IPv6 Implications for Network Scanning

Tim Chown
tjc@ecs.soton.ac.uk

IETF 68, 19th March 2007
Prague

draft-ietf-v6ops-scanning-implications-01

Goals of the document

- Note the properties of the vastly increased host address space in an IPv6 subnet (/64) or site (/48)
    - With respect to traditional network scanning probes or worms as seen today for IPv4 networks
- Describe new methods that attackers may use to locate nodes for further exploitation
    - Given the target host address space is so large
- Make suggestions to administrators to mitigate against the new attack methods
- Publish as Informational

Status

- This is a revised -02 WG draft
  - Revised in response to WGLC
  - Relatively minor edits

- Referenced in two mature v6ops drafts
  - LNP for IPv6 (formerly NAP)
    - draft-ietf-v6ops-nap-06
  - ICMP filtering recommendations
    - draft-ietf-v6ops-icmpv6-filtering-recs-03

Changes since -01

- Changed to new boilerplate
- Split alternative methods to on and off-link
- Added note on learning about prefixes in general
- Added note on CGAs
- Added note on EUI-64s and MAC addresses
- Added note on populating reverse DNS
- Added Teredo host discovery note (2.17, RFC4380)
- Added note on RFC3306 usage
- Updated acknowledgements and references

Next steps?

- Have addressed WGLC comments in -02
  - Now had two revisions/updates as a WG item
- Is there any more to add to the document?
  - Reissue WGLC?
- Comments?