信息安全作业 8

190110429-何为

1. ARP 欺骗的原理是什么？

答：

（1） ARP 协议：当主机接收到 ARP 应答数据包的时候，就使用应答数据包内的数据对本地的 ARP 缓存进行更新或添加。

（2） 根据该协议，假设主机 D 想监听主机 A 和主机 C 之间的通信内容，只需给 A 和 C 发送 ARP 应答，告诉主机 A：主机 C 的 MAC 地址是 D 的物理地址，告诉主机 C：主机 A 的 MAC 地址是 D 的物理地址。

（3） 这样，A 想要发送给 C 的数据实际上发送给了 D，D 在嗅探到数据后将此数据转发给 C。C 回应 A 的数据也发给了 D，D 嗅探之后转发给 A。

2. DNS 欺骗是如何实现的？

答：

冒充域名服务器，然后把查询的 IP 地址设为攻击者的 IP 地址，这样的话，用户上网就只能看到攻击者的主页，而不是用户想要取得的网站的主页了，这就是 DNS 欺骗的基本原理。

3. 不使用 strcpy()函数，写一个能引起缓冲区溢出的小程序，并简要解释该程序为什么会引起缓冲区溢出。

答：

代码如下：

```
#include <iostream.h>
int main()
{
      char str[4] = {0};
      scanf("%s", str);
      return 0;
}
```

因为 scanf()在读入时不会进行边界检查，因此在输入字符串的时候，如果输入的字符串超过了指定的长度，会造成溢出错误。