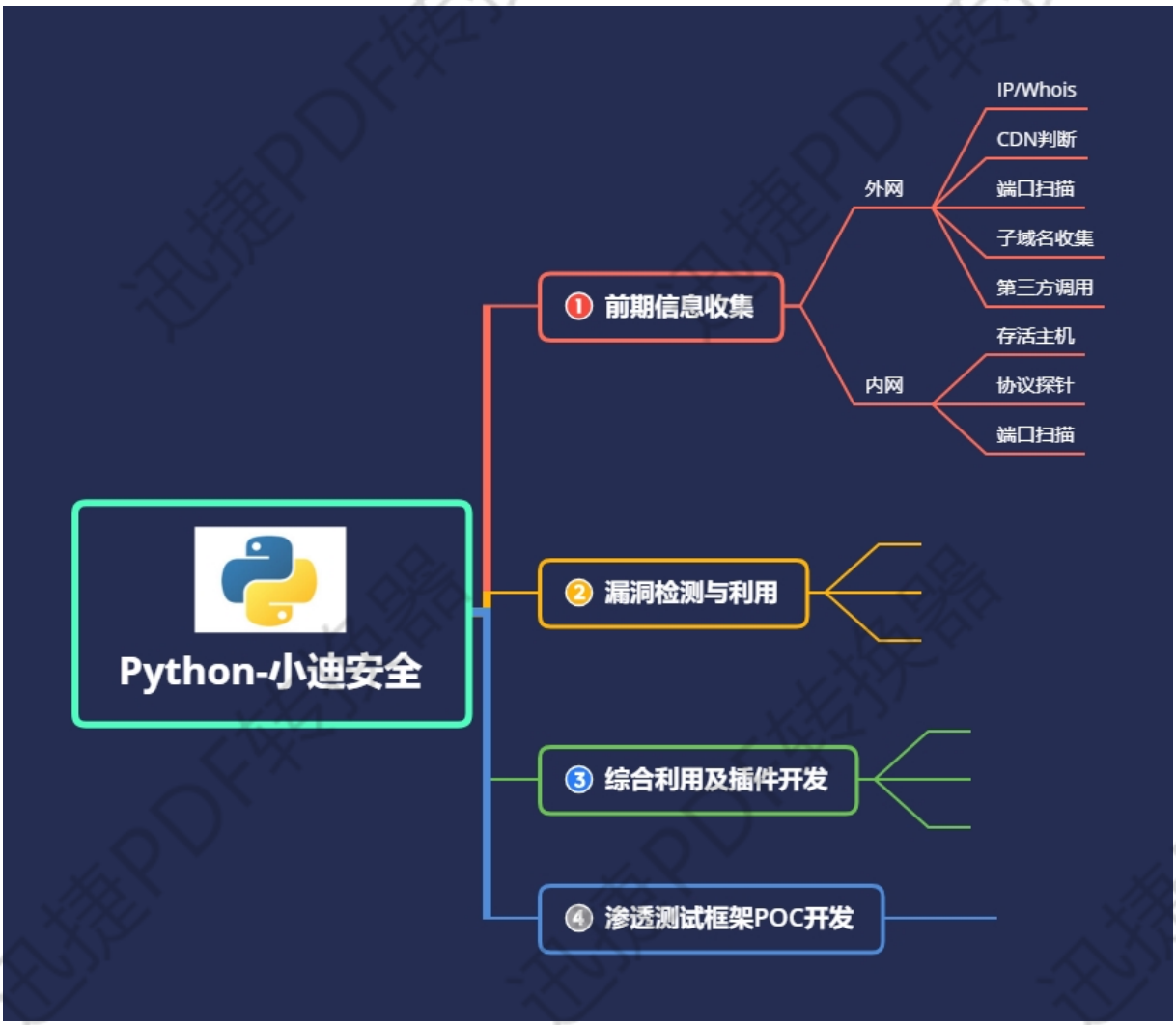
Python 开发-内外网收集 Socket&子域名 &DNS

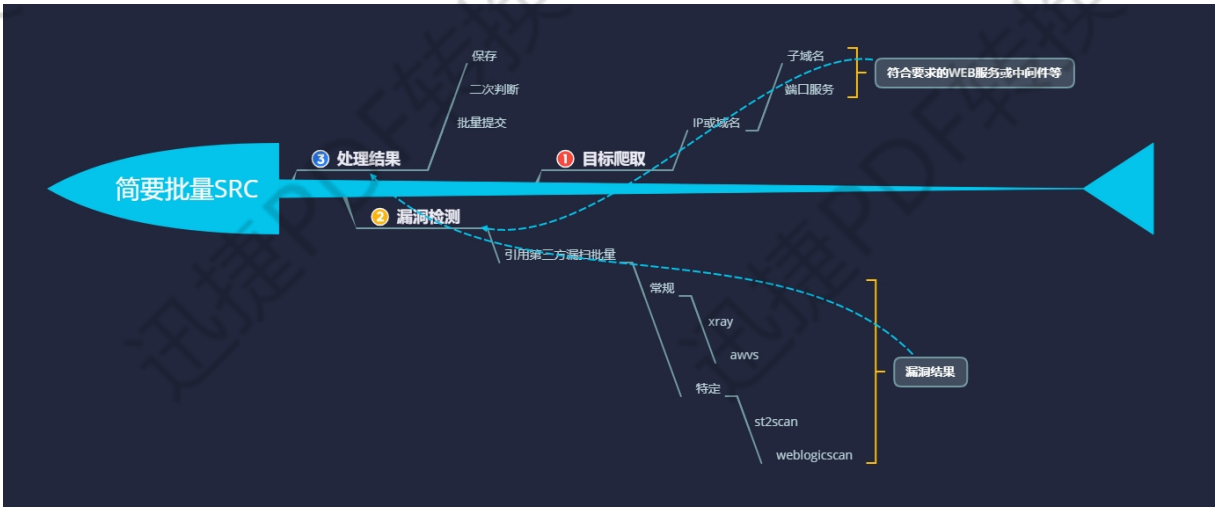


#应急响应补充知识点
挖矿靶机分析 PDF 外加其他

#Python 开发相关知识点：
1.开发基础环境配置说明
Windows10+Pycharm
2.Python 开发学习的意义
学习相关安全工具原理
掌握自定义工具及拓展开发

解决实战中无工具或手工麻烦批量化等情况
在二次开发 Bypass，日常任务，批量测试利用等方面均有帮助
如：SRC 批量收集并利用，AWD 批量利用获取 FLAG，CTF 加解密脚本等
3.本篇直播涉及的技术方向
Socket，爬虫，正则表达式，框架开发等

#本次直播涉及知识点：
Socket 部分技术，进程命令执行，交互参数执行，NMAP 工具模块使用，异常处理等



演示案例：

- IP&Whois&系统指纹获取代码段-外网
- CDN&子域名&端口扫描&交互代码段-外网
- IP&计算机名&存活主机&端口扫描代码段-内网
- Py 格式解析环境与可执行程序格式转换-Pyinstaller

```
import socket,os,time,sys
from whois import whois

#ip 查询-socket
def ip_check(url):
ip=socket.gethostbyname(url)
print(ip)

#whois 查询-模块库获取
def whois_check(url):
data=whois(url)
print(data)
```

```
#CDN 判断-利用返回 IP 数目进行判断
def cdn_check(url):
ns="nslookup "+url
#data=os.system(ns)
#print(data) #结果无法读取操作
data=os.popen(ns,"r").read()
if data.count(".")>8:
print("存在 CDN")
else:
print("不存在 CDN")

#子域名查询
#1.利用字典记载爆破进行查询
#2.利用 bing 或第三方接口进行查询
def zym_list_check(url):
url=url.replace("www.","")
for zym_list in open("dic.txt"):
zym_list=zym_list.replace("\n","")
zym_list_url=zym_list+"."+url
try:
ip=socket.gethostbyname(zym_list_url)
print(zym_list_url+"->"+ip)
time.sleep(0.1)
except Exception as e:
print(zym_list_url+"->"+"error")
time.sleep(0.1)

def zym_api_check(url):
url=url.replace("www.", "")

#端口扫描
#1.自写 socket 协议 tcp,udp 扫描
#2.调用第三方 masscan,nmap 等扫描
def port_check(url):
ip = socket.gethostbyname(url)
#ip="192.168.76.155"
#ports={'21','22','135','443','445','80','1433','3306',"3389",'1521','8000','7002','7001','8080',"9090",'8089',
"4848}
server = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
#for port in ports:
try:
data=server.connect_ex((ip, 80))
if data==0:
print(ip+":"+str(80)+"|open")
else:
```

```
print(ip+":"+str(80)+"|close")
pass
except Exception as err:
print("error")

#系统判断-
#1.基于 TTL 值进行判断
#2.基于第三方脚本进行判断
def os_check(url):
data = os.popen("nmap\\nmap -O "+url, "r").read()
print(data)

if __name__ == '__main__':
print("Test：python test.py www.xiaodi8.com all")
url = sys.argv[1]
check = sys.argv[2]
#print(url +"\n"+ check)
if check=="all":
ip_check(url)
whois_check(url)
cdn_check(url)
os_check(url)
#port_check(url)
zym_list_check(url)

#zym_list_check("www.xueersi.com")
#port_check("www.xiaodi8.com")
#os_check("www.xiaodi8.com")
import nmap

#内网主机信息探针
#1.原生利用 ping 进行获取
#2.原生利用 icmp,tcp,udp 等协议获取
#3.利用第三方模块库 nmap 等加载扫描获取
def nmapscan():
nm = nmap.PortScanner()
try:
data=nm.scan(hosts='192.168.76.0/24', arguments='-T4 -F')
print(nm.all_hosts())
print(nm.csv())
print(data)
except Exception as err:
print("error")

if __name__ == '__main__':
```

nmapscan()

涉及资源：

https://www.jb51.net/softs/598504.html

https://www.cnblogs.com/csnd/p/11807823.html

https://pan.baidu.com/s/13y3U6jX3WUYmnfKnXT8abQ 提取码：xiao

https://pan.baidu.com/s/1tQS1mUelmEh3I68AL7yXGg 提取码：xiao
