edulearn
Revista Multidisciplinar

Vol. 1 | Núm. 2 | Abril – Junio 2026
DOI: https://doi.org/10.64973/jqpsh245
ISSN: 3151-8370
Fecha de recepción: 24/04/2026
Fecha de aceptación: 11/05/2026
Fecha de publicación: 30/06/2026

Ataques DHCP Spoofing y DHCP Starvation en redes LAN: simulación, análisis de impacto y medidas de mitigación

DHCP Spoofing and DHCP Starvation Attacks in LAN Networks: Simulation, Impact Analysis, and Mitigation Measures

Gabriel Emilio García Mazón [1]*, Bryan Steven Moreno Morocho [1]

Adrian Alonso Vega Macas [1], Freddy Daniel Zambrano Pineda [1]

[1] *Universidad Técnica de Machala, Ecuador.*

* *Autor de Correspondencia: ggarcia7@utmachala.edu.ec*

Resumen: Los ataques de DHCP Spoofing y DHCP Starvation constituyen amenazas relevantes para la seguridad de las redes LAN, debido a que permiten la suplantación de servidores DHCP legítimos, el agotamiento de direcciones IP disponibles y la redirección del tráfico hacia equipos controlados por un atacante. Este estudio tuvo como objetivo simular, analizar y evaluar el impacto de estos ataques en un entorno virtualizado mediante GNS3, VMware, Kali Linux y herramientas especializadas como Ettercap, Yersinia, Dnsmasq y Wireshark. Para ello, se diseñaron dos escenarios de prueba: el primero orientado a la suplantación de la puerta de enlace mediante respuestas DHCP falsas, y el segundo enfocado en el agotamiento del pool de direcciones del servidor legítimo, seguido de la asignación de parámetros de red maliciosos. Los resultados evidenciaron que las vulnerabilidades del protocolo DHCP pueden ser explotadas para alterar la configuración de los clientes y comprometer la disponibilidad, integridad y confidencialidad del tráfico en redes locales. Asimismo, se comprobó la utilidad de mecanismos de defensa como DHCP Snooping, IP Source Guard, Dynamic ARP Inspection y limitación de solicitudes DHCP. El estudio aporta evidencia práctica para fortalecer la prevención, detección y mitigación de amenazas DHCP en infraestructuras LAN.

Palabras clave: DHCP Spoofing, DHCP Starvation, Seguridad de redes, GNS3, medidas de mitigación.

Abstract: Spoofing and DHCP Starvation attacks constitute significant threats to the security of LAN networks, as they enable the impersonation of legitimate DHCP servers, the exhaustion of available IP addresses, and the redirection of traffic toward devices controlled by an attacker. This study aimed to simulate, analyze, and evaluate the impact of these attacks in a virtualized environment using GNS3, VMware, Kali Linux, and specialized tools such as Ettercap, Yersinia, Dnsmasq, and Wireshark. For this purpose, two test scenarios were designed: the first focused on gateway impersonation through false DHCP responses, and the second focused on exhausting the address pool of the legitimate server, followed by the assignment of malicious network parameters. The results showed that DHCP protocol vulnerabilities can be exploited to alter client configuration and compromise the availability, integrity, and confidentiality of traffic in local networks. Likewise, the usefulness of defense mechanisms such as DHCP Snooping, IP Source Guard, Dynamic ARP Inspection, and DHCP request rate limiting was verified. This study provides practical evidence to strengthen the prevention, detection, and mitigation of DHCP-based threats in LAN infrastructures.

Keywords: DHCP Spoofing, DHCP Starvation, Network security, GNS3, mitigation measures.

1. Introducción

La seguridad de las redes locales constituye un componente esencial en la protección de la información, la continuidad operativa y la confiabilidad de los servicios digitales. En entornos institucionales, académicos y empresariales, los dispositivos conectados dependen de protocolos de red que automatizan procesos fundamentales, como la asignación de direcciones IP, puertas de enlace y servidores DNS. Entre estos protocolos, DHCP (Dynamic Host Configuration Protocol) cumple una función central al permitir que los equipos obtengan automáticamente los parámetros necesarios para comunicarse dentro de una red (Droms, 1997). No obstante, su diseño carece de mecanismos robustos de autenticación, lo que lo convierte en un objetivo vulnerable frente a ataques de suplantación y manipulación de tráfico (AbdulGhaffar et al., 2023; Droms, 2001).

Dentro de este contexto, los ataques DHCP Spoofing y DHCP Starvation representan amenazas relevantes para las redes LAN. El DHCP Spoofing permite que un atacante suplante un servidor DHCP legítimo y entregue configuraciones falsas a los clientes de la red, como una puerta de enlace maliciosa o servidores DNS controlados por el atacante. Por su parte, el DHCP Starvation busca agotar el pool de direcciones IP disponibles del servidor legítimo mediante múltiples solicitudes fraudulentas, generando condiciones para que un servidor DHCP falso asigne parámetros de red no autorizados. Estas técnicas pueden facilitar la redirección del tráfico, la interceptación de comunicaciones y la ejecución de ataques de tipo Man-in-the-Middle, comprometiendo la disponibilidad, integridad y confidencialidad de la información transmitida en la red (Cruz et al., 2017; Pradana & Budiman, 2021; Syed et al., 2022).

La protección frente a este tipo de amenazas es un desafío importante para los administradores de redes, especialmente en infraestructuras donde el crecimiento de dispositivos conectados aumenta la superficie de ataque. Aunque existen mecanismos de defensa como DHCP Snooping, IP Source Guard, Dynamic ARP Inspection y la limitación de solicitudes DHCP por puerto, su efectividad depende de una configuración adecuada y de la comprensión del comportamiento del tráfico durante el ataque. En este sentido, los entornos de simulación permiten analizar escenarios de riesgo sin

comprometer redes productivas, facilitando la observación técnica de los ataques y la evaluación de medidas preventivas en condiciones controladas.

A partir de esta problemática, el presente estudio se orienta a responder la siguiente pregunta de investigación: ¿cómo afectan los ataques DHCP Spoofing y DHCP Starvation la configuración y seguridad de los clientes en una red LAN simulada, y qué medidas de mitigación permiten reducir su impacto? Para abordar esta interrogante, se desarrolló un laboratorio virtualizado mediante GNS3, VMware y Kali Linux, empleando herramientas especializadas como Ettercap, Yersinia, Dnsmasq y Wireshark. El estudio se estructuró en dos escenarios: el primero centrado en la suplantación de la puerta de enlace mediante respuestas DHCP falsas, y el segundo enfocado en el agotamiento del pool de direcciones del servidor legítimo, seguido de la asignación de parámetros maliciosos por parte de un servidor DHCP falso.

El objetivo general de esta investigación es simular, analizar y evaluar el impacto de ataques DHCP Spoofing y DHCP Starvation en redes LAN virtualizadas, así como valorar la utilidad de mecanismos de mitigación orientados a la seguridad de capa 2. De manera específica, se busca: identificar el comportamiento del tráfico DHCP durante los ataques, comprobar los efectos sobre la configuración de los clientes, analizar la efectividad de medidas defensivas como DHCP Snooping, IP Source Guard y Dynamic ARP Inspection, y proponer recomendaciones técnicas para fortalecer la prevención y detección de amenazas DHCP en infraestructuras de red locales.

Este trabajo aporta evidencia práctica sobre la explotación de vulnerabilidades asociadas al protocolo DHCP y ofrece una aproximación experimental para comprender su impacto en redes LAN. Además, proporciona una base técnica útil para docentes, estudiantes y profesionales de tecnologías de la información interesados en la seguridad de redes, la simulación de ataques y la implementación de controles preventivos en entornos controlados.

2. Metodología

El presente estudio se desarrolló bajo un enfoque aplicado, de tipo experimental-descriptivo, debido a que se diseñaron escenarios controlados de simulación para

observar el comportamiento de ataques DHCP Spoofing y DHCP Starvation en redes LAN virtualizadas, así como la respuesta de diferentes mecanismos de mitigación. El diseño metodológico correspondió a un estudio experimental en laboratorio, basado en la construcción, ejecución y comparación de escenarios de red con y sin medidas de seguridad. El contexto de la investigación fue un entorno virtualizado mediante VMware y GNS3, lo que permitió recrear condiciones similares a una red local institucional o empresarial sin comprometer infraestructuras reales ni exponer información sensible (Ramón et al., 2023).

La unidad de análisis estuvo conformada por dos topologías de red simuladas. La primera topología incluyó un router configurado como servidor DHCP legítimo, un switch y dos máquinas virtuales: una con Kali Linux, que cumplió el rol de atacante, y otra con Ubuntu, que actuó como cliente víctima. Este escenario permitió evaluar un ataque de DHCP Spoofing mediante la suplantación de la puerta de enlace, utilizando respuestas DHCP falsas generadas desde la máquina atacante. La segunda topología estuvo compuesta por un router con servicio DHCP habilitado, un switch principal y varios hosts conectados a la red 192.168.10.0/24, incluyendo una máquina Kali Linux. En este caso se evaluó un ataque de DHCP Starvation mediante el agotamiento del pool de direcciones IP del servidor legítimo, seguido de la asignación de parámetros de red maliciosos desde un servidor DHCP falso configurado con Dnsmasq.

La selección de los escenarios fue intencional y respondió a criterios técnicos de pertinencia, reproducibilidad y seguridad. Se eligieron topologías que permitieran representar dos formas comunes de explotación del protocolo DHCP: la suplantación directa del servidor legítimo y el agotamiento de direcciones IP disponibles. Asimismo, se consideró la posibilidad de aplicar controles defensivos a nivel de switch, tales como DHCP Snooping, IP Source Guard, Dynamic ARP Inspection y limitación de solicitudes DHCP por puerto, con el fin de comparar el comportamiento de la red antes y después de la implementación de dichas medidas (Ponce Guerrero, 2024).

Para la recolección de datos se empleó la observación experimental del comportamiento de la red, la captura de tráfico, la verificación de configuraciones IP, las pruebas de conectividad y el análisis de registros generados por las herramientas utilizadas. Los principales instrumentos fueron GNS3 para la simulación de routers y switches, VMware para la ejecución de máquinas virtuales, Kali Linux como plataforma de ataque, Ubuntu como cliente víctima, Ettercap para la generación de respuestas DHCP falsas, Yersinia para la ejecución del ataque de agotamiento de direcciones, Dnsmasq para la configuración del servidor DHCP malicioso y Wireshark para la captura y análisis de paquetes DHCP.

El procedimiento se desarrolló en cinco fases. En la primera fase se construyeron las topologías en GNS3 y se configuraron los dispositivos de red, incluyendo direccionamiento IP, servicio DHCP, VLAN, enlaces troncales y conectividad básica entre los nodos. En la segunda fase se verificó el funcionamiento normal de la red mediante pruebas de conectividad y revisión de las direcciones asignadas por el servidor DHCP legítimo. En la tercera fase se ejecutaron los ataques: en el primer escenario se utilizó Ettercap para enviar respuestas DHCP falsas y modificar la puerta de enlace del cliente víctima; en el segundo escenario se empleó Yersinia para generar múltiples solicitudes DHCP Discovery hasta agotar el pool de direcciones del servidor legítimo, permitiendo posteriormente que Dnsmasq asignara direcciones IP maliciosas desde Kali Linux. En la cuarta fase se capturó y examinó el tráfico mediante Wireshark, identificando paquetes DHCP Discover, Offer, Request y ACK, así como cambios en la dirección IP, puerta de enlace y origen de la asignación DHCP. Finalmente, en la quinta fase se aplicaron medidas de mitigación en el switch y se comparó el comportamiento de la red frente a los ataques.

El análisis de la información fue descriptivo y comparativo. Se revisaron los cambios producidos en la configuración de los clientes, la asignación de direcciones IP legítimas o maliciosas, la modificación de la puerta de enlace, la disponibilidad del pool DHCP, la respuesta del switch ante tráfico anómalo y la efectividad de las medidas de defensa implementadas. La comparación entre escenarios permitió determinar el impacto de los ataques sobre la seguridad de la red y valorar la utilidad de los controles aplicados para prevenir, limitar o bloquear la suplantación DHCP y el agotamiento de direcciones IP.

Desde el punto de vista ético y de seguridad, las pruebas se realizaron exclusivamente en un entorno virtualizado y aislado, sin intervención sobre redes productivas, usuarios reales ni datos institucionales sensibles. Por tanto, el estudio no requirió consentimiento informado, ya que no involucró participantes humanos ni procesamiento de información personal. Esta condición permitió ejecutar las pruebas de manera controlada, reduciendo riesgos y garantizando que las actividades tuvieran fines académicos, experimentales y formativos.

3. Resultados

Los resultados se organizaron en función de los dos escenarios experimentales implementados en GNS3. El primer escenario correspondió a un ataque de DHCP Spoofing mediante suplantación de la puerta de enlace, mientras que el segundo evaluó un ataque de DHCP Starvation combinado con la asignación de parámetros maliciosos por parte de un servidor DHCP falso. En ambos casos, se verificó previamente la conectividad de los dispositivos y la asignación normal de direcciones IP desde el servidor DHCP legítimo.

3.1. Resultados del escenario 1: DHCP Spoofing mediante Ettercap

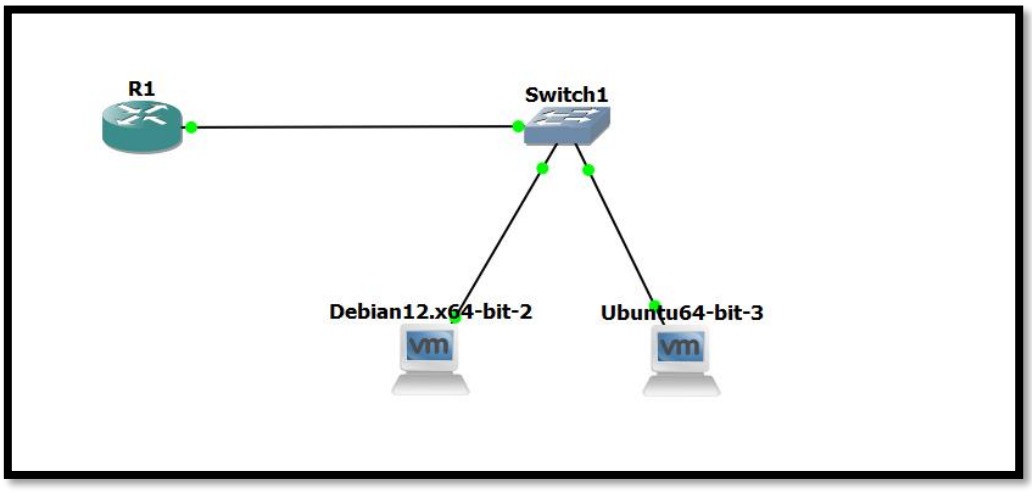

Ilustración 1. Topología Caso Práctico 1

En el primer escenario se configuró una red compuesta por un router con servicio DHCP habilitado, un switch y dos máquinas virtuales: Kali Linux como equipo atacante y Ubuntu como equipo víctima. Antes de ejecutar el ataque, las pruebas de conectividad

confirmaron la comunicación entre el router, Kali Linux y Ubuntu. Asimismo, se verificó que la máquina Ubuntu recibía una dirección IP válida desde el servidor DHCP legítimo.

Ilustración 2. Conectividad entre los dispositivos

Posteriormente, desde Kali Linux se ejecutó Ettercap para generar respuestas DHCP falsas. Durante la configuración del ataque se definió una puerta de enlace maliciosa correspondiente al equipo atacante. Una vez reactivado el servicio DHCP en la máquina víctima, se observó que Ubuntu mantuvo la dirección IP 192.168.1.12; sin embargo, la puerta de enlace cambió de 192.168.1.1, correspondiente al router legítimo, a 192.168.1.11, correspondiente al equipo atacante. Este cambio confirmó que la víctima aceptó parámetros de red proporcionados por el servidor DHCP falso.

Ilustración 3. Ataque de respuestas DHCP falsas usando Ettercap

La captura realizada con Wireshark permitió observar paquetes DHCP asociados al proceso de asignación, incluyendo respuestas enviadas desde el servidor falso hacia la máquina víctima. De igual manera, los registros de Ettercap evidenciaron el envío de paquetes DHCP falsificados. Como resultado, el tráfico de la máquina víctima quedó direccionado hacia la puerta de enlace controlada por el atacante.

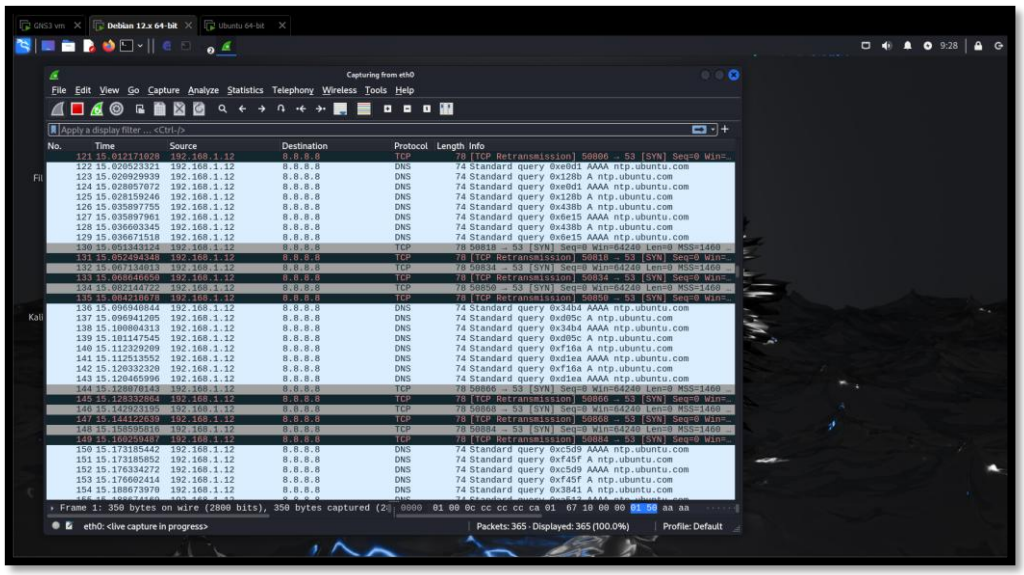

Ilustración 4. Verificación de ataque usando Wireshark

3.2. Herramientas de análisis forense digital aplicadas a entornos reales

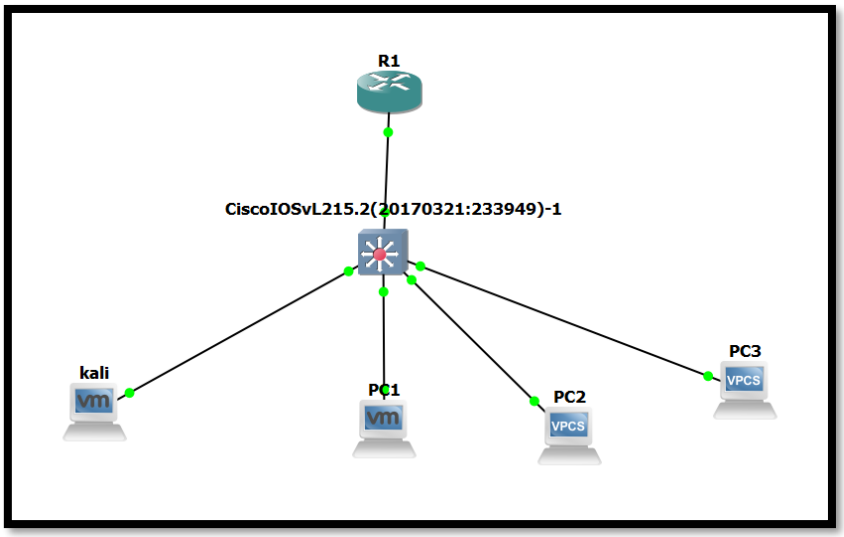

Ilustración 5. Topología Caso Práctico 2

En el segundo escenario se implementó una topología compuesta por un router, un switch principal y cuatro hosts conectados a la red 192.168.10.0/24, incluyendo una máquina Kali Linux como atacante. Se configuró la VLAN 10 en el switch y una subinterfaz en el router para gestionar el tráfico de dicha VLAN. El servidor DHCP legítimo fue configurado con un rango limitado de direcciones IP entre 192.168.10.21 y 192.168.10.30.

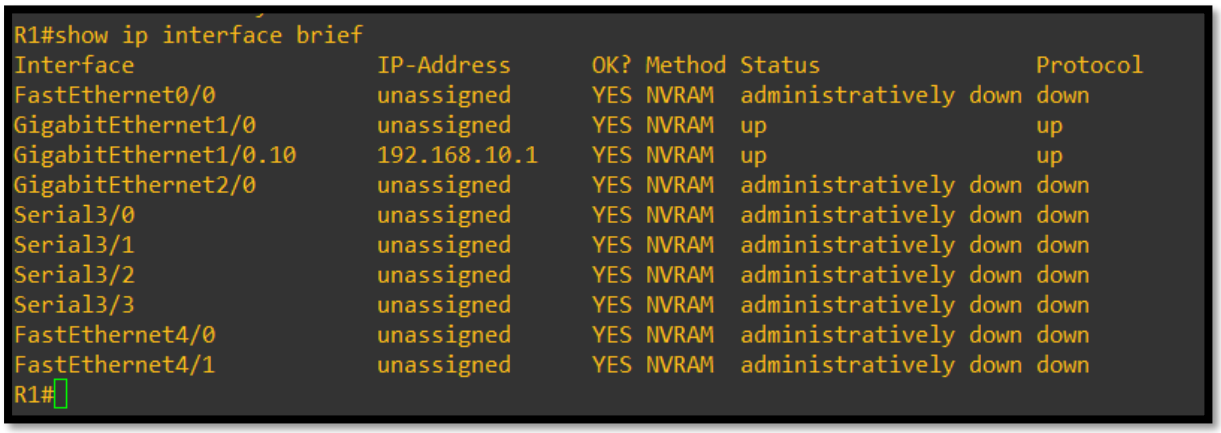

Ilustración 6. Configuración de Interfaces R1 Caso Práctico 2

Antes del ataque, el router asignó direcciones IP legítimas a los hosts conectados. Luego, mediante Yersinia, se ejecutó un ataque de DHCP Discovery orientado a saturar el servidor legítimo con múltiples solicitudes. Como resultado, el pool de direcciones IP disponibles fue agotado. Posteriormente, el servidor DHCP falso configurado en Kali Linux mediante Dnsmasq asignó parámetros de red maliciosos dentro del rango 10.2.2.0/24. En particular, se evidenció que uno de los hosts recibió la dirección IP 10.2.2.93, asignada por el servidor DHCP falso.

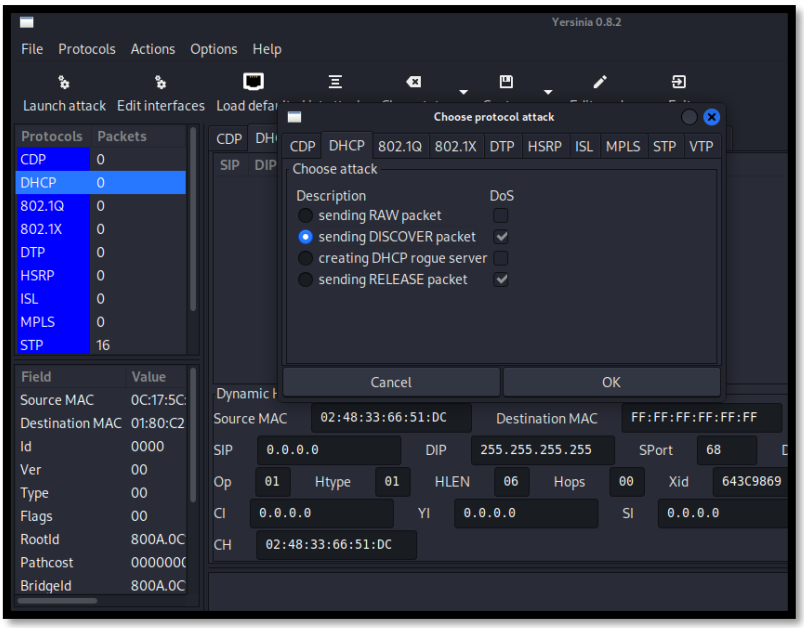

Ilustración 7. Ejecución de ataque DHCP Discovery Caso Práctico 2

Después de comprobar la efectividad del ataque, se aplicaron medidas de mitigación en el switch. Se habilitó DHCP Snooping en las VLAN configuradas, se marcó como confiable el puerto conectado al servidor DHCP legítimo y se configuraron los puertos de usuario como no confiables. Además, se aplicó IP Source Guard, Dynamic ARP Inspection y una limitación de tasa de solicitudes DHCP de 10 paquetes por segundo. Tras estas configuraciones, el switch detectó el exceso de tráfico DHCP y colocó la interfaz del atacante en estado err-disable, bloqueando el tráfico malicioso. Luego de aplicar las medidas de seguridad, un host solicitó dirección IP y recibió una dirección del rango legítimo, específicamente 192.168.10.21, lo que confirmó que el servidor DHCP falso ya no podía asignar direcciones maliciosas.

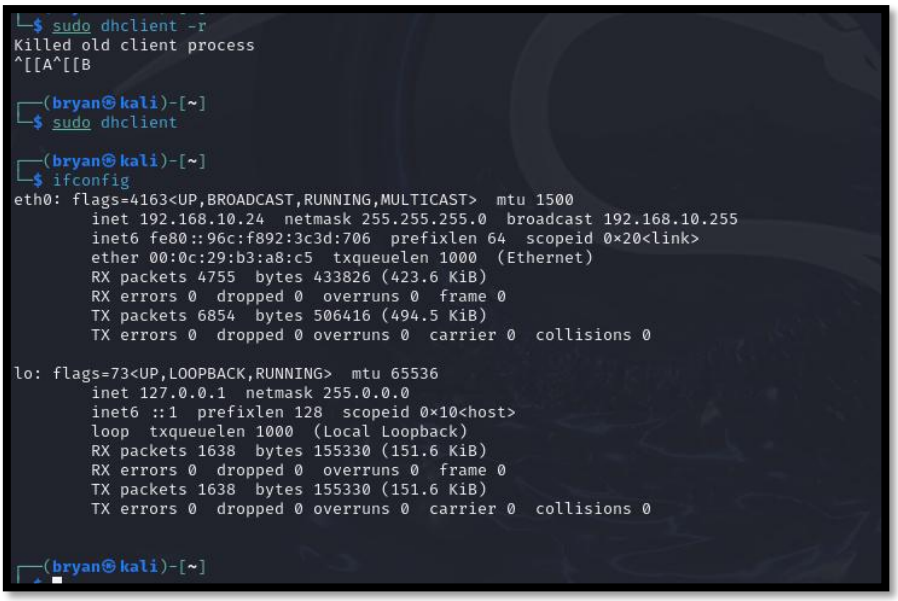

Ilustración 8. Asignación de IP a PC2 mediante un servidor DHCP falso Caso Práctico 2

Tabla 1. Escenario de aplicación DHCP

Escenario evaluado	Ataque aplicado	Condición inicial de la red	Resultado sin medidas de mitigación	Medidas de seguridad aplicadas	Resultado posterior a la mitigación
Suplantación DHCP mediante puerta de enlace falsa	DHCP Spoofing con Ettercap	El cliente Ubuntu recibía una dirección IP válida desde el servidor DHCP legítimo del router.	La máquina víctima mantuvo la dirección IP 192.168.1.12, pero cambió su puerta de enlace de 192.168.1.1 a 192.168.1.11, correspondiente al equipo atacante.	No se aplicaron medidas de mitigación en este escenario.	No evaluado en este escenario.
Agotamiento del pool DHCP y	DHCP Starvation con	El router asignaba direcciones IP	El pool de direcciones del servidor DHCP	DHCP Snooping, IP Source	El switch bloqueó el tráfico

asignación maliciosa	Yersinia y servidor DHCP falso con Dnsmasq	legítimas dentro del rango 192.168.10.21–192.168.10.30.	legítimo fue agotado y el servidor DHCP falso asignó una dirección maliciosa del rango 10.2.2.0/24.	Guard, Dynamic ARP Inspection y limitación de solicitudes DHCP a 10 paquetes por segundo.	anómalo mediante el estado err-disable y el host recibió una dirección IP legítima del servidor autorizado.

4. Discusión

Los resultados obtenidos evidencian que el protocolo DHCP presenta vulnerabilidades relevantes cuando opera en redes LAN sin mecanismos de autenticación o control a nivel de switch. En el primer escenario, la aceptación de una puerta de enlace falsa por parte de la máquina víctima demuestra que un atacante conectado a la misma red puede manipular parámetros críticos de configuración. Aunque la dirección IP del cliente no cambió, la modificación de la puerta de enlace fue suficiente para redirigir el tráfico hacia el equipo atacante. Este hallazgo confirma que el impacto del DHCP Spoofing no depende únicamente de la asignación de una nueva dirección IP, sino también de la alteración de parámetros como gateway y DNS, los cuales pueden facilitar ataques de intermediario o Man-in-the-Middle.

En el segundo escenario, el agotamiento del pool de direcciones del servidor DHCP legítimo permitió que un servidor falso asignara direcciones IP maliciosas a los hosts de la red. Este resultado confirma que el DHCP Starvation puede ser utilizado como una fase previa para facilitar ataques de suplantación DHCP. La combinación de Yersinia para generar solicitudes DHCP masivas y Dnsmasq para entregar configuraciones maliciosas demostró que, en ausencia de controles, el servidor legítimo puede perder capacidad de respuesta frente a clientes válidos. Este comportamiento coincide con los riesgos descritos en la literatura sobre vulnerabilidades del protocolo DHCP,

especialmente en relación con la ausencia de autenticación nativa y la posibilidad de manipular la configuración de los clientes (Pradana & Budiman, 2021; Uddin, 2022).

La aplicación de medidas defensivas en el segundo escenario permitió comprobar que los controles de seguridad de capa 2 son efectivos para reducir el impacto de estos ataques (Cisco, 2024; Pradana & Budiman, 2021). DHCP Snooping permitió diferenciar puertos confiables y no confiables, evitando que respuestas DHCP no autorizadas fueran aceptadas por la red. IP Source Guard y Dynamic ARP Inspection fortalecieron la validación de direcciones IP y MAC, mientras que la limitación de tasa de solicitudes DHCP permitió detectar y bloquear el comportamiento anómalo generado por el atacante. El estado err-disable activado en la interfaz comprometida evidenció una respuesta automática del switch frente al exceso de tráfico DHCP, lo que impidió que el ataque continuara afectando al servidor legítimo.

Estos hallazgos tienen implicaciones prácticas para la administración de redes institucionales, académicas y empresariales. En redes donde los puertos de acceso no cuentan con controles adecuados, un atacante interno o un dispositivo no autorizado puede alterar la configuración de los clientes y comprometer la confidencialidad, integridad y disponibilidad del tráfico. Por ello, la seguridad DHCP no debe limitarse a la configuración del servidor, sino que debe complementarse con controles en switches, segmentación mediante VLAN, monitoreo de tráfico y políticas de acceso a la red.

No obstante, el estudio presenta algunas limitaciones. En primer lugar, las pruebas se realizaron en un entorno virtualizado, por lo que los resultados pueden variar en infraestructuras físicas con mayor cantidad de dispositivos, tráfico real y configuraciones heterogéneas. En segundo lugar, los escenarios evaluados se centraron en ataques específicos de DHCP Spoofing y DHCP Starvation, sin incluir otros vectores complementarios como suplantación ARP avanzada, ataques DNS o mecanismos de evasión. En tercer lugar, la efectividad de las medidas de mitigación depende de una configuración correcta: si los puertos confiables se definen de forma incorrecta o si la tasa de solicitudes DHCP se establece sin considerar el tamaño de la red, podrían generarse bloqueos no deseados o falsos positivos.

En función de los objetivos planteados, el estudio permitió comprobar la efectividad de los ataques DHCP en entornos LAN no protegidos, identificar comportamientos anómalos asociados a solicitudes DHCP repetitivas y respuestas no autorizadas, y validar la utilidad de mecanismos de defensa como DHCP Snooping, IP Source Guard, Dynamic ARP Inspection y limitación de tasa. Para un estudio futuro, se recomienda ampliar las pruebas hacia escenarios con mayor número de hosts, integrar mecanismos de autenticación como 802.1X y explorar modelos de detección temprana basados en análisis automatizado del tráfico DHCP.

5. Conclusiones

El estudio permitió comprobar que los ataques DHCP Spoofing y DHCP Starvation representan riesgos significativos para la seguridad de redes LAN, debido a que pueden alterar parámetros críticos de configuración, agotar el pool de direcciones del servidor legítimo y facilitar la asignación de parámetros maliciosos mediante servidores DHCP falsos. Los resultados evidencian que la ausencia de mecanismos nativos de autenticación en el protocolo DHCP puede comprometer la disponibilidad, integridad y confidencialidad del tráfico, especialmente en redes sin controles adecuados a nivel de switch. Asimismo, se verificó que medidas como DHCP Snooping, IP Source Guard, Dynamic ARP Inspection y la limitación de solicitudes DHCP contribuyen a reducir el impacto de estos ataques, al bloquear tráfico anómalo y permitir que los clientes reciban direcciones desde el servidor autorizado. En este sentido, los entornos virtualizados como GNS3 y VMware resultan útiles para analizar amenazas de red de forma segura, controlada y replicable. Como línea futura, se recomienda ampliar la evaluación hacia redes con mayor número de hosts, tráfico más diverso y escenarios físicos o híbridos, además de considerar mecanismos de autenticación como 802.1X y modelos de detección temprana basados en análisis automatizado del tráfico DHCP (Lilaram et al., 2022).

Conflicto de intereses

Los autores declaran que no existe conflicto de intereses.

Financiamiento

Este trabajo no fue financiado por ninguna organización u empresa.

Declaración sobre inteligencia artificial

Los autores declaran que se utilizaron herramientas de inteligencia artificial generativa para los siguientes fines: Traducción del resumen. Los autores asumen la plena responsabilidad del contenido del manuscrito.

Aporte de los autores

Gabriel Emilio García Mazón: Participó en el diseño metodológico del estudio, la estructuración del artículo, la redacción del borrador original en las secciones de metodología y conclusiones, así como en la revisión y edición final del manuscrito.

Bryan Steven Moreno Morocho: Participó en la investigación experimental, configuración del entorno de simulación, uso de herramientas de software, generación de evidencias visuales y redacción del borrador original correspondiente a los resultados del segundo escenario experimental.

Adrián Alonso Vega Macas: Participó en la investigación experimental, validación de resultados, generación de evidencias visuales y redacción del borrador original correspondiente a los resultados del primer escenario experimental.

Freddy Daniel Zambrano Pineda: Participó en la conceptualización del estudio, apoyo metodológico, redacción del borrador original en las secciones de resumen e introducción, y supervisión general del desarrollo del manuscrito.

Referencias

AbdulGhaffar, A., Paul, S. K., & Matrawy, A. (2023). An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures. 2023 Biennial Symposium on Communications (BSC), 119–124. https://doi.org/10.1109/BSC57238.2023.10201458

Cisco. (2024). Troubleshoot Dynamic ARP Inspection (DAI) and IP Source Guard (IPSG) in Catalyst Switches. Cisco. https://www.cisco.com/c/en/us/support/docs/switches/lan-switch-software/222274-troubleshoot-dynamic-arp-inspection-dai.html

Cruz, J. C., López, A. Z., Cruz, C. A., & Cortez, J. V. (2017). ANÁLISIS DE ATAQUES DE RED DEL TIPO DHCP SPOOFING, TCP SYN FLOOD Y PAQUETES MALFORMADOS. 39(128).

Droms, R. (1997). Dynamic Host Configuration Protocol (No. RFC2131; p. RFC2131). RFC Editor. https://doi.org/10.17487/rfc2131

Droms, R. (2001). Authentication for DHCP Messages (W. Arbaugh, Ed.; No. RFC3118; p. RFC3118). RFC Editor. https://doi.org/10.17487/rfc3118

Lilaram, H., Talpur, S., Murtaza, A., Syed, S., & Khuhawar, F. (2022). Detection Of Server-Side DHCP DoS And Spoofing Attack Using Machine Learning Techniques.

Ponce Guerrero, J. L. (2024). Seguridad en redes LAN: La protección de datos hasta la prevención de intrusiones. Journal TechInnovation, 3(1), 4–14. https://doi.org/10.47230/Journal.TechInnovation.v3.n1.2024.4-14

Pradana, D. A., & Budiman, A. S. (2021). The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack. IJID (International Journal on Informatics for Development), 10(1), 38–46. https://doi.org/10.14421/ijid.2021.2287

Ramón, L., Pallo, R., Gracia, E., & Naranjo, V. (2023). Revista de Ciencias de Seguridad y Defensa Emulation of Denial of Service Attacks Using a LAN Topology in GNS3.

Syed, S., Khuhawar, F., Talpur, S., Memon, A. A., Luque-Nieto, M.-A., & Narejo, S. (2022). Analysis of Dynamic Host Control Protocol Implementation to Assess DoS Attacks. 2022 Global Conference on Wireless and Optical Technologies (GCWOT), 1–7. https://doi.org/10.1109/GCWOT53057.2022.9772887