基于 KylinOS 操作系统的客户端安全防护架构研究

杨 鑫[1]
YANG Xin

摘 要 随着信息安全问题愈发凸显，Windows 操作系统服务支持已经无法完全适应日益严峻的信息安全形势和复杂多变的应用场景，国产操作系统通过自主创新逐步实现了技术突破，开始走向大众视野，遍布各行业各单位多样化办公和业务场景。但来自互联网和内网的各种安全威胁影响着国产操作系统的正常运行，因此需要通过客户端安全防护策略，提高国产操作系统运行安全性和稳定性。文章以国产操作系统 KylinOS 为例，针对其面临的安全问题提出了一种新的客户端安全防护模型，从网络层安全和系统层安全两个层面，为 KylinOS 客户端提供了全方位立体安全防护。通过每个层面具体安全策略的原理分析与部署实施，保障了基础设施安全和数据信息传输安全。

关键词 KylinOS；客户端安全防护；网络层安全；系统层安全；全方位立体安全防护

doi：10.3969/j.issn.1672-9528.2025.12.034

0 引言

近年来，国产操作系统[1]在减少国外技术依赖、增强技术自主产权、确保用户信息安全、降低外部安全风险等方面发挥出了极其重要的作用。其中，具有代表性的银河麒麟[2]操作系统——KylinOS 是一款由国防科技大学研发，以 openKylin 等自主社区为依托的主流国产操作系统，以其良好的软硬件兼容性、便捷的软件升级与版本在线更新等功能广泛应用于企事业单位的业务系统、日常办公、教学科研等场景。

但是，复杂多变和不确定的信息安全环境使得 KylinOS 与 Windows 操作系统类似，同样会受到来自外部互联网以及内部局域网的各种安全威胁[3]，例如病毒、木马、恶意软件、APT 等攻击。为了确保国产操作系统客户端在日常使用中的可用性和稳定性，维护用户数据的安全性[4]，本文以 KylinOS V10 操作系统为例，提出了一种新的客户端安全防护架构模型，从网络层安全和系统层安全两个层面，研究了国产操作系统的安全防护策略设计与应用。

1 客户端安全防护模型整体架构

本文提出的 KylinOS 客户端安全防护模型整体架构包括网络层安全和系统层安全两部分，如图 1 所示。其中，网络层安全不特指 TCP/IP 模型中的网络层，泛指能够保障 KylinOS 操作系统客户端安全的相关措施，包括网络准入、接入层安全（包括防 DHCP 地址池私设和 IP 地址私设、防 ARP 攻击）和勒索病毒防护。其中，内网办公环境中普遍存在的 ARP 攻击、用户私设 IP 地址导致地址冲突、私设 DHCP 地址池导致无法正常上网等问题主要通过接入交换机中部署相应的安全策略来解决。网络准入规避了传统端口安全策略[5-6]需要手工绑定和维护的工作复杂性，通过 SDN 控制器中申请提交并审核通过后绑定的合法表项向接入交换机下发 OpenFlow 流表[7]，从而实现局域网内部不同网段之间互访以及正常访问互联网。勒索病毒的防护可以在交换机中部署高级 ACL 列表，并调用流策略来实现。

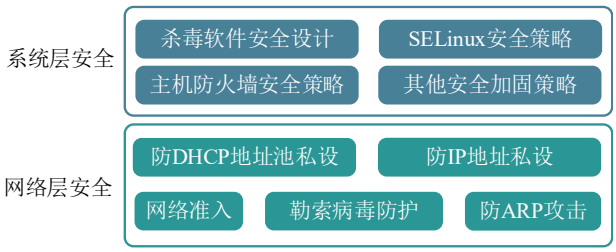

图 1 KylinOS 客户端安全防护架构图

系统层安全包括杀毒软件安全、主机防火墙安全、SELinux 安全策略[8]部署等。其中，杀毒软件采用网络部署方式，作为服务器的管理端为全网客户端提供病毒库实时更新、终端安全统一管理等服务，客户端能够对 KylinOS 操作系统中的相关安全威胁进行查杀处理并及时上报管理端，为病毒安全防护决策提供支撑。主机防火墙作为外部防火墙的补充，驻留在 KylinOS 操作系统中的安全防线，提供本地系统运行和文件处理安全防护。SELinux 作为内核模块嵌入到 KylinOS 操作系统中，能够作为安全补丁为主流 Linux 应用（例如 httpd、vsftpd 等）提供比传统 UNIX 权限更好的访问控制和更高的安全性。

1. 中共青海省委党校 青海西宁 810000

2 网络层安全防护设计与应用

2.1 网络准入

在扁平化的核心层与接入层二层网络结构中引入软件定义网络 SDN 体系架构[9]能够较为灵活地实现用户准入控制，减少网络运维复杂度和成本。SDN 体系结构由数据平面和控制平面组成，与传统数据平面、控制平面和管理平面集中在同一台网络设备中的模式不同，SDN 将控制平面与数据转发平面相分离，通过集中式控制器 Controller 对整个网络进行管理和编排，如图 2 所示。其中，位于控制层（即控制平面）的 SDN 控制器通过南向接口 OpenFlow 协议对转发层（即数据平面）的接入交换机进行管理和控制，二者通过 SDN 控制数据平面接口（control data plane interface, CDPI）进行通信。Controller 向接入交换机下发绑定用户 IP 地址、MAC 地址等信息的合法表项组成的 OpenFlow 流表（如图 3 所示）实现用户准入授权，而没有进行准入注册的用户则不会出现在 OpenFlow 流表中。

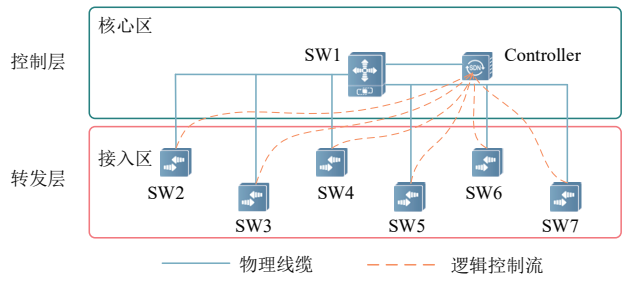

图 2 SDN 在网络中的部署架构

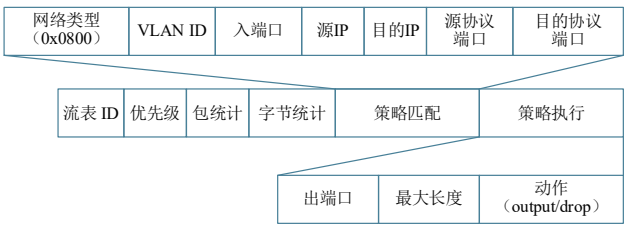

图 3 OpenFlow 流表结构图

Controller 能够基于建筑物的物理布局进行区域划分，提高终端可管理性，部分终端实现准入成功后的状态信息如表 1 所示。

表 1 终端准入成功状态信息表

名称	MAC	位置	IP	接入设备	接入时间	VID
PC1	C0:18:03:5C:8E:34	7F	192.168.11.10	JR-7F-1 192.168.99.1 Gi0/15	2025.03.26 18:19:57	11
PC2	8C:01:30:46:C1:A3	7F	192.168.11.20	JR-7F-2 192.168.99.2 Gi0/10	2025.05.06 09:11:04	11

2.2 防 DHCP 地址池私设

接入层中存在一种场景，当信息接入点的数量无法满足一间办公室的 KylinOS 客户端接入需求时，有时会部署一台具有多个 LAN 接口的无线路由器来解决。但是，同时带来的问题是无线路由器默认开启了 DHCP 功能，在 IP 地址采用动态分配的情况下，部分客户端错误获取了无线路由器地址池中的地址（例如 192.168.1.0/24 网段的地址），而非网络中合法 DHCP 服务器提供的地址，从而导致了这些客户端无法正常地访问网络。该问题发生的根本原因在于客户端是直接连接在无线路由器上的，对比跨网段或者跨设备的合法 DHCP 服务器而言，非法 DHCP Offer 报文会优先到达客户端，进而通过后续的 DHCP Request 报文和 DHCP ACK 报文使客户端获取到了非法 DHCP 服务器地址池中的地址，如图 4 所示。

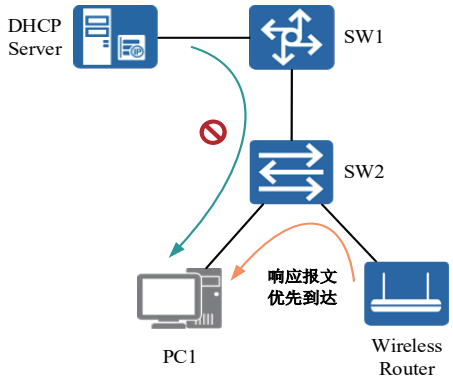

图 4 客户端获取非法 DHCP 服务器地址

为了防止 DHCP 地址池欺骗[10]，需要在接入交换机中部署 DHCP Snooping 功能，默认会将交换机的所有接口设置为 untrusted 模式。在该模式下，交换机不会转发所有接口上接收到的 DHCP 响应报文（包括 Offer 和 ACK 报文）。但是，由于合法 DHCP 服务器一般为核心交换机或者服务器区的专用服务器，因此可以将接入交换机上联至核心交换机的 trunk 接口设置为 trusted 模式，使得接入交换机只转发从 trunk 接口接收到的 DHCP 响应报文，从而规避了 DHCP 地址池欺骗的风险，如图 5 所示。

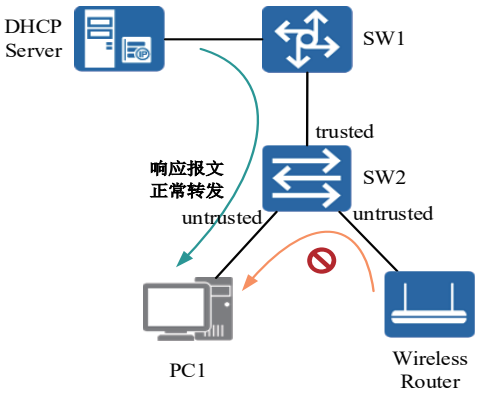

图 5 通过 DHCP Snooping 防止 DHCP 地址池私设

2.3 防 IP 地址私设

特定情形下，部分用户为了能够将自己 KylinOS 客户端动态获取的 IP 地址固定下来，会手工配置或者修改 IP 地址，这样有可能导致 IP 地址冲突或者 IP 地址参数配置错误 [11]，对网络的正常使用产生一定影响。通过在接入交换机连接客户端的接口上开启 IP 源抑制（IP source guard, IPSG）功能，使得 DHCP 服务器为客户端动态分配 IP 地址之后，在开启 DHCP Snooping 功能的交换机上同步生成动态 DHCP Snooping 绑定表（包括客户端获取的 IP 地址、MAC 地址、VLAN ID、接口 ID 等）。当交换机连接客户端的接口开启 IPSG 功能之后，DHCP Snooping 绑定表的信息会被放入 IPSG 绑定表中。当交换机收到需要转发的报文，并检查报文头部中的相关信息后，如果与 IPSG 绑定表项匹配，则转发报文，否则丢弃报文，如图 6 所示。因此，只有通过动态获取的 IP 地址才能够正常访问网络；如果 IP 地址是手工设置的，即使 IP 地址正确，也无法正常访问网络，因为 IPSG 绑定表项不存在，除非手工绑定该设备的合法表项。

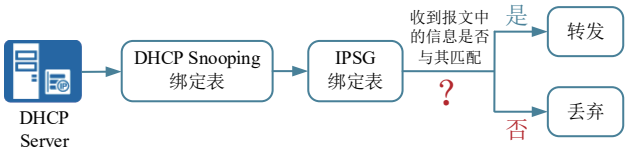

图 6 通过 IPSG 防止用户私设 IP 地址

2.4 防 ARP 攻击

数据通信过程有时是同网段的直接通信，有时是跨网段的间接通信。只有在源主机得到目的主机 MAC 地址或者网关 MAC 地址的前提下，数据帧才会封装完整正常转发。但是，在这个过程中如果有入侵者冒充网关设备或者目的主机，回复虚假的 MAC 地址给源主机，那么将会发生局域网中典型的 ARP 中间人攻击 [12]，如图 7 所示。

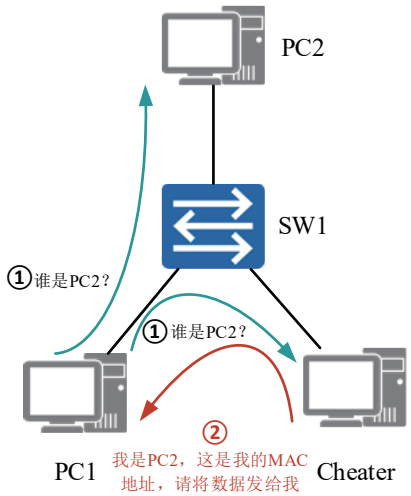

图 7 常见的 ARP 中间人攻击场景

ARP 攻击产生的结果轻者导致网络通信时断时续，重者可能导致发送的数据被入侵者获取。为了防御 ARP 中间人攻击，需要在接入交换机上部署动态 ARP 检测（dynamic ARP inspection, DAI）功能。动态 ARP 检测利用绑定表来防御中间人攻击，绑定表可以来源于静态手工配置或者从 DHCP Snooping 绑定表中获取。当开启动态 ARP 检测 DAI 功能的交换机收到 ARP 报文时，将检查此 ARP 报文对应的源 IP、源 MAC、VLAN ID 以及接口 ID 信息和绑定表中的信息是否匹配，如果信息匹配，说明发送该 ARP 报文的用户是合法用户，允许此用户的 ARP 报文通过，进而完成后续的数据封装和转发过程；否则就认定为是非法 ARP 攻击并丢弃该 ARP 报文，如图 8 所示。

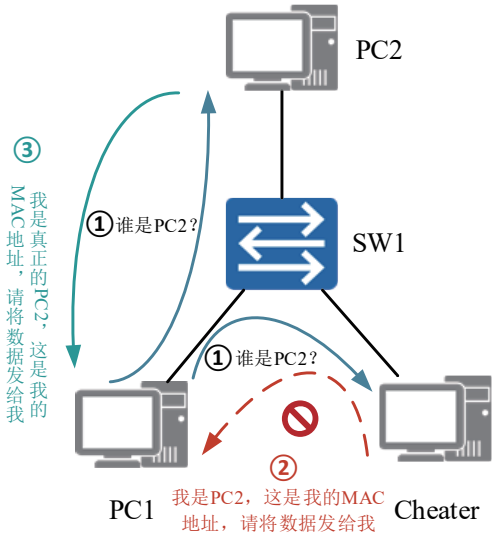

图 8 通过 DAI 防御 ARP 中间人攻击

2.5 端口隔离

在一些办公和科研场景中，为了确保安全性，不允许同部门用户之间互访，此时可以采用端口隔离 [13] 功能，实现同一 VLAN 端口之间的隔离，为用户提供一种更安全的组网方案。以华为接入交换机为例，默认情况下，开启端口隔离后，相同 VLAN 下的用户之间是无法互访的，但是用户可以正常地访问其他网段或者访问互联网（即默认执行二层隔离策略）。如果将三层访问也进行隔离，那么需要在系统视图下通过 port-isolate mode all 命令设置隔离模式为二层和三层均隔离。

2.6 勒索病毒防护

勒索病毒 [14-15] 是一种近年来伴随着比特币出现的特殊恶意软件，通过技术手段（如使用各种加密算法对文件进行加密）限制受害者对其系统以及数据进行访问。勒索病毒主要通过 Linux 操作系统中一些实现文件和打印共享以及系统远程调用的默认开放端口发起攻击，因此可以通过关闭这些端

口或者阻止发往这些高危端口的流量来确保系统和文件的安全性。勒索病毒在交换机中的防护主要通过高级访问控制列表匹配这些高危端口进行实现，详细访问控制规则举例如表 2 所示。

表 2 防勒索病毒访问控制规则

服务	协议	目标端口	匹配动作
RPCBind	TCP/UDP	111	允许
SMB	TCP	445/139	允许
NFSv3	TCP/UDP	111/ 设置固定端口	允许
NFSv4	TCP	2049	允许
CUPS/IPP	TCP	631	允许
XRDP	TCP	3389	允许

详细的勒索病毒防护策略实现如算法 1 所示，定义高级访问控制列表 G，根据需求添加目的高危端口所对应的访问控制规则，创建流分类器 High-Risk-Ports 匹配访问控制列表 G。创建流行为 Block，设置数据流匹配成功后执行的动作为 Deny 拒绝通过，创建流策略 Anti-Ransomware，联合调用流分类器 High-Risk-Ports 和流行为 Block，最后在业务 Vlanif 接口的出方向调用流策略 Anti-Ransomware。

算法 1 部署 Anti-Ransomware 策略

输入：高级 ACL G={rule1,rule2,…, rule$n$}

输出：用户 Vlanif 接口调用 Anti-Ransomware 策略

1: **procedure** ANTI-RANSOMWARE(G, High-Risk-Ports, Block, Anti-Ransomware)

2: 创建高级 ACL G

3: **for** i=1 to n do

4: G←rule[i]

5: **end for**

6: 创建流分类器 High-Risk-Ports

7: High-Risk-Portst←G

8: 创建流行为 Block

9: Define actiont←deny

10: 创建流策略 Anti-Ransomware

11: Anti-Ransomwarev←High-Risk-Ports Combine Block

12: 业务网段 Vlanif 接口出方向调用 Anti-Ransomware 策略

13: Vlanif n outbound←Anti-Ransomware

14: **end procedure**

对于 SSH、HTTP/HTTPS、FTP 等服务如果存在程序后门或者账号弱口令，也有可能引发勒索病毒攻击，但由于其较高的服务覆盖率不能将其直接禁止，可以采用更新服务软件或者框架、及时修复漏洞、配置复杂度较高的账户口令等方式进行预防。

随着人工智能的发展，目前已经出现成熟的解决方案能够通过深度学习模型针对网络中存在的勒索病毒等恶意软件进行实时检测和预测，并针对性进行干预和处理，例如 MalwareBazaar（样本数据库）+YARA（规则库）+ML（机器学习）。

3 系统层安全防护设计与应用

3.1 杀毒软件安全机制

为防范病毒、木马肆虐，部署网络版杀毒软件 [16] 能够通过快速定位查毒、病毒集中分析与监控、启发式扫描与防护等技术手段，快速查杀已知的数万种病毒（包括引导病毒、文件病毒、蠕虫、邮件病毒等）。网络版杀毒软件能够完美支持本文探讨的 KylinOS 操作系统，杀毒软件部署架构如图 10 所示。其中，为确保管理端（即服务器端）安全性，采用三权分立模式（包括系统管理员、安全管理员和审计管理员）对管理端进行运维。管理端可以向授权客户端下发配置、升级客户端病毒库、发起全网病毒查杀、启动计划任务等，方便网络运维人员对木马、病毒等进行威胁溯源、日志审计等管理操作，而非授权用户客户端病毒库则不允许更新。大部分安全管理操作对客户端来讲基本上是透明的，一方面减少了客户端日常安全管理的工作量，另一方面提高了网络运维人员在终端安全管理方面的效率。

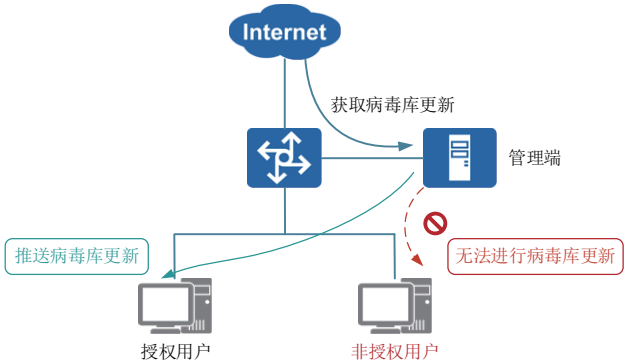

图 10 网络版杀毒软件部署架构

3.2 主机防火墙安全策略

局域网边界的硬件防火墙通过细粒度的安全访问策略过滤了大部分来自互联网外部的安全威胁，而客户端系统层防火墙（也称为主机防火墙）作为硬件防火墙的补充，能够在一定程度上进一步防止 KylinOS 客户端遭受来自其他客户端和外部用户的非授权访问。

主机防火墙不同于网络边界硬件防火墙，其上部署如下的安全访问策略确保当前主机的安全性。首先，主机防火墙默认处于启用状态，拒绝来自外部针对当前主机的所有流量；其次，针对外部用户访问该主机上运行的服务进程，启用 Inbound 方向允许访问的安全策略；再者，针对该主机需要访问的外部服务，启用 Outbound 方向允许访问的安全策略。

KylinOS 操作系统默认没有安装 firewalld 服务，因此需要首先使用命令 sudo apt install firewalld 安装该服务。firewalld 防火墙默认情况下处于开启状态，为了确保客户端操作系统的安全性，通常不建议将其进行关闭。以日常办公中比较常见的文件共享场景为例，在完成 vsftpd 服务器搭建之后，需要在防火墙中将 FTP 服务对外进行开放，因此需要在防火墙中添加如下永久安全策略，并重新加载安全策略使其生效。

```
user@user-TR4252:~/Desktop# sudo firewall-cmd --permanent --add-service=ftp
user@user-TR4252:~/Desktop# sudo firewall-cmd --reload
```

3.3 SELinux 安全机制

SELinux 是一种基于域 - 类型模型的强制访问控制安全子系统，由美国国家安全局在 Linux 开源社区帮助下开发并作为内核模块嵌入到 Linux 系统中，其目的在于让运行在当前主机上的各个服务进程受到制约，使其仅能够获得服务正常运行所需的系统资源，为各行业各部门内部使用这些 Linux 服务应用时提供更高的安全性。

在日常科研、教学和办公过程中，会经常使用 ftp 服务实现实时文件传输，在 KylinOS 操作系统中为进一步提高系统安全性，可以在 SELinux 安全子系统中放行如下 vsftpd 服务对应的安全规则。

```
user@user-TR4252:~/Desktop# sudo setenforce 0
user@user-TR4252:~/Desktop# sudo setsebool -P ftpd_full_access=on
user@user-TR4252:~/Desktop# sudo setenforce 1
```

3.4 其他安全加固措施

除此之外，还需要完成一些系统层面的设置，提高系统管理安全性。例如，为 root 用户设置复杂口令并禁止 root 用户远程 SSH 登录 KylinOS 操作系统，只分配普通用户非 root 账号和复杂登录口令满足其日常办公等需求。另外，网络管理人员还需及时关注 KylinOS 操作系统漏洞信息，如果存在风险及时根据官方建议进行漏洞修复。

4 总结与展望

本文围绕 KylinOS 操作系统在实际使用过程中可能面临的安全问题，从网络层安全和系统层安全两个层面，构筑基于该操作系统的客户端整体安全防护架构，研究了每一种安全防护机制对应的具体防护策略实施方案。虽然目前支持 KylinOS 操作系统的软件生态和适配性还在进一步完善，但是客户端安全问题刻不容缓，应当引起各行业各单位在使用过程中的高度重视。该基于 KylinOS 操作系统的客户端安全架构适用范围广，能够普遍应用于教育、政府、医疗等各个行业的网络环境当中，为国产客户端提供稳定安全的系统运行环境，大幅消除国产客户端可能存在的安全风险隐患。

参考文献：

[1] 张京林 . 国产操作系统产业化现状分析和发展探讨 [J]. 科技与创新 ,2016(20):27-29.

[2] 李震宁 . 银河麒麟操作系统开源生态实践 [J]. 软件和集成电路 ,2021(6):40-41.

[3] 庞新煜 . 局域网下的计算机网络安全技术应用分析 [J]. 电子元器件与信息技术 ,2021,5(1):22-23.

[4] 孙海涛 . 网络传输中数据安全及加密技术 [J]. 电子世界 ,2022(1):180-181.

[5] 胡玲芳 , 赵秀丽 . 浅谈交换机端口安全技术 [J]. 网络安全技术与应用 ,2021(7):18-19.

[6] 庞国莉 , 王小英 . 端口安全在园区网络安全中的应用设计 [J]. 科学技术创新 ,2021(35):88-90.

[7] 陈银 , 陈柯 , 任森 . 基于 SDN 技术的云化数据中心解决方案 [J]. 通信技术 ,2019,52(1):152-156.

[8] 曹妍 , 李燕萍 , 黄兰华 , 等 .SELinux 的安全机制 [J]. 轻工科技 ,2015,31(6):66-67.

[9] 张朝昆 , 崔勇 , 唐骞骞 , 等 . 软件定义网络 (SDN) 研究进展 [J]. 软件学报 ,2015,26(1):62-81.

[10] 谢杰民 . 关于 DHCP 服务攻击的安全防护策略 [J]. 信息与电脑 (理论版),2018(18):199-200.

[11] 欧贤 , 胡燕 .IP 地址欺骗与防范技术研究 [J]. 数字技术与应用 ,2015(11):203.

[12] 蒋继平 . 图书馆局域网 ARP 欺骗攻击分析与解决方案研究 [J]. 江西图书馆学刊 ,2009,39(4):106-107.

[13] 薛剑锋 .DCN 交换机端口隔离功能的应用测试 [J]. 网络安全和信息化 ,2021(3):81-82.

[14] 万子龙 . 勒索病毒攻击原理及检测方法研究 [J]. 江西通信科技 ,2019(3):42-44.

[15] 胡国强 . 从勒索病毒看网络信息安全的隐患与对策 [J]. 网络空间安全 ,2018,9(1):5-7.

[16] 王洪娟 . 基于七级防护模型的高校图书馆网络安全防护措施 [J]. 江西图书馆学刊 ,2008(1):111-113.

【作者简介】

杨鑫（1989—），男，甘肃民乐人，硕士研究生，中共青海省委党校信息技术部网络工程师，研究方向：虚拟现实、深度学习、计算机网络安全、操作系统，email:loongxin@yeah.net。

（收稿日期：2025-06-30　修回日期：2025-12-05）