CTF中的取证技术

翻译

若雨溪 于 2019-04-21 19:44:57 发布 1926 收藏 1
文章标签： ctf

分为两类：

流量分析：

Wireshark的基本使用方法

筛选器的使用：对协议版本、IP地址进行过滤。过滤后可以清晰的得到自己想要的信息。

追踪流

文件的导出

日志分析：通过日志分析寻找隐藏在其中的信息

SQL注入点的查找

WEBshell的查找

用户访问敏感路径的查找