DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL PARA REDES BASADAS EN EL PROTOCOLO MODBUS TCP POR MEDIO DE NETFPGA

RICHARD ARDILA CRUZ

SERGIO ALBERTO GARCIA ALVAREZ

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA
FACULTAD DE INGENIERÍA ELECTRÓNICA
PIEDECUESTA
2013

DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL PARA REDES BASADAS EN EL PROTOCOLO MODBUS TCP POR MEDIO DE NETFPGA

RICHARD ARDILA CRUZ

SERGIO ALBERTO GARCIA ALVAREZ

PROYECTO DE GRADO PARA OPTAR POR EL TITULO DE INGENIERO ELECTRONICO

DIRECTOR
Ph.D. Jhon Jairo padilla Aguilar

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA
FACULTAD DE INGENIERÍA ELECTRÓNICA
PIEDECUESTA
2013

Nota de aceptación

_____
_____
_____
_____
_____

_____
Firma del director de proyecto

_____
Firma del jurado

_____
Firma del jurado

AGRADECIMIENTOS

A Dios

Doctor Jhon Jairo Padilla Aguilar

Nuestras Familias

Nuestros Maestros

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN GENERAL DEL TRABAJO DE GRADO

TITULO: DISEÑO E IMPLEMENTACIÓN DE UN FIREWALL PARA REDES BASADAS EN EL PROTOCOLO MODBUS TCP POR MEDIO DE NETFPGA

AUTORES: **RICHARD ARDILA CRUZ, SERGIO ALBERTO GARCIA ALVAREZ**

FACULTAD: **INGENIERIA ELECTRONICA**

DIRECTOR: **JHON JAIRO PADILLA**

RESUMEN:

El campo de las redes industriales es de gran relevancia en la actualidad debido a que la automatización de los procesos se ha fusionado con las redes de computadores para conformar redes de Controladores tales como PLCs, Máquinas de control numérico, etc. Estas redes se gestionan mediante Sistemas de Supervisión y Control conocidos como SCADA. En las redes industriales, el envío de información desde el controlador hacia el instrumento de medición se realiza por medio de tramas de datos. Dado que los controladores manejan diferentes protocolos de comunicación tales como Profinet, Profibus o Modbus, y estos protocolos no fueron diseñados pensando en los ataques informáticos, las tramas de datos no se encuentran codificadas. Por tanto, alguien que tenga acceso a la red del proceso puede leer los paquetes y, si tiene el conocimiento adecuado, modificar las tramas que envía el instrumento controlador, por ejemplo un PLC (Programmable Logic Controller), y provocar daños al proceso que se pueden reflejar en pérdidas materiales o en el peor de los casos humanas. Buscando mayor seguridad en los procesos industriales, y con el ánimo constante de innovación, en este proyecto se desarrolló un Firewall para redes industriales basadas en el protocolo MODBUS/TCP. Dicho Firewall fue construido utilizando una tarjeta NetFPGA. Las pruebas se realizaron sobre una red MODBUS/TCP del laboratorio de Automatización de la Escuela de Ingenierías. El sistema desarrollado permite la defensa de la red ante ataques como DoS, spoofing y sniffing.

PALABARAS CLAVE: Seguridad, Redes, Datos, Control, NET-FPGA

GENERAL SUMMARY OF THE THESIS

TITLE: **DESIGN AND IMPLEMENTATION OF A FIREWALL FOR MODBUS/TCP NETWORKS WITH THE NETFPGA SYSTEM.**

AUTHOR(S): **RICHARD ARDILA CRUZ**
SERGIO ALBERTO GARCIA ALVAREZ

FACULTY: **ELECTRONIC ENGINEERING**

DIRECTOR: **JHON JAIRO PADILLA**

ABSTRACT:

Industrial Networks field is an important topic today because automation processes and computer networks have been combined into a new data network class named industrial data network. Such networks are composed by industrial controllers, sensors, valves, etc., which are interconnected by means of Ethernet and other types of computer networks.In industrial networks, information forwarding from the controller to the meter is performed via data frames. Since drivers handle different communication protocols such as Profinet, Profibus or Modbus, and these protocols were not designed thinking on computer attacks, then, no data frames are encoded. In consequence, someone with network access permission could read process data packets and, with the appropriate knowledge, such attacker could modify data frames sent by the instrument controller, eg a PLC (Programmable Logic Controller), and cause damage to the process. Such attacks could produce consequences as production losses, material losses and, in the worst case, human diseases.This project brings a solution to these cyber-security problems. Looking for make safer industrial processes and also, looking for innovation, in this project a network firewall based on MODBUS / TCP protocol was developed. This Firewall was built using a NetFPGA card. The tests were performed on a network based on MODBUS / TCP allocated at the Automation Laboratory of Engineering School at UPB Bucaramanga. Firewall developed counteracts several attacks such as DoS, spoofing and sniffing.

KEY WORDS: NetFPGA, industrial data networks, MODBUS/TCP, Firewall, cyber-security, FPGA

INTRODUCCIÓN

La seguridad en redes industriales nace en respuesta a un vacío tecnológico generado cuando se diseñaron los diferentes protocolos, ya que estos buscaban un buen rendimiento y eficiencia en los tiempos de los procesos a controlar, pero se fiaron de un aislamiento físico entre la red del proceso y la red corporativa, aislamiento que ya no existe en las empresas que han implementado la pirámide CIM (Computer Integrated Manufacturing).

Teniendo en cuenta lo anteriormente planteado, se realizó el diseño e implementación de un firewall que aísle la red SCADA (Supervisory Control And Data Acquisition) de la red corporativa, utilizando para tal función el sistema NetFPGA, que es una tarjeta PCI (Peripheral Component Interconnect), cuyo contenido es una FPGA(Field Programmable Gate Array) desarrollada por Xilinx y diseñada por la Universidad de Stanford como una herramienta especializada para construcción de Switches y Routers.[1]

Con la realización del firewall se pudo ampliar el uso que actualmente se le da a la NetFPGA permitiendo además estudiar y profundizar conceptos del sistema operativo Linux CentOS 5.5, el sistema operativo Linux Backtrack, y el entorno de desarrollo ISE de Xilinx 10.1.3 para desarrollo de circuitos con FPGAs de Xilinx. [2]

En la primera parte de este libro se encontrarán enunciadas las diferentes vulnerabilidades presentes en la red, donde se incluyen ataques tanto a los equipos que soportan el sistema SCADA como a los dispositivos controladores del proceso. Una vez definidas las posibles debilidades se definen las diferentes técnicas de seguridad implementadas actualmente en las redes industriales. Del mismo modo se presenta cómo se intervino la red física del proceso y la manera en que se realizó el seguimiento de los datos. Luego se describe el desarrollo del algoritmo diseñado para el filtrado de paquetes en la NetFPGA,al igual que las diferentes herramientas que facilitan la creación de las tramas y las lecturas de las mismas. Finalmente se presenta cómo mediante la implementación del firewall en la red se pudo realizar un correcto filtrado de paquetes en la red y se obtuvo una mejora en la seguridad de esta.

[1] NetFPGA [en linea] <http://www.netfpga.org/php/specs.php> [citado 29 de septiembre de 2012]
[2] Guia NetFPGA [en línea] < http://netfpga.org/foswiki/bin/view/NetFPGA/OneGig/Guide> [citado 18 de octubre de 2012]

1. OBJETIVOS

1.1 Objetivo general

Diseñar e implementar un firewall basado en el sistema NetFPGA para redes industriales que funcione con tecnología fundamentada en el protocolo de comunicación modbus TCP (Transmission Control Protocol).

1.2 Objetivos específicos

- Hacer un estudio de vulnerabilidades que permita Identificar cuáles son las debilidades presentes en las redes industriales que facilitan la entrada de intrusos a una red

- Estudiar las diferentes formas que actualmente se utilizan para el mejoramiento de la seguridad en las redes industriales utilizando Firewalls.

- Intervenir la red física del sistema automatizado para hacer seguimiento de los paquetes de datos que se envían.

- Desarrollar un algoritmo mediante el cual se evite el paso de paquetes no deseados a la red del proceso industrial.

- Comprobar que la implementación del firewall en la red garantiza el filtrado de la información.

2. MARCO TEORICO

2.1 ¿QUE SON LAS REDES INDUSTRIALES?

Dado que la automatización de procesos ha revolucionado la industria, se ha generado cierta dependencia con muchas de estas nuevas infraestructuras ya que son claves, no solo para la realización de un proceso, sino porque de estas depende la economía de la empresa o para garantizar la prestación adecuada de un servicio. Existen diferentes ejemplos de estas automatizaciones, llamadas "infraestructuras críticas", tales como, el tratamiento de aguas residuales, la producción de gas y petróleo, la generación de energía o las telecomunicaciones que son procesos que han sido automatizados, y de los que dependen muchas personas.[3]

El control de los procesos automatizados gira entorno a los sistemas SCADA (Supervisory Control And Data Acquisition) y DCS (Distributed Control System), pero estos sistemas son susceptibles a los ataques físicos o de software. Es así, que se hizo necesaria la creación de diferentes entidades encargadas de generar planes de protección para estas infraestructuras, estas son un esfuerzo combinado entre las empresas públicas y el gobierno con el fin de proteger la inversión y la prestación de servicios.

El sistema SCADA provee una interconexión de diversos dispositivos que se encuentran en la parte inferior de la pirámide CIM (Computer Integrated Manufacturing), dichos dispositivos, que pueden ser sensores o actuadores, son monitoreados y controlados por el sistema SCADA a través de un PC o PLC (Programmable Logic Controller), una configuración típica de un sistema SCADA se muestra en la Figura 1.[4]

[3] A.Nicholson. SCADA security in the light of Cyber-Warfare. EN: Computers & Security. N° 31 (Junio de 2012); pag 418-436

[4] Patel, M. Development of a novel SCADA system for laboratory testing. ISA Transactions. N° 43 (Julio de 2004); pag 477-490

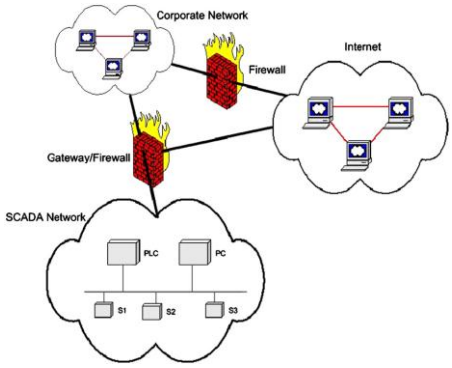


FIGURA 1. Sistema SCADA típico[5]

Estos sistemas se encuentran en una central de control que usualmente están físicamente separadas de la fábrica y ofrecen facilidades de comunicación. Estas centrales cuentan con diferentes interfaces que dan a conocer a quien vigila el estado del proceso la manera en que se comporta toda la red. Además, las centrales de control también tienen la posibilidad de interconectarse con los niveles superiores de la pirámide CIM, como lo son el MES y el ERP por medio de gateways o puertas de enlace que permiten interconectar las redes de los diferentes niveles.

Las comunicaciones con una red SCADA incluyen la conexión entre los dispositivos maestros y los esclavos. Cabe aclarar que un dispositivo maestro es el que puede controlar la operación de cualquier otro dispositivo, a los que se les llama esclavos, un ejemplo de los dispositivos maestros son los PLC, siendo los esclavos simples sensores o actuadores.

Cuando se empezó a diseñar e implementar los sistemas SCADA, la meta era tener un sistema confiable y el énfasis era que se proporcionaran características que garantizaran que las tareas de control se cumplieran pese a las limitaciones de red. Debido a esto, en la actualidad el error conceptual con respecto a la seguridad informática más común se encuentra en creer que la red del SCADA se encuentra aislada electrónicamente y que no es posible acceder a ella para atacarla.[6]

Se ha tenido la concepción de que la seguridad en los sistemas SCADA se debe realizar de manera física es decir más restricciones de acceso, más personal de seguridad, etc; sin embargo, el incremento en la conectividad entre los diferentes

[5] IGURE,Vinay. Security issues in SCADA networks, EN: Computers & Security. N° 25 (Octubre de 2006); pag 498-506.

[6] Padilla, Jhon Jairo. Redes industriales, notas de clase [en línea¨].< http://jpadilla.docentes.upbbga.edu.co/redes_industriales/programa_redes_industriales.htm> [citado en 4 de mayo de 2012]

niveles de la pirámide CIM (ver Figura 2.) ha llevado a que la red “aislada” se interconecte con los niveles MES (Manufacturing Execution System) y ERP(Enterprise Resource Planning), generando grietas en la seguridad de las redes del sistema SCADA dado que existen múltiples puntos de acceso al sistema DCS desde cualquier parte de la red y, si bien esta se encuentra aislada por medio de un firewall, pueden existir otros canales de comunicación no protegidos para acceder acceder a la red interna, tales como líneas telefónicas móviles y fijas con servicio de datos e Internet.

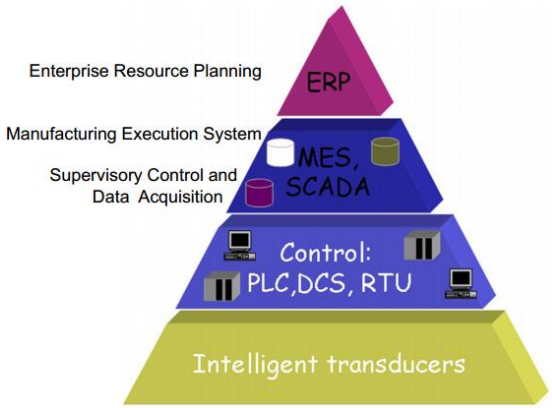


FIGURA 2. PIRAMIDE CIM[7]

A través de los años se han creado estándares para la comunicación de los sistemas SCADA con el fin de abrir el mercado y la competencia, beneficiando a los usuarios finales en la consecución de equipos con los mismos estándares pero con diferentes marcas. El problema es que esto facilita que, cuando se conoce estos estándares y la manera en que trabajan dichos sistemas, se puedan atacar mediante herramientas informáticas creadas para tal fin.

Los ataques que se generen a una red industrial pueden comprometer la fiabilidad, integridad o confidencialidad del proceso. Un ejemplo de ello es que por medio de un Sniffing que rastree la trasmisión de datos a través de la red, se puede violar la confidencialidad de la información.

Existen diferentes soluciones en la seguridad de los sistemas SCADA, a continuación se tratan los que se consideran pueden contribuir en el mejoramiento de la seguridad en las redes:

[7] Padilla, Jhon Jairo. Introducción a las Redes industriales, notas de clase [en línea¨].< http://jpadilla.docentes.upbbga.edu.co/redes_industriales/1-Introduccion.pdf> [citado en 17 de octubre de 2012]

- Control de acceso:

Consiste en controlar quienes pueden entrar o no a la red. Si bien es algo que suena muy básico, es importante recordar que los sistemas SCADA se encuentran conectados a niveles superiores . Aunque existen las conocidas gateways (puertas de control de acceso), estas muchas veces no incluyen protocolos de seguridad, por lo que se hace necesario el desarrollo de unas gateways que integren mecanismos de autenticación garantizando la confidencialidad de los datos.

- Firewalls y sistemas detectores de intrusos:

La función básica de un firewall es la de bloquear el tráfico no autorizado, impidiendo que comunicaciones no autorizadas entren a la red protegida, estableciendo una puerta de acceso entre la red exterior y la red local del sistema SCADA. Así, si por ejemplo se configura el firewall para reconocer y retransmitir el paso solo del tráfico que maneje el protocolo MODBUS, el firewall desechara cualquier otro tráfico. [8]

2.2 RESEÑA HISTORICA DE LAS REDES INDUSTRIALES[9]

La automatización industrial ha surgido en la historia con el fin de satisfacer necesidades humanas, en la línea de tiempo se puede evidenciar de la siguiente forma:

- *Principios el siglo XX hasta los años 50*: se dió origen a las máquinas en la revolución industrial, se empezaron a utilizar elementos mecánicos y electromagnéticos como motores, relés, temporizadores, contadores, entre otros.
- *Años 50*: se empieza a utilizar la electrónica con el uso de semiconductores, reducción de tamaño en los armarios eléctricos para resolver la problemática por grandes volúmenes en armarios.
- *Año 1968*: Bedford associates desarrolla un prototipo de controlador industrial considerado como el primer PLC, el cual generaba mayor practicidad en su implementación, ya que era reutilizable, fácil de programar, basado en semiconductores y su área de acción era a nivel industrial.
- *Años 70:* en la década de los 70 se dio la siguiente evolución.

[8] IGURE,Vinay. Security issues in SCADA networks, EN: Computers & Security. N° 25 (Octubre de 2006); pag 498-506.

[9]

    - implementación de los primeros ordenadores digitales que eran más flexibles y fácil de programar pero no eran aptos para la industria
    - incorporación del microprocesador permitiendo la realización de cálculos, además se logró establecer comunicación para enviar órdenes de control desde un ordenador central a los autómatas.
    - se realizaron mejoras en los autómatas estableciendo conexiones más flexibles de sensores y actuadores, además se implementaron comunicaciones y lenguajes de programación más potentes
- *Años 80:* en esta época se añadieron mejoras para optimizar procesos, aumentando velocidad de procesamiento, disminución de dimensiones e implementación de técnicas de control complejas, además se la introducción de lenguajes de programación (contactos, lista de instrucciones, GRAFCET, entre otros).
- *Actualidad:* actualmente la automatización se enfoca en el mejoramiento de velocidad de procesamiento y dimensiones de los autómatas haciéndolos más compactos y sencillos con el fin de establecer redes industriales en diferentes estándares de comunicaciones basándose en arquitecturas como la pirámide CIM teniendo en cuenta la producción integrada y controlada por ordenador con múltiples autómatas.

2.3 BENEFICIOS Y TIPOS DE REDES INDUSTRIALES[10]

Las redes industriales se originaron a partir de las redes de campo (fieldbus), las cuales desarrollaron un protocolo de comunicación que permite la interacción de los instrumentos de medida y control de procesos en una misma plataforma. Este tipo de comunicación se fundamenta principalmente en señales analógicas, ya sean señales neumáticas 3 a 15 psi en las válvulas de control o señales electrónicas 4-20mA.

Beneficios de las redes industriales:

- Tiempo de operación reducido, ya que permite el trabajo de dispositivos simultáneamente (operación paralela)
- Procesamiento de gran cantidad de información a altas velocidades
- Integración rápida y simple de los subsistemas que componen la red
- Permite la detección de fallas en el proceso mediante supervisión y monitoreo desde una estación central de control

[10] KNAPP,Eric. Industrial Network Security:Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress 2011; p 341.

- Permite la programación desde un terminal remoto

Tipos de redes industriales:

- Ethernet: consiste en la transmisión de datos por medio de paquetes, donde el acceso a la red utiliza un modelo CSMA/CD ("Carrier Sense Multiple Access with Collision Detection"). Este tipo de red es ampliamente conocida y además se encuentra estandarizada, por lo cual muchos sistemas la implementan, pero posee limitantes por tener un ancho de banda bajo y porque se debe mantener el control de las colisiones. La topología más utilizada en la actualidad para estas redes es la Estrella, por lo que se utilizan Switches para interconectar los dispositivos que componen el DCS.

- Fieldbus (Buses de campo): son sistemas de comunicación digital bidireccional con topología en Bus, ideal para operar sistemas de control y monitoreo. Pueden utilizar protocolos diseñados particularmente para estas topologías, aunque también podrían utilizar la arquitectura de protocolos TCP/IP.

- Profibus: es un sistema de comunicación para bus de campo, que puede ser implementado para comunicación extensa y compleja, además permite la transmisión crítica en el tiempo de datos a alta velocidad.

- CAN (Control Area Network): permiten la comunicación entre dispositivos mediante un bus serial, se caracteriza por la comunicación directa entre dispositivos sin implementación de controladores con el fin de obtener respuestas rápidas y los costos para su implementación son bajos.

- Device-Net: es una red que se emplea principalmente en procesos de fabricación, ya que permite una comunicación punto a punto y permite la transmisión de señales de datos y potencia por medio del mismo cable.

Protocolos para buses de campo[11]:

- Protocolo BITBUS: sistema de comunicación serial, basado en líneas compartidas (implementación de varias estaciones de comunicación en un mismo par de cable), este protocolo se encuentra optimizado para la transmisión de pequeños mensajes en tiempo real.
- Protocolo PROFIBUS: este protocolo permite la comunicación de dispositivos sin necesidad de adaptaciones mediante interfaces especiales, es empleado para la transmisión de datos a alta velocidad y tiempos críticos.

- Protocolo MODBUS: protocolo de comunicación desarrollado principalmente para transmisión de datos entre PLCs y dispositivos actuadores, mediante arquitectura maestro-esclavo.

3. SEGURIDAD EN REDES INDUSTRIALES

Para poder manejar la seguridad en una red se deben conocer cada uno de los dispositivos presentes en esta, al igual que el protocolo de comunicación Modbus, que es el que se usará en la red del proyecto. Es por esto, que inicialmente se presentará una breve descripción de los diferentes elementos que componen la red industrial a usar, omitiendo el sistema SCADA del cual ya se habló con anterioridad, y se analizará cuáles son las vulnerabilidades a las que está sujeta la red.

3.1 DISPOSITIVOS Y PROTOCOLO MODBUS DE LA RED INDUSTRIAL

3.1.1 Modbus

Es un protocolo de comunicación industrial que puede usarse en el nivel 2 o en el nivel 7 del modelo OSI (*open system interconnection.* fue implementado por Modicon en 1979, con el fin de establecer la comunicación entre PLCs (*Programmable Logic Controller).* Su funcionamiento se basa en la arquitectura maestro-esclavo, donde el esclavo ejecuta órdenes y el maestro se encarga de recibir instrucciones del usuario, para enviar órdenes a los esclavos y recibir los

[11] MENDIBURU, Henry A. Automatización medio ambiental, INDECOPI 2003;p53-57

resultados obtenidos en los esclavos (respuestas). El maestro puede establecer comunicación con los esclavos de dos formas:

“peer to peer”: permite la comunicación “maestro-esclavo” donde el maestro solicita información y y sólo el esclavo encuestado responde.

“broadcast”: permite la comunicación “maestro - todos los esclavos”, el maestro envía un comando a todos los esclavos de la red sin esperar respuesta.

El protocolo de comunicación MODBUS es uno de los más utilizados en los sistemas de automatización y control a nivel industrial, ya que es público, fácil de instalar y flexible en su operación. MODBUS maneja bloques de datos sin suponer restricciones,, lo que le permite mayor disponibilidad para la conexión de dispositivos electrónicos industriales.

MODBUS puede ser instalado en áreas de control, permitiendo la comunicación en redes de dispositivos, por ejemplo en sistemas de medida de temperatura, nivel, presión, humedad u otros enviando los resultados a un ordenador, también se usa para la conexión de un ordenador de supervisión con una RTU (remote terminal unit) y en sistemas SCADA.

Existentes dos variantes en redes MODBUS que constan de representaciones numéricas de los datos y detalles del protocolo diferentes como se observa en la tabla 1.

MODBUS RTU	MODBUS ASCII
Representación binaria compacta de los datos	Representación legible del protocolo pero menos eficiente, los bytes se envían codificados en ASCII
Finaliza la trama con un suma de CRC (cyclic redundancy check)	Finaliza la trama con un suma de LRC (longitudinal redundancy check)

Tabla 1. Modbus RTU/Modbus ASCII

MODBUS/TCP es muy semejante al formato RTU, pero establece la transmisión mediante paquetes TCP/IP. Cuando MODBUS es transmitido en TCP, se le añade en la cabecera una información adicional de longitud del mensaje, que permite conocer los límites del mismo, incluso si el mensaje es enviado en múltiples paquetes.

Los paquetes MODBUS TCP tienen la siguiente estructura

MBAP HEADER 7 bytes	FUNCTION CODE	DATA

MBAP HEADER: la cabecera tiene una longitud de 7 bytes y está compuesta por 4 campos.

- Identificador de trama (2 bytes): Es empleado para la transacción, el servidor MODBUS copia en la respuesta el identificador de la trama de la petición.
- Identificador de protocolo (2 bytes): Es empleado para los sistemas multiplexados. El protocolo MODBUS es identificado por el valor 0.
- Longitud (2 bytes): Este campo es un contador de bytes de los siguientes campos, incluyendo el identificador de unidad y el campo de datos.
- Identificador de unidad (1 byte): Este campo es puesto por el cliente MODBUS y es usado por el servidor para identificar un esclavo remoto conectado a la línea serial o a otros buses.

FUNCTION CODE: el código de función indica la acción asignada al controlador al que se le envía la información. En la tabla 2 se muestra la descripción y función de los códigos.

CODIGO	ACCIÓN	SIGNIFICADO
01	Leer bobinas (0:xxxx)	Obtiene el estado actual ON/OFF de un grupo de bobinas lógicas
02	Leer entradas (1:xxxx)	Obtiene el estado actual ON/OFF de un grupo de entradas lógicas
03	Leer Registros (4:xxxx)	Obtiene el valor binario de uno o más registros de almacenamiento
04	Leer Registros (3:xxxx)	Obtiene el valor binario de uno o más registros de entrada
05	Escribir Bobina (0:xxxx)	Fuerza el estado de una bobina

06	Escribir Registro (4:xxxx)	Escribe el valor binario de un registro de almacenamiento
15	Escribir Bobinas (0:xxxx)	Fuerza el estado de un grupo de bobinas
16	Escribir Registros (4:xxxx)	Escribe el valor binario de un grupo de registros de almacenamiento

Tabla 2. Function Code MODBUS

3.1.2 PLC (Programmable Logic Controller)

Un PLC se puede definir como un sistema basado en un microprocesador, cuyas partes fundamentales son la unidad central de proceso (CPU), en su mayoría tienen un puerto serial y un puerto Ethernet, cuenta con dos memorias, una ROM (Read Only Memory) que es la encargada de almacenar los programas para el correcto funcionamiento del sistema , y una memoria RAM (Random Access Memory) que es conformada por la memoria de datos y por la memoria de usuario.[12]

Cuenta con tres clases de entras y salidas que son digitales, analógicas o especiales. Las entradas digitales presentan dos estados up o down, mientras que las entradas análogas se encargan de convertir una magnitud analógica equivalente a una magnitud física en una expresión binaria, lo cual se realiza mediante conversores análogos- digitales (ADC).

3.1.3 RTU[13]

Las unidades remotas se encargan de recopilar datos de los elementos de campo y transmitirlos hacia la Unidad Central, a la vez que enviar los comandos de control a éstos.

Están basados, generalmente, en ordenadores que controlan directamente el proceso por medio de tarjetas convertidoras o por medio de comunicación con el centro de control donde se encuentra el PLC, dado que están diseñados para trabajar en campo su construcción es más robusta, es decir, soporta condiciones que un procesador normal no podría soportar.

[12] RAMAZAN,Bayindir. A water pumping control system with a programmable logic controller (PLC) and industrial wireless modules for industrial plants—An experimental setup. EN: ISA Transactions. N°50 (Abril de 2011); pag 321-328

[13] BAILEY, David. SCADA systems, hardware and firmware; EN: Practical SCADA for Industry, Newnes. P 17

3.2 VULNERABILIDADES EN LAS REDES INDUSTRIALES

3.2.1 SOFTWARE MALICIOSO[14]

Este tipo de software es desarrollado con el fin atentar con la seguridad de un sistema, mediante el robo de información, instalación de programas, daño de los dispositivos entre otros.

De acuerdo a su propagación, este tipo de software se clasifica de la siguiente manera:

Virus: se encuentran dentro de ficheros generalmente en ejecutables .exe y .src, este tipo de software actúa cuando se ejecutan los ficheros infectados propagando el virus a otros archivos

Gusanos: el gusano se propaga por redes p2p, generalmente por correo; entre sus acciones esta cambiar parámetros del sistemas, modificación de registros, ejecución de programas y cambios al arranque del sistema.

Troyanos: se introducen al ordenador por descargas y por medio de otros programas. Estos llevan consigo otras codificaciones maliciosas como virus, spyware, gusanos, entre otros.

El software malicioso se clasifica también por las acciones que ejecutan en el ordenador:

Adware: visualización de publicidad y recopilación de información.

Bloqueador: obstruye la ejecución de programas y aplicaciones.

Keylogger: captura los caracteres ejecutados con el teclado, se usa generalmente para capturar datos de acceso a cuentas.

Spyware: captura información del equipo para enviarla a un servidor determinado; es comúnmente utilizado en el sector bancario.

Exploit: software que utiliza las vulnerabilidades de los sistemas para tener acceso desautorizado.

Backdoor: permite el acceso de forma remota al sistema operativo.

[14] Instituto Nacional de Tecnologías de la Comunicación [En linea] <http://www.inteco.es/Formacion/Amenazas/Virus/> [Citado 2013]

Rootkit: obtiene el control de administrador en los sistemas, obteniendo los privilegios del mismo para realizar la acción que desee.

Así como los mencionados anteriormente existen más codificaciones malintencionadas que buscan poner en riesgo la seguridad de los sistemas, por esta razón se debe tener precaución a la hora de navegar en la red e interactuar con información de dispositivos extraíbles que son los principales causantes de la infección de equipos.

3.2.2 CLASES DE ATAQUES [15]

Los ataques informáticos se pueden clasificar en dos clases:

- PASIVOS:

Son ataques que buscan obtener información que es transmitida en una red, con el fin de:

- Copiar información
- Analizar el tráfico (intercepción de identidad): lectura de cabeceras permitiendo la identificación de origen y destinatario.

- ACTIVOS

Este tipo de ataque implica la modificación del flujo de datos transmitidos o la creación de un falso flujo de datos. A su vez, los ataques activos se dividen en:

- Suplantación de identidad (falsificación de identidad): fingir ser otra identidad o clonar una identidad. Como se observa en la Figura 3 en esta clase de ataques Darth (el atacante) se hace pasar por Bob para enviar un mensaje a Alice.

[15] STALLINGS, William. Cryptography and Network Security. Prentice Hall Press,2005. 592 p.

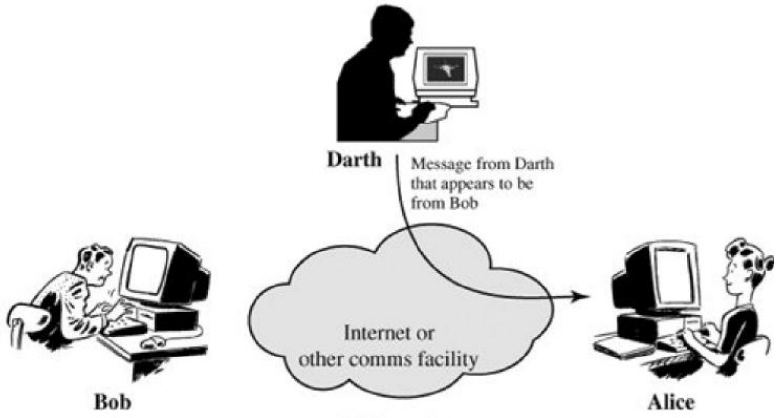


FIGURA 3. Suplantación[16]

- Repetición (Reactuación): retransmitir mensajes con el fin de provocar fallas en el sistema. En la Figura 4 se puede observar la manera en que funciona este ataque; Bob envía un mensaje a Alice (victima) sin saber que Darth (atacante) captura los mensajes para retransmitirlos posteriormente.

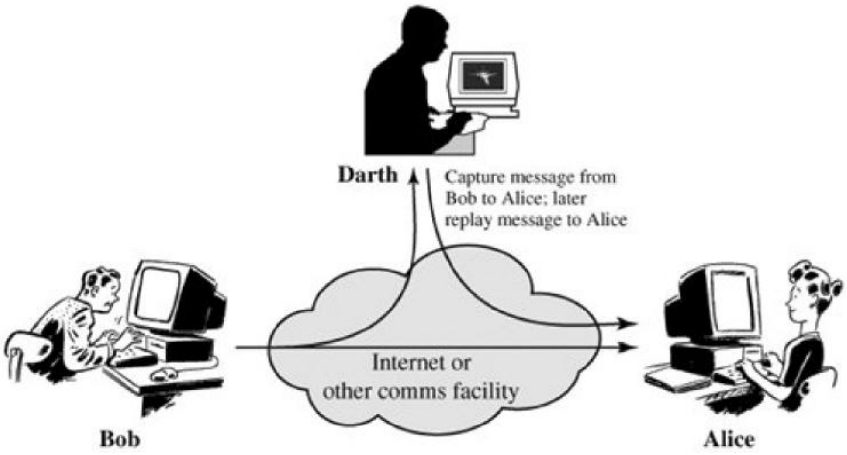


FIGURA 4. Repetición[17]

- Modificación de mensajes (alteración de mensajes): alterar, retrasar, reordenar la información. En el ataque descrito en la Figura 5 se observa la manera en que funciona este ataque; Bob envía un mensaje a Alice

[16] STALLINGS, William. Cryptography and Network Security. Prentice Hall Press,2005. 592 p.
[17] STALLINGS, William. Cryptography and Network Security. Prentice Hall Press,2005. 592 p

(victima) sin saber que Darth (atacante) captura los mensajes con el fin de modificarlos y enviarlos posteriormente para causar fallas en el sistema.

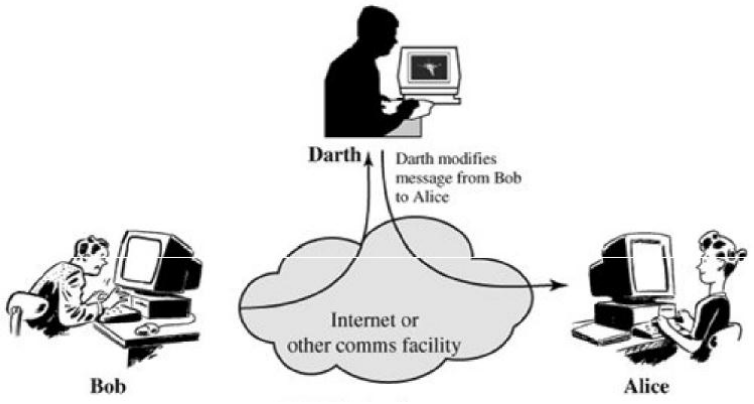


FIGURA 5. Modificación de paquetes[18]

- Interrupción de servicio :dejar fuera de servicio algún recurso del sistema (denegación de servicios) (ver figura 6)

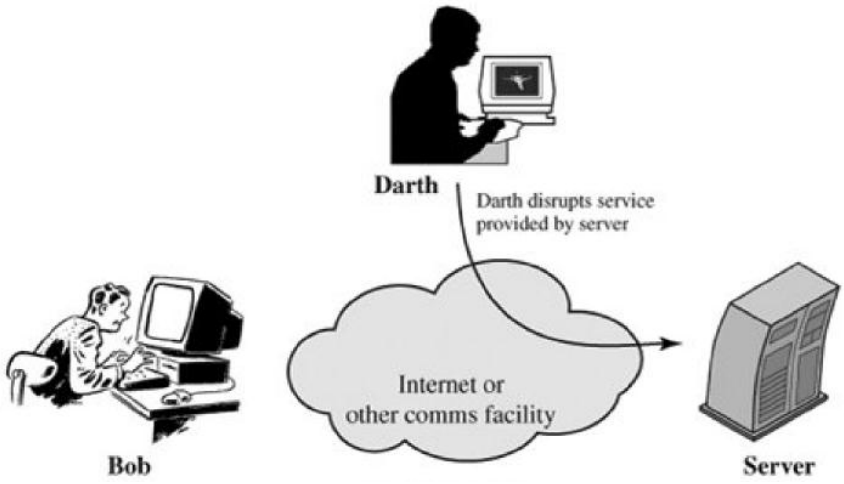


FIGURA 6. DoS[19]

[18] STALLINGS, William. Cryptography and Network Security. Prentice Hall Press,2005. 592 p
[19] Introducción a la seguridad. [en línea] <http://jcef.sourceforge.net/doc/introsecurity.pdf> [citado en 2012]

3.2.3 PROGRAMAS PARA ATACAR UNA RED

3.2.3.1 WireShark[20]

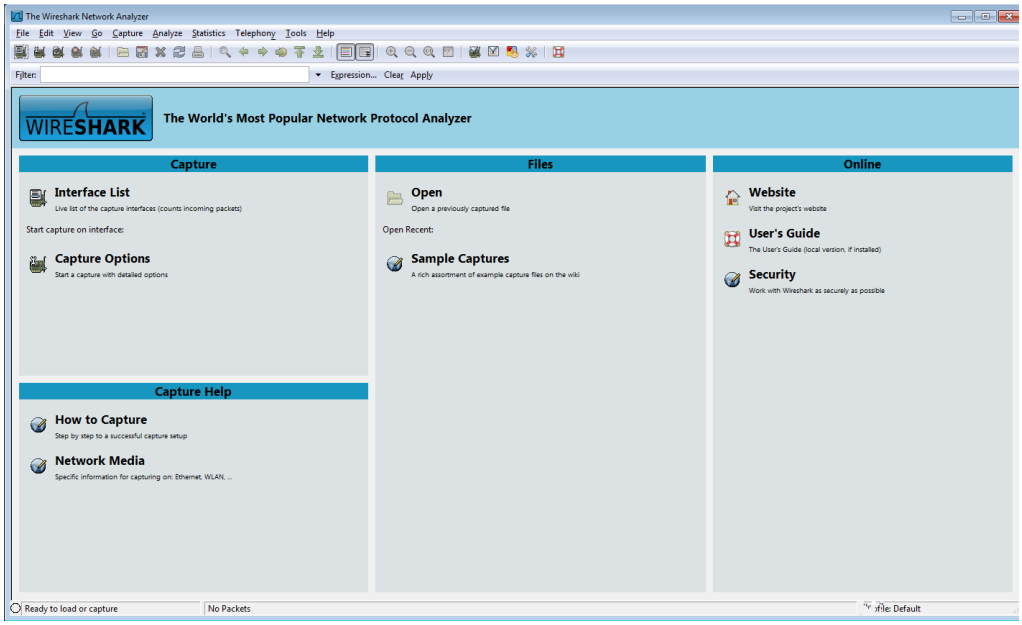


FIGURA 7. Entorno WireShark

Es un software libre implementado para análisis, solución y prevención de problemas en redes de comunicación mediante la captura de tráfico que circula por medio de la red, con la cual se pueden hacer los análisis respectivos utilizando las herramientas de wireshark, algunas de las formas de análisis son:

a. La forma más sencilla es con la ventana donde se visualiza el tráfico, ya que en dicha ventana se puede evidenciar la dirección IP de origen, dirección IP destino, el tipo de protocolo que transporta, descripción breve de la función del paquete y la información útil del paquete.

Para la captura de los datos en la red se debe configurar el modo promiscuo (Ver Figura 8) para lograr visualizar los datos de toda la red y no únicamente los del ordenador desde el cual se ejecuta la acción.

[20] CHAPPELL,Laura. Wireshark Network Analisis 2nd edition,Chappell University,2012, 1094 p.

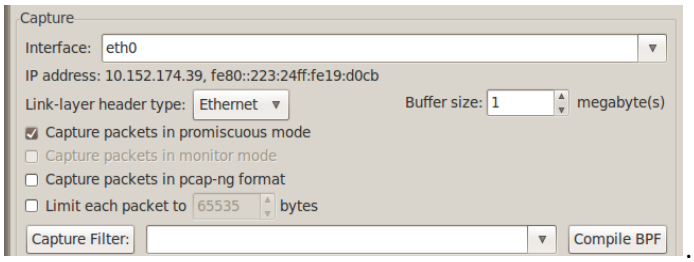


FIGURA 8. Configuración captura de datos

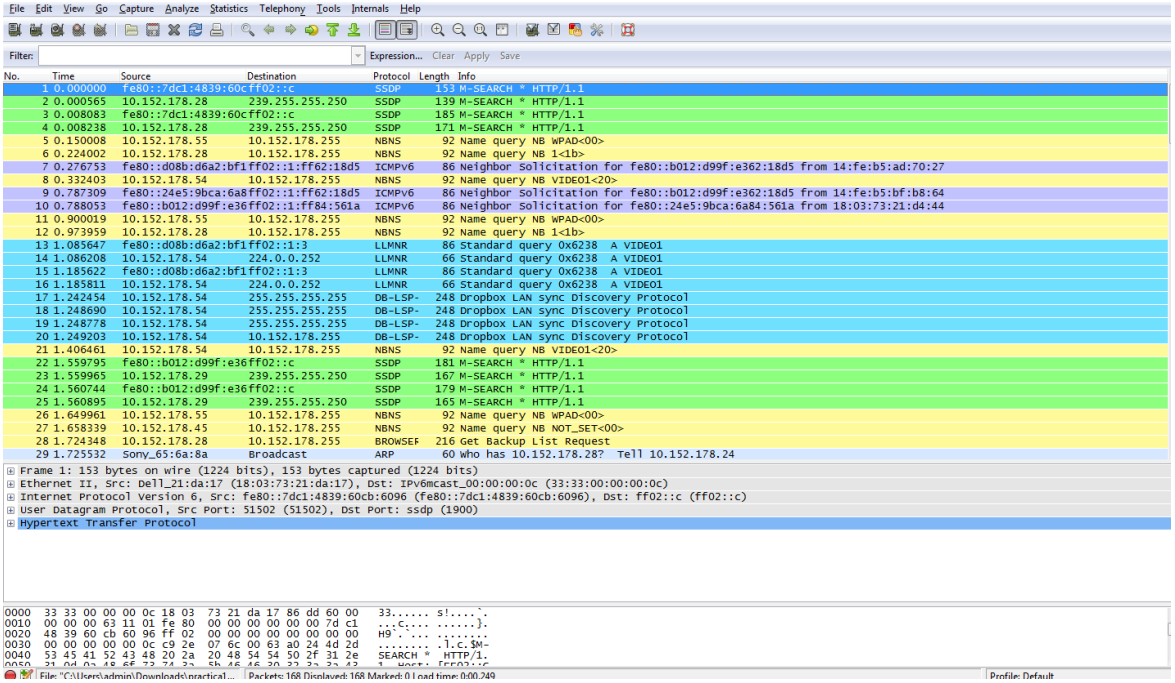
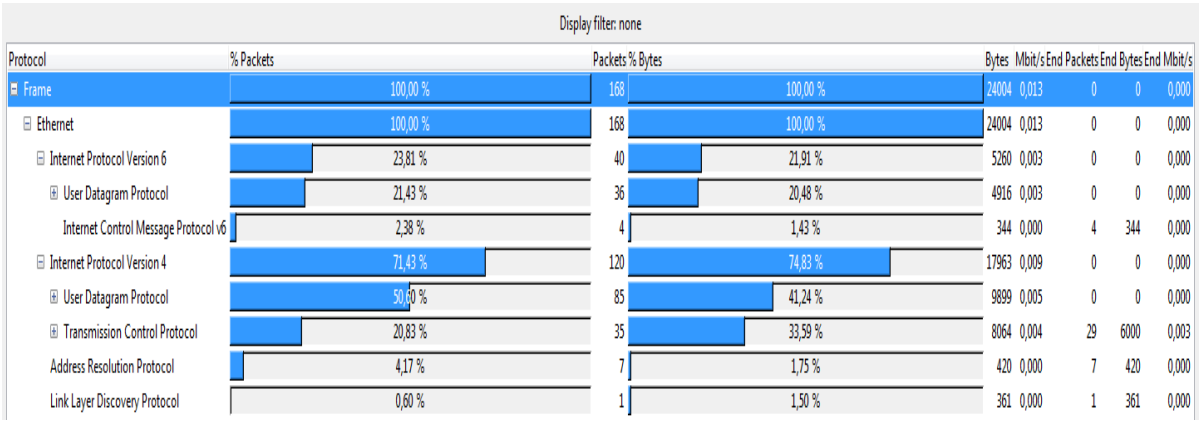


FIGURA 9. Visualización de datos capturados

b. Otra forma es mediante “Protocol hierarchy”,con el uso de esta herramienta se puede observar el árbol de protocolos (Ethernet, IP, TCP, UDP, protocolos de aplicaciones, ARP, PPP)



Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	168	100,00 %	24004	0,013	0	0	0,000
Ethernet	100,00 %	168	100,00 %	24004	0,013	0	0	0,000
Internet Protocol Version 6	23,81 %	40	21,91 %	5260	0,003	0	0	0,000
User Datagram Protocol	21,43 %	36	20,48 %	4916	0,003	0	0	0,000
Internet Control Message Protocol v6	2,38 %	4	1,43 %	344	0,000	4	344	0,000
Internet Protocol Version 4	71,43 %	120	74,83 %	17963	0,009	0	0	0,000
User Datagram Protocol	50,60 %	85	41,24 %	9899	0,005	0	0	0,000
Transmission Control Protocol	20,83 %	35	33,59 %	8064	0,004	29	6000	0,003
Address Resolution Protocol	4,17 %	7	1,75 %	420	0,000	7	420	0,000
Link Layer Discovery Protocol	0,60 %	1	1,50 %	361	0,000	1	361	0,000

FIGURA 10. Protocol Hierarchy

c. Otra herramienta para análisis de paquetes en la red son las gráficas del tráfico en función del tiempo.

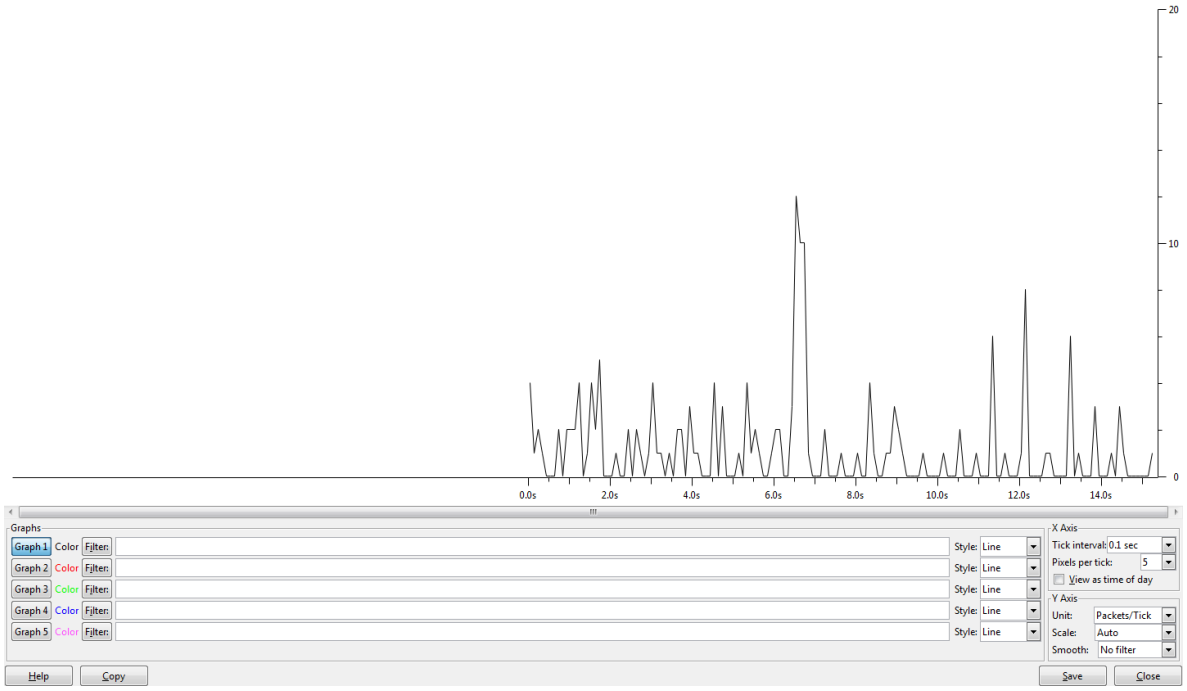


FIGURA 11. Análisis del tráfico en función del tiempo

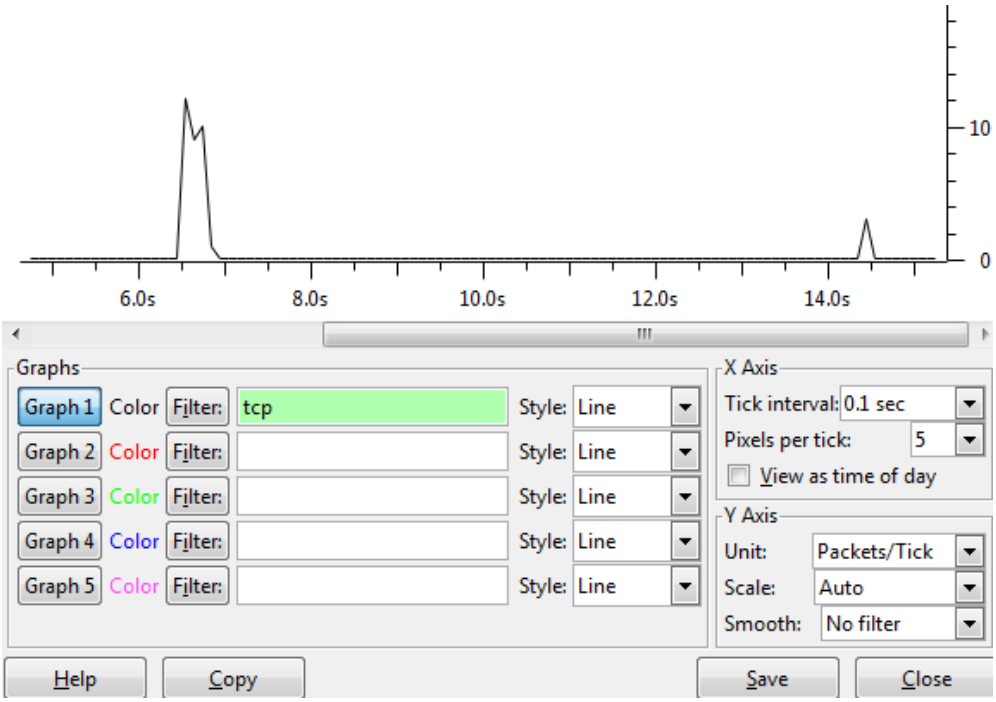


FIGURA 12. Filtrado de paquetes

3.2.3.2 SCAPY[21]

Scapy es una herramienta para manipular paquetes desarrollada con el lenguaje Phyton con la cual se puede codificar, decodificar, enviar y capturar paquetes en una red, además mediante este software es posible escanear características y vulnerabilidades de las redes permitiendo realizar ataques con gran facilidad.

3.2.3.3 NetDiscover

Es una herramienta que reconoce las direcciones activas dentro de una red, desarrollada generalmente para redes Wireless que no tengan un servidor DHCP, pero también es usada en redes que cuenten con hub /switch cableados.

NetDiscover permite encontrar de manera rápida las direcciones IP que se encuentren asociadas a la red en la que se encuentra ejecutando la operación de búsqueda.[22]

[21] MAXWELL, Adam. The very unofficial dummies guide to scapy. Enero 2012;p47
[22] Netdiscover [en línea] < http://nixgeneration.com/~jaime/netdiscover/> [citado en 2013]

3.2.3.4 Metasploit

Es una aplicación desarrollada para verificar posibles problemas de seguridad, mostrando las diferentes vulnerabilidades presentes en los diferentes sistemas operativos que se encuentran en circulación actualmente Su fin es proporcionar un conocimiento sobre los riesgos existentes e impulsar la innovación de herramientas capaces de mitigar estos peligros. Las exploraciones se realizan en diferentes áreas, incluyendo las aplicaciones web, contraseñas y la llamada ingeniería social.[23]

3.2.3.5 NMAP

Nmap es una herramienta de exploración de redes y de sondeo de puertos, lo que permite verificar el nivel de seguridad de un equipo, diseñado para analizar redes grandes a una rápida velocidad. Sin embargo, también funciona bien para el análisis de un solo computador. Opera enviando paquetes IP para determinar qué equipos se encuentran disponibles en una red, qué servicios ofrecen, los sistemas operativos que manejan o que tipos de firewalls se están usando en esta, lo que permite monitorear los servicios y la disponibilidad de los equipos.[24]

3.2.3.6 ZENMAP

Se define como la GUI de NMAP y permite un mayor entendimiento de los resultados obtenidos en los análisis a la red; además, diferencia de manera más eficiente los equipos seguros de los que no lo son y le da al atacante una idea más clara de que camino elegir para penetrar la red, para acceder a este basta con dirigirse al terminal y digitar el comando *zenmap* (Ver Figura 13).[25]

[23] MAYNOR,David. Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulenrability Research. Elsevier Inc, 2007; pag 1-64.
[24] OREBAUGH ,Angela. Nmap in the Enterprise: Your guide to network scanning. Elsevier Inc, 2008; pag 33-62.
[25] OREBAUGH, Angela. Nmap in the Enterprise: Your guide to network scanning. Elsevier Inc, 2008; pag 137-169.

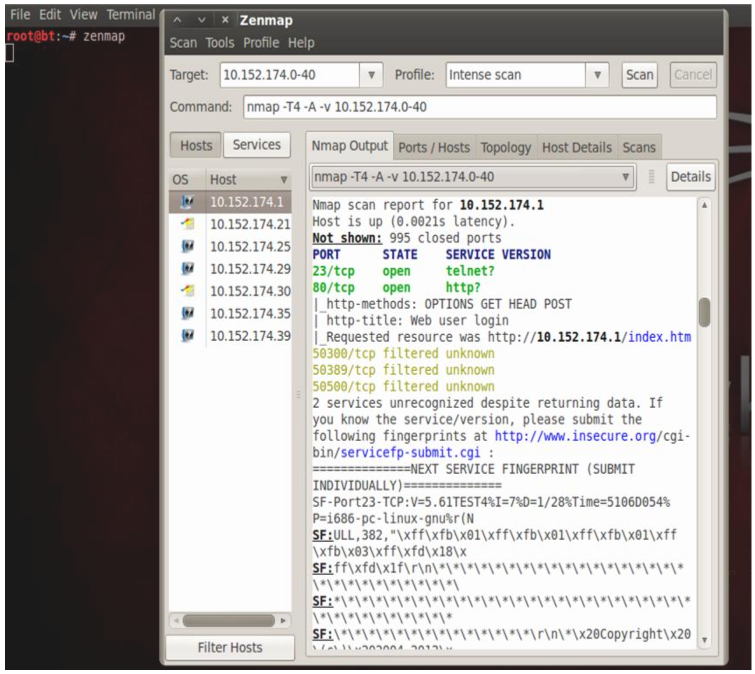


FIGURA 13. Análisis con Zenmap

3.2.3.7 ETTERCAP

Es una herramienta que permite realizar un ataque de escucha y modificación de paquetes a un objetivo específico, más conocido como ataque *man in the middle*. Para lograr esto, Ettercap cuenta con un complemento que permite realizar filtros para modificar la información de la víctima, dependiendo de las necesidades que se tengan estos filtros pueden ser programados o descargados de diferentes sitios, para su posterior compilación y ejecución, en este ejemplo exclusivamente se utiliza ettercap para escuchar las diferentes paginas donde la victima entra.[26]

Con tal fin se accede al menú de ayuda y se configura, dependiendo de la necesidad, cada una de las opciones a manejar.

[26] FAIRCLOTH, Jeremy. Network devices. EN: Penetration Tester's Open Source Toolkit. SYNGRESS, 2011; Pag 259-290.

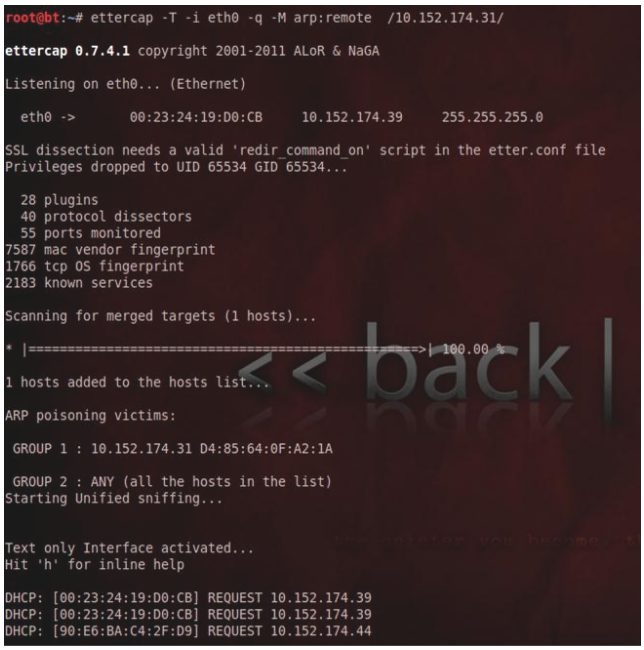


FIGURA 14. Detección de paquetes con ettercap

3.2.3.8 MACCHANGER

Es una herramienta que permite el cambio de dirección MAC; esto es funcional cuando dentro de una red se tiene una lista de permitidos, se puede complementar con otras aplicaciones con el fin de realizar un ataque de suplantación.

Para poder realizar el cambio de dirección mac, se requiere inicialmente dejar el equipo sin conexión, para esto se utiliza el comando *ifconfig eth0 down, P*osterior a esto, se procede a realizar el cambio de MAC; si no se conocen las extensiones del comando para realizar este cambio se accede a la ayuda con el comando *macchanger --help.*

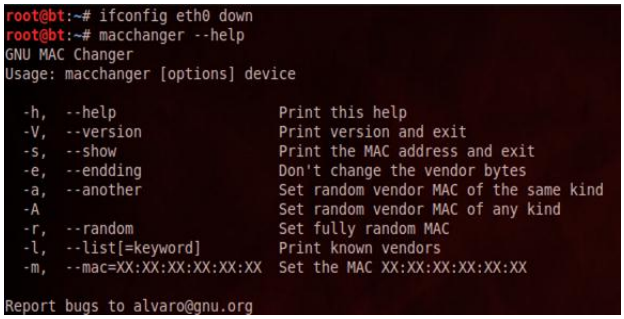


FIGURA 15. Menú de ayuda macchanger

Una vez familiarizado con el comando, se procede a realizar el cambio de dirección MAC con el comando de la figura 16.

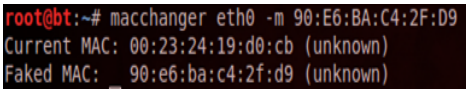


FIGURA 16. Comando macchanger

Una vez realizado este cambio se procede a reconectar el puerto a internet mediante el comando *ifconfig eth0 up* y se trabaja normalmente con esta dirección MAC. En caso de perder acceso a la red, aún cuando ya se encuentra encendido el puerto, digitar el comando *dhclient*, El cual asigna la dirección IP correcta.

3.2.4 Ataques Realizados a las redes industriales.

La vulnerabilidad de las redes industriales se ha hecho evidente en la última década, ya que los ataques a estas han venido en aumento. Ejemplos claros de estos son el STUXNEX y NIGTH DRAGON, cuyo fin es extraer y modificar archivos fundamentales para el correcto funcionamiento de la red.

3.2.4.1 STUXNET

Stuxnet es un virus informático diseñado para afectar sistemas industriales, descubierto el 17 de junio del 2010. Este gusano está condicionado para atacar equipos con sistema Windows ya que posee firmas certificadas por Realtek y JMicron que permiten la instalación transparente del gusano ofreciéndole al atacante la posibilidad de espiar y reprogramar los procesos industriales. Este virus es el primero con propiedades rootkit y enfatizado en sistemas de control, permitiendo las modificación de parámetros del sistema y además ocultando su presencia para no ser detectado, lo que dificulta la defensa de la red.

Tras la creación del virus, se especuló sobre sus orígenes y la forma como surgió pero mediante un comunicado, el New York Times confirmó que el virus informático fue desarrollado y financiado por Estados unidos e Israel con el fin de atacar las centrales nucleares de Irán, aunque la infección logro expandirse a otros países en el 2010.[27]

[27] GOLD, Steve. Stuxnet may be the work of state-backed hackers . EN: Network Security. Septiembre de 2010; pag 2 y 19.

En agosto de 2010 la empresa de seguridad Symantec dió a conocer información sobre los ordenadores infectados en diferentes países.

País	Ordenadores infectados
Irán	62.867
Indonesia	13.336
India	6.552
Estados Unidos	2.913
Australia	2.436
Gran Bretaña	1.038
Malasia	1.013
Pakistán	993
Alemania	15

Tabla 3. Ordenadores Infectados por Stuxnet

La propagación del gusano hacía uso de las vulnerabilidades del sistema Windows, los equipos eran infectados por medio de dispositivos extraíbles que contenían archivos .lnk que eran los encargados de infectar al equipo.

El virus detectado como Win32.Worm.Stuxnet infecta por igual a todos los sistemas basados en Windows atacando prioritariamente los sistemas SCADA (supervisory control and data acquisition) que tengan funcionando el software WinCC de Siemens.

Debido a la complejidad del problema generado por el ataque cibernético, BitDefender lanzó una herramienta que se encarga de eliminar todas las variantes conocidas de Stuxnet y aquellos rootkits que se implementaron para ocultar y darle privilegios al gusano.

Los problemas de seguridad informática cada día son más comunes por lo cual se deben contrarrestar para evitar consecuencias fatales. Alrededor de Stuxnet se han presenciado virus relacionados como Flame, Duqu, Stars, entre otros.

3.2.4.2 NIGHT DRAGON [28]

Este ataque tiene su origen en china y fue descubierto por la compañía McAfee en febrero del año 2011. Tenía como objetivo principal compañías de la industria petrolera, gas y petroquímica; su implementación aprovecha vulnerabilidades de Windows, cuentas de Active Directory y herramientas de administración remota. Esta amenaza comprometió los servicios web, servidores de la red interna mediante infiltraciones a diferentes ordenadores obteniendo información confidencial de cuentas de acceso y correos de ejecutivos. A pesar de los accesos remotos, los dispositivos de control y operación no se vieron comprometidos en los ataques realizados.

3.2.5 Vulnerabilidades en equipos SCHNEIDER[29]

Los instrumentos Schneider se han visto afectados por problemas que comprometen la seguridad de las comunicaciones de los equipos, algunas de las vulnerabilidades confirmadas son:

- HTTP Server Buffer Overflow
- XSS (Cross site scripting)
- FTP Server Buffer Overflow

Una de las vulnerabilidades que más compromete la seguridad de los equipos es la no autenticación entre el software Unity pro M y el PLC. Esto sucede porque en la comunicación MODBUS, el controlador no soporta modos de protección para prevenir cambios en la programación y configuración del equipo dejando un vacío de protección que puede generar consecuencias relevantes en la red industrial.

Estas vulnerabilidades fueron descubiertas durante una investigación de ciber-seguridad realizada por investigadores externos y de Schneider Electric. Hasta el momento no existe evidencia que estas vulnerabilidades hayan sido solucionadas.

---

[28] KNAPP,Eric. Industrial Network Security:Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress 2011; p 341.

[29] Important security notification – Quantum and Premium communication modules (ICSALERT-12-020-03) [en línea] < http://www.global-download.schneider-electric.com/mainRepository/EDMS_CORP7.nsf/69f5d72c7a0cf811c12573d800389503/05e789c0e6c47c6585257a63005d9d1f/$FILE/RES207378.pdf> [citado en 2013]

La recomendación que Schneider Electronic proporciona para proteger los equipos y la red industrial es la implementación de un firewall externo que permita mantener el control de flujo de la red, obtener limitaciones de acceso y establecer configuraciones que no permitan las modificaciones de los equipos de manera remota.

Se hace énfasis especial en los equipos SCHNEIDER, ya que se trabaja con un PLC fabricado por esta empresa, para obtener más información al respecto se anexa el documento facilitado por la empresa sobre las vulnerabilidades de sus equipos.

4. UTILIZACIÓN DE FIREWALLS EN LAS REDES

4.1 GENERALIDADES DE LOS FIREWALLS

4.1.1 Características y funcionalidades

- Es un filtro que se encarga de controlar el paso de información de una red, bloqueando el acceso no autorizado
- Bloquea el acceso a la red a personas y aplicaciones que no se encuentren autorizadas
- Puede ser configurado para permitir, limitar, cifrar, descifrar teniendo como base normas y criterios, lo que permite brindar seguridad y confianza en la operación de la red.
- Brinda una protección necesaria a la red pero puede ser insuficiente para cubrir la gran cantidad de problemas de seguridad.
- Un firewall puede ser configurado en hardware o software de acuerdo a las condiciones de funcionamiento y criterios de funcionalidad establecidos.

4.1.2 Criterios de funcionamiento de los firewalls

- Service Control :

Determina a que servicios de internet se puede acceder, entrando o saliendo, la función del firewall es la de filtrar el tráfico en base a la dirección IP y al número del puerto TCP.

- Direction Control:

Determina la dirección en la que las solicitudes de servicio particular pueden ser inicializadas para fluir a través del firewall

- User Control:

Control de acceso de un servicio de acuerdo a que usuario está tratando de acceder a él. Aplicado típicamente a usuarios dentro del perímetro del firewall, conocidos como usuarios locales.

- Behavior Control:

Controla como se utilizan determinados servicios presentes en la red y quien puede acceder a ellos.[30]

4.1.3 Limitaciones de un firewall

- Un firewall no puede proteger de ataques en sectores de la red donde no se aplique.
- El firewall no puede proteger de las amenazas a las que está sometida la red por parte de usuarios permitidos en el uso interno.
- El cortafuego no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen en Internet.

4.1.4 Firewalls más comunes

- Firewall de filtrado de paquetes: es un filtro de paquetes basado en la inspección de origen, destino y dirección MAC.
- Firewall de aplicación: no permite el tráfico directo entre dos redes, este tipo de firewall inspecciona la información de cada paquete de la red. Para este tipo de cortafuego se implementan los proxy.
- Firewall personal: firewall implementado por software mediante computadoras filtrando la comunicación entre el computador y el resto de la red.[31]

---

[30] Kamara,Seny. Analysis of vulnerabilities in Internet firewalls [en línea]. < http://www.sciencedirect.com.consultaremota.upb.edu.co/science/article/pii/S0167404803003109 > [citado en 6 de mayo 2012]

[31] Stojanovski,Nenad.Architecture of a Identity based firewall system.[en linea] <http://airccse.org/journal/nsa/0711ijnsa03.pdf >[citado en 5 de mayo de 2012]

4.1.5 Filtrado de paquetes

Un firewall de filtrado de paquetes tiene como función el enrutamiento de la red interna y externa basándose en políticas y condiciones establecidas de acuerdo a parámetros de los paquetes como dirección IP de origen y destino, puertos implementados, protocolos e información del tipo de paquete, de esta forma el firewall controla el flujo de la comunicación en la red.

Comúnmente en la redes al implementar un firewall bloquean las conexiones entre la red externa e interna exceptuando algunos servicios que resultan necesarios, con el fin de evitar servicios que puedan alterar el comportamiento de la red interna[32].

4.2 ARQUITECTURAS[33]

4.2.1 Arquitectura Dual-Homed Host

Este tipo de firewall implementa dos interfaces de red que permiten aislar una red interna de una red externa no confiable como internet. El aislamiento se realiza mediante el bloqueo total del tráfico IP entre dichas redes. Esta arquitectura de firewall debe tener el enrutamiento inhabilitado y la única ruta entre los segmentos de red es por medio de la función de capa de aplicación(Ver Figura 17).

[32] FIREWALLS [en línea] <http://spi1.nisu.org/recop/al01/dulzon/index.html> [citado en 2013]
[33] ZWICKY, Elizabeth. O'Reilly Media, Inc, USA; Edición: 2nd Revised edition ,O'reilly, 2000, 896 p.

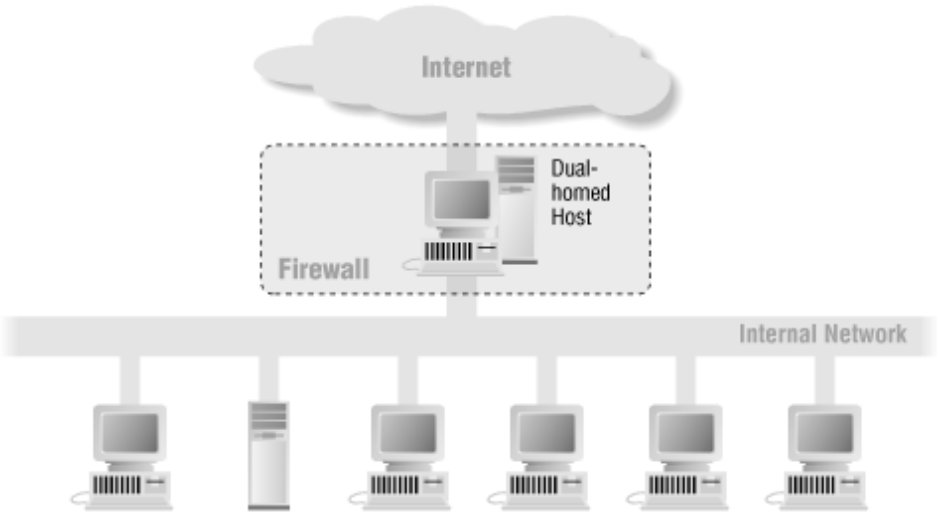


FIGURA 17.Arquitectura Dual-homed Host

4.2.2 Arquitectura Screened Host

Este tipo de firewall provee un nivel de seguridad por medio del filtrado de paquetes combinando un *screening router*, que es el encargado de realizar el filtrado de paquetes, con un *bastion host,* que es configurado especialmente para resistir los posibles ataques. La configuración establecida permite que el *bastion host* sea el único sistema de la red interna que puede interactuar con la red externa; en cuanto al filtrado de paquetes, el host establece las comunicaciones permitidas por medio de políticas de seguridad (Ver Figura 18).

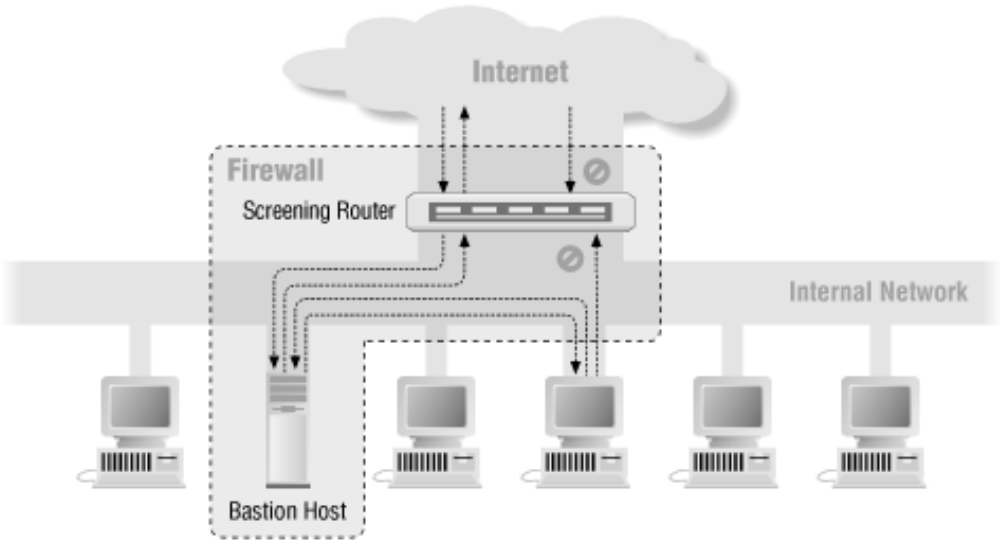


FIGURA 18.Arquitectura Screening Router

4.2.3 Arquitectura Screened Subnet

En este caso se crea una subred entre la red interna y externa con el fin de fortalecer la seguridad, ya que en el caso de la arquitectura anterior la seguridad dependía del *bastion host* y si se encuentran vulnerabilidades en el mismo se puede colocar en riesgo la red interna. Este tipo de arquitectura resulta muy segura pero aumenta la complejidad de su implementación y configuración.Para emplear este sistema es necesario tener un router exterior para bloquear el tráfico no deseado en ambos sentidos, también se debe usar un router interior que bloquea el tráfico no deseado tanto hacia la subred como hacia la red interna (Ver Figura 19).[34]

[34] HUNT, Ray. Internet/Intranet firewall security-policy, architecture and transaction services. EN: Computer Communications. N° 21 (Septiembre de 1998); pag 1107-1123.

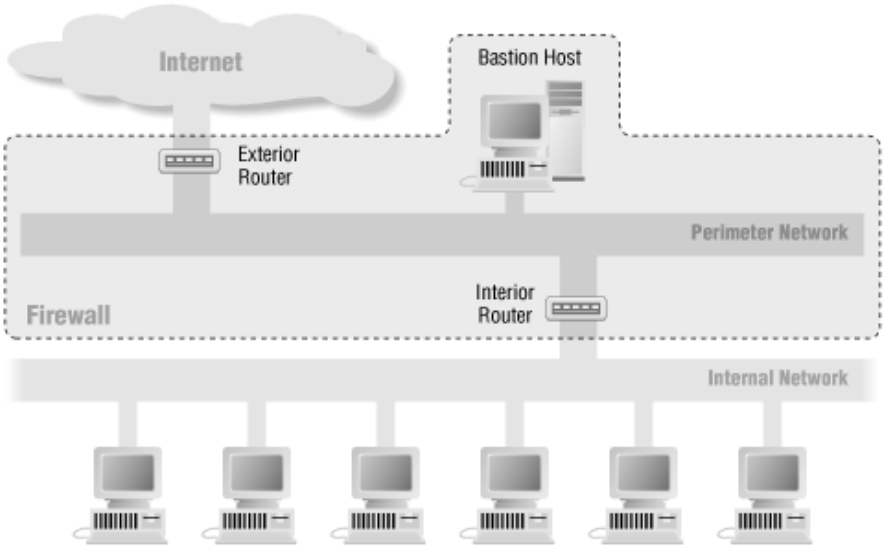


FIGURA 19.Arquitectura Screened Subnet

4.3 FIREWALL CON LINUX

Iptables es una herramienta construida sobre netfilter que permite filtrar paquetes, realizar traducciones de red para IPv4 y mantener registros. Iptables se usa para la creación de firewalls que se vinculan al kernel de linux donde el administrador puede definir políticas de filtrado de paquetes que pasan a través de la red. Para implementa un firewall con la herramienta iptables se debe realizar el siguiente procedimiento[35].

Vaciar reglas:

```
root@bt:~# iptables -F
root@bt:~# iptables -X
root@bt:~# iptables -t nat -F
root@bt:~#
```

FIGURA 20.Vaciado de reglas en iptables

Establecer políticas determinadas, esta serie de comandos se deben implementar cada vez que se quiere configurar un nuevo firewall con iptables:

[35] Stanger, James. Hack Proofing Linux:The Only Way to Stop a Hacker Is to Think Like One, Elsevier Inc, 2001; pag 445-506.

FIGURA 21.Politicas predeterminadas del firewall

Para hacer la primera prueba se envió un ping por línea de comando a la URL www.google.com con el fin de mostrar la comunicación con el sitio web (Ver Figura 22).

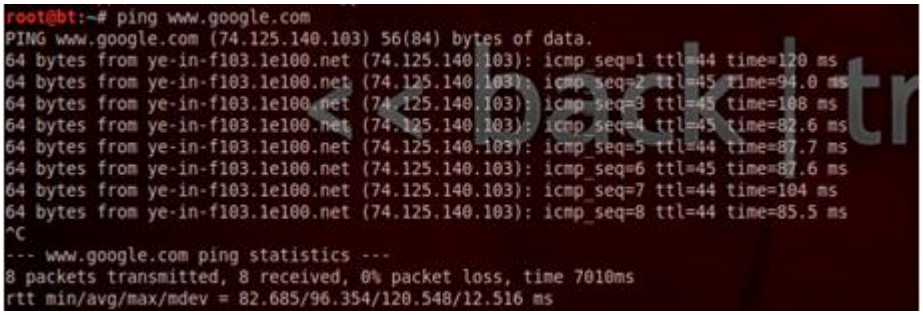


Figura 22.Prueba de comunicación con página web

Ahora se procede a restringir el acceso a la dirección IP que corresponde al URL mencionada con anterioridad bloqueando el tráfico con la misma, esta acción se realiza de la manera mostrada en la Figura 23:

FIGURA 23.Restriccíon a página web

Ahora se comprueba la comunicación enviando un nuevo ping a la IP de la URL (Ver Figura 24).

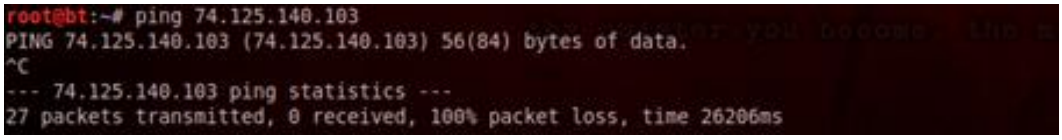


FIGURA 24.Prueba de comunicación con regla de iptables

Con iptables es posible bloquear el tráfico y el acceso a la red por medio de variedad de parámetros, a continuación se mostrara la forma de aplicar restricciones a protocolos específicos y puertos con el fin de fortalecer los puntos que hacen débiles las redes; en la figura 25 se muestra una regla de bloqueo al protocolo ICMP.

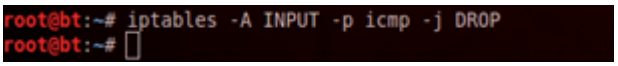


FIGURA 25. Bloqueo del protocolo ICMP

Como se puedo observar en la imagen es similar al caso anterior solo que –s es utilizado para indicar direcciones IP y –p es utilizado para dar acciones a un protocolo.

Cuando se envía un ping desde otro ordenador de la red este se encapsula en el protocolo ICMP, por esta razón la acción aplicada con anterioridad de comprueba enviando un ping al ordenador donde se configuró iptables (Ver Figura 26).

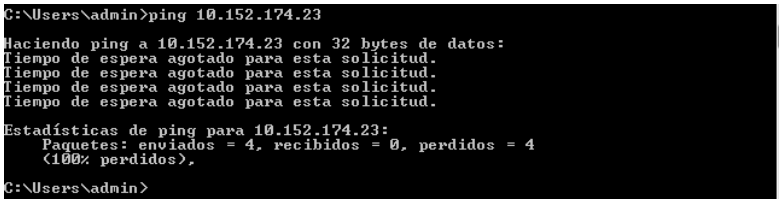


FIGURA 26. Prueba de comunicación protocolo ICMP

En la figura 27 se bloquearan 2 puertos que son utilizados comúnmente para atacar, la comprobación del filtro realiza mediante la implementación de NMAP.

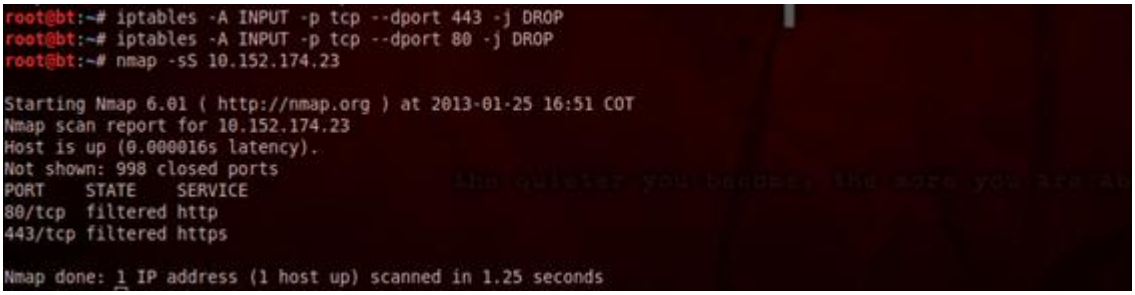


FIGURA 27. Prueba nmap

4.4 FIREWALLS COMERCIALES PARA REDES INDUSTRIALES

4.4.1 TOFINO FIREWALL[36]

Tofino Security fue fundada en 2006 por Eric Byres. El nombre de la compañía corresponde al de una pequeña ciudad en la isla de Vancouver. Tofino proporciona dispositivos prácticos y efectivos para controlar la seguridad en redes industriales y sistemas SCADA.

Uno de los productos ofrecidos por la compañía es Tofino Firewall LSM. La

[36] TOFINO Firewall [en línea] < http://www.tofinosecurity.com/products/Tofino-Firewall-LSM> [citado en 2013]

función principal de dicho firewall es realizar análisis y escaneo de tráfico para bloquear y reportar comunicaciones no autorizadas con el fin de tener el control de tráfico de la red basándose en una serie de reglas definidas por el operario mediante la cual se establece el trafico permitido (Ver Figura 28).

FIGURA 28 .Tofino Firewall

Tofino proporciona plantillas predefinidas para operar en 25 familias de controladores industriales, incluyendo reglas definidas para proteger los dispositivos con vulnerabilidades conocidas.

Con un funcionamiento similar pero aplicado a redes Modbus TCP la compañía provee el Tofino Modbus TCP Enforcer LSM (Ver Figura 29).

FIGURA 29. Tofino Modbus[37]

La compañía Tofino Security se encuentra relacionada con otras compañías

[37] Firewall MODBUS [en línea] <http://www.tofinosecurity.com/products/Tofino-Modbus-TCP-Enforcer-LSM> [citado en 2013]

establecidas en el sector industrial como MTL instruments, Honeywell, Invensys[38].

El producto ofrecido por Tofino en la actualidad es el Tofino 9211-ET (Ver Figura 30), dispositivo que va conectado entre el dispositivo de control y el Switch/Router de la red industrial, protegiendo, individualmente, a cada uno de estos dispositivos de posibles ataques mediante las reglas que vienen previamente programadas en el firewall[39].

FIGURA 30. Tofino 9211-ET[40]

4.4.2 SWITCH CON FIREWALL DE CISCO

Cisco es una empresa estadounidense que tiene su mercado enfatizado en la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones, ya sean routers, switches, hubs, firewalls, entre otros.

Esta compañía ofrece en el mercado un switch industrial configurable dedicado a redes MODBUS TCP, mediante el cual se puede establecer un sistema de seguridad mediante Access Control List (ACL) y que permite el trafico solamente de las direcciones IP de origen asignadas; de esta forma se logra contrarrestar los ataques de denegación de servicios.

La configuración se realiza de la siguiente forma:

interface Ethernet0/0

ip address 10.1.1.1 255.255.255.0

ip access-group 1 in

!

[38] Firewall MODBUS [en línea] <http://www.tofinosecurity.com/products/Tofino-Modbus-TCP-Enforcer-LSM> [citado en 2013]

[39] Datasheet EPS9211 [en línea] <http://www.mtl-inst.com/images/uploads/datasheets/tofino/EPS9211-ET.pdf> [citado en 2013]

[40] Datasheet EPS9211 [en línea] <http://www.mtl-inst.com/images/uploads/datasheets/tofino/EPS9211-ET.pdf> [citado en 2013]

access-list 1 permit 10.1.1.0 0.0.0.255

Con este switch también es posible limitar la velocidad del tráfico de paquetes, mejorando la calidad de servicio.

5. ANALISIS DE TRÁFICO EN LA RED

Para realizar la captura de los paquetes enviados en la comunicación servidor-PLC fue necesario instalar el software Wireshark en el servidor e iniciar la captura del tráfico a través puerto de comunicación del servidor durante 3.8 minutos, tiempo en el cual se estableció la conexión con el PLC. Se programó e interactuó con la interfaz del software Unity Pro M, que se encarga de la configuración y control del funcionamiento del PLC. Esta captura también puede ser realizada desde otro ordenador que se conecte a la red utilizando el modo promiscuo del Wireshark.

Los datos capturados fueron obtenidos en el laboratorio de automatización industrial, en la red basada en el protocolo MODBUS TCP.

No.	Time	Source	Destination	Protocol	Length	Info
30	20.852716000	192.168.10.10	192.168.10.3	Modbus/TCP	65	query: trans: 4; unit: 0, func: 90: Unknown function (90)
31	20.860778000	192.168.10.3	192.168.10.10	Modbus/TCP	112	response: trans: 4; unit: 0, func: 90: Unknown function (90)
32	20.868322000	192.168.10.10	192.168.10.3	Modbus/TCP	65	query: trans: 5; unit: 0, func: 90: Unknown function (90)
33	20.880842000	192.168.10.3	192.168.10.10	Modbus/TCP	173	response: trans: 5; unit: 0, func: 90: Unknown function (90)
34	20.899957000	192.168.10.10	192.168.10.3	Modbus/TCP	64	query: trans: 6; unit: 0, func: 90: Unknown function (90)
35	20.910789000	192.168.10.3	192.168.10.10	Modbus/TCP	130	response: trans: 6; unit: 0, func: 90: Unknown function (90)
36	20.970068000	192.168.10.10	192.168.10.3	Modbus/TCP	65	query: trans: 7; unit: 0, func: 90: Unknown function (90)
37	20.980705000	192.168.10.3	192.168.10.10	Modbus/TCP	77	response: trans: 7; unit: 0, func: 90: Unknown function (90)
38	21.009364000	192.168.10.10	192.168.10.3	Modbus/TCP	288	query: trans: 8; unit: 0, func: 90: Unknown function (90)
39	21.021373000	192.168.10.3	192.168.10.10	Modbus/TCP	288	response: trans: 8; unit: 0, func: 90: Unknown function (90)
40	21.050139000	192.168.10.10	192.168.10.3	Modbus/TCP	64	query: trans: 9; unit: 0, func: 90: Unknown function (90)
41	21.060789000	192.168.10.3	192.168.10.10	Modbus/TCP	130	response: trans: 9; unit: 0, func: 90: Unknown function (90)
42	21.093920000	192.168.10.10	192.168.10.3	Modbus/TCP	64	query: trans: 10; unit: 0, func: 90: Unknown function (90)
43	21.100855000	192.168.10.3	192.168.10.10	Modbus/TCP	130	response: trans: 10; unit: 0, func: 90: Unknown function (90)
44	21.118385000	192.168.10.10	192.168.10.3	Modbus/TCP	73	query: trans: 11; unit: 0, func: 90: Unknown function (90)
45	21.130909000	192.168.10.3	192.168.10.10	Modbus/TCP	167	response: trans: 11; unit: 0, func: 90: Unknown function (90)
46	21.149565000	192.168.10.10	192.168.10.3	Modbus/TCP	73	query: trans: 12; unit: 0, func: 90: Unknown function (90)

12334	232.792218000	192.168.10.3	192.168.10.10	TCP	64	asa-appl-proto > ams [ACK] Seq=126694 Ack=104302 Win=4096 Len=0 [ETHERNET
12335	232.793249000	192.168.10.3	192.168.10.10	Modbus/TCP	64	response: trans: 5879; unit: 0, func: 90: Unknown function (90)
12336	232.813656000	192.168.10.10	192.168.10.3	Modbus/TCP	74	query: trans: 5880; unit: 0, func: 90: Unknown function (90)
12337	232.822792000	192.168.10.3	192.168.10.10	Modbus/TCP	64	response: trans: 5880; unit: 0, func: 90: Unknown function (90)
12338	232.860498000	192.168.10.10	192.168.10.3	Modbus/TCP	68	query: trans: 5881; unit: 0, func: 90: Unknown function (90)
12339	232.872773000	192.168.10.3	192.168.10.10	Modbus/TCP	71	response: trans: 5881; unit: 0, func: 90: Unknown function (90)
12340	232.891793000	192.168.10.10	192.168.10.3	Modbus/TCP	74	query: trans: 5882; unit: 0, func: 90: Unknown function (90)
12341	232.902832000	192.168.10.3	192.168.10.10	Modbus/TCP	78	response: trans: 5882; unit: 0, func: 90: Unknown function (90)
12342	232.923049000	192.168.10.10	192.168.10.3	Modbus/TCP	81	query: trans: 5883; unit: 0, func: 90: Unknown function (90)
12343	232.932785000	192.168.10.3	192.168.10.10	Modbus/TCP	64	response: trans: 5883; unit: 0, func: 90: Unknown function (90)
12344	233.001123000	192.168.10.10	192.168.10.3	Modbus/TCP	68	query: trans: 5884; unit: 0, func: 90: Unknown function (90)

FIGURA 31. Datos capturados en la red

Como se puede observar en las imágenes anteriores se capturaron 12344 paquetes en 233 segundos (3.8 minutos), dichos paquetes muestran la comunicación entre las direcciones IP 192.168.10.10 y 192.168.10.3 que corresponden al servidor y PLC respectivamente.

- Análisis de datos mediante la herramienta jerarquía de protocolos de Wireshark

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	12344	100,00 %	975526	0,033	0	0	0,000
Ethernet	100,00 %	12344	100,00 %	975526	0,033	0	0	0,000
Logical-Link Control	0,11 %	14	0,07 %	728	0,000	0	0	0,000
Internetwork Packet eXchange	0,11 %	14	0,07 %	728	0,000	0	0	0,000
Internet Protocol Version 4	99,81 %	12321	99,87 %	974266	0,033	0	0	0,000
User Datagram Protocol	0,52 %	64	0,62 %	6046	0,000	0	0	0,000
NetBIOS Name Service	0,51 %	63	0,59 %	5796	0,000	63	5796	0,000
NetBIOS Datagram Service	0,01 %	1	0,03 %	250	0,000	0	0	0,000
Transmission Control Protocol	99,30 %	12257	99,25 %	968220	0,033	521	32714	0,001
Modbus/TCP	95,07 %	11736	95,90 %	935506	0,032	0	0	0,000
Address Resolution Protocol	0,07 %	9	0,05 %	532	0,000	9	532	0,000

FIGURA 32. Datos jerarquizados mediante wireshark

En la Figura 32 se puede visualizar la totalidad de paquetes enviados por protocolo de los datos capturados. Se puede comprobar que el protocolo que usa la red para la comunicación es Modbus TCP que corresponde al 95.07 % del número total de paquetes.

- Mediante la gráfica del ancho de banda en función del tiempo se puede visualizar como es la utilización del canal de comunicación a través del tiempo.

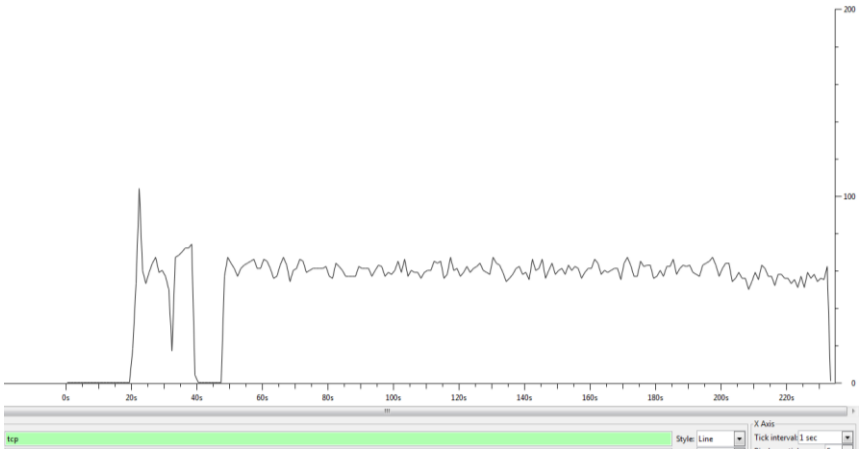


FIGURA 33. Bits a través del tiempo

Los paquetes de los datos contienen parámetros similares a otras comunicaciones que se pueden visualizar mediante wireshark.

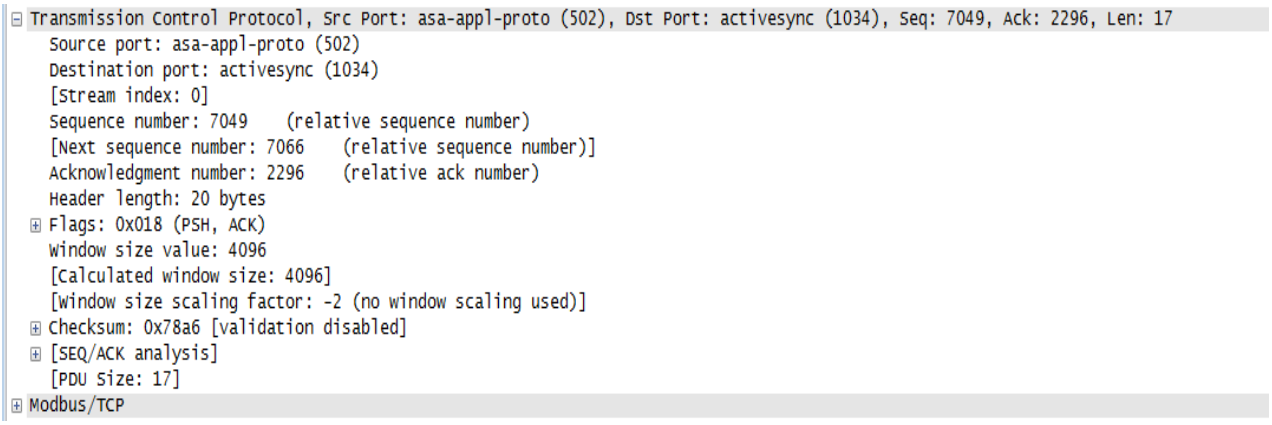


FIGURA 34. Parametros de los paquetes obtenidos

Como se observa en la figura 34, en la información de parámetros del paquete que se está visualizando en la imagen, se puede notar que el paquete sale de PLC (192.168.10.3) utilizando el puerto 502 y llega al servidor (192.168.10.10) mediante el puerto 1034.

Como se puede observar, se siguen implementando los mismos puertos de comunicación en los dispositivos, de esta manera se logra identificar que el puerto que utiliza el PLC es el 502, mientras que el servidor implementa el 1034, por lo tanto se puede deducir que mediante dichos puertos se realizan los procesos de control, programación, e interacción servidor-PLC

6. ETAPAS DE DESARROLLO

Para la realización del proyecto fue necesario fundamentar el conocimiento con la ayuda de libros y publicaciones, ya que el tema de seguridad en redes industriales, utilizando firewalls, no se ha aplicado con fortaleza en la actualidad[41], por esta razón no fue posible encontrar soportes físicos de funcionamiento de sistemas de seguridad aplicados. Resulta de gran importancia tener bases fuertes

[41] Ralston,Patricia. Cyber security risk assessment for SCADA and DCS networks [en línea].<http://www.sciencedirect.com.consultaremota.upb.edu.co/science/article/pii/S0019057807000754> [citado en 6 de mayo 2012]

en el conocimiento de redes, especialmente en la comunicación MODBUS TCP que resulta siendo el foco principal del proyecto.

Este proyecto se realizó con la colaboración del Laboratorio de Automatización industrial de la Escuela de Ingeniería, el cual prestó el prototipo de red industrial basada en el protocolo Modbus/TCP. También se contó con equipos del laboratorio de Redes de Telecomunicaciones de la Facultad de Ingeniería Electrónica (sistema NetFPGA).

6.1 Diseño

7. Estudio de las herramientas de ataque

Las herramientas para realizar ataques, previamente reseñadas en la sección 3.2.3, permiten obtener datos y manipular equipos en cualquier clase de red. Para poder entender plenamente como funciona cada una de estas herramientas, y las diversas opciones que manejan, se realizaron algunas pruebas, las cuales son descritas a continuación.

7.1 Pruebas con SCAPY[42]

7.1.1 Instalación de SCAPY

Para la utilización de la herramienta Scapy se debe iniciar descargando e instalando el programa para esto es recomendado un ordenador con Linux Backtrack, ya que este posee mayor practicidad para aplicación en redes. Para el proceso de instalación debe dar los siguientes comandos:

$ cd /tmp

$ wget scapy.net

$ unzip scapy-latest.zip

$ cd scapy-2.*

$ sudo python setup.py install

[42] MAYNOR, David. Syngress Force Emerging Threat Analysis. Elsevier Inc, 2006; pag 577-596

Una vez instalado se puede iniciar Scapy de la siguiente forma

$ sudo scapy

7.1.2 Creación de paquetes con scapy[43]

Scapy le permite al usuario crear paquetes con características determinadas que se adecuen a la necesidad de la red mediante el establecimiento de parámetros.

Para iniciar la creación de paquetes se debe establecer inicialmente los parámetros de la capa IP en la cual se introduce la dirección de origen (se puede seleccionar cualquier dirección, lo que facilita la suplantación) y la dirección destino del paquete. Para tal fin se utiliza el comando *capa_IP=IP(src="dirección origen",dst="dirección destino")*(ver Figura 35).

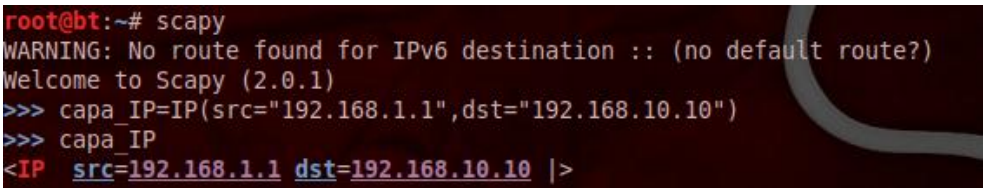


FIGURA 35.Modificación capa_IP

Luego de la capa IP se debe modificar la capa TCP en caso de crear un paquete con dicho protocolo, aunque también puede ser UDP o ICMP, en dicha capa se establece el puerto de origen y destino del paquete (Ver Figura36).

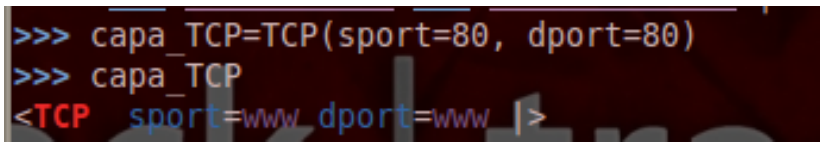


FIGURA 36.Modificación capa_TCP

Luego se guarda el mensaje que va contener el paquete (ver Figura 37).

FIGURA 37.Creación payload

[43] Manipulación avanzada de paquetes TCP/IP con scapy.[en línea]<http://www.hackxcrack.es/cuadernos/tcpip2/> [citado en 2013]

Por último se arma el paquete para ser enviado para esto se debe usar “/” para unir las capas creadas (ver Figura 38).

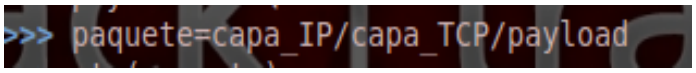
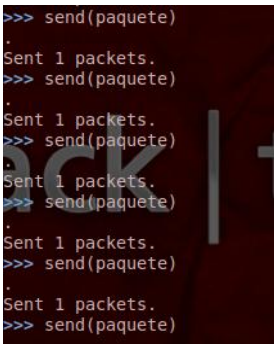


FIGURA 38.Creación del paquete

El envío del paquete se hace mediante el comando SEND, como se observa en la figura 39.



FGIURA 39. Envió del paquete

Para comprobar el funcionamiento del ataque se visualizan mediante wireshark los paquetes que salen del ordenador 192.168.1.1 en el cual se armó el paquete (ver Figura 40).

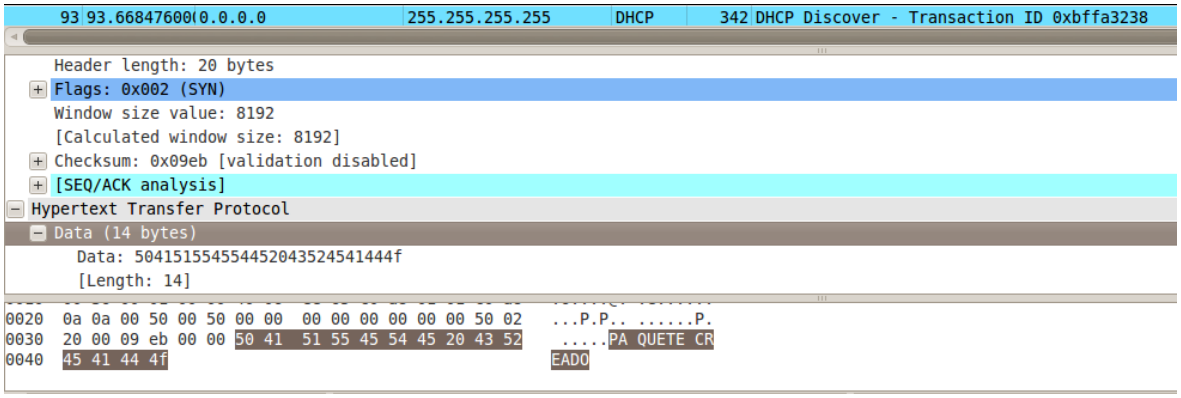


FIGURA 40. Captura de paquetes enviados

Por último se verifica que el ordenador 192.168.10.10 recibe el paquete (ver Figura 41).

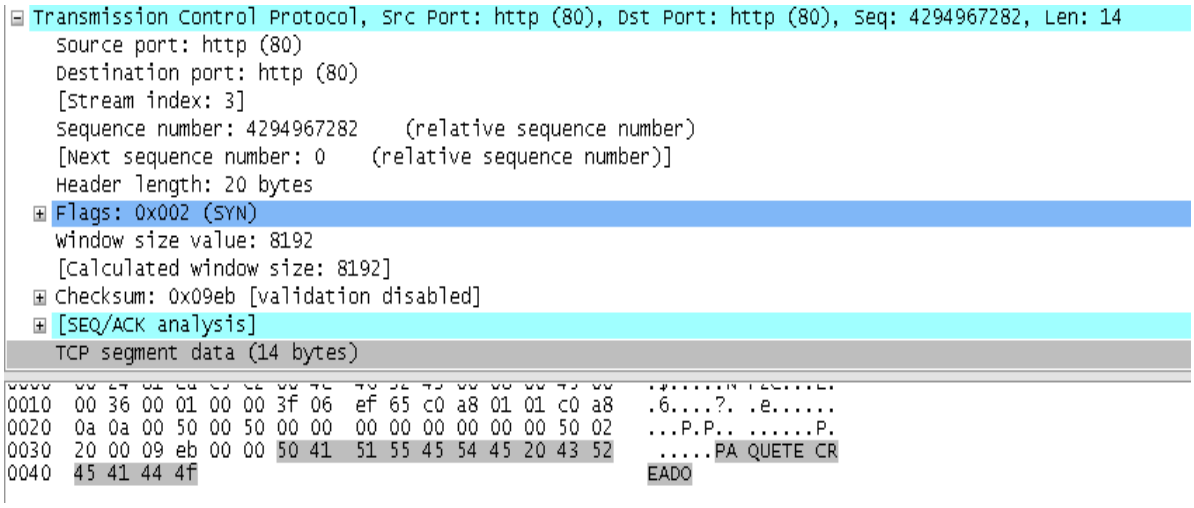


FIGURA 41. Recepción de paquetes

La creación y envió de paquetes se puede hacer de forma más práctica de la siguiente forma:

- Para enviar paquetes se utiliza la siguiente estructura *send(IP(dst="10.1.99.2")/ICMP()/"Prueba")* (ver Figura 42).

FIGURA 42. Comando send para envió de paquetes

- En el caso anterior se envió el paquete en el protocolo ICMP (Internet Control Message Protocol), pero dicho protocolo puede variar de la siguiente manera *send(IP(dst="10.1.99.2")/TCP()/"Prueba")* (ver figura 43)

FIGURA 43. Confirmación de envió de paquetes

Ahora se envía el paquete con dirección de origen establecida mediante la instrucción *send(IP(src="192.168.0.2",dst="192.168.0.1")/TCP()/"Prueba")*

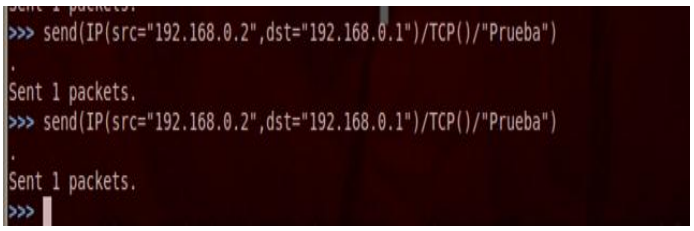


FIGURA 44.Modificación de protocolo

7.1.3 Visualizar paquetes con scapy

Scapy puede ser utilizado como sniffer para visualización y análisis de paquetes. Para esto es necesario implementar el comando *a=sniff()*. Después de utilizado el comando sniff se empieza a capturar el tráfico a traves de la red hasta que se presione CONTROL+C y luego se puede visualizar la información mediante el comando *a.nsummary()* (VER Figura 45)

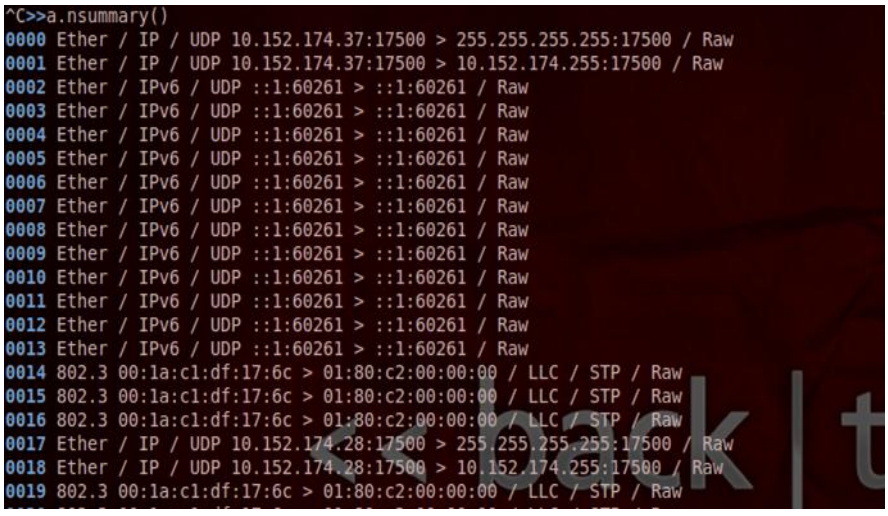


FIGURA 45.Visualización de paquetes con scapy

7.1.4 Uso de arping

Mediante la implementación del comando arping es posible visualizar la tabla de enrutamiento de la red, identificando las direcciones IP y MAC de cada dispositivo que contiene la red además de mostrar el fabricante de dichos dispositivos. Para

implementar esta se debe digitar en el terminal: *arping("10.152.174.*")*, donde el * simboliza que se realiza ping a toda la red(Ver Figura 46).

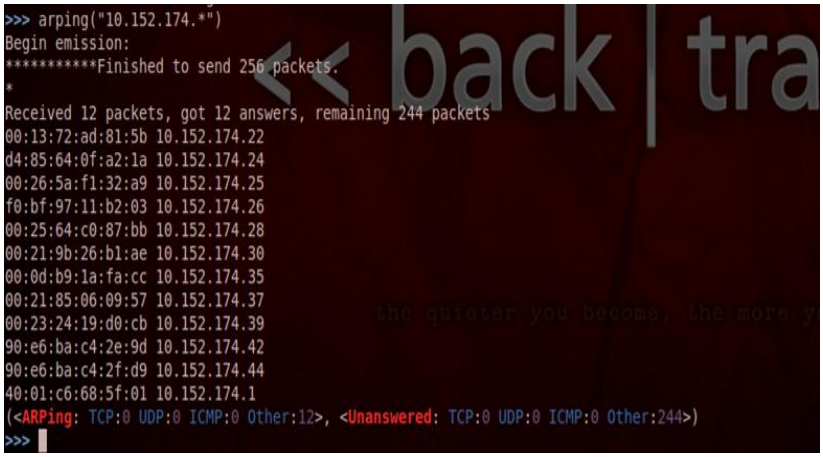


FIGURA 46.arping

7.1.5 Lectura de archivos .pcap

Los archivos .pcap contienen una serie de paquetes provenientes de una conversación determinada, mediante Scapy es posible leer el contenido de cada paquete identificando parámetros de los mismos mediante la siguiente instrucción *pkts = rdpcap("/tmp/prueba.pcap")*. Para el caso específico de la prueba el archivo a leer fue “prueba.pcap” y se encuentra almacenado en la carpeta “tmp”, para visualizar su contenido se digita *pkts.nsummary()* (ver Figura 47).

FIGURA 47. Lectura de archivos .pcap con scapy

7.1.6 Inyección de archivos .pcap

Al inyectar archivos .pcap se reproducen los mensajes en la red, para realizar esta función se implementa el siguiente comando *pkts = rdpcap("/tmp/prueba.pcap")*. Para enviar los paquetes se digita *send(pkts)* (Ver Figura 48).

FIGURA 48.Envió de archivos .pcap con scapy

Los comandos mostrados anteriormente corresponden a las funciones básicas y necesarias para implementar Scapy pero esta herramienta contiene una cantidad amplia de comandos que permiten desarrollar funciones complejas dependiendo de la necesidad del usuario además permite la creación de paquetes en detalle con características establecidas.

7.1.7 DHCP denegación de servicios con scapy

Como ya se ha mencionado este ataque busca colapsar la red para impedir que los dispositivos de la red afectados ofrezcan los servicios a los usuarios. Para la realización de ataque se debe implementar la instrucción *conf.checkIPaddr = False*, y a continuación el comando donde se configuran las reglas del ataque: *dhcp_discover=Ether(src=RandMAC(),dst="ff:ff:ff:ff:ff:ff")/IP(src="0.0.0.0",dst="10.152.174.39")/UDP(sport=80,dport=80)/BOOTP(chaddr=RandString(12,'0123456789abcdef'))/DHCP(options=[("message-type","discover"),"end"])*. Finalmente se procede a lanzar el ataque mediante la instrucción *sendp(dhcp_discover,loop=1)* (Ver Figura 49).

FIGURA 49.Creación del paquete para atacar

7.2 Pruebas con Metasploit

Para poder acceder a esta herramienta se debe ejecutar desde el terminal el comando *msfconsole*, el cual entra a la aplicación (Ver Figura 50).

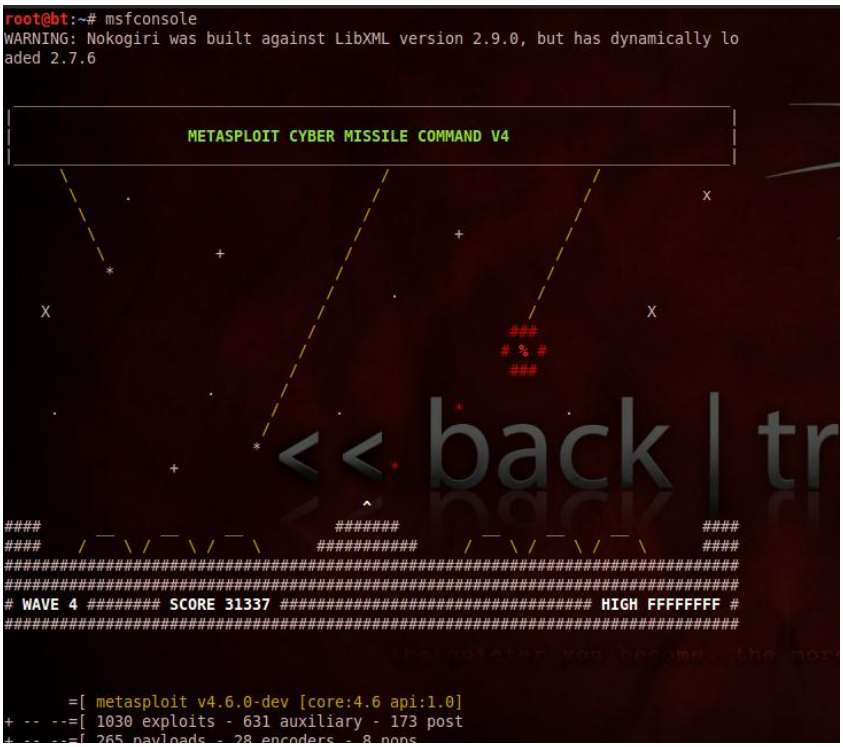


FIGURA 50.Entorno de metasploit

Si se desea observar las diferentes opciones que se tienen para atacar determinada vulnerabilidad se utliza el comando *search*, seguido del nombre del objetivo (Ver Figura 51).

FIGURA 51. Busqueda de vulnerabilidades

Desde aquí se selecciona el ataque que se pretende realizar, para esto se copia la dirección de este anteponiendo la palabra *use* (Ver Figura 52).

FIGURA 52. Selección de ataque

Dentro de esta dirección se configuran las diferentes opciones que se manejan, puerto de destino, servidor, IP de víctima, entre otros, dependiendo del ataque a realizar(Ver Figura 53).

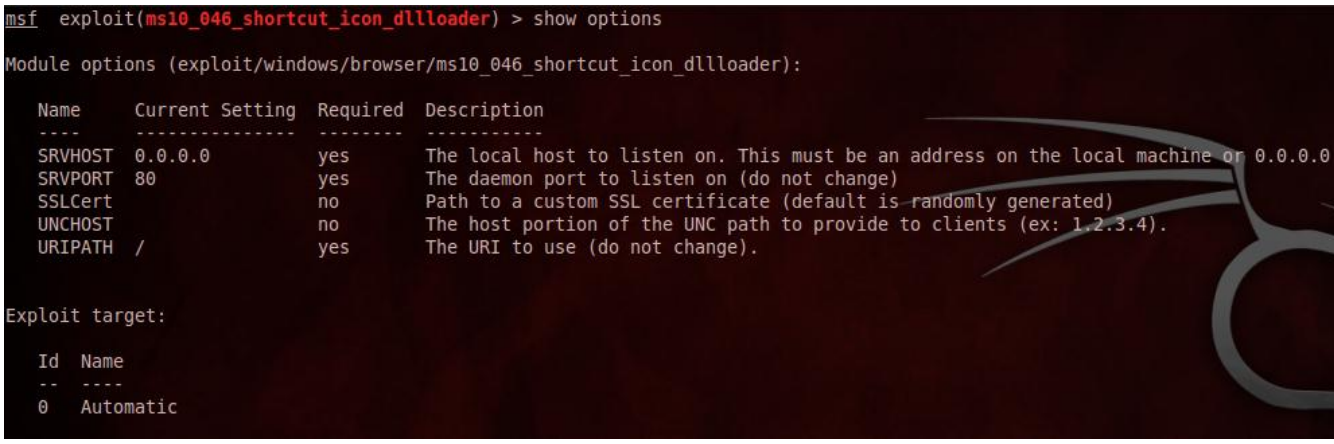


FIGURA 53. Menú de opciones del ataque a desplegar

Una vez configuradas las opciones se procede a lanzar el ataque, para esto se usa el comando *exploit* (Ver Figura 54).

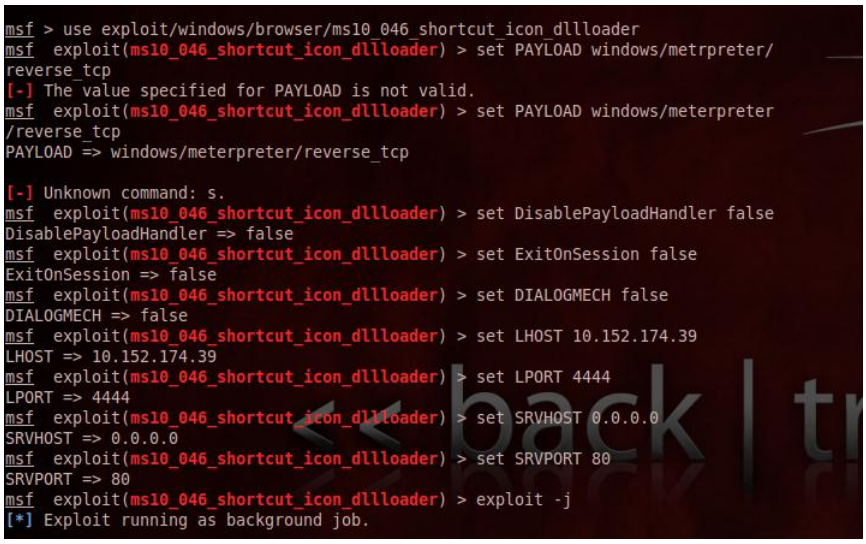


FIGURA 54. Ejecución del ataque

Cuando se obtenga la salida *Server started* se procede a hacer que la víctima entre a este por medio de la URL suministrada y de esa forma poder entrar a controlar su sistema operativo (Ver Figura 55).

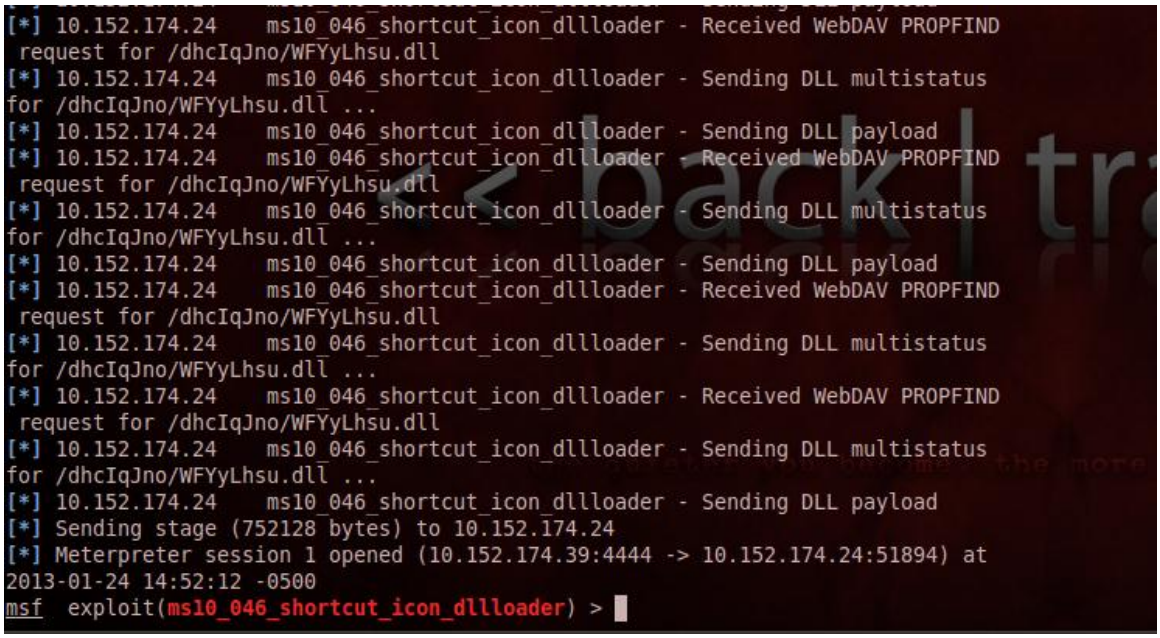


FIGURA 55. Conexión con equipo víctima

Teniendo la session 1 abierta, se procede a tomar el control del pc de la víctima por medio del comando *sessions -i* seguido del número de sesión a controlar (Ver Figura 56).

FIGURA 56. Sesión activa con equipo victima

Con *ps*, por ejemplo, es posible acceder a la lista de procesos que maneja el pc de la victima (Ver Figura 57).

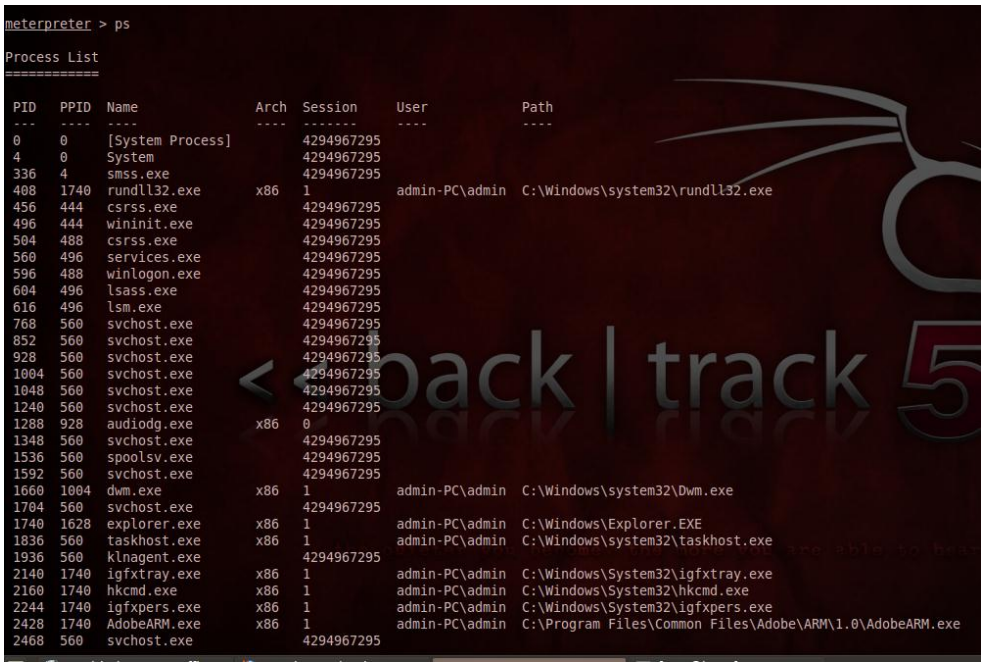


FIGURA 57. Tabla de procesos activos en equipo víctima

Para acceder a la consola se digita *shell*, lo que nos envia hacia la consola de windows, desde donde podemos manipular los procesos (Ver Figura 58).

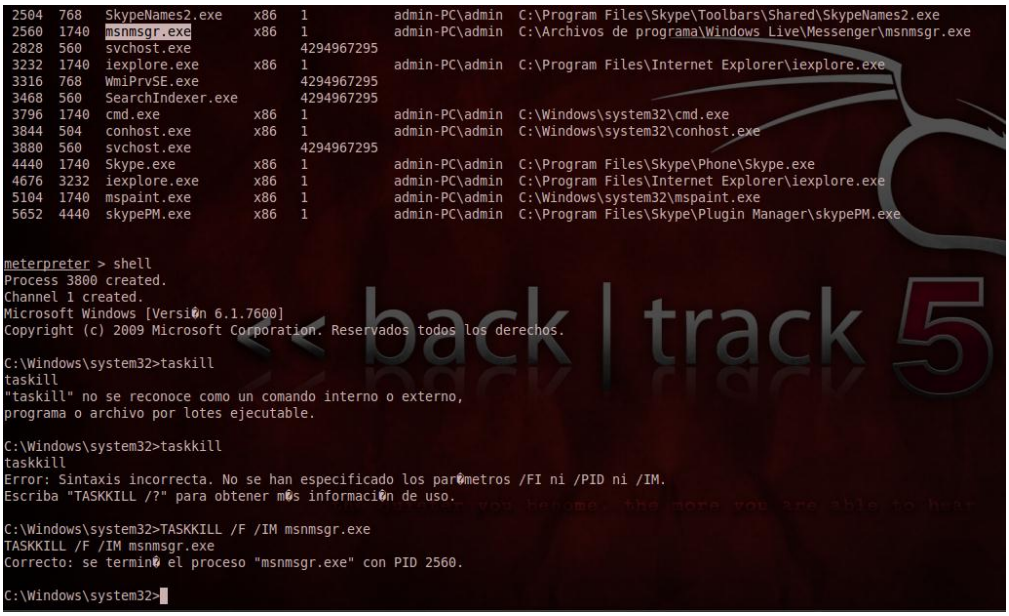


FIGURA 58. Manejo de consola mediante equipo remoto

De esta manera se pueden explotar las debilidades presentes, en todos los sistemas operativos existentes y en los programas diseñados para estos, siempre y cuando se tenga el conocimiento y las herramientas adecuadas para realizar dichas pruebas.

7.3 Pruebas con Nmap

Para poder obtener mayores detalles de la red, Nmap cuenta con diferentes extensiones, algunas de estas se enuncian a continuación

-sP (Sondeo ping) esta opción se aplica cuando se quiere descubrir que sistemas se encuentran conectados a una red, mediante un sondeo ping, el cual consiste en enviar paquetes a los objetivos, esto es útil ya que los atacantes cuentan con una lista de las IP de los equipos (Ver Figura 59).[44]

Esta opción envía una solicitud de eco ICMP y un paquete TCP al puerto 80.

[44] OREBAUGH, Angela. Nmap in the Enterprise: Your guide to network scanning. Elsevier Inc, 2008; pag 161-183.

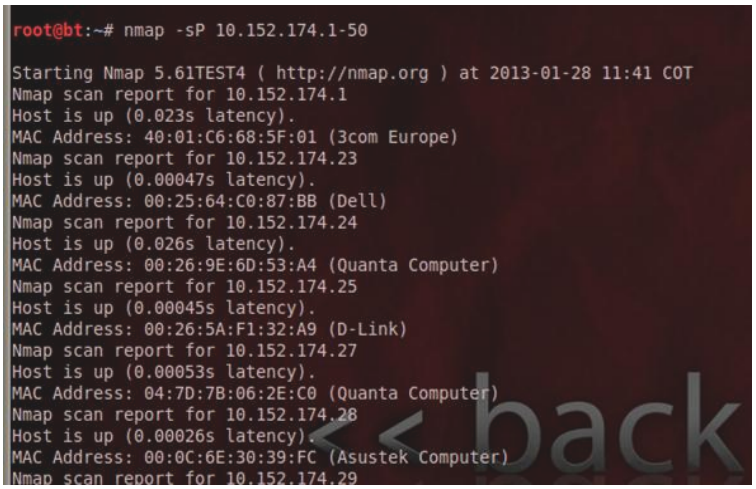


FIGURA 59. Nmap --sP

Para poder realizar un análisis de puertos es importante conocer las diferentes respuestas que se pueden obtener cuando se hace un sondeo de estos, Nmap tiene 6 posibles estados para estos.

Abierto: Es un puerto por donde se puede realizar un posible ataque ya que acepta conexiones TCP o paquetes UDP, para tratar de proteger estos puertos se utilizan los Firewalls o, si no son esenciales para el funcionamiento de una aplicación, cerrarlos.

Cerrado: Es un puerto accesible pero que no tiene ninguna aplicación en él, ya que estos puertos no se encuentran filtrados es posible hacerles un seguimiento y esperar que sean utilizados por una aplicación.

Filtrado: Al obtener este estado se interpreta que Nmap no puede determinar si el puerto se encuentra abierto o cerrado ya que los paquetes enviados no alcanzan el puerto, este filtrado puede provenir de un firewall o de un enrutador.

No Filtrado: Los paquetes de Nmap llegan al puerto pero no es posible determinar si se encuentra abierto o cerrado el puerto.

Abierto|Filtrado y Cerrado|Filtrado : Nmap no puede determinar si el puerto se encuentra filtrado, cerrado o abierto ya que existe ausencia de respuesta, lo que puede significar que se descartaron o se eliminó cualquier respuesta asociada.[45]

[45] Introducción al análisis de puertos [en línea] < http://nmap.org/man/es/man-port-scanning-basics.html> [citado en 2013]

-sS (sondeo TCP SYN) Es el más utilizado ya que se realiza rápidamente, en una red donde no existe firewall, a esta técnica se le conoce como sondeo medio abierto, ya que no completa las conexiones TCP, se envía un paquete SYN, y espera una respuesta para determinar si se encuentra abierto, cerrado o filtrado (Ver Figura 60).

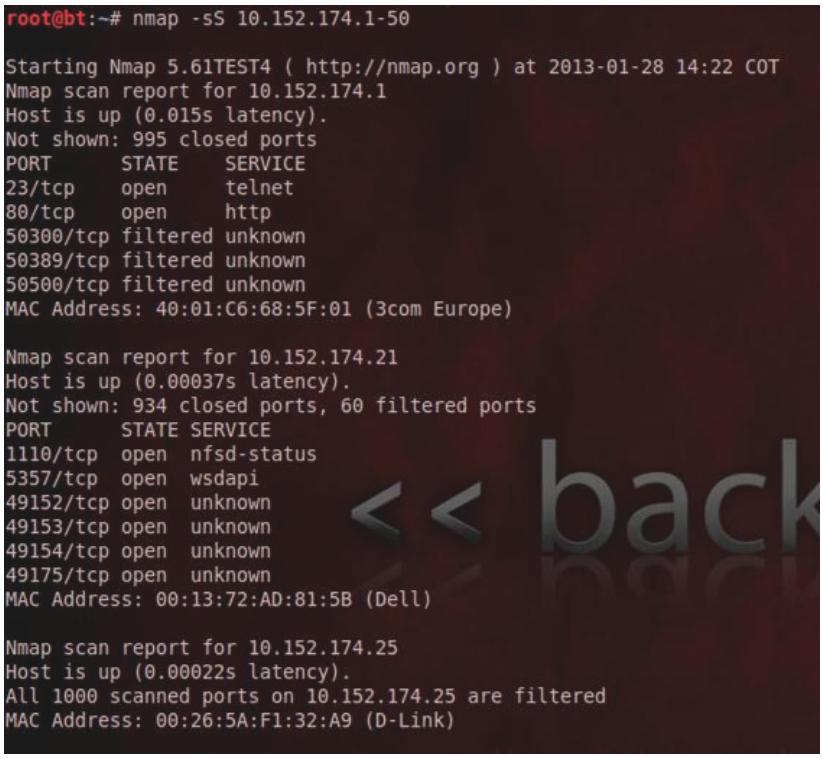


FIGURA 60. Nmap -sS

-sU (sondeo UDP) Se realiza generalmente cuando se obtiene como respuesta en un analisis -sS que los puertos se TCP se encuentran filtrados, ya que tambíen es un protocolo muy utilizado, 3 de los servicios más comunes son DNS, SNMP y DHCP, es un sondeo que requiere de mayor tiempo de ejecución respecto al realizado anteriormente, su funcionamiento se basa en el envio de paquetes, vacios, de cabecera UDP para cada puerto que sea objetivo.[46]

[46] Tecnicas de sondeo de puertos [en línea] < http://nmap.org/man/es/man-port-scanning-techniques.html> [citado en 2013]

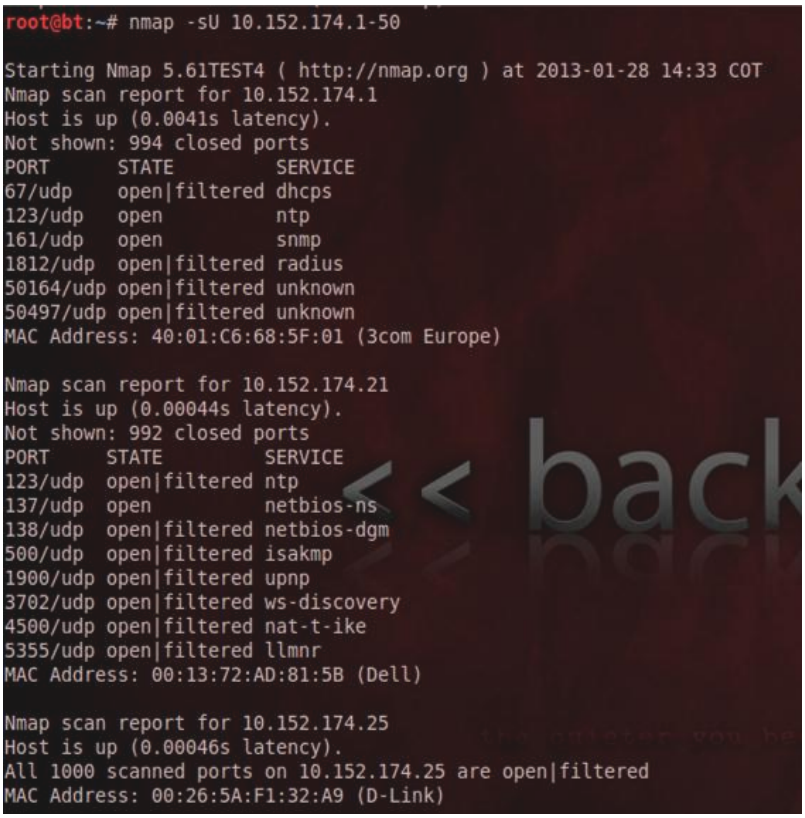


FIGURA 61. Nmap -sU

-sV (Detección de versiones) se aplica este tipo de sondeo cuando se quiere obtener mayor información sobre lo que se está ejecutando en los puertos, tanto TCP como UDP, con el fin de tener mayor claridad sobre el objetivo de un posible ataque (Ver Figura 62).

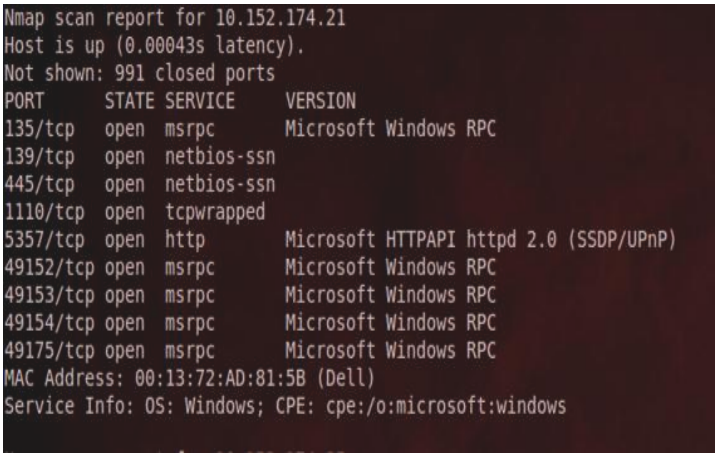


FIGURA 62. Nmap --sV

-O (detección de sistema operativo) se hace mediante varias pruebas realizadas y el posterior análisis de las huellas dejadas por los sistemas en la base de datos de nmap, la cual, si encuentra coincidencias, enseña que tipo de sistema operativo, al igual que la versión, manejan los computadores conectados a la red (Ver Figura 63).[47]

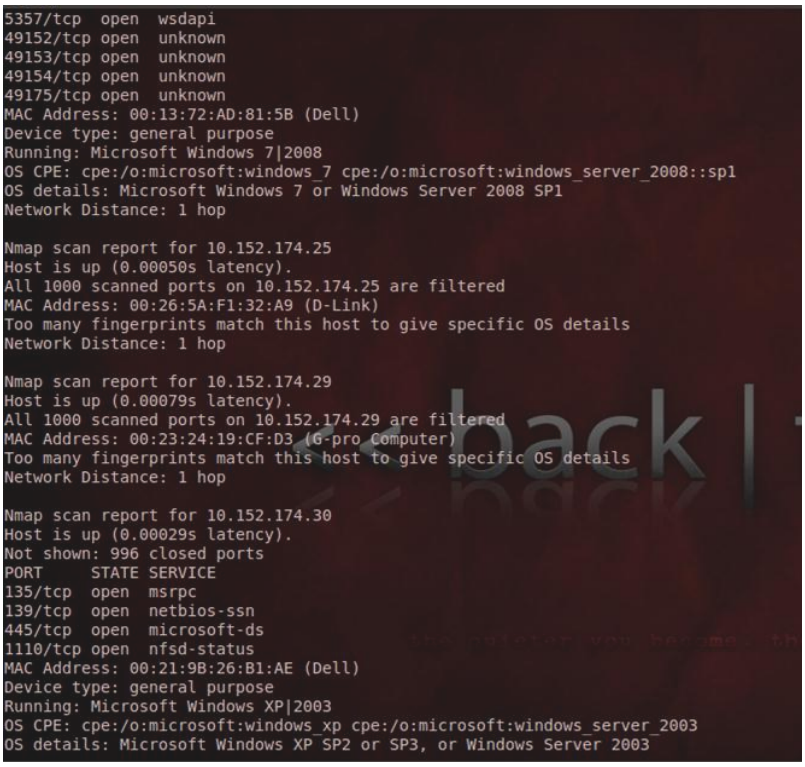


FIGURA 63. Nmap -O

--mtu (fragmentación de paquetes) Este tipo de herramientas se utiliza cuando el pc que se quiere analizar cuenta con un firewall, como lo es iptables, y no se puede acceder a su información, se debe tener en cuenta que este tipo de fragmentación debe ser múltiplo de 8 para poder fragmentar correctamente el paquete.

[47] Detección de servicios y versiones [en línea] < http://nmap.org/man/es/man-version-detection.html> [citado en 2013]

7.4 Pruebas con Zenmap

Su manejo es muy intuitivo y, para quienes estén dando los primeros pasos, cuenta con una serie de pruebas por defecto que permiten conocer el estado completo de la red, contiene además una característica adicional que permite analizar la topología de la red (Ver Figura 64), la cual muestra las diferentes conexiones por las cuales debe pasar antes de llegar al punto desde donde se realiza el escaneo, en este caso en específico solo se muestra la red donde se encuentra conectado el equipo ya que la seguridad con la que cuenta la red no permite que podamos ver más allá de esta.

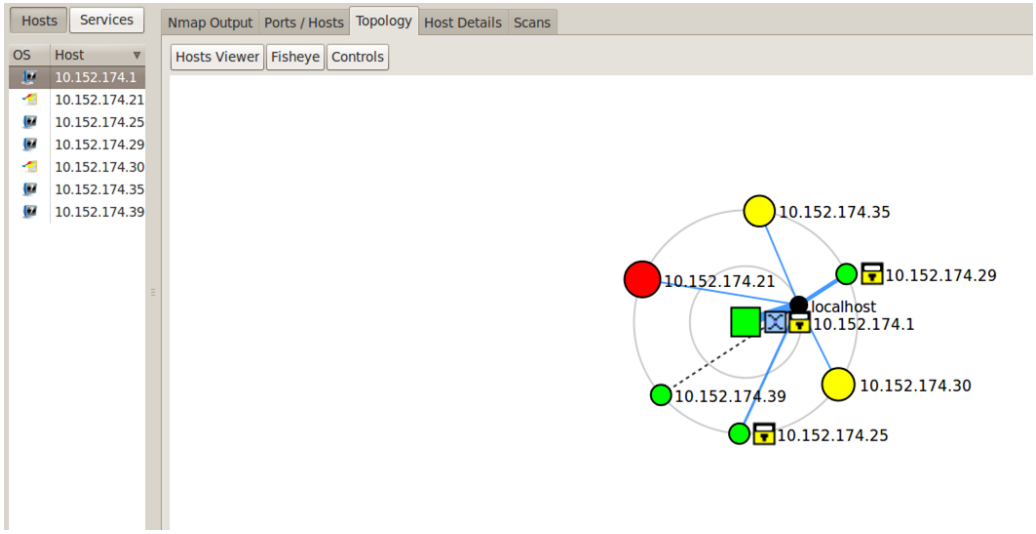


FIGURA 64. Topología de una red con zenmap

Dependiendo del análisis aplicado muestra además las características de cada uno de los equipos conectados a la red (Ver Figura 65). .

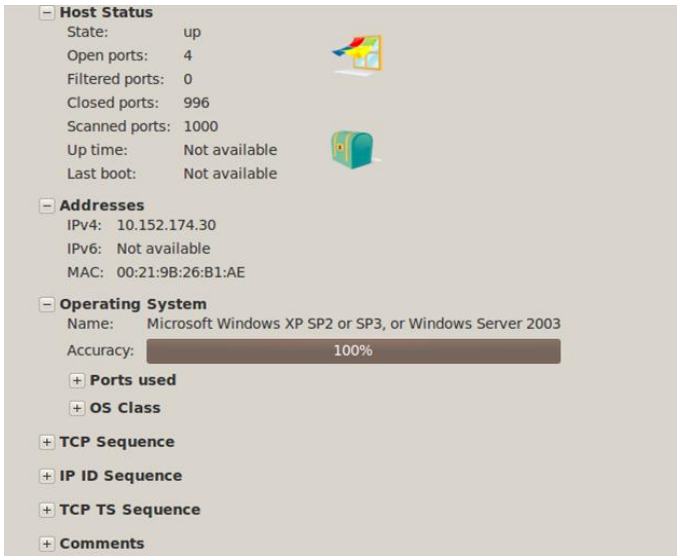


FIGURA 65. Detección de sistema operativo con zenmap

7.5 Pruebas NetDiscover

Dispone de diferentes opciones las cuales pueden ser desplegadas con el comando mostrado en la Figura 66:

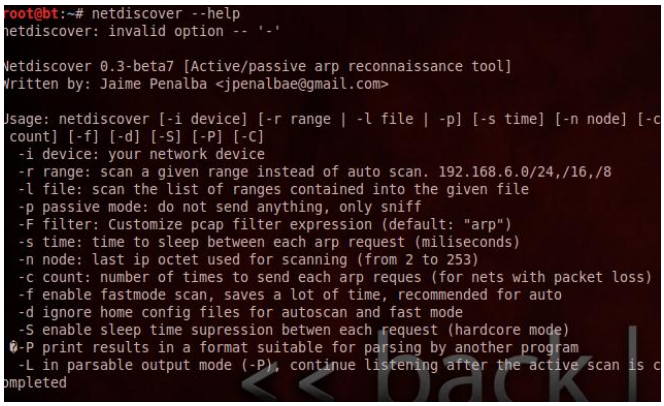


FIGURA 66. Menú de ayuda de netdiscover

Específicamente para este proyecto esta aplicación fue usada para descubrir las direcciones IP y MAC de los equipos asociados a la red, obteniendo los siguientes resultados en una de las pruebas aplicadas (Ver Figura 67).

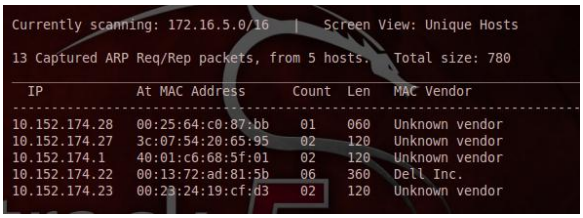


FIGURA 67.Equipos conectados encontrados mediante netdiscover

8. Descripción de la red industrial a atacar

8.1 Topología

La red industrial intervenida se compone del servidor (192.168.10.10) y el PLC (192.168.10.3). En este caso ademas se interconecta otro ordenador (192.168.10.2) con linux backtrack con el fin de realizar cada uno de los ataques a la red, la comunicación entre los dispositivos se logra mediante un switch 3COM 4500. La red puede ser visualizada en la figura 68.

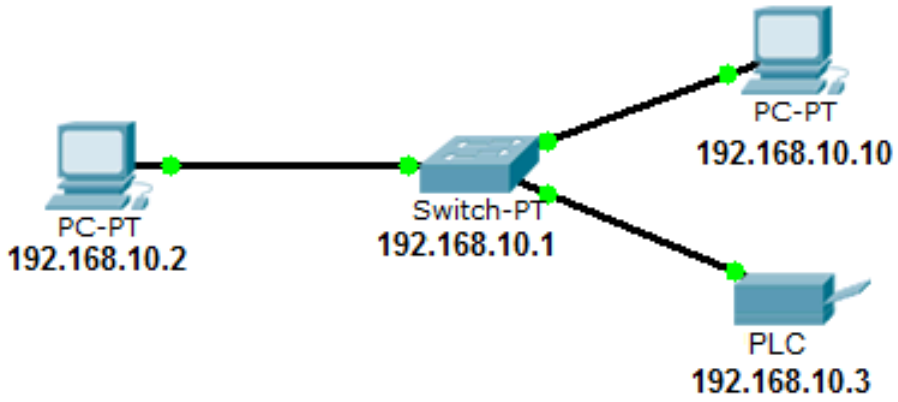


FIGURA 68. Topología de red Industrial implementada

8.2 Descripción de dispositivos

- Switch 3COM 4500[48]

[48] Familia 3Com® Switch 4500 10/100[En línea] <http://www.tarconis.com/documentos/3COM_4500ds.pdf> [citado en 2013]

Figura 69. Switch 3COM 4500

Este dispositivo proporciona una conectividad LAN segura y flexible con diversas funcionalidades de seguridad, calidad de servicio (QoS) y administración para proporcionar una conectividad de extremo inteligente para las aplicaciones empresariales esenciales. El switch consta de 24 puertos 10/100 y dos puertos gigabit de uso dual.

- PLC TSX Modicon Premium[49]

Controlador programable para control de máquinas que permite optimizar procesos dando practicidad y mejorando la productividad de la industria además de reducir costos. El dispositivo cuenta con las siguientes características:

- CPU de alto rendimiento
- Sistema multitarea de alto nivel
- Puertos de conectividad integrados: puerto USB, puerto Ethernet TCP/IP, puerto master FIP, puerto en serie

[49] Schneider Electric [en línea] <http://www.schneider-electric.cl/sites/chile/es/productos-servicios/automatizacion-control/oferta-de-productos/presentacion-de-rango.page?c_filepath=/templatedata/Offer_Presentation/3_Range_Datasheet/data/es/local/automation_and_control/modicon_premium.xml#> [citado 2013]

FIGURA 70. PLC TSX Modicon Premium

- Servidor del PLC

FIGURA 71. Servidor con Unity PRO

Este ordenador establece comunicación con el dispositivo programable con el fin de tener el control del mismo. Mediante el uso del software UNITY PRO M, se logra programar las funciones y tareas que debe realizar el control para luego ser transferidas al PLC por medio de las herramientas del software que también permiten colocar el dispositivo en funcionamiento (Modalidad RUN), o en su defecto pararlo (Modalidad STOP), dicha comunicación se logra a través del protocolo MODBUS TCP.

- Ordenador atacante

En este caso se tiene un ordenador con el sistema operativo Linux backtrack, que ofrece versatilidad de funciones para aplicación en redes para el análisis y explotación de las vulnerabilidades de las redes.

Figura72. Equipo con Backtrack

9. Análisis de vulnerabilidades de la red industrial a atacar

Además de los ataques descritos en la sección anterior, la red industrial es vulnerable a otro tipo de ataques, debido al protocolo y los puertos que se utilizan para la comunicación entre dispositivos. Estos ataques se estudiaron y realizaron en la red prototipo y se explicarán a continuación.

9.1 Ataques con Metasploit para dispositivos Scheneider[50]

Dentro de todas las vulnerabilidades que metasploit puede atacar, se encuentran 3 para equipos de Schneider Electronics, de los cuales se lograron implementar 2, ya que el otro modulo tiene una función que no se aplica para el PLC presente en el laboratorio. Dichos ataques son:

modicon_command – Schneider Modicon Remote Start/Stop Command

Mediante este comando se puede realizar de manera remota un cambio en el estado del PLC, el cual puede variar entre STOP y RUN; lo que trae como consecuencia una eventual alteración del proceso y por ende de la producción.

[50] Metasploit Modules [en línea] < http://www.digitalbond.com/tools/basecamp/metasploit-modules/> [citado en 2013]

Para utilizar este comando se accede desde el terminal de linux a metasploit como ya se ha explicado con anterioridad y se busca el directorio que contiene el ataque, para posteriormente observar que parámetros se requieren para que sea efectivo (ver figura 73)

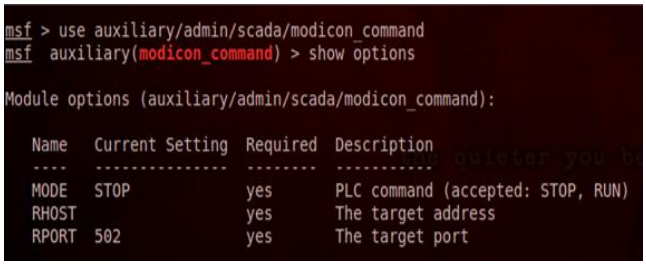


Figura 73. Opciones del comando remote start/stop de metasploit

Una vez configurados los parámetros se procede a ejecutar el ataque. Es importante resaltar que para que este sea efectivo se debe tener acceso a la red y no tener ninguna regla que bloquee el puerto por el cual se comunica el PLC, es decir el puerto 502, ya que desde allí se envía un código de función modbus que realiza comandos administrativos sin autenticación.

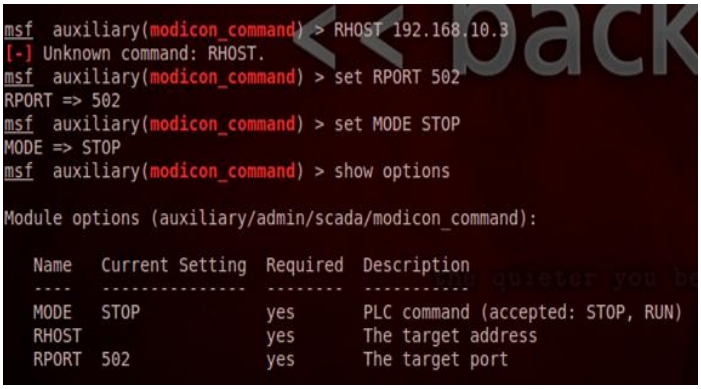


FIGURA 74. Configuración del comando remote start/stop

modicon_stux_transfer - Schneider Modicon Ladder Logic Upload/Download

Es un ataque que funciona de manera similar al stuxnet, de allí que tenga como prefijo stux.Para realizar este ataque se debe tener acceso a la lógica del PLC, lo cual es posible con el comando RECV dispuesto en el módulo para conocer la información contenida y realizar cambios en esta, para posteriormente ser reenviada mediante el comando SEND, también dispuesto en el módulo. De igual forma, el puerto utilizado para este ataque es el 502, por lo que se hace fundamental el bloqueo de este puerto fuera de la red que contiene al PLC para

evitar posibles fallas en la seguridad del proceso.

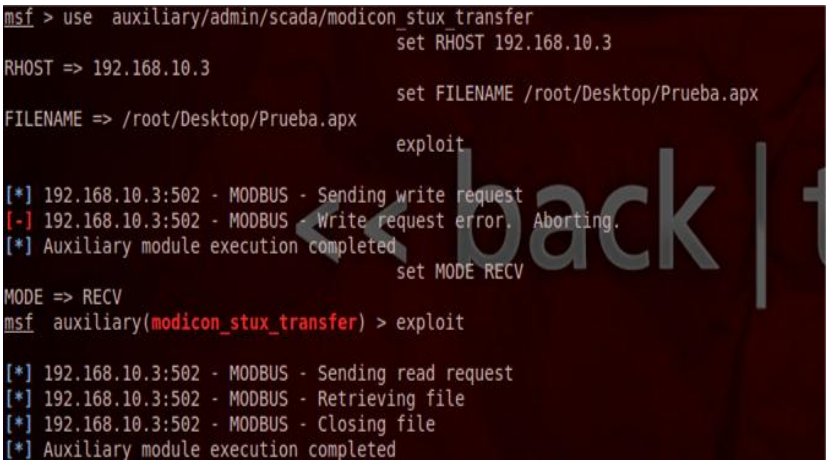


FIGURA 75. Demostración Comando modicon_stux_transfer

modicon_password_recovery - Schneider Modicon Quantum Password Recovery

Este ataque permite restablecer los parámetros de usuario y contraseña del PLC, dejando sin acceso al usuario legitimo del dispositivo. Este exploit usa el puerto de comunicación numero 21 correspondiente al protocolo FTP (file transfer protocol), por donde se proporcionan los servicios de acceso (login, password). Al restablecer los valores originales por los deseados por el atacante, se expone la red dejando comprometida la seguridad de la misma. Este ataque no se realizó en la red intervenida en el presente proyecto porque las condiciones de funcionamiento de los dispositivos no manejan este tipo de acceso, pero a continuación se muestra cómo se genera el ataque.

FIGURA 76. Configuración módulo modicon_password_recovery

9.2 Tabla de contenido general de los ataques

Sintetizando la información y en busca de una mayor claridad, a continuación se presenta una tabla con el fin de mostrar los diferentes ataques realizados, la clase de estos y como afectan la red.

Software	Tipo de ataque	Ataques
Wireshark	Pasivo	• Sniffing (captura de paquetes)
Scapy	Pasivo y activo	• Sniffing • Envió de paquetes con suplantación • Denegación de servicios DHCP
Nmap	Pasivo	• Escaneo de puertos y exploración de la red
NetDiscover	Pasivo	• Reconocimiento de direcciones IP presentes en la red
Zenmap	Pasivo	• Escaneo de puertos y exploración de la red
Metasploit	Activo	• Acceso remoto a dispositivos • Denegación de servicios • Explota vulnerabilidades de los dispositivos
Macchanger	Activo	• Suplantación de identidad
Ettercap	Activo	• Man in the middle

Tabla 4. Ataques Realizados a la Red Industrial

10. DESARROLLO DEL FIREWALL CON NetFPGA

Es importante aclarar que al estudiar los diferentes módulos previamente desarrollados para el proyecto U2- route, se concluyó que no era necesario realizar un nuevo módulo ya que los existentes se podían adaptar a las necesidades del firewall.

Para comprender de manera más detallada como se obtuvo el firewall, se hace necesario detallar la herramienta utilizada y los diferentes módulos, al igual que los diferentes pasos que se dieron hasta llegar al prototipo final.

10.1 NETFPGA

La tarjeta NetFPGA es una plataforma de hardware reconfigurable de gran desempeño para su implementación en redes de alta velocidad, dotada de recursos que permiten una funcionalidad eficiente en la construcción de switches, routers, sistemas de seguridad entre otros.

10.1.1 Características de la tarjeta NetFPGA:

- Conector PCI bus estándar de 32 bits, 33 Mhz
- 4 interfaces GbitEthernet (1Gbps)
- Un chip FPGA Virtex-2, con reloj de 125 Mhz
- 4 bancos de memoria SRAM y DRAM

10.1.2 Ventajas del uso de la tarjeta NetFPGA

- El procesador principal del ordenador puede implementar DMA (Direct Memory Acces) para leer y escribir registros de la NetFPGA
- Proporciona un camino de datos acelerados por hardware debido a la conectividad mediante 4 puertos a 1Gbps y el acceso a bancos de memoria ubicados en la tarjeta.[51]

[51] Características NetFPGA. [en línea] < http://www.netfpga.org/php/specs.php > [citado 18 de octubre de 2012]

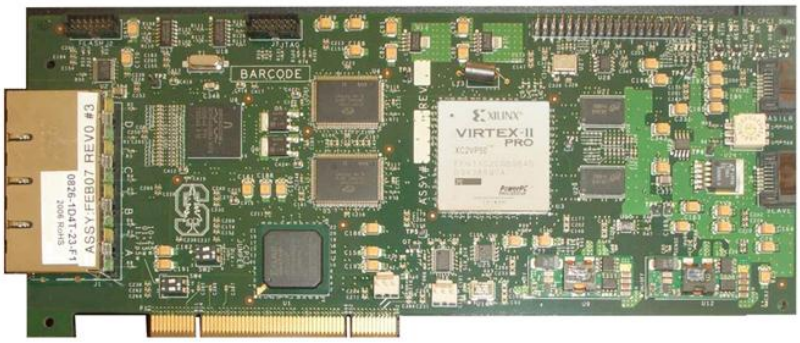


Figura 77. Tarjeta NetFPGA

10.2 MÓDULO REFERENCE ROUTER[52]

Para la introducción al manejo de la tarjeta NetFPGA, fue necesario obtener el proyecto Reference Router ,desarrollado en la Universidad de Stanford, que se encuentra disponible para descarga en la página www.netfpga.org. Este proyecto consiste en un Router IPv4 conformado por diferentes módulos como se muestra a continuación:

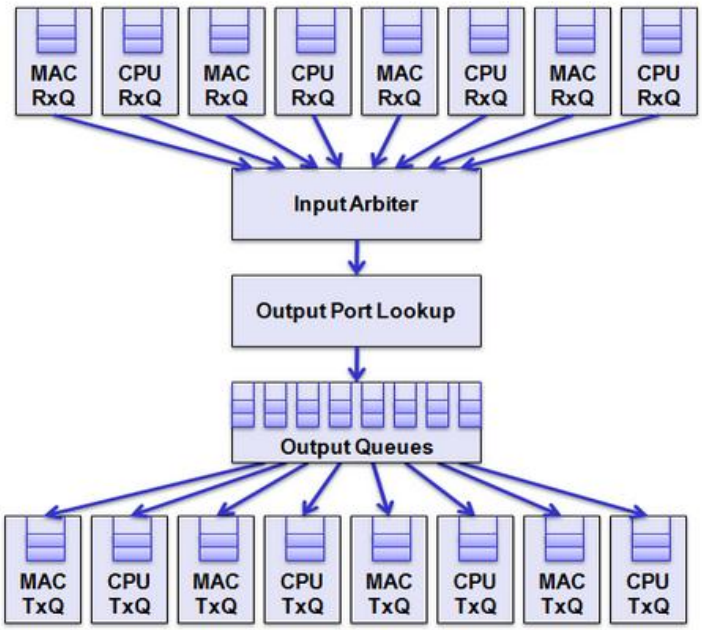


FIGURA 78. Modulos Reference Router[53]

[52] PADILLA, Jhon Jairo. U2 route: Guía Práctica. Sic Editorial Ltda, 2011; pag 47-52

La primera línea de módulos corresponde a la recepción de paquetes donde se encuentran las colas de tipo MAC que se encargan de obtener los datos de los puertos Ethernet de la tarjeta y las colas de tipo CPU que almacenan los datos obtenidos por medio de la interfaz PCI.

El segundo módulo, denominado “Input Arbiter”, se encarga de seleccionar la cola de entrada con disponibilidad para enviar paquetes al siguiente modulo. Dicho proceso se realiza basado en la estrategia Round Robin, que permite seleccionar de forma equitativa y en orden racional.

El tercer módulo del diagrama denominado “Output Port Lookup” es el encargado de tomar la decisión del puerto de salida de los paquetes basándose en la tabla de enrutamiento configurada en la NetFPGA.

En el último módulo se almacenan los paquetes hasta que la cola de transmisión, MAC o CPU, indique que se encuentra disponible para aceptar el paquete para transmisión.

10.3 MÓDULO TOKENR BUCKET [54]

Este módulo se basa en un algoritmo diseñado para controlar la cantidad de tráfico que puede ser inyectado a una red. Para un mayor entendimiento del algoritmo se puede realizar la analogía con un balde donde llegan determinada cantidad de fichas. Cada ficha (token) otorga permiso para transmitir un determinado número de bytes. Las tramas pasan siempre y cuando el balde no se encuentre vacío y haya suficientes tokens como para dar permiso a la cantidad de bytes de la trama en turno, convirtiéndose en una especie de embudo de red. Esté módulo cuenta con tres parámetros que son:

Profundidad del Balde: Indica el número máximo de tokens que se pueden almacenar en el balde, sus unidad es (Token), y para el caso específico del proyecto U2-route, es una variable de 16 bits que toma el nombre el *tam_bucket.*

Tamaño del Token: Indica el número de bytes que pueden que se pueden transmitir por cada Token, su unidad es dada en bytes/Token. Es una variable de 16 bits que toma en el módulo el nombre de *tam_token.*

---

[53] Reference Router [en línea] <http://keb302.ecs.umass.edu/de4web/DE4_NetFPGA/?q=node/23> [citado en 2013]

[54] PADILLA, Jhon Jairo. U2 route: Teoría y Diseño. Sic Editorial Ltda, 2011; pag 62-65

Tasa de Tokens: Es la tasa de llegada de los Tokens al balde. En el módulo se usaron dos registros conectados en cascada que determinan el valor del divisor de frecuencia de reloj del sistema, el cual es de 125 Mhz, para obtener la frecuencia de llegada del Token. Estos registros se denominan *tasa_lleg* y *bas_temp.*

Además de esto se deben tener en cuenta dos ecuaciones que determinan las características del diseño del Token, las cuales son: *tamaño máximo de la ráfaga,* que se consigue al mutiplicar la profundidad del balde con el tamaño del Token (ecuación 1) y la tasa media que se obtiene al mutiplicar la tasa de Tokens y el tamaño del Token (ecuación 2).

$$tam\max rafaga = b * m\ (bytes) \quad \text{(Ecuación 1)}$$

$$tasa\ media = r * m(\frac{bytes}{seg}) \quad \text{(Ecuación 2)}$$

Este módulo cuenta con la característica de eliminar los paquetes una vez se iguale el tamaño máximo de la ráfaga, lo que resulta útil en caso de estar expuestos a un ataque de denegación de servicios.

10.4 MÓDULO CLASIFICADOR DE PAQUETES

Este módulo fue diseñado pensando en proveer calidad de servicio dentro de una red mediante la clasificación de estos. Buscando mayor eficiencia el tráfico que maneja una red debe ser seleccionado basado en reglas definidas con anterioridad, dichas reglas pueden indicar que un paquete sea marcado con un valor determinado en el campo DSCP.

Para este clasificador el paquete a procesar proviene del módulo Input Arbiter, una vez recibido el paquete se deben identificar 5 campos (puerto origen, puerto de destino, puerto de fuente, puerto destino e identificación de protocolo) para comparar los valores existentes en la configuración con los valores de los encabezados del paquete. Una vez comparados los campos, el clasificador modifica el campo TOS (type of service) de la cabecera IPv4.

El módulo clasificador se encuentra entre los módulos Input Arbiter y Output Port Lookup, tal como se observa a continuación en la figura 79.

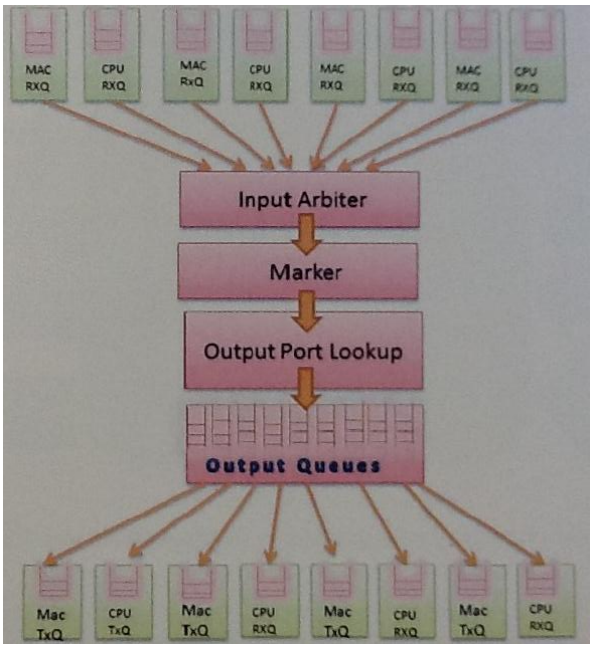


FIGURA 79. Módulos Marcador

10.5 Proyecto U2-Route[55]

Este proyecto se desarrolló como un proyecto investigativo que contó con la intervención de los grupos GITEL de la UPB seccional Bucaramanga y TIC'S de la Universidad Católica de Pereira y contó con el apoyo de Colciencias y RENATA.

U2-Route se define como una herramienta para la enseñanza e investigación en enrutamiento y conceptos de calidad de servicio sobre internet. Está basada en un router que permite la modificación o creación de módulos que lo componen.

Dadas las características de U2-Route, este proyecto permite probar nuevas tecnologías para el tratamiento de paquetes mediante prototipos físicos, pruebas y mediciones durante la ejecución de experimentos de enrutamiento, lo cual con las herramientas es una limitante.

[55] PADILLA, Jhon Jairo. U2 route: Teoría y Diseño. Sic Editorial Ltda, 2011; pag 13

10.6 Manejo del CLI (Command Line Interface)[56]

Es una interfaz de línea de comandos que permite configurar los módulos del hardware. Fue desarrollado por la Universidad de Stanford para poder programar los diferentes registros de la tarjeta NetFPGA.

Este CLI aparece dentro de la carpeta SW del proyecto y se ejecuta digitando el comando *./cli* cuando se está en dicha carpeta.

Dependiendo del módulo que se tenga cargado se puede hacer uso de diferentes funciones, algunos de los cuales son:

- Comando setmac

Es el comando encargado de configurar la dirección MAC de los puertos físicos, en la línea de comando se debe teclear la palabra setmac, inmediatamente aparecerá otra línea con un prompt >> que indica que debe ingresarse la información del puerto y la dirección MAC.

- Comando setarp

Permite configurar la tabla ARP (Address Resolution Protocol) del Router relacionando las direcciones IP con las direcciones MAC de cada uno de los puertos físicos.Para acceder a esta opción se digita setarp e inmediatamente aparecerá una nueva línea con un prompt >> que indica que debe agregarse la identificación de la entrada de la tabla, la dirección IP del puerto y la dirección MAC del puerto físico.

- Comando setip

Este comando permite ingresar cada una de las entradas de la tabla de enrutamiento IP del Router. Para acceder a esta opción se digita setip e inmediatamente aparecerá una nueva línea con un prompt >> que indica que debe agregarse la entrada de la tabla, la dirección IP de la subre, la máscara de la subred, la dirección IP del siguiente salto y finalmente el puerto físico de salida.

[56] PADILLA, Jhon Jairo. U2 route: Guía Práctica. Sic Editorial Ltda, 2011; pag 65-70

- Comando Settos

Permite configurar la prioridad de los paquetes que pasan por la red, Los datos ingresados por el usuario contienen la información de los puertos de origen y destino, la identificación del protocolo y el código de servicios diferenciados.

- Comando Settok

Toma los parámetros del módulo Token Bucket y los almacena en los registros respectivos de la NetFPGA. Para acceder a esta opción se digita settok e inmediatamente aparecerá una nueva línea con un prompt >> que indica que debe agregarse el número de bytes que permite transmitir un token, el máximo número de Tokens que puede almacenar el balde y los dos divisores de frecuencia para obtener la tasa de llegada de los tokens.

10.7 CLI desarrollado para el proyecto U2-Route[57]

Ya que el CLI original no permitía automatizar los procesos de registro se realizaron modificaciones a este para que se puedan ejecutar estas opciones desde el terminal de CentOS. Estos comandos son:

- Comando cli –r :Este comando remplaza al comando setip .

- Comando cli –a :Comando equivalente al comando setarp.
- Comando cli –m :Comando equivamente al comando setmac.
- Comando cli –k :Este comando configura el token bucket, por lo que remplaza el comando settok.
- Comando cli –t :Este comando es equivalente al comando settos.

10.8 Pruebas de Configuración del reference router original

a. Objetivo de la prueba

Para la configuración del proyecto se puede utilizar la herramienta de configuración original o la versión modificada diseñada por el equipo del proyecto U2-ROUTE, aunque la base de los parámetros siguen siendo los mismos. Se realizó la configuración según lo descrito en (libro U2-route guía práctica).

[57] PADILLA, Jhon Jairo. U2 route: Guía Práctica. Sic Editorial Ltda, 2011; pag 68-72

El objetivo de esta prueba fue establecer comunicación entre dos ordenadores implementando la NetFPGA con el fin de analizar su funcionamiento.

b. Topología

Para la prueba se hizo uso de dos ordenares configurados con los parámetros adecuados para implementar el proyecto *reference router* mediante la NetFPGA como se muestra en la figura 80.

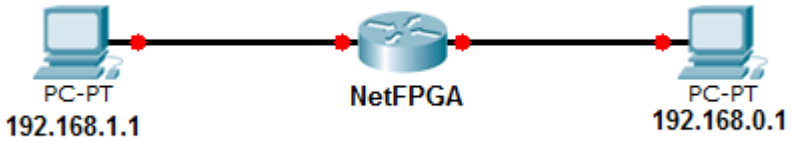


FIGURA 80. Topología de dos equipos conectados a la NetFPGA

c. Procedimiento

A continuación se muestra la configuración con la versión modificada, mediante la cual se realizaron las pruebas de funcionamiento del Reference Router.

- Programar la interfaz PCI

  cpci_reprogram.pl -all

- Descargar el archivo Bitfile
  nf_download /root/netfpga/bitfiles/reference_router.bit

- Configurar las direcciones IP de los puertos a implementar

  Ifconfig eth0 192.168.1.1
  Ifconfig eth1 192.168.0.1
  Ifconfig nf2c1 192.168.1.2
  Ifconfig nf2c0 192.168.0.2

- Entrar a la carpeta SW del proyecto reference router
  Cd /root/netfpga/projects/reference_router/sw/

- Configurar la tabla de enrutamiento

  ./cli –r 0 192.168.1.0 255.255.255.0 192.168.1.1 2
  ./cli –r 1 192.168.0.0 255.255.255.0 192.168.0.1 1

- Configurar la tabla ARP del reference router

  ./cli -a 0 192.168.1.1 00:15:17:d6:1d:fc
  ./cli -a 1 192.168.0.1 00:15:17:d6:1d:fd

- Configurar las direcciones MAC del reference router
  ./cli -m 1 00:4E:46:32:43:00
  ./cli -m 2 00:4E:46:32:43:01

- Configurar la tabla ARP en LINUX
  arp -i nf2c0 -s 192.168.0.2 00:4E:46:32:43:00
  arp -i nf2c1 -s 192.168.1.2 00:4E:46:32:43:01
  arp -i eth0 -s 192.168.1.1 00:15:17:d6:1d:fc
  arp -i eth1 -s 192.168.0.1 00:15:17:d6:1d:fd

d. Resultados

- La verificacion de configuracion del ROUTER se observa a continuación:

Mediante el comando *./cli –L arp* se despliega la lista de la configuración hecha mediante el comando setarp, de igual forma modificando el ultimo campo de este comando por *rutas* o *mac* se puede observar la configuración realizada mediante *setip* y *setmac* respectivamente, la salida de cada una de estas listas se muestran a continuación; inicialmente en la figura 81 (a) se muestra la tabla arp configurada, en la figura 81(b) se muestra la configuración final del enrutamiento y en la figura 81 (C) se muestran las mac de los puertos fisicos de la NetFPGA.

```
[root@localhost sw]# ./cli -L arp
Found net device: nf2c0
> Entry #1:   IP: 192.168.1.1, MAC: 0:15:17:d6:1d:fc
Entry #2:   IP: 192.168.0.1, MAC: 0:15:17:d6:1d:fd
Entry #3:   --Invalid--
```

a. Tabla arp

```
[root@localhost sw]# ./cli -L rutas
Found net device: nf2c0
> Entry #0:   Subnet: 192.168.1.0, Mask: 0xffffff00, Next Hop: 192.168.1.1, Port: 0x02
Entry #1:   Subnet: 192.168.0.0, Mask: 0xffffff00, Next Hop: 192.168.0.1, Port: 0x01
Entry #2:   --Invalid--
```

b. Tabla de rutas

```
> [root@localhost sw]# ./cli -L mac
Found net device: nf2c0
> Port #1:   MAC: 0:4e:46:32:43:0
Port #2:   MAC: 0:4e:46:32:43:1
Port #3:   MAC: ca:fe:f0:d:0:3
Port #4:   MAC: ca:fe:f0:d:0:4
```

c. Tabla MAC

- En la figura 82 se muestra el funcionamiento del módulo reference router usando wireshark para capturar los paquetes que pasan por los puertos fisicos de la NetFPGA.

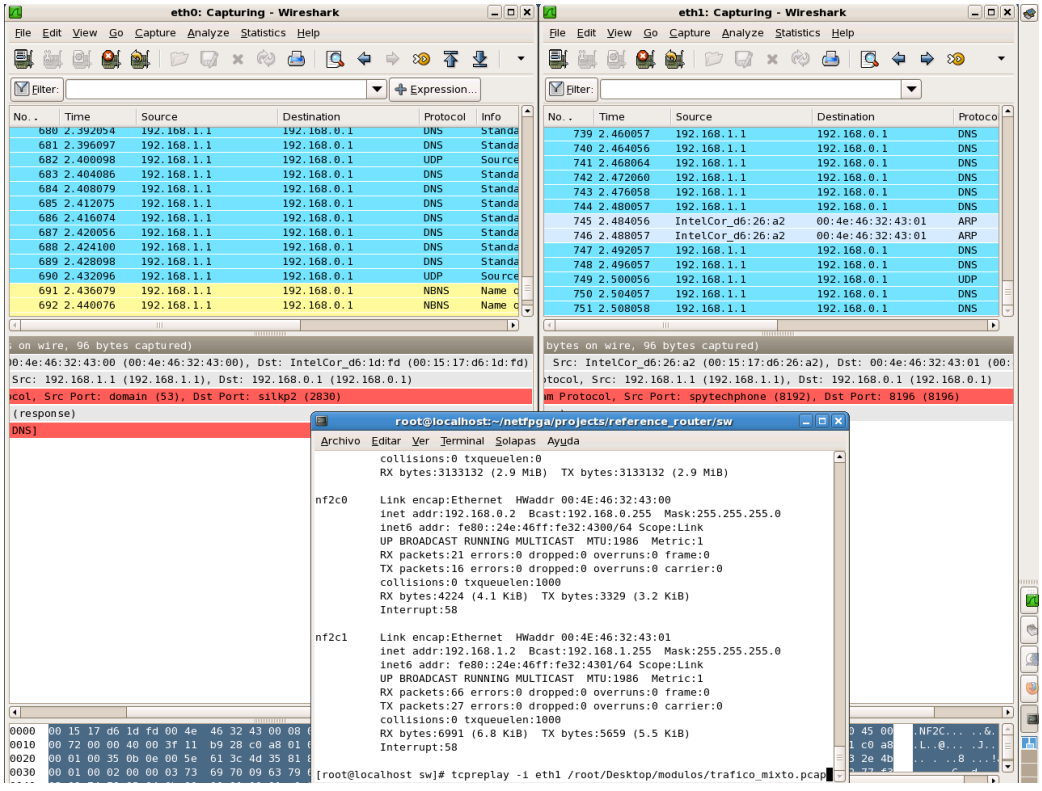


FIGURA 82. Prueba reference router con wireshark

En la imagen anterior se puede visualizar la interacción de comunicación entre los puertos eth0 y eth1 debido al enrutamiento asignado. Realizando pruebas con base a la configuración anterior se logró comprobar el router funcionaba de forma unidireccional y solo se podía establecer comunicación en un solo sentido, por lo cual fue necesario cambiar la configuración del mismo. Esto se describirá en la siguiente prueba.

10.9 Configuración bidireccional del Reference Router

a. Objetivo

Como se demostró con anterioridad mediante la configuración del reference router se obtuvo una comunicación unidireccional, por esta razón se hace necesario realizar cambios en la configuración con el fin de obtener una comunicación bidireccional.

b. Topología

Para la prueba se hizo uso de dos ordenares configurados con los parámetros adecuados para implementar el proyecto reference router mediante la NetFPGA como se muestra en la figura 83.

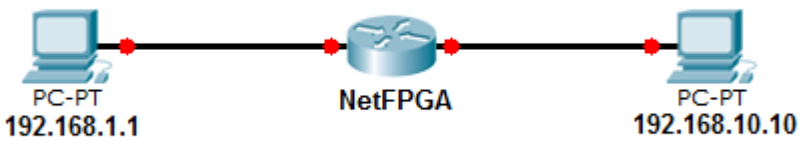


FIGURA 83. Topología Reference Router bidireccional

c. Procedimiento

Después de realizar las pruebas pertinentes para poder comunicar los dos equipos se tomó la decisión de dejar vacía la regla que contiene la tabla de enrutamiento, si bien esto hace que todas las direcciones que se tengan en una sub red puedan realizar el enrutamiento, este se limita con la configuración de reglas en iptables, de tal modo solo el equipo asignado puede tener acceso a la puerta de enlace sin ser bloqueado, esto se hace con el fin de evitar posibles intrusiones en la red y la configuración puede variar de acuerdo a las necesidades que se tengan entro de la red.

Para poder establecer la comunicación entre dos subredes diferentes se realizó la siguiente configuración en un terminal, la cual es ejecutada con un Shell cada vez que se quiera reconfigurar:

```
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
echo 1 > /proc/sys/net/ipv4/ip_forward

cpci_reprogram.pl -all
nf_download /root/netfpga/bitfiles/reference_router.bit


ifconfig nf2c1 192.168.1.2
ifconfig nf2c0 192.168.10.6

/root/netfpga/projects/reference_router/sw/cli -a 0 192.168.1.1 00:23:24:19:CF:D3
/root/netfpga/projects/reference_router/sw/cli -a 1 192.168.10.10
00:24:81:EA:C5:C2

/root/netfpga/projects/reference_router/sw/cli -m 2 00:4E:46:32:43:01
/root/netfpga/projects/reference_router/sw/cli -m 1 00:4E:46:32:43:00

/root/netfpga/projects/reference_router/sw/cli -L rutas
/root/netfpga/projects/reference_router/sw/cli -L arp
arp -a
```

d. Resultados

Para comprobar el correcto enrutamiento se realiza un ping entre los equipos, mediante wireshark se garantizó que los paquetes estuvieran siendo enviados y que la respectiva respuesta llegara

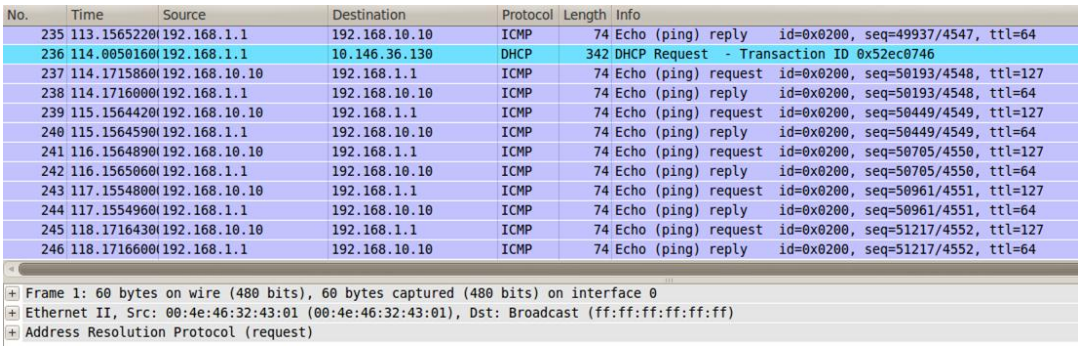


FIGURA 84. Prueba PING entre dos equipos con reference router

Es importante resaltar que para lograr la comunicación entre los equipos en las puertas de enlace de estos debe estar la dirección IP de los puertos usados en la NetFPGA, de otro modo no se podrá establecer comunicación entre ningún equipo

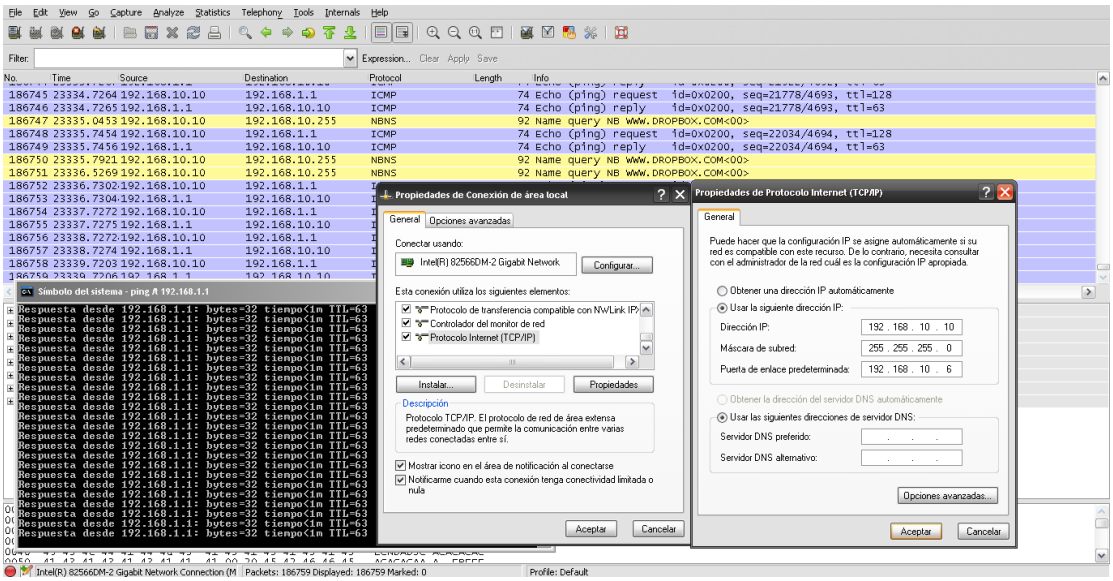


FIGURA 85. Configuración de puerta de enlace

Una vez conectados los equipos se pueden realizar los diferentes ataques mencionados con anterioridad y acceder a información de los equipos. Esto se observa en la figura 86.

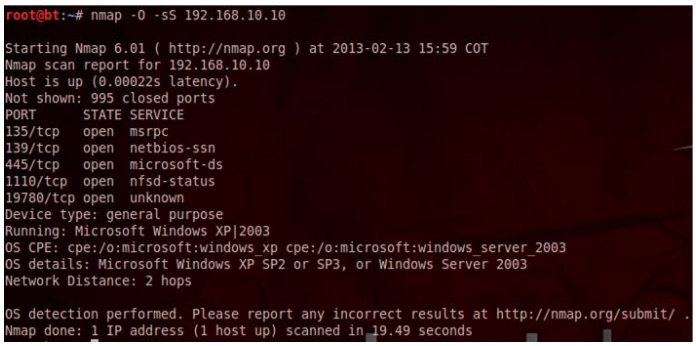


FIGURA 86. Ataque nmap con equipos conectados mediante reference router

10.10 Pruebas de comunicación en la red industrial

a. Objetivo

Implementar la NetFPGA para establecer una comunicación bidireccional que permita comunicar la red interna (industrial) y la red externa.

b. Topología

Al realizar las pruebas dentro de la red industrial se encontró que el switch que tiene la red no soporta la velocidad con la que trabajan los puertos Ethernet de la NetFPGA, debido a que la velocidad de estos son de 1Gb y el switch transmite a 100 Mb, por lo que se hizo necesaria la implementación de uno de los switches 3com 4500 con los que se cuenta en el laboratorio de redes.

Si bien se podría pensar que este cambio puede alterar el comportamiento de una red real, es importante aclarar que la única diferencia que existe entre el switch 3com y el Schneider es la cantidad de puertos disponibles, ya que el segundo mencionado tiene menor cantidad de puertos con el fin de evitar la congestión dentro de la red.

La red establecida se compone del ordenador externo de la red que se conecta a la tarjeta NetFPGA que establece la comunicación con el switch 3COM que contiene la red industrial compuesta por el PLC y su servidor. En la figura 87 se puede visualizar dicha configuración.

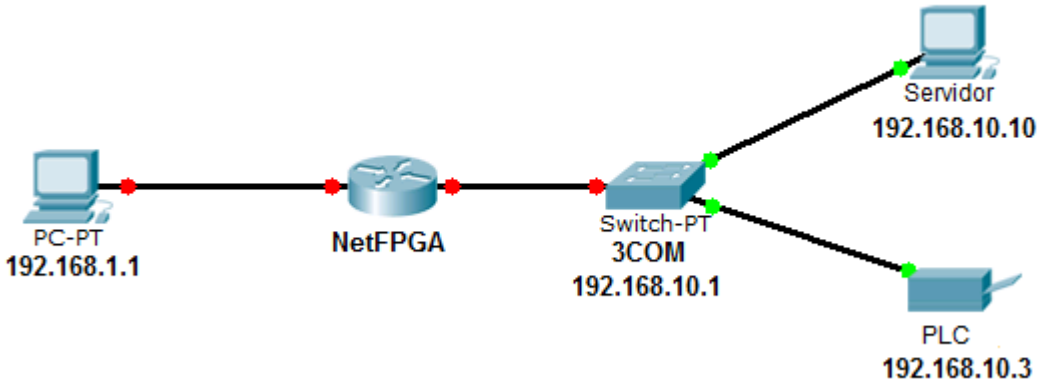


FIGURA 87. Topología red industrial con reference router

c. Procedimiento

Para establecer la comunicación entre los diferentes dispositivos se debe efectuar un cambio en la tabla ARP agregando los parámetros del switch.

```
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
echo 1 > /proc/sys/net/ipv4/ip_forward

cpci_reprogram.pl -all
nf_download /root/netfpga/bitfiles/reference_router.bit


ifconfig nf2c1 192.168.1.2
ifconfig nf2c0 192.168.10.6

/root/netfpga/projects/reference_router/sw/cli -a 0 192.168.1.1 00:23:24:19:CF:D3

/root/netfpga/projects/reference_router/sw/cli -a 1 192.168.10.1
40:01:C6:BD:AE:C1

/root/netfpga/projects/reference_router/sw/cli -m 2 00:4E:46:32:43:01
/root/netfpga/projects/reference_router/sw/cli -m 1 00:4E:46:32:43:00

/root/netfpga/projects/reference_router/sw/cli -L rutas
/root/netfpga/projects/reference_router/sw/cli -L arp
arp –a
```

d. Resultados

El resultado del enrutamiento se conoce aplicando un ping entre los equipos involucrados, buscando comprobar que los dos se encuentran comunicados entre sí.

No.	Time	Source	Destination	Protocol	Length	Info
2626	877.6014000(	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0200, seq=27667/4972, ttl=64
2627	877.9950250(	192.168.1.1	10.146.36.130	DHCP	342	DHCP Request - Transaction ID 0x52ec0746
2628	878.5926160(	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) request id=0x0200, seq=27923/4973, ttl=127
2629	878.5926370(	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0200, seq=27923/4973, ttl=64
2630	879.5926280(	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) request id=0x0200, seq=28179/4974, ttl=127
2631	879.5926480(	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0200, seq=28179/4974, ttl=64
2632	880.5926290(	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) request id=0x0200, seq=28435/4975, ttl=127
2633	880.5926480(	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0200, seq=28435/4975, ttl=64
2634	881.5926160(	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) request id=0x0200, seq=28691/4976, ttl=127
2635	881.5926370(	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0200, seq=28691/4976, ttl=64
2636	882.5926500(	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) request id=0x0200, seq=28947/4977, ttl=127
2637	882.5926710(	192.168.1.1	192.168.1.2	ICMP	74	Echo (ping) reply id=0x0200, seq=28947/4977, ttl=64

FIGURA 88.Resultados de comunicación en la red industrial con Reference Router

La topología presente en la red se puede obtener realizando un análisis con Zenmap, dicho análisis arrojó como resultado la manera en que cada uno de los equipos está conectado a la red y la forma en que se realiza el enrutamiento, el localhost representa el equipo desde donde se realizó la prueba y a su vez como esté se conecta con el switch y los equipos que se encuentran conectados a él, en este caso específico se tratan del PLC y el Servidor.

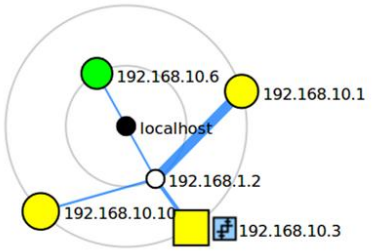


FIGURA 89. Topología de red con Zenmap

De igual manera se analizan los diferentes puertos abiertos de los equipos por donde pueden ser atacados para poder ser contrarrestados posteriormente, en la figura 89 en particular se observa que el PLC tiene 4 puertos TCP abiertos, se encuentra conectado a la red y tiene un sistema operativo VxWorks 5.4.

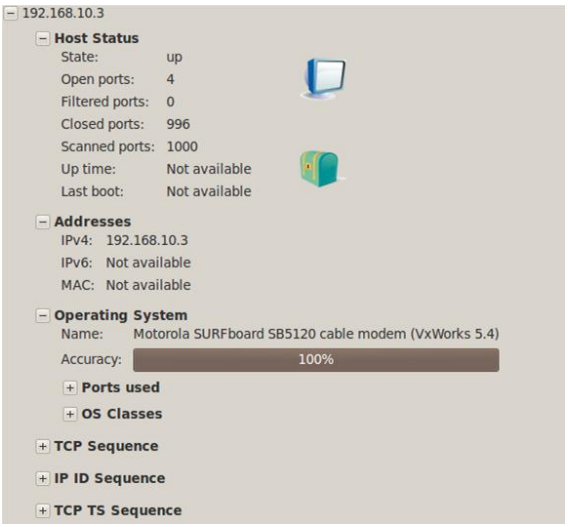


FIGURA 90. Respuesta al análisis del PLC mediante Zenmap

10.11 Reference Router e IPTABLES

a. Objetivo

Utilizar la tarjeta NetFPGA para establecer la comunicación entre la red externa e interna, limitando servicios que comprometen la seguridad de la red interna mediante el bloqueo de puertos utilizando la herramienta IPTABLES de Linux, de esta forma se obtiene el primer prototipo de firewall para la red industrial protegiendo el PLC y el servidor.

b. Topología

Para esta prueba se configuran los parámetros adecuados en cada uno de los dispositivos y es establece la red como se muestra en la figura 91.

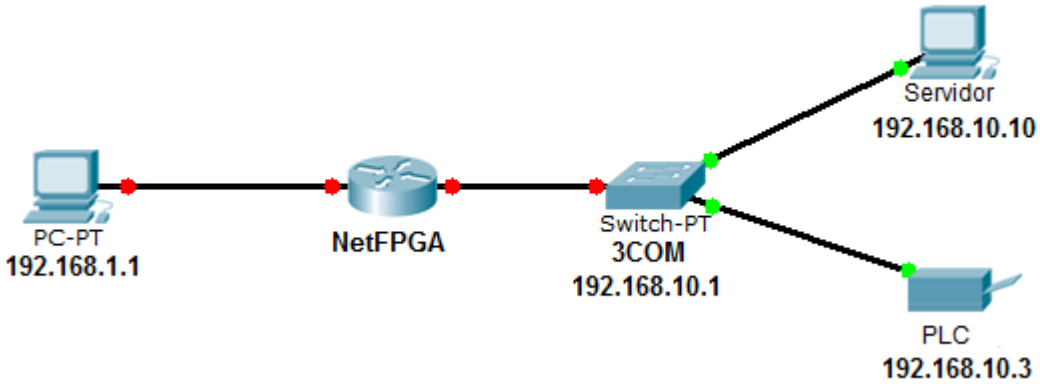


FIGURA 91.Topología de red industrial

c. Procedimiento

- se configuran los parámetros iniciales y las políticas determinadas de IPTABLES

```
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
```

- configuracion bidireccional del reference router

```
echo 1 > /proc/sys/net/ipv4/ip_forward

cpci_reprogram.pl -all
nf_download /root/netfpga/bitfiles/reference_router.bit


ifconfig nf2c1 192.168.1.2
ifconfig nf2c0 192.168.10.6

/root/netfpga/projects/reference_router/sw/cli -a 0 192.168.1.1 00:23:24:19:CF:D3
/root/netfpga/projects/reference_router/sw/cli -a 1 192.168.10.1
40:01:C6:BD:AE:C1
```

```
/root/netfpga/projects/reference_router/sw/cli -m 2 00:4E:46:32:43:01
/root/netfpga/projects/reference_router/sw/cli -m 1 00:4E:46:32:43:00
```

- Establecer reglas de IPTABLES

Es importante mencionar que con la implementación del módulo configurado se logran contrarrestar los ataques dándole más fiabilidad a la red. Tratándose de un tema de seguridad es importante hacer sistemas sólidos y complejos, por esta razón no está de más complementar el funcionamiento de la NetFPGA con el firewall de Linux configurado de la siguiente manera:

```
iptables -A FORWARD -p icmp -s 192.168.1.2 -j DROP  #bloquear ping
iptables -A FORWARD -p icmp -s 192.168.10.6 -j DROP #bloquear ping
iptables -A FORWARD -p icmp -d 192.168.10.3 -j DROP #bloquear ping
iptables -A FORWARD -p tcp --dport 502 -j DROP  #bloquear puerto MODBUS
iptables -A INPUT -p tcp --dport 513 -j DROP   #bloquear servicio rlogin
iptables -A INPUT -p tcp --dport 514 -j DROP   #bloquear servicio rsh
iptables -A INPUT -p udp --dport 69 -j DROP   #bloquear servicio TFTP
iptables -A INPUT -p tcp --dport 1034 -j DROP #puerto que utiliza el computador
```

De esta forma se logra configurar el firewall de forma adecuada, cada uno de los puertos bloqueados para la red constituyen a un riesgo potencial para la seguridad de la red interna por esta razón se establecen dichas políticas.

Puerto 502: Puerto de comunicación implementado por el PLC
Puerto 513: Usado para el servicio de login remoto
Puerto 514: Usado para los servicios de rsh que se implementa para usos remotos
Puerto 69: Servicios TFTP, utilizados para crear y transferir archivos dentro del sistema

De esta forma se bloquean diversos ataques que pueden resultar peligrosos para la red y los equipos que la integran.

d. Resultados

Se implementó el software metasploit para atacar el PLC mediante su dirección IP 192.169.10.3, pero al bloquear el puerto 502 no es posible realizar el cambio de estado en el PLC, ni mucho menos sustraer la programación que este presenta, ya que el módulo de metasploit encargado de realizar estos ataques agota el tiempo de espera. Esto se puede visualizar en la figura 92.

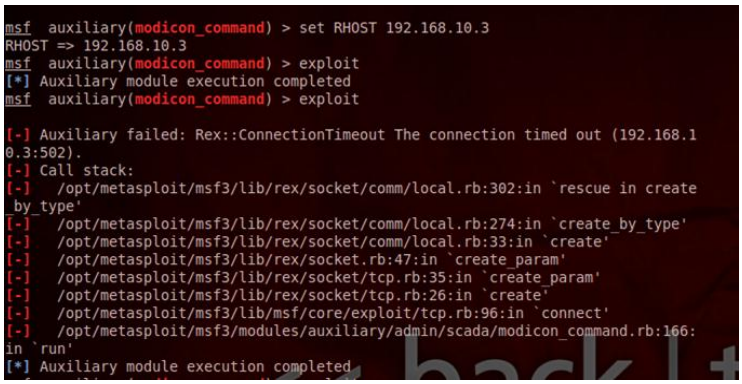


FIGURA 92. Bloqueo del ataque modicon_comand mediante iptables

Al realizar el bloqueo de puertos y protocolos también se impide el paso de paquetes ICMP que son los encargados de realizar el ping y son utilizados por diferentes herramientas como Nmap para realizar sus sondeos a la red, lo que garantiza una mejora notable en la seguridad de esta, ya que no se puede acceder a las posibles vulnerabilidades presentes en los equipos. Esto se observa en la figura 93.Se observa que se hace ping a la dirección del PLC y no se establece la comunicación.

FIGURA 93. Bloqueo de ping en la red industrial mediante iptables

10.12 FIREWALL RECHAZADOR DE PAQUETES

a. Criterios de diseño

Se decide utilizar el proyecto tokenr_bucket del sistema U2-Route con el fin de neutralizar los ataques de denegación de servicio. Se parte del hecho que los ataques de denegación de servicio envían una gran cantidad de paquetes para saturar el equipo víctima. El algoritmo de token bucket que se utiliza elimina los paquetes que no cumplen con los parámetros de QoS (que superan el tamaño de la ráfaga), por lo que se conoce como un token bucket rechazador. Un argumento en contra de usar este algoritmo sería que se pierden ciertos paquetes. Sin embargo, partimos del supuesto de que hay un comportamiento anormal en que el atacante envía demasiados paquetes, por lo que si esto ocurre, no hay problema en que se pierdan órdenes en la red industrial, ya que son producto de un ataque.

Como el Firewall se pone en el borde de la red hacia el exterior, las órdenes internas de la red industrial no se ven afectadas.

El algoritmo del token bucket también sirve como método para contrarrestar ataques que buscan encontrar vulnerabilidades, tales como los realizados con metasploit, nmap, netdiscover, etc. Esto se debe a que el principio que estos programas utilizan es el envío de ráfagas hacia los equipos de la red. Por tanto, el algoritmo de token bucket rechazador fue sintonizado hasta encontrar los valores que permitían que no prosperasen estos ataques.

Se intentó hacer algo similar con el token bucket recortador (retrasa los paquetes), pero se tuvo el inconveniente que ante el ataque de denegación de servicio se llenaba el buffer de almacenamiento de la netfpga y se bloqueaba el firewall.

b. Topología

Una vez configurado el firewall en la tarjeta NetFPGA se implementa en la red industrial con el fin de comprobar que las vulnerabilidades y los ataques presentados con anterioridad, ya no comprometen la seguridad de la red debido al funcionamiento del mismo.

Para realizar las pruebas se implementó la NetFPGA estableciendo la comunicación de la red industrial con la red interna como se muestra en la figura 94.

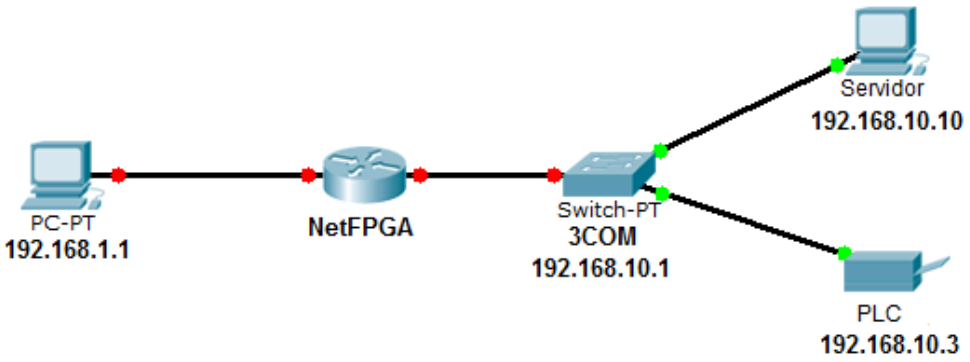


FIGURA 94.Topología de la Red Industrial con Firewall

c. Procedimiento

Como se mencionó anteriormente el módulo del token bucket rechazador se ajusta a las necesidades del proyecto por las características de su funcionamiento, por

esta razón a continuación se realizara la configuración del mismo mediante el CLI original. Este módulo se basa en el proyecto Reference Router, por esta razón fue necesario hacer los estudios preliminares de funcionamiento mostrados en el desarrollo del proyecto.

Configuración mediante el terminal de Linux

```
echo 1 > /proc/sys/net/ipv4/ip_forward

cpci_reprogram.pl –all

nf_download /root/netfpga/bitfiles/tokenr_bucket.bit

ifconfig nf2c1 192.168.1.2
ifconfig nf2c0 192.168.10.6
cd /root/netfpga/projects/tokenr_bucket/sw/
./cli
setarp 0 192.168.1.1 00:23:24:19:CF:D3
setarp 1 192.168.10.1 40:01:C6:BD:AE:C1
setarp 2 192.168.1.2 00:4E:46:32:43:01
setarp 3 192.168.10.6 00:4E:46:32:43:00
setmac 2 00:4E:46:32:43:01
setmac 1 00:4E:46:32:43:00
settok a 2e ef ff
```

Para llegar a los datos que se usaron en el comando settok se realizó un proceso de sintonización el cual tuvo como fin encontrar valores que no interfieran con una comunicación normal, pero no permitan que se realice un ataque de denegación de servicio, se realizaron una serie de pruebas con un archivo que contenía 12.777 paquetes buscando que solo pasaran aproximadamente el 15% de estos. Se deja un tamaño determinado de token y de bucket para obtener un tamaño de tasa máximo de la ráfaga constante y así variar solo los dos divisores de frecuencia para modificar la velocidad a la que llegan los tokens al bucket y por ende la tasa media.

Tam_token	Tam_bucket	Base_Temp	Tasa_lleg	Paquetes
A	2E	AA	A8	12761
A	2E	AA	A9	12741
A	2E	AA	AA	12669
A	2E	AA	AB	12597
A	2E	AA	B2	12113
A	2E	AA	B9	11667
A	2E	EF	FF	1680

Tabla 5. Pruebas de sintonización Tokenr bucket

Cabe resaltar que en las pruebas realizadas del firewall final no se incluye el uso de iptables porque en las pruebas preliminares en el proyecto ya se comprobó la funcionalidad de dicha herramienta, solo se hace mención como un complemento que puede proporcionar mayor seguridad a la red

d. Resultados

Para obtener los resultados de funcionamiento se realizan los ataques desarrollados en la realización del proyecto

- NetDiscover

a. Objetivo

Escanear la red con el fin de encontrar los dispositivos conectados verificando el funcionamiento del firewall.

b. Procedimiento y resultados

Se realizó un escaneo de la red con el software Netdiscover, como se puede observar en la imagen que se presenta en la figura 95, no se obtuvo resultado de la información de la red ni los dispositivos que la componen, lo que brinda privacidad a la red ocultando identidades que luego pueden ser objeto de suplantación.

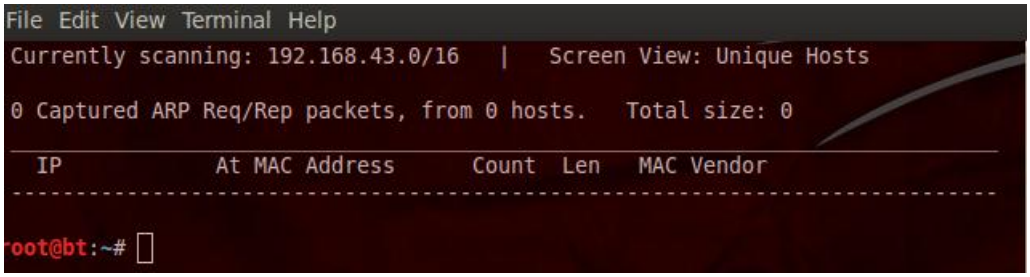


FIGURA 95.Bloqueo del ataque NetDiscover.

- Nmap

a. Objetivo

Escanear la red mediante NMAP y determinar la fiabilidad del firewall ante dicha herramienta.

b. Procedimiento y resultados

Se hace uso del software NMAP en sus diferentes opciones de escaneo como se mostró con anterioridad en el proyecto (sS, sU, O, mtu), para determinar puertos abiertos y los sistemas operativos que utilizan los dispositivos que permitan encontrar vulnerabilidades y puntos clave a la hora de atacar, al implementar el software se encontró un bloqueo en la prueba debido al firewall como se muestra en la figura 96.

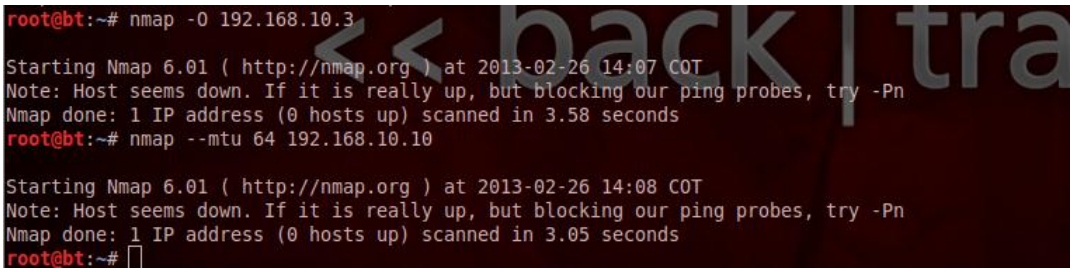


FIGURA 96.Bloqueo Nmap con firewall implementado

A consecuencia del bloqueo de NMAP, el software ZENMAP también queda inhabilitado ya que la base de funcionamiento es la misma.

- Metasploit

a. Objetivo

Implementar las herramientas de metasploit para atacar la red determinando la fiabilidad del firewall ante ataques activos que comprometen la seguridad del sistema.

b. Procedimiento y resultados

Se implementó METASPLOIT para realizar ataques activos a la red, en la figura 97 que se muestra a continuación se logra visualizar él envió del ataque STOP/RUN

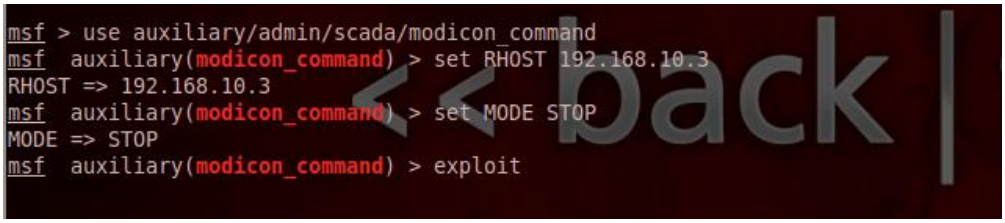


FIGURA 97. Bloqueo ataque modicon_command mediante firewall

Antes de realizar la prueba el PLC fue configurado de forma adecuada y su funcionamiento puesto en modo RUN, el objetivo del ataque era cambiar el modo de funcionamiento a modalidad STOP como se logró con anterioridad, pero debido al firewall el exploit enviado no alcanza su objetivo y su envió no es satisfactorio, por lo cual se mantiene el funcionamiento de la red como su servidor lo establece.

Ahora como en el caso anterior se realiza el proceso para extraer la programación del PLC, obteniendo el mismo resultado, como se muestra en la figura 98.

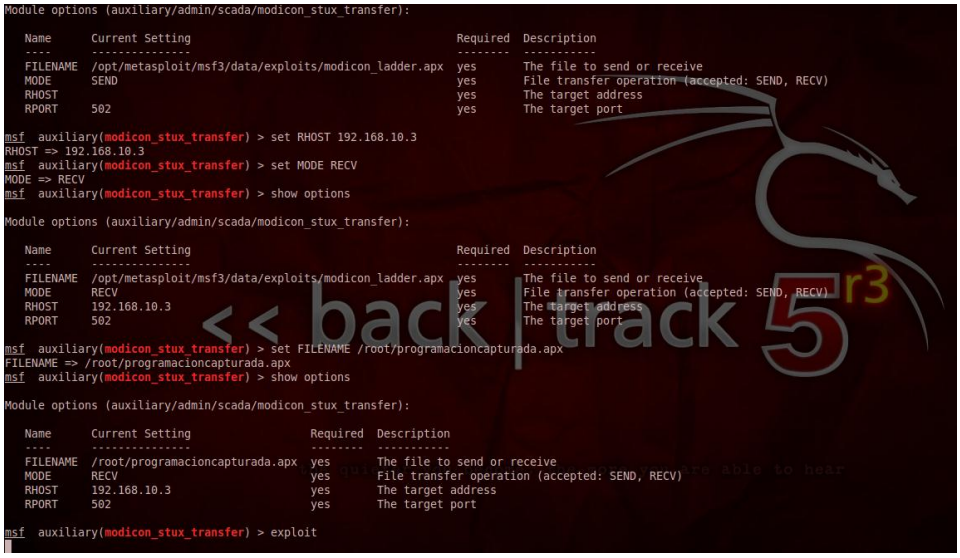


FIGURA 98. Bloqueo ataque modicon_stux_transfer mediante firewall

En la figura 99 se muestra que la comunicación de la red se encuentra habilitada y que los ataques fueron bloqueados por la implementación del firewall en este caso no se bloqueó el ping entre los equipos porque no se configuraron las reglas complementarias de IPTABLES.

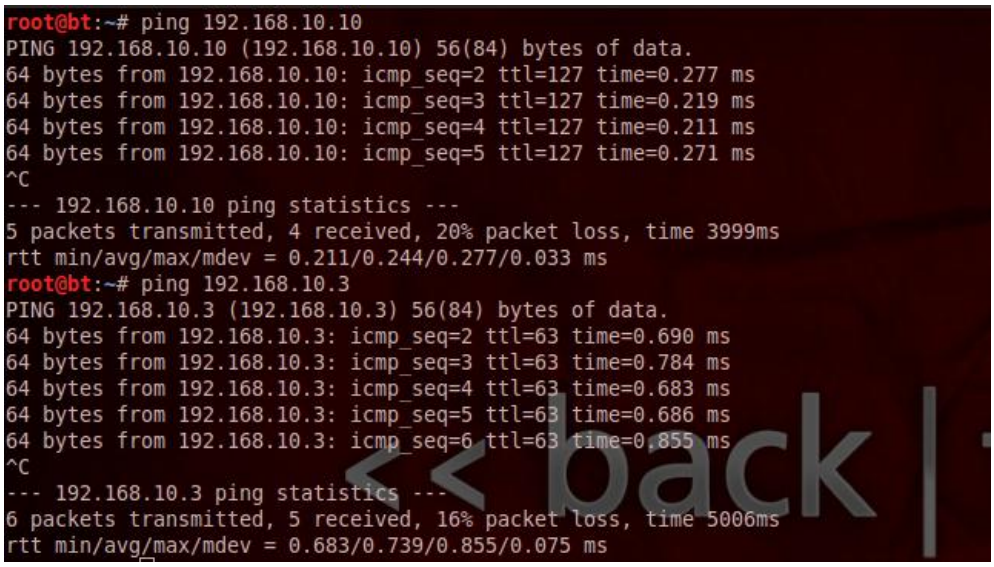


FIGURA 99.Bloqueo PING mediante firewall

10.13 DISEÑO DEL FIREWALL CON FILTRADO DE PAQUETES

a.criterios de diseño

Para el diseño del firewall con función de filtrado se hace uso del proyecto packet_market del sistema U2-Route, el cual fue modificado con el fin de adecuarlo a las necesidades del proyecto permitiendo la limitación de flujo de paquetes brindando seguridad a la red.

b. procedimiento

Como se mencionó con anterioridad fue necesario modificar el proyecto packet_market, ya que este únicamente realizaba la marcación de paquetes, por esta razón se complementaron las líneas de programación agregando condicionales que permiten eliminar paquetes que cumplen con ciertas características establecidas.

La configuración del firewall de filtrado de paquetes se realiza mediante el CLI modificado de la siguiente forma:

iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain

echo 1 > /proc/sys/net/ipv4/ip_forward

cpci_reprogram.pl -all
nf_download /root/netfpga/bitfiles/packet_marker.bit

ifconfig nf2c1 192.168.1.2
ifconfig nf2c0 192.168.10.6

/root/netfpga/projects/packet_marker/sw/cli -a 2 192.168.1.2 00:4E:46:32:43:01
/root/netfpga/projects/packet_marker/sw/cli -a 3 192.168.10.6 00:4E:46:32:43:00
/root/netfpga/projects/packet_marker/sw/cli -a 0 192.168.1.1 00:23:24:19:CF:D3
/root/netfpga/projects/packet_marker/sw/cli -a 1 192.168.10.10 00:23:24:19:d0:cb

/root/netfpga/projects/packet_marker/sw/cli -r 0 192.168.1.0 255.255.255.0 192.168.1.1 2
/root/netfpga/projects/packet_marker/sw/cli -r 1 192.168.10.0 255.255.255.0 192.168.10.10 1

/root/netfpga/projects/packet_marker/sw/cli -m 2 00:4E:46:32:43:01
/root/netfpga/projects/packet_marker/sw/cli -m 1 00:4E:46:32:43:00

/root/netfpga/projects/packet_marker/sw/cli -L rutas
/root/netfpga/projects/packet_marker/sw/cli -L arp
/root/netfpga/projects/packet_marker/sw/cli -L tos

iptables -nL

El programa permite establecer 15 reglas para el filtrado de paquetes basándose en los puertos de comunicación implementados. Para la eliminar paquetes se debe realizar la marcación con el valor hexadecimal “a”, ya que en la programación del proyecto se estableció que los paquetes que se marcan con dicho valor son eliminados. La configuración de las reglas en la netfpga se hacen mediante la función “-t” del cli modificado

/root/netfpga/projects/packet_marker/sw/cli -t 0 a 6 c29 50

Donde:

0	Equivale al número de la regla (0-14)
a	Corresponde al valor hexadecimal con el cual se marca el campo DSCP del paquete
6	Identificación numérica del protocolo
C29	Puerto de origen en hexadecimal
50	Puerto destino en hexadecimal

Tabla 6. Descripción regla de filtrado

c. Resultados

Para comprobar el funcionamiento del filtrado de paquetes se inyecto un archivo *.pcap* que contiene 8623 paquetes constituidos de la siguiente forma

Numero de paquetes	Puerto origen	Puerto destino
4083	3113	80
4540	56891	80

Tabla 7. Número de paquetes por puerto

En la figura 100 se muestra la captura de los paquetes sin reglas de filtrado programadas.

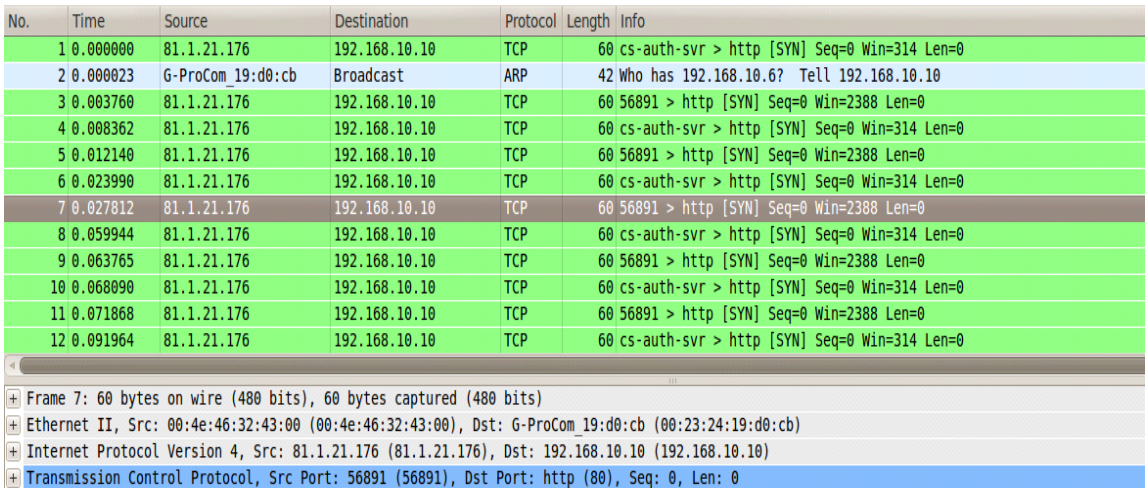


FIGURA 100. Paquetes sin regla de filtrado

Luego se configura la siguiente regla

/root/netfpga/projects/packet_marker/sw/cli -t 0 a 6 c29 50

Dicha regla marca con el valor “a” los paquetes TCP que tiene Puerto de origen c29 (3113 en decimal) y puerto destino 50 (80 en decimal), al marcarlos con el valor mencionado son eliminados por esta razón como se muestra en la figura 101 solo llegan los paquetes que no están marcados.

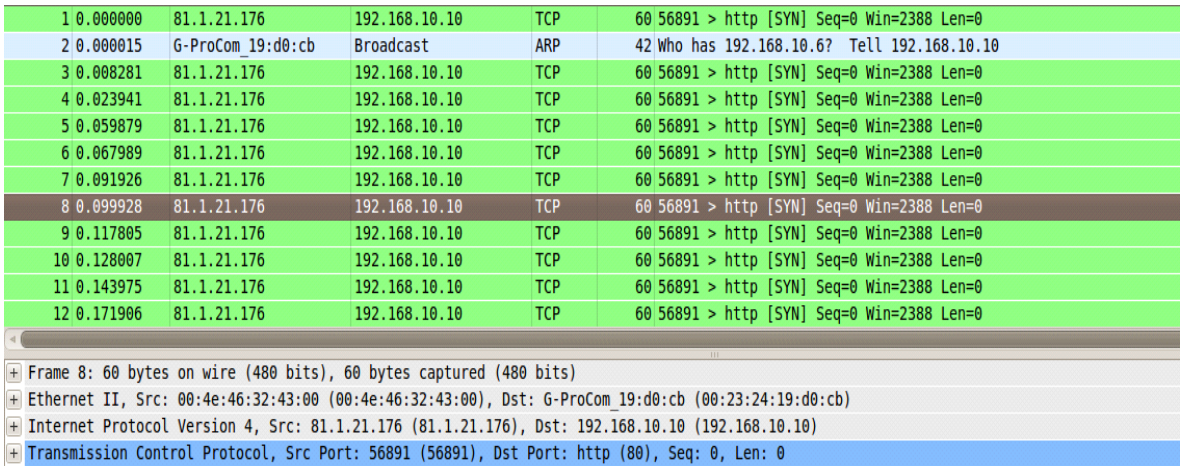


FIGURA 101.Regla de filtrado al puerto c29

Luego se reemplaza la regla para bloquear el flujo de paquetes provenientes del puerto 56891(decimal) y habilitar de nuevo el flujo de los paquetes provenientes del puerto 3113 (decimal)

/root/netfpga/projects/packet_marker/sw/cli -t 0 a 6 de3b 50

Como se puede visualizar en la figura 102 solo llegan los paquetes provenientes del puerto 3113 (decimal)

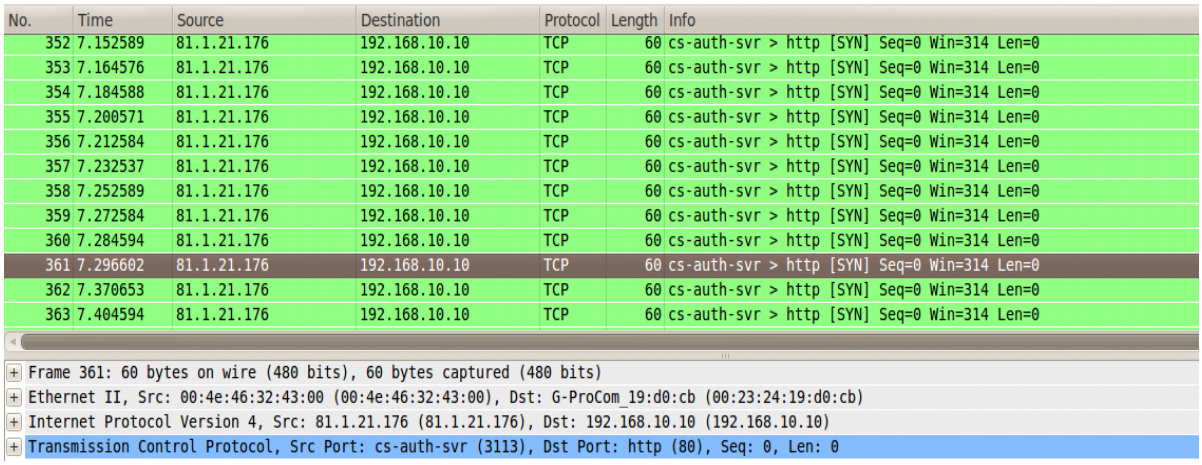


FIGURA 102. Regla de filtrado al puerto de3b

Si se desea bloquear el flujo de todos los paquetes del archivo *.pcap* de prueba se debe configurar de la siguiente forma.

/root/netfpga/projects/packet_marker/sw/cli -t 0 a 6 c29 50

/root/netfpga/projects/packet_marker/sw/cli -t 1 a 6 de3b 50

Una vez obtenido el filtrado de paquetes deseado se realizó un análisis en el cual se determinó que para el control de flujo de las comunicaciones resultaba más conveniente el uso de una lista de permitidos como se realiza en los dispositivos comerciales para seguridad, por esta razón se modificó el funcionamiento del filtrado de paquetes para que únicamente los paquetes que fueran marcados con el valor numérico “a” puedan atravesar la red y el resto de paquetes no marcados son rechazados por la NetFPGA, para que esta manera el usuario pueda establecer la lista de permitidos contrarrestando los ataques que comprometan la red.

CONCLUSIONES Y TRABAJOS FUTUROS

- Durante el desarrollo del proyecto se comprobó la necesidad de establecer criterios de seguridad en las redes de comunicación especialmente cuando las consecuencias de un mal manejo puede afectar la vida de personas.

- Todo sistema de comunicación es vulnerable y puede ser objetivo de ataques, por esta razón establecer políticas de seguridad que permitan reducir los riesgos potenciales es de suma importancia, también es cierto que día a día se producen nuevos software maliciosos que afectan la red, por esta razón es necesario estar a la vanguardia de estos temas y establecer los nuevos criterios pertinentes para brindar seguridad.

- A raíz del auge tecnológico que se vive en la actualidad se hace necesario automatizar los diferentes procesos industriales para mantenerse competitivos en el mercado, por esta razón es de gran importancia desarrollar sistemas de seguridad para las redes industriales que brinden seguridad a los procesos y a la vida de las personas.

- El uso de la tarjeta NetFPGA para crear un firewall es de gran importancia, ya que es una herramienta poco documentada y explorada dificultando la explotación de vulnerabilidades del sistema.

- Actualmente cualquier persona con intenciones maliciosas puede instruirse para atentar contra los sistemas de comunicación, debido a la gran cantidad de documentos y tutoriales que mediante el uso de programas, como los mencionados en el proyecto, permiten explotar las debilidades de cada una de las redes.

- La implementación adecuada del sistema Linux Backtrack con fines de análisis y detección de problemas en la red resulta de gran utilidad a la hora de crear un firewall, ya que permite identificar de manera práctica vulnerabilidades y posibles riesgos de la red con el fin de fortalecer los puntos frágiles mediante criterios de seguridad, aunque este sistema operativo también facilita el trabajo de los atacantes cuando se tienen bajos niveles de seguridad.

- Se comprobó de manera práctica que mediante la implementación de firewall desarrollado en el proyecto se logra fortalecer la seguridad de la red, bloqueando el acceso de programas que comprometen la seguridad del sistemas, aunque es importante mencionar que el personal operario de los procesos juega un papel fundamental para mantener la estabilidad del mismo porque los ataques que se hacen a nivel interno en la red industrial tienen todos los privilegios del sistema.

- Se debe resaltar que durante el desarrollo del proyecto se encontraron limitantes en algunos módulos previamente programados en la NetFPGA, como lo fue el priority token, lo que impidió que dichos módulos pudieran ser implementados correctamente.

BIBLIOGRAFIA

A.Nicholson. SCADA security in the light of Cyber-Warfare. EN: Computers & Security. N° 31 (Junio de 2012); pag 418-436.

BAILEY, David. SCADA systems, hardware and firmware; EN: Practical SCADA for Industry, Newnes. P 17.

CHAPPELL,Laura. Wireshark Network Analisis 2nd edition,Chappell University,2012, 1094 p.

FAIRCLOTH, Jeremy. Network devices. EN: Penetration Tester's Open Source Toolkit. SYNGRESS, 2011; Pag 259-290.

GOLD, Steve. Stuxnet may be the work of state-backed hackers . EN: Network Security. Septiembre de 2010; pag 2 y 19.

HUITSING, Peter. Attack taxonomies for the Modbus protocols. EN: International Journal of Critical Infrastructure Protection. N° 1 (Diciembre de 2008); Pag 37-44

HUNT, Ray. Internet/Intranet firewall security-policy, architecture and transaction services. EN: Computer Communications. N° 21 (Septiembre de 1998); pag 1107-1123.

IGURE,Vinay. Security issues in SCADA networks, EN: Computers & Security. N° 25 (Octubre de 2006); pag 498-506.

KAMARA,Seny. Analysis of vulnerabilities in Internet firewalls.EN: Computers & Security. N° 22 (Abril de 2003); pag 214-232.

KNAPP,Eric. Industrial Network Security:Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress 2011; p 341.

MAYNOR,David. Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulenrability Research. Elsevier Inc, 2007; pag 1-64.

MAYNOR, David. Syngress Force Emerging Threat Analysis. Elsevier Inc, 2006; pag 577-596

MAXWELL, Adam. The very unofficial dummies guide to scapy. Enero 2012;p47

MENDIBURU, Henry A. Automatización medio ambiental, INDECOPI 2003; p 53-57

OREBAUGH ,Angela. Nmap in the Enterprise: Your guide to network scanning. Elsevier Inc, 2008; pag

PADILLA, Jhon Jairo. Introducción a las Redes industriales, notas de clase [en línea¨].<http://jpadilla.docentes.upbbga.edu.co/redes_industriales/1Introduccion.pdf> [citado en 17 de octubre de 2012]

PADILLA, Jhon Jairo. U2 route: Guía Práctica. Sic Editorial Ltda, 2011; pag 117

PADILLA, Jhon Jairo. U2 route: Teoría y Diseño . Sic Editorial Ltda, 2011; pag 110

PATEL, M. Development of a novel SCADA system for laboratory testing. En: ISA Transactions. N° 43 (Julio de 2004); pag 477-490.

NAI, Igor. An experimental investigation of malware attacks on SCADA systems. EN:International Journal of Critical Infrastructure Protection. N° 2 (Diciembre de 2009); pag 139-145.

RALSTON,Patricia. Cyber security risk assessment for SCADA and DCS networks. EN: ISA Transactions. N°46 (Octubre de 2007); pag 583-584.

RAMAZAN,Bayindir. A water pumping control system with a programmable logic controller (PLC) and industrial wireless modules for industrial plants—An experimental setup. EN: ISA Transactions. N°50 (Abril de 2011); pag 321-328

STALLINGS, William. Cryptography and Network Security. Prentice Hall Press,2005. P 592.

STANGER, James. Hack Proofing Linux:The Only Way to Stop a Hacker Is to Think Like One, Elsevier Inc, 2001; pag 445-506.

STOJANOVSKI,Nenad.Architecture of a Identity based firewall system.EN: International Journal of Network Security & Its Applications (IJNSA). N° 3(Julio de 2011); pag 23-31.

ZWICKY, Elizabeth. O'Reilly Media, Inc, USA; Edición: 2nd Revised edition ,O'reilly, 2000, 896 p.

NetFPGA [en linea] <http://www.netfpga.org/php/specs.php> [citado 29 de septiembre de 2012]

Características NetFPGA. [en línea] < http://www.netfpga.org/php/specs.php > [citado 18 de octubre de 2012]

Guia NetFPGA [en línea] < http://netfpga.org/foswiki/bin/view/NetFPGA/OneGig/Guide> [citado 18 de octubre de 2012]

Introducción a la seguridad. [en línea] <http://jcef.sourceforge.net/doc/introsecurity.pdf> [citado 25 de octubre 2012].

Netdiscover [en línea] < http://nixgeneration.com/~jaime/netdiscover/> [citado 5 de enero de 2013]

Important security notification – Quantum and Premium communication modules (ICSALERT-12-020-03) [en línea] < http://www.global-download.schneider-electric.com/mainRepository/EDMS_CORP7.nsf/69f5d72c7a0cf811c12573d80038 9503/05e789c0e6c47c6585257a63005d9d1f/$FILE/RES207378.pdf> [citado 15 de enero de 2013]

FIREWALLS [en línea] <http://spi1.nisu.org/recop/al01/dulzon/index.html> [citado 17 de enero de 2013]

TOFINO Firewall [en línea] < http://www.tofinosecurity.com/products/Tofino-Firewall-LSM> [citado 25 de enero de 2013]

Firewall MODBUS [en línea] <http://www.tofinosecurity.com/products/Tofino-Modbus-TCP-Enforcer-LSM> [citado 25 de enero de 2013]

Datasheet EPS9211 [en línea] <http://www.mtl-inst.com/images/uploads/datasheets/tofino/EPS9211-ET.pdf> [citado 25 de enero de 2013]

Introducción al análisis de puertos [en línea] < http://nmap.org/man/es/man-port-scanning-basics.html> [citado 26 de enero de 2013]

Tecnicas de sondeo de puertos [en línea] < http://nmap.org/man/es/man-port-scanning-techniques.html> [citado 26 de enero de 2013]

Detección de servicios y versiones [en línea] < http://nmap.org/man/es/man-version-detection.html> [citado 26 de enero de 2013]

Manipulación avanzada de paquetes TCP/IP con scapy.[en línea]<http://www.hackxcrack.es/cuadernos/tcpip2/> [citado 29 de enero de 2013]

Metasploit Modules [en línea] < http://www.digitalbond.com/tools/basecamp/metasploit-modules/> [citado 2 de febrero de 2013]

Reference Router [en línea] <http://keb302.ecs.umass.edu/de4web/DE4_NetFPGA/?q=node/23> [citado 3 de febrero de 2013]

Familia 3Com® Switch 4500 10/100[En línea] <http://www.tarconis.com/documentos/3COM_4500ds.pdf> [citado en 2013]

Schneider Electric [en línea] <http://www.schneider-electric.cl/sites/chile/es/productos-servicios/automatizacion-control/oferta-de-productos/presentacion-de-rango.page?c_filepath=/templatedata/Offer_Presentation/3_Range_Datasheet/data/es/local/automation_and_control/modicon_premium.xml#> [citado 2013]