THC-IPV6
A toolkit for attacking IPv6 and ICMPv6

Marc “van Hauser” Heuse

Hello, my name is …


Kids, back in 2005 …

The first IPv6/ICMPv6 attack toolkit

Today: 60 tools

Design

- Packet Crafting Library
- One small tool per attack idea
- Easy to use (even by mommy)
- Requiring Linux + Ethernet, works in VM

The only IPv6 toolkit that can send into PPTP, 6to4 and 802.1q tunnels

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: dnssecwalk
- 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_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
- fake_dnsupdate6
- fake_mld26
- fake_mld6
- fake_mldrouter6
- fake_pim6
- fake_solicitate6
- inject_alive6
- thcping6
- toobig6

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 ☺

Others – what else you can use

- Fernando Gont's ipv6-toolkit
  - www.si6networks.com/research/tools.html
- Scapy
  - www.secdev.org/projects/scapy/

You need to be an expert to use either of these, but they give total control on what and how to send

Testing IPv6 Firewalls with thc-ipv6


c't
magazin für computer technik
11
Ab 300 Euro
Notebook-Schnäppchen
Subnotebooks, Arbeitstiere, Multimedia-Riesen und Chromebooks
WLAN-Speicheradapter
IPv6-Firewalls
Faktura als Webdienst
Samsung Galaxy S4 im Test
Günstige Windows-Phones
Industrieanlagen gehackt
Linux auf aktuellen PCs
OpenGL-Shader mit Qt
Tipps für Wenigdrucker
Kabel-TV unverschlüsselt
Raus aus der Apple-Google-Microsoft-Cloud
Datenkraken ade
Kalender, Kontakte, E-Mail unter eigener Kontrolle

The Candidates!

Check Point®
SOFTWARE TECHNOLOGIES LTD.

What should a firewall do for IPv6?

Correct handling of IPv6, Extension Headers and ICMPv6

Filter invalid source addresses

Check Extension Headers
Filter Extension Headers

Check Extension Header Options
Filter Extension Header Options

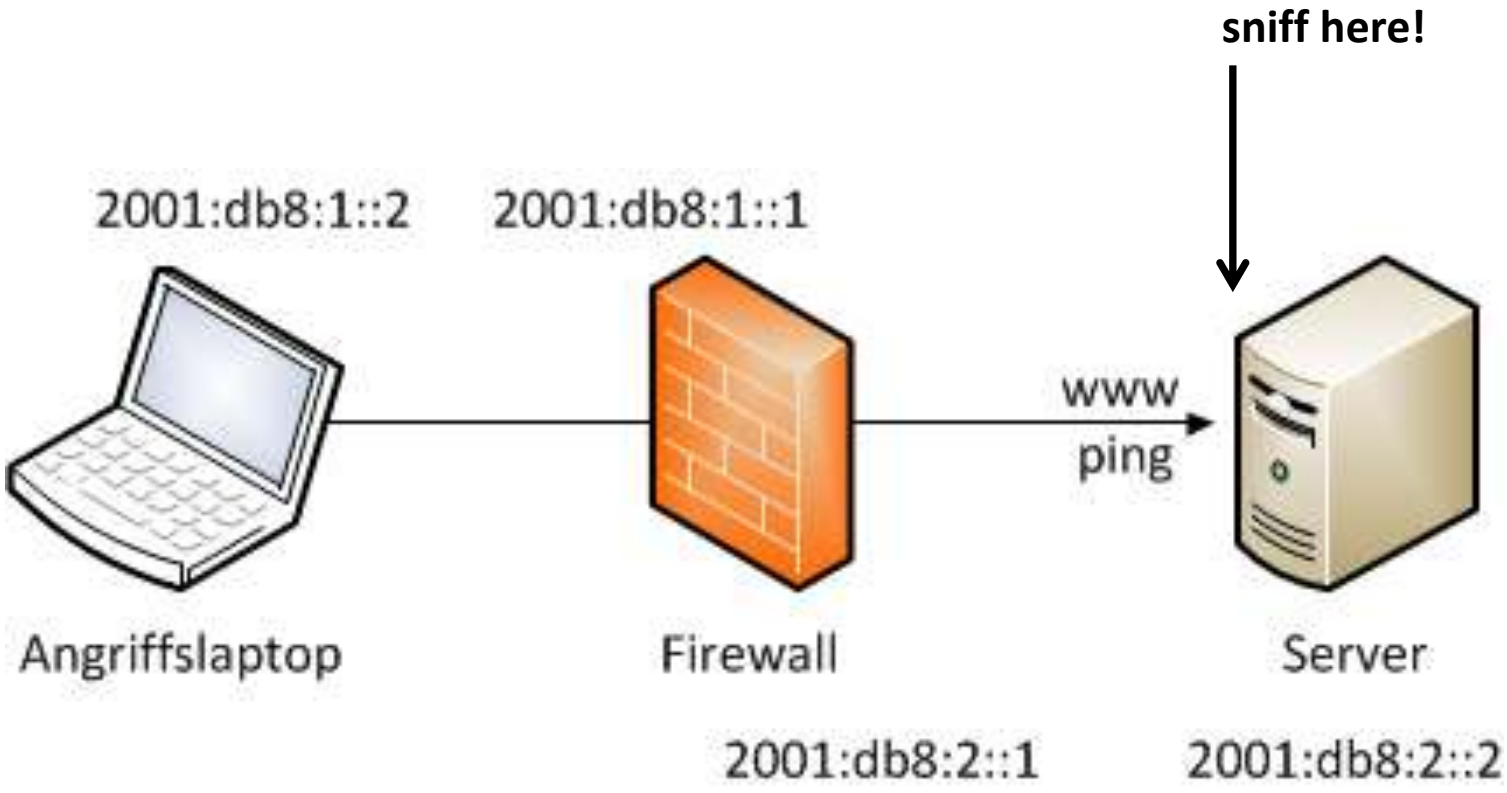
Handle Fragmentation securely

No rule bypass due Fragmentation
No rule bypass due Extension Headers

Handle ICMPv6 stateful

Check for harmful ICMPv6 content

Test Setup


sniff here!
2001:db8:1::2
2001:db8:1::1
www
ping
Angriffslaptop
Firewall
Server
2001:db8:2::1
2001:db8:2::2

YES

Please do this at home!

Filter bypass due EH and/or Fragmentation

- Test bypass techniques to open port:

```
firewall6 eth0 2001:db8:2::2 80
```

- Test bypass techniques to filtered port:

```
firewall6 eth0 2001:db8:2::2 22
```

Test results

All pass

ICMPv6 & Extension Header support

- Test what the firewall supports:

```
implementation6 -p eth0 2001:db8:2::2
```

Test results (Default settings)

- Cisco
  - only Source Routing Option is dropped
  - all extension header pass
- Fortinet
  - all extension header pass
  - Source Routing Option is not dropped
- Juniper
  - only Source Routing Option is dropped
  - all extension header pas
  - all ICMPv6 packets get through

Fragmentation Resource Issues

- CPU/RAM exhaustion tests:

```
for TEST in `seq 1 33`; do
  timeout -s KILL 60 \
  fragmentation6 -p -f eth0 \
   2001:db8:2::2 $TEST
done
```

Test results

All are shaky, showing small/medium impact on packet forwarding

Testing anti-spoofing protection

- Network vendors call this the RPF check:

```
thcping6 eth0 2001:db8:2::ab9a
          2001:db8:2::2
```

Test results

Fortinet does not filter the spoofed packets!

Stateful ICMPv6

- TooBig messages not belonging to a connection:

```
toobig6 -u eth0 2001:db8:1::3
        2001:db8:2::2 1280
```

Test results

Juniper does not filter the spoofed packet!

(because of erroneous defaults)

Harmful ICMPv6 packet contents

- TooBig message with impossible small or large values:

```
toobig6 eth0 2001:db8:1::2
     2001:db8:2::2 48

toobig6 eth0 2001:db8:1::2
   2001:db8:2::2 100000
```

Test results

All let this pass

NDP Exhaustion Tests

- Perform NDP Exhaustion attacks with ICMPv6 TooBig and EchoRequest:

```
ndpexhaust26 -c –r eth0 2001:db8:2::
```

```
ndpexhaust26 -c –r -p eth0
        2001:db8:2::
```

Test results

Fortinet & Cisco get 100% CPU

(also after doing vendor recommended settings)

SYN Flooding Tests

- Send SYN packets to port 80 and random ports, send SYN-ACK to random ports, send ACK packets to port 80:

```
thcsyn6 eth0 2001:db8:2::2 80
thcsyn6 eth0 2001:db8:2::2 x
thcsyn6 -S eth0 2001:db8:2::2 x
thcsyn6 -A eth0 2001:db8:2::2 80
```

Test results

All get 100% CPU

(also after doing vendor recommended settings)

At some point in the test:

lost all IPv6 filter rules, defaulted to open, not visible in GUI

In Conclusion …

Hints on how to filter IPv6 on firewalls

- http://heise.de/-1851747

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