【CTF】后续深入学习内容

转载

aichuo1897 于 2017-05-31 17:15:00 发布 201 收藏
文章标签： 爬虫 运维 操作系统
原文链接：http://www.cnblogs.com/viphhs/p/6925106.html

1、i春秋

https://www.ichunqiu.com/course/451

搜索black hat，可以看到黑帽大会的内容。免费。

2、wireshark

基础篇

1）由于Wireshark是一款开源的软件，因此我们可以分析该软件的源代码来找出协议解析错误的原因。在其官方网站上，我们就可以下载到软件的源码。

https://www.wireshark.org/docs/wsar_html/epan/dir_439f766e1074d620bb0af091af8f0d3e.html

2）复习一下3次握手

3）tshark，kali linux，grep

3、二进制安全学习规划（以下3-7点摘录自**长亭科技**的杨坤博士在**ichunqiu**的课程）

1）汇编 CMU 18-447

https://www.ece.cmu.edu/~ece447/s15/doku.php

2）编译原理

https://web.stanford.edu/class/cs143/

有实验

3）操作系统

https://pdos.csail.mit.edu/6.828/2016/

有实验，JOS；a simple unix

4、CTF历史资料库

1）https://github.com/ctfs

2）http://pwnable.kr/

3）http://smashthestack.org/

4）9447，CCC，hitcon，plaid ，boston key party，defcon等各类ctf

5) http://websec.fr/

6)http://io.netgarage.org/

5、网络协议的实现（http，DNS，SMB，UPnP）；脚本引擎；内核引擎Linux、Android，Apple iOS，索尼PS4等

6、学习历史漏洞CVEs，大会日程，挖掘新漏洞（代码审计、逆向工程），模糊测试（猜想程序员容易跌倒的地方）。

7、前沿方向：漏洞利用防护机制、漏洞自动挖掘机制。

【Python学习】

1、ADO老师 https://www.ichunqiu.com/course/53441

1）第二课，正则表达式例题，在Python3中，需要注意编码的处理。

https://segmentfault.com/q/1010000004926244/a-1020000004926714 （里面有两个链接，可以读一读）

https://stackoverflow.com/questions/14472650/python-3-encode-decode-vs-bytes-str （可以学习文章中在IDLE中逐行调试代码）

https://wiki.python.org/moin/ForLoop for循环，处理lists

2）自己写的样例：

```
# coding: utf-8
import re
html = '''<li><a name="business" id="business-tzfz" href="../yz/business-tzfz.htm">投资发展</a></li>
<li><a name="business" id="business-scjy" href="../yz/business-scjy.htm">生产经营</a></li>
<li><a name="business" id="business-jsyx" href="../yz/business-jsyx.htm">技术运行</a></li>
<li><a name="business" id="business-cwgl" href="../yz/business-cwgl.htm">财务管理</a></li>
<li><a name="business" id="business-jkah" href="../yz/business-jkah.htm">健康安环</a></li>
<li><a name="business" id="business-sbgl" href="../yz/business-sbgl.htm">设备管理</a></li>
<li><a name="business" id="business-wzgy" href="../yz/business-wzgy.htm">物资供应</a></li>
<li><a name="business" id="business-rlzy" href="../yz/business-rlzy.htm">人力资源</a></li>
<li><a name="business" id="business-kjxx" href="../yz/business-kjxx.htm">科技信息</a></li>
<li><a name="business" id="business-xzgl" href="../yz/business-xzgl.htm">行政管理</a></li>
<li><a name="business" id="business-qygggl" href="../yz/business-qygggl.htm">企业改革管理</a></li>

''' # 需要使用三个单引号

title = re.findall(r'htm">(.*?)</a></li>', html)
print (title)
for i in title: #最后需要加入分号
print(i)
```

3）检索资料时，尽量使用bing或者google，搜索英文的内容。例如lists，python3。

2、WEB编程（简单爬虫）

1）urllib，urllib2，requests

在python3中使用的是urllib.requests（这个和requests不一样，需要单独安装）。

2）样例：

```
f = urllib.request.urlopen('http://www.python.org/')
```

print （f.read())

3）爬虫练习题：

http://www.heibanke.com/lesson/crawler_ex00/ 题目

https://ericfu.me/solution-to-heibanke-crawler-ex/ writeup

http://vjson.com/wordpress/%E7%88%AC%E8%99%AB%E9%97%AF%E5%85%B3%E7%AC%AC%E4%BA%

4）待进一步了解内容：如何爬取需登录的网站？

https://juejin.im/entry/566fdee660b2d0be157516c8

5）安装pip和requests

先安装pip，然后再命令行里面安装pip install requests（需要联网）

http://docs.python-guide.org/en/latest/starting/install3/win/#install3-windows

6)从官网学习

https://docs.python.org/3.5/library/datetime.html#strftime-strptime-behavior

3、Beautiful Soup 官方文档

https://www.crummy.com/software/BeautifulSoup/bs4/doc.zh/#id28

4、到github自己读一些python文档

https://github.com/geekcomputers/Python/blob/master/dir_test.py

5、余弦技能表推荐的书籍：

https://learnpythonthehardway.org/book/ex26.html

【逆向工程】

1、逆向**https://www.blackh4t.org/archives/1793.html**

转载于:https://www.cnblogs.com/viphhs/p/6925106.html