

Attacking IPv6

by Gregg Zepp

Improved security measures are part of IPv6; however, is not without its share of vulnerabilities. Because of the need for public servers to be DNS reachable, scanning will still occur. And, when organizations adopt this protocol, they may forget to lock it down or they may feel they have improved security just through its implementation. Security still needs to be configured. Also, many system administrators lack the knowledge on how to properly implement the protocol. They unknowingly cause vulnerabilities by leaving default settings in place or implement incorrect configurations.

For example, filtering rules. Sometimes network hardware does not support IPv6 filtering rules. Filtering IPv6 can sometimes be more critical than IPv4. The reason for this is because the expanded address space often allows the allocation of globally addressable IPv6 addresses to hosts that would normally have to use the private IPv4 addresses specified by RFC 1918. [1]

IPv6 includes a number of new security features improving its defenses over the lack of security in IPv4. The following is a list of IPv6 security features it utilizes for defense.

IPv6 defenses [2]:

- IPsec (Authentication and Encryption) - is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream.
- Secure Neighbor discovery (SEND) - the SEND protocol is a security extension of the Neighbor Discovery Protocol (NDP) in IPv6. NDP replaces IPv4 ARP and is responsible for discovery of other nodes on the link, determining the link layer addresses of other nodes, finding available routers, and maintaining reachability information about the paths to other active neighbor nodes.
- Crypto-generated Address (CGA) - is a method for binding a public signature key to an IPv6 address in the Secure Neighbor Discovery Protocol (SEND).
- Unique Local Addresses (ULAs) - is an IPv6 address in the block fc00::/7 defined in [RFC 4193](#). They are supposed to be used for systems that are not connected to the Internet.
- IPV6_PROTECTION_LEVEL socket option - Enables developers to place access restrictions on IPv6 sockets. [3]

Despite the new security mechanisms in IPv6, a number of vulnerabilities remain in the new protocol. Of course, issues will exist where firewalls and IDS/IPS systems are incompatible with IPv6. However, other security issues are there? What follows is a series of threats to the security of IPv6.

Threats to security of IPv6:

1. Easy to remember addresses might be implemented.
2. Since the lower 64 bits of the address (EUI-64) are derived from the 48 bit MAC address of the network interface, it remains a constant across the network. This raises privacy, tracking, and network mapping concerns (as mapping can

reveal subnet infrastructures). [4] Configuring EUI-64 based IPv6 addresses on a Cisco router is as easy as:
Router(config-if)# ipv6 address X:X::/prefix eui-64, but is not recommended. [5]

3. Source Routing. Mostly used as a diagnostic tool, source routing allows a packet to specify the route, as a list of IP addresses, that should be used to reply to it. This capability can be abused in IP address spoofing attacks by enabling the spoofer to see responses that normally would be routed directly to the spoofed address. Because of this (and other source routing abuses), most routers are configured to drop packets that have source routing information and have been since the mid-90s. Ten years or more would seem to be enough time to ensure that the 'next generation' of IP (IPv6 was originally billed as 'IPng') missed out on repeating these mistakes of the past; sadly, that is not the case.

IPv6 introduces something called a 'routing header' into the protocol as part of the extension headers, which are meant to replace the IPv4 options field. Three types of routing header are defined, one of which is unused (type 1) and another which is only used by Mobile IPv6 implementations (type 2). It is the third (type 0) that is the cause of all the current uproar. Also known as RH0 headers, they contain a list of hosts to be 'visited' on the way back to the source address. It should be noted that the IPv6 RFC mentions IPv4 source routing as part of the description of RH0. [6]

On Cisco routers, source routing is ENABLED by default. Thus, if a network admin did not do the following:
Router(config)# no ipv6 source-routing

... an IPv6 configured router is still susceptible to spoofing attacks. [4]

4. IPv6 still supports multicast. Attackers can identify key resources on a network and attack them. For example, the "all node" address (FF02::1) and "all router" addresses of (FF02::2) and (FF05::2) may be used as new attack vectors. If multicast addresses are not filtered at border routers, they could be readable to outsiders.

Are there any tools to help in the locking down or monitoring of IPv6 in one's network? There are. The following are some tools to assist in the security assessment of one's IPv6 implementation. [7]

IPv6 Security Tools:

- **IPTrap** listens to several TCP ports to simulate fake services (X11, Netbios, DNS, etc). When a remote client connects to one of these ports, his IP address gets immediately firewalled and an alert is logged. It runs with iptables and ipchains, but any external script can also be launched. IPv6 is supported. [8]
- **AESOP** is a TCP-proxy that supports many advanced and powerful features. Aesop makes use of strong cryptography for all its data-transmission up to the end-link. Another powerful feature of Aesop is that Aesop proxies can be transparently stacked into a secure chain. Aesop supports IPv6 and can be used as secure IPv4-to-IPv6 tunnel for TCP connections. Aesop is implemented using multiplexing and is therefore fast and lightweight. [9]

Attacking IPv6:

Recon:

1. The following Windows **PING** command-line options support IPv6 [10]:

- **-i HopLimit**
Sets the value of the Hop Limit field in the IPv6 header. The default value is 128. The `-i` option is also used to set the value of the Time-to-Live (TTL) field in the IPv4 header.
- **-R**
Forces Ping to trace the round-trip path by sending the ICMPv6 Echo Request message to the destination and to include an IPv6 Routing extension header with the sending node as the next destination.
- **-S SourceAddr**
Forces Ping to use a specified IPv6 source address.
- **-4**
Forces Ping to use an IPv4 address when the DNS name query for a host name returns both IPv4 and IPv6 addresses.
- **-6**
Forces Ping to use an IPv6 address when the DNS name query for a host name returns both IPv4 and IPv6 addresses.

2. The following Windows **TRACERT** command-line options support IPv6 [10]:

- **-R**
Forces Tracert to trace the round-trip path by sending the ICMPv6 Echo Request message to the destination, including an IPv6 Routing extension header with the sending node as the next destination
- **-S SourceAddr**
Forces Tracert to use a specified IPv6 source address
- **-4**
Forces Tracert to use an IPv4 address when the DNS name query for a host name returns both IPv4 and IPv6 addresses
- **-6**
Forces Tracert to use an IPv6 address when the DNS name query for a host name returns both IPv4 and IPv6 addresses

The **Netstat** tool displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IPv4 routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), the IPv6 routing table, and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). [10]

WebSite 1: www.ipv6tools.org/ (Tried a couple of IPv6 addresses, but didn't seem to work. Useful?)

WebSite 2: <http://ipv4.whatismyv6.com/> (works)

Scanning Tools:

1. **Nmap**: Since 2002, Nmap has offered IPv6 support. In particular, ping scanning (TCP-only), connect scanning, and version detection all support IPv6. The command syntax is the same except that you also add the `-6` option. Also, in

order to perform an IPv6 scan, both the source (your host) and the target of the scan must be configured for IPv6. It must have an IPv6 address and routing information. And, one must use IPv6 syntax if specifying an address rather than a hostname. An address might look like -> 3ffe:7501:4819:2000:210:f3ff:fe03:14d0, so hostnames are recommended. If your ISP (like most of them) does not allocate IPv6 addresses, free tunnel brokers are widely available and work fine with Nmap. For example, the free IPv6 tunnel broker service at <http://www.tunnelbroker.net>. Other tunnel brokers are [listed at Wikipedia](#). 6to4 tunnels are another popular, free approach. The scan output looks the same as with IPv4, with the IPv6 address on an "interesting ports" line being the only IPv6 give away. [11]

2. **CHScanner**: CHScanner is an ARP, IPv4 and IPv6 network scanner with 31 scan methods: it scans for open ports, protocols, NetBIOS information and Windows shares, SNMP information, and WMI (WBEM) information. It also have the ability to turn on (using Wake-On-LAN) and to shutdown or reboot a remote Windows host. Features an automatic (scriptable) working mode, a hunt mode, a passive mode and the normal scanning mode. [12]

3. **Other Scanning tools**: IPv6 Security Scanner, Halfscan6, Scan6, Strobe, Netcat6

Protocol Analyzer/Packet Capture Tools:

1. **COLD** is both a network analysis tool and a protocol analyzer. It is distributed freely, so its usage is free and the package are freely available. COLD is a network monitoring and protocol analyzing tool which allows to study, maintain and troubleshoot networks by extracting flowing data and printing out the contents and structure. COLD has been developed for troubleshooting, educational, security and commercial purposes only. [13]

2. **The Hacker's Choice (THC-6)** produces a toolkit for analyzing inherent protocol weaknesses of IPV6 and ICMP6, and includes an easy to use packet factory library: freeworld.thc.org/thc-ipv6/

3. **Other Packet Capture tools**: Snort, TCPdump, Solaris Snoop, Windump, WireShark, NetPeek, Sniffer Pro

4. **Packet-Level attack kits**: Spak6, Isic6

Duplicate Address Detection (DAD) / Router Hijacking

Duplicate Address Detection (DAD) is a new networking stack feature not previously available in IPv4. When an address is being added, the DAD detects a duplicate address that is already being used on the network. It sends out a multicast message to the network neighborhood, and requires at least one second to listen for responses from other nodes. If no responses are received in that time, the relocatable IPv6 address is considered free to use. [14] DAD can be used for "neighbor (router) solicitation" to verify the existence of an address to be configured. Neighbor Solicitation messages can be used to determine if more than one node is assigned the same unicast address.

1. **Hyenae** is a highly flexible and platform independent network packet generator and can assist in neighbor solicitation and router hijacking. It allows you to reproduce low level Ethernet attack scenarios (such as MITM, DoS, and DDoS) to reveal the potential security vulnerabilities in a network. Besides smart wildcard-based address randomization and a highly customizable packet generation control, Hyenae comes with a clusterable remote daemon for setting up distributed attack networks. [15]

Packet Forgers: SendIP, Packit, Spak6

DoS Tools: 6tunneldos, 4to6ddos, Imps6-tools

Covert Channel/Backdoor: Relay6, 6tunnel, NT6tunnel, Netcat6, VoodooNet

Citations:

1. Gordon Lyon, *Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning*, (Insecure.com LLC, 2008); 267.
2. Wikipedia.org. Note: Site utilized for the definitions of the list of IPv6 security features.
3. IPv6 Windows developer resource: [msdn.microsoft.com/en-us/library/aa832668\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa832668(v=VS.85).aspx)
4. Whitepaper: <http://documents.iss.net/whitepapers/IPv6.pdf>
5. IPv6 Addressing and Routing Protocols (Cisco): www.pacnug.org/pacnug5/track2/presos/ipv6-2.pdf
6. Site: lwn.net/Articles/232781/
7. Security in IPv6: www.6diss.org/tutorials/security.pdf
8. Site: www.securityfocus.com/tools/2027
9. Site: www.securiteam.com/tools/6I00Q203FU.html
10. Site: computernetworkingnotes.com/ccna_certifications/ipv6_enabled_tools.htm
11. Gordon Lyon, *Nmap Network Scanning: Official Nmap Project Guide to Network Discovery and Security Scanning*, (Insecure.com LLC, 2008); 408.
12. Tool site: pentestit.com/2010/03/14/chscanner-multilayer-multiprotocol-arp-ipv4-ipv6-icmp-network-scanner-tool/
13. Tool site: www.ipv4.it/cold/
14. HP site: docs.hp.com/en/B3936-90079/aphs05.html
15. Tool site: freshmeat.net/projects/hyena/