Computer Science and Application 计算机科学与应用, 2024, 14(4), 308-315
Published Online April 2024 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2024.144100

Hans汉斯

高校网络攻防安全浅析

——以伊犁师范大学为例

张　斌，张体谅*，刘新茂，田沛涛

伊犁师范大学信号检测与控制技术重点实验平台，新疆　伊宁

收稿日期：2024年3月25日；录用日期：2024年4月22日；发布日期：2024年4月30日

摘　要

随着信息技术的飞速发展，互联网已经深入人心，网络安全问题也相伴而生，针对高校信息基础设施的网络事件频发，侵犯个人隐私，窃取个人信息，网络诈骗等违法犯罪依然猖獗，网络安全的威胁来源和供给手段也在不断变化，网路攻击和防护是矛和盾的较量，只有深入了解网络攻击的技术方法和攻击路径，才能知己知彼，百战不殆。本文结合攻防演练中常用的攻击和防御手段，从攻防两端视角总结校园网攻击的路径和防护手段，助力高校一站式适配多种安全风险场景，构建实时自适应安全防护能力，搭建以人员和业务为核心的安全体系，全面提升校园网络安全，促进高校数字化安全转型。

关键词

高校，攻击，防御，网络安全，数字化转型

An Analysis of Network Attack and Defense Security in Colleges and Universities

—Taking Yili Normal University as an Example

Bin Zhang, Tiliang Zhang*, Xinmao Liu, Peitao Tian

Key Experimental Platform for Signal Detection and Control Technology, Yili Normal University, Yining Xinjiang

Received: Mar. 25th, 2024; accepted: Apr. 22nd, 2024; published: Apr. 30th, 2024

Abstract

With the rapid development of information technology, the Internet has been deeply rooted in people's hearts, network security issues are also accompanied by the frequent occurrence of net-

*通讯作者。

文章引用: 张斌, 张体谅, 刘新茂, 田沛涛. 高校网络攻防安全浅析[J]. 计算机科学与应用, 2024, 14(4): 308-315.
DOI: 10.12677/csa.2024.144100

work incidents against the university information infrastructure, invasion of personal privacy, theft of personal information, network fraud and other crimes are still rampant, network security threat sources and means of supply are also constantly changing, network attacks and protection is a battle of spears and shields, only an in-depth understanding of network attack techniques and attack paths can know the enemy and know ourselves. Only with an in-depth understanding of the technology of network attacks and attack paths can we know ourselves and the enemy and not be in danger. This paper combines the attack and defense means commonly used in attack and defense drills to summarize the path of campus network attack and protection means from the perspective of both attack and defense, to comprehensively enhance campus network security, to promote the digital transformation of schools, and to provide a reference for the reinforcement of campus network security in the biased areas.

Keywords

Higher Education, Attacks, Defense, Cyber Security, Digital Transformation

1. 引言

近年来，教育系统已经成为网络攻击的重点区域，特别是高校面临的 APT 攻击逐渐增多。通过近几年开展的攻防演练监测数据统计，攻击方会主要是通过社工或者技术手段进行攻击。主要方法是通过情报收集、防线突破、通道建立、分布攻击[1]。对于已经确定的目标进行针对性的突破，如收集互联网暴露面的数据、通过爬虫抓取有价值信息，不断收集公开的漏洞和 0 day 漏洞，持续性对攻击目标进行扫描，确定资产属性及部署应用，再比对武器库，构建目标攻击面，或通过哄骗利诱收取有价值情报，从而突破防线，建立通道并利用相关工具采用多种方式进行横向或者纵向渗透。不断的制作攻击工具进行复杂的分布攻击，实行精准目标攻击[2]。

具体来说，高校的供应链、师生安全意识情况较为突出，很多系统都可以通过互联网直接访问，一旦其软件产品出现了可被远程利用的安全漏洞，将会产生大面积的、连片式的网络安全风险。此外，近几年来数据安全和个人信息相关的安全事件有所增加，因此，攻防演练已成为检验高校网络安全综合防御水平的“试金石”和提升网络攻击应对能力的“磨刀石”。

孙子兵法有云：“知己知彼，百战不殆；不知彼而知己，一胜一负；不知彼，每战必殆。”这同样适用于校园网络攻防领域，充分了解攻击手段是取得胜利的关键。网络攻防不仅是一种技术手段，还是一种战略思维，而网络防御需要建立在深入了解攻击者的心理和攻击手段的基础上，掌握攻击模式和攻击路径，对其攻击行为进行有效防御和应付，从而建立一个完善的网络安全管理体系和完善的安全管理规范和操作流程。为了有效应对 AI 赋能网络攻击的安全威胁，结合攻防演练中常用的攻击和防御手段，防范安全威胁、构建对等能力角度加强智能化校园网络安全系建设。

2. 校园网络攻击方法和路径

根据近几年新疆高校攻防演练监测，常见的攻击技术手段有利用 0 day 漏洞、集权类设备攻击、社会工程学攻击、供应链攻击、临时测试开发环境工具，攻击者绕过高校的网络防守策略，采用新型攻击方法，进行战术性的攻击。

虽然我们采用新思路和新方法积极变革安全措施，不断建设和完善自身的网络安全体系，但在实际演练中，安全防护体系还是经常被“打穿”究其原因，很多情况下并不是安全体系不健全，而是策略和意识存在漏洞，在高校的特殊的场景中，学生团体人数众多，他们思维灵活、个性活泼，大多是时间都在互联网上学习交友，网络安全意识一旦疏忽，就会导致网络安全风险，利用这一特定场景攻击者不断寻找路径和方法进行渗透。

2.1. 高校数据情报收集

高校网络攻击在收集情报时，往往关注以下几类目标：

1) 学校各类资产，比如，教职工数据、学生数据、科研数据；
2) 学校组织机构庞大，从关注度较低的二级单位所属系统寻找突破口；
3) 选用对外开放且用户量大、业务线长的目标系统作为突破口；
4) 新上线系统往往存在安全漏洞和防护措施确实、易成为攻击的突破口；
5) 测试系统、已停机未下线的系统缺乏统一安全管控；
6) 高校私有云平台的建设，如云计算平台、超融合平台；
7) 移动应用、物联网等新技术应用防护不到位，存在安全隐患；
8) 通过供应链的攻击，迂回攻击目标系统；
9) 安全意识疏忽，导致信息泄露。

2.2. 高校网络防线突破

高校网络防线突破往往是从互联网测发起网络攻击，在突破高校外网后进入校内网，之后进一步突破内网，进而控制位于核心网络区域的目标系统，攻击方法如图 1 所示。

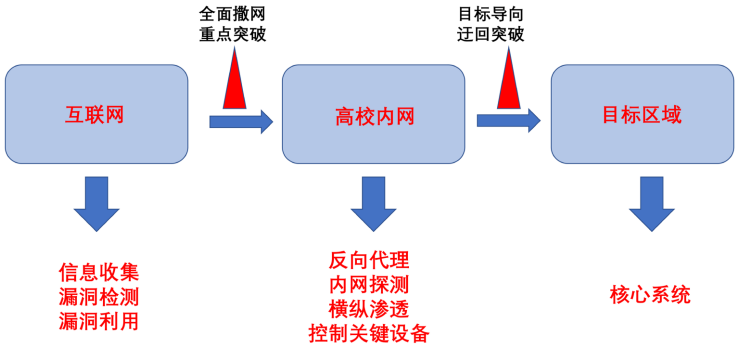

Figure 1. Methods of attack
图 1. 攻击方法

1) 入口突破

攻击者针对特定目标进行信息收集、对象建模、收集域名、IP、服务、供应商。或者是在互联网上暴漏的员工邮箱、源代码、测试账号的敏感信息。通过交互式挖掘工具，如 kali Maltego 分析各个要素之间的关系，发现安全漏洞，找准突破口。

2) 内网渗透

进入校园内网后，找准立足点，建立后门，实施隐藏，长期控制，同时选择合适的主机建立跳板。

3) 通道建立

利用网络开放的端口建立数据的反向代理建立数据通道，在校内进行低强度的网络扫描，摸清网络

拓扑结构，再利用漏洞、弱口令等在网段内进行横向渗透，在网段间进行纵向渗透，控制域控服务器、DNS 服务器、运维人员主机、堡垒机等核心服务，如图 2 所示。

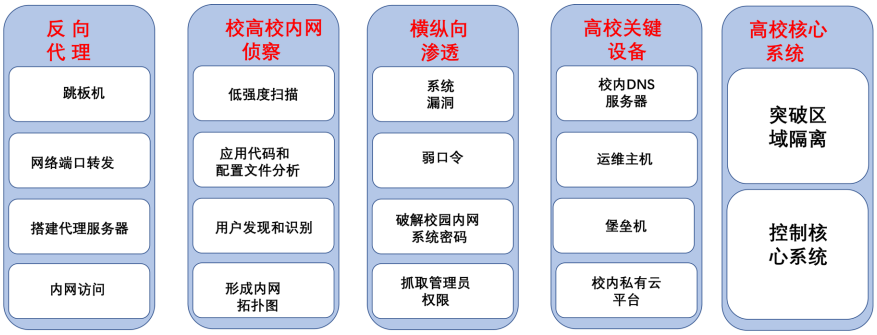

Figure 2. Attack path
图 2. 攻击路径

3. 校园网路安全防护策略

校园网网络攻击手段层出不穷，需要一套“组合拳”，才能为网络保驾护航，在了解攻击者的“三板斧”的基础上，知己知彼，才能守好校园网网络安全阵地，根据攻击技术，以动态、主动的防御举措，不断优化现有防护体系和加强安全意识。

3.1. 资产清理

1) 校内敏感信息梳理

网络及应用系统的相关技术文档。网络拓扑、设备密码、源代码等敏感信息，通过 IT 资产信息(如域名、IP、开放端口、证书信息、ISP 备案信息等)作为敏感特征[3]，再配合关键词(网络拓扑图、学号、邮件、说明书)搜索，理清暴漏面的敏感信息。在互联网上这些信息包含各类搜索引擎、学术网站、网盘、文库、社交平台等。

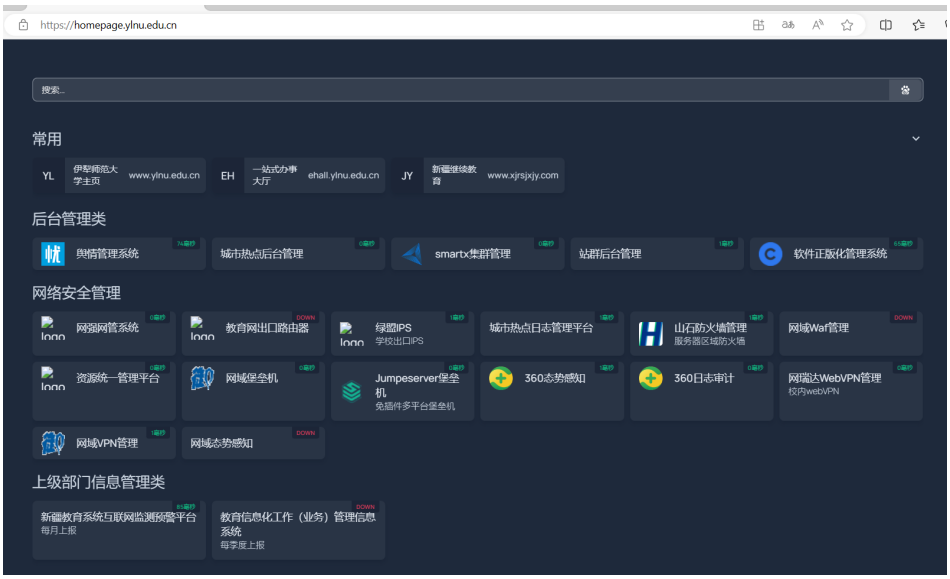

Figure 3. One click login
图 3. 一键登录

2) 校园网络边界梳理

对互联网、教育网等边界、校内各个系统进行精准的梳理，构建基于 Python 技术的校园网搜索引擎设计静态页面[4]，管理人员在特定办公场通过静态页面所一键式登录各个系统，确保网络的管理安全如图 3 所示。

3) 校内资产梳理

摸清家底，在互联网络上暴漏的设备、应用、数据库清查，关闭不必要的主机、应用和开放端口，开展内网信息系统、网络设备资产梳理，线下废弃不明归属的主机。

3.2. 网络安全加固

3.2.1. 技术防护

在校内不同区域、不同层面建立安全保护机制，构建纵深防御体系。综合运用校内态势感知、流量检测、追踪溯源等手段进行动态防御，对 DNS 域控制器、堡垒机、单点登录系开展重点防御[5]。构建威胁情报机制，通过威胁情报对 IP 地址、恶意域名、恶意软件指纹等精准快速识别攻击意图、定位攻击阶段，及时采取阻断措施。

针对集权类系统或重要业务系统，在高校 DMZ 处部署蜜罐设备，诱导攻击者攻击、窃取虚假数据，从而达到延缓攻击、监测告警、分析研判、追踪溯源的目标，最终定位攻击阶段，及时采取阻断措施。

1) 纵深防御

精准校内网络整体网络拓扑，组建团队，各负其责，构建人防、技防、物防的防守体系，检测及时、分析准确、处置高效；其次从管理组织架构、技术防护措施、安全事件应急处置等各方面能进行整体的安全评估，确定校内的安全防护能力和工作协作默契程度。

2) 动态防御

针对网络安全威胁利用校内防火墙、IPS、态势感知、WAF 等设备进行硬件防护，通过网络安全态势感知与安全设备联动，主动分析所有的威胁，对安全阻断设备的策略作出动态响应处置，及时将攻击方阻挡在防守网络之外，从而构建大纵深立体化防御体系，威胁情报和态势感知系统及时推送短信或者邮件信息，第一时间发现并阻断攻防的入侵行为，及时安全自查及优化、分析技术和问题整改措施计划。

3) 重点防御

技术对校内资产情况进行深入排查，详细了解资产软硬件信息、部署情况、访问用户情况、资产的安全性等信息，并使用漏洞扫描系统对网络内部的各节点设备进行安全漏洞及系统弱口令扫描，对发现的安全隐患及时处置，做到设备不留安全隐患，同时要提高响应速度及时发现漏洞[6]。

针对威胁信息，梳理网络攻击路径，明确源和目的类型、位置和途径，针对性的调整网络防护策略，同时梳理和目标系统相关联的资产，形成资产清单、对资产清单安全漏洞和威胁进一步排查，及时修复漏洞补丁和安全策略。

建立监控和告警机制：使用监控和告警系统实时监测 DNS 服务器的状态和性能，一旦发现异常情况，及时通过短信和微信通知，以便运维人员能够及时采取措施及时处理[7]。

实施等级保护：加强对关键基础资产的保护，重要资产在运行过程中有可能与其它资产系统互联互通引入安全风险，加强互联安全，把重要资产和非重要资产一起构建一体化的防御策略，从而实现整体防控[8]。

协同联防：整合校内技术力量，建立学校信息员队伍，和地方网信办、教育部门协同处置安全威胁，齐心协力共同应对形成强大的防御能力。

3.2.2. 处置机制

从校园网络安全攻击和防御双视角出发，建立威胁处理闭环机制，针对威胁事件通过校内全设备实行联动处置机制，主动阻断安全攻击行为，特殊事件通过人工策略进行处置，谁建设谁负责，及时形成威胁闭环机制。同时针对威胁情报及时归类，评估威胁的特性和特征，实行多部门协同，每一个事件进行管理，处理的问题事件都要验证，通过系统建设和流程设置，打造完整的发现 + 处置机制，建立健全应急处置流程和闭环策略，提高信息安全处理效率[9]，如图 4 所示。

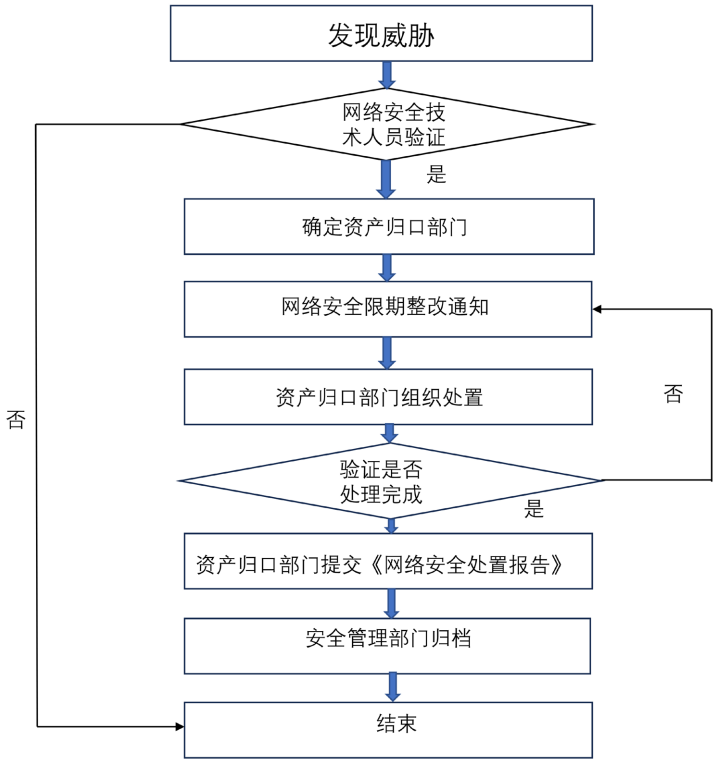

Figure 4. Threat handling process
图 4. 威胁处置流程

当发现重要安全事件或风险在内部传播时，通过技术手段通过态势感知平台去联动防火墙、EDR、日志审计、上网行为管理等安全设备主动出击亮剑沙场，通过其联动处置进行阻断、控制，避免影响扩大，构建主动出击的“检测”–“分析”–“阻断”–“溯源”–“反制”的事件闭环流程[10]。

3.3. 制度建设

1) 加强管理人员素质

培养安全意识和责任心，管理人员应具备高度的安全意识，认识到网络攻击对组织的危害，牢固树立保护网络安全的责任[11]。

2) 学习安全知识和技能

管理人员应具备一定的网络安全知识和技能，包括对常见威胁的了解、安全漏洞的识别和修补等。

3) 建立合理的权限和访问控制机制

设立明确的权限和访问策略，确保合适的人员只能获得所需的系统权限和资源访问。同时，应定期审查和更新权限设置，及时调整与职责不符的权限，防止恶意行为。

4) 完善网络安全制度建设

根据学校特定环境制定网络安全政策和管理规定，明确网络安全的目标、要求和流程。包括网络使用准则、密码管理、系统漏洞修补、备份与恢复等内容，对员工在网络使用中的行为给予明确指导。

建立安全审计和监控机制，制定相应的安全审计和监控制度，对网络空间的行为进行监测和审查。通过对网络活动和日志的实时监控和分析，可以及时发现潜在的风险和异常行为，并采取相应的措施。

责任划分：重新平衡网络安全空间责任，将网络安全的责任从个人转移到软件开发商和其它拥有必要资源及专业知识的机构手中，为了建设我们想要的安全和有弹性的未来，塑造市场力量，把网络安全责任意识从最脆弱的群体上转移出去，使我们的数字生态系统更值得信任。

4. 总结与建议

针对高校的新型攻击方式和路径，本文提出了全面的安全防护策略，一定程度上提高了校园的安全等级。但是高校网络安全始终是一个棘手的问题，并时时刻刻伴随着我们，我们必须高度重视。结合新时代、新技术、新发展理念，不断适应当前复杂多变的网络安全形势，积极应变，采用先进技术，创新的安全管理理念，为高校赋能，保障高校教育安全发展[12]。

我校在新形势下不断增加了网络安全攻防演练的投入，建设网络安全实验室、培养网络攻防人才，组建攻防团队、构建基于攻防对抗视角的新型网络安全防御框架，加速了安全事件处置的能力、主动检测威胁的能力、主动溯源攻击行为的能力，但是远远不够，我们还要从如下几点长期坚持：

1) 思想上高度重视

承认漏洞，正式威胁，采取适度防御，加强检测工作，落实相应，建立对威胁的防护来保证系统安全，所有的防护检测相应都是依据安全策略实施。

2) 时间上快速相应

以 PPDR 模型为基础，建立基于时间的校内快速相应安全模型，以攻防演练模拟为场景，采取安全防御措施，通过不同的攻击手段来计算攻破该防守措施所需要的时间，尽量减少网络安全威胁。

3) 技术上创新

构建高校健壮网络，利用 IPv6 + 安全技术，区块链技术、云计算技术等轻量部署，加密传输，安全服务上云等；建立台式感知平台、威胁情报机构，杜绝“木桶”效应。

基金项目

伊犁师范大学校级科研项目(2023YSYY005)。

参考文献

[1] 吴楠青, 刘后丞, 权华, 等. 攻防演习中从攻击方角度分析防守方可采取的应对措施[J]. 网络安全技术与应用, 2023(7): 1-2.

[2] 刘秋尘. 网络安全攻防演练中攻防双方技术概述[J]. 现代电视技术, 2023(6): 156-158+117.

[3] 刘志军, 戴高远, 田葆, 等. 域名系统风险分析及安全防护架构[J]. 广东通信技术, 2023, 43(8): 42-45.

[4] 闫丽丽. 基于 Python 技术的校园网搜索引擎设计[J]. 信息与电脑(理论版), 2023, 35(17): 183-185.

[5] 邓东林. 网络安全攻防演练中的防守方案设计[J]. 网络安全和信息化, 2022(9): 109-113.

[6] 王晟, 张通凯, 李超峰. 网络安全漏洞管理与漏洞情报库建设分析[J]. 电信工程技术与标准化, 2023, 36(12): 65-68+81. https://doi.org/10.13992/j.cnki.tetas.2023.12.010

[7] 韦娟, 徐建军. 校园网络安全“管理+运维”体系探索[J]. 网络安全技术与应用, 2024(1): 87-89.

[8] 田嘉豪, 胡吉祥. 等级保护 2.0 中渗透测试技术的研究[J]. 网络安全技术与应用, 2024(1): 11-12.

[9] 马宜东. 在攻防演练中提升网络防御能力[J]. 网络安全和信息化, 2023(4): 48-50.

[10] 张荣鑫. 如何组织一场网络安全攻防演练[J]. 保密工作, 2023(5): 56. https://doi.org/10.19407/j.cnki.cn11-2785/d.2023.05.014

[11] 杜金朋, 梁婷婷. 网络安全攻防技术在实际业务系统中的应用[J]. 网络安全和信息化, 2024(2): 117-119.

[12] 张耕源. 论网络空间安全与攻防技术[J]. 信息系统工程, 2023(12): 137-140.