主动防御的网络安全蓝队工具设计与应用

关新元
广西制造工程职业技术学院，广西 南宁 530105
DOI: 10.61369/TACS.2026080015

摘　　要： 课题主要研究网络攻防中协助蓝队防守的技术，旨在辅助蓝队有效进行网络安全防御，对用户系统进行检查并增强其抵御攻击的能力。项目采用 Python 语言设计与实现。首先，通过安全基线检查功能，帮助蓝队快速识别用户系统的潜在安全漏洞与配置异常，及时提醒用户进行系统维护与更新。其次，结合日志分析模块，可对服务器网络活动进行深入监控，及时发现异常行为，同时支持对 Windows 系统进行日志分析，协助用户发现潜在安全威胁、监测系统健康状态。最后，溯源辅助功能支持蓝队对恶意 IP 进行快速、精准的溯源，辅助用户掌握攻击者相关信息，有效提升应对安全威胁的能力。该工具将为蓝队在网络攻防中提供合理、有效的防御支撑，应对不断增长的网络安全挑战，成为网络防御的得力助手。

关 键 词： 蓝队；网络安全；检查；流量解密；溯源辅助

Design and Application of a Proactive Defense Cybersecurity Blue Team Tool

Guan Xinyuan
Guangxi Vocational and Technical College of Manufacture Engineering, NanNing, Guangxi 530105

Abstract: This research primarily focuses on technologies that assist blue team defense in cyber attacks and defenses, aiming to help the blue team conduct effective network security defense, inspect user systems, and enhance their ability to resist attacks.The project is designed and implemented using the Python language. First, through the security baseline check function, it helps the blue team quickly identify potential security vulnerabilities and configuration anomalies in user systems, promptly reminding users to perform system maintenance and updates. Second, combined with a log analysis module, it enables in-depth monitoring of server network activities and timely detection of abnormal behaviors. It also supports log analysis for Windows systems, helping users discover potential security threats and monitor system health status. Finally, the traceability assistance function allows the blue team to perform fast and accurate tracing of malicious IP addresses, assisting users in grasping attacker-related information and effectively improving their ability to respond to security threats. This tool will provide reasonable and effective defensive support for the blue team in cyber attacks and defenses, addressing growing cybersecurity challenges and serving as a capable assistant for network defense.

Keywords: blue team; network security; inspection; traffic decryption; tracing assistance

引言

近年来，网络攻击事件频发，个人隐私泄露、企业数据被盗、国家基础设施受损等问题日益严重，网络犯罪已成为全球第三大“经济体”，预计2026年造成损失将达12万亿美元。在我国加快推进网络强国战略的背景下，网络安全防护已成为企业常态工作，但现有设备难以应对复杂多变的威胁。因此，开发网络攻防蓝队工具具有重要意义，可帮助防守方高效完成安全监测、日志分析、攻击溯源等任务，降低人力成本，提升防御效率。当前，国内外已有威胁情报平台、AI 安全产品、云安全服务及攻防演练机制，技术基础成熟。从技术、经济及法律角度分析，该工具具备可行性，开发成本低，符合法规要求，有助于提升整体网络安全防护能力。

一、需求分析

网络攻防蓝队工具面向网络安全团队、信息安全专业人员和系统管理员等，旨在监测和应对安全威胁。具体需求为：（1）漏洞检测修复，及时发现并提供建议；（2）实时监测警报，监测网络活动、异常行为和潜在入侵并报警；（3）日志分析追踪，分析

课题项目：基于主动防御的网络安全蓝队工具设计与应用的研究项目（项目编号：ZZXYXJKT202510）。
作者简介：关新元，男，广西制造工程职业技术学院人工智能学院信息安全专任教师，研究方向为网络信息安全。

Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.

系统日志等以追踪攻击者活动和溯源；（4）可视化报告，可视化呈现安全数据和报告。此外，用户希望工具界面简洁、操作流畅，具备良好性能和稳定性。深入分析用户需求可增强工具实用性和满意度，提高竞争力。

二、开发技术

基于 Python 语言实现，用到 re、sys、time、requests、subprocess、json 等基础库。此外，还用到 psutil 库，这是强大的跨平台 Python 库，可获取系统信息、管理进程，能帮助开发者监控、管理和控制系统资源，可在主流操作系统上运行，开发者能自由查看、修改和分发，是功能强大、易用灵活的系统管理工具库。工具还使用 Geoip2 库，这是 IP 地址定位库，可根据 IP 地址查找位置信息，使用 MaxMind 公司的 IP 地址数据库，提供方便的 Python API，能提供国家、城市等多种信息，还可使用 IPv6 地址查询

三、功能设计

（一）整体功能设计

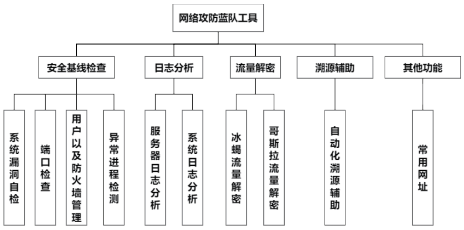


图1 网络攻防蓝队工具模块功能图

工具主要包括五大功能，分别是安全基线检查、日志分析、流量解密、溯源辅助、其他功能。

（二）安全基线检查模块

安全基准检查是网络防护关键手段，能保证信息系统安全设定合格、减少侵袭风险。先依据行业规范制定安全规范或最优实践，管理员或团队用自动化或手工方式评估系统，发现设定错误等问题后进行修正，以满足安全基准要求。此检查可保证系统基础安全、降低侵袭风险、维护数据资产，是机构信息安全管理关键部分。

安全基准检查模块有四个功能：

（1）端口检测：检测系统端口，回显端口号、进程号和异常端口，便于排查。

（2）进程排查：筛选使用率前五的进程，检测有无异常。

（3）用户及防火墙管理：可快速管理并查看用户（含影子用户），还能检测并一键开启防火墙。

（4）漏洞自检：搜集系统信息并对照微软官网检测漏洞，快速发现系统漏洞。

（三）日志分析模块

日志分析是网络安全重要一环，通过审查、分析系统日志数据识别安全事件与威胁。Apache、Nginx、Windows 等系统会产生大量日志，分析这些日志可发现潜在安全威胁、监测系统健康并提供调查线索。日志分析关键步骤包括收集、存储、分析和应用。要确保系统配置正确以生成并收集日志，收集存储后进行分析，通过自定义脚本解析日志文件，提取信息并统计。用户根据分析结果行动，发现异常或威胁及时修复应对，还可用于系统优化和改进安全策略。日志分析对网络安全管理不可或缺，工具中的日志分析模块可助用户发现应对安全威胁与异常，分析系统日志能了解运行状况、监测用户活动和发现潜在攻击。

（四）攻击流量解密模块

在网络安全领域，Webshell 管理工具是常见威胁，流量解密对抗此类恶意工具至关重要。以冰蝎和哥斯拉等远程访问工具为例，这类工具利用加密和编码技术实现通信隐藏，可有效绕过传统安全防御机制，使其行为难以被检测和识别。而流量解密可还原分析网络流量，及时发现、应对和清除威胁。Webshell 管理工具通过加密通信与远程控制服务器交互攻击，本工具流量解密功能可对冰蝎和哥斯拉流量解密，还原通信内容，识别恶意指令和攻击行为，阻断远程控制，减轻损失。总之，流量解密对抗 Webshell 工具流量十分重要，能揭示恶意工具意图和行为，检测远程控制命令和攻击行为，提高组织对网络安全威胁的识别与应对能力，保护网络和数据安全。

（五）溯源辅助功能模块

溯源行为在网络攻防中具有重要的意义和价值。该功能可以帮助确定攻击来源、收集证据和取证、加强安全防御，以及保护网络资产和敏感信息。通过追踪和识别攻击源头，可以及时发现和应对网络攻击，维护网络的安全稳定，保护利益和声誉。因此，在网络安全管理中，溯源是一项至关重要的任务，对于确保网络安全和防御网络攻击具有较为重要的作用。

四、功能实现

（一）安全基线检查功能实现

1. 系统漏洞自检

（1）脚本从微软官网 API 获取受影响产品的 CVE 漏洞信息并存储到数据库。

（2）利用 Shodan 平台查询 CVE 漏洞是否有对应的 EXP，通过检索 CVE 漏洞号在 Shodan 平台的搜索结果判断是否有公开 EXP。

（3）脚本自动读取用户系统版本，据此查找 CVE，根据系统版本和补丁信息在数据库中检索相关 CVE 漏洞信息并检查是否有对应 EXP，若存在则回显到功能窗口。

2. 端口检查

该功能主要由两个函数完成。首先，start_port_analysis 函数用于执行端口分析，利用 Python 的 subprocess 库执行 Windows 系统命令 netstat -ano，捕获输出结果，该命令可显示网络连接和监听端口信息。然后将输出结果按行分割并遍历，在工具 GUI 界面显示结果。接着，用正则表达式提取每行中的 IP 地址和端口号，存于 ip_port_matches 列表，检查是否存在常见异常端口（如

 Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.

22、445、3389等），若有则在图形化界面显示提示信息。另一个函数 Iptransform，先筛除本机网络连接中的局域网 IP，再筛选出外部地址的 IP，通过 Geoip2 库获取 IP 对应的具体位置信息，如国家、地区、经纬度等。

（二）日志分析功能实现

1. 服务器日志分析

服务器日志分析针对 Apache 和 Nginx 主流服务器。代码是用于分析日志文件的 Python 脚本，主要对指定日志文件分析，包括统计 IP 访问次数、检测 SQL 注入攻击和攻击者访问的敏感路径或 Webshell 痕迹。整体上，该功能实现对 Apache 和 Nginx 日志文件简单分析，可帮助用户发现异常行为和潜在安全威胁，通过统计 IP 访问次数、检测攻击和敏感路径，助用户及时应对网络攻击。

2. 系统日志分析

该功能是针对 Windows 系统的日志分析。通过编写 PS1 文件，检查 Windows 系统的电脑异常开关机、崩溃等事件。

（三）攻击流量解密功能实现

本功能通过编写 Python 脚本对冰蝎的攻击流量进行解密。针对冰蝎的加解密方式，写出对应解密函数，主要包括了对 PHP、ASP、C# 和 Java 四种语言的解密函数。这些函数都接受四个参数：密钥、语言类型、待解密的载荷、待解密的数据类型（请求或响应）。根据不一样的语言类型和数据类型，选择调用与之相对应的解密函数进行解密最后打印解密结果。在异常处理方面，解密过程中如果遇到异常情况（如解密失败），会进行适当的异常处理，并打印异常信息。

通过命令行参数传入密钥、语言类型、待解密的载荷和数据类型，调用相应的解密函数进行解密，并打印解密结果。

（四）溯源辅助功能实现

本功能主要用于对攻击者的自动化溯源。当用户确定下恶意 IP 后，输入到工具中，点击按钮后即可进行溯源辅助。脚本通过命令行参数传入目标 IP 地址，然后依次进行 IP 地理位置定位、IP 反查网站域名、备案信息查询、Whois 信息查询和端口扫描。脚本使用了多个第三方库，包括 Geoip2、Whois、Requests、Re、Lxml、Json、Nmap 等，通过这些库实现了各种功能的实现。这个脚本的目的是通过多种方式对攻击者的 IP 地址进行分析和溯源，从而了解攻击者的位置、所属组织、攻击方式等信息，为进一步的防御和追踪甚至反制提供帮助。

（五）常用网址展示

该功能主要是给出一些防守方的常用网址，例如常见的威胁情报查询网站、资产测绘网站、网站信息查询网站、常用搜索网站。可以让用户在利用工具的同时使用这些网站，达到相辅相成的效果。

五、结语

本文主要讲述了一个在网络攻防中防守人员使用的蓝队工具，研究并实现了蓝队工具，在对自身系统进行全面安全检查的同时，又能根据攻击者的攻击情况，基于溯源、分析、流量解密等功能来对攻击者进行分析，帮助网络安全中的防守方及时采取措施以减少资产损失。随着信息技术的不断发展和普及，网络安全已经成为了现代社会中不可或缺的一部分。未来，随着人工智能、大数据、物联网等新兴技术的快速发展和应用，网络安全领域也将面临新的挑战和机遇。

参考文献

[1] 马天骐 . 企业信息安全体系构建 [J]. 企业管理 ,2024(04):113-115.

[2] 王方宁 . 安全基线管理系统的研究与实现 [D]. 西安电子科技大学 ,2018.

[3] 贺承玮 , 陈柯序 . 网络安全等级保护测评中网络安全现场测评方法 [J]. 网络安全技术与应用 ,2024(01):12-14.

[4] 史方旭 . 面向系统日志的异常检测方法研究与实现 [D]. 北京邮电大学 ,2024.

[5] 吴可 . 基于机器学习的 Web 日志异常流量检测技术研究 [D]. 电子科技大学 ,2022.

[6] 李时雨 . 基于日志的 Web 攻击痕迹关联分析技术研究与实现 [D]. 北京邮电大学 ,2022.

[7] 王世通 . 基于 HTTP 协议的 WebShell 检测研究 [D]. 北京邮电大学 ,2022.

[8] 何恬 . 基于攻击行为的网络攻击溯源关键技术研究 [D]. 江南大学 ,2024.

[9] 李立山 . 企业入侵检测系统的设计与实现 [D]. 北京交通大学 ,2022.

[10] 韩中 , 荀和平 , 陈益全 , 等 .Web 云服务监控的 Python 技术实现 [J]. 长江信息通信 ,2022,35(05):88-91.

Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.