《电子证据分析》课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 实验名称 |  | 姓名 |  |
| 班级 |  | 学号 |  |
| 实验日期 |  | 指导老师 |  |
| 实验环境  (实验软硬件要求) | wireshark 、 浏览器、 windows terminal preview 、 winhex | | |
| 实验目的 | （给出本次实验所涉及并要求掌握的知识点）  *要求掌握从数据包中还原相关的数据的操作流程。*  *了解电脑注册表的原理以及部分注册表的较为重要的键值的位置和含义。* | | |

|  |  |
| --- | --- |
| 实验内容 | 1. 使用抓包工具 wireshark 抓包完整的下载图片的过程，并且在抓取的数据包中还原出下载下来的图片   选择 [www.4399.com](http://www.4399.com) 中的随意一张图片。    选定好图片后，一边打开抓包工具 wireshark 一边开始进行下载操作。    然后选择一下保存图片的位置，我为了方便后面的查看，就放在了桌面。  然后等待下载完成。完成之后，停止抓包。    但是这些里面的数据有很多，并不是很好找，需要使用追踪 tcp 流来进一步的帮助查找。  终于在第二十个流里面找到了我们下载的数据。    很显然，我们的确是找到了我们需要的数据包，这里可以直接将文件导出来，或者自己手动对数据进行操作将其保存到新的文件中去就行。  直接导出的操作如下：    根据名字找到文件就行了。      文件和我们下载的是一样的。  下面的是原本下载的图片的属性    下面的是我们还原出来的    字节数是一样的。（windows还有一个占用空间，所以会看着更大一些）  手动的话，需要使用 winhex ，将在我们这个pcpng文件里面的图片的数据找到。  数据包里面有很多图片，需要确定哪个是我们需要的。  在这里我们在到了GET部分，那么下面的一个FFD8就一定是了。往下找就可以了    在此处找到了FFD8。    随后找到尾部 FFD9 即可。    最后导出到一个新文件就行了。  （下面才是我们导出来的，第一个是我们之前自动导出的）  查看属性也是一样的。    但是，现在的大多数网站还是用的是HTTPS。所以，这里就继续用HTTPS的网站来试试。  在查阅了网上HTTPS解密的相关知识后，了解到，现在主要还是需要服务器的私钥或者使用浏览器导出的 pre-master-secrect 文件进行解密。当然的，我们没有 HTTPS 的服务器证书。所以就使用第二种办法。  首先要随便在想要的位置创建一个文件。    这个文件就会设置为导出的 pre-master-secrect 文件。  然后添加环境变量。        然后用 wireshark 导入这个文件就行。      之后，再使用追踪 TLS 流就会发现可以看到明文了。  但是这样有一点要注意。需要注意的是RSA算法，一定要让wireshark 抓到 Client Key Exchange的包，因为预主密钥在这个报文里面，否则无法看到明文。（这个也是我做了好几次实验都失败的原因……）  但是这里也会有问题。一旦TLS的数据包里面出现 Ignored Unknown Record 。那么整个报文就会变成下面那样一片白。    而且后面的时候很多数据包在追踪的时候会报错。所以，这里到后面就失败了……  使用开发工具 autoruns 查看自己注册表里面的开机自启动程序有哪些。  可以看到，下图就是完整的内容。 |
| 实验总结 | （对本次实验涉及到的知识点的重难点归纳、实验心得、思考与建议）  本次实验主要让我们了解了关于利用网络数据包的数据进行还原的操作。当时在这个实验过程中，我也发现了一些比较特殊的地方，例如在下载操作时，我仅仅进行了一次的下载图片，当时在这里却发现了有多个的HTTP的GET。并且在进行导出后也可以看到很多图片。很显然不管有没有下载我们的浏览器都会将网页上的内容下载到本地中去。那么我们再进行这样的还原的过程中，如果遇到了两个完全一样的数据，一个是浏览器下载的缓存，另一个是我们下载的另存为图片。这样的两个数据包又要怎么样去区分开来？  对于现在的网络，很多网站都会选择使用 HTTPS 。但是在取证的过程中，我们又该怎么解密呢？我们没有服务器的私钥，也没有不一定就能获得到 pre-master-secrect 文件。这个时候怎么办？  针对于注册表的实验，老师上课的时候明说一共会有三个”RUN”的地方，但是我这里仅仅找到了两个。这个和老师说的是不一样的。 |
| 评分 |  |