IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. IV (Sep.- Oct. 2017), PP 66-70
www.iosrjournals.org

A Study of Two Different Attacks to IPv6 Network

Ayman M. A. Shabour [1], M.A. Elshaikh [2]

[1](*Faculty of Graduate Studies and Scientific Research /*
The National Ribat University / Sudan/ shabour313@hotmail.com)

[2](*Faculty of Computer Science and Information Technology / Sudan University of Science and technology*
, Sudan / mawad_elshaikh@yahoo.com)

Abstract: *In the lights of today and future advancing technologies, the demand of IPv6 internet protocol, had becomes crucial for its usages & benefits. This paper investigates the use of information messages to build a visual perception and follow-up of IPv6-based cyber-attacks on IPv6 networks IPv6 , (DOS)& ARP poisoning , Packet analyzer(wireshark) and open source tools(virtualbox, Linux kali system, Ubuntu Linux server) are used ,to verify the existence of attacks on IPV6. The experimental results ,proved that the traces of simulated attacks extend form the link layer to the application layer.*

Keywords: *Internet Protocol version 6(IPv6), Internet Protocol version 4(IPv4) Transfer Control Protocol(TCP), Address Resolution Protocol(ARP), Denial of Service(DOS), Internet Control Message Protocol version6 (ICMPv6)****.***

Date of Submission: 06-10-2017 Date of acceptance: 27-10-2017

I. Introduction

Internet Protocol Version6 (IPv6) which intended to replace IPv4 in the worldwide Internet mainly due to the address exhaustion of IPv4. IPv6 extremely enhances the address space from 32 bits to 128 bits. It means the future expansion of the Internet is now dependent on the successful global deployment of the next generation of Internet protocol[1]. IPv6 address security it's similar to IPv4 security .Transporting packets mechanism in the network almost the same. The mostly unaffected layer is upper layer which is responsible for transporting application data. However, because IPv6 mandates the inclusion of IP security (IPsec),it has often been stated that IPv6 is more secure than IPv4, Although this may be true in an ideal environment with well-coded applications, a robust identity infrastructure, and efficient key management, in reality the same problems that plague IPv4 IPsec deployment will affect IPv6 IPsec deployment. IPv6 is not protected with any kind of cryptography. Additionally, because most security breaches occur at the application level. The IPv6 security features introduced mainly by way of two dedicated extension headers which is the Authentication Header (AH) and the Encrypted Security Payload (ESP), with complementary capabilities. The two headers can be used together to provide all the security features simultaneously. Also IPv6 support another new features IPv6 including increased address space, auto configuration, quality of service capabilities, and network-layer security, all these previous features can be used to prevent various network attack methods including IP spoofing, some Denial of Service attacks , data modification and sniffing behavior [2].

II. Overview of Neighbor Discovery Protocol

Neighbor Discovery Protocol is replacer of Address Resolution Protocol in IPv4 networks, and its a family of different functions related to other IPv6 nodes on the same link such as finding routers and other nodes, maintaining reachability information about active neighbors (Neighbor Unreachability Detection - NUD) or configuring their own unique IPv6 addresses via Auto configuration (Duplicate Address Detection – DAD). The corresponding (parallel/ Matching) five ICMPv6 messages with neighbor discovery are specified below: [3]

The Router Solicitation message

Which is ICMPv6 informational message type 133, is sent by a node in order to discover any routers on the link? It is therefore sent to the all-routers multicast address ff02::2. As an option, this message carries the link-layer address of the requesting node. This has the advantage that the responding router directly knows to which node the answering packet should be sent. If a router is present on the link, it answers immediately with a Router Advertisement[4].

The Router Advertisement message

It is ICMPv6 informational message type 134 and contain one or more prefixes, the prefixes have lifetime, and used stateless or state full auto configuration.

The Neighbor Solicitation message

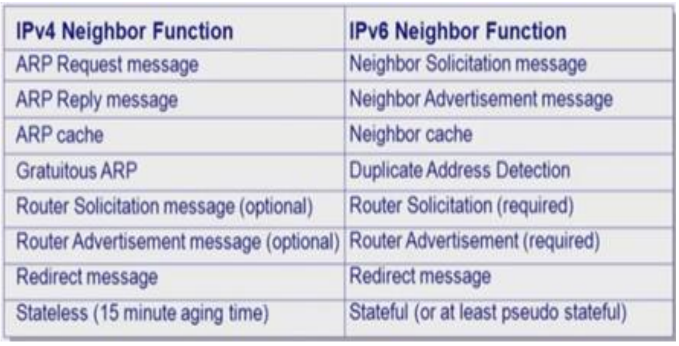
It is ICMPv6 informational message type 135, and used by the node to get Link Layer address of neighbor.

The Neighbor Advertisement message

It is ICMPv6 informational message type 136, and through it the neighbor solicitation response to.

The Neighbor Redirect Message

It is ICMPv6 informational message type 136 , It is sent from a router to a node in order to indicate a more appropriate first-hop node along the path to the destination network. This can either be another router on the same link or a directly connected neighbor node in the case that the originating node did not expect it on the same link due to other used IPv6 prefixes. A redirect message contains two addresses, namely the Target Address which is the best next hop and the Destination Address which is the address of the destination of the original IPv6 packet. The table (1) below comparing between IPv6 neighbors Discovery and IPv4 ARP.



IPv4 Neighbor Function	IPv6 Neighbor Function
ARP Request message	Neighbor Solicitation message
ARP Reply message	Neighbor Advertisement message
ARP cache	Neighbor cache
Gratuitous ARP	Duplicate Address Detection
Router Solicitation message (optional)	Router Solicitation (required)
Router Advertisement message (optional)	Router Advertisement (required)
Redirect message	Redirect message
Stateless (15 minute aging time)	Stateful (or at least pseudo stateful)

III. Problem Statement & Objective

According to previous researches, still there is attacks can happen in a solely IPV6 networks which inherit from previous IPv4.The goal of these papers is to present the observation of effect of ARP poisoning and Denial of service attack in IPv6 networks .To approve that these tow type of attacks can happen in IPv6 networks.

IV. Methodology

Using Linux Kali system to exploit the link layer in IPv6 protocol against the ARP spoofing and Denial of service attacks, via different scenarios of experiment’s and captured logged by wireshark network analyzer.

Network Topology and Experiments

The environment presented in these papers done over virtualization technology via virtualbox[5] which used to created Linux kali system as attacker machine[6] , Ubuntu Linux server version 14.0.4 as webserver .The packets captured and analysis by wireshark application[7] which controlled from windows7 machine as client access. The network diagram below in figure 1 describe the details

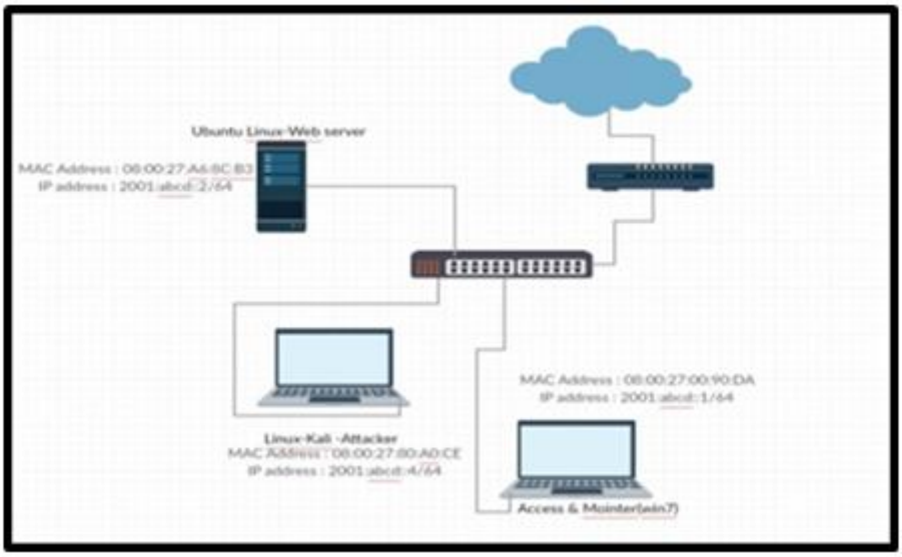
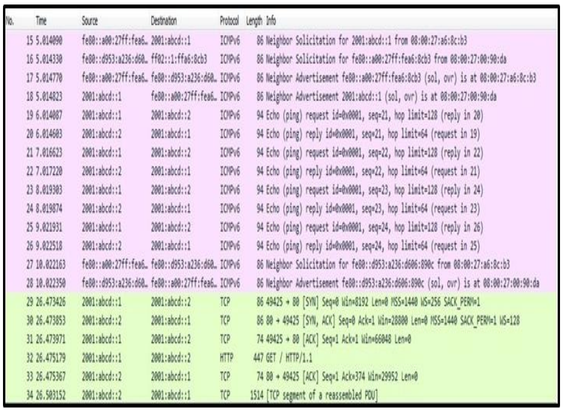

Ubuntu Linux Web server
MAC Address : 08:00:27:A6:8C:B3
IP address : 2001:abcd::2/64
MAC Address : 08:00:27:00:90:DA
IP address : 2001:abcd::1/64
Linux-Kali -Attacker
MAC Address : 08:00:27:80:A0:CE
IP address : 2001:abcd::4/64
Access & Mointer(win7)

Figure 1:Network diagram

V. The ARP poisoning Attack

ARP spoofing is the technique of forging fake ARP messages on a network. The attacker updates a host's ARP cache with false information via spoofed ARP Replies. Man-in-the-middle (MITM) attack: In this attack, an attacker places himself in the middle of two hosts that are communicating. The attacker makes sure that all traffic between the hosts pass through him and is able to see the entire traffic the attacker effectively used the neighbor solicitation and neighbor advertisement messages to perform a Man-in-the-Middle attack .

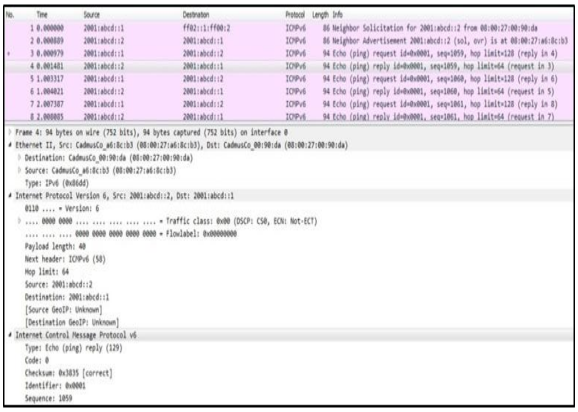
The traffic between web server and client before attack its seem that are running normal and smoothly, and accessing web services from the client machine , the client sent its neighbor solicitation for webserver from its link layer address over ICMPv6 and the webserver replay in neighbor advertisement with its link address also. When the client make echo request ping, the server replay with echo normally and the IP6 appeared in source and destination packages instead of link layer address. And the client access website in the webserver via TCP and HTTP normally without need for more solicitation and advertisement messages,figure2 below explained these situation .



```
No.   Time       Source                Destination           Protocol Length Info
   15 5.014090   fe80::a00:27ff:fea6…  2001:abcd::1          ICMPv6    86 Neighbor Solicitation for 2001:abcd::1 from 08:00:27:a6:8c:b3
   16 5.014330   fe80::d953:a236:d60…  ff02::1:ffa6:8cb3     ICMPv6    86 Neighbor Solicitation for fe80::a00:27ff:fea6:8cb3 from 08:00:27:00:90:da
   17 5.014770   fe80::a00:27ff:fea6…  fe80::d953:a236:d60…  ICMPv6    86 Neighbor Advertisement fe80::a00:27ff:fea6:8cb3 (sol, ovr) is at 08:00:27:a6:8c:b3
   18 5.014823   2001:abcd::1          fe80::a00:27ff:fea6…  ICMPv6    86 Neighbor Advertisement 2001:abcd::1 (sol, ovr) is at 08:00:27:00:90:da
   19 6.014087   2001:abcd::1          2001:abcd::2          ICMPv6    94 Echo (ping) request id=0x0001, seq=21, hop limit=128 (reply in 20)
   20 6.014603   2001:abcd::2          2001:abcd::1          ICMPv6    94 Echo (ping) reply id=0x0001, seq=21, hop limit=64 (request in 19)
   21 7.016623   2001:abcd::1          2001:abcd::2          ICMPv6    94 Echo (ping) request id=0x0001, seq=22, hop limit=128 (reply in 22)
   22 7.017220   2001:abcd::2          2001:abcd::1          ICMPv6    94 Echo (ping) reply id=0x0001, seq=22, hop limit=64 (request in 21)
   23 8.019303   2001:abcd::1          2001:abcd::2          ICMPv6    94 Echo (ping) request id=0x0001, seq=23, hop limit=128 (reply in 24)
   24 8.019874   2001:abcd::2          2001:abcd::1          ICMPv6    94 Echo (ping) reply id=0x0001, seq=23, hop limit=64 (request in 23)
   25 9.021931   2001:abcd::1          2001:abcd::2          ICMPv6    94 Echo (ping) request id=0x0001, seq=24, hop limit=128 (reply in 26)
   26 9.022518   2001:abcd::2          2001:abcd::1          ICMPv6    94 Echo (ping) reply id=0x0001, seq=24, hop limit=64 (request in 25)
   27 10.022163  fe80::a00:27ff:fea6…  fe80::d953:a236:d60…  ICMPv6    86 Neighbor Solicitation for fe80::d953:a236:d606:890c from 08:00:27:a6:8c:b3
   28 10.022350  fe80::d953:a236:d60…  fe80::a00:27ff:fea6…  ICMPv6    86 Neighbor Advertisement fe80::d953:a236:d606:890c (sol, ovr) is at 08:00:27:00:90:da
   29 26.473426  2001:abcd::1          2001:abcd::2          TCP       86 49425 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
   30 26.473853  2001:abcd::2          2001:abcd::1          TCP       86 80 → 49425 [SYN, ACK] Seq=0 Ack=1 Win=28800 Len=0 MSS=1440 SACK_PERM=1 WS=128
   31 26.473971  2001:abcd::1          2001:abcd::2          TCP       74 49425 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
   32 26.475179  2001:abcd::1          2001:abcd::2          HTTP     447 GET / HTTP/1.1
   33 26.475367  2001:abcd::2          2001:abcd::1          TCP       74 80 → 49425 [ACK] Seq=1 Ack=374 Win=29952 Len=0
   34 26.503152  2001:abcd::2          2001:abcd::1          TCP     1514 [TCP segment of a reassembled PDU]
```

Figure2: Monitor Of Packets in Normal Operation

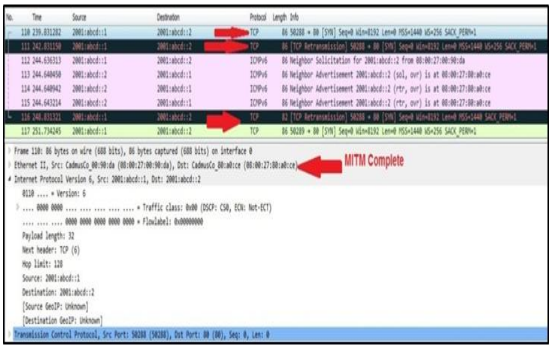
If the attack lunched after above situation by command #atk6-parasite6 eth0 2001: abcd::2 fake-mac , The client access and the server used their link layer address for neighbor solicitation and advertisement over ICMPv6 , the attacker repeatedly sends spoofed neighbor advertisement messages and overrides other entries . The neighbor advertisements sent by both the Attacker and web server have the override flag set to 1. the attacker replay its [ACK] flag by [SYN] flag , and repeated send [ACK] and [TCP Retransmission] instead of web server, and the web site not more been access. The attacker send a neighbor advertisement to client computer saying that it has the IP that belongs to web server, figure3 below explained these scenario.



```
No.   Time       Source          Destination     Protocol Length Info
    1 0.000000   2001:abcd::1    ff02::1:ff00:2  ICMPv6    86 Neighbor Solicitation for 2001:abcd::2 from 08:00:27:00:90:da
    2 0.000889   2001:abcd::2    2001:abcd::1    ICMPv6    86 Neighbor Advertisement 2001:abcd::2 (sol, ovr) is at 08:00:27:a6:8c:b3
    3 0.000979   2001:abcd::1    2001:abcd::2    ICMPv6    94 Echo (ping) request id=0x0001, seq=1059, hop limit=128 (reply in 4)
    4 0.001481   2001:abcd::2    2001:abcd::1    ICMPv6    94 Echo (ping) reply id=0x0001, seq=1059, hop limit=64 (request in 3)
    5 1.003317   2001:abcd::1    2001:abcd::2    ICMPv6    94 Echo (ping) request id=0x0001, seq=1060, hop limit=128 (reply in 6)
    6 1.004021   2001:abcd::2    2001:abcd::1    ICMPv6    94 Echo (ping) reply id=0x0001, seq=1060, hop limit=64 (request in 5)
    7 2.007387   2001:abcd::1    2001:abcd::2    ICMPv6    94 Echo (ping) request id=0x0001, seq=1061, hop limit=128 (reply in 8)
    8 2.008085   2001:abcd::2    2001:abcd::1    ICMPv6    94 Echo (ping) reply id=0x0001, seq=1061, hop limit=64 (request in 7)

▷ Frame 4: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
◢ Ethernet II, Src: CadmusCo_a6:8c:b3 (08:00:27:a6:8c:b3), Dst: CadmusCo_00:90:da (08:00:27:00:90:da)
  ▷ Destination: CadmusCo_00:90:da (08:00:27:00:90:da)
  ▷ Source: CadmusCo_a6:8c:b3 (08:00:27:a6:8c:b3)
    Type: IPv6 (0x86dd)
◢ Internet Protocol Version 6, Src: 2001:abcd::2, Dst: 2001:abcd::1
    0110 .... = Version: 6
  ▷ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 40
    Next header: ICMPv6 (58)
    Hop limit: 64
    Source: 2001:abcd::2
    Destination: 2001:abcd::1
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
◢ Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x3835 [correct]
    Identifier: 0x0001
    Sequence: 1059
```

Figure3: Monitor of packets in ARP attack

The changing of the attack scenario like lunch attack before an active communication between client and server or after continues communication link, didn’t produce any changes in the result. But still the attacker effectively used the neighbor solicitation and neighbor advertisement messages to perform ARP poisoning attack and the form of a Man-in-the-Middle attack take place, and figure 4 prove that.



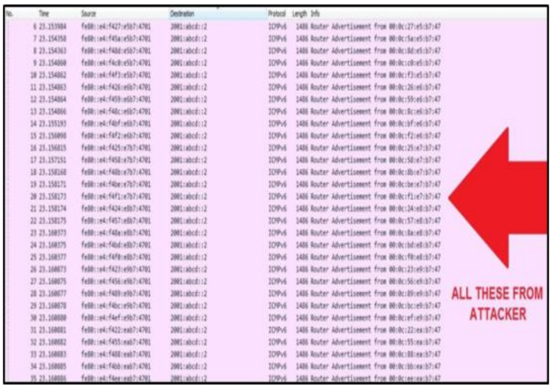
```
No.  Time        Source        Destination   Protocol Length Info
 110 239.831282  2001:abcd::1  2001:abcd::2  TCP      86 50288 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
 111 242.831150  2001:abcd::1  2001:abcd::2  TCP      86 [TCP Retransmission] 50288 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1
 112 244.636313  2001:abcd::1  2001:abcd::2  ICMPv6   86 Neighbor Solicitation for 2001:abcd::2 from 08:00:27:00:90:da
 113 244.640450  2001:abcd::2  2001:abcd::1  ICMPv6   86 Neighbor Advertisement 2001:abcd::2 (sol, ovr) is at 08:00:27:80:a0:ce
 114 244.640942  2001:abcd::2  2001:abcd::1  ICMPv6   86 Neighbor Advertisement 2001:abcd::2 (rtr, ovr) is at 08:00:27:80:a0:ce
 115 244.643214  2001:abcd::2  2001:abcd::1  ICMPv6   86 Neighbor Advertisement 2001:abcd::2 (rtr, ovr) is at 08:00:27:80:a0:ce
 116 248.831321  2001:abcd::1  2001:abcd::2  TCP      82 [TCP Retransmission] 50288 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 SACK_PERM=1
 117 251.734245  2001:abcd::1  2001:abcd::2  TCP      86 50289 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1

> Frame 110: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
> Ethernet II, Src: CadmusCo_00:90:da (08:00:27:00:90:da), Dst: CadmusCo_80:a0:ce (08:00:27:80:a0:ce)
▲ Internet Protocol Version 6, Src: 2001:abcd::1, Dst: 2001:abcd::2
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 32
    Next header: TCP (6)
    Hop limit: 128
    Source: 2001:abcd::1
    Destination: 2001:abcd::2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
> Transmission Control Protocol, Src Port: 50288 (50288), Dst Port: 80 (80), Seq: 0, Len: 0
```

MITM Complete

Figure 4: Man-in-the Middle in ARP attack

2. The Denial of Service Attack

The goal of a denial of service attack is to deny legitimate users to access the a particular resource or services. in these papers the attacks lunched against host and network resource. When the attack lunched by command #atk6-flood_route26 eth0 2001:abcd::2, the attacker start sending continue router advertisement as much flooded the network , simultaneously the client sending repeated solicitation message to web server .The ping request sent from client to webserver while attacking running countered by host unreachable and DOS attack successfully utilization the resources . At the same time When the client try to browse web site [2001: abcd::2] ,its unable to reached it, and the error generated ,and the web server not been reachable more for users and the attacker success take place. The figure 5 below explained how attacker flood the network.



```
No.  Time       Source                   Destination   Protocol Length Info
   6 23.153984  fe80::e4:f427:e5b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:27:e5:b7:47
   7 23.154358  fe80::e4:f45a:e5b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:5a:e5:b7:47
   8 23.154363  fe80::e4:f48d:e5b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:8d:e5:b7:47
   9 23.154860  fe80::e4:f4c0:e5b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:c0:e5:b7:47
  10 23.154862  fe80::e4:f4f3:e5b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:f3:e5:b7:47
  11 23.154863  fe80::e4:f426:e6b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:26:e6:b7:47
  12 23.154864  fe80::e4:f459:e6b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:59:e6:b7:47
  13 23.154866  fe80::e4:f48c:e6b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:8c:e6:b7:47
  14 23.155193  fe80::e4:f4bf:e6b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:bf:e6:b7:47
  15 23.156098  fe80::e4:f4f2:e6b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:f2:e6:b7:47
  16 23.156815  fe80::e4:f425:e7b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:25:e7:b7:47
  17 23.157151  fe80::e4:f458:e7b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:58:e7:b7:47
  18 23.158168  fe80::e4:f48b:e7b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:8b:e7:b7:47
  19 23.158171  fe80::e4:f4be:e7b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:be:e7:b7:47
  20 23.158173  fe80::e4:f4f1:e7b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:f1:e7:b7:47
  21 23.158174  fe80::e4:f424:e8b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:24:e8:b7:47
  22 23.158175  fe80::e4:f457:e8b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:57:e8:b7:47
  23 23.160373  fe80::e4:f48a:e8b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:8a:e8:b7:47
  24 23.160375  fe80::e4:f4bd:e8b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:bd:e8:b7:47
  25 23.160377  fe80::e4:f4f0:e8b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:f0:e8:b7:47
  26 23.160873  fe80::e4:f423:e9b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:23:e9:b7:47
  27 23.160875  fe80::e4:f456:e9b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:56:e9:b7:47
  28 23.160877  fe80::e4:f489:e9b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:89:e9:b7:47
  29 23.160878  fe80::e4:f4bc:e9b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:bc:e9:b7:47
  30 23.160880  fe80::e4:f4ef:e9b7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:ef:e9:b7:47
  31 23.160881  fe80::e4:f422:eab7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:22:ea:b7:47
  32 23.160882  fe80::e4:f455:eab7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:55:ea:b7:47
  33 23.160883  fe80::e4:f488:eab7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:88:ea:b7:47
  34 23.160885  fe80::e4:f4bb:eab7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:bb:ea:b7:47
  35 23.160886  fe80::e4:f4ee:eab7:4701  2001:abcd::2  ICMPv6   1486 Router Advertisement from 00:0c:ee:ea:b7:47
```

ALL THESE FROM ATTACKER

Figure 5: attacker advertisement in DOS Attack

The swapping of experiment steps to lunch attack while browsing or before browsing it didn’t produce any changes. The attacker effectively used the router advertisement messages and neighbor solicitation to perform a Denial Of Service Attack successfully .

VI. Conclusion

In The Denial of Service Attack , the attacker successfully flooded the network by router advertisement messages and neighbor solicitation messages and perform denial of service , and echo requests not reached the destination and web server also been unreachable. In ARP poisoning Attack, when the client sent its neighbor solicitation ,and the web server reply by its own neighbor advertisement, the attacker sent neighbor advertisement to client that it has the IP belong to the web server, and the attacker repeated spoofed neighbor advertisement messages, so the echo request from client been replayed from attacker since its impersonating the web server, and continue generates a Neighbor solicitation message to find the real destination of the packet. Then, the attacker forwards the reply to client computer and completes a Man-in-the-Middle attack ,On the other hand when client try to access web server, the attacker replay its [ACK] flag by [SYN] flag , and repeated send [ACK] and [TCP Retransmission] instead of web server, and the web site not more been access.

References

[1] ICANN. Available Pool of Unallocated IPv4 Interne Addresses .Internet : https://www.icann.org/en/system/files/press-materials/release-03feb11-en.pdf .February.3,2011 accessed [May.10,2017]

[2] UK ESSAYS . Ipv4 Internet Protocol Security Features Computer Science Essay. Internet : https://www.ukessays.com/essays/computer-science/ipv4-internet-protocol-security-features-computer-science-essay.php#ftn1. March.23,2015 accessed [May.10,2017]

[3] [RFC 4861] Narten, T., Nordmark, E., Simpson, W., Soliman,H. "Neighbor Discovery for IP version 6 (IPv6)". September 2007.Available : https://tools.ietf.org/html/rfc4861 .accessed [June .16,2017]

[4] [RFC 5175] B.Haberman,R .Hinden "IPv6 Router Advertisement Flags Option" March 2008 Available : https://tools.ietf.org/html/rfc5175 . accessed [June .16,2017] https://www.virtualbox.org/ accessed March.20, 2017

[5] Wireshark User's Guide :for Wireshark 1.7 by Ulf Lamping,Richard Sharpe,Ed.Warnicke Copyright © 2004-2011; Source: https://www.wireshark.org/about.html accessed March.20, 2017

[6] Van Hauser ,The Hackers Choice (THC-IPv6)" https://www.thc.org/thc-IPv6/README accessed March.20, 2017

Ayman M. A. Shabour . "A Study of Two Different Attacks to IPv6 Network." IOSR Journal of Computer Engineering (IOSR-JCE) , vol. 19, no. 5, 2017, pp. 66–70.