Network Monitor 3

New ideas for analyzing network traffic
Intro

- Paul Long
  - Technical Evangelist for Network Monitor
  - Previously Network Support in our Critical Response Group (CPR)
  - With MS for last 17 years
History

- Netmon2.x
  - Stale parsers, difficult to update
  - Unsafe DLL architecture for parsers
  - Finding traffic limited to building filters manually
Network Monitor 3!

- Scriptable Parsers (using NPL)
  - Network Monitor Parsing Language
- Process Tracking
- Conversation Tree
- Frame Reassembly
- NM API
- Wireless Management Sniffing
Parsers today

- Easy to Develop Using NPL
- Parsers for All Windows Protocols on MSDN
- Most Common Public Protocols
Simple Ethernet Parser

**Protocol** Ethernet = FormatString("From %s to %s", Src, Dest)
{
    MacAddress Dest;
    MacAddress Src;
    UINT16 Type;
}

**Protocol** Frame
{
    Ethernet myEthernet;
}

**UnsignedNumber** MacAddress
{
    Size = 6;
    DisplayFormat = FormatString("%02X-%02X-%02X
-%02X-%02X-%02X", this[5], this[4], this[3], this[2], this[1], this[0]);
}
Parser future

- More Parsers for
  - Office
  - SharePoint
  - Office Communication Services
- Open Source Project on http://Codeplex
  - Use Parsers and our Engine to Write Tools
  - Submit New Parsers
Narrowing Down Traffic

- Process Tracking
- Conversation Tree
- Find Conversation
- Right Click add to filter
- IntelliSense
- Reassembly
Simple Scripting with NMCap

- NMCap simple capture tool
  - Start/Stop using filters, times, durations
  - Chain and Circular captures
  - Capture Filters. Same as UI
Complex Scripting with API

- NMAPI
  - Start/Stop capture programmatically
  - Filter using same format as UI
  - Inspect data fields
More API Details

- Create a Parser Object
  - NmAddFilter(…, “tcp.port==80”, …)
  - NmAddField(…, “smb.Command”, …)
- To Retrieve Frame Data
  - NmGetFrame(…)
  - NmGetFieldValueNumber8Bit(…)
  - NMEvaluateFilter(…)
Analyzing Data with NMAPI

- NMEventCap – How do I stop on a Event Log?
- TopUsers – How can I find the Top Talkers?
- TopProtocols – Which protocol is the busiest?
- SMBExprrt – Tell me about SMB traffic!
Future of NM3

- Parsers on [http://codeplex](http://codeplex)
- Experts on [http://codeplex](http://codeplex)
- More parsers for public and MS products
- Continued work UI
  - Capturing on Alternate Interfaces
  - Windows ETL Log parsing
  - Views of Frame Data
  - API Enhancements
Get Network Monitor 3.2