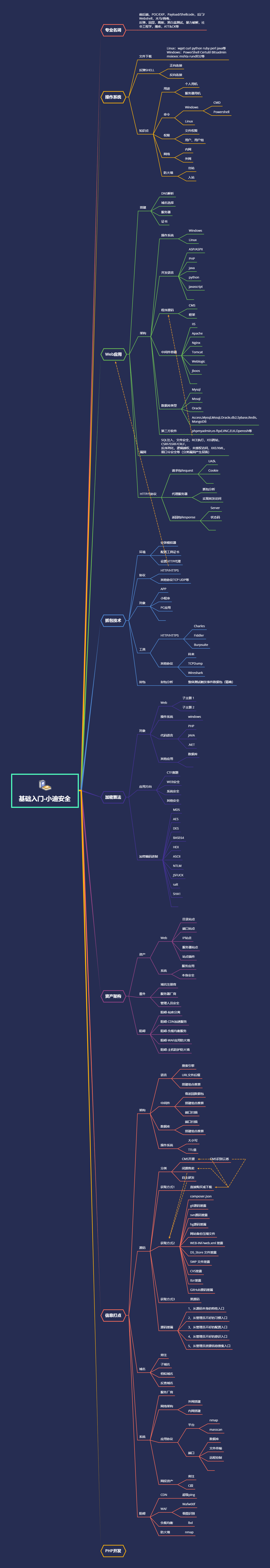
信息打点-系统篇&端口扫描&CDN服务&负载均衡&WAF防火墙



#知识点：

获取网络信息-服务厂商&网络架构

2、获取服务信息-应用协议&内网资产

3、获取阻碍信息-CDN&WAF&负载&防火墙

#详细点:

CDN服务，WAF防火墙，负载均衡，防火墙阻碍？

演示案例：

* 网络信息获取-服务厂商&网络架构
* 服务信息获取-协议应用&内网资产
* 阻碍信息获取-CDN&WAF&负载&防火墙

#相关利用项目：

Masscan：https://github.com/robertdavidgraham/masscan

Wafw00f：https://github.com/EnableSecurity/wafw00f

Kali上自带Nmap，Masscan，lbd等项目，超级ping：ping.chinaz.com

超级ping：CDN服务识别

Masscan：端口扫描，应用协议

Wafw00f：Web应用防护防火墙识别

Nmap：端口扫描，应用协议，防火墙识别

lbd：负载均衡，广域网负载均衡，应用层负载均衡

#端口协议安全：

https://www.se7ensec.cn/2018/11/28/%E7%AB%AF%E5%8F%A3%E6%B8%97%E9%80%8F%E6%80%BB%E7%BB%93/

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)