BlackBox

Michael Koerfer – 19.05.2017

Preamble

Despite all the monitoring tolls such as HP OpenView, IBM Tivoli, Multi Router Traffic Grapher (MRTG), Munin, Nagios..., which prepare this data and make it available to the administrator, sometimes you need the data in raw format.

Overview

- Hardware
- Virtualization
- OS + Configuration
- tshark
- Implementation
- Conclusion

Hardware

- Home

- Checkout out a Fujitsu Futro S550-2 Thin Client

- AMD Sempron 200U CPU
- 1 GB RAM
- 1 x 1000 Mbit/s
- > 8 GB CF HDD *extra
- 2 x USB Network 1000 Mbit/s *extra
- Amazon $50

- SOHO

- Checkout out a PC Engines APU.1D Bundle

- AMD Embedded G-Series T40E APU
- 2 GB RAM
- 16 GB MicroSD HDD *extra
- 3 x 1000 MBit/s
- Amazon $300

- Companies

- Checkout out a PowerEdge R230 Rack Server

- Intel® Xeon® E3-1220 v5 - 4 Core
- 8 GB RAM
- 500 GB SATA
- On-Board LOM 1GBE Dual Port
- Dell $1430

Virtualization

- VMWare or VirtualBox*

- Debian Linux or what you want
- Minimal installation, no GUI etc.
- > 1 CPU
- > 1 GB RAM
- > 8 GB VHD
- 3 NIC's
- Follow the next steps and enjoy
- *Nice for a HackLab

OS + Configuration

Debian Version 8.8 aka Jessie

```
- ifconfig "LAN0" -arp promisc 0.0.0.0 up
- ifconfig "LAN1" -arp promisc 0.0.0.0 up
- brctl addbr br0
- brctl addif br0 "LAN0"
- brctl addif br0 "LAN1"
- ifconfig br0 -arp promisc 0.0.0.0 up
```

- To operate the Blackbox via SSH, use a separate network segment. This can be configured manually with ifconfig.

tshark

- Recording raw data with tshark

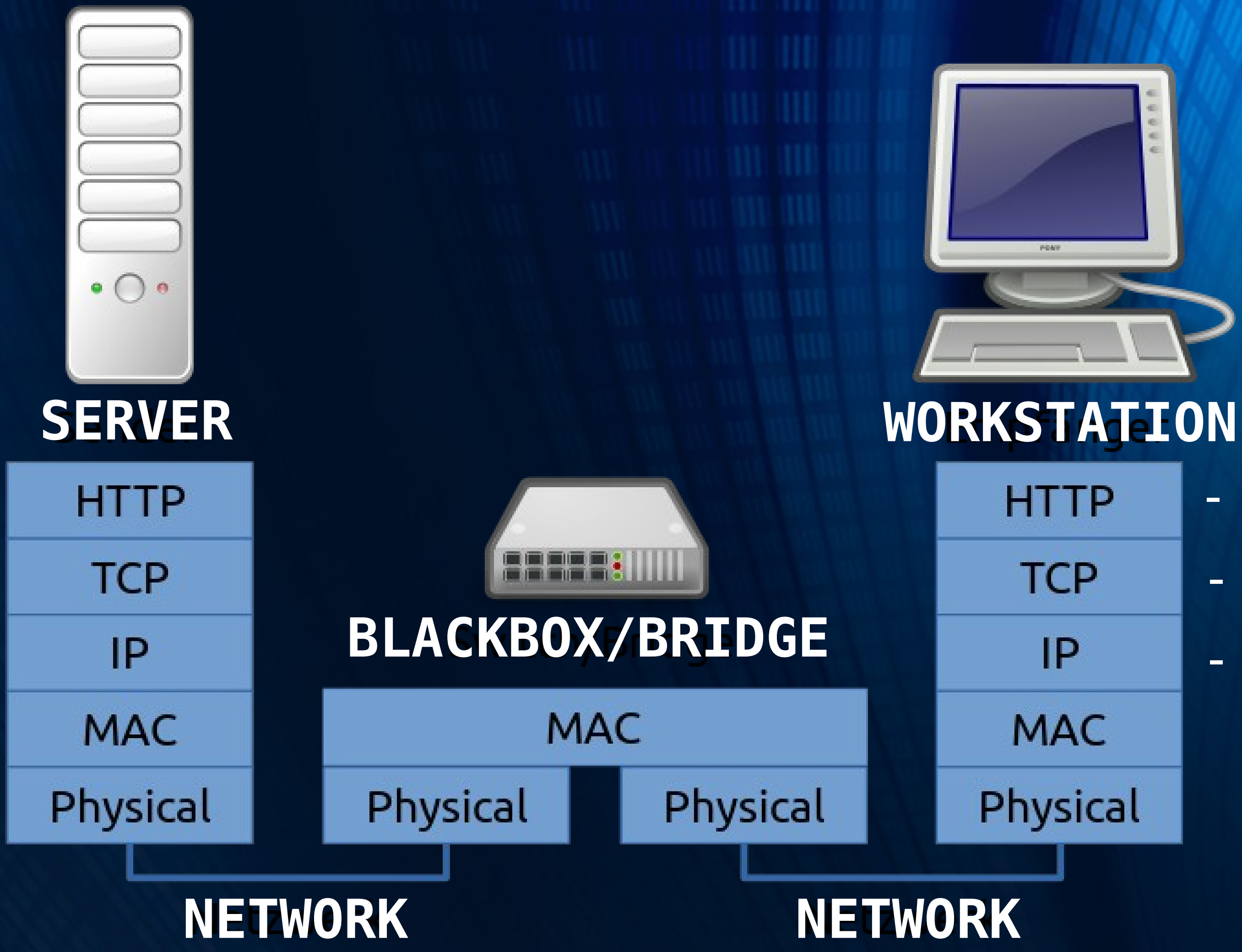
```
- tshark -q -n -b filesize:25000 -w /"path"/"name".pcap -i br0 &
```

- "path" you can customize for local or network storage

- All configuration options

https://www.wireshark.org/docs/man-pages/tshark.html

Implementation



SERVER

HTTP
TCP
IP
MAC
Physical

BLACKBOX/BRIDGE

MAC
Physical
Physical

WORKSTATION

HTTP
TCP
IP
MAC
Physical

NETWORK

NETWORK

- between client and server
- between network segments
- between …

Source: Wikimedia

- Quick to configure
- Easy to virtualize
- Transparent
- Passive element
- Raw data
- Extended and subsequent analysis
- Errors and attacks on devices and the running services can be analyzed live or subsequently.

Live Demo

Questions ????????

Thank you

Author: Michael Koerfer

E-mail: michael_koerfer@posteo.de

Twitter: @D_70WN