Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

# Analysing the Impact of Common IPv6 Attacks on Different Operating Systems in Local Networks

Omar Hasan AlhagAli
Department of Web Technologies, Syrian Virtual University, Damascus, Syria.
Department of Bachelor in Information Technology, Syrian Virtual University.
Damascus, Syria
P. H. D. Bassel Alkhatib
Damascus University.
Damascus, Syria.

***Abstract*—The continuous growth of internet requirements necessitates new technologies that can support large numbers of users, services, and increasing demands. IPv6, designed as a network protocol, addresses these needs. IPv6 is referred to as the Next-Generation Internet Protocol due to its new features that make it the focus of attention and future directions. This protocol was introduced to address the main issue of address exhaustion in IPv4. IPv6, the sixth version of the protocol, has achieved many important features and has overcome some of the weaknesses present in the fourth version, IPv4. One of the most significant features is finding a more suitable solution to the problem of real address depletion. It also achieves automatic address configuration using one of two methods: DHCPv6 (Dynamic Host Configuration Protocol version 6) or the second method, SLAAC (Stateless Address Autoconfiguration). It further enhances the efficiency of route aggregation for routing paths and allows internet users to connect to networks through a "plug-and-play" approach. IPv6 introduces key new protocols, including ICMPv6 for address configuration, NDP, and DAD for detecting duplicates. This prompts the need for security techniques due to emerging vulnerabilities. This research will involve analysing several attacks, including false router advertisements, virtual router deletion attacks, flood attacks using Neighbour Solicitation (NS) messages, and Smurf attacks using ICMPv6 request messages. These attacks will be executed using the Scapy program on a local network composed of different operating systems (Windows & Linux) through the Virtual Box simulation program. Subsequently, these attacks will be analysed using Wireshark, then their impact on various systems will be studied.**

***Keywords*—IPv6 Attacks; DDos; ICMPv6; NDP.**

## I.INTRODUCTION

The evolution of internet protocols has marked a captivating journey that has shaped today's interconnected world. From the foundational IPv4 to the ground-breaking IPv6, each phase of this evolution has addressed challenges and unlocked novel possibilities in digital communication.

The journey from IPv4 to IPv6 vividly underscores the dynamic nature of technological progress. While IPv4's address space was initially perceived as vast, the exponential expansion of the digital realm gradually exposed its limitations. As the number of connected devices surged, the challenges posed by IPv4's finite address space came to the forefront. The imminent exhaustion of available IPv4 addresses necessitated innovative solutions to ensure continued growth and network stability. Interim solutions like Network Address Translation (NAT) and sub-netting were introduced to tackle this pressing concern. NAT facilitated multiple devices to share a single public IP address, extending the utility of the existing address pool. In tandem, sub-netting improved IP address allocation within organizations. However, these measures introduced complexities that hindered direct device communication [11].

Amid these challenges, IPv6 emerged as the definitive solution. With its expansive 128-bit address space, IPv6 eliminated the need for NAT and fostered direct device-to-device communication. Beyond addressing numerical constraints, IPv6 introduced architectural refinements and robust security enhancements, reaffirming its future-oriented design.

IPv6 brought transformative improvements, such as streamlined header formats, simplified routing mechanisms, enhanced mobility support, and embedded security mechanisms. These enhancements laid the foundation for a more efficient, secure, and adaptable networking framework. However, the integration of auxiliary protocols like ICMPv6 and NDP into IPv6 gave rise to new security challenges [10].

While essential for efficient network operations, ICMPv6, responsible for network diagnostics, and NDP, governing neighbour relationships, introduced potential vulnerabilities that could be exploited.

These security challenges materialized in notable attacks like the IPv6 False Router Advertisement (FRA) Attack, Router Deletion Attack, NS Flood Attack, and ICMPv6 Smurf Attack. These tactics had the potential to disrupt network functionality, manipulate routing tables, and exploit resources, ultimately compromising network integrity.

While conventional firewalls and packet filters control ports between network resources and the external environment, they fall short in detecting intrusion attempts. Effective network security demands mechanisms that deeply analyse transmitted data, beyond merely inspecting packet

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

headers. This necessitates the use of more advanced filtering and protection mechanisms.

This research delves into theoretical exploration, focusing on prominent types of IPv6 addresses and their applications. It also examines the automated configuration methods, both stateless and stateful, along with auxiliary protocols for IPv6, namely ICMPv6 and NDP protocols. On the practical front, the study involves implementing various attacks on operating systems and countering them within a local network environment. The study encompasses False Router Advertisement (FRA), Router Deletion Attack, NS Flood Attack, and ICMPv6 Smurf Attack. These attacks were executed using Scapy and analysed using the Wireshark software. This study contributes to a comprehensive understanding of IPv6 security enhancements and offers practical insights for bolstering defined mechanisms against such attacks.

We would like to note that this ongoing research project represents the first part of a series of studies that we will be conducting in the future.

The rest of this article is organized as follows: Section 2 related works, Section 3 presents network concepts (types of IPv6 addresses, ICMPv6, NDP, IPv6 attacks), Section 4 Experiments and Results, Section 5 Comparison with related works, Section 6 future works and Section 7 contains conclusions.

## II. RELATED WORK

As IPv6 adoption continues to expand, so does the need to secure this new protocol.

Targeting auxiliary IPv6 protocols such as ICMPv6 and NDP (Neighbour Discovery Protocol) is one of the most common and severe forms of IPv6 attacks. These protocols play a vital role in supporting network routing and registration processes. Therefore, protecting them is essential to ensuring the continuity of services and communications over IPv6.

In this context, classifying intrusion detection rules is essential for understanding how security and definitions against IPv6 attacks are implemented. These rules can be categorized into two main types: the first type is Rule-based attack detection, while the second type leverages artificial intelligence and machine learning to identify unknown and unexpected attack patterns.

### A. Rule-based attack detection

Al-Shareeda, Mahmood A., et al [1] proposed a rule-based detection method called SADetection for deployment in IPv6 link-local networks to identify SLAAC attacks. They emphasize that SADetection can identify both illegal Router Advertisement (RA) messages and concealed RA messages within packets that contain extension headers. The researchers have found that SADetection exhibits an impressive detection accuracy of 98%, providing effective protection for IPv6 link-local networks against SLAAC attacks.

Rehman, Shafiq Ul, and Selvakumar Manickam [7] presented mechanisms relying on rule-based approaches to detect Denial of Service (DoS) attacks that are based on the Duplicate Address Detection (DAD) process during the automatic configuration of addresses in local IPv6 networks. The focus of the researchers was limited to DoS attacks and did not include mention of other attack types based on the NDP and ICMPv6 protocols.

Bansal, Gunjan, et al [8] presented a new scheme for intrusion detection for NDP-based attacks (IPv6 NDP DoS Attacks), which combines the best of passive and active detection mechanisms. It appears that the research focuses on detecting attacks targeting the NDP (Neighbor Discovery Protocol) in IPv6 networks.

### B. AI-based attack detection

Saad, Redhwan MA, et al [2] presented the development and evaluation of the v6IIDS intelligent framework for detecting ICMPv6 DDoS attacks in IPv6 networks. This framework incorporates the use of machine learning techniques and artificial neural networks to analyze traffic patterns and identify unusual patterns, thereby enhancing the accuracy of attack detection. The researchers concluded that the results demonstrate the high effectiveness of the v6IIDS framework in safeguarding IPv6 networks and reducing the time required for detection and response. The researchers focused solely on the detection process without addressing the mitigation of attacks.

Saad, R. M., et al [3] presented a mechanism for detecting ICMPv6 flood attacks using DENFIS algorithms to detect Denial of Service (DoS) attacks in IPv6 networks. The researchers employed the Fuzzy Inference Classifier to identify DoS attacks based on ICMPv6 exploitation in IPv6 networks. They utilized a realistic network environment within a university lab. The researchers concluded that the Fuzzy Inference Classifier is capable of detecting attacks only.

Elejla, Omar E., et al [4] employed classification algorithms to construct an IDS system for detecting ICMPv6-based DDoS attacks. They explained that these algorithms are capable of detecting DDoS attacks, with varying levels of detection capability. However, the researchers emphasized that the results did not reach a level of reliability that qualifies for building the intended models in real-world scenarios. Therefore, there is a need to improve the classification algorithms or fine-tune the classifier parameters to achieve better results.

Shah, Syafiq Bin Ibrahim, et al [5] suggested a hybrid approach to entropy-based technology in conjunction with an adaptive threshold algorithm for detecting Denial of Service (DoS) router advertisement flooding attacks. Through dynamic threshold adaptation and the selection of the suitable entropy feature, the proposed technology is capable of detecting various DoS RA flooding attack scenarios. It is important to note that this approach is not designed to detect other types of attacks.

Elejla, O.E.; Anbar, M.; Hamouda, S.; Faisal, S.; Bahashwan, A.A.; Hasbullah, I.H [6] proposed a deep learning-based approach to detect DDoS attacks that flood IPv6 networks through the ICMPv6 protocol. They utilized two algorithms (IGR and chi-square) to select features and identify a set of features that aid in detecting ICMPv6 DDoS flood attacks. However, this approach was unable to detect attacks based on the NDP protocol or any other types of attacks.

Elejla, Omar E., et al [9] utilized feature-based classification to identify invasive Router Advertisement (RA) attacks aimed

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

at disrupting IPv6 networks. They introduced representative features derived from flow-based data representation, enabling effective RA flooding attack detection. The potential for further improvement exists through the inclusion of additional features or the selection of a subset of these features, all while avoiding detection by plagiarism detectors.

## III. NETWORKING CONCEPTS

### A. Types of IPv6 addresses

An IPv6 address is a 128-bit numerical label assigned to An IPv6 address is a 128-bit numerical label assigned to each device on an IPv6-enabled network. IPv6 addresses are used to identify and locate devices ipv6 in the network.

IPv6 addresses are organized into different types, each serving a specific purpose in network communication, Common Types of IPv6 Addresses:

1. Unicast Address:

Unicast addresses are used for one-to-one communication between devices on the network [13]. There are three types of unicast IPv6 addresses:

- Global Unicast Address: The global unicast address is similar to public IPv4 addresses. It is globally routable and uniquely identifies a device on the IPv6 Internet. Routers use global unicast addresses to forward data packets across different networks.
- Unique Local Address (ULA): The Unique Local Address is used for private communication within an organization or local network. It is akin to IPv4's private addresses (e.g., 192.168.x.x) and is not routable over the global Internet.
- Link-Local Address: The link-local address is automatically configured on every IPv6-enabled device when it joins a network segment. It is used for communication within the local network segment and does not extend beyond it.

2. Multicast Address:

Multicast addresses are utilized for one-to-many communication, allowing data to be sent to multiple devices simultaneously. In IPv6, multicast addresses start with the prefix "ff00::/8" [15]

3. Anycast Address:

Anycast addresses are assigned to multiple devices, but data sent to this address is routed to the nearest device in the anycast group based on network topology. Anycast is used to provide efficient and fault-tolerant services by directing traffic to the closest available server [14].

### B. Internet Control Message Protocol version 6 (ICMPv6):

ICMPv6 is an integral part of IPv6 and operates at the network layer of the OSI model. Just like ICMP in IPv4, ICMPv6 is used for various purposes, including network diagnostics, error reporting, and quality-of-service adjustments. It facilitates communication between IPv6 devices, enabling them to exchange control and error information efficiently [16].

Here's an overview of common ICMPv6 message types (see Table 1):

TABLE I. ICMPV6 MESSAGE TYPES.

| Message Type (Decimal) | Description and Purpose |
|---|---|
| 128 | Echo Request (Ping) - Network reachability testing |
| 129 | Echo Reply (Ping Response) |
| 133 | Router Solicitation - Inquiring about routers |
| 134 | Router Advertisement - Network configuration |
| 135 | Neighbour Solicitation - Discovering the neighbour's link-layer address |
| 136 | Neighbour Advertisement - Response to Neighbour Solicitation |
| 137 | Redirect Message - Informing hosts of a better next-hop |

### C. Network Discovery Protocol (NDP)

Network Discovery Protocol (NDP) in IPv6 is a fundamental protocol that plays a crucial role in the neighbour discovery, address resolution, and router discovery within an IPv6 network. NDP replaces the functions of Address Resolution Protocol (ARP) used in IPv4 networks [12].

- NDP's Role in the OSI Model Link Layer

Neighbour Discovery: Devices on an IPv6 network use NDP to discover neighbouring devices and their link-layer addresses. This process is essential for efficient communication between devices on the same network segment.

- Address Resolution: NDP allows devices to resolve the Layer 3 IPv6 addresses to their corresponding Layer 2 link-layer addresses (such as MAC addresses) used for data link transmission.
- Router Discovery: NDP enables hosts to discover and learn the presence of routers on the network, providing them with essential information for proper packet forwarding and default gateway selection.

1. Duplicate Address Detection (DAD): When a device joins an IPv6 network or configures a new IPv6 address, NDP ensures the uniqueness of the address by performing DAD, which checks if another device on the same link is already using the same address.

2. Redirect: Routers can send ICMPv6 Redirect messages to inform hosts about a better next-hop for a particular destination.

- NDP uses several ICMPv6 (Internet Control Message Protocol for IPv6) messages to perform its functions. Critical Role of ICMPv6 Messages in Network Operations:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

1. Router Solicitation (RS) Message: Hosts use the Router Solicitation message to discover routers on the network. When a device joins an IPv6 network or when it needs to refresh its router information, it sends an RS message to the all-routers multicast address.
2. Router Advertisement (RA) Message: Routers periodically send Router Advertisement messages to the all-node multicast address. These messages inform hosts about the presence of the router, the network's default router, and various network parameters such as the network prefix and hop limit.
3. Neighbour Solicitation (NS) Message: Devices use Neighbour Solicitation messages to determine the link-layer address of a neighbour, such as a neighbouring host or router. When a device wants to send data to another device but lacks the link-layer address, it sends an NS message to the target device's solicited-node multicast address.
4. Neighbour Advertisement (NA) Message: In response to an NS message, the target device sends a Neighbour Advertisement message, providing its link-layer address. This message helps the sender complete the address resolution process.
5. Redirect Message: Routers can send Redirect messages to inform hosts about a better next-hop for a specific destination. This helps optimize the packet forwarding process.

C. IPV6 Attacks

As the world shifts towards adopting IPv6 (Internet Protocol version 6) to accommodate the exponential growth of connected devices, network administrators must be vigilant against potential security threats. Attackers have honed their techniques to exploit IPv6 vulnerabilities, posing risks to network integrity and user data [17]. We explore different types of IPv6 attacks:

1) False Router Advertisement (FRA):

The IPv6 False Router Advertisement Attack manipulates the Neighbour Discovery Protocol (NDP) mechanism, exploiting vulnerabilities in router advertisement processing. Attackers send deceptive Router Advertisement (RA) messages that falsely claim to be legitimate routers within the network. These malicious RAs may be introduced through various means, including rogue devices, NDP spoofing, or exploiting weak authentication mechanisms [18].

- Consequences of the Attack:

1. Traffic Diversion: Fraudulent RAs can misdirect network traffic through unauthorized routes under the attacker's control. This enables attackers to intercept sensitive data or conduct Man-in-the-Middle (MITM) attacks, compromising data confidentiality and integrity.
2. Denial of Service (DoS): By sending a flood of false RAs, attackers can overwhelm devices, leading to network congestion and service unavailability for legitimate users.
3. Rogue Router Inclusion: Attackers can inject rogue router entries into the network's routing table, causing devices to use unauthorized routers for communication. This opens the door for further exploitation and unauthorized access.
4. Network Disruption: Acceptance of fraudulent RAs by devices can result in incorrect routing information, leading to network instability and communication disruptions.

2) Router Deletion Attack:

Before delving into the attack, let's briefly recap the IPv6 Router Advertisement (RA) process. RAs are ICMPv6 messages sent periodically by routers to announce their presence and network configuration details to neighbouring devices. Hosts on the network use RAs to auto-configure their IPv6 addresses and discover the default gateway.

The IPv6 Router Deletion Attack aims to disrupt the RA process by maliciously manipulating or suppressing legitimate RA messages [19]. This attack typically involves two main techniques:

- Main Techniques in This Attack Typically Involve:

*1)* RA Spoofing:

In this technique, attackers send forged RA messages, impersonating legitimate routers on the network. The forged RAs may contain incorrect information, such as an invalid or unreachable default gateway. As a result, hosts may update their routing tables, leading to traffic being redirected to unintended destinations or a complete loss of connectivity.

*2)* RA Suppression:

In this method, attackers intentionally suppress or block legitimate RAs from reaching hosts. By doing so, the hosts may lose their default gateway information and become isolated from the network, leading to service disruptions and potentially compromising critical communications.

- Consequences of the Attack:

The IPv6 Router Deletion Attack can have severe consequences for network operations:

*a.* Denial of Service (DoS): The attack can cause service disruptions, preventing hosts from accessing network resources and the Internet.

*b.* Man-in-the-Middle (MITM) Attacks: With legitimate routers removed from the network, attackers can impersonate routers and intercept network traffic, leading to potential data theft or tampering.

*c.* Traffic Diversion: By manipulating routing information, attackers can redirect network traffic to their malicious devices, allowing them to eavesdrop or carry out further attacks.

3) NS Flood Attack:

The IPv6 NS Flood Attack is a Distributed Denial of Service (DDoS) attack that targets the Neighbour Discovery Protocol (NDP), a critical component of IPv6 networks. NDP facilitates neighbour discovery, address resolution, and router discovery processes, making it an attractive target for malicious actors [20].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

In this attack, the attacker floods the network with a massive number of fake Neighbour Solicitation (NS) messages. These NS messages are multicast to the solicited-node multicast address of different devices on the network. By impersonating multiple devices and saturating the network with NS messages, the attacker aims to exhaust network resources and overwhelm devices' processing capabilities.

- Consequences of an IPv6 NS Flood Attack:

1. Resource Exhaustion: The flood of NS messages consumes network resources, such as bandwidth and processing power, causing slowdowns and service disruptions.
2. Service Disruption: Legitimate devices struggle to handle the excessive NS messages, leading to a significant degradation in service performance or even complete service unavailability.
3. Network Congestion: The sheer volume of NS messages congests the network, hindering normal traffic flow and leading to communication delays.
4. Denial of Service (DoS): The attack ultimately results in a denial of service for legitimate users, rendering the network inaccessible or severely limited in functionality communication.

4) ICMPv6 Smurf Attack:

The ICMPv6 Smurf attack is a network-based denial-of-service (DoS) attack that targets IPv6 networks. It is a variant of the traditional IPv4 Smurf attack but adapted to exploit vulnerabilities in the ICMPv6 protocol. We will explore the ICMPv6 Smurf attack, its working mechanism, and potential consequences [21].

- How the ICMPv6 Smurf Attack Works:

The ICMPv6 Smurf attack leverages ICMPv6 Echo Request (Ping) packets to launch a large-scale distributed attack. The attacker sends a flood of ICMPv6 Echo Requests to the IPv6 all-nodes multicast address. These packets are intended to be processed by all nodes on the network, causing them to reply with ICMPv6 Echo Reply packets to the spoofed source address. However, in the ICMPv6 Smurf attack, the source address is manipulated to be the target victim's address. Consequently, all nodes on the network flood the victim with ICMPv6 Echo Reply packets, overwhelming its resources and causing a denial-of-service condition

- Consequences of an ICMPv6 Smurf Attack:

The ICMPv6 Smurf attack can have severe consequences for the targeted victim and the entire network:

1. Network Congestion: The excessive ICMPv6 traffic generated by the attack saturates the victim's network bandwidth, causing network congestion and disrupting legitimate communication.
2. Resource Exhaustion: The victim’s performance.
3. Service Disruption: The sustained attack can lead to a complete service disruption for the victim, rendering its services inaccessible to legitimate users.

## IV. EXPERIMENTS AND RESULTS

A local network was designed, comprising a diverse set of operating systems including Windows and Linux, utilizing the Virtual Box software. All systems within the local network operate according to the sixth version of the Internet protocol, IPv6,(seeTable2).

Attacks were constructed and executed within the local network to target specific operating systems. This was achieved by aiming at their respective IPv6 addresses or targeting a group of systems using the Multicast broadcast address. Python 3.6 and Scapy 2.3.2 were employed for this purpose, along with the THC-IPv6 tool. Finally, the attack packets and exchanged messages were analysed using Wireshark 3.4.3.

Table 2: Used operating systems and IPv6 addresses.

| *The device's role in the tested network* | *Operating System* | *IPv6* |
|---|---|---|
| Attacker | Kali Linux | Fe80::a00:36ff:fbfb:a54 |
| Victim | Windows 7 | Fe80::acd6:6b51:3647:9724 |
| Victim | Windows 10 | Fe80::91c8:6406:16f7:a366 |
| Victim | Linux kali | fe80::a00:29fe:55fe:ff75 |
| Victim | Ubuntu Linux | Fe80::a00:56ed:ff47:e520 |
| Victim | Kali Linux (for Smurf Attack) | Fe80::6bb6:79c6:ac16:d3f6 |
| Default Active Router | | Fe80::5054:ff:fe12:3500 |

The following attacks (see Table 3) were executed, the results were analyzed, and measures were taken to counter them.

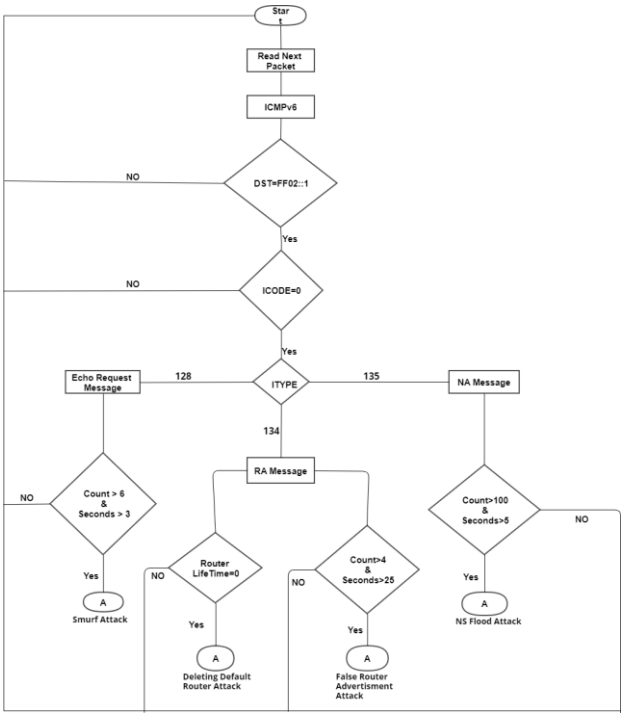
Table 3: Attacks that were used in the testbed.

| SN | Attack name |
|---|---|
| 1 | False Router Advertisement Attack |
| 2 | IPv6 Router Deletion Attack |
| 3 | NS Flood Attack |
| 4 | ICMPv6 Smurf Attack |

The following figure (See Figure 1) illustrates the attack detection diagram.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

Figure 1: The diagram for the proposed attack detection schema.




A. False Router Advertisement Attack

This type of attack follows the form of a Man-in-the-Middle (MITM) attack. In this scenario, the compromised device sends a falsified message to advertise a rogue Router Advertisement (RA). This enables the attacker to announce a counterfeit prefix and define other gateways within the network. Additionally, it allows the attacker to eavesdrop on the exchanged information between users on the network.

This attack was executed, and the false prefix (2020:bad0::) was announced using both Scapy, (see Figure 2) and THC-IPv6, (see Figure 3) against various operating systems that comprise the testbed network.

```
>>> packet_ipv6_specification=IPv6(dst="ff02::1")
>>> Router_Advertisement=ICMPv6ND_RA(chlim=255, prf=1)
>>> Source_local_address=ICMPv6NDOptSrcLLAddr(lladdr="08:00:27:fb:0a:54")
>>> optmtu=ICMPv6NDOptMTU(mtu=1200)
>>> prefix=ICMPv6NDOptPrefixInfo(prefixlen=64, prefix="2020:bad0::")
>>> prefix_of_new_router=ICMPv6NDOptNewRtrPrefix(prefix="fe80::a00:27ff:fefb:a54")
>>> bogus_router_packet=(packet_ipv6_specification/Router_Advertisement/Source_local_
address/prefix/prefix_of_new_router)
>>> send(bogus_router_packet, count=1000, loop=1, inter=6)
.....
```

Figure 2: Executing the False Router Advertisement Attack Using Scapy.

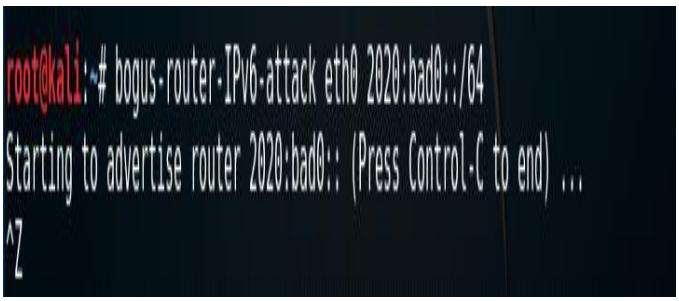



Figure 3: Executing the False Router Advertisement Attack Using THC-IPv6.

The following table (see Table 4) illustrates the key data related to the execution of the attack.

Table *4*: Simulation data in the False Router Advertisement Attack.

| *Simulation Duration* | *Iterations* | *Data Size* |
|---|---|---|
| 100s | 21 | 4.494 KB |

The following figure, (see Figure 4) illustrates the utilized throughput in simulating this attack, where each spiked pulse represents an attack packet. The total count of these in this testbed is 21 Router Advertisement (RA) directed attack packets.

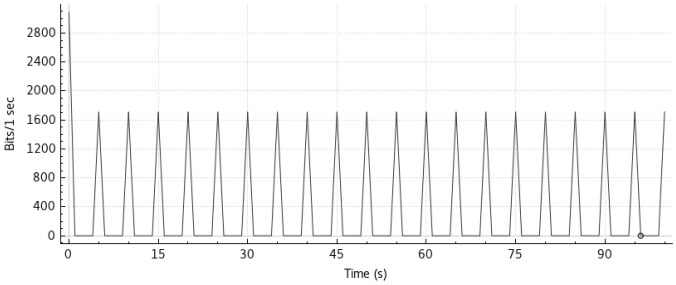



Figure 4: The modified throughput used in the false router advertisement.

The following figure, (see Figure 5) illustrates the impact of the False Router Advertisement Attack on routing paths in the Windows 10 operating system.

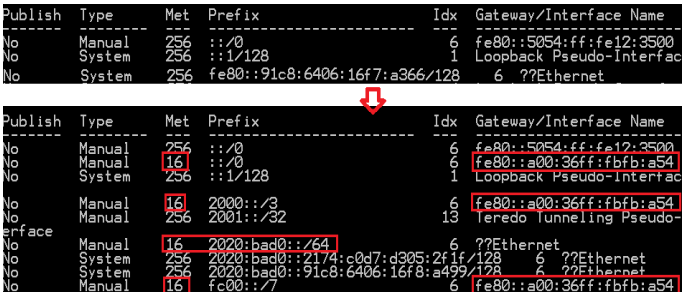



Figure 5: The Impact of the Attack on Routing Paths in the Windows 10 Operating System.

The following figure, (see Figure 6) illustrates the impact of the False Router Advertisement Attack on routing paths in the Windows 7 operating system.

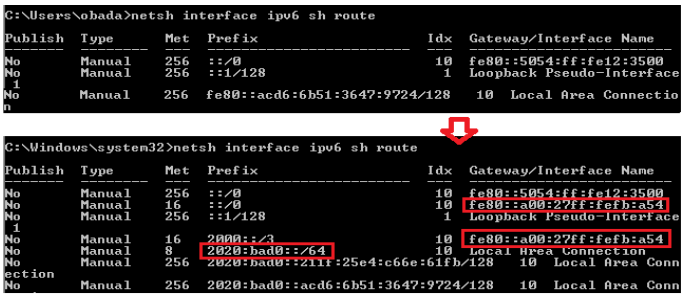



Figure 6: The Impact of the Attack on Routing Paths in the Windows 7 Operating System.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

The address ::/0 refers to the default route address of the network and the prefix 2000::/3 points to global unicast addresses. After executing this type of attack on tested modern Windows operating systems, we deduce that the attacker's device address (Fe80::a00:36ff:fbfb:a54) is adopted as the new gateway for the network. Additionally, the forged prefix (2020:bad0::/64) is used in the local network with higher priority. Priority increases as the value of the parameter (Metric), representing the cost of this route according to the routing algorithm used, decreases.

The following figure, (see Figure 7) illustrates the impact of the False Router Advertisement Attack on routing paths in the Kali Linux operating system.

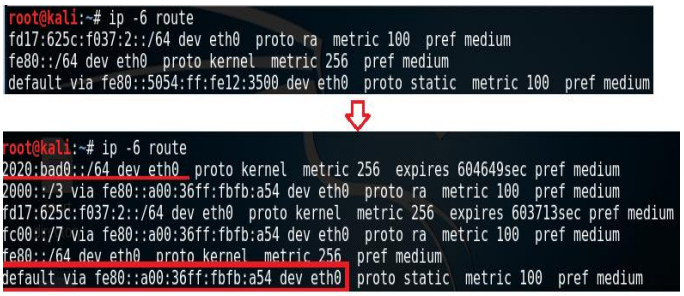



Figure 7: The Impact of the Attack on Routing Paths in the Kali Linux Operating System.

We found that the correct addresses did not appear at all in the routing paths within the Kali Linux operating system after executing this attack. Additionally, we infer that this system utilizes the false prefix and the attacker's address as a virtual gateway, but with medium priority. The following figure, (see Figure 8) illustrates the impact of the False Router Advertisement Attack on routing paths in the Ubuntu Linux operating system.

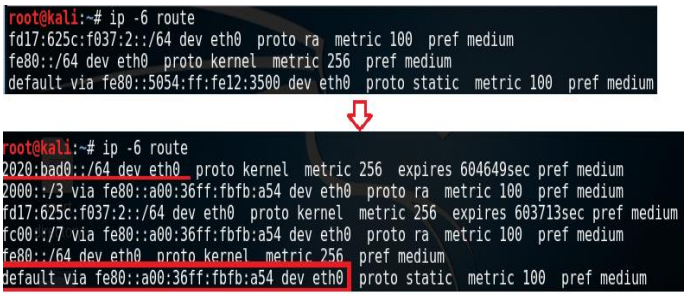



Figure 8: The Impact of the Attack on Routing Paths in the Ubuntu Linux Operating System.

This attack on the Ubuntu Linux system results in the utilization of a forged prefix address, and the adoption of the attacker's device address as a virtual gateway with a similar priority to the genuine router address. However, this is done with a higher Router Lifetime and a larger hop limit value. Using a higher Router Lifetime value along with the continuous and frequent transmission of forged Router Advertisement (RA) packets will lead to the utilization of the attacker's device address as a virtual gateway once the valid RA packets' lifetime expires.

Upon analyzing the packets of the sent router advertisement, (see Figure 9) we discover that the attacker has proclaimed his address as a virtual router address, along with a fabricated prefix, all with a high priority.

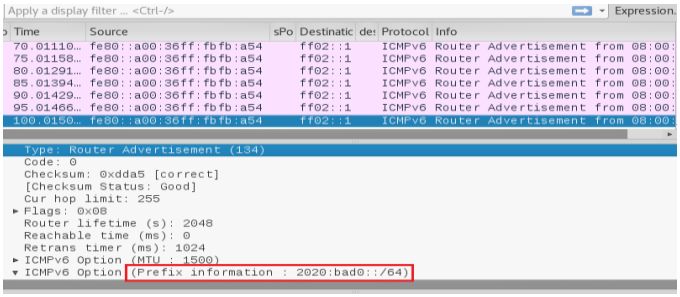



Figure 9: Analysis of Sent RA Packets in the False Router Advertisement Attack.

The data appears in the form of hexadecimal bytes, where we find the Type field, followed by the Code field, and then the Checksum field. Following these, the data continues with the field indicating the hop count value, which is represented here by the byte with a value of 'ff,' corresponding to 255 in decimal format. Then, the byte '08' corresponds to the maximum priority for the router. The following figure, (see Figure 10) illustrates the details of the sent router advertisement packets.

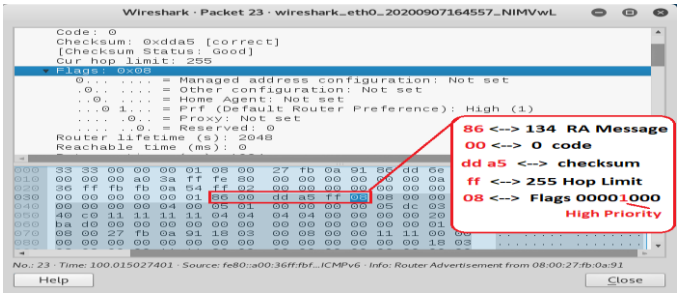



Figure 10: Details of the Router Advertisement Packet Sent in the False Router Advertisement Attack.

The default time interval between periodic Advertisement messages ranges from 200 to 600 seconds according to RFC 4861 [22]. These Advertisement messages are formed either in response to received Neighbour Solicitation messages from a device or periodically directed towards the FF02::1 address in the network's normal state. The priority of these packets is also set by default to the medium value "00" and according to the value 64 for the Hop Limit field.

What distinguishes these attacks is the utmost priority given to Router Advertisement (RA) messages, aimed at overriding other routers. This is achieved by using the maximum value for the Hop Limit field to ensure the continued use of transmitted packets as they traverse the network. Additionally, the attacker seeks to maintain a very close time interval for continuous self-advertisement. Hence, this rule, (see Figure 11) has been added to detect this type of attack.

```
alert icmp any any -> FF02::1 any (itype:134; icode:0; msg:"Bogus router attack
detection"; content:"|ff 08|"; offset:0; depth:2; detection_filter:track by_dst, count
4, seconds 25; classtype:bogus router attack; priority:1; sid:1000007; rev:1;)
```

Figure 11: Detection rule for False Router Advertisement Attack.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

To detect a large number of Router Advertisement (RA) messages sent at close time intervals (4 targeted advertisement packets every 25 seconds) that violate recommended values, a detection filter was employed. This filter tracks incoming messages toward the same destination. Content detection options were added to unveil the maximum priority of the router and the maximum value of the hop count used by the attacker in these messages.

The value 0 in the offset field indicates that content search should begin at the payload data's start. Meanwhile, the value 2 in the depth option indicates that content search should extend by 2 bytes. This rule is specific to ICMPv6 messages returning from all ports and addresses toward the FF02::1 address.

Furthermore, the value 134 in the type field is used to indicate RA messages, along with the value 0 in the code field. The detection system triggers an alert upon matching the packets causing the attack, (see Figure 12).

```
09/18-18:06:48.208906  [**] [1:1000007:1] Bogus router attack detection [**] [Classification: Denial of
Service attack (MITM type) detection] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:fefb:a54' -> ff02::1
09/18-18:06:53.209625  [**] [1:1000007:1] Bogus router attack detection [**] [Classification: Denial of
Service attack (MITM type) detection] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:fefb:a54' -> ff02::1
09/18-18:06:58.210135  [**] [1:1000007:1] Bogus router attack detection [**] [Classification: Denial of
Service attack (MITM type) detection] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:fefb:a54' -> ff02::1
09/18-18:07:03.211143  [**] [1:1000007:1] Bogus router attack detection [**] [Classification: Denial of
Service attack (MITM type) detection] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:fefb:a54' -> ff02::1
09/18-18:07:08.211324  [**] [1:1000007:1] Bogus router attack detection [**] [Classification: Denial of
Service attack (MITM type) detection] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:fefb:a54' -> ff02::1
09/18-18:07:13.211983  [**] [1:1000007:1] Bogus router attack detection [**] [Classification: Denial of
Service attack (MITM type) detection] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:feft:a54' -> ff02::1
09/18-18:07:18.212454  [**] [1:1000007:1] Bogus router attack detection [**] [Classification: Denial of
Service attack (MITM type) detection] [Priority: 1] {IPV6-ICMP} fe80::a00:27ff:feft:a54' -> ff02::1
```

Figure 12: Alert messages resulting from detecting a False Router Advertisement Attack.

Similarly, a similar rule has been added that employs a drop action instead of an alert action for discarding non-compliant packets. This allows for filtering matching packets and halting the attack after 25 seconds of its initiation, which is the threshold after which the proposed system begins to block packets causing the attack. The genuine router, which is announced, is then reused based on the correct adjacency announcement packets that are sent at regular intervals.

## B. IPv6 Router Deletion Attack

The attacker sends a targeted false advertisement message, where the source address is the default gateway's address with a zero lifetime, aiming to remove it from the router list in the network. (see Figures 13&14).

```
>>> ipv6_packet_specification=IPv6(src="fe80::5054:ff:fe12:3500",dst="ff02::1")
>>> router_advertisement_message=ICMPv6ND_RA(prf=1, routerlifetime=0, reachable
time=0, retranstimer=0)
>>> local_address=ICMPv6NDOptSrcLLAddr(lladdr="52:54:00:12:35:00")
>>> packet_of_the_attack=ipv6_packet_specification/router_advertisement_message
/local_address
>>> send(packet_of_the_attack)
.
Sent 1 packets.
```

Figure 13: Executing the Effective Router Deletion Attack Using Scapy.

```
root@kali:~# removing-ipv6-real-router eth0 '*'
Starting to sending router kill entries for * (Press Control-C to end) ...
Sent RA kill packet for fe80::5054:ff:fe12:3500
Sent RA kill packet for fe80::5054:ff:fe12:3500
^Z
```

Figure 14: Executing the Effective Router Deletion Attack Using TCH-IPv6.

The simulation mechanisms data implemented in this attack's scenario, (see Table 5).

Table 5: Simulation data in the Router Deletion Attack.

| *Simulation Duration* | *Iterations* | *Data Size* |
|---|---|---|
| 207s | 2 | 18.931 KB |

The following figure, (see Figure 15) illustrates the throughput modifier used in simulating this attack, depicting the two attack packets representing false router advertisement messages that lead to the effective router deletion.

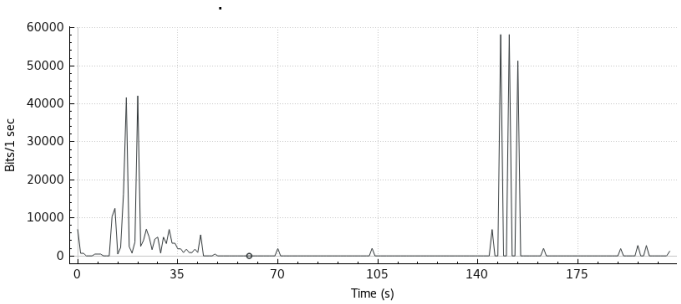



Figure 15: The throughput utilized in the Router Deletion Attack.

The impact of the attack used in various operating systems is evident in the following figures. Windows 10, (see Figure 16), Windows 7, (see Figure 17), Kali Linux, (see Figure 18), and Ubuntu Linux, (see Figure 19).

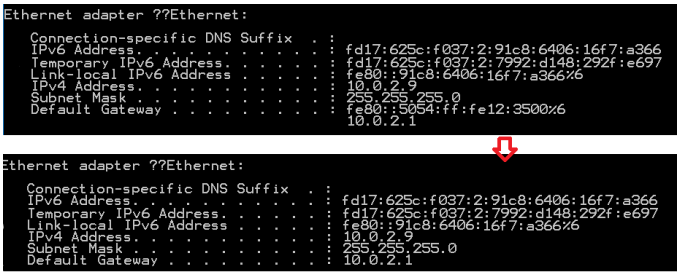



Figure 16: Disabling the Active Router in Windows 10.

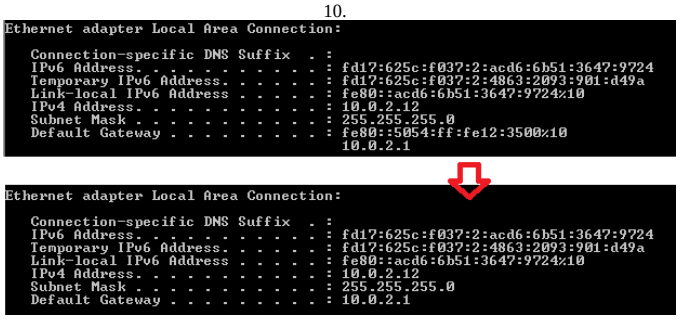
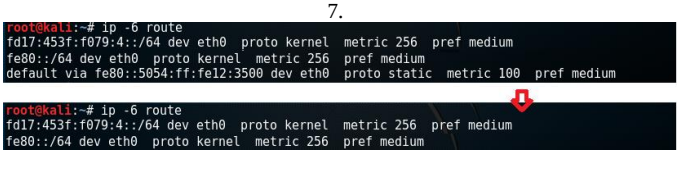



Figure 17: Disabling the Active Router in Windows 7.



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

the exchanged packets over the network, (see figure 20) reveals the attacker sending a directed false advertisement message originating from the default gateway's address – after monitoring this address for its usage - with a high priority and a time-to-live of zero, aiming to delete it from the routing tables employed in this network.

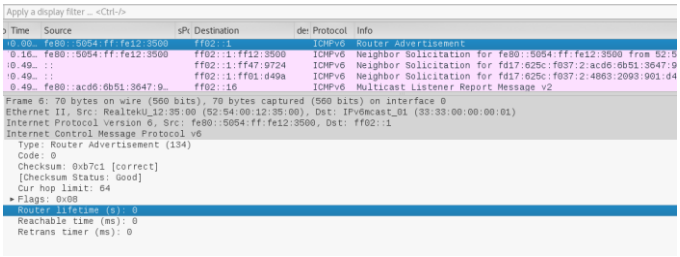



Figure 20: Analysis of False Router Advertisement Packets Used in the Router Deletion Attack.

The following figure, (see Figure 21) illustrates the details of a Router Advertisement message packet's data in hexadecimal byte format. The bytes designated for the Type, Code, and Checksum fields are sequentially displayed, followed by the Hop Limit field and the Flags field, with a value of 08, corresponding to the maximum priority designation of the announcing router in this packet. Subsequently, there is a zeroed Lifetime field of 2 bytes in size (00 00).

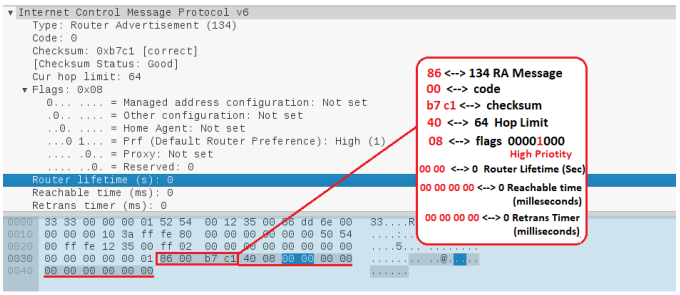



Figure 21: Details of the Router Advertisement (RA) Packet in the Router Deletion Attack.

A new rule has been added that pertains to Router Advertisement (RA) messages in the ICMPv6 protocol, (see Figure 22) with different source and destination ports in the direction of the FF02::1 address. Detection is accomplished by matching both the contents of the flag fields and the lifetime time which consists of 3 bytes in hexadecimal format. The option offset:1 indicates that the search process should begin after 1 byte from the start of the payload data, while the option depth:3 signifies that the content search process should extend over a length of 3 bytes. This is imperative due to the necessity of not utilizing high-priority values in RA packets when the advertised lifetime value is zero. It must strictly adhere to the medium value (00), as specified in the document (RFC 4191) [23]. This is based on changes in the format of Router Advertisement message announcements outlined in documents (RFC 2461) [24] and (RFC 3775) [25].

```
alert icmp any any -> any any (itype:134; icode:0; msg:"deleting default router atttack
detection"; content:"|08 00 00 00 00 00 00 00 00 00 00 00|"; offset:1; depth:11;
classtype:deleting default router attack; priority:1; sid:1000019; rev:1;)
```

Figure 22: Effective Router Deletion Attack Detection Rule.

The detection results of these packets appear in the following figure, (see figure 23).

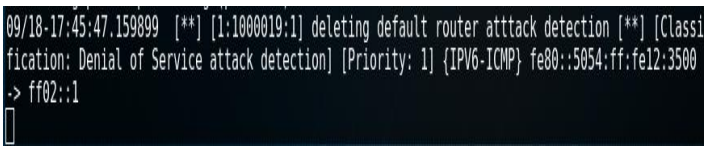



Figure 23: The alert triggered upon detecting an active Router Deletion Attack.

To prevent the execution of this attack, another rule has been added that mirrors the previous one but with a "drop" action for non-compliant router advertisement packets. These packets have a zero lifetime and are assigned the highest priority of virtual router addresses, instead of merely being deleted.

## C. NS Flood Attack

The attack was executed using THC-IPv6 tools over the eth0 interface, (see figure 24). On the test network, encompassing various operating systems.

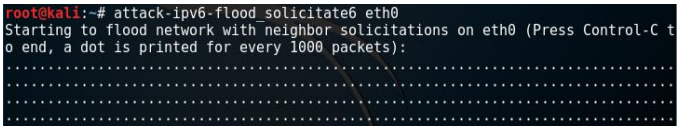



Figure 24: Executing the NS Flooding Attack Using THC-IPv6.

The simulation process parameters utilized in executing the attack are presented in the following table, (see Table 6) encompassing the attack duration, number of packet repetitions, and the size of the utilized data.

Table 6: Simulation data in the NS Flooding Attack.

| *Simulation Duration* | *Iterations* | *Data Size* |
|---|---|---|
| 74s | 463586 | 18.931 KB |

(See Figure 25) illustrates the throughput modifier used in simulating this attack

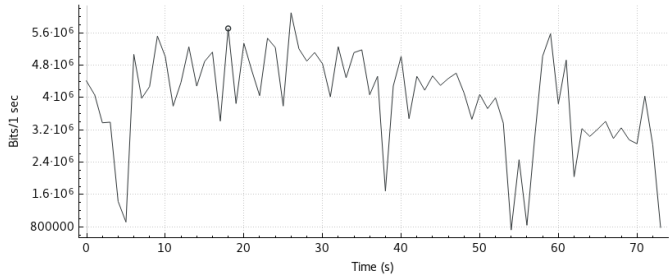



Figure 25: The transmission rate in the NS Flood Attack.

The following figure, (see Figure 26) illustrates the impact of the NS Flood Attack on Windows 7, Windows 10, Kali Linux, and Ubuntu Linux operating systems.

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

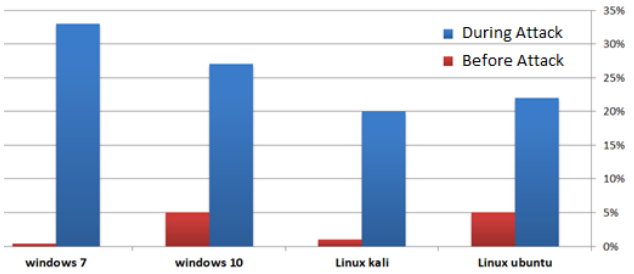



Figure 26: The impact of the NS flood attack on CPU utilization.

We find that the impact of this attack on tested Windows systems is greater than that on Linux systems and that updating Windows systems contributed to mitigating CPU consumption during the attack execution. To comprehend the mechanism of the attack-causing packets, the transmitted packets were analyzed using Wireshark software (see Figure 27). A significant number of Neighbor Solicitation (NS) advertisement messages appear, utilizing random source addresses.

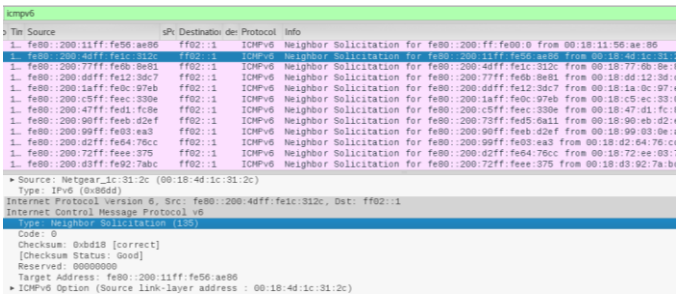


Figure 27: Analysing Sent Neighbour Solicitation Packets.

To detect these attacks, a rule has been added to the proposed system that deals with Internet Control Messages arriving from all addresses and ports to the multicast address of the group of host devices on the network (FF02::1) across all ports. (See Figure 28), this is done while specifying values for the type and code fields specific to Neighbour Solicitation (NS) messages. Additionally, a detection filter has been employed to track this pattern of messages, based on an experimentally determined threshold of 100 messages every 5 seconds.

```
alert icmp any any -> any ff02::1 (msg:"ICMPv6/NS flooding"; itype:135; icode:0; detection_filter:track by_dst,
count 100, seconds 5; classtype:ICMPv6 Flooding Attack/Neighbor Solicitation; priority:1; sid:1000001; rev:1;)
```

Figure 28: Flood Attack Detection Rule Utilizing NS Messages.

(See Figure 29) depicts the result of detecting this attack through the initiation of alert messages by the proposed system.

```
09/21-19:22:08.380178  [**] [1:1000001:1] ICMPv6/NS flooding [**] [Classification: Denial
of Service attack detection] [Priority: 1] {IPV6-ICMP} fe80::200:45ff:fe99:d3c7 -> ff02::1
09/21-19:22:08.380180  [**] [1:1000001:1] ICMPv6/NS flooding [**] [Classification: Denial
of Service attack detection] [Priority: 1] {IPV6-ICMP} fe80::200:57ff:feb6:d113 -> ff02::1
09/21-19:22:08.380181  [**] [1:1000001:1] ICMPv6/NS flooding [**] [Classification: Denial
of Service attack detection] [Priority: 1] {IPV6-ICMP} fe80::200:a9ff:fe09:90f9 -> ff02::1
09/21-19:22:08.380183  [**] [1:1000001:1] ICMPv6/NS flooding [**] [Classification: Denial
of Service attack detection] [Priority: 1] {IPV6-ICMP} fe80::200:ebff:fe20:328c -> ff02::1
09/21-19:22:08.380184  [**] [1:1000001:1] ICMPv6/NS flooding [**] [Classification: Denial
of Service attack detection] [Priority: 1] {IPV6-ICMP} fe80::200:6fff:fe9c:3af4 -> ff02::1
09/21-19:22:08.380186  [**] [1:1000001:1] ICMPv6/NS flooding [**] [Classification: Denial
of Service attack detection] [Priority: 1] {IPV6-ICMP} fe80::200:d6ff:fe90:b885 -> ff02::1
09/21-19:22:08.380188  [**] [1:1000001:1] ICMPv6/NS flooding [**] [Classification: Denial
of Service attack detection] [Priority: 1] {IPV6-ICMP} fe80::200:e4ff:fe98:2b65 -> ff02::1
```

Figure 29: Alert messages resulting from detecting a flood attack via NS messages.

To mitigate the impact of this attack on the targeted device, another rule similar to the previous one was added, replacing the alert action with a drop action to discard the packets causing the attack. The drop action was applied at the 52nd second after the attack execution started, (see Figure 30).

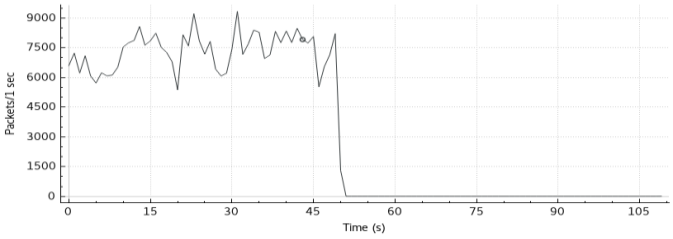



Figure 30: Neutralizing the impact of incoming Neighbour Solicitation (NS) attack packets on the targeted device.

## D. ICMPv6 Smurf Attack

This is one type of Distributed Denial of Service (DDoS) attack where an attempt is made to utilize network devices to execute the attack. This involves sending a large number of these messages, causing the Echo Reply messages issued by the network devices to be directed toward the targeted device to exhaust its processing units.

In this attack, the address of the targeted device is used as the source address for the Echo Request messages in ICMPv6. The multicast address FF02::1, which refers to the group of all hosts on the local network, is used as the destination address.

This attack was executed against the Linux Kali operating system, where its address (fe80::a00:29fe:55fe:ff75) is utilized to send the attack packets, using the THC-IPv6 tool (see Figure 31), using Scapy (see Figure 32).

```
root@kali:~# ipv6-smurf-attack-using-dst-multicast-address eth0 fe80::a00:29fe:55fe:ff75
Warning: unprefered IPv6 address had to be selected
Starting smurf6 attack against fe80::a00:29fe:55fe:ff75 (Press Control-C to end) ...
^Z
```

Figure 31: Executing the ICMPv6 Smurf Attack Using THC-IPv6.

```
>>> IPv6(src="fe80::a00:29fe:55fe:ff75", dst="ff02::1")
<IPv6  src=fe80::a00:29fe:55fe:ff75 dst=ff02::1 |>
>>> fakedpacket=(IPv6(src="fe80::a00:29fe:55fe:ff75", dst="ff02::1"))/ICMPv6EchoRequest()
>>> send(fakedpacket, inter=0.00000001, count=80000000000000)
```

Figure 32: Executing the ICMPv6 Smurf Attack Using Scapy.

The simulation process parameters utilized in executing the attack are presented in the following table, (see Table 7) encompassing the attack duration, number of packet repetitions, and the size of the utilized data.

Table 7: Simulation data in the ICMPv6 Smurf Attack.

| *Simulation Duration* | *Iterations* | *Data Size* |
|---|---|---|
| 212.3s | 1.084.464 | 74.011 MB |

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

(See Figure 33) illustrates the transfer throughput used in simulating this attack.

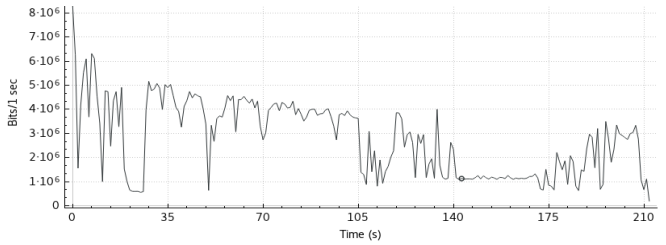



Figure 33: The transmission rate in the ICMPv6 Smurf Attack.

The transmitted and received packets between the targeted device and the rest of the tested network devices were analysed, (see Figure 34).

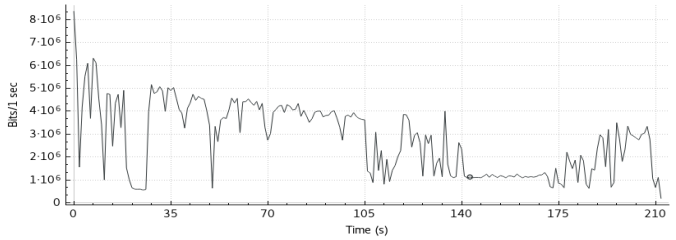



Figure 34: The transmission rate in the ICMPv6 Smurf Attack.

From the source addresses of these packets, we can infer that some operating systems nominate the incoming Neighbour Solicitation messages towards the address FF02::1 but do not direct the response messages towards the targeted device (fe80::a00:29fe:55fe:ff75), which are Windows systems. On the other hand, other systems participate in executing the attack, as is the case with the tested Linux systems, (see Table 8).

Table 8: Operating Systems Responding.

| *Operating System* | *Kali Linux* | *Ubuntu Linux* | *Windows 7* | *Windows 10* |
|---|---|---|---|---|
| *IPv6 Address* | Fe80::6bb6:79c6:ac16:d3f6 | Fe80::a00:56ed:ff47:e520 | Fe80::acd6:6b51:3647:9724 | Fe80::91c8:6406:16f7:a366 |
| *Filtering Attack Packets* | No | No | Yes | Yes |

The following rule has been added to the proposed detection system to identify this type of attack, (see Figure 35).

```
alert icmp any any -> FF02::1 any (itype:128; icode:0; msg:"Fake Echo Request using IPv6 multicast
destination FF02::1"; detection_filter:track by_dst, count 6, seconds 3; classtype:IPv6-Smurf
attack; priority:1; sid:1000012; rev:1;)
```

Figure 35: Detection Rule for attack that uses Multicast Address as the Destination Address for Request Messages.

This rule specializes in displaying alert messages for detecting ICMPv6 control protocol messages that originate from all addresses and ports towards the multicast destination address FF02::1. The value 128 in the type field (itype) indicates request messages in ICMPv6 while specifying the value 0 in the code field (icode).

A detection filter is used that relies on tracking incoming messages to the same destination address (Track by destination) based on an experimentally determined threshold of 6 packets every 3 seconds. Additionally, an appropriate classification is added for the attack type (IPv6-Smurf Attack) and it is marked with high importance (Priority: 1). (See Figure 36) illustrates the alert that appears when this attack pattern is detected.

```
04/24-17:28:35.229698  [**] [1:1000012:1] Fake Echo Request using IPv6 multicast dest
ination FF02::1 [**] [Classification: DoS attack detection] [Priority: 1] {IPV6-ICMP}
 fe80::a00:29fe:ff75 -> ff02::1
04/24-17:28:35.229701  [**] [1:1000012:1] Fake Echo Request using IPv6 multicast dest
ination FF02::1 [**] [Classification: DoS attack detection] [Priority: 1] {IPV6-ICMP}
 fe80::a00:29fe:ff75 -> ff02::1
04/24-17:28:35.229705  [**] [1:1000012:1] Fake Echo Request using IPv6 multicast dest
ination FF02::1 [**] [Classification: DoS attack detection] [Priority: 1] {IPV6-ICMP}
 fe80::a00:29fe:ff75 -> ff02::1
04/24-17:28:35.229709  [**] [1:1000012:1] Fake Echo Request using IPv6 multicast dest
ination FF02::1 [**] [Classification: DoS attack detection] [Priority: 1] {IPV6-ICMP}
 fe80::a00:29fe:ff75 -> ff02::1
```

Figure 36: Alert messages that appear when an IPv6-Smurf attack is detected.

To mitigate the impact of this type of attack on the targeted devices, a rule similar to the previous one has been added, but with the use of the "drop" action instead of "alert." The result of applying these rules appears as follows at the second 37 since the start of the attack execution, (See Figure 37), where the process of filtering the attack-causing packets begins.

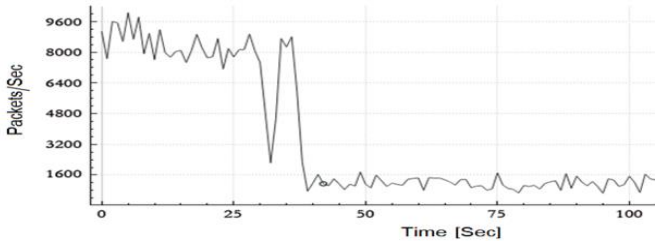



Figure 37: Delete IPv6-Smurf attack packets using filtering rules.

Table 9: Summary of the Impact of Attacks on Operating Systems.

| *Operating System* | *IPv6 Address* | *Attack Name* | *Attack Packet Filtering by default* | *Filtering Attack Packets by a rule* |
|---|---|---|---|---|
| *Kali Linux* | Fe80::6bb6:79c6:ac16:d3f6 | False Router Advertisement Attack | No | Yes-100% |
| | | IPv6 Router Deletion Attack | No | Yes-100% |
| | | NS Flood Attack | No | Yes-92% |
| | | ICMPv6 Smurf Attack | No | Yes-100% |

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

| | | | | |
|---|---|---|---|---|
| **Ubuntu Linux** | Fe80::a00:56ed:ff47:e520 | False Router Advertisement Attack | No | Yes-100% |
| | | IPv6 Router Deletion Attack | No | Yes-100% |
| | | NS Flood Attack | No | Yes-92% |
| | | ICMPv6 Smurf Attack | No | Yes-100% |
| **Windows 7** | Fe80::acd6:6b51:3647:9724 | False Router Advertisement Attack | No | Yes-100% |
| | | IPv6 Router Deletion Attack | No | Yes-100% |
| | | NS Flood Attack | No | Yes-92% |
| | | ICMPv6 Smurf Attack | Yes | Yes-100% |
| **Windows 10** | Fe80::91c8:6406:16f7:a366 | False Router Advertisement Attack | Yes | Yes-100% |
| | | IPv6 Router Deletion Attack | No | Yes-100% |
| | | NS Flood Attack | No | Yes-92% |
| | | ICMPv6 Smurf Attack | Yes | Yes-100% |

## V. COMPARISON WITH RELATED WORKS

Most studies have primarily focused on detection techniques without emphasizing the analytical aspect. Additionally, these studies addressed only a single type of attack, unlike our research, which tackled a variety of attacks on different operating systems. (See table 10):

Table *10*: summary comparison of search results with related works.

| | Approach | Contribution | Limitation |
|---|---|---|---|
| | Al-Shareeda, Manickam, Saare, Omar [1] | - Detecting SLAAC attacks using rule-based detection techniques.<br>- The research addressed the impact of the attack on Linux CentOS and Windows 10. | - The research focused on a single attack only.<br>- Relying on a single ICMPv6 message, which is the RA (Router Advertisement ) message.<br>- There are no rules to drop the attack. |
| | Saad, Anbar, Manickam, Alomari [2] | Detecting ICMPv6 DDoS attacks using artificial intelligence techniques. | - Relying on a single ICMPv6 message, the Echo Request Message.<br>- The research did not address countermeasures for the attacks. |
| | Saad, Almomani, Altaher, Gupta, and Manickam [3] | Detecting ICMPv6 DoS attack using DENFIS algorithms. | The research only addressed DoS attacks. |
| | Elejla, Belaton, Anbar, Alabsi, Al-Ani [4] | Detecting ICMPv6 DDoS attacks using classification algorithms for IDS. | Unreliable results for building real identity models. |
| | Shah, Anbar, Al-Ani, Al-Ani [5] | Detecting DoS RA attacks using entropy-based and outlier detection algorithms. | - The research focused solely on DoS RA attacks.<br>- The research did not cover other types of attacks. |
| | Elejla, Anbar, Hamouda, Faisal, Hasbullah [6] | Detecting ICMPv6 attacks using deep learning artificial intelligence techniques. | Model's low accuracy in detecting attacks due to the use of non-informative features. |
| | Rehman, Manickam [7] | Detecting IPv6 DoS attacks during the Duplicate Address Detection process. | - Relied on rules for attack detection.<br>- Used a local network environment. |
| | Bansal, Kumar, Biswas, Nandi [8] | Detecting IPv6 NDP DoS Attacks. | - The research relied on rule-based detection methods to detect attacks.<br>- The research focused solely on NDP protocol attacks. |
| | Elejla, Anbar, Belaton, Smadi [9] | Detecting RA Advertisement Flooding Attacks using Multiple Classification Techniques to | Relying on a single type of attack. |

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

| | | | |
|---|---|---|---|
| | | Build Models. | |
| | Our proposed study | - Detecting a variety of attacks on different operating systems.<br>- Relying on three types of ICMPv6 messages: RA (Router Advertisement), NA (Neighbor Advertisement), and Echo Request messages.<br>- Rule-based techniques for detecting and dropping attacks. | - Using a local network environment.<br>- Relying on rule-based for attack detection. |

## VI. FUTURE WORKS

In addition to the current research, we will further expand my research in multiple directions in the future. Among these directions, we will work on exploring and detecting other types of cyberattacks and developing strategies to counter them. We will also strive to develop advanced artificial intelligence models for the detection and analysis of cyberattacks more effectively and efficiently. Furthermore, we will conduct comprehensive analyses of attacks on operating systems expected to be released in the future, all while ensuring the originality and integrity of my work.

Additionally, we plan to delve into the analysis of random samples of IPv6 protocol packets to detect new data related to suspicious packets that may have triggered cyberattacks. We will also focus on studying the evolution of the system proposed in this research, working on its further development to effectively address emerging types of attacks. Moreover, we intend to dedicate our research efforts to the detection and analysis of novel attack vectors targeting the IPv6 protocol and its auxiliary protocols, thoroughly examining these attacks and their impacts on various operating systems.

## VII. CONCLUSIONS

The proposed system can trigger alert messages upon detecting attacks from request message attacks that use the multicast address (FF02::1) as the destination address in IPv6 networks. It reduces the number of participating packets in the attack by 92% and also detects and prevents the execution of router deletion attacks completely and immediately or after 30 seconds in the false router advertisement attack. Regarding flooding attacks, the rules used in the proposed system can detect attacks that use the same IPv6 address for both source and destination and fully filter out the packets causing the attack.

ACKNOWLEDGMENT

The authors express their gratitude to all those who offered any form of assistance in completing this work, with special thanks to the IJER Foundation.

## REFERENCES

[1] Al-Shareeda, Mahmood A., et al. "SADetection: Security Mechanisms to Detect SLAAC Attack in IPv6 Link-Local Network." Informatica 46.9 (2023).
[2] Saad, Redhwan MA, et al. "An intelligent icmpv6 ddos flooding-attack detection framework (v6iids) using back-propagation neural network." IETE Technical Review 33.3 (2016): 244-255.
[3] Saad, R. M., et al. "ICMPv6 flood attack detection using DENFIS algorithms." Indian J. Sci. Technol 7.2 (2014): 168-173.
[4] Elejla, Omar E., et al. "Comparison of classification algorithms on ICMPv6-based DDoS attacks detection." Computational Science and Technology: 5th ICCST 2018, Kota Kinabalu, Malaysia, 29-30 August 2018. Springer Singapore, 2019.
[5] Shah, Syafiq Bin Ibrahim, et al. "Hybridizing entropy based mechanism with adaptive threshold algorithm to detect RA flooding attack in IPv6 networks." Computational Science and Technology: 5th ICCST 2018, Kota Kinabalu, Malaysia, 29-30 August 2018. Springer Singapore, 2019.
[6] Elejla, O.E.; Anbar, M.; Hamouda, S.; Faisal, S.; Bahashwan, A.A.; Hasbullah, I.H. Deep-Learning-Based Approach to Detect ICMPv6 Flooding DDoS Attacks on IPv6 Networks. Appl. Sci. 2022, 12, 6150. https://doi.org/10.3390/app12126150.
[7] Rehman, Shafiq Ul, and Selvakumar Manickam. "Rule-based mechanism to detect Denial of Service (DoS) attacks on Duplicate Address Detection process in IPv6 link local communication." 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions). IEEE, 2015.
[8] Bansal, Gunjan, et al. "Detection of NDP based attacks using MLD." Proceedings of the Fifth International Conference on Security of Information and Networks. 2012.
[9] Elejla, Omar E., et al. "A new set of features for detecting router advertisement flooding attacks." 2017 Palestinian International Conference on Information and Communication Technology (PICICT). IEEE, 2017.
[10] Stallings, William. "IPv6: the new Internet protocol." IEEE Communications Magazine 34.7 (1996): 96-108.
[11] Francis, Paul. "Is the Internet going NUTSS?." IEEE Internet Computing 7.6 (2003): 94-96.
[12] Ahmed, Amjed Sid Ahmed Mohamed Sid, Rosilah Hassan, and Nor Effendy Othman. "IPv6 neighbor discovery protocol specifications, threats and countermeasures: a survey." IEEE Access 5 (2017): 18187-18210.
[13] Batiha, Khaldoun. "IMPROVING IPV6 ADDRESSING TYPES AND SIZE." International Journal of Computer Networks & Communications 5.4 (2013): 41.
[14] Johnson, David, and Stephen Deering. Reserved IPv6 subnet anycast addresses. No. rfc2526. 1999.
[15] Haberman, Brian. Allocation Guidelines for IPv6 Multicast Addresses. No. rfc3307. 2002.
[16] Loshin, Peter. "IPv6: Theory, protocol, and practice." (2004).
[17] Ullrich, J., et al. "IPv6 Security: Attacks and Countermeasures in a." SBA Research (2014).
[18] http://networksecuritystories.pbworks.com/w/file/fetch/66230509/IPv6%20Rogue%20Router%20Advertisement%20Attack.pdf
[19] https://www.first.org/resources/papers/conf2015/first_2015-herberg-frank_ipv6-security_20150618.pdf
[20] Najjar, F.; Bsoul, Q.; Al-Refai, H. An Analysis of Neighbor Discovery Protocol Attacks. Computers 2023, 12, 125. https://doi.org/10.3390/computers12060125
[21] https://core.ac.uk/download/pdf/78390261.pdf
[22] Narten, Thomas, et al. "RFC 4861: Neighbor discovery for IP version 6 (IPv6)." (2007).
[23] Draves, Richard, and Dave Thaler. Default router preferences and more-specific routes. No. rfc4191. 2005.
[24] Narten, T., E. Nordmark, and W. Simpson. "RFC 2461. Neighbour Discovery for IP version 6." (1998).
[25] Johnson, David, Charles Perkins, and Jari Arkko. "RFC 3775: Mobility support in IPv6." (2004).