高校校园网漏洞挖掘与防御技术研究

宋　伟　黎银环　肖智坤　雷绍缨
（江门职业技术学院信息工程学院，广东 江门 529000）

摘要：黑客攻防是一场没有硝烟的战争，虽然普通人很少能感受到，但是全世界无时无刻不进行着这场战役，互联网的世界，黑客的身影几乎是无处不在的，西方世界无时无刻不想着渗透进我们的网络，随着近期 360 公司揭开了美国入侵西北工业大学的事实，让我们深刻的意识到了高校网络安全的重要性，本文从高校校园网漏洞挖掘与防御的两个角度剖析校园网安全。

关键词：黑客攻防；校园网；漏洞挖掘

一、概述

（一）研究背景

“没有网络安全就没有国家安全”，早在 2014 年国家网络安全小组组长习近平主席就提出了这样的口号，网络安全被提到了战略发展的高度，随着 360 公司陆续揭开了美国国家安全部门在我国的高校、科研机构、企事业公司植入远程木马程序，用于窃取我们珍贵的科研资料，网络安全变得极为重要，发展一支可靠的网络安全大军尤为迫切。

（二）研究现状

2016 年由公安部主导的“护网行动”掀起了国内网络攻防的高潮，国家机关、企事业单位、高校科研单位等全行业的纳入行动中来，奇安信、长亭科技、绿盟等一些网安公司也都参与组织了“红蓝对抗”，收效显著，地方政府上也如火如荼的投入精力融入进来，如广东省公安厅组织了“粤盾行动”，江门市公安局组织了“邑盾行动”，积极响应国家号召，展开攻防演练，做好网络安全的防备工作。

（三）研究意义

虽然国家大力发展网络安全，但是高校作为一块需要被防守的阵地，目前在运维方面还存在着诸多安全问题，网络结构复杂，也缺乏经验丰富的网络安全防御人员，对于正在发生的黑客攻防事件缺乏应急响应的能力，对此迫切地需要一些指导建议，加上网络攻防的手段可谓日新月异，新的漏洞层出不穷，那么防御手段也需要及时地得到更新，这是一项长期持久的活动。

二 . 校园网常见漏洞分析

校园网是一个庞杂的网络结构，有着网络结构复杂，设备繁多，系统繁多，应用系统繁多等特点，具体问题粗略的从三个大方向分析列举如下。

（一）网络设备漏洞

作为校园网的架构主体，路由器、交换机、防火墙、IDS、IPS、日志审计、内容审计、ACS、WAF、AC、AP、无线控制器等诸多硬件系统，硬件都有操作系统，一些版本的系统可能存在着严重的安全隐患，一方面是这些硬件基本上很少更新，另一方面是非专业人员不知道如何给这些系统打补丁或者是更换系统，这是一件比较棘手的事情，稍有不慎会导致网络的中断，影响到正常的运作，好在一点的是很多黑客关注的重点不在这里，他们更多关注的电脑操作系统、软件系统和 WEB 等对象，但这只是针对大多数的白帽子黑客，而对于目的性很强的黑帽子黑客来说，他们绝对不会忽视这个环节。

（二）操作系统漏洞

校园网内有各种在线应用系统，上网用户也很多，也很集中，线上可能有着各种操作系统 windows、linux 等，其中线上的服务器系统有 windows server 2003 到 windows server 2012 等各个版本，个人用户 win7 以上各个版本，linux 有着 redhat、centos、ubuntu、debian 等各种系统，线上系统虽然可能安装有防火墙，但系统补丁更新不及时，甚至无更新，个人用户大多数没有安全防护意识，存在防护上的真空。

（三）web 应用系统漏洞

每一所大学都有着诸多在线 web 应用系统，为方便管理与更新，一些大学将门户站点也部署在网络中心，另外还有 OA 办公系统、科研管理系统、财务管理系统、教研系统等等，这些系统在开发的时候一般只注重功能的实现，虽然使用起来方便，加上开发者大多数都不太懂从网络安全的角度出发，所以就导致大多数系统都存在着不同程度的安全问题。

三、校园网漏洞挖掘

园区网漏洞虽然繁多，作为一名渗透测试人员可在授权的情况下使用各种手段做出如下工作开展。

（一）资产扫描、发现目标

白盒测试中可以直接明确要测试的目标，而黑盒测试需要摸着石头过河，全方位探测敏感信息，来测试可能存在的安全隐患问题，在此我们可以使用一些必要的测试手段来了解校园网全网结构以及可能存在问题的敏感信息，如可使用 kali 下资产扫描工具 Maltego。

子域名挖掘：在每个域名之下必然存在着各个系统，以江门职业技术学院为例，jmpt.edu.cn，其下有 www.jmpt.edu.cn，jwc.jmpt.edu.cn，newoa.jmpt.edu.cn 等为数众多的子域名，需要用使用域名挖掘手段进行扫描，子域名挖掘有在线子域名扫描系统，kali 下也有 Aquatone 等工具。

C 段扫描：探索完网络主体架构之后可以使用 C 段分段扫描网络，发现敏感目标信息，使用 NMAP 工具可以实现此目的，在此过程中要注意不要触发追踪系统、防火墙以及 IDS 等设备。

（二）网络设备漏洞挖掘

在 3.1 阶段发现的目标中可以发现校园网的主体架构设备，路由器、交换机等，一些校园网采用的是思科等公司的设备，这些设备运行稳定，但是通常存在使用时间年限较长，且基本上不会更新其 IOS 系统，更不会打补丁，这就给擅长挖掘漏洞的黑帽子黑客很多操作空间，我们可以根据扫描到的信息去国家漏洞资源库或者 CVE 等站点查询相关漏洞以及攻击的手段。

常规漏洞挖掘方式：在 kali linux 系统下也可以方便快捷的使用 searchsploit 查询是否有相应的攻击的手段，这些攻击的对象包含硬件设备操作系统漏洞本身，如思科的是 IOS 系统，华为的是 VRP 系统等，通过漏洞本身可能开展的有溢出攻击或者直接获得远程访问权限等，在攻击成功之后如果能够直接登录系统则可以进一步对设备配置，甚至可以配置监事会话来实现内网全网数据的监听，抓取内网远程登录、远程桌面等明文密码数据，又或者

将抓取到的 MD5 秘钥进行撞库破解，又或者展开 DNS、ARP 等欺骗攻击，将用户诱导到钓鱼网站。

暴力破解漏洞挖掘方式：网络设备通常都开通了 telnet、SSH 或者远程 web 登录管理，一些硬件设备没有对登录本身的次数做限制，这样就导致黑客在攻击时可以尝试社工手段或者用暴力破解方式获得登录账户和秘钥，从而控制设备本身，通过建立 VPN 连接通道可以随时穿透到内网中来进行 ATP 渗透攻击。

（三）操作系统漏洞挖掘

服务器分为 WINDOWS 和 LINUX 系统，一些校园网服务器使用了一些 windows server 系统，从 windows server2003 到 windows server2012 甚至更高不等，windows 系统漏洞爆料可谓层出不穷，在微软官方站点可以查阅其发布的漏洞信息，也可以从 CVE 等站点去查询，虽然微软官方会及时的在第一时间发布补丁信息，但是作为校园网的管理方却很少会去更新这些补丁信息，这就导致了攻击存在着无限可能性，linux 系统也存在同样的问题，且 linux 存在着种类繁多，版本繁多的问题，如常见的就有 redhat、centos、ubuntu、debian 等，一般的系统管理员很难做到熟悉全部的 LINUX 如何操作，更不要说如何更新系统和软件。

通过这些系统或者软件漏洞攻击成功之后还可以进一步使用远程控制木马来反弹到黑客的控制端，又或者使用更为隐蔽的流量转发技术，如 SSH 隧道转发技术等穿透内网，绕过防火墙到达黑客控制端。

常规漏洞挖掘方式：操作系统的漏洞挖掘一般使用漏洞扫描工具进行扫描探测，如 nmap、nessus、awvs、nikto 等，也有一些厂家的商业版漏洞扫描软件，如赛门铁克的 web 漏洞扫描系统，扫描到漏洞之后还可以直接定位到攻击方法页面，方便用户直接进行攻击测试。

知名漏洞挖掘方式：校园网内部还有着为数众多的 win7 系统，如图书查询系统，学生和教师用户端，这些系统存在通用漏洞如知名的 MS17-010 漏洞，使用 Metasploit 下的辅助工具直接开展 C 段扫描就可以发现大批量存在该漏洞的用户，通过漏洞攻击后可直接获得管理员权限，还可以安插后门，制作成跳板方便后续的 APT 攻击。

复杂情况漏洞挖掘方式：校园网中的内网软件服务众多，攻击手段也是花样繁多，如弱口令攻击；FTP 服务器攻击，攻击成功之后进行提权，还可以上传包含木马的文件诱导用户下载运行；邮件欺骗攻击，使用邮件来发送钓鱼邮件；DNS 欺骗 +ARP 欺骗将用户诱导到钓鱼网站；直接攻击软件漏洞等等，漏洞挖掘手段依据现实情况而定，此处不能尽数。

（四）web 应用系统漏洞挖掘

校园网存在着多种 web 应用系统，比如门户站点、OA 办公系统、科研管理系统、财务管理系统、教研系统等等，开发使用的语言也是多种多样，有 php、asp、jsp 等，中间件使用的也是多种多样，iis、apache、nginx、php、tomcat 等，数据库使用的也是花样繁多，如 mysql，mssql，db2，oracle 等，对于开发者和使用者来说，他们都只关注功能的实现，安全问题自然是一地鸡毛，若是在以前这倒似乎没什么问题，web 系统漏洞挖掘大致分为以下手段。

源代码审计挖掘方式：对网站使用源代码审计工具进行审计，发现可能存在的函数以及变量，进行逐个加固，这是一项工作量极大的活动，可以使用 rips、sexy 等工具辅助进行审计，提高工作效率，这要求黑客同时具备了高深的开发水平。

使用漏扫工具扫描挖掘方式：使用 Nessus、awvs、appscan、burpsuite、nikto、御剑后台工具等对 web 系统发起漏洞扫描，可以发现中间件以及常见的 owasp top 10 漏洞，根据扫描报告展开攻击测试。

根据经验渗透进行挖掘方式：扫描工具发现的漏洞非常有限，一些注入漏洞、CSRF、XSS 越权等漏洞有时只能通过手工方式进行测试，攻击的手段花样也因人而异，还有一些如数据库注入漏洞，虽然使用 sqlmap 配合众多的脚本对目标系统进行测试，但是如果对方部署了 waf 系统对工具进行限制，那么此时就只能用手工方式逐个探测，逐步挖掘。

四、校园网漏洞防御

黑客攻击手段繁多，作为防守的一方，我们也需要尽心尽力，筑起网安长城。

（一）部署网络安全设备防御

校园网当中的硬件网络安全设备是我们筑起的第一道防御长城，防火墙、IDS、IPS、WAF、4S 审计系统、上网认证系统，数据库审计系统等是基本的防护手段，通过防火墙的规则将安全进行了分区管理、IDS 实现攻击报警、IPS 进行攻击防御、WAF 可以有效地防范大多数 WEB 系统攻击，4S 审计可以进行追溯攻击源，上网认证系统可以方式非法用户接入，数据库审计系统可以做到数据库攻击精准回溯。

（二）部署补丁升级系统

防范漏洞攻击的最有效手段就是堵住漏洞，在校内部署一台补丁升级服务器，同时在校内一些线上系统部署升级客户端，及时更新各个在线系统存在的系统漏洞和软件漏洞。

（三）自我渗透测试与漏洞评估

随着网络安全的重要性越来越强地体现出来，各地地方政府也会组织相应的攻防演练活动，比如广东省组织的“粤盾行动”，江门市组织的“邑盾行动”，如果可以让攻击队伍在活动后出具相应的攻击测试报告，及时填补漏洞，其次可以在每年的校园技术节组织开放学生参加授权的渗透测试活动，提高学生的水平同时填补漏洞，何乐而不为。

参考文献：

[1] 陈广勇，祝国邦，范春玲 .《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）标准解读 [J]. 信息网络安全，2019（07）：1-7.

[2] 韩晓露，刘云，张振江，吕欣，李阳 . 网络安全态势感知理论与技术综述及难点问题研究 [J]. 信息安全与通信保密，2019（07）：61-71.

[3] 段忠祥 .“等级保护”背景下智慧校园网络数据安全问题研究 [J]. 网络安全技术与应用，2020，20（9）：88-90.

[4] 谢振坛，申伟 . 校园网络安全管理现状与对策探究 [J]. 教学与管理，2019（18）：52-54.

[5] 张晓晓，郭绍永 . 浅谈高校校园网网络安全管理的研究与实施 [J]. 信息系统工程，2017（6）：58.

[6] 吕志远，陈靓，冯梅，等 . 拟态防御理论在企业内网安全防护中的应用 [J]. 小型微型计算机系统，2019，40（1）：69-76.

（支持项目：2023 年广东省科技创新战略专项基金 pdjh2023b1035：高校校园网信息安全漏洞挖掘技术应用研究）