

企业安全应急响应流程

Key老师

本次课重点：

了解企业遭受安全事件，我们应该有什么样的流程，什么排查思路，安全事件确认及分类。

- 1、应急响应流程
- 2、排查方向
- 3、事件确认及分类
- 4、实战演练分享

- 木马演示
- WEB服务器入侵事件
 - LINUX通过SSH入侵WEB服务器攻防演练
- 系统入侵事件
 - WINDWOS通过3389入侵攻防演练
- 网络攻击
 - DDOS原理及攻防演练
 - DNS原理及攻防演练
 - DHCP原理及攻防演练
 - ARP原理及攻防演练

一、响应流程

- 1.1事件发生

运维监控人员、客服审核人员等发现问题，进行安全告警

- 1.2事件确认及分类

收集事件信息、分析网络活动相关程序，日志和数据，判断事件的严重性，评估出问题的严重等级，是否向上进行汇报等。

- 1.3事件响应

各部门通力合作，处理安全问题，具体解决问题，避免存在漏洞未修补、后门未清除等残留问题。

- 1.4事件关闭

处理完事件之后，需要关闭事件，并写出安全应急处理分析报告

二、分析方向

- 2.1 文件分析
- `find` `ls --full-time` `md5sum`
- 文件日期
- 文件增改
- 最近使用文件

三、分析方向

- 2.2日志分析
 - cat /var/log/XXX.log
 - LINUX系统日志分析
 - WINDOWS系统日志分析
 - 应用日志分析
 - tomcat
 - nginx
 - apache等应用日志

三、分析方向

• 2.3进程分析

- top\ps\netstat -ntplu \systemctl list-unit-files\systemctl status
- certutil -hashfile .\inst.ini WIN10查看哈希
- CPU或内存资源占用过多、时间过高
- 进程的路径不合法
- 正在运行的进程
- 正在运行的服务
- 正在运行的程序
- 计划任务
- 文件哈希查看

三、分析方向

- 2.4 身份信息分析
 - 本地以及域账号用户
 - 异常的身份验证

三、分析方向

- 2.5网络分析
 - 网络设备配置
 - DNS配置
 - 路由配置
 - 监听端口和相关服务
 - 最近建立的网络连接
 - RDP / VPN / SSH 等会话

三、分析方向

- 2.6配置分析
- cat\ getenforce\ iptables -L\ echo \$PATH
- 查看Linux SE, IPTABLES等配置
- 查看环境变量

三、分析方向

- 2.7 监控查看
- 如zabbix等监控查看

三、事件确认及分类

- 病毒、木马、蠕虫事件
- **Web**服务器入侵事件
- 第三方服务入侵事件
- 个人系统入侵事件
- 网络攻击事件

六、实战演练

- 木马演示
- WEB服务器入侵事件
 - LINUX通过SSH入侵WEB服务器攻防演练
- 第三方服务入侵事件 【不演示】
- 系统入侵事件
 - WINDWOS通过3389入侵攻防演练
- 网络攻击
 - DDOS原理及攻防演练
 - DNS原理及攻防演练
 - DHCP原理及攻防演练
 - ARP原理及攻防演练

Thank you

Key老师