如何利用Wireshark解密TLS加密报文

应用审计 孔凡安 3天前 发表

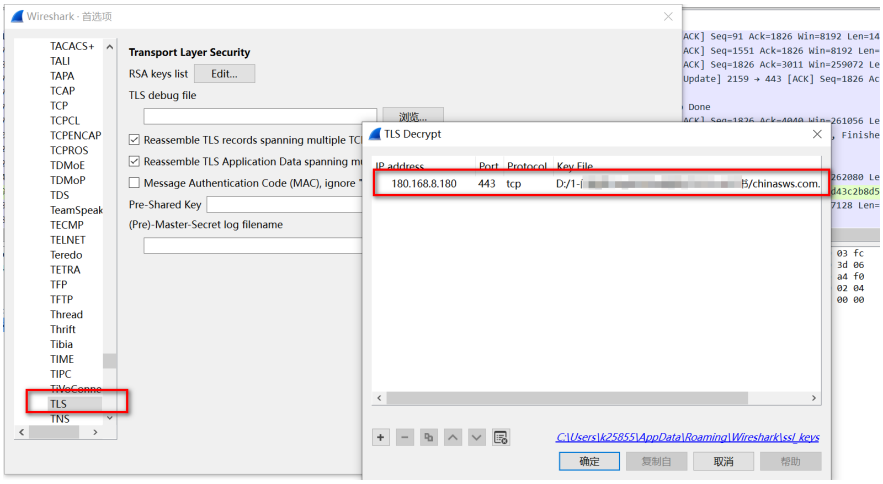
问题描述

如何利用Wireshark工具解密TLS加密报文：
1. 需要有服务器的key文件；
2. 涉及ECDHE算法的报文无法解密

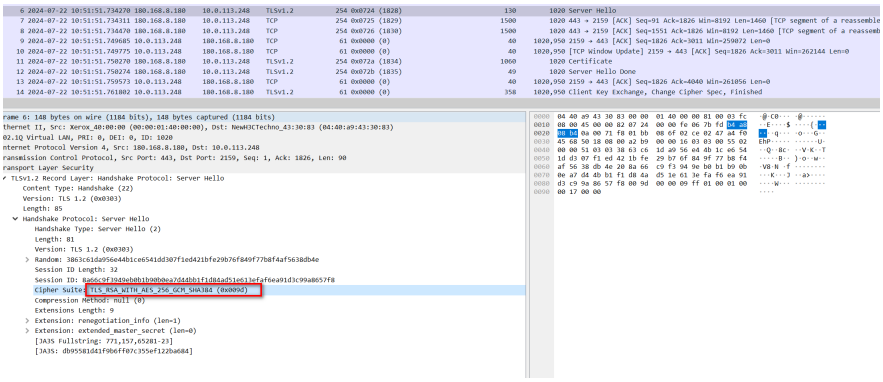
> 1. 打开首选项
> 在 Wireshark 中，前往 Edit -> Preferences 或按键盘快捷键 Ctrl + Shift + P 开启首选项窗口。
>
> 2. 导航到 TLS 设置
> 在首选项窗口中，导航到 Protocols -> TLS 部分。
>
> 3. 导入 RSA 私钥
> 在 TLS 选项中，找到 RSA keys list 选项，点击 Edit 按钮。
>
> 步骤详细说明：
> 点击 New：打开新建一个新的私钥配置条目。
>
> 填写相应信息：
>
> IP Address：输入服务器的 IP 地址。
> Port：输入端口号（通常是 443，代表 HTTPS 流量）。
> Protocol：通常输入 http 或其他协议。
> Key File：通过浏览按钮选择你的 RSA 私钥文件路径（例如：/path/to/your/private_key.pem）。
> 确认并保存：点击 OK 进行保存，返回上层界面，再次点击 OK 确认所有配置。

解决方法

实践操作：



解密效果如下：
TLS协商的算法：



解密后的报文如下，关注目标端口为443.但是报文内容明文显示。如下：