木马攻击实战演练

Key老师

重点

一、通过实际安全演练回顾应急排查流程
二、本次分享攻击方法只可在实验环境中测试

环境介绍

攻击者
kail:192.168.188.134
下载地址：https://mirrors.aliyun.com/kali-images/kali-2021.3/kali-linux-2021.3-live-i386.iso

被攻击者：
win10: 192.168.188.132

总结

windows木马排查方向
1、可能通过网络连接观察异常的端口或者IP通信
2、可以通过任务管理器，详细信息，找到异常文件，使用杀毒软件检测

防御：
1、开启windows 防火墙
2、安装正版杀毒软件

Thank you