OFICINA DE POSGRADOS

TEMA:

POLÍTICAS DE CIBER SEGURIDAD PARA LOS DISPOSITIVOS DE CAPA-DOS EN EL CENTRO DE DATOS DEL HOSPITAL DE LATACUNGA

Proyecto de investigación previo a la obtención Magister en Ciber Seguridad

Línea de Investigación:

Protección de Datos y Comunicaciones

Autor:

Ing. Richard Omar Chalan Analuisa

Director:

Ing. Diego Fernando Ávila Pesantez PhD.

Ambato – Ecuador

Marzo 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

TEMA:

POLÍTICAS DE CIBER, SEGURIDAD PARA LOS DISPOSITIVOS DE CAPA-DOS EN EL CENTRO DE DATOS DEL HOSPITAL DE LATACUNGA

LÍNEA DE INVESTIGACIÓN:

Protección de Datos y Comunicaciones

Autor: Ing. Richard Omar Chalan Analuisa

Alberto Leopoldo Arellano Aucancela, Mg.
CALIFICADOR

f _____

Firmado electrónicamente por:
ALBERTO LEOPOLDO ARELLANO AUCANCELA

José Marcelo Balseca Manzano, Mg.
Calificador

f _____

Diego Fernando Avila Pesanatez, Mg.
Calificador

f _____

Firmado electrónicamente por:
DIEGO FERNANDO AVILA PESANTEZ

Juan Carlos Acosta Teneda, P. PhD.
Director Oficina de Postgrados

f _____

Pontificia Universidad Católica del Ecuador
OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villaroel, Dr.
Secretario General Pucesa

f _____

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

AMBATO - ECUADOR

Marzo 2022

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: RICHARD OMAR CHALAN ANALUISA, con CC. 180469756-1 autor del trabajo de graduación intitulado: "POLÍTICAS DE CIBER, SEGURIDAD PARA LOS DISPOSITIVOS DE CAPA-DOS EN EL CENTRO DE DATOS DEL HOSPITAL DE LATACUNGA", previa a la obtención del título profesional de MAGISTER EN CIBERSRGURIDAD, en la OFICINA DE POSGRADOS.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, marzo 2022

Richard Omar Chalán Analuisa
CC.180469756-1

AGRADECIMIENTO

El más sincero agradecimiento a la Pontificia Universidad Católica del Ecuador sede Ambato, por brindarme la posibilidad de alcanzar una profesión para servicio de la sociedad.

Agradezco al Ing. Diego Ávila por brindarme su asistencia para llevar a cabo el trabajo de titulación de posgrado y por haberme permitido recurrir a su calidad de persona y experiencia, para encaminar con éxito el presente trabajo.

Richard Omar

DEDICATORIA

El trabajo de titulación es un placer dedicar a mi esposa, mi hija y a mis padres Luis y Elvia, quienes siempre me apoyaron para culminar mi estudio, y creyeron siempre en mí con su apoyo incondicional en todos los instantes. A quienes me han dado motivación en mis momentos de flaqueza, gracias a su apoyo en todos los sentidos de mi ser, al tener a ustedes un buen ejemplo hacia mi vida profesional, es esta la razón en que este triunfo, se los dedico a Ustedes por ser mi todo y mi razón de superación.

RESUMEN

En el documento, se analizó la problemática de ausencia de políticas de ciberseguridad en los equipos de comunicaciones del Hospital General de Latacunga y la falta de las misma provocan que los equipos sean atacados en la mayoría de los casos por usuarios internos quienes disponen de permisos no autorizados a los equipos de red por tal motivo, se realizó pruebas de esfuerzo a los equipos de capa de enlace para mejorar la seguridad de los mismos que están instalados en el centro de datos y que están expuestos. Esto debido a que no existen mecanismos de ciber, seguridad en los dispositivos de conmutación. Para la implementación de las políticas de ciber seguridad, se utilizó dos ambientes de pruebas, la primera es la simulación y se aplica parámetros de configuración con el equipo físico de marca huawei, se utilizó la herramienta de virtualización VMWARE para la instalación del software de emulación de red multiproveedor EVE-NG para dispositivos con sistemas operativos huawei, el que permitió realizar las pruebas de vulnerabilidades en una computadora virtual con sistema operativo Parrot con las herramientas Openvas y Yersinia tales como: Vlan hopping, ataque MITM, ataque Mac Arp, ataque DHCP Starvition, ataque STP en los equipos de capa dos de la marca Huawei. Se tomó como referencia a la norma ISO 27032 que permitió seguir los lineamientos de cada fase para proponer las políticas de ciber, seguridad para estos dispositivos al final, se elaboraron políticas de ciber, seguridad para dispositivos de capa dos que consistió en adicionar configuraciones y habilitar funcionalidades que depende del requerimiento de la institución al aplicar las políticas de ciber seguridad, se logró mitigar una cantidad significativa de 100% por ciento en referencia al punto inicial de las vulnerabilidades de la infraestructura de esta casa de salud.

Palabras clave: Políticas Ciber, seguridad, Vulnerabilidad, Dispositivos Capa Dos, Herramientas Para Vulnerabilidades, Vlan Hopping, Ataque Mitm, Ataque Mac Arp, Ataque Dhcp Starvition, Ataque Stp.

ABSTRACT

The document analyzed the problem of lack of cybersecurity policies in the communications equipment of the General Hospital of Latacunga and the lack of the same cause the equipment to be attacked in most cases by internal users who have unauthorized permissions to network equipment, for this reason, stress tests were performed to link-layer equipment to improve the security of the same that are installed in the data center and are exposed. This is due to the fact that there are no cybersecurity mechanisms in switching devices. For the implementation of the cybersecurity policies, two test environments were used, the first one is the simulation and the second one is applying configuration parameters with the physical equipment of the Huawei brand. The VMWARE virtualization tool was used to install the EVE-NG multi-vendor network emulation software for devices with Huawei operating systems, which allowed testing vulnerabilities in a virtual computer with Parrot operating system with Openvas and Yersinia tools such as Vlan hopping, MITM attack, Mac Arp attack, DHCP Starvition attack, STP attack in layer two equipment of the Huawei brand. The ISO 27032 standard was taken as a reference that allowed following the guidelines of each phase to propose cybersecurity policies for these devices, at the end cybersecurity policies, were developed for layer two devices that consisted of adding configurations and enabling functionalities depending on the requirement of the institution to apply cybersecurity policies were able to mitigate a significant amount of 100% percent about the starting point of the vulnerabilities of the infrastructure of this house of health. Keywords: Cybersecurity Policies, Vulnerability, Layer Two Devices, Vulnerability Tools, Vlan Hopping, Mitm Attack, Mac Arp Attack, Dhcp Starvition Attack, Stp Attack.

Keywords: Cyber, security Policies, Vulnerability, Layer Two Devices, Vulnerability Tools, Vlan Hopping, Mitm Attack, Mac Arp Attack, Dhcp Starvition Attack, Stp Attack.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El uso en la actualidad de las tecnologías de la información y de las comunicaciones, se tornan cada vez más importante para el funcionamiento de las actividades de la sociedad, ha generado que muchas labores dependan de la conexión a Internet, da paso al uso inadecuado del ciberespacio. Esto constituye una puerta de ingreso para que producir delitos informáticos, que progresivamente aparecen amenazas tecnológicas (híbridas) donde no existe ni actores ni fronteras, los ciberataques afectan directamente al desarrollo de las actividades y paralizarían el funcionamiento de la infraestructura, ocasiona grandes pérdidas socioeconómicas.

El entorno digital actual considera los riesgos y la responsabilidad que implica el uso de la infraestructura de redes, y la importancia de la seguridad de cada una de las capas de modelo OSI (Open System Interconection) que la constituyen, su interacción permite la comunicación hacia el internet. La ciber seguridad representa un dilema de seguridad para todos los estados, porque su zona de acción es desconocida y peligrosa en el ciberespacio.

La creciente incorporación de la tecnología en la vida cotidiana y en especial el campo de la salud, está provoca un riesgo en la atención sanitaria, donde el activo más valioso es el dinamismo de la información y la seguridad que implica. Sin embargo, aún requieren avances en la definición de las políticas de ciber, seguridad enfocados a los dispositivos de la infraestructura de red tópico que es analizada, a continuación.

Según el informe de IBM y el instituto de Ponemon en el 2016, la frecuencia de violaciones a los dispositivos de enlace de datos de la capa dos en la industria de la salud ha aumentado desde 2010 y se encuentra entre los sectores más afectados por los ciberataques a nivel mundial. Debido a su inmutabilidad, la información que accede, a través de violaciones de datos sanitarios es de especial interés para los delincuentes, que provocan un daño psicosocial si los datos privados están comprometidos.(Argaw et al. 2020)

La importancia de la disponibilidad los dispositivos de red capa dos y capas superiores para el uso del internet, se ha tornado fundamental en la infraestructura tecnológica en toda institución. Cabe destacar, que la falta de políticas de ciber, seguridad inadecuada facilita que los ataques sean generados por usuarios externos y sobre todo los usuarios internos, provoca redes zombis o terminales infectados, permite el acceso no autorizado a los recursos y servicios de la infraestructura red. En el caso de las instituciones públicas quienes prestan servicios de salud, los equipos de la infraestructura de red son importantes para mantener la comunicación entre la red integral de salud, estas permiten la transmisión, la recolección de los datos y mantienen la disponible la información en línea. Con el pasar del tiempo, los piratas informáticos descubren nuevas estrategias para ganar dinero y en tanto la salud, se convierte en un flanco fácil debido a la capacidad de vender grandes lotes de datos personales con fines de lucro(Finkle 2014).

Cabe indicar que a nivel internacional la oficina Federal de Investigaciones (FBI) advirtió a los servidores de atención médica, que se protegieran contra los ataques cibernéticos, después de que uno de los operadores de hospitales más grandes de EE. UU., Community Health Systems Inc, indicaron que piratas informáticos del oriente habían ingresado sin permisos en su red informática y robado la información personal de 4,5 millones de pacientes. Los peritos en seguridad recomiendan que los delincuentes informáticos apuntan más a las instituciones de la salud, valorada en 3 billones de dólares, que tiene muchas empresas que aún dependen de sistemas informáticos antiguos y no utilizan las últimas funciones de seguridad (Finkle 2014).

Con la repotenciación en los sistemas informáticos del Hospital de General de Latacunga en el año 2017 y con la implementación de un centro datos en el área de Tecnologías de la Información y Comunicaciones (TIC), se ve necesario realizar este trabajo para reforzar la seguridad informática, ante todo tomar medidas preventivas acerca de esta problemática puesto, que se ha evidenciado la necesidad de analizar y realizar configuraciones adicionales a los dispositivos, que se sigue el estándar la

NORMA ISO 27032 en la actualidad los mismos, se encuentra vulnerables sin ninguna restricción de políticas, que ocasionarían un ataque cibernético, enfocado a la denegación de servicios distribuidos (DDoS).

La infraestructura de red del hospital son de marca Huawei y que la ausencia de restricciones y seguridades provocan las siguientes vulnerabilidades y ataques en la capa de enlace son: ataques a direcciones MAC, al protocolo ARP, STP, DHCP starvation y Vlan hopping. En estos tiempos existen técnicas que permiten explotar y aprovechar estas vulnerabilidades, por medio de herramientas que serían instalados en dispositivos de los usuarios finales (Kim y Lee 2019).

Este proyecto está enfocado a fortalecer la integridad y disponibilidad de las comunicaciones, mediante la aplicación de políticas y mecanismos que brindan seguridad para mantener a estos dispositivos activos en la red.

Realizar de manera cuasiexperimental al aplicar la norma ISO 27032 de la ciber seguridad, siguiendo las fases: a) el entendimiento de la organización, b) análisis de riesgos, c) plan de acción y d) implementación. Con la ayuda de la herramienta OPENVAS, se va a realizar el análisis y pruebas de vulnerabilidades a los dispositivos de capa dos. Para continuar con las pruebas y experimentos, se realiza en el emulador EVE-ENG community**,** con las herramientas yersinia, dsniff para mitigar los ataques MAC-ARP, DHCP Starvation, Vlan Hooping y STP.

Una vez, que se ha descrito la situación problémica el problema, se define ¿Cómo solucionarían los problemas de seguridad en los dispositivos de capa dos del centro de datos del Hospital de Latacunga?

OBJETIVO GENERAL

- Implementar políticas de ciber, seguridad para los dispositivos de capa dos en el centro de datos del Hospital General de Latacunga, para la mejora de la gestión del soporte técnico en la unidad de tecnología de la información de la institución.

OBJETIVOS ESPECÍFICOS

- Analizar una metodología para la implementación de políticas de ciber, seguridad para mitigar el riesgo de indisponibilidad en dispositivos de capa dos del centro de datos del Hospital de Latacunga.
- Aplicar las políticas de ciber seguridad analizadas y mitigar la problemática de disponibilidad de los dispositivos de capa dos en la infraestructura de red del Hospital de Latacunga.
- Comparar los resultados de la implementación de políticas de ciber, seguridad con un escenario de antes y después basado con la indisponibilidad de los dispositivos de conmutación.

JUSTIFICACIÓN

Se justifica el presente trabajo de investigación como un proyecto que contribuya a la ciber, seguridad de los equipos de red de capa dos de la institución hospitalaria, las políticas de ciber seguridad, se enfocan al área de tecnologías de la información, cabe decir que estos equipos carecen de políticas que protejan a la infraestructura y el no considerar lo mencionado hace que los usuarios conectados a la red interna tengan o accedan a privilegios de administrador lo que hace que la información y la infraestructura estén vulnerables.

Por esto es conveniente realizar guías relevantes para mejorar la seguridad informática de los equipos de red para los dispositivos capa dos que mejorar su administración

para incursionar en un modelo integrativo de políticas de ciber, seguridad en los dispositivos de conmutación de la casa de salud para mitigar ciber-ataques. Este documento, se convierte en un modelo de seguridad hacia la innovación. Por lo tanto, hoy en día toda institución necesita administrar los riesgos que conlleva la exposición de los equipos de red y garantizar la operatividad de los dispositivos y reducir el costo de las operaciones en mantenimiento correctivos de seguridad de las redes e información.

Para aplicar políticas de ciber, seguridad en dispositivos de capa dos en la institución, se hace uso de las técnicas de protección ante los principales ataques a la MAC-Address, vlan hopping, ataque del hombre en la mitad, del protocolo de spanning tree, los cuales, son las principales amenazas a nivel de capa de enlace que dejaría sin servicio de red a la institución, provoca pérdidas de recursos y la ineficiencia del funcionamiento de esta casa de salud.

CAPÍTULO I: ESTADO DEL ARTE Y LA PRÁCTICA

1. Ciberseguridad en la Red

Se refiere a la capacidad de protección a nivel que aplicaran a los activos físicos y digitales, como a la información que es procesada, almacenada o transportada, la seguridad de la red, se basa en principios y conceptos específicos relacionados con los activos, las protecciones que están destinadas a detectar, reaccionar y recuperar, se de ataques, controlar las amenazas de los internos y brindar una defensa profunda(Rojas 2012).

El implementar una cantidad enorme de controles de seguridad informática para proteger los activos digitales y físicos de los empleados en las empresas, mediante el monitoreo de las acciones, lo cual, acarrea a sentimientos perjudiciales sobre el uso inadecuado que con o sin, se pretende dañar o poner en peligro significativamente la infraestructura de comunicación. El rol que desempeña el ser humano (como atacante o protector de la información) tiene un impacto en las organizaciones de la institución que depende de sus rolles en función de las políticas de ciber, seguridad definidas como lo indica(Heffel y Linares s. f.) .

Los expertos en seguridad TI, toman en cuenta que la seguridad de la información no únicamente, garantiza por medio del empleo de restricciones de seguridad sofisticados sino, que se enfocaran y tendrán en cuenta en sus tácticas de custodia al factor humano, dado el accionar del personal no espera que tengan (voluntario o involuntario) provoca la anulación de los perímetros de seguridad implementados, provoca brechas de seguridad indispensables, con las consiguientes secuelas y pérdidas económicas. La capa dos envía tramas, que contienen un conjunto definido de datos que incluye información de direccionamiento y control, dirección entre los dispositivos de origen y de destino.

1.1. Vulnerabilidades y ataques a dispositivos en capa-dos

Las personas que administran la red implementan seguridades en software y hardware, da mayor importancia a capa superiores del modelo OSI. Sin embargo, descuidan las capas inferiores que son infraestructuras más vulnerables. según el reporte del FBI el 80% de los ataques a la capa de red provienen de la intranet de la organización, debido a que el 99% de las interfaz de los equipos de comunicación están sin restricciones, por factores de gestión de los equipos del administrador de red, tal es el caso que cualquiera usuario conectarían a los en equipos mención (Xia et al. 2020).

Un Sniffer o analizador de datos de red, es uno de los eslabones que provoca la liberación sin con, sentimiento de información sensible como son los datos de los usuarios y contra, señas de equipos o programas. Estas aplicaciones de analizadores son herramientas tanto de la parte lógica y la física, han perfeccionado con el fin de generar un monitoreo inquebrantable del tráfico de la red interna y externa. Este programa, se encarga de examinar los flujos de paquetes de datos que recorren entre los equipos de la infraestructura de red ya sea de manera interno o externo. Una de estas razones es el protocolo de Rapid Spanning Tree(Ren et al. 2020).

Estas utilidades son di, señadas para facilitar el trabajo de los administradores de la red de la institución hacia los dispositivos de la capa de enlace perjudican seriamente la seguridad. Por lo que resulta lógico, que los profesionales de seguridad de la red, también, mitigarían los ataques a la infraestructura de red a nivel de capa dos como son:(Bresteau et al. 2018; Umasuthan 2016)

- Ataque de suplantación de identidad
- Ataques a la MAC-ARP.
- Ataque STP
- Ataques a Vlans Hopping
- Ataques DHCP starvation

1.2. Ataque de suplantación de identidad Sniffer para robo identidad

Un Sniffer o analizar de red es utilizado para suplantar identidad, estas utilidades son tanto de hardware o de software, que han desarrollado con el objetivo de generar un captura y monitoreo constante del tráfico de la red local o externa. Este rastreo, se encarga de analizar los flujos de paquetes de datos que son enviados y recibidos entre los equipos de la red, ya sea a nivel interno o externo, utilizado en converger (Ren et al. 2020).

1.3. Ataques basados en MAC y ARP

De las siglas Address Resolution Protocol (ARP) es un protocolo de nivel de capa de enlace, responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP (Molina y Gabriela s. f.).

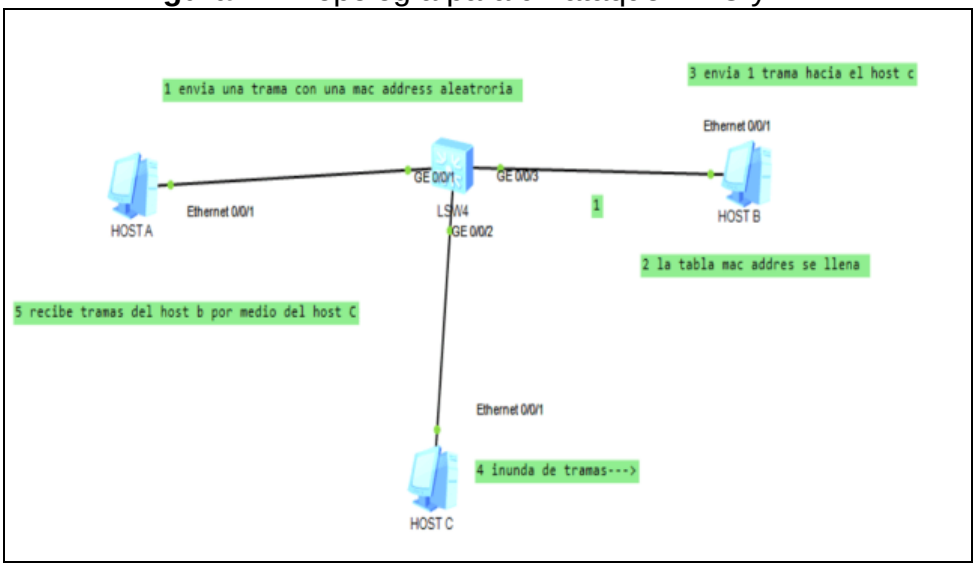
Su funcionalidad envía un paquete (ARP request) a la dirección de difusión de la red (broadcast con MAC = xx xx xx xx xx xx) que contiene la dirección IP por lo, que se pregunta y espera a que esa máquina responda (ARP reply) con la dirección Ethernet que le corresponde. Cada host mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan.

En la infraestructura dos hosts, comunican si solo si conocen sus direcciones MAC, de lo contrario, envía un mensaje de solicitud de transmisión ARP a todos los demás hosts de la red, y el que tenga la dirección IP coincidente responde con un mensaje de respuesta ARP unicast con su dirección MAC, debido a que la interfaz no está protegida y allane el camino, para que el atacante envenene la caché con entradas falsas. El envenenamiento de la memoria caché ARP provocaría efectos devastadores sustanciales en la red. Los hosts malévolos de la red realizarían muchos tipos de ataques a la red, como suplantación de ARP, ataque Man-in-the-Middle (MitM), ataque

de denegación de servicio (DoS), se pasar por los hosts contaminados e inunda el tráfico de la red y demás (B y Nagamalai 2018).

En la figura 1-1, muestra una topología estrella para realizar un envenenamiento de caché ARP, con pares IP-MAC falsos que serían realizado por cualquier persona, que esté en la intranet de la institución y con algún conocimiento de scripting y utiliza varias herramientas de código abierto, para llevar a cabo el ataque a la red. La memoria caché ARP, llenaría de dos formas ya sea de forma estática por una red más pequeña o dinámicamente por la mayor cantidad de hosts (Prabadevi, Jeyanthi, y Abraham 2020).

Figura 1-1 Topología para un ataque MAC y ARP



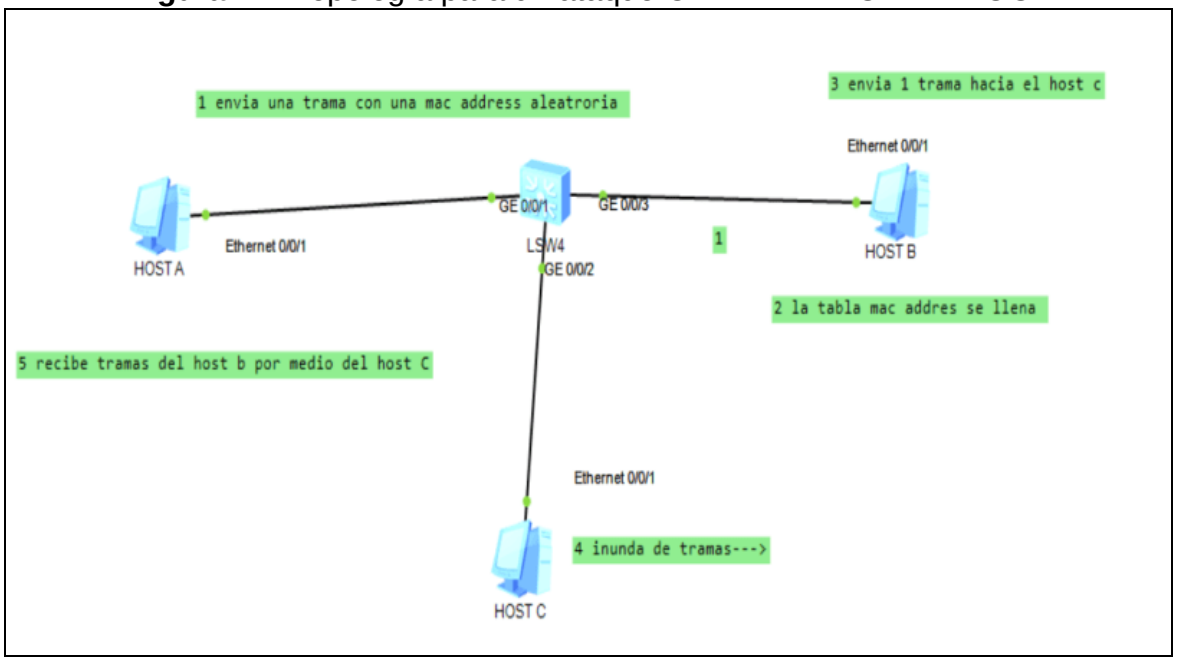
Fuente: Elaboración propia

Con lo expuesto determina las siguientes formas de ataque por MAC y ARP:

1.4. Cam Table Overflow

El principio del ataque es el consumo de hardware del switch como, se observa en la figura 2-1 que mantiene la tabla de Forwarding, que relaciona las MAC con los puertos de conexión a esta tabla, denomina CAM (Content Addressable Memory). Si esta memoria CAM llega a inundar, se, el equipo funciona como un HUB, en otras palabras, todo paquete que recibe el switch donde si la dirección MAC destino, no se encuentra en la tabla MAC ésta tabla, encuentre llena el paquete es enviado por todos sus puertos sin control. Esto permitiría a un atacante capturar todo el tráfico con un sniffer instalado en algún terminal de la red.

Figura 1-2 Topología para un ataque CAM TABLE OVERFLOOD



Fuente: Elaboración propia

1.5. ARP Spoofing

Este ataque tiene que ver con el funcionamiento del protocolo ARP y la memoria caché del switch donde almacena la información para ello, envía un pedido al protocolo ARP que le reenvía y posteriormente, almacena en la tabla de direcciones MAC del switch durante una frecuencia de tiempo determinado, así ‘‘también’’ existen los protocolos GARP3 que contienen la dirección MAC y la IP del host y envían la petición de broadcast a todos los equipos de capa de enlace de la infraestructura de red para que todos los hosts conectados y activos en la red y actualicen en la memoria caché ARP existentes en ella actualicen su memoria caché ARP pero es importante indicar, que se aplica a los dispositivos que están configurados con direccionamiento dinámicos y aquellos que acepten estas solicitudes.

Estos paquetes no generan respuestas por parte de los Hots que los reciben, pero si una máquina lo recibe lo asigna a su tabla. Al ser mensajes de broadcast no están di, señados para suministrar ningún tipo de validación para su identificación en la transacción por ende el falsificar la información de los paquetes de lo que llevan sería muy simple y con, serva él envió de los paquetes en frecuencia cortos como para que la memoria cache de los equipos no elimine la información de entradas, conseguiría generar conexiones lógicas diferentes a las conexiones reales.

1.6. Ataque Vlan

La vulnerabilidad relacionada con las Vlan consiste en el salto de Vlan, un atacante al estar en una Vlan definida en la interfaz de los equipos que ingresarían al tráfico en diferentes Vlans, que normalmente no estaría accesible, por lo que pasaría por alto a un dispositivo de Capa 3.

Los ataques de salto de Vlan ocurrirán en las siguientes etapas:

- El primer paso es cambiar el modo del conmutador conectado a la PC del hacker del puerto de acceso, al modo del puerto troncal.

- Esto implica que, al configurar el puerto de acceso, los paquetes Ethernet que contienen la etiqueta Vlan y eliminan del puerto de acceso debido al formato de paquete incorrecto.

- El atacante envía paquetes del protocolo de enlace troncal dinámico LNP que cambiaran el puerto del conmutador del modo de acceso al modo troncal. Si reciben paquetes LNP, el conmutador cuya función LNP está habilitada cambia el estado del puerto al que llega el paquete LNP del modo de acceso al modo de troncal.

- Luego, el atacante inserta una etiqueta con la ID de Vlan a la, que se envía el paqueteen el paquete normal, y el paquete reenvía a esa Vlan, e inserta una ID de Vlan de 20 en el paquete y el paquete transmitiría a la PC víctima que pertenece a la Vlan 20.(Mahmood, Mohsin, y Akber 2020)

Para el cual, se ha encontrado los siguientes ataques como son:

1.6.1. Ataque Vlan Hopping

Es un método de atacar a los recursos en red en una Vlan que hace a un atacante use privilegios de interface como puertos troncales (trunk) quienes permite insertar al atacante etiquetas (tag), la cual, permite tener acceso a las diferentes Vlans.

El concepto básico detrás de todos los ataques de salto de Vlan es para un host atacante en una Vlan para tener acceso al tráfico en otras Vlan que normalmente no serían accesibles. Hay dos métodos principales Vlan Hopping: switch spoofing y doble etiquetado.

1.6.2. A Ataque Switch Spoofing

Un delincuente informático de red configura un dispositivo para simular el funcionamiento como un switch que emula con etiquetas 802.1Q, se utiliza para negociar enlaces entre dos dispositivos y así, también, la negociación del tipo de encapsulación.

El sistema del atacante sería un enlace trunk al switch, enviarían paquetes para cualquier Vlan soportada por el enlace trunk, y finalmente, el atacante comunica con cualquier dispositivo en cualquiera de las Vlan asociadas.

1.6.2.1. Ataque A Vlans – Double Tagging.

Es un ataque de etiquetado doble, un host atacante antepone dos etiquetas Vlan a paquetes que transmite. El primer encabezado (corresponde a la Vlan que el atacante es realmente un miembro) es despojado por un primer conmutador que encuentre el paquete, y entonces envía el paquete. El segundo falso, el encabezado es entonces visible para el segundo conmutador, que se encuentra con el paquete. Este falso encabezado Vlan indica que el paquete está destinado para un host en un segundo, Vlan de destino. El paquete es enviado al host de destino como si tratara de tráfico en la capa 2. Mediante este método, la máquina atacante pasaría por alto medidas de seguridad de la capa 3, que se utilizan para aislar lógicamente los hosts de los demás (Mahmood et al. 2020).

1.7. Ataques basados en DHCP Starvation

Son ataques que realiza en contra el servidor DHCP con el objetivo de inundarlo de peticiones DHCP DISCOVER con direcciones MAC falsificadas que, con el fin de inundar el espacio de direcciones asignables en el equipo, agota completamente el espacio de los equipos de direcciones MAC asignables en un cierto tiempo, el objetivo del ataque es que el servidor DHCP no sea capaz de responder a otros Hots, y así el atacante realiza otro tipo de ataque denominado (DHCP Rogue). Esto da lugar a un DHCP ROGUE ATTACK (Prabadevi et al. 2020).

1.7.1. Ataques basados en STP

El protocolo de Spanning Tree (STP) es el protocolo que sirve para gestionar o administrar la presencia de bucles físicos en la topología de red, debido a la existencia de enlaces redundantes (importantes en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo stp admite a los dispositivos de capa dos activar o desactivar involuntariamente las líneas de conexión (Mehra y Krishnan 2018).

Los bucles infinitos ocurren si hay rutas alternativas hacia una misma máquina o segmento de red de destino. Estas rutas alternativas son necesarias para proporcionar redundancia, que ofrece una mayor fiabilidad. Si existen varios enlaces, en el caso que uno falle, otro enlace soporta el tráfico de la red. Los problemas aparecen si utilizan dispositivos de interconexión de nivel de enlace, como un puente de red o un conmutador de paquetes. Si hay bucles en la topología de red, los dispositivos de interconexión de nivel de enlace reenvían indefinidamente las tramas Broadcast y multicast, al no existir ningún campo TTL (Time To Live) en la Capa 2, tal y como ocurre en la Capa 3.

De esta manera consume una gran cantidad de ancho de banda, y en muchos casos la red queda sin servicio. Un Router, por el contrario, sí evitaría este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos

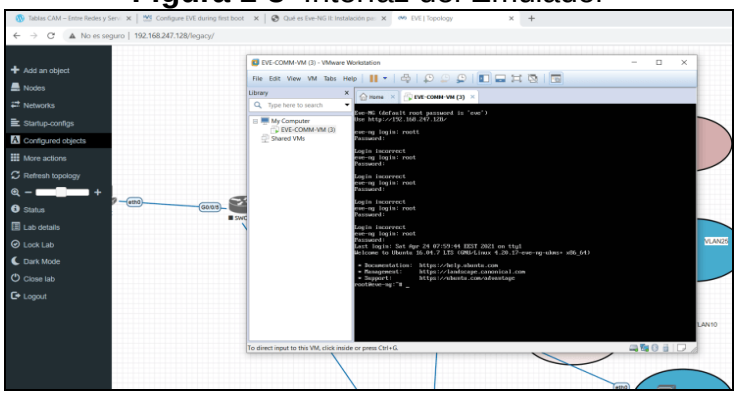
redundantes, pero crear una topología lógica libre de bucles. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como re, serva, para activarlos, en caso de que falle el camino inicial (Umasuthan 2016).

Si la configuración del protocolo STP varía, si una parte de la red redundante llega a ser inalcanzable físicamente en la infraestructura de red, el algoritmo STP reconfigura los enlaces y restablece la conectividad únicamente habilita de manera correcta, activa uno de los enlaces de re, serva previamente configurado. Si el protocolo falla, provoca que ambas conexiones estén activas comparablemente, lo que provoca un bucle de tráfico en la LAN(Mehra y Krishnan 2018).

1.8. Herramientas para detectar vulnerabilidad en dispositivos de capa-dos

Para simular el ataque de seguridad en los dispositivos de capa de enlace, utiliza las herramientas de análisis de vulnerabilidades Openvas, la que escanea y al aplicar diferentes métodos de explotación propios de la herramienta. Sin embargo, la herramienta solo consiguió emitir resultados de ataque de MAC, por consiguiente, no determinarían los diferentes ataques, que se realizan nivel de capa de enlace. Por lo tanto, la configuración de cada uno de los dispositivos de análisis y determinan la falta de configuraciones para mitigar ataques.

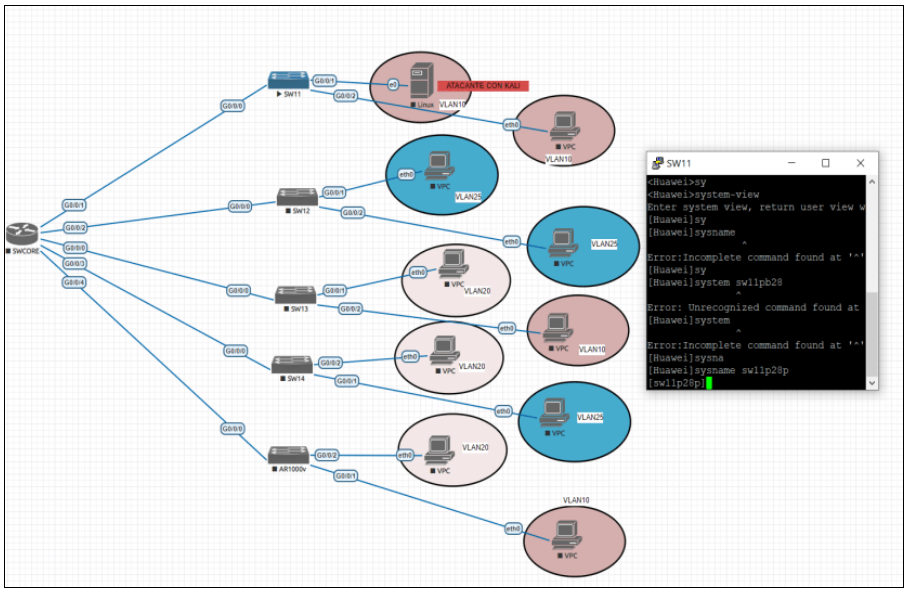
Figura 1-3 Interfaz del Emulador



Fuente: Elaboración propia

Para continuar con el análisis de ataques, ha realizado pruebas en el simulador ENSP con resultados mínimos. Sin embargo, el análisis y él estudió, se utiliza la herramienta EVE-NG, observa en la figura 1-3 pantalla de inicio de la herramienta que permite realizar las pruebas de vulnerabilidades para equipos de tecnología Huawei, que están instalados en la casa de salud, utiliza dispositivos de capa dos con terminales, que son utilizados como clientes finales, así también, con equipos con sistema operativo Linux, que permiten instalar aplicativos como son: yersinia, dsniff (Mehra y Krishnan 2018).

Figura 1-4 Topología de la red en Eve-ng

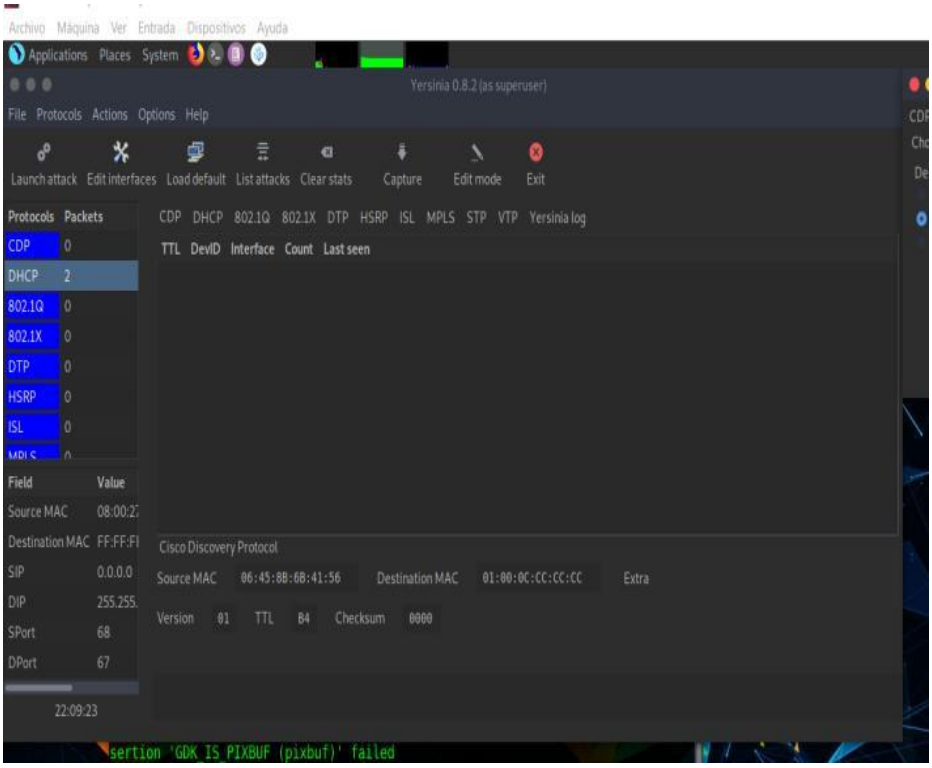


Fuente: Elaboración propia

1.8.1.1. Yersinia

Yersinia es un software que permite realizar ataques de capa 2, se observa la interfaz del programa en la figura 5-1. Con el fin de descubrir las vulnerabilidades que tienen el diferente protocolo de red, y los riesgos que están expuestos. Yersinia implementa ataques de suplantación e incumplimiento de parámetros para el protocolo de configuración dinámica del host a ser analizado (Kim y Lee 2019).

Figura 1-5 Interfaz de herramienta Yersinia



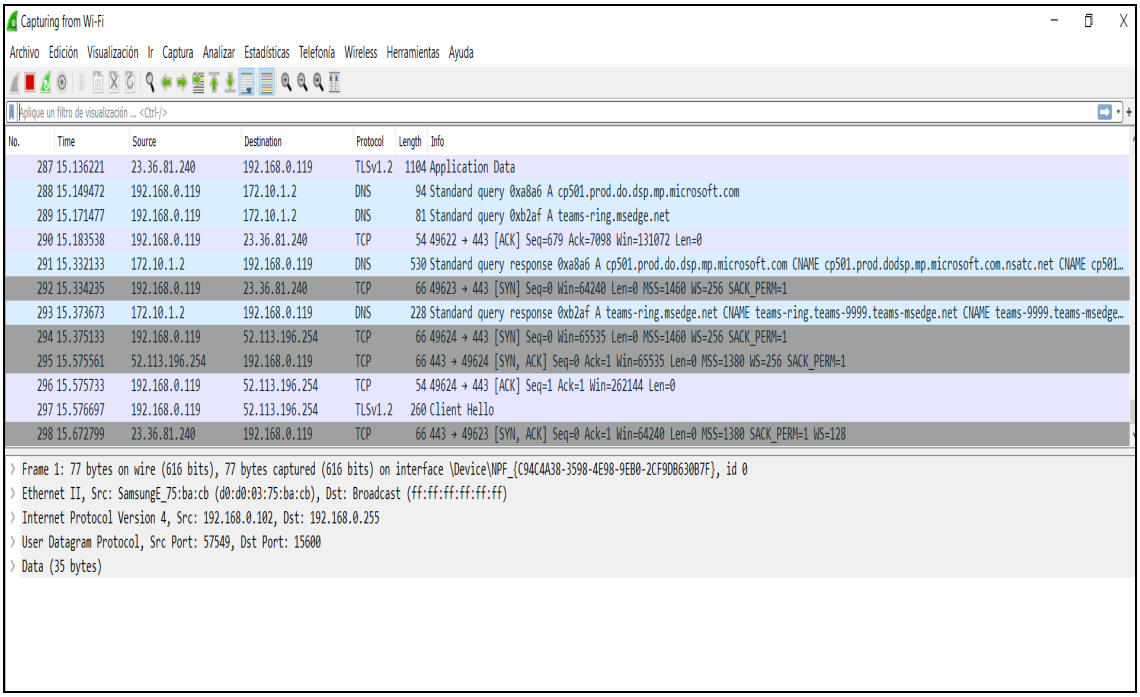
Fuente: Elaboración propia

1.8.1.2. Wireshark Analizador

La figura 6-1 muestra la pantalla de inicio de wireshark es un concentrador de varias herramientas en una aplicación, se utiliza para analizar la estructura del tráfico de la red en busca de posibles errores de configuración y ataques de seguridad, el identificar

muchos tipos de encapsulación, aislar y mostrar todos los campos de un paquete de red. Con todas esas capacidades, pensarían que Wireshark sería difícil de aprender.

Figura 1-6 Interface de herramienta



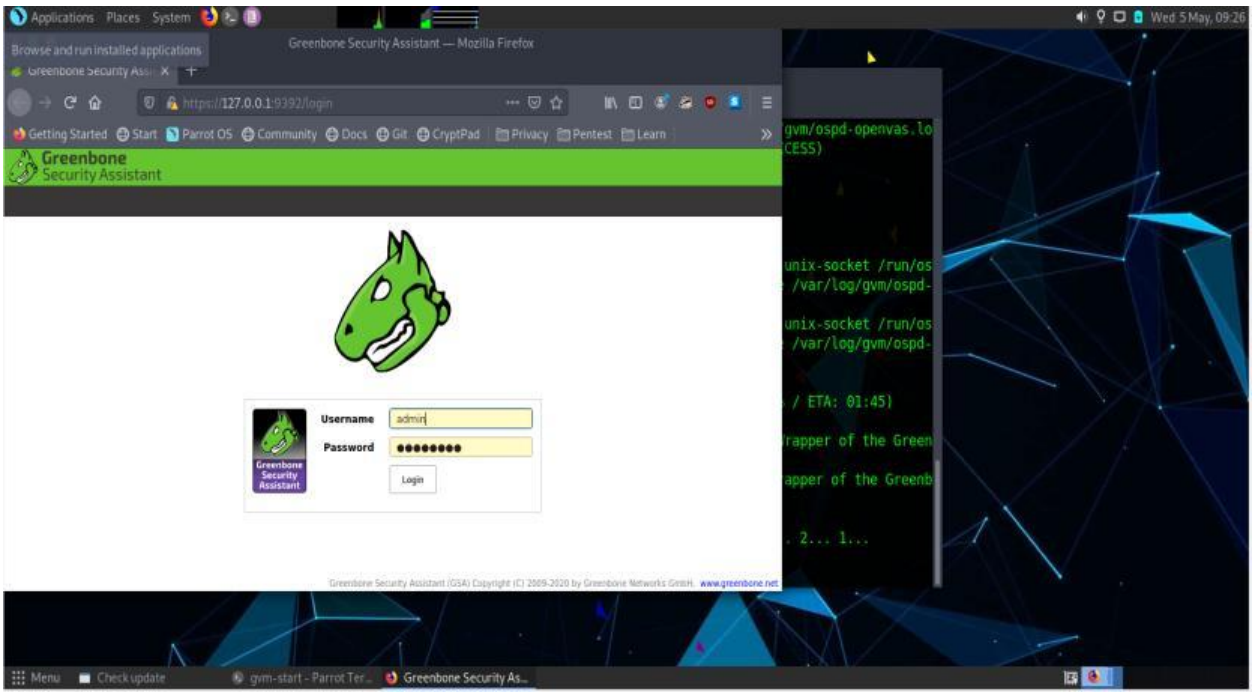
Fuente: Elaboración propia

En Wireshark los filtros, se refieren a Berkeley Packet Filters, que en realidad es un lenguaje de microprogramación que compila y ejecuta en tiempo de ejecución contra paquetes interceptados por herramientas como tcpdump y Wireshark.(Ndatinya et al. 2015)

1.8.1.3. Openvas para Análisis de Vulnerabilidades

Es una herramienta par escáner de vulnerabilidades en redes, servidores y aplicaciones. Puesto que integra con otras herramientas de seguridad y la posibilidad de desarrollar plugins y network vulnerability (Xia et al. 2020).

Figura *1*-7 Interfaz de herramienta Openvas



Fuente: Elaboración propia

El escaneo de vulnerabilidades es una práctica indispensable para los especialistas en ciber, seguridad. Estos individuos emplean vulnerabilidad herramientas de escaneo para identificar debilidades en los sistemas y probar para eliminar las deficiencias descubiertas para que el sistema de seguridad esté asegurado. Los resultados del escaneo de tales herramientas que utiliza para evaluar el nivel de riesgo general de los sistemas en para gestionar las vulnerabilidades descubiertas de forma priorizada.

Se espera que lo utilicen usuarios avanzados, como la ciber, seguridad especialistas o pentesters, los escáneres de vulnerabilidades no fueron di, señados y pensar en la usabilidad. Sin embargo, la usabilidad de tales herramientas es de gran importancia para generar y resultados de escaneo completos y para evaluar el escaneo informes correctamente, de modo que los ataques no deseados debido a inadvertidos, se prevendría las vulnerabilidades residuales en los sistemas proactivamente (Aksu, Altuncu, y Bicakci 2019).

1.9. Mecanismos para proteger los dispositivos de capa dos

A través del análisis de tráfico en la red, se logra identificar los servicios que circulan por la red, que concluye mediante la aplicación de reglas y la priorización de servicios lograr minimizar las vulnerabilidades de los dispositivos de capa dos de la red de datos, que ocasionan en ciertos momentos la saturación de la red de datos. Mediante la segmentación a los hosts, se logra dividir y agrupar a por cada departamento con un distinto direccionamiento de red, de este modo, el di, seño resulta efectivo para la administración y gestión del direccionamiento IP de cada subred y para la implementación de las políticas para cada subred (Castillo y Eduardo 2020).

1.9.1. Medidas de protección

Los delincuentes informáticos que actúan en contra de la infraestructura de la red LAN de capa dos, se ve comprometida debido a que los administradores de red regularmente implementan soluciones de seguridad para proteger los componentes en la Capa 3 y hasta la Capa 7. Por ejemplo, si un atacante con acceso a la infraestructura de la red interna y captura las tramas de información en la Capa 2, entonces la seguridad implementada en las capas anteriores sería inútil por tal razón, se describe a continuación, los posibles ataques a la capa dos:

1.9.2. Seguridad para acceso SSH a dispositivos de red

SSH (Secure Shell) es un protocolo que proporciona acceso remoto seguro a dispositivos de la red. La comunicación entre el cliente es encriptado con el protocolo SSH, evitando que terceras personas puedan descubrir el usuario y contraseña ni lo que se escribe durante toda la sesión.

1.9.3. Limitar la velocidad del tipo de paquetes

Limitar la velocidad de los paquetes (información) para que el CPU del equipo, no se sobrecargue y que provoque que el dispositivo no funcione de la mejor manera y considera las siguientes características:

- Los paquetes enviados a la CPU se clasifican según los tipos de protocolo.
- El ancho de banda, la prioridad y la longitud del paquete, que se envían desde el cliente y de reenvío al CPU.
- Se controla el ancho de banda de reenvío total.

De esta manera, la cantidad de paquetes enviados a la CPU del switch está bajo control y el ancho de banda es asegurado para los servicios de mayor prioridad, también, la sobrecarga del CPU es prevenida y genera una alarma si ocurre un ataque.

Actualmente los servicios son afectados negativamente por personas o sistemas automatizados y son atacada debido a las siguientes razones: a) Los paquetes de protocolo válidos, no se distinguen de los paquetes de protocolo no válidos, b) En consecuencia, la CPU aumenta su uso de recursos considerablemente y los paquetes válidos, no se procesarían correctamente, y c) Los paquetes de algunos protocolos son enviados a la CPU a través del mismo canal. Si un loopback ocurre en un cierto tipo de paquete de protocolo afecta, también, la transmisión de otros paquetes de protocolo.

1.9.4. Seguridad de puertos en los dispositivos de capa-dos

Activar la seguridad: en los Switch por defecto, la seguridad de puertos esta desactivada.

- Registrador de direcciones MAC: En esta opción uno digita en una interface que la MAC Address sea fija, o simplemente ponerla en modo Sticky, lo que

hace que la interfaz aprenda la dirección MAC del primer equipo, que se conecte.

- Limitar el número de direcciones de MAC: Esta opción hace que haya un número de máximo de MAC Address por aprender en esta interfaz y aprendería de 1 a 132 MAC.
- Violación de seguridad: En esta opción le indica al Switch que hacer en caso de que hay una Violación de seguridad, una dirección MAC, por ejemplo, que no esté autorizada a enviar tráfico.
- La interfaz en modo Protegido sólo permite tráfico de direcciones MAC permitidas en la configuración del equipo descarte el tráfico del resto, no se notifica sobre la intrusión.
- La interfaz en modo Restrict: envía un mensaje SNMP al administrador de red y el tráfico de la interfaz permite comunicación únicamente a las MAC especificadas del resto.
- La interfaz en modo Shutdown: el puerto de la interfaz esta inhabilitada y pasa al estado err-disable (no shutdown en el puerto)

1.9.5. Interfaz de confianza para enviar el DHCP STARVATION

Configurar las interfaces del switch para permitir que los clientes DHCP obtengan direcciones IP solo de servidores DHCP autorizados, configure las interfaces conectadas directa o indirectamente a los servidores DHCP confiables por el administrador configura como interfaces confiables, y otras interfaces como interfaces que no confiables. Esto para evita que los servidores DHCP falsos asignen direcciones IP a los clientes DHCP (Yaibuates y Chaisricharoen 2020).

1.9.6. Seguridad de ACL en los dispositivos

Una Access Control List (ACL) es un servicio que incluye reglas ordenadas que restringen procesos en el dispositivo y que contienen la dirección de origen, dirección destino restricción de número de puerto en los paquetes. Se configurar una ACL para rechazar todo acceso Telnet desde la red inalámbrica al servidor local (Ha, segawa et al. 2016).

1.9.7. Seguridad STP para dispositivos de capa dos

BPDU Guard es una mejora del protocolo STP que, si está habilitada, coloca un puerto en modo errdisable si reciba cualquier paquete BPDU en ese puerto. Esta función generalmente configura al puertos de acceso donde, no se espera recibir ningún paquete BPDU, que llegue desde dispositivos conectados a estos puertos, por ejemplo, computadoras, impresoras, teléfonos IP u otros dispositivos de usuario root final (Ochoa Palomino 2019).

1.10. Datos estadísticos de vulnerabilidades en la infraestructura de red

El 56 % de los ataques cibernéticos, se centran en la denegación de servicio (Ddos) los cuales, están enfocados principalmente en capas superiores del modelo OSI, sin embargo, las vulnerabilidades revisadas en párrafos anteriores de los dispositivos de capa dos, se identificarían que directamente están orientados a dejar sin servicio a la infraestructura (Chakraborty et al. 2019).

En el sector salud cada vez está es objetivo de piratas informáticos debido a la información sensible, que se maneja y que son explotados con fines socio económicos.(Argaw et al. 2020)Adicional en el Ecuador desconocen los datos específicos de ataques a dispositivos de capa dos puesto que aun la mayoría del personal que administra las redes de la infraestructura, se centra a que los dispositivos

de la infraestructura de red funcionen con el desconocimiento de los riesgos que corren al no implementar políticas de ciber, seguridad (Anón s. f.).

1.10.1. Normas ISO de ciber, seguridad para la gestión de Redes

Para definir las políticas de ciber seguridad se utiliza las normas ISO establecidas por la Organización Internacional para la Estandarización y los estándares de ciber, seguridad. En este sentido, la norma ISO/IEC 27001 es certificable para seguridad informática, la cual, detalla los requerimientos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de seguridad de Información (SGSI). Cada empresa u organización es un mundo diferente y la manera como implementan las restricciones para lograr los resultados de mejora, se hace uso de la norma ISO 27032 (Carrillo et al. 2020).

La norma ISO 27032 brinda la disposición para fortalecer el estado de la Ciber, seguridad utiliza los items técnicos y estratégicos importantes que están alineados con la seguridad en: las Redes, el internet, información y aplicaciones.(Anón s. f.). Además, esta norma permite obtener una visión general de la ciber, seguridad de la organización, que tiene como fin ayudar a cubrir las buenas prácticas aplicada a las partes involucradas en el ciberespacio, para la interrelación entre la ciber, seguridad y otro tipo de seguridad de la organización (entorno físico) establece un mecanismo de colaboración entre ellas como describe en la figura 8-1.

Figura 1-8 Faces de la norma ISO 27032

Fuente: www.i, secauditors.com/consultoria-csf-iso-27032

CAPÍTULO II: Caracterización de la institución

El Hospital General de Latacunga es una casa de salud que proporciona servicios de salud con la mejor calidad en cuanto a la asistencia de salud especializada de segundo nivel, al través de su portafolio de servicio, se observa a detalle en la figura 1-2 y cumplir con la responsabilidad de recuperación y rehabilitación de la salud, docencia e investigación, acorde a las políticas del Ministerio de Salud Pública (Dz3 MSP s. f.). La figura 1-2 muestra el organigrama de la institución, que permite identificar su estructura y visualizar al área de TI, como parte del área administrativa y esencial de la institución para la administración de los equipos de red.

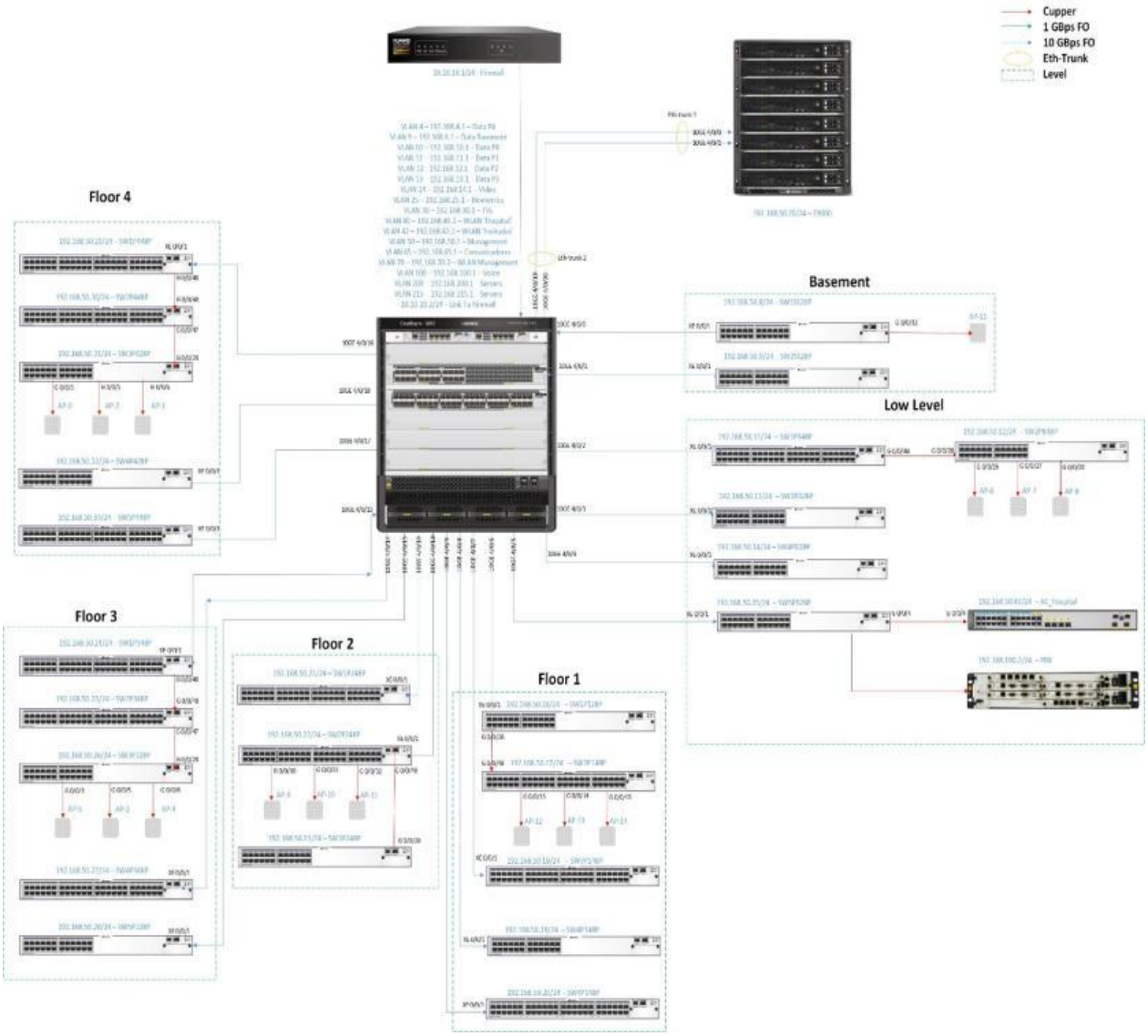
Figura *2*-1 Diagrama de la estructura institucional

Fuente: Elaboración Propia

El personal de TI de la institución está a cargo de la infraestructura de red, mantener la administración y las seguridades de la infraestructura de manera básica. En la figura

2.1 muestra la topología y la distribución de los equipos de red que tiene como parte modular un SWCORE y la topología en estrella con lazos redundantes en etapas donde la troncal principal son comunicados por cable de cobre UTP hacia los dispositivos decapa dos de cada uno de los segmentos de red.

Figura *2*-2 Topología de red de la institución del Hospital



Fuente: Elaboración Propia

METODOLÓGICA INVESTIGACIÓN

En este apartado define el tipo de investigación a utilizar, se diseñó métodos, técnicas e instrumentos con su respectiva validación, con el objetivo de mitigar ataques a los dispositivos de capa dos del hospital general de Latacunga.

Para ello, se usa un método cualitativo basado en un estudio general para el cálculo del riesgo de vulnerabilidades, realiza ataques controlados y medidas de solución, puesto que abarcar dispositivos de capa dos de la infraestructura tecnológica del hospital. Las herramientas como: Openvas, WireshARP y Nmap son utilizadas para la exploración y el escaneo de las vulnerabilidades de la red de comunicaciones de la marca Huawei instalados en la institución.

2.1. Tipo de Investigación y Enfoque de investigación

El tipo de estudio es científico investigativo aplicada, porque se basa en los conocimientos existentes; de nivel exploratorio y descriptivo, el que permite detallar y explicar las vulnerabilidades como resultado de la falta de políticas de seguridad para dispositivos de capa dos para el centro de datos de la institución de salud.

2.1.1. Tipo de la recolección de la información

Este trabajo aparece a partir de los problemas identificados en el área de TICS, no dispone de un control adecuado de activos intangibles informáticos los cuales, se encuentran con sistemas operativos sin soporte, no licenciados y una incompleta configuración de la administración de seguridad de dispositivos de conmutación.

2.2. Método de Investigación

El método seleccionado es el científico, de tipo mixta porque contienen aspectos cualitativos y cuantitativos, también, es exploratoria descriptiva y documental mediante la cual, se realiza la observación sistemática que dan lugar a la formulación del problema: La aplicación de políticas de ciber, seguridad disminuyes las vulnerabilidades de los dispositivos de capa dos. Esta problemática, se basa en el razonamiento deductivo y mediante la experimentación levanta un escenario de prueba adecuado, para finalmente analizar los resultados que permitan obtener soluciones apropiadas para cumplir con la pregunta planteada en esta investigación.

2.2.1. Población de estudio

Para el cálculo de la muestra de la investigación, se tomó los datos del Ministerio de Salud Pública de la zona 3 debido a que las instituciones cuentan con infraestructura similar marca huawei; donde indica que construyeron y repotenciaron 12 casa de salud, para lo cual, se eligió al Hospital General de Latacunga que cuenta con el siguiente equipamiento en su infraestructura de red como muestra la tabla 1-2.

Tabla 2-1: Equipamiento marca y modelo de la red de la institución.

ítem	Marca	Modelo	Versión	Cantidad	Tipo	Ubicación
1	Huawei	cloudengine 12800	V100R006C0	1	SWCORE	Centro de Datos
2	Huawei	USG6300	V200R008C0	1	FIREWALL	Centro de Datos
3	Huawei	S5720	V200R008C0	25	SWITCH	Centro de Datos (7), piso 1, Piso 2, Piso 3
4	Huawei	Ac6605s	V100R005C50	1	CONTROLADORE WIRELESS	Centro de Datos
5	Huawei	Ap 7030de	V100R005C50	12	ACCES POINT	Centro de Datos

Fuente: elaboración propia

2.2.2. Técnicas de recolección de datos

Para esta investigación la recolección de información, se usa las técnicas mostradas, a continuación, por tal razón utiliza los siguientes programas y describen en la tabla 2-2:

- ***Encuesta al personal:*** Dentro de esta técnica, se aplicó encuestas dirigidas a los administradores de red, para identificar la problemática existente en la institución.

- ***Búsqueda de información:*** a través de esta técnica, se obtiene fuentes de información referenciados por expertos en el tema y aprobada por la comunidad científica como son documentación científica y tesis de desarrollos.

- ***Pruebas:*** a través de pruebas de concepto demuestran que una aplicación o servicio serían vulnerable al realiza experimentos en escenarios de laboratorio.

Tabla 2-1: Sistemas y herramientas utilizadas en el desarrollo**.**

Herramienta	Descripción
S.O WINDOWS 10	Sistema operativo de Microsoft, instalado las herramientas para las pruebas respectivas.
ENSP	Es un emulador propio de Huawei que permite probar configuraciones, para aprender el funcionamiento de esta tecnología, pero con limitaciones de inyectar protocolos.
EVE-NG	Es un software de emulación de red multiproveedor con una interfaz html5, la que permite una fácil interacción para hacer uso de imágenes quemu marca Huawei
VMARE	Software de virtualización
VIRTUALBOX	Software de virtualización
KALI LINUX	Sistema operativo dedicado a auditorias y pruebas de esfuerzo para seguridad informática
PARROT DEBIAN	Sistema operativo dedicado a auditorias y pruebas de esfuerzo para seguridad informática
YERSINIA	Es una herramienta utilizada para probar y detectar debilidades de la seguridad de la capa 2 en los protocolos de red puesto que soporta los protocolos: Spanning Tree Protocol (STP) Cisco Discovery Protocol (CDP)

	Dynamic Trunking Protocol (DTP) Dynamic Host Configuration Protocol (DHCP) Hot Standby Router Protocol (HSRP) IEEE 802.1q, Inter-Switch Link Protocol (ISL) VLAN Trunking Protocol (VTP)
DSNIFF	Es un conjunto de herramientas de análisis de tráfico de red y rastreo de contraseñas y soporta los protocolos: Telnet SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP , OSPF , PPTP MS-CHAP , NFS , VRRP , YP / NIS , SOCKS , X11 , CVS , IRC.
OPENVAS	Es una herramienta de software libre especializado en el escaneo y gestión de vulnerabilidades para sistemas y equipos informáticos.

Fuente: Elaboración Propia

- ***Observación:*** Esta técnica permite obtener información registrada durante la experimentación, mediante las pruebas de concepto en los escenarios de simulación.

2.3. Políticas de Ciberseguridad al aplicar la norma ISO 27032

Para realizar una valoración integral de las debilidades a una red LAN, se sigue la norma ISO 27032, que enfatiza en las cuatro fases que permite calcular el nivel de seguridad en una red.

Se realiza las pruebas de vulnerabilidades y en otros casos de intrusión, donde evalúan minuciosamente los niveles de seguridad en los dispositivos de capa de enlace, utiliza el emulador EVE-ng integra pocas imágenes quemu de cada modelo de equipo de red de la marca Huawei simultáneamente con un sistema operativo Linux, y b) pruebas en equipos físicos reales en un ambiente controlado.

2.4. Fase I

2.4.1. Entendimiento de la Organización

El Hospital General de Latacunga es una institución pública provee de servicios de salud a la colectividad de la provincia de Cotopaxi apoya, también, a unidades operativas de nivel uno. Con la integración de la red integral de salud (RIS) un paciente sería atendido en cualquier parte del Ecuador y contar con su historial médico, por lo que, es importante que la institución mantenga su disponibilidad de conexión en la red de 24/7, que permita subir y descargar información a las plataformas gubernamentales, compartir exámenes médicos y evoluciones de enfermedades.

La institución consta con servicios como: consulta externa, emergencia, medicina, interna, cirugía general, laboratorio, medicina transfusional, UCI, quirófano, área de quemados, pediatría, centro obstétrico, maternidad, neonatología, traumatología cardiovascular, neurocirugía, rayos x, farmacia, mantenimiento, gestión administrativa, y área de tecnologías. Estas generan información, la cual, es compartida para ministerio de Salud Pública.

Los datos que genera el personal de la institución son analizadas y digitalizadas por equipos biomédicos, así como la atención médica que son recopilados a través de equipos de cómputo. En el centro de datos de la institución existen switches, PBX de telefonía y servidores. Los equipos de red que funcionan en el centro de datos de la institución no cuentan con mecanismos de ciber seguridad, que se encuentran propensos a ataques.

2.5. Fase II

2.5.1. Análisis de Riesgos

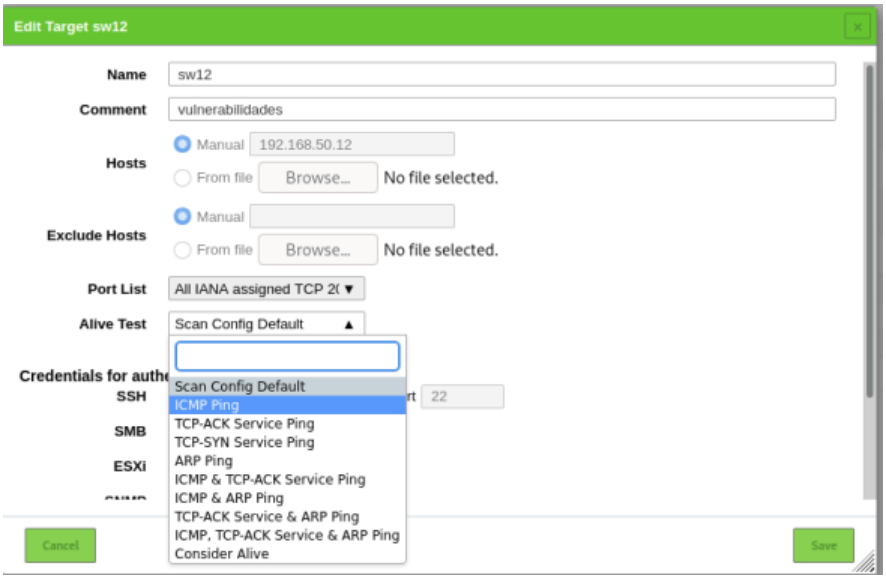
En esta fase, se lleva a cabo la evaluación con encuestas, herramientas y técnicas para detectar amenazas, vulnerabilidades de los equipos de capa de conmutación de la institución.

2.6. Análisis de vulnerabilidades con la herramienta OPENVAS

Para empezar la detección de vulnerabilidades con la herramienta OPENVAS instalada sobre un sistema operativo Linux (Parrot), que permite realizar un análisis de la infraestructura de red, se configura el identificador gateway del equipo, que permitió obtener el informe en formato PDF (Anexo 1) la información estadística de cada uno de los equipos de red.

En la figura 2-3 muestra los parámetros a configurar y la dirección adicional, para escoger el tipo de prueba requerido.

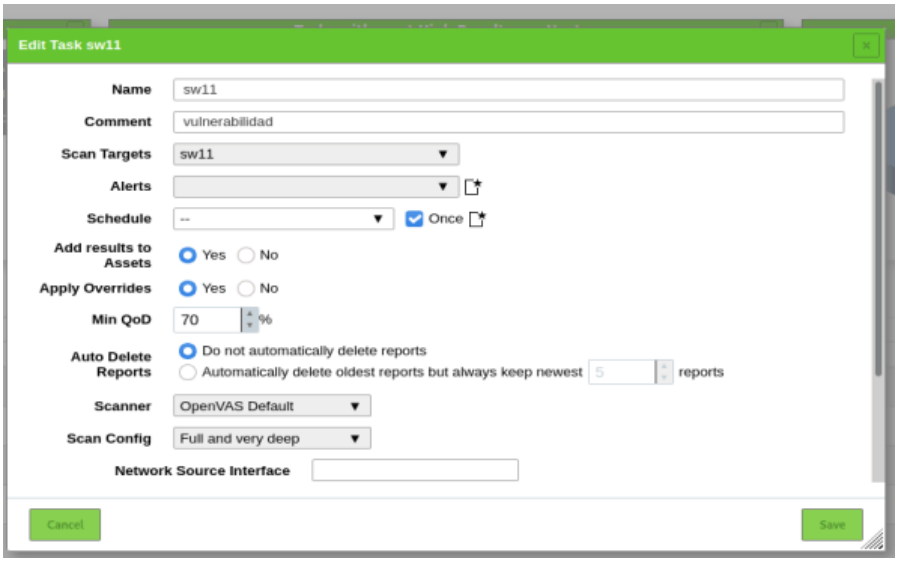
Figura *2*-1 Procedimiento para Openvas



Fuente: Elaboración Propia

En el paso siguiente en la figura 2-4, se agrega la tarea con el nivel de escaneo que requiere realizar esto depende de que profundidad, se realiza las pruebas y las características de protocolos vulnerables.

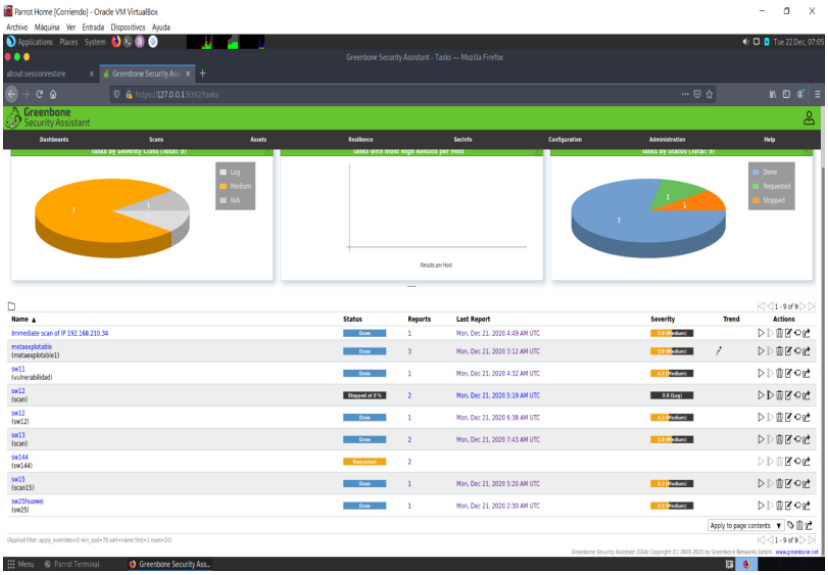
Figura *2*-2 Procedimiento para escoger el equipo openvas



Fuente: Elaboración Propia

Entonces ejecuta la tarea de escaneo y que depende del procesador del equipo el análisis es rápido y para terminar la prueba genera como resultado un documento pdf en la figura 2-5.

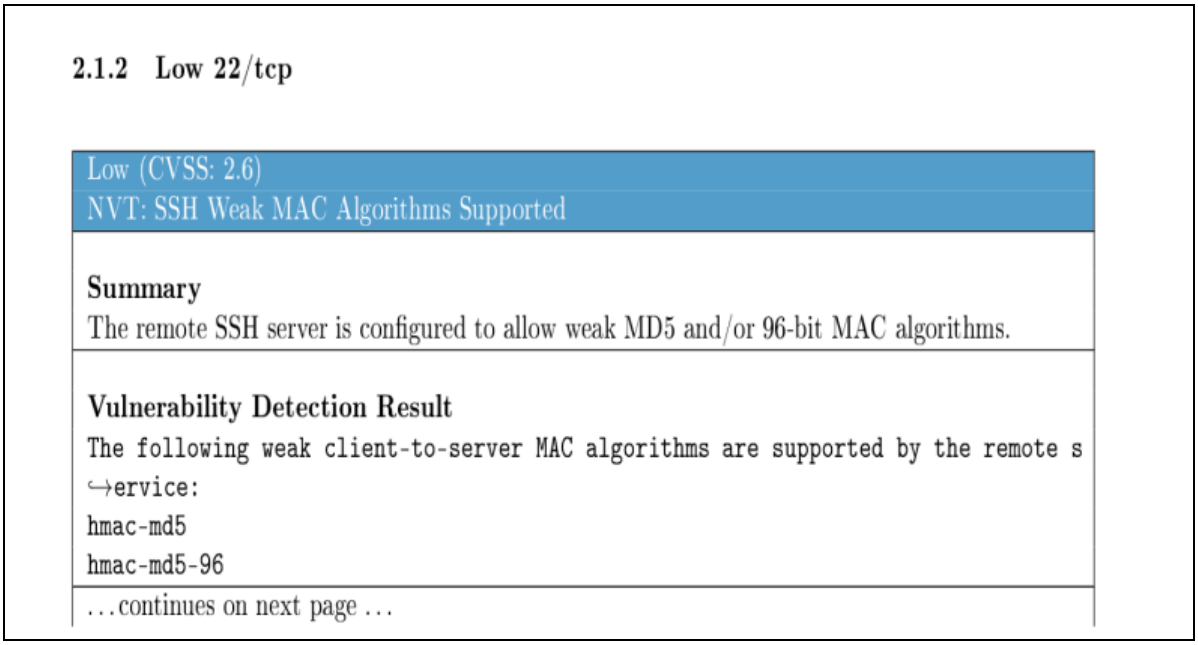
Figura *2*-3 Análisis de Openvas



Fuente: Elaboración Propia

Una vez finalizada el escaneo del dispositivo analizado, se genera un apartado con el detalle del nivel de vulnerabilidad en la figura 2-6, el sistema Openvas da como resultado problemas con el algoritmo de direcciones MAC.

Figura *2*-4 Resultado de problemas con baja configuración con las direcciones MAC



2.1.2 Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

Summary
The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.

Vulnerability Detection Result
The following weak client-to-server MAC algorithms are supported by the remote s
↪ervice:
hmac-md5
hmac-md5-96

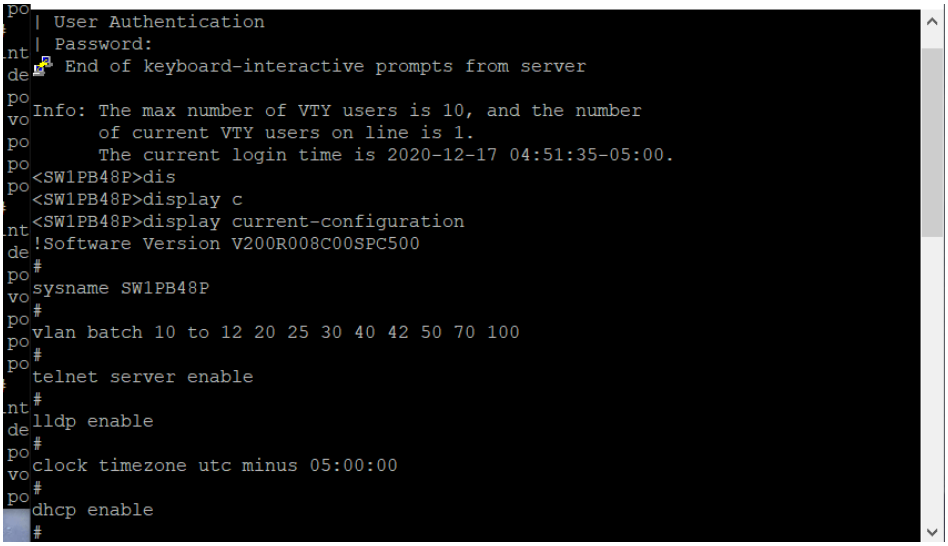
...continues on next page ...

Fuente: Elaboración Propia

2.6.1. Vulnerabilidad del ataque hombre en la mitad

El SSH es un protocolo de administración de modo remoto que le permite al administrador controlar y modificar sus servidores remotos, a través de Internet mediante un mecanismo de autenticación, que proporciona un mecanismo para autenticar un usuario remoto; también transfiere entradas desde el cliente al host y retransmite la salida de vuelta al cliente. El servicio stelnet se creó como un reemplazo para Telnet ya que no cifra su información, y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada. Se debe desactivar el protocolo telnet en los dispositivos operativos de capa dos del centro de datos de la institución, así también configurar el protocolo SSH.

Figura *2*-5 Estructura para un ataque MAC y ARP



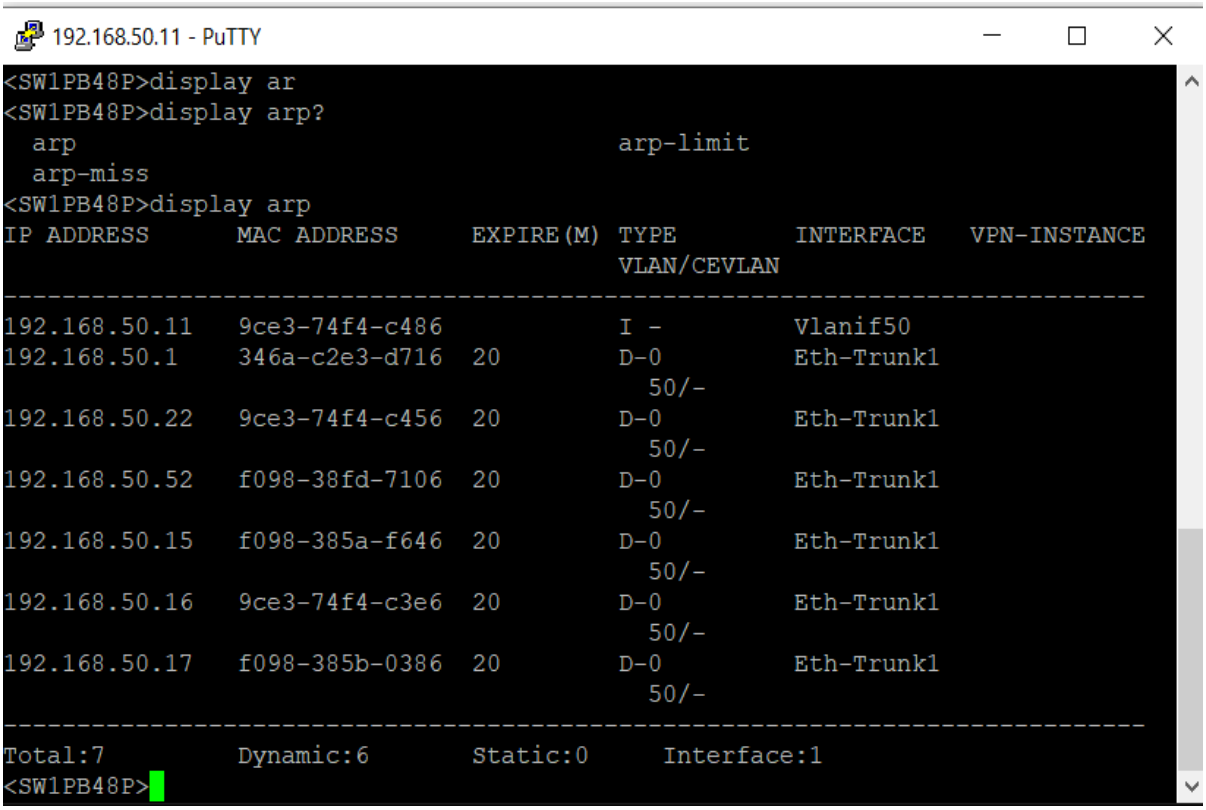
Fuente: Elaboración Propia

Se observa en la figura 2-7 la política para prevenir el ataque del hombre en la mitad, no se encuentra restringido en la red Wireless de la institución, debido a la existencia de una red WIFI-abierta, la cual, tiene acceso a las Vlan de gestión y Vlan de servidores que provocaría que algún ataque ingresaría por ese medio.

2.6.2. Vulnerabilidad de los equipos para un ataque MAC-ARP

En la figura 8-2 identifica la configuración del dispositivo marca Huawei modelo S5720-36C-PWR-EI-AC la existencia de alguna configuración que evita el ataque de ARP.

Figura *2*-6 Ausencia de configuración ante un ataque MAC



Fuente: Elaboración Propia

Al ingresar a un terminal SSH con el comando ‘‘display current-configuration ’’ en la figura 2-9 muestra la configuración general del dispositivo, como se observa no está habilitada y que están expuestas a ataques ‘’ARP esta disable.’’

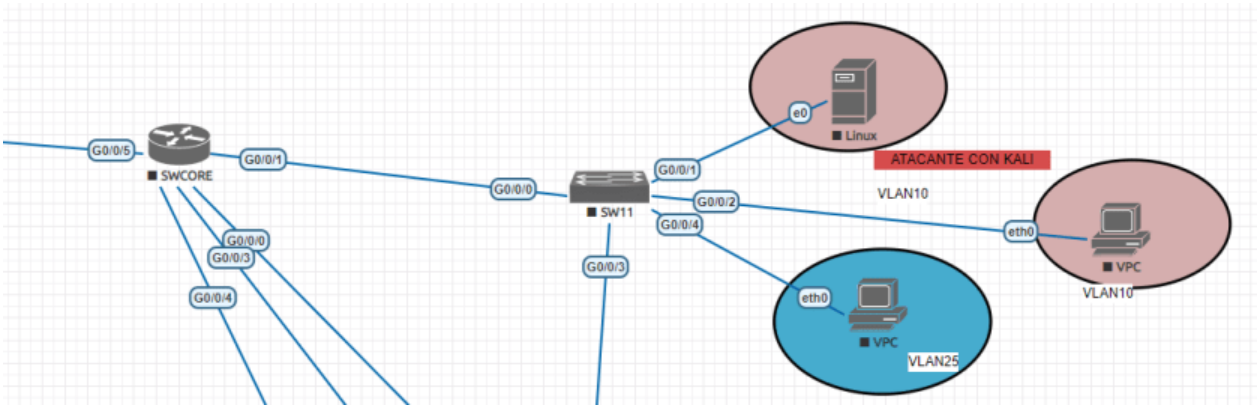
Figura *2*-7 Protocolos de protección deshabilitados

```
<SW3P228P>
<SW3P228P>display arp anti-attack configuration all
ARP anti-attack packet-check configuration:
------------------------------------------------------------------------------
Sender-MAC checking function: disable
Dst-MAC checking function: disable
IP checking function: disable
------------------------------------------------------------------------------

ARP gateway-duplicate anti-attack function: disabled

ARP anti-attack log-trap-timer: 0 second(s)
(The log and trap timer of speed-limit, default is 0 and means disabled.)

ARP anti-attack entry-check mode:
Vlanif      Mode
------------------------------------------------------------------------------
All         disabled
------------------------------------------------------------------------------

ARP rate-limit configuration:
------------------------------------------------------------------------------
Global configuration:
Interface configuration:
```

Fuente: Elaboración Propia

En la topología de la figura 2-9 muestra la manera de distribución de un equipo de capa dos utilizado para las pruebas de vulnerabilidad en la máquina con linux donde está instalado yersinia.

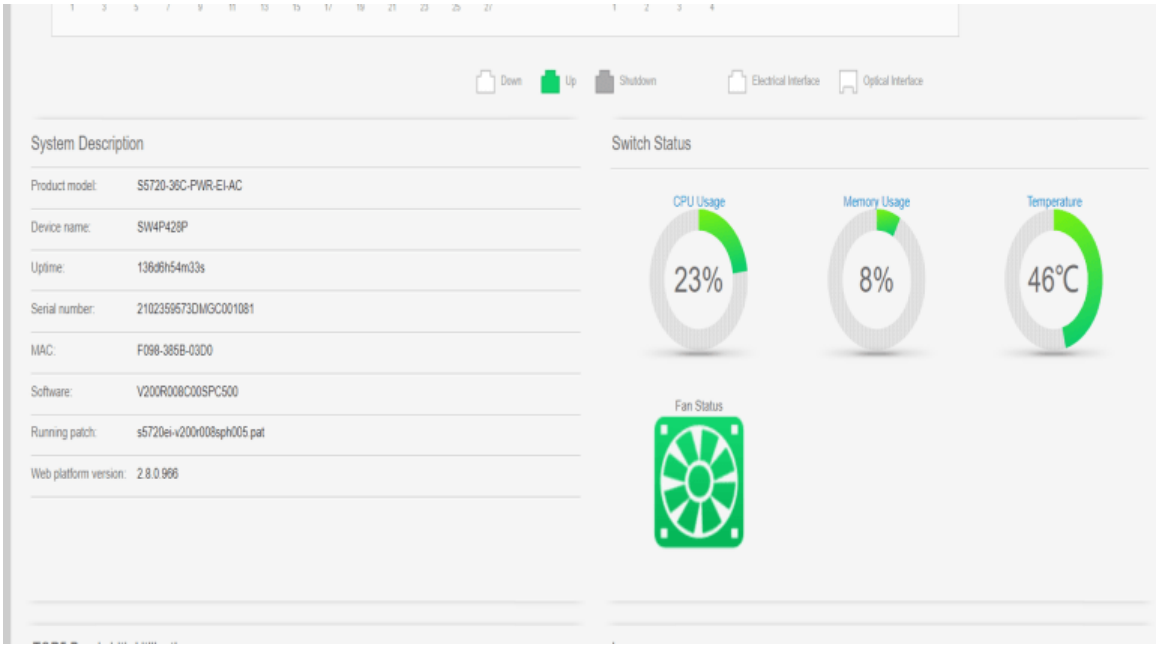
Figura *2*-8 Topología de la institución en EVE.NG al aplica yersinia



Fuente: Elaboración Propia

Se observar el estado inicial de la CPU del switch antes del ataque ARP del equipo, en la figura 2-11 evidencia el estado a condiciones normales del switch.

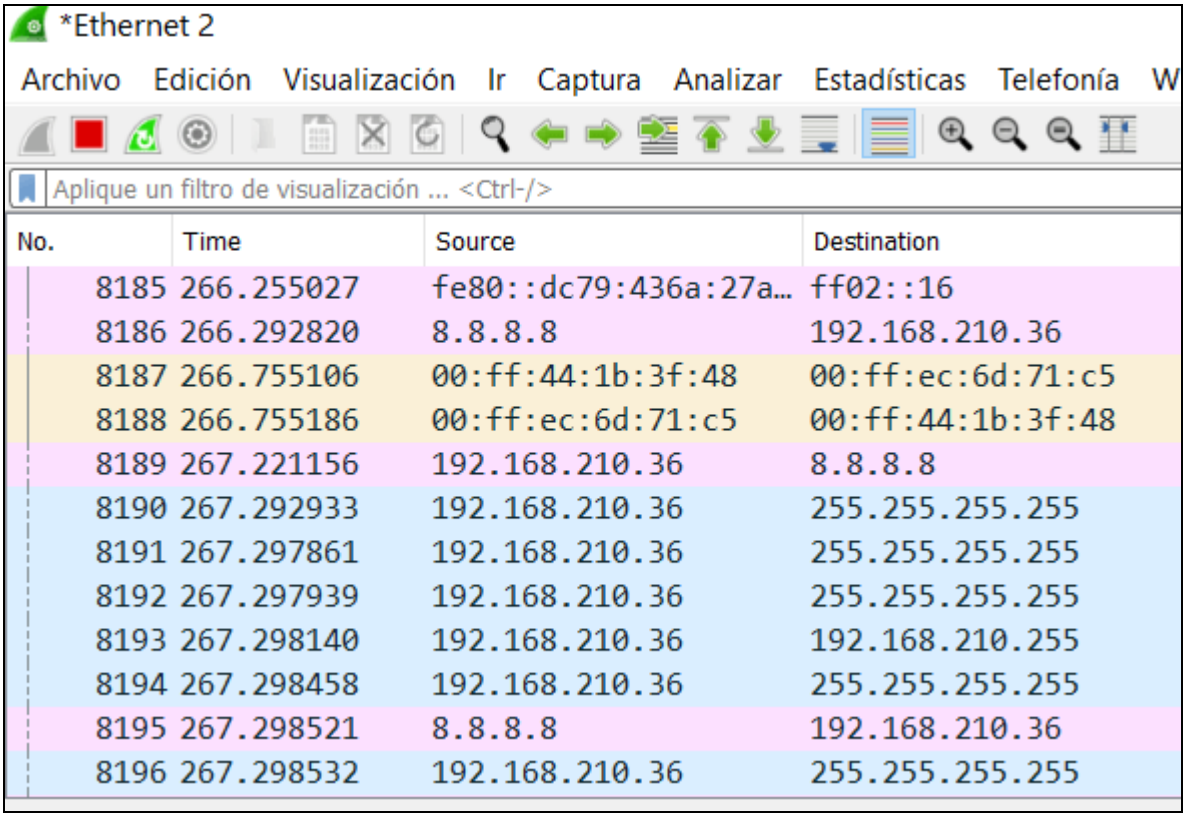
Figura *2*-9 Estado del equipo al realizar el ataque aumento de uso de CPU



Fuente: Elaboración Propia

Se utiliza la herramienta yersinia para enviar peticiones ARP e identifica las direcciones MAC Address, que en el switch son identificados, se observa en la figura 2-12 en un corto tiempo de ejecución de la herramienta.

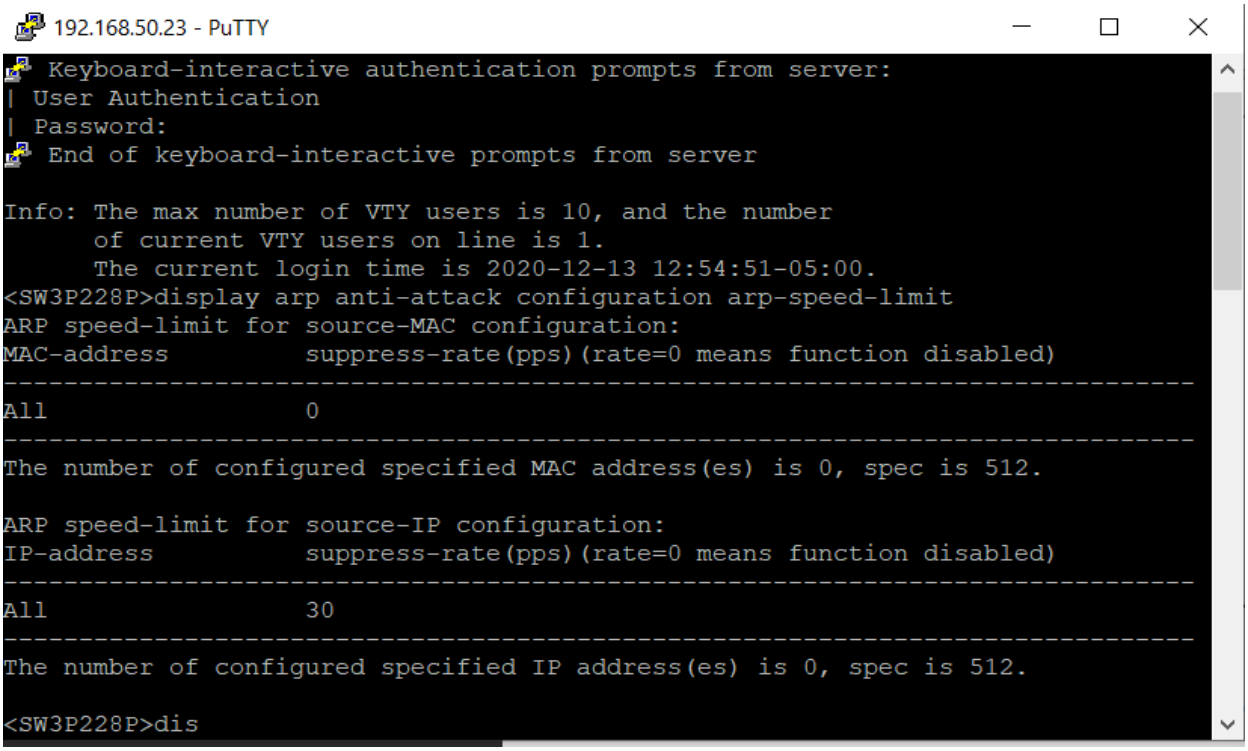
Figura *2*-10 Analisis de la au, sencia de configuración para limitar paquetes al equipo



Fuente: Elaboración Propia

Se observa en la figura 2-12 al agregar la configuración de ‘‘ARP anti-attack ’’el dispositivo evita ataques, que se relacionan con ARP y MAC Address y agrega en la configuración general para evitar la denegación de servicio.

Figura *2*-11 Broadcast del ataque en wiresharck

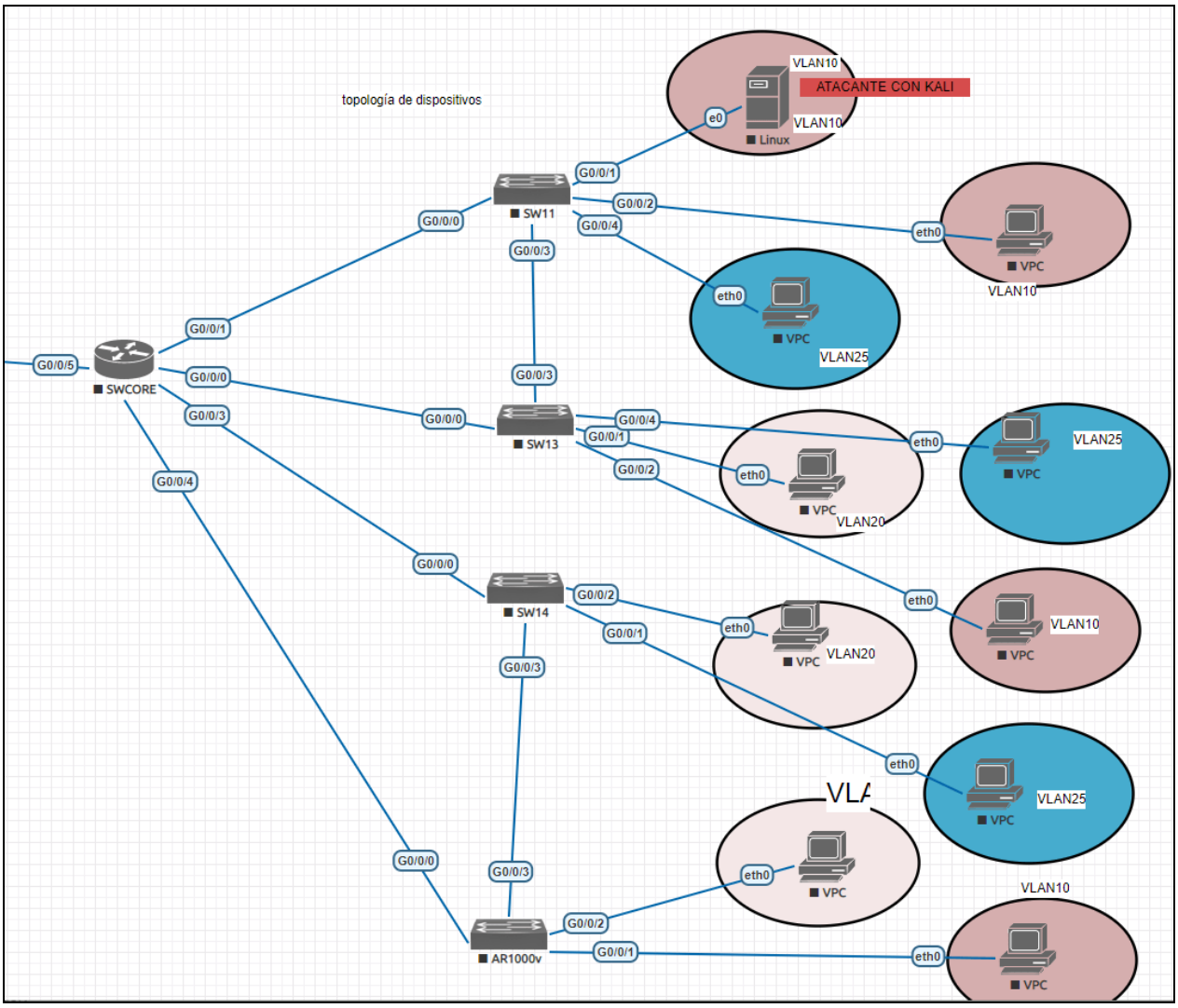


Fuente: Elaboración Propia

2.6.3. Vulnerabilidad del ataque STP

Para el desarrollo de esta vulnerabilidad utilizo el emulador EVE-NG, se observa en la figura 2-14. Puesto que en la topología real de la infraestructura existe pocos enlaces redundantes hacia otros equipos.

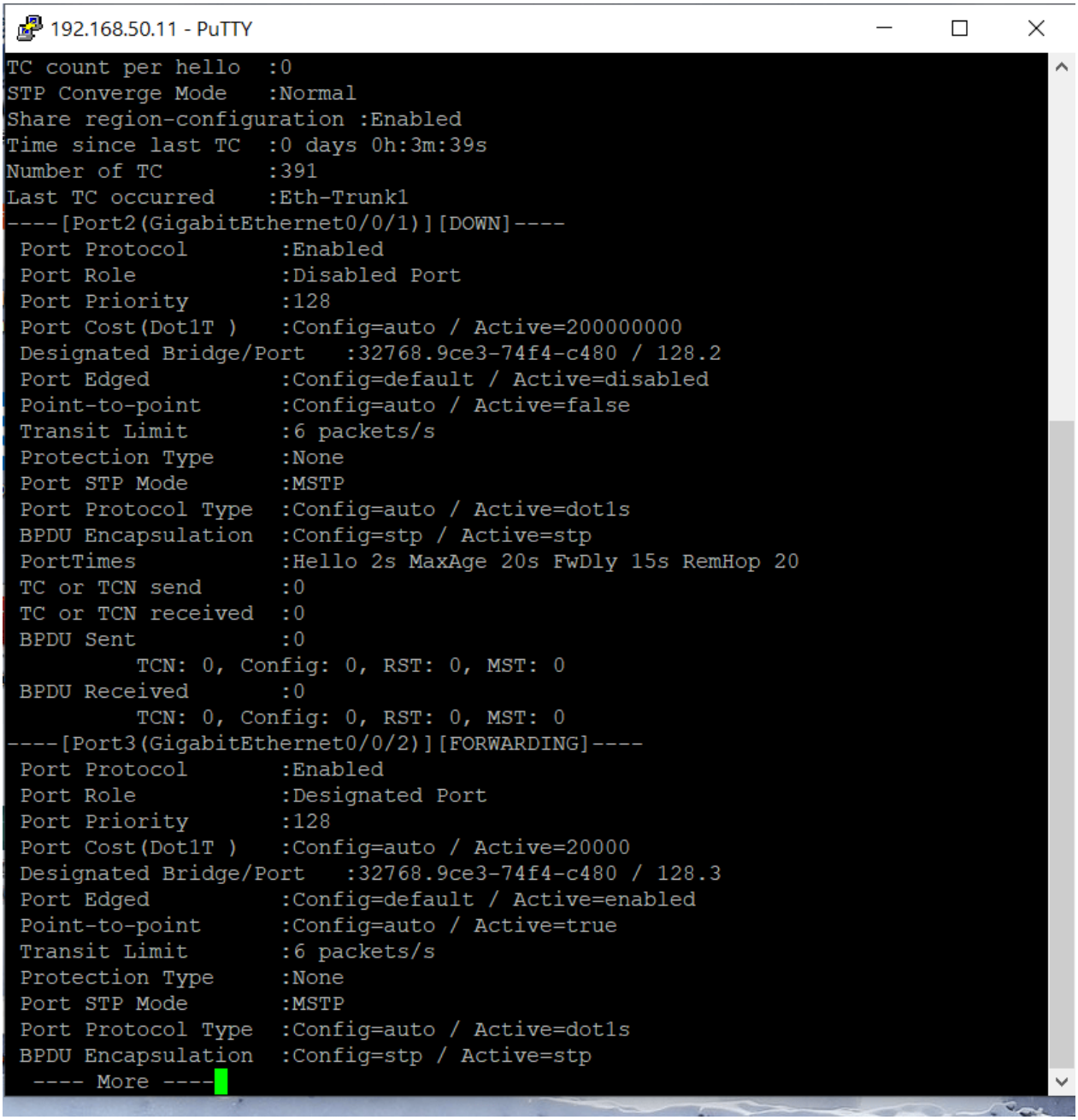
Figura 2-12 Topología en Eve-Ng



Fuente: Elaboración Propia

Al ejecutar el comando ‘‘Display current’’en la interfaz del switch 11 en la figura 2-14 de la configuración, se observa en el cliente, que no existe configuración de acorde a la protección del protocolo STP.

Figura 2-13 Ausencia de configuraciones de protección ante bucles

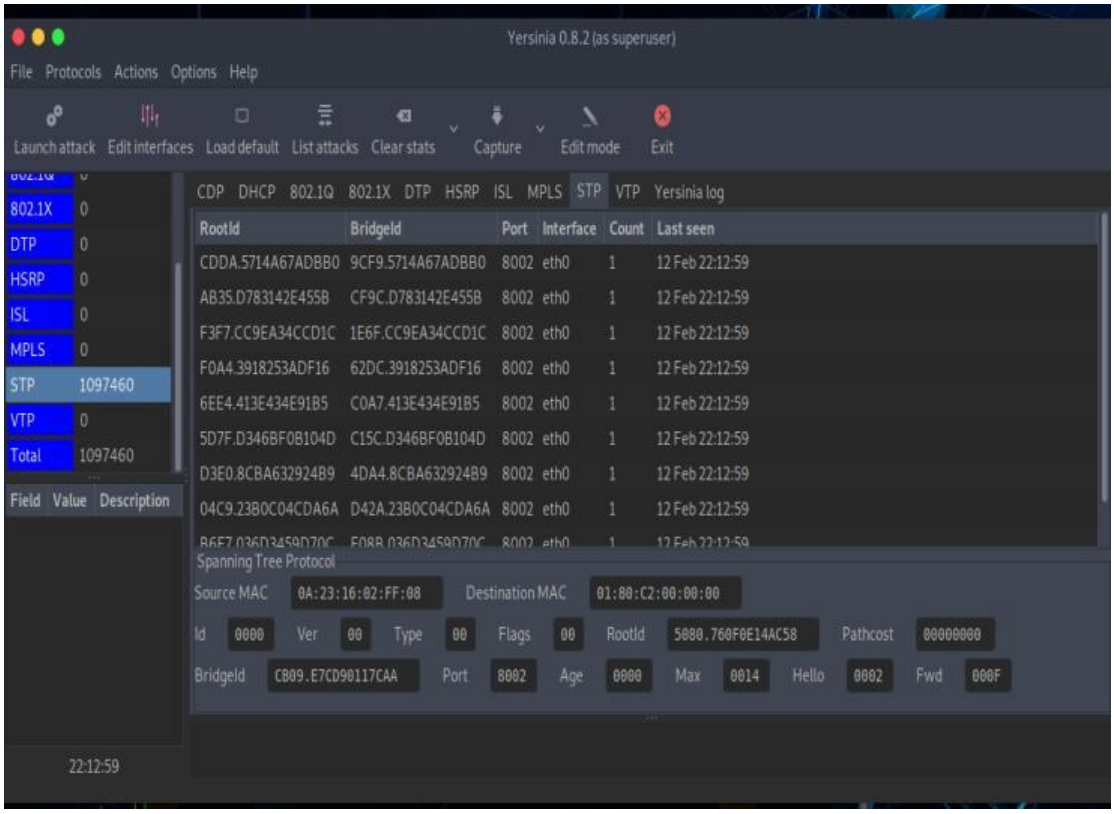


Fuente: Elaboración Propia

Se observa en la figura 2-15 la ausencia de alguna configuración en los equipos que proteja y mitigue ataques relacionados con el STP. Al hacer uso de la herramienta yersinia en la figura 13-2, montado sobre un sistema operativo

PARROT, que se envió tramas STP que provoca un aumento de consumo de recursos del equipo.

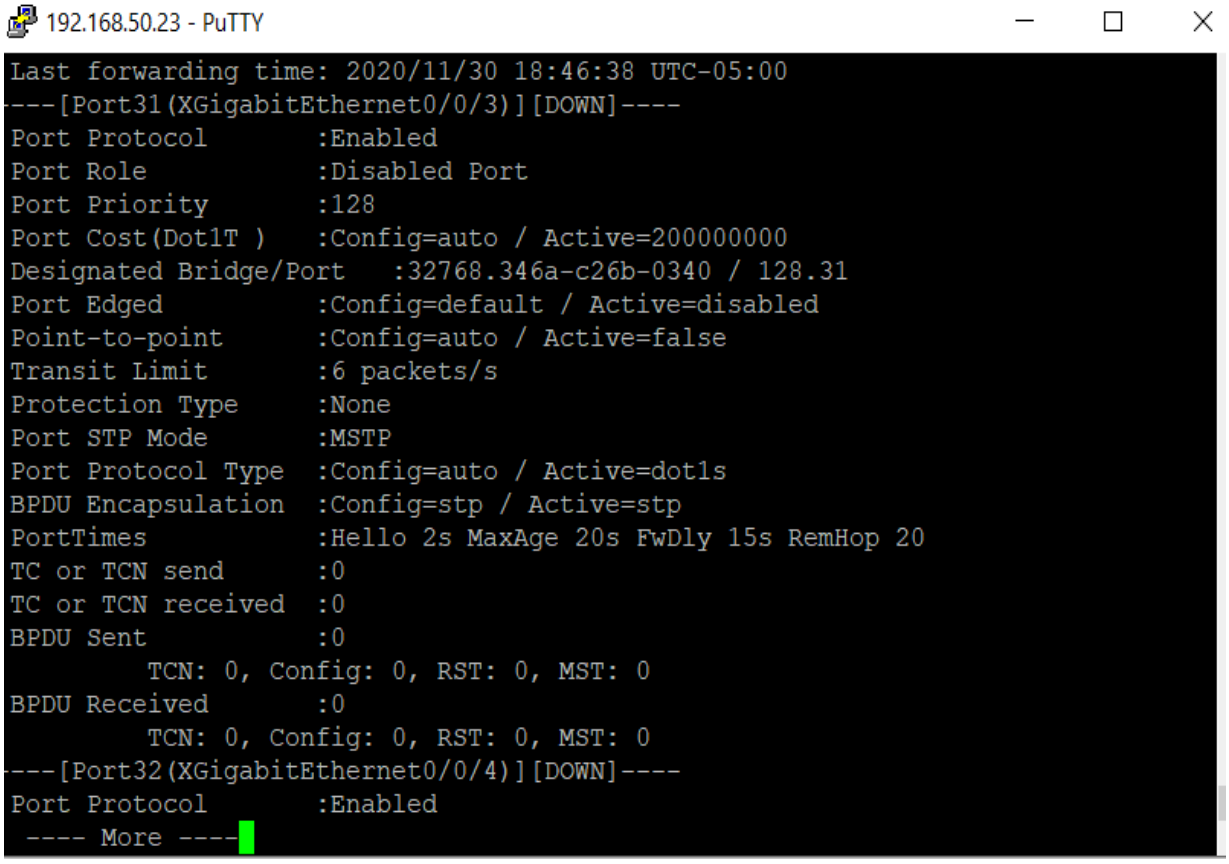
Figura *2*-14 Se inicia al escoger el tipo de ataque



Fuente: Elaboración Propia

Observa una alteración en la figura 2-16 y al ejecutar el comando ‘‘display current’’ configuración indica que ha realizado en un ambiente aislado y controlado en el equipo real.

Figura *2*-15 Protocolos de protección deshabilitados

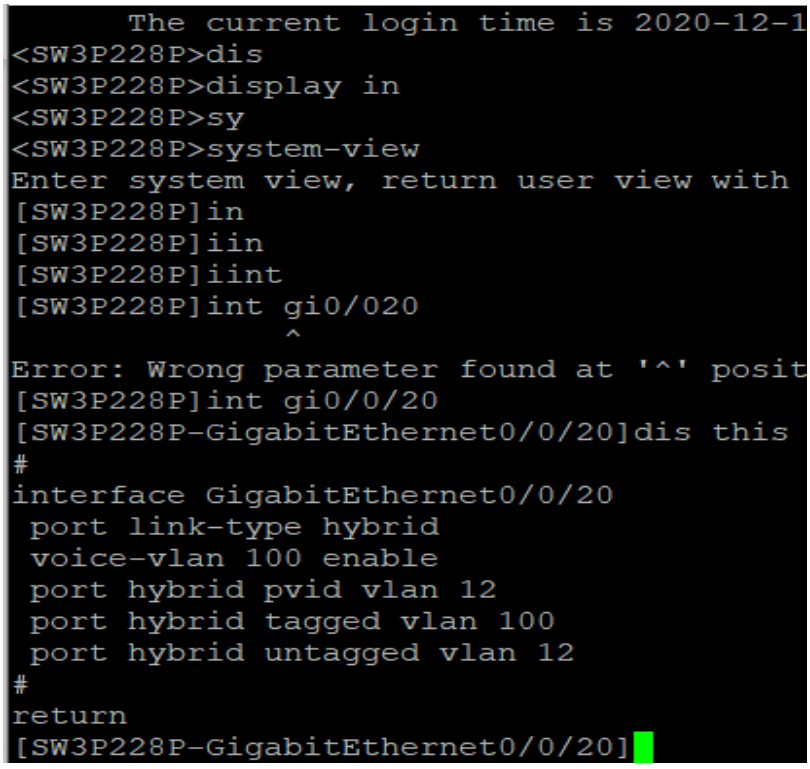


Fuente: Elaboración Propia

2.6.4. Vulnerabilidad del ataque DHCP STARVATION

Se envía muchas solicitudes DHCP con diferentes direcciones MAC hasta usar todas las direcciones IP disponibles en un rango, lo que provoca una denegación de servicio y los dispositivos legítimos no obtendrían direcciones IP, se observa el equipo está vulnerable a este tipo de ataques en la figura 2-18.

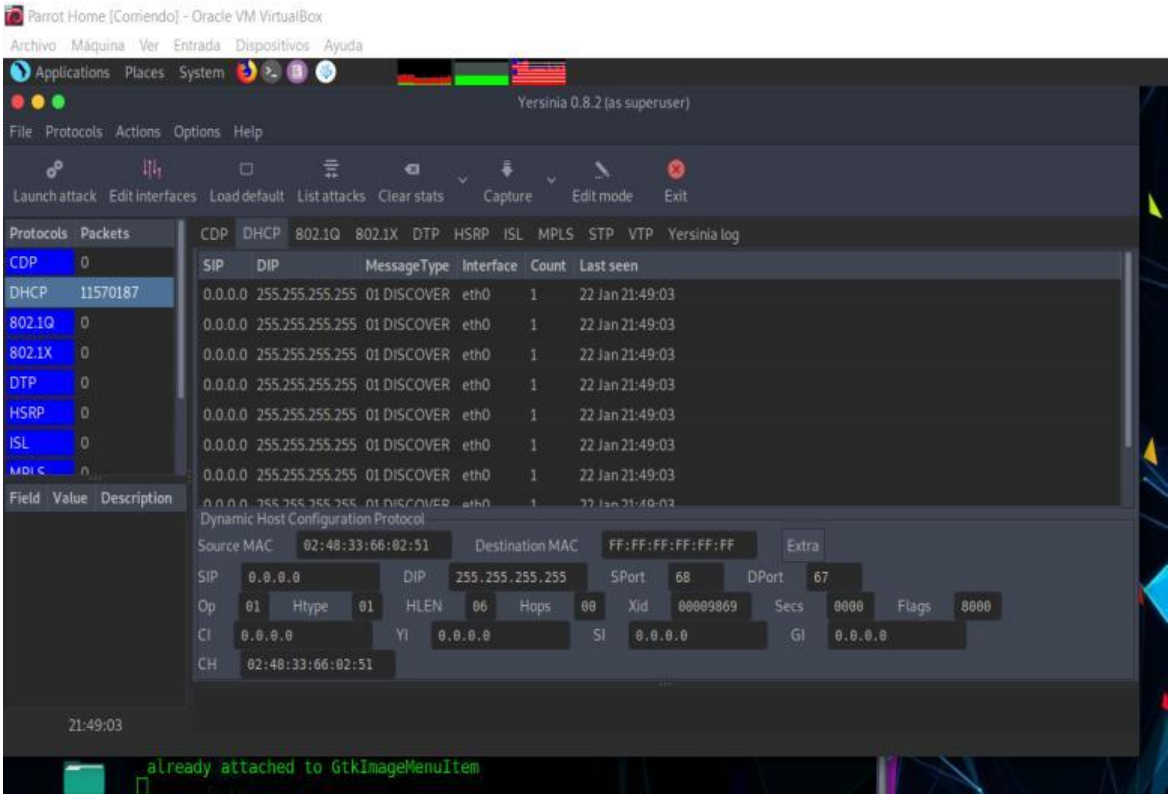
Figura *2*-16 Ausencia de configuración para proteger al equipo de un ataque STP



Fuente: Elaboración Propia

Se observa ninguna seguridad implementada para evitar el ataque DHCP starvation y se evidencia en la figura 2-18, porque la herramienta yersinia esta enviado información.

Figura *2*-17 Ataque hacia el equipo

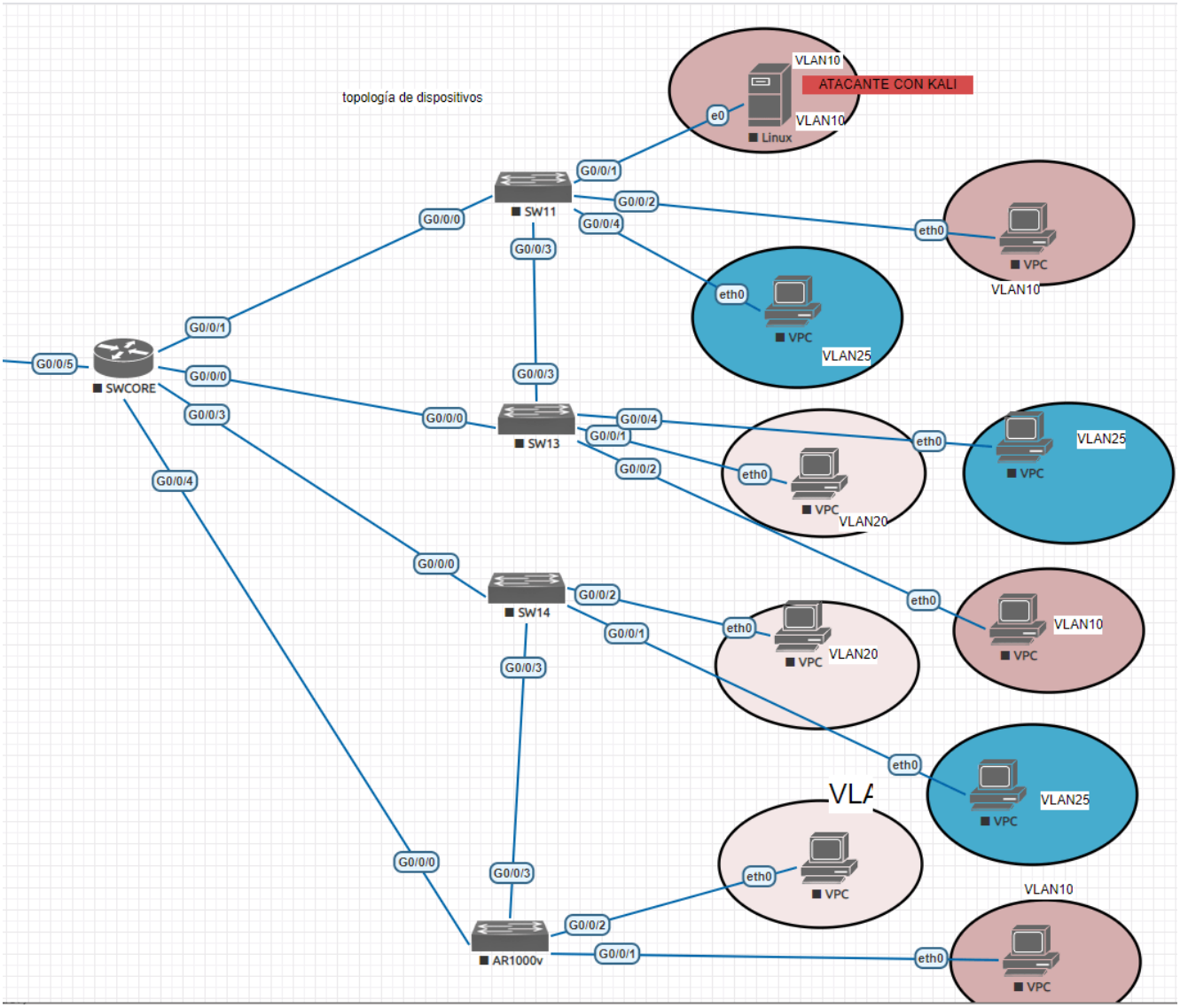


Fuente: Elaboración Propia

2.6.5. Vulnerabilidad del ataque DHCP DISCOVERY

En la marca Huawei es LNP o LLDP y consiste en inundar de mensajes DISCOVERY hacia los dispositivos de red que provoca una Denegación del servicio (DoS). Se observa en la topología de la figura 2-19. YERSINIA es la herramienta para realizar este tipo de ataques.

Figura *2*-18 Bucles de la topología de la institución en el emulador EVE-NG



Fuente: Elaboración Propia

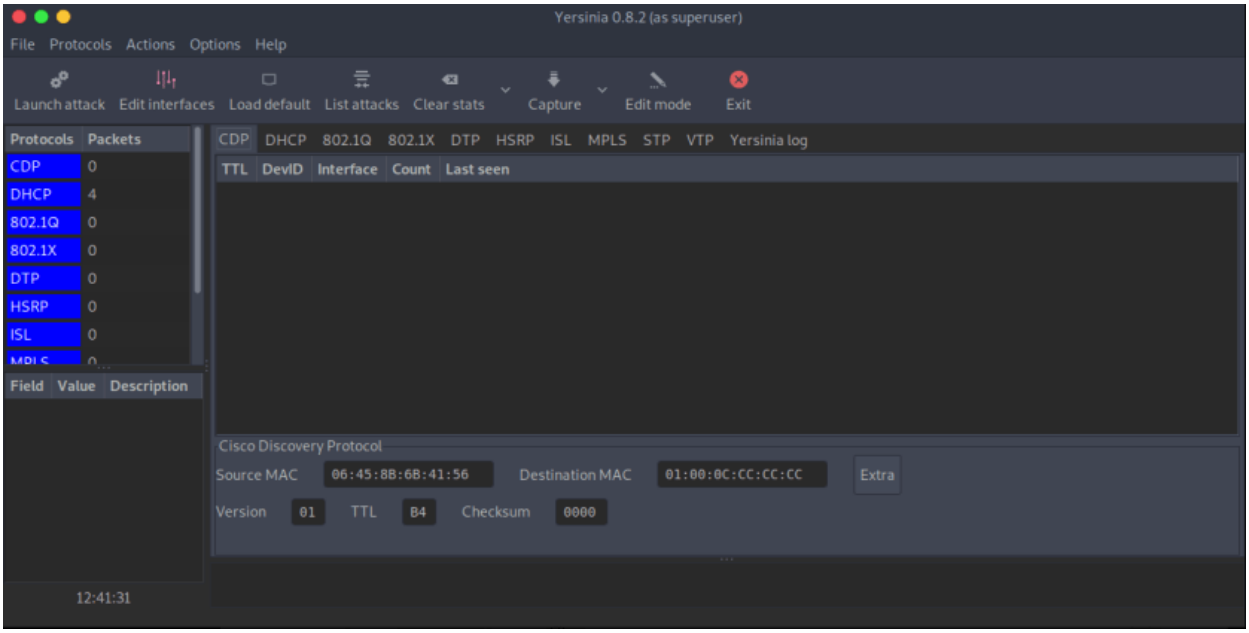
Se observa en la figura 2-20 el protocolo LLDP esta activado, sin embargo, hay que agregar políticas mediante ACL en las interfaces de cada dispositivo.

Figura *2*-19 Configuración del protocolo LLDP

Fuente: Elaboración Propia

En la figura 2-21 muestra la explotación de la vulnerabilidad con la herramienta yersinia, la cual, envía tramas de LLDP para cambiar el switch principal incluso cambiar la prioridad.

Figura *2*-20 Protocolo el ataque LLDP

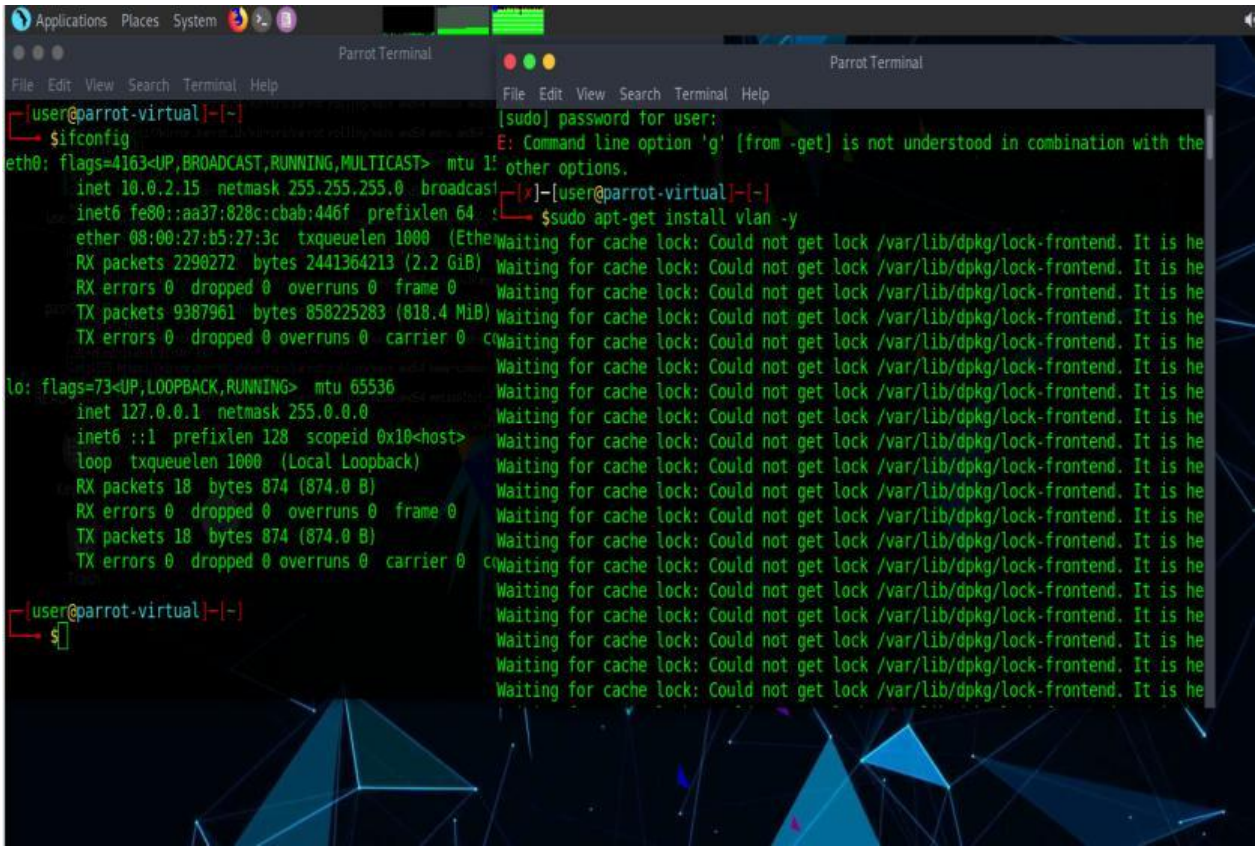


Fuente: Elaboración Propia

2.6.6. Vulnerabilidad del ataque Vlan Hopping

El atacante conecta un cable en un puerto del switch no autorizado, mismo que está configurado de manera predeterminada como Dynamic Desirable.

Figura *2*-21 El atacante está en una Vlan



Fuente: elaboración propia

La capacidad dentro del switch determina automáticamente sus conexiones por puerto individual figura 2-23, se trata de un puerto de acceso, conecta un dispositivo de usuario final y caso contrario es una interfaz troncal, que se configura automáticamente y produciría el ataque (Baxevanos, 2014).

2.7. Identificación de Vulnerabilidades

En esta fase determinó las vulnerabilidades de los dispositivos de capa dos, los huecos de seguridad que un atacante como usuario con privilegios y permisos aprovecharan para tener acceso sin autorización a la red, y que esto posible por las potenciales vulnerabilidades tecnológicas causadas debido a una escasa configuración. Esto evidenció tras una revisión directa de la infraestructura de red existente.

La tabla 1-3 muestra las amenazas para identificar otras vulnerabilidades en la red, es el usuario interno la principal amenaza para ingresar a la infraestructura de red, por la incorrecta asignación de límites y permisos que tienen dentro de la organización.

Tabla 2-4: Resumen de los ataques a la capa de enlace**.**

Ataque principal	Funcionamiento	Ataque derivado
Ataque hombre en la mitad	Si la manera de ingresar al equipo es por telnet y que una persona interceptaría información, que afecte de alguna manera con usuarios y contra, señas.	Ataque mitm
Ataque ARP y MAC	El switch empieza a comportarse como un hub debido a que la tabla CAM se llena y no se aceptan nuevas entradas y cuando la tabla CAM no almacena más asociaciones MAC-Puerto el switch empieza a enviar por todos los puertos de que dispone (Broadcast) las tramas que tengan una dirección MAC destino no almacenada en la tabla CAM	Ataque CAM table overflow Ataque ARP spoofing
Ataque STP	Un delincuente de la red envía mensajes BPDU que fuerza recálculos STP para así lograr escalar privilegios de root y esto trae como con, secuencia que, es root ob, serva la información en las tramas que no le corresponde.	Ataque STP
Ataque DHCP starvation	Consiste en inundar con peticiones DHCP_REQUEST al servidor DHCP, con direcciones MAC modificadas y con el objetivo de agotar su espacio de direcciones asignables con el fin de que el servidor DHCP no sea capaz de responder a otros hots y así realizar otro tipo de ataques (DHCP rogue)	Ataque DHCP starvation
Ataque vlan hooping	Los switches implementan Vlan, los usuarios conectan a puertos de acceso que son miembros. Vlan HOPPING es si un usuario gana acceso a una Vlan no asignada al puerto del switch, donde el usuario conecta.	Ataque switch spoofing, Ataque a vlans–double tagging

Fuente: Elaboración Propia

2.8. Fase III Plan de Acción

La norma **ISO 27032** presenta las buenas prácticas de ciber, seguridad, permite que estas fueran implementadas en los diferentes hospitales de la coordinación zonal 3 de salud, dado que el objetivo es generar lineamientos para la protección de los dispositivos de la capa de enlace. Con lo expuesto y con el resultado del diagnóstico, que se genera mediante el entendimiento de la institución, mencionado en la fase I, la organización conocería e identificar los puntos clave, en los cuales, está más débil de tal manera los fortalece, con las buenas prácticas de la ISO27032, mediante la implementación de controles.

Ya en este punto realiza las configuraciones adicionales a los dispositivos de capa dos y utiliza las herramientas de emulación EVE-NG, YERSINIA, DSNIFF que permite ver el comportamiento al ponerlos en ejecución.

2.8.1. Política para proteger ataque del hombre en la mitad

a) Utilizar los protocolos SSHV2/STELNET para ingresar a la configuración de los dispositivos marca Huawei.
b) Agregar un ACL para restringir a que Vlan acceda a la Vlan dedicada a la gestión.

En la figura 24-2 muestra la configuración agregada del protocolo Stelnet que en el apartado de la fase dos, muestra únicamente el uso del protocolo telnet.

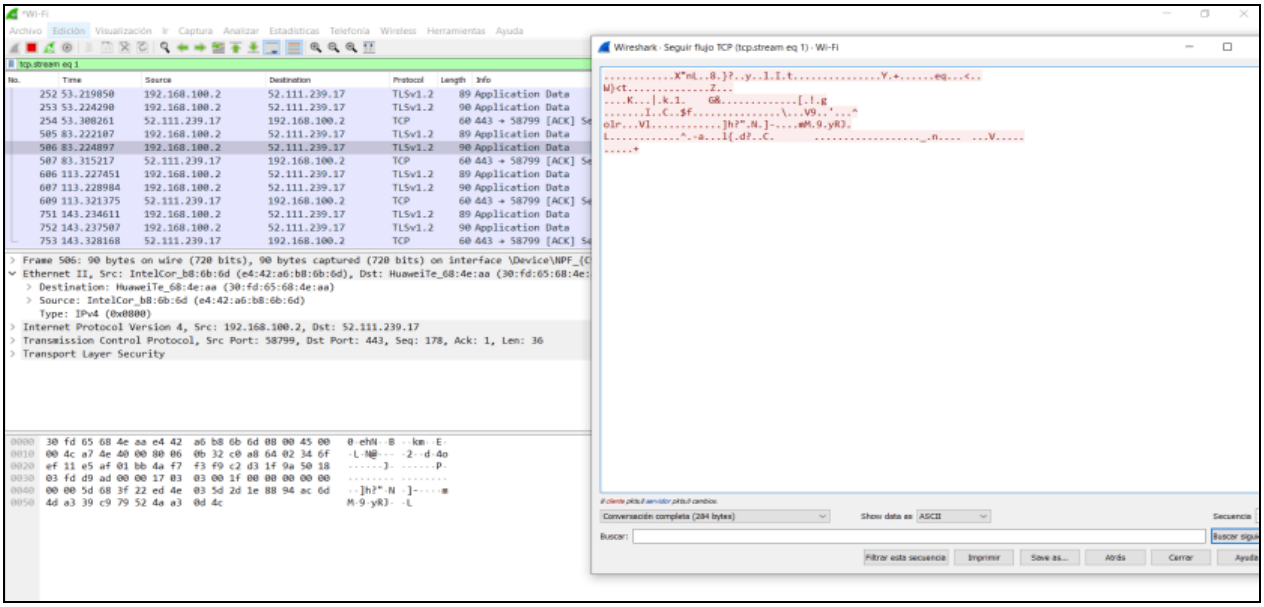
Figura *2*-22 Protocolos de protección

```
stelnet server enable
ssh authentication-type default password
ssh user huawei
ssh user huawei authentication-type password
ssh user huawei service-type all
ssh client first-time enable
ssh client 192.168.50.1 assign rsa-key 192.168.50.1
#
user-interface con 0
 authentication-mode password
 set authentication password cipher $1a$)Y5W8i9#x3$)sx4AI`#P%"qAy8BSr.3D6!!LY^F
:/-E\.Ud8g($
user-interface vty 0 4
 authentication-mode aaa
user-interface vty 16 20
#
```

Fuente: Elaboración Propia

Al realizar un analizar de tráfico con la herramienta wireshark, se observa en la figura 2-24, los datos están es encriptados lo que permite asegurar que no se observe las configuraciones, que se hagan en el equipo en modo configuración.

Figura *2*-23 Resultado en el wireshark



Fuente: Elaboración Propia

2.8.2. Política para proteger ataques ARP y MAC

Ausencia de controles en las interfaces finales de los usuarios como son:

- Limitar en cada interfaz de la cantidad de direcciones MAC que se pueden aprender para que en el momento que se alcance la cantidad máximo de direcciones Mac se descarten los paquetes de direcciones no conocidas.
- Limitar la tasa de paquetes ARP según las direcciones MAC de origen y las direcciones IP de origen.
- Asignar estática de direcciones MAC en los puertos para que solo paquetes de ciertas MAC sean procesados.

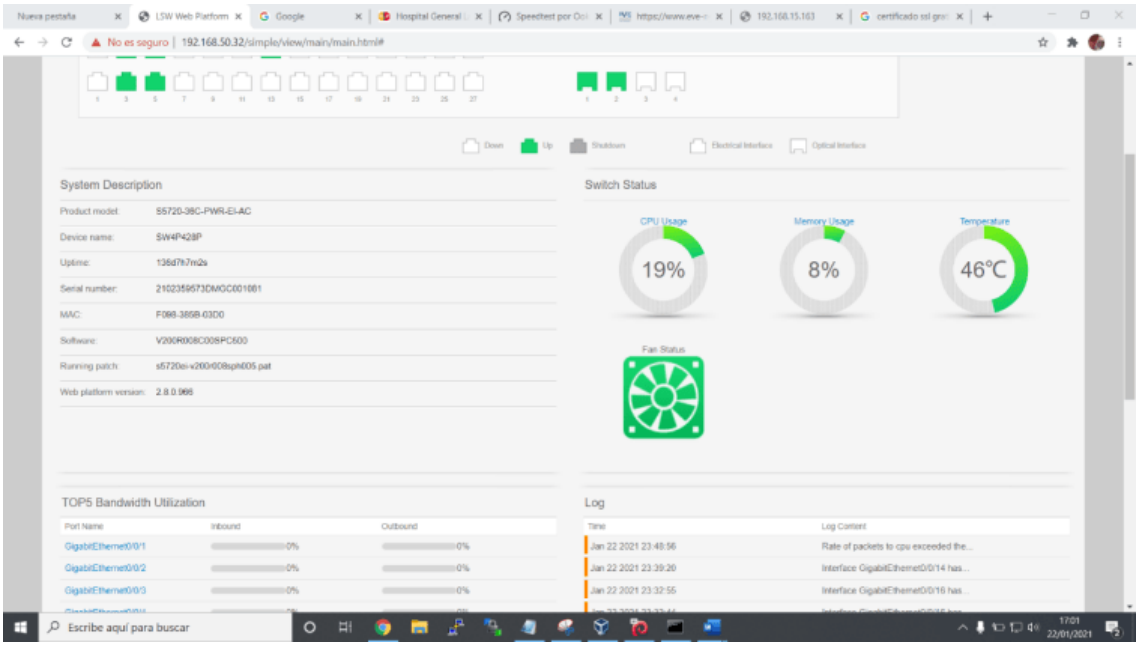
- El aprendizaje de direcciones MAC persistentes, al conectar un dispositivo a un puerto, este aprenda la MAC del mismo y no acepte la conexión de ningún otro dispositivo.

Habilitar las funciones de registro y alarma para posibles ataques en los dispositivos de pruebas como son:

- Limitar la interfaz para evitar acceso a un gran número de paquetes broadcast, unicast o multicast.
- Interfaces sin uso estan en modo apagado (shutdown).
- Interfaces que no estén es utilizadas así estar en ‘‘modo Access’’ y evidencia que están sin ninguna línea de configuración.
- Habilitar la detección de violaciones de seguridad en el caso que produzcan, se apague el puerto.

Una vez realizado la configuración a la interfaz, se evidencia en la figura 24-2 que la CPU del dispositivo no aumenta el rendimiento del CPU ante el ataque.

Figura *2*-24 Análisis del resultado en el wireshark



Fuente: Elaboración Propia

Políticas para proteger de un ataque STP

Para proteger al equipo de posibles ataques, en la figura 25-2 considera las siguientes acciones analizada en la fase dos de análisis de riesgos en los equipos, se consideró realizar las siguientes acciones:

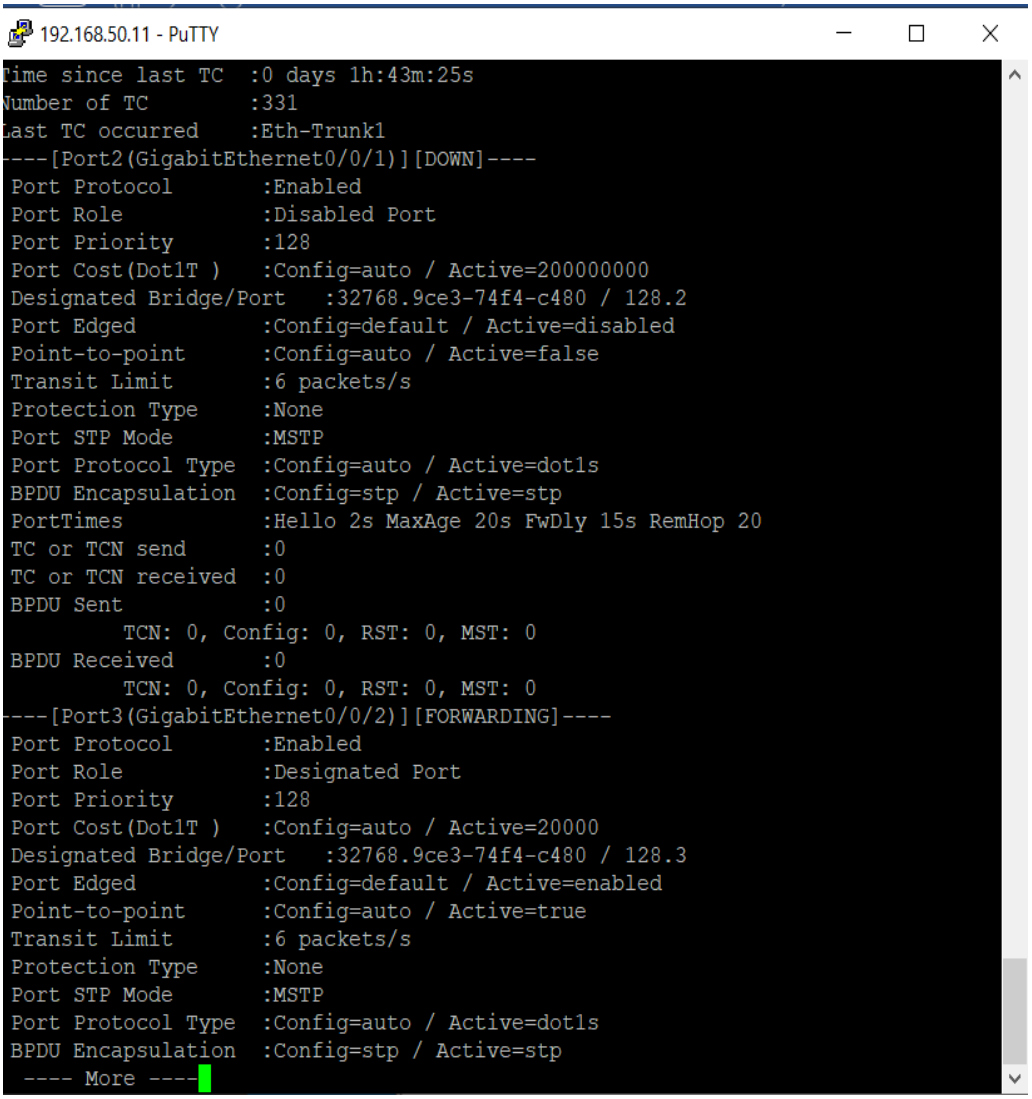
No deshabilitar el proceso STP.

Habilitar la protección para paquetes BPDU en un dispositivo de conmutación.

Habilitar la configuración de protección de cambio de topología.

Habilitar la protección de root primario en la interfaz donde exista redundancia en el lazo.

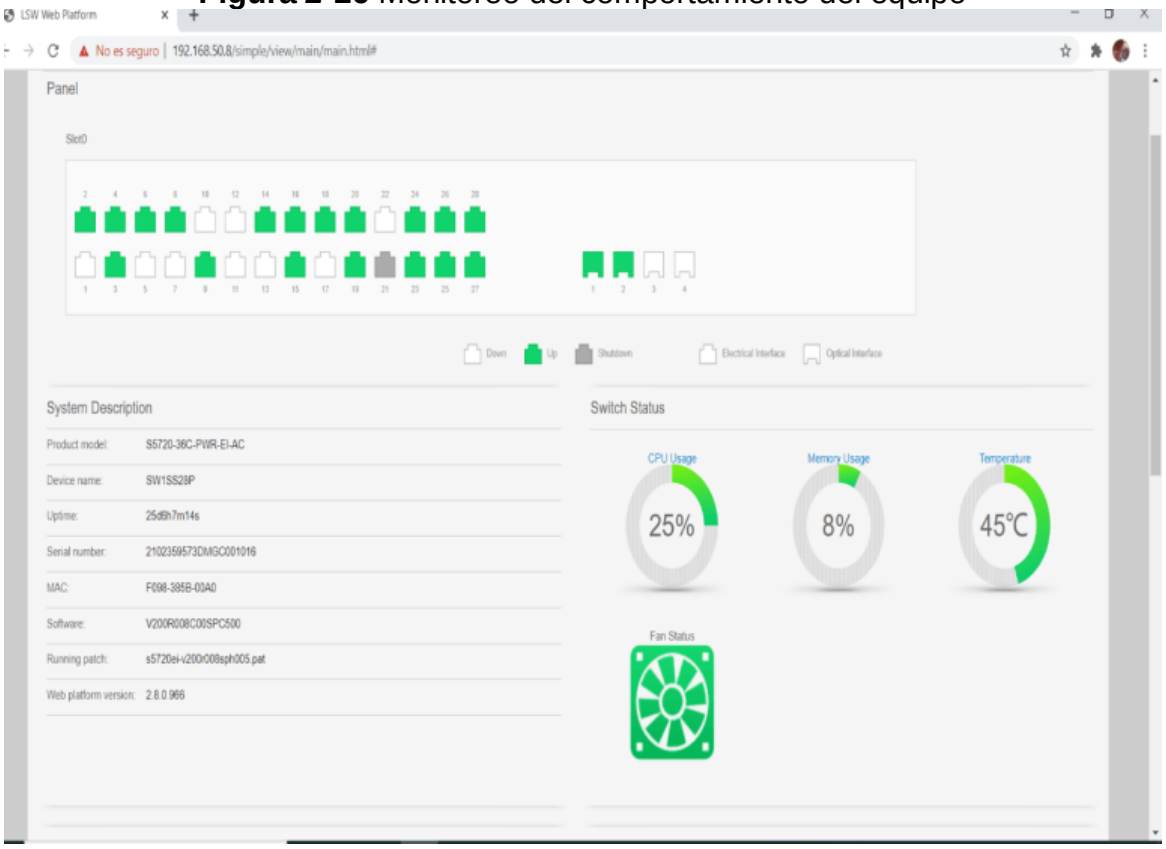
Figura 2-25 Habilita los protocolos de protección



Fuente: Elaboración Propia

Una vez realizado la configuración a la interfaz, se evidencia en la figura 26-2 que la CPU del dispositivo no aumenta a comparación inicial del ataque.

Figura *2*-26 Monitoreo del comportamiento del equipo



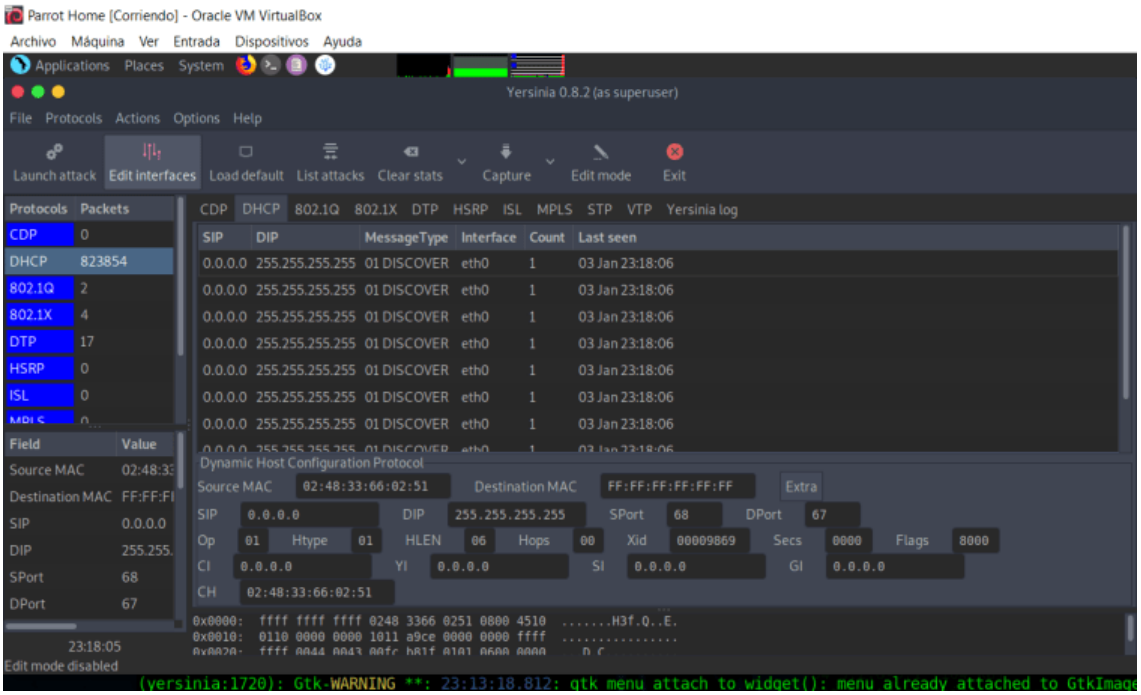
Fuente: Elaboración Propia

2.8.3. Política para proteger de ataques DHCP starvation

En el caso de posibles ataques de DHCP agregar las siguientes configuraciones:
Configurar las interfaces para la detección de paquetes de solicitud DHCP para proteger, se contra ataques de agotamiento de DHCP.

Configurar la detección de direcciones MAC para proteger, se contra ataques DHCP DoS.

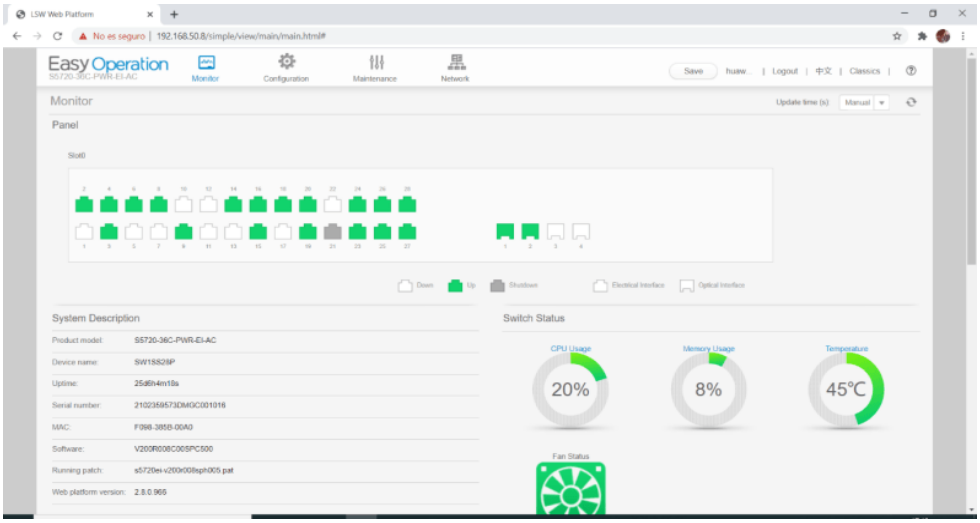
Figura *2*-27 Analiza el resultado en la interfaz de yersinia



Fuente: Elaboración Propia

Una vez implementado la configuración adicional y la comprobación, se visualiza en la figura 2-29 el comportamiento de la CPU del equipo.

Figura *2*-28 Analiza el estado del CPU del equipo



Fuente: Elaboración Propia

Se observa en la figura 2-28 al realizar el ataque el comportamiento de la CPU del switch no afectado.

2.8.4. Política para proteger de ataques Vlan

Se agrega las siguientes configuraciones para mitigar el ataque:
Desactivar el auto trunking por defecto, se activa las interfaces en modo Access.
Deshabilitar las interfaces que no estén es utilizado.
No utilizar la Vlan nativa.

2.9. Fase IV Implementación

Una vez identificadas las vulnerabilidades existentes en los equipos de capa dos del centro de datos, se detalla en la tabla resumen 2-2 realiza la encuesta de conocimientos con problemas relacionados con vulnerabilidades de la capa de enlace al personal de TI quienes administran la red y la protegen de ataques relacionados con los mismas, también, las consecuencias que resultaría como un ataque DdoS.
Se realiza la encuentra a tres personas del área de tecnologías de la información de la institución quienes son responsables de la gestión de la infraestructura especialmente a los dispositivos de capa dos, se muestra en la tabla 2-4.

Tabla 2-4: Encuesta de reconocimiento de ciber seguridad al personal de TI de la institución**.**

Descripción	Analista de tecnologías de información		Analista de soporte técnico		Analista de soporte técnico	
	SI	NO	SI	NO	SI	NO
La infraestructura posee switchs administrables	X			X		x
Conoce de ciberataques de DoS.		X		X		X
Conoce de ataques existentes a nivel de capa de enlace.		X		X		X
Conoce métodos de protección para ataque del hombre en la mitad		X		X		X
Conoce métodos de protección para ataques a nivel de MAC-ADDRES		X		X		X
Conoce de métodos de protección de ataques ARP		X		X		X
Conoce de métodos de protección de ataque producidos por los bucles por el protocolo STP		X		X		X
Conoce de métodos de protección de ataque de vlan hopping		X		X		X

Fuente: elaboración propia

Al continuar de realizar el análisis de vulnerabilidades en los dispositivos de capa dos, en el escenario de estudio, se determina que disminuirían las vulnerabilidades al agregar configuraciones puesto que no vienen habilitadas por defecto en los switchs a nivel global de los equipos y a nivel de interfaz.

2.9.1. Ataque del hombre en la mitad

Tabla 2-5: Política de ciber seguridad para un ataque MITM**.**

Política	Configuración actual	Configuraciones implementadas
Utilizar los protocolos SSH/stelnet para ingresar a la configuración del switch de capa dos de la marca huawei ACL para negar que vlan accadan a la vlan de	# telnet server enable # # user-interfaz con 0 authentication-mode password	# stelnet server enable ssh authentication-type default password ssh user huawei ssh user huawei

adminitración. [~SWCORE] acl 2001 [~SWCORE-acl4-basic-2006] rule permit source 192.168.10.1 32r [*SWCORE-acl4-basic-2006] quit **[*SWCORE] SSH server acl 2001** **[~SWCORE] save**	, set authentication password cipher $1a$-Zq0CXuTu~$$JR"X:EwC<&_}4>Na$rQyO{YCX$vQUQqPRSY^U^Q$ u, ser-interfaz vty 0 4 authentication-mode aaa u, ser privilege level 1 protocol inbound telnet u, ser-interfaz vty 16 20 #	authentication-type password ssh user huawei service-type all ssh client first-time enable #

Fuente: Elaboración Propia

2.9.2. Ataque MAC y ARP

Tabla 2-62: Política de ciber seguridad para ataques MAC y ARP**.**

Política	Configuración actual	Configuraciones implementadas
Au, sencia de controles en las interfaces finales de los usuarios como son: . • Limitar en cada interfaz la cantidad de direcciones MAC que puedan acceder para que se pueden aprender para que en el momento que se alcance el máximo se descarten los paquetes de direcciones no conocidas.	# interfaz GigabitEthernet0/0/27 port default vlan 14 #	Se agrega una linea de configuración a nivel global # ARP speed-limit source-ip maximum 50 # Agregar la siguinte linea de configuración a cada vlan creada en el switch # interfaz Vlanif4 ARP-limit maximum 20 # Para proteger al switch de la inundación de MACs, se agrega a cada interfaz las siguientes lineas de configuracion port-, security enable port-, security max-MAC-num 5 port-, security protect-action restrict MAC-learning priority 4 ARP anti-attack rate-limit enable ARP anti-attack rate-limit packet 51 blocktimer 70

• Limitar la tasa de los paquetes ARP según las direcciones MAC de origen y las direcciones • Asignar de manera estática las direcciones MAC en los puertos para que solo paquetes de ciertas MAC sean procesados. • Habilitar el aprendizaje de direcciones MAC, de manera que, al conectar un dispositivo a una interfaz, este aprenda la MAC del mismo y no acepte la conexión de ningún otro dispositivo. IP de origen . Habilitar las funciones de registro y alarma para posibles ataques. Limitar la interfaz para evitar acceso a un exceso número de paquetes broadccast, unnicast o multicasst. Interfaces sin uso estar modo apagado shutdown. Interfaces que no estén es utilizadas: estar en ‘‘modo access’’ Habilitar la opción de localización de violaciones de la seguridad, que en el caso que suceda cambie de estado el interfaz.		

Fuente: Elaboración Propia

2.9.3. Ataque de STP

Tabla 3-74: Política de ciber seguridad para un ataque STP**.**

Política	Configuración actual	Configuraciones implementadas
Mantener habilitado STP. Habilitar la protección BPDU en un dispositivo de conmutación. Habilitar la configuración de protección de cambio de topología. Habilitar la protección de root primario en el interfaz del lazo. Evitar bucles a, segura que el tráfico no vuelva tormenta de broadcast.	No existe protecciones para el protocolo STP	La configuración se debe realizar en configuración global # STP instance 0 root primary STP bpdu-protection STP tc-protection # Se debe agregar la configuración adicional a las interfaces de acceso para evitar que se dé una tormenta. # interfaz GigabitEthernet0/0/27 description Puerto para PC y Teléfono port link-type hybrid voice-vlan 100 enable port hybrid pvid vlan 4 port hybrid tagged vlan 100 port hybrid untagged vlan 4 storm-control broadcast min-rate 5000 max-rate 8000 storm-control action error-down storm-control enable trap STP edged-port enable #

Fuente: Elaboración Propia

2.9.4. Ataque de DHCP Starvition

Tabla 2-8: Política de ciber seguridad para un ataque DHCP STARVATION**.**

Política	Configuración actual	Configuraciones implementadas
Habilitar el comando DHCP SNOOPING que trabaja sobre diferentes tipos de ataques como: DHCP starvation Ataque DoS	No existe protecciones para proteger de esta vulnerabilidad	Paso 1 La configuración realiza en configuración global # DHCP server group DHCPgroup1 DHCP snooping check DHCP-chaddr enable # dhcp server group dhcpgroup1 dhcp snooping enable ipv4 arp dhcp-snooping-detect enable dhcp snooping check dhcp-rate enable dhcp snooping check dhcp-rate 90 dhcp snooping alarm dhcp-rate enable dhcp snooping alarm dhcp-rate threshold 500 # Se agrega la configuración adicional a las interfaces de acceso. # dhcp snooping enable dhcp snooping check dhcp-giaddr enable dhcp snooping check dhcp-request enable dhcp snooping alarm dhcp-request enable dhcp snooping alarm dhcp-

		request threshold 120 dhcp snooping max-user-number 20 DHCP snooping alarm DHCP-chaddr enable DHCP snooping alarm DHCP

Fuente: Elaboración Propia

2.9.5. Ataque de Vlan Hopping

Tabla 5-9: Política de ciber seguridad para un ataque Vlan Hopping**.**

Política	Configuración actual	Configuraciones implementadas
Desactivar el auto trunkin por defecto al activar las interfaces en modo access Deshabilitar las interfaces que no estén es utilizado No utilizar la vlan nativa .	No existe protecciones para esta vulnerabilidad debido a que la interfaz está configurada y encendida interfaz GigabitEthernet0/0/25 description Puerto para PC y Telefono port link-type hybrid voice-vlan 100 enable #	La configuración realiza en configuración global # STP instance 10 root primary STP bpdu-protection STP tc-protection # A continuación, agregar la configuración adicional a las interfaces de acceso para evitar que alguien ingre, se a la red # interfaz GigabitEthernet0/0/25 description Puerto para PC y Telefono shutdown port link-type hybrid voice-vlan 100 enable #

Fuente: Elaboración Propia

CAPÍTULO III ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Luego de realizar el análisis de vulnerabilidades a los dispositivos de capa-dos en escenario real, se determina que las vulnerabilidades descritas en el capítulo 2 tiene como finalidad el ataque de denegación de servicio DDoS de mayor a menor importancia, la más común y en la que menos, se preocupa el administrador es habilitar y deshabilitar protocolo, las demás vulnerabilidades son de igual manera problemas de configuración, que no vienen por defecto en los Switchs.

3.1. Política para el Ataque hombre en la mitad

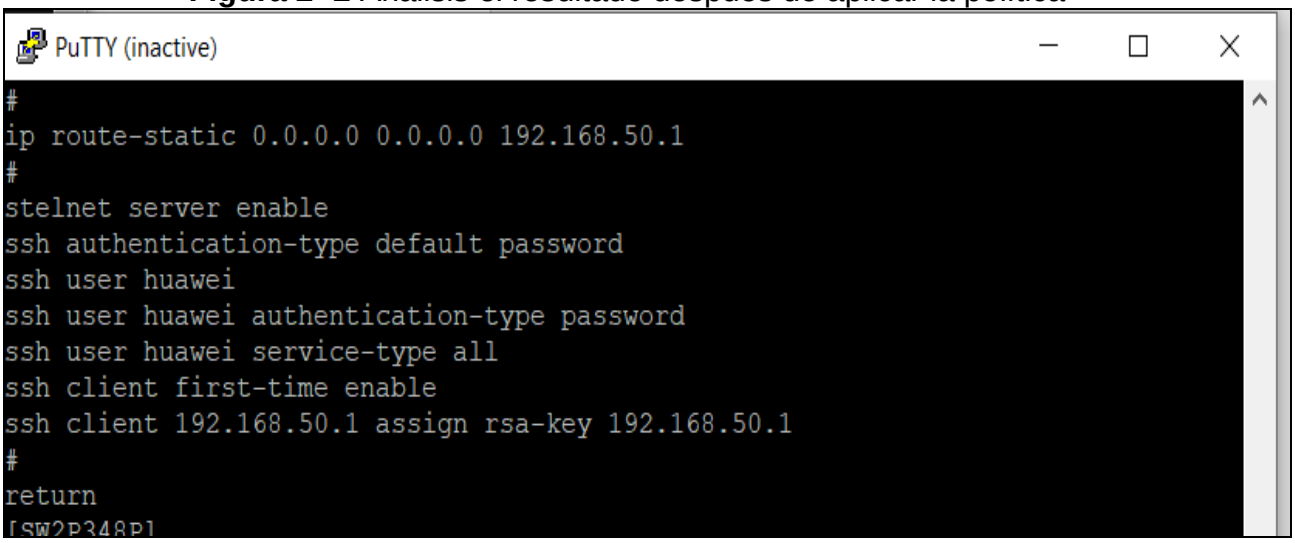
Para mitigar el riesgo de captura de información, se ha implementado el protocolo STELNET en los equipos marca Huawei. En la figura 1-3 indica la captura de la información cifrada de las políticas propuestas, tanto a nivel tecnológico como a nivel organizacional, operacional y físico para mitigar los ataques de hombre en la mitad a nivel de capa 2 presentada en la Tabla 4.

Figura 3-1 Resultado después de aplicar la política

Fuente: Elaboración Propia

En la figura 2-3, se observa el código agregado al switch de borde que permite mitigar este riesgo.

Figura 2- 2 Análisis el resultado después de aplicar la política



Fuente: Elaboración Propia

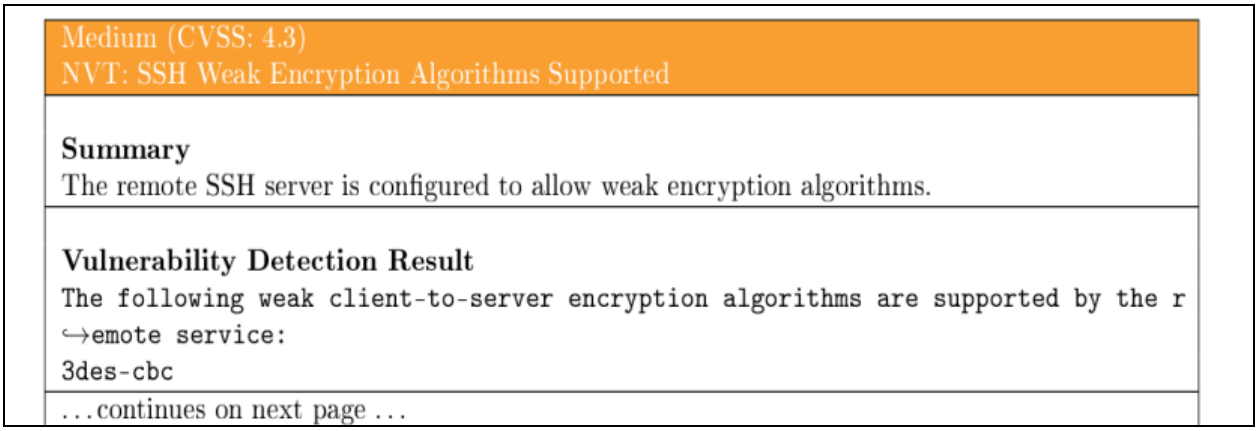
En la figura 3-3, se muestra la captura de tramas al mismo tiempo ingresa al equipo por stelnet y evidencia que la información está cifrada.

Figura 3-0 Captura de información cifrada

Fuente: Elaboración Propia

Para comprobar que la mitigación haya sido superada, se muestra el resultado en la figura 4-3 el resultado del análisis del equipo con la herramienta OPENVAS y con la implementación de las configuraciones.

Figura 3-3 Análisis el resultado después de aplicar la política



Fuente: Elaboración Propia

3.2. Política para el ataque MAC ARP

Se presentan las políticas de ciber, seguridad para los dispositivos de capa dos de la marca Huawei ante un ataque MAC ARP, que en su estado inicial carece de algún mecanismo de proteger ante un ataque y es evidencia en la figura 5-3.

Figura 3-4 Análisis el resultado después de aplicar la política

Fuente: Elaboración Propia

En la figura 6-3 muestra el código en la configuración global del switch agregado en el dispositivo de capa que permite mitigar este riesgo.

Figura 3-5 Implementación configuraciones ausentes

```
#
dhcp enable
#
dhcp snooping enable
dhcp snooping check dhcp-rate enable
dhcp snooping check dhcp-rate 90
dhcp snooping alarm dhcp-rate enable
dhcp snooping alarm dhcp-rate threshold 500
#
arp speed-limit source-ip maximum 50
#
```

Fuente: Elaboración Propia

En la figura 7-3 muestra la configuración agregada a la interfaz y que no está es utilizada.

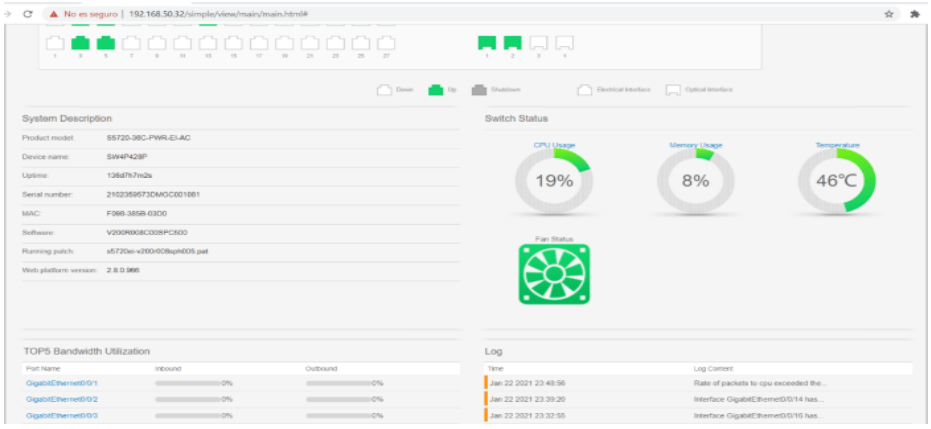
Figura 3-6 Implementación y configuraciones

```
#
interface GigabitEthernet0/0/46
 description Puerto para PC y Telefono
 shutdown
 port link-type hybrid
 voice-vlan 100 enable
 port hybrid pvid vlan 4
 port hybrid tagged vlan 100
 port hybrid untagged vlan 4
 port-security enable
 port-security max-mac-num 4
 port-security mac-address sticky
 arp anti-attack check user-bind enable
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping max-user-number 2
#
```

Fuente: Elaboración Propia

Al ejecutar el comando con la herramienta Yersinia, se observa en el dispositivo que no altera su consumo de recursos de la CPU del equipo que muestra la gráfica, a continuación.

Figura 3-7 Habilita los protocolos de protección



Fuente: Elaboración Propia

3.3. Política para el ataque a Vlan Hopping

Debido a la ausencia de medidas de protección para mitigar un ataque de Vlan HOPPING, que se aprovecha los diseños débiles de configuración, y al no contar con herramientas para su detección aprovecharían estas debilidades, lo que significa que el atacante realizaría acciones maliciosas dentro de la red LAN y el comando DHCP snooping permite proteger de diferentes ataques en el campo CHADDR y el MAC de origen y que comprueban las direcciones de los paquetes DHCP.

Cuando las direcciones DHCP de los paquetes son considerados como paquetes de suplantación de identidad estas son descartas directamente la imagen muestra la aplicación de la política.

Figura 3-8 Análisis el resultado después de aplicar la política

Fuente: Elaboración Propia

Al realizar las pruebas y mecanismos dentro del capítulo dos en un entorno controlado de equipos, se evidencia que no existe configuración que proteja a los mismo de

ataques dentro de los dispositivos de capa dos, que se detalla en la tabla 1-6. Para mitigar la vulneración.

Se realizó la siguiente configuración adicional a los dispositivos, para evitar este ataque y que el dispositivo quedaría en una DDoS. A forma de resumen las políticas propuestas tanto a nivel tecnológico como a nivel organizacional, operacional y físico para mitigar los ataques de Vlan a nivel de capa 2. En la figura 10-3 muestra la configuración adicional agregada a la interfaz para evitar ataques de Vlan hopping

Figura 3-9 Implementa configuraciones ausentes

```
interface GigabitEthernet0/0/47
 port link-type trunk
 port trunk allow-pass vlan 4 10 to 11 14 25 30 40 42 50 70 100
 port trunk allow-pass vlan 110
 dhcp snooping trusted
#
```

Fuente: Elaboración Propia

3.4. Política para el ataque DHCP

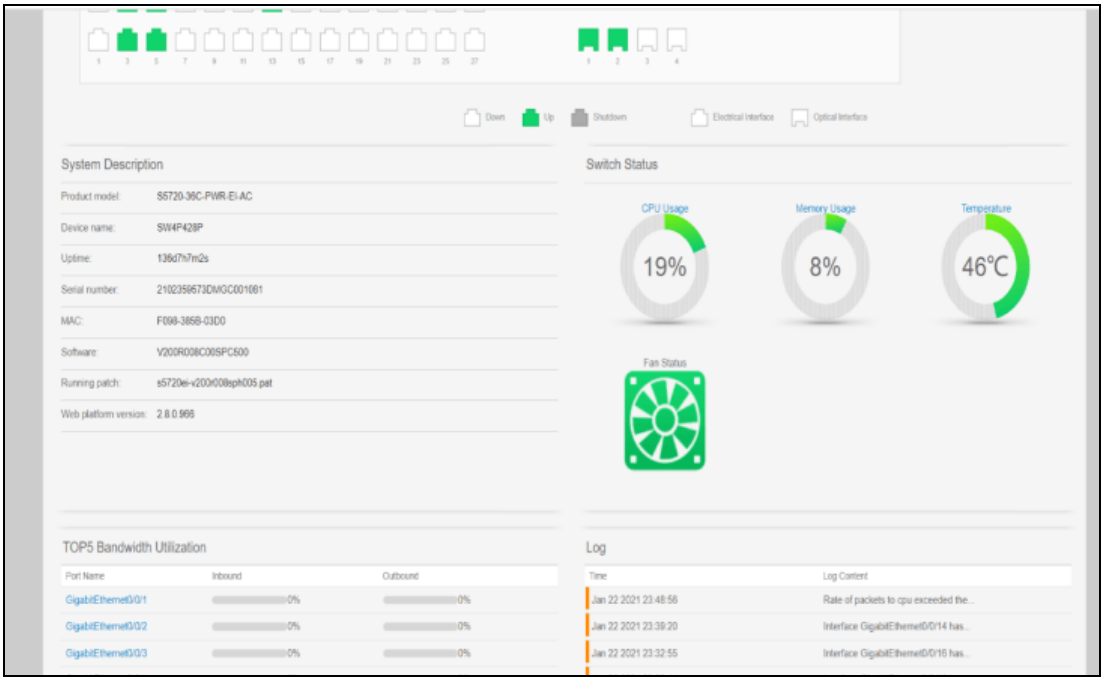
Al agregar la configuración a la interfaz, se observa en la figura 11-3, que tiene el resultado que el CPU del equipo no incrementa el consumo de recurso del equipo como muestra en la figura 12-3.

Figura 3-10 Implementación configuraciones au, sentes DHCP

```
#
dhcp enable
#
dhcp snooping enable
dhcp snooping check dhcp-rate enable
dhcp snooping check dhcp-rate 90
dhcp snooping alarm dhcp-rate enable
dhcp snooping alarm dhcp-rate threshold 500
#
arp speed-limit source-ip maximum 50
#
```

Fuente: Elaboración Propia

Figura 3-11 Resultado después de aplicar la política



Fuente: Elaboración Propia

3.5. Política para el ataque STP

En este tipo de ataque las tramas de BPDU incorrectas, se envían a los conmutadores para modificar la topología del árbol de expansión implementada en la red. Al explotar STP, un atacante realizaría un ataque de hombre en el medio (MITM) que permite escuchar a escondidas en el tráfico que pasa entre dos nodos en una red.

Figura 3-12 Resultado al aplicar la política

Fuente: Elaboración Propia

En la figura 13-3, a continuación, muestra la configuración en modo configuración global que permite la protección ante ataques de cambios de root.

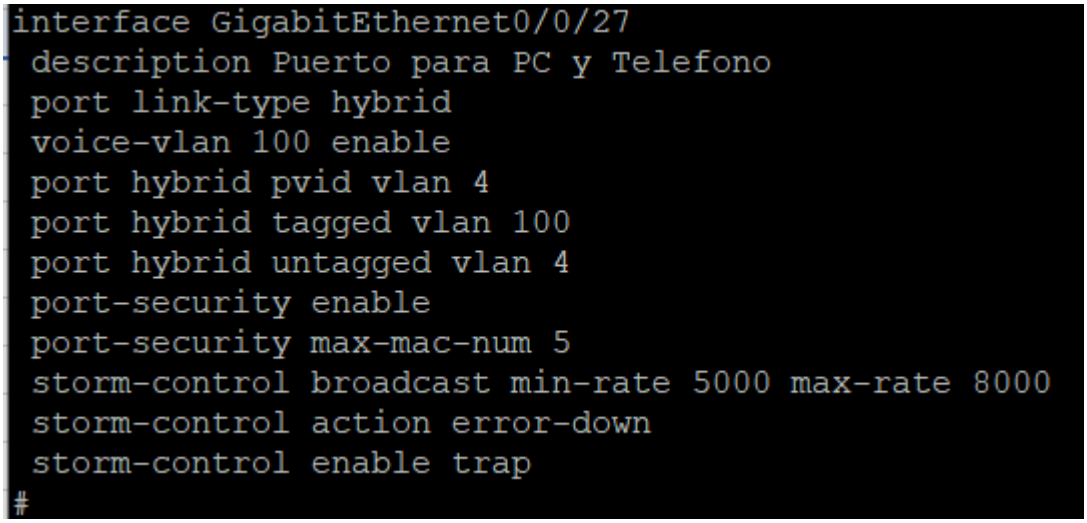
Figura 3-13 Configuraciones ausentes

```
#
stp instance 0 root primary
stp bpdu-protection
stp tc-protection
#
lldp enable
#
```

Fuente: Elaboración Propia

En la figura 14-3 muestra la línea de código que hay que agregar en cada una de las interfaces.

Figura 3-14 Configuraciones ausentes



Fuente: Elaboración Propia

CONCLUSIONES

- Se analizó la metodología establecida en la NORMA ISO 27032 para la implementación de políticas de ciber seguridad, el cual, permitió mitigar el riesgo de la indisponibilidad en los dispositivos de capa dos del centro de datos del Hospital de Latacunga.

- Se aplicó las políticas de ciber, seguridad, las cuales, permitieron reducir los ataques del hombre en la mitad, DHCP, STP Vlan hopping y ARP, se hace uso de las herramientas de seguridad informática de los dispositivos de capa dos de la institución, al agregar los parámetros y líneas de configuración en los equipos de capa dos. Esto permitió mejor el grado de seguridad en la infraestructura de red, en la casa de salud pública

- Se comparó los resultados de la implementación de políticas de ciber, seguridad con un escenario antes y después de su implementación, el mismo que permitió evidenciar que sin las políticas de seguridad implementadas en los equipos estaban expuestos en su totalidad a riesgos y vulnerabilidades tanto en configuración, como en capacitación del personal encargado. Mientras que, con la aplicación de las políticas, se pudo reducir los riesgos de ataque.

RECOMENDACIONES

- Toda organización tanto pública y privada está propensa a ataques informáticos, por lo que, es recomendable la implementación de políticas de seguridad a nivel de LAN, es el área más vulnerable de las organizaciones, debido a que los usuarios internos son quienes tienen mayor privilegio y permisos para acceder a información confidencial, es decir, ingresar a cualquier lugar de la organización sin ninguna restricción.

- A pesar de la identificación de las vulnerabilidades, es recomendable que las organizaciones tengan planes de contingencias y que estén preparadas para superar cualquier eventualidad que dificulte las actividades diarias del personal, esto se logra si el Departamento de Tecnologías de la Información y Comunicaciones regula el cumplimiento y evaluación en cuanto a la aplicación de las políticas de seguridad.

- Los administradores de red dan la misma atención de seguridad a los diferentes recursos de la infraestructura puesto que la capa dos del modelo OSI es propensa a ataques internos que provoca la denegación de servicio.

BIBLIOGRAFÍA

Aksu, M. Uğur, Enes Altuncu, y Kemal Bicakci. 2019. «A First Look at the Usability of OpenVAS Vulnerability Scanner». en *Proceedings 2019 Workshop on Usable security*. San Diego, CA: Internet Society.

Anón. s. f. «Acunetix Web Application Vulnerability Report 2020». *Acunetix*. Recuperado 7 de marzo de 2020a (https://www.acunetix.com/acunetix-web-application-vulnerability-report/).

Anón. s. f. «Implementación de un Marco de Ciber, seguridad ISO 27032 | Internet security Auditors». Recuperado 31 de marzo de 2020b (https://www.i, secauditors.com/consultoria-csf-iso-27032).

Argaw, Salem T., Juan R. Troncoso-Pastoriza, Darren Lacey, Marie-Valentine Florin, Franck Calcavecchia, Deni, se Anderson, Wayne Burleson, Jan-Michael Vogel, Chana O'Leary, Bruce Eshaya-Chauvin, y Antoine Flahault. 2020. «Cyber, security of Hospitals: Discussing the Challenges and Working towards Mitigating the Risks». *BMC Medical Informatics and Decision Making* 20(1):146. doi: 10.1186/s12911-020-01161-7.

B, Prabadevi, y Jeyanthi Nagamalai. 2018. «A framework to mitigate ARP sniffing attacks by cache poisoning». *International Journal of Advanced Intelligence Paradigms* 10:146. doi: 10.1504/IJAIP.2018.089496.

Bresteau, Corentin, Simon Guigui, Paul Berthier, y Jo, se M. Fernandez. 2018. «On the security of aeronautical datalink communications: Problems and solutions». Pp. 1A4-1-1A4-13 en *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*. Herndon, VA: IEEE.

Carrillo, J. J. M., N. A. Zambrano, T. J. L. Zambrano, y M. Z. Bravo. 2020. «Cyber, security process: Methodological guide for its implementation.» *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao* 2020(E29):41-50.

Castillo, Salcedo, y Juan Eduardo. 2020. «Di, seño y emulación de una red de datos con priorización de servicios en la Unidad Educativa Suizo Ambato».

Chakraborty, Sushmita, Praveen Kumar, Bhawna Sinha, Assistnat Professor, y Head. 2019. «A STUDY ON DDOS ATTACKS, DANGER AND ITS PREVENTION». doi: 10.1729/Journal.20847.

Dz3 MSP. s. f. «HOSPITAL GENERAL LATACUNGA». *hgl.mspz3.gob.ec*. Recuperado 4 de marzo de 2020 (http://hgl.mspz3.gob.ec/index.html).

Finkle, Caroline Humer, Jim. 2014. «Your medical record is worth more to hackers than your credit card». *Reuters*, septiembre 24.

Ha, segawa, Hirokazu, Yukiko Yamaguchi, Hajime Shimada, y Hiroki Takakura. 2016. «An Automated ACL Generation System for secure Internal Network». Pp. 559-64 en *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*. Atlanta, GA, USA: IEEE.

Heffel, Walter Ernesto, y Samuel Linares. s. f. «Ciber, seguridad industrial en la distribución de energía eléctrica». 126.

Kim, Kwangjun, y Manhee Lee. 2019. «SNMP-Ba, sed Detection of VLAN Hopping Attack Risk». Pp. 267-72 en *Information Science and Applications 2018*, *Lecture Notes in Electrical Engineering*, editado por K. J. Kim y N. Baek. Singapore: Springer.

Mahmood, Shahid, Syed Muhammad Mohsin, y Abrar Akber. 2020. *Network security Issues of Data Link Layer: An Overview*.

Mehra, Rakshit, y Kishore V. Krishnan. 2018. «Analyzing security Attack on Layer 2 and Comparing the Performance of Different Routing Protocols». Pp. 611-16 en *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. Bangalore, India: IEEE.

Molina, Bermúdez, y Kelly Gabriela. s. f. «Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001- sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros». 180.

Ndatinya, Vivens, Zhifeng Xiao, Vasudeva Manepalli, Ke Meng, y Yang Xiao. 2015. «Network forensics analysis using Wireshark». *International Journal of security and Networks* 10:91. doi: 10.1504/IJSN.2015.070421.

Ochoa Palomino, Angel. 2019. «Di, seño de una Red de seguridad Informática para la Protección del Sistema Web de un Call Center ante Ataques Informáticos Aplicando la Norma ISO 27033». Licenciatura, Universidad Peruana de Ciencias Aplicadas, Lima.

Prabadevi, B., N. Jeyanthi, y Ajith Abraham. 2020. «An Analysis of security Solutions for ARP Poisoning Attacks and Its Effects on Medical Computing». *International Journal of System Assurance Engineering and Management* 11(1):1-14. doi: 10.1007/s13198-019-00919-1.

Ren, Ming, Yanhui Tian, Siqi Kong, Dali Zhou, y Danping Li. 2020. *An detection algorithm for ARP man-in-the-middle attack ba, sed on data packet forwarding behavior characteristics*.

Rojas, Inoguchi. 2012. «Gestión de la ciber, seguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016». v2:49.

Umasuthan, Vivek. 2016. «Protecting the Communications Network at Layer 2». Pp. 1-5 en *2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*. Dallas, TX, USA: IEEE.

Xia, Yongjun, jin Wang, Chang Liu, y Kaiming Yu. 2020. «Design and Implementation of Vulnerability Scanning Tools for Intelligent Substation Industrial Control System Ba, sed on Openvas». *IOP Conference series: Earth and Environmental Science* 440:042031. doi: 10.1088/1755-1315/440/4/042031.

Yaibuates, Mayoon, y Roungsan Chaisricharoen. 2020. «A Combination of ICMP and ARP for DHCP Malicious Attack Identification». Pp. 15-19 en *2020 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON)*. Pattaya, Thailand: IEEE.

ANEXOS

ANEXO 1 Resultado obtenidos con la herramienta Openvas en formato pdf

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.50.13	0	2	0	0	0
Total: 1	0	2	0	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 2 results selected by the filtering described above. Before filtering there were 17 results.

2 Results per Host

2.1 192.168.50.13

Host scan start Mon Dec 21 07:44:42 2020 UTC
Host scan end Mon Dec 21 07:58:27 2020 UTC

Service (Port)	Threat Level
443/tcp	Medium

2.1.1 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

... continues on next page ...

... continued from previous page ...

TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:
TLS_RSA_WITH_RC4_128_SHA
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_RC4_128_SHA

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2020-11-26T08:02:59Z

References
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977

Medium (CVSS: 4.0)
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Summary
The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result
`Server Temporary Key Size: 512 bits`

Impact
An attacker might be able to decrypt the SSL/TLS communication offline.

Solution
Solution type: Workaround

... continues on next page ...

... continued from previous page ...

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).
For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight
The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

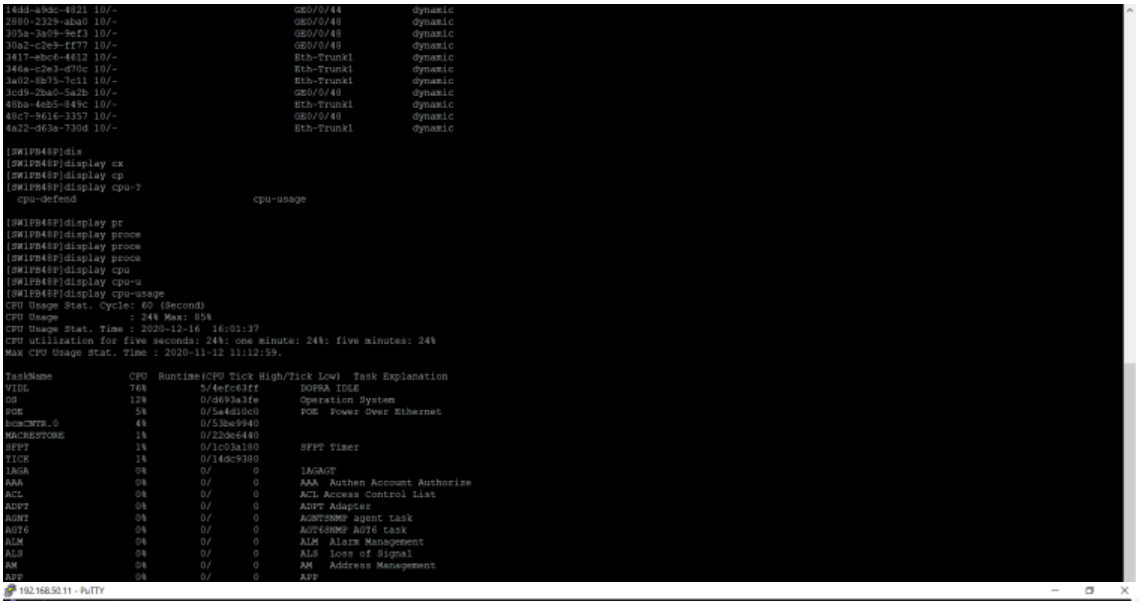
Vulnerability Detection Method
Checks the DHE temporary public key size.
Details: `SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili.`
`↪..`
OID:1.3.6.1.4.1.25623.1.0.106223
Version used: `2020-08-25T06:34:32Z`

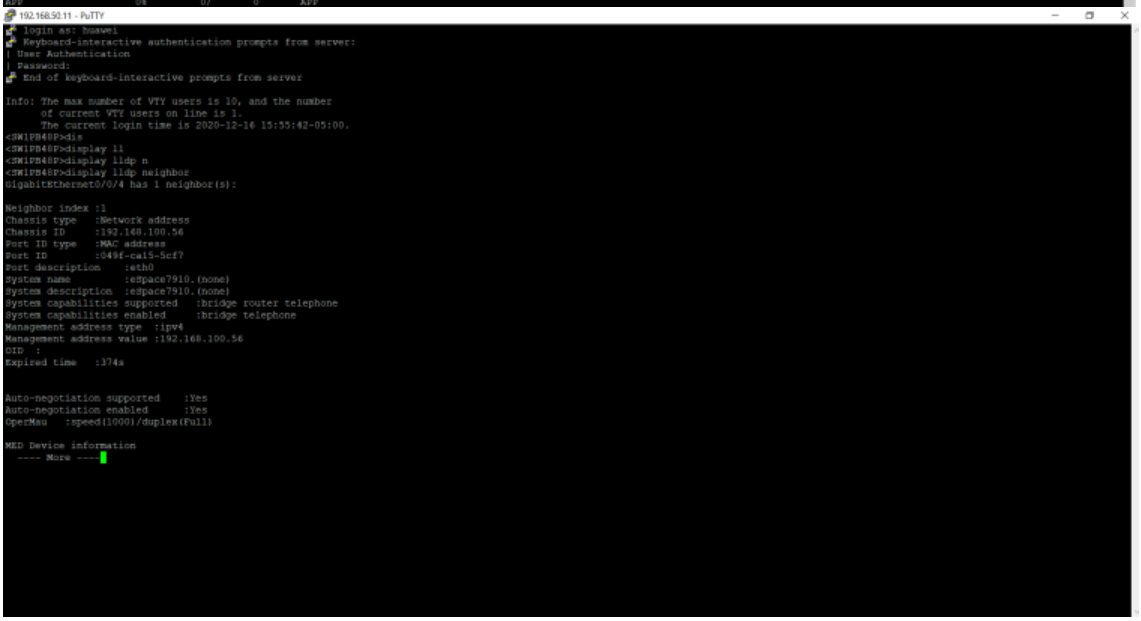
References
`url: https://weakdh.org/`
`url: https://weakdh.org/sysadmin.html`

[return to 192.168.50.13]

ANEXO2

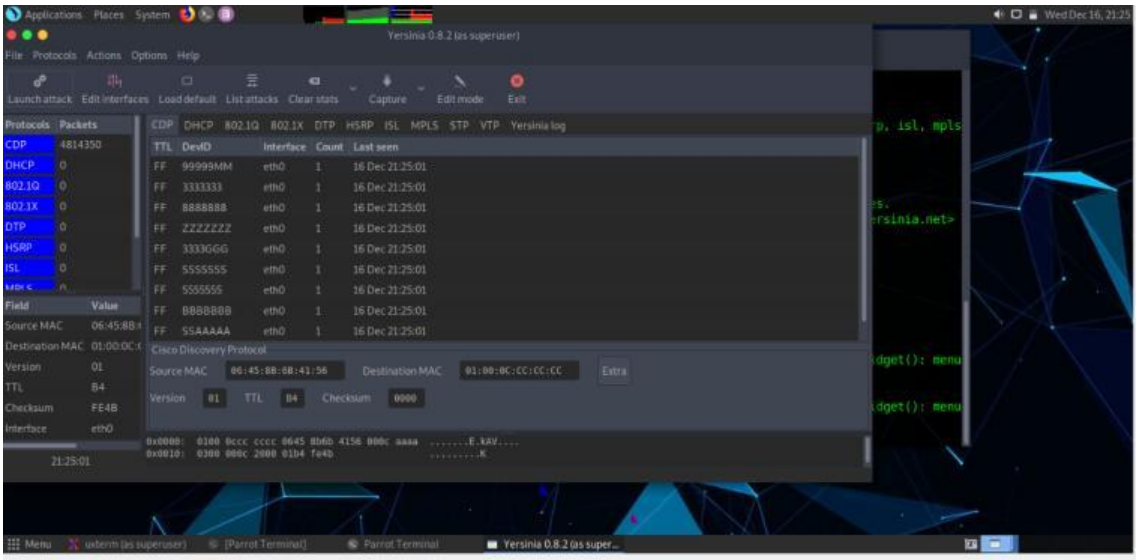
IMÁGENES DE CONFIGURACIÓN RESULTANTE DE LOS EQUIPO

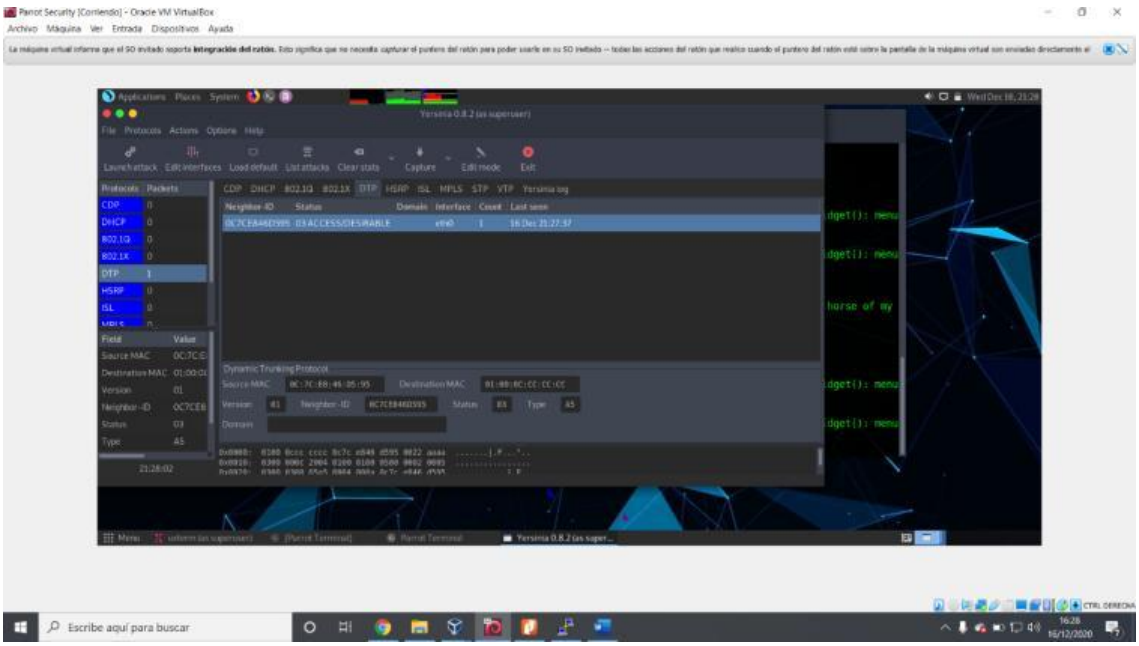


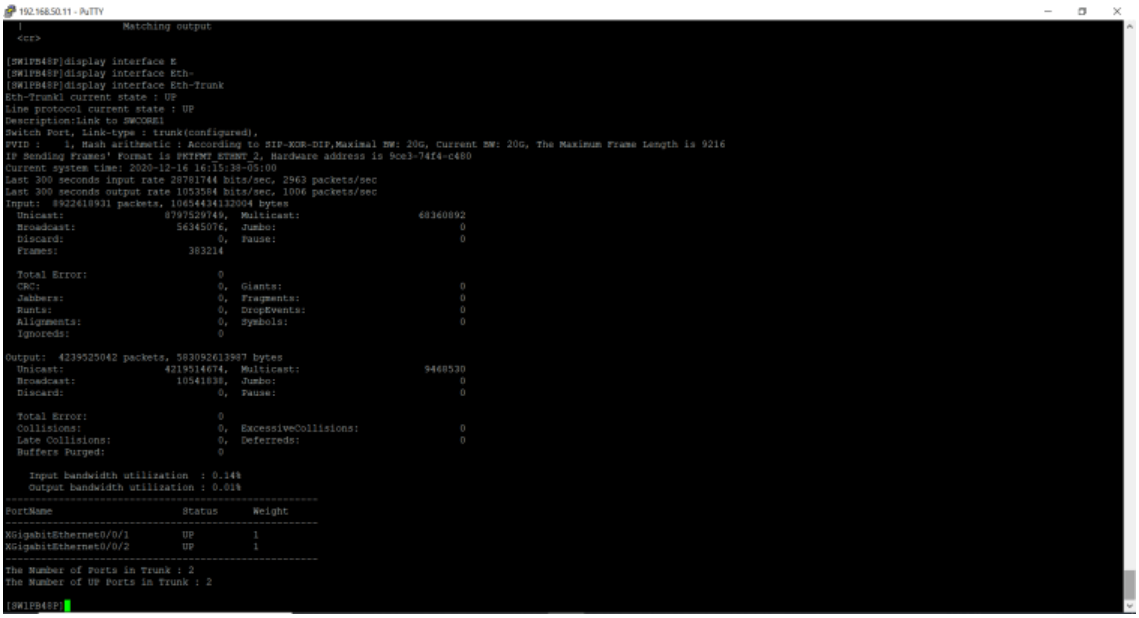


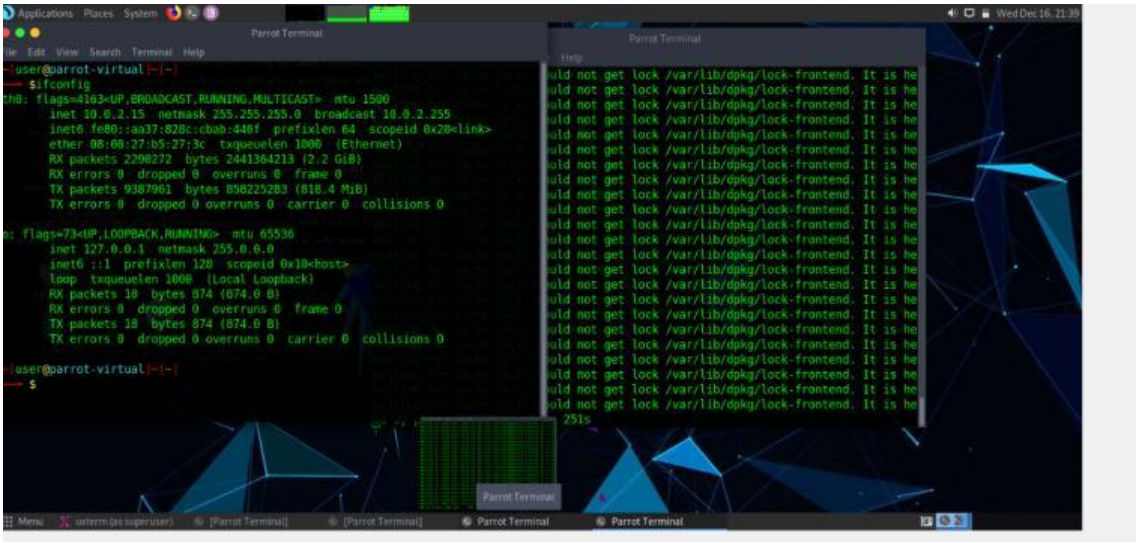
```
[SW1PB48P]dis
[SW1PB48P]display l
[SW1PB48P]display ll
[SW1PB48P]display lldp tr
[SW1PB48P]display lldp tra
[SW1PB48P]display lldp ?
  local       Information about the local device or ports
  neighbor    Neighbor information
  statistics  Statistics information
  tlv-config  Enable TLV information

[SW1PB48P]display lldp sta
[SW1PB48P]display lldp statistics
LLDP statistics global Information:
Statistics for MEth0/0/1:
Transmitted Frames Total: 0
Received Frames Total:    0         Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0

Statistics for GigabitEthernet0/0/1:
Transmitted Frames Total: 0
Received Frames Total:    0         Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0

Statistics for GigabitEthernet0/0/2:
Transmitted Frames Total: 98494
Received Frames Total:    0         Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0

Statistics for GigabitEthernet0/0/3:
Transmitted Frames Total: 0
Received Frames Total:    0         Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0
  ---- More ----
```

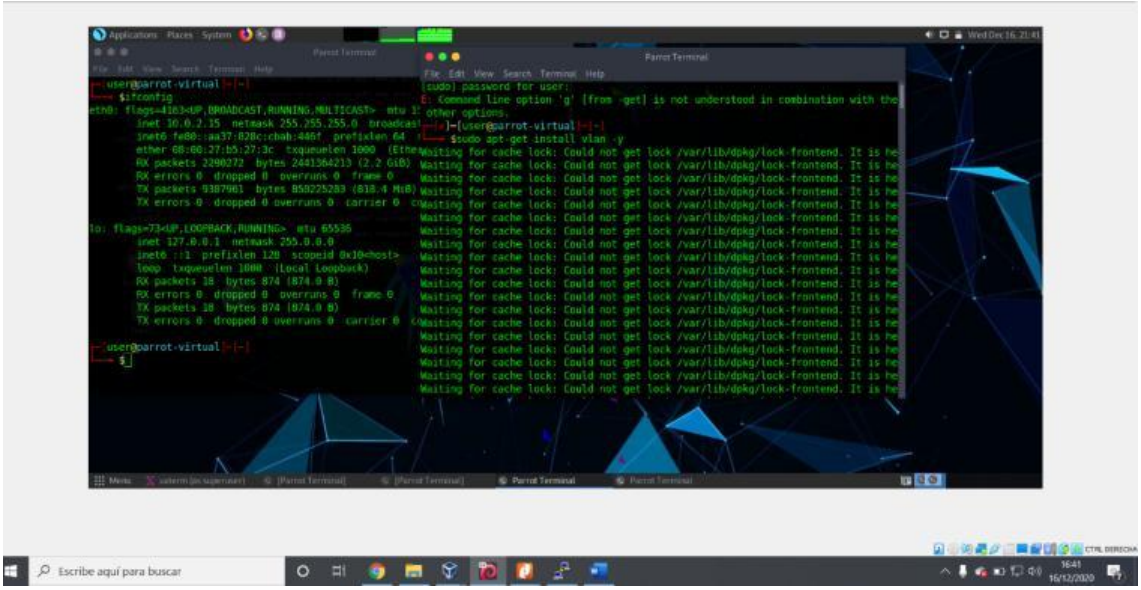
```
Statistics for MEth0/0/1:
Transmitted Frames Total: 0
Received Frames Total:    0         Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0

Statistics for GigabitEthernet0/0/1:
Transmitted Frames Total: 0
Received Frames Total:    0         Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0

Statistics for GigabitEthernet0/0/2:
Transmitted Frames Total: 98494
Received Frames Total:    0         Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0

Statistics for GigabitEthernet0/0/3:
Transmitted Frames Total: 0
Received Frames Total:    0         Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0

[SW1PB48P]display cpu-usage
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage            : 24% Max: 85%
CPU Usage Stat. Time : 2020-12-16  16:04:21
CPU utilization for five seconds: 24%; one minute: 24%; five minutes: 24%
Max CPU Usage Stat. Time : 2020-11-12 11:12:59.

TaskName            CPU  Runtime(CPU Tick High/Tick Low)  Task Explanation
VIDL                76%        5/4efc63ff       DOPRA IDLE
OS                  12%        0/d693a3fe       Operation System
POE                  5%        0/5a4d10c0       POE  Power Over Ethernet
bcmCNTR.0            4%        0/51a80a80
MACRESTORE           1%        0/232aaf80
SFPT                 1%        0/1c03a180       SFPT Timer
TICK                 1%        0/17d78400
1AGA                 0%        0/       0       1AGAGT
AAA                  0%        0/       0       AAA  Authen Account Authorize
ACL                  0%        0/  4c4b40       ACL Access Control List
ADPT                 0%        0/       0       ADPT Adapter
AGNT                 0%        0/       0       AGNTSNMP agent task
AGT6                 0%        0/       0       AGT6SNMP AGT6 task
AIM                  0%        0/       0       AIM  Alarm Management
ALS                  0%        0/  989680       ALS  Loss of Signal
AM                   0%        0/       0       AM  Address Management
APP                  0%        0/       0       APP
  ---- More ----
```

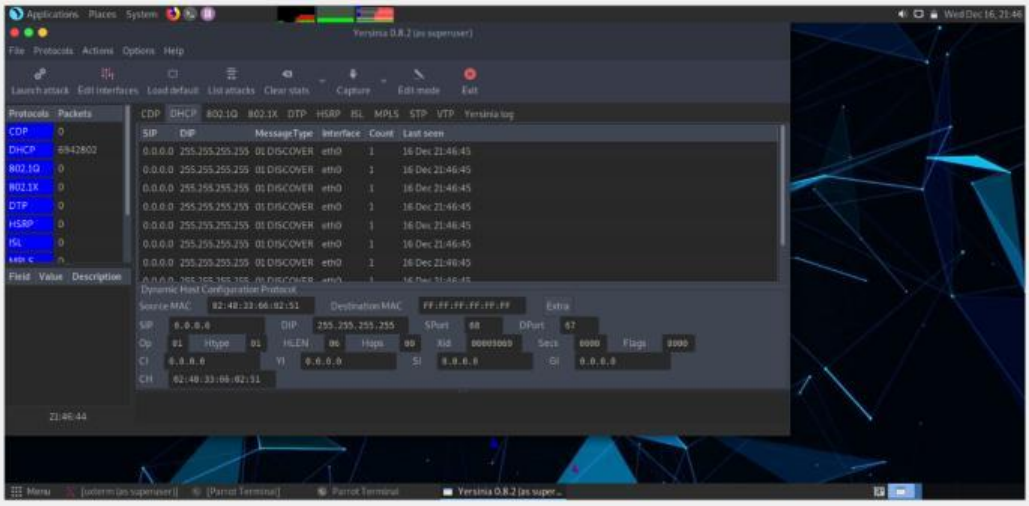

Applications Places System
Wed Dec 16, 21:25
Yersinia 0.8.2 (as superuser)
File Protocols Actions Options Help
Launch attack Edit interfaces Load default List attacks Clear stats Capture Edit mode Exit
Protocols Packets
CDP 4814350
DHCP 0
802.1Q 0
802.1X 0
DTP 0
HSRP 0
ISL 0
Field Value
Source MAC 06:45:8B:
Destination MAC 01:00:0C:
Version 01
TTL B4
Checksum FE4B
Interface eth0
21:25:01
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log
TTL DevID Interface Count Last seen
FF 99999MM eth0 1 16 Dec 21:25:01
FF 3333333 eth0 1 16 Dec 21:25:01
FF 8888888 eth0 1 16 Dec 21:25:01
FF ZZZZZZZ eth0 1 16 Dec 21:25:01
FF 3333GGG eth0 1 16 Dec 21:25:01
FF 5555555 eth0 1 16 Dec 21:25:01
FF 5555555 eth0 1 16 Dec 21:25:01
FF BBBBBBB eth0 1 16 Dec 21:25:01
FF SSAAAAA eth0 1 16 Dec 21:25:01
Cisco Discovery Protocol
Source MAC 06:45:8B:6B:41:56
Destination MAC 01:00:0C:CC:CC:CC
Extra
Version 01 TTL B4 Checksum 0000
0x0000: 0100 0ccc cccc 0645 8b6b 4156 000c aaaa .....E.kAV....
0x0010: 0300 000c 2000 01b4 fe4b .....K
Menu
Parrot Terminal
Yersinia 0.8.2 (as super...


Parrot Security [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Yersinia 0.8.2 (as superuser)
Dynamic Trunking Protocol
Escribe aquí para buscar
16:28
16/12/2020

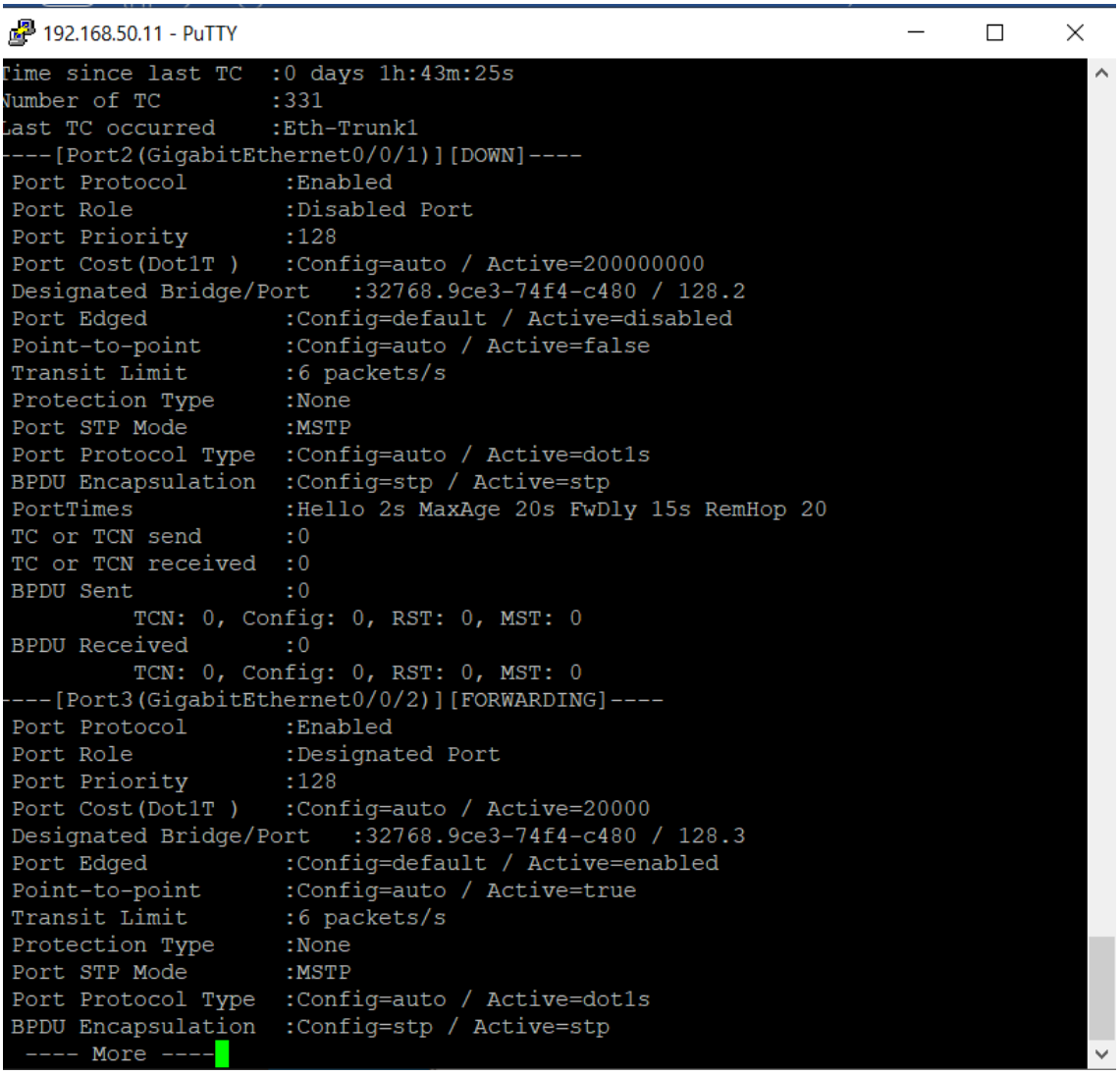

192.168.50.11 - PuTTY
Matching output
<cr>
[SW1PB48P]display interface E
[SW1PB48P]display interface Eth-
[SW1PB48P]display interface Eth-Trunk
Eth-Trunk1 current state : UP
Line protocol current state : UP
Description:Link to SWCORE1
Switch Port, Link-type : trunk(configured),
PVID : 1, Hash arithmetic : According to SIP-XOR-DIP,Maximal BW: 20G, Current BW: 20G, The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 9ce3-74f4-c480
Current system time: 2020-12-16 16:15:38-05:00
Last 300 seconds input rate 28781744 bits/sec, 2963 packets/sec
Last 300 seconds output rate 1053584 bits/sec, 1006 packets/sec
Input: 8922610931 packets, 10654434132004 bytes
Unicast: 8797529749, Multicast: 68360892
Broadcast: 56345076, Jumbo: 0
Discard: 0, Pause: 0
Frames: 383214
Total Error: 0
CRC: 0, Giants: 0
Jabbers: 0, Fragments: 0
Runts: 0, DropEvents: 0
Alignments: 0, Symbols: 0
Ignoreds: 0
Output: 4239525042 packets, 583092613987 bytes
Unicast: 4219514674, Multicast: 9468530
Broadcast: 10541838, Jumbo: 0
Discard: 0, Pause: 0
Total Error: 0
Collisions: 0, ExcessiveCollisions: 0
Late Collisions: 0, Deferreds: 0
Buffers Purged: 0
Input bandwidth utilization : 0.14%
Output bandwidth utilization : 0.01%
PortName Status Weight
XGigabitEthernet0/0/1 UP 1
XGigabitEthernet0/0/2 UP 1
The Number of Ports in Trunk : 2
The Number of UP Ports in Trunk : 2
[SW1PB48P]

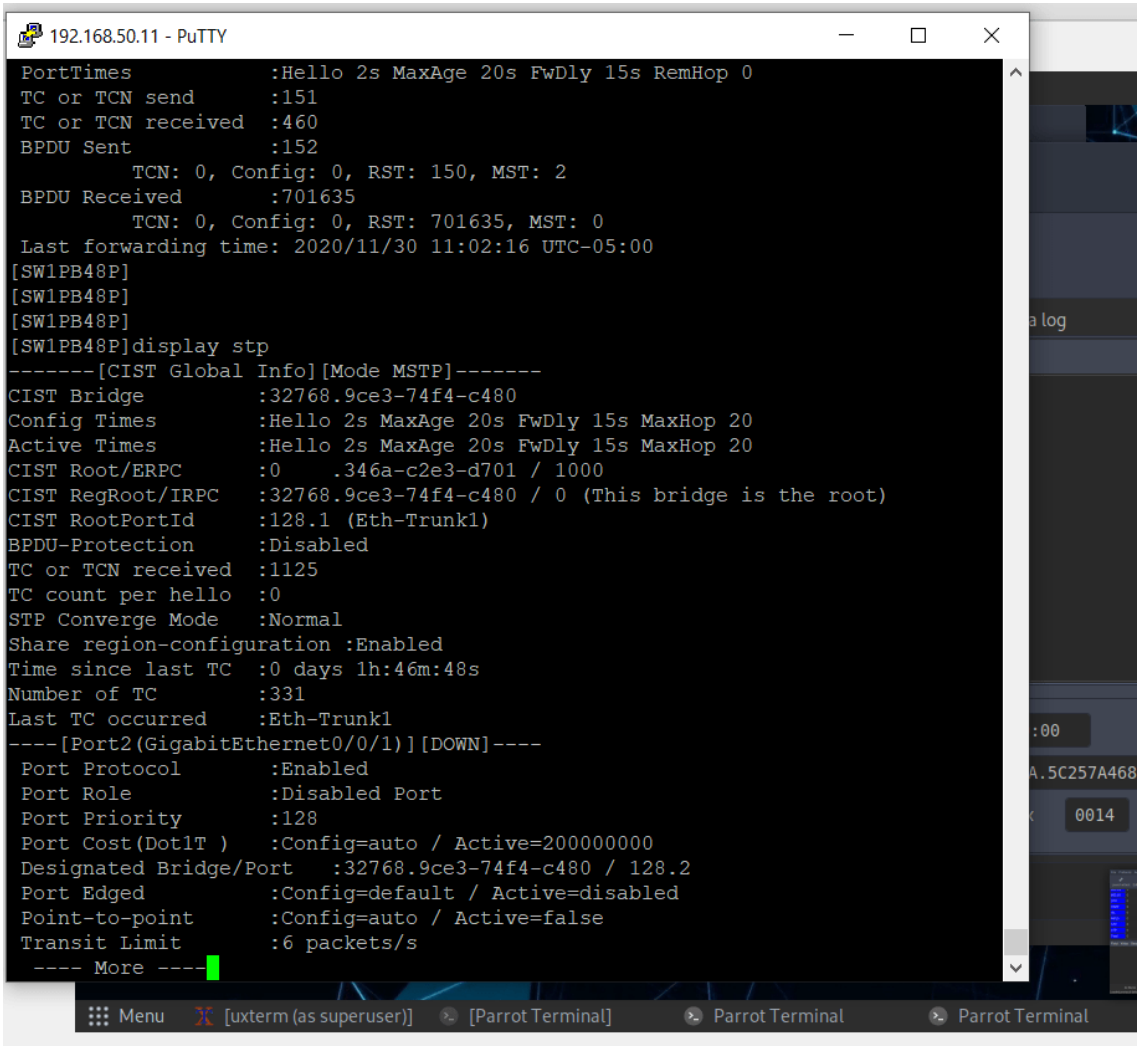

Applications Places System
Wed Dec 16, 21:39
Parrot Terminal
File Edit View Search Terminal Help
user@parrot-virtual
$ifconfig
flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::aa37:828c:cbab:446f prefixlen 64 scopeid 0x20<link>
ether 08:00:27:b5:27:3c txqueuelen 1000 (Ethernet)
RX packets 2298272 bytes 2441364213 (2.2 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 9387961 bytes 858225283 (818.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 18 bytes 874 (874.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 18 bytes 874 (874.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
user@parrot-virtual
$
Parrot Terminal
Could not get lock /var/lib/dpkg/lock-frontend. It is he
251s
Menu
Parrot Terminal
Parrot Terminal

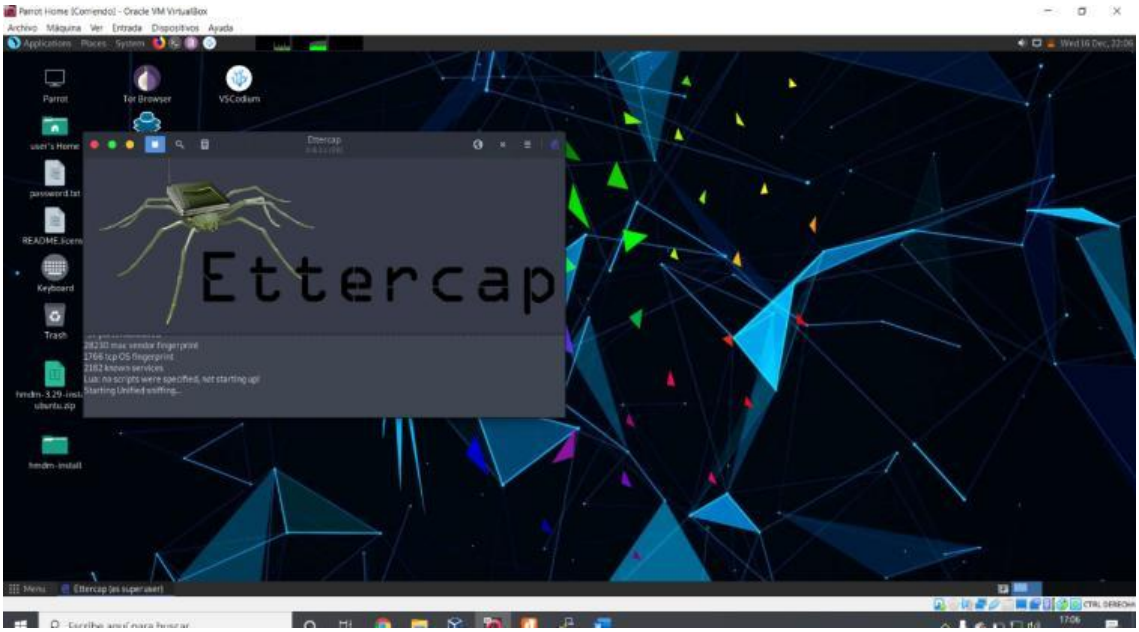

Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
user@parrot-virtual
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast
inet6 fe80::aa37:828c:cbab:446f prefixlen 64
ether 08:00:27:b5:27:3c txqueuelen 1000 (Ethernet)
RX packets 2200272 bytes 2441364213 (2.2 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 9387901 bytes 859225283 (818.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 18 bytes 874 (874.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 18 bytes 874 (874.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0
user@parrot-virtual
$
Parrot Terminal
File Edit View Search Terminal Help
[sudo] password for user:
E: Command line option 'g' [from -get] is not understood in combination with the
other options.
[user@parrot-virtual]
$sudo apt-get install vlan -y
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is he
Menu
Parrot Terminal
Escribe aquí para buscar
16:41
16/12/2020

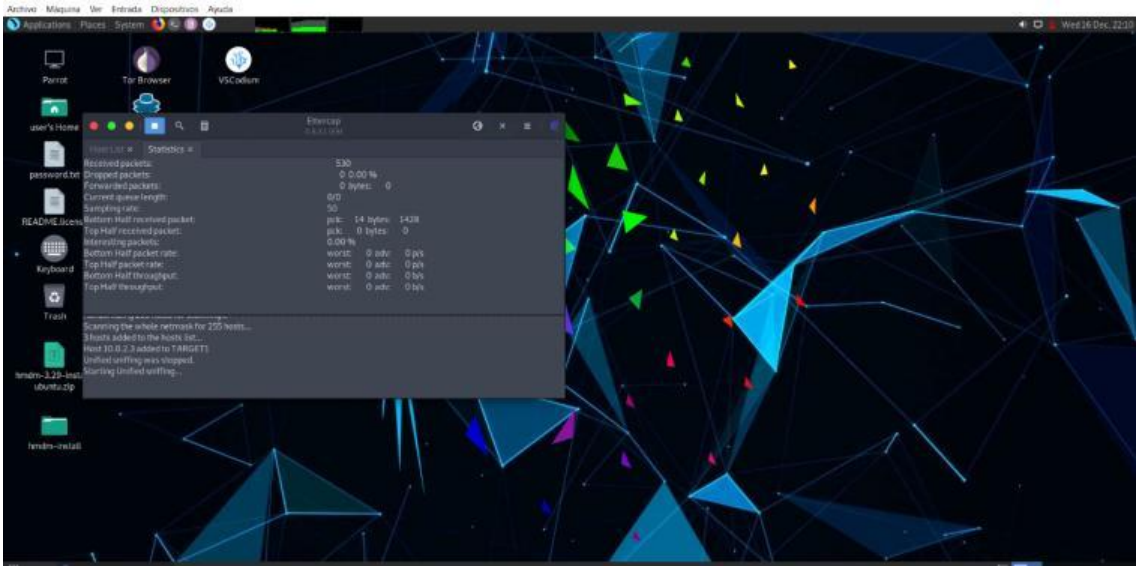

Applications Places System
Yersinia 0.8.2 (as superuser)
File Protocols Actions Options Help
Launch attack
Edit interfaces
Load default
List attacks
Clear stats
Capture
Edit mode
Exit
Protocols Packets
CDP 0
DHCP 6942802
802.1Q 0
802.1X 0
DTP 0
HSRP 0
ISL 0
Field Value Description
CDP DHCP 802.1Q 802.1X DTP HSRP ISL MPLS STP VTP Yersinia log
SIP DIP MessageType Interface Count Last seen
0.0.0.0 255.255.255.255 01 DISCOVER eth0 1 16 Dec 21:46:45
Dynamic Host Configuration Protocol
Source MAC 02:48:33:66:02:51
Destination MAC FF:FF:FF:FF:FF:FF
Extra
SIP 0.0.0.0
DIP 255.255.255.255
SPort 68
DPort 67
Op 01
Htype 01
HLEN 06
Hops 00
Xid 00003069
Secs 0000
Flags 0000
CI 0.0.0.0
YI 0.0.0.0
SI 0.0.0.0
GI 0.0.0.0
CH 02:48:33:66:02:51
21:46:44
Menu
Parrot Terminal
Yersinia 0.8.2 (as super...

STRP


192.168.50.11 - PuTTY
Time since last TC :0 days 1h:43m:25s
Number of TC :331
Last TC occurred :Eth-Trunk1
----[Port2(GigabitEthernet0/0/1)][DOWN]----
Port Protocol :Enabled
Port Role :Disabled Port
Port Priority :128
Port Cost(Dot1T) :Config=auto / Active=200000000
Designated Bridge/Port :32768.9ce3-74f4-c480 / 128.2
Port Edged :Config=default / Active=disabled
Point-to-point :Config=auto / Active=false
Transit Limit :6 packets/s
Protection Type :None
Port STP Mode :MSTP
Port Protocol Type :Config=auto / Active=dot1s
BPDU Encapsulation :Config=stp / Active=stp
PortTimes :Hello 2s MaxAge 20s FwDly 15s RemHop 20
TC or TCN send :0
TC or TCN received :0
BPDU Sent :0
TCN: 0, Config: 0, RST: 0, MST: 0
BPDU Received :0
TCN: 0, Config: 0, RST: 0, MST: 0
----[Port3(GigabitEthernet0/0/2)][FORWARDING]----
Port Protocol :Enabled
Port Role :Designated Port
Port Priority :128
Port Cost(Dot1T) :Config=auto / Active=20000
Designated Bridge/Port :32768.9ce3-74f4-c480 / 128.3
Port Edged :Config=default / Active=enabled
Point-to-point :Config=auto / Active=true
Transit Limit :6 packets/s
Protection Type :None
Port STP Mode :MSTP
Port Protocol Type :Config=auto / Active=dot1s
BPDU Encapsulation :Config=stp / Active=stp
---- More ----


192.168.50.11 - PuTTY
PortTimes :Hello 2s MaxAge 20s FwDly 15s RemHop 0
TC or TCN send :151
TC or TCN received :460
BPDU Sent :152
TCN: 0, Config: 0, RST: 150, MST: 2
BPDU Received :701635
TCN: 0, Config: 0, RST: 701635, MST: 0
Last forwarding time: 2020/11/30 11:02:16 UTC-05:00
[SW1PB48P]
[SW1PB48P]
[SW1PB48P]
[SW1PB48P]display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge :32768.9ce3-74f4-c480
Config Times :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC :0 .346a-c2e3-d701 / 1000
CIST RegRoot/IRPC :32768.9ce3-74f4-c480 / 0 (This bridge is the root)
CIST RootPortId :128.1 (Eth-Trunk1)
BPDU-Protection :Disabled
TC or TCN received :1125
TC count per hello :0
STP Converge Mode :Normal
Share region-configuration :Enabled
Time since last TC :0 days 1h:46m:48s
Number of TC :331
Last TC occurred :Eth-Trunk1
----[Port2(GigabitEthernet0/0/1)][DOWN]----
Port Protocol :Enabled
Port Role :Disabled Port
Port Priority :128
Port Cost(Dot1T) :Config=auto / Active=200000000
Designated Bridge/Port :32768.9ce3-74f4-c480 / 128.2
Port Edged :Config=default / Active=disabled
Point-to-point :Config=auto / Active=false
Transit Limit :6 packets/s
---- More ----
Menu
[uxterm (as superuser)]
[Parrot Terminal]
Parrot Terminal
Parrot Terminal


Parrot Home [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Parrot
Tor Browser
VSCodium
user's Home
password.txt
README.license
Keyboard
Trash
hmdm-3.29-insta
ubuntu.zip
hmdm-install
Ettercap
Ettercap


Archivo Máquina Ver Entrada Dispositivos Ayuda
Parrot
Tor Browser
VSCodium
user's Home
password.txt
README.license
Keyboard
Trash
hmdm-3.29-insta
ubuntu.zip
hmdm-install
Ettercap
Statistics
Received packets: 530
Dropped packets: 0 0.00 %
Forwarded packets: 0 bytes: 0
Current queue length: 0/0
Sampling rate: 50
0.00 %
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
Unified sniffing was stopped.
Starting Unified sniffing...