Misc 总结 ----流量分析 HTTPS认识

M1n3 / 2018-01-18 23:02:02 / 浏览数 3211 安全技术 CTF 顶(0) 踩(0)

网络协议—HTTPS

实验目的

了解HTTPS的原理
掌握解密https的方法

实验环境

- 操作机：Windows XP
  - 实验工具：
    - Wireshark2.2

实验内容

SSL (Secure Socket Layer)安全套接字层协议；TLS(Transport Layer Security)传输层安全协议。SSL/TLS是保护计算机网络通讯安全的一类加密协议，它们在传输层上给原先非安全的应用层协议提供加密保护，如非安全的HTTP协议即可被SS

实验一

解密HTTPS流量

方法一 pre-master-secret

先追踪一个解密前的TCP流：`tcp.stream eq 1`(在对应的数据包右键追踪流，选择TCP流)：

可见SSL层数据是乱码，不可获取到流量具体信息。

Windows或linux环境，配置环境变量`SSLKEYLOGFILE=./path/*.log`，浏览器在访问https时会将与网站https建立连接后的会话私钥保存下来。在wireshark中，通过编辑 - 首选项 - 协议(protocols) - SSL - (Pre)-Master-Secret log filename 指定SSLKEYLOGFILE文件，即可解密流量(流量包)中的HTTPS流量。

此时，继续看`tcp.stream eq 1`这个TCP流：

此时，数据已经可以被解密，分组详情多出了HTTP字段的信息，分组字节流也出现的解密之后的SSL数据(Decrypted SSL Data)。

方法二 服务端私钥

在某些CTF题目中，给了流量包的情况下，往往会再通过某些信息给一个SSL的私钥文件。同样在wireshark中协议SSL设置：

可以在这里导入私钥，password为保存私钥时指定的加密密码，为了防止私钥丢失被解开。

利用这个方法同样可以解密SSL流量。

注释

这个流量包中，解密之后的流量包含HTTP2.0协议，对应下图HTTP2.0报文格式试一试把：

https.pcapng.zip (0.89 MB) 下载附件
点击收藏 | 0 关注 | 1
上一篇：企业信息安全团队建设 下一篇：渗透测试技巧之一个XSS引发的漏洞...
1. 5 条回复


王天 2018-01-19 10:30:59

这个帖子的附件是什么

0 回复Ta


M1n3 2018-01-19 14:18:49

@王天 流量包 算是题吧

0 回复Ta


saviour2 2018-01-22 09:50:23

下载学习一下

0 回复Ta

1815837370479554 2018-05-29 14:58:44

学习 学习

1 回复Ta

四川民工返乡 2018-10-05 16:34:21

厉害了~~~~~学习学习

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板