攻击类型

Mitnick attack

1. 探测信赖关系
2. 发送SYN给x-terminal建立连接，预测 x-terminal的序列号
3. 发送SYN给Server，SYN Flooding攻击，使Server不能响应其他任何连接请求，同时也不会对不请自来的SYN-ACKs发送RST
4. 利用IP 欺骗向x-terminal发送SYN，根据预测的序列号，发送ACK给x-terminal,连接建立完成
5. 发送指令 : rsh x-terminal "echo + + >>/.rhosts"，该指令在x-terminal上建立起使得任何主机都可以无须口令而行访问的/.rhosts文件，然后断开连接。
6. 发送RESETs给Server，清空连接队列，防止其他试图连接Server的人发现异常

基于ARP协议的攻击

ARP缓存中毒

ARP介绍

ARP是个地址解析协议。最直白的说法是：在IP-以太网中，当一个上层协议要发包时，有了节点的IP地址，ARP就能提供该节点的MAC地址。

ARP缓存： ARP cache 是个用来储存(IP, MAC)地址的缓冲区。当ARP被询问一个已知IP地址节点的MAC地址时，先在ARP cache 查看，若存在，就直接返回MAC地址，若不存在，才发送ARP request向局域网查询。【在A不知道B的MAC地址的情况下，A就广播一个ARP请求包，请求包中填有B的IP(192.168.1.2)，以太网中的所有计算机都会接收这个请求，而正常的情况下只有B会给出ARP应答包，包中就填充上了B的MAC地址，并回复给A。A得到ARP应答后，将B的MAC地址放入本机缓存，便于下次使用。本机MAC缓存是有生存期的，生存期结束后，将再次重复上面的过程。】【ARP请求和ARP回复。请求和回复的目的在于确定与特定IP地址相关的硬件MAC地址，这样流量才能够在网络上找到目的地。请求数据包被发送给网络段上的每台设备并发出信息"我的IP地址是XX.XX.XX.XX，我的MAC地址是 XX:XX:XX:XX:XX:XX，我需要将信息发送给这个IP地址XX.XX.XX.XX，但是我不知道它的硬件地址，请这个IP地址将其MAC地址回复给我?"回复会以ARP回复数据包的形式，并回复说"你好，传递设备，我就是你要找的IP地址XX.XX.XX.XX，我的MAC地址是 XX:XX:XX:XX:XX:XX"，收到回复后，传递设备会更新其ARP缓存表，然后设备就可以与另一台设备进行通信。】

ARP欺骗： 任何机器都可以向另一台主机发送ARP回复数据包，并迫使主机更新其ARP缓存。假冒IP和MAC。

ARP协议并不只在发送了ARP请求才接收ARP应答。当计算机接收到ARP应答数据包的时候，就会对本地的ARP缓存进行更新，将应答中的IP和MAC地址存储在ARP缓存中。

因此，当局域网中的某台机器B向A发送一个自己伪造的ARP应答，而如果这个应答是B冒充C伪造来的，即IP地址为C的IP，而MAC地址是伪造的，则当A接收到B伪造的ARP应答后，就会更新本地的ARP缓存，这样在A看来C的IP地址没有变，而它的MAC地址已经不是原来那个了。由于局域网的网络流通不是根据IP地址进行，而是按照MAC地址进行传输。所以，那个伪造出来的MAC地址在A上被改变成一个不存在的MAC地址，这样就会造成网络不通，导致A不能Ping通C！这就是一个简单的ARP欺骗。

危害：

1. **拒绝服务** 一个黑客可以只做简单的操作就将一个重要的IP地址和一个错误的MAC地址绑定。例如，黑客可以发送一个ARP响应报文 (到你的计算机) 将你所在网络的路由器 (即我们常说的网关，译者注) IP地址和一个根本不存在的MAC地址绑定起来。你的计算机以为它知道默认网关在哪，但是事实上它的所有数据包，其目的地址都不在这个网络的网段上 (因为那个不存在的MAC不在此局域网的网段上，译者注)，它们最后消逝在了无尽的比特流中 (即因数据包的生命周期到了而信号消失，译者注)。仅仅这一下，黑客就能阻止你连上因特网。
2. **中间人攻击** 黑客利用ARP缓存中毒来截获你的局域网中两台设备之间的网络信息。例如，我们假象黑客想要窃听你的计算机，192.168.0.12，和你的网络路由器 (即网关，译者注)，192.168.0.1，之间的通信信息。黑客先发送一个恶意的ARP “响应” (因为在此之前根本没有请求) 到你的路由器，将他的计算机的MAC地址和192.168.0.12绑定。然后，黑客在发送一个恶意的ARP响应到你的计算机，将他的MAC地址和192.168.0.1绑定起来。现在你的机器以为黑客的计算机是你的路由器了。最后，黑客开启一个叫IP转发的系统功能。这个功能让黑客能将所有来自你的计算机的网络信息转发到路由器。现在，只要你尝试上网，你的计算机就会将网络信息发送到黑客的机器上，然后黑客再将其转发到路由器。由于黑客仍然将你的信息转发到网络路由器，所以你并不会察觉到他已经截获了所有你的网络信息，或许还窃听了你的明文密码或者劫持了你曾经安全的网络会话
3. **MAC洪泛** MAC洪泛是一种旨在网络交换机的ARP缓存中毒技术。当这些交换机流量超载时它们常常进入到 “集线器” 模式。在 “集线器” 模式中，交换机由于太过繁忙而不能执行它的端口安全检测功能，而是仅仅向网络中的每一台计算机广播所有的网络数据。利用大量的假冒ARP响应数据包去洪泛一台交换机的ARP映射表，黑客能使大多数制造商的交换机超载，然后当交换机进入 “集线器” 模式时，就可以发送 (恶意的) 包去嗅探你的局域网。

防御

1. **小型网络** 静态IP地址和静态ARP映射表。
2. **大型网络** “端口安全” 功能是允许你强制使你的交换机在每个端口只允许 (IP地址对应的) 一个MAC地址通过。这个功能会阻止黑客改变他机器的MAC地址或试图映射多个MAC地址到他的机器上。
3. **一般网络** ARP监视工具，比如ARPwatch，当有不正常的ARP通信时它会提醒你。

利用Ip协议发起的工具

Denial of Service Attack

1st fragment: offset = 0

2nd fragment: offset = 64800

在早期的计算机中，目标计算机会分配64k的内存空间，但大多数操作系统都会崩溃

TearDrop

将Ip报文分片，使得第二个分片完全被第一个分片包含，目标计算机在进行Ip报文重组的时候将导致系统崩溃。

Overlapping attacks against firewalls

利用Ip报文分片重叠，逃过防火墙的检查。防火墙一般被设置为只检测第一个分片，然后对TCP的报头进行检查。

Tiny Fragment Attack

将Ip报文分片的第一个分片设置为68byts，将前面60byts填充为Ip报文头部，余下8byts只包含TCP的源端口和目的端口。

Overlapping Fragment Attack

将第二个分片的偏移设置为1，FO=1

利用ICMP协议实现的攻击

Smurf Attacks

Ping an IP-directed broadcast address, with the (spoofed) IP of a victim as the source address.

Until1999,standad required routers to forward such packets. Impact: All hosts on the network will respond to the victim, and thus overwhelm the victim.

This is a denial-of-service attack.

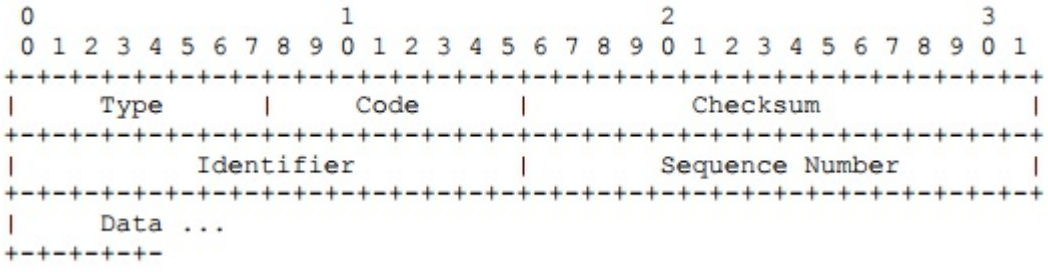
The key idea of this attack: Amplification and IP spoofing This is a protocol vulnerability. To solve this problem, we can do the following:

- Disable IP-directed broadcasts at the router.
- Configure the operating system to prevent the machine from responding to ICMP packets sent to IP broadcast addresses.

```
/proc/sys/net/ipv4/icmp_echo_ignore_all
/proc/sys/net/ipv4/icmp_echo_ignore_broadcast
```

Ping of Death

ping包icmp数据报的结构如下：



其中，前三个域是每一种类型icmp报文都相同的。icmp报文中没有关于报文长度的字段，所以icmp最大长度为ip报文最大长度减去20bytes的ip头长度。既是，65535-20=65515.

ping of death 攻击 是通过在最后分段中，改变其正确的偏移量和段长度的组合，使系统在接收到全部分段并重组报文时总的长度超过了65535字节，导致内存溢出，这时主机就会出现内存分配错误而导致TCP/IP堆栈崩溃，导致死机！

ICMP Redirect Attack

Send an ICMP redirect packet to the victim, asking it to send its packet to another “router”

Impact: man-in-the-middle attacks or DOS attacks