互联网大数据攻防靶场实战系统设计与研究

Design and Research of Actual Combat System for Internet Big Data Attack and Defense Range

程国辉，赵　霓（辽宁邮电规划设计院有限公司，辽宁 沈阳 110179）
Cheng Guohui，Zhao Ni（Liaoning Planning and Designing Institute of Posts and Telecommunications Co.，Ltd.，Shenyang 110179，China）

摘　要：
随着大数据的广泛应用，其安全问题日渐突出。为了进一步提升大数据攻防能力，以数据存储中心和电信互联网网络结构为基础，吸收国外搭建网络靶场攻防设计的理念，提出了一种符合我国实际情况的网络攻防靶场实战系统建设思路和软件架构，为保障大数据安全，避免遭受突发攻击，减少灾害性损失提供有力支撑。

关键词：
大数据；网络靶场；数据安全；互联网；SDN；DMZ
doi：10.12045/j.issn.1007-3043.2019.08.017
中图分类号：TN919.2
文献标识码：A
文章编号：1007-3043（2019）08-0077-05

Abstract：
With the wide application of big data，its security problem is becoming increasingly prominent. In order to further improve the defensive and offensive ability of big data，based on the data storage center and the telecom Internet network structure，absorbing the idea of building the cyber range attack and defense design abroad，it puts forward a construction idea and software architecture of the network attack and defense range actual combat system in accordance with the actual situation of our country，which provides strong support for ensuring the safety of big data，avoiding sudden attacks and reducing disaster losses.

Keywords：
Big data；Cyber range；Data security；Internet；SDN；DMZ

引用格式：程国辉，赵霓. 互联网大数据攻防靶场实战系统设计与研究[J]. 邮电设计技术，2019(8)：77-81.

0 引言

互联网的发展使全球各行各业的数据呈现爆发式增长和海量聚集的特点，大数据平台日益成为国家管理、社会治理、经济发展、人民生活的重要基础设施。平台存放了大量的国家、社会和企业数据，甚至还有国家敏感部门的静态和实时数据。目前大数据平台的系统还不能抵抗所有的网络定向攻击，而便利的互联网电子数据流可以攻击网络的每个角落。原贵阳市委书记陈刚在面对庞大的大数据产业园和密集的机柜设备时，曾经说过“弱不禁风却感觉良好，重病缠身而浑然不知”。外表规模巨大的大数据体系和脆弱的安全防护形成了强烈的反差。

国家提出要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力，切实维护广大人民群众利益、社会稳定、国家安全，加强网络和大数据安全研究，保护大数据不受侵扰、盗窃，在互联网各关键节点设置防御阻滞攻击手段势在必行。但互联网网络空间斗争比现实斗争更加激烈，同样充满硝烟。国家互联网应急中心发布的《2017年我国互联网网络安全态势综述》显示，我国境内感染远程控制木马、僵尸网络木马和流量劫持木马的主机数量分列前3位，分别达843万、239万和30万台主机。

本文正是基于以上背景，采用“以实战化训练增强实战化能力，在战斗中解决战斗”的思路，提出符合实际情况的网络靶场建设方案，搭建平时攻防演练，战时主动进攻的靶场平台。

收稿日期：2019-06-10

1 网络靶场发展现状

1.1 国外方案研究

2008年1月，美国率先启动国家赛博靶场项目（NCR——National Cyber Range），建设目标是提供虚拟环境来模拟真实的网络做攻防，针对敌对方做电子攻击和网络攻击试验，以维护美国的全球网络霸权，保证在未来网络战争中掌握绝对主动权。NCR项目的主要特点如下。

a）完全重现真实的物理网络物理拓扑结构，配置有核心、汇聚路由器、三层交换机、BAS和SR服务器、防火墙、入侵检测设备、有线无线接入等。

b）通过系统扫描和整理，力图整理网络节点中各种计算机平台和网络服务的工作状态和关键接口（主要针对计算机系统和硬盘数据存储区域）。

c）从制度上总结并分析不同安全意识等级网管人员的管理策略、方法以及工作习惯（主要针对人员管理和保密习惯）。

d）将攻防日志形成记录，根据所提供的数据进行处理和分析，将结果展现给研究人员和指战员，再次完善系统。

2010年10月，英国国防大臣认为网络安全已经成为国家的重大挑战，有必要建设网络实验场。该网络靶场由美国军火商诺·格公司搭建，是第一个可以用于商业用途的网络靶场。其基本体系结构包括评估、组件测试、研发和训练4个方面，基本上照搬美国的NCR模式，但对网络仿真模拟进行了局部优化。

1.2 国内方案研究

截至2017年，我国网络靶场建设仍然处于项目研究和起步阶段，但是研发和实验平台已经形成一定规模。依托国内部分省市大数据平台，在部分大学校园内建立了网络攻防靶场实战竞赛平台，在封闭的真实对抗环境（包括DMZ区、数据区、内网服务区、终端）中开展攻防演练。但是，在国家级网络靶场建设方面，目前只有贵阳经济开发区着手建设国家大数据安全靶场，其平台的主要出发点，多立足于技术人员的训练提升，和国际上网络实战需求相比，还存在一定差距。

本文结合国外靶场平台建设情况，分析国内电信网络、大数据网络架构特性和数据存储模式，依据软件设计模块理论和人工智能专家系统的知识模型，提出靶场建设系统软件架构设计思路和架构设想。

2 网络架构及数据存储

2.1 城域网组网模式

国内通信运营商网络分为骨干网、省网以及城域网。城域网是一个城市范围内的重要通信网。在网络安全的攻防中，最重要、竞争最激烈的部分均在城域网中发生。城域网均建有核心路由器，用于对业务控制点（SR）和宽带接入服务器（BRAS）的汇接。其中，SR主要用于互联网专线、行业应用、集团虚拟专网的接入，BRAS主要用于公众用户的语音、互联网、IP-TV等流媒体业务的接入。

无论是美国还是英国的靶场攻防系统，均没有考虑攻击过程中的截击方案，这就好比飞行的箭雨落在了最后的盾牌上，而没有在攻击箭飞行的路途中予以消灭。城域网中易于攻击的关键部位包括SR和BRAS，在关键部位可以采取特殊的截击措施。

现有的城域网架构将向SDN架构发展演进，SDN将网络设备上的控制权分离出来，由集中的控制器管理，不再依赖底层网络设备（路由器、交换机、防火墙）。网络管理员可以通过编程的方式对网络路由和规则策略进行修改，从而实现更好的数据交换性能。因此，SDN以及相关的程序设计软件将成为网络及大数据安全防护的核心阵地，共同构成官方的“阵地战”体系。

2.2 大数据存储模式

现有的大数据中心包括政府部门、大企业和行业机构，主要采用以下2种方式进行建设：一是建设独立机房，配置网络和防火墙设备，建立DMZ区域；二是将所建设的服务器平台放置于运营商IDC机房中或者放置于各地政府独立建设的大数据中心机房矩阵机柜中。无论采用上述哪种方式，均要利用DMZ技术开发相应的防火墙解决方案。DMZ通常是一个过滤的子网，它在内部网络和外部网络之间构造了一个安全地带，其网络结构如图1所示。

DMZ区域通常包括堡垒主机、Modem池以及所有的公共服务器。这些已经配置的设备，需要通过计算机软件进行编程，经内部接口连接到靶场系统中，形成防御体系。

3 网络靶场建设方案

3.1 软件架构总体设计

本文在深刻理解国外靶场软件系统的基础上，将

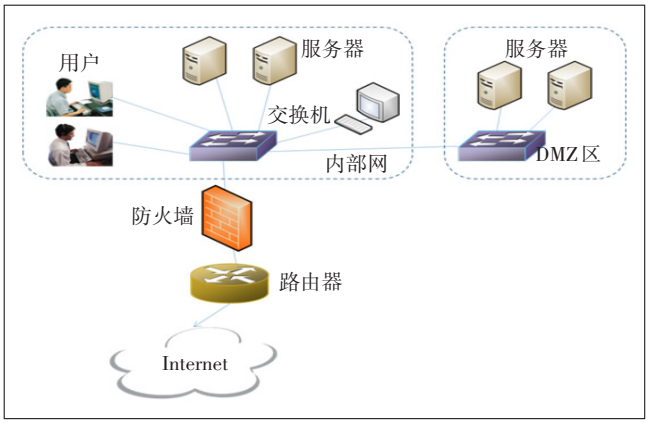

图1　常见的大数据存储服务器DMZ结构

已经建设于城域网的互联网网络监测功能、网络控制设备信息、防火墙、入侵检测与防御系统（IDS和IPS）、网络杀毒、统一威胁管理（UTM）和构建于系统上的靶场软件通过软硬件平台一体化设计，形成一个有力且全方位、灵活反应、多层次阶梯截击、“阵地战和人民战争相结合”的攻防体系平台，其软件建设逻辑层次方案如图2所示。

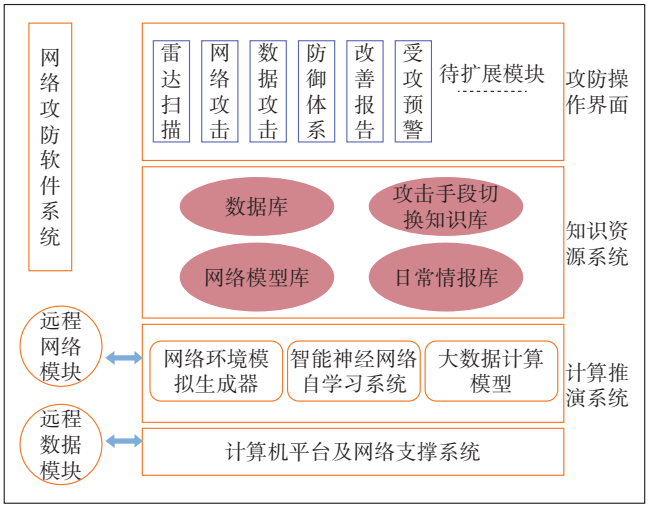

图2　网络靶场攻防软件体系设计框架

攻防操作界面：此部分供攻防演练人员和系统维护人员使用。从功能上看，为了增加对敌、对己的了解，专门设计雷达扫描功能模块，通过此模块扫描预备攻击地点网络结构、网络组成单元、大数据所在位置、IP地址规划、网络协议等。此项功能在非作战状态下可用来收集情报，并将相关信息存储到网络数据模型库中，以备战时之需。攻击模块分为网络攻击和数据攻击2个部分，它可以针对敌方的网络安全体系和数据服务器存储安全体系分别采用对应的工具进行攻击，模拟实战。

知识资源系统：设置独立的日常情报库，在和平时期，收集世界各地的网络组网信息，包括网络拓扑、设备种类、路由策略、端口状态、关键设备的漏洞登记等；在日常雷达扫描中，及时发现对方的有关数据和安全管理信息文档并不断更新。

计算推演系统：引入AI功能，利用神经元网络系统对防御和攻击不断进行演练和学习，在模拟实战中获取经验，在攻防中不断进步。AI功能让系统能自主学习，从而不断升级知识库和专家推演系统，并通过输出报告的方式供人工检阅。系统可以根据预定攻击对象，模拟生成对方的网络环境，在动态实时准确的模拟环境下演练攻击程序。

软硬件支撑平台：不建议采用B/S模式进行建设，应直接基于云计算平台，增加系统的可靠性和多CPU运行能力，与互联网中的SDN/SFN互联，与大数据中的防火墙、堡垒机互联，并通过对方已经开发的软件模块进行互动。

远程数据模块和远程网络模块：兼做网络防护和网络进攻。作为防御模块时，可以存放在网络中的关键设备（如SR、BRAS、CR、OLT）上或集中存放在SDN服务器上，在数据存储区域的防护服务上运行，与网络攻防演练系统互动；作为进攻模块时，可以开发为类似病毒植入软件，在雷达扫描发现漏洞后将该模块潜伏注入软件，在战斗时呼应主体软件系统的唤醒，从而进入工作模式。

3.2 网络探测算法

若将一个城域网比作一座城池，对于进攻方来说，掌握该城市架构和城防系统是取得进攻胜利的关键。本套系统的关键技术是雷达扫描，而雷达扫描是通过系统自动探测计算与人工手段相互补充的模式实现的。

在城域网的网络作战中，首先要掌握对方网络，策反必要的间谍网元（SPY NetUnit），也叫探子，其主要任务是发送目的端口号为1024～65535的UDP数据包，由探测源S向路由器接口M发送，利用路由器返回端口不可达报文来标识该路由器的各接口（用近端接口标识该路由器，并将其他接口置于该路由器的“其他接口”信息中）。探测的目标包括对方的出口路由器、汇聚路由器、BRAS、DNS服务器、FTP路由器、SDN网络服务器等各个路由器控制的IP地址及端口所在的网段。本系统摒弃了早期基于原始协议（ping和tra-

cert）获得拓扑的方法，借鉴相对成熟的基于SNMP的拓扑发现算法。这是因为早期算法发现速度慢，受限条件多，准确性不高。目前国外如HP公司已经开发出了基于SNMP拓扑发现算法的真实产品，该算法简单、易实现，发现速度快且结果准确，缺点是必须有间谍网元或者间谍设备配合才能获取到SNMP协议口令。

探子的培养和策反涉及到病毒和木马技术，其中比较容易策反的是网络中的计算机或服务器设备。由于路由器采用嵌入式操作系统或基于UNIX的操作系统，在策反中必须借助人工手段来窃取Profile文件，才能擦除密码，顺利进入系统。路由表中包含了丰富的网络拓扑信息，是网络拓扑结构的逻辑映像。通过分析数据包的目的地址和路由表中的网络地址，可确定数据包的正确流向。分析路由器的部分路由表，可以看出：若交付类型为直接投递，则可以判断目的子网与该路由器直连；若交付类型为间接投递，则此时下一跳项指向了该路由器直连的下一个路由器B。然后，通过访问路由器B的路由表，又可以获知它的直连网络与直连路由器。这样依此类推进行遍历访问，最后可生成整个网络的拓扑结构。

先假设路由器R_i和R_j，通过某2个接口间接连接，然后判断该连接是否和路由器R_i、R_j的AFT中已有信息相矛盾。如果找不到矛盾，则这个连接可能存在；如果矛盾，则这条连接肯定不存在，具体如图3所示。

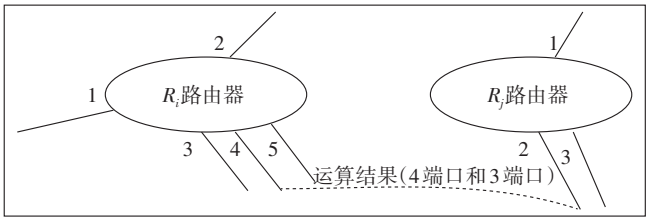

图3 路由器之间端口直连关系判定算法示意图

根据子网内路由器之间的间接连接关系，就可以确定路由器之间的直接连接关系。设子网内的所有路由器构成的集合为G，根据STP协议，路由器之间将构成一棵树。任选其中一个路由器R_i为根，假设R_i通过n个端口与其他路由器构成间接连接，则可以将G-R_i构成一个子集，子集中包含n个元素，每个元素是与R_i的某个端口p之间间接连接的路由器的集合，设为G_p，在G_p中任选一个路由器R_j，则R_j必然通过某个端口q和R_i的端口p存在间接连接关系。如果R_i不通过端口q与G_p中的其他路由器间接连接，则可以判定R_i的端口q与R_j的端口p是直接连接状态，这就是AFT利用集合数学算法的基本思想。

假设以R_1作为种子，或者作为被策反的设备，可从其管理信息库（MIB）中取出每个路由器的接口地址和子网掩码，并据此计算出各个子网的子网地址。

假设X为网络中的某个路由器，则X_i为该路由器的某个接口，从MIB中取出的路由器X_i的接口地址集合为：IP-SET={x|x∈路由器的接口地址}

从MIB中取出的子网掩码地址集合为：Mask-SET = {y|y∈路由器的子网掩码}

由于1个接口地址对应1个子网掩码，而且接口地址x与其对应的子网掩码y两者逻辑相与可以得到网络号i，即X_i∈IP- SET可以唯一确定一个Y_i∈Mask - SET，即$X_i \rightarrow Y_i$。

令$Z_i=X_i \& Y_i$，则Z_i即为子网地址集合，设该集合为Sub-Net。根据IP地址规范，可以从子网掩码推测可能的IP地址。

综上，得出计算可能IP地址的方法。

a）X_i∈IP-SET唯一确定Y_i∈Mask-SET，即$X_i \rightarrow Y_i$。

b）将两者相与，即$Z_i=X_i \& Y_i$。

c）根据子网掩码得到非零部分的可能值与Z_i相加，就可以得到可能IP地址的集合，设该集合为GuseeIP- Set。本系统综合采用STP算法，借鉴实际获得的资料，根据网管所得到的设备属性，采用人工手段对获取的网络结构进行修正完善。

3.3 进攻路径

如图4所示，在发生对抗时，根据策反设备或者Spy netUnit发送的IGMP包和MIB获得的路由表，分析对方路由器网络结构。同理，BRAS设备的网络结构也是可以分析的，通过设备ID号，可获得所有网络设备的结构图。首先进攻网络路由，以“掐断”要害部位为目的。一般情况下，对方的网络系统和大数据系统较为完善、庞大，因此，一定要保证在最短的时间内让要害部位“中断”运行，达到“一剑锁喉”的目的。其次，要根据进攻目的，进行局部细分区域进攻。获取并下载所需要的数据，必要时破坏其数据，然后对DMZ区域进行进攻。最后，采用枚举试探进攻，根据已经获取的防护口令，依次对路由进行循环攻击测试，直至达到目的为止。由于这种方式耗时较长，因此，在进攻过程中可以灵活依次采用事先设定好的程序分别进行尝试攻击。

3.4 方案特点

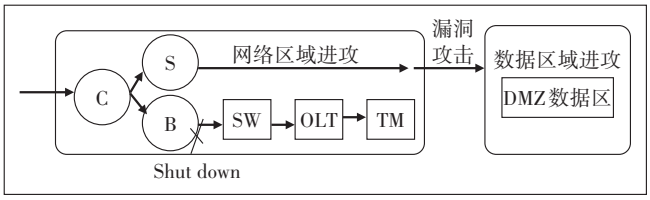

图4　网络靶场进攻路由显示

与已经公开的攻防演练系统相比，本方案具有如下特点。

a）本方案融合已有的网络安全技术和大数据存储安全技术，完成攻防一体化设计。

b）建设平台可以作为区域级的软件设计架构基础。

c）将AI引入攻防系统设计，系统自动建立保护机制和对抗复杂攻击能力。

d）本方案增加雷达扫描功能模块，在战时可以主动快速获取对方情况；在和平时期可以用于防御监测，收集整理网络上的情报资源，分类存储，记录可攻击区域。

3.5 应用举例

目前，基于上述方案的攻防系统已部署在某城市IP城域网内进行实战演练。该市属于网络战密集地带，演练采用网络靶场模式，系统连接于该市城域网。考虑到我国的军事特点，在实践中优先使用系统的防御功能；探测系统只作为仿真模拟，没有实际投入到对别国网络结构的探测和攻击测试中。

图5为网络雷达对抗子系统和网络防御子系统在实际使用中的展现。通过扫描该市的网络，可知其自身的安全性为86分，扫描中发现其中一个汇聚节点存在被攻击的可能性；通过网络整理和自修复，网络的对外防御能力达到97分，网络系统达成预定目标，防御系统运行正常并发挥作用。为抵御来自其他国家的网络攻击，该系统还需要进一步提高安全等级，尤其是城域网内的各种计算机和服务器设备，需加强漏洞修补，避免成为敌对国家的探子。

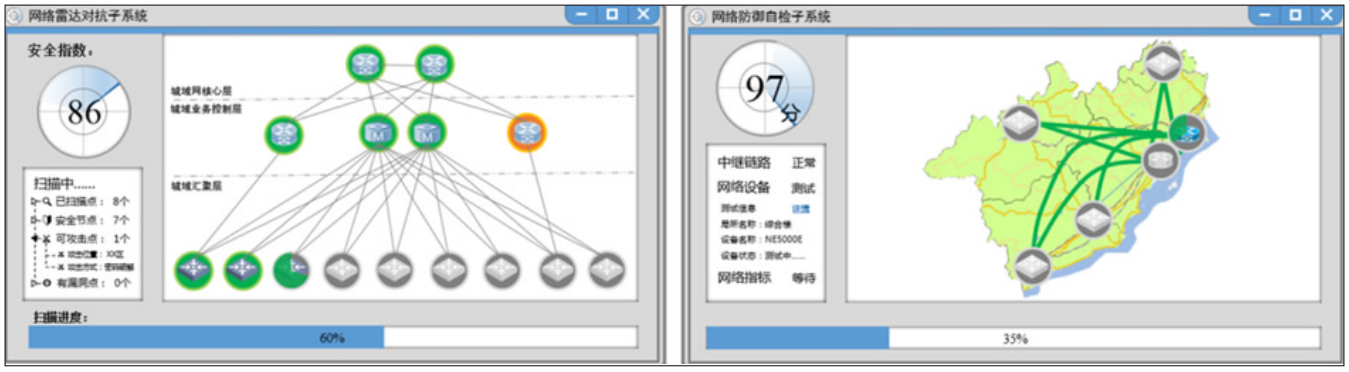

图5　系统运行演示图

4 未来发展与展望

网络大数据攻防演练系统作为我国大数据发展过程中新生事物，一方面承担着现有计算机网络和大数据平台的安全防护功能，另一方面也要为将来可能发生的网络战争做好铺垫准备。在日常的网络安全学习和培训中，攻防演练系统也可以作为基础知识学习和实践平台，帮助学员进一步熟悉FTP服务器攻击、木马查杀、IIS溢出攻击、防洪水flood攻击等。网络和数据安全工作严格来说，只有起点没有终点。互联网大数据攻防体系需要不断演练、完善和补充，才能在未来的信息化战争中成为真正的网络长城。

参考文献：

[1] INGOLS K, LIPPMANN R, PIWOWARSKI K. Practical Attack Graph Generation for Network Defense[C]// Computer Security Applications Conference. 2006.

[2] WANG F, GANG P, CHE W, et al. Design Method for Virtual Network Attack and Defense Platform[J]. Aasri Procedia, 2012(3): 335-340.

[3] 程静，雷璟，袁雪芬. 国家网络靶场的建设与发展[J]. 中国电子科学研究院学报，2014，9(5)：446-452.

[4] 徐川，唐建，唐红. 网络攻防对抗虚拟实验系统的设计与实现[J]. 计算机工程与设计，2011，32(4)：1268-1271.

作者简介：

程国辉，毕业于东北大学，高级工程师，硕士，主要从事通信网络规划和设计工作；赵霓，毕业于沈阳工业学院，高级工程师，主要从事通信网络规划和设计工作。