

服务器入侵实战演练

Key老师

- 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

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:

LINUX: 192.168.188.130

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:

LINUX: 192.168.188.130

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

服务器网页篡改排查方向

- 1、排查网页修改时间
- 2、查看日志，分析服务器登陆时间及IP

防御：

- 1、服务器密码强密码
- 2、22端口不对公网直接开放
- 3、使用堡垒机及指定IP登陆

Thank you

Key老师