EagleX Benutzung im Pool

Linux-Edition

Stand: 2014/11/03 -12-

Dominique Petersen <petersen@internet-sicherheit.de>
Thomas Schyra <schyra@internet-sicherheit.de>
Peter Honerbom <honerbom@internet-sicherheit.de>
Institut für Internet-Sicherheit, https://www.internet-sicherheit.de
Westfälische Hochschule

Inhaltsverzeichnis

Einleitung

Der EagleX-Client ist das mächtige Analyse-Tool des Internet-Analyse-Systems. Mit Hilfe dieses Expertenwerkzeuges können die Daten, die die Sonden sammeln, graphisch visualisiert werden. Für die Benutzung des EagleX-Clients gibt es ein ausführliches Handbuch[1] für die Benutzung.

Da auf einen Server des if(is) zugegriffen wird funktioniert diese EagleX-Edition nur im Pool A4.1.07 des Fachbereichs Informatik und im if(is), kann jedoch nicht von Zuhause oder über das ZIM-WLAN benutzt werden!

EagleX-Client

Es existieren derzeit zwei verschiedene Versionen des EagleX-Clients. Ein reines Java-Programm (Rich Client), welches auf dem Client-PC ausgeführt wird, und eine Web-Version, die im Browser ausgeführt wird. Die Web-Version funktioniert hierbei ähnlich wie die ursprüngliche Java-Version, bietet allerdings ein wenig andere Funktionalität. Für das Praktikum können gerne beide Versionen ausprobiert und verwendet werden. Es ist möglich, dass der Funktionsumfang der Web-Version noch während des Praktikums erweitert wird. Sie werden in diesem Fall per Moodle informiert.

Rich-Client-Version

Installation

Die Installation ist denkbar einfach. Als Erstes wird durch Klick auf „Dash-Startseite" oder über die „Super Taste“ (früher bekannt als „Windows Taste“) das Suchfeld geöffnet. Dort tippen Sie nun „Terminal“ ein und öffnen den gefundenen Eintrag. Dadurch wird eine Konsole geöffnet.

Dann wird ein neues Verzeichnis für den EagleX-Client angelegt (z.B. im Home-Dir):

```
$ cd ~
$ mkdir EagleX
```

1 https://www.internet-sicherheit.de/fileadmin/docs/internet-fruewarn-systeme/ias/IAS-EagleX-Benutzerdokumentation-2.3.pdf

Danach muss das Skript „updateEagleXPool.sh.tar.bz2“[1] herunter geladen (z.B. mit dem Firefox) und im eben angelegten Ordner gespeichert werden.

Das Archiv entpacken:

```
$ cd EagleX
$ tar -xjvf updateEagleXPool.sh.tar.bz2
```

Nun müssen Rechte vergeben werden, damit das Skript ausführbar ist:

```
$ chmod a+x updateEagleXPool.sh
```

Jetzt sind alle notwendigen Schritte für die Installation des EagleX abgeschlossen.

Starten

Als Erstes wird eine mittels „Applikationen -> Zubehör -> Terminal“ eine Konsole geöffnet.

Danach muss in das oben angelegte Verzeichnis gewechselt werden:

```
$ cd ~/EagleX
```

Nun muss nur noch das zuvor installierte Skript ausgeführt werden:

```
$ ./updateEagleXPool.sh
```

Das Skript prüft bei jedem Start, ob es eine neue Version vom EagleX-Client gibt. Wenn ja, lädt es diese herunter und entpackt sie. Danach wird der EagleX-Client gestartet.

Anmeldung

Nach dem Start des EagleX-Clients öffnet sich der Anmeldedialog. Dort müssen die Authentikationsdaten (User und Passwort) eingetragen werden. Der Benutzername ist nach dem Format „pool_nws_X“ (X = Gruppennummer) vergeben. Das Passwort ist nach demselben Format initial vergeben. Nach der ersten Anmeldung muss das Passwort direkt geändert werden! Als Server muss der Hostname „application-server.srv.ifs.if-is.net“ oder die IP-Adresse „10.0.2.40“ eingestellt sein.

1 http://www.internet-sicherheit.de/fileadmin/docs/vorlesungen/nws_praktika/updateEagleXPool.sh.tar.bz2

Web-Version

Achtung: Die Web-Version ist noch im „Beta“-Stadium und beinhaltet andere Funktionen!

Um auf den Web-EagleX zuzugreifen, muss im Browser (Firefox empfohlen) nur der folgende Link eingegeben werden:
https://ias.internet-sicherheit.de/IASWebEagleX/
Da das Zertifikat von StartCom signiert ist, muss dies in manchen Browsern möglicherweise erst noch manuell akzeptiert werden.

Nach dem Laden öffnet sich der Anmeldedialog. Dort müssen die Authentikationsdaten (User und Passwort) eingetragen werden. Der Benutzername ist nach dem Format „pool_nws_X“ (X = Gruppennummer) vergeben. Das Passwort ist nach demselben Format initial vergeben. Nach der ersten Anmeldung muss das Passwort direkt geändert werden!