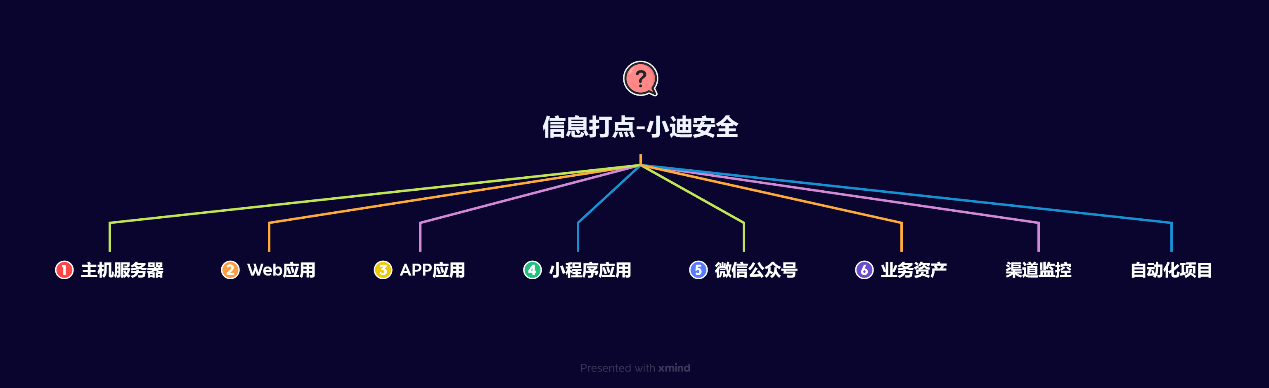
信息收集-主机服务器&系统识别&IP资产&反查技术&端口扫描&协议探针&角色定性



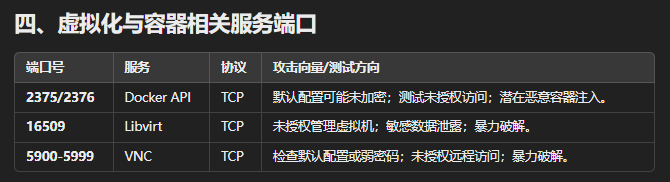
#知识点：  
1、信息收集-服务器系统-操作系统&IP资产  
2、信息收集-服务器系统-端口扫描&服务定性  
  
#章节点：(待补充)  
#具体点：(待补充)

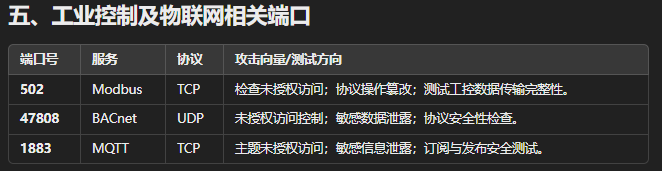


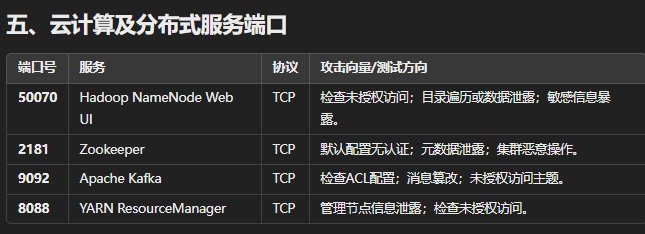


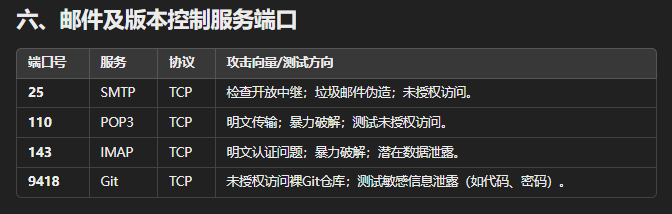














演示案例：

* 应用服务器-操作系统&IP资产
* 应用服务器-端口扫描&角色定性

#操作系统  
1、Web大小写  
2、端口服务特征  
3、TTL值判断返回  
  
#IP资产  
归属地查询  
归属云厂商  
IP反查机构  
IP反查域名  
IP-C段查询  
这里可以转换成Web上，机构上，从而获取更多信息  
  
#端口资产  
1、网络资产引擎：直接使用网络测绘引擎(Fofa、Hunter、Quake、00信安等搜索IP；此类网络资产测绘引擎都是每隔一段时间会对全网的网络资产去做一个轮询，那可能每个引擎的轮询周期、扫描精准度都不同，故建议可使用不同的搜索引擎以获取更多资产。  
地址导航：https://dh.aabyss.cn/  
参考：https://mp.weixin.qq.com/s/FRgPQKJDj2xRCduwPfZrTw  
  
2、在线端口扫描：百度或google直接搜索在线端口扫描就会有一些网站，同理很多功能都可以直接搜索在线xxx；例如在线正则提取解析、在线编码转换等。  
  
3、本地离线工具：推荐使用Nmap、Masscan、Fscan、KScan，其中Nmap最为准确，但最慢；Masscan最快，误报相对更高。  
端口扫描：https://xz.aliyun.com/t/15753  
演示：Yakit Nmap TscanPlus FScan Tanggo等  
考虑：1、防火墙 2、内网环境  
可能出现案例：数据库端口开放，但进行端口扫描，发现数据库端口没有开放（排除防火墙）\*注意：扫描中选择扫描协议是绕过安全组防火墙设置的一种手法，具体成功需看出网入网配置  
  
#应用服务  
见上图端口协议对应服务应用  
  
#角色定性判定  
1、网站服务器  
2、数据库服务器  
3、邮件系统服务器  
4、文件存储服务器  
5、网络通信服务器  
6、安全系统服务器

涉及资源：[资源下载地址](https://docs.qq.com/doc/DQ3Z6RkNpaUtMcEFr)