针对 SSL 的中间人攻击演示和防范

1、中间人攻击概述

中间人攻击（Man-in-the-Middle Attack, MITM）是一种由来已久的网络入侵手段，并且在今天仍然有着广泛的发展空间，如 SMB 会话劫持、DNS 欺骗等攻击都是典型的 MITM 攻击。简而言之，所谓的 MITM 攻击就是通过拦截正常的网络通信数据，并进行数据篡改和嗅探，而通信的双方却毫不知情。

随着计算机通信网技术的不断发展，MITM 攻击也越来越多样化。最初，攻击者只要将网卡设为混杂模式，伪装成代理服务器监听特定的流量就可以实现攻击，这是因为很多通信协议都是以明文来进行传输的，如 HTTP、FTP、Telnet 等。后来，随着交换机代替集线器，简单的嗅探攻击已经不能成功，必须先进行 ARP 欺骗才行。如今，越来越多的服务商（网上银行，邮箱登陆）开始采用加密通信，SSL(Secure Sockets Layer 安全套接层)是一种广泛使用的技术，HTTPS、FTPS 等都是建立在其基础上的。笔者将以常见的 Gmail 邮箱登陆为例，探讨针对 SSL 的 MITM 攻击的两种实现方式。

2、环境的搭建

网络环境：

网关：192.168.18.254；

攻击主机：192.168.18.102，VMware 虚拟机；

被攻击主机：192.168.18.100，Windows7，IE9；

攻击目标：

Gmail 邮箱登陆 (HTTPS 协议)

账户：test0101.ssl@gmail.com

密码：abcd7890

3、两种针对 SSL 的中间人攻击

Cain & Abel

Cain&Abel 是由 Oxid.it 公司开发的一款针对 Microsoft 操作系统的网络攻击利器，它操作简单、功能强大，尤以 ARP 欺骗攻击著称。Cain 不仅能实现针对 HTTP 的 MITM 攻击，也能对 HTTPS 进行攻击。基本的攻击过程为：

ARP 欺骗，使得攻击者能截获所有目标主机的网络流量；

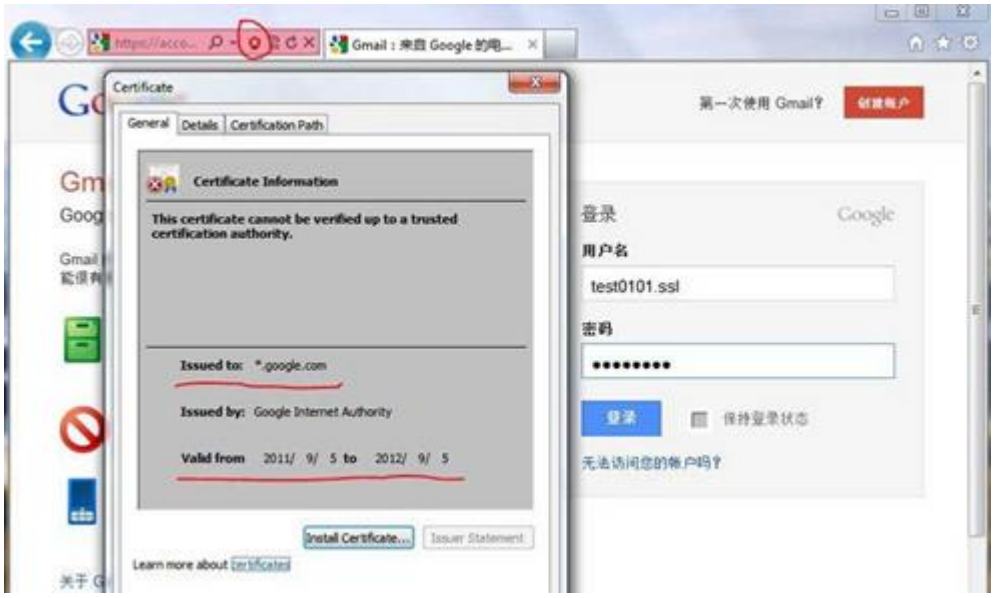
攻击者不是一个简单的中继，一方面它在服务器端与浏览器进行 SSL 握手，同时作为一个 SSL 客户又与目标服务器进行另一次 SSL 握手；

通过建立两条 SSL 连接，使得攻击者成为一个"中间人"。

由于 SSL 握手时要通过证书来验证彼此的身份，攻击者并不知道目标服务器所使用的私钥，在这种情况下，要成功实施攻击，攻击者必须进行证书的伪造，浏览器通常会向用户发出警告，并由用户自行决定是否信任该证书。下面进行详细的图文说明。

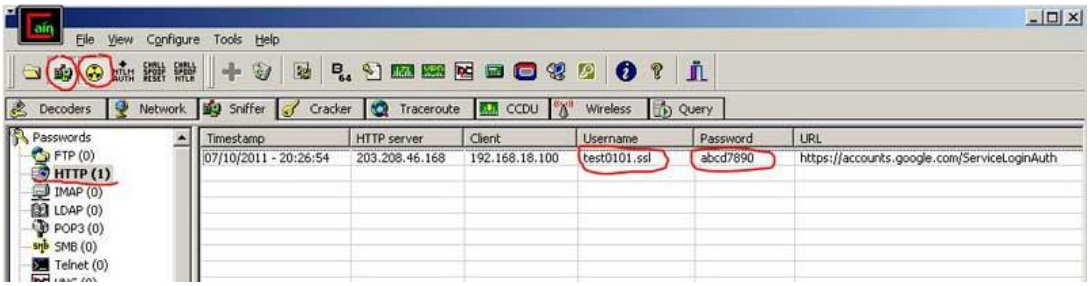
正常 Gmail 的登陆画面。

被攻击者需要选择是否信任证书，可以看到伪造的证书信息与上图中真实证书还是有很大的区别的。



登陆邮箱后的画面，可以看到证书错误的提示依然是很醒目的。

攻击者已成功嗅探到 Gmail 邮箱的登陆用户名和密码。



通过以上分析可以发现，用户对于伪造证书的判断是攻击能否成功的关键，如果用户有着较强的安全意识和丰富的网络知识那么被攻击的可能性将大大降

低，毕竟浏览器中的安全提示还是非常醒目的。笔者相信随着网络知识的不断普及，这种攻击手段的生存空间会不断被挤压。

sslstrip

Cain & Abel 虽然能实现 SSL 攻击，但是伪造证书的局限性还是很明显的，sslstrip 是在 09 年黑帽大会上由 Moxie Marlinspike 提出的一种针对 SSL 攻击的方法，其思想非常简单：

ARP 欺骗，使得攻击者能截获所有目标主机的网络流量；

攻击者利用用户对于地址栏中 HTTPS 与 HTTP 的疏忽，将所有的 HTTPS 连接都用 HTTP 来代替；

同时，与目标服务器建立正常的 HTTPS 连接；

由于 HTTP 通信是明文传输，攻击者能轻松实施嗅探。

笔者将采用 BackTrack 作为攻击平台，BackTrack 是基于 Linux 的一套渗透测试工具包，目前，国内各大论坛有很多关于使用 BackTrack 来进行无线 wifi 密码破解的教程，其实它在其他领域也有着极其强大的功能。

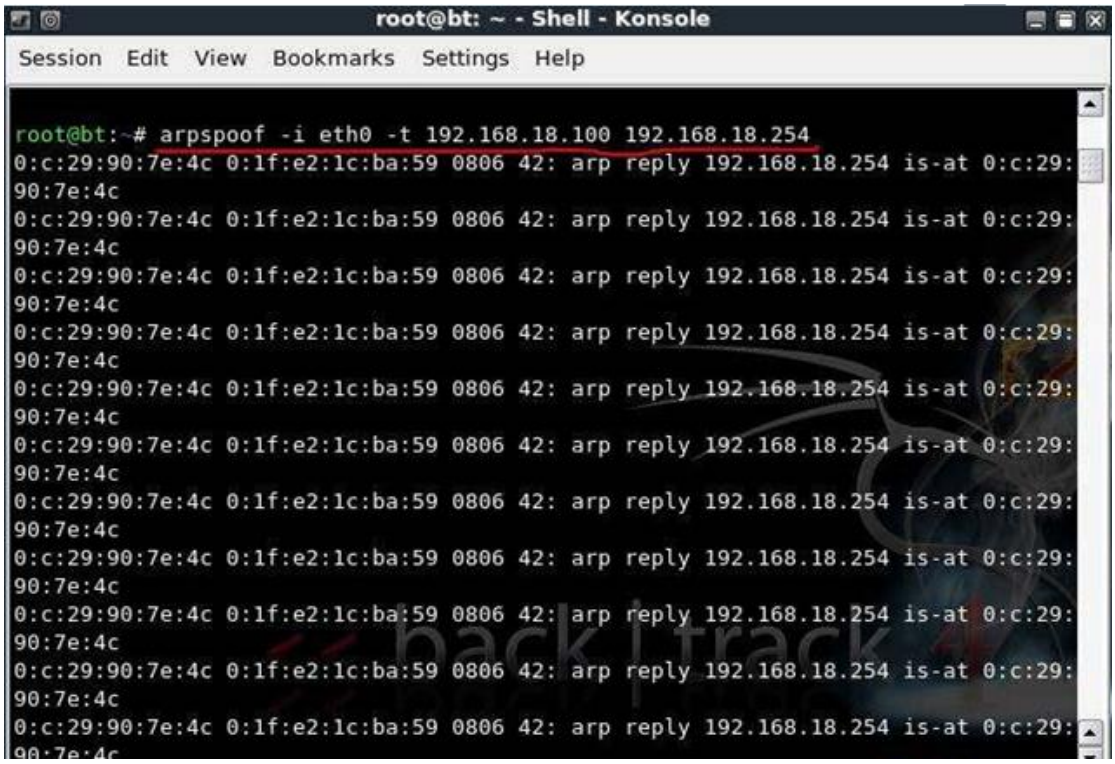
步骤一：启用内核包转发，修改/proc/sys/net/ipv4/ip_forward 文件，内容为 1;

echo 1 > /proc/sys/net/ipv4/ip_forward 步骤二：端口转发，10000 为 sslstrip 的监听端口；

iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000

步骤三：shell1，ARP 欺骗；

arpspoof -i eth0 -t 192.168.18.100 192.168.18.254

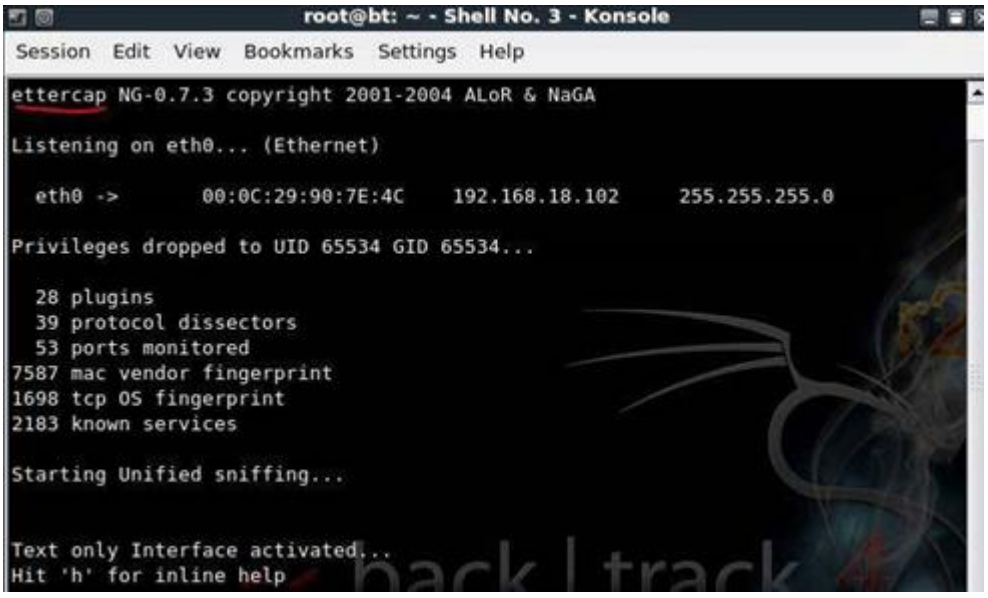


步骤四：shell2，开启 sslstrip；

sslstrip -a -k -f<img wp-image-2530"="" height="499" data-cke-saved-src=http://images.51cto.com/files/uploadimg/20121120/1326016.jpg" src=http://images.51cto.com/files/uploadimg/20121120/1326016.jpg">

步骤五：嗅探得到登陆 Gmail 邮箱的用户名和密码；

ettercap -T -q -i eth0



那么这种方法是否是万能的呢，下面就来看看被攻击者浏览器的变化。

可以看到，网页上没有任何不安全的警告或是提示，只是原先的 HTTPS 连接已经被 HTTP 连接所替换，并且为增加迷惑性，网页的图标被修改成了一个银色的锁图案。但是，假的毕竟是假的，一方面无法查看到任何证书的信息，另外如果在网址前输入 https://，则网页无法发开。因此，sslstrip 并不是万能的攻击方法。

4、小结

网络安全技术日新月异的同时，攻击方法也在悄然发生着变化，采用了 SSL 加密通信并不一定能保证通信的隐密性和完整性，为此，笔者展示了两种 SSL 的中间人攻击方法，前者是常规思路，后者则另辟蹊径。希望今后大家能提高警惕，准确辨识你的通信是否正遭到攻击，尤其是在完成重要操作时，如网银交易等。