实战攻防演习之

红队视角下的防御体系突破

奇安信安服团队

2019.8

前　言

网络实战攻防演习，是新形势下关键信息系统网络安全保护工作的重要组成部分。演习通常是以实际运行的信息系统为保护目标，通过有监督的攻防对抗，尽可能地模拟真实的网络攻击，以此来检验信息系统的实际安全性和运维保障的实际有效性。

2016 年以来，在国家监管机构的有力推动下，网络实战攻防演习日益得到重视，演习范围越来越广，演习周期越来越长，演习规模越来越大。国家有关部门组织的全国性网络实战攻防演习从 2016 年仅有几家参演单位，到 2019 年已扩展到上百家参演单位；同时各省、各市、各行业的监管机构，也都在积极地筹备和组织各自管辖范围内的实战演习。一时间，网络实战攻防演习遍地开花。

在演习规模不断扩大的同时，攻防双方的技术水平和对抗能力也在博弈中不断升级。

2016 年，网络实战攻防演习尚处于起步阶段，攻防重点大多集中于互联网入口或内网边界。

2017 年，实战攻防演习开始与重大活动的网络安全保障工作紧密结合。就演习成果来看，从互联网侧发起的直接攻击仍然普遍十分有效；而系统的外层防护一旦被突破，横向移动、跨域攻击，往往都比较容易实现。

2018 年，网络实战攻防演习开始向行业和地方深入。伴随着演习经验的不断丰富和大数据安全技术的广泛应用，防守方对攻击行为的监测、发现和溯源能力大幅增强，与之相应的，攻击队开始更多地转向精准攻击和供应链攻击等新型作战策略。

2019 年以来．网络实战攻防演习工作受到了监管部门、政企

机构和安全企业的空前重视。流量分析、EDR、蜜罐、白名单等专业监测与防护技术被防守队广泛采用。攻击难度的加大也迫使攻击队全面升级，诸如 0day 漏洞攻击、1day 漏洞攻击、身份仿冒、钓鱼 WiFi、鱼叉邮件、水坑攻击等高级攻击手法，在实战攻防演练中均已不再罕见，攻防演习与网络实战的水平更加接近。

如何更好地参与网络实战攻防演习？如何更好地借助实战攻防演习提升自身的安全能力？这已经成为大型政企机构运营者关心的重要问题。

作为国内前沿的网络安全企业，奇安信集团已成为全国各类网络实战攻防演习的主力军。奇安信集团安服团队结合 200 余次实战攻防演习经验，总结编撰了这套实战攻防演习系列丛书，分别从红队视角、蓝队视角和紫队视角，来解读网络实战攻防演习的要领，以及如何结合演习提升政企机构的安全能力。

需要说明的是，实战攻防演习中的红方与蓝方对抗实际上是沿用了军事演习的概念和方法，一般来说，红方与蓝方分别代表攻击方与防守方。不过，红方和蓝方的名词定义尚无严格的规定，也有一些实际的攻防演习，将蓝队设为攻击队、将红队设为防守队。在本系列丛书中，我们依据绝大多数网络安全工作者的习惯，统一将攻击队命名为红队，将防守队命名为蓝队，而紫队则代表组织演练的机构。

《红队视角下的防御体系突破》是本系列丛书的第一本。本书希望通过归纳总结红队常用的攻击策略和攻击战术，帮助政企机构理解攻方思维，以便提升演习水平，构筑更有效的安全防御体系。正所谓“知己知彼，百战不殆”。

目　　录

第一章 什么是红队

红队，一般是指网络实战攻防演习中的攻击一方。

红队一般会针对目标系统、人员、软件、硬件和设备同时执行的多角度、混合、对抗性的模拟攻击；通过实现系统提权、控制业务、获取数据等目标，来发现系统、技术、人员和基础架构中存在的网络安全隐患或薄弱环节。

红队人员并不是一般意义上的电脑黑客。因为黑客往往以攻破系统，获取利益为目标；而红队则是以发现系统薄弱环节，提升系统安全性为目标。此外，对于一般的黑客来说，只要发现某一种攻击方法可以有效地达成目标，通常就没有必要再去尝试其他的攻击方法和途径；但红队的目标则是要尽可能地找出系统中存在的所有安全问题，因此往往会穷尽已知的“所有”方法来完成攻击。换句话说，红队人员需要的是全面的攻防能力，而不仅仅是一两招很牛的黑客技术。

红队的工作也与业界熟知的渗透测试有所区别。渗透测试通常是按照规范技术流程对目标系统进行的安全性测试；而红队攻击一般只限定攻击范围和攻击时段，对具体的攻击方法则没有太多限制。渗透测试过程一般只要验证漏洞的存在即可，而红队攻击则要求实际获取系统权限或系统数据。此外，渗透测试一般都会明确要求禁止使用社工手段（通过对人的诱导、欺骗等方法完成攻击），而红队则可以在一定范围内使用社工手段。

还有一点必须说明：虽然实战攻防演习过程中通常不会严格限定红队的攻击手法，但所有技术的使用，目标的达成，也必须严格遵守国家相关的法律和法规。

在演习实践中，红队通常会以 3 人为一个战斗小组，1 人为

组长。组长通常是红队中综合能力最强的人，需要较强的组织意识、应变能力和丰富的实战经验。而 2 名组员则往往需要各有所长，具备边界突破、横向移动（利用一台受控设备攻击其他相邻设备）、情报收集或武器制作等某一方面或几个方面的专长。

红队工作对其成员的能力要求往往是综合性的、全面性的。红队成员不仅要会熟练使用各种黑客工具、分析工具，还要熟知目标系统及其安全配置，并具备一定的代码开发能力，以便应对特殊问题。

第二章 红队三板斧——攻击的三个阶段

红队的攻击并非是天马行空的撞大运，而是一个有章可循、科学合理的作战过程。一般来说，红队的工作可分为三个阶段：情报收集、建立据点和横向移动。我们也常将这个三个阶段称为红队工作的“三板斧”。

一、 第一阶段：情报收集

当红队专家接到目标任务后，并不会像渗透测试那样在简单收集数据后直接去尝试各种常见漏洞，而是先去做情报侦察和信息收集工作。收集的内容包括组织架构、IT 资产、敏感信息泄露、供应商信息等各个方面。组织架构包括单位部门划分、人员信息、工作职能、下属单位等；IT 资产包括域名、IP 地址、C 段、开放端口、运行服务、WEB 中间件、WEB 应用、移动应用、网络架构等；敏感信息泄露包括代码泄露、文档信息泄露、邮箱信息泄露、历史漏洞泄露信息等方面；供应商信息包括相关合同、系统、软件、硬件、代码、服务、人员等相关信息。

掌握了目标企业相关人员信息和组织架构，可以快速定位关键人物以便实施鱼叉攻击，或确定内网横纵向渗透路径；而收集了 IT 资产信息，可以为漏洞发现和利用提供数据支撑；掌握企业与供应商合作相关信息，可为有针对性开展供应链攻击提供素材。而究竟是要社工钓鱼，还是直接利用漏洞攻击，抑或是从供应链下手，一般取决于哪块是安全防护的薄弱环节，以及红队对攻击路径的选择。

二、 第二阶段：建立据点

在找到薄弱环节后，红队专家会尝试利用漏洞或社工等方法去获取外网系统控制权限，一般称之为“打点”或撕口子。在这

个过程中，红队专家会尝试绕过 WAF、IPS、杀毒软件等防护设备或软件，用最少的流量、最小的动作去实现漏洞利用。

通过撕开的口子，寻找和内网联通的通道，再进一步进行深入渗透，这个由外到内的过程一般称之为纵向渗透，如果没有找到内外联通的 DMZ 区（Demilitarized Zone，隔离区），红队专家会继续撕口子，直到找到接入内网的点为止。

当红队专家找到合适的口子后，便可以把这个点作为从外网进入内网的根据地。通过 frp、ewsocks、reGeorg 等工具在这个点上建立隧道，形成从外网到内网的跳板，将它作为实施内网渗透的坚实据点。

若权限不足以建立跳板，红队专家通常会利用系统、程序或服务漏洞进行提权操作，以获得更高权限；若据点是非稳定的 PC 机，则会进行持久化操作，保证 PC 机重启后，据点依然可以在线。

三、 第三阶段：横向移动

进入内网后，红队专家一般会在本机以及内部网络开展进一步信息收集和情报刺探工作。包括收集当前计算机的网络连接、进程列表、命令执行历史记录、数据库信息、当前用户信息、管理员登录信息、总结密码规律、补丁更新频率等信息；同时对内网的其他计算机或服务器的 IP、主机名、开放端口、开放服务、开放应用等情况进行情报刺探。再利用内网计算机、服务器不及时修复漏洞、不做安全防护、同口令等弱点来进行横向渗透扩大战果。

对于含有域的内网，红队专家会在扩大战果的同时去寻找域管理员登录的蛛丝马迹。一旦发现某台服务器有域管理员登录，就可以利用 Mimikatz 等工具去尝试获得登录账号密码明文，或

者 Hashdump 工具去导出 NTLM 哈希，继而实现对域控服务器的渗透控制。

在内网漫游过程中，红队专家会重点关注邮件服务器权限、OA 系统权限、版本控制服务器权限、集中运维管理平台权限、统一认证系统权限、域控权限等位置，尝试突破核心系统权限、控制核心业务、获取核心数据，最终完成目标突破工作。

第三章 红队也套路——常用的攻击战术

在红队的实战过程中，红队专家们逐渐摸出了一些套路、总结了一些经验：有后台或登录入口的，会尽量尝试通过弱口令等方式进入系统；找不到系统漏洞时，会尝试社工钓鱼，从人开展突破；有安全防护设备的，会尽量少用或不用扫描器，使用 EXP 力求一击即中；针对蓝队防守严密的系统，会尝试从子公司或供应链来开展工作。建立据点过程中，会用多种手段多点潜伏，防患于未然。

下面介绍四种红队最常用的攻击战术。

一、 利用弱口令获得权限

弱密码、默认密码、通用密码和已泄露密码通常是红队专家们关注的重点。实际工作中，通过脆弱口令获得权限的情况占据90%以上。

很多企业员工用类似 zhangsan、zhangsan001、zhangsan123、zhangsan888 这种账号拼音或其简单变形，或者 123456、888888、生日、身份证后 6 位、手机号后 6 位等做密码。导致通过信息收集后，生成简单的密码字典进行枚举即可攻陷邮箱、OA 等账号。

还有很多员工喜欢在多个不同网站上设置同一套密码，其密码早已经被泄露并录入到了社工库中；或者针对未启用 SSO 验证的内网业务系统，均习惯使用同一套账户密码。这导致从某一途径获取了其账户密码后，通过凭证复用的方式可以轻而易举地登录到此员工所使用的其他业务系统中，为打开新的攻击面提供了便捷。

很多通用系统在安装后会设置默认管理密码，然而有些管理员从来没有修改过密码，如 admin/admin、test/123456、

admin/admin888 等密码广泛存在于内外网系统后台，一旦进入后台系统，便有很大可能性获得服务器控制权限；同样，有很多管理员为了管理方便，用同一套密码管理不同服务器。当一台服务器被攻陷并窃取到密码后，进而可以扩展至多台服务器甚至造成域控制器沦陷的风险。

二、 利用社工来进入内网

计算机“从来”不会犯错误，程序怎么写，逻辑便怎么执行；在一台计算机上怎样执行，在另外一台计算机也同样执行。但人却会犯各种各样的错误，同一名员工在不同情况下的同一件事情上可能会犯不同的错误，不同的员工在同一情况的同一件事情上也可能会犯不同错误。很多情况下，当红队专家发现搞系统困难时，通常会把思路转到“搞人”（社工、钓鱼等）。

很多员工对接收的木马、钓鱼邮件没有防范意识。红队专家可针对某目标员工获取邮箱权限后，再通过此邮箱发送钓鱼邮件。大多数员工由于信任内部员工发出的邮件，从而轻易点击了夹带在钓鱼邮件中的恶意附件。一旦员工个人电脑沦陷，红队专家可以员工 PC 作为跳板实施横向内网渗透，继而攻击目标系统或其他系统、甚至攻击域控制器导致内网沦陷。

当然，社工不仅仅局限于使用电子邮件，通过客服系统、聊天软件、电话等方式有时也能取得不错的效果。像当年经典的黑客“朽木”入侵某大型互联网公司，所采用的就是通过客服系统反馈客户端软件存在问题无法运行，继而向客服发送了木马文件，最终木马上线后成功控制了该公司核心系统，就是一个经典的案例。有时，黑客会利用企业中不太懂安全的员工来打开局面，譬如给法务人员发律师函、给人力资源人员发简历、给销售人员发采购需求等等。

一旦控制了相关员工计算机，便可以进一步实施信息收集。譬如大部分员工为了日常计算机操作中的方便，以明文的方式在桌面或“我的文档”存储了包含系统地址以及账号密码的文档；此外大多数员工也习惯使用浏览器的记住密码功能，浏览器记住密码功能大部分依赖系统的 API 进行加密，所存储的密码是可逆的。红队在导出保存的密码后，可以在受控机上建立跳板，用受控员工的 IP、账号、密码来登录，简直没有比这更方便的了。

三、 利用旁路攻击实施渗透

在有蓝队防守的红队工作中，有时总部的网站防守得较为严密，红队专家很难直面硬钢，撬开进入内网的大门。此种情况下，通常红队不会去硬攻城门，而是会想方设法去找“下水道”，或者挖地道去迂回进攻。

红队实战中发现，绝大部分企业的下属子公司之间，以及下属公司与集团总部之间的内部网络均未进行有效隔离。很多部委单位、大型央企均习惯使用单独架设一条专用网络来打通各地区之间的内网连接，但同时又忽视了针对此类内网的安全建设，缺乏足够有效的网络访问控制，导致子公司、分公司一旦被突破，红队可通过内网横向渗透直接攻击到集团总部，漫游企业整个内网，攻击任意系统。

例如 A 子公司位于深圳，B 子公司位于广州，而总部位于北京。当 A 子公司或 B 子公司被突破后，都可以毫无阻拦地进入到总部网络中来；而另外一种情况，A 与 B 子公司可能仅需要访问总部位于北京的业务系统，而 A 与 B 不需要有业务上的往来，理论上应该限制 A 与 B 之间的网络访问。但实际情况是，一条专线内网通往全国各地，一处沦陷可以导致处处沦陷。

另外大部分企业对开放于互联网的边界设备较为信任，如

VPN 系统、虚拟化桌面系统、邮件服务系统等。考虑到此类设备通常访问内网的重要业务，为了避免影响到员工的正常使用，企业没有在其传输通道上增加更多的防护手段；再加上此类系统多会集成统一登录，一旦获得了某个员工的账号密码，就可以通过这些系统突破边界直接进入内网中来。

譬如开放在内网边界的邮件服务通常缺乏审计、也未采用多因子认证，员工平时通过邮件传送大量内网的敏感信息，如服务器账户密码、重点人员通讯录等；当掌握员工账号密码后，在邮件中所获得的信息，会给红队下一步工作提供很多方便。

四、 秘密渗透与多点潜伏

红队工作一般不会大规模使用漏洞扫描器。目前主流的 WAF、IPS 等防护设备都有识别漏洞扫描器的能力，一旦发现后，可能第一时间触发报警或阻断 IP。因此信息收集和情报刺探是红队工作的基础，在数据积累的基础上，针对性地根据特定系统、特定平台、特定应用、特定版本，去寻找与之对应的漏洞，编写可以绕过防护设备的 EXP 来实施攻击操作，可以达到一击即中的目的。

现有的很多安全设备由于自身缺陷或安全防护能力薄弱，基本上不具备对这种针对性攻击进行及时有效发现和阻止攻击行为的能力。导致即便系统被入侵，红队获取到目标资料、数据后，被攻击单位尚未感知到入侵行为。此外由于安全人员技术能力薄弱，无法实现对攻击行为的发现、识别，无法给出有效的攻击阻断、漏洞溯源及系统修复策略，导致在攻击发生的很长一段时间内，对红队尚没有有效的应对措施。

红队专家在工作中，通常不会仅仅站在一个据点上去开展渗透工作，而是会采取不同的 Webshell、后门，利用不同的协议来

建立不同特征的据点。因为大部分应急响应过程并不能溯源攻击源头，也未必能分析完整攻击路径，缺乏联动防御。蓝队在防护设备告警时，大部分仅仅只处理告警设备中对应告警 IP 的服务器，而忽略了对攻击链的梳理，导致尽管处理了告警，仍未能将红队排除在内网之外，红队的据点可以快速“死灰复燃”；如果某些蓝队成员专业程度不高,缺乏安全意识,导致如针对 Windows 服务器应急运维的过程中，直接将自己的磁盘通过远程桌面共享挂载到被告警的服务器上行为，反而可以给红队进一步攻击蓝队成员的机会。

第四章　红队三十六计——经典攻击实例

古人带兵打仗讲三十六计，而红队实战亦是一个攻防对抗的过程，同样是人与人之间的较量，需要出谋划策、斗智斗勇。在这个过程中，有着“勾心斗角”、“尔虞我诈”，也有着勇往直前、正面硬刚。为此，我们精选了几个小案例，以三十六计为题向大家展现红队的常见攻击手法。

一、 浑水摸鱼——社工钓鱼突破系统

社会工程学（简称社工）在红队工作中占据着半壁江山，而钓鱼攻击则是社工中的最常使用的套路。钓鱼攻击通常具备一定的隐蔽性和欺骗性，不具备网络技术能力的人通常无法分辨内容的真伪；而针对特定目标及群体精心构造的鱼叉钓鱼攻击则可令具备一定网络技术能力的人防不胜防，可谓之渗透利器。

小 D 团队便接到这样一个工作目标：某企业的财务系统。通过前期踩点和信息收集发现，目标企业外网开放系统非常少，也没啥可利用的漏洞，很难通过打点的方式进入到内网。

不过还是让他们通过网上搜索以及一些开源社工库中收集到一批目标企业的工作人员邮箱列表。掌握这批邮箱列表后，小 D 便根据已泄露的密码规则、123456、888888 等常见弱口令、用户名密码相同，或用户名 123 这种弱口令等生成了一份弱口令字典。利用 hydra 等工具进行爆破，成功破解一名员工的邮箱密码。

小 D 对该名员工来往邮件分析发现，邮箱使用者为 IT 技术部员工。查看该邮箱发件箱，看到他历史发过的一封邮件如下：

标题：关于员工关掉 445 端口以及 3389 端口的操作过程

附件：操作流程.zip

小 D 决定浑水摸鱼，在此邮件的基础上进行改造伪装，构造钓鱼邮件如下。其中，zip 文件为带有木马的压缩文件。

标题：关于员工关掉 445 端口以及 3389 端口的操作补充

附件：操作流程补充.zip

为提高攻击成功率，通过对目标企业员工的分析，小 D 决定对财务部门以及几个跟财务相关的部门进行邮件群发。

小 D 发送了一批邮件，有好几个企业员工都被骗上线，打开了附件。控制了更多的主机，继而便控制了更多的邮箱。在钓鱼邮件的制作过程中，小 D 灵活根据目标的角色和特点来构造。譬如在查看邮件过程中，发现如下邮件：

尊敬的各位领导和同事，发现钓鱼邮件事件，内部定义为 19626 事件，请大家注意邮件附件后缀后.exe、.bat 等… …

小 D 同样采用浑水摸鱼的策略，利用以上邮件为母本，以假乱真构造以下邮件继续钓鱼：

尊敬的各位领导和同事，近期发现大量钓鱼邮件，以下为检测程序… …

附件：检测程序.zip

通过不断地获取更多的邮箱权限、系统权限，根据目标角色针对性设计钓鱼邮件，小 D 最终成功拿下目标！

二、 声东击西——混淆流量躲避侦察

在有蓝队（防守方）参与的实战攻防工作中，尤其是有蓝队排名或通报机制的工作中，红队与蓝队通常会产生对抗。IP 封堵与绕过、WAF 拦截与绕过、Webshell 查杀与免杀，红蓝之间通常会开展一场没有硝烟的战争。

小 Y 和所带领的团队就遭遇了这么一次：刚刚创建的跳板几

个小时内就被阻断了；刚刚上传的 Webshell 过不了几个小时就被查杀了。红队打到哪儿，蓝队就根据流量威胁审计跟到哪，不厌其烦，团队始终在目标的外围打转。

没有一个可以维持的据点，就没办法进一步开展内网突破。小 Y 和团队开展了一次头脑风暴，归纳分析了流量威胁审计的天然弱点，以及蓝队有可能出现的人员数量及技术能力不足等情况，制定了一套声东击西的攻击方案。

具体方法就是：同时寻找多个具有直接获取权限漏洞的系统，正面大流量进攻某个系统，吸引火力，侧面尽量减少流量直接拿权限并快速突破内网。

为此，小 Y 团队先通过信息搜集发现目标企业的某个外网 WEB 应用，并通过代码审计开展漏洞挖掘工作，成功发现多个严重的漏洞。另外发现该企业的一个营销网站，通过开展黑盒测试，发现存在文件上传漏洞。

小 Y 将团队兵分两路，除自己外的所有其他成员主攻营销网站，准备了许多分属不同 A 段的跳板，不在乎是否被发现，也不在乎是否封堵，甚至连漏洞扫描器都上了，力求对流量威胁分析系统开启一场规模浩大的“分布式拒绝服务”，让蓝队的防守人员忙于分析和应对；而自己则悄无声息地用不同的 IP 和浏览器指纹特征对 WEB 应用网站开展渗透，力求用最少的流量拿下服务器，让威胁数据淹没在营销网站的攻击洪水当中。

通过这样的攻击方案，小 Y 团队同时拿下营销网站和 WEB 应用网站，但在营销网站的动作更多，包括关闭杀软、提权、安置后门程序、批量进行内网扫描等众多敏感操作；同时在 WEB 应用网站利用营销网站上获得的内网信息，直接建立据点，开展内网渗透操作。

很快营销网站就被蓝方下线了，蓝队开始根据流量开展分析、溯源和加固工作；而此时小 Y 已经在 WEB 应用网站上搭建了 frp socks 代理，内网横向渗透拿下多台服务器，使用了多种协议木马，备份多个通道稳固权限，以防被防守方发现或直接踢出局。接续的几天服务器权限再未丢失，继续后渗透拿下域管理员、域控制器，最终拿下目标权限，工控设备权限等核心目标系统。

在渗透收尾的后期，小 Y 团队通过目标企业安全信息中心的员工邮件看到，蓝队此时依旧在对营销网站产生的数据报警做分析和上报防守战果等工作，然而此时该企业的目标系统其实早已经被红队拿下了。

三、 李代桃僵——旁路攻击搞定目标

其实在红队工作过程当中，也碰到过很多奇葩的事情：譬如有蓝队将整个网站的首页替换成了一张截图；有的将所有数据传输接口全部关闭了，然后采用 excel 表格的方式实现数据导入；有的将内网目标系统的 IP 做了限定，仅允许某个管理员 IP 访问等。

小 H 带领的红队就遇到类似的一次：目标企业把外网系统能关的都关了，甚至连邮件系统都做了策略，基本上没有办法实现打点和进入内网。

为此，小 H 团队通过充分信息收集后，决定采取“李代桃僵”的策略：既然母公司不让搞，那么就去搞子公司。然而工作过程中发现，子公司也做好了防护，而且基本上也关个遍。一不做，二不休，子公司不让搞，那么就搞子公司的子公司，搞它的孙公司。

于是，小 H 团队从孙公司下手，利用 sql 注入+命令执行漏洞成功进入(孙公司 A) DMZ 区。继续后渗透、内网横向移动控制

了孙公司域控、DMZ 服务器。在(孙公司 A)稳固权限后，尝试搜集最终目标内网信息、子公司信息，未发现目标系统信息。但发现(孙公司 A)可以连通(子公司 B)。

小 H 决定利用(孙公司 A)内网对(子公司 B)展开攻击。利用 tomcat 弱口令+上传漏洞进入(子公司 B)内网域，利用该服务器导出的密码在内网中横向渗透，继而拿下(子公司 B)多台域服务器，并在杀毒服务器获取到域管理员账号密码，最终获取(子公司 B)域控制器权限。

在(子公司 B)内做信息收集发现:（目标系统 x）托管在（子公司 C),（子公司 C）单独负责运营维护，而(子公司 B)内有 7 名员工与（目标系统 x）存在业务往来，7 名员工大部分时间在（子公司 C）办公，但办公电脑资产属于(子公司 B)，加入(子公司 B)的域，且办公电脑经常带回(子公司 B)。

根据收集到的情报信息，小 H 团队以(子公司 B)内的 7 名员工作为入口点，在其接入(子公司 B)内网时，利用域权限在其电脑种植木马后门。待其接入（子公司 C）内网时，继续通过员工计算机实施内网渗透，并获取（子公司 C）域控制权限。根据日志分析，锁定了（目标系统 x）管理员电脑，继而获取（目标系统 x）管理员登陆账号，最终获取（目标系统 x）控制权限。

四、 顺手牵羊——巧妙种马实施控制

红队永远不会像渗透测试那样，根据一个工作流程或者漏洞测试手册，按照规范去做就能完成任务。红队的工作永远是具有随机性、挑战性、对抗性的。在工作过程中，总会有各种出其不意的情况出现，只有能够随机应变，充分利用出现的各种机遇，才能最终突破目标完成任务，小 P 这次做的目标就是如此。

小 P 团队通过挖掘目标企业 OA 系统的 0Day 漏洞，继而获得

了 Webshell 权限。然而脚跟还没站稳，蓝队的管理员便发现了 OA 系统存在异常，对 OA 系统应用及数据库进行了服务器迁移，同时修复了漏洞。

本来是个很悲伤的事情，然而小 P 测试发现：蓝队虽然对 OA 系统进行了迁移并修复了漏洞，但是居然没有删除全部 Webshell 后门脚本。部分后门脚本仍然混杂在 OA 程序中，并被重新部署在新的服务器。攻击队依然可以连接之前植入的 Webshell，顺利提权，拿到了服务器权限。

拿到服务器权限后，小 P 团队发现蓝队的管理员居然连接到 OA 服务器进行管理操作，并将终端 PC 主机的磁盘全部挂载到 OA 服务器中。“既来之，则安之”，小 P 发现这是一个顺手牵羊的好机会。

小 P 团队小心翼翼地对管理员身份及远程终端磁盘文件进行确认，并向该管理员的终端磁盘写入了自启动后门程序。经过了一天的等待，蓝队管理员果然重启了终端主机，后门程序上线。在获取到管理员的终端权限后，小 P 很快发现，该管理员为单位运维人员，主要负责内部网络部署、服务器运维管理等工作。该管理员使用 MyBase 工具对重要服务器信息进行加密存储，攻击队通过键盘记录器，获取了 MyBase 主密钥，继而对 MyBase 数据文件进行了解密，最终获取了包括 VPN、堡垒机、虚拟化管理平台等关键系统的账号及口令。

最终，小 P 团队利用获取到的账号口令登录到虚拟化平台中，定位到演习目标系统的虚拟主机，并顺利获取了管理员权限。至此，工作正式完成！

五、 暗渡陈仓——迂回渗透取得突破

在有明确重点目标的实战攻防演习中，通常蓝队都会严防死

守、严阵以待，时时刻刻盯着从外网进来的所有流量，不管你攻还是不攻，他们始终坚守在那里。发现有可疑 IP 立即成段地封堵，一点机会都不留。此时，从正面硬刚显然不划算，红队一般会采取暗度陈仓的方式，绕过蓝队的防守线，从其他没有防守的地方去开展迂回攻击，小 M 这回遇到的就是这样一个硬骨头。

小 M 团队在确定攻击目标后，对目标企业的域名、ip 段、端口、业务等信息进行收集，并对可能存在漏洞目标进行尝试性攻击。结果发现大多数目标要么是都已关闭，要么是使用高强度的防护设备。在没有 0day 且时间有限情况下，小 M 决定放弃正面突破，采取暗度陈仓策略。

通过天眼查网站，小 M 了解到整个公司的子公司及附属业务分布情况，目标业务覆盖了香港、台湾、韩国、法国等地，其中香港包涵业务相对较多，极大可能有互相传送数据及办公协同的内网，故决定选择从香港作为切入点。

经过对香港业务进行一系列的踩点刺探，小 M 团队在目标企业的香港酒店业务网站找到一个 SA 权限的注入点，成功登陆后台并利用任意文件上传成功 getshell。通过数据库 SA 权限获取数据库服务器 system 权限，发现数据库服务器在域内且域管在登录状态。因服务器装有赛门铁克，因此采取添加证书的方式，成功绕过杀软并抓到域管密码，同时导出了域 hash 及域结构。

在导出的域结构中发现了国内域的机器，于是小 M 团队开始尝试从香港域向目标所在的国内域开展横向渗透。在国内域的 IP 段内找到一台服务器并 getshell，提权后抓取此服务器密码。利用抓取到的密码尝试登陆其他服务器，成功登陆到一台杀毒服务器，并在杀毒服务器上成功抓到国内域的域管密码。使用域管账号成功控制堡垒机、运维管理、vpn 等多个重要系统。

通过大量的信息收集，小 M 团队最终获得了渗透目标的 IP 地址，利用前期收集到的账号密码，成功登陆目标系统，并利用任意文件上传漏洞拿到服务器权限。

至此，整个渗透工作结束。

第五章　红队眼中的防守弱点

奇安信通过对政府、央企、银行、证券、民生、运营商、互联网等行业的红队实战工作，发现各行业安全防护具备如下特点：

一、 资产混乱、隔离策略不严格

除了大型银行之外，很多行业对自身资产情况比较混乱，没有严格的访问控制（ACL）策略，且办公网和互联网之间大部分相通，可以直接使远程控制程序上线。

除了大型银行与互联网行业外，其他很多行业在 DMZ 区和办公网之间不做或很少做隔离，网络区域划分也不严格，给了红队很多可乘之机。

此外，几乎所有行业的下级单位和上级单位的业务网都可以互通。而除了大型银行之外，其他很多行业的办公网也大部分完全相通，缺少必要的分区隔离。所以，红队往往可以轻易地实现实施从子公司入侵母公司，从一个部门入侵其他部门的策略。

二、 通用中间件未修复漏洞较多

通过中间件来看，Weblogic、Websphere、Tomcat、Apache、Nginx、IIS 都有使用。Weblogic 应用比较广泛，因存在反序列化漏洞，所以常常会被作为打点和内网渗透的突破点。所有行业基本上都有对外开放的邮件系统，可以针对邮件系统漏洞，譬如跨站漏洞、XXE 漏洞等来针对性开展攻击，也可以通过钓鱼邮件和鱼叉邮件攻击来开展社工工作，均是比较好的突破点。

三、 边界设备成为进入内网的缺口

从边界设备来看，大部分行业都会搭建 VPN 设备，可以利用 VPN 设备的一些 SQL 注入、加账号、远程命令执行等漏洞开展攻

击，亦可以采取钓鱼、爆破、弱口令等方式来取得账号权限，最终绕过外网打点环节，直接接入内网实施横向渗透。

四、 内网管理设备成扩大战果突破点

从内网系统和防护设备来看，大部分行业都有堡垒机、自动化运维、虚拟化、邮件系统和域环境，虽然这些是安全防护的集中管理设备，但往往由于缺乏定期的维护升级，反而都可以作为开展权限扩大的突破点。

附录 奇安信红队能力及攻防实践

自 2016 年奇安信集团协助相关部委首次承办网络实战攻防演习以来，这种新的网络安全检验模式已经有了长足的发展。

仅 2019 年上半年，奇安信就参与了全国范围内 60 多场实战攻防演习的红队活动，攻破了 200 余个目标系统。累计派出红队 85 支次、投入红队专家 246 人次、投入工作量 1793 人天。项目涵盖党政机关、公安、政企单位、民生、医疗、教育、金融、交通、电力、银行、保险、能源、传媒、生态、水利、旅游等各个行业。在实战演习过程中，奇安信集团派遣最优秀的红队高手全力参与工作，并在所有行业化的实战攻防演习排名中均列前 2 位，其中排名第 1 的次数高达 75%，是业内公认的红队王者。

在协助国家主管机关的工作中，针对等级保护重要信息系统以及国家关键基础设施，深入开展实战攻防工作，使得国家相关重点信息系统的整体安全性有了显著提高和可靠保障；在协助央、国企单位工作中，对企业本级以及下级单位的重点网络信息系统、敏感系统、工控系统，进行全面的红队渗透攻击，极大地提升了各级单位应对网络安全突发事件能力，大幅度提高了相关网络及系统的防护水平。

如今，奇安信集团已组建起 10 余支技术高强、能力突出的网络红队，聘请具备 APT 高级渗透实战经验的专职攻防专家 30 余人，是目前国内规模最大、人数最多的红队队伍。

实战攻防是个对抗的过程，无论对抗中的攻还是防，其目的都是为了提升网络的安全防护能力，加强安全应急的响应处置能力。奇安信集团将肩负“让网络更安全、让世界更美好”的使命，以攻促防，为提升网络安全水平贡献力量。