windows系统实战演练

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：
WINDOWS: 192.168.188.132

工具介绍

hydra又名九头蛇， 是一个网络帐号破解工具，支持多种协议,hydra在所有支持GCC的平台能很好的编译，包括Linux,所有版本的BSD,Mac OS, Solaris等

总结

个人电脑排查方向
1、查看日志，分析服务器登陆时间及IP
2、查看用户是否有异常

防御：
1、密码大小写，数字，字符不低于8位
2、3389如非必须，不开启个人电脑3389端口
3、如开启3389，指定固定IP可连接

Thank you