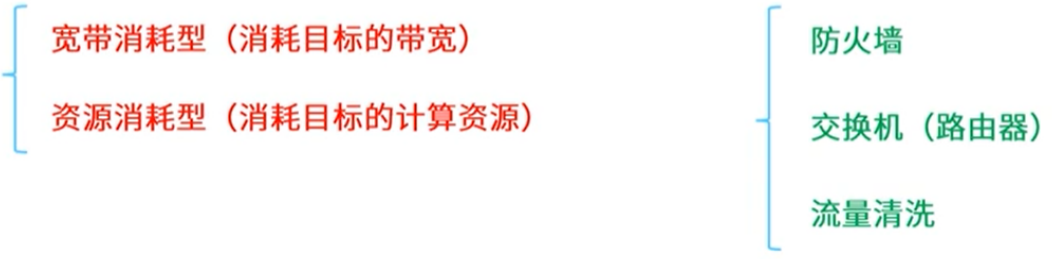
课程小结

攻击手段和防御策略

- **阻断服务攻击(Dos):**阻断服务攻击(Denial -of service attack) 想办法将目标网络资源用尽
- **Dos的变种DDOS**:分布式阻断服务攻击(Distributed Denial -of service attack)

阻断服务攻击是从攻击者的服务器请求过来的,这个很容易被定位到,目标太明显,另外通过安全策略把攻击的IP屏蔽掉就无法的攻击了.比较的难的是分布式恶阻断服务攻击.在互联网上有大量的"肉鸡",所谓肉鸡就是被病毒感染的计算机,攻击者可以通过远程来控制这些计算机.黑客通过指挥大量的肉鸡攻击你服务. 比如"

1. 不断的给你发送http请求
2. 不断的发送TCP/IP封包,握手,消耗你的宽带,直至崩溃
3. 人肉ddos,前端自己写的程序造成的,很悲催)



有下三种防御手段:

防火墙:好的硬件防火墙,可以根据异常流量的ip

识别的攻击者,一般正常流量是差不多的,肉鸡的话是尽可能消耗多一点的流量,防火墙可以识别出来并添加到黑名单.DDOS是需要成本的,撑不了很久的

交换机:和防火墙功能差不多的,只是更加高级.

流量清洗:也是同防火墙功能差不多的.

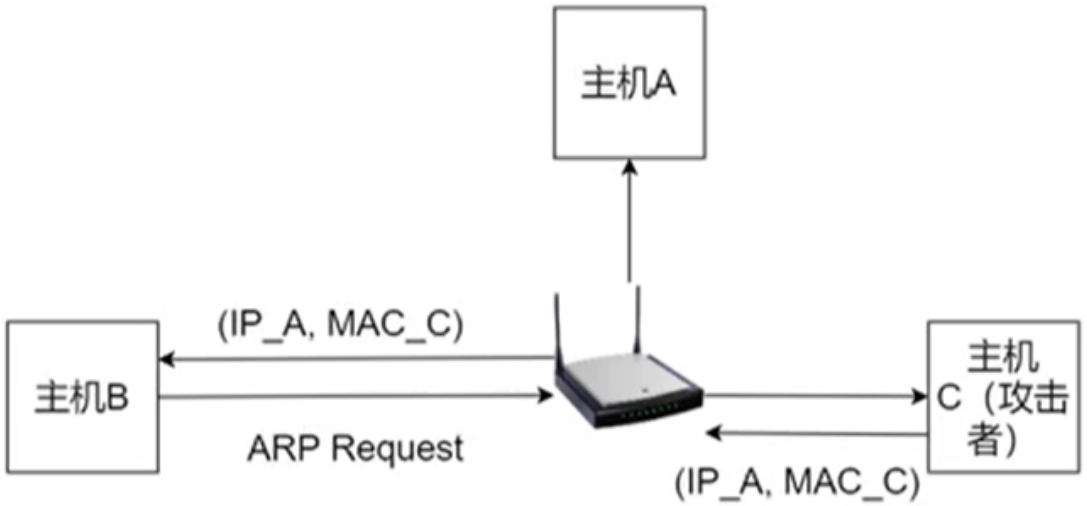
一般碰到DDOS工具,我们首先会联系运营商增加带宽,保证的用户能正常使用.ddos攻击支撑不了太长时间的.

- **地址解析欺骗(ARPS)**

早期就用来攻击现在主要是用来调试,在一个局域网当中

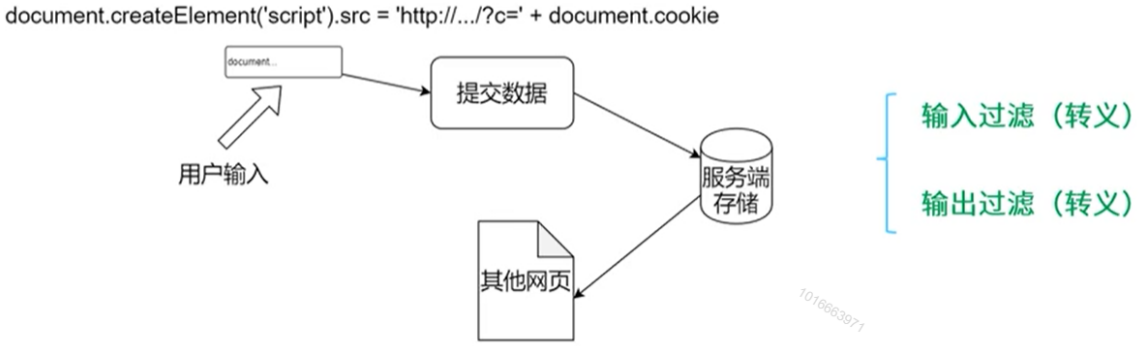
,每台主机在内网有自己IP,每个主机有自己的MAC地址,每一个主机都会定期发一个ARP请求,通过的路由广播出去.这时候攻击者就有机会了.主机B发送ARP到路由器,广播出去.主机A接收到,主机C攻击加入他模拟主机A的IP 但是MAC地址确实C的,这样主机B发送ARP请求,却被主机C给接收到了.路由只看MAC地址.主机A和主机B通讯中间都多个攻击者C,攻击者可能监听数据,或者篡改数据.

但是现在很少用于攻击了.都是用来局域网之间的调试了.



- **跨站脚本攻击(xss)**

原理:将跨站脚本(Cross site Scripting)注入到被攻击的网页上,用户打开网页会执行跨站脚本

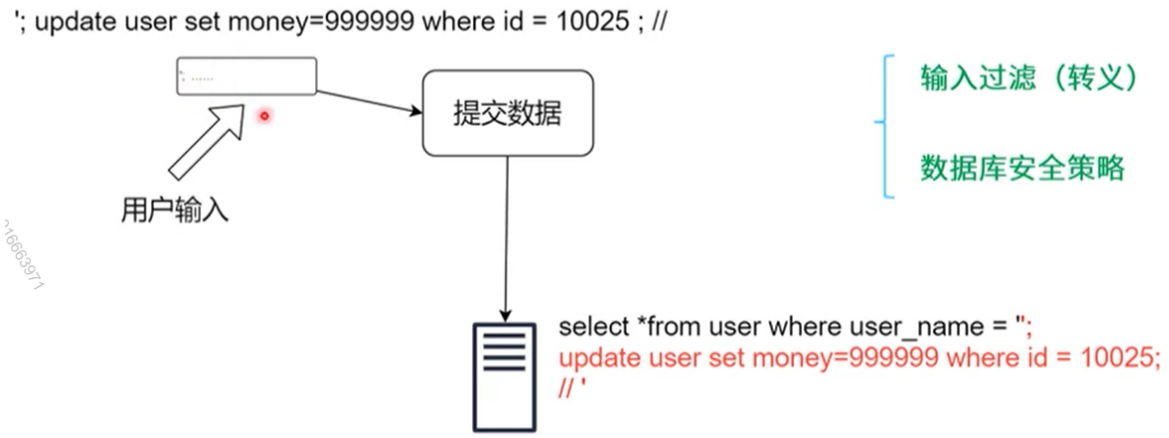


一般用户在输入的时候,黑客会输入一段简本的.然后提交数据到服务器.如果是一个文本的话还好,可以直接展示出来,如果是一个服务本机器的,提交的到服务器存储后,在页面显示出来的话,直接是一段script标签就直接执行了这段脚本.这样就被跨脚本攻击.最后多就是提交数据后,后面出现很多广告,或者恶意js.

如何防止,需要在输入过滤,在输出也进行过滤.

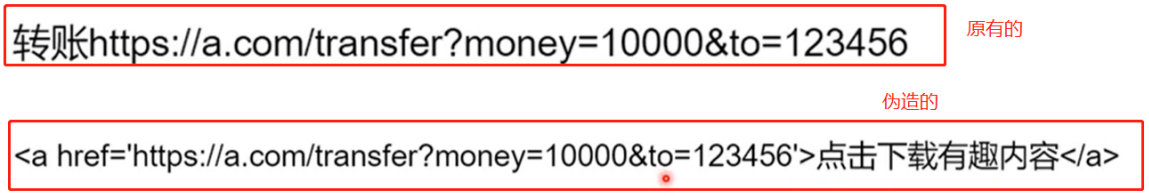
- **SQL注入**

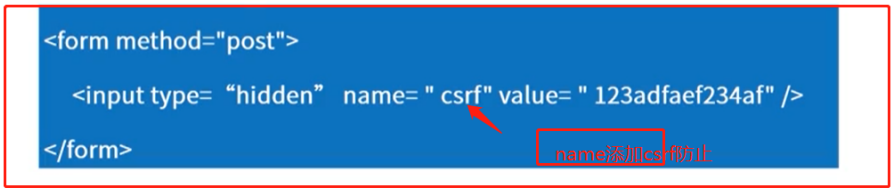
原理:在客户端的用户需要输入账号密码,黑客直接输入一段sql脚本,服务端如果没有做过滤的话,提交的服务端的sql脚本也会执行.这样就SQL注入就成功了.所以在和后端人员对接的话,提醒一下后端人员做sql过滤.需要输入过滤,使用数据库安全策略



- **跨站请求伪造(csrf)**

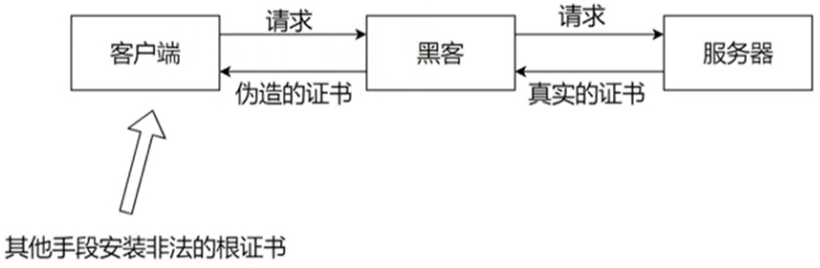
早期的时候大家都把get和post用混.





- **https中间人攻击**

https中间人攻击很重要的一点,黑客在客户端用其他手段安装非法的根证书.这个是非常重要的一点. 抓包和爬虫都是利用了中间人这特点.也是比较常用的



将黑客换成Fiddle,Chales,Whistle 这些合法工具，这个就是HTTPS抓包的原理

预防策略: 不要轻易安装一些非法根证书,保护电脑安全

课程小结

- 加强安全意识
- 安全是高压线，遵循公司SOP

密码不要随便给同事,相关密码需要保密,隐私需要保护等等.....