IPv6 Tools

BUILT-IN TOOLS

Ping / Traceroute

- Windows
  - Same as IPv4 (ping and tracert)
- Unix-like
  - Suffix with 6 (ping6 and traceroute6)
  - Must specific iface for link-local
  - Other commands
    - Try -4 or -6 to force mode

Fun with multi-cast

- http://www.iana.org/assignments/ipv6-multicast-addresses/
- Ping every link-local address
  -
    ```
    ping6 ff02::1%eth0
    ```
- Every router
  -
    ```
    ping6 ff02::2%eth0
    ```

http://www.thc.org/thc-ipv6/

THC IPv6 TOOLKIT

fake_router6

- Sends a Router Advertisement (RA)
  - Specify interface and prefix
  - `2001:db8::/32` is reserved for example networks
- Nodes with autoconf will set an IP
- Many other options

flood_router6

- Evil twin of previous command
- Sends out many thousand RAs
  - All different
- Autoconf devices inundated with IPs

detect-new-ipv6 / dos-new-ipv6

- ICMPv6 duplicate address detection (DAD)
- detect-new-ipv6
  - Prints out any new address
  - Options pipes them to a script (autorun nmap?)
- dos-new-ipv6
  - Responds to every DAD
  - Autoconf theoretically fails

alive6

- Neighbor discovery
- See what nodes are on network

fuzz_ipv6 / exploit6

- Tries sending various malformed packet
- fuzz_ipv6
  - Lets you control what is malformed
  - Send to a specific target
- exploit6
  - Tries known implementation exploits
  - Most of them are fixed already

parasite6 / redir6

- Attempt man in the middle attacks
- parasite6
  - Acts like a IPv4 ARP spoofer
  - Convince other node you own that IP
- redir6
  - Uses ICMPv6 redirect
  - Try to convince node you have better route