八方网域
bafangwy.com

DNS&DHCP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:192.168.188.130

被攻击者：
win10: 192.168.188.132

DNS&DHCP安装

DNS安装
yum install bind bind-utils -y

DHCP安装:
yum install dhcp

总结

DNS&DHCP排查方向
1、排查电脑本机hosts文件是否有静态绑定
2、重启浏览器，确认是否有浏览器缓存
3、ipconfig/all 查看 DHCP服务器及DNS服务器IP是否正确

防御：
1、网络接入认证
2、定期网络扫描，是否有内网IP提供DNS服务
3、dhcp Snooping开启，防止非法DHCP服务器

Thank you