奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

红蓝紫实战攻防

演习手册

THE PRACTICAL PLAYBOOK OF OFFENSE & DEFENSE
BY RED-BLUE-PURPLE TEAM

奇安信安服团队 奇安信行业安全研究中心 ◎著

1900+个目标系统攻破实战

520+家政企机构协同作战

2300+个业务系统隐患排除

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 2020 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、团队社工、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防能力？这已经成为大型政企机构运营者所关心的重要问题。

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220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防能力。

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，红蓝双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，在实际的攻防演习中，有将红队作为攻击队的，也有将蓝队作为攻击队的。在本系列丛书中，我们依据国内最新的相关工作实践要求，统一将攻击队命名为蓝队，将防守队命名为红队，而紫队则代表组织演习的机构。

《蓝队视角下的防御体系突破》是本系列丛书的第一册。本册希望通过归纳总结蓝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”。

《红队视角下的防御体系构建》是本系列丛书的第二册。本册希望通过归纳总结红队防御的四个阶段、应对攻击的常用策略，以及建立实战化安全体系的基本方法，帮助政企机构查找薄弱环节，更好地提升演

习水平，构筑更有效的安全防御体系。

《紫队视角下的实战攻防演习组织》是本系列丛书的第三册。本册重点介绍实战环境下的紫队工作，提出如何组织一场有效的实战攻防演习、如何组织在演习过程中的应急事件演练、如何组织对无法开展实战演习关基设施的沙盘推演。

目 录

蓝队视角下的防御体系突破

红队视角下的防御体系构建

紫队视角下的实战攻防演习组织

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

蓝队视角下的
防御体系突破

THE PRACTICAL PLAYBOOK OF OFFENSE BY BLUE TEAM

奇安信安服团队 奇安信行业安全研究中心 ◎著

244场蓝队攻击演习经验

1900余个目标系统攻破实战

6685人日累计投入

第一章 什么是蓝队

蓝队，在本书中是指网络实战攻防演习中的攻击一方。

蓝队一般会采用针对目标单位的从业人员，以及目标系统所在网络内的软件、硬件设备同时执行多角度、全方位、对抗性的混合式模拟攻击手段；通过技术手段实现系统提权、控制业务、获取数据等渗透目标，来发现系统、技术、人员、管理和基础架构等方面中存在的网络安全隐患或薄弱环节。

蓝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；而蓝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；但蓝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，蓝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。

蓝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；而蓝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，而蓝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），而蓝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蓝队的攻击手法，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，蓝队通常会以3人为一个战斗小组，1人为组长。组长通常是蓝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）、情报收集或武器研制等某一方面或几个方面的专长。

蓝队工作对其成员的能力要求往往是综合性的、全面性的。蓝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 蓝队演变趋势

“魔高一尺道高一丈”！防守能力提升的同时，攻击能力也在与时俱进。目前，蓝队的工作已经变得非常体系化、职业化和工具化，主要表现如下。

1）体系化

从漏洞准备、工具准备，到情报收集、内网渗透等，每个人都有明确的分工，有组织的形成团队作战能力，已经很少再有一个人干全套的情况了。

2）职业化

蓝队人员都来自各组织专职实战演习团队，有明确分工和职责，具备协同配合的职业操守，平时开展专业化训练。

3）工具化

工具专业化程度持续提升，除了使用常用渗透工具，基于开源代码的定制化工具应用增多，自动化攻击被大规模应用，如采用多 IP 出口的自动化攻击平台进行作业。

从实战对抗的手法来看，现如今的蓝队还呈现出社工化、强对抗和迂回攻击的特点。

1）社工化

利用“人”的弱点实施社会工程学攻击，是黑产团伙和高级威胁组织的常用手段，如今也被大量引入实战攻防演习当中。

除了钓鱼、水坑等传统社工攻击手法外，如今的蓝队还会经常通过在线客服、私信好友等多种交互平台进行社工攻击，以便更加高效的获取业务信息。社工手段的多变性往往会让防守方防不胜防。

2）强对抗

利用 0Day 漏洞、NDay 漏洞、免杀技术等方式与防守方进行高强度的技术对抗，也是近 1—2 年来蓝队在实战攻防演习中表现出的明显特点。特别的，蓝队人员大多出自安全机构，受过专业训练，因此往往会比民间黑客更加了解安全软件的防护机制和安全系统的运行原理，其使用的对抗技术也往往更具针对性。

3）迂回攻击

对于防护严密，有效监控的目标系统来说，正面攻击往往难以奏效。这就迫使蓝队越来越多的采用“曲线救国”的攻击方式，将战线拉长：从目标系统的同级单位和下级单位下手，从供应链及业务合作方下手，在防护相对薄弱的关联机构中寻找突破点，通过迂回攻击的方式攻破目标系统。

第三章 蓝队四板斧
——攻击的四个阶段

蓝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，蓝队的工作可分·为四个阶段：战前准备、情报收集、建立据点和横向移动。我们也常将这个四个阶段称为蓝队工作的“四板斧”。

一、第一阶段：准备阶段

在一场实战攻防演习作战开始前，蓝队人员主要会从以下几个方面来进行准备。

1）漏洞挖掘

漏洞一直是第一攻击力。前期的漏洞准备对于打开突破口显得非常重要，在实战中，漏洞挖掘工作一般会聚焦于互联网边界应用、网络设备、办公应用、运维系统、移动办公、集权管控等方面。此外，只是找到漏洞还不够，好的漏洞的利用方法也十分重要的。想要在不同的环境下达到稳定、深度的漏洞利用，这对漏洞挖掘人员来说是一个不小的挑战。

2）工具储备

工具的目的是为了提升工作效率，好的工具往往

能事半功倍，实战中，蓝队通常需要准备信息收集、钓鱼、远控、WebShell 管理、隧道、扫描器、漏洞利用等多种工具。

3）战法策略

团队作战考虑的是配合，因此，攻击队成员的分工角色就显得尤为重要，小的战役靠个人，大的战役一定是靠机制、流程以及团队合作。好的战法策略，对于一场大的战役来讲至关重要。

4）以赛代练

日常的任务中，需要挑选出一些具有代表性的任务来对蓝队进行有针对性的训练，有利于蓝队队员提高自身的技能。参加各类安全大赛将非常有助于蓝队队员的技术能力提升。

二、第二阶段：情报收集

当蓝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就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。收集的内容包括目标系统的组织架构、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、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，一般取决于安全防护的薄弱环节究竟在哪里，以及蓝队对攻击路径的选择。

三、第三阶段：建立据点

在找到薄弱环节后，蓝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，蓝队专家会尝试绕过 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，寻找和内网连通的通道，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），蓝队专家会继续撕口子，直到找到接入内网的点为止。

当蓝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，蓝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。

四、第四阶段：横向移动

进入内网后，蓝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，蓝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，或者用 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，蓝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。

第四章 蓝队也套路
——常用的攻击战术

在蓝队的实战过程中，蓝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。

下面介绍九种蓝队最常用的攻击战术。

一、利用弱口令以及通用口令

弱密码、默认密码、通用密码和已泄露密码通常是蓝队专家们关注的重点。实际工作中，通过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黑产交易的社工库中；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、利用互联网边界渗透内网

大部分企业都会有开放于互联网边界的设备或系统，如：VPN 系统、虚拟化桌面系统、邮件服务系统、官方网站等。正是由于这些设备或系统可以从互联网一侧直接访问，因此也往往会成为蓝队首先尝试的，突破边界的切入点。

此类设备或系统通常都会访问内网的重要业务，为了避免影响到员工使用，很多企业都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如果缺乏审计，也未采用多因子认证；员工平时又经常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。那么，当掌握相关员工的邮箱账号密码后，在邮件中所获得的信息，会给蓝队下一步工作提供很多方便。

三、利用通用产品组件漏洞

信息化的应用提高了工作效率，但其存在的安全漏洞也是蓝队人员喜欢的。历年实战攻防演习中，经常被利用的通用产品漏洞包括：邮件系统漏洞、OA 系统漏洞、中间件软件漏洞、数据库漏洞等。这些漏洞被利用后，可以使攻击方快速获取大量账户权限，进而控制目标系统。而作为防守方，漏洞利用往往很难被发现，相关活动常常被当作正常业务访问而被忽略。

四、利用安全产品 0Day 漏洞

安全产品自身也无法避免 0Day 攻击！！！安全产品也是一行行代码构成，也是包含了操作系统、数据库、各类组件等组合而成的产品。历年攻实战防演习中，被发现和利用的各类安全产品 0Day 漏洞，主要涉及安全网关、身份与访问管理、安全管理、终端安全等类型安全产品。这些安全产品的漏洞一旦被利用，可以使攻击方突破网络边界，获取控制权限进入网络；获取用户账户信息，并快速拿下相关设备和网络的控制权限。

安全产品的 0Day 漏洞常常是蓝队最好的攻击利器。

五、利用人性弱点社工钓鱼

利用人的安全意识不足或安全能力不足，实施社会工程学攻击，通过钓鱼邮件或社交平台进行诱骗，是蓝队专家经常使用的社工手法。在很多情况下，“搞人”要比“搞系统”容易得多。

钓鱼邮件是最经常被使用的攻击手法之一。蓝队专家常常会首先通过社工钓鱼或漏洞利用等手段盗取某些安全意识不强的员工邮箱账号；再通过盗取的邮箱，向该单位的其他员工或系统管理员发送钓鱼邮件，

骗取账号密码或投放木马程序。由于钓鱼邮件来自内部邮箱，“可信度”极高，所以，即便是安全意识较强的IT人员或管理员，也很容易被诱骗点开邮件中钓鱼链接或木马附件，进而导致关键终端被控，甚至整个网络沦陷。

冒充客户进行虚假投诉，也是一种常用的社工手法，攻击方会通过单人或多人配合的方式，通过在线客服平台、社交软件平台等，向客服人员进行虚假的问题反馈或投诉，设局诱使或迫使客服人员接收经过精心设计的带毒文件或带毒压缩包。一旦客服人员的心理防线被突破，打开了带毒文件或压缩包，客服人员的电脑就会成为攻击队打入内网的一个“立足点”。

除了客服人员外，很多非技术类岗位的工作人员也都很容易成为社工攻击的“外围目标”。例如，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，都是比较常用的社工方法。而且往往“百试百灵”。

六、利用供应链隐秘攻击

供应链攻击是迂回攻击的典型方式。攻击方会从IT（设备及软件）服务商、安全服务商、办公及生产服务商等供应链机构入手，寻找软件、设备及系统漏洞，

发现人员及管理薄弱点并实施攻击。常见的系统突破口包括：邮件系统、OA系统、安全设备、社交软件等；常见的突破方式包括软件漏洞，管理员弱口令等。

利用供应链攻击，可以实现第三方软件系统的恶意更新，第三方服务后台的秘密操控，以及物理边界的防御突破（如，受控的供应商驻场人员设备被接入内网）等多种复杂的攻击目标。

七、利用下属单位迂回攻击

在有红队防守的实战攻防演习中，有时总部的系统防守会较为严密，蓝队很难正面突破，很难直接撬开进入内网的大门。此时，尝试绕过正面防御，通过攻击防守相对薄弱的下属单位，再迂回攻入总部的目标系统，就是一种很“明智”的策略。

蓝队在大量实战中发现：绝大多数政企机构，其下属单位之间的内部网络，下属单位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、大型央企都习惯于使用单独架设的一条专用网络，来打通各地区之间的内网连接，但同时又普遍忽视了不同区域内网之间必要的隔离管控措施，缺乏足够有效的网络访问控制。

这就导致蓝队一旦突破了子公司或分公司的防线，便可以通过内网进行横向渗透，直接攻击到集团总部，或是漫游整个企业内网，进而攻击任意系统。

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，就可以毫无阻拦地进入到总部网络中来。事实上，A子公司与B子公司可能仅需要访问北京总部的部分业务系统；同时，A与B之间则可能完全不需要有任何业务上的往来。那么，从安全角度看，就应该严格限制A与B之间的网络访问。但实际情况常常是：一条专线内网通往全国各地，一处沦陷，处处沦陷。

八、秘密渗透

不同于民间黑客或黑产团伙，蓝队工作一般不会大规模使用漏洞扫描器，因为扫描活动特征明显，很容易暴露自己。例如，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蓝队工作的基础。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

达到隐秘攻击、一击即中的目的。

如果目标系统的防御纵深不够，或使用安全设备的能力不足，当面对这种针对性攻击时，往往就很难及时发现和阻止攻击行为。在攻防演习的实战中，常常使蓝队获取到目标资料和数据后，被攻击单位尚未感知到入侵行为。

如果参与演习的安全人员本身的技术能力也比较薄弱，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，则在攻击发生的很长一段时间内，防守一方可能都不会对蓝队的隐秘攻击采取有效的应对措施。

九、多点潜伏

蓝队专家在工作中，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，使用不同的后门程序，利用不同的协议来建立不同特征的据点。

事实上，大部分的应急响应过程并没有溯源到攻击源头，也未必能分析完整攻击路径。在防护设备告警时，很多防守方队员会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，从而导

致尽管处理了告警，但仍未能将蓝队排除在内网之外。而蓝队则可以通过多个潜伏据点，实现快速的“死灰复燃”。

如果某些防守方成员专业程度不高，安全意识不足，还有可能在蓝队的“伏击”之下暴露更多敏感信息。例如，在针对 Windows 服务器应急运维的过程中，有的防守方队员会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。这样做反而可以给秘密潜伏的蓝队进一步攻击防守方成员的机会。

第五章 蓝队三十六计
——经典攻击实例

古人带兵打仗讲三十六计。而蓝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更加具体的展现蓝队的常见攻击手法。

一、正面突破——跨网段控制工控设备

某企业为国内某大型制造业企业，内部生产网大量使用双网卡技术实现网络隔离。在本次实战攻防演习活动中，攻击队的目标是：获取该企业工控设备控制权限。

经过前期的情报收集与分析，攻击队制定了首先突破办公网，再通过办公网渗透进入工控网的战略部署。

1）突破办公内网

攻击队首先选择将该企业的门户网站作为突破口，并利用一个 0Day 漏洞获取了该门户网站应用及操作系统的管理员权限，从而获取到该企业办公内网的接入

权限。

在横向移动过程中，攻击队又探测到该企业内网中的多个服务系统和多台服务器。使用已经获得门户网站管理员账号和密码进行撞库攻击，成功登录并控制了该企业内网中的绝大多数服务器。这表明，该企业内网中的有大量系统服务器都使用了相同的管理账号和密码。

至此，攻击队突破办公网的第一阶段目标顺利完成，并取得了巨大的战果。接下来的目标就是找到工控网络的突破口。

2）定位运维人员

对已经被攻破的服务器系统进行全面排查，攻击队发现，有多台服务器中存储了用 Excel 明文记录的密码本，密码本中包含所有系统用户的账号和密码。同时，服务器上还明文存储了大量机构内部敏感文件，包括企业 IT 部门的组织架构等信息。结合组织架构及密码本信息，攻击队成功定位到了一位工控系统的运维人员，并对其联网行为展开了长时间的监控。

3）突破工控网

经过一段时间的监控，攻击队发现该运维人员自己的办公终端上有嵌套使用远程桌面的情况，即：首

先通过远程桌面登录一台主机A；继而，操作人又用主机A继续通过远程桌面，登陆另一网段的主机B。通过与密码本进行比对，发现主机A和B都是该企业工控系统中的主机设备，但各自处于网络拓扑结构中不同的层级。其中，B主机之下连有关键的工控设备。

进一步分析发现，主机A使用了双网卡，两个网卡分别对应不同网段，但是两个网卡之间没有采取任何隔离措施。同时，主机B也是一台双网卡主机，其上部署了隔离卡软件进行双网卡切换。

最终，攻击队发现了B主机上隔离卡软件的一个重大设计缺陷，并利用该缺陷成功绕过双网卡的隔离机制，成功拿到了工控设备的操作权限，可以随意停止、启动、复位相应的工控设备，某些操作可对设备的生产过程造成直接且严重的伤害。

同时，攻击队的另一组人马继续摸排受控主机的用途和存储文件。功夫不负有心人，攻击队最终又发现一台“生产主操作室”的主机设备，其上存储有生产专用的文件，内容包括一些涉密文件，一旦被窃取，后果难以想象。

二、百折不挠——社工钓鱼突破边界

某企业为某大型特种设备制造商，同时具有比较成熟的互联网服务经验。在本次实战攻防演习活动中，攻击队的目标是：获取该企业一个核心业务管控平台的控制权限。

攻击队在前期的情报收集工作中发现，该企业内部的网络防御体系比较健全，正面突破比较困难。经过头脑风暴，大家达成共识——要通过社工方法进行迂回入侵。

1）寻找社工突破口

攻击队首先想到的社工方法也是最常见的邮件钓鱼。但考虑到该企业相对完善的网络防御体系，猜测其内网中很可能已经部署了邮件检测类的防御手段，简单的使用邮件钓鱼，很有可能会被发现。

进一步的情报搜集发现：该企业使用了微信客服平台，而且微信客服平台可以进行实时聊天并发送文件。考虑到客服人员一般没有很强的技术功底，安全意识往往相对薄弱，攻击队最终商定：将社工对象确定为微信客服人员，并以投诉为话题尝试对客服进行钓鱼。

2）冒充客户反馈问题

于是，一名攻击队队员开始冒充客户，在该企业的微信客服平台上进行留言投诉，并要求客服人员接收名为“证据视频录像”的压缩文件包。该压缩包实际上是攻击队精心伪装的，带有木马程序的文件包。让攻击队意想不到的是，该客服人员以安全为由，果断的拒绝接收来源的不明文件。显然，攻击队可能低估了该企业客服人员的安全意识素养。

3）社工升级攻破心理防线

不过，攻击队并没有放弃，而是进一步采用多人协作的方式，对当班客服人员进行了轮番轰炸，要求客服人员报上工号，并威胁将要对其客服质量进行投诉。经过1个多小时的拉锯战，客服人员的心理防线最终被攻破，最终接收了带毒压缩包，并打开了木马文件。该客服人员的终端设备最终被控制。

以受控终端为据点，攻击队成功打入该企业的内网，后又利用一个未能及时修复的系统漏洞获取到关键设备控制权限，再结合内网的信息收集，最终成功获取到管控平台的权限。

三、迂回曲折——供应链定点攻击

某超大型企业为一个国家级关键信息基础设施运

营管理方，一旦发生安全事故，将直接危害国家安全及人民生命财产安全。在本次实战攻防演习活动中，攻击队的目标是：获取该企业内部系统的安全管控权限。

根据攻击队前期的情报收集摸排，该企业的办公网络及核心工业控制系统得到了非常严密的安全防护，对互联网暴露的业务系统较少，而且业务系统做了安全加固及多层防护，同时也拥有较强的日常网络安全运维保障能力。想要正面突破，非常困难。

前期情报分析还显示，该企业虽然规模大、人员多，但并不具备独立的IT系统研发和运维能力，其核心IT系统的建设和运维，实际上大多来自外部采购或外包服务。于是，攻击队根据这一特点，制定了从供应链入手的整体攻击策略。

1）寻找目标供应商

攻击队首先通过检索“喜报”“中标”“签约”“合作”“验收”等关键词，在全网范围内，对该企业的供应商及商业合作伙伴进行地毯式排查，最终选定将该企业的专用即时通信系统开发商A公司作为主要攻击目标。

情报显示，A公司为该企业开发的专用即时通信

系统刚刚完成开发，推测该系统目前尚处于测试阶段，A公司应该有交付和运维人员长期驻场为该企业提供运维全服务。如果能拿下驻场人员的终端设备，则可以成功进入该公司的内网系统。

2）盗取管理员账号

分析发现，A公司开发的即时通信软件也在其公司内部进行使用。而该软件的网络服务管理后台，存在一个已知的系统安全漏洞。攻击队利用该漏洞获取了服务器的控制权，并通过访问服务器的数据库系统，获取了后台管理员的账号和密码。

3）定位驻场人员

攻击队使用管理员的账号和密码登录服务器后，发现该系统的聊天记录在服务器上是准明文（低强度加密或变换）存储的，而且管理员可以不受限制的翻阅其公司内部的历史聊天记录。

攻击队对聊天记录进行关键字检索后发现：A公司有三名员工的聊天记录中，多次出现目标企业名、OA、运维等字眼；并且这三名员工的登录IP经常落在目标企业的专属网段上。因此，攻击队判断，这三名员工就是A公司在目标企业的驻场人员。

4）定向恶意升级包

攻击队最初的设想是，通过被控的即时通信软件服务器，向三名驻场人员定向发送恶意升级包。但这种攻击方法需要修改服务器系统配置，稍有不慎，就可能扩大攻击面，给演习工作造成不必要的损失，同时也有可能暴露自身攻击活动。

为实现对三名驻场人员更加隐蔽的定向攻击，攻击队对A公司的即时通信软件系统进行了更加深入的安全分析，发现其客户端软件对服务器的身份安全验证、对升级包的合法性校验机制都存在设计缺欠。

于是，攻击队利用上述缺欠，通过中间人攻击，对服务器推送给三名驻场人员的客户端软件升级包进行了劫持和篡改。最终三名驻场人员都在完全没有任何感知的情况下，在各自的PC机上安装了攻击队伪装设计的恶意升级包。

5）横向移动

攻击队以驻场人员的运维机作为跳板机进入内网后，开始进行横向移动。

攻击队首先找到了该企业的一台域控服务器，并利用一个近期最新曝出的域控系统安全漏洞，获取了该主域的域账号密码哈希信息。但防守队很快地发现

了此次攻击，并将该域控服务器进行了隔离。

不过，攻击队并没有放弃，又在内网中找到了一套终端安全管理系统。攻击队经过现场挖掘，找到了该系统的一个新的 0Day 漏洞，并利用该漏洞成功的获取了管理员权限。在成功登录管理系统后台后，攻击方可实现任意命令的下发和执行，能够控制该安全管理系统所辖范围内的所有终端设备。

第六章 蓝队眼中的防守弱点

奇安信通过对政府、央企、银行、证券、民生、运营商、互联网等行业的蓝队实战工作，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，给了蓝队很多可乘之机。

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，蓝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。

五、安全设备自身安全成为新的风险点

“锁”出问题了给防守工作带来极大挑战。每年

攻防演习都会报出某某安全设备自身存在某某漏洞被利用、被控制，反应出安全设备厂商自身安全开发和检测能力没有做到位，而作为用户又缺乏必要的安全检测流程及工作的开展，给蓝队人员留下了“后门”，最终形成新的风险点。

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

红队视角下的防御体系构建

THE PRACTICAL PLAYBOOK OF DEFENSE BY RED TEAM

奇安信安服团队 奇安信行业安全研究中心 ◎著

380余场红队防守演习经验

520余政企机构协同作战

37 381人日累计投入

第一章 什么是红队

红队，在本书中是指网络实战攻防演习中的防守一方。

红队一般是以参演单位现有的网络安全防护体系为基础，在实战攻防演习期间组建的防守队伍。红队的主要工作包括演习前安全检查、整改与加固，演习期间网络安全监测、预警、分析、验证、处置，后期复盘总结现有防护工作中的不足之处，为后续常态化的网络安全防护措施提供优化依据等。

实战攻防演习时，红队通常会在日常安全运维工作的基础上，以实战思维进一步加强安全防护措施，包括提升管理组织规格、扩大威胁监控范围、完善监测与防护手段、增加安全分析频率、提高应急响应速度、增强溯源反制能力、建立情报收集利用机制等，提升整体防守能力。

需要特别说明的是：红队并不仅仅由实战演习中目标系统运营单位一家独立承担，而是由目标系统运营单位、攻防专家、安全厂商、软件开发商、网络运维队伍、云提供商等多方组成的防守队伍。组成红队的各个团队在演习中的角色与分工情况如下。

目标系统运营单位：负责红队整体的指挥、组织和协调。

安全运营团队：负责整体防护和攻击监控工作。

攻防专家：负责对安全监控中发现的可疑攻击进行分析研判，指导安全运营团队、软件开发商等相关部门进行漏洞整改等一系列工作。

安全厂商：负责对自身产品的可用性、可靠性和防护监控策略是否合理进行调整。

软件开发商：负责对自身系统安全加固、监控和配合攻防专家对发现的安全问题进行整改。

网络运维队伍：负责配合安全专家对网络架构安全、出口整体优化、网络监控、溯源等工作。

云提供商（如有）：负责对自身云系统安全加固，以及对云上系统的安全性进行监控，同时协助攻防专家对发现的问题进行整改。

其他：某些情况下还会有其他组成人员，需要根据实际情况具体分配工作。

特别强调，作为红队，了解对手（蓝队）的情况非常重要，正所谓知彼才能知己，从攻击队角度出发，

了解攻击队的思路与打法，了解攻击队思维，并结合本单位实际网络环境、运营管理情况，制定相应的技术防御和响应机制，才能在防守过程中争取到更多的主动权。

第二章 红队演变趋势

2016年和2017年，由于监管单位的推动，部分单位开始逐步参与监管单位组织的实战攻防演习，这个阶段各单位主要是作为防守方参加演习。到了2018年和2019年，实战攻防演习不论是从单场演习的参演单位数量、攻击队伍数量，还是攻守双方的技术能力等方面都迅速增强。实战攻防演习已经成为公认的检验各单位网络安全建设水平和安全防护能力的重要手段，各单位也从以往单纯的参与监管单位组织的演习，逐渐演变成自行组织内部演习或联合组织行业演习。

进入2020年，随着实战攻防演习中真刀实枪的不断对抗和磨砺，攻守双方在相互较量中都取得了快速发展和进步，迫于攻击队技战法迅速发展带来的压力，防守队也发生了很大的变化。

1）防守重心扩大

2020年之前的实战攻防演习，主要是以攻陷靶标系统为目标，达到发现防守队安全建设和防护短板，提升各单位安全意识的目的。攻击队的主要得分点是拿下靶标系统和路径中的关键集权系统、服务器等权限，非靶标系统得分很少。因此，防守队的防守重心往往会聚焦到靶标系统及相关路径资产上。

对于大部分参加过实战攻防演习的单位来说，对自身的安全问题和短板已经有了充分认识，也都开展了安全建设整改工作。对于这些单位，急需的是通过实战攻防演习检验更多重要系统的安全性，发现更全面的安全风险。因此，2020 年开始，不论是监管单位还是单位自身，在组织攻防演习时，都会逐步降低演习中靶标系统的权重，鼓励攻击更多的单位、系统，发现更多的问题和风险。同样，防守队的防守重心也就从靶标系统为主，扩大到所有重要业务系统、所有重要设备和资产、所有的相关上下级单位。

2）持续加强监测防护手段

随着近几年攻防技术的快速发展，实战攻防演习中各种攻击手段层出不穷、花样百出，各单位在演习中切实感受到了攻击队带来的严重威胁以及防守的巨大压力，防守队的监测和防护体系面临巨大挑战。防守队对于在攻防对抗中确实能够发挥重大作用的安全产品趋之若鹜，投入大量资金来采购和部署。

2018—2019 年，除了传统安全产品外，全流量威胁检测类产品在攻防对抗中证明了自己，获取了各单位的青睐，到了 2020 年，主机威胁检测、蜜罐以及威胁情报等产品服务迅速成熟并在演习中证明了对主流攻击的监测和防护能力，防守队开始大规模的部署使

用。除此之外，钓鱼攻击、供应链攻击等还没有有效的防护产品，不过随着在实战中的快速打磨，相应产品也会迅速成熟和广泛使用。

3）被动防守到正面对抗

要说变化，2020 年防守队最大的变化应该是从被动挨打迅速转变为正面对抗、择机反制。之前，演习中的大部分防守队发现攻击后基本就是封堵 IP、下线系统、修复漏洞，之后接着等待下一波攻击。敌在暗、我在明，只能被动挨打。2020 年开始，大量的防守队加强了溯源和反制能力，跟攻击队展开了正面对抗，也取得了很多战果。

要具备正面对抗能力，需要重点加强以下几方面。

快速响应。实战中讲究兵贵神速，在发现攻击时，只有最快速的确认攻击方式、定位受害主机、采取处置措施，才能够有效阻止攻击，并为下一步的溯源和反制争取时间。

准确溯源。俗话说知己知彼百战百胜，要想和攻击队正面对抗，首先得找到攻击队的位置，并想办法获取攻击队的足够信息，才能有针对性的制定反制策略开展反击。

精准反制。反制其实就是防守队发起的攻击。防

守队在准确溯源的基础上，需要攻击经验丰富的人员才能够有效精准的实施反制。当然，也有些单位会利用蜜罐等产品埋好陷阱，等着攻击队跳进来之后，利用陷阱中的木马等快速攻陷攻击队系统。

第三章 红队四步走——防守的四个阶段

在实战环境下的防护工作，无论是面对常态化的一般网络攻击，还是面对有组织、有规模的高级攻击，对于防护单位而言，都是对其网络安全防御体系的直接挑战。在实战环境中，红队需要按照备战、临战、实战和战后四个阶段来开展安全防护工作。

一、备战阶段——不打无准备之仗

在实战攻防工作开始之前，首先应当充分地了解自身安全防护状况与存在的不足，从管理组织架构、技术防护措施、安全运维处置等各方面能进行安全评估，确定自身的安全防护能力和工作协同默契程度，为后续工作提供能力支撑。这就是备战阶段的主要工作。

在实战攻防环境中，我们往往会面临技术、管理和运营等多方面限制。技术方面：基础能力薄弱、安全策略不当和安全措施不完善、产品部署位置不当、防护产品自身安全有问题、监控手段不熟悉、监控手段单一等问题普遍存在；管理方面：制度缺失，职责不明，应急响应机制不完善等问题也很常见；运营方面：

资产梳理不清晰、业务架构不了解、漏洞整改不彻底、安全监测分析与处置能力不足等问题随处可见。这些不足往往会导致整体防护能力存在短板，对安全事件的监测、预警、分析和处置效率低下。

针对上述情况，红队在演习之前，需要从以下几个方面进行准备与改进。

1）技术方面

为了及时发现自身安全隐患和薄弱环节，需要有针对性地开展自查工作，并进行安全整改加固，内容包括系统资产梳理、应用组件梳理、业务逻辑安全、交互协议梳理、安全基线检查、网络安全策略检查、Web安全检测、关键网络安全风险检查、安全措施梳理和完善、公开情报收集、应急预案完善与演练等。

为了检验监控措施的有效性，还需对安全产品自身的安全性、部署位置、覆盖面进行评估；为了更快的发现问题，尽量部署全流量威胁检测、网络分析系统、蜜罐、主机监测等安全防护设备，提高监控工作的有效性、时效性、准确性；监测人员还需对安全产品熟练掌握、优化安全产品规则。

2）管理方面

一是建立合理的安全组织架构，明确工作职责，

建立具体的工作小组，同时结合工作小组的责任和内容，有针对性地制定工作计划、技术方案、相关方协同机制及工作内容，责任到人、明确到位，按照工作实施计划进行进度和质量把控，确保管理工作落实到位，技术工作有效执行。

二是建立有效的工作沟通机制，通过安全可信的即时通讯工具建立实战工作指挥群，及时发布工作通知，共享信息数据，了解工作情况，实现快速、有效的工作沟通和信息传递。

3）运营方面

成立防护工作组并明确工作职责，责任到人，开展并落实技术检查、整改和安全监测、预警、分析、验证和处置等运营工作，加强安全技术防护能力。完善安全监测、预警和分析措施，增强监测手段多元化，建立完善的安全事件应急处置机构和可落地的流程机制，提高事件的处置效率。

同时，所有的防护工作包括预警、分析、验证、处置和后续的整改加固都必须以监测发现安全威胁、漏洞隐患为前提才能开展。其中，全流量安全威胁检测分析系统是防护工作的重要关键节点，并以此为核心，有效地开展相关防护工作。

二、临战阶段——战前动员鼓舞士气

经历了备战阶段的查缺补漏、城防加固等工作，安全防护能力在技术方面、管理方面和运营方面上都有了较大的提升。为了能更好的协同配合，高效的应对实战阶段的攻击，减少分析处置事件的时间，提高防守的效果，还需要做好临战阶段的动员工作。

做好临战阶段的工作建议从三个方面开展。

1）召开战前动员会

战前动员主要进行三部分的工作：一是在实战演习开始前，通过召开现场战前动员会的形式，进行战前动员，统一思想，统一战术、提高斗志，达成共识。二是强调防守工作中注意的事项，攻击手段多种多样，为防止防守人员被攻击利用，要严格遵守纪律红线、做到令行禁止。三是提高大家的攻防意识，对攻击过程进行剖析，对常见的攻击手段部署针对性的防守要点，做到有的放矢。

2）宣贯工作流程

宣贯工作流程的目的一是对参与防守工作的人员进行任务分工，说明工作职责、各司其职。二是固化每日工作流程、各岗位协同配合，做好攻击事件前期的监测、中期的研判和后期的处置工作。三是宣贯制

定的工作排班计划、交接班要求等。通过工作流程做到防守工作有序有效，提升防守的效果。

3）组织战术培训

战术培训会主要工作内容有两项：一是由安全专家分享其他单位的网络安全实战攻防演练相关经验，协助防守队制定不同攻击场景的防守战术。二是安全专家对演练评分规则的详细解读，提高参演人员对演练的认知。

三、实战阶段——全面监测及时处置

攻守双方在实战阶段正式展开全面对抗。防护方须依据备战明确的组织和职责，集中精力和兵力，做到监测及时、分析准确、处置高效，力求系统不破，数据不失。

在实战阶段，从技术角度总结应重点做好以下四点。

1）全面开展安全监测预警

实战阶段监测人员需具备基本的安全数据分析能力，根据监测数据，情报信息能基本判断攻击有效性，如存疑应立即协同专业分析人员协助分析，确保监控可以实时发现，不漏报，为处置工作提供准确信息，

同时监测工作应覆盖整个攻击队攻击时间。

2）全局性分析研判工作

在实战防护中，分析研判应作为核心环节，分析研判人员要具备攻防技术能力，熟悉网络和业务。分析研判人员作为整个防护工作的大脑，应充分发挥专家和指挥棒的作用。向前，对监测人员发现的攻击预警、威胁情报进行分析确认，向后，指导协助事件处置人员对确认的攻击进行处置。

3）提高事件处置效率效果

确定攻击事件成功后，最重要的是在最短时间内采取技术手段遏制攻击、防止蔓延。事件处置环节，应联合网络、主机、应用和安全等多个岗位人员协同处置。

4）追踪溯源，全面反制

在发现攻击事件后，防守队伍可根据安全防护设备、安全监测设备产生的告警信息、样本信息等，结合各种情报系统追踪溯源。条件允许时，可通过部署诱捕系统反制攻击队攻击终端，做到追踪溯源、防守反制。

四、战后整顿——实战之后的改进

演习的结束也是防护工作改进的开始。在实战工作完成后应进行充分、全面复盘分析，总结经验、教训。有两方面工作需要开展。

一是通过复盘会找出攻防演习备战阶段、临战阶段、实战阶段中的工作方案、组织管理、工作启动会、系统资产梳理、安全自查及优化、基础安全监测与防护设备的部署、安全意识、应急预案及演练、注意事项、队伍协同、情报共享和使用等过程还存在哪些纰漏和不足，输出技术和管理两方面问题整改措施计划。同时，各单位还需立即总结攻防演习防守策略，如情报技术、反制战术、防守作战指挥策略等，为演习队伍在下一次保障提供防守技术指导。

二是网络攻防演练活动不是一次性保障工作，其最终目的是单位通过演习发现网络安全建设存在的不足，改进和提升整体安全防御能力，通过相对独立的安全运营思路，以数据为中心建立整体网络安全防护体系，进而发挥出最有效的安全能力。因此单位通过网络攻防演练积累的经验，沿用演习期间形成的安全运营机制、安全监测技术和应急响应策略等，在日常安全工作中提供持续安全运营能力，使网络安全防护

措施持续发挥成效，进而真实有效的提升安全防护的能力。同时，单位还需加快整顿演习发现的网络安全体系建设的不足，以代替演习后保障队伍力量缩减，而导致的整体安全防御降低的能力。

最后，单位参与和自我组织网络攻防演练活动，充分积累演练活动经验，锻炼安全保障队伍，不断完善整体网络安全体系和持续提高安全运营能力。

第四章 红队应对攻击的常用策略

知己知彼，百战不殆。政企安全部门只有在多次经历实战攻防的洗礼，通过实战对攻击队的攻击手段不断深入了解，才能不断发现自身安全防护能力的缺失，防护手段应随着攻击手段的变化升级而进行相应的改变和提升，将是未来的主流防护思想。

攻击队一般会在前期搜集情报，寻找突破口、建立突破据点；中期横向移动打内网，尽可能多地控制服务器或直接打击目标系统；后期会删日志、清工具、写后门、建立持久控制权限。针对攻击队的常用套路，红队应对攻击的常用策略可总结为收缩战线、纵深防御、守护核心、协同作战、主动防御、应急处突和溯源反制等。

一、收缩战线：缩小攻击暴露面

攻击队首先会通过各种渠道收集目标单位的各种信息，收集的情报越详细，攻击则会越隐蔽，越快速。此外，攻击队往往不会正面攻击防护较好的系统，而是找一些可能连防守者自己都不知道的薄弱环节下手。这就要求防守者一定要充分了解自己暴露在互联网的系统、端口、后台管理系统、与外单位互联的网络路

径等信息。哪方面考虑不到位、哪方面往往就是被攻陷的点。互联网暴露面越多，越容易被攻击队“声东击西”，最终导致防守者顾此失彼，眼看着被攻击却无能为力。结合多年的防守经验，可从如下几方面收敛互联网暴露面。

1）敏感信息搜集

攻击队会采用社工、工具等多种技术手段，对目标单位可能暴露在互联网上的敏感信息进行搜集，为后期攻击做充分准备。防守队除了定期对全员进行安全意识培训，不准将带有敏感信息的文件上传至公共信息平台外，针对漏网之鱼还可以通过定期开展敏感信息泄露搜集服务，能够及时发现在互联网上已暴露的本单位敏感信息，提前采取应对措施，降低本单位敏感信息暴露的风险，增加攻击队搜集敏感信息的时间成本，为后续攻击抬高难度。

2）攻击路径梳理

知晓攻击队有可能从哪些地方攻击进来，对防守力量如何部署起关键作用。由于政企机构的网络不断变化、系统不断增加，往往会增加新的系统和产生新的网络边界。防守队一定要定期梳理自己的网络边界、可能被攻击的路径，尽可能梳理绘制出每个业务系统的网络访问路径，包括对互联网开放的系统、内部访

问系统（含测试系统），尤其是内部系统全国联网的单位更要注重此项梳理工作。

3）互联网攻击面收敛

一些系统维护者为了方便，往往会把维护的后台、测试系统和高危端口私自开放在互联网上，方便维护的同时也方便了攻击队。攻击队最喜欢攻击的 Web 服务就是网站后台，以及安全状况比较差的测试系统。红队可通过开展互联网资产发现服务，对本单位开放在互联网上的管理后台、测试系统、无人维护的僵尸系统（含域名）、拟下线未下线的系统、高危服务端口、疏漏的未纳入防护范围的互联网开放系统以及其他重要资产信息（中间件、数据库等）进行发现和梳理，提前进行整改处理，不断降低互联网侧攻击入口的暴露。

4）外部接入网络梳理

如果正面攻击不成，攻击队往往会选择攻击供应商、下级单位、业务合作单位等与目标单位有业务连接的其他单位，通过这些单位直接绕到目标系统内网。防守队应对这些外部的接入网络进行梳理，尤其是未经过安全防护设备就直接连进来的单位，应先连接防护设备，再接入内网。防守队还应建立起本单位内部网络与其他单位进行对接的联络沟通机制，发现从其

他单位过来的网络行为异常时，能及时反馈到其他单位，协同排查，尽快查明原因，以便后续协同处置。

5）隐蔽入口梳理

由于API接口、VPN、WiFi这些入口往往会被安全人员忽略，这往往是攻击队最喜欢的突破口，一旦搞定则畅通无阻。安全人员一定要梳理Web服务的API隐藏接口、不用的VPN、WiFi账号等，便于重点防守。

二、纵深防御：立体防渗透

收缩战线工作完成后，针对实战攻击，防守队应对自身安全状态开展全面体检，此时可结合战争中的纵深防御理论来审视当前网络安全防护能力。从互联网端防护、内外部访问控制（安全域间甚至每台机器之间）、主机层防护、供应链安全甚至物理层近源攻击的防护，都需要考虑进去。通过层层防护，尽量拖慢攻击队扩大战果的时间，将损失降至最小。

1）资产动态梳理

清晰的信息资产是防守工作的基石，对整个防守工作是否能顺利开展起决定作用。防守队应该通过开展资产梳理工作，形成信息资产列表，至少包括单位环境中所有的业务系统、框架结构、IP地址（公网、

内网）、数据库、应用组件、网络设备、安全设备、归属信息、业务系统接口调用信息等，结合收缩战线工作的成果，最终形成准确清晰的资产列表，并定期动态梳理，不断更新，确保资产信息的准确性，为正式防守工作奠定基础。

2）互联网端防护

互联网作为防护单位最外部的接口，是重点防护区域。互联网端的防护工作可通过接入第三方云防护平台、部署网络安全防护设备和进行攻击检测两方面开展。需部署的网络安全防护设备包括：下一代防火墙、防病毒网关、全流量分析设备、防垃圾邮件网关、WAF、IPS 等。攻击检测方面，如果有条件，可以事先对互联网系统进行一次完整的渗透测试，检测互联网系统安全状况，查找存在的漏洞。

3）访问策略梳理

访问控制策略的严格与否，对防守工作至关重要。从实战经验来看，严格的访问控制策略，对攻击队都能产生极大的阻碍。防守队应通过访问控制策略梳理工作，重新厘清不同安全域的访问策略，包括互联网边界、业务系统（含主机）之间、办公环境、运维环境、集权系统的访问、以及内部与外部单位对接访问、无线网络策略等访问控制措施。

防守队应依照“最小原则”，只给必须使用的用户开放访问权限。按此原则梳理访问控制策略，禁止私自开放服务或者内部全通的情况出现。这样，无论是阻止攻击队撕破边界打点，还是增加进入内部后开展横向渗透的难度，都是非常简单有效的手段。通过严格的访问控制措施尽可能地为攻击队制造障碍。

4）主机加固防护

当攻击队从突破点进入内网后，首先做的就是攻击同网段主机。主机防护强弱直接决定了攻击队内网攻击成果的大小。防守队应从以下几个方面对主机进行防护：对主机进行漏洞扫描，基线加固；最小化软件安装，关闭不必要的服务；杜绝主机弱口令，结合堡垒机开启双因子认证登录；高危漏洞必须打补丁（包括装在系统上的软件高危漏洞）；开启日志审计功能。部署主机防护软件对服务进程、重要文件等进行监控，条件允许的情况下，还可开启防护软件的“软蜜罐”功能，进行攻击行为诱捕。

5）供应链安全

攻击队擅长对各行业中广泛使用的软件、框架或设备进行研究储备，发现其中的安全漏洞，在攻防对抗中进行有的放矢，突破防守队网络边界，甚至拿下目标系统权限。

政企机构在安全运营工作中，应重视与供应链厂商建立安全应对机制，要求供应链厂商建立起自身网络环境（如搭建带有客户业务的测试环境，还对互联网提供开放）、产品的安全保障机制（包括源码、管理工具、技术文档、漏洞补丁等方面的管理），一旦暴露出安全问题，应及时给政企机构提供修复方案或处置措施。

同时，供应链厂商也应建立内部情报渠道，提高产品的安全性，为政企机构提供更可靠，更安全的产品和服务。

三、守护核心：找到关键点

正式防守工作中，根据系统的重要性划分出防守工作重点，找到关键点，集中力量进行防守。根据实战攻防经验，核心关键点一般包括：靶标系统、集权类系统、具有重要数据的业务系统等，在防守前应针对这些重点系统再次进行梳理和整改，梳理的越细越好。必要情况下对这些系统进行单独的评估，充分检验重点核心系统的安全性。同时在正式防守工作，对重点系统的流量、日志进行实时监控和分析。

1）靶标系统

靶标系统是实战中攻防双方关注的焦点，靶标系

统失陷，则意味这防守队的出局。防守队在靶标系统的选择与防护中应更具有针对性。首先靶标系统应经过多次安全测试，自身安全有保障；其次应梳理清与靶标系统有互通的网络，重新进行网络策略梳理，按照最小原则进行访问；最后靶标系统应部署在内部网络中，尽可能避免直接对互联网开放。条件允许的情况下，还可以对靶标系统主机部署安全防护软件，对靶标系统主机进行进程白名单限制，在防守中，可实时监测靶标系统的安全状态。

2）集权系统

集权系统一般包括单位自建的云管理平台、核心网络设备、堡垒机、SOC 平台、VPN 等，它们是攻击队最喜欢打的内部系统，一旦被拿下，则集权系统所控制的主机可同样视为已被拿下，杀伤力巨大。

集权系统是内部防护的重中之重。防守队一般可从以下几个方面做好防护：集权系统的主机安全、集权系统已知漏洞加固或打补丁、集权系统的弱口令、集权系统访问控制、集权系统配置安全以及集权系统安全测试等。

3）重要业务系统

重要业务系统如果被攻击队攻破，也会作为攻击

重要成果的一部分，因此，在防守过程中，也应该被重点防护。针对此类系统除了常规的安全测试、软件、系统补丁升级及安全基线加固外，还应针对此类系统加强监测，并对其业务数据进行重点防护，可通过部署数据库审计系统、DLP 系统加强对数据的安全保护。

四、协同作战：体系化支撑

面对大规模有组织的攻击时，攻击手段会不断快速变化升级，防守队在现场人员能力无法应对攻击的情况下，还应该借助后端技术资源，相互配合协同作战，建立体系化支撑，才能有效应对防守工作中面临的各种挑战。

1）产品应急支撑

产品的安全正常运行是防守工作顺利开展的前提。但在实际中不可避免的会出现产品故障、产品漏洞等问题，影响到防守工作。因此防守队需要会同各类产品的原厂商或供应商，建立起产品应急支撑机制，在产品出现故障、安全问题时，能够快速的得到响应和解决。

2）安全事件应急支撑

安全事件的应急处置，一般会涉及政企机构的多个不同部门人员，防守队在组建安全事件应急团队时，

应充分考虑哪些人员纳入到应急支撑团队中。在实战中需要对发生的安全事件应急处置时，如果应急团队因技术能力等原因无法完成对安全事件的处置时，可考虑寻求其他技术支撑单位的帮助，来弥补本单位应急处置能力的不足。

3）情报支撑

随着攻防演练向行业化，地区化发展，攻击手段的日益丰富，0Day、NDay 漏洞、钓鱼、社工、近源攻击的频繁使用以及攻击队信息搜集能力的大大提高，攻击队已发展成为集团军作战模式。

所以，在实战阶段，仅凭一个单位的防守力量可能无法真正的防护住攻击队伍的狂轰滥炸。在各自的防护能力之外，各个单位防守队伍须建立有效的安全情报网，通过民间、同行业、厂商、国家、国际漏洞库收集情报，形成情报甄别，情报利用机制，高效快速的抵御攻击队攻击。攻防演练对抗本质就是信息战，谁掌握的情报越多越准确谁就能立于不败之地。

4）样本数据分析支撑

现场防守人员在监测中发现可疑、异常文件时，可将可疑、异常文件提交至后端样本数据分析团队，根据样本分析结果，判断攻击入侵程度，及时开展应

对处置工作。

5）追踪溯源支撑

当现场防守人员发现攻击队的入侵痕迹后，需对攻击队的行为、目的、身份等开展溯源工作时，可寻求追踪溯源团队的帮助，凭借追踪溯源团队的技术力量，分析出攻击队的攻击行为、攻击目的乃至攻击队的身份。必要情况下，还可以一起对攻击队开展反制工作，最大化扩展防守成果。

五、主动防御：全方位监控

近两年的红蓝对抗，攻击队的手段越来越隐蔽，越来越单刀直入，通过0Day、NDay直指系统漏洞，直接获得系统控制权限。

红队需拥有完整的系统隔离手段，蓝队成功攻击到内网之后，会对内网进行横向渗透。所以系统与系统之间的隔离，就显得尤为重要！红队必须清楚哪些系统之间有关联、访问控制措施是什么！在发生攻击事件后，应当立即评估受害系统范围和关联的其他系统，并及时做出应对的访问控制策略，防止内部持续的横向渗透。

任何攻击都会留下痕迹。攻击队会尽量隐藏痕迹、

防止被发现。而防守者恰好相反，需要尽早发现攻击痕迹，并通过分析攻击痕迹，调整防守策略、溯源攻击路径、甚至对可疑攻击源进行反制。建立全方位的安全监控体系是防守者最有力的武器，总结多年实战经验，有效的安全监控体系需在如下几方面开展。

1）自动化的 IP 封禁

在整个红蓝对抗的过程中，如果红队成员 7×24 小时不间断从安全设备的告警中识别风险，将极大地消耗监测人员、处置人员的精力。通过部署态势感知与安全设备联动，收取全网安全设备的告警信息，当态势感知系统收到安全告警信息后，根据预设规则自动下达边界封禁策略，使封禁设备能够做出及时有效的阻断和拦截，大大降低了人工的参与程度，提高整个红队的防守效率。

2）全流量网络监控

任何攻击都要通过网络，并产生网络流量。攻击数据和正常数据肯定是不同的，通过全网络流量去捕获攻击行为是目前最有效的安全监控方式。红队或防守者通过全流量安全监控设备，结合安全人员的分析，可快速发现攻击行为，并提前做出针对性防守动作。

3）主机监控

任何攻击最终目标是获取主机（服务器或终端）权限。通过部署合理的主机安全软件，审计命令执行过程、监控文件创建进程，及时发现恶意代码或WebShell，并结合网络全流量监控措施，可以更清晰、准确、快速地找到被攻击的真实目标主机。

4）日志监控

对系统和软件的日志监控同样必不可少。日志信息是帮助防守队分析攻击路径的一种有效手段。攻击队攻击成功后，打扫战场的首要任务就是删除日志，或者切断主机日志的外发，以防止防守队追踪。防守队应建立一套独立的日志分析和存储机制，重要目标系统可派专人对目标系统日志和中间件日志进行恶意行为监控分析。

5）蜜罐诱捕

随着红蓝对抗的持续化发展，蜜罐技术是改变红队被动挨打局面的一把利剑！其特点是诱导攻击队攻击伪装目标，持续消耗攻击队资源，保护真实资产，监控期间针对所有的攻击行为进行分析，可意外捕获0Day信息。

目前的蜜罐技术可分为3种：自制蜜罐、高交互

蜜罐和低交互蜜罐，也可诱导攻击队下载远控程序，定位攻击队自然人身份，提升主动防御能力，让对抗工作由被动变主动。

6）情报工作支撑

现场防守队员在防守中，一是要善于利用情报搜集工作提供的各种情报成果，根据情报内容及时对现有环境进行筛查和处置。二是对已获取的情报，请求后端资源对情报进行分析和辨别，以方便采取应对措施。

六、应急处突：完备的方案

通过近几年的红蓝对抗发展来看，红蓝对抗初期，蓝队成员通过普通攻击的方式，不使用 0Day 或其他攻击方式，就能轻松突破红队的防守阵地。

但是，红队防护体系的发展早已从只有防火墙做访问控制，到现在逐步完善了 WAF、IPS、IDS、EDR 等多种防护设备，使红队无法突破，从而逼迫红队成员通过使用 0Day、NDay、现场社工、钓鱼等多种方式入侵红队目标，呈无法预估的特点。

所以应急处突是近两年红蓝对抗中发展的趋势，同时也是整个红队防守水平的体现之处，不仅考验应

急处置人员的技术能力，更检验多部门（单位）协同能力，所以制定应急预案应当从以下几个方面进行。

一是完善各级组织结构，如：监测组、研判组、应急处置组（网络小组、系统运维小组、应用开发小组、数据库小组）、协调组等。

二是明确各方人员，在各个组内担任的角色，如：监测组的监测人员。

三是明确各方人员，在各个组内担任的职责，如：监测组的监测人员，负责某台设备的监测，并且7×24小时不得离岗等。

四是明确各方设备的能力与作用，如：防护类设备、流量类设备、主机检测类设备等。

五是制定可能出现的攻击成功场景，如：Web攻击成功场景、反序列化攻击成功场景、WebShell上传成功场景等。

六是明确突发事件的处置流程，将攻击场景规划至不同的处置流程：上机查证类处置流程、非上机查证类处置流程等。

七、溯源反制：人才是关键

溯源工作一直是安全的重要组成部分，无论在平常的运维工作，还是红蓝对抗的特殊时期，在发生安全事件后，能有效防止被再次入侵的有效手段，就是溯源工作！

在红蓝对抗的特殊时期，防守队中一定要有经验丰富、思路清晰的溯源人员，能够第一时间进行应急响应，按照应急预案分工，快速查清入侵过程，并及时调整防护策略，防止再次入侵，同时也为反制人员提供溯源到的真实 IP，进行反制工作。

反制工作是防守队反渗透能力的体现，普通的防守队员一般也只具备监测、分析、研判的能力，缺少反渗透的实力。这将使防守队一直属于被动的一方，因为防守队没有可反制的固定目标，也很难从成千上百的攻击 IP 里，确定哪些可能是攻击队的地址，这就要求防守队中要有经验丰富的反渗透的人员。

经验丰富的反渗透人员会通过告警日志，分析攻击 IP、攻击手法等内容，对攻击 IP 进行端口扫描、IP 反查域名、威胁情报等信息收集类工作，通过收集到的信息进行反渗透。

防守队还可通过效防攻击队社工手段，诱导攻击

队进入诱捕陷阱，从而达到反制的目的，定位攻击队自然人身份信息。

第五章 建立实战化的安全体系

安全的本质是对抗。对抗是攻防双方能力的较量，是一个动态的过程。业务在发展，网络在变化，技术在变化，人员在变化，攻击手段也在不断变化。所以网络安全没有“一招鲜”的方式，需要在日常工作中，不断积累不断创新，不断适应变化，持续地构建自身的安全能力，才能面对随时可能威胁系统的各种攻击，不能临阵磨枪、仓促应对，必须立足根本、打好基础，加强安全建设、构建专业化的安全团队，优化安全运营过程，并针对各种攻击事件采取重点防护才是根本。

防守队不应再以“修修补补，哪里出问题堵哪里”的思维来解决问题，而应未雨绸缪，从管理、技术、运行等方面建立系统化、实战化的安全体系，有效应对实战环境下的安全挑战。

一、完善面向实战的纵深防御体系

实战攻防演习的真实对抗表明，攻防是不对称的。通常情况下，攻击队只需要撕开一个点，就会有所“收获”，甚至可以通过攻击一个点，拿下一座“城池”。

但对于防守工作来说，考虑的却是安全工作的方方面面，仅关注某个或某些防护点，已经满足不了防

护需求。实战攻防演习过程中，攻击队或多或少还有些攻击约束要求，但真实的网络攻击则完全无拘无束，与实战攻防演习相比较，真实的网络攻击更加隐蔽而强大。

为应对真实网络攻击行为，仅仅建立合规型的安全体系是远远不够的。随着云计算、大数据、人工智能等新型技术的广泛应用，信息基础架构层面变得更加复杂，传统的安全思路已越来越难以适应安全保障能力的要求。必须通过新思路、新技术、新方法，从体系化的规划和建设角度，建立纵深防御体系架构，整体提升面向实战的防护能力。

从应对实战角度出发，对现有安全架构进行梳理，以安全能力建设为核心思路，面向主要风险重新设计政企机构整体安全架构，通过多种安全能力的组合和结构性设计形成真正的纵深防御体系，并努力将安全工作前移，确保安全与信息化“三同步”（同步规划、同步建设、同步运行），建立起能够具备实战防护能力、有效应对高级威胁、持续迭代演进提升的安全防御体系。

二、形成面向过程的动态防御能力

在实战攻防对抗中，攻击队总是延续信息收集、

攻击探测、提权、持久化的一个个循环过程。攻击队总是通过不断的探测发现环境漏洞，并尝试绕过现有的防御体系，成功的入侵到网络环境中。如果防御体系的安全策略长期保持不变，一定会被“意志坚定”的攻击队得手。所以，为了应对攻击队的持续变化的攻击行为，需要防御体系自身具有一定适应性的动态检测能力和响应能力。

在攻防对抗实践中，防守对应利用现有安全设备的集成能力和威胁情报能力，通过云端威胁情报的数据，让防御体系中的检测设备和防护设备发现更多的攻击行为，并依据设备的安全策略做出动态的响应处置，把攻击队阻挡在边界之外。同时，在设备响应处置方面，也需要通过攻击队的攻击行为和动机支持多样化的防护能力，例如封堵 IP、拦截具有漏洞的 URL 页面访问等策略。

通过动态防御体系，不仅可以有效拦截攻击队的攻击行为，同时还可以迷惑攻击队，让攻击队的探测行为失去方向，让更多的攻击队知难而退，从而在对抗过程中占得先机。

三、建设以人为本的主动防御能力

安全的本质是对抗，对抗两端是人与人的较量。

攻防双方都在对抗过程中不断提升各自的攻防能力。在这个过程中，就需要建立一个高技术的安全运营团队，利用现有的防御体系和安全设备，持续地检测内部的安全事件告警与异常行为，通过安全事件告警和异常行为分析，发现已进入到内部的攻击队，并对其采取安全措施，压缩攻击队停留在内部的时间。

构建主动防御的基础是可以采集到内部的大量的、有效的数据，包括安全设备的告警、流量信息、账号信息等。为了对内部网络影响最小，采用流量威胁分析的方式，实现“全网”流量威胁感知，特别是关键的边界流量、内部重要区域的流量。安全运营团队应利用专业的攻防技能，从这些流量威胁告警数据中发现攻击线索，并对已发现的攻击线索进行威胁巡猎、拓展，一步步找到真实的攻击点和受害目标。

主动防御能力主要表现为构建安全运营的闭环，包括以下几个方面。

在漏洞的运营方面，形成持续的评估发现、风险分析、加固处置的闭环，减少内部的受攻击面，提升网络环境的内生安全。

在安全事件运营方面，对实战中的攻击事件的行为做到“可发现、可分析、可处置”的闭环管理过程，

实现安全事件的全生命周期的管理，压缩攻击队停留在内部的时间，降低安全事件的负面影响。

在资产运营方面，逐步建立起配置管理库（CMDB），定期开展暴露资产发现，并定期更新配置管理库，这样才能使安全运营团队快速定义攻击源和具有漏洞的资产，通过对未知资产处置和漏洞加固，减少内外部的受攻击面。

四、基于情报数据的精准防御能力

在实战攻防对抗中，封堵 IP 是很多防守队的主要响应手段。这种手段相对来讲简单、粗暴。同时，采用这种手段，容易造成对业务可用性的影响，主要体现在以下两个方面。

1）如果是检测设备误报，就会导致被封堵的 IP 并非是真实的攻击 IP，这会影响到互联网用户的业务。

2）如果攻击 IP 自身是一个 IDC 出口 IP，那么封堵该 IP，就可能造成 IDC 后端大量用户的业务不可用。

所以，从常态化安全运行的角度来看，防守队应当逐步建立基于情报数据的精准防御能力。具体来说，

主要包括以下几个方面。

首先，防守队需要建设一种精准防御的响应能力，在实战攻防对抗中针对不同的攻击IP、攻击行为可采用更加细粒度、精准的防御手段。

结合实战攻防对抗场景，防守队可以利用威胁情报数据共享机制，实现攻击源的精准检测与告警，促进精准防御。减少检测设备误报导致业务部分中断的影响。此外，让威胁情报数据共享在多点安全设备上共同作用，可以形成多样化、细粒度化的精准防御。例如，在网络流量检测设备、终端检测与响应系统、主机防护系统等。

其次，为了最小化攻防活动对业务可用性的影响，需要设计多样化的精准防御手段与措施，既要延缓攻击，同时也要实现业务连续性需要。

例如，从受害目标系统维度去考虑设计精准防御能力，围绕不同的目标系统，采取不同的响应策略。如果是针对非实时业务系统的攻击，可以考虑通过防火墙封禁IP的模式；但如果是针对实时业务系统的攻击，就应考虑在WAF设备上拦截具有漏洞的页面访问请求，从而达到实时业务系统的影响最小化。

最后，为了保证实战攻防对抗过程不会大面积失

陷，在重要主机侧应加强主机安全防护，阻止主机层面的恶意代码运行与异常进程操作。例如域控服务器、网管服务器、OA 服务器、邮件服务器等。

五、打造高效一体的联防联控机制

在实战攻防对抗中，攻击是一个点，攻击队可以从一个点就攻破整座“城池”。所以在防守的各个阶段，不应只是安全部门在孤独的战斗，而是需要更多的资源、更多的部门协同工作，才有可能做好全面的防守工作。

例如，一个攻击队正在对某个具有漏洞的应用系统渗透攻击，在检测发现层面，需要安全运营团队的监控分析发现问题，然后通知网络部门进行临时封堵攻击 IP，同时要让开发部门对应用系统的漏洞尽快进行修复。这样才能在最短时间内让攻击事件的处置形成闭环。

在实战攻防对抗中，要求防守队一定要建立起联防联控的机制，分工明确、信息通畅。唯有如此，才能打好实战攻防演习的战斗工作。联防联控的关键点。

1）安全系统协同

通过安全系统的接口实现系统之间的集成，提升

安全系统的联动，实现特定安全攻击事件的自动化处置，提高安全事件的响应处置效率。

2）内部人员协同

内部的安全部门、网络部门、开发部门、业务部门全力配合实战攻防对抗工作组完成每个阶段的工作，同时在安全值守阶段全力配合工作组做好安全监控与处置的工作。

3）外部人员协同

实战攻防对抗是一个高频的对抗活动，在这期间，需要外部的专业安全厂商配合工作组一起来防守，各个厂商之间应依据产品特点和职能分工落实各自工作，并在期间做到信息通讯顺畅、听从指挥。

4）平台支撑、高效沟通

为了加强内部团队的沟通与协同，在内部通过指挥平台实现各部门、各角色之间的流程化、电子化沟通，提升沟通协同效率，助力联防联控有效运转。

六、强化行之有效的整体防御能力

2020 年的实战攻防演习的最新要求是：与报备目标系统同等重要的系统被攻陷也要参照报备目标系统规则扣分。

这就对大型机构的防守队带来了前所未有的防守压力。原来通行的防守策略是重兵屯在总部（目标系统一般在总部），提升总部的整体防御能力。但是随着实战攻防演习规则的演变，总部和分支机构就变的同等重要。

从攻击路径来看，分支机构的安全能力一般弱于总部，同时分支机构和总部网络层面是相通的，并且早期安全建设的时候往往会默认对方的网络是可信的；在安全防护层面，总部一般也仅仅是对来自分支机构的访问请求设置一些比较粗犷的访问控制措施。这些安全隐患都会给攻击队留出机会，使攻击队可以从薄弱点进入，然后横向移动到总部的目标系统。

因此，防守队只有将总部和分支机构进行统一的安全规划和管理，形成一个整体防御能力，才能有效的开展实战攻防对抗。在整体防御能力上，建议防守队开展如下工作。

1）互联网出口统一管理

条件允许的情况下，应尽量上收分支机构的互联网出入口。统一管理的好处是集中防御、节约成本、降低风险。同时，在整体上开展互联网侧的各类风险排查，包括互联网未知资产、敏感信息泄露、社工信

息的清理等工作。

2）加强分支机构防御能力

如果无法实现分支机构的互联网出入口统一管理，则分支机构需要参考总部的安全体系建设完善其自身的防御能力，避免成为安全中的短板。

3）全面统筹、协同防御

在准备阶段，应配合总部开展风险排查；在实战值守阶段，与防守队一起安全值守，并配置适当的安全监控人员、安全分析处置人员，配合防守队做好整体的防御，配合防守队做好攻击的应急处置等工作。

奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商

紫队视角下的
实战攻防演习组织

THE PRACTICAL PLAYBOOK OF ORGANIZATION BY PURPLE TEAM

奇安信安服团队 奇安信行业安全研究中心 ◎著

220余次紫队演习组织经验

2300余个业务系统隐患排除

4000日累计投入

第一章 什么是紫队

紫队，在本书中是指网络实战攻防演习中的组织方。

紫队是在实战攻防演习中，以组织方角色，开展演习的整体组织协调工作，负责演习组织、过程监控、技术指导、应急保障、风险控制、演习总结、技术措施与策略优化建议等各类工作。

紫队组织蓝队对实际环境实施攻击，组织红队实施防守，目的是通过演习检验参演单位安全威胁应对能力、攻击事件检测发现能力、事件分析研判能力、事件响应处置能力以及应急响应机制与流程的有效性，提升参演单位的安全实战能力。

此外，针对某些不宜在实网中直接攻防的系统，或某些不宜实际执行的危险操作，紫队可以组织攻防双方进行沙盘推演工作，以便进一步深入评估网络安全风险及可能面临的损失与破坏。

下面，就针对紫队组织网络实战攻防演习的要素、形式和关键点分别进行介绍。

第二章　如何组织一场实战攻防演习

一、实战攻防演习组织要素

组织一次网络实战攻防演习，组织要素包括：组织单位、演习技术支撑单位、攻击队伍、防守单位这四个部分。

组织单位负责总体把控、资源协调、演习准备、演习组织、演习总结、落实整改等相关工作等。

演习技术支撑单位由专业安全公司提供对应技术支撑和保障，实现攻防对抗演习环境搭建和攻防演习可视化展示。

攻击队伍，一般由多家安全厂商独立组队，每支攻击队一般配备3—5人。在获得授权前提下，以资产探查、工具扫描和人工渗透为主进行渗透攻击，以获取演习目标系统权限和数据。

防守队伍，由参演单位、安全厂商等人员组成，主要负责对防守方所管辖的资产进行防护，在演习过程中尽可能不被蓝队拿到权限和数据。

二、实战攻防演习组织形式

网络实战攻防演习的组织形式根据实际需要出发，

主要有以下两种。

1）由国家、行业主管部门、监管机构组织的演习

此类演习一般由各级公安机关、各级网信部门、政府、金融、交通、卫生、教育、电力、运营商等国家、行业主管部门或监管机构组织开展。针对行业关键信息基础设施和重要系统，组织攻击队以及行业内各企事业单位进行网络实战攻防演习。

2）大型企事业单位自行组织演习

央企、银行、金融企业、运营商、行政机构、事业单位及其他政企单位，针对业务安全防御体系建设有效性的验证需求，组织攻击队以及企事业单位进行实战攻防演习。

二、实战攻防演习组织关键

实战攻防演习得以成功实施，组织工作包括：演习范围、周期、场地、设备、攻防队伍组建、规则制定、视频录制等多个方面。

演习范围：优先选择重点（非涉密）关键业务系统及网络。

演习周期：结合实际业务开展，一般建议1—2周。

演习场地：依据演习规模选择相应的场地，可以

容纳指挥部、攻击方、防守方，三方场地分开。

演习设备：搭建攻防演习平台、视频监控系统，为攻击方人员配发专用电脑（或提供虚拟攻击终端）等。

攻击方组建：选择参演单位自有人员或聘请第三方安全服务商专业人员组建。

防守队组建：以各参演单位自有安全技术人员为主，聘请第三方安全服务商专业人员为辅构建防守队伍。

演习规则制定：演习前明确制定攻击规则、防守规则和评分规则，保障攻防过程有理有据，避免攻击过程对业务运行造成不必要的影响。

演习视频录制：录制演习的全过程视频，作为演习汇报材料以及网络安全教育素材，内容包括：演习工作准备、攻击队攻击过程、防守队防守过程以及裁判组评分过程等内容。

第三章 攻防演习组织的不同阶段

实战攻防演习的组织一般可分为五个阶段。

1）组织策划阶段

此阶段明确演习最终实现的目标，组织策划演习各项工作，形成可落地、可实施的实战攻防演习方案，并需得到领导层认可。

2）前期准备阶段

在已确定实施方案基础上开展资源和人员的准备，落实人财物。

3）实战攻防演习阶段

是整个演习的核心，由组织方协调攻防两方及其他参演单位完成演习工作，包括演习启动、演习过程、演习保障等。

4）应急演练阶段

针对演习过程中发生的突发事件，由组织方协调攻防双方完成应急响应工作，及时恢复业务和检验防守方的应急响应能力和机制。

5）演习总结阶段

先恢复所有业务系统至日常运行状态，再进行工

作成果汇总，为后期整改建设提供依据。

在某些情况下，演习过程还可能会追加第六个阶段，即沙盘推演阶段。所谓沙盘推演：是实战演习的补充，对无法进行实战演习的关基系统开展沙盘推演，评估真实网络攻击可能对政企机构及公共安全产生的实际影响。

沙盘推演并不是实战攻防演习的必选阶段，其整体策划和组织过程也分为多个阶段。关于沙盘推演的组织过程，我们将在下一章中进行独立的论述与说明。

下面依次对除沙盘推演外的上述各个阶段进行详细介绍。

一、组织策划阶段

网络实战攻防演习是否成功，组织策划环节非常关键。组织策划阶段主要从建立演习组织、确定演习目标、制定演习规则、确定演习流程、搭建演习平台、应急保障措施这六个方面进行合理规划、精心编排，这样才能指导后续演习工作开展。

（一）建立演习组织

为确保攻防演习工作顺利进行，成立实战攻防演习工作组及各参演小组，组织架构通常如图 1 所示。

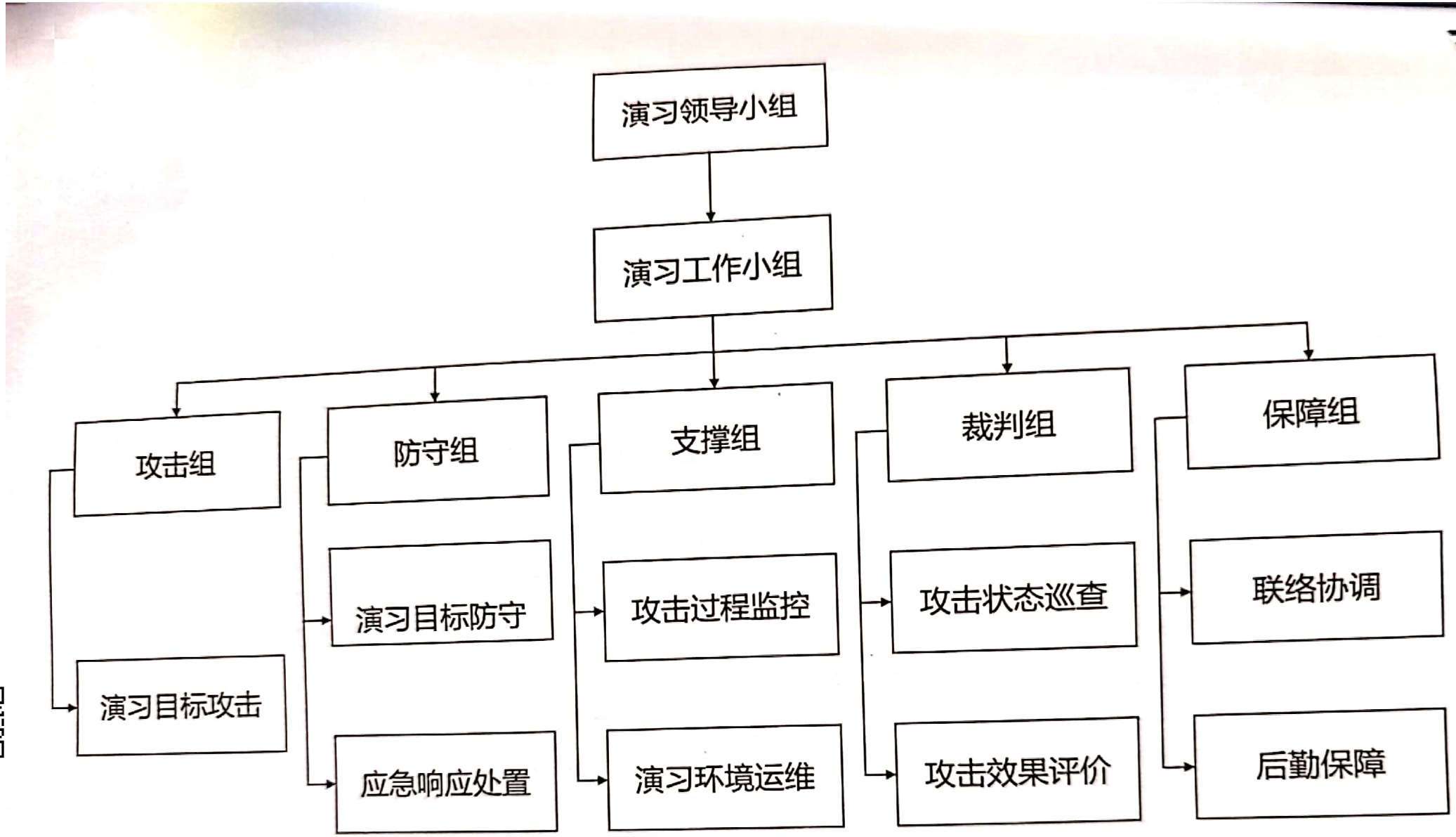

图1 演习组织机构设置示意图

演习指挥小组（指挥部）：由组织单位相关部门领导和技术专家共同组成，负责演习工作总体指挥和调度。

演习工作小组：由演习指挥小组指派专人构成，负责演习工作具体实施和保障。下设如下实施小组。

1）攻击组

由参演单位及安全厂商攻击人员构成，一般由攻防渗透人员、代码审计人员、内网攻防渗透人员等技术人员组成。负责对演习目标实施攻击。

2）防守组

由各个防护单位运维技术人员和安全运营人员组成，负责监测演习目标，发现攻击行为，遏制攻击行为，进行响应处置。

3）支撑组

其职责是攻防过程整体监控，主要工作为攻防过程中实时状态监控、阻断处置操作等，保障攻防演习过程安全、有序开展。演习组织方，即紫队需要负责演习环境运维，维护演习 IT 环境和演习监控平台正常运行。

4）裁判组

由攻防演习主导单位组织形成专家组和裁判组，负责攻防演习过程中巡查各个攻击小组，即蓝队的攻击状态，监督攻击行为是否符合演习规则，并对攻击效果进行评价。专家组负责对演习整体方案进行研究，在演习过程中对攻击效果进行总体把控，对攻击成果进行研判，保障演习安全可控。裁判组负责在演习过程中对攻击状态和防守状态进行巡查，对攻击方操作进行把控，对攻击成果判定相应分数，依据公平、公正原则对参演攻击队和防守单位给予排名。

5）保障组

由演习组织方指定工作人员组成，负责演习过程中协调联络和后勤保障等相关事宜，包括演习过程中应急响应保障、演习场地保障、演习过程中视频采集等工作。

（二）确定演习目标

依据实战攻防演习需要达到的演习效果，对参演单位业务和信息系统全面梳理，可以由演习组织方选定或由参演单位上报，最终选取确认演习目标系统。通常会选择关键信息基础设施、重要业务系统、门户网站等作为演习首选目标。

（三）制定演习规则

依据演习目标结合实际演习场景，细化攻击规则、防守规则和评分规则。为了鼓励和提升防守单位防守技术能力，可以适当增加防守方反击得分规则。

演习时间：通常为工作日5×8小时，组织单位视情况还可以安排为7×24小时。

沟通方式：即时通信软件、邮件、电话等。

（四）确定演习流程

实战攻防演习正式开始后的流程一般如图2所示。

1）确认人员就位

确认攻击组人员以及攻防演习组织方、防守组人员按要求到位。

2）确认演习环境

攻击组与技术支撑组确认演习现场和演习平台准备就绪。

3）确认准备工作

防守组确认参演系统备份情况，目标系统是否正常，并已做好相关备份工作。

4）演习开始

各方确认准备完毕，演习正式开始。

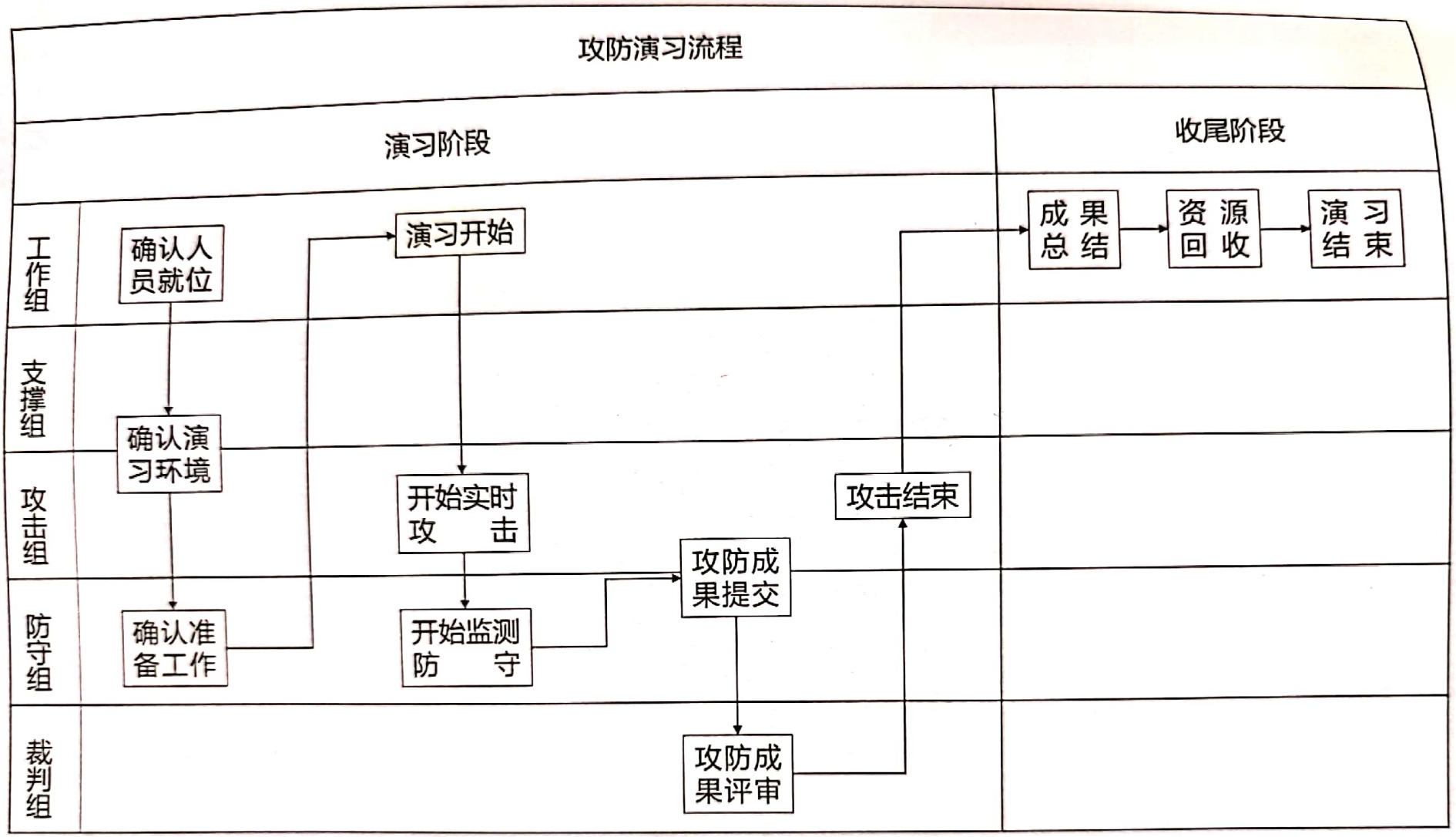

图2 实战攻防演习流程示意图

5）攻击组实施攻击

蓝队对目标系统开展网络攻击，记录攻击过程和成果证据。

6）防守组监测攻击

防守组可利用安全设备对网络攻击进行监测，对发现的攻击行为进行分析确认，详细记录监测数据。

7）提交成果

演习过程中，蓝队人员发现可利用安全漏洞，将获取的权限和成果截图保存，通过平台进行提交。

8）漏洞确认及研判

由专家组对提交的漏洞进行确认，确认漏洞的真实性，并根据演习计分规则进行分数评判。

9）攻击结束

在演习规定时间外，攻击组人员停止对目标系统的攻击。

10）成果总结

演习工作组协调各参演小组，对演习中产生的成果、问题、数据进行汇总，输出相关演习总结报告。

11）资源回收

由演习工作组负责对各类设备、网络资源进行回

收，同时对相关演习数据进行回收处理，并监督攻击组人员对在演习过程中使用的木马、脚本等数据进行清除。

12）演习结束

对所有目标系统攻击结束后，工作小组还需要进行内部总结汇报，演习结束。

（五）搭建演习平台

为了保证演习过程安全可靠，需搭建攻防演习平台，演习平台可为攻击人员提供攻击IP、反弹回联虚拟机、虚拟网络分组。攻击方通过平台进行实时攻击和成果提交，防守方通过平台进行防守成果上报，保障所有操作可追溯、可审计，尽可能地降低演习所产生的风险。

（六）应急保障措施

指攻防演习中发生不可控突发事件，导致演习过程中断、终止时，所需要采取的处置措施预案。需要预先对可能发生的紧急事件（如断电、断网、业务停顿等）做出临时处置安排措施。攻防演习中一旦参演系统出现问题，防守方应采取临时处置安排措施，及时向指挥部报告，由指挥部通知蓝队在第一时间停止攻击。指挥部应组织攻、防双方制定攻击演习应急相

应预案，具体应急响应预案在演习实施方案中完善。

二、前期准备阶段

实战攻防演习能否顺利、高效开展，必须提前做好两项准备工作，一是资源准备，涉及场地、演习平台、演习设备、演习备案、演习授权、保密工作以及规则制定等；二是人员准备，包括攻击人员、防守人员的选拔、审核和队伍组建等。

1）资源准备

演习场地布置：演习展示大屏、办公桌椅、攻击队网络搭建、演习会场布置等。

演习平台搭建：攻防平台开通、攻击方账户开通、IP分配、防守方账户开通，做好平台运行保障工作。

演习人员专用电脑：配备专用电脑，安装安全监控软件、防病毒软件、录屏软件等，做好事件回溯机制。

视频监控部署：部署攻防演习场地办公环境监控，做好物理环境监控保障。

演习备案：演习组织方向上级主管单位及监管机构（公安、网信等）进行演习备案。

演习授权：演习组织方向攻击队和平台提供方进

行正式授权，确保演习工作在授权范围内有序进行。

保密协议：与参与演习工作的第三方人员签署相关保密协议，确保信息安全。

攻击规则制定：攻击规则包括攻击队接入方式、攻击时间、攻击范围、特定攻击事件报备等，明确禁止使用的攻击行为，如；导致业务瘫痪、信息篡改、信息泄露、潜伏控制等动作。

评分规则制定：依据攻击规则和防守规则，制定相应评分规则。例如，防守方评分规则包括：发现类、消除类、应急处置类、追踪溯源类、演习总结类加分项以及减分项等；攻击方评分规则包括：目标系统、集权类系统、账户信息、重要关键信息系统加分以及违规减分项等。

2）人员准备

蓝队：组建攻击队，确定攻击队数量，每队参与人员数量建议3—5人、对人员进行技术能力、背景等方面审核，确定防守方负责人并构建攻击方组织架构，签订保密协议；向攻击人员宣贯攻击规则及演习相关要求。

红队：组建防守队，确定采用本组织人员作为防守人员，或请第三方人员加入，对人员进行技术能力、

背景等方面审核，确定防守方负责人并构建防守方组织架构。第三方人员签署保密协议，向防守方宣贯防守规则及演习相关要求。

三、实战攻防演习阶段

（一）演习启动

演习组织方组织相关单位召开启动会议，部署实战攻防演习工作，对攻防双方提出明确工作要求、制定相关约束措施，确定相应的应急预案，明确演习时间，宣布正式开始演习。

实战攻防演习启动会的召开是整个演习过程的开始，启动会需要准备好相关领导发言，宣布规则、时间、纪律要求，攻防方人员签到与鉴别，攻击方抽签分组等工作。启动会约为30分钟，确保会议相关单位及部门领导及人员到位。

（二）演习过程

演习过程中组织方依据演习策划内容，协调攻击方和防守方实施演习，在过程中开展包括演习监控、演习研判、应急处置等主要工作。

1）演习监控

演习过程中攻方和守方的实时状态以及比分状况

将通过安全可靠的方式接入到组织方内部的指挥调度大屏，领导、裁判、监控人员可以随时进行指导、视察。全程对被攻击系统的运行状态进行监控，对攻击人员操作行为进行监控，对攻击成果进行监控，对防守方攻击发现、响应处置进行监控，掌握演习全过程，达到公平、公正、可控的实战攻防演习。

2）演习研判

演习过程中对攻击方及防守方成果进行研判，从攻击方及防守方的过程结果进行研判评分。对攻击方的评分机制包括：攻击方对目标系统攻击所造成实际危害程度、准确性、攻击时间长短以及漏洞贡献数量等，对防守方的评分机制包括：发现攻击行为、响应流程、防御手段、防守时间等。通过多个角度进行综合评分，从而得出攻击方及防守方最终得分和排名。

3）演习处置

演习过程中如遇突发事件，防守方无法有效应对时，由演习组织方提供应急处置人员对防守方出现的问题快速定位、分析、恢复保障演习系统或相关系统安全稳定运行，实现演习过程安全可控。

4）演习保障

人员安全保障：演习开始后需要每日对攻防方人

员签到与鉴别，保障参与人员全程一致，避免出现替换人员的现象，保障演习过程公平、公正。

攻击过程监控：演习开始后，通过演习平台监控攻击人员的操作行为，并进行网络全流量监控；通过视频监控对物理环境及人员全程监控，并且每日输出日报，对演习进行总结。

专家研判：聘请专家裁判通过演习平台开展研判，确认攻击成果，确认防守成果，判定违规行为等，对攻击和防守给出准确的裁决。

攻击过程回溯：通过演习平台核对攻击方提交成果与攻击流量，发现违规行为及时处理。

信息通告：利用信息交互工具，如蓝信平台，建立指挥群统一发布和收集信息，做到信息快速同步。

人员保障：采用身份验证的方式对攻击方人员进行身份核查，派专人现场监督，建立应急团队待命处置突发事件，演习期间派医务人员实施医务保障。

资源保障：对设备、系统、网络链路每日例行检查，做好资源保障。

后勤保障：安排演习相关人员合理饮食、现场预备食物与水。

突发事件应急处置：确定紧急联系人列表，执行预案，突发事件报告指挥部，开展应急演练工作。

四、应急演练阶段

在演习过程中，针对参演单位失陷的业务系统，组织攻击队和参演单位进行应急事件处理，目的是通过应急演练，快速恢复业务和检验参演单位应急响应机制与流程，利用实战演习环境，将演练实战化，提升参演单位应急响应能力和完善应急响应机制。

（一）检测阶段

1）目标

接到事故报警后在服务对象的配合下对异常的系统进行初步分析，确认其是否真正发生了信息安全事件，制定进一步的响应策略，并保留证据。

2）角色

应急服务实施小组成员、样本分析组、漏洞分析组。

3）内容

a）检测范围及对象的确定

b）检测方案的确定

c）检测方案的实施

d）检测结果的处理

4）输出

撰写完成《应急响应检查单》。

（二）抑制阶段

1）目标

及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏，同时要确保封锁方法对涉及相关业务影响最小。

2）角色

应急服务实施小组成员、样本分析组、漏洞分析组。

3）内容

a）抑制方案的确定

b）抑制方案的认可

c）抑制方案的实施

d）抑制效果的判定

4）输出

撰写完成《应急处置方案》。

（三）根除阶段

1）目标

对事件进行抑制之后，通过对有关事件或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。

2）角色

应急服务实施小组成员、样本分析组、漏洞分析组。

3）内容

a）根除方案的确定

b）根除方案的认可

c）根除方案的实施

d）根除效果的判定

4）输出

撰写完成《根除处理记录表》。

（四）恢复阶段

1）目标

恢复安全事件所涉及的系统，并还原到正常状态，使业务能够正常进行，恢复工作应避免出现误操作导致数据的丢失。

2）角色

应急服务实施小组。

3）内容

a）恢复方案的确定

b）恢复信息系统

（五）总结阶段

1）目标

通过以上各个阶段的记录表格，回顾安全事件处理的全过程，整理与事件相关的各种信息，进行总结，并尽可能地把所有信息记录到文档中。

2）角色

应急服务实施小组。

3）内容

a）事故总结

应急服务实施小组应及时检查安全事件处理记录是否齐全，是否具备可塑性，并对事件处理过程进行总结和分析。应急处理总结的具体工作包括但不限于：事件发生的现象总结、事件发生的原因分析、系统的损害程度评估、事件损失估计、采取的主要应对措施、相关的工具文档（如专项预案、方案等）归档。

b）事故报告

应急服务实施小组应向服务对象提供完备的网络

安全事件处理报告、网络安全方面的措施和建议。

五、演习总结阶段

（一）演习恢复

演习结束需做好相关保障工作，如收集报告、清除后门、回收账户及权限、设备回收、网络恢复等工作，确保后续正常业务运行稳定。相关内容如下。

1）收集报告

收集攻击方提交的总结报告和防守方提交的总结报告并汇总信息。

2）清除后门

依据攻击方报告和监控到的攻击流量，将攻击方上传的后门进行清除。

3）账号及权限回收

攻击方提交报告后，收回攻击方所有账号及权限，包括攻击方在目标系统上新建的账号。

4）攻击方电脑回收

对攻击方电脑（或虚拟终端）进行格式化处理，清除过程数据。

5）网络访问权限回收

收回攻击方网络访问权限。

6）演习数据清理

当主办方完成演习数据导出后，对平台侧的演习数据进行清理。

（二）演习总结

演习总结主要包括由参演单位编写总结报告，评委专家汇总演习成果，演习全体单位召开总结会议，演习视频编排与宣传工作的开展。对整个演习进行全面总结，对发现问题积极开展整改，开展后期宣传工作，体现演习的实用性。

1）成果确认

以攻击方提供的攻击成果确认被攻陷目标的归属单位或部门，落实攻击成果。

2）数据统计

汇总攻防方和防守方成果，统计攻防数据，进行评分与排名。

3）总结会议

参演单位进行总结汇报，组织方对演习进行总体评价，攻防方与防守方进行经验分享，对成绩优异的参演队伍颁发奖杯和证书，对问题提出改进建议和整改计划。

4）视频汇报与宣传

制作实战攻防演习视频，供防守方在内部播放宣传，提高人员安全意识。

（三）整改建议

实战攻防演习工作完成后，演习组织方组织专业技术人员和专家，汇总、分析所有攻击数据，进行充分、全面的复盘分析，总结经验教训，并对不足之处给出合理整改建议，为防守方提供具有针对性的详细过程分析报告，随后下发参演防守单位，督促整改并上报整改结果。后续防守方应不断优化防护工作模式，循序渐进完善安全防护措施，优化安全策略，强化人员队伍技术能力，整体提升网络安全防护水平。

第四章 沙盘推演组织的不同阶段

沙盘推演是在实战攻防演习的基础上，继攻击路线、攻击手段等方面的有效性在被证实的基础上，评估真实网络攻击可能对政企机构及公共安全产生的实际影响，包括经济损失、声誉损失和可能的社会影响等。同时，对攻防过程中应急响应的有效性进行全过程评估。

传统的实战攻防演习，更多关注的是技术层面、管理层面的安全风险和攻击有效性。所以，沙盘推演并不是传统攻防演习的必选阶段。但是，作为安全损失评估的重要过程，沙盘推演给演习机构进行科学合理的安全规划、安全建设和安全投入提供了关键性的参考依据。因此，沙盘推演的概念和方法一经提出，就备受关注，并在越来越多的实战攻防演习中被吸收和采纳。

沙盘推演的整体策划和组织过程也分为多个阶段。一般来说，主要包括以下四个阶段。

一、组织策划阶段

组织策划阶段的主要目的是通过建立推演组织、明确推演目标、搭建推演平台、确定推演流程和制定

推演规则等工作并形成策划方案，为沙盘推演打下基础。

（一）建立推演组织

为保证沙盘推演工作的顺利完成，组建沙盘推演工作小组，组织架构具体如图 3 所示。

1）指挥组

指挥组主要由推演组织单位组成，主要负责推演工作的指挥协调、过程策划、人员选定，规则制定等工作。

2）攻击组

攻击组主要由攻防演习中攻击队人员组成，负责攻击方案制定、讲解等工作。

3）防守组

防守组主要由参演企业网络安全人员、业务系统负责人、目标企业相关财务、法务和公关人员组成。业务系统负责人的作用为评估网络攻击对企业业务产生的影响，包括但不限于以下几个方面。

a）财务人员负责评估模拟攻击可能造成的经济损失。

图3 沙盘推演组织架构示意图

b）法务人员负责评估模拟攻击可能造成的政策监管风险。

c）公关人员负责评估模拟攻击可能造成的声誉影响。

4）专家组

专家组主要由组织单位邀请行业专家和高级技术专家组成，主要负责对推演过程中攻防双方方案可行性进行点评并打分。

（二）明确攻击目标

依据沙盘推演需要达到的目标及影响范围，选定推演拟攻击的目标系统。一般应优先选择关键业务系统，覆盖多区域的业务专网作为模拟攻击目标进行推演。

（三）搭建推演平台

为了体现推演过程中攻防双方结果，方便专家组根据评分规则进行点评，需搭建沙盘推演平台，推演平台可为在攻防双方推演过程中展示攻防手段和为专家组依据评分规则进行评分。

（四）确定推演流程

推演阶段是沙盘推演过程中最重要的阶段，推演

过程根据不同的业务场景分为多场推演，每场推演依据不同的攻击方案设定为一轮或多轮。图4所示为可参考的一般推演流程。

1）攻击组讲解攻击方案

由攻击组结合实战演习结果对提供攻击方案的可行性论证，同时说明攻击过程预计将会投入的间、人力和物力，以及相关投入的科学性。

2）防守组提问

由防守组对攻击组提出的攻击方案及攻击思路进行提问和置辩，以确认攻击方案的可行性。

3）防守组汇报防守方案

防守组针对攻击组提出的攻防方案，提出可行的防守方案并与攻击组置辩相关方案的可行性。

4）攻击组补充发言

根据防守方已经确认的可行性方案，提出自己将要采取的实际攻击及进一步行动，如数据篡改、窃取、删除等，攻击范围，攻击效果等可行性。

5）防守组补充发言

提出自己的应急响应方案，并估算投入成本，包括投入的时间、人力、物力等。

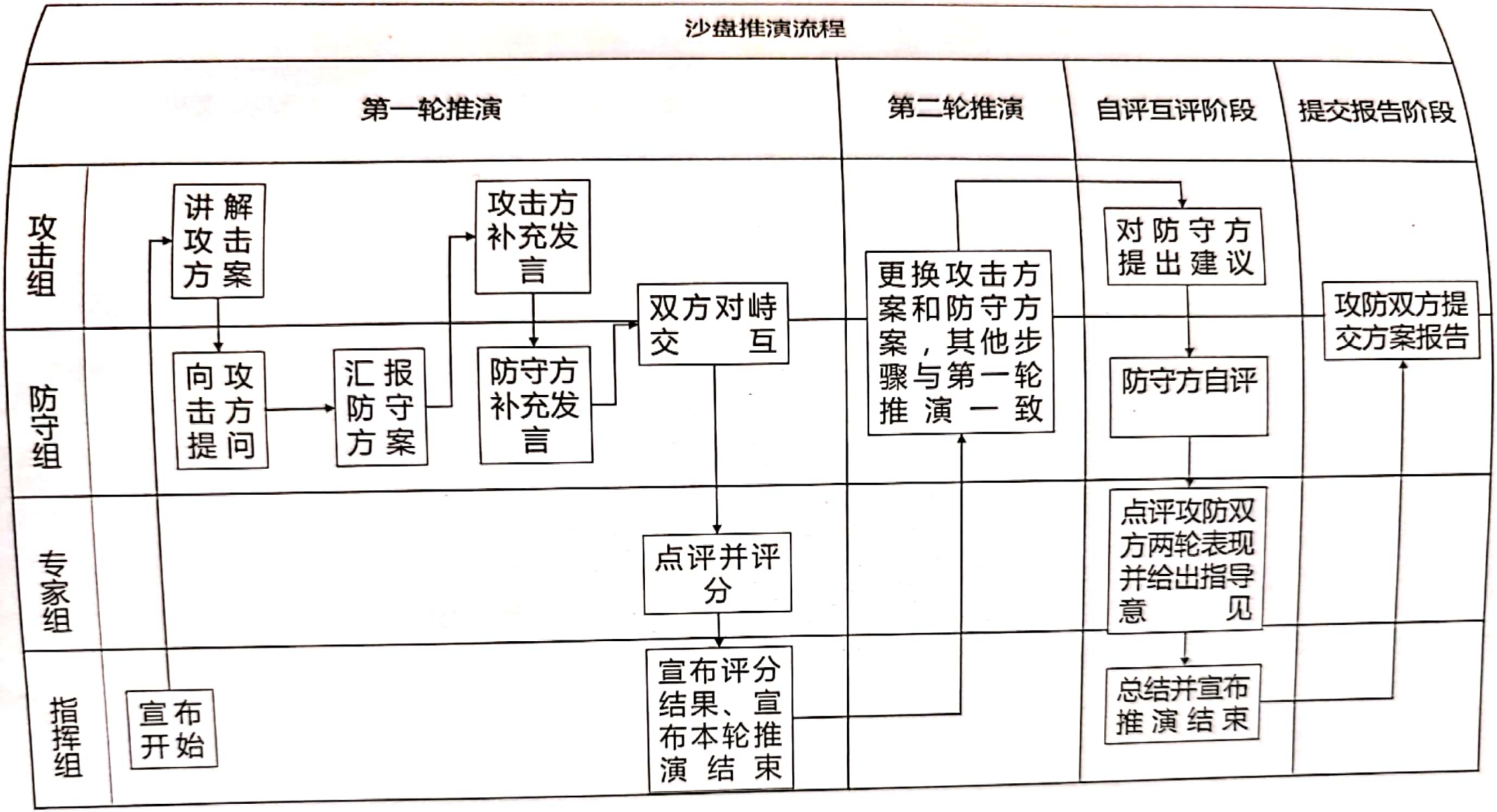

图4 沙盘推演流程示意图

6）双方对峙交互

双方对对峙过程进行交互，论证双方投入的时间、人力、物力的可行性，避免出现理论可行，而实施成本过高的假设出现。

7）专家组点评并评分

双方发言结束后，由专家组人员对攻防双方表现进行评价，并根据打分规则，对攻防双方表现进行评分。

8）宣布第一轮评分结果

指挥组宣布评分结果及主要结论，并宣布第一轮推演结束。

按照以上流程，依据攻击组其他攻击方案开展后面几轮推演工作。并在多轮推演结束后，开展以下工作。

1）攻击组对防守组提出建议

攻击组针对上述两轮推演对防守组提出安全建议。

2）防守组自评

防守组对两轮防守策略、方案、表现进行自评。

3）专家组点评

综合两轮推演，专家组对攻击组和防守组依据评分规则使用评分平台对攻防双方进行评分，并给出指导意见。

4）宣布推演结束

指挥组宣布推演结束。

5）提交报告

攻防双方提交方案报告。

（五）制定推演规则

沙盘推演第一要素是规则，如，攻方如何证明攻击路线和攻击手段的有效性。守方如何证明其应对措施和有效性及可能的响应周期。攻防双方需共同对评估结果的科学性提供保障，制定规则的目标也是保证这种结果的科学性，指挥组应依据实际环境，制定相应的评分规则。

推演周期一般建议1—2天，单场推演建议不超过3小时。

建议攻击组的攻击方案在推演开始前1小时内再向防守组公布，因为做好攻击方案保密工作，是最大限度模拟实际攻击过程，检验防守方反应能力的有效方法。攻防双方推演时间需控制在指定范围内。

二、推演准备阶段

推演准备阶段的主要目的是基于策划方案，依据推演实际环境进行演示环境搭建，初步形成推演演示

环境，主要工作内容为攻击方案筛选、推演平台搭建、推演展台搭建、推演人员准备等工作。

（一）攻击方案筛选

推演准备阶段需要由攻击方提前提交攻击方案，由专家组进行评审，并指导攻击方对方案进行调整与优化，选取优秀方案纳入推演环节。

（二）推演平台搭建

依据现场实际场景，搭建推演平台，导入攻击组方案形成攻击路线图，并在推演开始前导入防守组方案，主要用于防守组质辩过程中防守方案的展示，开通对应专家组账号。

（三）推演展台搭建

依据推演模式选择可容纳攻击组、防守组、专家组、导调组等人员的场地。根据现场环境的实际情况，搭建展示大屏、攻防展台、灯光等会场布置。

（四）推演人员准备

1）攻击组人员准备

攻击组人员可为攻防演习阶段蓝队或邀请第三方蓝队人员，攻击组人员需具备蓝队攻击经验，了解防守方网络架构及安全脆弱点并能够制定专项攻击方案等能力，建议组建2队，每队2—3人。涉及第三方蓝

队人员加入，需签订保密协议，并宣贯推演规则。

2）防守组人员准备

防守组人员为实际目标系统网络安全运营人员和业务系统负责人以及财务、会务和公关等评估人员组成，防守推演人员建议至少组建2组，每组2—3人。

3）现场保障人员准备

应由指挥组组建现场保障团队，主要负责对推演现场环境、展示、平台等运行保障工作。

4）现场摄制人员准备

如需现场对推演过程进行拍摄，指挥组需组建现场拍摄团队进行拍摄。

5）主持人准备

主持人主要负责推演全过程中现场节奏把控，由指挥组指定对应人员负责。

三、沙盘推演阶段

推演过程由指挥组依据推演策划内容，协调攻击组与防守组实施推演，推演过程中主要包括推演过程、评估影响、专家评分等工作。

（一）推演过程

沙盘推演主要由攻防双方根据对应方案展开阐述

和对峙，推演过程中指挥组应确保双方在质证过程中按规则执行，确保双方关注点不跑偏。

（二）评估影响

推演过程中，需由评估人员，即防守方会务人员、财务人员和公关人员在攻防双方质证结束后对推演影响进行评估，并输出攻防双方本次推演的可行性评估方案及评估损失文档。

（三）专家评分

攻防双方对峙结束后，专家组依据评分规则对攻防双方方案可行性进行点评、评分。如：攻击方评分规则主要从：技术水平、攻击危害性、可实现性等方面；防守方评分规则主要从：监测、发现、应急处置、协调配合等方面。

（四）推演保障

现场保障：需对现场平台、展台、网络链路例行检查，做好资源保障；确定紧急联系人列表，主要负责推演现场平台或展台突发故障应急事宜，执行预案，突发事件报告指挥组。

四、总结评估阶段

总结阶段的工作目的是通过对沙盘推演整体过程

进行复盘、总结汇报。推演结束后，攻击方和防守方需向指挥组提供本次推演相关材料，由指挥组进行评审以及后续工作开展。

第五章 实战攻防演习风险规避措施

实战攻防演习前需制定攻防演习约束措施，规避可能出现的风险，明确提出攻防操作的限定规则，保证攻防演习能够在有限范围内安全开展。

一、演习限定攻击目标系统，不限定攻击路径

演习时，可通过多种路径进行攻击，不对攻击方所采用的攻击路径进行限定。在攻击路径中发现的安全漏洞和隐患，攻击方实施的攻击应及时向演习指挥部报备，不允许对其进行破坏性的操作，避免影响业务系统正常运行。

二、除授权外，演习不允许使用拒绝服务攻击

由于演习在真实环境下开展，为不影响被攻击对象业务的正常开展，演习除非经演习主办方授权，否则不允许使用 SYN FLOOD、CC 等拒绝服务攻击手段。

三、网页篡改攻击方式的说明

演习只针对互联网系统或重要应用的一级或二级页面进行篡改，以检验防守方的应急响应和侦查调查能力。演习过程中，攻击团队要围绕攻击目标系统进行攻击渗透，在获取网站控制权限后，需先请示演习

指挥部，演习指挥部同意后在指定网页张贴特定图片（由演习指挥部下发）。如目标系统的互联网网站和业务应用防护严密，攻击团队可以将与目标系统关系较为密切的业务应用作为渗透目标。

四、演习禁止采用的攻击方式

实战攻防演习中的攻防手法也有一些禁区。设置禁区的目的是确保通过演习发现的信息系统安全问题真实有效。一般来说，禁止采用的攻击方式主要有三种：

1）禁止通过收买防守方人员进行攻击；

2）禁止通过物理入侵、截断监听外部光纤等方式进行攻击；

3）禁止采用无线电干扰机等直接影响目标系统运行的攻击方式。

五、攻击方木马使用要求

木马控制端须使用由演习指挥部统一提供的软件，所使用的木马应不具有自动删除目标系统文件、损坏引导扇区、主动扩散、感染文件、造成服务器宕机等破坏性功能。演习禁止使用具有破坏性和感染性的病毒、蠕虫。

六、非法攻击阻断及通报

为加强对各攻击团队攻击的监测，通过攻防演习平台开展演习全过程的监督、记录、审计和展现，避免演习影响业务正常运行。演习指挥部应组织技术支持单位对攻击全流量进行记录、分析，在发现不合规攻击行为时，阻断非法攻击行为，并转由人工处置，对攻击团队进行通报。

红蓝紫实战攻防

演习手册

THE PRACTICAL PLAYBOOK OF OFFENSE & DEFENSE
BY RED-BLUE-PURPLE TEAM

蓝队视角下的防御体系突破

本系列丛书的第一册，希望通过归纳总结蓝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”。

红队视角下的防御体系构建

本系列丛书的第二册，希望通过归纳总结红队防御的四个阶段、应对攻击的常用策略，以及建立实战化安全体系的基本方法，帮助政企机构查找薄弱环节，更好地提升演习水平，构筑更有效的安全防御体系。

紫队视角下的实战攻防演习组织

本系列丛书的第三册，重点介绍实战环境下的紫队工作，提出如何组织一场有效的实战攻防演习、如何组织在演习过程中的应急事件演练、如何组织对无法开展实战演习关基设施的沙盘推演。

奇安信客服电话

客服热线：4009-303-120、400-678-3600

7×24应急响应：4009-727-120

奇安信集团官网

奇安信微信公众号