Windbgshark: the unified traffic instrumentation tool $^{[1,2,3]}$

1. Virtualized
2. For Windows
3. For vulnerability researchers and reverse engineers
Preamble

There are so many fuzzers, frameworks, code debuggers, etc.

Give me a simple network debugging tool under windows instead.

Why?
I tried physical MITM

* ...or virtual

+ obvious

– no localhost traffic
I tried user-mode magic

* code debuggers
* hooks, binary instrumentation
* LSP

+ stack backtraces available
+ ssl decryption is possible (ospy)

- not handy for traffic manipulation
- x64?
- layer < 7? non-winsock? (ICMP, SMB, ...)
I tried handling network interfaces

* NDIS

+ one driver for all traffic
  - no localhost traffic
  - need to reconstruct TCP/IP stack
I tried some kernel-mode magic

* Windows Filtering Platform
  + unified
  + multi-level (OSI)

  – only starting from Vista

  (reasonable trade-off, TDI on WinXP is almost the same)
We developed windbgshark

...VM-based traffic manipulation tool

* wfp driver as a mechanism (guest OS)
* windbg extension as a control interface (host OS)
* wireshark for packet analysis (host OS)
Theory of operation
Quickstart

> !load windbgshark
> !strace on
> g
...
> !packet 100 +AAAAAAAAA
[look in wireshark]
> g
...

Quickstart
Thanks!

http://code.google.com/p/windbgshark

Questions?