【译】重踏蜜罐可视化之旅

□ / 2017-07-17 14:01:00 / 浏览数 4663 安全技术 技术讨论 顶(0) 踩(0)

在上篇博客中，我提到过很快会再出篇新的可视化蜜罐文章。但由于一些原因推迟到今日，所以我想对期待这篇文章的读者说声抱歉。我自认为我已经选择了关于可视化蜜罐

问题

在上篇博客中，我已经讨论了可视化蜜罐数据。这次，我发现对于我的Cowrie蜜罐和Dionaea数据来说，最好的选择就是使用 Kippo-Graph和DionaeaFR。

我的上篇博客详细介绍了一些你需要了解的曲折和技巧，这样便于你正常运行 Kippo-Graph和DionaeaFR。但问题是随着底层软件的依赖新版本的发布，
关于曲折和技巧的清单可能会增加或者变动。但最本质的问题却是当大多数底层依赖的软件要更新了，而用来视觉化的包却没有及时更新。

即使你在蜜罐服务器上成功的运行了Kippo-Graph和DionaeaFR，再次重新配置所有东西只是时间问题
。我的习惯是是定期重构我的蜜罐——频率也许是每一个月或二个月 。

你需要了解的是构建新的网络环境或重新安装蜜罐从来都不是问题，这是一个很快的过程（参见上篇博客）。我完成这些大概需要5-10分钟。

每次都得重装前端软件又是一个单独的故事，这也是我开始写本文的原因。

寻找解决方案

在这次案例中，我总结出了最佳实践方案，那就是在虚拟机里安装视觉化软件。在虚拟机中我可以做出任何有助于软件正常工作的调整，并且再也不担心什么时候重构蜜罐

在我决定用那个方法后，突然我就意识到可能存在其他可以使用的视觉化方案。

自从我初步试验了下现代蜜罐网络（MHN）技术后，我就对使用ELK技术栈来可视化我的蜜罐数据非常感兴趣。对于不熟悉ELK技术栈的朋友，这里简单介绍下：ELK技术栈

- E - Elasticsearch
- L - Logstash
- K - Kibana

简而言之，Logstash以不同的形式处理日志文件，然后将数据发送给Elasticsearch索引去分类、组织和检索。最后Kibana提出了一种方法，在浏览器中对存储在Elasticsear

现在，我打算使用本地虚拟机作为可视化服务器成为了可能，同时可搭载ELK。

如果你刚开始使用ELK技术栈组件，我认为最好的入门视频是Minsuk
Heo的这个。尽管有时他的口音很糟糕，但在我看来，这依然是互联网上最好的"从头开始了解ELK"的视频。

尝试ELK

通常情况，ELKstack环境会包含额外用来发送服务器数据到ELK电脑上的组件。Elastic公司提供了Filebeats工具来完成这个操作。这个过程的数据流看起来是这样的：

> Data source(s) —> Filebeats –> Logstash –>Elasticsearch –> Kibana

当我意识到这种数据流方式并不是我想要的方案时，我就知道如果不按照这个流程来，如何去实现这么个效果，这必然是我的第一个难题，因为我的ELK
stack在我的家庭电脑上的一台虚拟机上运行，而我的蜜罐部署在云中。接着这个问题的第二部分出现了，因为我找遍了所有的文档和指导手册，但它们都是以上面那种用法

在Mirko的教程帮助下，我可以给我的Cowrie蜜罐数据构造索引了，然后使用Kibana进行可视化展示。这真的很容易，因为Cowrie可以以JSON格式本地记录其数据。很快

但对于Dionaea来说，使用ELK又是另一个故事了。

Dionaea有个选项是支持数据记录到JSON格式文件的。该文件后缀是yaml，你一定会启用的文件（与Dionaea中其他的服务和handler一样）。在测试过程中，我曾经使用

为了解决这个问题，我决定在本地虚拟机上安装DionaeaFR去观察我的Dionaea数据。 但直到我在推特上向Ignacio
Sanmilan发送了关于Dionaea和MHN的消息，这个问题才感觉快被解决了。第二天，他向我发送了一条链接展示了他完成的最基本可视化效果。那效果太难忘了。在那之后
。

在得知Ignacio能够快速的重组前端界面后，这促使我开始思考是否要制作自己的Dionaea主控界面。但事实证明这比我想象的要困难的多了（很明显我的php很烂）。所以

安装配置

以下是我的honeypot可视化解决方案的运行安装过程的详细信息

VM配置

1. VirturalBox配64位Linux Mint（GuestAdditions）

2. 1处理器 / 3GB RAM / 50GB固态
3. 1个共享文件夹

可选项

如果你通过共享文件夹在VM和主机之间传输数据，下面的命令会有助于你可能遇上的问题。

```
sudo adduser username vboxsf
```

安装步骤

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install curl
sudo apt-get install software-properties-common
sudo apt-get install ubuntu-restricted-extras
```

ELK的安装

ELK stack的安装需要较新的JDK版本。

你可以从这)下载最新的JDK

在写这篇文章前我已经下载了jdk1.8.0_131-linux-x64.tar.gz，现在将这个压缩文件拷贝到/opt文件夹下：

```
sudo cp jdk1.8.0_131-linux-x64.tar.gz /opt
cd /opt
tar -zxvf jdk1.8.0_131-linux-x64.tar.gz
chown -R root jdk1.8.0_131
```

解压后可以删除原始的tar.gz文件了。

下一步，需要安装一些java组件的可选项了。

```
sudo update-alternatives --install /usr/bin/java java /opt/jdk1.8.0_60/bin/java 1
sudo update-alternatives --install /usr/bin/javac javac /opt/jdk1.8.0_60/bin/javac 1
sudo update-alternatives --install /usr/bin/jar jar /opt/jdk1.8.0_60/bin/jar 1
```

java的版本是必须手动设置的，命令如下：

```
sudo update-alternatives --config java
```

所以选择你刚才安装的版本。

如果有需要的话，你可以通过命令行运行它们来进行测试（比如，输入java命令，确保运行了正确的版本）

ELK Stack

有很多方法安装和运行ELK组件。其中一种方式是下载DEB后缀文件的组件，然后通过GDebi安装他们。安装完成后，你可以将组件作为服务运行，并配置成自启动。这过程

在我的初次试用ELK和Cowrie中，我没有使用Logstash。毕竟我们只需要将本地数据存储到索引中然后将其可视化。这也是Mirko Nasato在他博客中提到的如何导入数据的方式。我们将继续使用这个，而不用Logstash处理数据。

选项一：将ELK组件以服务运行

访问Elastic网站，下载最新的组件 —— Elasticsearch, Logstash 和 Kibana（Linux用户应该下载.DEB文件）

下载完成后，使用GDebi安装每个组件。这种安装方式默认安装在/usr/share/elasticsearch目录下（其他组件也是安装类似的目录下）。

接着通过下面的命令启动服务：

```
sudo service elasticsearch start
sudo service kibana start
```

将ELK设置成开机启动

先判断你的系统使用的是SysV还是systemd

```
ps -p 1
```

假设你使用systemd来运行ElasticSearch（比如，Elementary OS）。

通过下面的命令启动和停止ElasticSearch：

```
sudo systemctl start elasticsearch.service
sudo systemctl stop elasticsearch.service
```

接着为了让Elasticsearch开机自启，运行下面的命令：

```
sudo /bin/systemctl daemon-reload
sudo /bin/systemctl enable elasticsearch.service
```

假设你使用SysV init来运行ElasticSearch（比如 Linux Mint）

通过下面的命令启动和停止ElasticSearch：

```
sudo -i service elasticsearch start
sudo -i service elasticsearch stop
```

接着配置Elastic自启：

```
sudo update-rc.d elasticsearch defaults 95 10
```

对于Kibana和logstash来说，你也可以这样配置。

选项二：按需运行ELK组件

我将虚拟机配置成按需运行ELK，所以我从这下载了ELK Stack组件文件，格式是tar.gz。

打开终端窗口，将下载目录下的文件拷贝到/opt文件夹下。

```
sudo cp elasticsearch-5.4.3.tar.gz /opt
sudo cp kibana-5.4.3-linux-x86_64.tar.gz /opt
sudo cp logstash-5.4.3.tar.gz /opt
```

接着，切换目录到/opt下，解压所有文件：

```
cd /opt
sudo tar -zxvf elasticsearch-5.4.3.tar.gz
sudo tar -zxvf kibana-5.4.3-linux-x86_64.tar.gz
sudo tar -zxvf logstash-5.4.3.tar.gz
```

现在你可以启动Elasticsearch，举个例子，你只需要这么做：

```
cd elasticsearch-5.4.3
./bin/elasticsearch
```

对于Kibana和Logstash来说，过程是一样的

配置修改

在启动组件前，我对配置文件进行了最小的修改，尽管这并不是必须的。我使用了下面的命令来修改文件：

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

接着，修改Cluster和Node的名字，我是这样改的：

```
cluster-name: honeypot-cluster
node-name: honeypots
```

然后，我还将`network.host:192.168.0.1`改成了`network-host: localhost`。

保存退出。

启动，访问ELK

现在你已经运行了ELK，我们可以通过浏览器在本地的9200端口和5601端口分别访问Elasticsearch和Kibana了。

使用ELK工作吧

我已经将下面会提到的脚本上传到了github。

首先我们需要的是存储数据的Elasticsearch索引。一般来说，索引的创建非常简单。在终端下输入下面的命令就可以创建叫做test的索引了。

```
curl -XPUT &amp;#39;localhost:9200/test&amp;#39;
```

你应该能看到true的结果返回，你也可以通过下面的这个命令来验证test索引的存在。

```
curl -XGET &#39;localhost:9200/test?pretty&#39;
```

这个脚本在Elasticsearch创建了Cowrie索引，同时也提供了映射信息：

```
./create_index.sh             
```

现在，你需要将数据存入新的Elasticsearch索引。下面的这个脚本会循环遍历名为'cowrie'文件夹然后使用'./bulk_index.sh'脚本处理每个文件。这个脚本会在cowrie数据文

```
for JSON in cowrie/*.*; do ./bulk_index.sh $JSON; done
```

现在你已经将数据存到了Elasticsearch索引中，接着可以通过Kibana来进行可视化了。

使用Kibana

- 打开浏览器，访问localhost:5601
- 在要求你创建索引名的字段位置，删掉原来的logstash-*，然后输入cowrie
- 确认勾选了以时间为索引的复选框
- 点击创建
- 在左侧菜单点击发现去校验和观察你的数据
- 此时最可能出现的情况是，右上角的数据只显示了最近15分钟—— 你可以自己调整范围。

接着，添加可视化选项。

- 点击左侧菜单的可视化
- 点击创建可视化视图，然后关闭。

（温馨提示：我并不打算指导你如何在Kibana中创建可视化视图，因为网络上有很多非常棒的相关资源）

目前来说，我们所遇到的ELK困惑中只有一个尚未解决，就是将IP地址转为地理位置以便在地图上标注出来。为了完成这个，我们需要借助Logstash的力量。到目前为止，我

可视化Dionaea数据

因为在之前的博客中介绍了DionaeaFR，所以这里不会深入任何相关的细节。关于DionaeaFR安装唯一要注意的新内容是现在有一个脚本，它能够完成所有繁重的操作。我

在DionaeaFR安装完成后，你可以通过这个脚本来启动。在那之后，你可以通过本地8000端口来访问。

结论和未完成的部分

就本文的大部分来说，我并不满意这篇文章。因为有太多未完成的。在你考虑如何将你捕获的数据进行展示和计算时，希望这篇漫长的蜜罐可视化文章能够给你一些启发。

关于这个主题，下面的条目是我仍想继续做的：

Kibana

1. 找到能够在一次可视化中展示多个字段的方法（比如同时显示用户名/密码）
2. 清理修改Kibana主控板—— 删除可视化标签
3. 将IP地址转为地理位置，以便在地图上显示
4. 找出使Dionaea Json再次正常工作的解决方法，便于我使用ELK展示数据

amChars

1. 试着通过amCharst来重新构造DionaeaFR来展示数据

我想这些意味着未来的某个时候还有下篇（希望很快就来）【译者注：外国人真墨迹，就四个字的意思-未完待续-要扯那么多】

[原文在这]

上一篇：【译】Windows2012上如何... 下一篇：利用免费资源快速搭建分布式扫描架构

1. 2 条回复


hades 2017-07-18 01:09:58

淡定~~

0 回复Ta

c0de 2017-07-18 02:13:29

可以尝试一下，不过蜜罐可以带一些主动性。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板