## 以攻促防：企业蓝军建设思考

**01 高悬的达摩克利斯之剑**



2017年4月，黑客组织Shadow Brokers公布一批美国国家安全局（NSA）的网络漏洞军火库。背靠国家，NSA拥有强大的通杀型0day漏洞挖掘和利用能力，这批漏洞库指哪打哪，堪称军火库中的核武器，其中就包含Windows永恒之蓝漏洞利用工具。军火库的泄露也造成了核武器平民化，被黑产利用来传播勒索蠕虫病毒。还记得WannaCry肆虐的景象吗？全球数百万台电脑包括大型企业、政府机构都受攻击，威力可见一斑。

而这只是无数攻击案例中的一个。

”

人们在享受网络技术发展带来的便利时，鲜少能意识到头上高悬的达摩克利斯之剑——**安全**。层出不穷的漏洞越发多样化，这把剑高悬在我们头顶摇摇欲坠，没有什么防护手段可以一劳永逸一招制敌，任何疏忽大意都可能给黑客提供可乘之机。

然而具体到单个企业层面，自身安全事故却相对低频，且在业务层面极少有直接感知。尚未发生事故，或者说攻击没有直接造成损失，很可能会给人带来安全防护足够完善、业务数据足够安全的错觉，甚至导致防护手段逐渐落后，安全流程越发陈旧，人员意识日益懈怠。

等到那把剑真的掉落之时，一切都将为时太晚。

**02 从大到强的试炼之路**



这也解释了为什么近年来全球安全事故频发，国内外都极为重视网络安全。正如国家提出，**没有网络安全就没有国家安全**。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，是把我国从网络大国建设为网络强国的关键。

但并不是所有漏洞都能通过自动化工具检测发现。因此，国内外都在如火如荼地开展国家网络安全实战演练。中国公安部组织的护网行动集结全国优秀渗透测试工程师开展风险可控的攻击演习，美国国土安全部组织的Cyber Storm也每两年开展一次网络安全实战演练。

从大到强，网络安全实战演练必不可少。它是网络安全建设的试金石和助燃器，是检验企业安全防护水平的试炼之地。只有持续暴露网络安全防护、监测和应急处置的缺陷并优化改进，才能抵挡黑客不断变换的猛烈攻击。

**那么问题来了，谁来引领这条“试炼之路”呢？**

对于腾讯这样体量庞大，业务繁多，拥有海量数据资产公司而言，需要一支既了解公司业务，又能够以黑客视角持续渗透公司资产的内部攻击队伍，这样才会更容易意识到公司各项安全隐患，把风险消弭于萌芽之前。

腾讯蓝军，就此应运而生。



**03 当我们谈蓝军时，我们在谈些什么？**



蓝军这个概念，其实军事领域早已有之。

国内蓝军扮演假想敌（即敌方部队），与红军（我方正面部队）开展实战演习，帮助红军查缺补漏，提升作战能力。网络安全红蓝对抗的概念也源自于此，通过开展APT高级持续性威胁攻击演习来全方位检验企业的安全稳健性和威胁监测及响应能力。

红军作为企业防守方，通过安全加固、攻击监测、应急处置等手段来保障企业安全，而蓝军作为攻击方，以发现安全漏洞，获取业务权限或数据为目标，利用各种攻击手段，试图绕过红军层层防护，达成既定目标。需要注意，欧美采用红队（Red Team）代表攻击方，蓝队（Blue Team）代表防守方，颜色代表正好相反，常常容易让大家搞混。

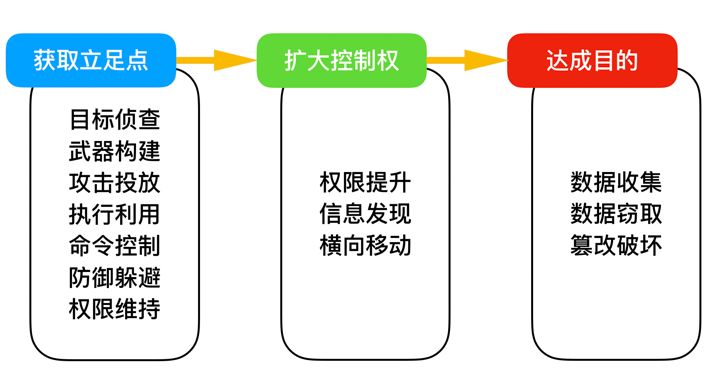
企业网络蓝军工作内容主要包括**"渗透测试（Penetration Testing）"和"红蓝对抗（Red Teaming）**"，其实所使用的攻击技术大同小异，主要区别在侧重点不同。渗透测试侧重尽量用较短的时间去挖掘尽可能多的安全漏洞，一般不太关注攻击行为是否被监测发现，即便被发现也不会立刻遭拦截，**目的是帮助业务系统暴露和收敛更多风险**。红蓝对抗相反，通常采用背靠背方式贴近真实攻击，侧重绕过防御体系，毫无声息达成获取业务权限或数据的目标，不求发现全部风险点，因为攻击动作越多被发现的概率越大，一旦被发现，红军就会把蓝军踢出战场，**目的是检验在真实攻击中纵深防御能力、告警运营质量、应急处置能力**，当然这过程中也会发现业务系统安全漏洞。

腾讯蓝军（Tencent Force）由腾讯TEG安全平台部于2006年组建。彼时自动化漏洞检测能力还比较弱，更多的安全漏洞得靠人肉发现，在这个背景下，腾讯蓝军正式成立，从此捷报频传，十余年专注于前沿安全攻防技术研究、实战演练、渗透测试、安全评估、培训赋能等，采用攻击者视角在真实网络环境开展实战演习，检验安全防护策略、响应机制的充分性与有效性，并推动优化提升。

**可见，当我们谈蓝军时，我们在谈的绝不仅仅只是单纯的模拟黑客，而是环环相扣的周密筹划，缜密侦查、精心设计，以及针对性的防守建议等等。**

**04 环环相扣，浅析网络攻击杀伤链**



想要了解蓝军的整个攻击生命周期，可以通过网络攻击杀伤链来进行：首先通过多种手段获取立足点，在此基础上通过权限提升、信息发现和横向移动扩大控制权，最后达成数据收集、窃取和篡改破坏等目的。

**下面结合腾讯蓝军十多年的攻防实战演练经验，试对各个阶段的攻击手法与技术简要分析如下：**

01第一阶段：获取立足点

**目标侦查：**利用一系列侦查手段获取目标的资产、人员、环境等信息，为实施攻击提供基础信息支持，信息的全面性和准确性很大程度确定攻击的路径、战果和效率。比如通过DNS域传送漏洞、域名注册信息反查、域名枚举等手段获取域名资产信息，通过域名解析、网段扫描等手段获取IP资产信息，通过网站扫描、端口探测等手段获取程序指纹信息，通过在搜索引擎、社交网站、网盘、Github等平台检索以及社工欺骗等手段获取组织架构、员工信息、源代码、账户密码、常用软件、常上网站、安全防护策略、外包服务供应商等信息，通过实地考察获取职场和机房的网络、门禁、办公等环境信息。

**武器构建**：根据前期收集到的信息，针对性制作攻击代码。如果尝试对HR进行攻击，那么可以设计植入木马的简历文档，如果计划从线上服务入手，可以通过自动化扫描、人工测试等手段对目标资产进行漏洞探测，发现可利用的0day漏洞。在目前公开的APT案例中，至少有80%是从攻击员工办公电脑入手，因为人是系统最大的漏洞，利用社会工程学的攻击成功率高，同时攻陷员工电脑后更容易摸清内部网络及扩大控制范围。

**攻击投放**：利用各种手段将攻击载荷投递到目标。比如利用命令注入、文件上传、SQL注入、SSRF、XSS、溢出等漏洞直接远程攻击线上服务，利用邮件钓鱼、U盘摆渡攻击、水坑攻击、软硬件供应链攻击、网络劫持等方式入侵服务器、员工电脑、网络设备。

**执行利用**：不同环境采用不同的执行方式，在受限环境可利用系统组件或合法程序执行加载恶意代码，从而突破系统限制或隐藏自身，达到木马顺利运行的目的。比如在Windows环境使用系统内置程序PowerShell执行脚本，恶意代码仅存在于内存中，文件不落地，类似可使用的执行方式非常多。

**命令控制**：建立具有各种隐蔽级别的通道来操控目标设备或进入目标内网。比如通过WebShell（如Caidao、Weevely）、Reverse Shell（如Bash/Python/PowerShell）、远控木马RAT（如Cobalt Strike/Metasploit Meterpreter）、远程桌面访问软件（如TeamViewer/VNC），使用多层代理、传输加密、端口复用、Domain Fronting等方式、采用TCP/UDP/HTTP/HTTPS/DNS/ICMP/SMTP等网络协议，甚至模仿其他正常应用通信流量，做到实时监控和遥控目标设备；通过端口转发（如netsh/iptables）、Socks代理（如ssh -D）、HttpTunnel（如reGeorg）、企业VPN通道等方式穿透企业内网，突破网络边界。

**防御躲避**：利用检测对抗技术、攻击痕迹清除等方式逃避入侵检测、杀毒软件等安全系统的发现和追溯。比如使用肉鸡发起攻击避免暴露黑客真实IP，构造畸形请求包绕过WAF，将恶意代码注入到正常合法进程/文件内，利用白名单、反调试、无文件等手段绕过病毒检测（如使用知名企业合法数字证书给恶意程序签名），清除或破坏应用访问/系统登陆操作日志，降低行为活动频率等等。

**权限维持**：通过劫持合法程序、驻留系统自启动后门、创建隐藏管理员账户等方式实现长期控制，即使系统重启或重装也不会消失。比如替换系统辅助功能（如放大镜、软键盘）、劫持动态连接库、利用Windows服务启动项/Linux定时任务crontab配置随系统自启动、设置suid特权程序、安装bootkit木马、盗用原有合法账户密码等等。

02第二阶段：扩大控制权

**权限提升：**利用系统弱点或配置不当等方式获取超级管理员级别权限。比如利用最新Windows/Linux内核提权漏洞，管理员权限运行的第三方软件存在漏洞可利用，管理员权限定时执行的程序文件因权限设置不当致使普通用户也可篡改程序，管理员密码随意存放在服务器普通文件里等等。

**信息发现**：通过本地搜索、内网扫描和嗅探等方式确认已可以获取或控制的数据及进一步了解内部网络和可能利用的风险点。比如通过本机翻箱倒柜获取用户列表、进程列表、网络连接、配置文件、程序代码、数据库内容、运维操作记录、系统账户密码、浏览器保存密码、邮件内容等信息；通过内存导出、键盘记录、网络嗅探获取用户凭据；通过查询Windows域全部账户和主机，分析出企业完整的组织机构/人员、重要机器等信息；通过内网主机存活探测、远程服务探测描绘出内网结构拓扑图、内网应用服务以及可能的风险点；通过访问内部OA网站尤其是知识分享平台获取业务架构、代码、服务器等信息。

**横向移动**：通过内网渗透攻击获取更多服务器权限和数据。一般来说黑客偏爱攻击拥有企业网络、机器、数据相关管理权限的系统，比如说Windows域控、补丁服务器、邮箱系统、内部即时通讯工具、跳板机、运维运营平台、密码系统、代码管理平台等，道理很简单，一旦攻破这些系统就几乎能够控制全部机器，进而获取目标业务数据；黑客也喜欢攻击企业高管、目标业务员工、网络管理员的电脑，因为这些人员掌握的信息更重要，也更接近黑客目的。其中一种常见的内网渗透思路是由于大多数企业内部网络隔离精细度不足（尤其是大型企业服务器数量太多，隔离成本大），内网站点安全性低（重点防御外部攻击，内部系统安全投入少），内网高危应用服务没有鉴权认证（比如Docker/Kubernetes/Redis/Hadoop等应用在未鉴权的情况下可造成服务器直接被入侵控制，不少人以为内网很安全所以没有开启鉴权），服务器帐号密码普遍通用（为了方便管理甚至全部服务器密码都一样），这些情况可以让黑客在内网渗透时很轻易获取到一些服务器的控制权限，然后逐一登陆服务器抓用户登陆凭证（一台服务器存在多个账户），再使用这些凭证尝试登陆其他服务器，若登陆成功后又继续抓其他用户登陆凭证，这些新拿到的凭证又可能可以登陆其他服务器，通过反复尝试登陆、抓取凭证这一经典套路，逐步扩大服务器控制范围，最终甚至可能做到全程使用合法用户凭证登陆任意服务器，就好似运维管理员正常登陆进行运维一样。

03第三阶段：达成目的

**数据收集**：搜集源代码、数据库、资产信息、技术方案、商业机密、邮件内容等攻击目标数据。

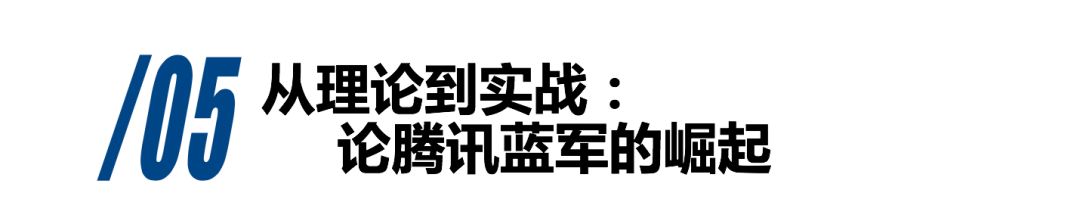
**数据窃取**：对数据进行加密、压缩、分段处理，通过HTTP(S)/FTP/DNS/SMTP等网络协议主动对外传送、使用Web对外提供访问下载、物理U盘拷贝，或业务接口直接查询回显等方式将数据传输到黑客手中。

**篡改破坏**：通过修改数据进行非法获利，摧毁数据进行打击报复等。

具体攻击手法非常多，不是每次攻击都会涉及到方方面面。比如说攻击目的是获取某系统数据，假设该系统本身存在SQL注入漏洞，那直接从外网利用SQL注入漏洞获取数据就能达成目的，不用考虑那么多复杂的攻击手法，黑客会根据目的和现状倒推出最佳手段，而不是盲目开展。

安全演习也是如此，根据演习诉求和目的按需开展。MITRE ATT&CK攻击矩阵是一个基于全球APT组织真实入侵事件中整理出攻击战术、技术和过程的知识库，很有参考价值，不过有些操作实例不够详实，我们进行了细化和扩展，后续也会持续分享出来。

**05 从理论到实战：论腾讯蓝军的崛起**



古人云，纸上得来终觉浅，绝知此事要躬行。上文详述了网络攻击杀伤链，腾讯蓝军成军十余载，正是一个从理论到实战，从纸上到躬行的过程。

**自2006年成军以来，**我们对QQ、QQ空间、微信、支付、小程序、腾讯云、游戏等重要业务都开展过渗透测试，发现并消除了大量潜在安全风险。去年公司大力推进自研业务上云，安全平台部为自研上云提供安全规范、安全防护、安全评估、安全情报、安全检测等一整套安全解决方案和服务，蓝军也紧跟发展步伐，重点对多个腾讯云基础组件开展渗透测试，提升腾讯云的整体安全性。

**2008年，**腾讯自主研发的服务器安全系统（代号“洋葱”）正式上线，蓝军开启APT红蓝对抗演练，每年开展数十次演习持续助力提升检测能力。APT红蓝对抗演习分成两种模式，一种是**策略场景反向验证**，侧重检验策略的覆盖深广程度和有效性，蓝军梳理各种攻击场景尽可能全面的攻击手法，包括网上已经公开和自己研究具有对抗意义的技术，不定期在测试环境进行批量演练，在生产环境进行突袭演练。另一种是**以获取服务器或数据控制权限为目标的完整攻击演习**，侧重检验在真实攻击中纵深检测能力、告警运营质量、应急处置能力以及业务安全状况。重要业务的外网安全防护往往比较强，直接攻击的难度大，而一部分安全投入少的业务和安全意识薄弱的人员就成为了黑客的突破口，首先黑进内网，然后渗透内网，间接攻击重要业务。蓝军陆续对重要业务和基础IT设施展开多次渗透，帮助提升内网的安全防护能力和攻击检测能力。商业间谍/内鬼往往天然拥有一些合法权限，潜伏久了也可能了解到一些安全检测策略，所以这些也是蓝军扮演的角色，帮助公司增强监控和审计能力。

**2015年，**蓝军和DDoS防护团队（“宙斯盾”）联合全面梳理DDoS防护算法覆盖场景，对宙斯盾开展多次DDoS攻击演习检验，发现多项防护算法缺陷，之后结合业务场景和行业发展针对性的配合优化，明显提升了宙斯盾的服务质量。

**2016年，**蓝军涉足风控安全，对腾讯前端风控安全开展多次红蓝对抗，提供大量优化建议和方向，帮助完善构建了基于前端的风控能力（腾讯防水墙了解一下）。

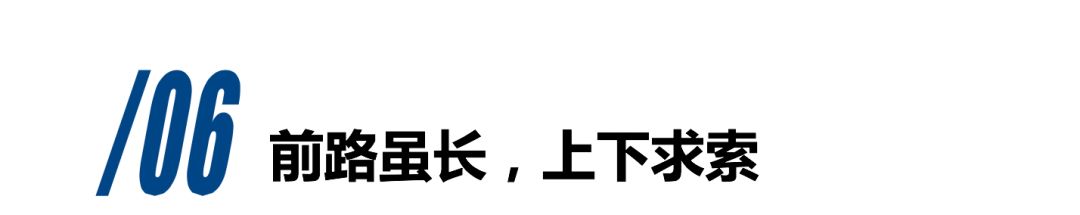
**2018年，**蓝军正式对外赋能，应数字广东、腾讯云的要求，蓝军对数字广东开展红蓝对抗演习，蓝军从远程渗透外网站点、员工钓鱼邮件攻击、抵达办公职场展开物理攻击等方面发起攻击发现多个安全风险，助力数字广东提高安全加固和防护能力。同时，在公安部去年组织的贵阳大数据及网络安全攻防演练活动中，由数字广东安全、腾讯云安全、科恩、腾讯IT、安平组成的蓝军联合团队凭借可攻可守的能力，进攻时获得了最高分，防守时保障靶标一直到演练结束都没有被攻破，成为唯一没被攻破的红色靶标，也荣获“技术创新一等奖”。

经过多年激烈的红蓝对抗演习，红蓝双方你追我赶，相互促进，公司安全防护体系有着非常大的提升，服务器安全系统（“洋葱”）、DDoS防护系统（“宙斯盾”）、Web应用防火墙（“门神”）、Web漏洞检测系统（“洞犀”）等公司安全系统的技术能力都取得了不错的提升。在腾讯产业互联网大战略下，这些系统也在进行沉淀总结，将十余年的安全积累输出到第三方用户，如联合腾讯云安全团队共同打造的大禹DDoS防护产品、护航“一部手机游云南”的洞悉产品、腾讯云红蓝对抗专家服务等，如检测覆盖网络攻击杀伤链各环节的“洋葱”对外也推出了产品化版本等。

另外在2012年成立的腾讯安全应急响应中心（TSRC），借助外部安全研究员/情报员的力量，鼓励在安全可靠的前提下和我们并肩作战，发现腾讯外网业务安全隐患和防护缺陷，至今有国内外数万名参与进来，这可以认为是腾讯蓝军的扩展延伸。在这里也非常感谢外部力量对我们的帮助。

热烈欢迎各位渗透测试/红蓝对抗专家投递简历加入我们，或者成为腾讯安全白帽，和我们一起守护亿万用户安全。

**06 前路虽长，上下求索**



网络安全的本质在对抗，对抗的本质在攻防两端能力较量，但攻防从来都是不对等的，攻击方优势远大于防御方，蓝军的存在就是帮助消灭不对等。首先，企业网络蓝军与国家级APT组织相比，在人力、物力、财力等资源投入存在非常大的悬殊，蓝军如何持续及时掌握最新APT攻击技术是非常有挑战的事情。其次，攻击场景众多以及业务需求旺盛，需要开展的演练工作非常多，人力有限的蓝军如何高效完成使命也非常有挑战。

相信未来会有更多企业建设网络蓝军，投入更多资源研究前沿APT攻击技术，以及建设更智能的蓝军自动化攻击平台提高演习效率。我们也会把实战演练中的技术心得、攻防思考等第一时间分享出来，敬请关注腾讯蓝军官方网站https://force.tencent.com/。

原文链接：https://mp.weixin.qq.com/s/8iJs2ON66NY1Jdbt7c-BTA