Introduction to Network Sniffing

STL!/unix/usr/group

Tutorial Session

8 May 2024

Grant Taylor & Lee Lammert

Unix Gray Beard **Chief Scientist @Omnitec**

Ubiquitous Technology

- Today, we take tech for granted
  - HW & SW is omnipresent and multi-faceted
  - Vendors like to hide all the details [MS, Apple, et al]
  - Hard to understand all the moving parts [HW & SW], much less how they are connected
- Each device communicates with a number of other devices (aka servers, cloud applications, et al) over a **Network**

Information Networks

- Networks are:
  - Faster than printing paper **or** sneakers
  - Leap huge distances in a single bound
  - Required for people and businesses today
- Networks have:
  - Media (wire or radio)
  - Protocol (UDP or TCP)
  - Port Number (1-65535)
  - Packets of data

Network Problems

- What happens if something is not operating as expected?
  - When a problem occurs, the only information about the problem is probably in a **log** *somewhere*
  - What if the problem cannot be identified with a log entry or the log is not available?
- In many cases, the only way to solve the problem is to actually look at the packet traffic **ON** the network!

Inspecting packets

- Capturing packets on the network uses a network analyzer, protocol analyzer, sniffer, or, ..
- per Wikipedia, the standard term would be **Packet Analyzer**:

  Computer software or hardware that can intercept and log traffic passing over a [digital] network

Using Packet Capture

- By capturing actual packets on the network, it is possible to see what is really being sent instead of pawing through the alerts & logs
- Retrieving the data from those packets, however requires reversing the process used to send then **ON** the network

Practical examples

- Analyze DNS traffic as part of investigating DKIM workarounds.
- Troubleshoot network printing
- Troubleshooting an Xymon client
- Impress your friends
- Learn something new
- Win a bet

Packet capture tools

Free/Open Source

- Tcpdump
- Wireshark
- EtherApe
- Etherfind/Snoop
- WinDump

Paid/Commercial

- Manage Engine
- PRTG IP Sniffer
- Solar Winds
- LiveAction Omnipeek
- Netresec Network Miner
- Steelcentral
- Capsa

This month – installing tcpdump

- apt install tcpdump
- zypper in tcpdump
- yum install tcpdump

- Testing:

  tcpdump -i eth0

- Simple, eh?

Using tcpdump

- The power of tcpdump is in the command switches:

tcpdump [-AbdDefhHIJKlLnNOpqStuUvxX#] [-B buffer_size]
[-c count]
[-C file_size] [-G rotate_seconds] [-F file]
[-i interface] [-j tstamp_type] [-m module] [-M secret]
[--number] [-Q in|out|inout]
[-r file] [-V file] [-s snaplen] [-T type] [-w file]
[-W filecount]
[-E spi@ipaddr algo:secret,...]
[-y datalinktype] [-z postrotate-command] [-Z user]
[--time-stamp-precision=tstamp_precision]
[--immediate-mode] [--version]
[expression]

But WAIT! There's MORE!

- Stay tuned for the next few month for:
  - Installing Wireshark
  - Capturing specific data (e.g. DNS)
  - Using a separate workstation fordata collection to avoid possible issues on the system being monitored
- Solving problems with SLUUG systems

Thank you!

SLUUG Sysadmin Team

Grant Taylor
Unix Gray Beard
Grant Taylor <gtaylor@tnetconsulting.net>

Lee Lammert
Chief Scientist @Omnitec
Lee Lammert <lvl@omnitec.net>