Wireshark Developer and User Conference

A-8 SMB/CIFS Analysis

June 25, 2012 3:45-5:00pm

Betty DuBois

Chief Network Investigator | DuBois Training & Consulting, LLC

Betty@DTCpackets.com

SHARKFEST **‘12**

UC Berkeley

June 24-27, 2012

Agenda

- Goals of the protocol
- Command categories
- Throughput
- Response time

Goals of the Protocol

- File transfer – it's just like FTP only completely different
  - File, directory, and share access authentication
  - File and record locking
  - File and directory change notification
  - Extended file attribute handling
  - Opportunistic locks
- Protocol dialect negotiation
- Browsing for SMB Protocol
- Network printing

Command Categories

- Session establishment and control
  - Negotiate protocol dialect
  - Session setup / user authentication
  - AD tree connect
- File access
  - Location in directory structure
    - Find
  - Privileges
    - Get info, set info, lock, break (lock), ioctl
  - Access
    - Create, close, read, write

Filters

- **smb2.nt_status > 0** will yield any Error response
  - STATUS_PENDING (0x00000103)
  - STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
  - STATUS_OBJECT_NAME_NOT_FOUND (0xc0000034)
- Follow a session by right clicking **sbmb2.sesid** and apply as filter
- Use “join_domain_fail.pcap” and 445stream242.pcap” for practice

Throughput

- I/O graphs
- TCP Stream graphs
- Delta times in the continuation packets

- Use “FileShare.pcapng” or “445stream242.pcap” to practice

Service Response Time

- Statistics>Service Response>SMB2
  - Request to first response
    - Unchecked “Allow subdissector to reassemble TCP streams” in TCP protocol preferences
  - Request to last response
    - Checked “Allow subdissector to reassemble TCP streams” in TCP protocol preferences

I/O Graphs - Load

- Change Y Axis Unit to Advanced
- It is plotting request/response queue depth over time
  - Client issues lots of commands, plot goes up
  - Server sends responses, plot goes down
- Just like TCP bytes in flight shows how much data has been sent but not yet acknowledged, LOAD tells how much request load the server is under, and how quickly the client moves to next request.

Questions?

- Of the hundreds of places I looked, where did I find the best stuff?
  - http://wiki.wireshark.org/Presentations
    - Ronnie Sahlberg
  - www.snia.org/snia_events
    - Storage Developer Conference. There are presentations archived from 2008-2012
    - Gordon Ross http://www.youtube.com/playlist?list=PL815B920058599FEE&feature=plcp
  - msdn.microsoft.com
  - Google: Server Message Block (SMB) Version 2 Protocol Specification and read the spec :)

Questions?