How to inspect content of TCP-packages?

# Scope of this task:

We collect data with the TCP dump tool. Inspection and analysis is done with wireshark. Later, we derive a procedure to inspect a Hadoop cluster automatically in order to contribute to the security report.

# Prepare the machines

## Install the tcpdump tool

On the quickstart VM we have tcpdump preinstalled.

$ sudo yum install wireshark

## Install wireshark

$ sudo yum install wireshark

$ sudo yum install wireshark-gnome

## Install nmap

$ sudo yum install nmap

# Inspect open ports

$ sudo nmap -sS -sV -O -PN -p1-65535 127.0.0.1 -oX nmap.out.xml

This scan lasts around 3 minutes.

## Do a testdump

$ tcpdump -i eth6 tcp -w QSVM.dump.pcap

$ wireshark

For unencrypted traffic, the protocol type can be identified, but not for encrypted data.



Now we plan to inspect communication to the navigator services. Specifically, we have some known communication channels as described in this sketch:



<https://www.cloudera.com/documentation/enterprise/latest/topics/cm_ig_ports_cm.html>

Navigator Audit server, Navigator Metadata server, and Activity Monitor are in our scope. Here in our current cluster all three services run on the same host. Relevant ports are:

7187 NMS

7186 NAS

9998 ActMon

9999 ActMon

We use tcpdump on the host and collect traffic data in a file.