Network Reconnaissance in IPv6 Networks

(draft-gont-opsec-ipv6-host-scanning)

Fernando Gont Tim Chown

IETF 85
Atlanta, GA, USA. November 4-9, 2012

Motivation

- IPv6 address scans usually (and incorrectly) assumed to be unfeasible
  - They are not mitigated as appropriate
- IPv6 host scanning also useful for defensive purposes
  - Penetration-testing tools are incorporating IPv6 support
- There is a clear need of some light in this area

draft-gont-opsec-ipv6-host-scanning

- Initial version analyzed address scanning attacks in IPv6
  - Thorough analysis of the search space
  - Implementation techniques for IPv6 scanners
- Current version
  - Explores other host scanning techniques
  - Merges contents of RFC 5157
  - Formally obsoletes RFC 5157

Main changes since previous version

- Added an applicability table
  - Requires login access? Requires local access?
- Added the following reconnaissance vectors:
  - DNS-advertised hosts
  - Public Archives
  - Application participation
  - Inspection of Neighbor Cache and Routing Table
  - Inspection of system configuration and log files
  - Glean information from routing protocols

Moving forward

- Accept as opsec wg item?