Welcome to

# Everything you need to know about IPv6 security I can manage in 30min

## IPv6 Day Copenhagen November 2017

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramshoej@Github

# Overview of IPv6

oh well, not everything I guess, but hopefully a little overview

- Parallels relevant for security
- Known IPv6 problems
- IPv4 attack kits and tools
- IPv6 attack kits and tools
- Resources

# Implications


For an IPv4 enterprise network, the existence of an IPv6 overlay network has several of implications:

- The IPv4 firewalls can be bypassed by the IPv6 traffic, and leave the security door wide open.
- Intrusion detection mechanisms not expecting IPv6 traffic may be confused and allow intrusion
- In some cases (for example, with the IPv6 transition technology known as 6to4), an internal PC can communicate directly with another internal PC and evade all intrusion protection and detection systems (IPS/IDS). Botnet command and control channels are known to use these kind of tunnels.

You ALREADY have IPv6, so better check it!

# Parallels relevant for security

IPv4 came from the old internet, IPv6 is also quite old

- IPv4 has ARP, IPv6 has NDP - layer 2
- IPv4 firewalls dont care about ARP
- IPv6 firewalls must allow ICMPv6
  `https://home.nuug.no/~peter/pf/newest/icmp6.html`
- IPv4 has small subnets, typically /24s on LAN
- IPv6 has /64s - which are quite a lot of addresses

and of course all higher level attacks, PHP and SQL injections stay the same

# ICMPv6 has more

Starting from the bottom

- Autoconfiguration - what is the network prefix
- Duplicate Address Detection - can I use this address
- Neighbor Discovery - which neighbors exist
- Link layer addresses - ”ARP” for IPv6
- Neighbor Unreachability Detection, or NUD - neighbors still alive

all of these can of course be a target

Hint: segmentation is always good

# ICMPv6 sample rules

```
## allow icmp6 for getting address using IPv6 autoconfiguration from router
pass inet6 proto ipv6-icmp all icmp6-type routeradv
pass inet6 proto ipv6-icmp all icmp6-type routersol

## allow icmp6 for getting neighbor addresses
pass inet6 proto ipv6-icmp all icmp6-type neighbradv
pass inet6 proto ipv6-icmp all icmp6-type neighbrsol

## allow icmp6 echo, not required, but sometimes nice
pass in inet6 proto ipv6-icmp all icmp6-type echoreq

## pass icmp-types: unreachable, time exceeded, parameter problem
pass in inet6 proto ipv6-icmp all icmp6-type 1 3 4
```

Also, ICMPv4 allow types 3,4,11,12 thank you!

3 unreach Destination unreachable

4 squench Packet loss, slow down

11 timex Time exceeded

12 paramprob Invalid IP header

# Known IPv6 problems

- Type 0 routing header - was a problem, could inject traffic
  Deprecation of Type 0 Routing Headers in IPv6 RFC-5095
  https://tools.ietf.org/html/rfc5095
- Big subnets, on linknets, use smaller such as /126

# IPv4 attack kits and tools

We had lots of hacker tools earlier for IPv4, oldish, libnet based:

- libnet network packet assembly/injection library
- ISIC IP stack integrity checker
- SING Send ICMP Nasty Garbage
- Nemesis command line IP stack, send IP without coding
- Scapy Python interface to network packets, generic

# IPv6 attack kits and tools

Generic tools which support IPv6:

- hping3 `http://www.hping.org/`
- Nping `https://nmap.org/nping/`
- Scapy `http://www.secdev.org/projects/scapy/`
- ERNW Loki `https://www.ernw.de/research/loki.html`

Specialised tools:

- THC IPv6 attack toolkit `https://github.com/vanhauser-thc/thc-ipv6`
- SI6 Networks' IPv6 Toolkit A security assessment and troubleshooting tool for the IPv6 protocols `https://www.si6networks.com/tools/ipv6toolkit/`
- Chiron is a multi-threaded tool written in Python and based on Scapy. `https://www.secfu.net/tools-scripts/`

# THC IPv6 [0x03] some example tools

- - parasite6: icmp neighbor solitication/advertisement spoofer, puts you as man-in-the-middle, same as ARP mitm (and parasite)
- - alive6: an effective alive scanng, which will detect all systems listening to this address
- - dnsdict6: parallized dns ipv6 dictionary bruteforcer
- - fake_router6: announce yourself as a router on the network, with the highest priority
- - redir6: redirect traffic to you intelligently (man-in-the-middle) with a clever icmp6 redirect spoofer
- - toobig6: mtu decreaser with the same intelligence as redir6
- - detect-new-ip6: detect new ip6 devices which join the network, you can run a script to automatically scan these systems etc.
- - dos-new-ip6: detect new ip6 devices and tell them that their chosen IP collides on the network (DOS).
- - trace6: very fast traceroute6 with supports ICMP6 echo request and TCP-SYN

- - flood_router6: flood a target with random router advertisements
- - flood_advertise6: flood a target with random neighbor advertisements
- - exploit6: known ipv6 vulnerabilities to test against a target
- - denial6: a collection of denial-of-service tests againsts a target
- - fuzz_ip6: fuzzer for ipv6
- - implementation6: performs various implementation checks on ipv6
- - implementation6d: listen daemon for implementation6 to check behind a fw
- - fake_mld6: announce yourself in a multicast group of your choice on the net
- - fake_mld26: same but for MLDv2
- - fake_mldrouter6: fake MLD router messages
- - fake_mipv6: steal a mobile IP to yours if IPSEC is not needed for authentication
- - fake_advertiser6: announce yourself on the network
- - smurf6: local smurfer
- - rsmurf6: remote smurfer, known to work only against linux at the moment

- - sendpees6: a tool by willdamn(ad)gmail.com, which generates a neighbor solicitation requests with a lot of CGAs (crypto stuff ;-) to keep the CPU busy. nice.
- - thcping6: sends a hand crafted ping6 packet

and more tools for you to discover

# IPv6 scanner tools

Regular pentesting scanner tools with IPv6 support:

- Nmap (”Network Mapper”) port scanner and accompanying software Nping, Ndiff, Ncat https://nmap.org/ has support for IPv6. Due to most subnets being /64 it cannot perform a full subnet scan, just too many IPs.
- Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.

# Questions?

Henrik Lund Kramshøj hlk@zencurity.dk

Need DDoS testing or pentest, ask me!

You are always welcome to send me questions later via email

Did you notice how a lot of the links in this presentation use HTTPS - encrypted

# Further IPv6 Security Resources

- TROOPERS conference `https://www.troopers.de/`
- Good article with more links `https://insinuator.net/2015/06/is-ipv6-more-secure-than-ipv4-or-less/`
- ERNW - excellent information about security and IPv6 too `https://www.ernw.de/tag/ipv6/index.html`

Feel free to send me information about packet tools, love learning new ones ☺