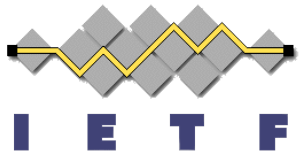
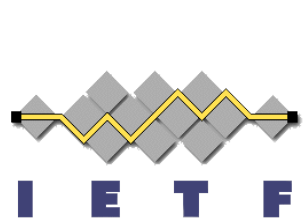
IPv6 Implications for TCP/UDP Port Scanning

Tim Chown
tjc@ecs.soton.ac.uk



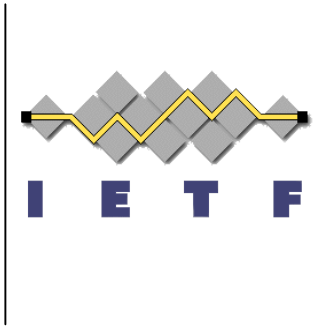
IETF 65, March 23rd 2006
Dallas, TX

Rationale



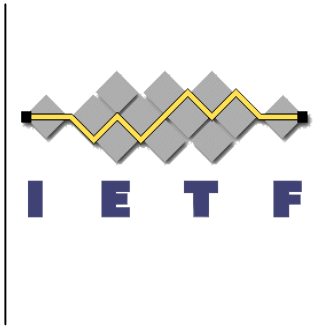
- The goals of the document are currently to
  - Note the properties of the vastly increased host address space in an IPv6 subnet (/64) or site (/48)
    - With respect to traditional port scanning probes
  - Describe new methods that attackers may use to identify target nodes
    - Given the target host address space is so large
  - Make recommendations to administrators to mitigate against new attack vectors
  - Publish document as Informational in the first instance

Traditional port scanning



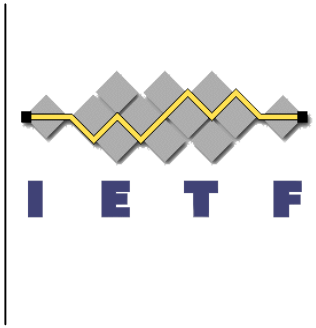
- To scan one port per node in a /64 IPv6 subnet per second would require 500 billion years
  - Can reduce search space from 64 to 24 bits
    - If SLAAC used, knowing :fffe: padding & vendor codes
  - Not practical; unlikely to be used by attackers
- Scans also used by worms
  - Active propagation intra- or inter-subnet
    - Address space used much more densely in IPv4 site
  - Need to identify target nodes
- Used by local admins for ‘defensive’ scanning
  - Market for IPv4 ‘penetration testing’ - what’s IPv6 market?

Recommendations



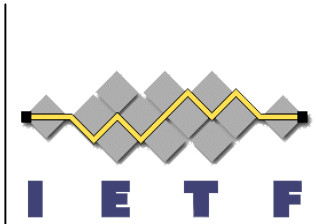
- For administrators
  - Consider subnet/host numbering plans
    - Potential for rolling server addresses
  - Consider where addresses/prefixes may be gleaned
    - Passive or active gathering
    - Mail headers, application access logs, etc
    - Possible site-scope multicast operations
  - Use of RFC3041 to reduce useful lifetime of exposed address information to an attacker
    - Contradicts ease of management
  - Considerations for ‘defensive’ scanning

Comments received on -02



- Title should be about ‘address’ not ‘port’ scanning
  - Or perhaps ‘host address discovery’
- Look at Bellovin paper
  - http://www.cs.columbia.edu/~smb/papers/v6worms.pdf
- Attackers will find a way; don’t suggest IPv6 offers protection; document new attack vectors and offer recommendations
- RFC3041 is a good thing
- Exposed to weakest of protocols in dual-stack network

Next steps?



- Various edits
  - Need to expand Section 3 on attack vectors
  - Add conclusions
- Is direction of document useful?
  - WG adoption?
  - Referenced in two mature v6ops drafts
    - NAP and ICMP filtering
- Comments?