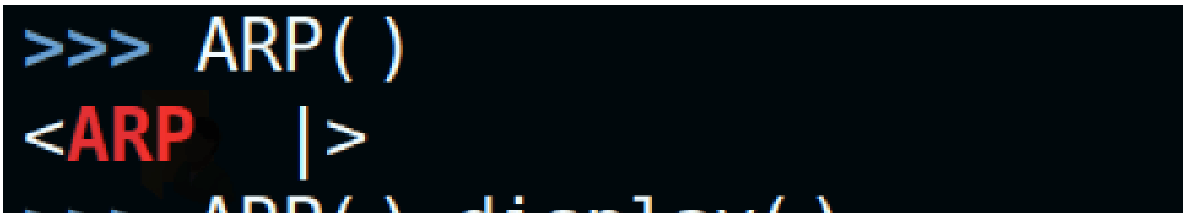
Scapy

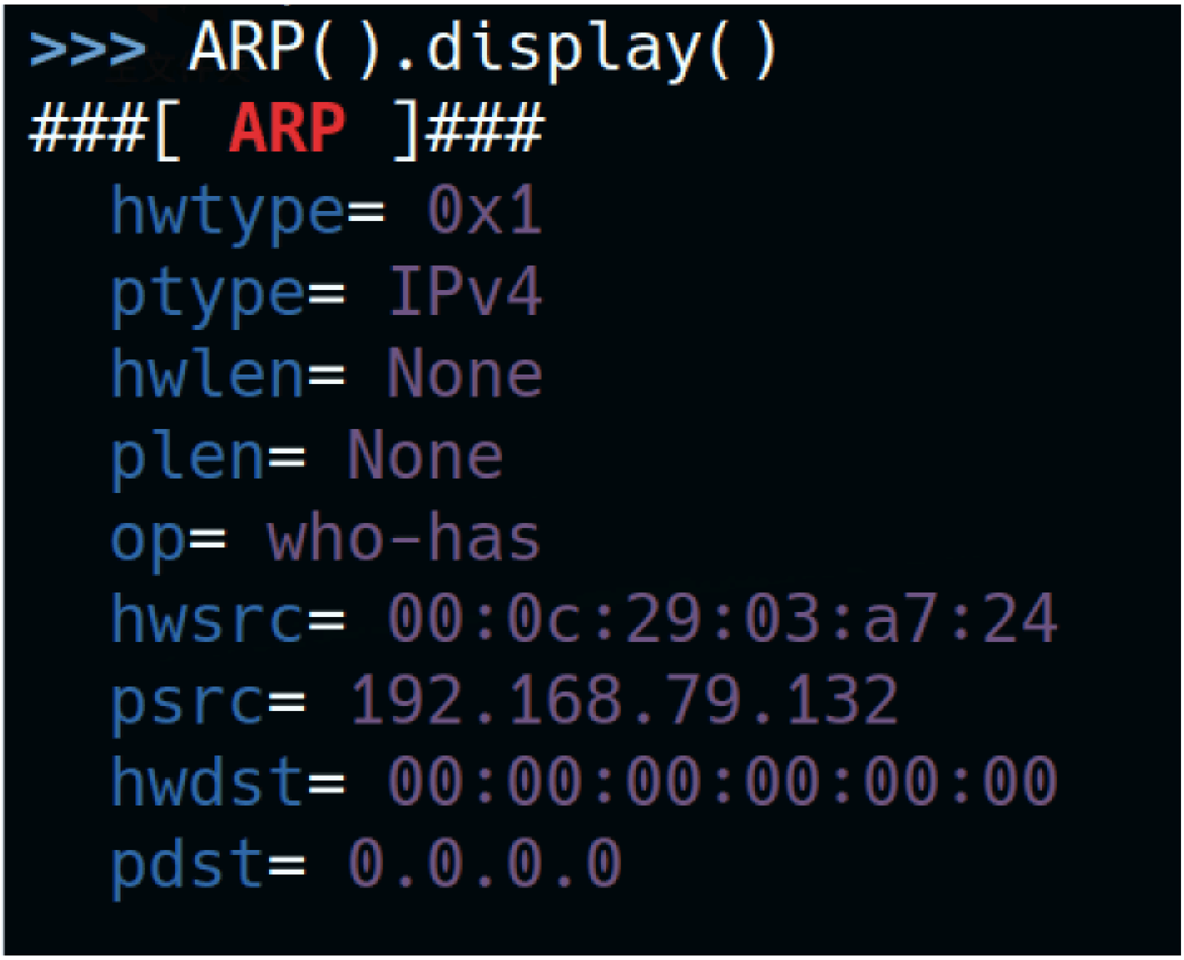
Scapy是Python上的一个强大的构造网络数据包的模块，它可以完成绝大多数工具所能完成的功能，例如：扫描，网络发现，跟踪路由，探测，单元测试，攻击等。。。它也可以发送无效数据帧、注入修改的802.11数据帧、在WEP上解码加密通道（VOIP）、ARP缓存攻击（VLAN） 等。

一，修改或构造包头（ARP）
1.调用ARP函数
ARP()



```
>>> ARP()
<ARP  |>
>>> ARP().display()
```

2.数据包结构
ARP().display()
显示ARP数据包结构

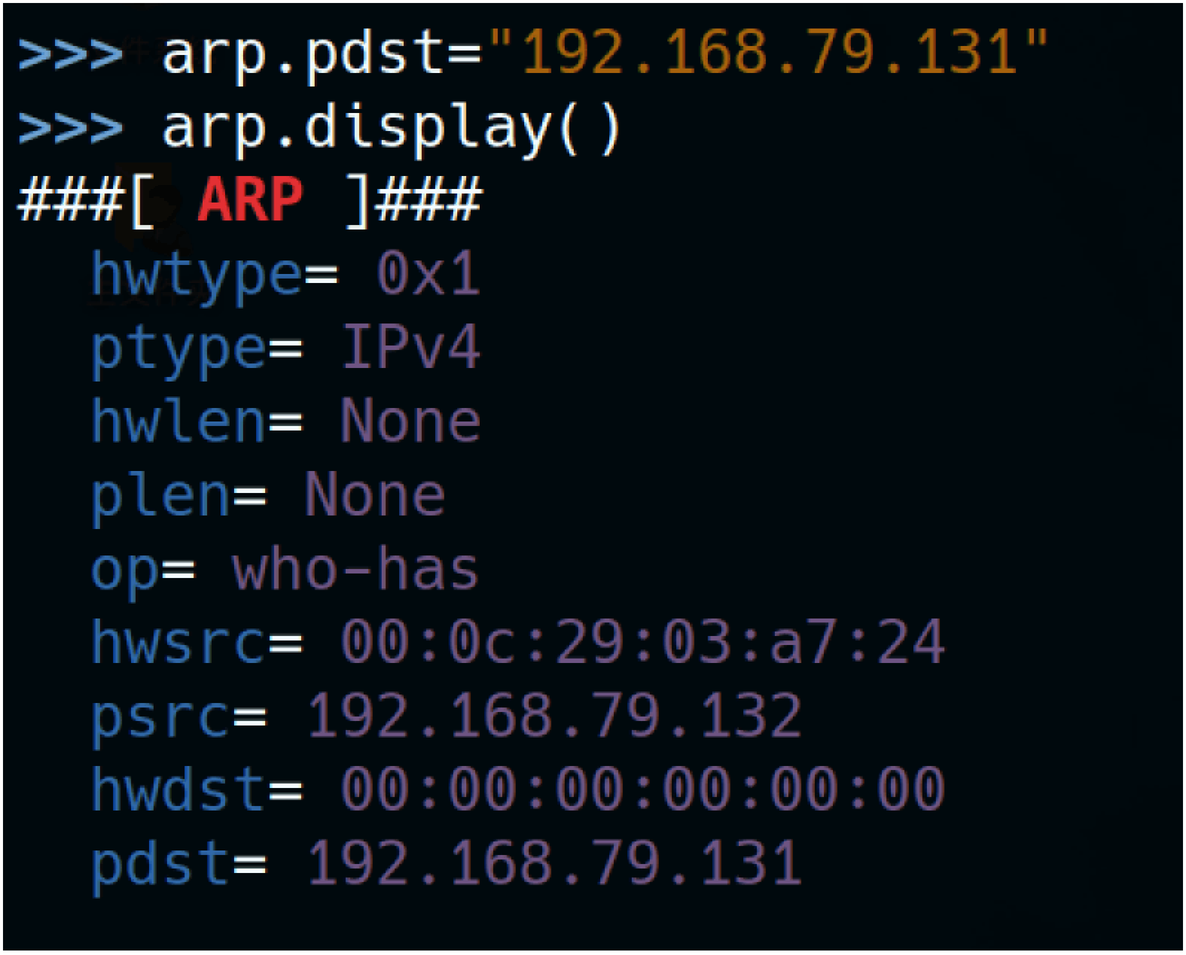


```
>>> ARP().display()
###[ ARP ]###
  hwtype= 0x1
  ptype= IPv4
  hwlen= None
  plen= None
  op= who-has
  hwsrc= 00:0c:29:03:a7:24
  psrc= 192.168.79.132
  hwdst= 00:00:00:00:00:00
  pdst= 0.0.0.0
```

3.修改数据包结构

arp.pdst=“192.168.79.131”

在arp数据包中修改pdst地址为192.168.79.131

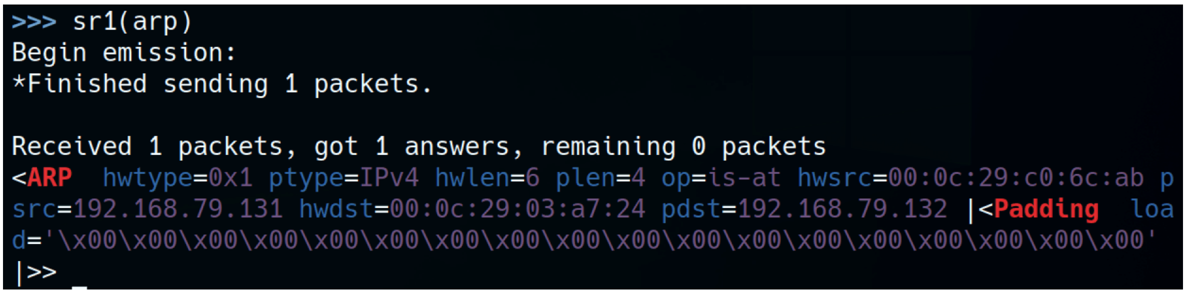


```
>>> arp.pdst="192.168.79.131"
>>> arp.display()
###[ ARP ]###
  hwtype= 0x1
  ptype= IPv4
  hwlen= None
  plen= None
  op= who-has
  hwsrc= 00:0c:29:03:a7:24
  psrc= 192.168.79.132
  hwdst= 00:00:00:00:00:00
  pdst= 192.168.79.131
```

3.发送数据包

sr1(arp)

发送数据包



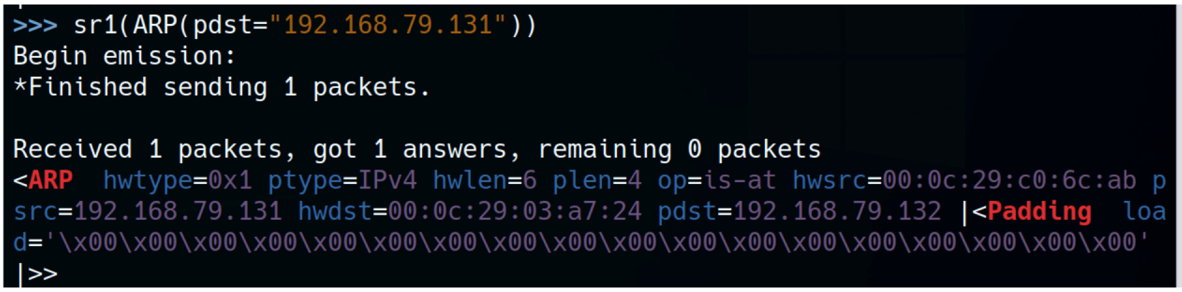
```
>>> sr1(arp)
Begin emission:
*Finished sending 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
<ARP  hwtype=0x1 ptype=IPv4 hwlen=6 plen=4 op=is-at hwsrc=00:0c:29:c0:6c:ab p
src=192.168.79.131 hwdst=00:0c:29:03:a7:24 pdst=192.168.79.132 |<Padding  loa
d='\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
|>>
```

4.一句话方式

(1)

sr1(ARP(pdst="192.168.79.131"))

将ARP包发送至192.168.79.131



```
>>> sr1(ARP(pdst="192.168.79.131"))
Begin emission:
*Finished sending 1 packets.

Received 1 packets, got 1 answers, remaining 0 packets
<ARP  hwtype=0x1 ptype=IPv4 hwlen=6 plen=4 op=is-at hwsrc=00:0c:29:c0:6c:ab p
src=192.168.79.131 hwdst=00:0c:29:03:a7:24 pdst=192.168.79.132 |<Padding  loa
d='\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'
|>>
```

（2）

```
sr1(ARP(pdst="192.168.79.131"),timeout=1,verbose=1)
```

将ARP包发送至192.168.79.131，丢失一个，保留一个

二，构造一个TCP/IP包

```
i = IP()
```

定义一个三层的包头

```
t = TCP()
```

定义一个四层包头

```
r = (i/t)
```

将三层和四层的包头组合起来

```
r.display
```

来将来显示数据包内容

```
r[IP].dst="192.168.78.103"
```

在 IP包头中设置dst目标

```
r[TCP].flags="A"
```

设置数据包中的flags 为Ack

```
a=sr1(r)
```

发送一个数据包向目标请求

```
r.display
```

显示收到的数据包内容

```
a=sr1(r, timeout=1)
```

发送一个请求包，如果没有响应认定离线。

一句话命令

```
a = sr1(IP(dst="192.168.79.131")/TCP(dport=80,flags='A') ,timeout=1)
```

设置数据包目标192.168.79.131，TCP包发送80端口。Ack.发送一次、