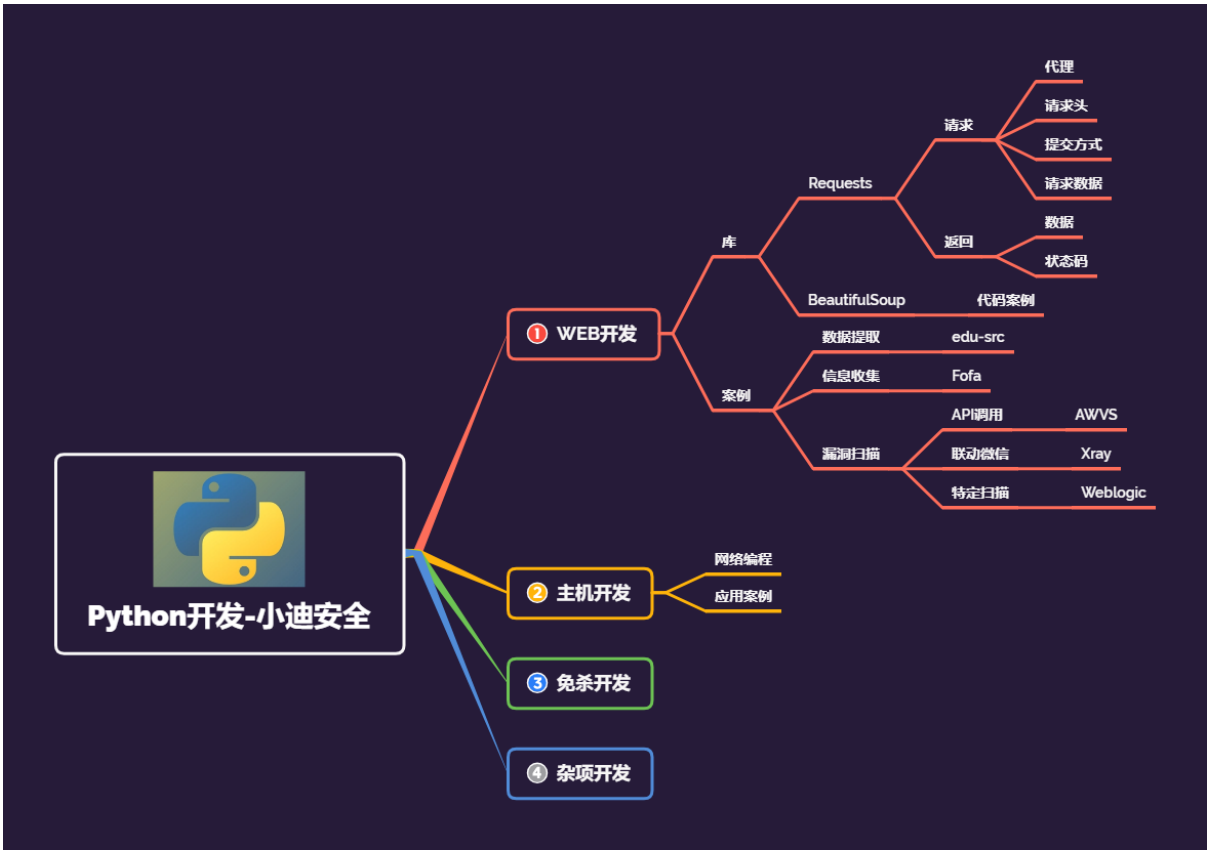
安全开发-Python-蓝队项目&流量攻击分析&文件动态监控&Webshell 检测



#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

#章节点：

Web 爬虫解析类

多线程异步处理类

Socket 网络通讯类

其他第三方库数据类

#应用点：

信息打点，POC&EXP 利用，工具 API 调用，文件流量监控，工具脚本开发,远控后门等

演示案例：

- Python-蓝队项目-Scapy 流量分析
- Python-蓝队项目-Watchdog 文件行为
- Python-蓝队项目-Webshell 文件接口检测

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）

```
#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
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址