Defcon CTF IPv6 Experiences

Chris Eagle

Background

- Member of group that ran Defcon CTF from 2009-20012 (DC 17-20)
- Historically Defcon CTF had used IPv4 and FreeBSD based targets
- Many teams had infrastructure geared for this scenario
- Wanted to mix things up a little

DC19 / 2011

- 12 Teams
- FreeBSD targets, IPv6 only network
  - Each team had a /64
- Teams provided a cable to their server and a cable to their router

DC19 / 2011

- Many teams had no idea how to properly configure IPv6
  - Most problems a result of blocking ICMPv6
- Many teams had no shellcode for FreeBSD/IPv6
  - No FreeBSD/IPv6 payload support in Metasploit at the time
- At least one team had to scrap its entire firewall/IDS infrastructure as it was v4 only
- ~15Gb pcaps no analysis to date

DC20 / 2012

- Roughly same infrastructure
  - Many teams better prepared
- Teams provided cable to their router and a tap cable from their server
  - Precluded inline security devices
- 20 teams
- ~44Gb compressed pcaps no analysis to date

Summary

- Almost 60 Gb of mostly malicious IPv6 traffic
  - Can make available on request
  - Someday they will be posted publicly
- No analysis to date
  - Mostly application layer attacks
  - No idea whether any IP layer attacks were performed