

这是一篇原本想谈用开源工具AssetsView做企业安全的文字，但还是忍不住多说些什么，包括基于网络层的大规模网络管理在内，成为我时常想关注想学习的内容。

缘由最近心血来潮，想把IT资产管理这件困难的事情在思想上理一理。一是遵从合规要求，真正意义上干漂亮这个事，同时更希望通过自动化工具实现资产识别和风险检测，

## 一、 拓扑发现的二三事

### (一) 拓扑发现是什么

拓扑发现是网络设备与网络连接之间的探索和映射过程，通过技术手段获取网络节点的存在信息和节点之间的连接信息，从而形成网络拓扑图。拓扑发现的过程能够动态进行

### (二) 怎样实现拓扑发现

现实世界我们有很多商业化的工具可以做拓扑发现，功能强大，包括大量的网络安全功能；也有包括LanTopoLog这样的免费软件可以体验。

这些工具背后的技术很多与网络2层或3层有关，包括SNMP协议、网络活性探测和路由分析技术（指OSPF、EIRGP这样的路由协议），以及厂商的Cisco Discovery Protocol (CDP)和Juniper Discovery Protocol

(JDP)等等。这些技术一般都属于网络工程师所接触的高级技能范畴，日常都不大去涉及，玩深玩透更是有难度。不过笔者非常建议大家多去了解一下这一块内容，这能够帮

### (三) 拓扑发现的网络安全功能

可以预期通过拓扑发现技术，可以不断识别网络地址空间，并不断探索网络的边界；可以持续地对终端设备进行普查，这种审查发生在网络核心，不需要安装终端；同时，能

这些能力能够发现未曾记录在档案的网络，发现网络中的无赖设备，甚至发现有威胁特征的设备，等等。而消除这些网络安全风险所付出的代价又较小，这也是我青睐于拓扑

## 二、 AssetsView安装教程

商业工具和免费工具往往由于“只有一块钱做安全”和扩展性较差这样的理由直接枪毙掉，因此选择开源软件，进行二次开发也成为持续能力的重要保证。Assets View是偶然发现的安全类开源软件，并且使用了拓扑技术实现资产发现、网络拓扑管理，这很符合我的关注点。为此，我决定搭建这样的一套系统。

由于系统前端Web采用PHP+MYSQL开发，后端拓扑发现使用C实现，我分两步搭建。

### (一) Web前端部署

虽然与拓扑发现有关，但AssetsViews与很多LAMP系统的搭建别无二致。具体给出CentOS 7下面的安装脚本：

#### 1. 安装MySql数据库

```
yum -y install mariadb-server mariadb
```

```
systemctl start mariadb.service
```

```
systemctl enable mariadb.service
```

MySQL的数据导入使用source指令即可，数据库脚本文件路径在“data\db”。

#### 2.安装Apache服务器

```
yum -y install httpd
```

```
systemctl enable httpd.service
```

```
systemctl start httpd.service
```

#### 3.开启CentOS 7的防火墙

```
firewall-cmd --permanent --zone=public --add-service=http
```

```
firewall-cmd --permanent --zone=public --add-service=https
```

```
firewall-cmd --reload
```

#### 4.安装PHP和需要扩展模块

```
yum -y php php-mysql
```

LAMP环境部署完成后，可以将AssetsView导入Web目录，并配置Apache权限。之所以修改Apache权限，主要由于AssetsView使用了Apache的URL地址重写功能。

另外，大家在访问Web时会遇到部分JS调用异常的问题，这是由于“static\js\json”下面的JS文件内存在固定IP的缘故，删除或者替换为自己主机的IP，调用异常的情况就能解决。

#### (四) 后端源码编译

如果，你和我一样尝试过对topo\_scan模块进行编译，就知道整个编译过程并不顺利，有依赖库、数据库配置需要去修改，而且在GCC环境下，遗留的C代码总有一些错误。

既然topo\_scan基于nmap，那么以nmap编译为基础，整个过程就会顺利不少。附上过程：

建立开发环境

```
yum groupinstall "Development Tools"
```

```
yum install glib2-devel mariadb-devel net-snmp-devel
```

下载nmap-7.12.tar.bz2，默认使用的是7.12版本的nmap，暂时还没测试过7.50。

```
bzip2 -cd nmap-7.12.tar.bz2 | tar xvf -
```

```
cd nmap-7.12
```

```
./configure
```

```
make
```

为了降低编译过程的难度，最好将修改后topo\_scan源码与nmap源码合并编译。为了实现外部定义数据库连接信息，笔者引入RapidJSON作为配置管理工具，对应的文件为

我将修改后的源码附上，大家可以做参考。为了达成编译，需要对nmap下Makefile文件的做一定的修改，包括源码文件列表，具体为Makefile文件展示部分：

Makefile文件引用

```
export SRCS = main.cc handle_hash.cc thread_pool.cc common.cc icmp_snmp.cc handle_mysql.cc handle_snmp.cc switch_link.cc queue.cc
```

```
export HDRS = charpool.h FingerPrintResults.h FPEngine.h idle_scan.h MACLookup.h nmap_amigaos.h nmap_dns.h nmap_error.h nmap_host.h
```

```
OBJS = handle_hash.o thread_pool.o common.o icmp_snmp.o handle_mysql.o handle_snmp.o switch_link.o queue.o main_nmap.o charpool.o
```

对Makefile文件的修改，算是玩了一个小把戏，也是遵循nmap的源码结构做的微调。个人体会，在基于成熟的开源项目做开发时，一定要迎合原有的体系去做功能调整，这样才能

AssetsViews的效果图大家可以在项目主页去看，目前修改后的topo\_scan代码仍在网络核心层SNMP代码部分的测试过程中。根据目前测试的情况，后续需要修订部分代码。

### 三、 总结

一直觉得做网络安全，学习路由、交换的知识是很有必要的，最终虽不一定去考证去配置设备，但学会规划网络，理解复杂网络技术，对于做好网络安全大有裨益，这样才能真

最后，向AssetsView的作者致谢，他开了个好头。

### 四、 参考资料

<https://github.com/Cryin/AssetsView>

<https://www.ipswitch.com/resources/best-practices/topology-discovery>

<https://laptopolog.com/>

<https://nmap.org/>

<http://code.tencent.com/rapidjson.html>

topo\_scan.rar (0.1 MB) [下载附件](#)

点击收藏 | 0 关注 | 0

[上一篇：Assets View资产发现、网...](#) [下一篇：狗汪汪玩转无线电——GPS Hac...](#)

1. 12 条回复



[hades](#) 2017-07-07 01:58:25

辛苦了~~

0 回复Ta

---



[c0de](#) 2017-07-07 03:09:48

很详细，非常好。

0 回复Ta

---



[lazy0](#) 2017-07-14 07:47:55

想问一下楼主搭建能正常新建扫描吗，我这里使用不了，好像也没找到他要调用哪个php文件

0 回复Ta

---



[奶酪只有一块](#) 2017-07-18 03:10:26

Not Found

The requested URL /AssetsView/Dashboard/loginpage was not found on this server.

搭建到这里就不行了。

0 回复Ta

---



[lazytricks](#) 2017-07-18 06:56:57

topo\_scan可以正常运行，但不是通过Web界面管理，目前的代码是单次运行完成后退出。

另外，我再使用的过程中，确定发现Web前端和topo扫描器彼此之间存在调用的割裂，所以也在抽空重新部分代码，这点我再文章里有提过。如果，你有时间，可以联系我，我正在准备重写topo扫描器。

1 回复Ta

---



[lazytricks](#) 2017-07-18 06:59:54

这是由于URL虚化产生的异常，你需要开启Apache服务器的URL重新功能，具体参照<http://httpd.apache.org/docs/2.4/mod/core.html#accessfilename>。

0 回复Ta

---



[hades](#) 2017-07-18 07:38:11

棒棒哒 你这头像太搞笑了~~

0 回复Ta

---



[ko0zh1](#) 2017-08-30 14:27:31

非常好

0 回复Ta

---



[21guns](#) 2018-01-17 11:03:20

LAMP环境部署完成后，可以将AssetsView导入Web目录，并配置Apache权限。之所以修改Apache权限，主要由于AssetsView使用了Apache的URL地址重写功能。

楼主针对上面这段，有没有具体命令啊？

0 回复Ta

---



[zhi\\*\\*\\*\\*yang](#) 2019-03-19 09:20:02

[@lazytricks](#) 附件的topo\_scan源码可以编译吗？攻城狮大神

0 回复Ta

---



[先知朱金奇](#) 2019-03-20 09:21:39

功能不完整啊，展示端无法创建扫描任务，scan端没有被调用，功能都有，但是没有做串联，现在有没有完整地代码呀

0 回复Ta



[先知朱金奇](#) 2019-03-20 09:29:28

[@lazytricks](#) 有没有写完的完整代码呀

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](#)