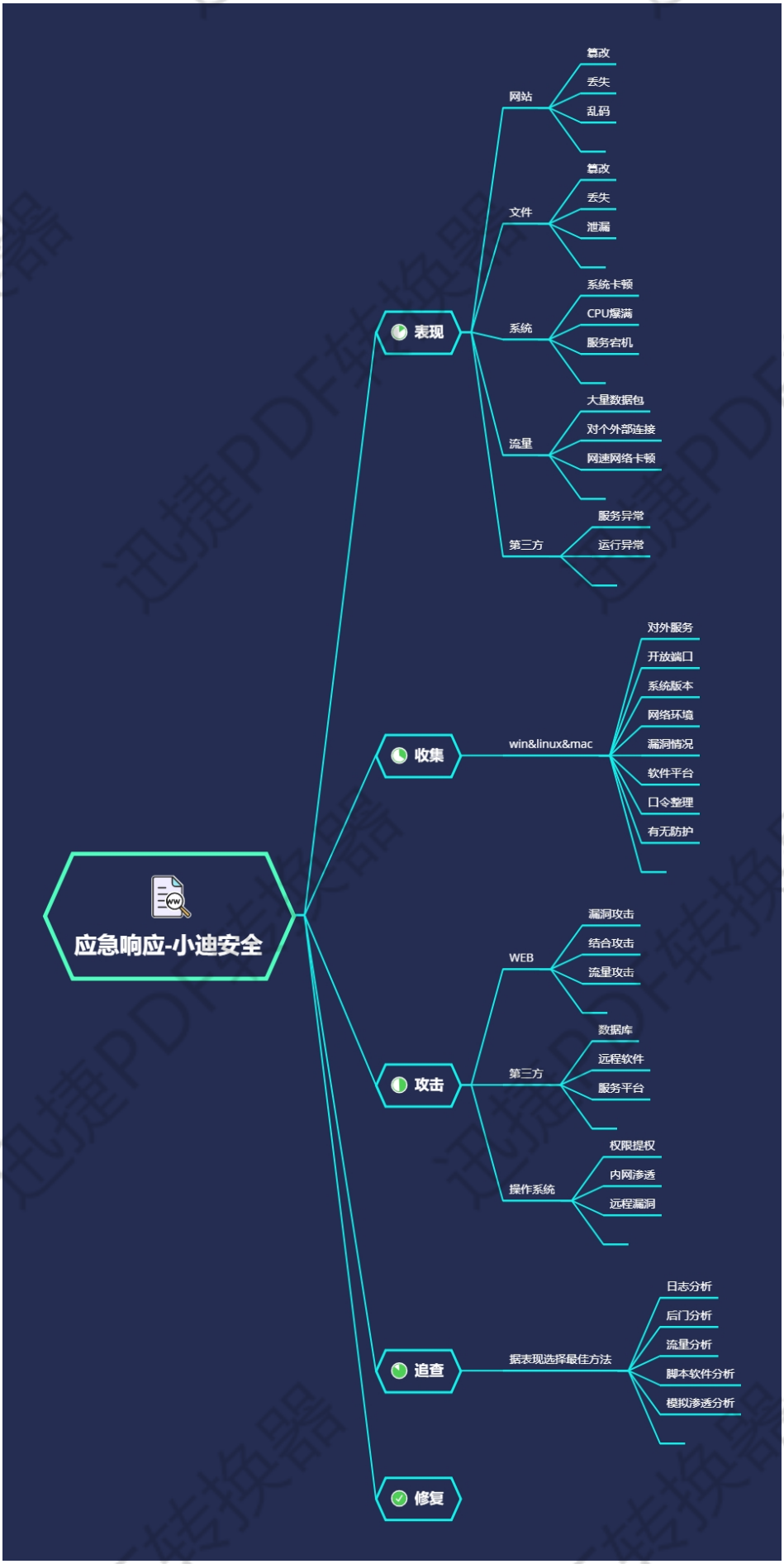
应急响应-WEB 分析 php&javaweb&自动化工具


应急响应-小迪安全
表现
网站
篡改
丢失
乱码
文件
篡改
丢失
泄漏
系统
系统卡顿
CPU爆满
服务宕机
流量
大量数据包
对个外部连接
网速网络卡顿
第三方
服务异常
运行异常
收集
win&linux&mac
对外服务
开放端口
系统版本
网络环境
漏洞情况
软件平台
口令整理
有无防护
攻击
WEB
漏洞攻击
结合攻击
流量攻击
第三方
数据库
远程软件
服务平台
操作系统
权限提权
内网渗透
远程漏洞
追查
据表现选择最佳方法
日志分析
后门分析
流量分析
脚本软件分析
模拟渗透分析
修复

#应急响应：
保护阶段，分析阶段，复现阶段，修复阶段，建议阶段
目的：分析出攻击时间，攻击操作，攻击后果，安全修复等并给出合理解决方案。

#必备知识点：
1.熟悉常见的 WEB 安全攻击技术
2.熟悉相关日志启用及存储查看等
3.熟悉日志中记录数据分类及分析等

#准备工作：
1.收集目标服务器各类信息
2.部署相关分析软件及平台等
3.整理相关安全渗透工具指纹库
4.针对异常表现第一时间触发思路

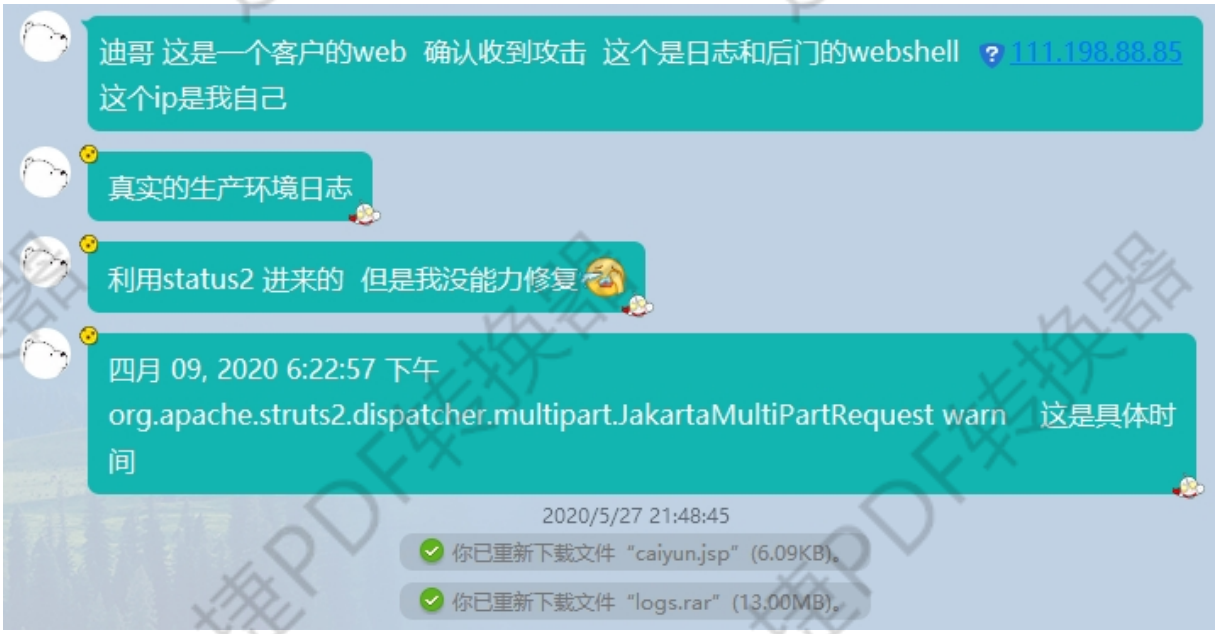
从表现预估入侵面及权限面进行排查
#有明确信息网站被入侵：
基于时间 基于操作 基于指纹 基于其他

#无明确信息网站被入侵：
1.WEB 漏洞-检查源码类别及漏洞情况
2.中间件漏洞-检查对应版本及漏洞情况
3.第三方应用漏洞-检查是否存在漏洞应用
4.操作系统层面漏洞-检查是否存在系统漏洞
5.其他安全问题(口令,后门等)-检查相关应用口令及后门扫描

#常见分析方法：
指纹库搜索，日志时间分析，后门追查分析，漏洞检查分析等

演示案例：

- Windows+IIS+Sql-日志,搜索
- Linux+BT_Nginx+tp5-日志,后门
- Linux+Javaweb+st2-日志,后门,时间
- 360 星图日志自动分析工具-演示,展望



涉及资源：

https://wangzhan.qianxin.com/activity/xingtu

https://www.cnblogs.com/xiaozi/p/13198071.html

https://www.cnblogs.com/xiaozi/p/12679777.html

https://pan.baidu.com/s/1tQS1mUelmEh3I68AL7yXGg 提取码：xiao
