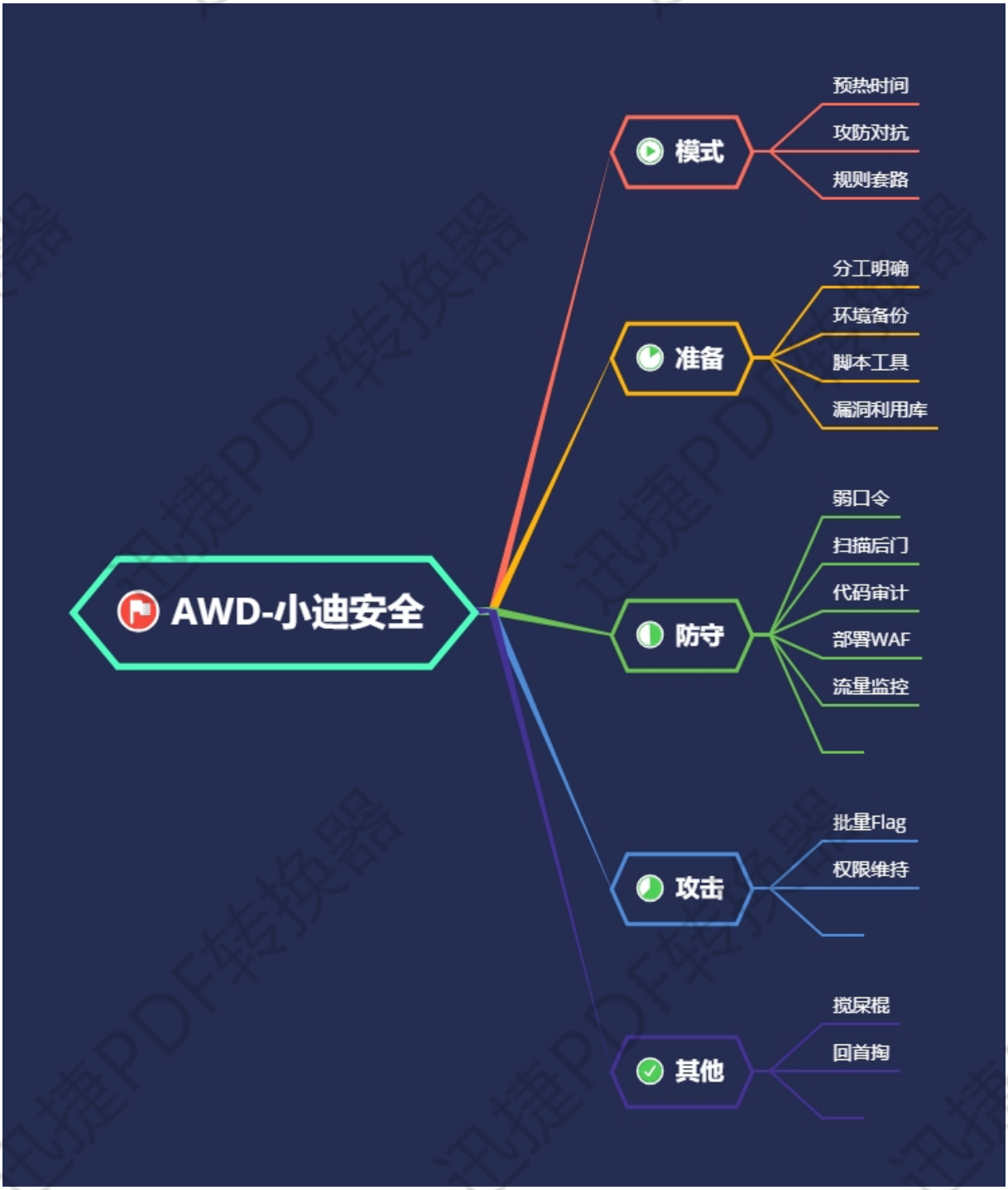
红蓝对抗-AWD 监控&不死马&垃圾包&资源库



演示案例：

- 防守-流量监控-实时获取访问数据包流量
- 攻击-权限维持-不死脚本后门生成及查杀

- 其他-恶意操作-搅屎棍发包回首掏共权限
- 准备-漏洞资源-漏洞资料库及脚本工具库

#案例 1-防守-流量监控-实时获取访问数据包流量
利用 WEB 访问监控配合文件监控能实现 WEB 攻击分析及后门清除操作，确保写入后门操作失效，也能确保分析到无后门攻击漏洞的数据包便于后期利用
1.分析有后门或无后门的攻击行为数据包找到漏洞进行修复
2.分析到成功攻击的数据包进行自我利用，用来攻击其他队伍

#案例 2-攻击-权限维持-不死脚本后门生成及查杀
在攻击利用后门获取 Flag 时，不死后门的权限维持尤为重要，同样防守方也要掌握对其不死后门的查杀和利用，这样才能获取更高的分数，对比文件监控前后问题

#案例 3-其他-恶意操作-搅屎棍发包回首掏共权限
作为各种技术大家都要用的情况下，一个好的攻击漏洞和思路不被捕获和发现，一个好的套路浪费对手的时间，搅屎棍发包回首掏共权限利用思路可以尝试使用

#案例 4-准备-漏洞资源-漏洞资料库及脚本工具库
比赛准备：如何收集并整理好漏洞，文档资料，脚本工具等
漏洞库：exploitdb，github 监控最新信息，平常自己收集整理
文档资料：零组类似文档离线版爬虫，各类资料，平常自己收集整理
脚本工具：忍者系统配合自己常用工具，github 监控 awd 脚本，收集整理

涉及资源：

https://pan.baidu.com/s/1qR0Mb2ZdToQ7A1khqbiHuQ 提取码：xiao
