中间人攻击实验

计 64 翁家翌 2016011446

2017.11

1 实验环境

攻击者：Ubuntu 16.04.3 LTS
路由：小米路由（Openwrt 内核）、手机热点
靶机：Ubuntu 16.04、Win10、Macbook Pro、iPhone、iPad、小米手机等

2 实验原理

1. 使用 scapy 构造 arp 包，对网关和受害者发送欺骗信息，修改其 arp 缓存
2. scapy 脚本嗅探所有 src/dst 为靶机 ip 地址，并且含有 IP 层信息的包，将其修改 src/dst 之后转发
3. 配置本机 iptables，其中 ip_forward 选项设置为 1，并且转发 53,80,443 端口至本机 8080 端口，以便 mitmproxy 进行处理；将用脚本处理之后的包发送至原地址

其中，攻击脚本为 mitm.py，包含构造 ARP 报文、嗅探数据包的功能；修改 http 数据流的脚本为 a.py，实现了将所有图片旋转 180° 的功能

3 实验现象

3.1 Ubuntu 16.04

查看路由和靶机的 arp 缓存，发现修改成功
修改 iptables 配置，如图1所示：

图 1: iptables 的配置情况

以 root 权限运行命令 python3 mitm.py 和 mitmproxy -T -s a.py，查看截获的流量，发现靶机成功被欺骗。(忘记截图了)

经过测试，虚拟机环境下的 Ubuntu 也能够被欺骗。

3.2 Win10

配置与之前相同。Win10 被成功欺骗。在 Win10 上使用 Chrome 浏览器进行测试，效果如下：

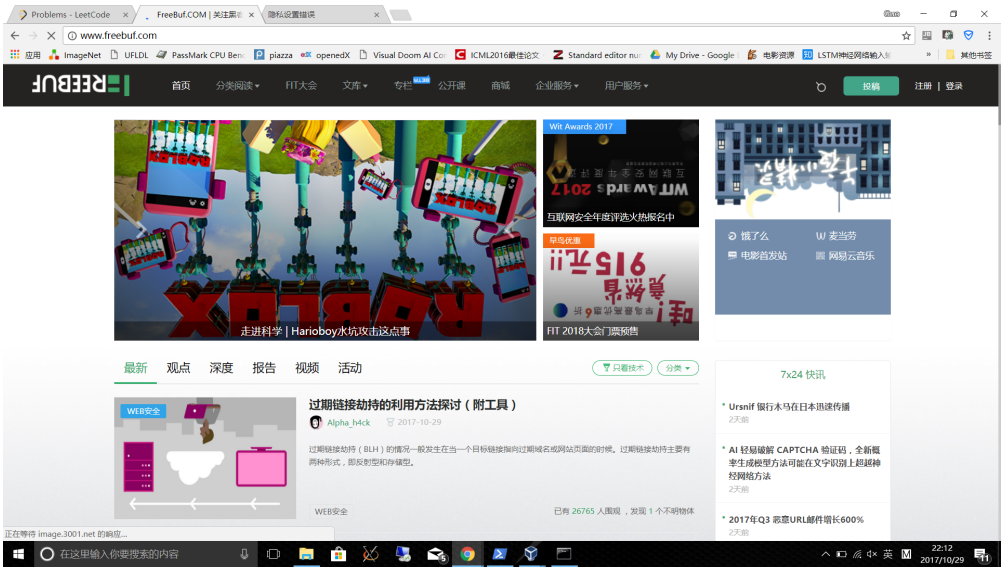

图 2: 访问 http://www.freebuf.com

图2显示了靶机访问 http 网站的现象，可以看到访问正常，但是所有图片都被倒置了。在测试的时候，访问网页的速度较慢，可能是因为图片处理的速度不够快导致。

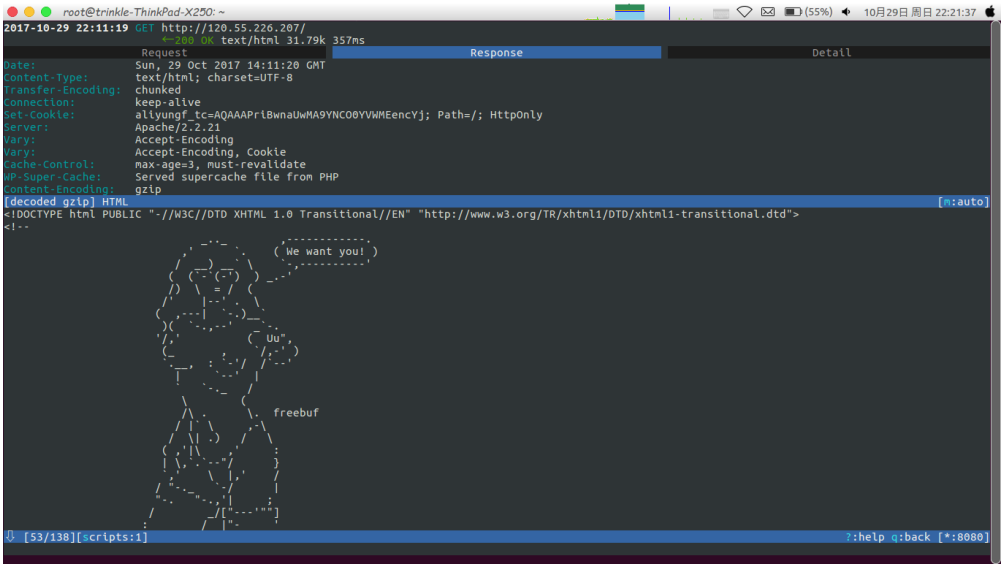

图 3: 在攻击者上看到的 http 流量报文

图3显示了攻击者机器上看到的 http 报文的数据。

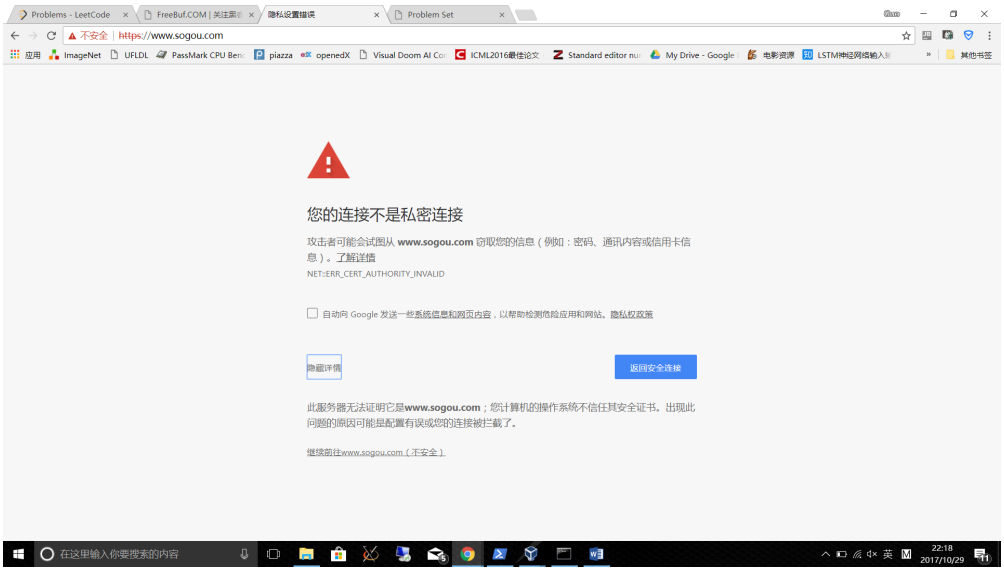

图 4: 访问 https://www.sogou.com

图4显示了靶机浏览器访问 https 网站的现象，可以看到浏览器提示链接不安全；但是如果点击最下面的超链接继续前往 www.sogou.com (不安全)，就会出现目标网页，并且攻击者能够看到 https 的数据信息。

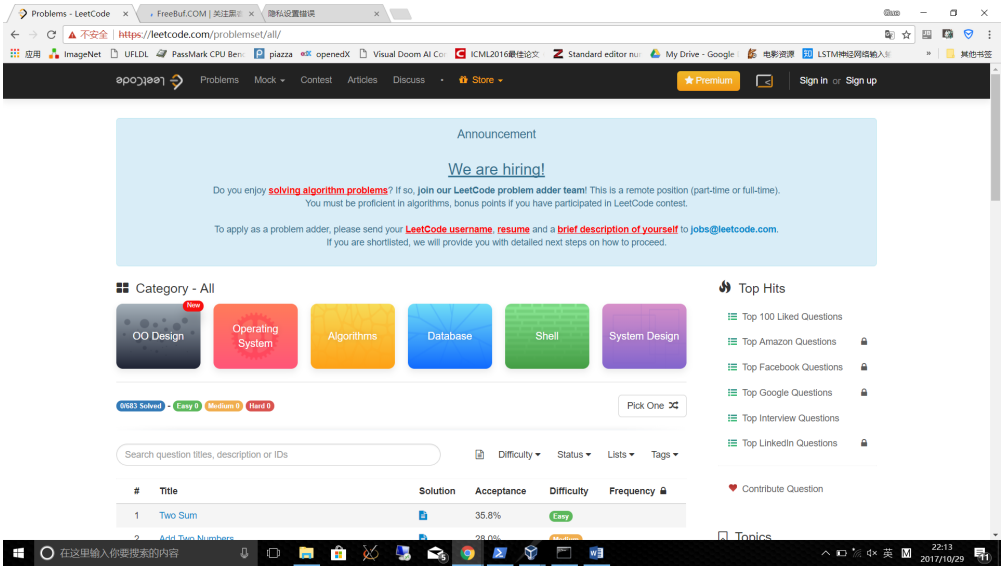

图 5: 访问 https://leetcode.com

图5显示了靶机访问 https 网页，并且点击“继续前往”的选项之后的现象。可以看到在左上方的 https 被划了红线，并且里面的网页图片也被倒置 (LeetCode 的图标)。因此，看到如图4这种现象的网站，尽量不要选择不安全的访问方式，否则及有可能被中间人攻击。

图6显示了靶机访问 http://learn.tsinghua.edu.cn，并且随便敲了一个用户名和密码点击登录之后，在攻击者机器上看到的 https 报文。可以看到 POST 中 URLEncoded form 中的数据被一览无余。可见校园网的这些网站信息安全保护措施并不完美，应该全部使用 https 进行加密，而不是只在登录的时候使用 https 加密数据。

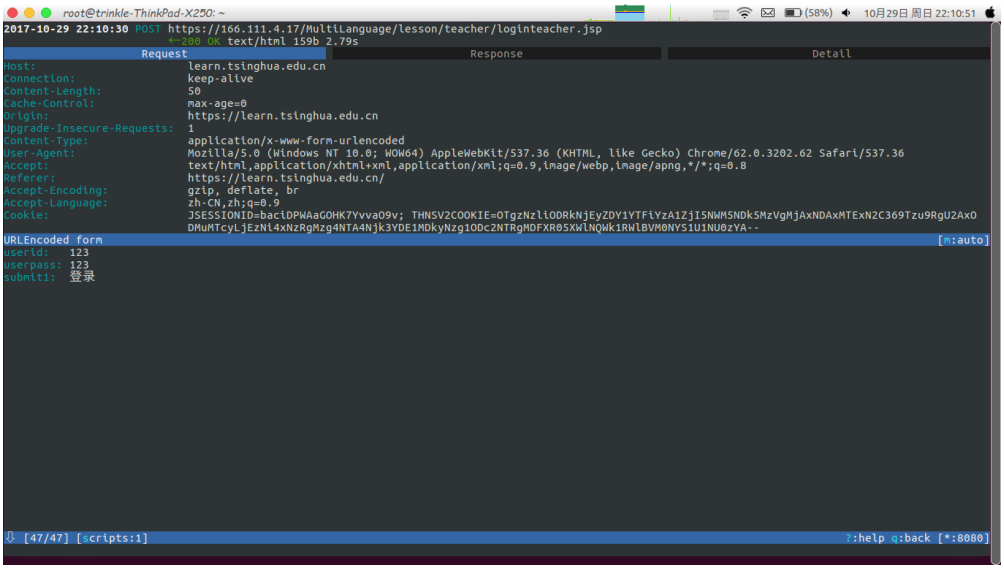

图 6: 登录网络学堂

3.3 Macbook Pro

配置与之前相同。发现无法进行欺骗。

使用命令 arp -n 查看 arp 缓存，发现 arp 缓存正常，未被修改。我猜想系统可能防 arp 毒化攻击。

3.4 iPad/iPhone

配置与之前相同。发现欺骗有时成功，有时不成功。可能是设备问题？

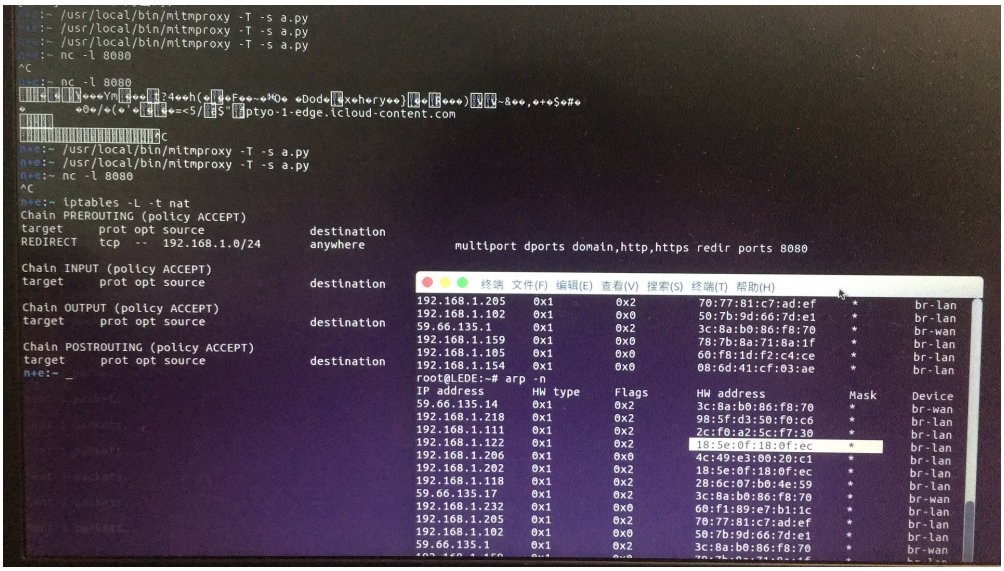

图 7: 路由器的 arp 缓存

图7和图8显示了路由器和 iPad 上的 arp 缓存，显示的 MAC 地址均为攻击者设备的 MAC 地址。

图9显示了在 iPad 上查看微信朋友圈图片的截图，可见微信的朋友圈的图片传输使用

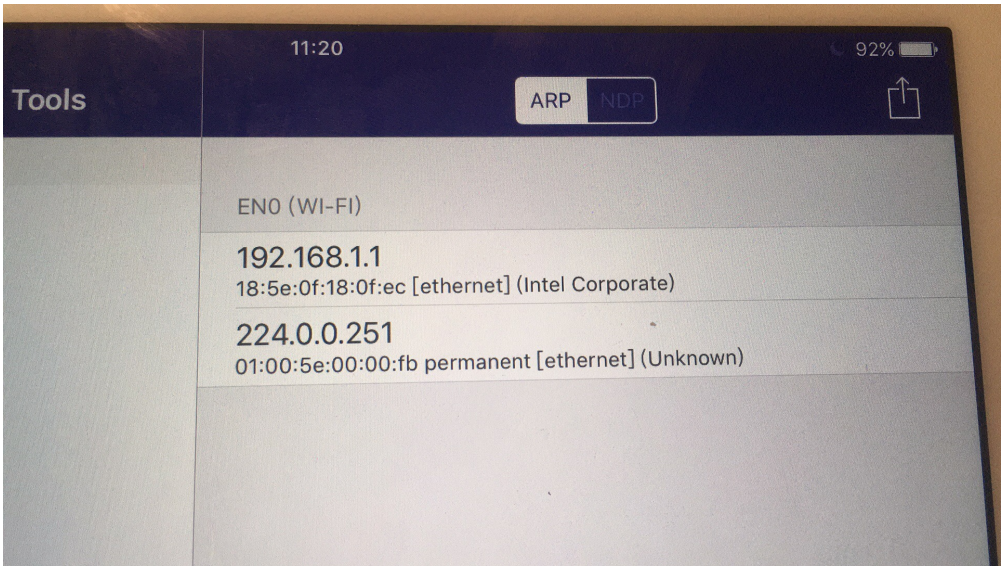

图 8: iPad 上的 arp 缓存

图 9: 查看微信朋友圈中的图片

http 协议。但是如果在群聊中发图片，发现不能被倒置，可能原因是这些图片传输走的是微信自己的协议。

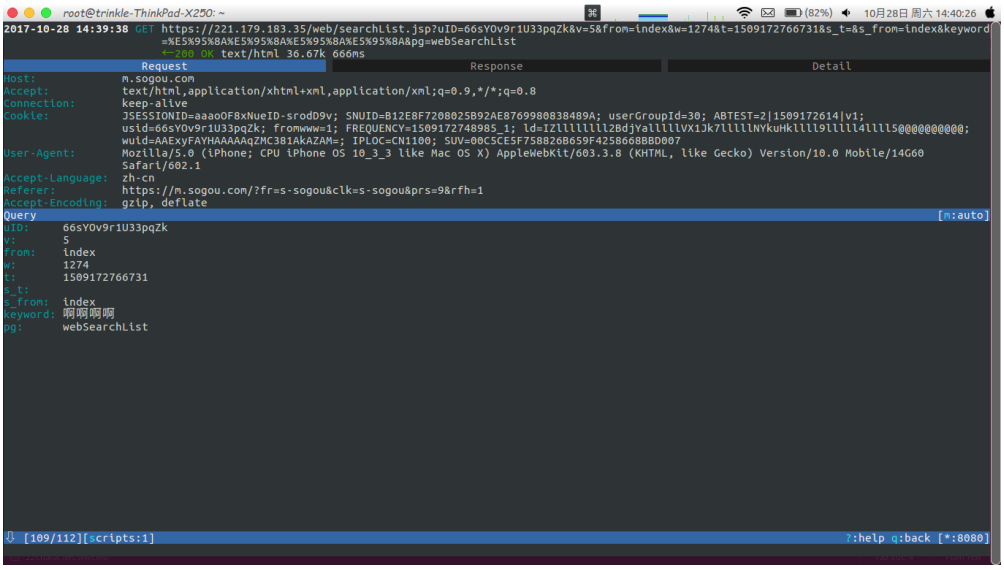

图 10: 在 iPhone 上使用搜狗搜索

图10显示了在 iPhone 上使用搜狗搜索，在攻击者机器上看到的报文信息。同之前 Win10 一样，会出来一个提示框，说链接不安全/证书有问题，然后一旦点击继续，流量就会被中间人截获，比如图11所示，网络学堂的帐号密码直接被窃听。

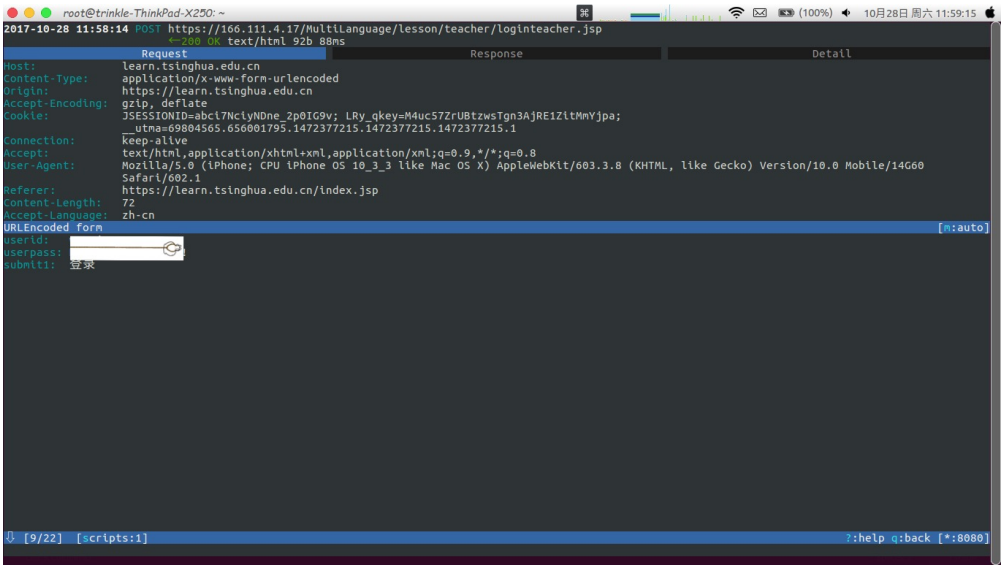

图 11: 在 iPhone 上登录网页版网络学堂

3.5 小米手机

配置与之前相同。发现无法被欺骗，并且无法上网。考虑到之前 Macbook Pro 上的现象，只好手动将手机连接的 wifi 的代理手动设置为攻击者的 ip 地址和 8080 端口，发现能够被欺骗。

测试了一下 AtTsinghua，发现一部分的密码使用 MD5 进行传输，另一部分使用明文传输，可见 AtTsinghua 也并不安全。

3.6 攻击者为 Ubuntu 虚拟机

配置与之前相同。靶机为原来的攻击者。虚拟机网络设置为 VirtualBox 中的“桥接网卡-全部允许”选项。发现欺骗不成功。

查看 arp 缓存，发现 arp 的包发送出去了，但是 MAC 地址为虚拟机所在的 Win10 的 MAC 地址。我们尝试过手动修改 arp 的 hwsrc 参数，可是仍然无济于事。猜想：在 arp 包发送出去的时候，Win10 自动转发，并且写上自己的 MAC 地址。于是双方 arp 的缓存被改为了 Win10 的 MAC 地址，所有的流量都到了 Windows 上，无法被 Ubuntu 虚拟机所监听。