IPv6 Attack Detection

Author: Toan Pham

August 28, 2012

1 Introduction

As the end of GSoC 2012 will come in the next few days, i am proud to announce IPv6-guard. IPv6-guard is an IPv6 attack detector tool including some defense mechanisms to protect against most of recent attacks on ipv6 protocol suite.

2 IPv6-Guard

2.0.1 How it works

At first, the tool will gather "genuine" informations of connected network. Those information includes IP and MAC address of neighbors and routers on the network.After first time run, IPv6-guard will save this information to use later, if anything has change,it will ask for confirmation (User can edit "/data/genuine.info" to add more interface if need). If the network is under attack, some invalid information might be detected and it will ask you to verify what information is "genuine". IPv6-Guard will use collected information and signatures against every received packet to detect and mitigate IPv6 attacks from the network.

Output:

```
Trusted ? [Y/n] y Got fe80::9c4e:a8a4:c6b9:7e6c / 6c:62:6d:07:7e:8c
Mac Manufacture : Micro-St  # Micro-Star INT'L CO., LTD
Trusted ? [Y/n] y
{'fe80::c540:56ed:bfae:6a45':
'6c:62:6d:af:57:4a', 'fe80::e56e:67c8:a60b:7ea4':
'e8:39:35:3b:58:5c', 'fe80::f2de:f1ff:fe2f:3cc3':
'f0:de:f1:2f:3c:c3', 'fe80::15a9:3a36:834c:e0ba':
'e8:39:35:3a:24:b8', 'fe80::8452:71:b94e:cdb9'
```

2.1 Examples

- flood_advertise6

  Output:

```
[FLOOD PACKET]
    Time   :  2012-08-22 08:27:12
    From   :  00:18:18:a5:65:5b (Cisco Systems)
    To     :  33:33:00:00:00:01 (Unknow)
    Desc   :  flood_advertise6
```

This feature detect flood on a target with random neighbor advertisements. It is based on configured packet rate and a few heuristic algorithms.

- flood_solicitate6

  Output:

```
[FAKE NEIGHBOR SOLICITATION]
    Time : 2012-08-22 08:22:14
    From : 90:84:0d:84:b7:b2 (Apple, Inc)
    To : 33:33:ff:00:00:09 (Unknow)
    Desc : parasite6
```

- fake_router6 or flood_router6

  Output:

```
[FAKE ROUTER ADVERTISMENT]
    Time   :  2012-08-22 08:28:42
    From   :  00:18:ab:36:4d:ac
    (BEIJING LHWT MICROELECTRONICS INC.)
    To     :  33:33:00:00:00:01 (Unknow)
    Desc   :  fake_router6
```

  This is an example to detect fake_router6 attack by announcing a host as a router on the network with the highest priority. To protect host against this attack, the tool will send a packet with routerlifetime=0 to reset that fake router and invalid route in routing table.

  Also, when this attack is occured, the tool will also clean up host interface using "genuine" information collected earlier.

  Before

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

    inet 192.168.56.1 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 2a01:9c11:db7e:d849:800:27ff:fe00:0 prefixlen 64 scopeid
    inet6 2a01:99ac:6b62:841a:800:27ff:fe00:0 prefixlen 64 scopeid
    inet6 2a01:b5ab:3408:9545:800:27ff:fe00:0 prefixlen 64 scopeid
    inet6 2a01:43c1:e2c6:6d96:800:27ff:fe00:0 prefixlen 64 scopeid
    inet6 fe80::800:27ff:fe00:0 prefixlen 64 scopeid 0x20<link>
```

  Cleaning up

```
Clean ip 2a01:9c81:e745:eef2:800:27ff:fe00:0
Mon Aug 20 21:16:44 2012
Delete an ipv6 address of interface eth0 from 2a01:9c81:e745:
    eef2:800:27ff:fe00:0
```

After

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

    inet 192.168.56.1 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::800:27ff:fe00:0 prefixlen 64 scopeid 0x20<link>
    ether 0a:00:27:00:00:00 txqueuelen 1000 (Ethernet)
```

- smurf6

  Output:

```
[FLOOD NEIGHBOR SOLICITATION]
    Time   :  2012-08-22 08:28:42
    From   :  00:18:ab:36:4d:ac
    (BEIJING LHWT MICROELECTRONICS INC.)
    To     :  33:33:00:00:00:01 (Unknow)
    Desc   :  rsmurf6 |  sendpees6
```

  Detect smurf6 attack in which using our ip address with another MAC address.

2.2 Supported Attack Detections

Currently, this tool could detect various IPv6 attacks including:

- parasite6: icmp neighbor solitication/advertisement spoofer
- fake_router6: fake router address (mitm)
- flood_router6: flood router advertisement packet
- flood_advertise6: flood neighbor advertisement packet
- fake_advertiser6: fake neighbor ip (mitm)
- smurf6: flood icmp echo packet
- rsmurf6: remote smurfer
- fuzz_ip6: flood ipv6 packet
- fake_mld6: fake multicast group
- sendpees6: Generates a neighbor solicitation requests with a lot of CGAs.

For protection, some simple methods are being implemented such as

- Reset routerlifetime to delete fake route in routing table
- Clear all invalid entries on attacked interface

2.3 Synopsis

```
# python2 6shield.py -i <interface> -c <config>

     - interface    interface to sniffing and detect attack
     - config       configuration file

ex:
# python2 6shield.py -i eth0
```

2.4 Configuration

This tool includes a configuration file to detect attacks from thc-ipv6 tool. If another tool using similar techniques with different packet rate, you could add a new section for it

```
[generic] manuFile=manuf ; mac/manufacturer file
; attack tool ( command line option)
[thc-ipv6]
routerLifetime=9999  ; router lifetime that attack using
naLimit=10           ; Neighbor Advertisement packet/second limitation
raLimit=10           ; Router Advertisement packet/second limitation
icmpLimit=10         ; ICMP Echo packet per second limitation
limitRate=20         ; IPv6 control packet per second limitation
```

2.5 Future Works

- Improve detection method to lower false positive chance
- Improve protection method

3 Final words

- Thanks Google for such a program for student
- Thanks Honeynet Project for this cool project
- Thanks Thanh Nguyen for help me finish this project