Computer Science and Application 计算机科学与应用, 2022, 12(3), 516-526
Published Online March 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.123052

Hans汉斯

高校网络攻击溯源体系建设研究

梁锺烨，马　绚，朱尚明

华东政法大学信息化办公室，上海

收稿日期：2022年2月8日；录用日期：2022年3月3日；发布日期：2022年3月11日

摘　要

目前的攻击溯源研究在应对APT等使用跳板及公共网络服务的网络攻击时，追踪溯源能力有限。为高效准确追踪针对高校的网络攻击源头、溯源攻击者的攻击过程，依据高校实际所处网络拓扑环境并结合当下常见的网络攻击方式，对公网用户、VPN用户、校内有线用户、校园无线用户四种网络访问情形下的网络追踪溯源体系建设进行了探讨和研究，提出了可行的溯源解决方案。网络管理者可依此方案追踪到攻击数据包的来源并定位攻击者，继而针对溯源结果采取网络安全应急措施，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险，优化网络防护方案。实际测试结果表明，在符合溯源的前提条件下，均可准确溯源到攻击者。针对校内有线网络用户，由于缺乏认证功能，还存在一些技术和管理上的限制，后续还需进一步的调整和优化。

关键词

网络溯源，IP溯源，网络流量识别

Research on Traceability System Construction of Network Attacks at Universities

Zhongye Liang, Xuan Ma, Shangming Zhu

Informatization Office of East China University of Politics and Law, Shanghai

Received: Feb. 8th, 2022; accepted: Mar. 3rd, 2022; published: Mar. 11th, 2022

Abstract

The current research on attack traceability has limited ability to track and trace the source when dealing with APT and other network attacks using springboards and public network services.

文章引用: 梁锺烨, 马绚, 朱尚明. 高校网络攻击溯源体系建设研究[J]. 计算机科学与应用, 2022, 12(3): 516-526.
DOI: 10.12677/csa.2022.123052

Based on the common network attacks and the actual network topology of colleges and universities, construction of the network traceability system under four network access scenarios: network users, VPN users, campus wired users, and campus wireless users is discussed and studied. Network administrators can trace the source of attack packets and locate attacks according to this scheme. Then, emergency measures can be taken to deal with the security risks such as system vulnerabilities, computer viruses, network attacks, network intrusion, and the network protection scheme can be optimized. Shown by the actual test results, attackers can be accurately traced to the source under the preconditions of traceability. For campus wired network users, there are still some technical and management restrictions due to the lack of authentication function, which need to be further adjusted and optimized in the future.

Keywords

Network Traceability, IP Traceability, Network Traffic Identification

1. 引言

随着高校信息化建设的不断发展，校园业务系统建设的不断完善，高校信息安全已经成为不可忽视的问题，网络攻击者可能会利用系统漏洞向目标主机发送特定的攻击数据包或执行恶意代码等攻击行为，文献[1]分析了部分场景下校园网安全威胁[1]。由于网络攻击行为，不仅消耗网络带宽、占用系统资源，而且影响用户正常访问互联网资源造成业务中断或者造成高校业务中断等不良影响，此外，也会增加互联链路的结算成本。当信息系统遭受网络攻击后，须立时做好安全防护并及时追溯攻击源头，若能追踪到攻击数据包的来源并定位攻击者，就可以执行如过滤攻击数据包、流量封堵等应急措施，同时也可以根据溯源结果，对攻击者进行溯源并采取相应法律手段[2]。因此，高校构建网络溯源体系势在必行。

网络攻击追踪溯源需要利用各种手段追踪网络攻击的发起者，并结合相关技术定位攻击源和攻击路径，实现网络取证能力，网络溯源在网络安全领域具有非常重要的价值。

2. 网络攻击溯源流程

网络追踪溯源本质是追踪查询网络攻击的源头，通过分析不同节点的流量及状态，追查定位攻击者，利用技术手段重构并定位攻击者及攻击路径。基于追溯结果，安全负责人可以在调整优化安全部署策略，迅速减小网络攻击的危害程度，缓解攻击所带来的破坏面，同时也可作为证据提交相关机构对攻击者进行法律制裁[2]。在溯源过程中，若能获取到被攻击网络所处拓扑环境，对网络溯源追踪将起到决定性作用。由于网络所归属机构的规章制度，网络拓扑结构无法直接对外展示，因而追踪者在有些情况下无法直接获取被攻击环境的网络拓扑结构。同时，为防止追踪，部分攻击者会采用如匿名、跳板、代理、僵尸网络、匿名网络、虚拟 IP [3]等技术伪造隐藏自己的 IP，在这种情况下，网络拓扑将更难描绘，溯源问题也将变得复杂。

2.1. 网络攻击追踪溯源技术

文献[3] [4] [5] [6] [7]介绍了几种常见的网络攻击场景下的网络攻击分析工具及分析技术。通常，网络攻击溯源技术可以分为基于日志存储查询的追踪溯源技术、基于路由器输入调试的追踪溯源技术、基

于数据包标记的追踪溯源技术、基于单独发送溯源信息的追踪溯源技术、基于 SDN 的日志追踪溯源技术、基于 SDN 的路由器输入调试追踪溯源技术、基于威胁情报的追踪溯源技术、混合追踪溯源技术等[3] [4]。通常，我们可以通过日志分析、存储查询、数据包标记等方式获取有效的电子证据，通过对网络中的数据流进行分析，恢复出攻击路径。文献[5]对静态痕迹、提取技术、动态痕迹提取技术和 Volatility 取证[5]相关实用技术进行了研究；文献[6]分别对虚假 IP 追踪、Botnet 追踪、匿名网络追踪、跳板追踪、局域网追踪[6]的优劣进行了总结；文献[7]对计算机网络追踪溯源技术的应用进行研究和总结[7]。

2.2. 溯源的前提条件

根据高校现有网络架构和安全设备部署情况，网络攻击溯源需要的前提条件如下：

前提 1. 所有的业务服务器本地时间必须准确，可以通过 NTP 进行时间同步。提供相对准确的时间点或者时间范围，便于溯源时在海量日志中进行检索，快速溯源。

前提 2. 如果校内有线网络用户使用 DHCP 获取地址，可以追溯到 MAC 地址，如果此 MAC 地址对应的设备在线，可以查询出 MAC 地址对应的接入交换机的端口号，从而找出对应的房间号；如果此 IP 地址对应的设备不在线，则只能溯源到设备 MAC 地址，但无法继续向下追踪；如果校内有线网络用户使用静态配置地址，设备在线时可以通过设备对应的交换机端口找到对应的房间号，设备如果不在线，则只能追溯到 IP 地址。

2.3. 溯源流程

高校出口网络的典型组网结构一般由核心交换机、链路负载均衡设备、流量控制系统、防火墙、VPN 设备、防病毒网关、IPS、WAF、日志审计、数据库审计、网页防篡改、堡垒机、DHCP 服务器等几部分构成。根据对高校网络组网结构和访问用户的分析梳理，设计网络溯源流程如图 1 所示，具体描述如下。

1) 发现网络安全攻击或者事件，上报网络安全主管部门，创建溯源任务。

2) 确定受影响的服务器的 IP 地址和相应的服务类型。

3) 如果受影响的业务服务器具备日志记录功能，业务管理负责人登录业务服务器，查询业务服务器上的日志，根据事件发生的时间点或者时间区域对访问日志进行检索，查出相应的攻击源 IP 便于后续的工作。

4) 如果受影响的业务服务器不具备日志记录功能，根据事件发生的时间点进行判断：

① 如果是当天发生的事件，由网络管理员结合事件时间点在数据中心防火墙上进行日志检索，查出相应的攻击源 IP；如果受影响的业务服务器是 Web 应用服务器而且在 WAF 防火墙的保护策略中，由 WAF 管理员结合事件时间点在 WAF 防火墙上进行日志检索，查出相应的攻击源 IP 便于后续的工作。

② 如果非当天发生事件，由网络管理员结合事件时间点在日志审计设备上进行日志检索，查出相应的攻击源 IP。

5) 根据步骤(3)或步骤(4)，定位出攻击源 IP，对源 IP 进行分类处置：

① 如果源 IP 是公网 IP，由网络管理员结合事件时间点在日志审计系统上进行日志检索，查出相应的攻击源 IP，只能追溯到源 IP。

② 如果源 IP 属于 VPN 用户 IP，由 VPN 管理员结合事件时间点在 VPN 设备上进行日志检索，查出对应的 VPN 账号。

③ 如果源 IP 属于校园网有线网络用户，由 DNS 管理员、网络管理员配合根据事件发生时间点在 DHCP 设备上进行日志检索，查出对应的 MAC 地址。如果此 MAC 地址在线，可以根据 MAC 在交换机上查询，追溯到房间号和端口号。

④ 如果源 IP 属于校园网无线网路用户，由网络管理员根据事件发生时间点在上网认证设备上进行日志检索，查出对应的无线网络上网账号。

本文根据高校出口网络的典型组网结构及用户来源，模拟出 4 种场景下用户网络溯源方案。

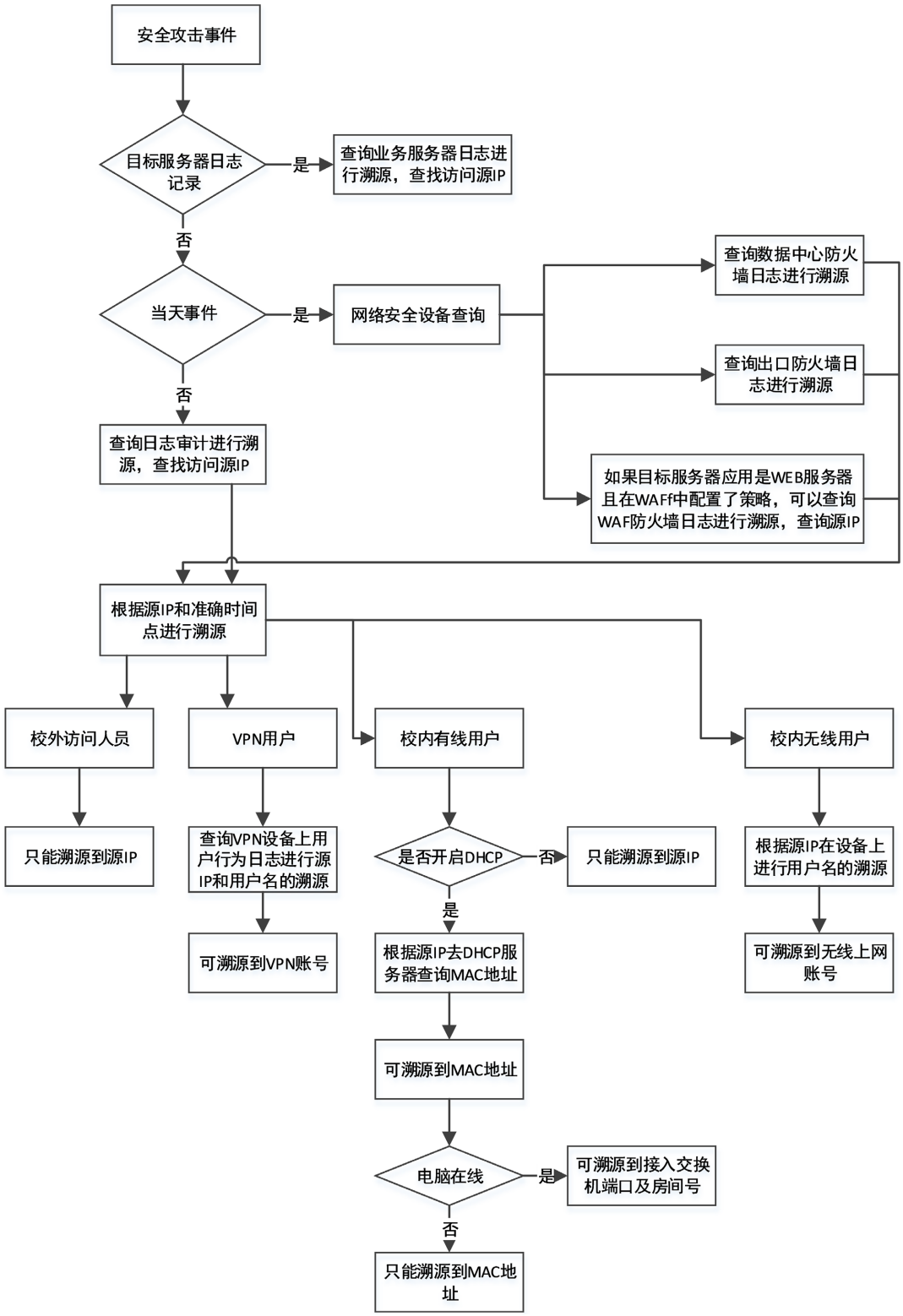


Figure 1. Network traceability flowchart
图 1. 网络溯源流程图

3. 网络溯源验证方案

根据对访问用户来源的分类，可以简单分为公网用户、VPN 用户、校内有线用户和校内无线用户。四针对校内 WEB 应用访问，根据不同的用户类型进行网络溯源验证方案如下。

1) 公网用户网络溯源方案

① 选取两个移动终端，关闭 WIFI，访问 http://www.ip138.com，获取当前的公网 IP 地址及访问时间点；

② 打开手机浏览器访问 https://*.*.edu.cn/，按图 1 网络溯源流程进行溯源，如果能溯源出源公网 IP，则溯源成功。

2) VPN 用户网络溯源方案

① 选取两个手机终端，关闭 WIFI，打开 VPN 软件并用帐号登录；获取当前的 IP 地址及访问时间点；

② 认证成功后，打开手机浏览器访问 https://*.*.edu.cn/；

③ 按图 1 网络溯源流程进行溯源，如果能溯源出 VPN 帐号，则溯源成功。

3) 校内有线网络用户溯源方案

① 选取两台电脑，连接办公室的信息面板，打开浏览器访问 https://*.*.edu.cn；

② 按图 1 网络溯源流程进行溯源，如果能溯源出 MAC 地址和对应的房间号，则溯源成功。

4) 校内无线网络用户溯源方案

① 选取两个笔记本电脑，连接校园网 WIFI，打开浏览器访问 https://*.*.edu.cn；

② 按图 1 网络溯源流程进行溯源，如果能溯源出无线用户的上网帐号，则溯源成功。

4. 网络攻击溯源验证

以华东政法大学某校内 Web 应用为示例，我们对公网用户、VPN 用户、校内有线用户和校内无线用户的溯源方案分别进行了验证。

4.1. 公网用户网络溯源验证

执行章节 2 中描述的公网用户网络溯源方案，详细记录结果如下：

① 将测试手机的无线网络关闭，打开 4G，获取其公网 IP 地址 114.87.190.2 (由运营商分配)，并记录其访问的时间点，如图 2、图 3 所示。

Figure 2. IP address query
图 2. IP 地址查询

Figure 3. Time of visit
图 3. 访问的时间点

② 打开浏览器访问 https://*.*.edu.cn/，并进行相应数据访问，如图 4 所示。

③ 按图 1 网络溯源流程进行溯源，在日志审计设备上根据时间点和相应的设备进行日志检索，如图 4、图 5 所示，即可追溯到源 IP 为 114.87.190.2。

Figure 4. Log audit device retrieval results
图 4. 日志审计设备检索

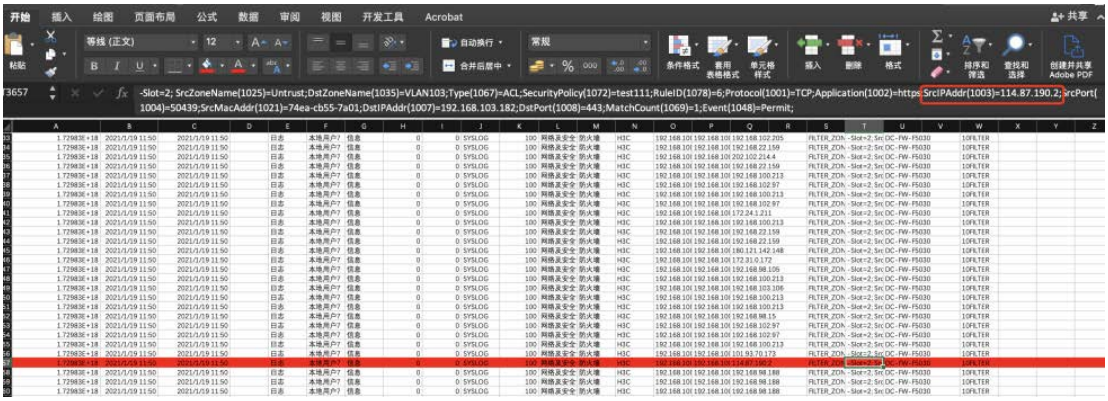


Figure 5. Log audit device retrieval details
图 5. 日志审计设备检索详情

4.2. VPN 用户网络溯源验证

执行章节 2 中描述的 VPN 用户网络溯源方案，详细记录结果如下：

① 测试终端使用 VPN 测试账号登录，用户获取 VPN 分配的私网地址为 172.31.0.44，并记录系统时间为 2021 年 1 月 27 日 11:35:10。

② 访问站点*.*.edu.cn，在日志审计设备上根据时间点和相应的设备信息进行日志检索。对日志进行分析，可以追溯到 VPN 账号和对应的 VPN 设备分配的私网 IP 地址 172.31.0.44，如图 6 所示。

Figure 6. Log audit device retrieval results
图 6. 日志审计设备检索

③ 通过溯源的私网 IP 地址 172.31.0.44 和 VPN 用户的访问记录可以成功溯源到 VPN 账号(和①一致)，用户溯源验证完成，如图 7 和图 8 所示。

4.3. 校内有线网络用户网络溯源验证

执行章节 2 中描述的校内有线网络用户网络溯源方案，记录结果如下：

① 测试电脑连接校园有线网络，通过 DHCP 服务器分配地址为 192.168.13.106，并记录系统时间为 2021 年 1 月 26 日 12:30:53。

② 通过校园网有线网络访问站点为*.*.edu.cn，在日志审计设备上根据时间点和相应的设备信息进行日志检索。

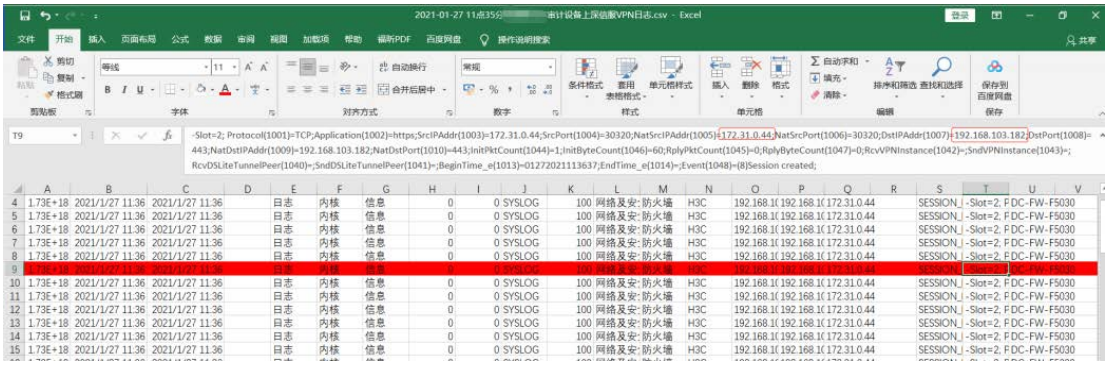


Figure 7. Log audit device retrieval details
图 7. 日志审计设备检索详情

Figure 8. Traceability account
图 8. VPN 用户的访问记录溯源账户

③ 对导出的日志进行分析，追溯源 IP 为 192.168.13.106，此 IP 地址属于有线网络业务网段地址，根据 DCHP 服务器上的日志进行查询，查出 192.168.13.106 对应的 MAC 地址为 98:fa:9b:f9:56:29，如图 9~11 所示。

Figure 9. Log audit device retrieval results
图 9. 日志审计设备检索

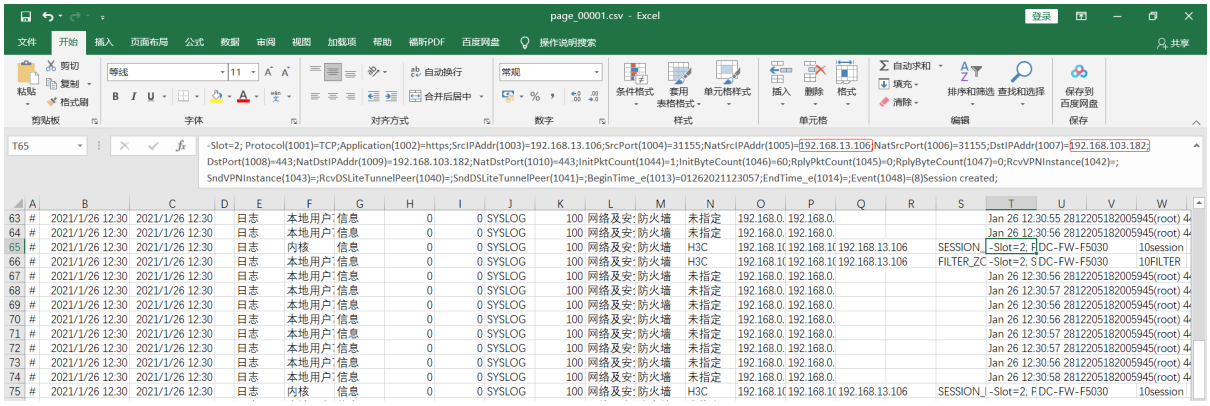
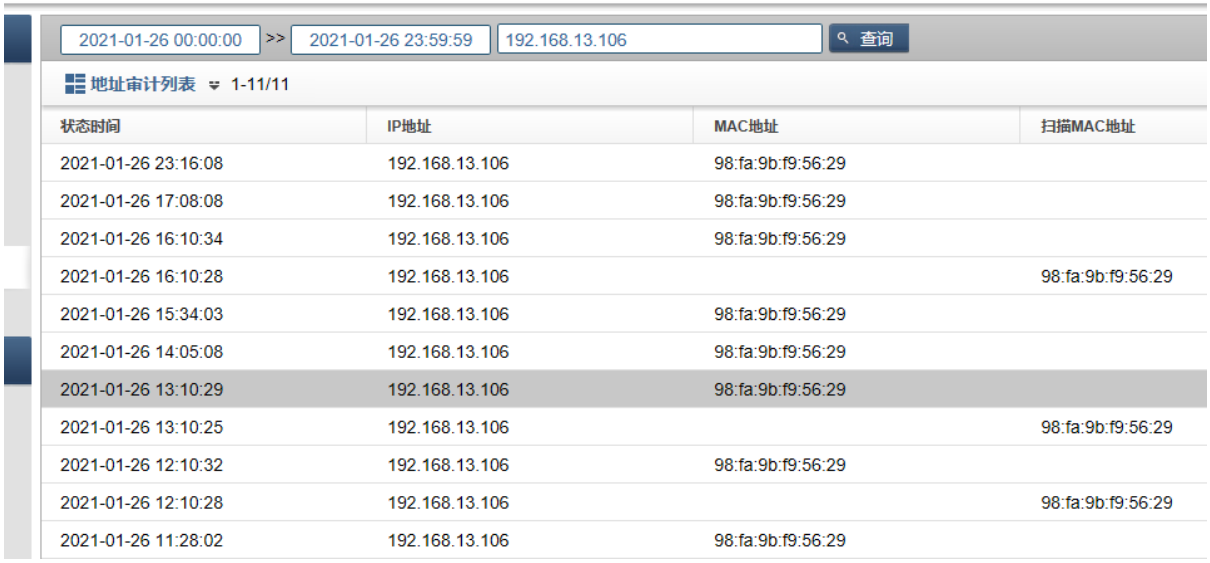


Figure 10. Log audit device retrieval details
图 10. 日志审计设备检索详情



状态时间	IP地址	MAC地址	扫描MAC地址
2021-01-26 23:16:08	192.168.13.106	98:fa:9b:f9:56:29	
2021-01-26 17:08:08	192.168.13.106	98:fa:9b:f9:56:29	
2021-01-26 16:10:34	192.168.13.106	98:fa:9b:f9:56:29	
2021-01-26 16:10:28	192.168.13.106		98:fa:9b:f9:56:29
2021-01-26 15:34:03	192.168.13.106	98:fa:9b:f9:56:29	
2021-01-26 14:05:08	192.168.13.106	98:fa:9b:f9:56:29	
2021-01-26 13:10:29	192.168.13.106	98:fa:9b:f9:56:29	
2021-01-26 13:10:25	192.168.13.106		98:fa:9b:f9:56:29
2021-01-26 12:10:32	192.168.13.106	98:fa:9b:f9:56:29	
2021-01-26 12:10:28	192.168.13.106		98:fa:9b:f9:56:29
2021-01-26 11:28:02	192.168.13.106	98:fa:9b:f9:56:29	

Figure 11. Reverse query MAC address
图 11. 反向查询 MAC 地址

④ 根据源 MAC (98:fa:9b:f9:56:29)地址在交换机上进行查询，定位用户在某校区某楼 A313 的接入交换 GE1/0/10 端口。根据此信息定位出房间号，结果显示匹配 4.2.3 测试中 DHCP 分配的 IP 地址所在位置，如图 12 所示。在查询的过程中，有两种情况：如果此 MAC 地址对应的设备在线，可以查询出 MAC 地址对应的接入交换机的端口号，从而找出对应的房间号；如果此 MAC 地址对应的设备不在线，只能溯源到 MAC 地址。

```
  <cr>
<SJ.MZL.A313-ASL2-IP13.251>dis mac-address 98fa-9bf9-5629
MAC ADDR        VLAN ID  STATE          PORT INDEX                AGING TIME(s)
98fa-9bf9-5629  1813     LEARNED        GigabitEthernet1/0/10     AGING

  ---  1 MAC address(es) found  ---
<SJ.MZL.A313-ASL2-IP13.251>dis arp 192.168.13.106
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
192.168.13.106   98fa-9bf9-5629  1813     GE1/0/10              20    D
<SJ.MZL.A313-ASL2-IP13.251>
```

Figure 12. Query access location
图 12. 根据源 MAC 地址查询接入位置

4.4. 校内无线网络用户网络溯源验证

执行章节 2 中描述的校内无线网络用户网络溯源方案，记录结果如下：

① 测试手机连接校园无线网络，通过 DHCP 获取无线网络私网 IP 地址为 172.19.69.89，如图 13 所示。

② 访问站点*.*.edu.cn，并在日志审计设备上根据时间点和相应的设备信息进行日志检索。

③ 通过对检索出来的日志进行分析可以溯源到源 IP 地址为 172.19.69.89，为无线网络业务段地址，如图 14 和图 15 所示。

⑥ 按《网络溯源详细方案》进行溯源，在认证设备搜索无线客户端 IP 地址(172.19.69.89)的认证记录，溯源到上网用户账号为 wgf，如图 16 所示，用户溯源验证完成。

Figure 13. Wireless network IP address
图 13. 无线网络 IP 地址

Figure 14. Log audit device retrieval results
图 14. 日志审计设备检索

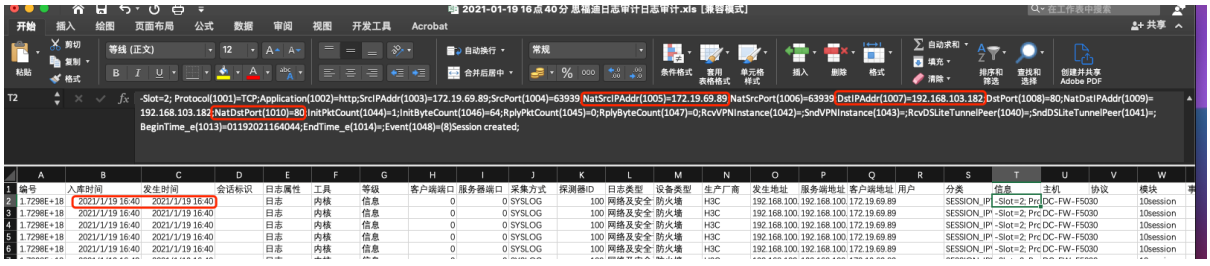


Figure 15. Log audit device retrieval details
图 15. 日志审计设备检索详情

Figure 16. Traceable Internet user account
图 16. 通过 IP 溯源上网用户账号

验证结果表明，四种方案均溯源成功，可普遍适用于校园网络犯罪的侦破，该方案对于解决网络攻击溯源问题显示出了一定的意义。在此基础上，可结合 IP 段分配的楼宇、交换机 ARP 表和桥接表，来更进一步定位攻击者所在的物理位置。

5. 结语

网络攻击溯源在高校网络安全防御体系中起到至关重要的作用，对于日常网络及安全运维管理有着十分重要的支撑作用。针对常见网络攻击，本文提出了一种溯源方案以追踪通常情况下的攻击源，基于现有网络架构梳理出网络攻击溯源流程，并根据流程进行了验证。攻击溯源流程合理，实现了攻击溯源的功能。但是针对校内有线网络用户，由于没有实现认证功能，还存在一些技术和管理上的限制，后续还需进一步的调整和优化。

参考文献

[1] 沈昀. IPv6 校园网安全威胁分析和防护[J]. 数字通信世界, 2020, 181(1): 25-26.

[2] Khan, S., Gani, A., Wahab, A., *et al.* (2016) Network Forensics: Review, Taxonomy, and Open Challenges. *Journal of Network & Computer Applications*, **66**, 214-235. https://doi.org/10.1016/j.jnca.2016.03.005

[3] 刘雪花. 丁丽萍, 郑涛, 等. 面向网络取证的网络攻击追踪溯源技术分析[J]. 软件学报, 2021, 32(1): 38-41.

[4] Jiang, J., Wang, J., Kong, B., *et al*. (2018) On the Survey of Network Attack Source Traceback. *Journal of Cyber Security*, **3**, 111-131.

[5] 何尾风. 面向溯源取证的网络攻击工具痕迹分析技术与实现[D]: [硕士学位论文]. 北京: 北京邮电大学, 2018.

[6] 姜建国, 王继志, 孔斌, 等. 网络攻击源追踪技术研究综述[J]. 信息安全学报, 2018, 3(1): 111-131.

[7] 王江. 试论计算机网络追踪溯源技术[J]. 数字通信世界, 2019, 178(10): 61-61.