BSides Calgary 2017

Title: Using Netflow & Open Source Tools for Network Behavioral Analysis
Presenter: Yves B. Desharnais, MBA, CISSP, PCIP

Instructions for running the demo.

The demo was done under CentOS 7, but the solution was also tested under Ubuntu so most instructions should work on most Linux systems (and potentially other OSes).

1) Install OS
2) Install Fluentd (instructions: https://docs.fluentd.org/v0.12/categories/installation)
   a) Generally as regular user (I remember having issues installing as root)
3) Install other required packages
   a) The default NetFlow plugin, unless using my plugin
      i) `sudo /opt/td-agent/embedded/bin/fluent-gem install fluent-plugin-netflow`
   b) The MariaDB / MySQL package
      i) Dependencies (needs to recompile code)
         (1) `sudo yum install gcc mysql-devel ruby-devel rubygems mariadb-server`
   c) Secure mysql
      i) `sudo mysql_secure_installation`
   d) Install the fluentd mysql plugin
      i) `sudo /opt/td-agent/embedded/bin/fluent-gem install fluent-plugin-mysql-prepared-statement`
   e) Enable/start MySQL (now MariaDB) daemon
      i) `systemctl enable mariadb`
      ii) `systemctl start mariadb`
   f) Allow firewall traffic through local firewall (IPTables, firewalld, etc.)
4) Install demo code
   a) As root, from the unzipped archive folder:
      i) `mv /etc/td-agent/td-agent.conf mv /etc/td-agent/td-agent.back`
      ii) `cp -R etc/td-agent/* /etc/td-agent/`
      iii) `chmod -R 740 /etc/td-agent`
   b) For demo 8, we need to create the databases and users (I would recommend changing the passwords…)
      i) `mysql –u root –p < demo8.sql`
   c) For demo 9, we need to:
      i) Create the database and user: `mysql –u root –p < demo9.sql`
      ii) Create the file structure for our interprocess communications
         (1) `cp -R logmon /`
         (2) `chmod -R 775 /logmon`
      iii) setup the cron jobs, adding line to "`crontab –e`", for example:
         (1) `0 0 * * * * /logmon/cron/ping/sweep.sh # Daily at midnight`
         (2) `*/5 * * * * /logmon/cron/nmap/nmapcronq.sh # Every 5 minutes`
   d) edit the /etc/td-agent/td-agent.conf and to select the right demo include file
   e) run the service
      i) `sudo service td-agent start` (or restart)