UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

MODALIDAD: EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA

"ANÁLISIS DE VULNERABILIDADES EN LA RED LAN USANDO HERRAMIENTAS DE HACKING ÉTICO PARA UNA EMPRESA DE LA PROVINCIA DE SANTA ELENA".

AUTOR

SUÁREZ PANCHANA LISSETTE CAROLINA

LA LIBERTAD – ECUADOR

PAO 2021-2

APROBACIÓN DEL TUTOR

En mi calidad de tutor/tutora del trabajo de componente práctico del examen de carácter completivo: **"ANÁLISIS DE VULNERABILIDADES EN LA RED LAN USANDO HERRAMIENTAS DE HACKING ÉTICO PARA UNA EMPRESA DE LA PROVINCIA DE SANTA ELENA"**, elaborado por el/la sr/ta. (a) **SUÁREZ PANCHANA LISSETTE CAROLINA** del Autor, de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

La Libertad, febrero de 2022.

Ing. Lídice Haz López, Msi.

DECLARACIÓN

El contenido del presente componente práctico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Lissette Suárez

Lissette Carolina Suárez Panchana

AGRADECIMIENTO

Agradezco a Dios en primer lugar, por regalarme un día más de vida y la sabiduría que me ha brindado para culminar esta etapa de mi vida y hasta donde he llegado.

A la universidad que me abrió las puertas de su seno científico para poder estudiar mi carrera, así como también a mis formadores, personas de gran sabiduría, que brindaron sus conocimientos, quienes se han esforzado a llegar al punto en el que me encuentro, no ha sido sencillo el proceso, pero gracias a cada uno por la dedicación.

Agradezco a mis docentes guía y mi docente tutor de proyecto, por haberme brindado la oportunidad de recurrir a su capacidad y conocimientos científicos, así como también haberme tenido toda la paciencia del mundo para guiarme durante todo el desarrollo del proyecto.

Mi agradecimiento a la entidad y al encargado del área de TI por haber aceptado que se realice este proceso en su prestigiosa entidad.

A quienes fueron mis compañeros de clases durante todos los niveles de estudios, ya que gracias al compañerismo, amistad y apoyo moral han aportado en un alto porcentaje a mis ganas de seguir adelante en mi carrera profesional.

Lissette Carolina Suárez Panchana

DEDICATORIA

Yo, Lissette Carolina Suárez Panchana, dedico este trabajo a: mis padres, quienes han sido mi apoyo en cada momento y me han brindado las fuerzas por seguir adelante, a mi abuela que está en el cielo, que cada día me brindaba su apoyo incondicional y a mi familia que siempre estamos unidos en las buenas y en las malas.

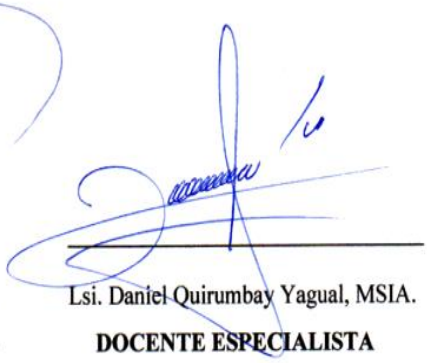
A Dios, que siempre me brinda de su sabiduría para concluir, con cada una de las metas propuestas.

Lissette Carolina Suárez Panchana

TRIBUNAL DE GRADO

Ing. Washington Torres Guin, Mgt.

DIRECTOR DE LA CARRERA DE TECNOLOGÍA DE LA INFORMACIÓN

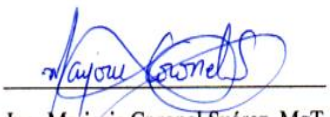


Lsi. Daniel Quirumbay Yagual, MSIA.

DOCENTE ESPECIALISTA

Ing. Lídice Haz López, Msi

DOCENTE TUTOR



Ing. Marjorie Coronel Suárez, MgT.

DOCENTE GUIA UIC

RESUMEN

Las tecnologías de la información cada día están en constante actualización, las empresas públicas y privadas deben contar con sistemas de seguridad. Los ataques a la hora de navegar por internet pueden ser muy diversos, que ponen en riesgos la privacidad y seguridad de los datos. Es por esto que las empresas deben contar con personas especializadas.

El propósito de este proyecto es a un análisis de vulnerabilidades, que consiste en definir, clasificar y priorizar las debilidades, para proporcionar una evaluación de las posibles amenazas previsibles y reaccionar de manera apropiada. Después de haber cumplido con todo el análisis de vulnerabilidades se realizan propuestas de políticas de seguridad informática, cambios en la infraestructura del cableado de red y seguridad en los equipos informáticos, siguiendo los procedimientos establecidos que permiten identificar y reducir a corto o mediano plazo los diferentes riesgos, así como incidentes que involucran la información que pueden ser accidentales o provocados como alteraciones, acceso no autorizados, o en su defecto, fuga o pérdida de información.

CAPÍTULO I

Índice de Ilustración

Índice de Tabla

INTRODUCCIÓN

La seguridad de red combina varias capas de defensa en el perímetro y la red, cada capa de seguridad de red implementa políticas y controles, donde los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad [1].

Las empresas públicas como privadas están siendo el blanco de instrucciones maliciosas debidos a las pocas actualizaciones de los sistemas operativos para Routers y Switches que vienen embebido en estos, también la no implementación de mecanismos de seguridad informáticas han hecho que los mismos estén expuestos a ataques informáticos, denegación de servicios códigos maliciosos, fallas en conexiones a la red y alteración en las configuraciones, es importante realizar un análisis de vulnerabilidad, implementando políticas de seguridad y controles que eviten estos posibles ataques obteniendo el acceso a información de carácter confidencial.

Este documento de componente practico para el examen complexivo está conformado por los siguientes capítulos:

Capítulo I: La fundamentación, donde se identifica el planteamiento del problema, se describen el alcance del proyecto, los objetivos, la justificación, el alcance y metodología del proyecto que es implementada en la entidad pública.

Capítulo II: Se detalla la fundamentación teoría, definiciones conceptuales, herramientas que se implementarán culminando con el desarrollo de la metodología establecida con cada una de las fases del proyecto.

Capítulo III: La propuesta está compuesta por los requerimientos, diagrama de red, con un reporte de las 5 fases planteadas y culminando con sus respectivas conclusiones y recomendaciones**.**

CAPÍTULO I

1 FUNDAMENTACIÓN

1.1 ANTECEDENTES

Los ataques en las redes, en sus primeros años, involucraban poca satisfacción técnica. Los ataques internos se establecían en utilizar los permisos para alterar la información, mientras que los externos se basaban en acceder a la red con el único objetivo de averiguar una clave válida [2]. Con el pasar de los años los ataques, se han desarrollado formas cada vez más sofisticadas para explorar vulnerabilidad en el diseño, configuración y operación de los sistemas [2]. Esto permitió a los nuevos atacantes tomar el control de sistemas completos, provocando caos y en muchos casos llevaron a la desaparición de aquellas organizaciones o empresas con alto grado de dependencia tecnológica (bancos, servicios automáticos, etc.) [3].

Hoy en día, las amenazas pueden ocurrir en cualquier momento, todo sistema de información presenta un riesgo mínimo o relativamente grande; por lo tanto, existe la probabilidad en que una amenaza se concrete por medio de una vulnerabilidad o un punto débil [4].

El establecimiento dedicado al consumo del líquido vital es el sistema que permite llevar el agua potable hasta los domicilios de la población [5], con su único objetivo de brindar la prestación de servicios públicos como alcantarillado sanitario, alcantarillado pluvial, tratamientos de aguas servidas y de agua potable en una población. Cuenta con el apoyo de los gobiernos autónomos descentralizados-municipales de los cantones [6].

No tener medidas de seguridad en la red de las empresas se torna un problema que está en crecimiento, donde los atacantes cada día desarrollan sus habilidades y buscan como extraer información valiosa de cualquier entidad ya sea pública o privada, donde las empresas se ven obligadas a la atención y la vigilancia constantemente en realizar análisis de las vulnerabilidades, de manera que se pueden aplicar las medidas correctas.

Mediante una entrevista (**Ver anexo 1),** al encargo del Área técnica se logró obtener dicha información, que actualmente la empresa cuenta con 20 departamentos, en el cual el servicio de internet se torna saturado sin conocer las razones específicas de la ralentización de la conectividad generando malestar en cada departamento al no poder acceder de manera usual a los servicios y de enviar información valiosa.

La empresa hace varios años, fue atacada por ciberdelincuentes, el hecho ocurrió que uno de los trabajadores no tenía el conocimiento de la importancia de tener cuidado de que es lo que descargamos de internet, en vista que ingresaban a páginas web, desde las máquinas de la empresa y descargaban archivos que no competen a la entidad, donde existió pérdida de información valiosa, debido a que los atacantes encriptaron los datos, solicitando un rescate económico en criptomonedas para liberarlos, ante dicho caso los problemas que hay en dicha institución, se debe que externas personas usan la misma red, no existe control donde se restringe el acceso a sitios de suma importancia y de mayor necesidad, esto permite que un intruso pueda enviar archivos maliciosos a otros usuarios que se encuentran conectados en la misma red.

En varios departamentos los colaboradores, no poseen suficiente conocimiento acerca de recibir correos electrónicos falsos, que en muchos casos nos direccionan a un sitio web suplantado y nos pide el ingreso de información personal, tales como usuario y contraseña, de tal manera que se trata de un ataque de phishing, donde compromete datos de la empresa.

En el Instituto Politécnico Nacional de México, se desarrolló un Modelo de Seguridad para la medición de Vulnerabilidades y reducción de riesgos, que facilitan al administrador de la red conocer dichas vulnerabilidades con el fin de establecer una cultura de seguridad en la institución. [7].

En la Universidad Austral de Chile, uno de los trabajos de titulación: Vulnerabilidades de las redes Tcp/ip y principales mecanismos de seguridad, que uno de sus objetivos fue identificar las vulnerabilidades en una red, analiza los puertos principales donde se frecuenta violaciones por los ciberataques [8]. Con la recolección de datos y el análisis a las vulnerabilidades encontradas se aplicaron mecanismos de seguridad, de esta manera conocer la importancia de los factores que pueden alterar el funcionamiento en el manejo de la información, que es por eso por lo que se debe tener en consideración los factores que perjudican la red.

En nuestro país la Universidad Tecnológica Israel, realiza el tema de Titulación: Análisis de vulnerabilidades para la red LAN de la empresa “HIDROMAG” bajo la metodología “OSSTMM”, que permitió establecer recomendaciones sobre procedimientos de control, políticas, para la administración y protección de la información [2].

Con la recolección de información, herramientas, artículos y demás datos, sirven de base para realizar el análisis a la empresa ya mencionada anteriormente, herramientas utilizadas y metodología aplicada para encontrar las vulnerabilidades, lo cual es uno de los puntos débiles donde existe fuga y pérdida de información, así como también amenazas en los sistemas.

1.2 DESCRIPCIÓN DEL PROYECTO

El proyecto está enfocado a determinar las vulnerabilidades de la red empresarial, de esta manera aplicar mecanismos de seguridad, que permite disminuir vulnerabilidades por ataques de personas externas que desean interceptar información que solo competen a la entidad.

Se toma en cuenta definir las diferentes herramientas o software a utilizar para la recolección de la información, de tal manera poder analizar las posibles causas que hacen vulnerable la red y verificar cuales son los puntos débiles en la misma.

El proyecto está enfocado en 5 fases, que se llevará a cabo para determinar las vulnerabilidades de la red:

Fase de Reconocimiento.

Esta comprendida en un modo de reconocimiento pasivo, comprende la identificación de la topología de red objetivo de la entidad a estudiar, esta fase de iniciación de hacking defensivo se la denomina como footprinting.

Fase de Escaneo.

Se realiza un escaneo de la red mediante la técnica ping sweep, con el objetivo de obtener: equipos activos en la infraestructura de red, examinar dispositivos y de control de acceso, identificación de sistemas operativos, dirección MAC, puertos abiertos, direcciones IP y los recursos compartidos, mediante la herramienta, Advanced IP Scanner, Nmap.

Fases de identificación de vulnerabilidades

El objetivo principal de esta fase de la investigación es identificar, si la red es susceptible a no ser atacado, verificar que tan factible es la seguridad al conectarse en la red. Es indispensable definir grados de prioridades de los datos o información que estén expuestos, evitar la fuga de información.

Se usa también la Técnica Sniffing, que se encarga en captura información que se está enviando de una computadora a otras, esto quiero decir que captura todos los datos o paquetes que circulan por la red de esta forma casi desapercibida, por tal razón esta técnica es una arma de doble filo ya que pueden utilizar tanto como administradores de la red como una herramienta para detectar fallos o anomalías de la red pero también puede ser usado como un espiador de información por usuarios no autorizados.

- Identificar los puertos abiertos.
- Identificar total de usuarios conectados a la red.
- Routers y rutas de transmisión
- Información de protocolos.

Fase de Explotación de vulnerabilidades

Consiste en efectuar varias pruebas con las vulnerabilidades encontradas en la infraestructura de la red, para ellos se realiza:

- **Puerto TCP:** Puerto 22 y 23 administración remota.
  Este escenario es un ataque del puerto 22 y 23 se usa para conexiones de máquinas del departamento de Obras Públicas, protocolo de administración remota, que nos permite controlar y modificar.

Fase de reportes y solución

Se presenta un informe detallado de cada uno de los procesos realizados durante la fase de identificación, que indican con amplia descripción cada una de las vulnerabilidades encontradas, evidenciando con capturas de pantalla de cada proceso y se presentarán mecanismos de seguridad que se pueden llegar a implementar en la empresa.

Dentro de esta fase se recomienda un plan de políticas de seguridad computacional, que permite mejorar la calidad del uso de los recursos tecnológicos de la entidad, a través de estas medidas de seguridad, protegemos la información confidencial de la empresa evitando que usuarios externos puedan interceptar los datos.

Este proyecto contribuirá a la línea de investigación Tecnologías y Gestión de la Información, debido a que la propuesta está relacionada con temas de infraestructura y seguridad de las tecnologías de la información, que permitan generar información indispensable para la toma de decisiones [9].

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Identificar las vulnerabilidades de la red de datos utilizando la metodología de Hacking Ético para mejorar la seguridad informática de la empresa.

1.3.2 OBJETIVOS ESPECÍFICOS

- Identificar el diagrama de la red de datos mediante el reconocimiento de equipos y utilizando la herramienta Scanner IP.
- Analizar las vulnerabilidades encontradas en la red, a través de varias herramientas.
- Presentar un informe con las evidencias obtenidas, siguiendo el proceso de las fases establecidas de la metodología de hacking ético.

1.4 JUSTIFICACIÓN

El fin de realizar un análisis a la red como una herramienta que permita detectar posibles vulnerabilidades mediante herramienta de código abierto, al igual que dar posibles soluciones y controles para disminuir el grado de amenaza expuesto en cada vulnerabilidad y tener en lo posible bajo control de la misma, en la actualidad el contratar a una persona especializada puede ser algo demasiado costoso para las empresas o en el mayor de los casos no le dan importancia de realizar este tipo de análisis.

El levantamiento de información del número de equipos que se encuentran conectados en la red y ciertos departamentos permitirá el control de acceso y de recursos compartidos, Así mismo, con las restricciones en visitar páginas no confiables y descargas de software con infección con este estudio y evidencias recolectadas, se tomará las medidas respectivas de acuerdo con el tipo de vulnerabilidad que se encontró.

El presente proyecto está enfocado al PLAN DE CREACIÓN DE OPORTUNIDADES 2021-2025, haciendo énfasis en el eje 3, el cual detalla lo siguiente:

Eje 3: Seguridad Integral [10].

Objetivo 10: Garantizar la soberanía nacional, integridad territorial y seguridad del Estado [10].

Política 10.1: Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente a amenazas provenientes del Ciberespacio y proteger su infraestructura crítica [10].

1.5 ALCANCE

Se realizará un análisis de vulnerabilidades en una empresa de servicios que se encuentra ubicado en la provincia de Santa Elena. Esto permitirá determinar cuáles son las amenazas con mayores riesgos de materialización en la red de datos de la empresa.

Durante la evaluación y prueba, se tiene en cuenta que la técnica es de caja blanca son pruebas de unos puntos de vista interno enfocado en análisis integral, que evalúa la infraestructura de la red, obtienes información de contraseñas, IPs, logins y todos los demás que se refieren a la red, servidores, estructura y posibles medidas de seguridad, firewalls, etc.

Además, se presenta un informe con los resultados acorde a las necesidades y requerimientos que se presentan en la empresa. Mediante la recolección de información y herramientas utilizadas, no se profundizará en los equipos y software existentes, por lo cual excluimos del estudio.

El presente proyecto abarcará las siguientes fases:

Fase de reconocimiento.

- Identificar la topología de la infraestructura de red.

Fase de escaneo

- Levantamiento de los equipos activos en la infraestructura de red.
- Examinar dispositivos y de control de acceso.
- Identificación de sistemas operativos y dirección MAC.
- Identificación de direcciones IP’s, y los recursos compartidos
- Evitar comprender la integridad de la información.
- Tabular información encontrada.

Fases de identificación de vulnerabilidades

- Hacer el uso de las herramientas para el análisis de las vulnerabilidades.
- Identificar los niveles de control.

- Identificación de los puertos abiertos.
- **Fase de Explotación de vulnerabilidades:**
- Ejecución de pruebas con ayuda del sistema operativo Kali Linux y las herramientas que se llevarán a cabo.

Fase de reportes y control de seguridad

- Documentar cada uno del paso realizado durante el proceso de vulnerabilidades.
- Evidenciar el proceso realizado con captura de pantalla.

CAPÍTULO II

2 MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 MARCO CONCEPTUAL

Durante las últimas décadas, ha habido un cambio de paradigmas en el que los atacantes informáticos intentan explotar las vulnerabilidades en las entidades o instituciones. Para contrarrestar esto, debe cambiar su perspectiva sobre cómo percibe la seguridad, aprender sobre ataques específicos y aprender de ellos para prepararse tanto como sea posible [11]. Todos los días, nuevas amenazas, vulneran la seguridad de las redes informáticas de todo el mundo. Los piratas informáticos se están volviendo cada vez más maliciosos y están interesados en buscar ganancias financieras o incluso en interferir con el sistema para usar varias credenciales [12].

Los ataques ocurren porque los sistemas son vulnerables y ocurren con alguna puerta de entrada. Entre las principales.

Falta de inversión en hardware: las maquinas antiguas que ya no tienen la capacidad de recibir actualizaciones o nuevas fuentes de memoria, necesitan descartarse. Además de ser obsoletas, dificultan la innovación del negocio y cuentan con mayores oportunidades para problemas eléctricos [11].

Falta de inversión en software: empresas proveedoras de soluciones de tecnología difunden nuevos servicios periódicamente y tecnologías que pueden mejorar la TI corporativa, así como complementos que pueden agilizar el trabajo en los negocios. Para cada tipo de empresa y necesidad, existe un software nuevo que puede agregar agilidad al negocio.

Uso de dispositivos externos sin control: pendrives o discos duros externos que estén contaminados por algún tipo de virus y se conecten en alguna máquina conectada a la red, pueden infectar un sistema interno por medio de una entrada simple y de fácil acceso para cualquier persona. Además de eso, se pueden robar datos confidenciales.

Utilización de software no homologado para comunicación: Skype, WhatsApp, Messenger de Facebook, además de otras aplicaciones de mensajes instantáneos pueden comprometer la seguridad de cualquier negocio si existe el intercambio de links

maliciosos o si el usuario recibe algún archivo infectado o incluso por envío de materiales corporativos que sean estratégicos o confidenciales.

Falta de comunicación entre equipos: los miembros de TI deben estar coordinados con el equipo de seguridad digital para combatir amenazas comunes. Mientras que TI debe estar actualizado sobre las potenciales vulnerabilidades de los equipos conectados a la red, el equipo de seguridad debe estar atento a las amenazas más reales y cercanas al negocio.

Herramientas que se pueden utilizar para un escaneo de la red.

Advanced IP Scanner: Una de las herramientas más populares, que permite analizar la red LAN, en corto tiempo, además escanea todos los dispositivos conectados y las carpetas compartidas, de tal manera que ayudará si personas que no tienen nada que ver con la empresa y utilizan este recurso [13].

- **LanSpy:** Herramienta en seguridad de red y escáner de puertos, recopilar la mayor información, del mismo modo auditar la red si presenta problemas de seguridad, mostrar aplicaciones instaladas y no autorizadas, puertos abiertos entre otros [14].
- **Autoscan:** Herramienta que permite el escaneo del host y asignar un recurso, administrar sus servicios [15].
- **Nessus:** La herramienta entre sus usos permite ver los ataques de red en caso de que haya y errores de configuración [16].
- **NMAP:** Es una herramienta de búsqueda de seguridad de sistema informático, así como descubrir servicios en la red [13].
- **Network Scanner:** Escáner de Ip que se utiliza para escanear tanto grandes redes corporativas que tienen cientos de miles computadoras como pequeñas redes domésticas con varias computadoras [14].
- **GNS3:** Es utilizado por cientos de miles de ingenieros de redes en todo el mundo para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube [17].

- **GFI LANGUARD:** Consta de 3 puntos importantes, examinar, analizar y corregir vulnerabilidades de seguridad, por parte del encargado de área [18].

TIPOS DE PENTESTING

- **Caja Blanca:** Se trata de un test más completo y forma parte de un análisis integral de la estructura, con toda la información recolectada es relativamente fácil saber que puede ser modificado o mejorado [19].
- **Caja Negra:** Este tipo de test de instrucción más parecido a un ataque real. Es realizado por personal especializado externo a las organizaciones [19].
- **Caja Gris:** Es la mezcla de los dos anteriores, este tipo de pentest recomendado cuando se contrata a empresas especializadas [19].

2.2 MARCO TEÓRICO

Hacking Ético: ¿Qué es y para qué sirve?

El hacking ético, también conocida como sombrero blanco, es una forma en que un pirata informático conocido puede utilizar todo su conocimiento informático y de ciberseguridad para encontrar vulnerables. Los expertos involucrados en el hacking ético inician una serie de pruebas o pruebas conocidas como "pruebas de penetración" para superar las barreras de seguridad en varias organizaciones, probar la eficacia del desempeño de los sistemas de seguridad y demostrar debilidades y agujeros de seguridad en una red de su sistema [20].

Si se descubre un bug o vulnerabilidad, el hacker debe notificar a la empresa que lo contrató a través de un informe completo y ofrecer una solución para mejorar la seguridad de la información de la organización en cuestión [20].

A diferencia de los hackers de sombrero negro, estos no dañan a su organización, pero se convierten en una parte fundamental de su organización y no puede estar seguro de que sus archivos y actividades sean generalmente seguros [20].

Para conseguirlo, es necesario simular diferentes patrones de ataque empleando herramientas desarrolladas por métodos de ataque conocidos. Algunos de los componentes de un test de penetración son:

- Puertos de seguridad: cortafuegos, programas antivirus, filtros de paquetes, etc.
- Elementos de acoplamiento: puertos, conmutadores o routers.
- Servidores web, de base de datos, de archivos, etc.
- Equipos de telecomunicaciones.
- Aplicaciones web de todo tipo.
- Instalaciones de infraestructura: mecanismos de control de acceso.
- Conexiones inalámbricas: bluetooth, WLAN, etc.

Generalmente, los test de penetración se clasifican en:

- Pruebas de caja negra: los especialistas en hacking ético solo tienen a su disposición la dirección de la red, esto quiere decir que se realiza desde el punto de vista de las entradas y salidas que recibe o produce sin tomar en cuenta el funcionamiento interno.
- Pruebas de caja blanca: el punto de partida es un amplio conocimiento de los sistemas, como la IP, el software utilizado y los componentes de hardware, es decir, se llevan a cabo sobre las funciones internas.

¿Qué es ciberseguridad y su importancia?

La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes [21].

La seguridad de red: Es la práctica de proteger una red informática de los intrusos, ya sean atacantes dirigidos o malware oportunista [21].

La seguridad de las aplicaciones: Se enfoca en mantener el software y los dispositivos libres de amenazas. Una aplicación afectada podría brindar acceso a los datos que está destinada a proteger. La seguridad eficaz comienza en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo [21].

La seguridad de la información: Protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito [21].

La seguridad operativa: Incluye los procesos y decisiones para manejar y proteger los recursos de datos. Los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos se incluyen en esta categoría [21].

La recuperación ante desastres y la continuidad del negocio: Definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos. Las políticas de recuperación ante desastres dictan la forma en que la organización restaura sus operaciones e información para volver a la misma capacidad operativa que antes del evento. La continuidad del negocio es el plan al que recurre la organización cuando intenta operar sin determinados recursos [21].

La capacitación del usuario final: Aborda el factor de ciberseguridad más impredecible: las personas. Si se incumplen las buenas prácticas de seguridad, cualquier persona puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro. Enseñarles a los usuarios a eliminar los archivos adjuntos de correos electrónicos sospechosos, a no conectar unidades USB no identificadas y otras lecciones importantes es fundamental para la seguridad de cualquier organización [21].

TIPOS MAS COMUNES DE ATAQUE DE CIBERSEGURIDAD.

Malware: El término “malware” abarca distintos tipos de ataques, como software espía, virus. El malware explota esta vulnerabilidad para romper la red cuando los usuarios hacen clic en enlaces o archivos adjunto de correo electrónico peligrosos, su finalidad es instalar software malintencionado en los sistemas [22].

El malware es tan común que existe una gran variedad. Entre los más comunes son:

Ransomware: Es la versión malware de la nota de rescate de un secuestrador. Suele funcionar bloqueando o denegando el acceso a su dispositivo y sus archivos hasta que pague un rescate al hacker. Cualquier persona o grupo que guarde información esencial en sus dispositivos corre peligro frente a la amenaza del ransomware [22].

Spyware: Recopila información de un dispositivo o red, que luego será enviada al atacante. Hackers para visualizar la actividad en internet suelen usar el spyware, pueden acceder a datos personales, incluidas credenciales de tarjetas, información financiera o

de inicio de sesión, con el único propósito de robar la identidad o cometer algún fraude [22].

Adware: El objetivo de adware es crear ingreso para el desarrollador sometiendo a las víctimas a publicidad no deseada. Los más comunes son los juegos gratuitos y las barras de herramientas del navegador. Consiguen datos personales acerca de la víctima que después son personalizados para realizar anuncios [22].

Troyanos: Los antiguos poetas griegos hablaban de unos guerreros atenienses que se escondieron en un gigantesco caballo de madera para luego salir del interior, una vez que los troyanos lo arrastraron tras las murallas de la ciudad. Por tanto, un caballo de Troya es un vehículo que oculta atacantes. El malware troyano se infiltra en el dispositivo de una víctima presentándose como software legítimo. Una vez instalado, el troyano se activa y, en ocasiones, llega incluso a descargar malware adicional [22].

Redes de Robots (botnets): Una red de robots no es un tipo de malware, sino una red de equipos o de código informático que puede desarrollar o ejecutar malware. Los atacantes infectan un grupo de equipos con software malicioso conocido como "robots" (o "bots"), capaz de recibir órdenes desde su controlador. A continuación, estos equipos forman una red que proporciona al controlador acceso a una capacidad de procesamiento sustancial. Dicha capacidad puede emplearse para coordinar ataques, enviar spam, robar datos y crear anuncios falsos en su navegador [22].

2.3 METODOLOGÍA DEL PROYECTO

2.3.1 METODOLOGÍA DE INVESTIGACIÓN

Un estudio exploratorio se efectúa cuando no se ha realizado investigaciones previas o existe poca información acerca del objeto de estudio [23]. La presente evaluación de red, no se ha propuesto en la empresa, aunque existe un departamento de Tics, pero no se ha llegado a tal punto de saber qué es lo que ocurre en la red y el uso que le dan en la empresa, de esta manera se realizó la respectiva recolección de información, con revisiones de fuentes bibliográficas, entrevistas y observando métodos que se han llevado a cabo en dicha investigación.

Una investigación diagnóstica es un método de investigación que permite averiguar qué sucede en una situación particular, es decir una serie de eventos que tiene como finalidad identificar los factores que promovieron la aparición de estos eventos [24].

La investigación diagnóstica se realizó mediante entrevista a trabajadores de la empresa, para obtener un mayor conocimiento de la satisfacción y la seguridad en la red. A través de la recopilación de datos, se pudo identificar las necesidades y desarrollar métodos.

2.3.2 TÉCNICAS DE RECOLECIÓN DE INFORMACIÓN.

Para la recolección de información, se realizó entrevistas, fuentes bibliográficas. Mediante la observación se obtuvo información de cada departamento que conforma la entidad, como la infraestructura de red. La directiva de la empresa será beneficiario directo, mediante el análisis con la reducción de vulnerabilidades.

2.4 METODOLOGÍA DE DESARROLLO

Para el desarrollo del presente proyecto se aplicó la metodología general del hacking ético, propuestas en el libro "Seguridad Informática – Hacking Ético: conocer un ataque para una mejor defensa" [25].

Cuando efectuamos un hacking ético fue necesario establecer el alcance del mismo para poder elaborar un cronograma de trabajo ajustado a la realidad, desarrollo de pruebas de penetración y estudios de seguridad, teniendo como marco la posibilidad real de explotación independientemente de los indicadores de riesgos y vulnerabilidades [26].

Basados en los lineamientos de la metodología, el proyecto se enfocó en las fases descritas a continuación.

1. **Reconocimiento:** Dentro de fase de reconocimiento, se realizó la identificación de los objetivos a analizar el proyecto.
2. **Escaneo:** Se realizó un escaneo activo, de los equipos que se encuentran conectados en la red, se obtuvo direcciones IP, MAC, puertos abiertos en la red.
3. **Identificación de Vulnerabilidades:** En esta fase fue analizar la información recolectada anteriormente, de esta manera, comprender si existen inconvenientes en la red.
4. **Explotación de vulnerabilidades:** Comprendió en aplicar herramientas, métodos y técnicas para hacer vulnerables la red.

5. **Reportes y Control de seguridad:** Dentro de la fase de reporte se procedió a realizar un informe detallando lo encontrado de cada una de las fases aplicadas en el desarrollo del proyecto. En base de las vulnerabilidades identificadas se propuso mecanismos de seguridad para evitar que la red sufra posibles ataques.

Ilustración 1 - Fases de Metodología de Hacking Ético

CAPÍTULO III

3 PROPUESTA

3.1 REQUERIMIENTOS

RQ01	Se requiere realizar el reconocimiento de la infraestructura de red y realizar la topología.
RQ02	Para realizar la fase de escaneo se utiliza la herramienta de Kali Linux, para recocer las características de la red.
RQ03	Se requiere la configuración e instalación de aplicaciones según los requerimientos necesarios.
RQ04	Se requiere la instalación del sistema operativo Kali Linux, para trabajar en un entorno virtual.
RQ06	Reconocer los puertos abiertos en la red y determinar sus vulnerabilidades.
RQ07	Se pretende examinar los dispositivos que están conectados en la red, de tal manera tener el control de estos.
RQ08	Para verificar si las contraseñas con robustas, mediante la herramienta Putty.
RQ09	Basado en las evidencias recolectadas se propone mecanismos de seguridad para la red.
RQ10	Es necesario documentar cada proceso que se realiza en las fases.

Tabla 1 - Requerimientos del proyecto

3.2 DESARROLLO FASES HACKING ÉTICO

3.2.1 FASE 1-RECONOCIMIENTO

3.2.1.1 Objetivo de la Fase de Reconocimiento

Recopilar información de la topología de la red, para obtener el esquema de cableado estructurado.

Mediante la observación como técnica de recolección de información, para identificar la ubicación física de cada dispositivo que forma parte de la infraestructura de red, con el uso también de la herramienta Advanced IP Scanner obteniendo los dispositivos activos y no activos en la red.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

"ANÁLISIS DE VULNERABILIDADES EN LA RED LAN USANDO HERRAMIENTAS DE HACKING ÉTICO PARA UNA EMPRESA DE LA PROVINCIA DE SANTA ELENA."

Responsable: Lissette Suárez Panchana	**Nombre de la Fase:** Reconocimiento

Objetivo:

Recopilar información de la topología de la red.

Herramientas tecnológicas aplicadas:

En esta fase con la ayuda de una herramienta que nos permite ver los dispositivos activos y no activos y mediante la observación.

- Advaced Ip Scaner

Técnicas

Mediante la técnica de observación.

Resultados Obtenidos

En el desarrollo de la fase se obtuvo la topología de la red, está conformada por:

- 5 switch Tp-Link marca HP
- 15 departamentos, cada departamento conformado por 4 a 5 máquinas
- Impresoras, fax, 2 servidores.
- Vlan 27 y 28.
- Se pudo obtener los hosts activos con sus respectivos nombres, a través de la herramienta Advanced IP Scanner.
- Se realiza un escaneo más profundo a 2 departamentos:
  - Fiscalización
  - Dirección de recuperaciones.

Tabla 2 - Reporte Fase – Reconocimiento

3.2.2 FASE 2- ESCANEO

Mediante la herramienta de Nmap, se requiere identificar los dispositivos activos en la red para conocer direcciones IP, sistemas operativos y puertos abiertos, habiendo tomado en cuenta en la fase anterior a 2 departamentos.

3.2.2.1 Objetivo Fase de escaneo

Descubrir los hosts activos de la red local que se encuentran en las dos vlan 27 y 28. 192.168.28.1-255 192.168.27.1-255, mediante el uso de las herramientas Nmap de Kali Linux.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

"Análisis de vulnerabilidades en la red LAN usando herramientas de hacking ético para una empresa de la provincia de santa elena."

Responsable: Lissette Suárez Panchana	**Nombre de la Fase:** Escaneo

Objetivo:

Descubrir los hosts activos de la red local que se encuentran en las dos vlan 27 y 28. 192.168.28.1-255 192.168.27.1-255, mediante el uso de las herramientas Nmap de Kali Linux, Avanced ip Scanner.

Herramientas tecnológicas aplicadas:

- Sistema Operativo Kali Linux
- Computador
- Advaced Ip Scaner
- Zenmap

Técnicas

Mediante la técnica de ping sweep se obtiene información

Resultados Obtenidos

Direcciones IP
MAC
Sistema Operativo
Puertos Abiertos
NetBIOS
Servicios

- Se pudo obtener los hosts activos con sus respectivos nombres, a través de las herramientas. **(Ver anexo 3)**
- Se tuvo el acceso a unas de las máquinas, debido que se encontraba en red y habilitados los recursos compartidos. (**Ver anexo 4)**

Tabla 3 - Reporte Fase – Escaneo

3.2.3 FASE 3- IDENTIFICACION DE VULNERABILIDADES

Detectar las vulnerabilidades, que puedan afectar la integridad y seguridad de los equipos y medios de almacenamientos, se procedió a seccionar información obteniendo de esta manera, puertos abiertos en la red, tales como 22 y 23 para conexiones remotas.

En el departamento de fiscalización y dirección de recuperaciones con la herramienta Wireshark, se usó para interceptar el flujo de información en la red, debido que la información es compartida por varias computadoras, lo que hace esto posible es que un solo ordenador puede llegar a capturar la trama de información no destinadas a él.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

"ANÁLISIS DE VULNERABILIDADES EN LA RED LAN USANDO HERRAMIENTAS DE HACKING ÉTICO PARA UNA EMPRESA DE LA PROVINCIA DE SANTA ELENA."

Responsable: Lissette Suárez Panchana	**Nombre de la Fase:** Identificación de vulnerabilidades

Objetivo:

- Determinar las características técnicas en la red
- Identificar si los puertos de red presentan alguna vulnerabilidad

Herramientas tecnológicas aplicadas:

Computador

Técnicas

Mediante la técnica de observación.

Resultados Obtenidos

Para observar el procedimiento llevado a cabo en esta fase. **(Ver anexo 5)**

- Los puertos 22 y 3 destinados a conexiones remotas, se encuentran abiertos.
- Mediante la herramienta Wireshark cualquier protocolo que no está encriptado o cifrado es propenso o vulnerable al Sniffing.
- Sistemas operativos no se encuentran actualizados.

Tabla 4 - Reporte Fase – Identificación de vulnerabilidades.

3.2.4 FASE 4 – EXPLOTACIÓN DE VULNERABILIDADES

Durante el desarrollo de la fase se procedió a elaborar tres tipos de pruebas direccionadas a la red de datos.

- La primera prueba fue en tener acceso al puerto 23 por medio de la herramienta Putty.
- Mediante la técnica de Sniffing Pasivo (STP, CDP, DTP, VTP), se ejecutan una serie de protocolos activos, sin embargo, aunque no se esté interactuando con un computador, los switches, los Routers y demás dispositivos intercambian información, todo es esto puede llegar ser útil para el atacante que se encuentre conectado en la red.
- Mediante el llamado de MAC FLOODING ATTACK-ATAQUE, una capa de enlace de datos actúa como medio de comunicación entre dos hosts conectados directamente.
- Ataque Cracking a 2 puntos AP, mediante la técnica de fuerza bruta.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

"ANÁLISIS DE VULNERABILIDADES EN LA RED LAN USANDO HERRAMIENTAS DE HACKING ÉTICO PARA UNA EMPRESA DE LA PROVINCIA DE SANTA ELENA."

Responsable: Lissette Suárez Panchana	**Nombre de la Fase:** Explotación de vulnerabilidad.

Objetivo:

- Mediante la herramienta Putty tener el acceso al puerto 23 (**Telnet)**
- Limitación de hardware del switch para mantener la tabla relaciona las MAC con los puertos, dicha tabla se denomina CAM.
- La huella dactilar pasiva se basa en rastros de olfatear el sistema remoto. En función de las trazas de sniffer (como Wireshark) de los paquetes, podemos determinar el sistema operativo del host remoto.

Herramientas tecnológicas aplicadas:

- **GNS3, Máquinas virtuales:** MAC Flooding Attack
- **Wireshak:** Snniffing Pasivo
- **Putty:** Puerto 23
- **Cracking Password:** Airmong-ng, Aireplay-ng, Aircrack-ng

Técnicas

La técnica utilizada fue Ataque de inundación de MAC, Sniffing pasivo, Acceso al puerto 23, crackeo de contraseñas mediante fuerza bruta.

Tiempo de Ejecución:

- **MAC Flooding Attack:** 2 departamentos, 2 días diferentes de 3 hora cada ejecución
- **Snniffing Pasivo:** 45 min en preparación y 1 hora en ejecución.
- **Puerto 23:** 10 min de ejecución
- **Cracking Password:** 2 horas en preparación y ejecución.

Resultados Obtenidos

Para comprender el procedimiento de esta fase (**ver anexo 8)**

- Los puertos 22 y 23 destinados a conexiones remotas, se encuentran abiertos **(ver anexo 9)**.
- Mediante la herramienta Wireshark cualquier protocolo que no está encriptado o cifrado es propenso o vulnerable al Sniffing.
- Sistemas operativos no se encuentran actualizados.
- Se realiza el Flooding a los puertos que pertenecen a la misma VLAN del puerto donde se recibió la trama.
- Inundaciones de dirección MAC ficticias afectando el comportamiento de la conmutación de tramas del switch.
- El comportamiento del switch cuando se llena la tabla MAC, este se comporta

como hub enviando tramas recibidas a todos los puertos que pertenecen a la VLANs.

- ❖ Cracking por fuerza bruta no se obtuvo acceso.

Tabla 5 - Reporte Fase – Explotación

3.3 PROPUESTA DE MECANISMO DE SEGURIDAD

3.3.1 CONTROL DE SEGURIDAD (MAC FLOOFING ATTACK)

Dirigido para el departamento de TICs, para este tipo de ataque se debe tomar precauciones para asegurar los sistemas, para lograr eso es habilitando la función de seguridad del puerto usando el comando **SWITCHPORT PORT-SECURITY** se especifica la cantidad máxima de direcciones que se permiten en la interfaz usando el comando de valor **"SWITCHPORT PORT-SECURITY MAXIMUM"**.

Es importante tener en cuenta estos 4 puntos clave:

- Limitación de puertos.
- Asignación estática de direcciones MAC.
- Deshabilitar puertos que no utilicemos.
- Evitar conexiones de otros dispositivos.

3.3.2 CONTROL DE SEGURIDAD (SNIFFER PASIVO)

- A los equipos de seguridad deben monitorear constantemente las redes para detectar actividad anormal mediante el uso de sistemas de detección de intrusos o software de detección y respuesta de punto final. Los equipos de seguridad también deberían usar los mismos programas sniffers que los actores nefastos usan para detectar vulnerabilidades en la red.
- El uso de criptografía de los datos, que consiste en cifrar los datos bajo una serie de códigos que solo pueden ser interpretados con el conocimiento de los mismos. Este método es usado en la mayoría de las páginas WEB donde se requieren datos o contraseñas, ya que estas son de suma importancia y nadie ajeno debe conocerlas.
- Utilizar una VPN (red privada virtual), que cifra todo el tráfico y oculta los sitios WEB, los servicios y las aplicaciones que se utilizan. El empleo generalizado de esta estrategia pudiera dificultar, y quizás imposibilitar, en los próximos años, la tarea del atacante empleando sniffers.

POLIÍTICA GENERAL PARA EL USO ACEPTABLE DE LOS ACTIVOS

El objetivo de establecer políticas para el uso aceptable de los activos informáticos y recursos de red de la Empresa. Todos sus empleados, trabajadores temporales, contratistas, consultores están obligados a cumplir esta política.

GENERAL

- ❖ Todo el personal debe ejercer el buen juicio, con respecto al uso adecuado de los recursos informáticos de acuerdo con las políticas, normas y directrices de la empresa, los recursos no se podrán usar para ningún propósito ilegal o inapropiado.
- ❖ Los equipos informáticos serán asignados a un solo responsable, de tal manera que pueda hacer el bueno uso de estos.
- ❖ El personal que se encuentra en el departamento de TI constantemente debe monitorear y auditar equipos, sistemas y tráfico de red.
- ❖ Los dispositivos o usuarios que accedan a la red de inmediato serán desconectados.
- ❖ Todos los equipos que desean acceder a la red deben ser previamente autentificados o autorizados.

CONCLUSIONES

- Un escaneo de caja gris, basado en una metodología de hacking ético que proporcionó como guía para el proceso de cada una de las fases, permitiendo reconocer las vulnerabilidades de la red, para poder posteriormente analizar y mejorar la seguridad de la infraestructura.

- Realizar un análisis de vulnerabilidad, se debe tener conocimiento acerca de la infraestructura analizada, de tal manera determinar y cruzar información mostrada por los resultados en cada una de las fases que fueron planteadas y así de esta manera determinar cuáles fueron sus vulnerabilidades en los análisis realizados.

- Durante el levantamiento de información sobre los dispositivos, se observó que algunos de los equipos no cuentan con las actualizaciones constantes exponiéndolos a cualquier ataque informático provocando que la información de la empresa se vea expuesta.

- Kali Linux nos brinda varias herramientas para el uso de hacking ético, las cuales nos permitió conocer los puertos abiertos, como también el sistema operativo y así tener una mejor visión de la seguridad para tomar decisiones que mejoren la seguridad en la empresa.

RECOMENDACIONES

- El departamento de TI deberá efectuar pruebas y análisis de los equipos que presenten fallas o características obsoletas para comprobar que tales equipos no pueden ser reubicados dentro de la entidad y que no son de utilidad para la misma.

- Se recomienda capacitar a los trabajadores, que eviten mantener el registro de contraseñas en texto claro en cualquier parte de la oficina, sea esto en un papel, archivo de software o dispositivo de mano.

- Instalación y actualización regular de programas de antivirus que analicen las máquinas y dar soporte de forma rutinaria o como un control preventivo para la detección y eliminación de código malicioso, la comprobación de archivos en medios electrónico u ópticos, archivos recibidos por correo electrónico.

BIBLIOGRAFÍA

[1] C. N. Academy, «Cisco,» [En línea]. Available: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html. [Último acceso: 2021].

[2] N. N. E. ANDRES, 2019. [En línea]. Available: http://repositorio.uisrael.edu.ec/bitstream/47000/2044/1/UISRAEL-EC-SIS-378.242-2019-028.pdf.

[3] R. S. Peláez, «Análisis de seguridad de la familia de protocolos TCP/IP y sus servicios asociados,» de *Hacking TCP/IP Security*, 1 Edicion, 202, p. 143.

[4] N. R. Sanhez, «Tech Club (Tajamar),» 20 Febrero 2017. [En línea]. Available: https://techclub.tajamar.es/vulnerabilidades-en-redes/.

[5] OXFAM, 2017. [En línea]. Available: https://blog.oxfamintermon.org/la-importancia-del-abastecimiento-de-agua/.

[6] A. EP, «Aguapen EP,» [En línea]. Available: aguapen.gob.ec/index.php/institucion/quienes-somos.

[7] C. M. E. IVAN, Nobiembre 2010. [En línea]. Available: https://tesis.ipn.mx/bitstream/handle/123456789/8428/IF2.52.pdf?sequence=1&isAllowed=y.

[8] M. A. R. Gutierrez, «Cybertesis,» 2009. [En línea]. Available: http://cybertesis.uach.cl/tesis/uach/2009/bmfcir564v/doc/bmfcir564v.pdf.

[9] Upse, «FACSISTEL,» [En línea]. Available: http://facsistel.upse.edu.ec/index.php?option=com_content&view=article&id=58&Itemid=463. [Último acceso: 21 Abril 2021].

[10] S. N. D. D. PLANIFICACIÓN, «PLAN DE CREACION DE OPORTUNIDADES 2021-2025,» 2021. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf. [Último acceso: 2021].

[11] SYNNEX, «DIFITAL.LA,» 23 OCTUBRE 2018. [En línea]. Available: https://digital.la.synnex.com/8-tipos-principales-de-vulnerabilidad-de-seguridad-en-las-empresas.

[12] R. Ramiro, «CIBERSEGURIDAD,» 20 ENERO 2018. [En línea]. Available: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/. [Último acceso: 09 05 2021].

[13] C. Kumar, «GEEKFLARE,» 28 NOVIEMBRE 2020. [En línea]. Available: https://geekflare.com/es/network-scanner/.

[14] LizardSystems, «LizardSystems,» [En línea]. Available:

https://lizardsystems.com/products/.

[15] «Softfonic,» 2007. [En línea]. Available: https://autoscan-network.softonic.com/.

[16] «gb-advisors,» [En línea]. Available: https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/.

[17] G. T. LLC, «Primeros pasos con GNS3,» 2012. [En línea]. Available: https://docs.gns3.com/docs/#:~:text=GNS3%20is%20used%20by%20hundreds,even%20hosted%20in%20the%20cloud..

[18] G. LanGuard. [En línea]. Available: https://manuals.gfi.com/es/languard/content/acm/topics/about/how_gfi_languard_works.htm.

[19] E. C. I. d. C. p. a. E. I. B. School, «ENIIT,» [En línea]. Available: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting. [Último acceso: 2021].

[20] C. Valencia, «Tecnologia para los negocios,» 2018. [En línea]. Available: https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/. [Último acceso: Diciembre 2021].

[21] A. K. Lab, «Kaspersky,» 2021. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Último acceso: Diciembre 2021].

[22] I. Belcic, «Avast,» 19 Mayo 2021. [En línea]. Available: https://www.avast.com/es-es/c-malware. [Último acceso: 12 Septiembre 2021].

[23] R. Hernández Sampieri, C. Fernández Collado y P. Baptista Lucio, METODOLOGIA DE LA INVESTIGACION, México: Mc Graw Hill Education, 1998.

[24] G. González, «Lifeder,» [En línea]. Available: https://www.lifeder.com/investigacion-diagnostica/. [Último acceso: 26 Abril 2021].

[25] M. A. -. D. B. -. R. C. -. Davi, «Seguridad Informatica- Hacking Etico,» de *Conocer el ataque para una mejor defensa*, Ediciones ENI, 2018, p. 810.

[26] K. A. B, «FASES DE HACKING ETICO,» de *HACKING ETICO 101*, IEPI, 2013, p. 292.

[27] VmWare, «wmwareLatam,» VMware, Inc, [En línea]. Available: https://www.vmware.com/latam/products/workstation-pro/workstation-pro-evaluation.html. [Último acceso: 21 Abril 2021].

ANEXOS

ANEXO 1

Formato de entrevista.

Universidad Estatal Península de Santa Elena

Salinas – La Libertad

Entrevista al Tema de Proyecto de Titulación

ANÁLISIS DE VULNERABILIDADES EN REDES IP Y MECANISMOS DE SEGURIDAD PARA LA EMPRESA DE AGUA POTABLE

Objetivo: La presente entrevista tiene como objetivo conocer el estado actual de la red y de su seguridad, con la finalidad de realizar un estudio sobre las vulnerabilidad y recomendaciones para el control de la empresa.

Nombre: _____

Profesión: _____

Cargo Laboral: _____

Preguntas:

1.- ¿Cuenta con una conexión estable a internet de la empresa?

2.- ¿La empresa permite acceso limitado a los empleados para navegar en internet? ¿Cuáles son esas restricciones?

3.- ¿Cree usted que la empresa permite a usuarios externos que usen los recursos de la red?

4.- ¿En los últimos años ha sufrido un ataque por los ciberdelincuentes? ¿Qué tipo te ataque?

5.- ¿Conoce usted si empresa utiliza firewall u otros controles de acceso en los perímetros de la red para proteger los recursos?

6.- ¿Qué tipo de controles utiliza la empresa para cumplir las políticas de seguridad por contraseñas en todas las cuentas?

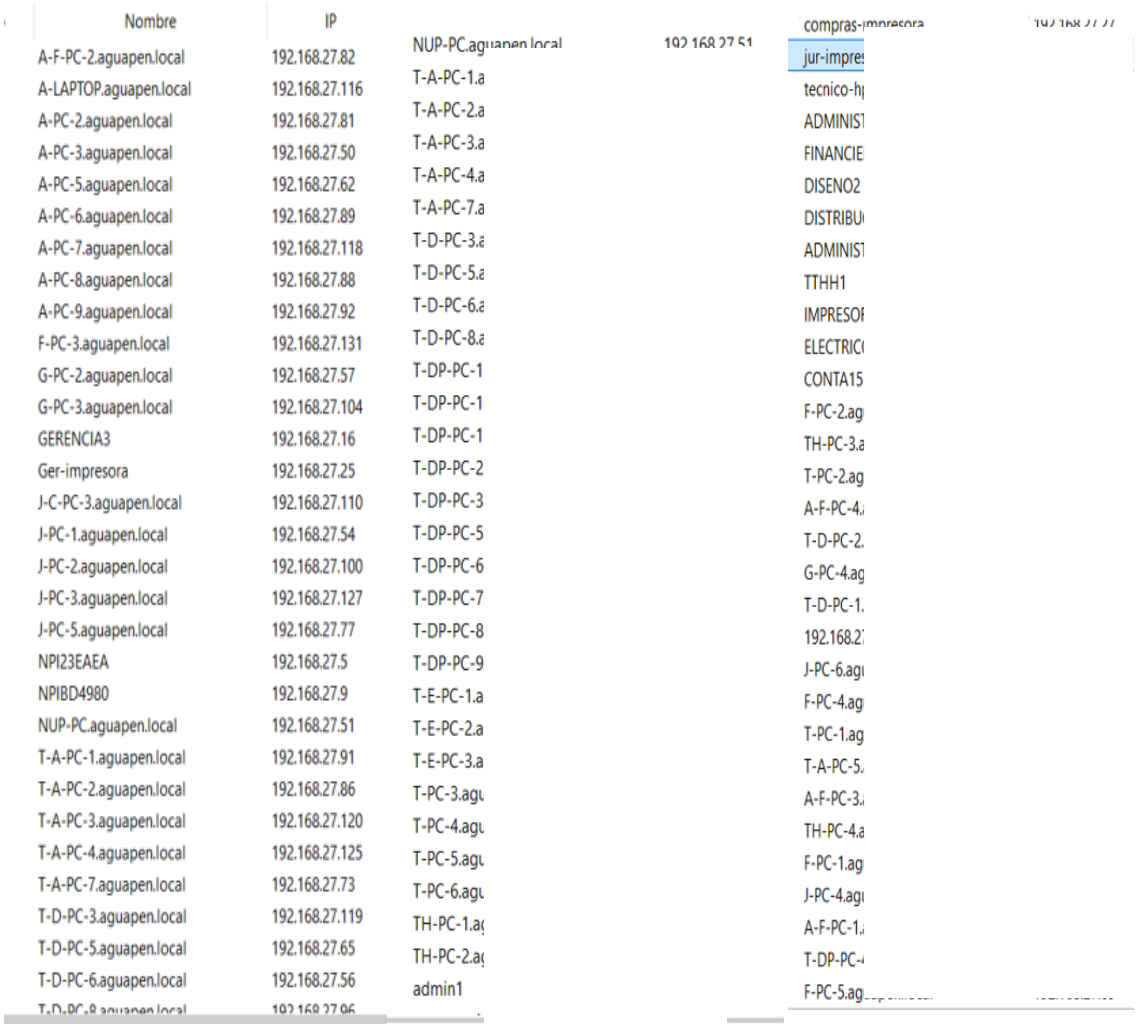
ANEXO 2

Desarrollo de la fase de reconocimiento

Para esta fase utilizamos la herramienta Advanced IP Scanner.

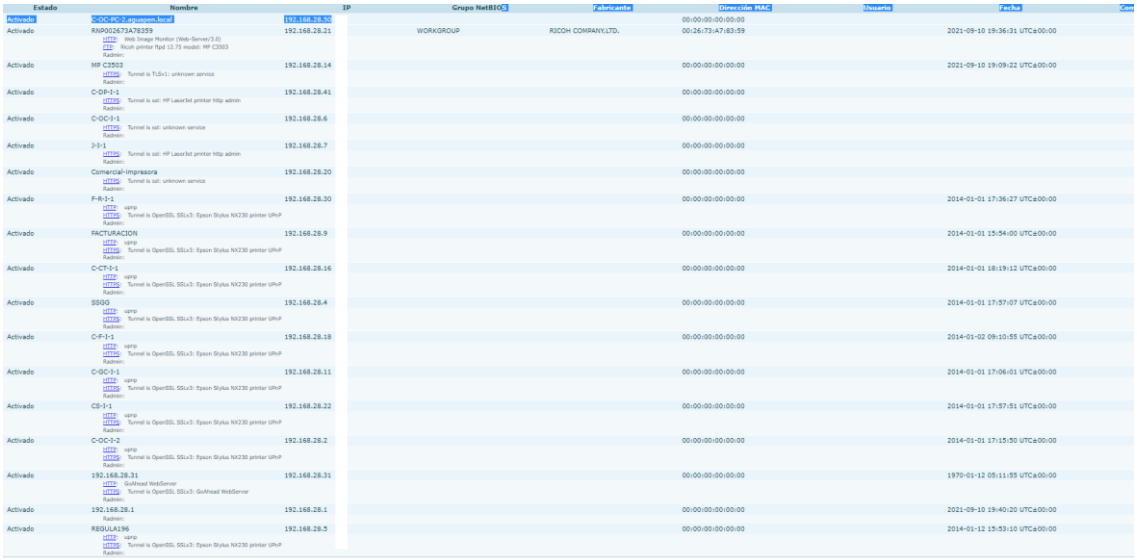
A continuación, fue instalada en Windows 10

VLAN 27



Nombre	IP
A-F-PC-2.aguapen.local	192.168.27.82
A-LAPTOP.aguapen.local	192.168.27.116
A-PC-2.aguapen.local	192.168.27.81
A-PC-3.aguapen.local	192.168.27.50
A-PC-5.aguapen.local	192.168.27.62
A-PC-6.aguapen.local	192.168.27.89
A-PC-7.aguapen.local	192.168.27.118
A-PC-8.aguapen.local	192.168.27.88
A-PC-9.aguapen.local	192.168.27.92
F-PC-3.aguapen.local	192.168.27.131
G-PC-2.aguapen.local	192.168.27.57
G-PC-3.aguapen.local	192.168.27.104
GERENCIA3	192.168.27.16
Ger-impresora	192.168.27.25
J-C-PC-3.aguapen.local	192.168.27.110
J-PC-1.aguapen.local	192.168.27.54
J-PC-2.aguapen.local	192.168.27.100
J-PC-3.aguapen.local	192.168.27.127
J-PC-5.aguapen.local	192.168.27.77
NPI23EAEA	192.168.27.5
NPIBD4980	192.168.27.9
NUP-PC.aguapen.local	192.168.27.51
T-A-PC-1.aguapen.local	192.168.27.91
T-A-PC-2.aguapen.local	192.168.27.86
T-A-PC-3.aguapen.local	192.168.27.120
T-A-PC-4.aguapen.local	192.168.27.125
T-A-PC-7.aguapen.local	192.168.27.73
T-D-PC-3.aguapen.local	192.168.27.119
T-D-PC-5.aguapen.local	192.168.27.65
T-D-PC-6.aguapen.local	192.168.27.56

VLAN 28



Estado	Nombre	IP	Grupo NetBIOS	Fabricante	Dirección MAC	Usuario	Fecha	Comentarios
Activado	C-OC-PC-2.aguapan.local	192.168.28.50			00:00:00:00:00:00			
Activado	RNP002673A7B359 HTTP: Web Image Monitor (Web-Server/3.0) P9100: Ricoh printer ftpd 12.75 model: MP C3503 Radmin:	192.168.28.21	WORKGROUP	RICOH COMPANY,LTD.	00:26:73:A7:B3:59		2021-09-10 19:36:31 UTC±00:00	
Activado	MP C3503 HTTPS: Tunnel is TLSv1: unknown service Radmin:	192.168.28.14			00:00:00:00:00:00		2021-09-10 19:09:22 UTC±00:00	
Activado	C-DP-I-1 HTTPS: Tunnel is ssl: HP LaserJet printer http admin Radmin:	192.168.28.41			00:00:00:00:00:00			
Activado	C-OC-I-1 HTTPS: Tunnel is ssl: unknown service Radmin:	192.168.28.6			00:00:00:00:00:00			
Activado	J-I-1 HTTPS: Tunnel is ssl: HP LaserJet printer http admin Radmin:	192.168.28.7			00:00:00:00:00:00			
Activado	Comercial-impresora HTTPS: Tunnel is ssl: unknown service Radmin:	192.168.28.20			00:00:00:00:00:00			
Activado	F-R-I-1 HTTP: upnp HTTPS: Tunnel is OpenSSL SSLv3: Epson Stylus NX230 printer UPnP Radmin:	192.168.28.30			00:00:00:00:00:00		2014-01-01 17:36:27 UTC±00:00	
Activado	FACTURACION HTTP: upnp HTTPS: Tunnel is OpenSSL SSLv3: Epson Stylus NX230 printer UPnP Radmin:	192.168.28.9			00:00:00:00:00:00		2014-01-01 15:54:00 UTC±00:00	
Activado	C-CT-I-1 HTTP: upnp HTTPS: Tunnel is OpenSSL SSLv3: Epson Stylus NX230 printer UPnP Radmin:	192.168.28.16			00:00:00:00:00:00		2014-01-01 18:19:12 UTC±00:00	
Activado	SSOO HTTP: upnp HTTPS: Tunnel is OpenSSL SSLv3: Epson Stylus NX230 printer UPnP Radmin:	192.168.28.4			00:00:00:00:00:00		2014-01-01 17:57:07 UTC±00:00	
Activado	C-F-I-1 HTTP: upnp HTTPS: Tunnel is OpenSSL SSLv3: Epson Stylus NX230 printer UPnP Radmin:	192.168.28.18			00:00:00:00:00:00		2014-01-02 09:10:55 UTC±00:00	
Activado	C-GC-I-1 HTTP: upnp HTTPS: Tunnel is OpenSSL SSLv3: Epson Stylus NX230 printer UPnP Radmin:	192.168.28.11			00:00:00:00:00:00		2014-01-01 17:06:01 UTC±00:00	
Activado	CS-I-1 HTTP: upnp HTTPS: Tunnel is OpenSSL SSLv3: Epson Stylus NX230 printer UPnP Radmin:	192.168.28.22			00:00:00:00:00:00		2014-01-01 17:57:51 UTC±00:00	
Activado	C-OC-I-2 HTTP: upnp HTTPS: Tunnel is OpenSSL SSLv3: Epson Stylus NX230 printer UPnP Radmin:	192.168.28.2			00:00:00:00:00:00		2014-01-01 17:15:50 UTC±00:00	
Activado	192.168.28.31 HTTP: GoAhead WebServer HTTPS: Tunnel is OpenSSL SSLv3: GoAhead WebServer Radmin:	192.168.28.31			00:00:00:00:00:00		1970-01-12 05:11:53 UTC±00:00	
Activado	192.168.28.1 Radmin:	192.168.28.1			00:00:00:00:00:00		2021-09-10 19:40:20 UTC±00:00	
Activado	REGULA196 HTTP: upnp HTTPS: Tunnel is OpenSSL SSLv3: Epson Stylus NX230 printer UPnP Radmin:	192.168.28.5			00:00:00:00:00:00		2014-01-12 15:53:10 UTC±00:00	

Estado	Nombre	IP	Grupo NetBIOS	Fabricante	Dirección MAC	Usuario	Fecha	Comentarios
Activado	turnero11 ocal	192.168.28.62	WORKGROUP	BIOSTAR Microtech Int'l Corp.	B8:97:5A:96:D0:46		2021-09-10 14:49:36 UTC-05:00	
Activado	C-GS-PC- ocal	192.168.28.57	AG	PEGATRON CORPORATION	E8:40:F2:5F:FE:0B			
Activado	C-SC-PC- ocal	192.168.28.70	AG	Hewlett Packard	A0:8C:FD:2B:67:2C		2021-09-10 14:50:33 UTC-05:00	
Activado	C-SC-PC- ocal RDP: soft SChannel TLS: unknown service	192.168.28.58	AC	Hewlett Packard	A0:8C:FD:2B:2E:8D			
Activado	T-F-PC-1. al RDP: soft SChannel TLS: unknown service	192.168.28.59			00:00:00:00:00:00			
Activado	C-F-PC-7 al	192.168.28.61			00:00:00:00:00:00			
Activado	S-PC-2.ag	192.168.28.67			00:00:00:00:00:00			
Activado	F-R-PC-1 al RDP: soft SChannel TLS: unknown service	192.168.28.68	AC		00:00:00:00:00:00		2021-09-10 14:52:32 UTC-05:00	
Activado	C-R-PC-4 al	192.168.28.69	AG	EliteGroup Computer Systems Co., LTD	94:C6:91:1E:1B:D9			
Activado	C-SC-PC- ocal RDP: soft SChannel TLS: unknown service	192.168.28.60	AGU	Hewlett Packard	A0:8C:FD:2B:2C:0E		2021-09-10 14:51:45 UTC-05:00	
Activado	SEGURID .local	192.168.28.55			00:00:00:00:00:00			
Activado	C-T-PC-3. al RDP: soft SChannel TLS: unknown service	192.168.28.51			00:00:00:00:00:00			
Activado	RECEPCI(local	192.168.28.56			00:00:00:00:00:00			
Activado	C-OC-PC- ocal	192.168.28.54			00:00:00:00:00:00		2021-09-10 14:50:47 UTC-05:00	

Estado	Nombre	IP	Grupo NetBIOS	Fabricante	Dirección MAC	Usuario	Fecha	Comentarios
Activado	C-DP-PC-1.a	192.168.28.100	AG	PEGATRON CORPORATION	7C:05:07:35:85:6B		2021-09-10 14:57:56 UTC-05:00	
Activado	C-F-PC-2.ag	192.168.28.93	AGU	PEGATRON CORPORATION	7C:05:07:35:99:9D		2021-09-10 14:59:03 UTC-05:00	
	RDP: Tu Channel TLS: unknown service							
Activado	C-SC-PC-6.a	192.168.28.88		Dell Inc.	50:9A:4C:1C:10:B6			
Activado	C-OC-PC-6.	192.168.28.74	AC	PEGATRON CORPORATION	7C:05:07:35:9E:F1		2021-09-10 14:59:03 UTC-05:00	
	RDP: Tu Channel TLS: unknown service							
Activado	C-F-PC-4.ag	192.168.28.71	AG	EliteGroup Computer Systems Co., LTD	94:C6:91:1E:22:5F			
Activado	C-DP-PC-7.	192.168.28.84			00:00:00:00:00:00			
Activado	C-OC-PC-3.	192.168.28.82			00:00:00:00:00:00			
Activado	C-T-PC-1.ag	192.168.28.96			00:00:00:00:00:00			
	RDP: Tu Channel TLS: unknown service							
Activado	C-DP-PC-4.	192.168.28.72			00:00:00:00:00:00			
Activado	C-SC-PC-2.	192.168.28.86			00:00:00:00:00:00			
Activado	C-OC-PC-1.	192.168.28.79			00:00:00:00:00:00			
Activado	C-GC-PC-4.	192.168.28.83	A		00:00:00:00:00:00		2021-09-10 14:57:58 UTC-05:00	
Activado	C-OC-PC-4.	192.168.28.80	AC		00:00:00:00:00:00		2021-09-10 14:57:59 UTC-05:00	
Activado	C-F-PC-6.ag	192.168.28.89	AG	PEGATRON CORPORATION	7C:05:07:35:A0:41			
Activado	C-PC-1.agu	192.168.28.98	AGU	Hewlett Packard	A0:8C:FD:2B:2E:8A		2021-09-10 19:57:53 UTC±00:00	
Activado	F-R-PC-4.ag	192.168.28.75	A	Hewlett Packard	A0:8C:FD:2B:2E:00		2021-09-10 14:59:06 UTC-05:00	
	RDP: Tu Channel TLS: unknown service							
Activado	A-SG-PC-1.	192.168.28.85	AG	AIO LCD PC BU / TPV	00:25:AB:53:0B:08		2021-09-10 14:58:00 UTC-05:00	
Activado	C-OC-PC-7.	192.168.28.73			00:00:00:00:00:00			
Activado	T-F-PC-2.ag	192.168.28.78			00:00:00:00:00:00			
Activado	C-DP-PC-2.	192.168.28.99			00:00:00:00:00:00			
Activado	C-OC-PC-5.	192.168.28.77			00:00:00:00:00:00			
Activado	CS-PC-2.ag	192.168.28.90			00:00:00:00:00:00			
Activado	A-SG-PC-2.	192.168.28.87			00:00:00:00:00:00			
Activado	CS-MAC Radmin:	192.168.28.91			00:00:00:00:00:00			
Activado	CS-PC-5.ag	192.168.28.92			00:00:00:00:00:00			
Activado	TURNERO.a	192.168.28.97			00:00:00:00:00:00			

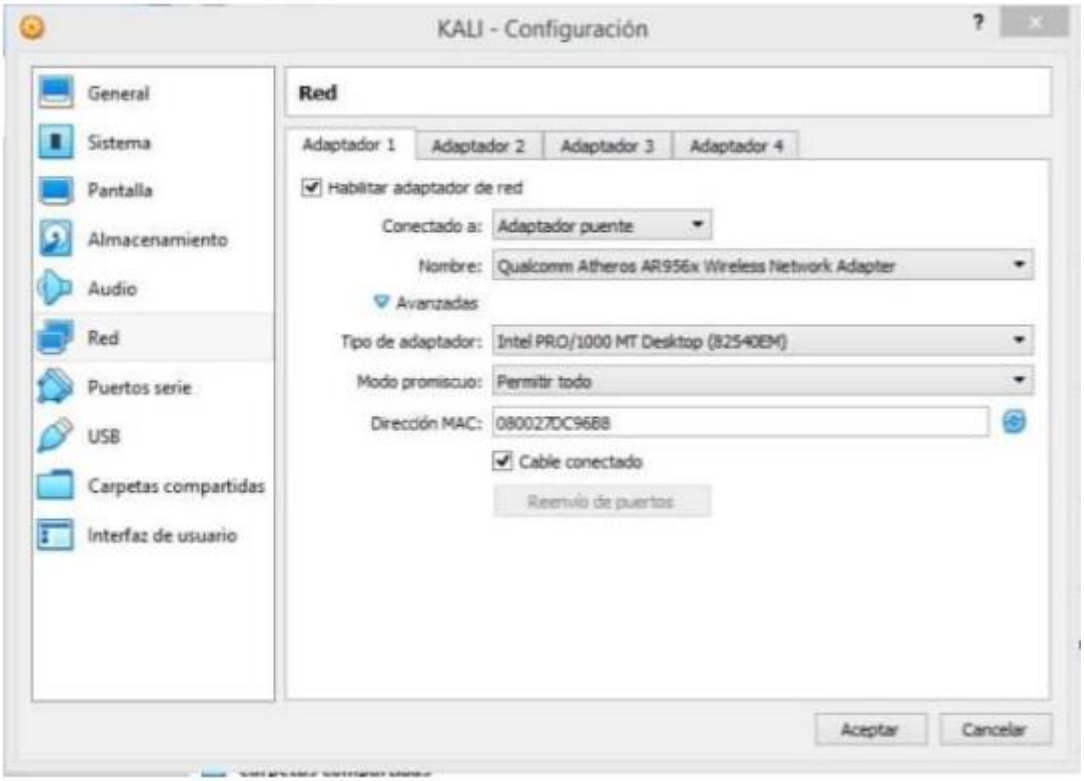
ANEXO 3

DESARROLLO DE LA FASE DE ESCANEO DE PUERTOS

En esta fase utilizamos 2 herramientas, la primera fue instalada en Windows 10 y el sistema operativo Kali Linux, la herramienta llamada NMAP.

Los siguientes pasos para realizar el escaneo de red.

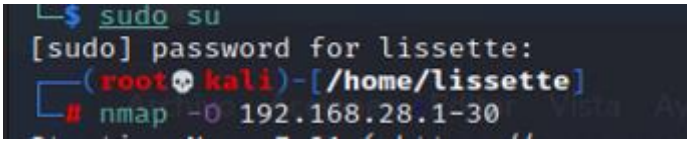
1. La máquina virtual antes de iniciar debe estar configurada en adaptador puente, para que la máquina que se encuentre forme parte de la red.



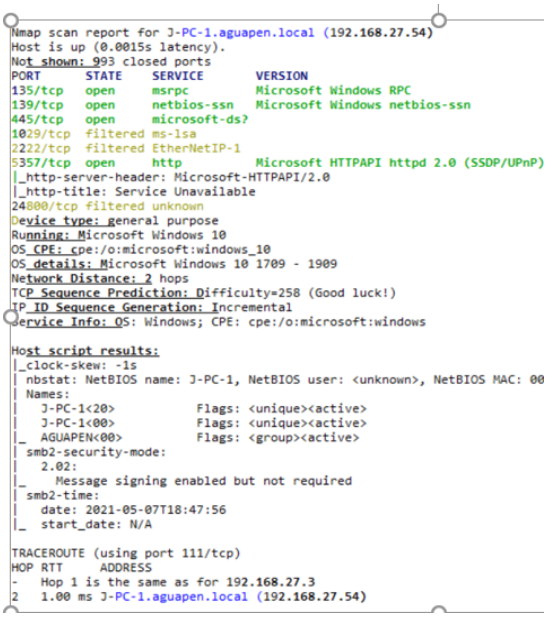
2. Una vez ejecutado los cambios, procedemos a iniciar la máquina virtual.

3. Luego abrimos una terminal, para ejecutar los comandos. Debemos iniciar como super usuario, por lo tanto, escribiremos sudo su y procederemos a digitar nuestra contraseña de usuario.
4. Escribimos Nmap --help para verificar que el programa se encuentre instalado en el sistema operativo. Si esto es correcto, debería de salir todas las funciones y comandos de la herramienta, de no ser así nos tocaría actualizar las librerías para instalarlo.

5. Después de haber hecho el proceso de verificación, pasaremos a digitar el comando para el escaneo, Nmap -O 192.168.28.1.0-35. El ultimo parámetro es el rango de direcciones IP que vamos a escanear, es decir que comenzará desde la 0 y terminará en la IP 35.

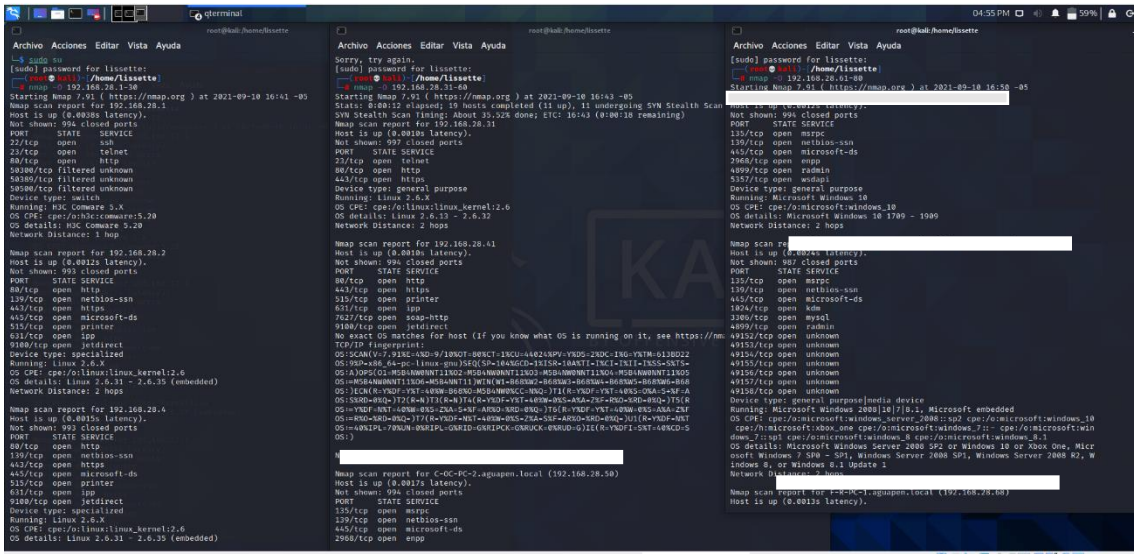


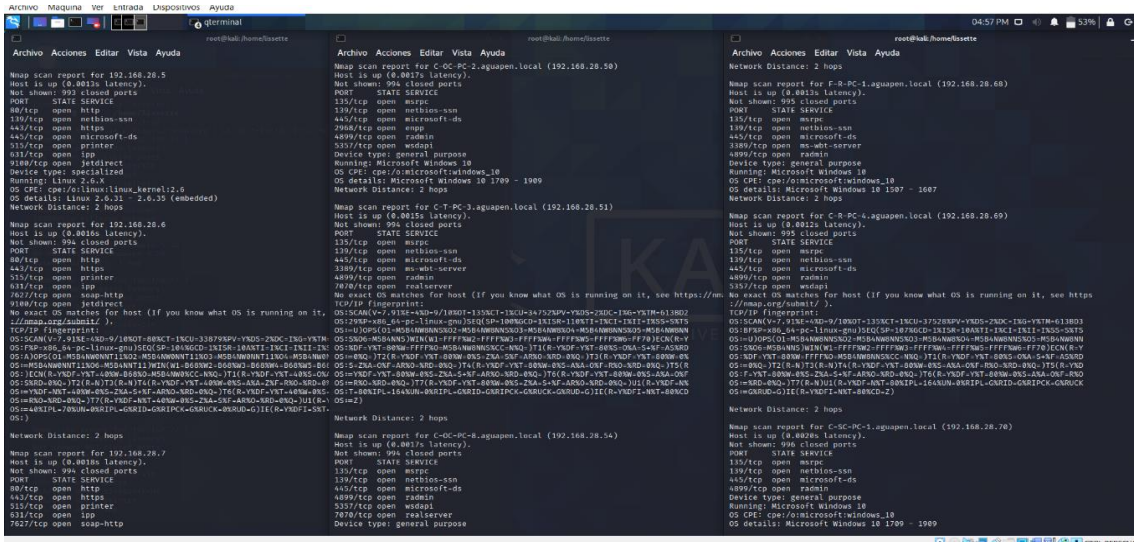
6. Iniciamos el escaneo y esperaremos que culmine para obtener la información que necesitamos.

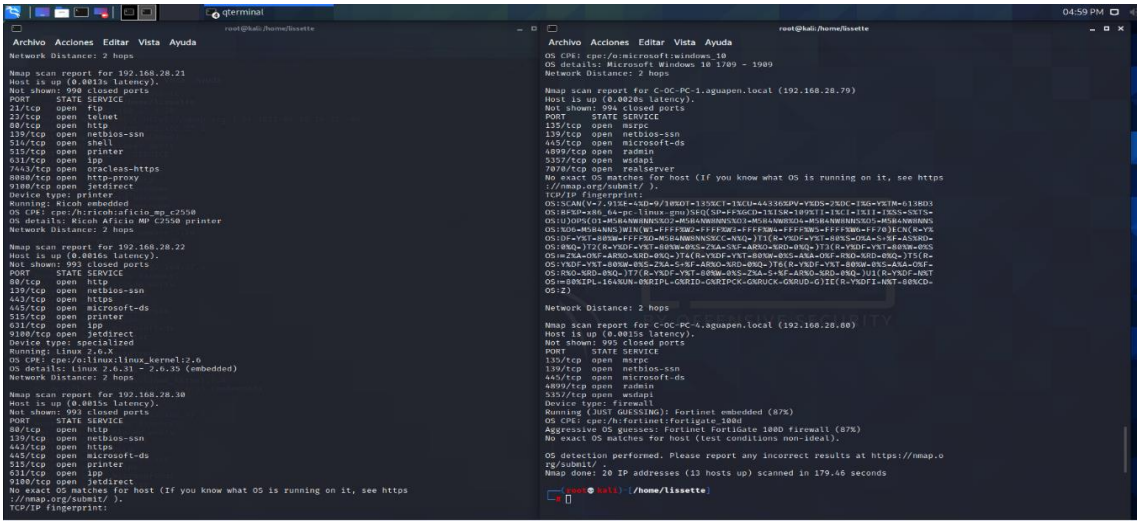


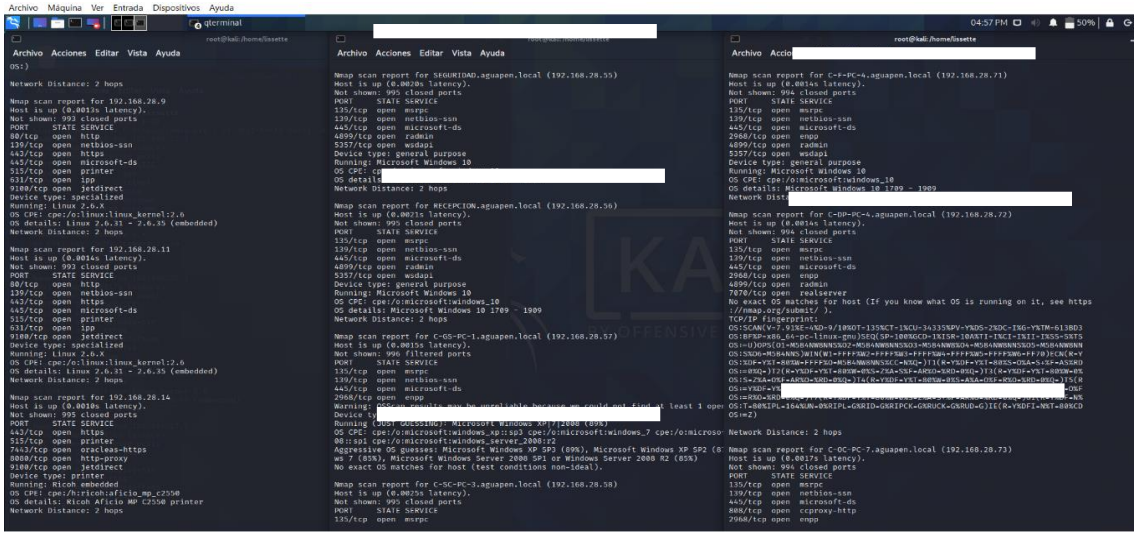
```
Nmap scan report for J-PC-1.aguapen.local (192.168.27.54)
Host is up (0.0015s latency).
Not shown: 993 closed ports
PORT      STATE    SERVICE       VERSION
135/tcp   open     msrpc         Microsoft Windows RPC
139/tcp   open     netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds?
1029/tcp  filtered ms-lsa
2222/tcp  filtered EtherNetIP-1
5357/tcp  open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
24800/tcp filtered unknown
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -1s
| nbstat: NetBIOS name: J-PC-1, NetBIOS user: <unknown>, NetBIOS MAC: 00
| Names:
|   J-PC-1<20>           Flags: <unique><active>
|   J-PC-1<00>           Flags: <unique><active>
|_  AGUAPEN<00>          Flags: <group><active>
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-07T18:47:56
|_  start_date: N/A

TRACEROUTE (using port 111/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 192.168.27.3
2   1.00 ms J-PC-1.aguapen.local (192.168.27.54)
```

```
Nmap scan report for 192.168.27.100
Host is up (0.0033s latency).
Not shown: 993 closed ports
PORT      STATE    SERVICE       VERSION
135/tcp   open     msrpc         Microsoft Windows RPC
139/tcp   open     netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds?
2034/tcp  filtered scoremgr
4899/tcp  open     radmin        Famatech Radmin 3.X (Radmin Aut
5357/tcp  open     http          Microsoft HTTPAPI httpd 2.0 (SS
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
49163/tcp filtered unknown
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (98%), M
(96%), Microsoft Windows Longhorn (94%), Microsoft Windows 10 17
(93%), Microsoft Windows 8 (93%), Microsoft Windows 10 1809 - 19
2008 R2 (92%), Microsoft Windows 8.1 Update 1 (92%), Microsoft W
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=241 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: J-PC-2, NetBIOS user: <unknown>, NetBIOS
Packard)
| Names:
|   J-PC-2<20>           Flags: <unique><active>
|   J-PC-2<00>           Flags: <unique><active>
|_  AGUAPEN<00>          Flags: <group><active>
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-07T18:49:15
|_  start_date: N/A

TRACEROUTE (using port 111/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 192.168.27.3
2   1.00 ms J-PC-2.aguapen.local (192.168.27.100)
```



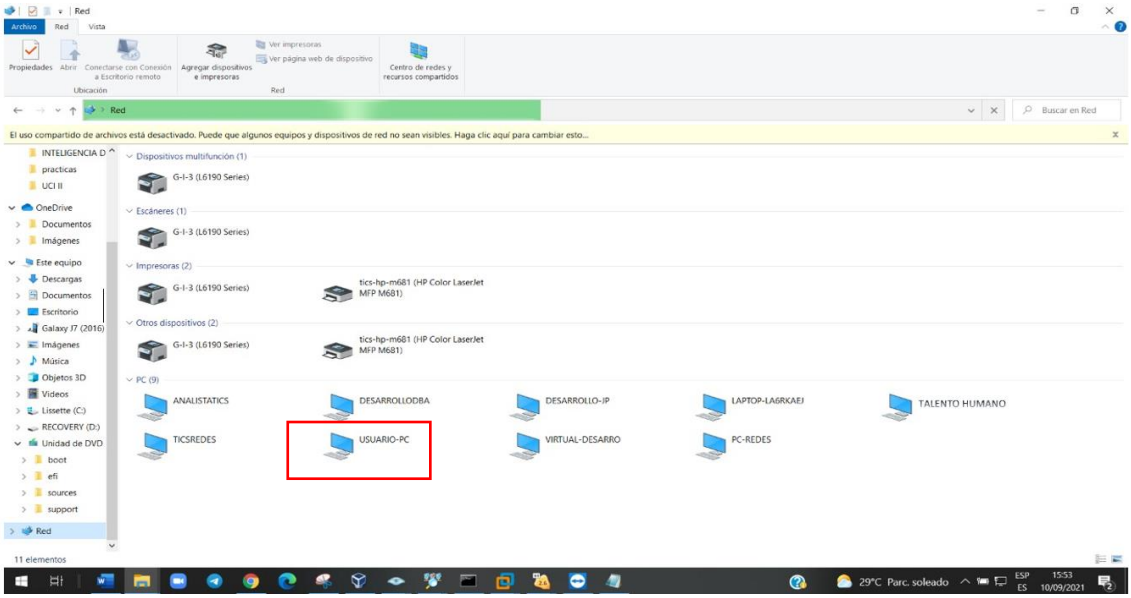


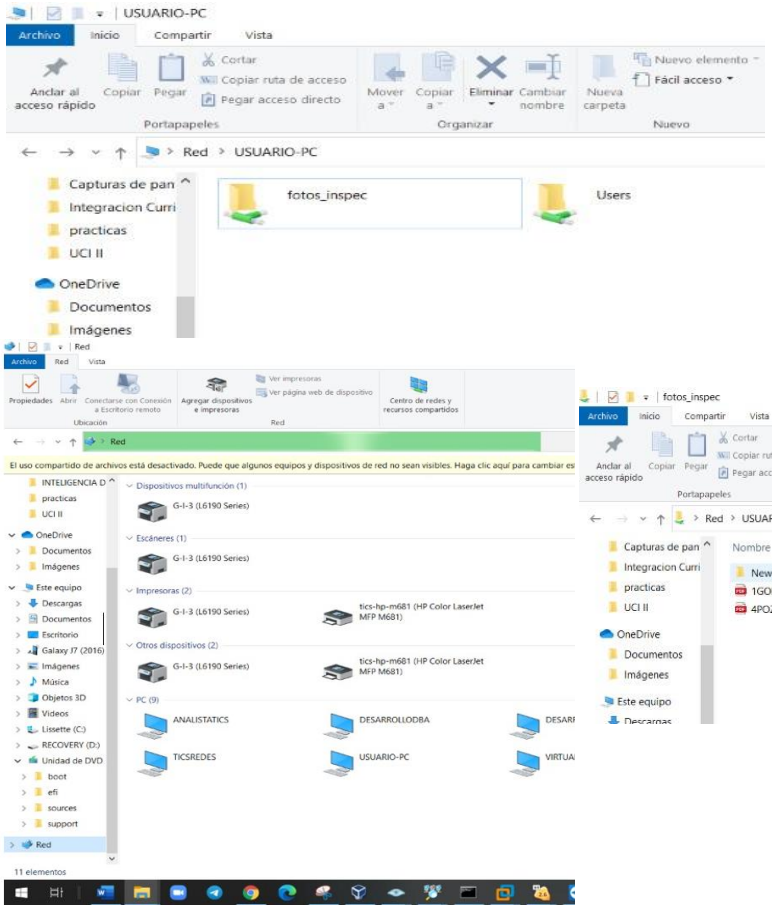


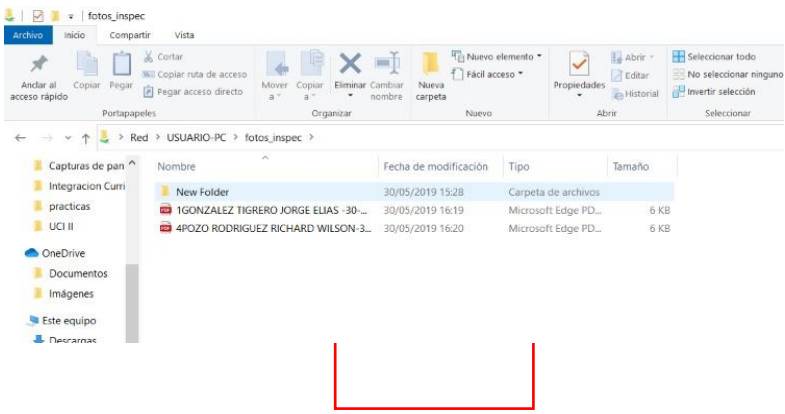


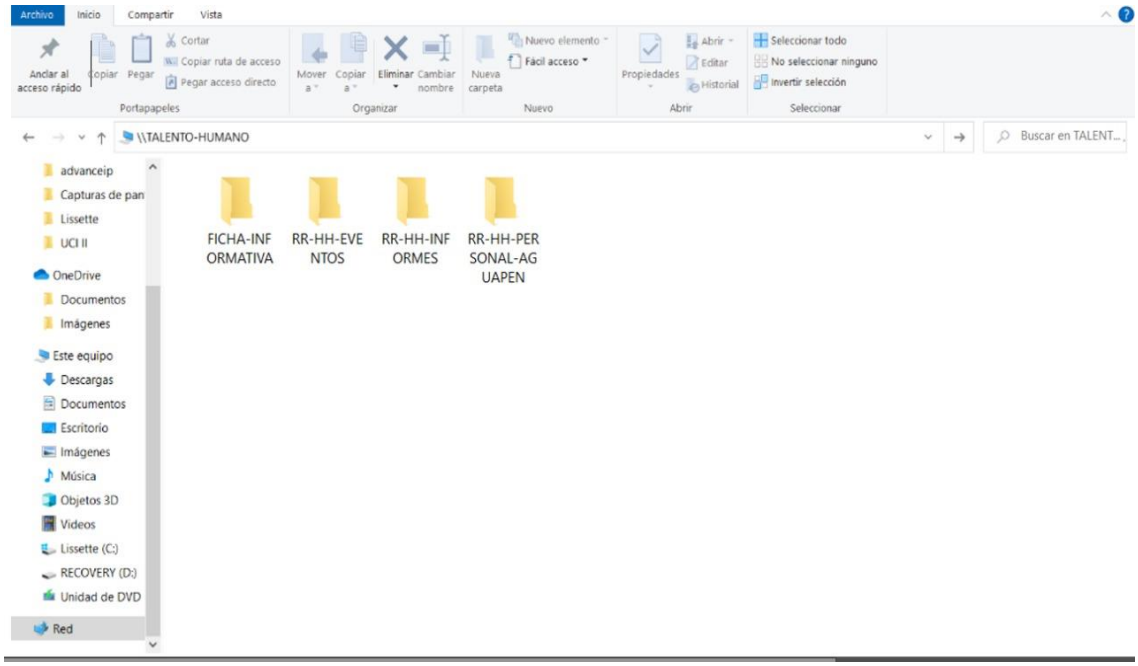
ANEXO 4

RECURSOS COMPARTIDOS









ANEXO 5

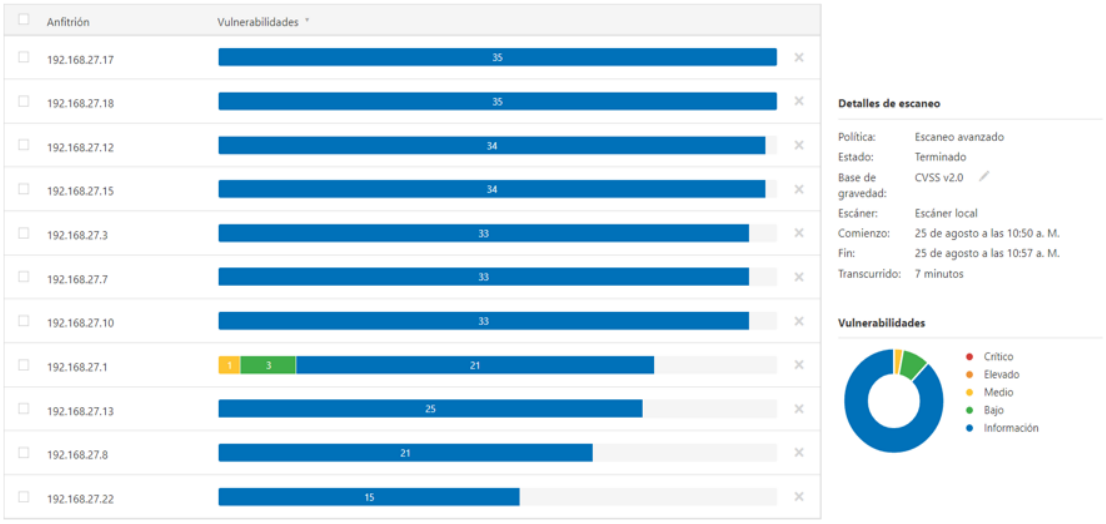
Etapa	Proceso	Resultados	Evidencias
Escaneo	En el rango 192.168.27.1-100 se ejecutó el escaño de la red con la herramienta Advanced IP Scanner, para detectar los puertos abiertos y los servicios activos de	El resultado obtenido indicó que se encontró 40 ip activas, correspondientes al host disponible	**Anexo 2**
		192.168.27.3 Equipo linux, servicios activos http, https, ipp,	**Anexo 9**

	las máquinas que se encuentren funcionando	printer, netbios-ssn, microsdoft-ds	
		192.168.27.1 Switch Hp, servicios activos ssh, telnet, http.	**Anexo 9**
		192.168.27.100 Equipo Windows 10, servicios activos: msrpc, netbios-ssn, micorsoft-ds, radmin, http.	**Anexo 10**
	En el rango 192.168.28.1-30 se ejecutó el escaño de la red con la herramienta Advanced IP Scanner, para detectar los puertos abierto y los servicios activos de las máquinas que se encuentren funcionando	El resultado obtenido indicó que se encontró 18 ip activas, correspondientes al host disponible	**Anexo 2**
		192.168.28.1 Switch Hp, servicios activos ssh, telnet, http.	**Anexo 11**
		192.168.28.21 impresora ricoh aficio mp c2550, servicios activos: ftp, telnet, netbios-ssn, Shell, ipp, oracleas-https, http, http-proxy, ipp,printer, netbios-ssn, microsdoft-ds,	**Anexo 12**

		shell	
	En el rango 192.168.28.31-60 se ejecutó el escaño de la red con la herramienta Advanced IP Scanner, para detectar los puertos abiertos y los servicios activos de las máquinas que se encuentren funcionando	El resultado obtenido indico que se encontró 20 ip activas, correspondientes al host disponible	**Anexo 2**
		192.168.28.56, equipo Windows 10, servicios activos: msrpc, netbios-ssn, Microsoft-ds, radmin, wsdapi	**Anexo 13**
	En el rango 192.168.28.61-80 se ejecutó el escaño de la red con la herramienta Advanced IP Scanner, para detectar los puertos abiertos y los servicios activos de las máquinas que se encuentren funcionando	El resultado obtenido indicó que se encontró 22 ip activas, correspondientes al host disponible	**Anexo 2**
		192.168.28.75 equipo Windows 10, servicios activos: msrpc, netbios-ssn, Microsoft-ds, enp-ms-wbt-server, radmin, wsdapi.	**Anexo 14**

ANEXO 6

VULNERABILIDAD DE PUERTOS



MEDIO Servidor Telnet sin cifrar

Descripción

El host remoto está ejecutando un servidor Telnet a través de un canal no cifrado.

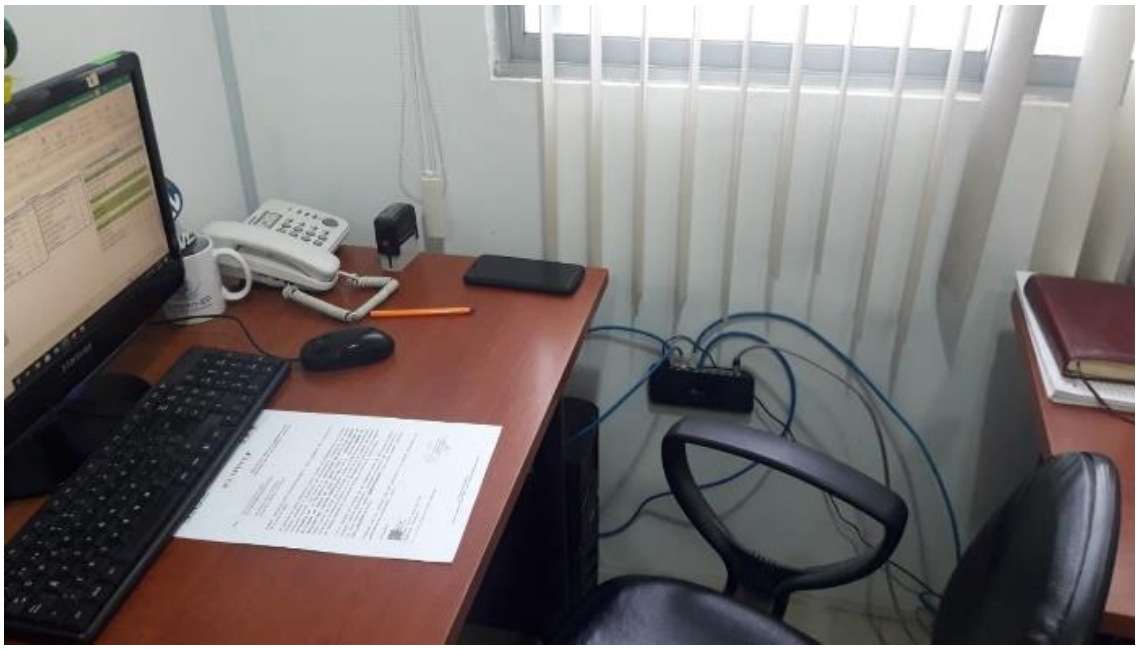
No se recomienda el uso de Telnet en un canal no cifrado, ya que los inicios de sesión, las contraseñas y los comandos se transfieren en texto sin cifrar. Esto permite que un atacante de intermediario remoto espíe una sesión Telnet para obtener credenciales u otra información confidencial y modificar el tráfico intercambiado entre un cliente y un servidor.

Se prefiere SSH sobre Telnet, ya que protege las credenciales de escuchas y puede canalizar flujos de datos adicionales, como una sesión X11.

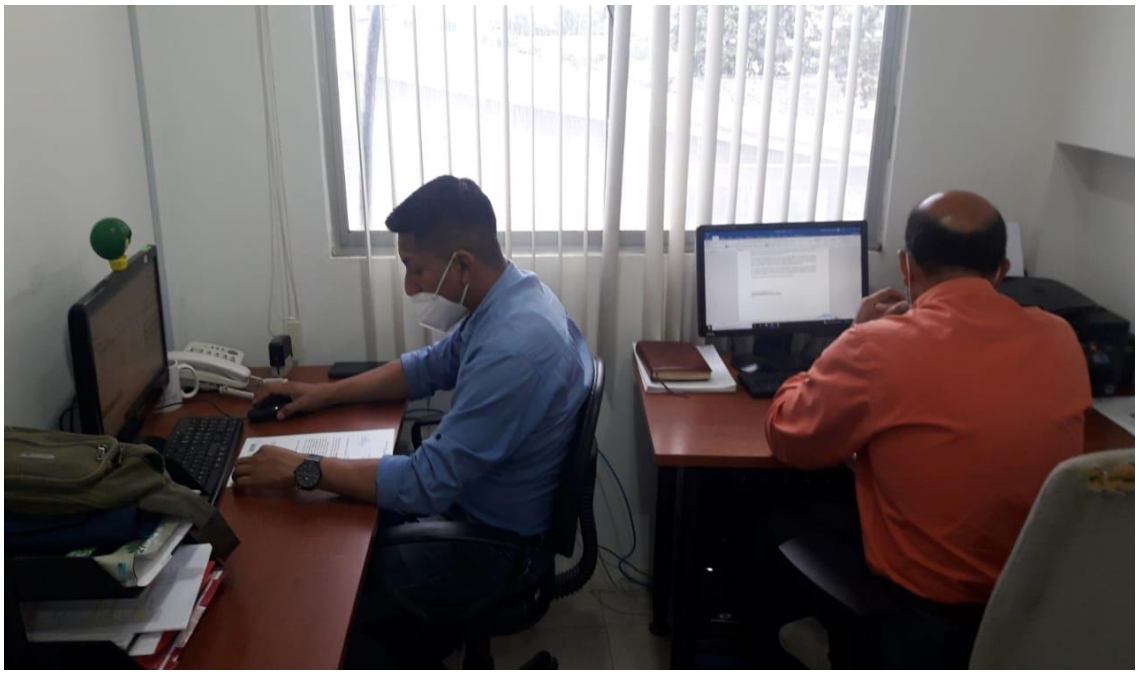
ANEXOS 7

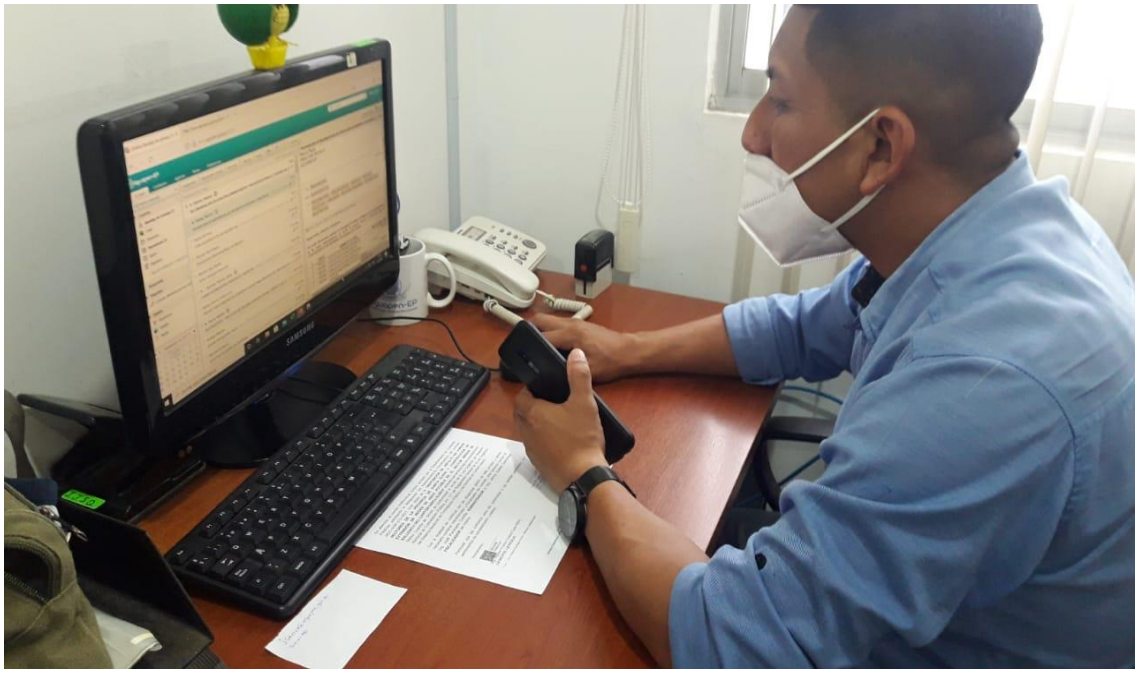
VULNERABILIDAD EN AP INALÁMBRICOS DEPARTAMENTO DE FISCALIZACIÓN Y DIRECCIÓN DE RECUPERACIONES.

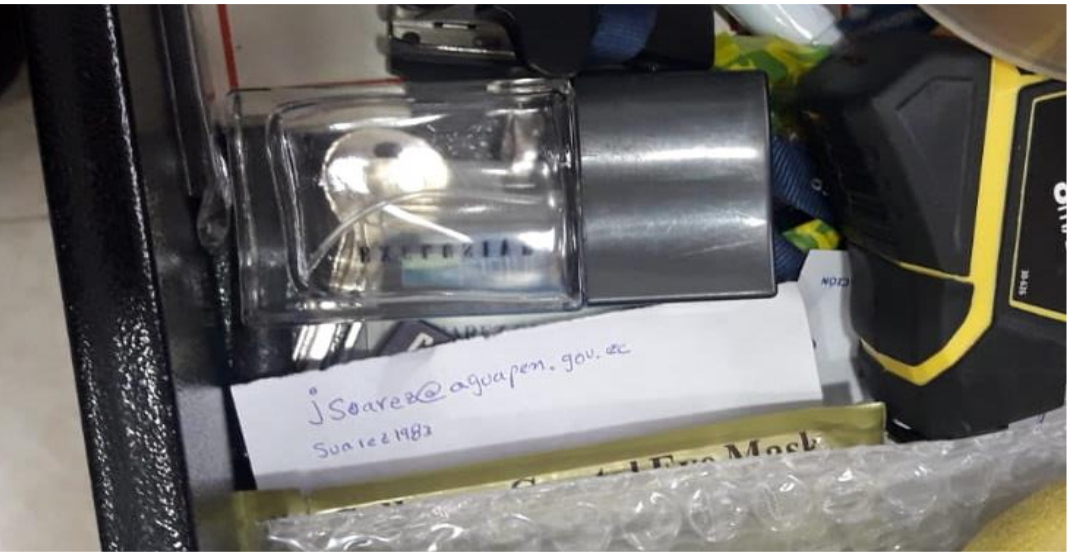

SOPORTE PARA TV



ANEXO 8







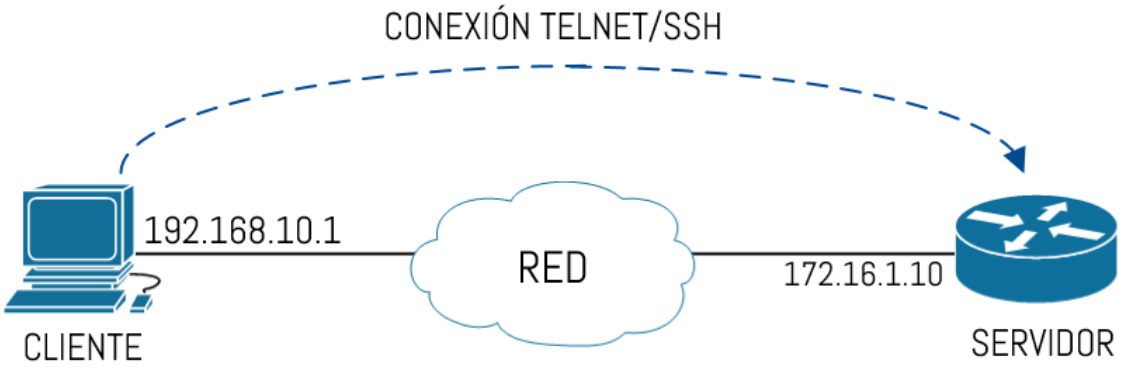
ANEXO 9

DESARROLLO DE EXPLOTACIÓN DE VULNERABILIDADES

ESCENARIO 1: ACCESO MEDIANTE EL PUERTO 22

Objetivo de la fase: Aplicar los tres tipos de pruebas direccionadas a la red.

Acceso remoto mediante telnet



Mediante el escaneo podemos verificar los dispositivos activos de la red, y sus puertos accesibles, lo que se pudo obtener a notar es lo siguiente:

- Existen computadores que mantienen el sistema operativo desactualizado de parches de seguridad y de versiones de Windows, lo que nos pudo decir el ingeniero encargado del departamento, es que están conscientes de ello, pero el inconveniente se da, que muchos de esos computadores mantienen programas y aplicativos que no mantienen soporte para sistemas operativos actualizados, lo que evita que se realice este respectivo mantenimiento.
- Mayormente los dispositivos que tienen el puerto 23 abiertos, son impresoras y escáneres.
- Nos percatamos que existen unos computadores que mantienen también estos puertos abiertos, por lo que podemos notar que sería fácil el acceso a esos computadores mediante una conexión remota.

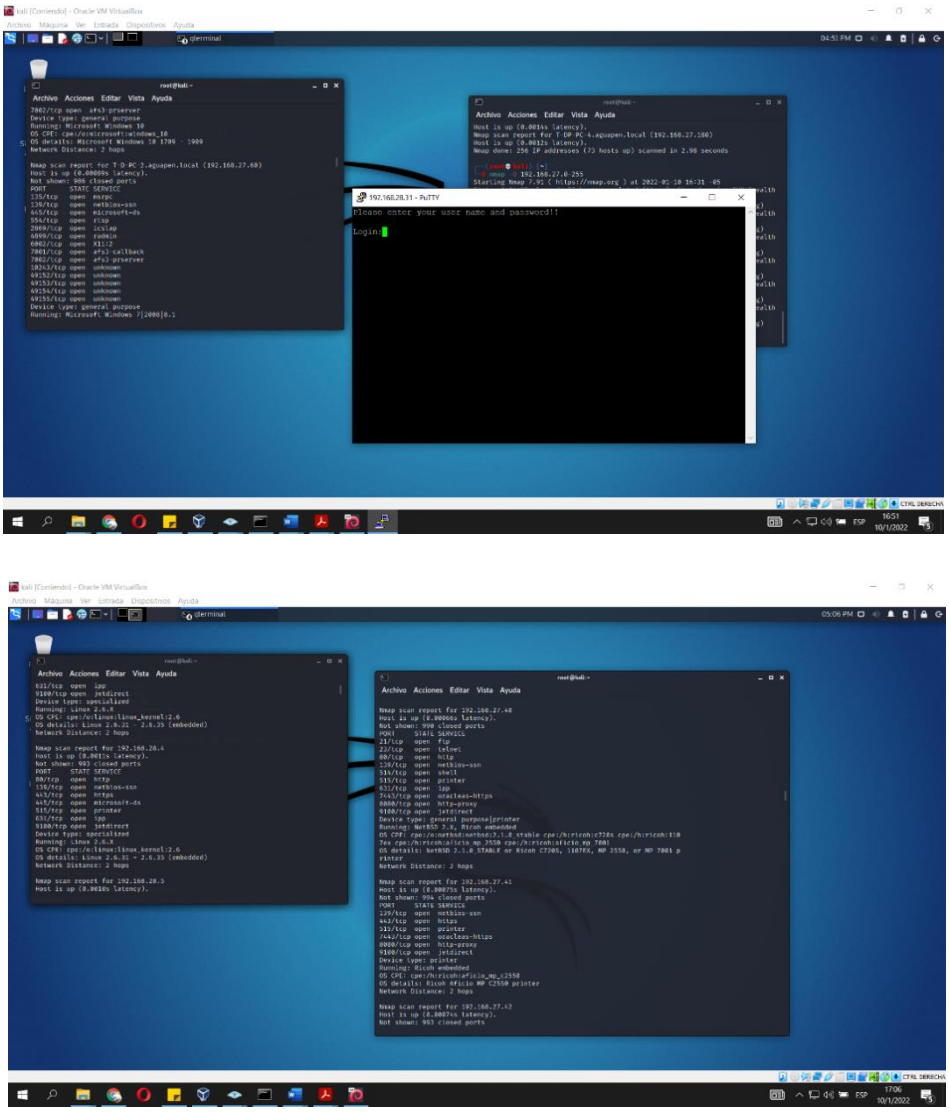


Ilustración 2 Acceso Mediante Puertos

Ilustración 3 Conexión Remota Telnet

A continuación, se realiza una prueba de conexión remota de uno de los computadores que mantienen el puerto de acceso remoto abierto.

Efectivamente se puede realizar la conexión, sin embargo, por restricciones de los encargados del departamento, no se pudo efectivizar la conectividad. En respuesta a esta

vulnerabilidad el personal encargado manifestó que estos puertos son abiertos por peticiones, una vez finalizado el requerimiento, se procede al respectivo cierre. Otra de las cuestiones que se percibió, es que el direccionamiento de IP y los departamentos están en un cambio, por implementación de nueva infraestructura en la red de datos.

ESCENARIO 2:

Objetivo de fase: Mediante la técnica de Sniffing Pasivo (STP, CDP, DTP, VTP), se ejecutan una serie de protocolos activos.

Paso 1:

Descargar la herramienta mediante el enlace: https://www.wireshark.org/

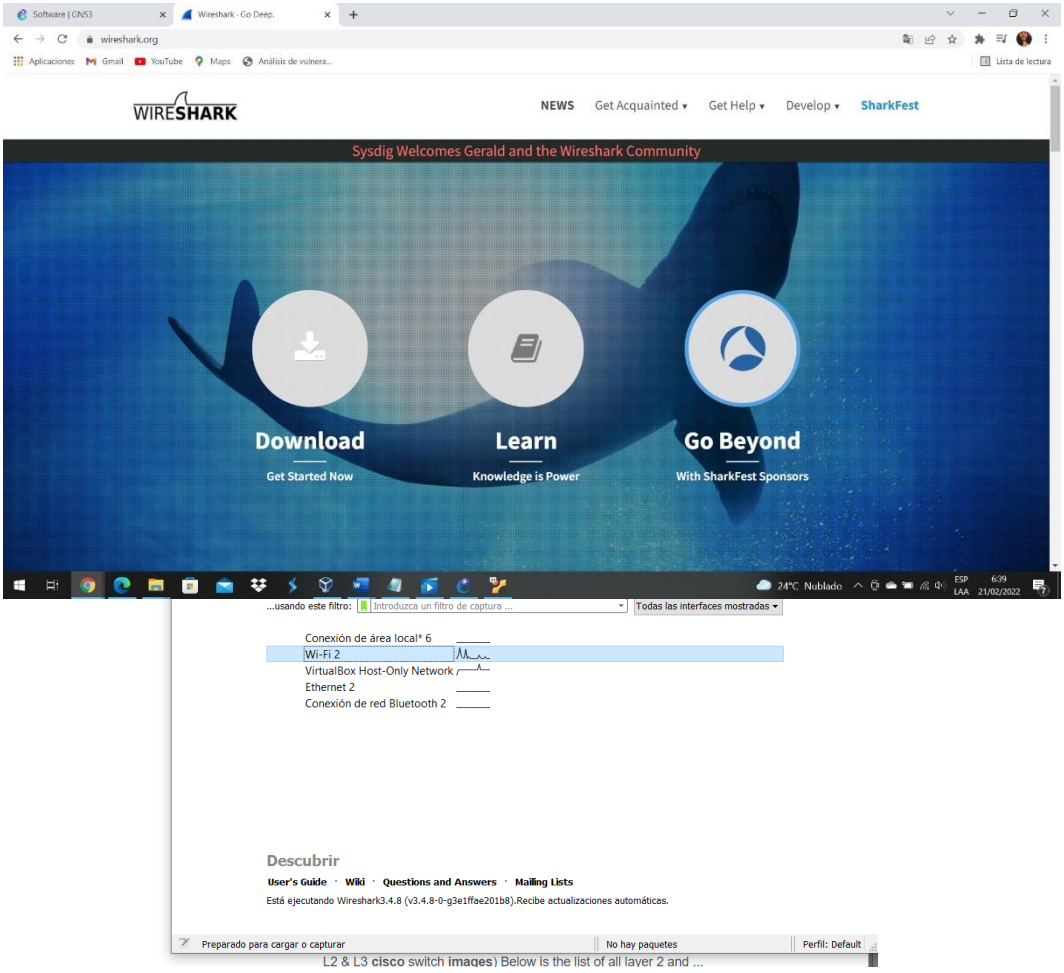
Se utiliza la herramienta Wireshack para captura paquetes, extrayendo datos desde el tráfico de la red en los departamentos de fiscalización y dirección de recuperaciones.

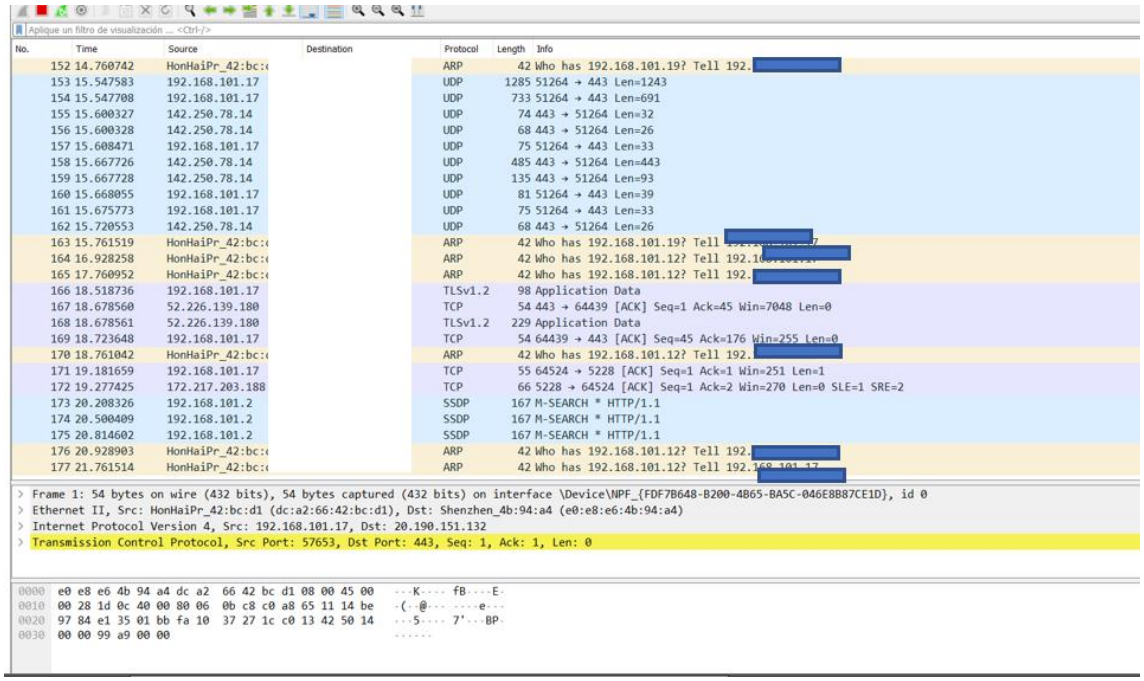
Herramienta: Wireshark

Contramedidas: Encriptación de datos, Sistemas de detección de Snniffers

Una vez descargada nos aparece una ventana de esta manera

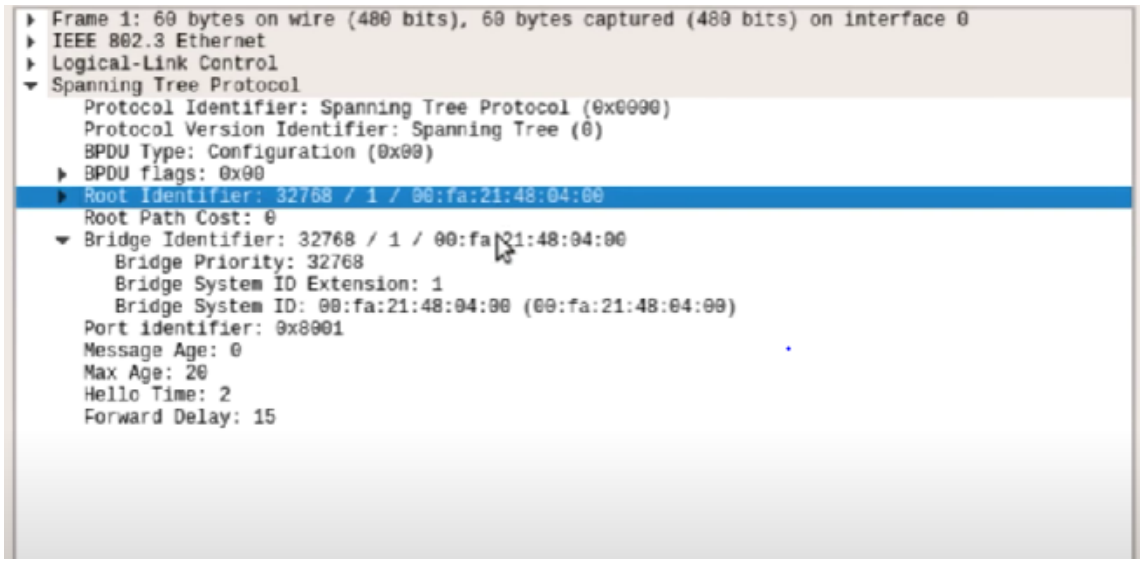
Paso 3: Esta ventana nos permitirá seleccionar nuestra tarjeta de red y activaremos la opción de resolución de nombre de red.





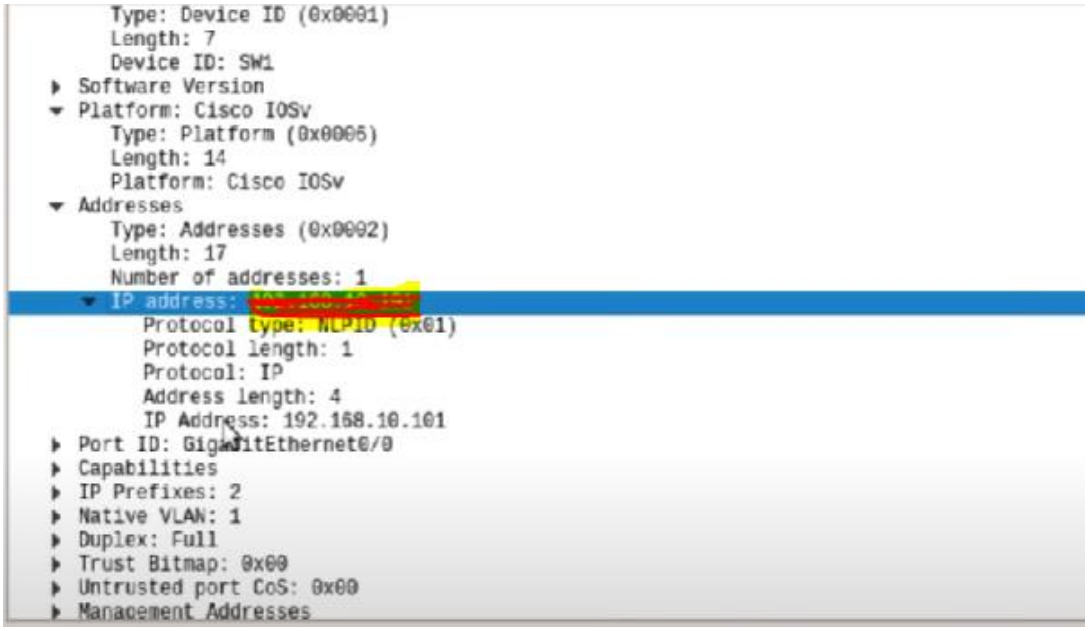
Paso 4: Detenemos por un momento la búsqueda y vemos lo que encontramos.

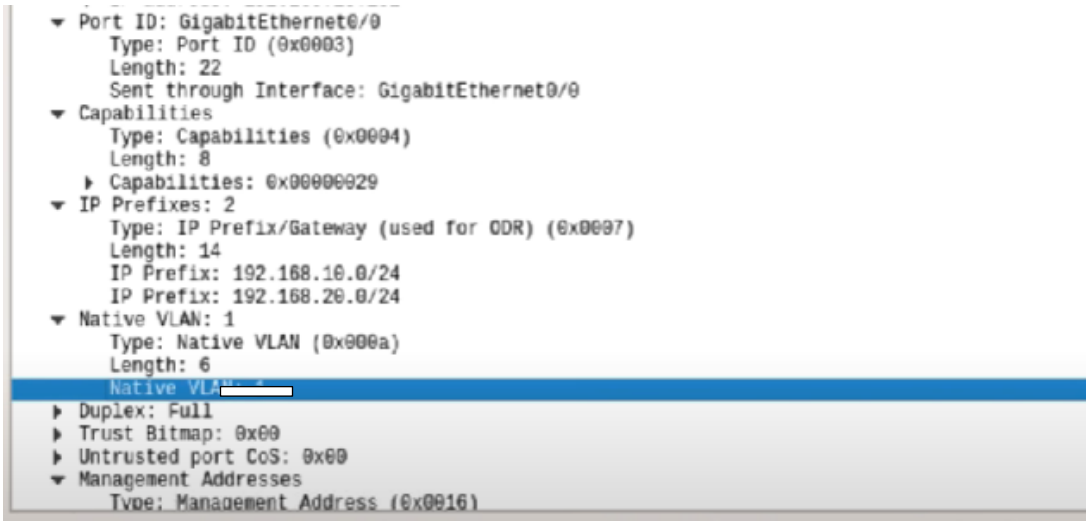
Analizamos el protocolo STP



- Que Vlan se está usando.
- Cuál es el Bridge

Protocolo CDP

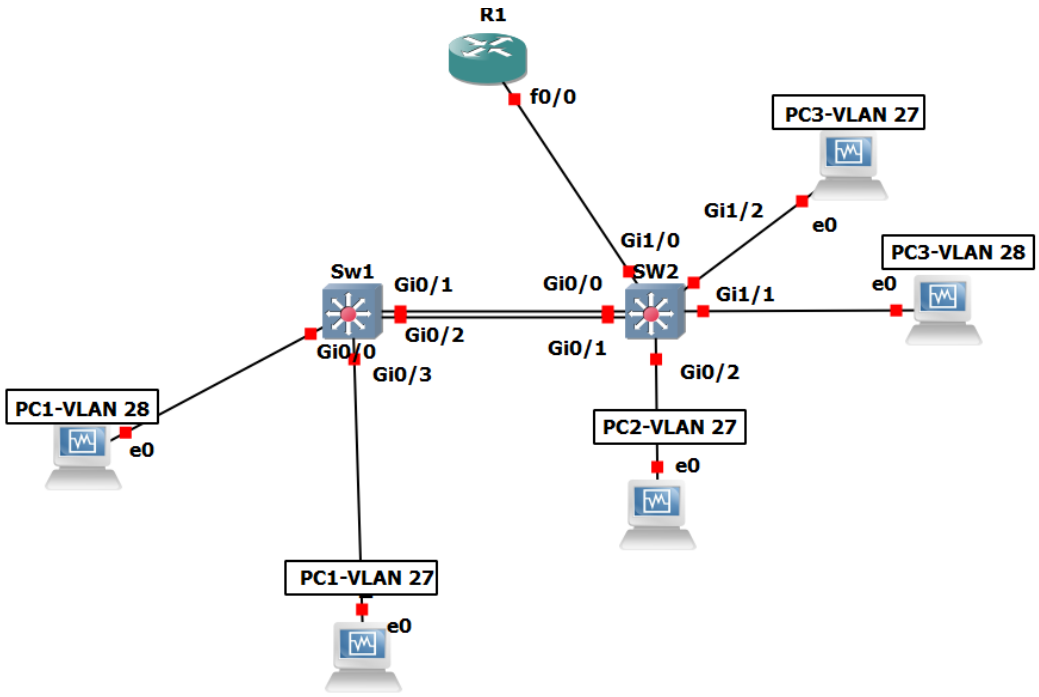




- Nombre del dispositivo
- Versión de Software
- Dirección IP.
- Vlans

ESCENARIO 3

MAC FLOOFING ATTACK

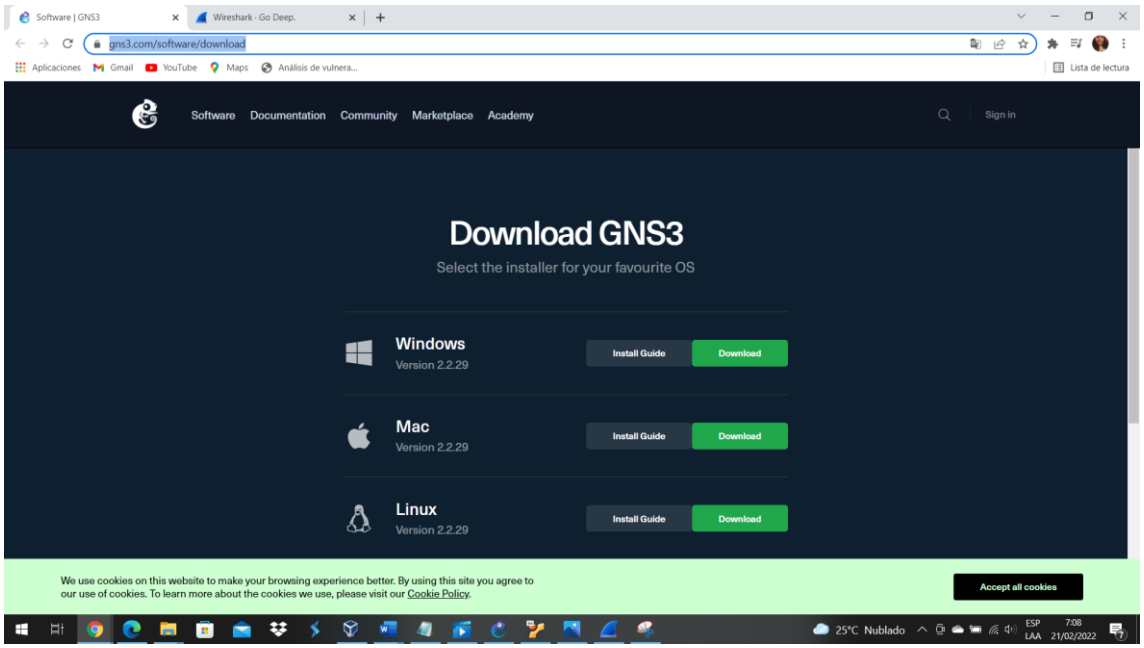


En el desarrollo de esta prueba se utiliza la herramienta de GNS3 y varias máquinas virtuales.

NS3 es un software utilizado por cientos de miles de ingenieros de redes a nivel mundial para emular, configurar, probar y solucionar problemas de redes virtuales y reales. Le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube.

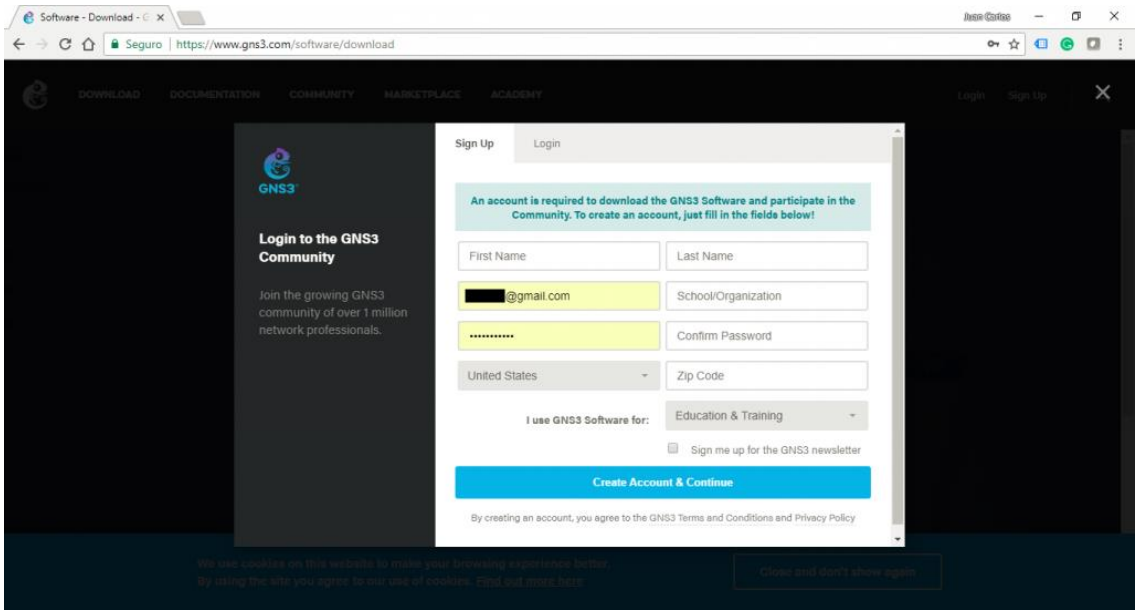
INSTALACION DE GNS3

Paso 1: En el siguiente link nos llevará a la página oficial para descargar https://www.gns3.com/software/download



Luego aparecerán dos opciones:

La primera es “Sign Up” nos permitirá configurar crear un usuario, para eso ingresar sus nombres y apellidos, además un correo electrónico y su contraseña, ingresar el país de procedencia y si corresponde el código postal. Finalmente ingresar para que hagan uso del software GNS3, bastará que coloquen que es para propósitos de Educación y Entrenamiento (Education and Training) y le dan click en el botón “Creat Account & Continue”.



La segunda opción “Login” nos da la pantalla para el acceso a usuarios previamente registrados, bastará colocar el correo y contraseña.

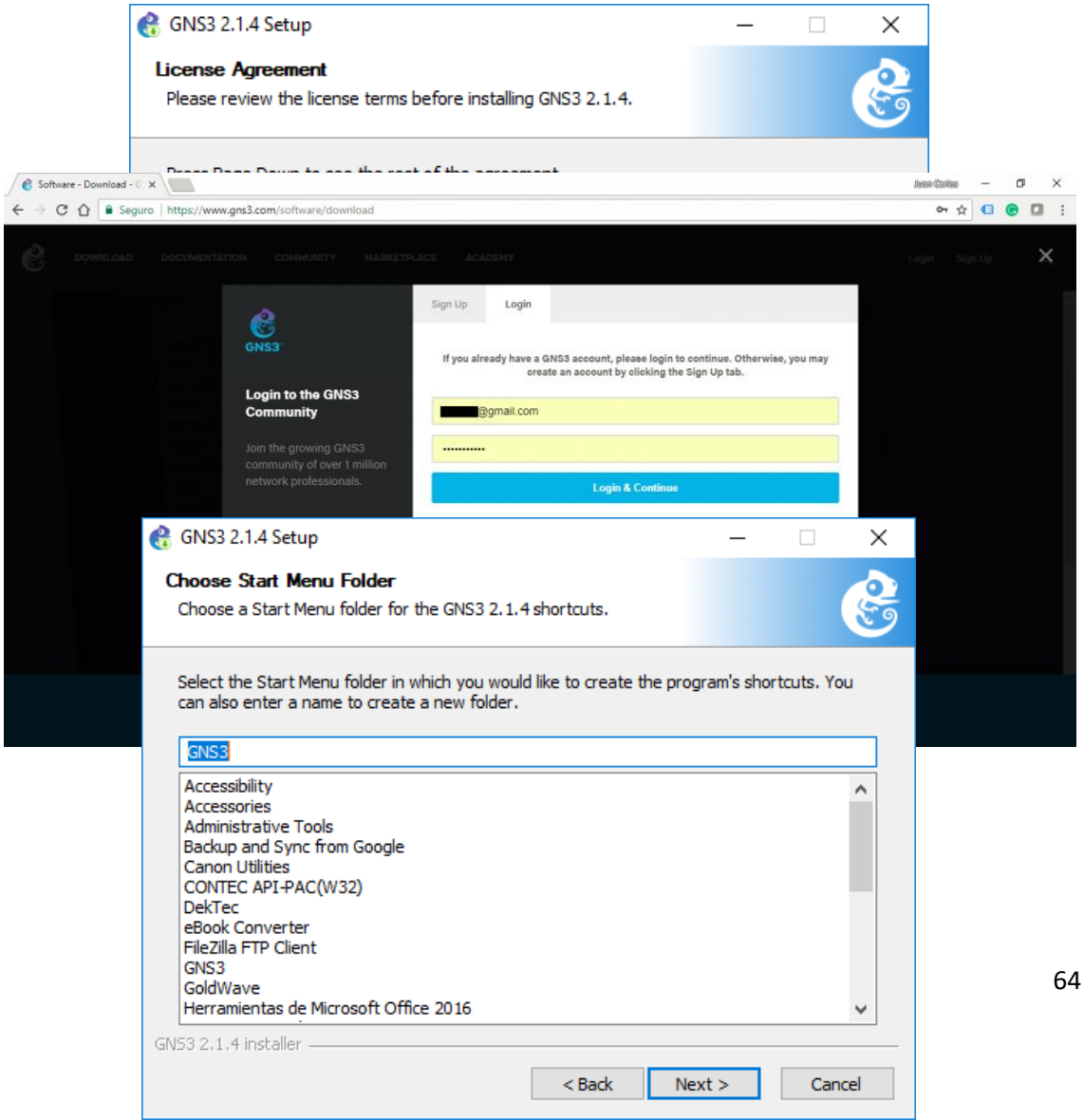
Paso 3:

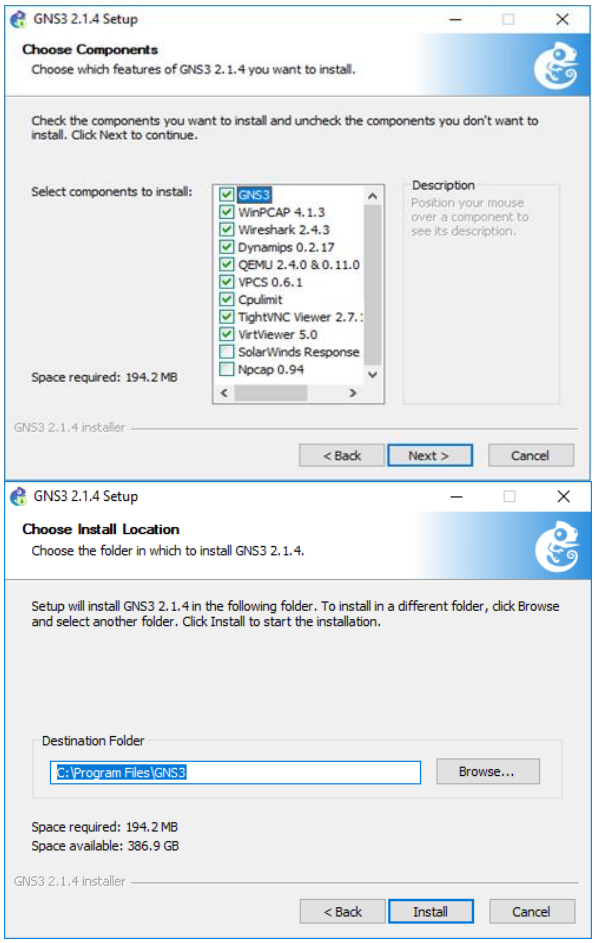
A continuación, se describe el procedimiento de instalación de GNS3 en Windows 10, la ejecución es similar para otras versiones de Windows.

Una vez finalizada la descarga se debe ejecutar el archivo, luego les pedirá permisos de administrador, le dan Ok y aparecerá la siguiente pantalla según la Figura 3.1, esta hace referencia al acuerdo de licencia para poder ejecutar la instalación GNS3. Dar Click en "Agree".

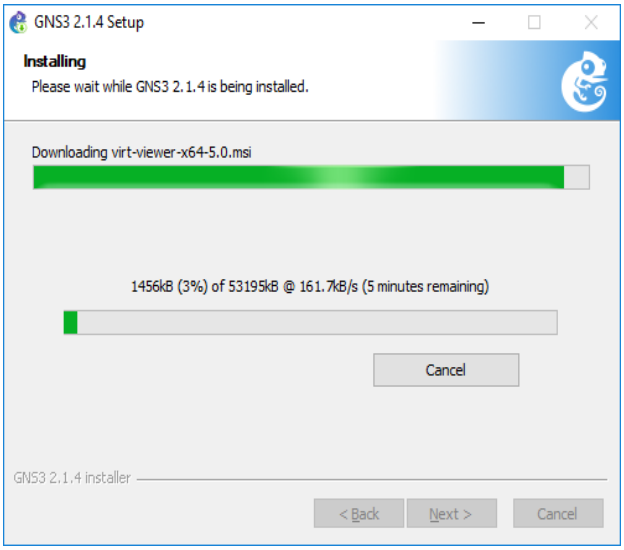
Luego se elige el Folder donde se instalará el acceso directo en el menú inicio, se recomienda dejarlo por defecto.

Paso 4: Selección de componentes para la instalación GNS3

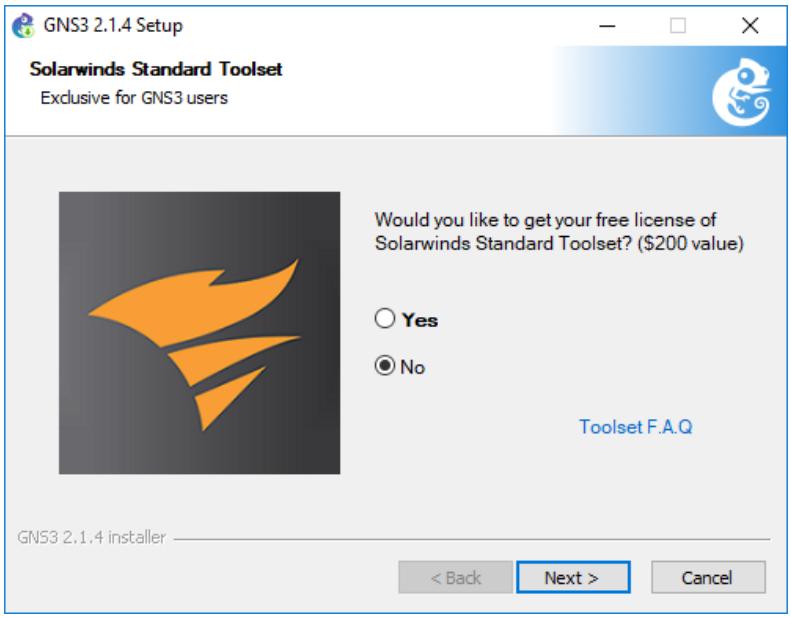




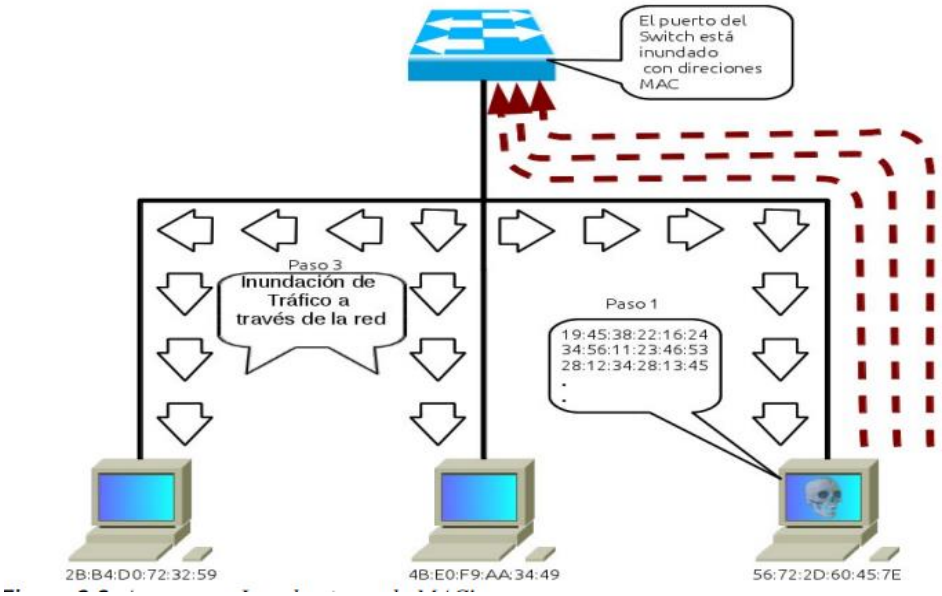
En algunos casos se requerirá la conexión a internet para poder descargar aplicaciones como el Wireshark.



Luego aparecerá una pantalla preguntando instalar la aplicación Solarwinds Standard Toolset, es una aplicación que ayuda en las tareas de administración, gestión y monitoreo de redes, si lo requieren lo pueden instalar.



Una vez instalada se realiza la configuración de imágenes y dispositivos para arma la topología analizar.



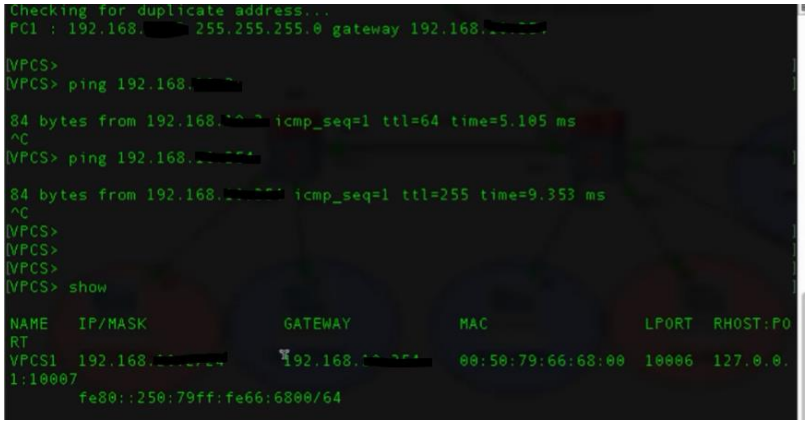
MAC Flooding Attack

Paso 1: Revisaremos la comunicación que existe entre PC2-VLAN 27 Y PC3-VLAN27

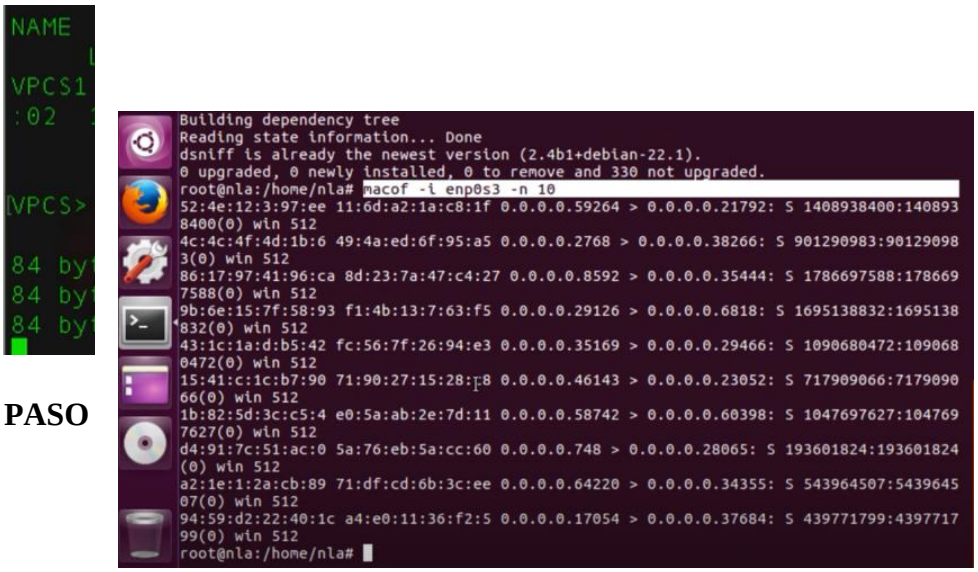
PC2

PC3

PASO 2:

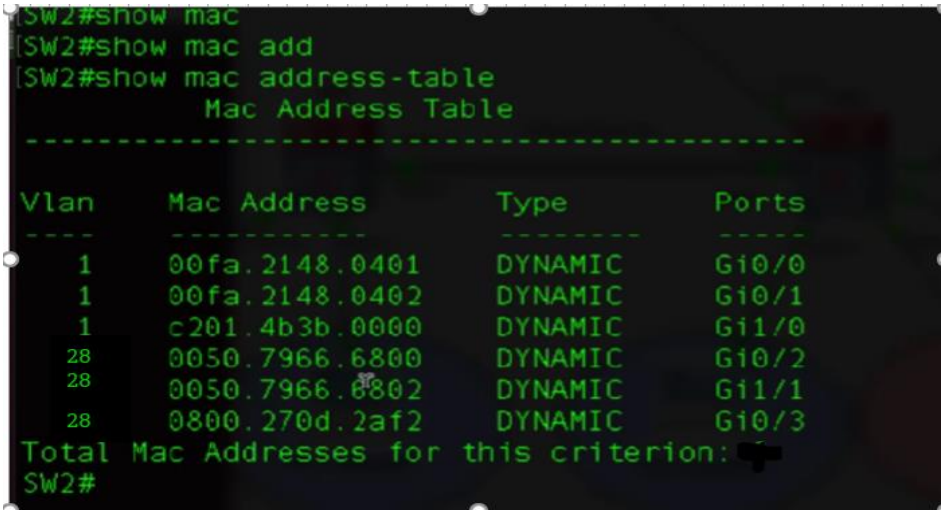


Revisamos la conexión entre ambas maquinas



PASO 3:

Revisaremos cuantas direcciones MAC tiene el Switch 2



Paso 4: Con el siguiente comando se instala la herramienta de dsniff en la máquina donde realizaremos el ataque.

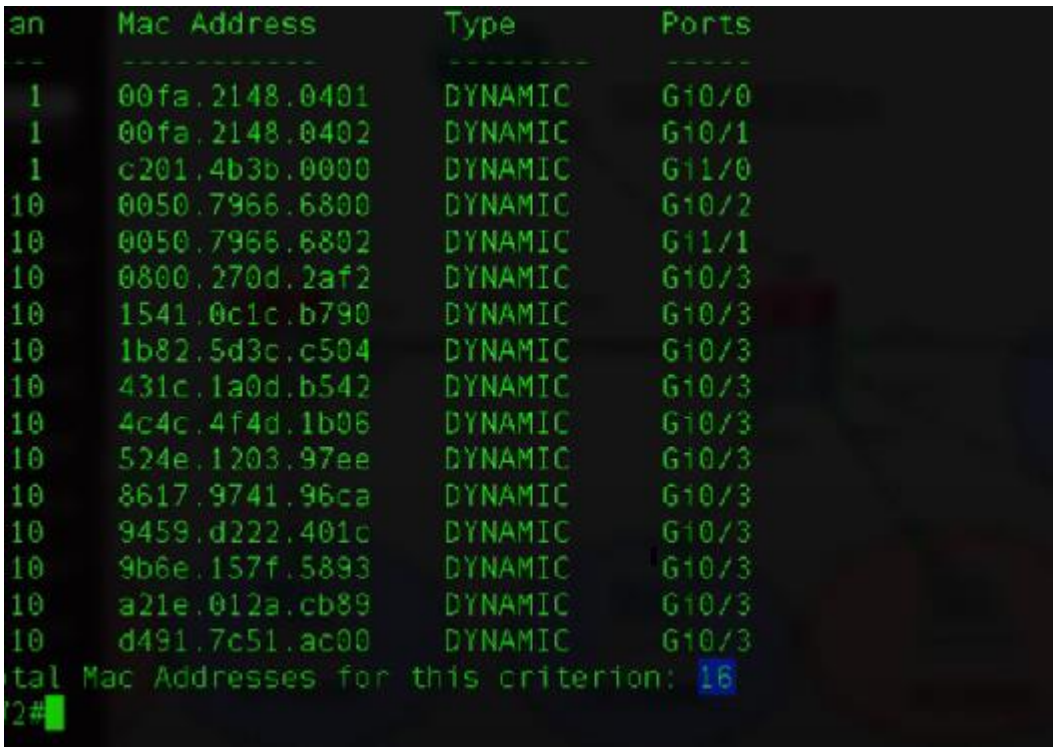
```
root@nla:/home/nla# apt-get install dsniff
```

Paso 5: El siguiente comando nos permite inundar la red

```
root@nla:/home/nla# macof -i enp0s3 -n 1
```

Se agregaron las 10 direcciones MAC

Paso 6: Verificamos en el Switch



an	Mac Address	Type	Ports
1	00fa.2148.0401	DYNAMIC	Gi0/0
1	00fa.2148.0402	DYNAMIC	Gi0/1
1	c201.4b3b.0000	DYNAMIC	Gi1/0
10	0050.7966.6800	DYNAMIC	Gi0/2
10	0050.7966.6802	DYNAMIC	Gi1/1
10	0800.270d.2af2	DYNAMIC	Gi0/3
10	1541.0c1c.b790	DYNAMIC	Gi0/3
10	1b82.5d3c.c504	DYNAMIC	Gi0/3
10	431c.1a0d.b542	DYNAMIC	Gi0/3
10	4c4c.4f4d.1b06	DYNAMIC	Gi0/3
10	524e.1203.97ee	DYNAMIC	Gi0/3
10	8617.9741.96ca	DYNAMIC	Gi0/3
10	9459.d222.401c	DYNAMIC	Gi0/3
10	9b6e.157f.5893	DYNAMIC	Gi0/3
10	a21e.012a.cb89	DYNAMIC	Gi0/3
10	d491.7c51.ac00	DYNAMIC	Gi0/3

tal Mac Addresses for this criterion: 16

2#

ANEXO 11

```
Nmap scan report for J-PC-2.aguapen.local (192.168.27.100)
Host is up (0.0029s latency).
Not shown: 994 closed ports
PORT      STATE    SERVICE        VERSION
135/tcp   open     msrpc          Microsoft Windows RPC
139/tcp   open     netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds?
2607/tcp filtered connection
4899/tcp open      radmin         Famatech Radmin 3.X (Radmin Authentication)
5357/tcp open      http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

ANEXO 12

```
┌──(lissette㉿kali)-[~]
└─$ nmap -O 192.168.28.1
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!
┌──(lissette㉿kali)-[~]
└─$ sudo su
[sudo] password for lissette:
┌──(root💀kali)-[/home/lissette]
└─# nmap -O 192.168.28.1-30
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-10 16:41 -05
Nmap scan report for 192.168.28.1
Host is up (0.0038s latency).
Not shown: 994 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
80/tcp    open     http
50300/tcp filtered unknown
50389/tcp filtered unknown
50500/tcp filtered unknown
Device type: switch
Running: H3C Comware 5.X
OS CPE: cpe:/o:h3c:comware:5.20
OS details: H3C Comware 5.20
```

ANEXO 13

```
Nmap scan report for 192.168.28.21
Host is up (0.0013s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
139/tcp  open  netbios-ssn
514/tcp  open  shell
515/tcp  open  printer
631/tcp  open  ipp
7443/tcp open  oracleas-https
8080/tcp open  http-proxy
9100/tcp open  jetdirect
Device type: printer
Running: Ricoh embedded
OS CPE: cpe:/h:ricoh:aficio_mp_c2550
OS details: Ricoh Aficio MP C2550 printer
Network Distance: 2 hops
```

ANEXO 14

```
Nmap scan report for RECEPCION.aguapen.local (192.168.28.56)
Host is up (0.0021s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
4899/tcp open  radmin
5357/tcp open  wsdapi
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 2 hops
```

ANEXO 15

```
Nmap scan report for F-R-PC-4.aguapen.local (192.168.28.75)
Host is up (0.0023s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2968/tcp open  enpp
3389/tcp open  ms-wbt-server
4899/tcp open  radmin
5357/tcp open  wsdapi
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 2 hops
```