ISSN: 1692-7257 - Volumen 1 – Número 33 - 2018

Revista Colombiana de
Tecnologías de Avanzada

Recibido23 de enero de 2018
Aceptado19 de julio de 218:

SISTEMA DE DETECCIÓN DE INTRUSOS A TRAVÉS DE UNA RED HONEYNET PARA ENTORNOS DE RED CABLEADA SOBRE IPV6

INTRUSION DETECTION SYSTEM THROUGH A HONEYNET NETWORK FOR NETWORK ENVIRONMENTS WIRED ON IPV6

MSc. Fabián Ranulfo Cuesta-Quintero, MSc. Luis Anderson Coronel-Rojas, MSc. Dewar Rico-Bautista, MSc. Edwin Barrientos-Avendaño, Ing. Oscar José Montañez-vergel, Ing. Carlos Mario Páez-Noriega2*

[*] **Universidad Francisco de Paula Santander Ocaña.** Grupo de Ingeniería en Innovación, Tecnología y Emprendimiento GRIITEM. Vía Acolsure, Sede el Algodonal, Ocaña Norte de Santander, Colombia. 5690088
E-mail: {fcuestaq, ebarrientosa, dwricob, lacoronelr, ojmontanezv, cmpaezn}@ufpso.edu.co.

Resumen: Las honeynet o redes señuelo son recursos de red que representan una medida de aseguramiento para toda organización que haga uso de las tecnologías de información y las comunicaciones. Esta herramienta es usada en el ámbito de la seguridad informática con la finalidad de atraer y analizar el comportamiento de los atacantes en internet. El propósito de este trabajo es presentar pruebas experimentales de los ataques informáticos más comunes en redes cableadas IPV6 a través de las herramientas como 6Guard, SNORT y Wireshark. También se evidencia en el artículo el diseño e implementación de una red Honeynet bajo IPv6, donde interactúan diferentes sistemas operativos. Dentro de los resultados obtenidos se pudo observar la detección completa de los ataques tipo THC-IPv6, como fake_router6, redir6, fake_advertise6, fake_solicitate6, flood_dhcp6, sendpees6, sendpeesmp6 y smurf6.

Palabras clave: IPV6, Honeynet, Honeypot, Honeydrive.

Abstract: Honeynets are network resources that represent an assurance measure for any organization that makes use of information and communication technologies. This tool is used in the field of computer security in order to attract and analyze the behavior of attackers on the Internet. The purpose of this work is to present experimental evidence of the most common computer attacks in IPV6 wired networks through tools such as 6Guard, SNORT and Wireshark. Also evidenced in the article is the design and implementation of a Honeynet network under IPv6, where different operating systems interact. Among the results obtained, we could observe the complete detection of THC-IPv6 type attacks, such as fake_router6, redir6, fake_advertise6, fake_solicitate6, flood_dhcp6, sendpees6, sendpeesmp6 and smurf6.

Keywords: IPV6, Honeynet, Honeypot, Honeydrive.

1. INTRODUCCIÓN

Los datos que viajan a través de internet se exponen a múltiples riesgos debido a la vulnerabilidad de las

redes, ocasionadas por personas de la misma compañía o empresa que tienen fácil acceso a la red; así también personas externas que logran violar la seguridad de la red (Katz. Matías David, 2013). El manual de seguridad en redes, de la coordinación de emergencia en redes teleinformáticas de la administración pública Argentina, Acert (2008), afirma, que la falta de medidas de seguridad en las redes es un problema que está en crecimiento.

Miguel & Gómez(2012), afirman que mientras Internet y las tecnologías digitales facilitan el acceso al conocimiento, al mismo tiempo hay ciertas barreras que impiden el acceso. Con el surgimiento de protocolos de comunicaciones como lo es IPv6(Rico-Bautista, Medina-Cárdenas, & Santos Jaimes, 2008; S. & R., 2007),promovido y promocionado por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, también aumentará el nivel amenazas para los cibernautas y la información que en ella circula(Hogg & Vyncke, 2009). Por lo tanto conocerlo podrá colocar a la institución un paso adelante de los atacantes para garantizar la confianza de sus usuarios y estar al tanto de las vulnerabilidades, posibles ataques, métodos y técnicas(Hogg & Vyncke, 2009).

El protocolo IPv6 proporciona unos niveles de seguridad mucho más altos que su antecesor, pero a su vez existe desconocimiento sobre los ataques realizados bajo este protocolo(Carpene, Johnstone, & Woodward, 2017; Hogg & Vyncke, 2009). Cuando se trabaja bajo ambientes de IPv4 se cuenta con un amplio conocimiento de defensa para los ataques debido a sus vulnerabilidades, que son aprovechadas por los hackers que al implementar métodos y técnicas, acceden a la red e información(Rico-Bautista, Medina-Cárdenas, & Rojas-Osorio, 2016). Por lo contrario, IPv6 por ser nuevo en su implementación, se encuentra en evolución así que no se conoce la totalidad de sus vulnerabilidades. Al implementar IPv6 sin tener un conocimiento sólido de los riesgos a los que se expone la información almacenada en los servidores se expone a situaciones críticas en las que el no saber qué hacer en casos en las que un atacante ha logrado penetrar el sistema de información(Rico-Bautista & Alvernia-Acevedo, 2017).

The Honeynet project, es una organización internacional de investigación de seguridad sin fines de lucro dedicada a investigar los últimos ataques y desarrollar herramientas de seguridad de código abierto para mejorar la seguridad en Internet. Este equipo de investigadores ha construido una red informática completa y totalmente cableada con sensores(Yin, Li, Ma, & Sun, 2004). Para este tipo de recursos de red como lo es una honeynet se hace operativo mencionar sus componentes, los Honeypots, que tiene como fin el proporcionar información valiosa sobre los métodos y recursos utilizados por la comunidad Blackhat para cometer ataques informáticos(Vinueza Jaramillo, 2012).

Reflejan un entorno de red productivo al trabajar con varios sistemas a la vez. Entre ellos Linux, Solaris, Windows, Router Cisco, etc. Por lo que un honeypot (tarro de miel) al recurso de red destinado a ser atacado o comprometido con la finalidad de identificar, evitar y en cierta medida, neutralizar los intentos de secuestrar sistemas y redes de información(Abbasi & Harris, 2009). Por último el honeywall es el principal componente de la arquitectura; actúa como puente transparente de la Honeynet y ejecuta las tareas de control, captura y análisis de los datos. Se implementa utilizando el sistema operativo Honeywall Roo V1.4 basado en CentOS 5.0 distribuido de forma gratuita por el proyecto Honeynet "The Honeynet Project"(Vinueza Jaramillo, 2012).

Internet de las cosas o IoT (Internet of Things)(Gershenfeld, Krikorian, & Cohen, 2004), se refiere a la conexión de objetos tecnológicos o que sean electrónicos a Internet, este concepto se deriva del avance de la tecnología y a la necesidad de compartir y controlar las cosas que nos rodean, incluyendo las necesidades de árboles y plantas (Li, Xu, & Zhao, 2015), (Luvisi & Lorenzini, 2014). Algunos de los campos en los que IoT se presenta fuertemente son: la adopción generalizada de redes basadas en el protocolo IP (Airehrour, Gutierrez, & Ray, 2016), la economía en la capacidad de cómputo, la miniaturización, los avances en el análisis de datos (Danieletto, Bui, & Zorzi, 2013) y el surgimiento de la computación en la nube, salud, herramientas de aprendizaje, seguridad (Flauzac, Gonzalez, & Nolot, 2015), optimización de procesos (Aziz, 2016), agricultura (Stočes, Vaněk, Masner, & Pavlík, 2016), entre otros.

2. MODELAMIENTO DE LA RED LAN HONEYNET

La topología propuesta se enmarco en un ambiente real IPv6 Unicast Routing en el Laboratorio de Redes y Telecomunicaciones de la universidad Francisco de Paula Santander Ocaña. Los requerimientos para la implementación del sistema de detección de intrusos – honeynet, se muestra a continuación.

2.1 Requerimientos hardware/software

A nivel de hardware los dispositivos necesarios que fueron utilizados para el desarrollo de la red honeynet son los mostrados en la tabla 1, (Hermidez, 2010).

TABLA 1. Requerimientos de hardware

REQUERIMIENTOS DE HARDWARE
Servidor marca hewlettpackard hp
2 switch cisco series 2960
1 Router cisco serie 1900
5 Computadores portátiles marca HP

Antes de iniciar a realizar cualquier instalación y configuración es importante tener definir las herramientas de software a utilizar teniendo en cuenta las actualizaciones de los sistemas operativos anfitriones y virtualizados. En la tabla 2 se especifican las herramientas utilizadas.

TABLA 2. Requerimientos de software

REQUERIMIENTOS DE SOFTWARE	
Sistemas operativos	
Windows 10	Víctima
Ubuntu 16.04 LTS	Servidor
Kali Linux 2017.3	Atacante
Honeydrive 3	Honeypots
Herramientas de análisis y detección de ataques	
Wireshark	Sniffer y lector de paquetes
snort	Sistema de detector de intrusos
6guard	Honeypot IPV6 – nativo
Dionaea-FR-ipv6	Honeypot IPV6 genérico
THC – IPV6	Kit de herramientas de ataques ipv6

2.2 Descripción de la topología propuesta

En la figura 1, se puede observar la topología de Honeynet utilizada para verificar el funcionamiento de los Honeypots, SNORT y de los ataques THC-IPv6 (Schütte, 2014).

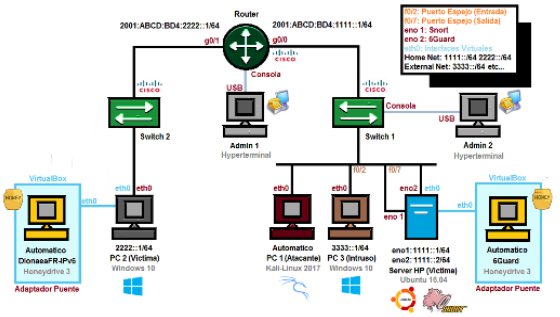

Figura 1. LAN Honeynet propuesta.

El entorno de la topología Honeynet es LAN y sin ningún tipo de conexión a Internet. Es de tipo IPv6 Unicast-Routing. Interactúan los Sistemas Operativos, Windows, Ubuntu, Kali Linux y Honeydrive. Los Firewalls de cada equipo están todos desactivados. 6Guard es el Honeypot principal de la Red Honeynet. Debe reconocer todos los ataques realizados por parte de la THC-IPv6 a nivel de enlace-local. 6Guard es capaz de reconocer ataques a cada miembro de la red, así como también ataques que se hagan a toda la red en sí. DionaeaFR-IPv6 es un Honeypot Secundario. Se sabe que su función es principalmente reconocer ataques provenientes de la Internet. Aun así, se dejara este Honeypot en la Honeynet para cuando se desee establecer conexión a internet por medio de IPv6. Kali Linux 2017.3 se instaló físicamente en un computador portátil y no en máquina virtual para esta topología. Para dejar al PC atacante con Kali Linux del lado del Switch 2 sería necesario instalar otro 6Guard de ese lado. Es necesario conectar los Honeypots de la máquina virtual y el Atacante, al Router por medio de la asignación de IPv6 Automática (Global). Al realizar el enrutamiento estático IPv6 con direcciones Globales, automáticamente se generan a cada máquina una dirección de anuncio de Router y una de Enlace-Local. Las direcciones de Enlace-Local generadas automáticamente son las que se utilizaron, para la realización y detección de ataques IPv6 por parte de 6Guard. Se añadió un PC 3 (Intruso) adicional para verificar la funcionalidad de SNORT, Este solo accederá a los servicios FTP, UDP e ICMPv6 de los demás computadores. SNORT contiene como Red Local a 1111::/64 (local) y 2222::/64 (remota). SNORT contiene como Red Externa todo lo que no sea la Red Local. (El Intruso). La Red Local actuó como víctima de atacantes, pero protegida con Honeypots. La Interfaz eno1 del Servidor HP cuenta con la función de Puerto Espejo para la detección garantizada de SNORT (por allí es donde este se comunica), y la eno2 no cuenta con Puerto Espejo, ya que por esta, es que se comunica 6Guard para

verificar su funcionamiento en esa condición, ya que se recomienda la implementación de esta función para aumentar su precisión de detección de ataques. Para dejar al PC Intruso del lado del Switch 2 fue necesario hacer VLAN, conectar ambos Switch por modo Trunk y finalmente realizar puerto espejo al puerto por donde ingresa dicha VLAN. Un solo PC podría actuar de Atacante y de Intruso a la vez, mediante el uso de Kali Linux como Máquina Virtual. Los Switch y Router utilizados son de la marca Cisco con soporte para Puerto Espejo e IPv6 Unicast-Routing respectivamente. Administrados y configurados por medio de Hyperterminal. Los archivos de registro de los Honeypots y de SNORT fueron revisados con Wireshark.

3. PRUEBAS EXPERIMENTALES

Las pruebas experimentales se realizaron a través de la herramienta 6Guard, esta es un Honeypot especializado de baja interacción destinado a detectar ataques en la capa de red del modelo ISO / OSI, más específicamente ataques IPv6 de enlace local. Se escogieron ataques de los cuatro grupos de la THC-IPv6. Todos fueron exitosamente detectados por el Honeypot 6Guard. Pero por el contrario DionaeaFR-IPv6 no detectó actividad alguna, ya que como se mencionó anteriormente este Honeypot es eficaz a la hora de conectar una Honeynet a internet por medio de IPv6. “En IPv4, se sabe qué es "ARP", aquí en IPv6, es reemplazado por ND expandido como Neighbor Discovery (Descubrimiento de Vecinos). ND combina la funcionalidad de ARP, ICMP, ICMP-Redirect y descubrimiento de Router que está presente en IPv4 (…). Básicamente, hay 5 tipos de mensajes ND: Solicitud de Router, Anuncio de Router, Solicitud de vecinos, Anuncio de vecinos y Redireccionamiento”.(Kali, 2015).

3.1 Prueba de Ataques THC-IPv6 Grupo I

El primer grupo de ataques de la THC-IPv6, llamado Grupo I, son los que realizan anuncios falsos de Router, esto es que el atacante se introduce a la red como un Router de alta prioridad y los computadores víctima se conectan a este y no al Router real. Este Grupo I también realiza ataques para redirigir el protocolo ICMPv6 y realiza ataques DOS si se proporciona una dirección de MAC local o de enlace no existente. Se seleccionó el ataque fake_router6 perteneciente al Grupo I(Information, n.d.). Fake_router6 es una herramienta dentro de las herramientas THC-IPv6 incluidas dentro de Kali Linux para probar las vulnerabilidades de ataque y la complejidad en los protocolos IPv6 e ICMPv6. (Kali, 2015). Se utilizó la siguiente línea de comando para ejecutar este ataque:

Fake_router6 eth0 bad::00/64

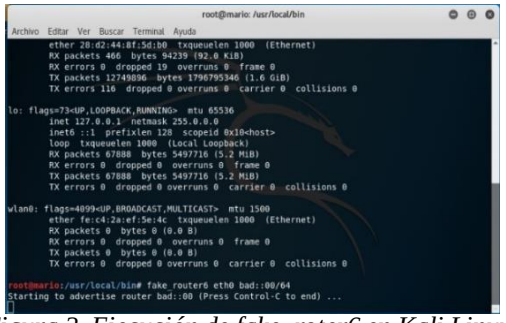

Figura 2. Ejecución de fake_roter6 en Kali Linux.

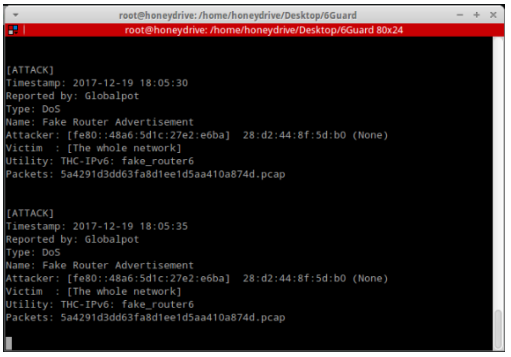

Figura 3. Detección de fake_router6 por 6Guard.

De la cual eth0 es la interfaz de salida y bad::00/64 es una dirección de enlace local que se le añadió a este Router falso creado por fake_router6 al cual se conectan los PCs víctimas, también funciona con direcciones de MAC falsas o con DNS falsos. Es de aclarar que esta información de Router Falso se puede visualizar en los PCs víctimas mediante el comando ipconfig (Windows) o ifconfig (Linux) en cmd o terminal al reiniciar el adaptador Ethernet, ver figura2. Por su parte 6Guard reconoció exitosamente este ataque realizado a toda la red detectando incluso la dirección de enlace local y la MAC del atacante, ver figura 3.

3.2 Prueba de Ataques THC-IPv6 Grupo II

El segundo grupo de ataques de la THC-IPv6, llamado Grupo II, son los que suplantan identidades, direcciones MAC e IP falsas y se anuncian a la red con esta información. También duplican direcciones, impidiendo así que algunos equipos se conecten a la red y desconectando los que ya estaban en la red, también realiza redireccionamiento de tráfico falso y también inundaciones a la red con anuncios y solicitudes falsas. Básicamente cumple con la misma función de los ataques del Grupo I,

solo que el Grupo II se enfoca en suplantar equipos y afectar a los demás mientras que el Grupo I se enfoca es en suplantar funciones de Routing. Se seleccionó el ataque fake_advertise6 perteneciente al Grupo II. Fake_advertise6 cumple la función de anunciar la dirección IPv6 en la red (con su propia MAC si no se especifica), enviándola a la dirección de multidifusión de todos los nodos si no se establece una dirección de destino. Se utilizó la siguiente línea de comando para ejecutar este ataque:
fake_advertise6 eth0 fe80::2c38:68f7:7920:3e7a ff02::1 66:66:66:66:66:66

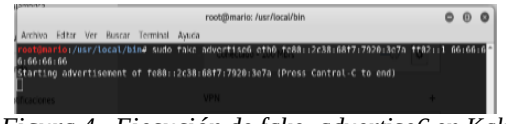

Figura 4. Ejecución de fake_advertise6 en Kali Linux.

De la cual eth0 es la interfaz de salida,fe80::2c38:68f7:7920:3e7a es la dirección de enlace local del PC Víctima a atacar (Server HP para este caso), ff02::1 es el blanco de ataque de la red por el cual se permite realizar el ataque especifico y 66:66:66:66:66:66 es una dirección MAC falsa que se le crea al atacante para que se anuncie a la red con esta, ver figura 4.

Figura 5. Detección de fake_advertise6 por 6Guard.

Al momento de crear una MAC o IP duplicada, inmediatamente el PC Víctima con la MAC o IP original se queda incomunicado ya que la prioridad la toma el Atacante, esto se puede comprobar fácilmente mediante el uso del comando Ping arrojando tiempo de espera agotado y perdiendo así todos los paquetes cuando anteriormente el equipo estaba comunicado y con envió de paquetes ICMP(Hogg & Vyncke, 2009).6Guard reconoció exitosamente este ataque detectando que se atacó por medio de la dirección de todos los nodos la dirección de enlace local afectada. La dirección MAC falsa es detectada, ver figura 5.

3.3 Prueba de Ataques THC-IPv6 Grupo III

El tercer grupo de ataques de la THC-IPv6, llamado Grupo III, son los que proporcionan falsa información de servidor, esto incluye suplantación o falsificación de DHCPv6, DNS o cliente. Los ataques pertenecientes a este grupo usualmente agotan el servicio ofrecido por estos protocolos y trabajan de la mano con ataques pertenecientes al Grupo II. También se usan para afectar todo tipo de funcionamiento relacionado con los protocolos que proporcionan servicios de red, tal como denegaciones e inundaciones. Se seleccionó el ataque flood_dhcpc6perteneciente al Grupo III. Flood_dhcpc6 es un ataque que cumple con la función de agotar las direcciones disponibles (que se asignan por medio de DHCPv6) suministradas dinámicamente por un servidor DNS. Está enfocado a un entorno LAN, no se consideró necesario incluir un servidor DNS en la red, sin embargo, el ataque fue realizado en el caso que la Honeynet se conectara a internet para agotar las direcciones automáticas suministradas por google.com, es por esto que a la hora de la detección de este ataque por parte del Honeypot 6Guard, no se generaron paquetes de esta detección pero si se generó la alerta correspondiente. Se utilizó la siguiente línea de comando para ejecutar este ataque:

flood_dhcpc6 –n –l –d google.com eth0

De la cual la opción –n usara la MAC real, -l solicita una dirección, pero no la adquiere, -d sirve para forzar actualizaciones DNS, google.com es el servidor y eth0 es la interfaz de salida. El comando –N usa la dirección link-local aparte de la MAC real, se recomienda ejecutar el ataque parasite6 (del Grupo II) en paralelo cuando no se ejecuta –N, este último ataque es generalmente ejecutado en conjunto con otros ataques ya que es un Spoofer (suplantador) de ARP y redirecciona tráfico falso. Se puede introducir una dirección IPv6 que suministre el Servicio de Dominio. Si no se introduce –n ni –N, se tomará una MAC aleatoria falsa. Si el pool de direcciones que ofrece el servidor DHCPv6 es demasiado grande, no tiene sentido el uso de este ataque solo. El ataque generalmente termina cuando el atacante corta el proceso, debido a que es inundación de direcciones, se tomara muchos paquetes de los cuales con uno solo de ellos es suficiente para poder ser analizado por un Sniffer de red. Debido que no se tiene conexión real a google.com solo se generó una sola alerta de la solicitud de inundación DHCP por parte de flood_dhcpc6 y de una manera superficial, ver figura 6.

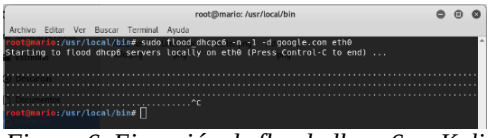

Figura 6. Ejecución de flood_dhcpc6 en Kali Linux.

6Guard reconoció el ataque, pero como no hay conexión a internet no se generaron paquetes. Debido a esto, en la figura 7, se generó solo una alerta (la última que aparece).

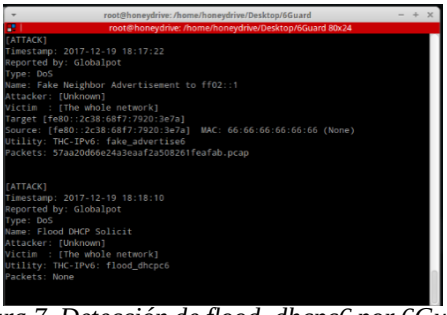

Figura 7. Detección de flood_dhcpc6 por 6Guard.

3.4 Prueba de Ataques THC-IPv6 Grupo IV

El cuarto grupo de ataques de la THC-IPv6, llamado Grupo IV, son los que realizan ataques de consumidor maligno, esto es que consumen mucho recurso de una red o de la CPU de una máquina. Solo sirven para ocasionar daño a un elemento en sí. Este grupo de la THC intenta desde un principio realizar ataques DOS, inundaciones, calentamientos a servidores, ataques pitufos (Smurf) etc… Así que sus principios son diferentes a los de los otros grupos que más que todo se basan en el Spoofing. Se seleccionó el ataque sendpeesmp6perteneciente al grupo IV. Este ataque se encarga de enviar muchísimos mensajes de solicitación de vecino, por lo cual si envía como blanco para realizar los ataques la dirección de todos los nodos (ff02::1) su efectividad incrementaría bastante. Estos mensajes vienen cargados de claves criptográficas, tipo RSA y CGA. sendpeesmp6 es una versión multi-hilo del ataque sendpees6. Se utilizó la siguiente línea de comando para ejecutar este ataque:

sendpeesmp6 eth0 1024fe80::a00:27ff:fe38:d1ec ff02::1

De la cual eth0 es la interfaz de salida, 1024 es el parámetro de duración del ataque, fe80::a00:27ff:fe38:d1ec, y ff02::1,es la dirección de blanco de ataque, dirección de todos los nodos.
Este ataque se realizó de manera rápida, lo suficiente para tomar capturas debido a su alta potencialidad de dañar recursos. En Windows Se puede visualizar el monitor de recursos para ver el consumo de CPU mientras el ataque es realizado, En Linux por medio del monitor de sistema, es una maniobra un poco peligrosa. El ataque termina cuando el atacante corta el proceso, debido a que es inundación de mensajes para dañar recursos, se tomara muchos paquetes de los cuales con uno solo de ellos es suficiente para poder ser analizado por un Sniffer de red, ver figura 8.

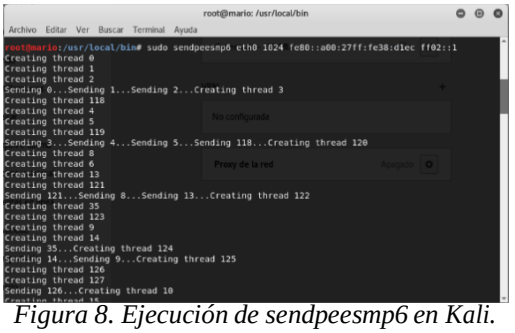

Figura 8. Ejecución de sendpeesmp6 en Kali.

Se reconoció una gran cantidad de alertas de este ataque, como se ejecutaron varios Honeypots 6Guard cada uno reconoce varios paquetes de esta inundación. Algunos como sendpees6, ver figura 9.

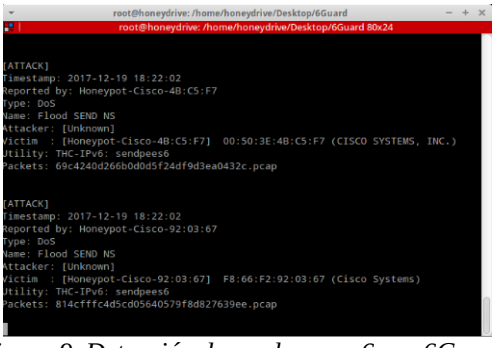

Figura 9. Detección de sendpeesmp6 por 6Guard.

3.5 Imprecisión en detección de algunos ataques por falta de Puerto Espejo

Como se registró anteriormente en el último ataque sendpeesmp6, 6Guard reconoció algunos ataques como sendpees6. Estas imprecisiones se deben a que la función de puerto espejo no fue utilizada para el puerto eno2 del servidor por el cual es que el Honeypot se comunica con la red y detecta los ataques. Sin embargo, esto no es obstáculo para 6Guard en reconocer información de los ataques.

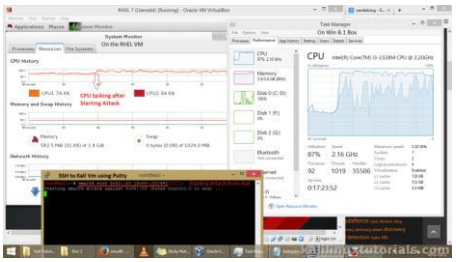

Figura 10. Uso de recurso de CPU elevado en Windows por causa de smurf6.

Uno de los ataques más peligrosos del Grupo IV de la THC-IPv6 fue ejecutado cuidadosamente; el ataquesmurf6. "Un ataque Smurf es un tipo de ataque DOS donde un atacante hace sonar la dirección de difusión con una dirección falsa de una víctima. Eventualmente, todos los nodos en la red obtienen una solicitud ICMP ping de la dirección IP de la víctima. Como resultado, todos los hosts responden a la dirección IP de la víctima convirtiéndola en un ataque DDoS. En IPv4 (Xia et al., 2014), este ataque no tendrá éxito en la mayoría de los Router y Switch modernos. Pero IPv6 sigue siendo vulnerable, ver figura 10, (Kali, 2015).

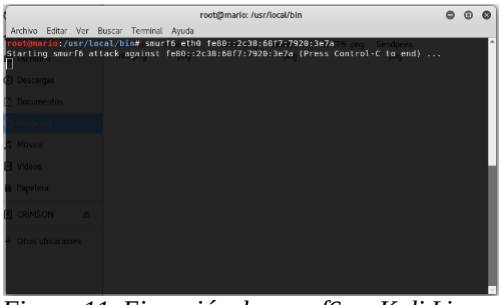

Figura 11. Ejecución de smurf6 en Kali Linux.

Smurf6 es un ataque bastante peligroso y complejo, que funciona perfectamente cuando se quiere inundar toda una red con paquetes ICMPv6. Se recomienda para 6Guard usar la función puerto espejo para reconocerlo totalmente. En este caso 6Guard se ejecutó sin puerto espejo, por lo que al reconocer la alerta de este ataque reconoció solo una parte de Smurf6 y lo reconoció como un ataque del Grupo de descubrimiento avanzado de Host utilizado por Nmap pues 6Guard reconoce ataques de los cuatro Grupos de la THC-IPv6 y del grupo Nmap. También reconoció a la víctima como si fuera el atacante, ver figuras 11 y 12.

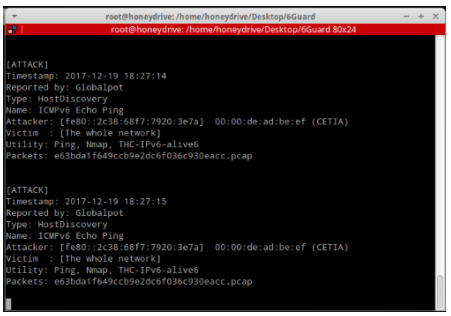

Figura 12. Detección imprecisa de smurf6 por 6Guard.

4. RESULTADOS DE LOS ATAQUES REALIZADOS

Los resultados de los ataques TCH-IPv6 a nivel de enlace local realizados durante las pruebas y detectados por 6Guard se resumen en la tabla 3. Sochor & Zuzcak(Sochor & Zuzcak, 2015), expresa que: "En el caso de un enfoque más específico de atacantes (es decir, centrarse en víctimas muy específicas), se produciría un problema para detectar un ataque RA / NA falso debido a la ausencia de un puerto espejo de conmutación, a pesar de que el principio de ataque sigue siendo el mismo. El módulo Globalpot fue el más activo en la detección de ataques, mientras que solo hubo informes esporádicos del módulo Análisis de eventos. Por otro lado, los informes del módulo de Análisis de Eventos solían ser los más precisos."

Tabla 3. Ataques Realizados Detectados por 6Guard

Ataque de THC-IPv6	Grupo	Detección
fake_router6	I	Completa
redir6	I	Completa
fake_advertise6	II	Completa
fake_solicitate6	II	Completa
flood_dhcpc6	III	Completa
sendpees6	IV	Completa
sendpeesmp6	IV	Parcial-Completa
smurf6	IV	Incompleta

6Guard es un detector de ataque IPv6 basado en Honeypot que tiene como objetivo detectar los ataques de nivel local de enlace, especialmente cuando la función de espejo de puerto del Switch no está disponible(Sochor & Zuzcak, 2015). DionaeaFR-IPv6, por su parte no mostro actividad alguna para los ataques realizados en LAN, la figura 13 se observa como DionaeaFR registra ataques provenientes de Internet.

Figura 13. Detección de ataques por DionaeaFR, Fuente: vanimpe.eu

4.1 Lectura de registros con Wireshark

Toda la información generada por SNORT y por 6Guard (y también por DionaeaFR-IPv6) es almacenada en distintos archivos de formato .log o .pcap que pueden ser leídos manualmente por un Sniffer de red como lo es Wireshark (Borja, 2011).

Wireshark: Captura a Tiempo real y registros de tráfico SNORT

SNORT también estuvo presente y funcional durante la fase de pruebas de ataques de la THC-IPv6, su función era alertar accesos no autorizados a la Red Local (1111::/64 y 2222::/64), provenientes de la Red Externa conformada por el PC intruso con dirección 3333::1/64.

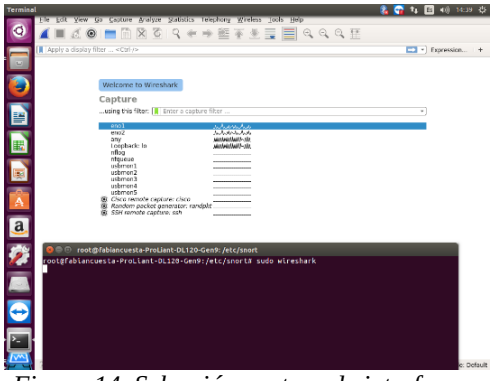

Figura 14. Selección captura de interfaces a tiempo real de Wireshark, Fuente: Autores

Wireshark viene preinstalado en la mayoría de las distribuciones de Linux. En el caso del Server HP con sistema operativo Ubuntu que es donde están instalados SNORT (interfaz eno1) y el Honeypot 6Guard (interfaz eno2), Wireshark ya venía preinstalado y listo para usarse. La interfaz eno1 fue seleccionada para capturar el tráfico a tiempo real detectado también por SNORT con las reglas asignadas, ver figura 14. Cabe Resaltar que SNORT puede generar archivos de registro como .logs y .pcaps para que sean leídos posteriormente por Wireshark, así como también Wireshark puede también guardar ese tipo de archivos de registro provenientes de su captura a tiempo real. SNORT solamente se detendrá cuando el administrador de la Red lo desee ya que cuando se pone a la escucha de tráfico su tiempo es indefinido. Esta información estará a disposición del administrador de la Red con detalles específicos, fechas y horas exactas, ver figura 15.

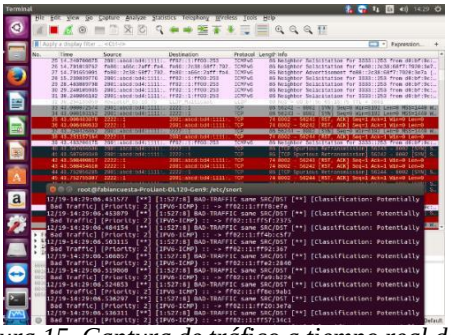

Figura 15. Captura de tráfico a tiempo real de la interfaz eno1 (puerto espejo) por parte de Wireshark y SNORT.

Wireshark: Lectura de paquetes .pcap de 6Guard y captura a tiempo real de ataques de la THC-IPv6.

La función específica de la Honeynet es detectar y recolectar toda la información disponible del atacante. Así que como se ha dicho anteriormente 6Guard genera paquetes .pcap que se guardan en la carpeta ./pcap, para que sean leídos por el administrador de la red por medio de Wireshark de una forma más concisa y detallada. Luego de finalizada la fase de Ataques de la THC-IPv6 se cargó uno de los paquetes .pcap generados por la detección de 6Guard de uno de los ataques para visualizarlo en Wireshark, ver figura 16.

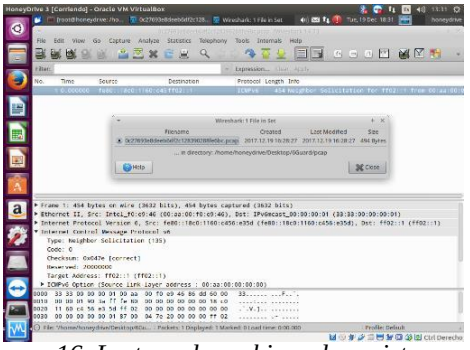

Figura 16. Lectura de archivos de registro .pcap en Wireshark generados por 6Guard.

Cabe recordar que 6Guard también genera archivos .log (guardados en la carpeta ./log) y estos también pueden ser leídos por Wireshark. También se realizó

captura a tiempo real del tráfico que circulaba por la interfaz eno2 del Server HP, por la cual 6Guard registra los ataques THC-IPv6 realizados en los diferentes lugares de la Honeynet LAN. Wireshark detecta todo el tráfico realizado por los ataques, pero sin la detección de que son ataques como tal, simplemente el tráfico recibido por dicha interfaz. Esta información puede ser utilizada para apoyar la suministrada por 6Guard o por cualquier otro tipo de Honeypot. En la figura 17, se puede apreciar el tráfico a tiempo real de la interfaz eno2 capturado por Wireshark. Allí se evidencia la conexión de una dirección IPv6 de enlace local de todos los nodos a un "Router" con dirección de enlace local bad:203… y dirección global 2002:1:2… Que de no ser por 6Guard no se sabría que toda esa información es falsa y generada por un ataque fake_router6. Una vez hecho esto, el administrador de la red humano adquiere todos los datos necesarios del atacante, realiza conclusiones y aprende de su carnada gracias a la recolección y análisis de toda esa información valiosa otorgada por la Honeynet y sus componentes para IPv6 presentados a lo largo de este documento. Lo que es tema para desarrollo de futuros estudios.

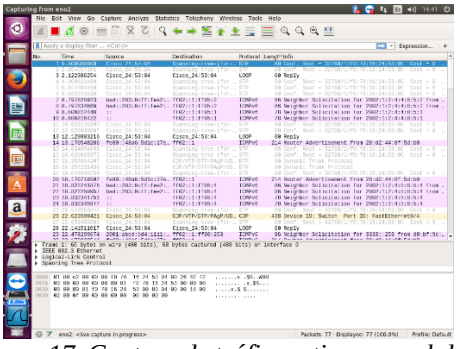

Figura 17. Captura de tráfico a tiempo real de la interfaz eno2 (6Guard) por parte de Wireshark, Fuente: Autores

5. CONCLUSIONES

Se realiza la implementación de una red Honeynet estática para entornos de red cableada apoyada en IPv6, en el laboratorio de redes y telecomunicaciones de la Universidad Francisco de Paula Santander Ocaña, utilizando herramientas como Ubuntu 16.04 LTS, Oracle VirtualBox, HoneyDrive 3, 6Guard, DionaeaFR, SNORT 2.9.2, Kali Linux 2017.3, Wireshark y las proporcionadas por el kit de THC-IPv6 donde se evidenció un completo conjunto de instrumentos para atacar las debilidades inherentes del protocolo de IPv6 e ICMPv6 y como estos varían en los diferentes sistemas operativos.

Con la finalidad de verificar el comportamiento de los ataques ante la Honeynet implementada se tomaron los detectados por 6guard que son subdivididos en 4 grupos y uno adicional. La ejecución y visualización de los ataques a través de la Honeynet se realizó satisfactoriamente excepto en algunos casos en donde para 6Guard, su precisión de detección disminuye. Estas imprecisiones se deben a falta de funciones mínimas como por ejemplo el Puerto Espejo. Sin embargo, esto no es obstáculo para el Honeypot en reconocer información de los ataques.

Por otro lado, para CDROM Honeywall Roo 1.4 se concluye que no hay compatibilidad entre este y el protocolo IPv6 o que no está documentada la implementación de este protocolo a un Honeywall Gateway, entonces por lo que se comprobó anteriormente no es posible realizar la implementación de un Honeywall Gateway a una Honeynet IPv6.

Enfocando los resultados finales de 6Guard, se puede hablar de que a partir de estos se puede obtener información muy valiosa y que tales resultados pueden ser evaluados de una manera totalmente positiva, el módulo Globalpot fue el más activo debido a su cercanía con Multicast Routing.

Como se generan cada día ataques de la THC-IPv6, estos se suman a una nueva ola de ataques IPv6, de la cual 6Guard es la primera recomendación para detectarlos. Junto con SNORT y demás Honeypots secundarios (Como Dionaea para la salida de LAN a Internet) se puede considerar como una herramienta clave para la mejora de la seguridad IPv6 en Entornos LAN.

Mediante los paquetes leídos por Wireshark se puede obtener un análisis más humano que sirve para tomar medidas luego de detectar al atacante y haber aprendido de él. También sirve el hecho de que el uso de IPv6 aún es reciente y limitado en las topologías LAN y muchos propietarios de Red al no querer realizar un pago justo para seguridad en IPv6 (debido a su escaso uso con respecto a IPv4), en el momento de que uno de estos Ataques se realice y se pierda información o elementos de valor como resultado de estos, lamentara no haber tenido en cuenta a IPv6 pues como se pudo observar, los ataques de la THC-IPv6 son ataques extremadamente complejos y peligrosos pero de muy fácil uso.

REFERENCIAS

Abbasi, F. H., & Harris, R. J. (2009). Experiences with a generation III virtual honeynet. *2009 Australasian Telecommunication Networks and Applications Conference, ATNAC 2009* -

Proceedings, (July 2014). https://doi.org/10.1109/ATNAC.2009.5464785

Acert. (2008). Manual de seguridad en redes.

Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications*, *66*. https://doi.org/10.1016/j.jnca.2016.03.006

Aziz, B. (2016). A formal model and analysis of an IoT protocol. *Ad Hoc Networks*. https://doi.org/10.1016/j.adhoc.2015.05.013

Borja, M. F. (2011). Análisis de tráfico con Wireshark, 52.

Carpene, C., Johnstone, M. N., & Woodward, A. J. (2017). The effectiveness of classification algorithms on IPv6 IID construction. *International Journal of Autonomous and Adaptive Communications Systems*, *10*(1), 15–22. https://doi.org/10.1504/IJAACS.2017.082735

Danieletto, M., Bui, N., & Zorzi, M. (2013). RAZOR: A compression and classification solution for the internet of things. *Sensors (Switzerland)*, *14*(1), 68–94. https://doi.org/10.3390/s140100068

Flauzac, O., Gonzalez, C., & Nolot, F. (2015). New security architecture for IoT network. In *Procedia Computer Science* (Vol. 52, pp. 1028–1033). Elsevier Masson SAS. https://doi.org/10.1016/j.procs.2015.05.099

Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). *The internet of things*. *Scientific American* (Vol. 291). https://doi.org/10.1038/scientificamerican1004-76

Hogg, C., & Vyncke, E. (2009). *IPv6 Security*. *Engineer*.

Information, F. F. (n.d.). ICMP for IPv6 Redirect ICMP for IPv6, (Mld), 1–8.

Kali. (2015). Kali linux tutorial.

Katz. Matías David. (2013). Redes y seguridad. *Alfaomega Grupo Editor*, (Mexico), 87.

Li, S., Xu, L. Da, & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Luvisi, A., & Lorenzini, G. (2014). RFID-plants in the smart city: Applications and outlook for urban green management. *Urban Forestry and Urban Greening*, *13*(4), 630–637. https://doi.org/10.1016/j.ufug.2014.07.003

Miguel, Sandra Edith; Gómez, Nancy Diana; Bongiovani, P. (2012). Acceso abierto real y potencial a la producción científica de un país. El caso argentino. *El Profesional de La Información*, *21*(2), 146–153.

S. A. A. Acevedo, D. R. Bautista. (2017). Análisis de una red en un entorno IPV6: una mirada desde las intrusiones de red y el modelo TCP/IP. REVISTA COLOMBIANA DE TECNOLOGÍAS DE AVANZADA, ISSN: 1692-7257. 1(29).

Alvernia Acevedo, S., & Rico Bautista, D. (2017). Análisis de una red en un entorno IPV6: una mirada desde las intrusiones de red y el modelo TCP/IP. REVISTA COLOMBIANA DE TECNOLOGÍAS DE AVANZADA, 1(29).

Rico-Bautista, D., Medina-Cárdenas, Y. C., & Rojas-Osorio, J. A. (2016). PENTESTING EMPLEANDO TECNICAS DE ETHICAL HACKING EN REDES IPv6. *Revista Ingenio UFPSO*, *11*(70–96), 1.

Rico-Bautista, D., Medina-Cárdenas, Y. C., & Santos Jaimes, L. M. (2008). Ipsec De Ipv6 En La Universidad De Pamplona. *Scientia Et Technica*, *2*(39), 320–325. https://doi.org/http://dx.doi.org/10.22517/23447214.3239

S., L. M., & R., D. W. (2007). IPV6 en la Universidad de Pamplona: Estado del arte. *Scientia Et Technica*, *XIII*, 415–420.

Schütte, M. (2014). The IPv6 Snort Plugin • Diploma thesis, (March).

Sochor, T., & Zuzcak, M. (2015). Application of honeypots in IPv6 networks. In *AIP Conference Proceedings* (Vol. 1648). https://doi.org/10.1063/1.4912767

Stočes, M., Vaněk, J., Masner, J., & Pavlík, J. (2016). Internet of Things (IoT) in Agriculture - Selected Aspects. *Agris On-Line Papers in Economics and Informatics*, *VIII*(1), 83–88. https://doi.org/10.7160/aol.2016.080108

Vinueza Jaramillo, T. A. (2012). Universidad Técnica Del Norte.

Xia, W., Tsou, T., Lopez, D., Lu, F., Sun, Q., Feng, W., … Xie, H. (2014). A software defined approach to unified IPv6 transition. *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?, K 2014*, 9–13. https://doi.org/10.1109/Kaleidoscope.2014.6858474

Yin, C., Li, M., Ma, J., & Sun, J. (2004). Honeypot and scan detection in intrusion detection system. In *Canadian Conference on Electrical and Computer Engineering* (Vol. 2, pp. 1107–1110).