校园网基础服务器的检测分析

丁伟[1,2,3]，贾硕[1,2,3]，洪沿[1,2,3]，夏震[1,2,3]

（1.东南大学网络空间安全学院，江苏 南京 211189；2. 东南大学江苏省计算机网络重点实验室，江苏 南京 211189；
3. 东南大学教育部计算机网络和信息集成重点实验室，江苏 南京 211189）

摘 要：论文首先就现有的网络空间搜索引擎存在的误判及漏判进行了讨论。在此基础上，基于一个自行开发的通用基础服务器检测平台 SRDS 建立了 CERNET 基础服务器库，可以准确定位 CERNET 中的 WEB、DNS、MAIL 和 NTP 四种基础服务器。通过对检测过程获取的信息进行分析，给出了十种异常检测条件。最后展示的校园网实测案例表明了相关工作的有效性和实用性。

关键词：服务器角色检测，网络空间搜索引擎，异常分析

中图分类号：TP393

Detection and Analysis of Campus Network Common Server Database

DING Wei[1,2,3], JIA Shuo[1,2,3], HONG Yan[1,2,3], XIA Zhen[1,2,3]

1. School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China

2. Jiangsu Provincial Key Laboratory of Computer Network Technology, Southeast University, Nanjing 211189, China

3. Key Laboratory of Computer Network and Information Integration of Ministry of Education, Southeast University, Nanjing 211189, China

Abstract: The paper first discusses the misjudgment and missed judgment of the existing cyberspace search engine. On this basis, based on a self-developed general-purpose basic server detection platform SRDS, the CERNET common server database is established, which can accurately detect the four common servers of WEB, DNS, MAIL and NTP in CERNET. Ten kinds of abnormal detection conditions are given by analyzing the information obtained during the detection process. The last demonstrated case of the campus network shows the effectiveness and practicality of the relevant work.

Key words: Server Role Detection; Cyberspace Search Engine; Anomaly Analysis

1. 引言

目前互联网中的主要服务均采用客户机/服务器（Client/Server，C/S）交互模式实现，即服务器在特定端口等待客户机的服务请求，客户机通过向服务器的特定端口发出服务请求后获取对应的服务，例如 Web、DNS、Email、NTP、FTP、Telnet 等均采用这种交互模式。在这种模式下，由于服务器需要并发支持多台客户机同时访问且 24 小时在线，所以对主机的资源要求较高。一般服务器均会安装常规操作系统，例如 Linux、Windows 和 Unix 等，并在上线之前完成服务软件的安装和配置。然而，由于管理者的不当操作或配置，可能导致服务器的行为与管理者的规划之间存在偏差，这些偏差往往并不非常容易发现，但会成为攻击者关注和利用的重点，导致网络安全事件的发生。比如，2014 年 4 月 7 日，广泛使用于多种网络服务中的开源安全组件 OpenSSL 就被爆出“心脏出血（OpenSSL Heartbleed）”漏洞[1]，全球数百万服务器受到影响，攻击者利用该漏洞窃取了大量用户密码和私钥。

当前主流的面向服务器的操作系统（如 CentOS、Windows Server 等）中通常都集成有一些常用服务器程序，并在初始安装时会默认开启这些服务。这些集成进操作系统的服务程序会存在漏洞，如微软 WEB 服务器中的 IIS 的文件解析漏洞、Apache Tomcat 的物理路径泄露漏洞等。一般的 DNS 服务器均会支持 DNSSEC 查询、支持 EDNS0，NTP 服务器会支持 MONLIST 命令，支持递归查询的 DNS 服务器以及支持 MONLIST 命令的 NTP 服务器容易被攻击者利用作为反射放大器来实现 DDoS 反射攻击。用户的服务器在安装和配置方面稍有不慎，在正式进入互联网后，很快就能被发现并利用，有时会造成很严重的后果。

在一般情况下，互联网上正常运行的服务在交互过程中，除了 IP 地址和端口信息外，还会留下一些与操作系统和服务器软件相关的指纹信息。因此，目前互联网上有一种专门的

提供这些服务器信息的搜索引擎服务，称为“网络空间搜索引擎”[1]。美国的 Shodan 和国内的 ZoomEye 是“互联网空间搜索引擎”中比较著名的两个，前者是全球第一个提供服务器角色服务的平台，后者则建立了国内第一个网络空间搜索引擎，下一节将对这两个平台进行简单的介绍。

本论文的研究工作基于基础服务器的检测展开，通过检测过程获取的信息和服务器配置的合理性等角度，尝试给出服务器检测和异常分析的规则，并将其应用到校园网实际环境中。

2. 相关背景

2.1. 网络空间搜索引擎

Shodan[3]是由美国著名安全专家 John Matherly 于 2009 年创建的全球第一个提供全网主机设备服务器角色信息搜索的平台。Shodan 除了针对各种基础服务器，还针对网络摄像头、打印机、车牌扫描仪等各种接入互联网且具有服务器角色的网络基础设备做扫描抓取并解析各个设备的 Banner[4]信息并提供给用户查询。

ZoomEye[5]是中国第一个服务器角色服务平台，由国内知名网络安全公司知道创宇开发 2013 年上线，目前已更新到第五个版本。ZoomEye 除了设备服务的扫描以外，更加关注 Web 服务器软件信息，增加了对 Web 服务器的指纹扫描，因此在 Web 服务识别方面提供的信息的详细和精准程度远高于 Shodan。

Shodan 和 ZoomEye 是两个比较有代表性的服务器角色查询平台，而且经过长时间的运营已经十分成熟，对安全工作的研究也提供了大量数据。但这些平台普遍存在着维护周期偏长、数据准确度不足、安全相关信息缺失和资源限制等缺陷。对于网络管理者来说，他们需要更加及时、准确、详细的数据，在这一点上无论是 Shodan 还是 ZoomEye，均不能令人满意。

2.2. 通用搜索引擎的局限性

局限性主要体现在漏判甚至误判的情况时有发生。为了验证 Shodan 和 ZoomEye 的误判和漏判情况。我们于 2018 年 4 月 28 日进行了一次验证实验。实验从接入 CERNET 南京节点网络的地址中选取了 100 个提供 DNS 服务的开放服务器，还有 100 个不提供 DNS 服务的主机。在不提供 DNS 服务的 100 个主机中，有 10 个曾经提供过 DNS 服务。对这 200 个地址现在实验当天进行了验证，然后分别从 Shodan 和 ZoomEye 平台查询对应信息，结果如表 2-1 所示：

表 2-1 Shodan 和 ZoomEye 检测准确度实验结果

平台	YY	YN	NN
Shodan	41	59	99
ZoomEye	18	82	95

注：YY 表示验证为提供 DNS 服务，从平台上可查到 DNS 服务器角色信息的主机数
YN 表示验证为提供 DNS 服务，从平台上查不到 DNS 服务器角色信息的主机数
NN 表示验证为不提供 DNS 服务，从平台上查不到 DNS 服务器角色信息的主机数
NY 表示验证为不提供 DNS 服务，从平台上可查到 DNS 服务器角色信息的主机数

上述实验结果表明现有平台确实会出现漏判和误判的情况。造成漏判和误判的原因是多方面的，但这个实验结果说明这些平台提供的信息并不完全可靠。

2.3. 通用基础服务器检测平台 SRDS

为了更好地掌控 CERNET 内的服务器，我们开发了一个通用基础服务器检测系统 SRDS (Server Role Detection System)。该系统目前在 iptas.edu.cn 处提供开放服务。目前该系统可以支持四种服务协议——WEB、DNS、SMTP 和 NTP 所对应的服务器检测，即对给定的地址和端口（或缺省端口）检测是否有服务器程序存在，如果有还会给出检测过程获取的 Banner 信息。系统结构如图 2-1 所示。

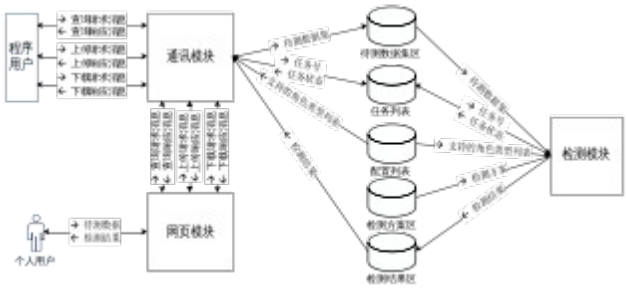


图 2-1 通用基础服务器检测平台 SRDS 结构图

在这个系统的支持下，我们建立了 CERNET 基础服务器库。

3. CERNET 基础服务器库

3.1. 检测思路和过程

SRDS 系统只能在给出的数据（IP:Port）的基础上进行检测。那么如何给出这些检测数据呢？不管是 Shodan 还是 ZoomEye 平台，其都是基于对 IP 地址的扫描来完成这项工作的，常用端口的扫描探测工具有 Nmap、Zmap[6]等。

在这方面，CERNET 基础服务器库的建立采用了完全不同的做法，检测数据的获取并不是基于扫描，而是利用 NBOS[7] (Network Behavior Observation System)平台，对得到的流记录数据进行地址初筛和扩展，并结合历史数据集最终得到提交给 SRDS 系统的待检测地址集。文献[8]介绍了 Web 服务器的地址集初筛和扩展的具体算法，该算法消耗资源较少，可以有效规避防火墙对扫描行为的拦截，只需探测约 3%的全网地址空间，就可以定位出网内几乎全部的 Web 服务器。DNS、Mail 和 NTP 服务器的待测地址集处理过程与 Web 服务器保持一致。

3.2. CERNET 基础服务器库

基于上述检测系统，我们对 CERNET 全网进行服务器检测，并建立基础服务器库。CERNET 基础服务库依次对所有主节点网络进行检测，在此过程中获取并保持检测结果。检测工作以每完成所有主节点的服务器检测为一个周期，当一个周期完整结束后立刻转入下一个新的周期。在现有条件下，每个周期的平均时长在 3~5 天。目前 CERNET 基础服务库已经稳定运行超过半年。

表 3-1 记录了在 2018 年 7 月 4 日至 7 月 22 日的四个检测周期内，CERNET 基础服务库收录的 CERNET 各个节点的四类服务器分布情况。需要说明的是由于 35 号主节点和 1 号节点数据源的缺失，服务器库目前储存的是剩余 36 个节点的有效结果。所有这些服务器的详细信息，都可以在库中查到。

表 3-1 7 月 4 日到 7 月 22 日全网各类服务器数量统计

检测日期	Web 服务器	DNS 服务器	Mail 服务器	NTP 服务器	总计
7/4-7/8	995569	28772	5118	11842	1041301
7/8-7/13	931926	28167	5097	11819	977009
7/13-7/17	943252	23310	5087	11850	983499
7/17-7/22	853848	22952	5016	11804	893936

CERNET 基础服务器库可以提供四种服务器信息的数据集，分别是 Web 服务器信息数据集 WSet、DNS 服务器信息数据集 DSet、Mail 服务器信息数据集 MSet、NTP 服务器信息数据集 NSet。每个数据集都包含着对应服务器信息的相关测度，均使用 JSON 格式的键-值格式存储。在异常检测规则的判定中需要用到的测度如表 3-2 所示：

表 3-2 服务器异常检测测度说明

测度	说明
ip	服务器的 ip 地址
port	开放对应服务的端口号
is_server	是否被判定为相应服务器，在不同的数据集中分别代表 Web、DNS、Mail、NTP 四种服务器。
status	响应状态码，从 HTTP 报文中的“Status-Code”信息中获取，无响应置 0。
dfltpage	是否默认页面，将 HTTP 响应报文中的 HTML 代码与常用的默认页面进行特征对比，符合条件判定为是，该测度置 1，默认值为 0。
org	对应服务器的校园网归属。
recursion	DNS 服务器是否支持递归查询，支持则该测度置为 1，不支持为 0，默认值为 0。
edns0	DNS 服务器是否支持 EDNS0，1 表示是，0 表示否，默认为 0。
dnssec	DNS 服务器是否支持 DNSSEC，1 表示是，0 表示否，默认为 0。
expn	Mail 服务器是否支持 EXPN 命令，1 表示支持，0 表示不支持，默认为 0。
vrfy	Mail 服务器是否支持 VRFY 命令，1 表示支持，0 表示不支持，默认为 0。
monlist	NTP 服务器是否支持 MONLIST 命令，1 表示支持，0 表示不支持，默认为 0。
roleLmt	该测度作为角色过多的界限，当实际操作时改测度可根据需求配置。
IPLLmt	该测度表示判定单位内服务器比例是否过高时该单位拥有的 IP 数目下限，我们只对单位归属 IP 数量达到该下限的单位进行服务器比例过高的判定。
pctLmt(role)	该组测度表示对应服务器比例过高的上限，与 IPLLmt 均为可配置参数。

由于不同的协议检测方案不同，所需测度也不一样，为了方便表示，我们使用“集合.测度”的形式来表示服务器信息数据中某一具体服务器对应的属性信息，如“WSet.ip”表示该 WEB 服务器的 IP 属性值，“NSet. monlist”表示 NTP 服务器的 monlist 属性值。

3.3. 检测结果

为了验证 CERNET 基础服务器库的准确性并与 Shodan、ZoomEye 平台的服务器角色信息进行对比，我们在 NBOS 系统的数据支持下，在 2018 年 3 月 5 日至 11 日期间对 CERNET 南京主节点所有接入单位约 126 万个归属地址进行了 DNS 服务探测实验。实验每次从未被探测的地址中随机选择一个目标地址探测其是否提供 DNS 服务，两个地址的探测间隔一段随机时间，从而降低地址探测的扫描特性，尽可能保证探测数据不受防火墙的干扰

探测实验最终检测到 1285 个提供 DNS 服务的主机，可以认为这就是实验期间南京节点 DNS 服务器的总数。

2018 年 3 月 12 日，我们分别从 Shodan 平台、ZoomEye 平台和 CERNET 基础服务器库查询这 1285 个地址的 DNS 服务器角色信息，计算了各个平台中对实验所发现的这 1285 个 DNS 服务器的查全率，统计结果如表 3-3 所示。

表 3-3 各服务器角色平台查全率对比

平台	查到 DNS 服务器地址数量	查全率
Shodan	514	40%
ZoomEye	222	17.30%
CERNET 基础服务器库	1285	100%

4. 基于服务器库的校园网服务器异常分析

CERNET 基础服务器库投入使用后，运行已经超过半年，较全面的收录了 CERNET 全网 4 种基础服务器的分布情况。不仅可以供网络管理员检索相关的服务器信息，还可以基于这些数据，结合数据分析的手段来对其应用进行扩展，达到充分挖掘数据潜在价值的目的本小节将介绍如何利用 CERNET 基础服务库进行异常分析并生成检测报告。

经过参阅有关文献和资料[9][10][11][12]，结合 CERNET 基础服务库提供的测度和数据，我们认为可以定位十种异常情况。

4.1. Web 服务器异常检测

1) Web 服务器使用默认页面

通常情况下，面向服务器配置的操作系统会集成 Web 服务器的应用程序，而且这些应用程序会默认开启。而大多数 Web 服务器应用程序都会设置一个用于测试的初始默认页面当服务器不提供 Web 服务时，管理者应该关闭这个服务器应用程序。如果一台 Web 服务器的初始页面是默认页面，那么这应该是一个管理员不掌控的情况。因此，使用默认页面的 WEB 服务器，可以认为是一种不正常的情况。我们选择某校的一个在 443 端口使用默认页面的服务器，并在浏览器中访问。如图 4-1 所示，经验证其 443 端口（HTTPS）首页是 Apache2 程序的默认页面。

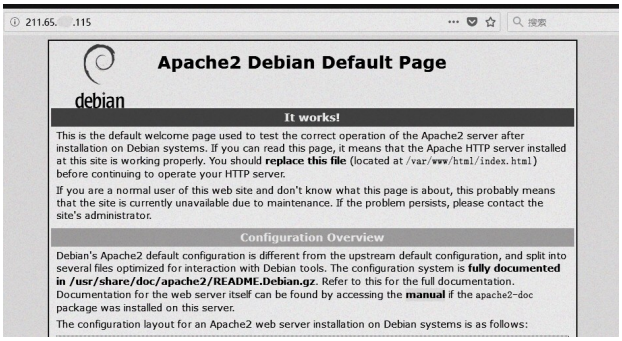


图 4-1 211.65.xxx.115 Web 服务器 443 端口首页

这个异常可以通过判定条件：

$$(web.org=X)\wedge(web.is_{server}=1)\wedge(web.dfltpage)$$

检测出。

2) Web 服务器响应状态码 5xx

Web 服务器基于 HTTP 协议，HTTP 响应码是反映 Web 服务器响应状态的一个三位数状态码，第一位定义了响应类别，取值从 1~5。其中 5xx 代表服务器发生错误，无法正常响应，提供服务。当响应状态码为 5xx 时，可以认为是一种异常情况。

这个异常可以通过判定条件：

$$(web.org=X)\wedge(web.is_{server}=1)\wedge(web.status\in[500,59$$

检测出。

4.2. DNS 服务器异常检测

由于互联网中大量配置不当的 DNS 服务器正在逐步成为攻击者进行反射攻击的放大器根据文献[13]，反射攻击控制报文的必要条件如下所示：

$$RR=ANY\wedge RD=1\wedge$$

$$EDNS0=1\wedge domain\grave{o}DNSSEC$$

其中，RR=ANY 表示查询类型是 ANY 类型，即获取所有资源记录；RD=1 表示服务器支持递归查询；EDNS0=1 表示支持 EDNS0 协议；domain ∈ DNSSEC 表示域名参数 domain 支持 DNSSEC 扩展。这四个条件中的后面三个，均可以通过服务器测度确定，因此将一个 DNS 服务器支持递归查询、支持 EDNS0 协议和支持 DNSSEC 扩展三个条件作为 DNS 服务器异常的判定标准。相对于两个 WEB 服务器的检测标准，这是约束力相对较弱的必要条件。

3) DNS 服务器支持递归查询

支持递归查询的 DNS 服务器很容易被攻击者冒充被攻击者地址利用，成为反射攻击的放大器。校园网等特定组织的 DNS 服务器，应当加入地址过滤机制，只允许组织内部的客户端进行递归查询；而用于提供权威解析的 DNS 服务器则应该关闭递归查询。

该异常可以通过判定条件：

$$(dns.org=X)\wedge(dns.is_{server}=1)\wedge(dns.recursion=1)$$

检测出。

4) DNS 服务器支持 EDNS0

支持 EDNS0 扩展的 DNS 服务器，可以突破 UDP 传输的 512 字节上限，达到更大的放大比例，因此会被很多攻击者选择作为反射攻击的放大器。管理者应该确定 DNS 服务器是否必须支持 EDNS0 扩展，如果有必要，则必须设置限值规则。

该异常可以通过判定条件：$(dns.org=X)\wedge(dns.is_{server}=1)\wedge(dns.edns0=$ 检测出。

5) DNS 服务器支持 DNSSEC 查询

支持 DNSSEC 查询的 DNS 服务器会因为数字签名存在较好的放大效果，进而被攻击者选为反射放大器。管理者应该确定 DNS 服务器是否必须支持 DNSSEC 扩展，如果有必要，则必须设置限值规则。

该异常可以通过判定条件：$(dns.org=X)\wedge(dns.is_{server}=1)\wedge(dns.edns0=$ 检测出。

4.3. Mail 服务器异常检测

6) Mail 服务器支持 EXPN

SMTP 协议的 EXPN 命令用于验证是否存在给定的邮箱列表。攻击者可以使用该命令查询服务器是否存在某特定用户名，一旦查询到就可以进行密码破解。因此，除去少量邮件系统会使用该指令做验证，Mail 服务器基本都会禁止使用该命令。管理者应该确定 Mail 服务器是否必须支持 EXPN 命令。

该异常可以通过判定条件：$(MSet.org=X)\wedge(MSet.is_{server}=1)\wedge(MSet.ex$ 检测出。

7) Mail 服务器支持 VRFY

VRFY 用于验证是否存在给定的邮箱，因此该命令存在和 EXPN 命令相同的安全风险。Mail 服务器基本都会禁止使用该命令。管理者应该确定 Mail 服务器是否必须支持 VRFY 命令。

该异常可以通过判定条件：$(MSet.org=X)\wedge(MSet.is_{server}=1)\wedge(MSet.vr$ 检测出。

4.4. NTP 服务器异常检测

8) NTP 服务器支持 MONLIST

NTP 协议中 MONLIST 指令[14]可以获取与目标 NTP 服务器进行过同步的最新 600 个客户机 IP。因此一个很小的请求报文，就能获取到大量的由 IP 地址组成的连续 UDP 报文。攻击者可以利用 NTP 服务器的 MONLIST 命令实现流量的数百倍放大比。该命令是为系统管理者设计用于管理服务器的服务情况的，不应在公网中使用。在公网中开放 MONLIST 命令的 NTP 服务器存在着巨大的安全风险，很容易被恶意利用。

该异常可以通过判定条件：$(NSet.org=X)\wedge(N\,Set.is_{server}=1)\wedge(N\,Set.monlist=1)$ 检测出。

4.5. 其他服务器异常检测

9) 单台主机多重角色

服务器的软硬件配置通常都比较高，管理者为了充分利用服务器资源，会在同一台主机上开通多种服务，这样就产生了单台主机拥有多重角色的情况。通过上面的分析可以发现每一种协议都存在着特定的风险，如果这些风险综合在一台主机上会产生更多的不稳定因素，任何一种服务出现异常都会导致整个服务器系统收到影响。因此，当单台主机的服务超过一定的界限，其安全隐患会极大提升。

用 $roleNum(IP)$ 表示一个 IP 同时具有的服务器角色数量，由于检测方案总共有 4 种，因此一个 IP 存在着双重角色，三重角色，四重角色三大类情况，共计 11 种。

双重角色，$roleNum(IP)=2$，共计 6 种情况:

1) $(WSet.org=X)\wedge(WSet.ip=DSet.ip)\wedge(WSet.is\_server=1)\wedge(DSet.is\_server=1)$

2) $(WSet.org=X)\wedge(WSet.ip=MSet.ip)\wedge(WSet.is\_server=1)\wedge(MSet.is\_server=1)$

3) $(WSet.org=X)\wedge(WSet.ip=NSet.ip)\wedge(WSet.is\_server=1)\wedge(NSet.is\_server=1)$

4) $(DSet.org=X)\wedge(DSet.ip=MSet.ip)\wedge(DSet.is\_server=1)\wedge(MSet.is\_server=1)$

5) $(.DSet\ org=X)\wedge(.DSet\ ip=.NSet\ ip)\wedge(DSet.is\_server=1)\wedge(NSet.is\_server=1)$

6) $(MSet.org=X)\wedge(MSet.ip=NSet.ip)\wedge(MSet.is\_server=1)\wedge(NSet.is\_server=1)$

三重角色，$roleNum(IP)=3$，共计 4 种情况:

1) $(WSet.org=X)\wedge(WSet.ip=DSet.ip=MSet.ip)\wedge(WSet.is\_server=1)\wedge(DSet.is\_server=1)\wedge(MSet.is\_server=1)$

2)

3)

$$(WSet.org = X) \wedge (WSet.ip = MSet.ip = NSet.ip) \wedge (WSet.is\_server = 1) \wedge (MSet.is\_server = 1) \wedge (NSet.is\_server = 1)$$

4)

$$(DSet.org = X) \wedge (DSet.ip = MSet.ip = NSet.ip) \wedge (DSet.is\_server = 1) \wedge (MSet.is\_server = 1) \wedge (NSet.is\_server = 1)$$

四重角色， $roleNum(IP)=4$ ，共计 1 种情况:

$$(WSet.org = X) \wedge (WSet.ip = DSet.ip = MSet.ip = Nset.ip) \wedge (WSet.is\_server = 1) \wedge (DSet.is\_server = 1) \wedge (MSet.is\_server = 1) \wedge (NSet.is\_server = 1)$$

$roleLmt$ 作为主机角色过多的上限，当 $roleNum(IP) \geq roleLmt$ 时，判定该服务器存在角色过多的异常情况。 $roleLmt$ 在实际工程中可根据需求配置。

10) 服务器比例过高

以 CERNET 为例，服务对象主要是校园网内部成员，其接入单位主要归属于校园网，即服务器 IP 和大多数客户机 IP 归属于同一个单位。校园网内的服务器数量与客户机数量应维持在一个合理范围。如果服务器比例过高，则有可能存在着管理员未知的服务开启状况或配置错误，需要提醒管理员注意。

判定服务器比例过高必须考虑归属单位的 IP 总数，若 IP 总数较少，则表示该单位的服务器主要客户机不在其归属之下，从而无法判断真正的服务器所占比例。因此，必须对单位拥有的 IP 数目设置一个下限，对于 IP 数目超过该下限的单位才进行服务器比例过高的判定对于每种特定的服务器由于其用途不同，所占的比例也不能统一划定标准，应该分别设置对应的比例上限。一个可以具体操作的公式如下：

$$(ipNum(X) \geq ipLLmt) \wedge \left(\frac{serverNum(X, role)}{ipNum(X)} > pctLmt(role), role \in \{web, dns, mail, ntp\}\right)$$

其中，serverNum(X,role)为服务器 role 在 X 单位下的总数，ipNum(X)为 X 单位下的 IP 总数。

4.6. 创建检测报告

对于上面提到的十种异常情况，根据安全隐患的严重程度，可以分为 Warn 和 Tip 两个等级。其中，Warn（警告）级别的异常主要是以下三类：

异常事件 1：NTP 服务器支持 MONLIST

异常事件 2：单台主机角色过多

异常事件 3：服务器比例过高

对于异常事件 2 和 3，其检测规则涉及了判定单台主机多重角色的数目 roleLmt、判定服务器过高时单位的 IP 数目下限 IPLLmt 和判定比例过高的界限 pctLmt（role）这三组测度。

5. 检测案例分析

基于上述检测规则，我们在 CERNET 服务器库的每个主节点的检测周期结束后，为每个校园网生成检测报告。在实践中，4.6 节中三组测度参数的取值为表 5-1 所示：

表 5-1 服务器异常规则相关参数

参数	取值
roleLmt	4
IPLLmt	256
pctLmt(web)	20%
pctLmt(dns)	2%
pctLmt(mail)	1%
pctLmt(ntp)	2%

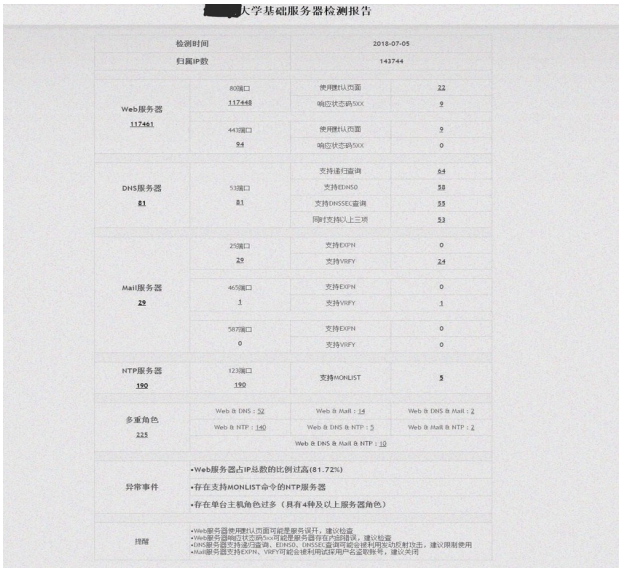
目前所有检测结果在 http://nbos2000.njnet6.edu.cn 处可以查询。下面给出几个检测案例。

案例一：

图 5-1 是 2018 年 7 月 5 日生成的 A 大学基础

服务器检测报告。报告中的各类检测数据均可以进一步点击查看其详情。可以看到，该校园网在服务器管理方面存在诸多问题。上一节介绍的三个 Warn 级别的异常在该学校均有出现，Web 服务器所占比例高达 81.72%，5 台 NTP 服务器支持 MONLIST 命令，有 10 台主机存在四重角色。

为了进一步分析该大学 Web 服务器比例异常的问题，我们对该校被判定为 Web 服务器的 IP 地址进行 Web 服务器探测，结果发现大量 IP 返回的 HTTP 报文完全相同。由此可以推测这是该校园网边界安全软件的配置策略用 ZoomEye 检测同样的 IP 地址发现，ZoomEye 也认为这些 IP 是在 80 端口提供 Web 服务的主机。



[redacted]大学基础服务器检测报告

检测时间		2018-07-05	
归属IP数		143744	
Web服务器 117461	80端口 117448	使用默认页面	22
		响应状态码5XX	9
	443端口 94	使用默认页面	9
		响应状态码5XX	0
DNS服务器 81	53端口 81	支持递归查询	64
		支持EDNS0	58
		支持DNSSEC查询	55
		同时支持以上三项	53
Mail服务器 29	25端口 29	支持EXPN	0
		支持VRFY	24
	465端口 1	支持EXPN	0
		支持VRFY	1
	587端口 0	支持EXPN	0
		支持VRFY	0
NTP服务器 190	123端口 190	支持MONLIST	5
多重角色 225	Web & DNS：52	Web & Mail：14	Web & DNS & Mail：2
	Web & NTP：140	Web & DNS & NTP：5	Web & Mail & NTP：2
	Web & DNS & Mail & NTP：10		
异常事件	•Web服务器占IP总数的比例过高(81.72%) •存在支持MONLIST命令的NTP服务器 •存在单台主机角色过多（具有4种及以上服务器角色）		
提醒	•Web服务器使用默认页面可能是服务误开，建议检查 •Web服务器响应状态码5xx可能是服务器存在内部错误，建议检查 •DNS服务器支持递归查询，EDNS0，DNSSEC查询可能会被利用发动反射攻击，建议限制使用 •Mail服务器支持EXPN、VRFY可能会被利用成垃圾用户名盗取账号，建议关闭		

图 5-1 A 大学的基础服务器检测报告（部分）

案例二：

图 5-2 是 2018 年 7 月 27 日生成的 B 高职院校
基础服务器检测报告。该院校 IP 归属共有 2048 个，其中 Web 服务器的数量为 509，占 IP 总数的 24.9%，DNS 服务器的数量为 1024，占 IP 总数的 50%，该学校存在严重的 Web、DNS 服务器比例过高的情况，需要及时解决。

该学校的 509 个在 443 端口提供服务的 Web 服务器均属于同一个/22 地址块，且首页内容完全一致，可以推测是出现服务器配置异常；1024 个 DNS 服务器有 1023 个是同一个/22 地址块，经推测也是服务器配置异常。

[redacted]学院基础服务器检测报告

检测时间		2018-07-27	
归属IP数		2048	
Web服务器 509	80端口 0	使用默认页面	0
		响应状态码5XX	0
	443端口 509	使用默认页面	0
		响应状态码5XX	0
DNS服务器 1024	53端口 1024	支持递归查询	1023
		支持EDNS0	1021
		支持DNSSEC查询	1023
		同时支持以上三项	1021
Mail服务器 0	25端口 0	支持EXPN	0
		支持VRFY	0
	465端口 0	支持EXPN	0
		支持VRFY	0
	587端口 0	支持EXPN	0
		支持VRFY	0
NTP服务器 0	123端口 0	支持MONLIST	0
多重角色 509	Web & DNS：509		
异常事件	•Web服务器占IP总数的比例过高(24.85%)，DNS服务器占IP总数的比例过高(50.0%)		
提醒	•DNS服务器支持递归查询，EDNS0，DNSSEC查询可能会被利用发动反射攻击，建议限制使用		

图 5-2 B 学院的基础服务器检测报告（部分）

案例三：

图 5-3 是 2018 年 7 月 19 日生成的 C 大学基础服务器检测报告。该院校 IP 归属共有 40960 个，各类服务器数量均控制在合理范围之内，除了个别服务器出现使用默认页面、响应状态码 5XX 两种 Tip 级的异常外，其他服务器均未出现异常。

[redacted]大学基础服务器检测报告

检测时间		2018-07-19	
归属IP数		40960	
Web服务器 339	80端口 334	使用默认页面	16
		响应状态码5XX	9
	443端口 40	使用默认页面	3
		响应状态码5XX	3
DNS服务器 6	53端口 6	支持递归查询	0
		支持EDNS0	0
		支持DNSSEC查询	0
		同时支持以上三项	0
Mail服务器 4	25端口 4	支持EXPN	0
		支持VRFY	0
	465端口 1	支持EXPN	0
		支持VRFY	0
	587端口 0	支持EXPN	0
		支持VRFY	0
NTP服务器 1	123端口 1	支持MONLIST	0
多重角色 2	Web & Mail：2		
异常事件	无		
提醒	•Web服务器使用默认页面可能是服务误开，建议检查 •Web服务器响应状态码5xx可能是服务器存在内部错误，建议检查		

图 5-3 C 大学的基础服务器检测报告

6. 总结与展望

论文讨论了校园网基础服务器的检测与分析问题。在现有网络空间搜索引擎的缺陷和局限性的基础上，给出了我们自己设计的 SRDS 基础服务器检测平台。应用该平台可以检测 CERNET 全网的 Web、DNS、Mail、NTP 四种基础服务器的指纹信息，并且基于检测结果可以进行基础服务器的异常分析。在异常分析中，我们主要从工程角度考虑，重点关注校园网内出现较多，影响较大的服务器异常情况，针对这些异常制定规则。检测结果虽然能在一定程度上避免网络边界对扫描行为的过滤，但是依然存在着改进空间。今后的工作将围绕服务器检测进行更深层次的研究，在保证研究工作实用属性的同时，提升检测平台的能力，以期获得更多可用数据，制定更加精细化的异常分析规则。

参考文献：

[1] Durumeric Z, Kasten J, Adrian D, et al. The Matter of Heartbleed[C]// Internet Measurement Conference, IMC, Vancouver, BC, Canada, 2014:475-488.

[2] Ma C. The Principles and Security Usages of Cyberspace Search Engine[J]. Cyberspace Security, 2016.

[3] Matherly J. Shodan[EB/OL]. https://www.shodan.io/, 2018.

[4] Lee S, Shin S H, Roh B H. Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning[C]// International Conference on Ubiquitous & Future Networks, ICUFN, Milan, Italy, 2017:1048-

1052.

[5] ZoomEye. ZoomEye - Cyberspace Search Engine[EB/OL]. https://www.zoomeye.org/, 2018.

[6] Durumeric Z, Wustrow E, Halderman J A. ZMap: fast internet-wide scanning and its security applications[C]//USENIX Security Symposium, Washington, DC, USA, 2013:605-620.

[7] 张维维, 龚俭, 丁伟,等. NBOS:一个基于流技术的精细化网管系统[C]// 中国教育和科研计算机网 cernet 学术年会. 2012.

[8] 丁伟, 洪沿, 夏震. 基于流记录的 HTTP80 端口服务检测和分析[J]. 华中科技大学学报(自然科学版), 2016, 44(11):34-38.

[9] 李勻. 网络渗透测试:保护网络安全的技术、工具和过程[M]. 电子工业出版社, 2007.

[10] Blum R. Open Source E-Mail Security[M]. Sams, 2002.

[11] 章思宇, 姜开达. DNS 拒绝服务攻击与对策[J]. 中国教育网络, 2014(11):51-53.

[12] 李刚, 丁伟. 东南大学:UDP 反射 DDoS 攻击原理和防范[J]. 中国教育网络, 2015(4):55-56.

[13] Kührer M, Hupperich T, Rossow C, et al. Exit from hell? reducing the impact of amplification DDoS attacks[C]// USENIX Security Symposium, San Diego, CA, USA, 2014:111–125.

[14] Ajain. How to detect NTP Amplification DoS Attacks | Qualys Blog[EB/OL]. https://blog.qualys.com/securitylabs/2014/01/21/how-qualysguard-detects-vulnerability-to-ntp-amplification-attacks, 2014-01-21

[15]