THC-IPV6 News

#1 IPv6 Hackers Meeting

Marc “van Hauser” Heuse
Hello, my name is ...
Short thc-ipv6 summary

Bla bla bla ☺
The first IPv6/ICMPv6 attack toolkit
Today: 60 tools
Scanning Tools!

- Alive Scanning:
  - Alive scanning techniques: alive6
  - ICMPv6 Inverse Lookup: inverse_lookup6
  - ICMPv6 Node Query: node_query6

- DNS enumeration:
  - Brute: dnsdict6
  - Reverse: dnsrevenum6
  - DNSSEC: dnsseccwalk

- Local Discovery:
  - NS: detect-new-ip6
  - Sniff: passive_discovery6

- Tracerouter: trace6

- Helper tools: address6
Man-in-the-Middle Spoofing Tools!

- ICMPv6 Redirects: redir6, redirsniff6
- NDP: parasite6, fake_advertise6
- RA: fake_router6, fake_router26
- DHCPv6: fake_dhcps6
- DNS: fake_dns6d
- Mobility: fake_mipv6
Denial-of-Service Tools!

- flood_advertise6
- flood_dhcpc6
- flood_mld6
- flood_mld26
- flood_mldrouter6
- flood_redirect6
- flood_router6
- flood_router26
- flood_solicitate6
- denial6
- dos-new-ip6
- exploit6
- fake_advertise6
- kill_router6
- ndpexhaust6
- ndpexhaust26
- rsmurf6
- sendpees6
- sendpeesmp6
- smurf6
- thcsyn6
Testing Tools!

- Extension headers + ICMPv6: implementation6
- Fragmentation: fragmentation6
- Firewall filtering: firewall6
- ICMPv6: randicmp6
- Fuzzer: fuzz_ip6
More Tools!

- covert_send6 + covert_send6d
- detect_sniffer6
- dump_router6
- inject_alive6
- thcping6
- toobig6
- four2six

- fake_dnsupdate6
- fake_mld26
- fake_mld6
- fake_mldrouter6
- fake_pim6
- fake_solicitate6
Little known feature: INJECTION
Injecting into:

802.1q
6in4
PPPoE
Why?

• Only way to test link-local BRAS security from subscriber line (PPPoE)
• Inject into tunnels that do not belong to you (6to4)
• Support environments with 802.1q VLANs
Setup for DSL PPPoE injection
Config by environment

- Set-up environment variable that describes the injection type and parameters
  
  ```
  export THC_IPV6_xxx=value,value,value
  ```

- Then just run the thc-ipv6 commands normally
Config 802.1q

- THC_IPV6_VLAN=srcmac,dstmac,vlan-id
- e.g.

  export THC_IPV6_VLAN=01:01:01:01:01:01:01,02:02:02:02:02:02:02,1
Config PPPoE

- THC_IPV6_PPPoE=srcmac,dstmac,ppp-sessionid

  e.g.

  export THC_IPV6_PPPoE=01:01:01:01:01:01:01,02:02:02:02:02:02:02,0f2b
Config 6in4

- THC_IPV6_6IN4=srcmac,dstmac,src-ipv4,dst-ipv4
- e.g.
  
  ```
  export THC_IPV6_6IN4=01:01:01:01:01:01:01,02:02:02:02:02:02:02,1.1.1.1,2.2.2.2
  ```
Getting the information

- **802.1q**
  
  tcpdump -i eth0 -n -vvv -e ether proto 0x8100

- **PPPoE**
  
  tcpdump -i eth0 -n -vvv -e ether proto 0x8864

- **6IN4**
  
  tcpdump -i eth0 -n -e ip proto 41
Running the tools

• Just run them

• You will always see the message
  
  Information: PPPoE injection/sniffing activated

  or

  Information: 6in4 injection/sniffing activated
Important!

• Configure yourself the source IPv6 address that is needed!
Session keep-alive

- If you need to keep the PPPoE/6in4 session alive:
  
  `inject_alive6 eth0`

- Takes care of echo request/reply (PPP and ICMP)

- Checks changing of PPPoE sessionID
Tools that not work

parasite6 fake_solicitate6 fake_advertise6
connect6 detect_sniffer6 flood_advertise6
flood_solicitate6 inverse_lookup6 dnsdict6
dnsrevenum6 fake_dnsupdate6 fake_dhcps6
flood_dhcpc6
More information

• File HOWOTO-INJECT in the thc-ipv6 package
What’s in upcoming v2.5
What’s new in upcoming v2.5

• **New: flood_redir6**
  – flooding with ICMPv6 redirects
  – 10-35% traffic loss on high-end Cisco routers
• **New: four2six**
  – send an IPv4 packet via an 4to6 gateway
What’s new in upcoming v2.5

• alive6:
  – Option -4 200.100.0/24 IPv4 address encoding scan option

• flood_router26:
  – more effectiveness against all vulnerable platforms 😊

• Small nice features for trace6, parasite6, fragmentation6 and randicmp6

• Many small changes to screen outputs, some changes to the library (IPv4 packet support) etc.
What do you think would be important tools and features that should be added?
Future

- More attack tools, e.g.
  - DHCPv6 client fuzzer
  - DHCPv6 server fuzzer
  - More configurable DHCPv6 fake server
  - More advances to scanning (alive6) and RA flooding (flood_router26)
  - More fragmentation weirdness tests
  - ...

If you want to contribute – contact me 😊
Contact
Contact

Marc Heuse

📞 +49 (0)177 961 15 60
📞 +49 (0)30 37 30 97 26
✉️ mh@mh-sec.de
🌐 www.mh-sec.de
✉️ winsstrasse 68
d-10405 berlin
End