ICMP

ICMP

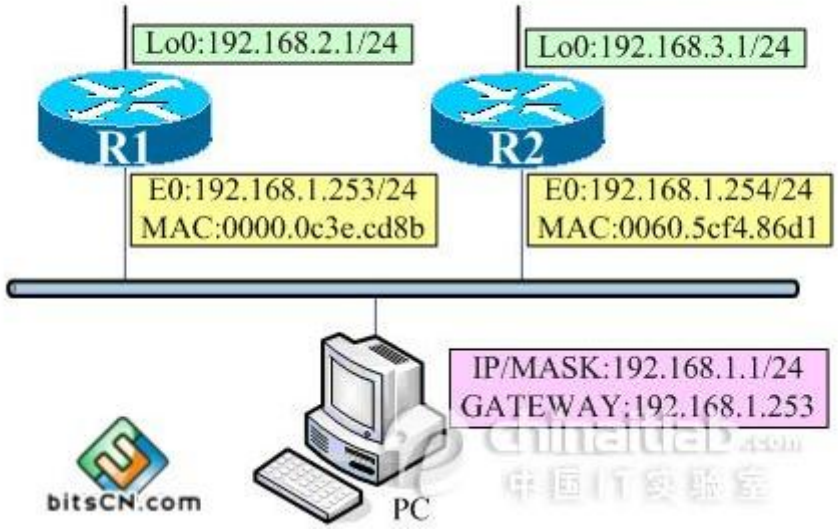
- 实验内容：
- ICMP重定向攻击
- 在特定的情况下，当路由器检测到一台机器使用非优化路由的时候，它会向该主机发送一个ICMP重定向报文，请求主机改变路由。路由器也会把初始数据报向它的目的地转发

ICMP

- 实验目的：
  - 构建一个ICMP重定向报文
  - 通过此报文构造一条新的网关记录，使得系统无法上网

ICMP

- ICMP重定向

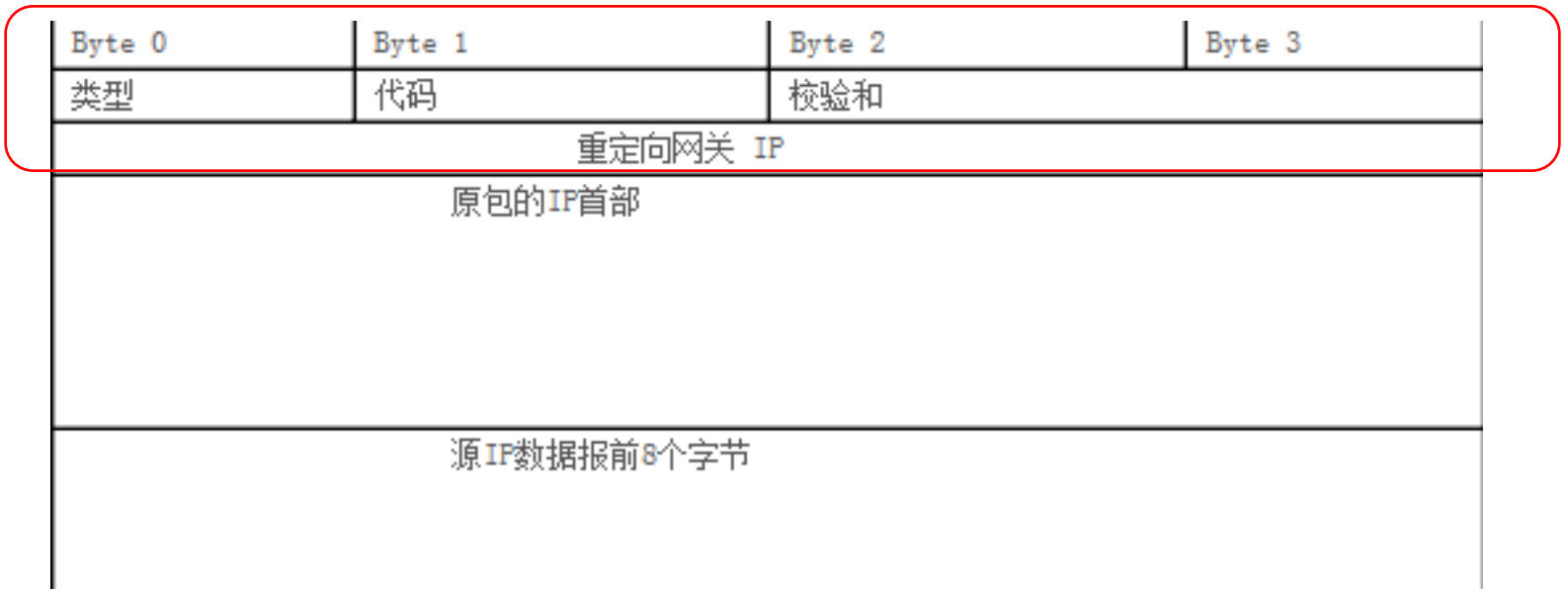


ICMP

- 主机PC要ping路由器R2的192.168.3.1，主机将判断出目标属于不同的网段，因此它要将ICMP请求包发往自己的默认网关192.168.1.253（路由器R1的E0接口）。但是，这之前主机PC首先必须发送ARP请求，请求路由器R1的E0（192.168.1.253）的MAC地址。
- 当路由器R1收到此ARP请求包后，它首先用ARP应答包回答主机PC的ARP请求（通知主机PC：路由器R1自己的E0接口的MAC地址）。然后，它（路由器R1）将此ICMP请求转发到路由器R2的E0接口：192.168.1.254（要求路由器R1正确配置了到网络192.168.3.0/24的路由）。此外，路由器R1还要发送一个ICMP重定向消息给主机PC，通知主机PC对于主机PC请求的地址的网关是：192.168.1.254。
- 路由器R2此时会发送一个ARP请求消息请求主机PC的MAC地址，而主机PC会发送ARP应答消息给路由器R2。最后路由器R2通过获得的主机PC的MAC地址信息，将ICMP应答消息发送给主机PC。

ICMP

- 构建ICMP字段部分（8+20+8）



ICMP

- 类型：
- 5 代表ICMP重定向报文
- ICMP重定向报文有四种不同类型的报文，有不同的代码值：
- 0 = 重定向网络的数据报；不仅对今后所有发往其地址引发该重定向报文的设备的数据报重定向，而且对发往该设备所在网络上所有其它设备的数据报重定向。
- 1 = 重定向主机的数据报；仅对今后所有发往初始数据报指向的具体设备地址的数据报重定向。
- 2 = 重定向网络和服务类型（TOS）的数据报；含义与编码值0相同，但只适用于今后与初始数据报具有相同TOS值的数据报。
- 3 = 重定向网络和主机类型的数据报；含义与编码值1相同，但只适用于今后与初始数据报具有相同TOS值的数据报。

ICMP

- ICMP报文包含在IP数据报中，属于IP的一个用户，IP头部就在ICMP报文的前面
- IP头部的Protocol值为1就说明这是一个ICMP报文

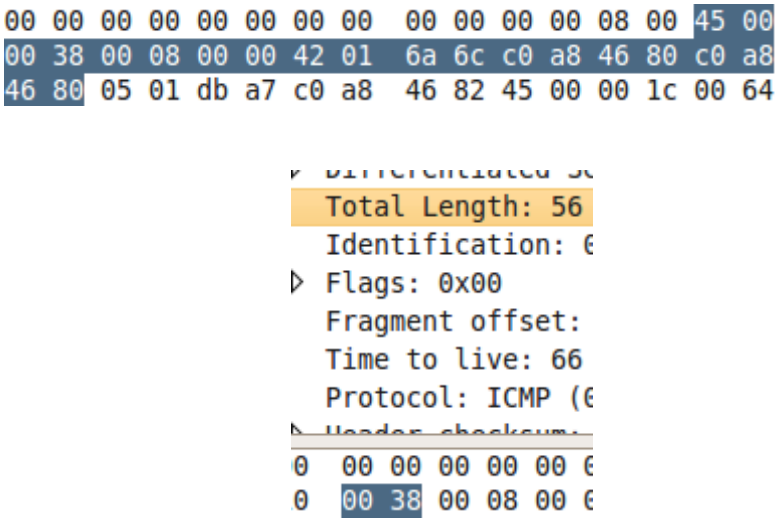
ICMP

- 构建重定向包

```
struct ip {
        u_int   ip_hl:4,                /* header length */
        ip_v:4;                 /* ip version */
        u_char  ip_tos;                 /* type of service */
        u_short ip_len;                 /* total length */
        u_short ip_id;                  /* identification */
        u_short ip_off;                 /* fragment offset */
        u_char  ip_ttl;                 /* time to live */
        u_char  ip_p;                   /* protocol */
        u_short ip_sum;                 /* checksum */
        struct  in_addr ip_src,ip_dst;  /* source and dest address */
};
```

ICMP

- ip->ip_len = htons( );
- ip头的长度20个字节+ICMP

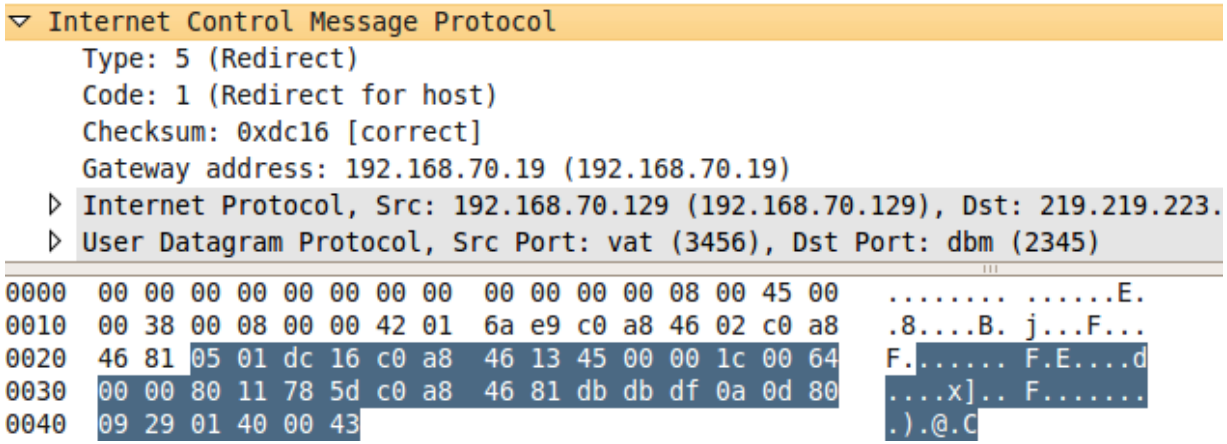


ICMP

- icmp->icmp_type = ICMP_REDIRECT;
-
- icmp->icmp_code = 1;
-
- icmp->icmp_cksum = 0;
- icmp->icmp_cksum = in_cksum((unsigned short *)icmp,36);

ICMP

- 重定向网关IP
- icmp->icmp_gwaddr



ICMP

- 原包的IP首部(20个字节)
- 跟上一个包相同即可
- struct ip *icmpip = (struct ip *)(buff+28);
- icmpip->ip_p = IPPROTO_UDP;

ICMP

- 源IP数据报的前八个字节
- struct udphdr * udp;
- udp = (struct udphdr *) (icmpip+1);
- udp->source
- udp->dest
- udp->len
- udp->check
-

ICMP

- 包构造好了
- icmp->icmp_cksum = 0;
- 计算（8+20+8）
- sendto(sockfd, buff, 56,0,(struct sockaddr *)&target,sizeof(target));
-

ICMP

- 路由设置的标准：
  - 新路由必须是直达的
  - 重定向包必须来自去往目标的当前路由
  - 重定向包不能通知主机用自己做路由
  - 被改变的路由必须是一条间接路由

ICMP

- 实验中的路由构建如下：
- A：攻击者（192.168.70.2）
- B：受害者（192.168.70.129）
- B中有路由信息通过192.168.70.2可以到达目的地219.219.223.10
- A向B发送一个重定向报文，使得网关地址192.168.70.2变成自己设定的icmp->icmp_gwaddr