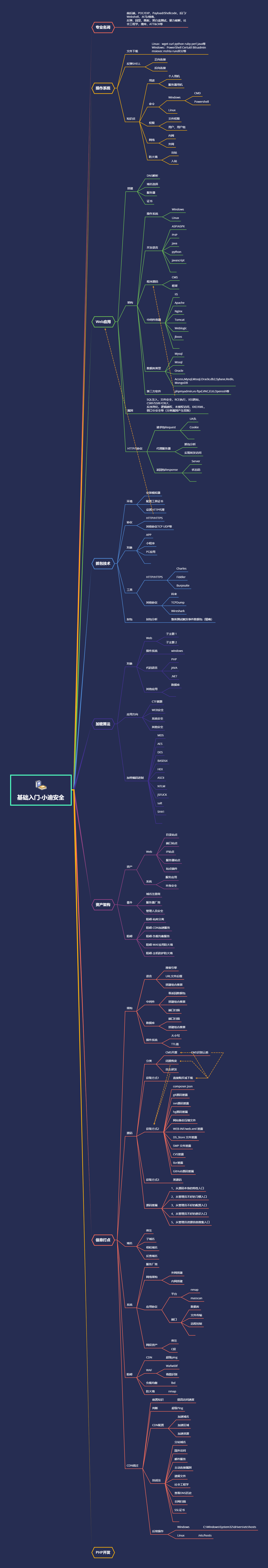
信息打点-CDN绕过篇&漏洞回链&接口探针&全网扫描&反向邮件



#知识点：

0、CDN知识-工作原理及阻碍

1、CDN配置-域名&区域&类型

2、CDN绕过-靠谱十余种技战法

3、CDN绑定-HOSTS绑定指向访问

演示案例：

* 真实应用-CDN绕过-漏洞&遗留文件
* 真实应用-CDN绕过-子域名查询操作
* 真实应用-CDN绕过-接口查询国外访问
* 真实应用-CDN绕过-主动邮件配合备案
* 真实应用-CDN绕过-全网扫描FuckCDN

#前置知识：

1.传统访问：用户访问域名–>解析服务器IP–>访问目标主机

2.普通CDN：用户访问域名–>CDN节点–>真实服务器IP–>访问目标主机

3.带WAF的CDN：用户访问域名–>CDN节点（WAF）–>真实服务器IP–>访问目标主机

#CDN配置：

配置1：加速域名-需要启用加速的域名

配置2：加速区域-需要启用加速的地区

配置3：加速类型-需要启用加速的资源

#判定标准：

nslookup,各地ping（出现多个IP即启用CDN服务）

#参考知识：

https://zhuanlan.zhihu.com/p/33440472

https://www.cnblogs.com/blacksunny/p/5771827.html

子域名，去掉www，邮件服务器，国外访问，证书查询，APP抓包

黑暗空间引擎，通过漏洞或泄露获取，扫全网，以量打量，第三方接口查询等

#案例资源：

超级Ping：https://www.17ce.com/

接口查询：https://get-site-ip.com/

国外请求：https://tools.ipip.net/cdn.php

全网扫描：https://github.com/Tai7sy/fuckcdn

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)