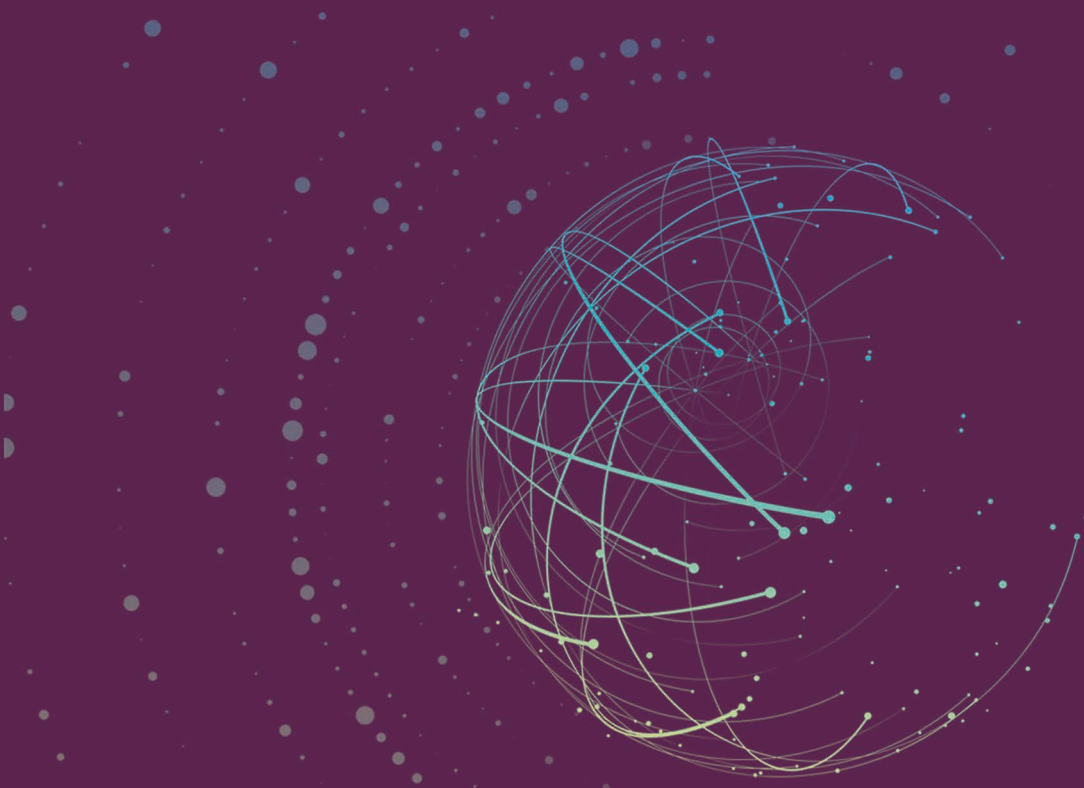
实战攻防演习之

奇安信
新一代网络安全领军者

紫队视角下的
实战攻防演习组织



奇安信安服团队

2019年8月

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，最大限度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。

作为国内领先的网络安全企业，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。

《紫队视角下的实战攻防演习组织》是本系列丛书的第三本。本书重点介绍实战环境下的紫队工作，提出组织实战攻防演习的四个阶段，给出实战攻防演习的组织要素、组织形式，明确演习各方的人员职责，描述每阶段需开展的重点工作，并提示在开展实战攻防演习时应规避的风险。

目 录

第一章　什么是紫队

紫队，一般是指网络实战攻防演习中的组织方。

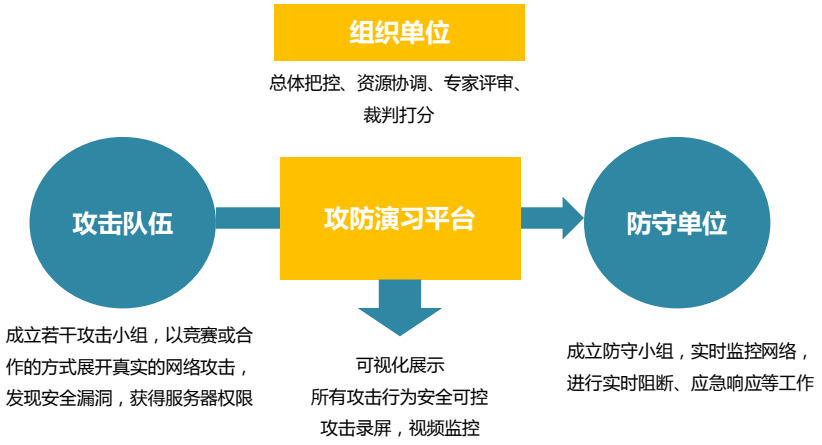
紫队是在实战攻防演习中，以组织方角色，开展演习的整体组织协调工作，负责演习组织、过程监控、技术指导、应急保障、演习总结、技术措施与策略优化建议等各类工作。

紫队组织红队对实际环境实施攻击，组织蓝队实施防守，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、事件分析研判能力和事件响应处置能力，提升被检测机构安全实战能力。

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。

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（即红队）、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，也即红队，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，也即蓝队，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红队拿到权限和数据。

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。

三、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。

第二章　实战攻防演习组织的四个阶段

实战攻防演习的组织可分为四个阶段：

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。

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。

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。

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。

下面依次进行详细介绍。

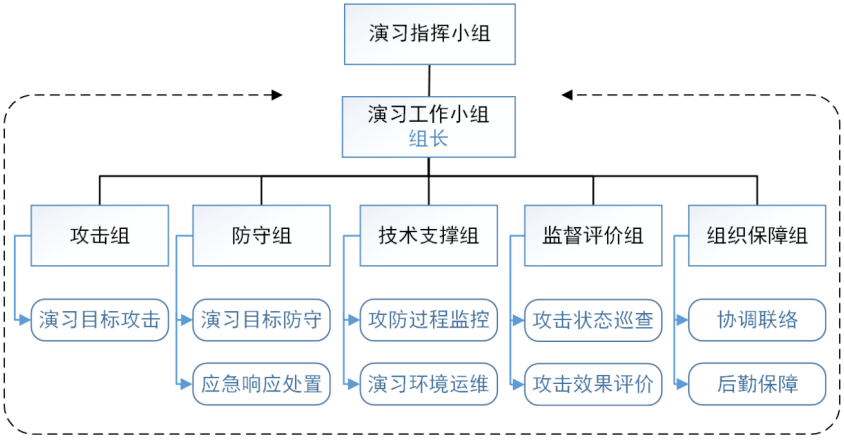
一、组织策划阶段

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，组织架构通常如下：



演习组织机构设置示意图

1）攻击组（红队）

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）技术支撑组

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）监督评价组

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，即红队的攻击状态，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）组织保障组

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

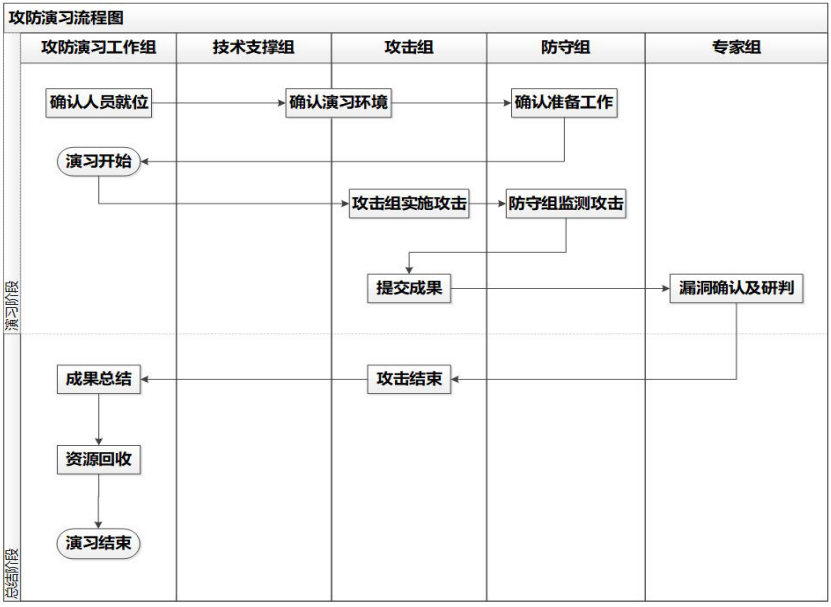
依据演习目标结合实际演习场景，细化攻击规则、防守规则和评分规则。为了鼓励和提升防守单位防守技术能力，可以适当增加防守方反击得分规则。

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所示：



1）确认人员就位

确认红队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。

5）攻击组实施攻击

红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，红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，演习平台包括：攻击场地、防守场地、攻击目标信息系统、指挥大厅、攻击行为分析中心。

1）攻击场地

攻击场地可分为场内攻击和场外攻击，搭建专用的网络环境并配以充足的攻击资源。正式攻击阶段，攻击小组在对应场所内实施真实性网络攻击。场地内部署攻防演习监控系统，协助技术专家监控攻击行为和流量，以确保演习中攻击的安全可控。

2）防守场地

防守场地主要是防守方演习环境，可通过部署视频监控系统将防守工作环境视频回传指挥中心。

3）攻击目标信息系统

攻击目标信息系统即防守方网络资产系统。防守方在被攻击系统开展相应的防御工作。

4）攻击行为分析中心

攻击行为分析中心通过部署网络安全审计设备对攻击者攻击行为进行收集及分析，实时监控攻击过程，由日志分析得出攻击步骤，建立完整的攻击场景，直观地反应目标主机受攻击的状况，并通过可视化大屏实时展现。

5）指挥大厅

演习过程中，攻方和守方的实时状态将接入到指挥大厅监控大屏，领导可以随时进行指导、视察。

（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，由指挥部通知红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，涉及到场地、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

红队：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。

蓝队：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。

四、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。

（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。

第三章　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

木马控制端需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。

附录　奇安信实战攻防演习组织经验

2018年至2019年上半年，奇安信已参与组织实战攻防演习56次，在演习组织上投入的工作量达1463人天。组织演习的对象包括部委、省市级政府、省公安和网信等主管机构，以及银行、交通、能源、民生、传媒、医疗、教育、生态、烟草、互联网公司等行业单位。演习的目标系统涵盖内外网、网站、大数据平台、交易系统、管理系统、工控系统、财务系统等各类业务系统和生产系统。

在所组织的实战攻防演习中，发现超过2300余台业务数据库、ERP系统、堡垒机、域控制器、测试系统等核心业务系统或服务器的权限可被获取，有效检验了参演客户在技术、管理、运营等方面存在的网络安全隐患。

奇安信安服团队