Computer Science and Application 计算机科学与应用, 2024, 14(4), 47-55
Published Online April 2024 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2024.144076

Hans汉斯

基于MySQL的蜜罐系统的构建

王铭轶，徐亚峰，陈骁宇，陈明昊，刘子豪

徐州工程学院信息工程学院(大数据学院)，江苏 徐州

收稿日期：2024年3月5日；录用日期：2024年4月5日；发布日期：2024年4月12日

摘　要

随着网络安全威胁的不断演变，主动发现漏洞和潜在风险成为规避网络威胁的有力措施，但是传统杀毒软件和防火墙等均属于被动防御技术，使用蜜罐能够捕获攻击者信息，实现对网络威胁的主动防御。基于MySQL的蜜罐系统包括MySQL服务器模拟和数据可视化展示Web端，通过模拟MySQL通信伪造数据请求，吸引攻击者，实时捕获攻击者信息，并详细记录攻击日志进行可视化展示，Web端可以实现查看当前服务器所捕获的攻击次数、溯源个数、攻击IP和攻击地址等全部恶意攻击者信息的功能。使用本系统有效降低了运维人员应急响应和溯源的成本难度，为网络安全提供有力支持。

关键词

主动防御，MySQL蜜罐，可视化，网络安全

Construction of Honeypot System Based on MySQL

Mingli Wang, Yafeng Xu, Xiaoyu Chen, Minghao Chen, Zihao Liu

College of Information Engineering (Big Data College), Xuzhou University of Technology, Xuzhou Jiangsu

Received: Mar. 5th, 2024; accepted: Apr. 5th, 2024; published: Apr. 12th, 2024

Abstract

As network security threats continue to evolve, proactive discovery of vulnerabilities and potential risks has become a powerful measure to avoid network threats. However, traditional anti-virus software and firewalls are passive defense technologies. The use of honeypots can capture attacker information and realize the active defense of network threats. The honeypot system based on MySQL includes MySQL server simulation and data visualization display Web side. It simulates MySQL communication and forges data requests to attract attackers, captures attacker information in real time, and records attack logs in detail for visual display. The Web side can view the

文章引用: 王铭轶, 徐亚峰, 陈骁宇, 陈明昊, 刘子豪. 基于 MySQL 的蜜罐系统的构建[J]. 计算机科学与应用, 2024, 14(4): 47-55. DOI: 10.12677/csa.2024.144076

current the function of all malicious attacker information such as the number of attacks, number of traces, attack IP and attack address captured by the server. The use of this system effectively reduces the cost and difficulty of emergency response and traceability for operation and maintenance personnel, and provides strong support for network security.

Keywords

Active Defense, MySQL Honeypot, Visualization, Network Security

1. 引言

在信息化时代背景下，互联网已经深刻融入人们的日常生活，成为不可或缺的重要组成部分。随着网络共享性和开放性的不断发展，相关网络安全问题也日渐突出，传统的被动防御技术无法有效抵御复杂多变的新型攻击。在这一背景下，蜜罐技术崭露头角，为主动防御提供了新的可能[1] [2]。本文旨在探讨现有蜜罐技术的局限性，明确问题所在，并提出基于 MySQL 的蜜罐系统的构建，以弥补传统防御技术的不足，实现对网络威胁的主动拦截和溯源，为网络安全提供有力支持。

本蜜罐系统采用 Python 语言开发，通过模拟 MySQL 服务的正常运行，使得攻击者在尝试入侵时暴露其行为。系统通过仿真 TCP/IP 套接字连接过程，模仿了客户端和服务器之间的通信过程，从而更好地识别和记录潜在的攻击行为，实现对攻击者攻击时间、攻击 IP、攻击者电脑用户名、攻击者微信 id 等信息的捕获功能，同时将捕获到的攻击者 IP (Internet Protocol，网际互连协议)与 IPv4 归属地位置 API (Application Programming Interface，应用程序编程接口)进行整合，以获取 json 格式的地理位置(精确到区县)信息。为更直观的查看攻击者信息，将蜜罐系统与 Web 服务进行整合，用户可通过 Web 端轻松查看当前服务器所捕获的全部恶意攻击者信息。这种综合性的设计不仅提高了系统的可视化水平，同时也增加了用户对系统运行情况的实时监控和感知，这种创新性的蜜罐系统设计有望提升网络安全防护水平。

2. 蜜罐技术简介

蜜罐的概念最初在 1989 年出版的《The Cuckoo’s Egg》小说中得以引入[3]，直至 20 世纪 90 年代末，蜜罐仍然只是管理员采用的一种主动防御思想。随着时间的推移，蜜罐技术逐渐发展成为一种全新的网络安全技术，对其定义目前仍存在一些争议。通常，蜜罐是指在高度监控环境下，通过真实或模拟的网络和服务来吸引并捕获攻击者，以便在攻击者攻击期间分析其行为的诱骗系统，这种系统被广泛用于信息搜集和预警目的[4]。蜜罐通常被设置为诱饵放置在网络中，旨在侦测攻击者的攻击行为。其设计目标主要在于欺骗和伪装，以便诱捕攻击者，方便管理员对其行为进行追踪和分析。

在 MySQL 协议中，客户端并不负责存储自身请求，而是通过服务端响应来执行相应操作。MySQL 服务端可利用 LOAD DATA LOCAL 命令读取 MySQL 客户端的任意文件，因此，我们可以通过伪造恶意服务器，向连接到该服务器的客户端发送一个读取文件的payload实现对应文件获取的功能。所以，MySQL 蜜罐的核心思想在于模拟一个 MySQL 服务端的正常通信过程，等待客户端发起 SQL 查询，并在响应时将我们构造的 Response TABULAR (即 LOAD DATA INFILE 的请求)发送给客户端。这样，客户端根据响

应内容执行上传本机文件的操作，达到我们获取攻击者相关信息的目标。

3. 系统设计与实现

本系统主要由 MySQL 服务器模拟、信息捕获、日志记录以及数据可视化展示四大部分组成，其中 MySQL 服务器模拟和数据可视化展示 Web 端是其核心部分。MySQL 服务器模拟部分基于 Python 的 socket 模块实现，Web 端通过 HTML + CSS + JS 和 PHP 等技术集成开发，实现蜜罐诱捕攻击和可视化管理功能[5]。通过这种多语言协作的方式设计实现本系统，充分发挥了各语言的优势，为项目的开发提供了灵活性和可扩展性。

3.1. MySQL 服务器模拟模块

MySQL 数据库通过 TCP/IP 协议与服务器进行通信，服务端与客户端的正常交互主要包括三个步骤。本模块主要实现对上述过程的模拟，完成正常 MySQL 服务器的虚拟伪装，具体认证过程分析如下。

首先，客户端通过指定服务器 IP 地址和端口号向服务器发起连接请求，服务器接受请求后进入握手阶段，交换通信参数和支持的功能。在这一阶段，服务器发送 Greeting 包，返回服务端的 Version 等信息如图 1 所示。这一过程确保双方建立了可靠的 TCP 连接，并通过握手协议确认彼此通信能力。为模拟正常 MySQL 服务器行为，蜜罐需要模拟发送类似的 Greeting 认证包以完成握手过程，确保在仿真环境中能够成功建立连接。

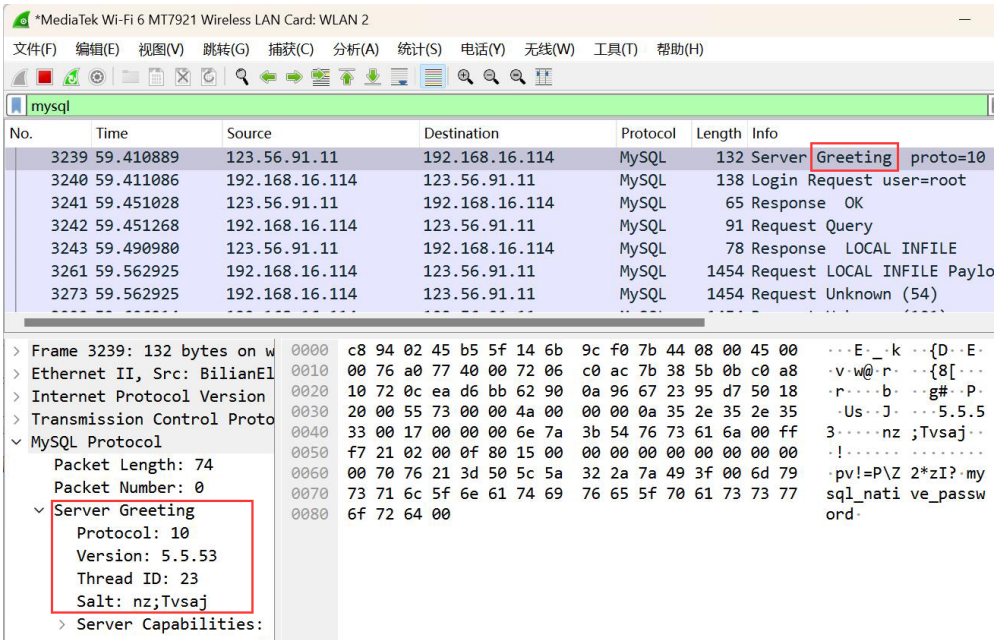

Figure 1. Greeting packet
图 1. Greeting 包

在连接建立后，MySQL 通过身份验证确保安全性。客户端在连接建立时发送身份验证信息如图 2 所示，通常是用户名和密码的组合，服务器在接收到客户端的身份验证信息后进行验证，若验证成功，则向客户端发送认证成功的响应包[6]，如图 3 所示，失败则导致连接被拒绝，保障数据库的安全性。在这一阶段，蜜罐需模拟发送类似正常 MySQL 服务器发送的 Response OK 的返回包，以欺骗潜在攻击者。

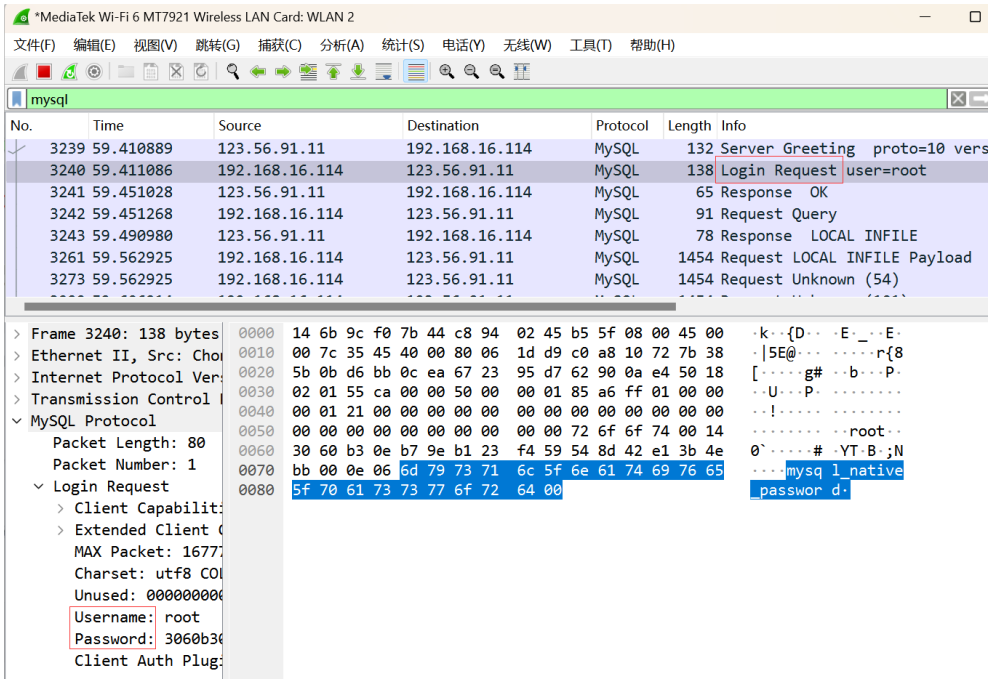

Figure 2. Client sends login request
图 2. 客户端发送登录请求

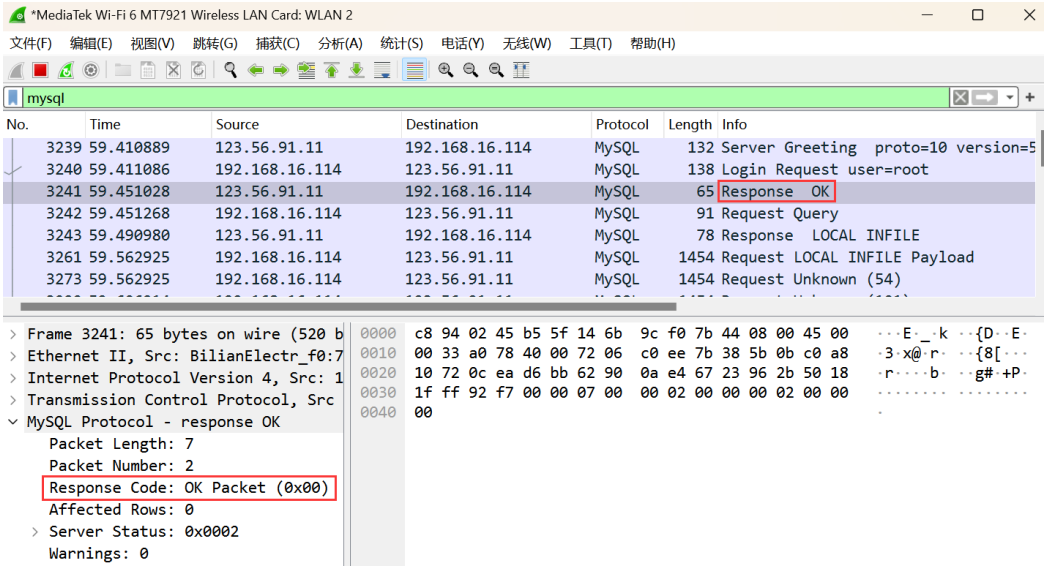

Figure 3. The server sends an authentication success packet
图 3. 服务器发送认证成功包

一旦身份验证成功，MySQL 进入通信阶段。客户端会向服务器发送 SQL 查询操作命令如图 4 所示，服务器执行命令并将结果返回给客户端。根据研究，大多数 MySQL 程序库和客户端在身份验证成功后会进行至少一次发送请求，用以探测目标平台的指纹信息，如使用“select @@version_comment limit 1” SQL 查询语句获取 MySQL 服务器版本的评论信息。在这个阶段，蜜罐需要向客户端发送我们构造的 Response TABULAR，即 LOAD DATA INFILE 请求。这样，客户端根据响应内容执行上传本机文件的操作，攻击者的文件信息就能被获取。MySQL 服务器模拟流程如图 5 所示。

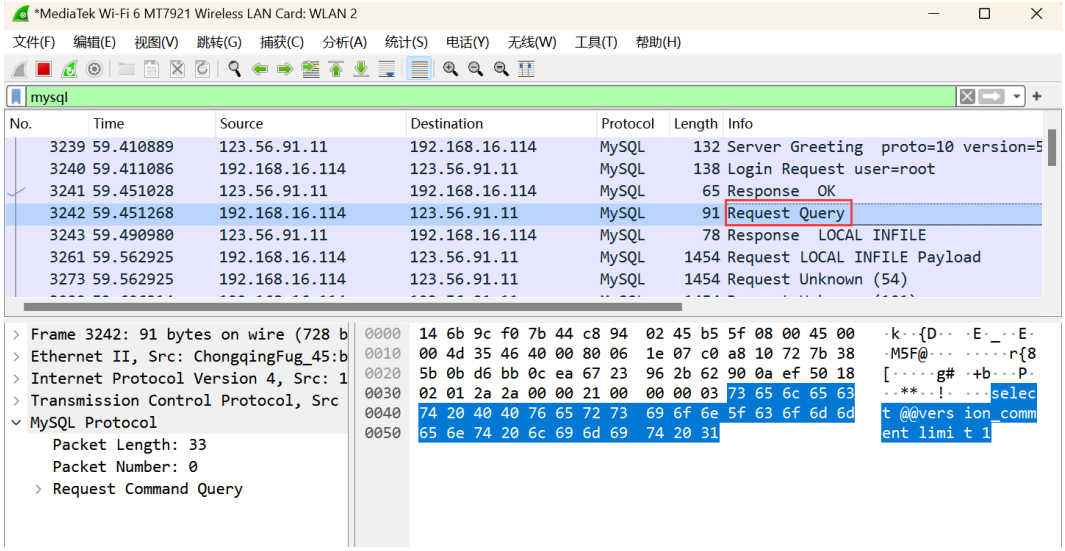

Figure 4. Client sends query packet
图 4. 客户端发送查询包

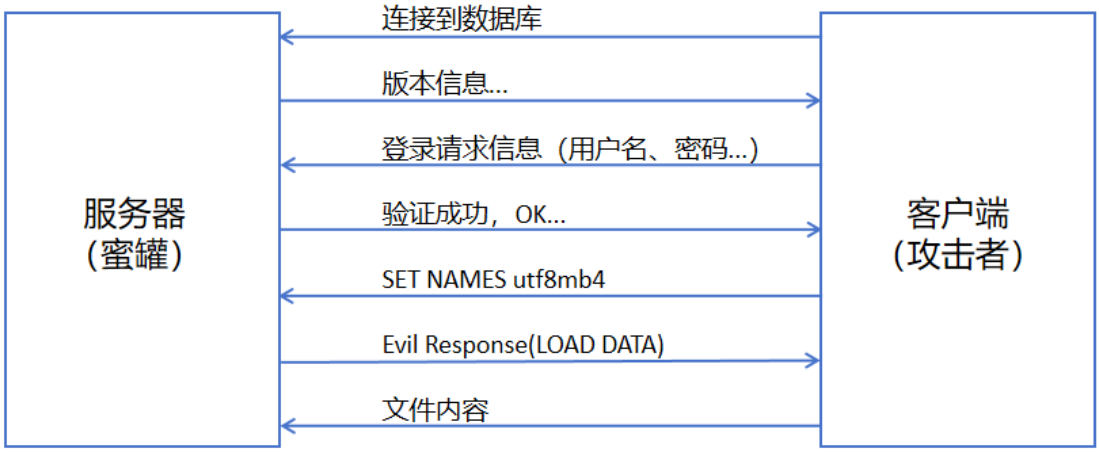

Figure 5. MySQL server simulation process
图 5. MySQL 服务器模拟流程

3.2. 信息捕获模块

在进行溯源过程中，首要任务是收集一系列方便获取类型固定能够揭示攻击者身份信息的文件，以便于后续调查和反制工作，本模块的主要职责是实现文件获取的功能。

MySQL 中 load data local infile " into table test fields terminated by '\n'; 语句可以实现读取客户端本地文件并插进表中的功能，因此我们可以通过伪造一个恶意的服务器，向连接服务器的客户端发送读取文件的 payload 完成信息捕获功能。在 Windows 操作系统中，微信的默认配置文件通常位于 C:\Users\username\Documents\WeChat Files\目录下，而微信 ID 则保存在 C:\Users\username\Documents\WeChat Files\All Users\config\config.data 文件中。为了获取 config.data 文件，我们需要了解攻击者的计算机用户名，而通常这个用户名可以在日志文件中找到。PFRO.log 是一个比较通用且文件名固定的日志文件，一般情况下，经过一段时间的使用，可以在 C:\Windows\PFRO.log 路径下找到包含计算机用户名的信息。

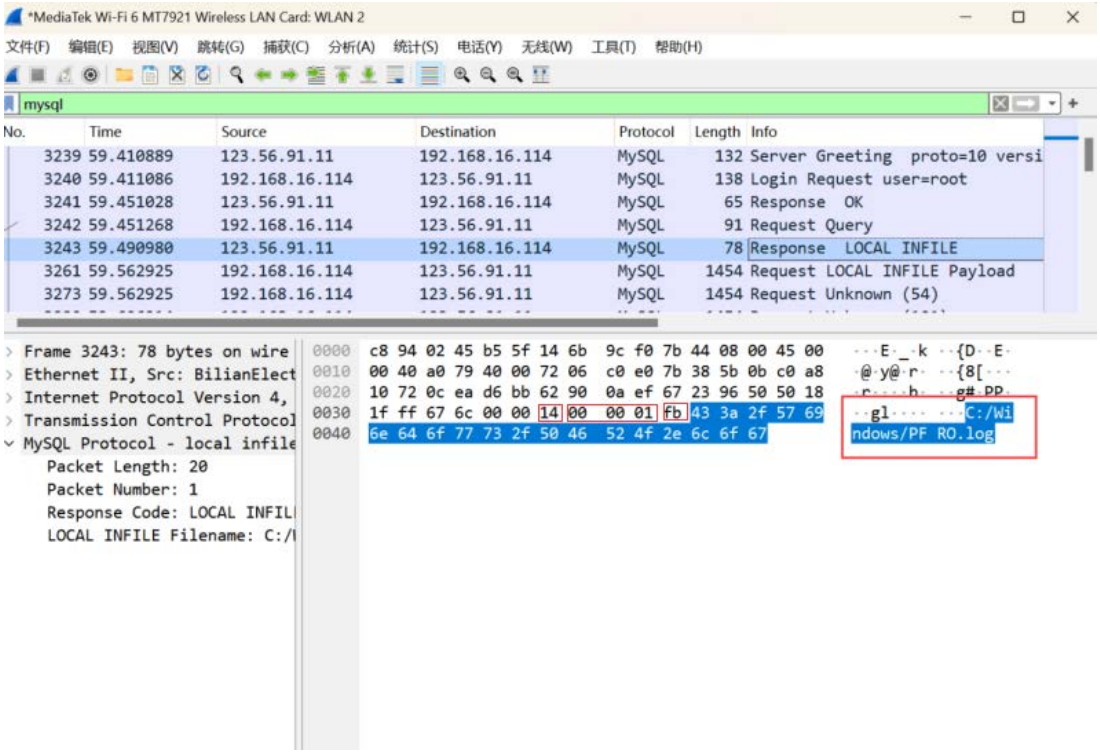

Figure 6. Reading file traffic packet for the first time
图 6. 第一次读取文件流量包

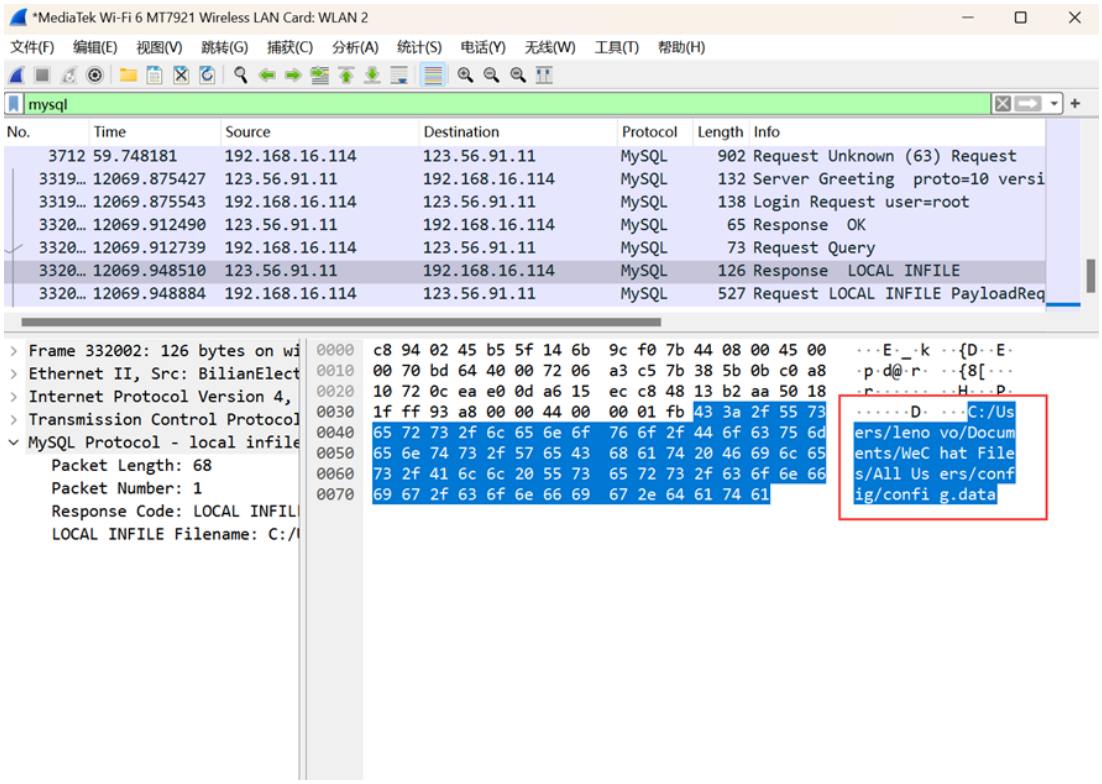

Figure 7. Read the file traffic packet for the second time
图 7. 第二次读取文件流量包

根据上文通信过程分析，在攻击者尝试连接时，MySQL 服务器返回一个包含版本注释信息的结果集，此时实现第一次文件读取，读取文件流量如图 6 所示。这里 000001 指数据包的序号，fb 指包的类型，最后一个框指要读取的文件名，而最前面的 14 是指文件名的长度，所以 payload 应该是 chr(len(filename) + 1) + "\x00\x00\x01\Xfb" + filename，此数据包是伪造的 MySQL 服务器发送读取 C:\Windows\PFRO.log 文件的数据请求(通过 MySQL 的 load data local infile ‘C:\Windows\PFRO.log’ into table test fields terminated by ‘\n’；语句向连接服务器的客户端发送读取文件的 payload)，此时我们读取攻击者 PC 上的“C:\Windows\PFRO.log”文件，并将结果以 base64 加密格式保存在 log 文件夹中相应 IP 文件夹的 PFRO.log 文件中。同时利用正则匹配技术提取用户的 username 信息。

当攻击者继续进行下一步(数据库增删改查等)操作时，会触发错误提示并断开数据库连接。此时实现第二次文件读取，系统将获得的用户名进行拼接并获取入侵者的微信配置文件，读取文件流量如图 7 所示。此数据包是伪造的 MySQL 服务器发送读取 C:\Users\lenovo\Documents\WeChat Files\All Users\config\config.data 文件的数据请求(通过 MySQL 的 load data local infile ‘C:\Users\lenovo\Documents\WeChat Files\All Users\config\config.data’ into table test fields terminated by ‘\n’；语句向连接服务器的客户端发送读取文件的 payload)，此时我们读取攻击者 PC 上的“C:\Users\lenovo\Documents\WeChat Files\All Users\config\config.data”文件，并将结果以 base64 加密格式保存在 log 文件夹中相应 IP 文件夹的 wx 文件中，同时利用正则匹配技术提取用户微信 id (wxid)信息。

3.3. 日志记录模块

日志记录模块的主要功能是对收集到的攻击者信息进行详细记录，以便管理员能够通过专业的日志审计工具生成全面的攻击者画像。具体记录的关键信息包括攻击时间、攻击 IP、电脑用户名、微信 ID 以及攻击者的定位等。这些重要数据将被准确地保存在名为“attack_log.log”的日志文件中，如图 8 所示。该日志文件的设计旨在确保信息的完整性和可读性，通过提供详实的攻击者信息，管理员可以进行追溯和审计，从而更有效地采取相应的安全措施。

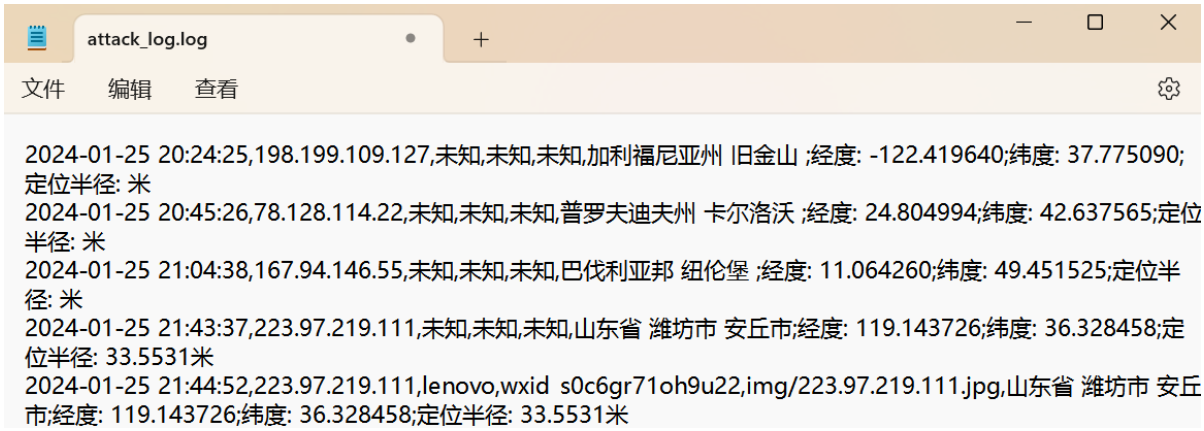

Figure 8. attack_log.log file information
图 8. attack_log.log 文件信息

3.4. 数据可视化展示

数据可视化是 Web 端管理界面，基于 html、css、js 以及 php 综合开发。模块采用基于表单的身份验证方式，管理员使用该系统前需首先完成登录认证。Web 端界面主要有数据大屏和事件汇总两大模

块，数据大屏实时展示当前日期时间、累计攻击次数、累计溯源个数、攻击 ip 排行及攻击地址等信息，同时用图表及滚动动画形式分别对攻击 ip 攻击地区排行进行可视化展示，当鼠标滑到攻击 ip 排行图表上时可展示攻击 ip 详细信息及攻击次数，滑到攻击地址排行单一地址上可展示该地址详细信息及其准确位置，如图 9 所示[7]。事件汇总界面对攻击时间、攻击 ip、攻击者电脑用户名，攻击者 wechatld 等信息进行逐条展示，每页展示 10 条数据记录，如图 10 所示；管理员可通过查看详情以及删除按钮实现对系统界面管理，完成详细信息展示和删除相关数据等操作，攻击者详情界面如图 11 所示。

Figure 9. System data large screen interface
图 9. 系统数据大屏界面

Figure 10. System event summary interface
图 10. 系统事件汇总界面

Figure 11. Attacker details interface
图 11. 攻击者详情界面

4. 结论

MySQL 数据库因其有着出色的执行效率和高度可扩展性并提供了稳定可靠的数据存储解决方案，已经成为众多开发者的普遍选择[8]。但是随着其被使用率的提高，越来越多针对 MySQL 的恶意攻击接连出现，传统的网络安全防御技术虽然能在一定程度上起到保护作用，但是对未知的攻击行为却显得无能为力，蜜罐技术在一定程度上可以弥补相关不足[9]。本系统基于 Python 伪装了 MySQL 蜜罐，捕获攻击者信息，同时与 Web 端可视化交互界面相结合，为攻击者溯源提供强力支持。

基金项目

本文为徐州工程学院大学生创新创业训练计划项目(xcx2023205)的阶段性成果之一。

参考文献

[1] 牟鑫明. 基于虚拟蜜罐的智能主动防御技术研究[D]: [硕士学位论文]. 沈阳: 沈阳理工大学, 2021.
[2] 张炳彦. 基于虚拟蜜罐的入侵检测可视化系统[D]: [硕士学位论文]. 济南: 济南大学, 2019.
[3] Stoll, C. (2005) The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage. Simon and Schuster, New York.
[4] 向全青. 基于网络扫描技术的动态蜜罐网络设计与实现[J]. 信息技术, 2013, 37(6): 157-161+165.
[5] 张勇, 卢强, 鲁晓, 等. 基于 MySQL 的科研论文管理系统设计与实现[J]. 微型电脑应用, 2023, 39(1): 4-6+10.
[6] 安延文. 数据库审计系统中 MySQL 协议的研究与解析[D]: [硕士学位论文]. 北京: 华北电力大学, 2016.
[7] 范诗帆, 程文志. 基于 Web 的医院食堂订餐系统设计与实现[J]. 无线互联科技, 2023, 20(16): 78-80.
[8] 郭晶晶, 刘学博. 基于 Java 的参数设置管理系统的设计与应用[J]. 山西电子技术, 2023(4): 54-56+60.
[9] 李珍珍. 基于蜜罐技术的网络安全防御系统的设计与实现[D]: [硕士学位论文]. 南京: 东南大学, 2019.