工控蜜罐日志分析

发表于 2021-02-16 分类于 Challenge ， 2019 ， 工业信息安全技能大赛 ， 深圳站
Challenge | 2019 | 工业信息安全技能大赛 | 深圳站 | 工控蜜罐日志分析

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/5960

题目描述

> *工控安全分析人员在互联网上部署了工控仿真蜜罐，通过蜜罐可抓取并分析互联网上针对工业资产的扫描行为，将存在高危扫描行为的IP加入防火墙黑名单可有效减少工业企业对于互联网的攻击面。分析出日志中针对西门子私有通信协议扫描最多的IP，分析该扫描组织。FLAG为该IP的域名。*

题目考点

- *日志分析*

解题思路

附件是一个henoypot.log，内容格式如图所示：

根据题目提示，Flag为某个IP对应的域名，于是可以编写脚本，首先提取出日志的IP，并且去重IP，然后再对每一个IP反查域名，寻找正确的域名，脚本和运行结果如下：

```
#-*- coding:utf-8 -*-
import fileinput
import re
import os
import shutil
def readIp():
 with open(r'/root/python/honeypot.log', 'r') as f:
      for line in f.readlines():
         result2 = re.findall('[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}',line) #匹配ip正则表达式
         if not result2 == []:
             result = result2[0] + '\n'
         with open('/root/python/ip.txt', 'a+') as w:
             w.write(result)
def setIp():#去重
 a=0
 readDir = "/root/python/ip.txt"
 writeDir = "/root/python/newip.txt"#new
 lines_seen = set()
 outfile = open(writeDir, "w")
 f = open(readDir, "r")
 for line in f:
   if line not in lines_seen:
     a+=1
     outfile.write(line)
     lines_seen.add(line)
 print(a)
 outfile.close()
def readDns():
 with open(r'/root/python/newip.txt', 'r') as g:
     for i in g.readlines():
         com=os.popen('nslookup %s'%i)
         comm=com.read()
         if comm.find('NXDOMAIN')==-1:
             print comm
if __name__ == '__main__':
 readIp()
 setIp()
 readDns()
```


挨个尝试提交域名，找到正确的域名为：scan-42.security.ipip.net

Flag

```
flag{scan-42.security.ipip.net}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/工业信息安全技能大赛/深圳站/6Q7AfKaJraA3sT7dLR8vZ5.html*

- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2019 # 工业信息安全技能大赛 # 深圳站
隐信道数据安全分析
组态软件安全分析