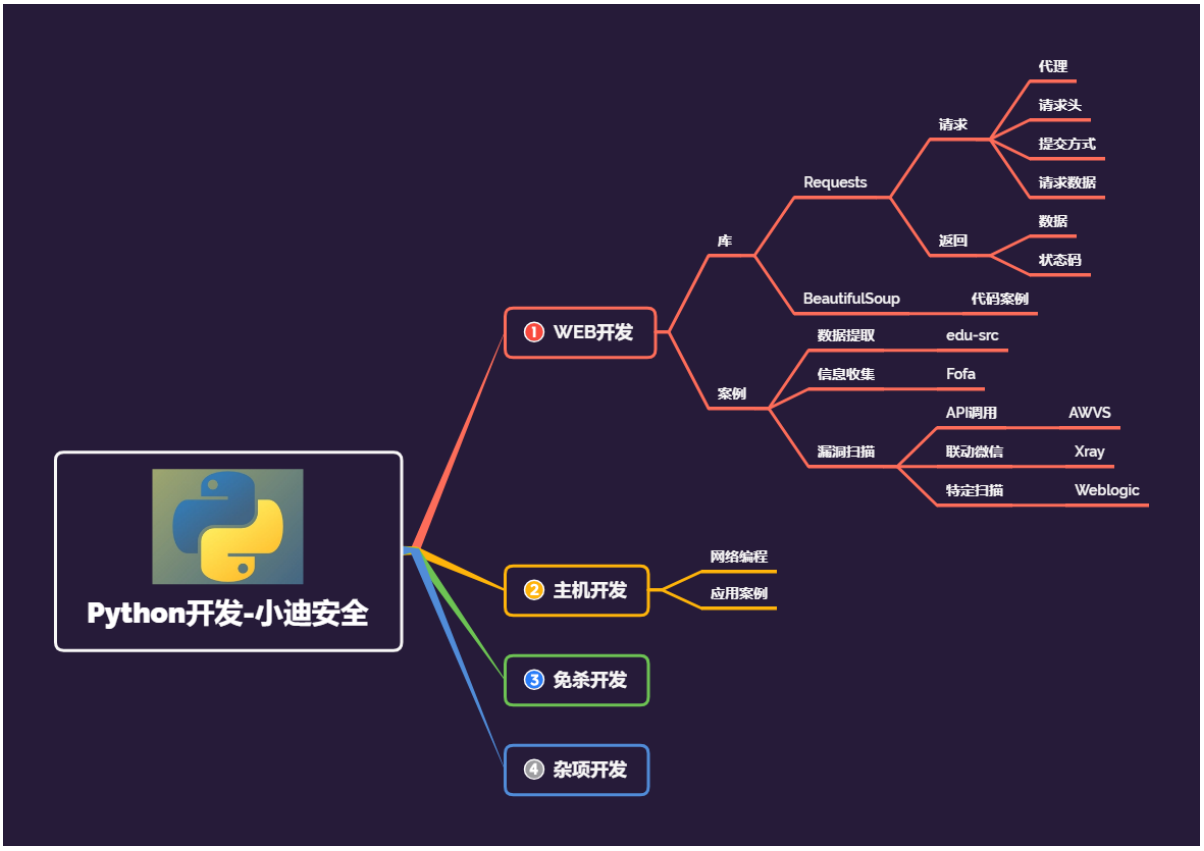
Day160　安全开发-Python-蓝队项目&流量攻击分析&文件动态监控&Webshell检测



1.知识点

- 1、Python-应用方向蓝队项目
- 2、Python-scapy&watchdog&接口
- 3、Python-流量数据&文件动态&文件定性

2.演示案例

```
Python蓝队项目说明：
1、漏洞攻击-先监控流量 发现攻击 预警（流量监控）
2、文件分析-发现新出文件 将文件上传至平台分析（文件监控）
3、文件处置-对文件进行隔离 处置（删除或重命名）（平台分析）
```

2.1 Python-蓝队项目-Scapy流量分析

```
#简单Demo
from scapy.all import *
def handelPacket(p):# p捕获到的数据包
    p.show()

sniff(prn=handelPacket,count=0)


from scapy.all import *

def packet_callback(packet):
    #print(packet.show())
    data=bytes(packet[TCP].payload)
    for info in data.split(b'\n'):
        #print(info)
        if b'Content-Disposition: form-data; name="' in info:
            print('文件上传攻击中...')
            pass

#filter 筛选
#iface 网卡
#prn 调用函数
```

```
#count 获取条数
#store 内存清除
#count:指定最多嗅探多少个符合要求的报文，设置为0时则一直捕获
#store:指定保存抓取的数据包或者丢弃，1为保存，0为丢弃
#offline:从pcap文件中读取数据包，而不进行嗅探，默认为None
#prn:为每个数据包定义一个回调函数，回调函数会在捕获到符合filter 的报文时被调用，通常使用 lambda 表达式来编写
#filter:用来筛选抓取的信息，其用法与常见抓包软件WireShark 等相同，遵循 BPF 语法
#L2socket:使用给定的L2socket
#timeout:在给定的事件后停止嗅探，默认为None
#opened_socket:对指定的对象使用.recv进行读取
#stop_filter:定义一个函数，决定在抓到指定的数据之后停止
#iface:指定抓包的网卡,不指定则代表所有网卡
#https://blog.csdn.net/qq_43619058/article/details/119037103
if __name__ == '__main__':
    sniff(filter='host 192.168.1.107 and tcp port 80',iface='以太网',prn=packet_callback,store=0)
    #sniff(filter='tcp port 80', iface='以太网', prn=packet_callback, store=0)
```

2.2 Python-蓝队项目-Watchdog文件行为

```
参考：https://www.jianshu.com/p/6c80ac3c8013
from watchdog.observers import Observer
from watchdog.events import *
import time

```

```
6  class FileEventHandler(FileSystemEventHandler):
7      def __init__(self):
8          FileSystemEventHandler.__init__(self)
9
10     def on_moved(self, event):
11         if event.is_directory:
12             print("directory moved from {0} to
   {1}".format(event.src_path, event.dest_path))
13         else:
14             print("file moved from {0} to
   {1}".format(event.src_path, event.dest_path))
15
16     def on_created(self, event):
17         if event.is_directory:
18             print("directory created:
   {0}".format(event.src_path))
19         else:
20             print("file created:
   {0}".format(event.src_path))
21
22     def on_deleted(self, event):
23         if event.is_directory:
24             print("directory deleted:
   {0}".format(event.src_path))
25         else:
26             print("file deleted:
   {0}".format(event.src_path))
27
28     def on_modified(self, event):
29         if event.is_directory:
30             print("directory modified:
   {0}".format(event.src_path))
```

```
        else:
            print("file modified: {0}".format(event.src_path))


if __name__ == "__main__":
    observer = Observer()
    event_handler = FileEventHandler()
    observer.schedule(event_handler, r"C:\Users\wyq\Desktop\1", True)
    observer.start()
    try:
        while True:
            time.sleep(1)
    except KeyboardInterrupt:
        observer.stop()
    observer.join()
```

2.3 Python-蓝队项目-Webshell文件接口检测

```
https://scanner.baidu.com/#/pages/intro
def file_upload_check(webfile):
    webfile=webfile.replace('\\','\\\\')
    print(webfile)
    cmd='curl https://scanner.baidu.com/enqueue -F archive=@%s' %webfile
    try:
        result = os.popen(cmd).read()
        results=json.loads(result)['url']
        print(results)
        with open('url.txt', 'a+', encoding='utf-8') as f:
```

```
            f.write(results + '\n')
            f.close()
        for url in open('url.txt'):
            url = url.replace('\n', '')
            print(url)
            try:
                s = requests.get(url).json()
                #print(s[0]['data'][0]['descr'])
                if s[0]['data'][0]['descr'] is None:
                    print('此文件无风险')
                else:
                    print('此文件有风险')
                    print(s[0]['data'][0]['descr'])
            except Exception as e:
                pass
    except Exception as e:
        print('此文件非脚本文件，无法检测')

file_upload_check('1.php')
```