1.捕获攻击源2.反制攻击者3.勾勒攻击者画像

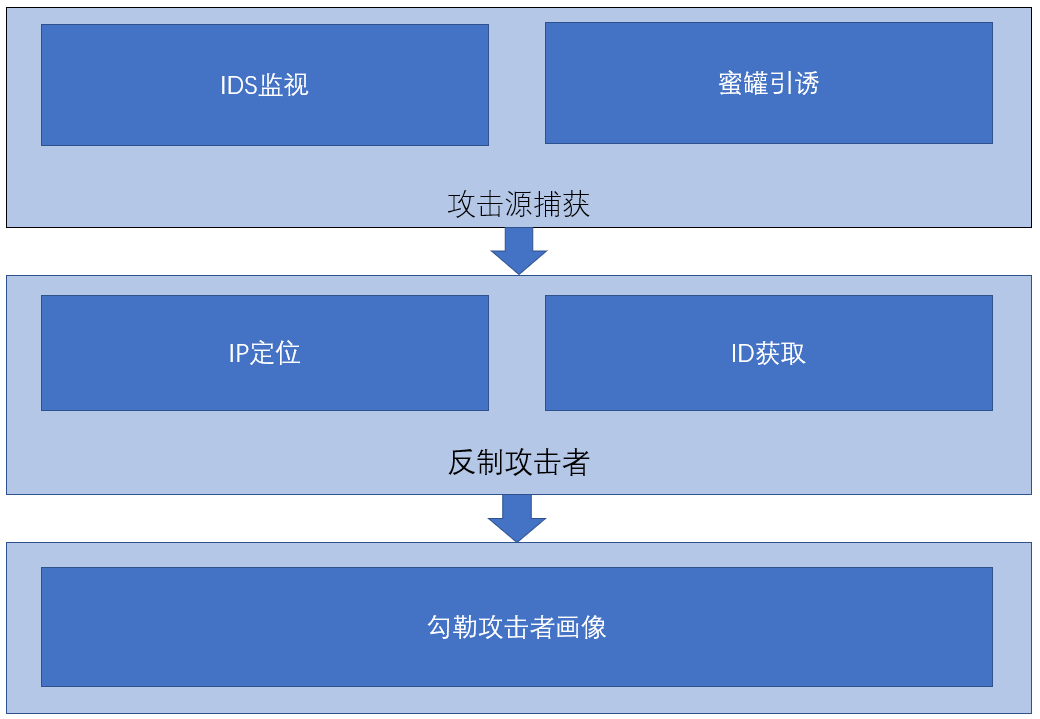


图1：攻击溯源流程

1. **捕获攻击源**

随着网络技术的不断发展，信息安全已经成为社会越来越重视的问题，一些不法分子利用网络漏洞窃取用户的重要信息。攻击者会向目标主机发送特定的攻击数据包或执行恶意行为。

如果能追踪这些攻击数据包的来源，定位攻击者的真实位置，受害主机不但可以采用应对措施，如在合适位置过滤攻击数据包，而且可以对攻击者采取法律手段。

本课题将采用两种方式方式来捕获攻击源。一是利用IDS进行监视，来确定攻击位置，并追踪其来源。二是制作蜜罐对攻击源进一步探索与挖掘。

**1.1利用IDS入侵检测系统来追踪攻击者地址**

入侵检测系统是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处便在于，IDS是一种积极主动的安全防护技术，IDS所能做到的不仅仅是记录事件，它还可以确定事件发生的位置，这是许多安全专家购买IDS的主要原因。通过追踪来源，可以更多地了解攻击者。这些经验不仅可以记录下攻击过程，同时也有助于确定解决方案。

利用IDS入侵检测系统，首先充分利用系统日志，追踪攻击者留下的踪迹，观察目录以及文件的异常改变与程序执行中的异常行为，收集攻击者的入侵信息，网络环境中的文件系统包含很多软件和数据文件，包含重要信息的文件和私有数据文件经常是攻击者修改或破坏的目标，另外利用检测系统收集物理形式的入侵信息，一是包括未授权的对网络硬件连接，二是对物理资源的未授权访问。然后通过模式匹配，统计分析和完整性分析这三种技术手段对收集到的数据进行分析，其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

本课题拟通过利用IDS入侵检测系统，首先收集攻击者信息，在进行数据分析，进而追踪攻击者地址。

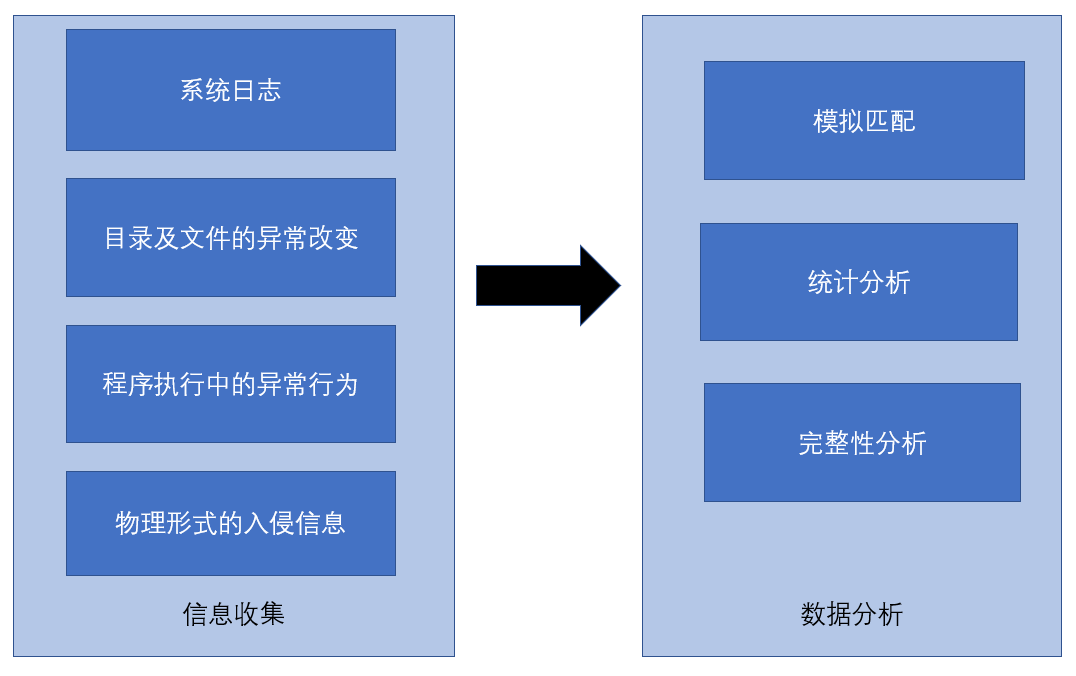


图2.IDS入侵检测流程

**1.2制作蜜罐引诱攻击者**

蜜罐系统主要作用是欺骗黑客，捕捉攻击行为。

蜜罐会提供一些和真正业务系统非常类似的服务，如数据库，Web，FTP，Mail，SSH，Samba等，里面也会存放一些看似有用的业务数据，而且这些服务都是存在安全漏洞，容易被各种攻击工具识别，从而吸引黑客攻击。然后在与黑客交互的过程中，后台记录从哪个IP，哪个账号进行了什么操作，并将日志传输到一台安全的服务器（防止黑客抹掉蜜罐的日志），一般接入SIEM（安全信息和事件管理）服务器，进行统一存储，分析并处理。

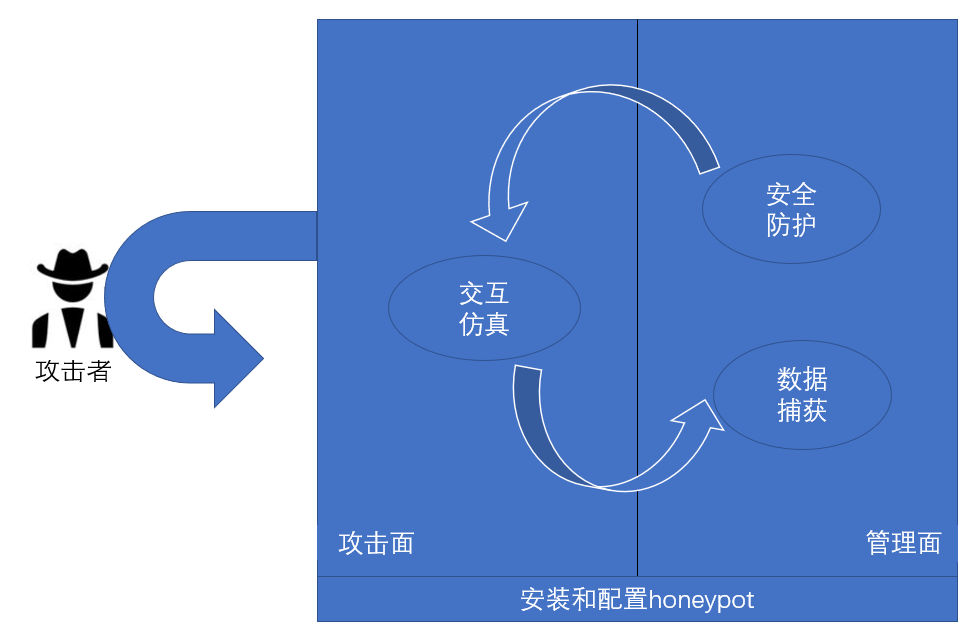
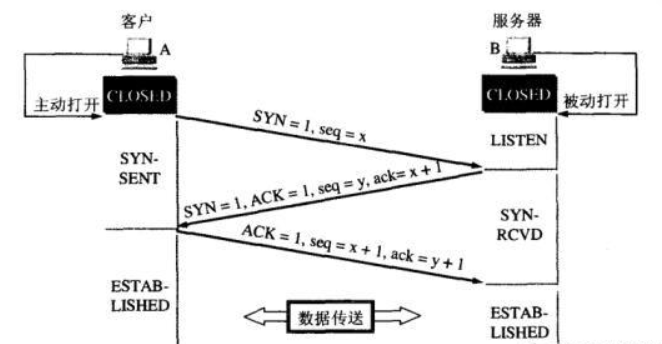


图3：蜜罐制作及引诱的实现

**2.反制攻击者**

我们拟采用端口扫描技术，通过对于特定的IP范围和端口范围进行穷举扫描，发现网络中开放的端口，从而为进一步的探查提供基本信息。

端口扫描一般针对TCP端口进行，利用TCP的三次握手建立连接的原理，通过连接是否成功来判断端口是否开放。端口扫描对于时间性能要求较高，耗时过长的扫描将大大降低扫描结果的可靠性。Masscan是一个互联网级别的高性能端口扫描工具，使用SYN包检测技术，号称能够在5分钟内完成对整个互联网所有的IP进行扫描。

图四：TCP三次握手

我们还拟通过搜索引擎、社交平台查询其ID并从技术论坛追溯邮箱，继续通过邮箱反追踪攻击者的真实姓名，通过姓名找到相关简历信息，达到反制攻击者的目的。

**3.勾勒攻击者画像**

在端口扫描过程中，Masscan会在短时间内对整个互联网所有的IP进行扫描，极大地增加了扫描效率。我们拟通过将这些扫描的结果进行整理，得到攻击者的攻击途径、攻击手段、攻击意图、IP地址、ID信息、邮箱等真实信息，将潜伏在暗处的攻击者拉出水面，找到造成攻击的真凶，勾勒出攻击者的画像，维护互联网用户的合法权益以及网络空间的安全，打击网络违法犯罪行为。

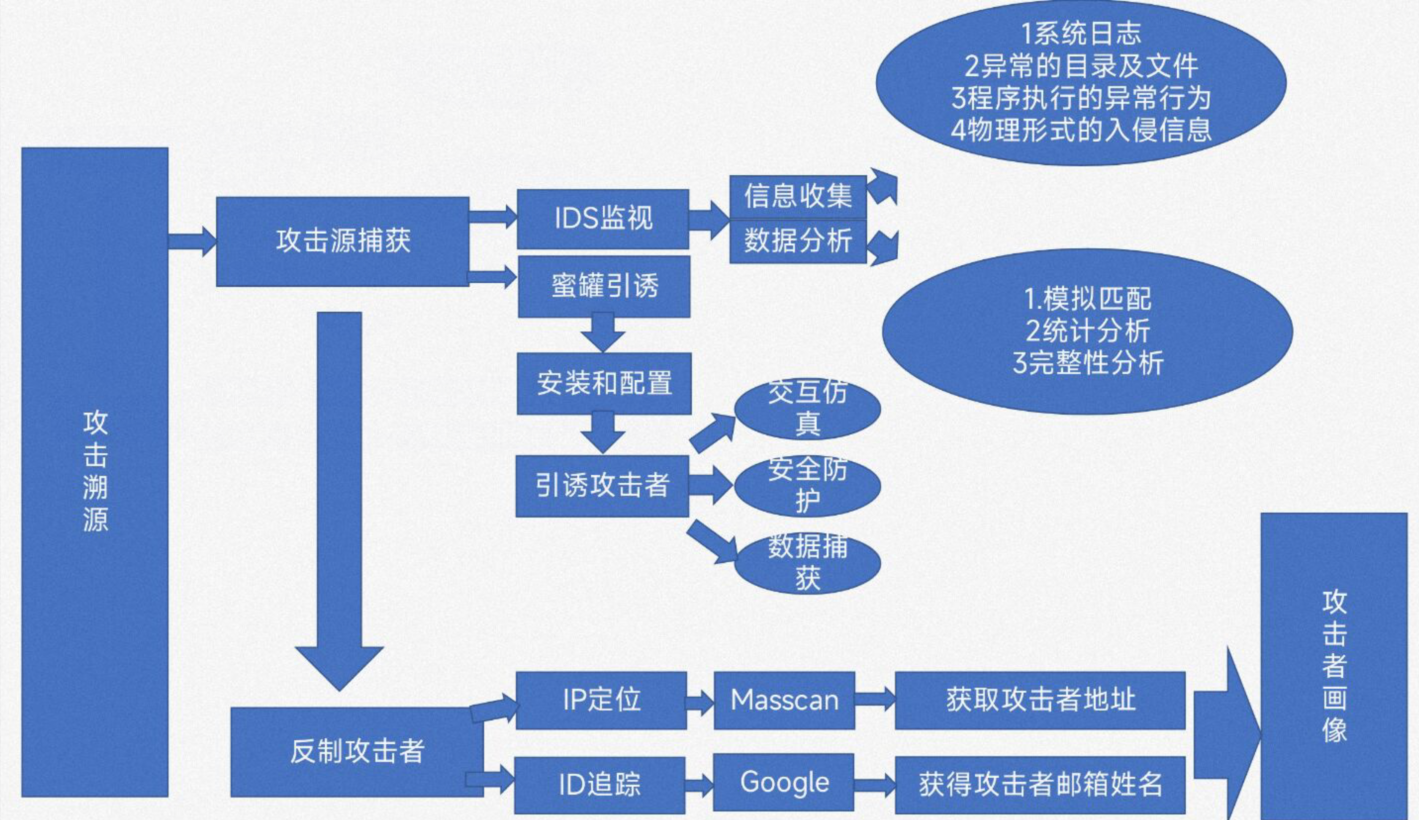


图5：攻击溯源实现