应急响应

1. web日志
2. 审计设备日志
3. 服务器对应的安全日志
4. 拓扑结构 端口情况
5. 服务器的安全策略
6. 日志保存时间
7. 系统现在什么情况 开了什么端口 服务 中间件 账号口令
8. 样本(webshell 脚本文件 可执行文件)
9. 攻击事件 攻击链路 梳理攻击流程
10. 服务器恢复

windows应急

第一步 web服务器的权限-dmz（www权限 user权限）-代理(出不出网 权限问题) -systeminfo (补丁 版本 基本信息)-tasklist-netstat ano （139 445 ）-cs（权限维持\横向）

业务平台沦陷，在态势感知识检测到，如何快速去响应

1. 态势感知 弱口令？ 漏洞？ 未授权？爆破？ 404 -> 200 断网隔离 上机

代理池-大于阈值-阻断 大批量ip poc 大量源ip请求同一个目的ip 但是请求包是不一样的 多个设备联动

问题 webshell排查?

1.静态排查 先遍历-特征码 特征值 危险函数 误报高易绕过

2.动态排查 webshell在执行命令的时候进程产生 linux -bash windows cmd webshell的http做成特征库 ids做一个检测 检测所有的http请求

3. 日志排查 webshell 不会在系统日志记录 web服务器日志。 一堆get请求里面突然出现post
4. 在线的 阿里伏魔 ct 牧云 河马 离线的D盾

webshell工具都自带修改文件时间戳 linux有个touch windows-powershell

内存马

java web-监听器listener-过滤器filter-servlet三个组件 。

原理 1. jvm加载 .java-.class 工具-注入java包->dump已经加载的class-> 反编译 ->源码webshell的检测

filter或者listener内存马-404 200   200

wheel -管理员组 linux系统加强系统的一个安全性。只允许用户su root 。wheel。

技战法

1. 得有新意 亮点。 国密 零信任 关键基础设施的可信认证。云上一体化。
2. 1500以内 不能技术性太强

方式

1.列出大纲

1. xxx技战法的概述
2. xxx技战法目的
3. 技术手段
4. 防守思路
5. 应急效果

举例

题目：态势感知的主动防御技战法

1. 态势感知的作用，利用了什么技术，怎么做到闭环，如何确保应用系统(关键基础设施)稳定运行。
2. 如何利用态势感知构建一个主动防御检测这么一个服务(怎么联动 快速发现)
3. 关联其他设备(防火墙，ids ips)
4. 清晰化攻击路径快速发现攻击行为。 日志 告警(筛选出外访问内)。
5. 针对人员和系统两个方面-构建一个有应急的体系 提高设备使用率。提高预警能力。