DDOS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
linux:192.168.188.131

Server：
linux:192.168.188.130

攻击方法介绍

CC攻击：攻击者借助代理服务器生成指向受害主机的合法请求，实现DDOS和伪装就叫：CC(Challenge Collapsar)，CC主要是用来攻击页面的。

SYN攻击：SYN攻击是黑客攻击的手段。SYN洪泛攻击的基础是依靠TCP建立连接时三次握手的设计。

纯流量攻击：发送大量垃圾流量

总结

八方网域
bafangwy.com

DDOS排查方向
1、监控查看公网出口网络流量
2、查看服务器网络链接
3、查看应用日志

防御：
1、接入第三方抗DDOS云平台

Thank you