ISBN: 978-628-95207-4-3. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2023.1.1.868

Vulnerability analysis of a Raspberry Pi in a simulated environment

Genessis M. Enriquez, Eng [1], y Néstor X. Arreaga, Msig[2]
[1,2] Escuela Superior Politécnica del Litoral, ESPOL, Polytechnic University, FIEC, Campus Gustavo Galindo Km. 30.5 Vía Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador, gemaenri@espol.edu.ec, *narreaga@espol.edu.ec*

Abstact– IoT devices are currently part of our environment, collecting confidential data and information. Therefore, it is important to know what vulnerabilities are present in the devices that are being used. This study shows that Raspberry Pi devices do not have a defense system that detects malicious or virus-infected files. This is one of the reasons why they are vulnerable to various attacks. To test this, three different attacks–Man In The Middle (MITM), Backdoor and Denial of Service (DoS)–were performed on the Raspberry Pi device using a virtual machine with the Kali Linux operating system. It is shown that Raspberry Pi with the Raspbian operating system is vulnerable to some of the test attacks. The time it takes for the attacker to execute the man-in-the-middle and backdoor attacks is 1 s. In the case of a Denial of Service (DoS) attack, it takes 60 seconds to execute. It was shown that an MITM attack takes much longer to prepare, approximately 15 min, than a DoS attack that takes 8 min.

Keywords-- Vulnerabilities, MITM, DoS, Raspberry Pi, backdoor.

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

Análisis de vulnerabilidades a un Raspberry Pi en un ambiente simulado

Genessis M. Enriquez, Ing [1], y Néstor X. Arreaga, Msig[2]
[1,2] Escuela Superior Politécnica del Litoral, ESPOL, Polytechnic University, FIEC, Campus Gustavo Galindo Km. 30.5 Vía Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador, gemaenri@espol.edu.ec, narreaga@espol.edu.ec

Resumen– ***Los dispositivos IoT actualmente forman parte de nuestro entorno, recopilando datos e información que debe ser confidencial. Por esta razón se debe saber que vulnerabilidades presentan los dispositivos que se estan usando. En este artículo se demuestra que los dispositivos Raspberry Pi no tienen un sistema de defensa que detecte archivos maliciosos o infectados por virus. Esta es una de las razones por la que son vulnerables a diversos ataques. Para comprobar esto, se realizaron tres diferentes ataques, Man In The Middle (MITM), Backdoor y Denegación de Servicio (DoS), al dispositivo Raspberry Pi usando una máquina virtual con sistema operativo Kali Linux. Se demuestra que Raspberry Pi con el sistema operativo Raspbian, es vulnerable a algunos de los ataques de prueba. El tiempo que le toma al atacante ejecutar los ataques Man In The Middle y backdoor es de 1 segundo. En el caso del ataque Denegación de Servicio (DoS) toma ejecutarlo 60 segundos. Se demostró que un ataque MITM toma mucho más tiempo en ser preparado aproximadamente 15 minutos, en comparación que un ataque DoS que te toma 8 minutos.***

Palabras Claves-- ***Vulnerabilidades, MITM, DoS, Raspberry Pi, backdoor.***

I. Introducción

Este trabajo de pruebas de pentest al dispositivo IoT Raspberry Pi 3 trata de demostrar que aún existen vulnerabilidades y problemas de ciberseguridad. Esto debe ser tomado en cuenta dado que los dispositivos IoT (Fig.1) [1] cada vez están más presentes en nuestro entorno. Ya que permiten conectar diversos objetos hacia Internet y obtener datos de nuestro alrededor que deben ser confidenciales. Pueden controlar de manera remota otros objetos, monitorear distintos ambientes, edificios, ciudades, vehículos entre otros.

Una de las principales preocupaciones de IoT son el escaso soporte de los dispositivos para la aplicación de parches/actualizaciones y la escasa potencia computacional. Además, no existen estándares de seguridad desarrollados para dispositivos IoT [2]. De esto derivan los problemas de vulnerabilidades inherentes y la incapacidad de detectar y defenderse de ataques externos según [3]. Adicional según [4] Raspberry Pi necesita un sistema operativo para funcionar, lo que lo expone a vulnerabilidades de software, dependiendo del sistema operativo que se instale.

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

Fig. 1. IoT en nuestro entorno. [1]

Los sistemas operativos que se pueden usar en una Raspberry son: Raspbian, Windows 10 IoT, OpenELEC, Ubuntu y RiscOS [4], en la Tabla I se presentan algunas vulnerabilidades de estos sistemas operativos. Una de las brechas de seguridad en un sistema es el usuario y contraseña predeterminado como es el caso de Raspbian. Al instalar el sistema Rasbian tiene el usuario por defecto pi y su contraseña raspberry, el cual puede ser cambiado despues de finalizar la instalacion.

Además, para usar los servicios de monitoreo, la mayoría le pide al usuario que proporcione información personal, en algunos casos privada, para recibir servicios personalizados. La seguridad y privacidad de estos datos son importantes y deben ser tomados en consideración al momento de diseñar una aplicación, un ecosistema y servicios de IoT. Se estima que el número de dispositivos de Internet de las cosas (IoT) superará los 75 000 millones de dispositivos para 2025 [5]. Este crecimiento también dará lugar al aumento de ataques, tanto en el hardware como en el software de los ambientes que usan dispositivos IoT.

TABLA I
Vulnerabilidades de los Sistemas Operativos que se pueden instalar en Raspberry Pi. [4]

Operating system	Vulnerability
Raspbian	Usuario y clave por defecto.
Windows 10	Portal de dispositivos Windows inseguro.
OpenELEC	Usuario y contraseña por defecto (y no modificables).
Ubuntu	Nada que comunicar.
RiscOS	Nada que comunicar.

Dado que los dispositivos IoT son atacados de manera frecuente se han realizado varios estudios de las

vulnerabilidades de IoT. Los problemas relacionados con la ciberseguridad en los sistemas de IoT ya han sido abordados por otros trabajos como en la literatura [6] donde se mencionan otros artículos que identifican las vulnerabilidades de los dispositivos IoT como en [3], [7], [8],[9] y en [10], [11] hablan del impacto y como mejorar la seguridad. Según el estudio realizado en [7] demostraron que una cantidad significativa de dispositivos loT, específicamente los dispositivos que se usan en el hogar, el trabajo y en ciudades, son vulnerables a estos ataques. El 12,92% de los dispositivos estudiados tienen riesgos 'Crítico', 'Alto', 'Medio' o 'Bajo'. De los 20.237 dispositivos vulnerables, el 40,16% eran cámaras web, el 7,1% de los dispositivos vulnerables eran televisores inteligentes. Finalmente, el 52,75% de los dispositivos vulnerables eran impresoras.

En [3] la investigación determinó que las inyecciones, la falsificación de solicitudes entre sitios, las secuencias de comandos entre sitios, la denegación de servicio y el desbordamiento de búfer son las vulnerabilidades más comunes con respecto a los ataques en la red. Según [8], las amenazas abarcan desde la escucha clandestina de los mensajes transmitidos, el robo de identidad y el acceso no autorizado a la inyección de código de software malicioso, etc. En 2019 se realizó un análisis de las vulnerabilidades del dispositivo IoT Raspberry Pi [9]. Se concluyó que el diseño del hardware de la Raspberry Pi está más enfocado en reducir los costos que en la seguridad. Y las principales fragilidades del sistema operativo son los usuarios y contraseñas predeterminados y los servicios no seguros.

Muchos dispositivos de IoT como sensores, microcontroladores, cámaras web, Raspberry Pi y otros, tienen varias vulnerabilidades. Estas permiten a los atacantes informáticos tener acceso a estos dispositivos o dañarlos, afectando su funcionamiento o atacando la arquitectura en la que se encuentran. En este artículo se quiere averiguar si Raspberry Pi es vulnerable a los ataques MITM (Man In The Middle) [12], backdoor [13] y Denegación de servicio (DoS) [14], con el objetivo de realizar un análisis de vulnerabilidades del dispositivo IoT usando una Raspberry Pi3 model b v1.2.

Se hicieron las pruebas de estos tres tipos de ataques a nivel de software, usando herramientas como Ettercap [15] y Wireshark [16] para el ataque MITM (Man In The Middle). Se uso Metasploit [17] para el ataque backdoor y el ataque de Denegación de servicio (DoS). Para el ataque DoS Raspberry Pi actuó como un servidor.

En la sección II se presentan los materiales y métodos que se utilizan para realizar las pruebas de vulnerabilidades del dispositivo IoT Raspberry Pi. Luego en la sección III. se presentan los resultados de las pruebas. Finalmente, en la seccin IV. se concluye este análisis de vulnerabilidades del dispositivo IoT Raspberry Pi.

II. MATERIALES Y M ÉTODOS

Para realizar las pruebas de penetración de Intrusiones (PENTEST) en el dispositivo IoT Raspberry Pi 3 model b v1.2 se utilizaron las siguientes herramientas: Oracle VM VirtualBox [18], una ma´quina virtual (VM) con sistema operativo Kali Linux (atacante), Raspberry Pi 3 model b v1.2, Advanced IP Scanner, VNC Viewer, Wireshark, Metasploit y Ettercap.

Raspberry Pi model b v1.2: Fig.2 computadora económica, del tamaño de la palma de la mano. Esta placa tiene 4 puertos USB integrados, un puerto Ethernet [19], LAN inalámbrica y BLE. Puerto HDMI, ranura para tarjeta SD y GPIO extendido de 40 pines.

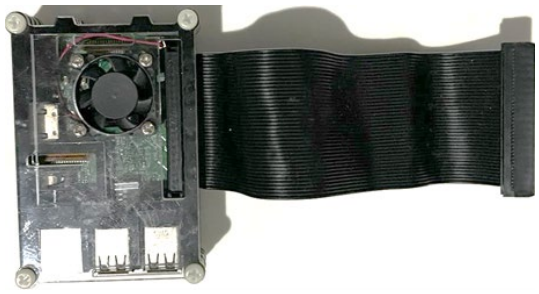

Fig. 2. Raspberry Pi model b v1.2.

Kali Linux: Fig.3 es una distribución de Linux que permite realizar pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa [20], por medio de las herramientas y funciones que tiene.

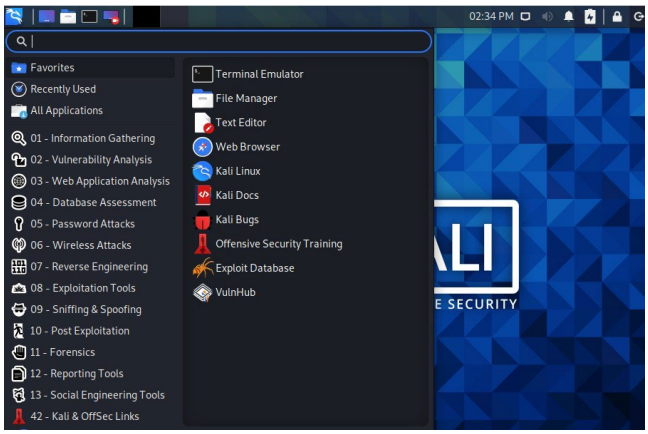

Fig. 3. Kali Linux.

Wireshark: Fig.4 es una herramienta usada para analizar paquetes y protocolos de red [16]. Detectar conexiones ocultas del propio malware con direcciones remotas para obtener otros archivos, capturar paquetes y encontrar vulnerabilidades y para estudiar protocolos de red.

Metasploit: es un grupo de herramientas que se utilizan para realizar ataques en aplicaciones IoT. Tiene una gama de mo´dulos (componentes de software que realizan un cierto ataque a un objetivo elegido). Una vez que se inicia se puede ejecutar comandos que usan un mo´dulo con un exploit en contra la aplicación para intentar vulnerarla [17].

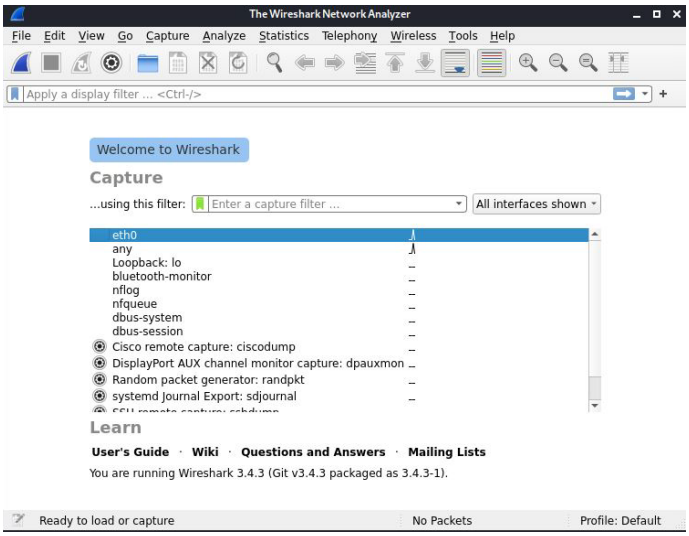

Fig. 4. Wireshark.

Ettercap: es una herramienta de seguridad de red de código abierto gratuita para ataques man-in-the-middle en LAN [15]. Se puede utilizar para análisis de protocolos de redes informáticas y auditorías de seguridad. Es capaz de interceptar el tráfico en un segmento de red, capturar contraseñas y realizar escuchas clandestinas en varios protocolos comunes. Además, se uso para todas las pruebas Advanced IP Scanner [21] Fig.5 (a) para escanear la dirección IP de la Raspberry y VNC Viewer [22] Fig.5 (b) para acceder a la Raspberry. Se realizaron tres pruebas para encontrar las vulnerabilidades de seguridad de Raspberry Pi.

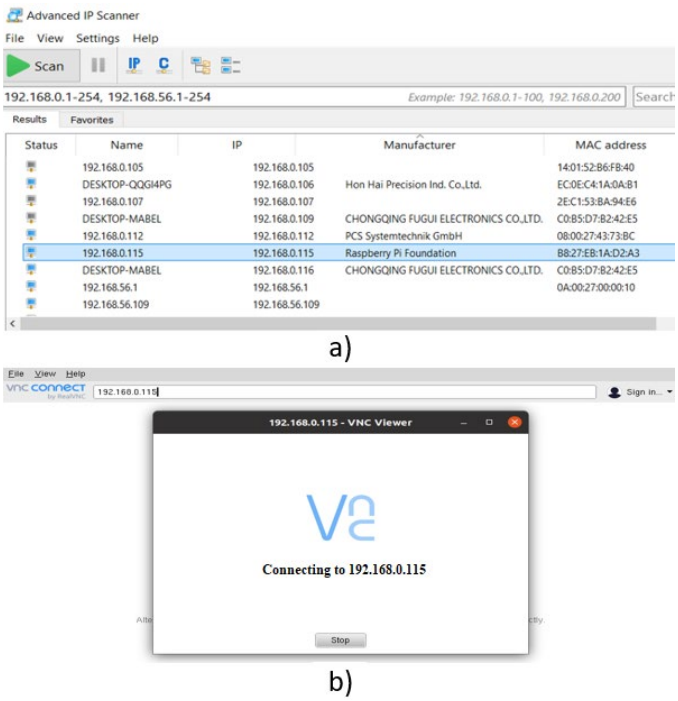

Fig. 5. Advanced IP Scanner y VNC Viewer

A. Ataque MITM (Man In The Middle) desde Kali Linux a una Raspberry Pi

Para la prueba 1 se realizó un ataque MITM (Man In The Middle) desde Kali Linux a una Raspberry Pi, con la siguiente topología de red Fig.6:

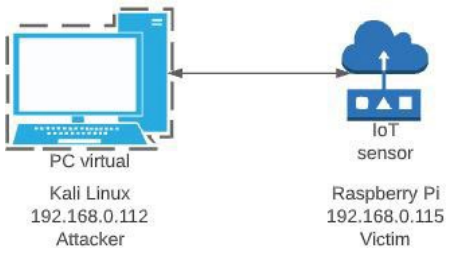

Fig. 6. Topología de la red - Prueba 1 en Raspberry Pi.

En esta prueba se uso 2 máquinas virtuales con los sistemas operativos: Kali Linux (atacante), Ubuntu (servidor) y el dispositivo Raspberry Pi como víctima. Adicional se usaron las herramientas Ettercap y Wireshark para ejecutar el ataque. Desde la VM Kali Linux se ejecutó el programa Ettercap y se escaneo los hosts de la red para hacer un ataque dirigido.

Se identificó la dirección IP 192.168.0.115 de Raspberry Pi (víctima) con ayuda de la herramienta Advanced IP Scanner. Se la seleccionó con dispositivo a monitorizar en el Target 1 y la dirección IP 192.168.0.102 de la VM Ubuntu (servidor) era la dirección IP que se suplanta. Como se observa en los cuadros rojos de la Fig.7, se realizó el ataque con la opción de ARP poisoning [15]. Además, con Wireshark se realizó una búsqueda del protocolo HTTP por medio de filtros, con la dirección IP de Raspberry Pi. Se pudo observar las credenciales de inicio de sesión, en el 3er cuadro rojo de la Fig.7, tanto el usuario como contraseña sin cifrar, que uso el usuario (víctima), en una página con el protocolo http desde su navegador.

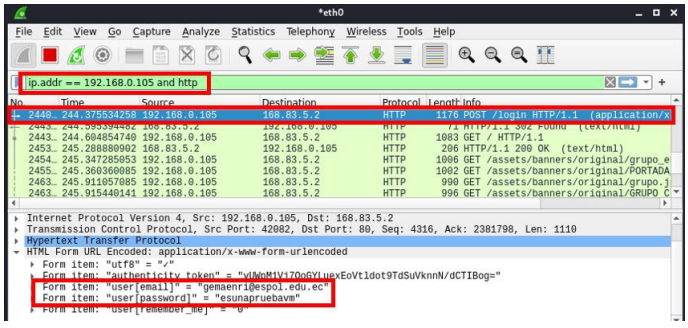

Fig. 7. Ataque MITM en Raspberry Pi.

B. Ataque backdoor desde Kali Linux usando Meterpreter a Raspberry Pi.

Para la prueba 2 se realizó un ataque backdoor desde Kali Linux a Raspberry Pi usando Meterpreter, con la siguiente topología de red Fig.8:

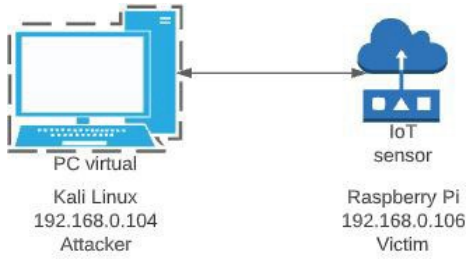

Fig. 8. Topología de la red - Prueba 2 en Raspberry Pi

En esta prueba se uso la máquina virtual con el sistema operativo Kali Linux (atacante), el dispositivo IoT Raspberry Pi (v´ıctima), se uso Metasploit para realizar el ataque. Desde la VM Kali Linux se creo una carga útil (payload) de Metasploit con el módulo msfpayload para Linux con el formato de la Fif. 9.

```
┌──(root㉿kali)-[/home/mabel]
└─# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.0.104 LPORT=4
444 -f elf > /home/mabel/Desktop/PruebaRpi.elf
```

Fig. 9. Formato del payload

Este archivo se tenia que ejecutar en el sistema de la víctima en este caso el dispositivo Raspberry Pi, pero primero se tuvo que dar permisos de ejecución al archivo. Al ejecutarlo se iniciaría un handler de escucha, esto es útil para cuando se ejecute el backdoor en la máquina Raspberry Pi y se conecte a la máquina atacante para poder tomar control remoto. Pero este ataque no se pudo dar ya que al ejecutarlo nos arrojaba un mensaje de error como se observa en la Fig.10. El error generado pudo ser al crear el archivo payload, porque la versión ingresada del sistema operativo en el que se iba a ejecutarse el archivo no era la correcta.

```
pi@raspberry:~ $ sudo su
root@raspberry:/home/pi# cd Downloads
root@raspberry:/home/pi/Downloads# ./PruebaRPi.elf
bash: ./PruebaRPi.elf: Permission denied
root@raspberry:/home/pi/Downloads# chmod 755 PruebaRPi.elf
root@raspberry:/home/pi/Downloads# ./PruebaRPi.elf
bash: ./PruebaRPi.elf: cannot execute binary file: Exec format error
root@raspberry:/home/pi/Downloads#
```

Fig. 10. Ataque backdoor a Raspberry Pi, mensaje de error al ejecutar el archivo

C. Denegaci´on de servicio (DoS) a Raspberry Pi como servidor.

Para la prueba 3 se realizo un ataque de denegación de servicio desde Kali Linux a Raspberry Pi como servidor usando Metasploit, con la siguiente topolog´ıa de red Fig.11:
En esta prueba se uso una máquina virtual con el sistema operativo Kali Linux (atacante) y el dispositivo IoT Raspberry Pi (v´ıctima). Se instaló un servidor web en Raspberry Pi con Apache y se instaló el administrador de base de datos MariaDB y módulos PHP. Desde la VM Kali Linux usando Metasploit se cargó el módulo auxiliar de synflood (inundación TCP SYN) [23] para realizar el ataque de denegación de servicio (DoS).

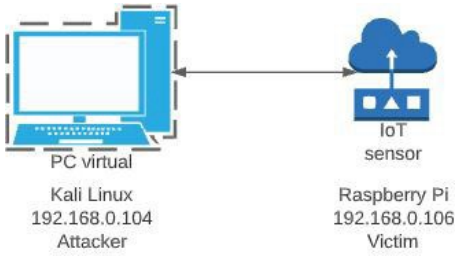

Fig. 11. Topología de la red - Prueba 3 en Raspberry Pi como servidor

Se uso la dirección IP 192.168.0.106 del servidor víctima y se ejecutó el ataque con el comando exploit. Al ejecutarse el ataque se tuvo que esperar un minuto para poder observar que el ataque afectaba al servidor web. Se intento cargar 4 páginas web Fig. 12 (a) en el navegador de la Raspberry, pero estas tardaron 4 minutos y 15 segundos en cargar. Debido a que el ataque satura la cantidad de conexiones disponibles que el servidor puede hacer. Por esta razón al intentar cargar la página del servidor con la dirección https://192.168.0.106 desde el navegador Fig. 12 (b), la página del servidor tardaba en cargar, unos 35 segundos.

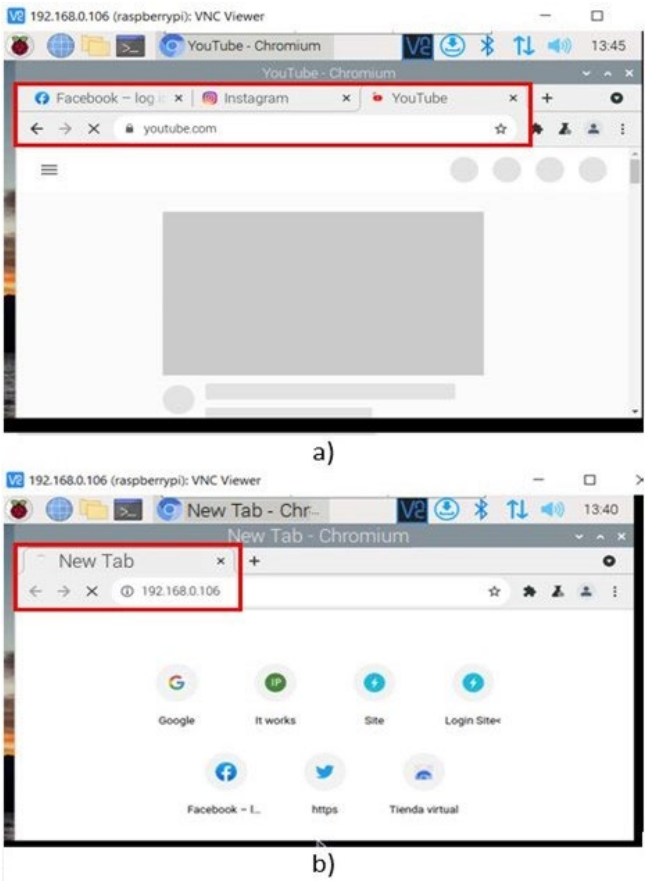

Fig. 12. Ataque DoS a la Raspberry Pi como servidor.

III. Resultados y Análisis

A. *Ataque MITM (Man In The Middle).*

Se pudo realizar un ataque MITM (Man In The Middle) desde Kali Linux y usando una máquina Ubuntu como servidor. Desde la maquina Kali Linux se utilizaron las herramien- tas Ettercap para ejecutar el MITM y Wireshark para capturar el tráfico de la red en eth0. Elaborar el ataque tomo alrededor de 15 minutos como se ve en la Fig. 14, de acuerdo con la Fig. 13 ejecutarlo tomo 1 segundo y se puede quedar a la escucha por tiempo indefinido. Se observo que se puede ver la información que el usuario envía en el navegador cuando la página que se utilizo tiene el protocolo http. Se debe recomendar usar solo páginas con el protocolo https, además buscar una manera para evitar el MITM y que el atacante no obtenga información del dispositivo.

Fig. 13. Gráfico de los tiempos de ejecución de las pruebas.

B. *Ataque backdoor desde Kali Linux usando Meterpreter.*

Se intento realizar un ataque backdoor desde Kali Linux, usando payloads y la interfaz de Metasploit Framework para escuchar a la maquina victima cuando esta ejecute el payload, que nos dejaría la puerta trasera, para que el atacante se conecte a la maquina víctima. Pero al dar los permisos de ejecución e intentar ejecutar el payload en la Raspberry Pi esta muestra un mensaje que nos indica que no se puede ejecutar el fichero binario, que tiene un formato ejecutable incorrecto.

Al probar este payload en la máquina virtual que simula una Raspberry en este si se ejecuta. Por lo que al dispositivo real no se pudo acceder por medio de este tipo de ataque. En este caso preparar el ataque le tomo 13 minutos como se ve en la Fig. 14. En la máquina virtual que simula una Raspberry de acuerdo con la Fig. 13 el ataque se ejecuto en 1 segundo y se tuvo acceso a esta.

C. *Denegación de servicio (DoS) a un servidor.*

Al realizar el ataque de denegación de servicio DoS al dispositivo IoT Raspberry Pi, se pudo observar que al intentar cargar 4 páginas web estas tardaban en cargar alrededor de 4 minutos y 15 segundos, que normalmente se tardan en cargar 40 segundos. Además, al realizar el ataque al servidor este tardo en cargar 35 segundos. Se puso más lenta la carga si se ejecutan 3 ataques adicionales desde 3 terminales. La ejecución del ataque es el mismo ya que es directamente al servidor y tomo un tiempo de 8 minutos prepararlo Fig. 14, de acuerdo con la Fig. 13 la ejecución del ataque toma 1 minuto aproximadamente. Este servidor puede ser al que se conecta Raspberry pi o Raspberry pi puede funcionar como un servidor para obtener información de sensores o de otros dispositivos IoT que tenga configurados. Si el servidor deja de funcionar, los datos que llegan podrían perderse.

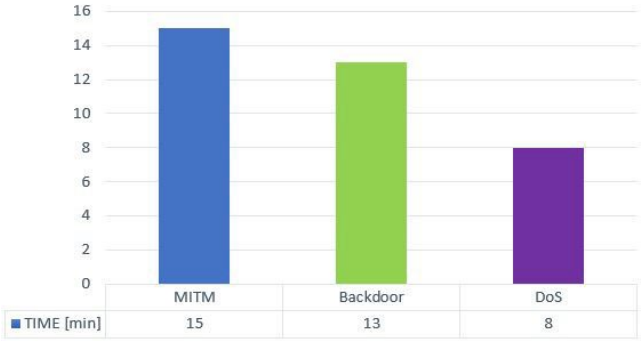

Fig. 14. Gráfico de los tiempos de elaboración del ataque.

En nuestra experiencia es más complejo preparar el ataque Man In The Middle. Debido a que se debe realizar más pasos, por esta razón el tiempo es de 15 minutos, pero al ejecutarlo solo toma 1 segundo en vulnerar el dispositivo. En el caso de Backdoor se tiene que el archivo infectado descargarlo ya sea por medio de internet o usando un USB, para ejecutarlo en la Raspberry y tener acceso, por esto tarde en elaborar el ataque 13 minutos. El ataque DoS es el menos complejo, ya que solo se debe ejecutar comandos desde Metasploit. Por lo que toma un tiempo de 8 minutos preparalo, en comparación de los otros 2 ataques. Pero tarda más tiempo en vulnerar la Raspberry Pi.

.

VI. Conclusiones

Las pruebas realizadas en Raspberry Pi demuestran que el dispositivo es vulnerable a ciertos ataques como Man In The Middle y Denegacio´n de Servicio (DoS). La Raspberry Pi puede ser vulnerada en menos de 1 minuto por cualquiera de estos ataques. Las vulnerabilidades que presenta el dispositivo se deben a que el sistema operativo Raspbian no tiene integrado un sistema que detecte virus o intrusiones tanto en el navegador como el sistema operativo. Debido a que estos sitemas de protección deben ser configuradas manualmente o ser instalados.

Para evitar el ataque MITM se debe usar páginas seguras con el protocolo https en el navegador. En el caso del ataque DoS se puede limitar la tasa de tráfico que provenga de un único host para evitar que se ponga lento o deje de funcionar. Como trabajo futuro se puede realizar pruebas con los ataques que no se probaron como: Envenenamiento de cache DNS, IP Spoofing, KeyLoggers, Ataque de secuencia TCP, otros. Y verificar que no se puede hacer un ataque backdoor de otro

tipo ya que el que se probo usando Meterpreter y el archivo payload no se ejecutó. Adicionalmente se puede realizar un análisis a Raspberry Pi usando otros sistemas operativos y luego realizar una comparación de los tiempos de ejecución y si puede ser Raspberry Pi vulnerada.

REFERENCIAS

[1] Interviewbit. *Top IOT interview questions and answers (2022) - interviewbit*. 2022. URL: https : / / www . interviewbit.com/iot-interview-questions/.

[2] Brittany D. Davis, Janelle C. Mason, and Mohd Anwar. "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study". In: *IEEE Internet of Things Journal* 7.10 (2020), pp. 10102–10110.

[3] Stavros Shiaeles, Nicholas Kolokotronis, and Emanuele Bellini. "IoT Vulnerability Data Crawling and Analy- sis". In: *2019 IEEE World Congress on Services (SER- VICES)*. Vol. 2642-939X. 2019, pp. 78–83.

[4] Jorge Sainz-Raso et al. "Security Vulnerabilities in Raspberry Pi– Analysis of the System Weaknesses". In: *IEEE Consumer Electronics Magazine* 8.6 (2019), pp. 47–52.

[5] Wei Zhou et al. "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved". In: *IEEE Internet of Things Journal* 6.2 (2018), pp. 1606–1616.

[6] Francesca Meneghello et al. "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices". In: *IEEE Internet of Things Journal* 6.5 (2019), pp. 8182–8201. 2935189.

[7] Ryan Williams et al. "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach". In: *2017 IEEE International Conference on Intelligence and Security Informatics (ISI)*. 2017, pp. 179–181.

[8] Waseem Iqbal et al. "An In-Depth Analysis of IoT Secu- rity Requirements, Challenges, and Their Countermea- sures via Software-Defined Security". In: *IEEE Internet of Things Journal* 7.10 (2020), pp. 10250–10276.

[9] Jorge Sainz-Raso et al. "Security Vulnerabilities in Raspberry Pi– Analysis of the System Weaknesses". In: *IEEE Consumer Electronics Magazine* 8.6 (2019), pp. 47–52.

[10] Segundo Moise´s Toapanta Toapanta, Romina Pamela Rodriguez Pesantes, and Luis Enrique Mafla Gallegos. "Impact of Cybersecurity Applied to IoT in Public Organizations in Latin America". In: *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. 2020, pp. 154–161.

[11] Olumide Kayode and Ali Saman Tosun. "Deep Q- Network for Enhanced Data Privacy and Security of IoT Traffic". In: *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*. 2020, pp. 1–6.

[12] Defiana Arnaldy and Audhika Rahmat Perdana. "Im- plementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack". In: *2019 2nd International Conference of Computer and Informatics Engineering (IC2IE)*. 2019, pp. 188–192.

[13] Huicong Loi and Aspen Olmsted. "Low-cost detection of backdoor malware". In: *2017 12th International Conference for Internet Technology and Secured Trans- actions (ICITST)*. 2017, pp. 197–198.

[14] Saifudin Usman, Idris Winarno, and Amang Sudar- sono. "Implementation of SDN-based IDS to protect Virtualization Server against HTTP DoS attacks". In: *2020 International Electronics Symposium (IES)*. 2020, pp. 195–198.

[15] K M Majidha Fathima and N. Santhiyakumari. "A Sur- vey On Network Packet Inspection And ARP Poisoning Using Wireshark And Ettercap". In: *2021 International Conference on Artificial Intelligence and Smart Sys- tems (ICAIS)*. 2021, pp. 1136–1141.

[16] Piyush Goyal and Anurag Goyal. "Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark". In: *2017 9th International Conference on Computational Intelligence and Communication Net- works (CICN)*. 2017, pp. 77–81.

[17] Himanshu Gupta and Rohit Kumar. "Protection against penetration attacks using Metasploit". In: *2015 4th International Conference on Reliability, Infocom Tech- nologies and Optimization (ICRITO) (Trends and Fu- ture Directions)*. 2015, pp. 1–4.

[18] Dejana T. Vojnak et al. "Performance Comparison of the type-2 hypervisor VirtualBox and VMWare Workstation". In: *2019 27th Telecommunications Fo- rum (TELFOR)*. 2019, pp. 1–4.

[19] Levin Varghese, Gerard Deepak, and A. Santhanavi- jayan. "An IoT Analytics Approach for Weather Fore- casting using Raspberry Pi 3 Model B+". In: *2019 Fifteenth International Conference on Information Pro- cessing (ICINPRO)*. 2019, pp. 1–5.

[20] Eiman Al Neyadi et al. "Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux". In: *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*. 2020, pp. 1–4.

[21] P. Mariaraja et al. "Design and Implementation of Advanced Automatic Driving System using Raspberry Pi". In: *2020 5th International Conference on Com- munication and Electronics Systems (ICCES)*. 2020, pp. 1362–1367.

[22] Sandip Das, Biswajit Jana, and Soumitra Kumar Man- dal. "Implementation of dimming controlled visible light communication using Raspberry Pi". In: Optical and Quantum Electronics 53.12 (2021), pp. 1–19

[23] Tushar Ubale and Ankit Kumar Jain. "SRL: An TCP SYNFLOOD DDoS Mitigation Approach in Software-Defined Networks". In: 2018 Second International Con- ference on Electronics, Communication and Aerospace Technology (ICECA). 2018, pp. 956–962.