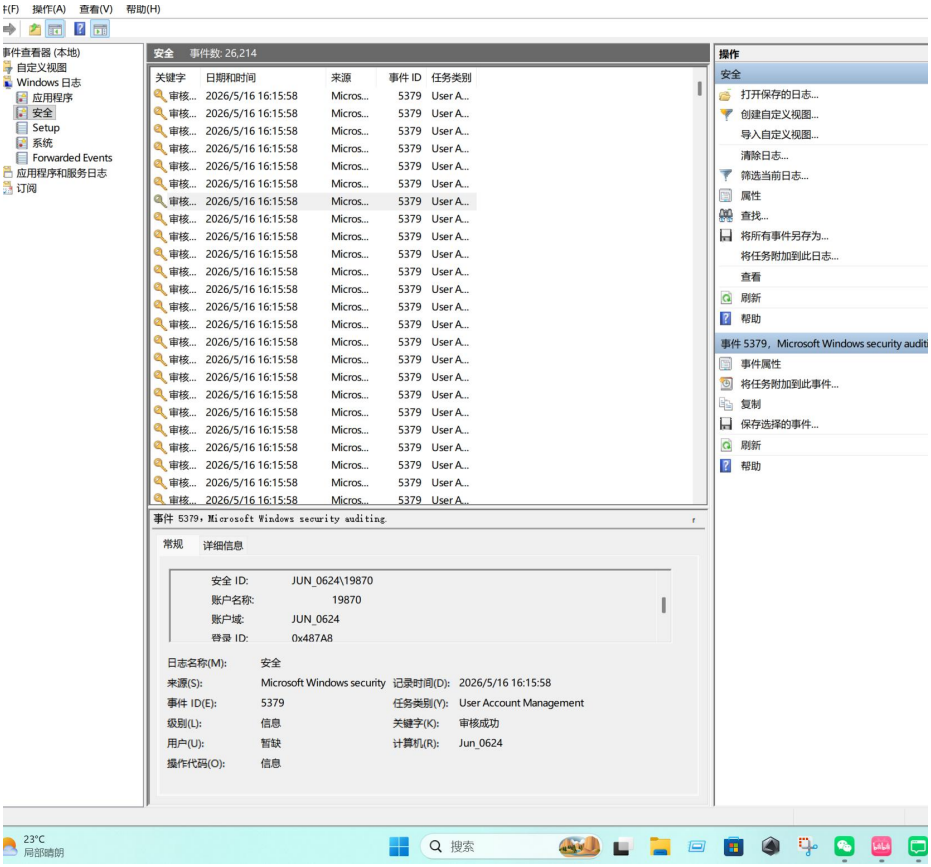
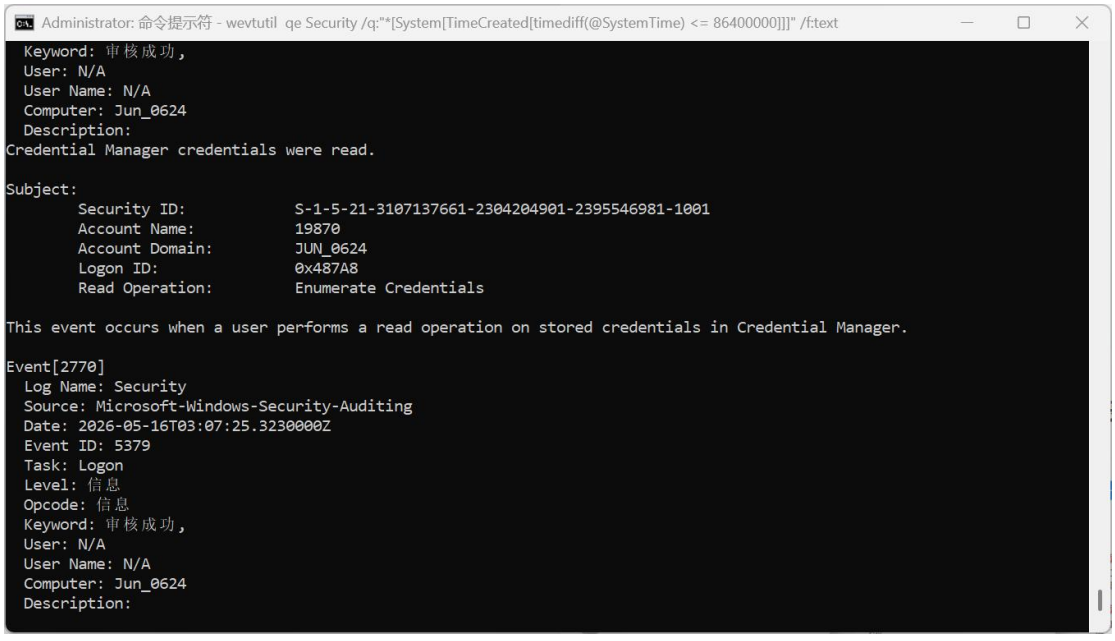
2026-05-10 | 14:332026-04-19 | 14:33

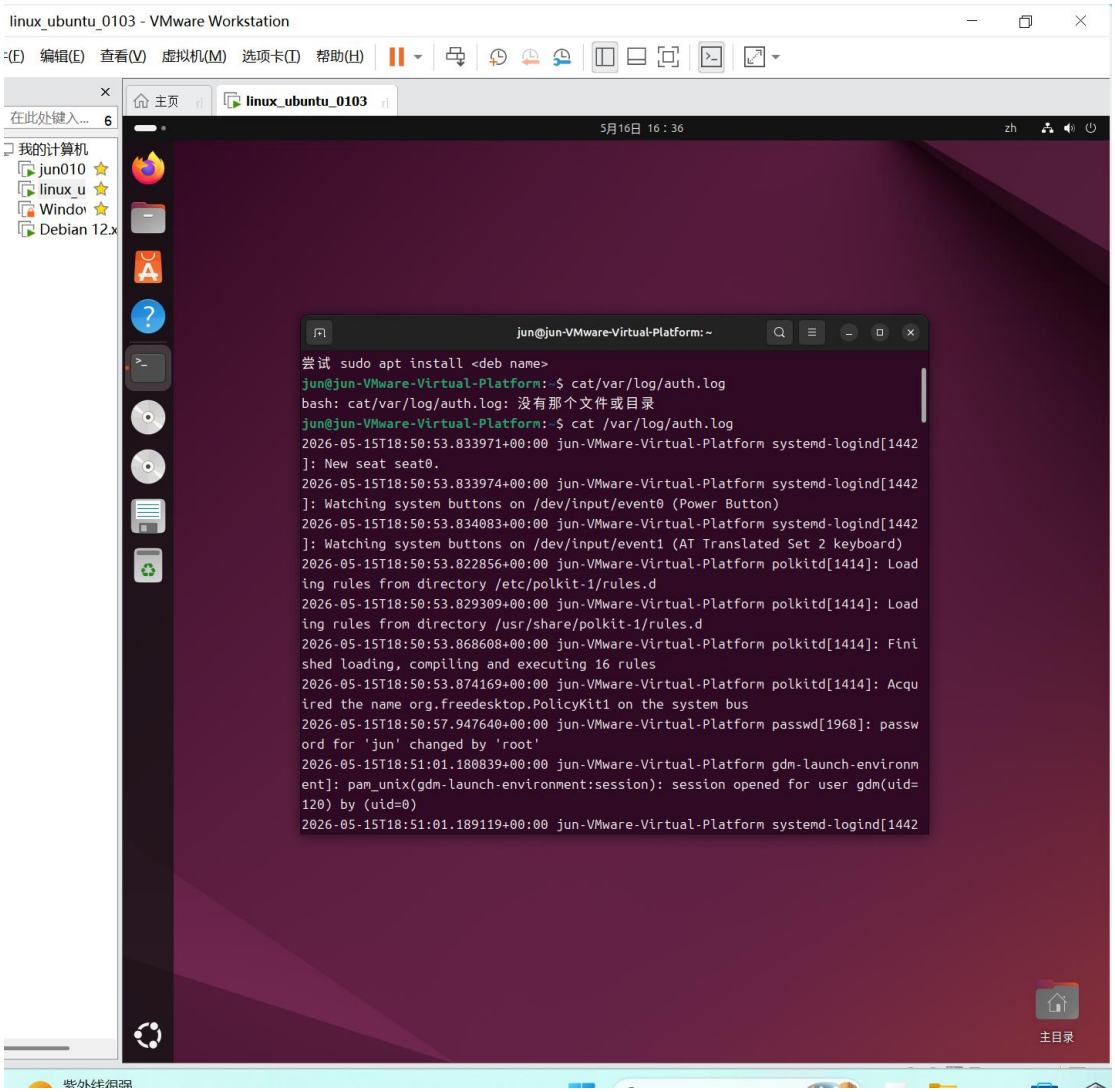
1.环境搭建：VMware 虚拟机双系统部署

在 Windows 主机上通过 VMware Workstation 完成 Ubuntu Linux 桌面版 虚拟机的安装与初始化配置

对比了 Windows 图形化操作系统与 Linux 命令行操作系统的核心差异







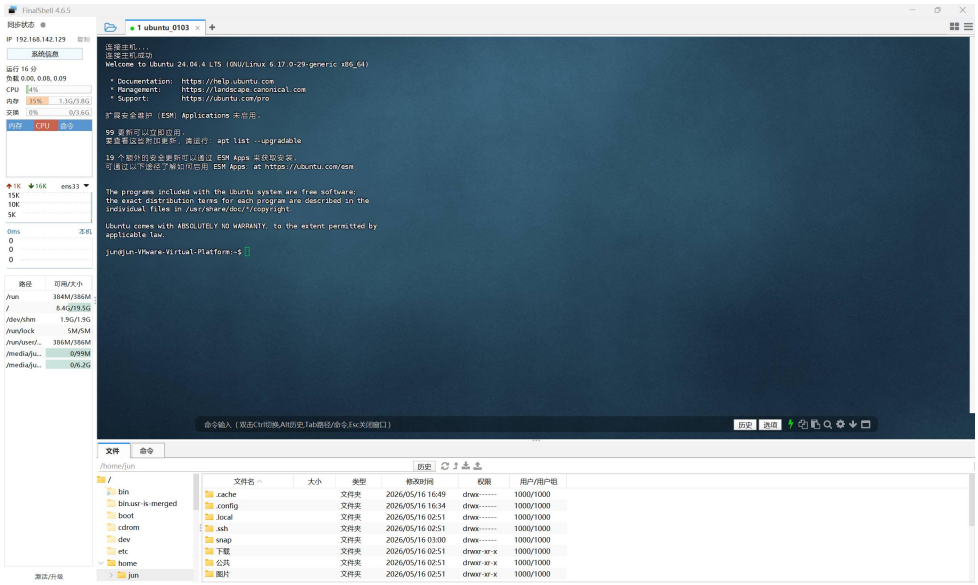
解决了虚拟机窗口切换、鼠标捕获、分辨率适配等基础操作问题

产生了关键疑问："有 Ubuntu 桌面为什么还要学命令行和 Vim"，并明确了 "桌面版仅用于学习，真实服务器全是无桌面命令行环境"的核心认知

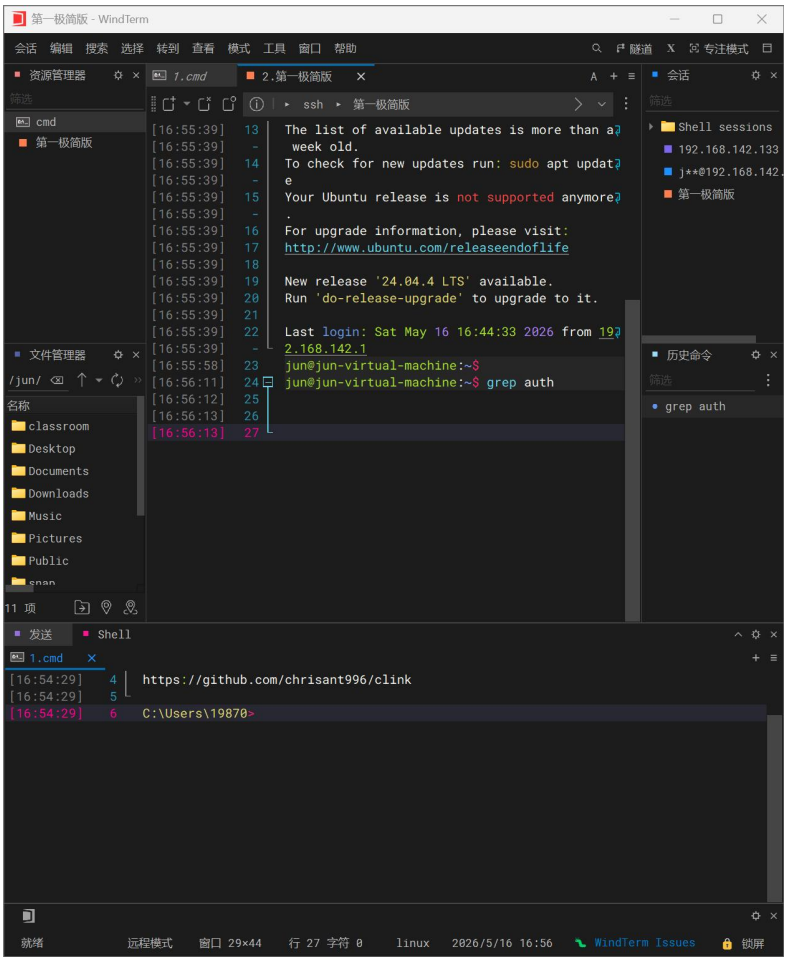
2. 远程连接：WindTerm SSH 工具实操

在 Windows 上安装并配置 WindTerm 终端工具

成功通过 SSH 协议 远程连接到本地 Ubuntu 虚拟机



（FinalShell 连接）



（WindTerm SSH 连接）

实现了脱离 VMware 虚拟机窗口，直接在 Windows 系统中操控 Linux 命令行

理解了这一操作的实际意义：完全模拟企业真实工作场景，所有云服务器、内网服务器都只能通过这种远程方式访问

3. 系统日志分析：Windows 与 Linux 日志对比

分别查看了 Windows 和 Linux 系统的安全日志

Windows：通过 "事件查看器" 图形界面查看安全事件日志

Linux：通过命令行查看 /var/log/auth.log 认证安全日志

对比了两类系统日志的格式、存储位置和查看方式的本质区别

建立了 "日志是网络安全应急响应、入侵排查第一手资料" 的核心认知

4. 核心技能：Linux Vim 编辑器从零到会

遇到并解决第一个报错：输入 vim test.txt 提示 "vim: 未找到命令"，通过 sudo apt update && sudo apt install vim -y 完成安装

掌握 Vim 完整操作流程：
新建 / 打开文件：vim 文件名
进入编辑模式：按 i 键（光标变为竖线）
退出编辑模式：按 Esc 键（光标变为方块）
保存并退出：:wq
查看文件内容：cat 文件名
解决关键卡点：搞懂了 Vim 两大核心模式的区别

编辑模式（竖线光标）：只能输入文字，不能使用任何快捷键
普通模式（方块光标）：才能使用光标移动、删除、复制等所有命令
学习了 Vim 基础光标移动快捷键:h(左)/j(下)/k(上)/l(右)、gg(文件头)、G(文件尾)

完成多次实操验证：新建文件、输入内容、修改内容、保存退出、查看结果，全部成功

5. 网安理论体系：建立学习目标与认知

学习了国际标准 NIST SP 800-61 应急响应四阶段：准备→检测分析→遏制根除恢复→事后复盘

理解了告警关联、IOC（失陷指标）、数字取证等网安核心概念

建立了清晰的学习路径认知：现在学习的 Linux 命令、Vim 编辑器、日志分析，都是未来从事网络安全、系统运维工作的必备基础技能