SafetyNet overview

Marc DeBonis
Systems Architect, Sr.
SETI-MIG
Background

- Major Windows system vulnerability
  - MS03-026 (Buffer overrun in RPC interface)
    - MS Hotfix released July 16th, 2003
    - Affected all version of Windows (NT and up)
  - Very little noise on Techsupport about it
  - Windows user community generally apathetic about it…
Reactive scanning

- Decided to attempt a reactive scan of the VT ip space to determine vulnerability
  - Scanned systems with Eeye tool on July 30th
    - 128.173.x.x and 198.82.x.x
      - Out of 15,000 pingable systems
      - Found over 2,000 vulnerable
  - Posted my results to Techsupport listserv and emailed Network Liaisons (NLs) responsible for the hosts I could find DNS entries for
Reactive scanning

- Continued this scan and report process…
  - August 14th (+2 weeks)
    - 105 systems still vulnerable
  - August 18th (+2.5 weeks)
    - 77 systems still vulnerable
    - Exploit in the wild, so I added trojan scanning
      - 81 systems likely trojaned
  - August 25th (students return) (+3 weeks)
    - 126 systems vulnerable
    - 347 systems likely trojaned
  - September 2nd (+4 weeks)
    - 110 systems vulnerable
    - 179 systems likely trojaned
Issues resulting

- Many people emailed me off list to express their thanks and help in preventing a major incident
- Small minority considered the scanning as an intrusion into their sovereign computing space
- Scanning revealed a developing “walled garden” syndrome across campus
  - Including incorrectly configured firewall settings
- Showed that some NLs are MIA
  - Some systems don’t have appropriate DNS mapping to ip addresses
Concept

- Concept stage September 9th, 2003
- Goal:
  - “To develop a centralized web application for VT computer users to proactively and remotely scan their systems for vulnerabilities and penetration testing”
- Requirements:
  - Modular
  - Centralized
  - Delegated authority model
  - Keep historical data of scans
Development

- Requirements doc defined
  - January 27th, 2004
  - Finalized and sponsored March 3rd, 2004
- Project Sponsor
  - Wayne Donald, IT Security Office, Director
- Systems and network lines ordered
- Project plan developed
  - Timeline for completion July 1st, 2004
SafetyNet overview

Marc DeBonis
Systems Architect, Sr.
SETI-MIG