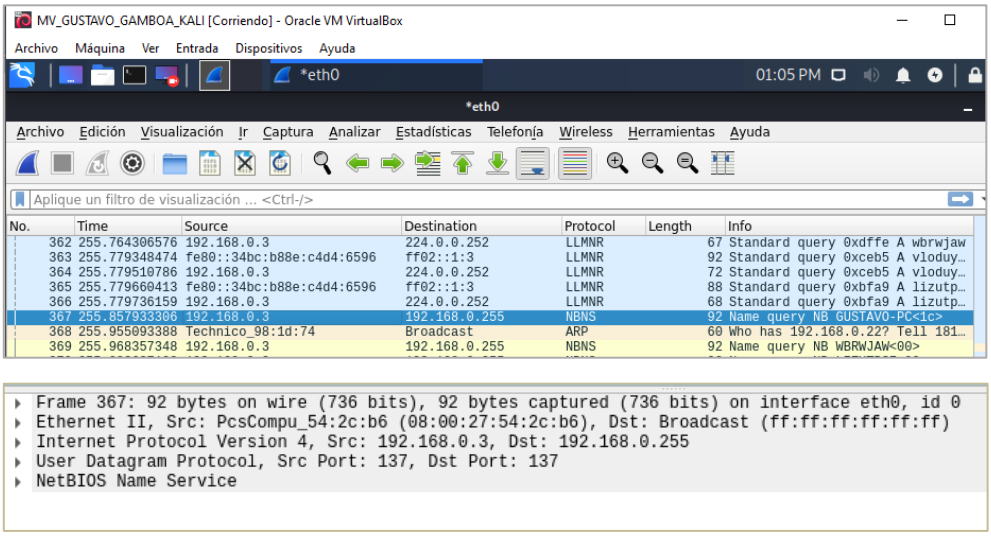


Figura 15 - Wireshark Dirección IP Web Server

En la parte inferior está el panel de bytes del paquete, que muestra los datos sin procesar del paquete seleccionado en una vista hexadecimal

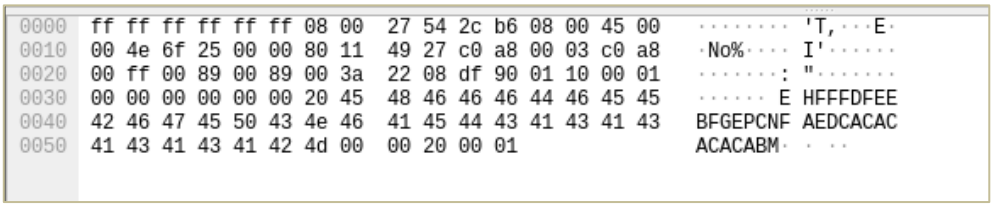


Figura 16 - Wireshark Bytes

6.2.4 Suplantación de identidad – Spoofing

Técnica de suplantación del servidor de nombres de dominio (DNS) el cual corresponde a un ataque en el cual son usados registros DNS modificados para reenrutar el tráfico a un sitio web falso que es similar al destino definido.

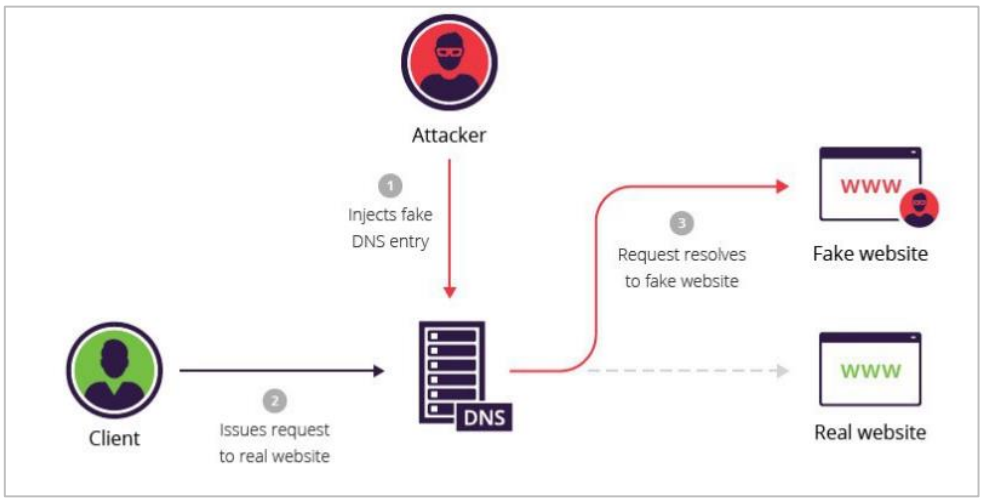


Figura 17 - Tomado de Imperva. Suplantación de DNS

Diagrama detallado de red, en el cual se pueda evidenciar todos los actores del ataque seleccionado, describa:

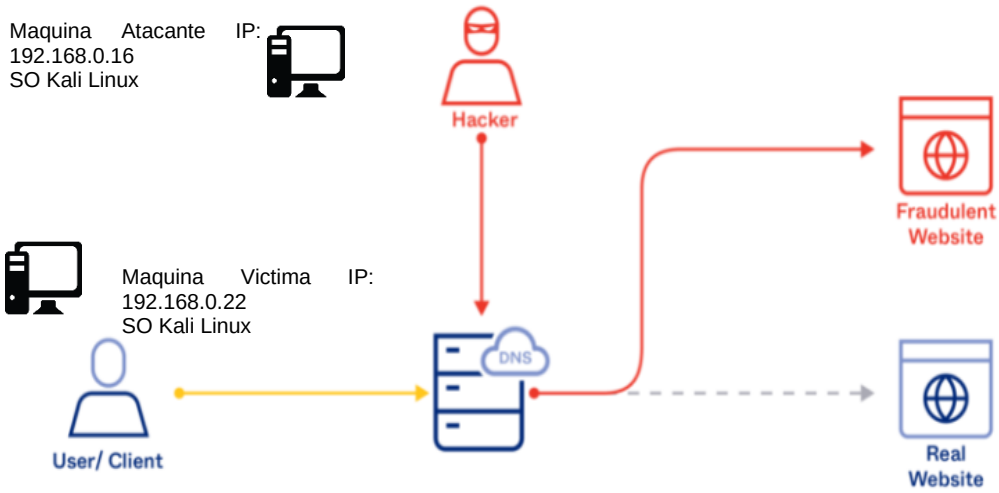


Figura 18 - Actores Ataque

6.2.5 Prueba de Spoofing

Maquina atacante 192.168.0.16 – Kali Linux

```
gustavo@kali:~$ sudo ifconfig
[sudo] password for gustavo:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.16  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe85:2957  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:85:29:57  txqueuelen 1000  (Ethernet)
        RX packets 253  bytes 23194 (22.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 230  bytes 17153 (16.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Maquina victima: 192.168.0.22 – Windows 10

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::f56b:3cda:9ad5:50d0%23
   Dirección IPv4. . . . . . . . . . . . : 192.168.0.22
   Máscara de subred . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.0.1

C:\Users\FliaGamboaBeltran>
```

Figura 19 - Kali Linux Identificar direcciones IP atacante y víctima

Modificamos el archivo index para personalizar la página web a la cual vamos a redireccionar a la víctima:

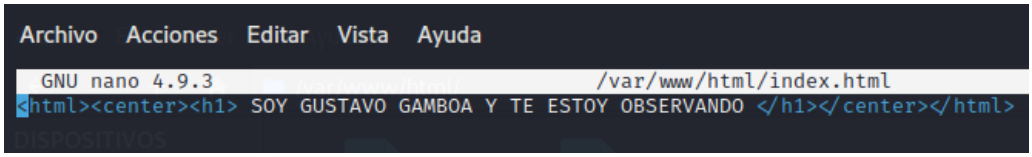


Figura 20 - Ataque Spoofing DNS File Index

Iniciamos el servicio de apache para garantizar que nuestro server web está operando:

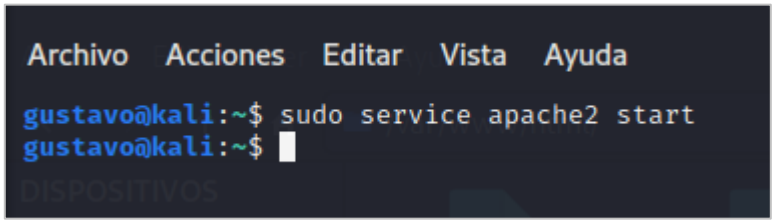


Figura 21 – Inicio Servicio Apache

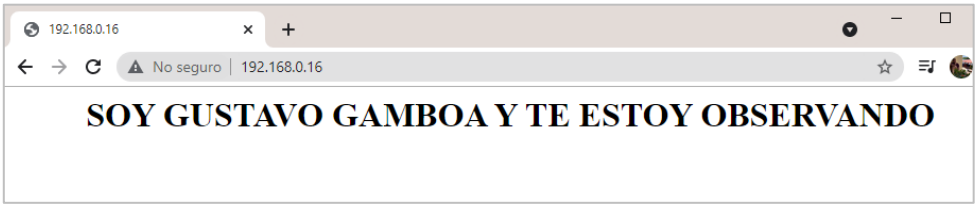


Figura 22 - Evidencia Ataque

Posteriormente debemos parametrizar el archivo etter.dns.

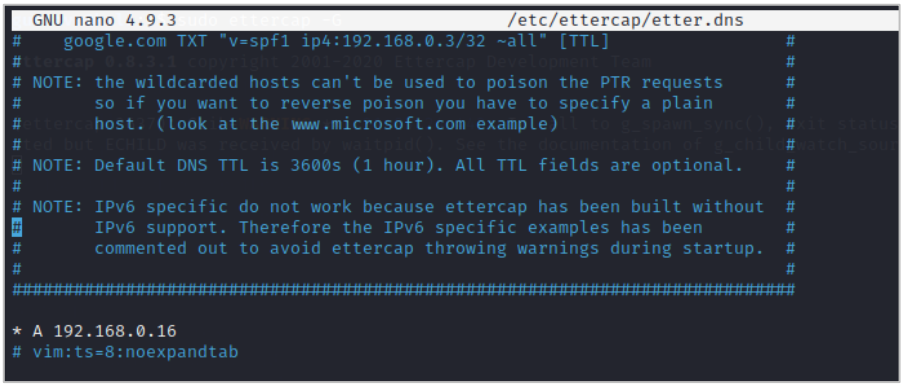


Figura 23 - File etter.dns

En el archivo archivo etter.conf ajustamos los valores a “0” de las líneas ec_uid = 0 y ecd_gid = 0.

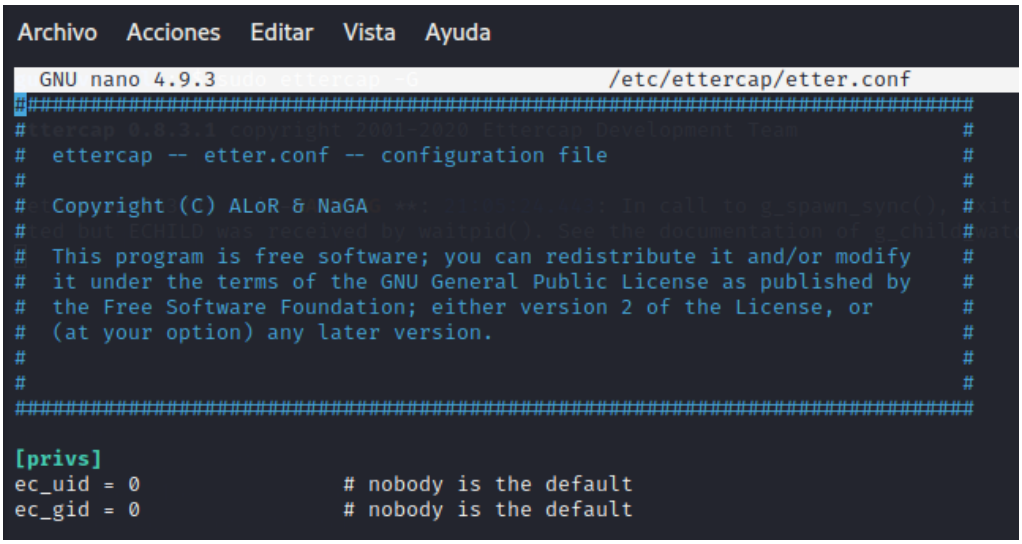


Figura 24 - Parametrización file etter

Ahora ejecutamos la herramienta ettercap en Kali Linux:

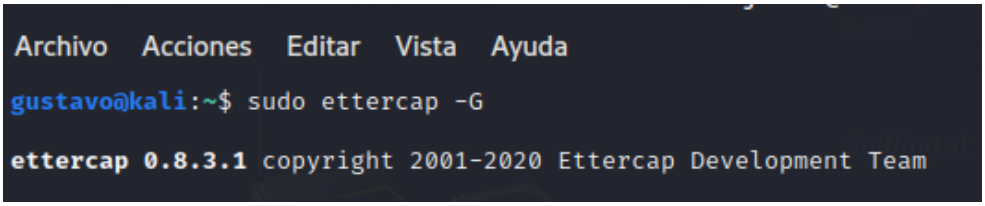


Figura 25 - Ettercap ejecución

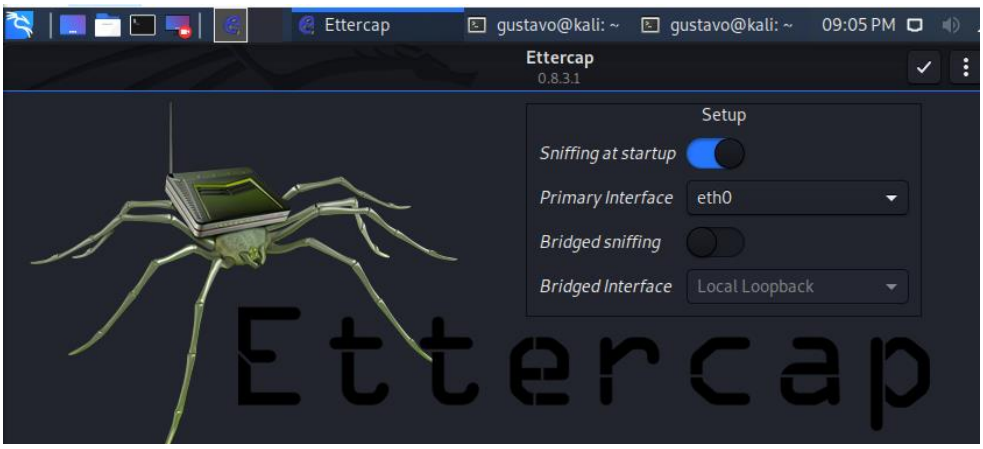


Figura 26 - Ettercap Interfaz

Escaneamos y listamos los hosts que tienen conexión a nuestra red:

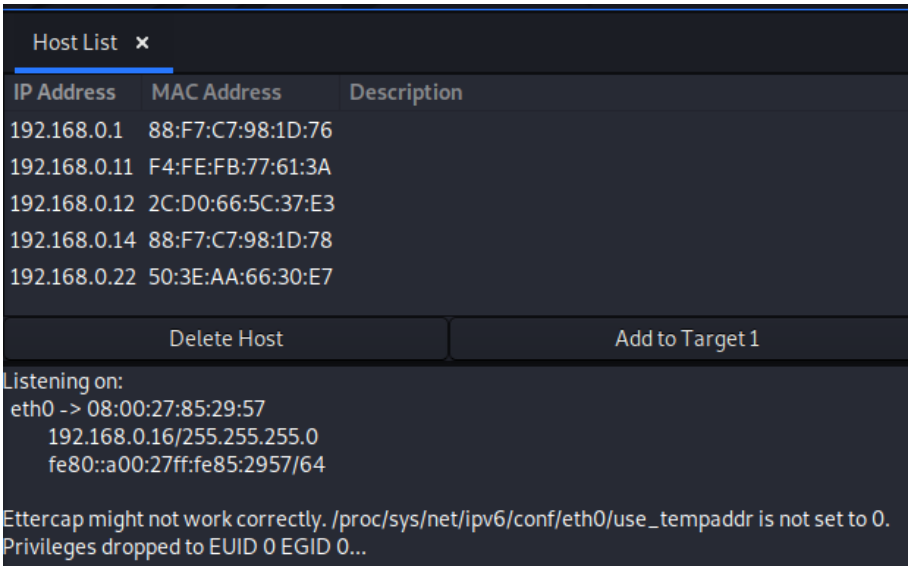


Figura 27 - Ettercap listado hosts

Definimos el target, la IP de la maquina víctima es: 192.168.0.22:

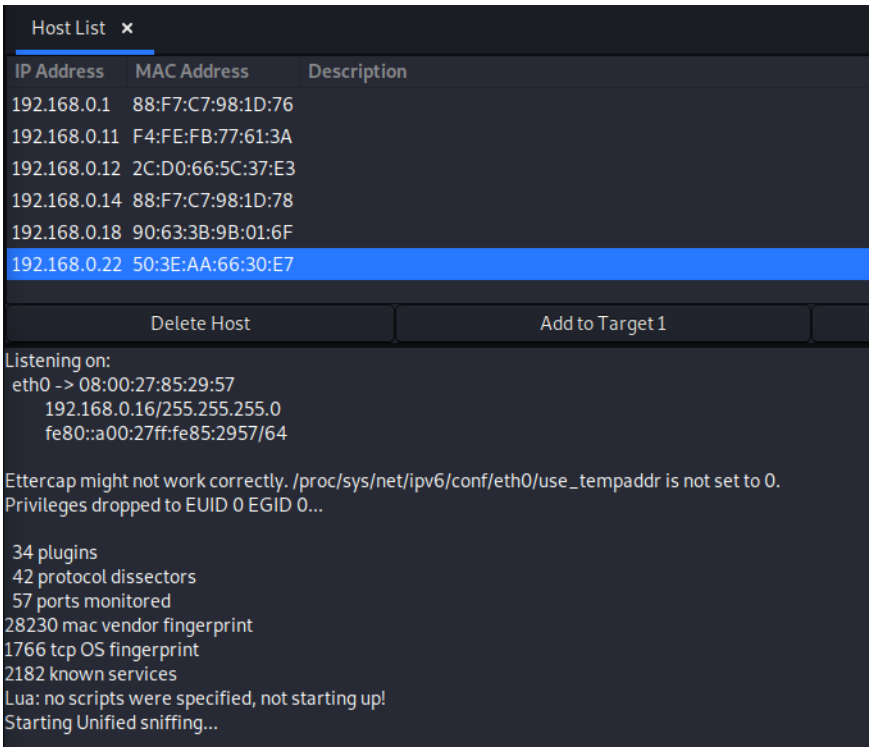


Figura 28 – Ettercap target

Activamos el ARP Poisoning:

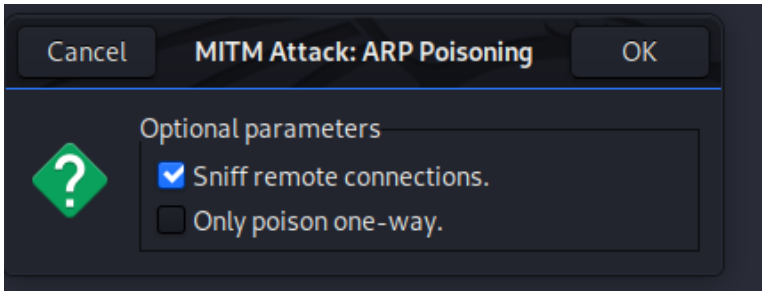


Figura 29 - Ettercap ARP Poisoning

Luego activamos el plugin dns_spoof:

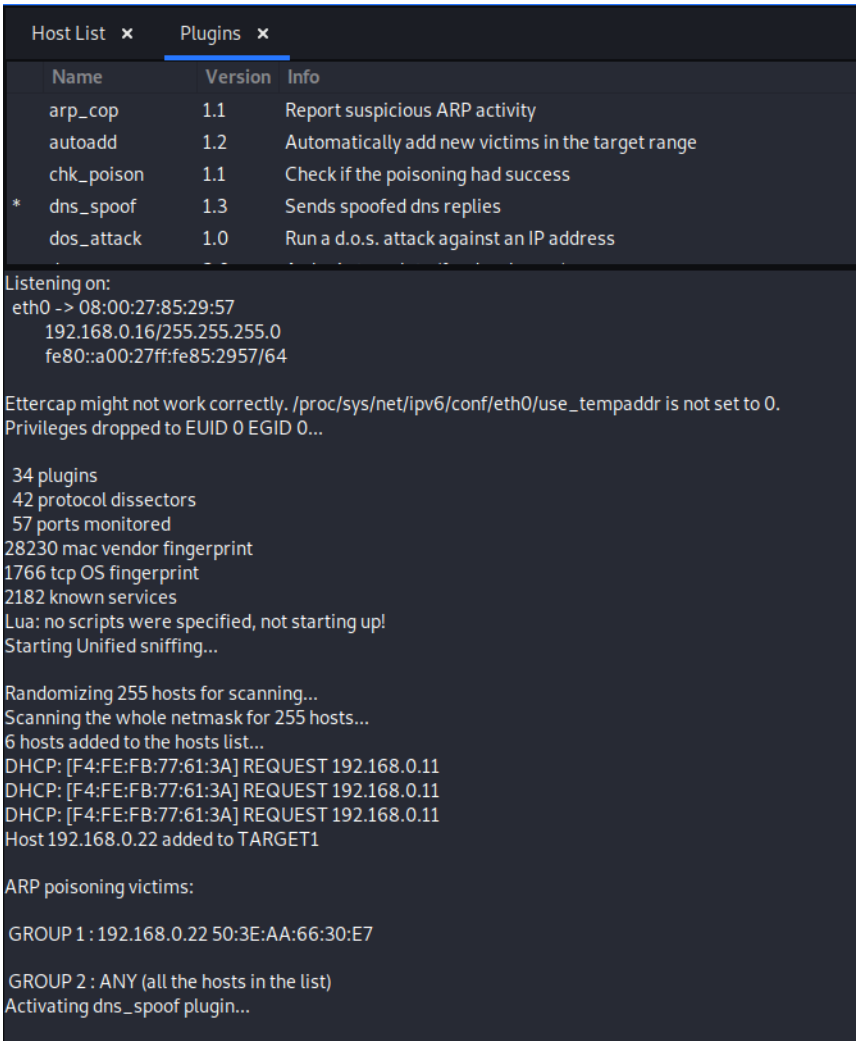


Figura 30 – Ettercap dns_spoof

En este momento hemos culminado la parametrización y el ataque ha sido lanzado, podemos observar que al consultar una página web (http), es redireccionada a nuestro servidor web apreciando el mensaje que previamente hemos configurado en el archivo index:

Figura 31 - Spoofing evidencia ataque

6.2.6 Protocolos FTP / SFTP

Pruebas ejecutadas bajo FTP Protocolo de Transferencia de Archivos

El protocolo que he seleccionado para proteger el tráfico de la red es SFTP ó Protocolo seguro de transmisión de archivos. Este Protocolo es un protocolo para transferir ficheros a través de la red de manera segura.

Prueba # 1 (Antes): Ejecutadas bajo FTP Protocolo de Transferencia de Archivos: Antes de realizar el análisis de tráfico hemos configurado nuestro servidor FTP con FileZilla Server:

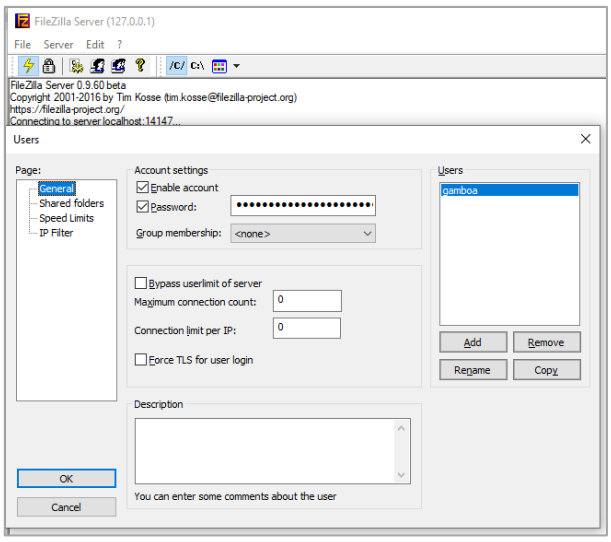


Figura 32 - FTP Server Configuración

Luego asignamos permisos al directorio para subir ficheros:

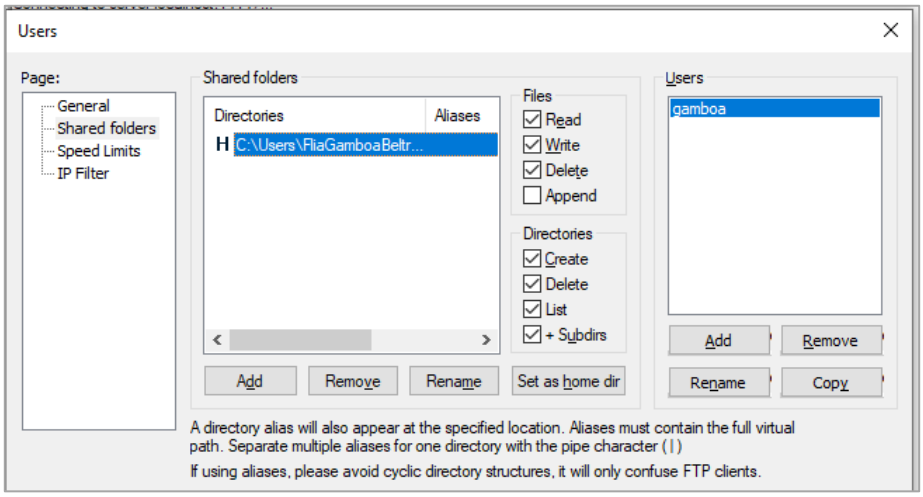


Figura 33 - FTP Permisos

Posteriormente configuramos nuestro FileZilla Client y configuramos la conexión, estableciendo los valores de Servidor, usuario y password:

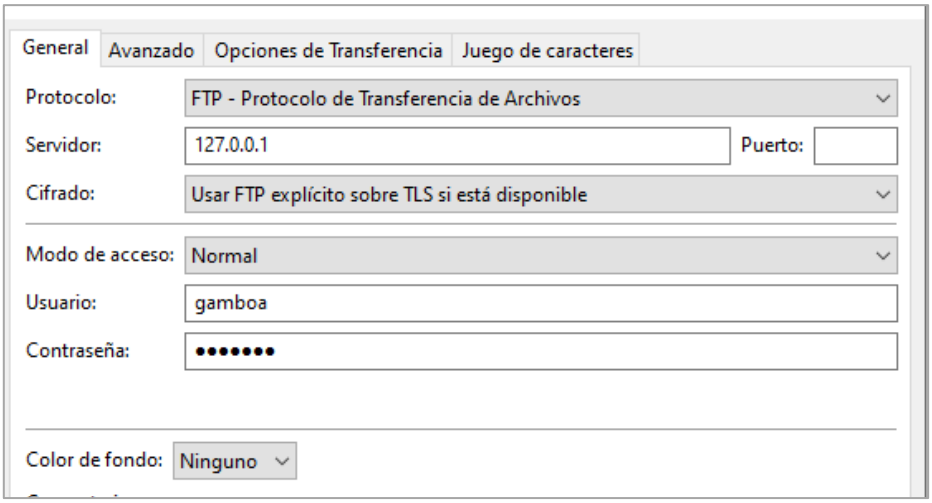


Figura 34 - FTP Configuración Server

Ahora vamos a conectarnos al servidor y realizar el cargue de un fichero “pruebas.txt.:

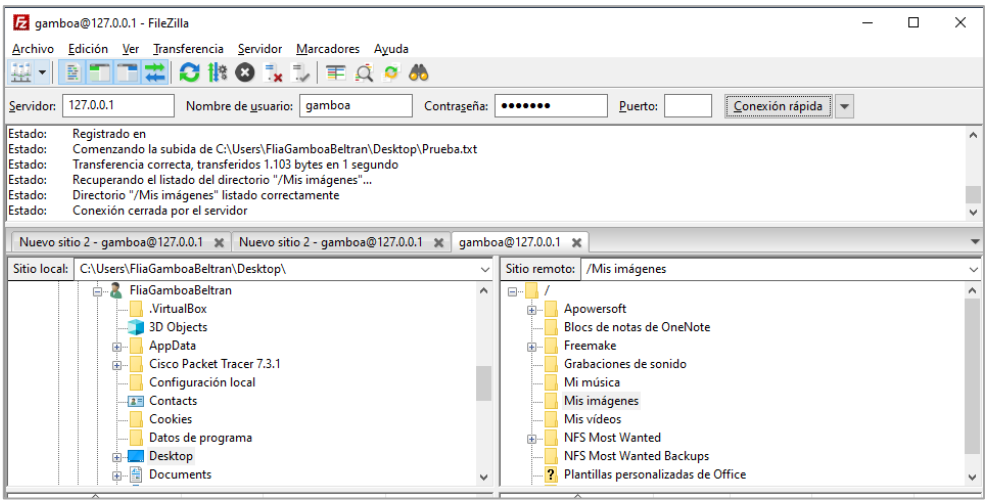


Figura 35 – Filezilla Cargue file

Luego nos dirijimos a nuestra ventana de analisis de trafico de wireshark, filtramos por protocolo FTP y podemos observar que ha capturado informacion relacionada con usuario, contraseña y el fichero que cargamos:

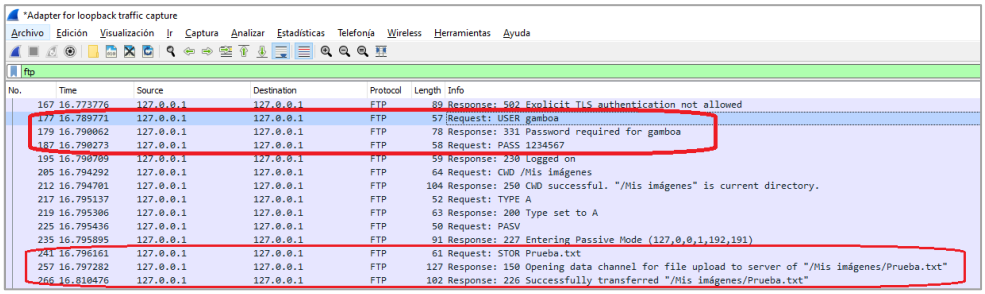


Figura 36 - Wireshark Análisis de trafico

Lo anterior deja en evidencia que el uso de FTP representa un riesgo de seguridad ya que no es una transferencia de datos segura debido a la falta de cifrado.

Prueba # 2 (Después): Ejecutadas bajo SFTP Protocolo de transferencia segura de archivos

Primero configuramos nuestro servidor SFTP en una máquina virtual de Ubuntu – Linux. Abrimos una terminal y ejecutamos admin:

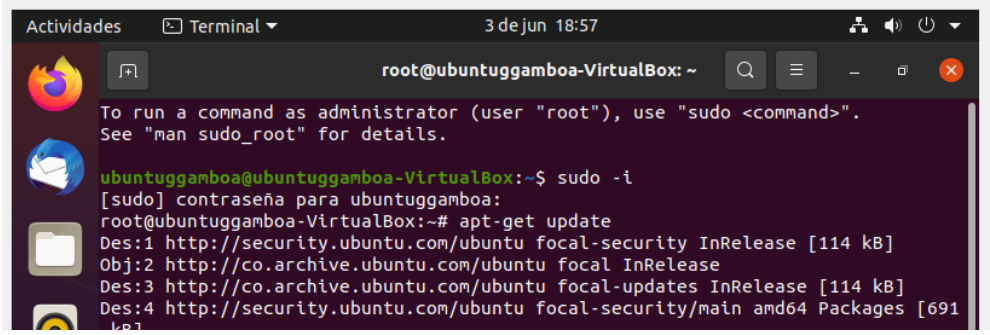


Figura 37 - Pruebas Protocolo SFTP Terminal

Instalamos el openssh-server:

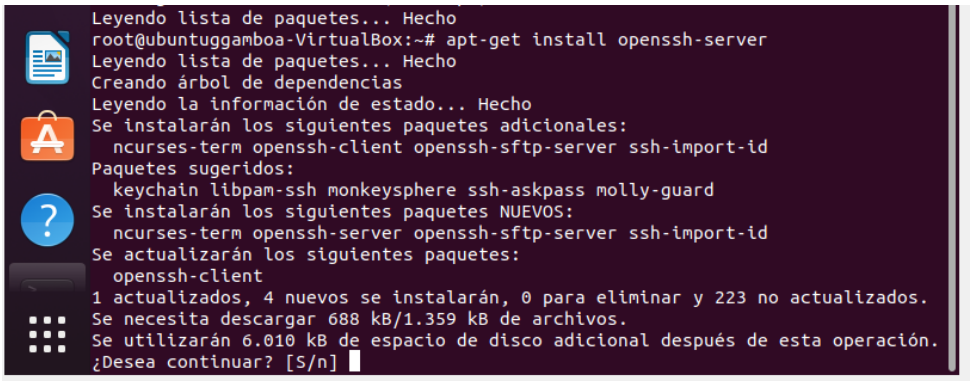


Figura 38 - Pruebas Protocolo SFTP Openssh-server

Creamos un grupo:

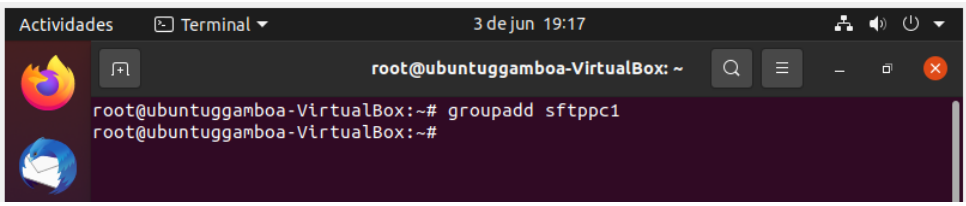


Figura 39 - Pruebas Protocolo SFTP Creación grupo

Observamos el id:

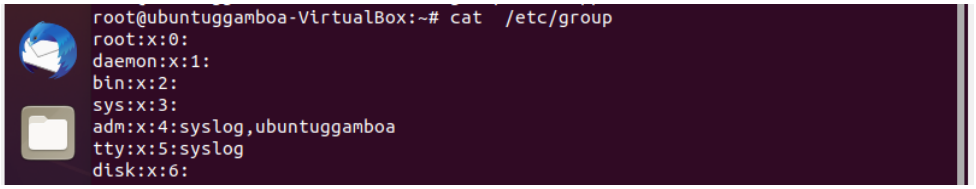


Figura 40 - Pruebas Protocolo SFTP ID

Creamos el usuario y asignamos contraseña:

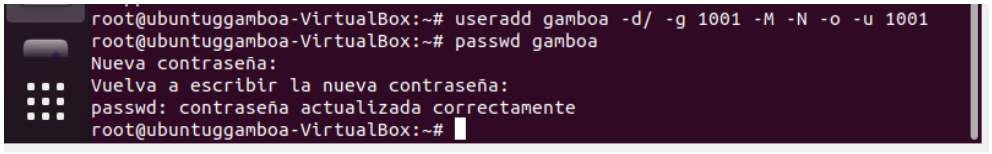


Figura 41- Pruebas Protocolo SFTP Creacion User

Hacemos una copia del fichero config:

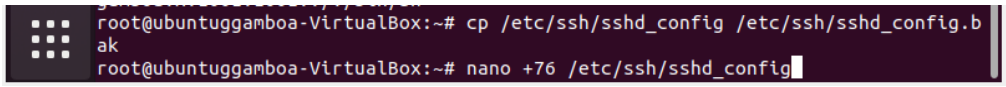


Figura 42 - Pruebas Protocolo SFTP Copia fichero

Hacemos modificaciones al archivo:

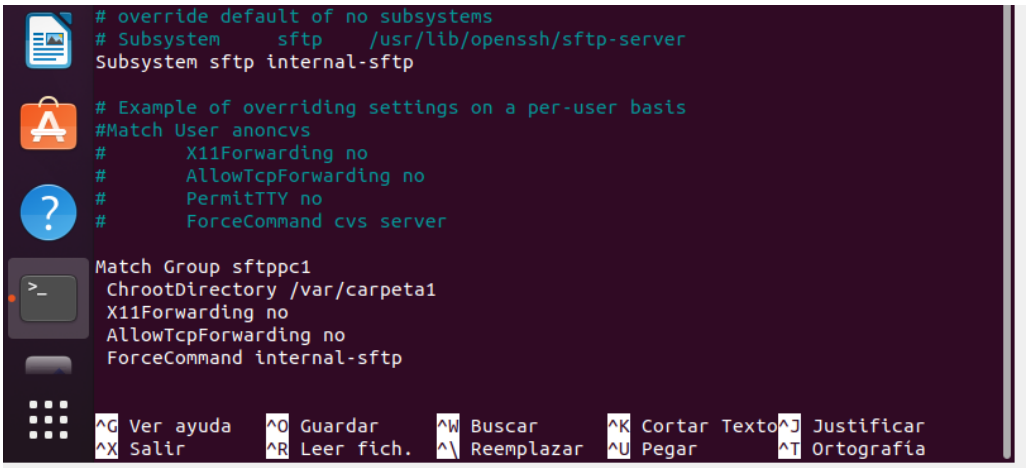


Figura 43 - Pruebas Protocolo SFTP Modificación archivo

Creamos el directorio:

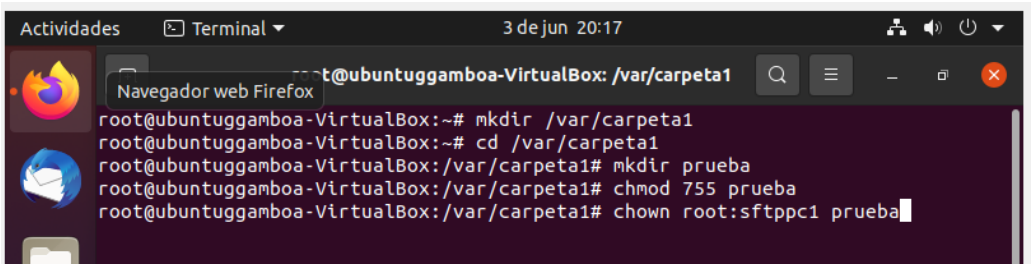


Figura 44 - Pruebas Protocolo SFTP Creacion directorio

Hacemos un restar del servicio:

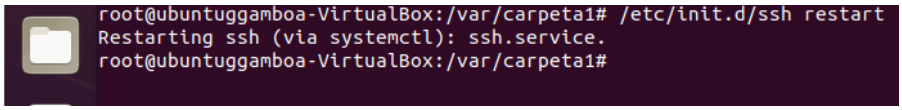


Figura 45 - Pruebas Protocolo SFTP Restart servicio

Tomamos la dirección IP, con el comando ifconfig:

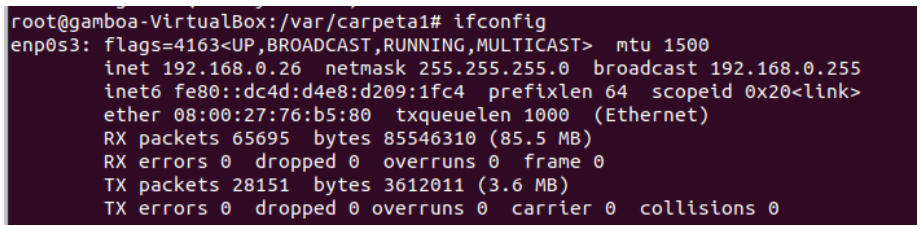


Figura 46- Pruebas Protocolo SFTP Dirección IP

Vamos a Filezilla cliente y configuramos la conexión SFTP.

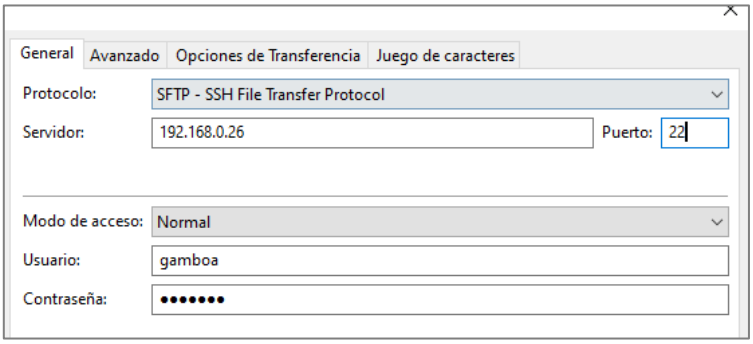


Figura 47 - Filezilla Conexion SFTP

Aceptamos la conexión:

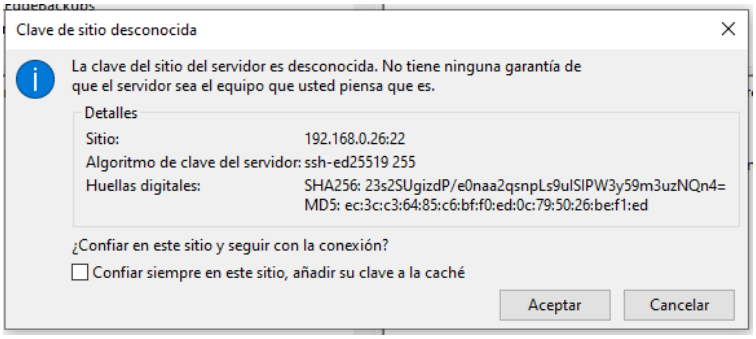


Figura 48 - Aceptar la conexión

Tomamos la dirección IP, con el comando ifconfig:

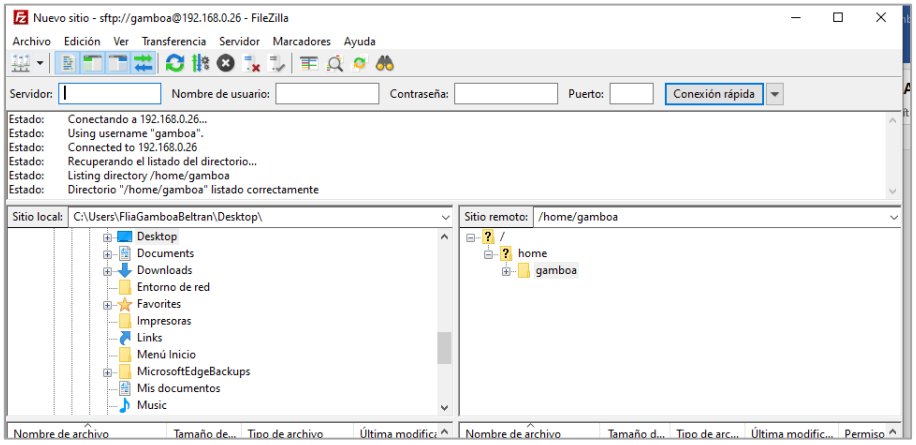
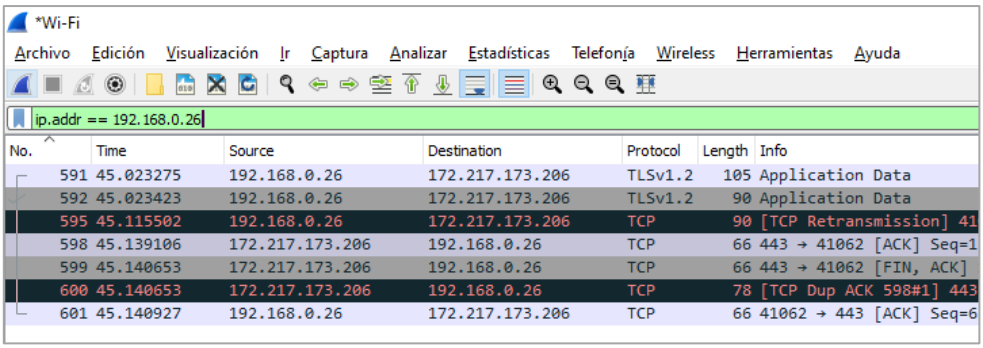


Figura 49 - Filezilla configuramos sitio

Vamos a realizar análisis de tráfico con Wireshark:



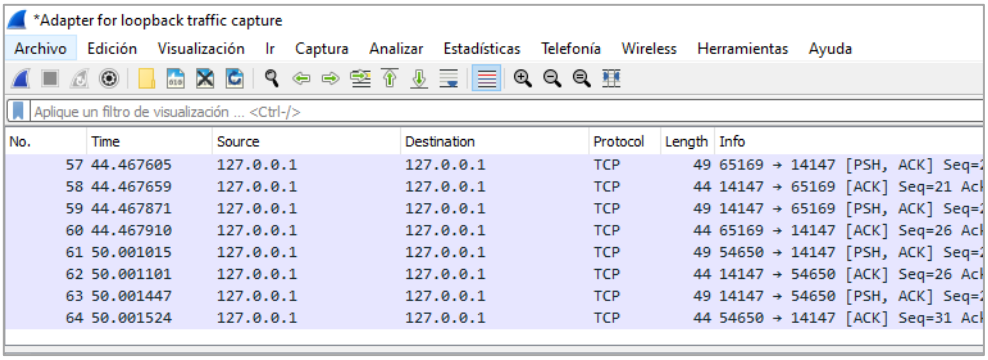


Figura 50 - Análisis de tráfico wireshark

Podemos evidenciar que utilizando el protocolo SFTP no se evidencian datos confidenciales ya que viajan cifrados.

SSH Ubuntu Linux

Inicialmente instalamos el servicio openssh-server en nuestra terminal de la máquina virtual de Linux Ubuntu:

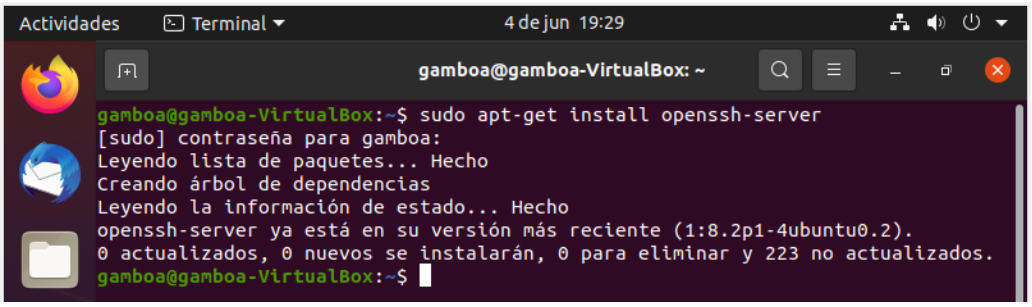


Figura 51 - Instalación openssh-server

Identificamos la direccion IP: 192.168.0.26

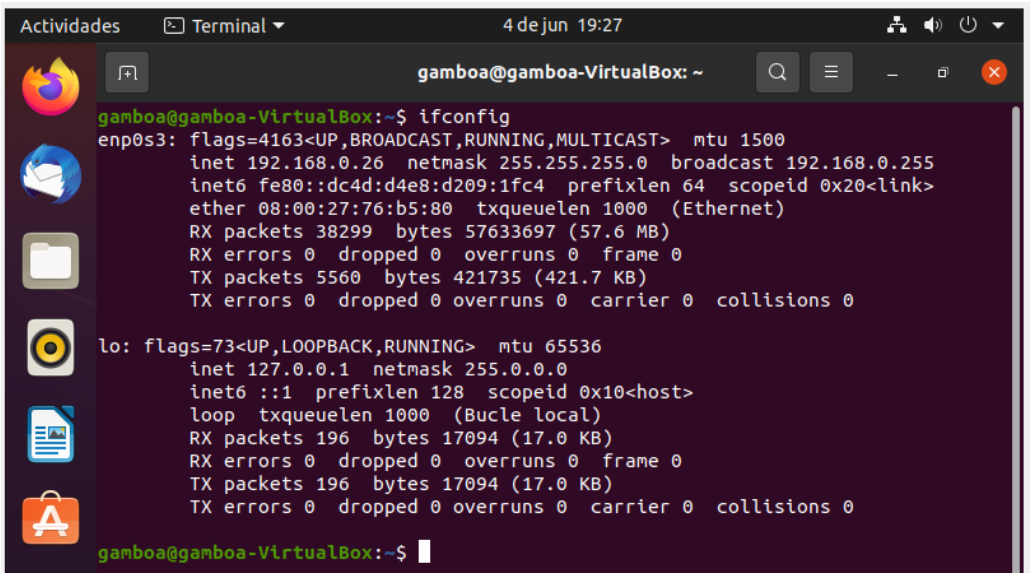


Figura 52 - Identificar direccion ip

Luego establecemos la conexión a traves de la herramienta de Putty desde nuestra maquina Windows:

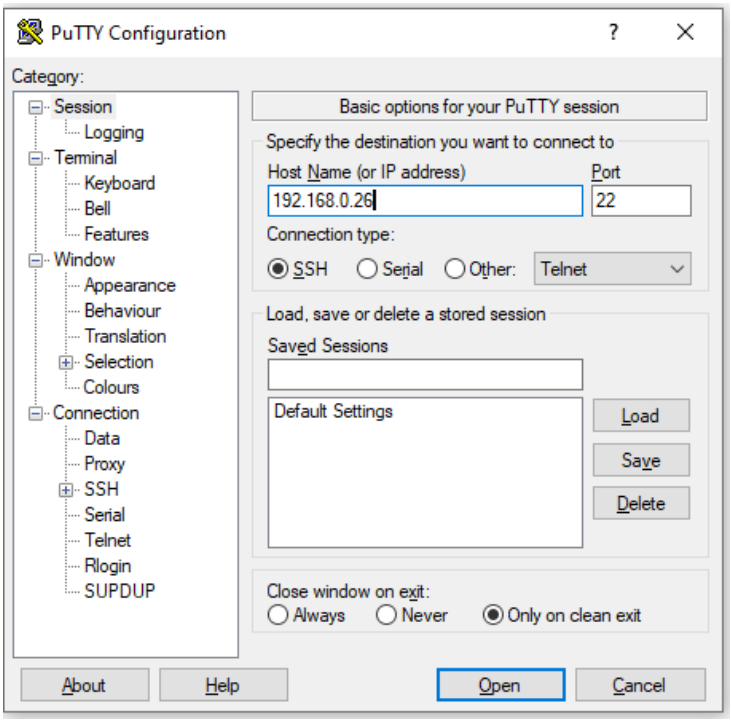


Figura 53 - Putty Configuración

Podemos evidenciar que la conexión se establece de manera satisfactoria, ingresamos user y password:

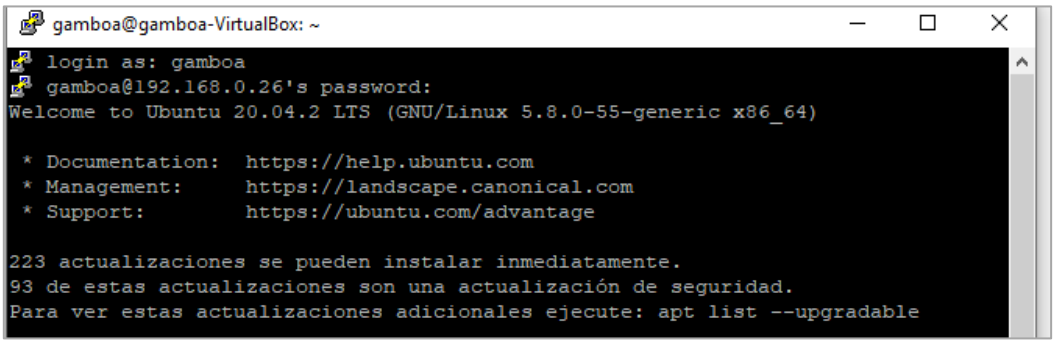


Figura 54 - Conexión establecida

El protocolo SSH utiliza encriptación para asegurar la conexión entre un cliente y un servidor.

Parámetros que permitan mejorar la seguridad de SSH:

- **MaxStartups:** limitar el número máximo de conexiones simultáneas al demonio SSH puede ayudar a proteger su servidor SSH de un ataque de fuerza bruta.
- **PermitEmptyPasswords**, denegar el inicio de sesión a los usuarios con una contraseña vacía (en blanco).
- **AllowUsers:** El uso de una lista blanca para permitir el acceso SSH de usuarios específicos y una lista negra para no permitir a otros usuarios mejorará su seguridad SSH.
- **DenyUsers**: Los usuarios especificos de esta lista no podrán conectarse.
- **LogLevel**, de forma predeterminada, SSH registra todo. Si desea registrar más información, como intentos fallidos de inicio de sesión. puede cambiar el valor de INFOa VERBOSE.

A continuacion nuestro archivo de configuracion de SSH donde ajustar los diferentes parametros:

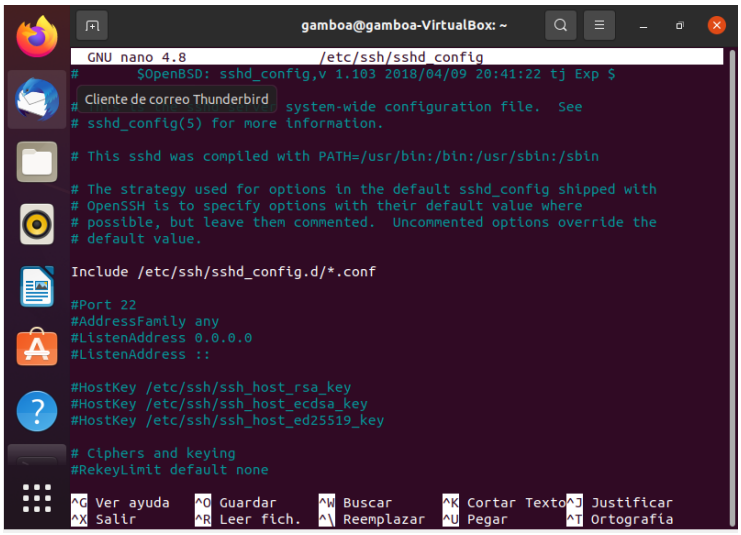


Figura 55 - File SSH

SSH Windows 10

Primero asignamos una dirección IP fija a nuestro adaptador de red:

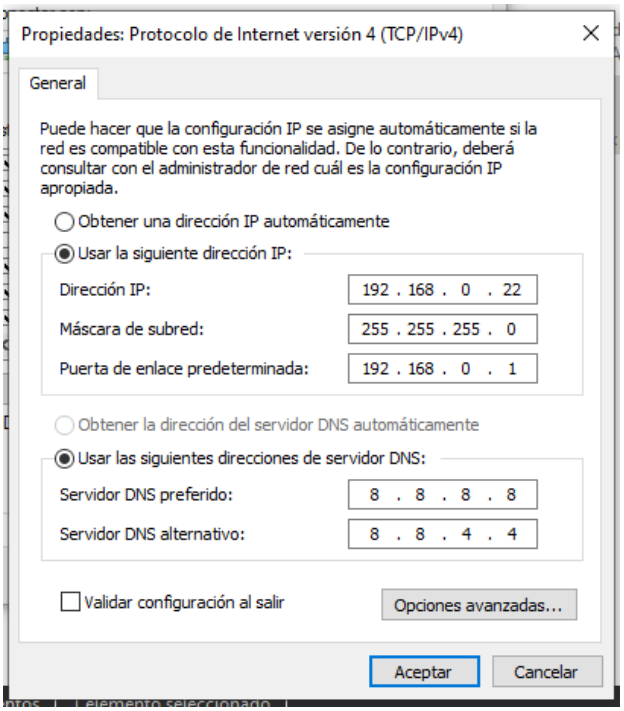


Figura 56 – Configuración de red

Confirmamos que la direccion IP sea tomada por el adaptador:

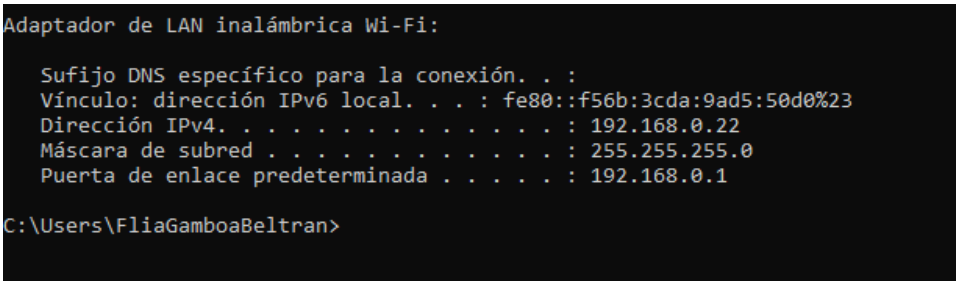


Figura 57 - Configuración de red WLAN

Ajustamos parametros del protocolo SSH incluyendo los de seguridad:

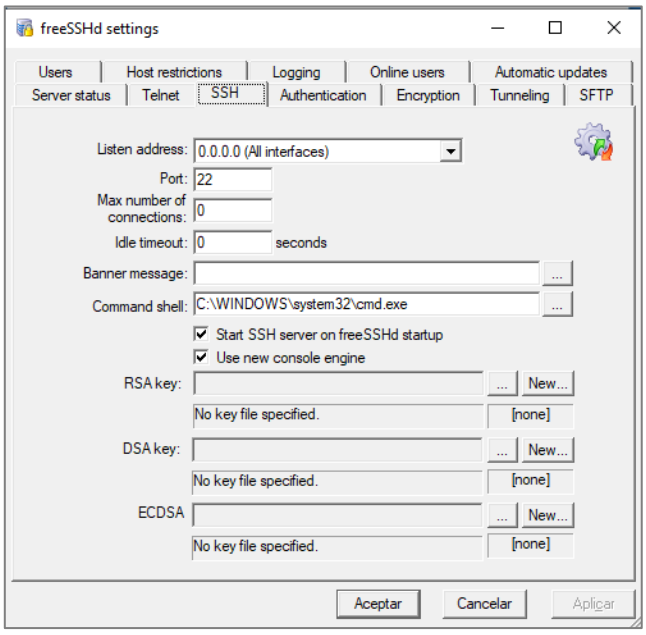


Figura 58 - SSH Configuraciones

Seleccionamos la autenticacion con password:

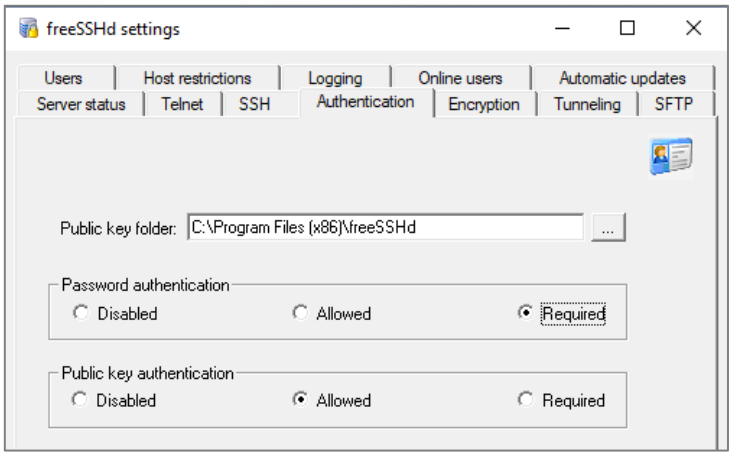


Figura 59 - Autenticación SSH

Selecionamos al algoritmo de encripcion mas seguro: AES256

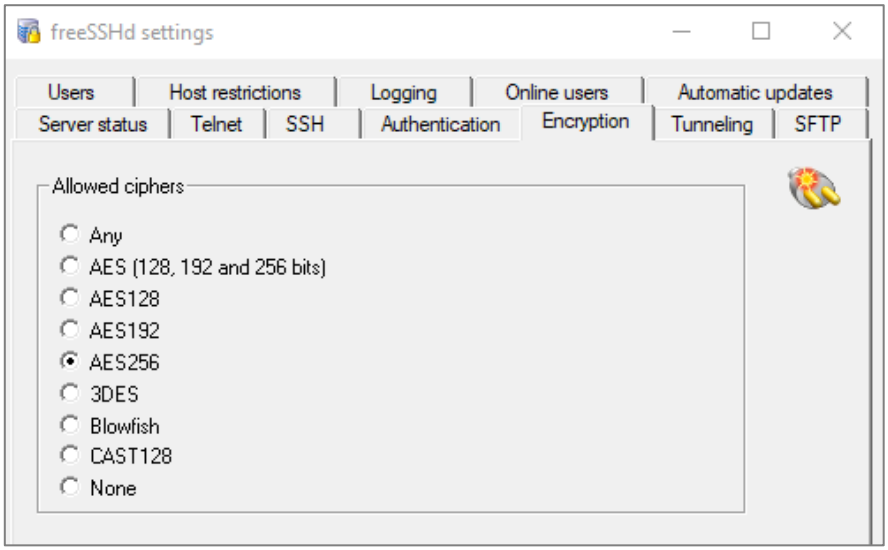


Figura 60 - SSH Algoritmo

Adicionamos usuario y asignamos password:

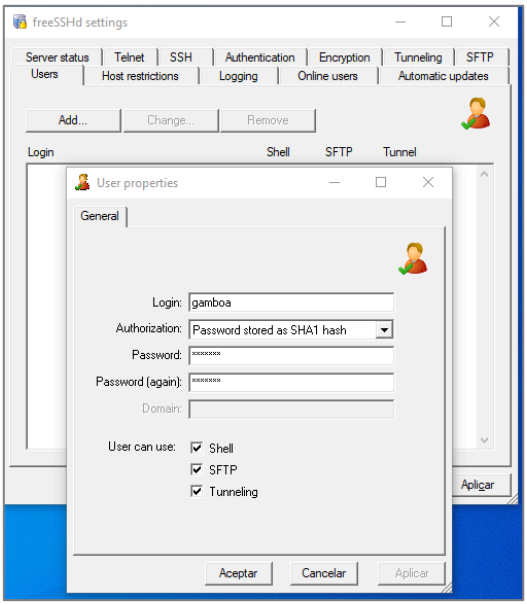


Figura 61 - SHH Login valores

Habilitamos la opcion de generar log de eventos:

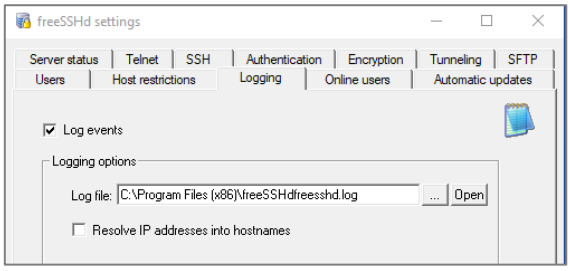


Figura 62 - Log eventos

Iniciamos los servicios:

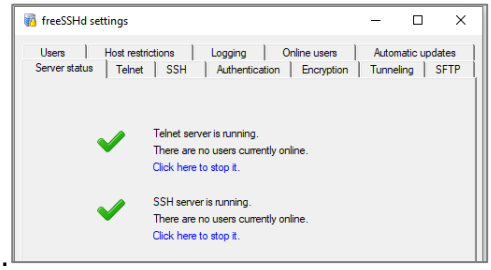


Figura 63 - Inicio de servicios

Vamos a nuestra herramienta de Putty y configuramos la conexión al servidor SSH:

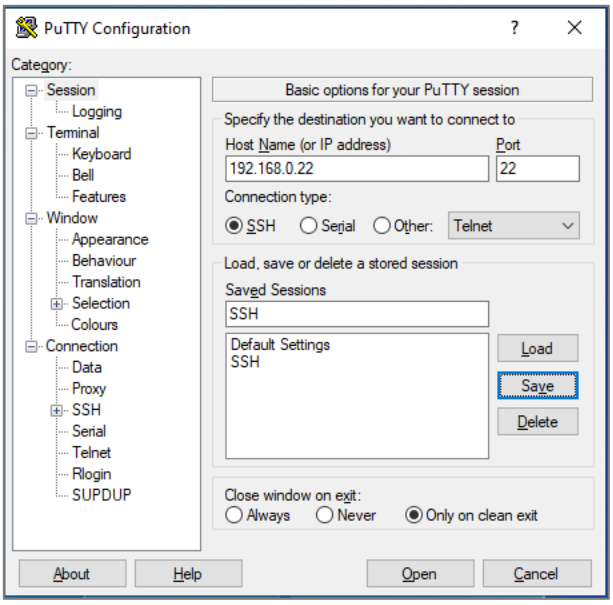


Figura 64 - Putty Configuración SSH Server

Luego de establecer la conexión, nos logueamos con las credenciales que configuramos:

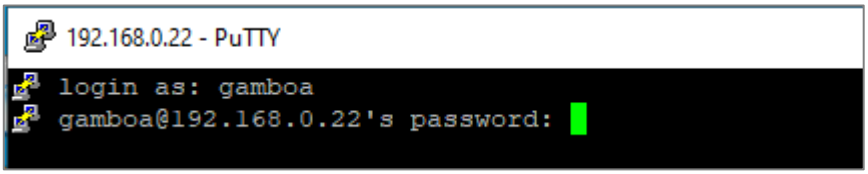


Figura 65 - Login

Realizamos una prueba creando una carpeta en la ubicación publica:

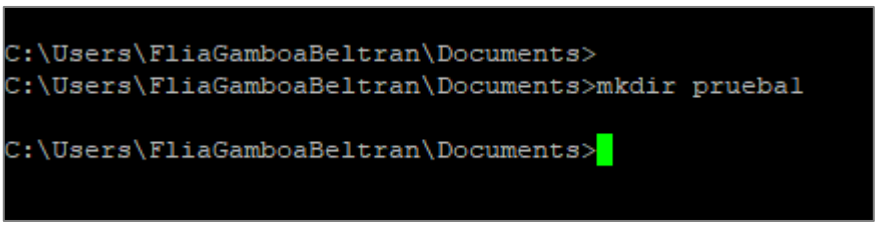


Figura 66 - Prueba de creacion directorio

Confirmamos que la carpeta fue creada:

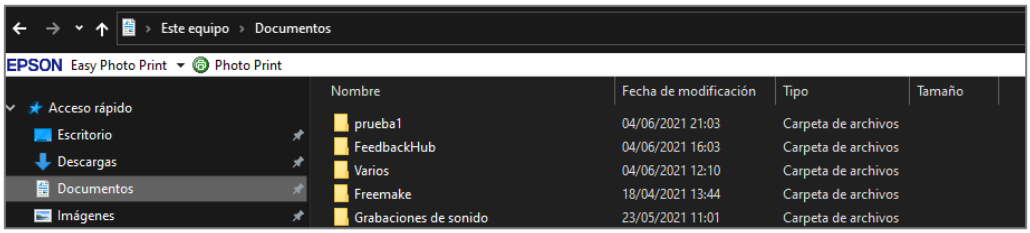


Figura 67 - Evidencia creación directorio

Podemos observar el registro que nuestro user posee una sesion establecida:

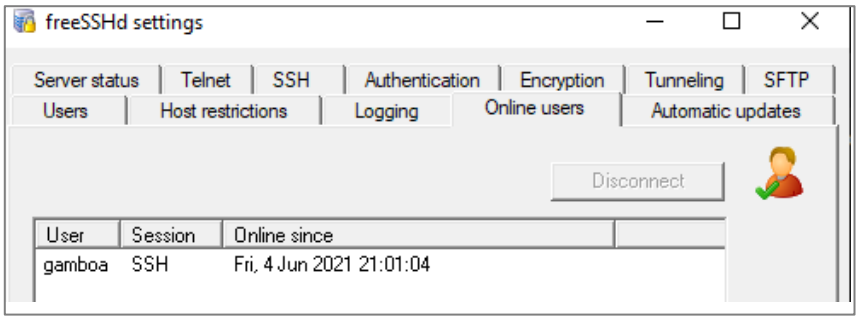


Figura 68 - Evidencia conexión

Así mismo podemos generar un log de eventos.

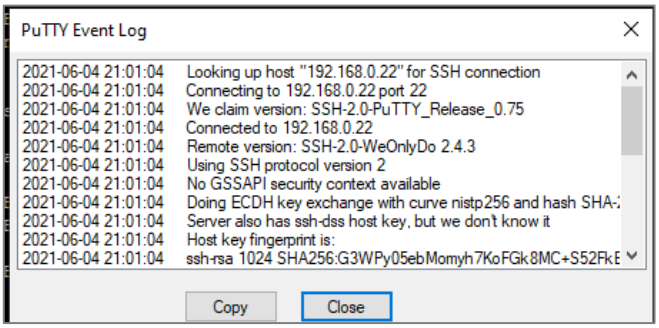


Figura 69 - Evidencia log eventos

6.3 PLAN DE CONTENCION – BLUE TEAM

Los equipos azules en ciberseguridad evalúan y analizan constantemente los sistemas de seguridad para aplicar parches, identificar fallas de seguridad, problemas de configuración relevantes para la seguridad y verificar el impacto de los controles de seguridad. Los equipos azules realizan todas las funciones del SOC (centro de operaciones de seguridad) y generalmente son responsables de la gestión de eventos, seguimiento de incidentes, inteligencia de amenazas, captura y análisis de paquetes y automatización de la seguridad.

- Protección de endpoints
- Registro (recopilación, análisis y normalización)
- NSM por capa de red
- Conceptos de monitoreo continuo de seguridad (CSM)
- Colección de eventos CSM
- Centralización de datos
- Eventos, alertas, anomalías e incidentes
- Sistemas de gestión de incidentes
- Plataformas de inteligencia de amenazas
- Triaje y análisis
- Sintonización de alertas
- Automatización de seguridad

6.2.1 Situación problema: Análisis Blue team

Las actividades de contención se realizaron basados en una situación problema que se describe a continuación:

WhiteHouse Security solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows 7 X64 analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico "sistema operativo, red", con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. WhiteHose Security le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

6.2.2 Acciones iniciales

Lo primero que hacemos es llevar a cabo una labor de contención que consiste en aislar de toda conectividad de red las áreas o PCs con el fin de que restar posibilidades de propagación del ataque. Posteriormente, teniendo en cuenta que el activo más importante de una organización es la información, es necesario respaldar o sacar de la red los dispositivos que almacenan toda la información confidencial y apreciada. Recordemos que la aplicación Rejjeto v2.3 instalada en el PC de la dependencia tiene asociado un exploit que puede terminar en una Shell reversa y una sesión abierta de meterpreter. . El puerto que abre la aplicación es el puerto 80.

De acuerdo a la consulta realizada Exploit Data Base se evidencia que existe una vulnerabilidad para esta aplicación CVE 2014-6287:

Figura 70 - Tomado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

"La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (aks HFS o HttpFileServer) 2.3x antes de 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia% 00 en una acción de búsqueda."

Figura 71 - Tomado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

6.2.3 Logs de eventos

En la parte de la indagación procedo a obtener los logs de eventos para conocer el registro detallado de las notificaciones del sistema, de la seguridad y de las aplicaciones almacenadas por el sistema operativo Windows:

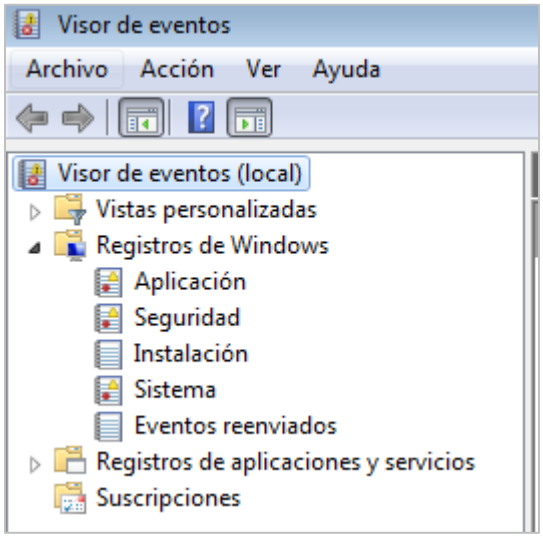


Figura 72 - Log eventos windows

- Eventos de aplicación:

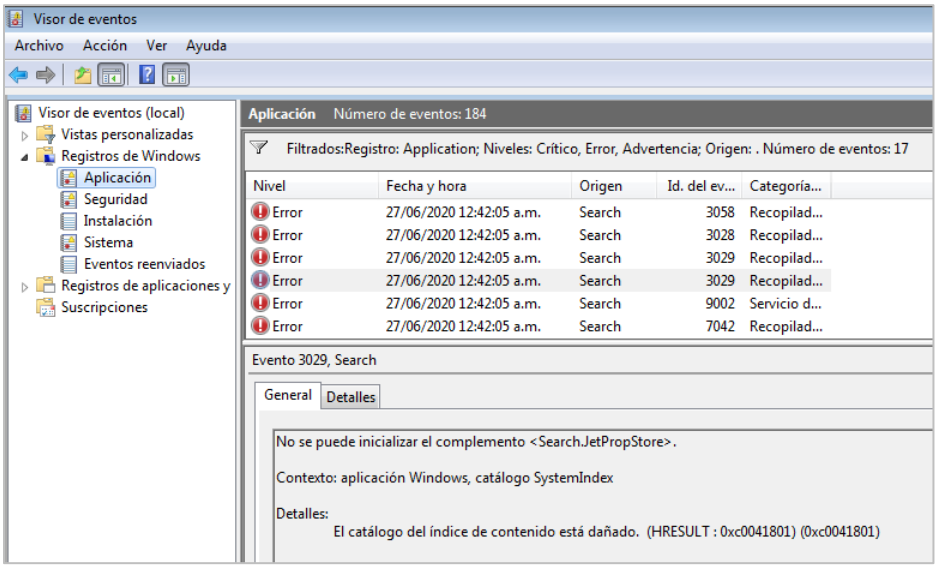
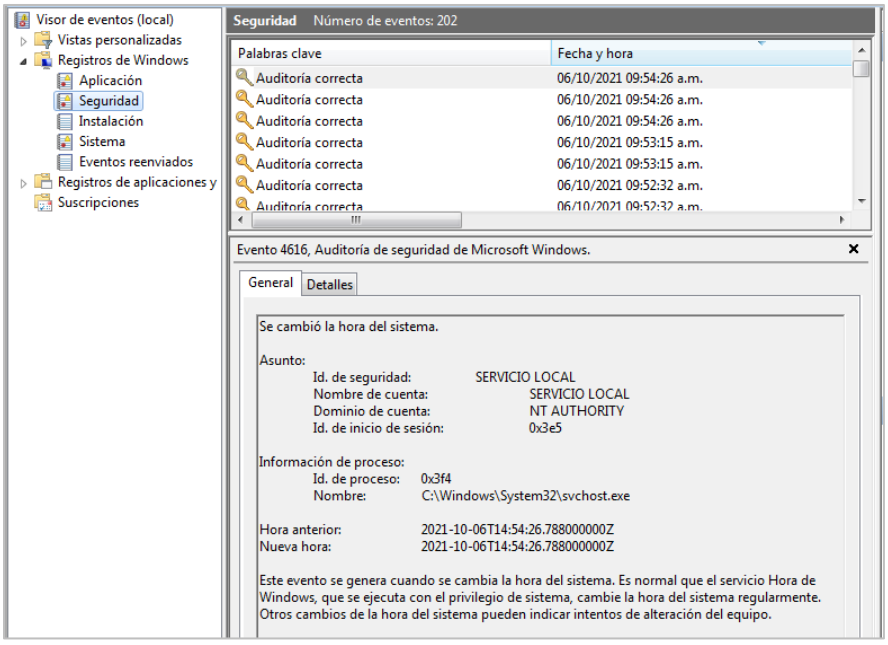


Figura 73 - Eventos aplicación

Eventos de seguridad:



Componente practico Gustavo Gamboa

Figura 74 - Eventos seguridad

Eventos del sistema:

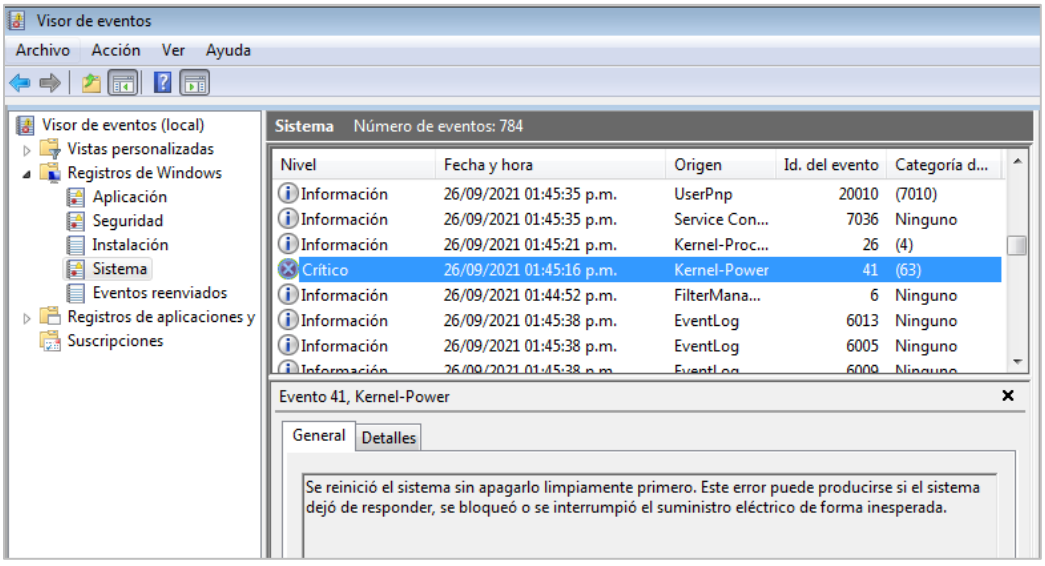


Figura 75 - Eventos sistema

6.2.4 Medidas de hardenización para que el ataque no se repita

Para reforzar al máximo posible la seguridad ejecutaría las siguientes actividades:

- Utilizar software antivirus (AV) actualizado
- Utilizar y mantener activado el firewall y con reglas activas y configuradas.
- Actualizaciones de seguridad y software periódicas y ejecución remota para todos los equipos de la organización cuando existan liberaciones del fabricante.
- Se habilitarán tareas programadas para ejecución de backups periódicos de información en los equipos que así lo requieran en ubicaciones diferentes definidas.
- Rastrear y administrar el uso de puertos, protocolos y servicios en dispositivos de red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes
- Utilizar una autenticación sólida para limitar el acceso no autorizado
- Aplicar parches críticos.
- Reforzar la autorización de todas las cuentas con el mínimo de privilegios
- Utilizar sistema de encriptación con algoritmos complejos
- Implementación de herramientas que se recomiendan para fortalecimiento de la seguridad como anti-spam, firewall, IDS, Antivirus, servicios de seguridad, detección de intrusos, detección de vulnerabilidades, consultorías, etc.
- Crear listas de acceso y perfiles de usuario para evitar que personal no autorizado tenga acceso a la red, se debe implementar una política de control de acceso e implementación de conexión segura.

6.2.5 CIS - Centro para la Seguridad de Internet

Primero quiero describir que es CIS y cuál es su objetivo. CIS Centro para la Seguridad de Internet es una organización sin ánimo de lucro con sede en New York que cuenta con cientos de profesionales de ciberseguridad de TI pertenecientes a agencias gubernamentales, militares, grandes corporaciones, conglomerados e instituciones académicas, Su objetivo es permitir un entorno de confianza en el ciberespacio.

Si debo trabajar con CIS “Center For Internet Security” lo utilizaría para compartir conocimiento con profesionales y tomar las buenas prácticas reflejadas en los controles de seguridad básicos definidos por esta organización.
Los controles de seguridad básico se listan a continuación:

- Control 1: Inventario y control de activos de hardware
- Control 2: Inventario y control de activos de software
- Control 3: Gestión continua de vulnerabilidades
- Control 4: Uso controlado de los privilegios administrativos
- Control 5: Configuración segura para el hardware y el software de los dispositivos móviles, laptops, estaciones de trabajo y servidores
- Control 6: Mantenimiento, monitoreo, y análisis de logs de auditoría
- Control 7: Protección de correo electrónico y navegador web
- Control 8: Defensas contra malware
- Control 9: Limitación y control de puertos de red, protocolos y servicios
- Control 10: Funciones de recuperación de datos
- Control 11: Configuración segura para dispositivos de red, tales como firewalls, routers y switches
- Control 12: Protección perimetral
- Control 13: Protección de datos
- Control 14: Control de acceso basado en la necesidad de saber

- Control 15: Control de acceso inalámbrico
- Control 16: Monitoreo y control de cuentas
- Control 17: Implementar un programa de concienciación y capacitación en seguridad
- Control 18: Seguridad del software de aplicación
- Control 19: Respuesta y gestión de incidentes
- Control 20: Pruebas de penetración y ejercicios de equipo rojo

6.2.6 SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management)

SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es un sistema de seguridad que busca proporcionar a las empresas una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos. Los sistemas SIEM tienen un control total sobre todos los eventos que suceden en la empresa para poder detectar cualquier tendencia o patrón fuera de lo común y así actuar de forma inmediata. SIEM es la evolución de dos tecnologías de seguridad anteriores:

- Gestión de eventos de seguridad (SEM). Detecta patrones de acceso fuera de lo común en tiempo real.
- Gestión de información de seguridad (SIM). Centralización de los registros de seguridad para interpretarlos y almacenarlos en tiempo real, facilitando la actuación inmediata.

Las principales características que posee el sistema SIEM son:

- Identificar entre amenazas reales y falsos incidentes.
- Monitorizar de forma centralizada todas las amenazas potenciales.

- Redirigir la actuación a personal cualificado para resolverlas.
- Aportar un mayor grado de conocimiento sobre los incidentes para facilitar su resolución.
- Documentar todo el proceso de detección, actuación y resolución.
- Cumplir con las normas y legislaciones vigentes en cuestión de protección de datos y seguridad.

6.2.7 Acciones para contención de ataques informáticos:

A nivel de hardware para contener un ataque informático:

Implementación Firewall:
Las principales características relacionadas con la protección con firewall.

- Varios niveles de protección
- Protección de red inalámbrica (Wi-Fi)
- Acceso a Internet y a la red
- Bloqueo contra el acceso no autorizado
- Protección contra malware
- Proporcionar acceso solo a paquetes de datos válidos
- Provisión de diferentes configuraciones
- Provisión de numerosas políticas de seguridad.
- Permitir pasar el tráfico autorizado que cumpla con un conjunto de reglas.
- El cortafuegos funciona como un sistema inmunológico contra el malware y el acceso no autorizado; por lo tanto, garantiza un sistema y un SO seguros.

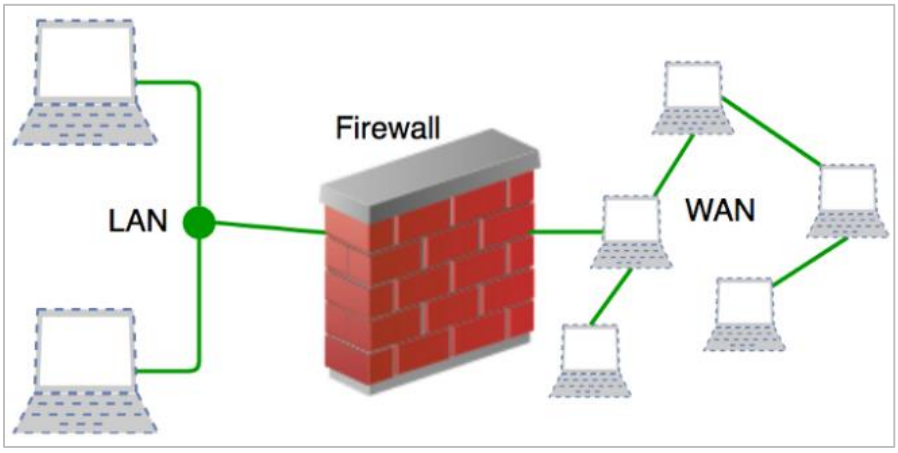


Figura 76 - Tomado de https://medium.com/@hninja049/understanding-firewall-and-functions-and-how-firewall-works-on-computer-networks-dbc5406a36f1

Implantación de DMZ

Una zona desmilitarizada (DMZ) es una red perimetral que protege la red de área local (LAN) interna de una organización del tráfico que no es de confianza.

El principal beneficio de una DMZ es proporcionar una red interna con una capa de seguridad avanzada al restringir el acceso a datos y servidores confidenciales. La DMZ también ofrece beneficios de seguridad adicionales, como:

- ✓ Habilitación del control de acceso:
- ✓ Prevención del reconocimiento de la red
- ✓ Bloqueo de la suplantación de identidad del Protocolo de Internet (IP)

Herramienta IDS

El sistema gratuito de detección de intrusos denominado Snort, es un sistema cuya funcionalidad se ejecuta en un entorno de red en tiempo real. Snort es proporcionado por Cisco Systems y cuenta con un motor para detectar los ataques y realizar un reconocimiento de los puertos, así mismo tiene la

capacidad de registrar, alertar y responder ante cualquier evento que se haya parametrizado y corresponda a cualquier tipo de ataque. Snort permite monitorear el tráfico que entra y sale para reconocer el tráfico que afecta la seguridad. Un punto importante es Snort puede ejecutarse en varios sistemas operativos. Por medio del uso de firmas Snort permite establecer un conjunto de reglas. Existe un grupo amplio de colaboradores a nivel mundial que brindan apoyo y soporte sobre la herramienta. El análisis potente de Snort de da en los puertos. El intento de los hackers de conectarse a otros hosts y escanear sus puertos como iniciadores de otros ataques. Este ejercicio se utiliza para identificar la existencia de hosts en una red o si un servicio en particular está en uso. Estos servicios incluyen correo electrónico, telnet, transferencia de archivos, HTTP y DNS.

Beneficios al utilizar Snort:

- ✓ Respuesta inmediata: permitirá proteger los entornos de ataques emergentes rápidamente. Permite ser personalizado para hacer cumplir sus propias reglas de seguridad.
- ✓ Precisión: reforzará la seguridad sin hacer grandes esfuerzos. Por ser una herramienta gratuita, la comunidad mundial de snort revisa, prueba y ofrece continuamente mejoras al código fuente. De esta manera la empresa se beneficia del conocimiento colectivo de los equipos de seguridad de todo el mundo a medida que sugieren cambios y a bajo costo.
- ✓ Adaptabilidad: este sistema se emplea como base para crear sus propias soluciones de seguridad de red únicas. Tiene fácil acceso al código fuente y a la documentación permitiendo que pueda agregar sus propias funciones.

7 CONCLUSIONES

El presente trabajo identificó los delitos informáticos y su regulación en nuestro país. Colombia logró dar un gran paso con la creación de la ley 1273 del 2009. Con esta norma se amplía el código penal para la protección de la información y de los datos, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Como equipo rojo se recopiló información sobre la pila de tecnología del objetivo. Se inició por descubrir qué sistemas operativos estaban en uso (por ejemplo: Windows, macOS o Linux), cada uno de los cuales contó con sus propias debilidades, identificando la marca y el modelo del equipo de red. Si se planea perpetrar un ataque físico en persona, como robar un disco duro, en lugar de montar un ataque remoto, será necesario validar qué controles físicos existen, como puertas, cerraduras, cámaras y personal de seguridad.

Se llevó a cabo una prueba de penetración en un ambiente controlado, la cual consistió en un ataque simulado autorizado que se realiza en un sistema informático para evaluar su seguridad. Se utilizaron las mismas herramientas, técnicas y procesos que los atacantes para encontrar y demostrar los impactos comerciales de las debilidades de sus sistemas

Cumpliendo el rol de equipo azul se reunieron datos y definimos cuales sistemas debían protegerse y se ejecutó una evaluación de riesgos. Una evaluación de riesgos es el proceso de identificar y analizar amenazas potenciales. Luego se establecieron medidas de seguridad para proteger los activos clave de la organización.

8 RECOMENDACIONES

Conocer la legislación y normativa de seguridad informática en Colombia es fundamental para evitar incurrir en delitos y sanciones penales. De acuerdo de la gravedad de cada delito se establecen penas y sanciones económicas, esto lo podemos conocer en detalle en el documento de cada ley.

Utilizar software antivirus (AV) actualizado, utilizar un firewall de aplicaciones web y controlar la inspección SSL / TLS. Establecer e implementar activamente la seguridad en la configuración de los activos de infraestructura de red, como enrutadores, firewalls y conmutadores.

Administrar los diferentes equipos de hardware en la empresa, de modo que solo tengan acceso los dispositivos autorizados y los no autorizados puedan identificarse y desconectarse rápidamente antes de que causen algún daño

Escanear en busca de vulnerabilidades y volver a verificar el inventario. Así mismo aplicar parches críticos. Rastrear y administrar el uso de puertos, protocolos y servicios en dispositivos de red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes. Rastrear y controlar el uso de redes inalámbricas, acces points y sistemas de clientes inalámbricos.

Registrar eventos para las personas que necesitan acceder ocasionalmente a las instalaciones informáticas, deben ser acompañadas por una persona autorizada, y se les exige que firmen la entrada y la salida en un cuaderno de bitácora que se lleva a tal efecto.

Asegurar de que solo se utilicen navegadores web y clientes de correo electrónico totalmente compatibles para minimizar su superficie de ataque.

Asegurar de poder controlar la instalación y ejecución de código malicioso en múltiples puntos de la empresa. Se deben utilizar herramientas automatizadas de monitoreo continuo para las estaciones de trabajo, dispositivos móviles con antivirus, servidores y anti-spyware, firewalls personales y funcionalidad IPS.

Aplicar una autenticación sólida para limitar el acceso no autorizado y evitar inicios de sesión no autorizados.

Detectar y bloquear la actividad de bots maliciosos (un vector común para los ataques de fuerza bruta y de relleno de credenciales).

Escanear e inventariar todas sus API. Limitar la autorización de la API a las funciones necesarias.

Asegurar de que los sistemas y datos críticos tengan una copia de seguridad adecuada al menos una vez por semana.

Reforzar la autorización de todas las cuentas con el mínimo de privilegios.

Implementar controles criptográficos que comprenden los controles más importantes y efectivos para proteger la información confidencial.

Probar la eficacia y la resistencia de los activos de la empresa mediante la identificación y explotación de las debilidades en los controles (personas, procesos y tecnología) y hacer ver como acciones y objetivos de un atacante.

9 BIBLIOGRAFÍA

Fortinet. Configuración del cortafuegos [en línea]. Importancia de la configuración básica del cortafuegos. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.fortinet.com/resources/cyberglossary/firewall-configuration

CWE. CWE-521: Requisitos de contraseña débil [en línea]. ID debilidad: 521. Consultado el 25 de mayo de 2021. Disponible en Internet: https://cwe.mitre.org/data/definitions/521.html

HORAN, Martin. Weak Password [en línea]. Passwords and Password Controls. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.sciencedirect.com/topics/computer-science/weak-password

CHAUHAN, Sudhanshu. The Biggest Disadvantages and Advantages of FTP [en línea]. FTP Today. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.ftptoday.com/blog/key-advantages-and-disadvantages-of-ftp

JELEN, Sara. Cybersecurity Red Team Versus Blue Team — Main Differences Explained [en línea]. Cibersecurity. Consultado el 25 de mayo de 2021. Disponible en Internet: https://securitytrails.com/blog/cybersecurity-red-blue-team

MILLER, Matt. ¿Qué Es Un Compromiso Del Equipo Rojo? [en línea]. Prueba de penetración. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.triaxiomsecurity.com/what-is-a-red-team-engagement/

Borda Pérez, M. (2013). El proceso de investigación: visión general de su desarrollo. (pp. 80-86). Barranquilla, Colombia: Universidad del Norte. Recuperado de: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/69882

Baena, Paz, Guillermina María Eugenia. (2014). Metodología de la investigación, Grupo Editorial Patria. ProQuest Ebook Central. (pp. 72-78) Recuperado de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/40362

Puerta Aponte, G. (26,11,2018). Proyecto de Seguridad Informática NTC 1486. [Archivo de video]. Recuperado de http://hdl.handle.net/10596/23728

Núñez, Y. S. (2020). Estructura de un Proyecto de Grado. Recuperado de: https://repository.unad.edu.co/handle/10596/3

Borda Pérez, M. (2013). El proceso de investigación: visión general de su desarrollo. 1-79. Barranquilla, Colombia: Universidad del Norte. (pp. 16–21). Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=710213&lang=es&site=eds-live&ebv=EB&ppid=pp_79

Ferreyro, A., & Longhi, A. L. D. (2014). Metodología de la investigación. Córdoba, Argentina: Encuentro Grupo Editor. (pp. 15-34) Recuperado de http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=847674&lang=es&site=eds-live

IDB (2020). CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE. Banco Interamericano de Desarrollo (pp. 20-31) Recuperado de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Bastidas D. (2015). Parafraseo: utilidad y técnicas de elaboración. Universidad de los Andes. (pp. 1-12) Recuperado de https://leo.uniandes.edu.co/index.php/menu-escritura/citas-y-referencias/95-parafraseo-utilidad-y-tecnicas-de-elaboracion

JUCOSA, Martí. El modelo TCP/IP capa a capa [en línea]. Modelo TCP/IP. Consultado el 10 de mayo de 2021. Disponible en Internet: https://aprendederedes.com/redes/introduccion/modelo-tcp-ip/

Oracle Corporation. El modelo TCP/IP capa a capa [en línea]. Guía de administración del sistema: servicios IP. Consultado el 10 de mayo de 2021. Disponible en Internet: https://docs.oracle.com/cd/E19957-01/820-2981/ipov-10/

Hitjethva. Secure The SSH Server On Ubuntu [en línea]. LinuxSSHUbuntu. Consultado el 10 de mayo de 2021. Disponible en Internet: https://aprendederedes.com/redes/introduccion/modelo-tcp-ip/

MILLER, Matt. Ventajas Y Desventajas De Los Compromisos Del Equipo Rojo [en línea]. Cibersecurity. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.triaxiomsecurity.com/advantages-and-disadvantages-of-red-team-engagements/

MILLER, Matt. Ventajas Y Desventajas De Los Compromisos Del Equipo Rojo [en línea]. Cibersecurity. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.triaxiomsecurity.com/advantages-and-disadvantages-of-red-team-engagements/

GLOSARIO. FTP vs SFTP: ¿Cuál es la diferencia?l [en línea]. Diferencia entre FTP y SFTP. Consultado el 25 de mayo de 2021. Disponible en Internet: https://kinsta.com/knowledgebase/ftp-vs-sftp/

CROWDSTRIKE. Definición de equipo rojo vs equipo azul [en línea]. Cibersecurity. Consultado el 25 de mayo de 2021. Disponible en Internet: https://kinsta.com/knowledgebase/ftp-vs-sftp/

IONOS. Por qué debería utilizar SFTP y FTPS en lugar de FTP [en línea]. FTP, SSH y WebDav. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.ionos.com/help/hosting/setting-up-and-managing-ftp-access/why-you-should-use-sftp-and-ftps-instead-of-ftp/

CALVELLO, Mara. Cómo utilizar SFTP para enviar archivos de forma rápida y segura [en línea] Categoría de transferencia de archivos administrada (MFT). Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.g2.com/articles/what-is-sftp

FIRCH, Jason. Tipos comunes de vulnerabilidades de seguridad de red en 2021 [en línea]. Vulnerabilidades en red. Consultado el 25 de mayo de 2021. Disponible en Internet: https://purplesec.us/common-network-vulnerabilities/

CEI. Las 5 vulnerabilidades de red más comunes para las empresas [en línea]. Malware y vulnerabilidades de red. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.copycei.com/5-most-common-network-vulnerabilities-for-businesses/

SIDHARTH, Mutreja. Entrenamiento del equipo rojo y entrenamiento del equipo azul [en línea]. Equipos de seguridad cibernética. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.cyberbit.com/blog/cybersecurity-training/red-team-training-blue-team-training-what-is-the-difference/

EMAGINED. Pruebas de penetración del equipo rojo vs equipo azul [en línea]. ¿Cuál es la diferencia entre el equipo rojo y el equipo azul?. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.cyberbit.com/blog/cybersecurity-training/red-team-training-blue-team-training-what-is-the-difference/

FIRCH, SCHOELFELD. Pruebas de penetración [en línea]. ¿Qué son las pruebas de penetración? Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.imperva.com/learn/application-security/penetration-testing/

SOFTWARETESTINGHELP. Una Guía Completa De Pruebas De Penetración Con Ejemplos De Casos De Prueba [en línea]. Causas de las vulnerabilidades. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.softwaretestinghelp.com/penetration-testing-guide/

UNIR REVISTA. Red Team, Blue Team y Purple Team. [en línea]. Ingeniería Y Tecnología. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.imperva.com/learn/application-security/penetration-testing/

TIM, Matthews. La guía completa para la organización CSIRT: cómo construir un equipo de respuesta a incidentes. [en línea]. ¿Qué es un CSIRT?. Consultado el 25 de mayo de 2021. Disponible en Internet: https://www.imperva.com/learn/application-security/penetration-testing/

10 ANEXOS

Link video Tarea 5:

https://youtu.be/H2Ru2nuzSr0