haxpo @ hitb

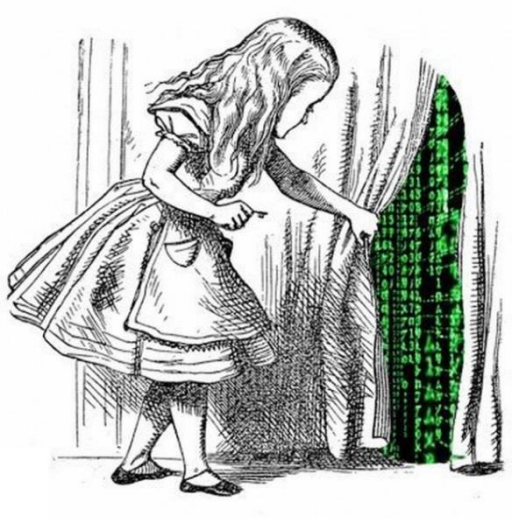
ERNW
providing security.

Penetration Testing in the Age of IPv6

Jayson Salazar
jsalazar@ernw.de

Rafael Schaefer
rschaefer@ernw.de

Road Map

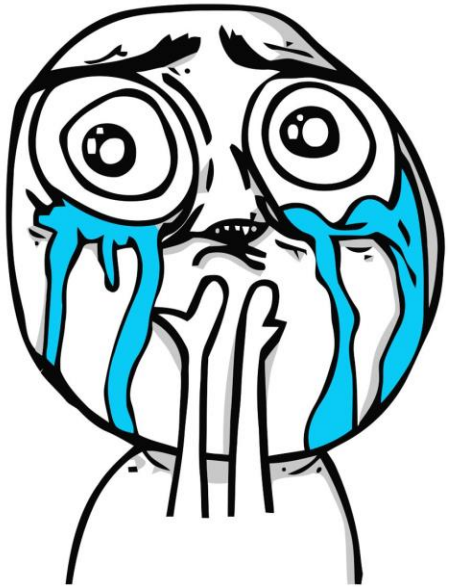


- Why IPv6 Penetration Testing?
- Introduction to IPv6, Core Protocols
- Attack Surface of IPv6 Networks
- IPv6 Compared to IPv4
- Tools of the Trade
- **DEMOS**
- Conclusions

Why IPv6 Penetration Testing?

Increasingly popular and astonishingly complex

The IPv6 Vision



- **Everything** gets a networking interface!
- Personal **appliances** are increasingly incorporating **networking capabilities**.
- Concrete efforts are being directed towards materializing the "**Internet of Things**."
- **IPv6 deployment** has been slowly but **steadily taking off**.

Two Questions come to Mind, though

- Is IPv6 **understood** sufficiently and **mature enough** for deployment?
- Do we have the **know-how** for **securing** such **shape-shifting networks**?

Source	Destination	Protocol	Len	Info
fe80::8271:1f06:54c2:6f0	ff02::1	ICMPv6	142	Router Advertisement from 80:71:1f:c2:06:f0
2001:67c:6ec:1620:f482:8175:abb1:6079	ff02::1:ffc2:6f0	ICMPv6	86	Neighbor Solicitation for fe80::8271:1f06:54
fe80::1c0a:bba2:a026:e0db	ff02::1:ffc2:6f0	ICMPv6	86	Neighbor Solicitation for fe80::8271:1f06:54
2001:67c:6ec:1620:f482:8175:abb1:6079	ff02::1:ffc2:6f0	ICMPv6	86	Neighbor Solicitation for fe80::8271:1f06:54
fe80::1c0a:bba2:a026:e0db	ff02::1:ffc2:6f0	ICMPv6	86	Neighbor Solicitation for fe80::8271:1f06:54
fe80::8271:1f06:54c2:6f0	fe80::da9d:67ff:fe98:eca6	ICMPv6	86	Neighbor Solicitation for fe80::da9d:67ff:fe
fe80::8271:1f06:54c2:6f0	fe80::da9d:67ff:fe98:eca6	ICMPv6	78	Neighbor Advertisement fe80::8271:1f06:54c2:
2001:67c:6ec:1620:f482:8175:abb1:6079	ff02::1:ffc2:6f0	ICMPv6	86	Neighbor Solicitation for 2001:67c:6ec:1620:
fe80::6154:4138:fb5a:163	ff02::1:ffc2:6f0	ICMPv6	86	Neighbor Solicitation for fe80::8271:1f06:54
2001:67c:6ec:1620:8470:56a5:142b:caac	ff02::1:ffc2:6f0	ICMPv6	86	Neighbor Solicitation for 2001:67c:6ec:1620:
fe80::1c0a:bba2:a026:e0db	ff02::1:ffc2:6f0	ICMPv6	86	Neighbor Solicitation for fe80::8271:1f06:54
2001:67c:6ec:1620:da9d:67ff:fe98:eca6	ff02::1	ICMPv6	62	Echo (ping) request id=0xf7c6, seq=0, hop li
2001:67c:6ec:1620:da9d:67ff:fe98:eca6	ff02::1	ICMPv6	78	Neighbor Advertisement 2001:67c:6ec:1620:da9

Introduction to Ipv6

Protocols Running the Show

What's New in IPv6? - I

- Several things have changed.
- Yes, the **HUGE address space** is the most well-know one.
- But, we also have the IPv6 **Extension Headers**

What's New in IPv6? - II

- Router Advertisements and the **Neighbor-Discovery** protocol
- Multicasting plays a major role in IPv6
- There are new complex beasts such as the **Multicast Listener Discovery** protocol

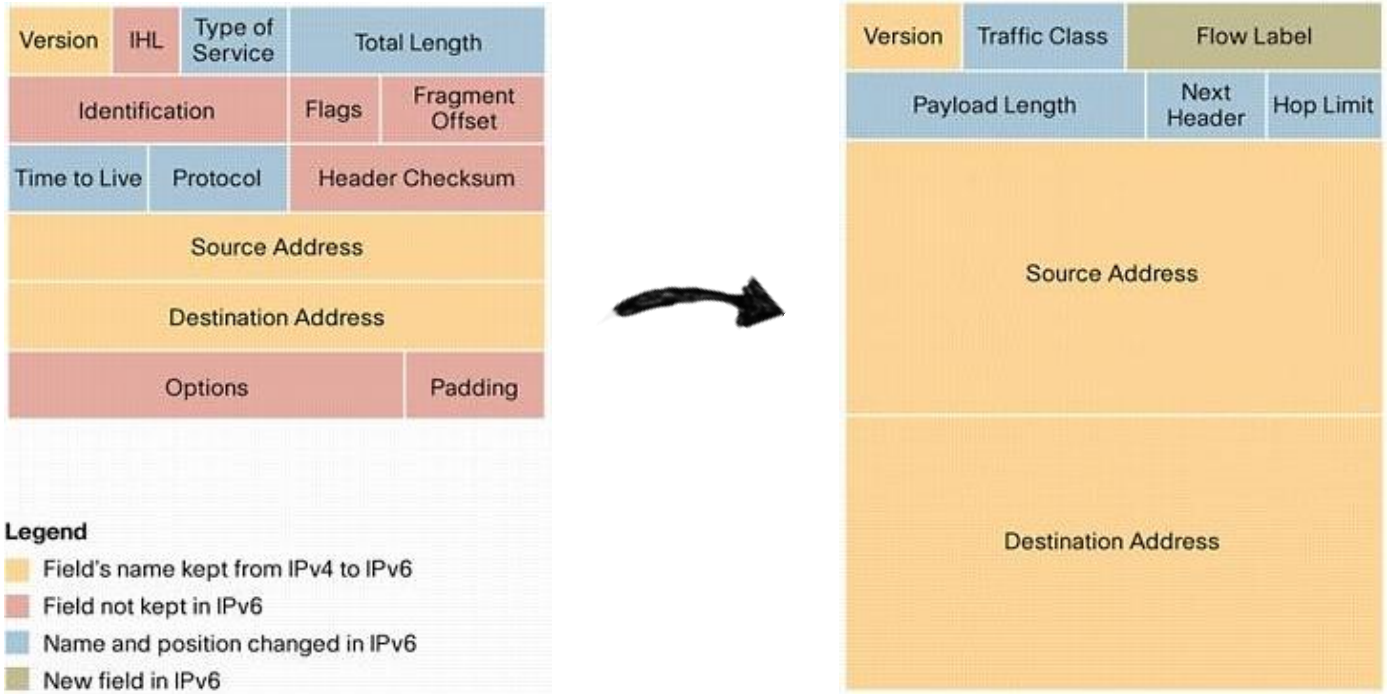
IPv6 in a Nutshell - I

- Networking is still networking, **BUT**
- Bigger **address-space**, **no NAT** needed or possible
- **ICMP** was **overhauled**, is the basis for other protocols
- **Oversimplifying**, ND is to IPv6 what ARP was to IPv4
- **ND** encompasses other minor **sub-functionalities**

IPv6 in a Nutshell - II

- **ND** is **more complex** than ARP
- **MLD** was created and **plays** a '**major**' role in IPv6. It's highly **complex**, often misunderstood and has some serious scalability **issues**.
- Half the **action** in **IPv6** happens on the **Local-Link**
- So, **what** are the **attack vectors** in **IPv6's** expanded attack surface?

A Look at the IPv4 and IPv6 Headers



ICMPv6 101

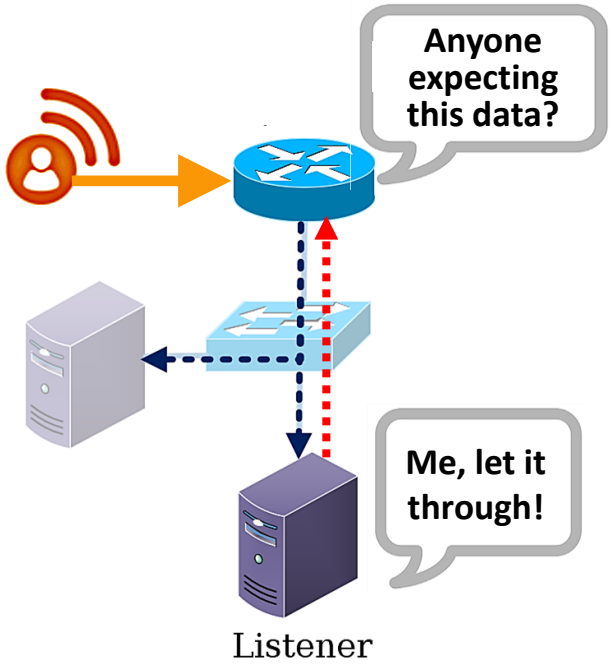
- First specified in **RFC 2462**, latest in **RFC 4443**.
- **ICMPv6** is an **integral** part of every **IPv6** implementation, the foundation of other protocols.

Type(Value)	Description
1	Destination Unreachable (with codes 0,1,2,4)
2	Packet too big (Code 0)
3	Time Exceeded (Code 0,1)
4	Parameter Problem (Code 0,1,2)
128	Echo Request (Code 0)
129	Echo Reply (Code 0)
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solitication
136	Neighbor Advertisement
137	Redirect

Neighbor Discovery 101

- **IS** the **soul** of the **Local-Link**
- ND's **duties**:
  - **Neighbor** Discovery
  - **Router** Discovery
  - **Prefix** Discovery
  - Parameter Discovery
  - Address **auto-configuration**
  - **Next-Hop** Determination
  - **Duplicate** Address **Detection**

Multicast Listener Discovery 101



- The **Querier** sends **periodical Queries** to which Listeners with reportable addresses reply.
- The **Querier** does **not learn which** or **how many** clients are interested in which sources.
- The **Querier** uses reported information for deciding what **ingress data** to **forward**.

haxpo @ hitb

ERNW providing security.

Attack Surface in IPv6 Networks

IPv6, a Fancy Code-Word for Excruciating Complexity

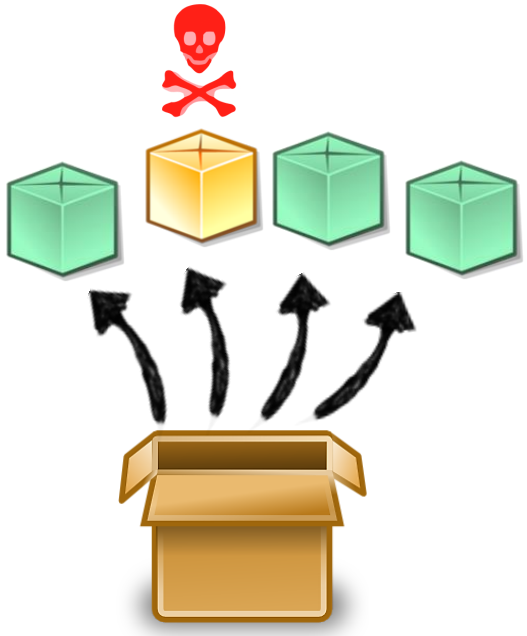
Host-Level Discrepancies

- Unexpected **differences** in **kernels** and IPv6-Stacks behavior.
  - Should packets with source-address 1 be processed on an external interface?
- These differences **lead** to **lack** of awareness with respect to **IPv6 hardening** in **different platforms**
- Also, **services** must often be **configured differently**. Hence, **admins** usually **slip**. E.g. services listening on all IPv6 capable interfaces.

Even Applications Behave Differently

- **Applications** working appropriately in IPv4 **usually lack IPv6 security capabilities**, mostly due to having been untested.
- One such example is the **Filezilla** server, whose **autoban** functionality **doesn't work** with **IPv6**.
- http://blog.webernetz.net/2014/05/14/filezilla-server-bug-autoban-does-not-work-with-ipv6/

Evil Fragmentation and Extension Headers



- All **Black-Listing** approaches to security controls **have** a **hard time** in **IPv6** networks.
- Mostly due to **extension-headers** and **fragmentation**.
- But also because of **ambiguities** in the RFCs
- This makes **possible** the **evasions** of IDPS devices and security mechanisms such as DHCPv6 Guard and RA-Guard.

Don't Forget Profiting from the Protocols

- **ICMPv6**, **ND** and **MLD** are **perfect** candidates for performing **reconnaissance**.
- **Complex protocols** with complex packet structures such as **MLD** make **perfect** targets for performing **DoS attacks**.
- A **poorly hardened Local-Link** in an IPv6 network makes leveraging **ND** for **malicious purposes**, e.g. MitM attacks.

By-Passing ACLs

- **ACLs** are most **effective** when the characteristics of **undesired behavior** are **clear**.
- **IPv6 provides** a **great** deal of **flexibility**, one does not have to be content with a ‘standard deployment’.
- However, this very **flexibility** is one **major enemy** of **ACLs** based filtering.
- **Which** packets **should be rejected**?
  - Those coming from a certain address?
  - With one extension-header or two?
  - Fragmented or not fragmented?

Fiddling with ND Messages

- **Fill**, and **keep filled**, the **Neighbor-Cache** of a legitimate host in the network.
- Reply with **spoofed Neighbor-Advertisements** to **Neighbor-Solicitations**.
- **Unsolicited** Spoofed **Neighbor-Advertisements** and **Neighbor-Solicitations**.
- **Flooding** hosts and causing a **DoS consumption** due to poorly implemented IPv6 stacks.
- Remember, the **Local-Link** is "**trustworthy**"

Playing with Router Advertisements

- **Router-Advertisements** are, as part of auto-configuration approach, **fundamental** part of IPv6.
- Once again, the **Local-Link** is considered **trustworthy**!
- A potential **attacker** can send **Rogue-RAs** into the network in order to cause **DoS** conditions or redirect traffic due to **host** using the **information** contained therein.
- **Lots** of **DoS conditions** to be found here!

IPv6 Compared to IPv4

The Good, the Bad and the Ugly

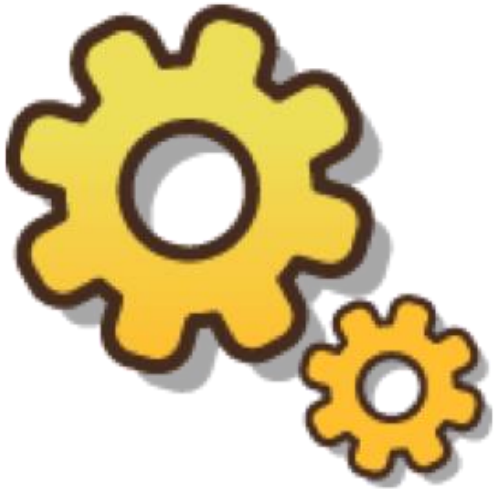
IPv6 vs. IPv4 some Numbers

Alexa Top	IPv6 enabled	Prozent
10	5	50%
100	32	32%
1000	162	16.2%
10000	955	9.55%
100000	8030	8.03%
500000	35041	7.01%
1.000.000.	...	...

So, What do we Find when we Look Further?

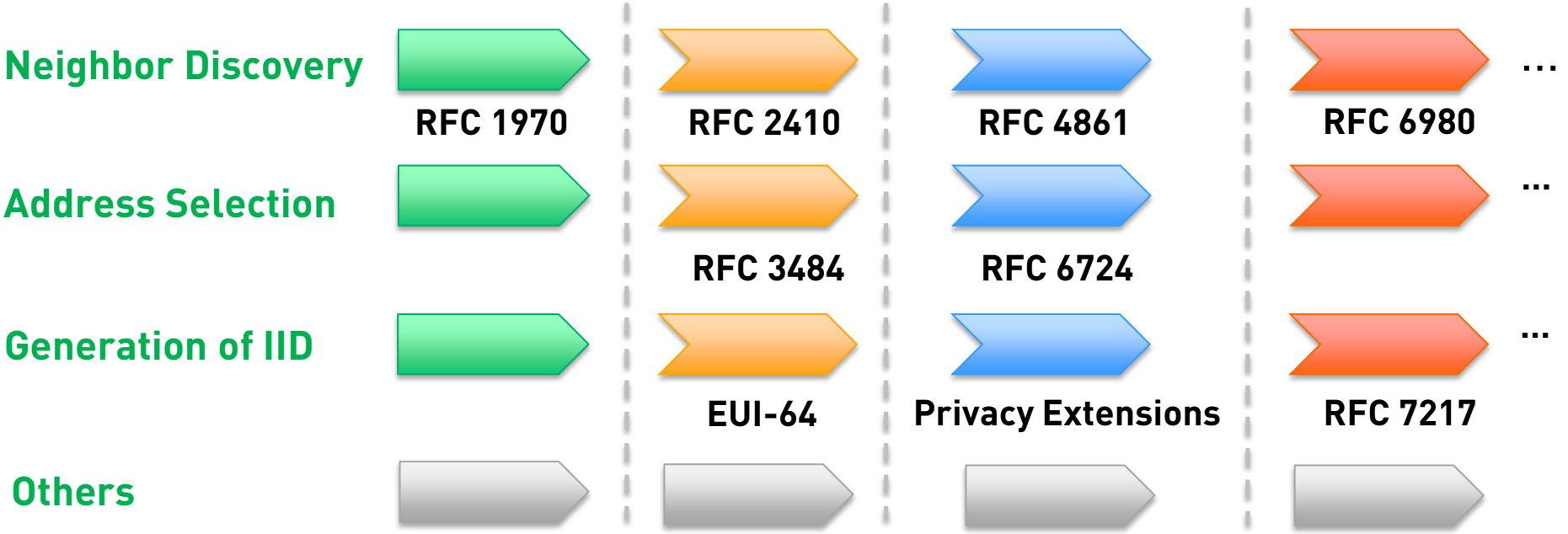
IPv6			IPv4		
PORT	STATE	SERVICE	PORT	STATE	SERVICE
22/tcp	open	ssh	80/tcp	open	http
			443/tcp	open	https
9090/tcp	filtered	zeus-admin			

Attacking Node Provisioning



- **IPv4** has been more or less a **stable** for the **last decade**.
- This **isn't** the **case** with **IPv6**
- **IPv6's vision** is one of **automation**, where your **fridge** can easily **join** the **cyber-party** called IoT.
- But, **what happens** when said **devices** present **heterogeneous** behavior?
- What always happens … **the network breaks**!

There are several IPv6 Stacks



What can we do about It?

Nothing!

What can we do about It?

- **Read** the **specifications** of your core **devices**!
- **Ask** the vendors for their **REAL security features**
- **Harden** your **network**

- **IPv6 IS NOT plug-and-play!**

- **Stay updated** with regard to IPv6:
  ERNW's hardening guides for IPv6

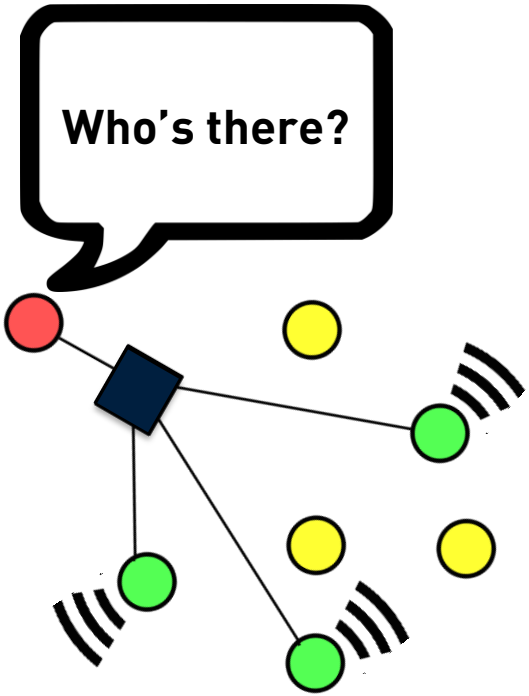
Why is IPv6 so Hard?

- **Trust model** and **automatized** provisioning.
- **Complexity**
- **Lack** of **awareness** and **understanding** of the technologies involved
- Stack **heterogeneity**
- **Limited resources** available to **defenders**

Tools of the Trade

How to Interact with the IPv6 Stack

Profiting from IPv6 for Reconnaissance



- **Leverage** ICMP as usual, **ICMPv6**.
- **IPv6** has 'done **away** with **broadcasting**', **employ multicasting** for host discovery.
- There's one protocol we haven't talked about, **MLD**. Every IPv6 host must reply to and process messages associated with the **Multicast-Listener-Discovery** protocol
- **Fragmentation** can help with **tricking systems** into replying to ICMPv6 ECHO-Requests.

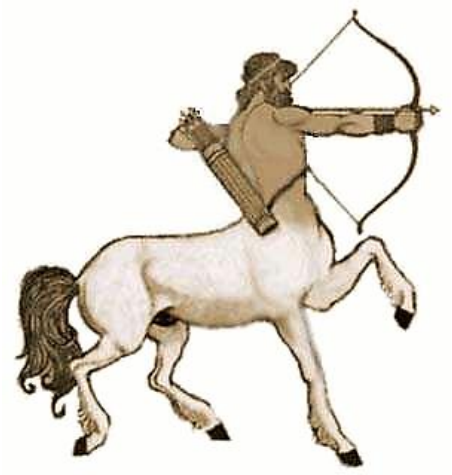
Some Well-Known Attacking Frameworks

- The **Hackers' Choice THC-IPv6** framework
  - https://www.thc.org/thc-ipv6/
- **Si6 Networks IPv6-Toolkit**
  - http://www.si6networks.com/tools/ipv6toolkit/
- **Anonios Atlasis' Chiron**
  - http://www.secfu.net
- **Although** they somewhat **overlap**, they also **complement** each other.

The Hackers' Choice IPv6 Toolkit

- A rich set of tools allowing certain interactions with IPv6 and its associated protocols.
- Although easy to use, it can hardly be customized
- Some interesting tools:
  - alive6
  - dnsrevnum6
  - ndpexaust
  - fake_router
  - flood_router
  - fake_advertise6

The Chiron IPv6 Testing Framework



- **Chiron** offers **several modules** geared towards different potential **attack vectors**:
  - IPv6 Scanner
  - IPv6 Link-Local Message Creator
  - IPv4-to-IPv6 Proxy
- Makes **no decisions for you** regarding the validity of the packets, it simply is IPv6-aware.
- Really **flexible**, but due to being written in **Python** and based on **Scapy** can be easily customized.

Good Ol' NMAP

- IPv6 host **fingerprinting** is a bit **immature** but **does the job** most of the time
- Useful **plugins**:
  - Targets-ipv6-multicast-mld
  - IPv6-ra-flood
  - Targets-ipv6-multicast-invalid-dst
  - Targets-ipv6-multicast-echo
  - IPv6-node-info
  - Resolveall

Internet of Things? Crash All the Things!

http://core0.staticworld.net/

- More like, **Internet** of **Broken Things**!
- If they are **connected** they have an **IPv6 stack**
- If they have an **IPv6 stack** they have **data buffers**
- If they have **data buffers**, **someone slipped** up
- If **someone slips**, attackers **profit**

- **Fuzzing** IPv6 stacks is incredibly important for empirically assessing the robustness of devices we rely on.

Metasploit and IPv6

- Several reconnaissance and post-exploitation modules support IPv6
- **It isn't** any **harder** than in IPv4
- Useful IPv6 modules:
  - auxiliary/gather/dns_srv_enum
  - auxiliary/scanner/discovery/ipv6_multicast_ping
  - auxiliary/scanner/discovery/ipv6_neighbor
  - auxiliary/scanner/discovery/ipv6_neighbor_router_advertisement
  - Good number of IPV6 payload-handlers for Meterpreter

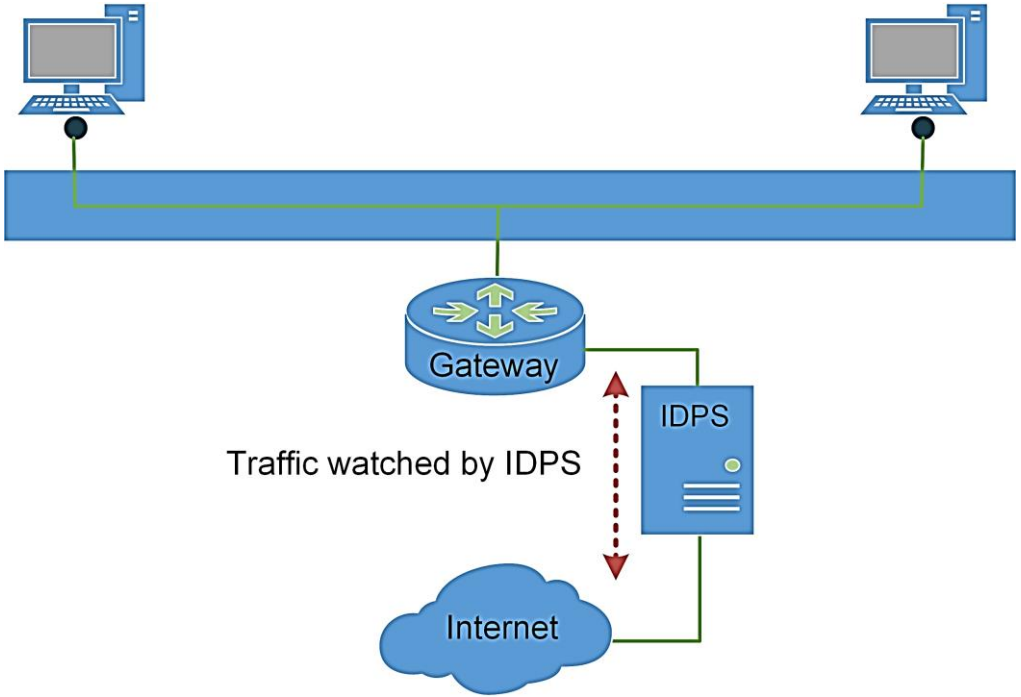
Web @ IPv6

- Enough networking, **what** do we do **web-penetration testing** with?
- There are **several alternatives**:
  - As usual, BURP
  - Arachni for automated tests
  - SQLMap for your post-exploitation needs
  - For getting the big picture, Nessus
- For more information see: Penetration Testing Tools that Support IPv6

DEMO I – Behind the Iron Curtains

Evading IDPS Devices with Fragmentation

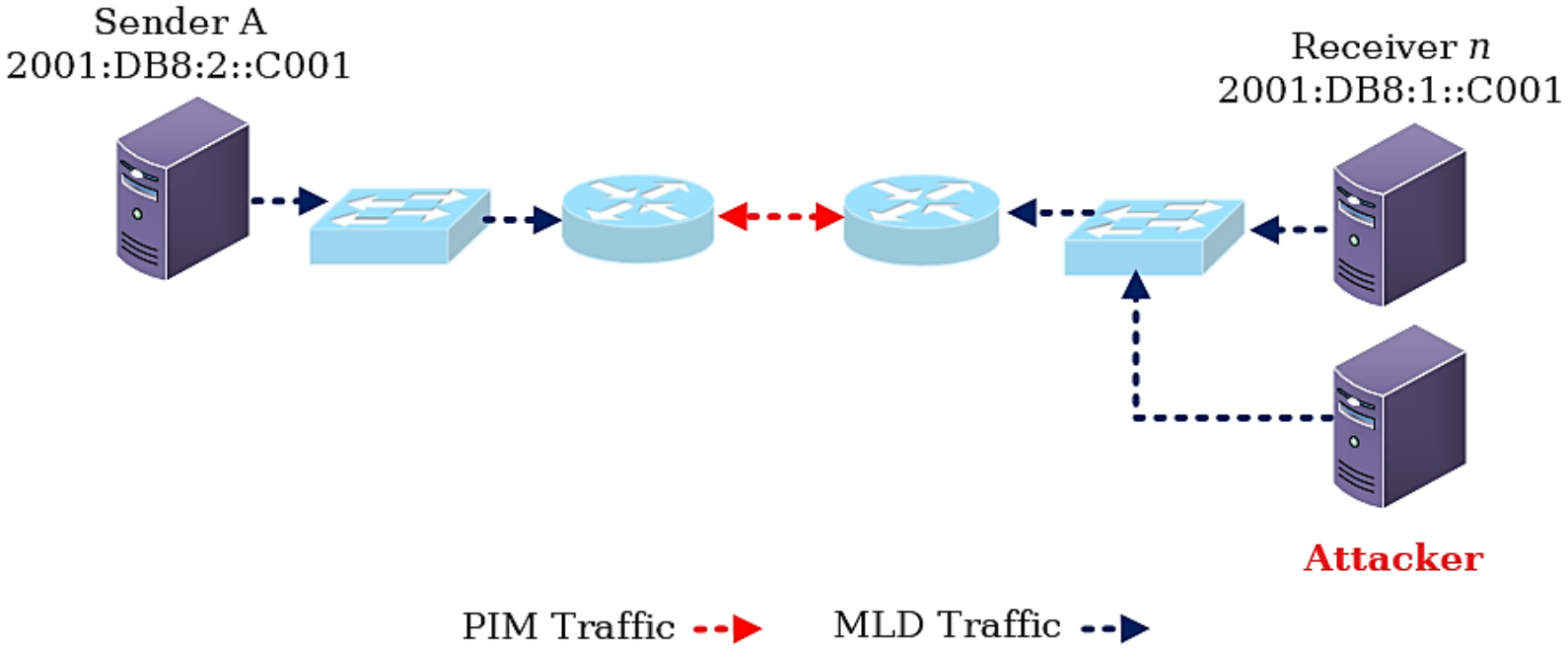
IDPSS Evasion – The Scenario



DEMO II – No Video-Conferencing for You

Abusing MLD to trigger DoS conditions in Routers

MLD - The Scenario



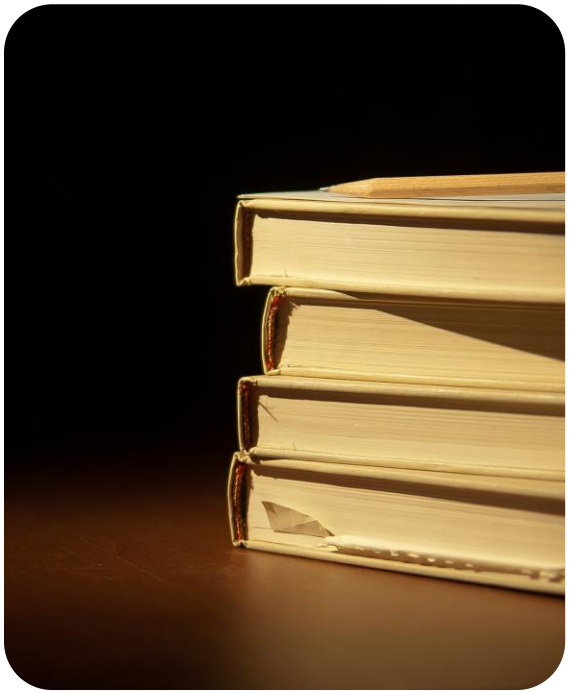
As anything in InfoSec, Stay Informed

- Our Blog with #IPv6 filter, insinuator.net
- IPv6 hackers' mailing-list
- IETF mailing-list, our personal favorite v6Ops.
- NANOG's mailing-list

Conclusions

- **Developments** are still **taking place** within the IPv6 specification; to deal with **IPv6** is to deal with **change** and the **associated** security **risks**.
- **Complexity Kills!**
- **IPv6** is **not IPv4** with a longer address space, **they differ** greatly.
- Since **understanding** is the **father** of situational **awareness**, and situational **awareness** is the **mother** of **security**, study and **understand IPv6**!

Some Resources for those Interested in More



- Regarding tools, this ERNW Newsletter is a good start: Penetration Testing Tools that Support IPv6
- For guidance with respect to hardening IPv6 networks, NIST's Guidelines for the Secure Deployment of IPv6
- TNO's Testing the Security of IPv6 Implementations offers a good, albeit in some cases exaggerated, overview of attack vectors present in IPv6.
- For thorough study of IPv6 security and its intricacies, Hagen's, Cisco's or Microsoft's books should do.

haxpo @ hitb

ERNW
providing security.

Thanks for your Time!

Enjoy Amsterdam!

Jayson Salazar
jsalazar@ernw.de

Rafael Schaefer
rschaefer@ernw.de