中国实战化白帽人才能力白皮书

2024.10

补天漏洞响应平台

全国网络空间安全行业产教融合共同体

奇安信安服团队

奇安信行业安全研究中心

北京理工大学

重庆电子科技职业大学

中国职业技术教育学会网络安全专委会

主要结论

- ✧ 白帽人才应该“能攻善守”。本次白皮书对实战化白帽人才能力图谱进行了重大扩充：首次将网络安全实战攻防演习中，防守侧人员需要掌握的 52 项能力纳入图谱；同时，将攻击侧人员需要掌握的能力图谱，从原有的 87 项能力扩充为 108 项能力。攻防合计包含 160 项具体能力。
- ✧ 本次白皮书改变了先前使用的“先分级再分类”的架构方式，而是完全以“知识图谱”的形式，重新架构能力图谱，这种方式更有利于明确白帽人才的培养目标和职业规划，更有利于专业学校组织教学和白帽人才自学发展。
- ✧ 本次白皮书，将 AI 辅助攻防、安全设备绕过、大模型安全等新兴攻防技术引入图谱。这些技术在近年来的网络安全实战攻防演习中，已经被越来越频繁的使用。
- ✧ 本次白皮书对 495 名白帽子进行了实战化能力调研。其中，70.4%的白帽子参与过网络安全实战攻防演习攻击队，73.8%的白帽子参与过演习防守队。同时，有 51.7%的白帽子表示自己攻防均可，攻击队防守队均参与过。
- ✧ 在攻击侧 7 大类实战化能力中，“Web 漏洞利用与挖掘”是最普及、最主要的一种攻击能力，白帽人才的平均掌握率超过六成。其次是“社工与渗透” 和“安全工具使用”，约半数的白帽人才掌握此类相关能力。各类“攻击辅助”能力和“编程与开发”能力的平均掌握率均在三成左右。与 2023 年相比，除了“编程与开发能力”的平均掌握率稍有下降外，其他各大类能力的平均掌握率均有 0.5%~3.2%不等的小幅提升。

关键字：实战化、白帽子、攻防演习、能力图谱、漏洞挖掘、安全检查、情报

目　　录

研究背景

本白皮书由补天漏洞响应平台、全国网络空间安全行业产教融合共同体、奇安信安服团队、奇安信行业安全研究中心、北京理工大学、重庆电子科技职业大学联合发布，并得到了中国职业技术教育学会网络安全专委会的指导。白皮书结合攻防双方的实战化要求，绘制了实战化白帽人才能力图谱，并以此为基础展开广泛调研，形成报告。

一、 能力图谱的升级

作为一名白帽子，仅仅会挖洞或简单的漏洞利用，是远远不够的，无满足网络安全的实战化要求。所谓实战化要求，是指在真实运行的系统环境中，在有真人参与的网络对抗中，实现有效攻防的综合性安全能力。

为全面提升中国白帽人才的实战化能力，2021 年 1 月，补天漏洞响应平台（简称：补天平台）、奇安信安服团队、奇安信行业安全研究中心首次联合发布《中国实战化白帽人才能力白皮书（2020）》（简称：《白皮书（2020）》）。《白皮书（2020》首次结合攻防实战要求，给出了攻击侧“实战化白帽人才能力图谱”。后经不断调整升级，到了 2023 年，图谱将实战化白帽人才的能力划分为 3 个级别、14 大类、87 项具体的能力，如下图所示。

以此图谱为基础，2021 年~2023 年，补天平台连续三年对全国白帽人才的实战化能力掌握情况展开广泛的调研分析，并发布《白皮书》。《白皮书》对实战化白帽人才的能力培养给出了明确的指导方向和市场分析，引起了大量用人单位、教育机构、特别是白帽子群体的高度关注和认可。

不过，随着网络安全攻防实战的不断发展以及 AI 大模型等新型技术的出现，2020 版的实战化白帽人才能力图谱的局限性也逐渐显现出来。主要体现在以下几个方面：

首先，2020 版图谱只考虑了攻击侧人员能力，而没有考虑防守侧人员能力，这就对白帽人才的能力发展产生了一定的局限性。从历年来的网络安全实战攻防演习情况来看，无论是攻击侧人员还是防守侧人员，其共同目标都是通过对抗性的实战演练，发现系统存在的安全漏洞或安全隐患。从这个角度看，防守侧人员所需要具备的安全能力也纳入到实战化白帽人才的能力图谱中。也就是说，白帽子，不仅要能攻，而且要善守。

其次，2020 版图谱是以技能的学习难度为基础，先分级后分类。但从知识学习的角度看，有些能力实际上是相互关联，甚至是前后相通的，如 Web 漏洞利用和 Web 漏洞挖掘、基础安全工具和高级安全工具、编写 PoC 或 EXP 利用和编写 PoC 或 EXP 高级利用等。如果以知识图谱的形式重新构架能力图谱，对于白帽人才的知识体系构建与学习会更有帮助。

此外，AI 辅助攻防、安全设备绕过、大模型安全等新兴攻防技术，在近年来的网络安全实战攻防演习中也被越来越频繁的使用。这些新兴的能力点，也很有必要补充到图谱之中。

下图给出了本次报告中攻击侧与防守侧能力图谱的总览（细分到小类）。

综上，在本次白皮书中，我们对能力图谱进行了全面的升级：

1） 将能力图谱从单纯的攻击侧能力，扩展为攻防两侧能力，并对攻击侧能力进行了全面扩充。新的图谱共包含 160 项能力，其中，攻击侧能力分为 7 大类、17 小类、108

项；防守侧能力分为 5 大类、12 小类、52 项能力。

2） 改变了先前使用的“先分级再分类”的架构方式，而是完全以“知识图谱”的形式，重新架构能力图谱，这种方式更有利于明确白帽人才的培养目标和职业规划。

3） 对每一项具体能力的学习难度进行标注。三个级别的学习难度分别：基础能力（1）、进阶能力（2）、高阶能力（3）。

二、 能力分析的方法

2024 年 8 月，补天漏洞响应平台再次对平台上活跃的 495 名白帽子进行了实战化能力调研，并形成了《白皮书（2024）》。

在本次白皮书中，继续使用“平均掌握率”来对比分析各项能力或各类能力的人才掌握水平。单项能力的平均掌握率，是指在受调研的白帽子群体中，掌握某项具体的实战化能力的白帽子人数占所有受调研白帽子总人数的比例。而某一小类多项能力的总体平均掌握率，则是各单项能力的平均掌握率的总平均值。某一大类能力的总体平均掌握率，则是各小类能力的平均掌握率的总平均值具体计算方法如下：

$$\text{单项能力的平均掌握率} = \frac{\text{掌握该项能力的白帽子人数}}{\text{受调研的白帽群体总人数}}$$

$$\text{小类能力平均掌握率} = \frac{1}{N} \cdot \sum_{n=1}^{N} \text{第}n\text{项能力的平均掌握率}$$

$$\text{大类能力平均掌握率} = \frac{1}{M} \cdot \sum_{m=1}^{M} \text{第}m\text{小类能力的平均掌握率}$$

在接下来的内容中，我们将首先通过一章的内容来介绍攻击侧和防守侧的实战化能力图谱的具体构成，再通过一章内容来分析当前各类不同的实战化能力的平均掌握率情况。附录中给出了调研结果的原始数据和各项能力的具体说明，以方便白帽人才学习和研究。

第一章 实战化白帽人才能力图谱

本章结合网络安全实战攻防演习实践，给出实战化白帽人才能力图谱的具体构成，其中：攻击侧为 7 大类、17 个小类、108 项能力，防守侧为 5 大类、12 小类、52 项能力。总计 160 项具体能力。本文附录对每一项技能的含义与要求，进行了详细的说明。

一、 攻击侧能力图谱

在网络安全实战攻防演习中，攻击侧成员通常需要拥有深厚的技术背景及综合性的攻防能力，具体包括 7 大类、17 小类、108 项能力。下图给出了实战化白帽人才能力图谱攻击侧的完整图谱。在图中，我们用颜色深浅来区分各项能力的学习难度。颜色由浅到深分别表示基础能力、进阶能力和高阶能力。

下面，我们对攻击侧的 7 大类能力，即 Web 漏洞利用与挖掘、系统层漏洞利用与挖掘、安全工具使用、编程与开发、社工与渗透、攻击辅助和其他攻击能力进行简要说明。具体到每个能力项的含义说明，详见本白皮书“附录 2 实战化白帽人才能力图谱攻击侧能力详解”。

（一） Web 漏洞利用与挖掘

Web 漏洞利用与挖掘是指针对 Web 系统或应用中存在的安全漏洞进利用和挖掘的攻击手段。具体又包括 Web 漏洞利用和 Web 漏洞挖掘两个方面。前者是指利用已知的各类 Web 漏洞进行攻击的技术能力，后者是指发现系统中存在的新的 Web 漏洞的能力。

从技术原理来看，最常见的 Web 漏洞主要包括以下 12 种类型：命令执行、SQL 注入、代码执行、逻辑漏洞、解析漏洞、信息泄露、XSS、配置错误、弱口令、反序列化、文件上传、权限绕过。针对这 12 种不同技术原理的漏洞进行利用和挖掘，就分别对应了 Web 漏洞

利用与挖掘各自包含的 12 项不同能力。

（二） 系统层漏洞利用与挖掘

为应对各种各样的网络攻击，操作系统内部有很多底层的安全机制。系统层漏洞利用与挖掘指针对操作系统、服务器或网络设备等系统层面的安全漏洞进行攻防利用与漏洞挖掘的能力。其中，系统层漏洞挖掘，要求具备能够深入分析系统架构、配置及源代码，发现系统层面的潜在安全漏洞，为增强系统防御提供关键信息和修复建议的能力。

系统层漏洞利用能力，主要包括 7 种最为常用的、典型的系统层安全机制，即 SafeSEH、DEP、PIE、NX、ASLR、SEHOP、GS。

而最常用的系统层漏洞挖掘能力（方法）主要包括 6 种，即代码跟踪、动态调试、Fuzzing 技术、补丁对比、软件逆向静态分析、系统安全机制分析。

（三） 安全工具使用

在攻击侧，安全工具的使用是指在安全分析或攻防实战过程中，通过使用一系列成熟的、专用的安全工具，对网络系统进行监测、分析，乃至实现特定的攻击活动的攻击方法。

其中比较常见的基础安全工具包括：Burp Suite、Sqlmap、Nmap、Wireshark、AppScan、AWVS、MSF、Cobalt Strike 等。

经常被用到的高级工具包括：IDA、Ghidra、Binwalk、OllyDbg、Peach fuzzer 等。

（四） 编程与开发

编写和优化攻击代码与脚本，用于渗透测试、漏洞利用，甚至是设计并实现木马程序、黑客工具，以支持攻防需求，是白帽子在攻击侧需要具备的较高级能力。编程与开发能力主要包括 Web 开发与编程、编写 PoC 或 EXP 等利用两个方面。

在 Web 开发与编程方面，白帽子最为经常遇到和需要掌握的编程语言包括：Java、PHP、Python、C/C++、Golang 等。

而编写 PoC 或 EXP 等利用，又可以分为一般利用和高级利用。编写 PoC 或 EXP 等一般利用主要包括针对 Web 漏洞、智能硬件/IoT 漏洞、WAF 等防护设备绕过等利用。编写 PoC 或 EXP 高级利用，则主要包括编写针对 Windows、Android、iOS、Linux、macOS 等操作系统，以及针对网络安全设备等的漏洞利用。

（五） 社工与渗透

在对目标网络进行入侵活动时，社会工程学（也称为社工钓鱼）方法和网络渗透方法是最为主要、最为常用的攻击手段。在此将二者合并简称为社工与渗透能力。

社工钓鱼，是指利用社会工程学手法，利用伪装、欺诈、诱导等方式，利用人的安全意识不足或安全能力不足，对目标机构特定人群实施网络攻击的一种手段。社工钓鱼，既是实战攻防演习中经常使用的作战手法，也是黑产团伙或黑客组织最为经常使用的攻击方式。在很多情况下，“搞人”要比“搞系统”容易得多。

社工钓鱼的方法和手段多种多样。在实战攻防演习中，最为常用，也是最为实用的技能主要有三种：社工库收集、鱼叉邮件与社交钓鱼。

内网渗透，是指当攻击方已经完成边界突破，成功入侵到政企机构内部网络之后，在机

构内部网络中实施进一步渗透攻击，逐层突破内部安全防护机制，扩大战果或最终拿下目标系统的攻击过程。

在实战攻防环境下，白帽子比较实用的内网渗透能力包括：工作组或域环境渗透、内网权限维持/提权、数据窃取、常见隧道工具使用、横向移动、免杀、云安全防护绕过与终端安全防护绕过等。

（六） 攻击辅助

攻击辅助是指能够提升攻击活动成功率，或避免自身非发现的各类辅助性技术手段。这些技术手段通常都不是直接的攻击技术，但与各种攻击技术、社工手法配合使用，就能大大提升攻击活动的效率和成功率。目前，攻击辅助能力主要体现在身份隐藏、大模型辅助及情报收集与分析三方面。

为避免自己的真实 IP、物理位置、设备特征等信息在远程入侵的过程中被网络安全设备记录，甚至被溯源追踪，攻击者一般都会利用各种方式来进行身份隐藏。在实战攻防演习中，攻击方所采用的身份隐藏技术主要有以下几类：匿名网络、盗取他人 ID/账号、使用跳板机、他人身份冒用和利用代理服务器等。

大模型辅助是指在网络攻防实战过程中，通过使用各种大模型工具，实现加速攻击效率、智能分析预测目标系统潜在弱点，并自动优化攻击手段等目的的攻击辅助方法。目前在白帽子中比较流行的大模型辅助方法包括：大模型深度伪造、大模型辅助爆破、大模型漏洞挖掘、大模型辅助开发、及大模型辅助 EXP 开发。

情报收集与分析是网络安全实战攻防演习过程中，攻击队必不可少的前期准备工作。只有充分的掌握目标系统的精准情报，才能实现对目标系统的高效攻击。具体来说，主要包括公开情报收集、开源安全情报、黑灰产情报、目标系统信息及关键人锁定等几个方面。

（七） 其他攻击能力

除了前述各项安全能力外，实战化白帽攻击人才还需要具备以下一些通用或特殊能力，包括大模型安全、掌握 CPU 指令集与团队协作等。

大模型安全是指能够对针对应用系统所使用的 AI 大模型本身进行攻击的一种安全能力。具体来说，又可以分为大模型越狱和大模型组件安全两个方向。由于大模型技术已经在众多行业中得到了普及应用，因此，大模型本身的安全问题也倍受关注。在 2024 年的网络安全实战攻防演习中，已经有攻击队能够通过对应用系统大模型的攻击，实现既定的攻击目标任务。

CPU 指令集，即 CPU 中用来计算和控制计算机系统的一套指令的集合。每一种不同的 CPU 在设计时都会有一系列与其他硬件电路相配合的指令系统。指令系统包括指令格式、寻址方式和数据形式。一台计算机的指令系统反应了该计算机的全部功能。机器类型不同，其指令集也不同。而白帽子对 CPU 指令集的掌握程度，将直接决定白帽子进行系统层漏洞挖掘与利用的能力水平。本文指掌握不同架构下的底层程序分析。目前，最为常见的 CPU 指令集包括 x86、MIPS、ARM 和 PowerPC。

随着网络安全实战攻防演习实践的不断深入和防守方的整体能力持续提升，白帽子单凭强大的个人能力单打独斗取得胜利的希望越来越小。而由 3~5 人组成的攻击小队，通过分工协作的方式高效完成攻击行动的模式已经越来越成熟。而对于白帽子来说，是否拥有团队协作的作战经验，在团队中扮演什么样的角色，也是白帽子实战化能力的重要指标。

团队作战，成功的关键的是协作与配合。通常来说，每只攻击队的成员都会有非常明确的分工和角色。在实战攻防演习实践中，攻击队比较常见的角色分工主要有 7 种，分别是：行动总指挥、情报收集人员、武器装备制造人员、打点实施人员、社工钓鱼人员、内网渗透人员、攻击成果报告撰写人员。需要说明的是，在实际演习过程中，一人分饰多个角色也是非常普遍的。

二、 防守侧能力图谱

白帽人才，既要能攻，也要善守。在网络安全实战攻防演习中，越来越多的白帽子已经投入防守侧工作当中，利用自己对攻击队的了解，能够更好的在防守侧大展拳脚。面对日益智能化、隐蔽化和复杂化的网络威胁，面对层出不穷的 0day 漏洞、供应链攻击、新的高级攻击手法、甚至是高级持续性威胁（APT）等，想要构建坚固的安全防线，不仅需要先进的技术支撑，更离不开高效的管理机制、专业的团队素养以及快速的应急响应、甚至追踪反制能力。在本次研究中，实战化白帽人才能力图谱防守侧主要包括 5 大类、12 小类、52 项具体能力。

下图给出了实战化白帽人才能力图谱防守侧的完整图谱。在图中，我们用颜色深浅来区分各项能力的学习难度。颜色由浅到深分别表示基础能力、进阶能力和高阶能力 。

需要说明的是，与攻击侧能力分类有所区别，防守侧的 5 大类能力分类与网络安全实战攻防演习过程中关键环节的执行次序有关。一般来说，演习开始前，要对系统进行“检查与整改”；演习开始后要对系统进行“监测与分析”；一旦发生问题，需要进行“响应与处置”；对于攻击活动进行处置的同时，防守队还需要对攻击队（攻击者）进行“溯源与反制”；除此以外还有一些“其他能力”贯穿整个演习过程。

下面就对防守侧人员需要掌握的网络安全能力进行简要说明。具体到每个能力项的含

义说明，详见本白皮书“附录 3 实战化白帽人才能力图谱防守侧能力详解”。

（一） 检查与整改

检查与整改，主要是指在网络安全运营过程中，或在网络安全实战攻防演习之前，对机构网络安全建设与运营的摸底排查和整改加固工作，目的是通过事前有针对性的自查工作，提前发现问题、提前消除隐患。其中包括：安全检查、整改加固与规则优化三个小类。

安全检查，是指按照特定的流程、框架和规范，对机构的网络安全建设与运营状况进行逐一排查并确定问题的过程。安全检查一般需要检查人员具备资产梳理、基线检查、渗透测试/漏洞发现、安全有效性验证等技术能力。

整改加固，是指对已经发现的安全漏洞、敏感信息泄露、资产暴露、策略不足、弱口令等问题进行及时定位和修补，提前排除各类技术隐患的安全工作。整改加固过程一般需要具备漏洞修复与升级、防护措施补全、安全设备加固和安全策略初始化等技术能力。

规则优化，是指根据攻防态势的动态变化、根据事件分析及追踪溯源的结果，对各类网络安全设备、网络安全系统的识别与拦截规则进行动态优化配置。具体包括：规则优化、降噪及威胁建模三个环节。

（二） 监测与分析

监测与分析，是指通过各类网络安全设备或系统，对机构内部网络中发生的各类网络安全威胁事件进行实时监测和分析研判的安全工作。监测与分析，不仅是日常网络安全运营过程中最主要的工作，也是网络安全实战攻防演习过程中最为主要的基础性工作。监测与分析工作，具体来说有可以分为告警监测与事件分析两大类。

告警监测，一般是指通过各类网络安全软件、设备及监测平台，对监测范围内的所有系统中发生的各类网络安全告警信息进行实时监测、汇总的安全工作。告警监测能力，在网络安全实战攻防演习的实战阶段，防守方最为基础性的实战化技能，也是日常网络安全运营工作中最为重要的基础技能。告警监测的主要范围一般包括：终端告警监测、服务器告警监测、流量告警监测、业务系统告警监测、蜜罐/蜜点告警监测及其他安全设备告警监测。

事件分析，是指当疑似网络安全事件发生时，安全人员对于安全事件的性质、原因、攻击面、攻击手段、临时响应措施等进行基本的分析、识别和研判的过程。具体包括：安全事件识别、攻击手法识别与被攻击目标识别三项。

（三） 响应与处置

在完成安全事件的分析或通过追踪溯源完成对攻击者的研判之后，安全人员需要在第一时间对网络安全防护系统进行优化配置，阻断网络攻击活动，阻止事件影响扩散，这就是响应与处置工作。要做好响应与处置工作，不仅需要具备基本的应急响应能力，还需要具备常见应急场景处置的经验。

应急响应，是指当安全事件发生之后，对系统进行的紧急抢救和处置措施，目的是阻断攻击活动，阻止安全事件的影响扩散。在应急响应过程中，应急人员一般需要具备多种主要能力，具体包括：失陷设备隔离、无补丁漏洞修复、数据恢复与应急工具包使用四大类。

常见应急场景处置，主要包括：常见木马/病毒、网页篡改、DDoS 防御、流量劫持恢复、数据泄露及 APT 等场景的处置。每一类特定的应急响应场景，都对应一系列特定的处置流程和专用方法。熟练掌握常见应急响应场景的处置方法，可以大大提升网络安全事件的响应与

处置效率。

（四） 溯源与反制

溯源与反制，是网络攻防活动中，防守方抑制攻击活动的重要举措。在网络安全实战攻防演习活动中，如果能够对攻击队进行有效的溯源和反制，可以为防守队获得额外积分。

溯源，也称为追踪溯源，是指对网络攻击活动的源头进行追溯的一种安全方法，内容一般包括但不限于：失陷资产判定、入侵路径还原、攻击者网络资产分析、攻击者行为特征分析、攻击者在网络空间及物理空间中定位、攻击者身份识别等多个方面。

反制，也称为攻击反制，是指在溯源的基础上，通过各种技术及社工手段，对攻击者进行渗透、控制、数据获取等反向攻击活动，以实现压制攻击活动、抓捕攻击者等目的。反制能力包括但不限于反向 Web 漏洞利用、黑客工具漏洞利用、反向社工、蜜罐/密点部署以及常见黑客工具使用等。

（五） 其他能力

除了前述各种安全能力外，防守一侧的实战化白帽防守人才还需要具备以下一些通用或特殊技能。

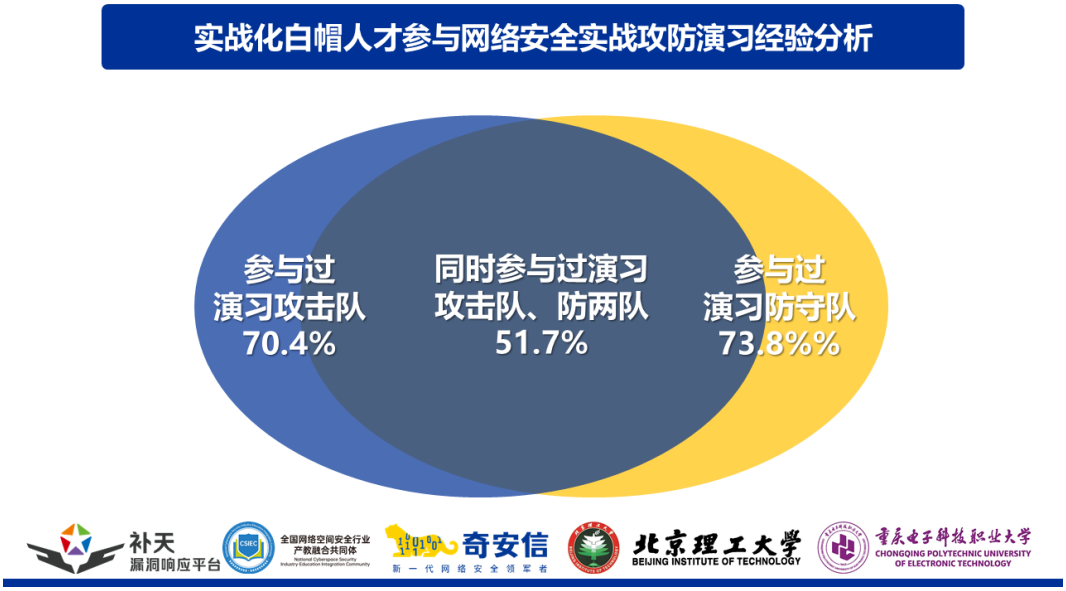
协同指挥与决策能力，是指在网络安全实战攻防演习过程中，对防守一方的整体指挥、组织和协调能力。这是一种比较高级的能力，不仅需要有扎实的技术基础，还需要有大量的防守实战经验和指挥作战经验。具体包括：安全规划、响应流程制定、防守角色分配及指挥与决策。

情报收集，是一项贯穿网络安全实战演习始终的重要工作。不论是在检查与整改阶段、监测与分析阶段、响应与处置阶段、还是溯源与反制阶段，都需要用到情报收集能力。因此，我们将情报收集能力单独提取出来，作为一项关键能力进行单独说明。特别的，这里所说的情报，并不一定都是“威胁情报”。企业日常建设、运营与宣传等工作的情报，也都有收集的意义和价值。具体包括：公开情报收集、威胁情报平台使用与自制情报收集工具三项。

报告撰写，是一项非常基础的文字能力，一般需要按照特定的规范进行书写。针对网络安全实战攻防演习防守一方的特定情况，撰写以下几类典型报告，是安全人员需要具备的基本能力，具体包括：应急处置报告、防守成果报告、总结整改报告三类。

第二章 实战化白帽人才能力现状

2024 年 8 月，根据“实战化白帽人才能力图谱”，补天漏洞响应平台针对平台上活跃的 495 名白帽子进行了实战化能力调研。其中，70.4%的白帽子参与过网络安全实战攻防演习攻击队，73.8%的白帽子参与过实战攻防演习防守队。同时，有 51.7%的白帽子表示自己攻防均可，攻击队防守队均参与过。



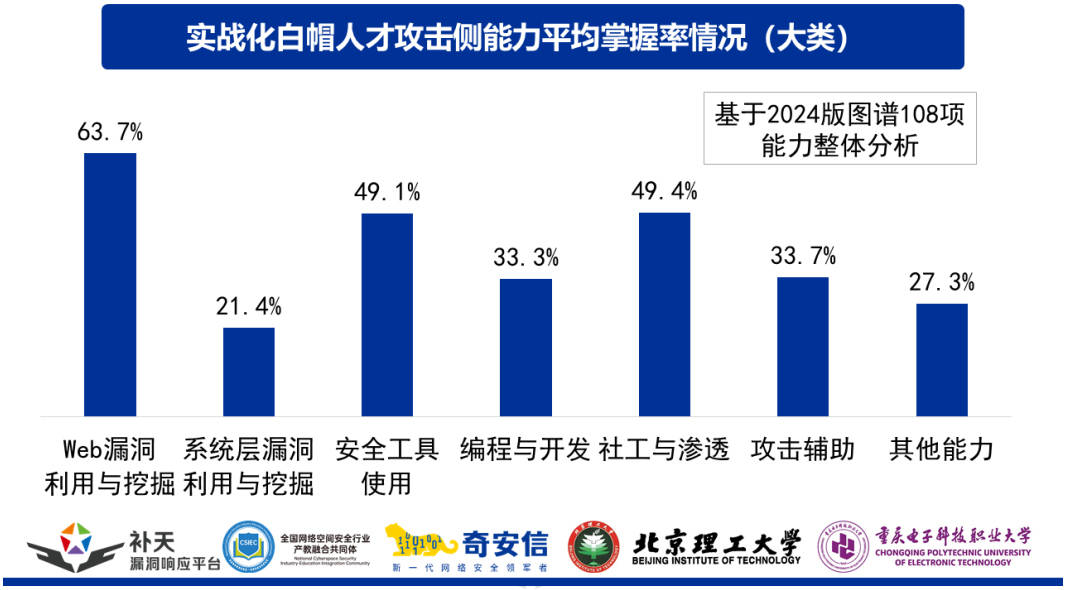
本章将对此次调研结果的整体情况进行介绍，包括大类分析和小类分析。具体到每一项能力的平均掌握率详情，请参见报告“附录 1 实战化白帽人才能力统计数据详情”。

一、 攻击侧现状分析

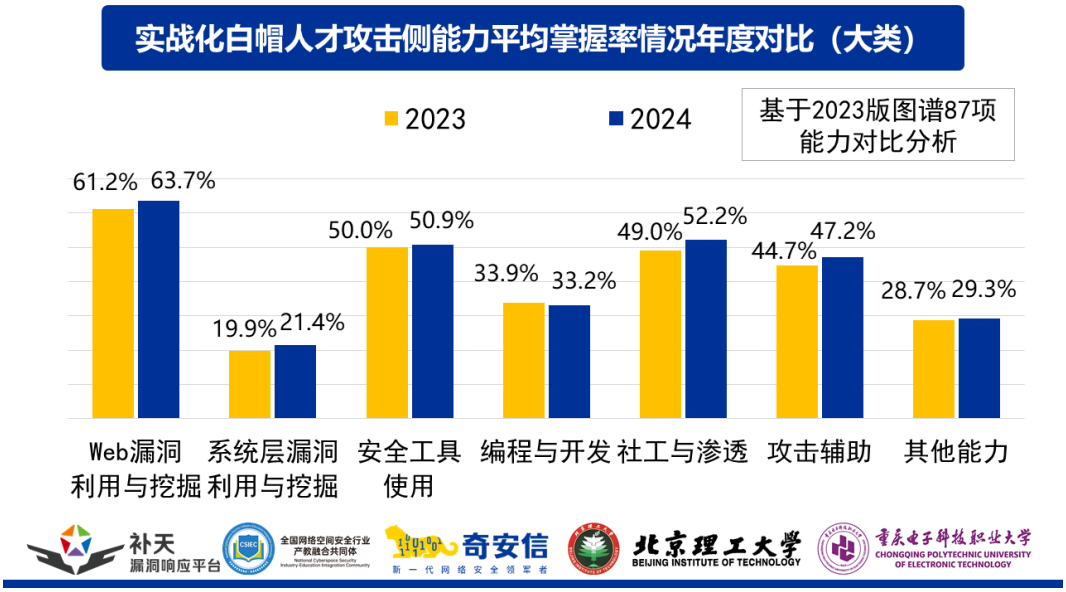
统计显示，国内白帽人才对于“实战化白帽人才能力图谱”给出的攻击侧 7 大类实战化能力的总体平均掌握率为 39.7%。其中，“Web 漏洞利用与挖掘”能力的平均掌握率最高，达到 63.7%是白帽人才中最普及、最主要的一种攻击能力。

其次是“社工与渗透” 和“安全工具使用”能力的平均掌握率分别是 49.4%和 49.1%，属于一半白帽子能够掌握或部分掌握的攻击能力。此外，各类“攻击辅助”能力的平均掌握率约为 33.7%，“编程与开发”能力的平均掌握率是 33.3%，也属于平均掌握率接近半数的安全能力，约 1/3 的白帽人才具备这两种能力。

各大类能力的平均掌握率情况详见下图。

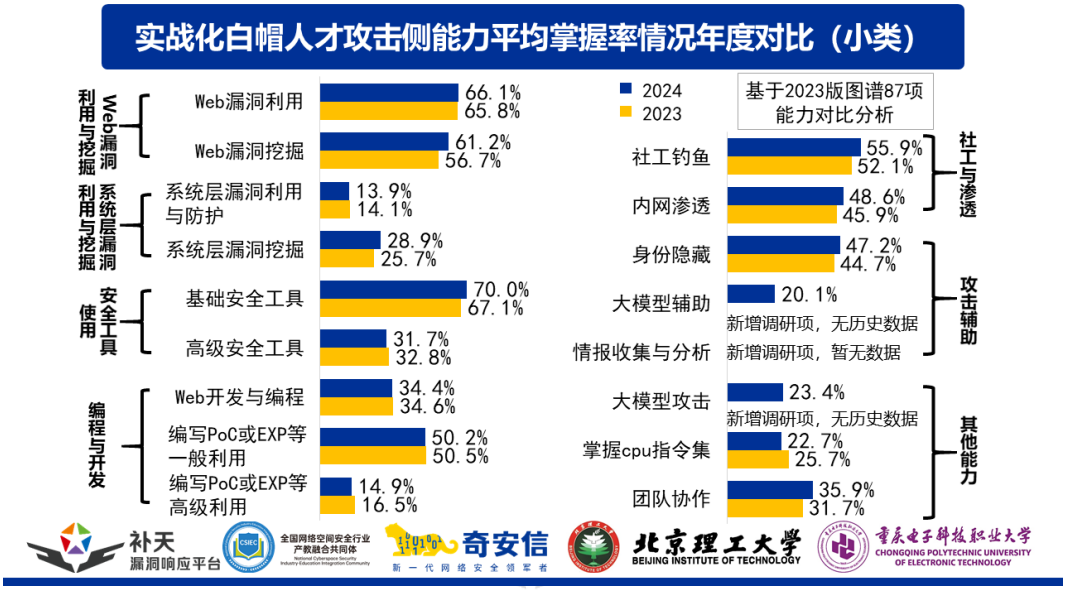


那么，与 2023 年相比，白帽人才对于实战化能力的掌握率情况有哪些变化呢？下图给出了 2023 年与 2024 年的情况对比。考虑到 2024 版图谱比 2023 版图谱增加了 21 项新的能力，为确保对比的一致性，下图给出的对比分析中，仅以 2023 版图谱中包含的 87 项能力为基础进行对比，暂不考虑新增能力项的影响。



从图中可见，基于 2023 版图谱 87 项能力的整体分析来看，2024 年白帽人才对于 7 大类实战化攻击能力整体掌握情况有普遍有所提升，总体平均掌握率从 2023 年的 41.0%，上涨到 2024 年的 42.6%，上涨了 1.6 个百分点。除了“编程与开发”能力的平均掌握率下降了 0.7 个百分点外，其他各大类能力的平均掌握率均有 0.5%~3.2%不等的小幅提升。

下图给出了以 2023 版图谱力为基础，分析的 17 个小类的实战化攻击能力的平均掌握率情况。如上，如果某一个小类下面的能力项为 2024 版图谱新增能力项，则该项能力的统计数据不计入对比分析。

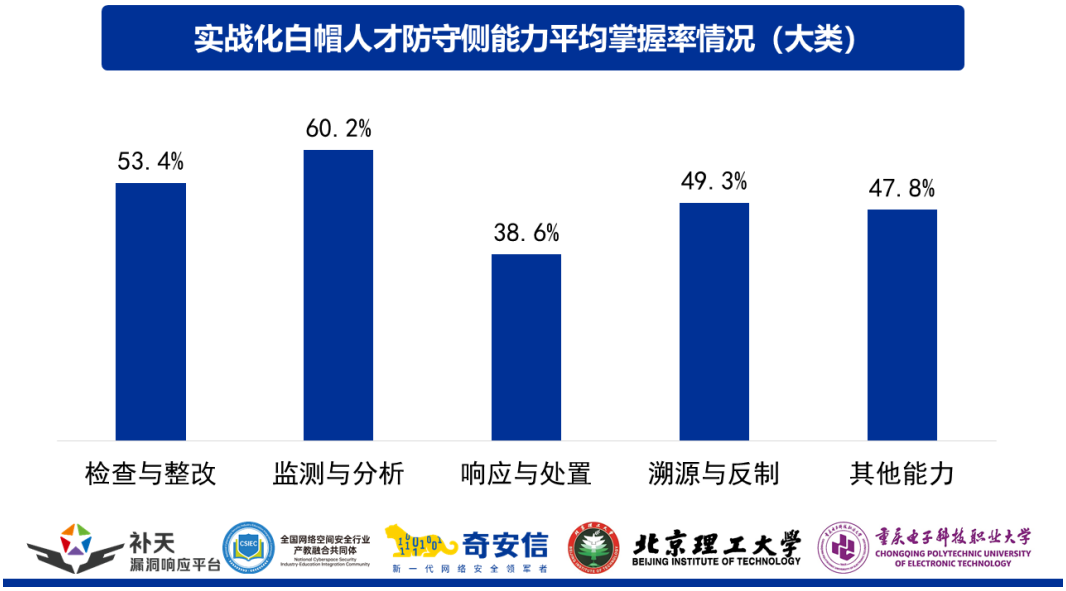


总体来看，2024 年和 2023 年相比，各小类能力的平均掌握率上下浮动相对稳定，均在 5 个百分点以内。但如果将 17 个小类能力的横向对比即可发现，实战化白帽人才攻击侧能力的掌握情况并没有很乐观。仅有 5 个小类的能力，白帽人才平均掌握率在 50%以上。其中，基础安全工具的掌握情况最好，2024 年“基础安全工具”的平均掌握率为 70.0%，排名第一；其次为“Web 漏洞利用”，平均掌握率为 66.1%；“Web 漏洞挖掘”的平均掌握率为 61.2%。

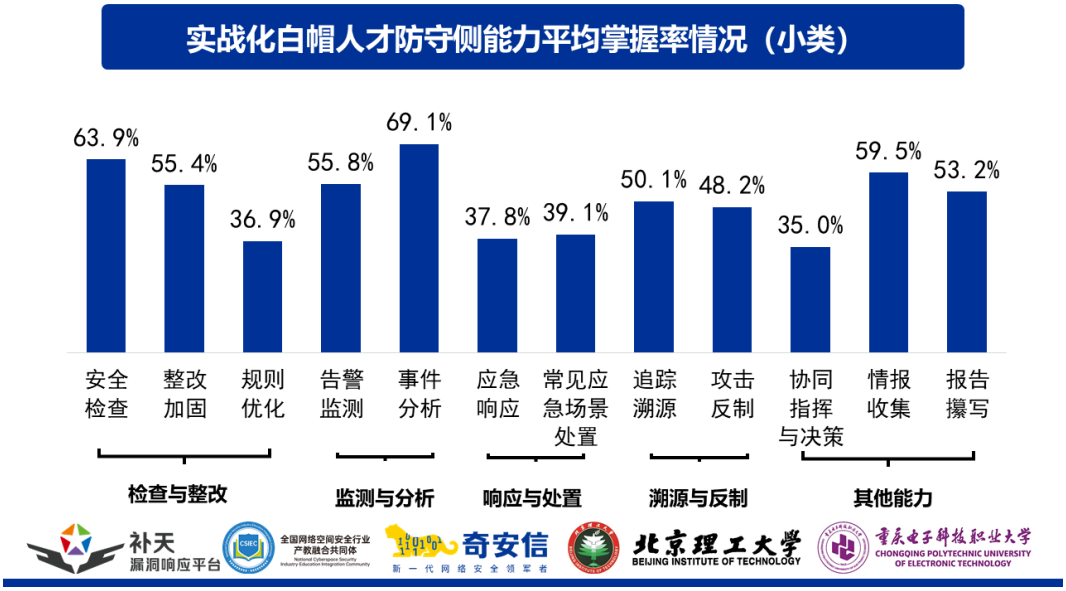
二、 防守侧现状分析

调研显示，在“实战化白帽人才能力图谱”所关注的防守侧 5 大类、12 小类、52 项能力中，各项能力的总体平均掌握率为 49.7%。与攻击侧的 42.6%相比略高一筹。

从能力大类来看，“监测与分析”能力的平均掌握率为 60.2%，掌握情况在 5 个大类中是最好水平。其次为“检查与整改”能力，平均掌握率为 53.4%、“溯源与反制”能力的平均掌握率 49.3%。“响应与处置”能力的平均掌握率最低，仅为 38.6%。具体分布如下图所示



具体到小类来看，防守侧白帽子的平均掌握率超过六成的能力为“事件分析”和“安全检查”，分别达到了 69.1%和 63.9%。此外，“情报收集”能力的平均掌握率也达到了 59.5%，接近六成。同时，“规则优化”、“应急响应”、“常见应急场景处置”、“协同指挥与决策”这几个小类的能力，白帽人才的平均掌握率不足 40%，是亟待加强人才培养的重要方向。



值得注意的是，在网络安全实战攻防演习中，“安全检查”作为防范与应对安全威胁的基石，其掌握情况的好坏直接关系到整个防御体系的稳固与响应效率。通过调研结果可见，大部分防守侧的白帽子能够熟练掌握安全检查工具与使用方法，具备了对系统、网络、应用等多层次多维度的安全检查能力，还具备基本的合规性与风险管理能力。但安全检查并非一次性任务，而是一个持续的过程，需要持续监控并维护完善的监控机制。

第三章　能力图谱与掌握情况总览

附录 1 实战化白帽人才能力调研统计数据详情

下表给出了实战化白帽人才能力图谱中，攻击侧白帽人才对于各项能力的平均掌握率情况，供各界研究者参考。在“学习难度”一栏中，1 表示基础能力、2 表示进阶能力、3 表示高阶能力。

大类	小类	能力项	平均掌握率（2023）	平均掌握率（2024）	学习难度
Web 漏洞利用与挖掘	Web 漏洞利用	命令执行	77.2%	75.3%	1
		SQL 注入	88.0%	87.5%	1
		代码执行	67.4%	65.4%	1
		逻辑漏洞	70.7%	72.1%	1
		解析漏洞	50.4%	50.4%	1
		信息泄露	69.1%	72.1%	1
		XSS	72.2%	70.2%	1
		配置错误	44.4%	45.6%	1
		弱口令	76.5%	79.0%	1
		反序列化	46.0%	44.8%	1
		文件上传	73.4%	74.4%	1
		权限绕过	54.3%	56.6%	1
	Web 漏洞挖掘	命令执行	66.2%	62.2%	2
		SQL 注入	79.5%	78.9%	2
		代码执行	55.6%	55.5%	2
		逻辑漏洞	62.7%	67.5%	2
		解析漏洞	39.8%	42.7%	2
		信息泄露	62.0%	70.0%	2
		XSS	62.6%	66.6%	2
		配置错误	41.5%	47.2%	2
		弱口令	68.0%	74.6%	2
		反序列化	34.4%	39.4%	2
		文件上传	62.6%	69.7%	2
		权限绕过	45.4%	60.0%	2
系统层漏洞利用与挖掘	系统层漏洞利用与防护	SafeSEH	19.5%	19.4%	3
		DEP	15.8%	11.1%	3
		PIE	17.0%	16.3%	3
		NX	15.3%	14.0%	3
		ASLR	12.7%	13.5%	3
		SEHOP	10.2%	10.6%	3
		GS	8.1%	12.7%	3
	系统层漏洞挖掘	代码跟踪	31.5%	35.0%	3
		动态调试	28.0%	32.4%	3

		Fuzzing 技术	33.8%	39.4%	3
		补丁对比	21.6%	19.7%	3
		软件逆向静态分析	24.5%	30.3%	3
		系统安全机制分析	14.5%	16.8%	3
安全工具使用	基础安全工具	Burp Suite	92.5%	91.2%	1
		Sqlmap	82.4%	83.7%	1
		AppScan	47.3%	48.5%	1
		AWVS	61.6%	61.7%	1
		Nmap	78.2%	80.3%	1
		Wireshark	65.4%	69.4%	1
		MSF	63.9%	66.8%	1
		Cobalt Strike	45.8%	58.6%	1
		DNSLog	-	60.6%	1
		HTTPLog	-	31.9%	1
		Goby	-	62.2%	1
		Behinder	-	70.7%	1
		AntSword	-	78.8%	1
	高级安全工具	IDA	52.1%	58.3%	3
		Ghidra	15.4%	17.4%	3
		Binwalk	31.1%	33.2%	3
		OllyDbg	27.4%	30.1%	3
		Peach fuzzer	38.0%	19.7%	3
编程与开发	Web 开发与编程	Java	32.8%	33.9%	2
		PHP	33.0%	35.2%	2
		Python	68.0%	64.3%	2
		C/C++	29.0%	24.1%	2
		Golang	10.4%	14.5%	2
	编写 PoC 或 EXP 等一般利用	Web 漏洞	87.1%	87.1%	2
		智能硬件/IOT 漏洞	13.9%	13.2%	2
		WAF 等防护设备绕过	-	29.5%	2
	编写 PoC 或 EXP 等高级利用	Windows 漏洞	27.4%	23.1%	3
		Android	17.4%	13.2%	3
		iOS	6.6%	7.5%	3
		Linux	25.1%	18.4%	3

		macOS	3.5%	5.2%	3
		网络安全设备	18.9%	22.0%	3
社工与渗透	社工钓鱼	社工库收集	62.6%	66.6%	2
		鱼叉邮件	34.8%	39.4%	2
		社交钓鱼	49.0%	54.2%	2
	内网渗透	工作组、域环境渗透	50.2%	52.6%	3
		横向移动	51.9%	54.2%	3
		内网权限维持/提权	55.6%	59.3%	3
		数据窃取	33.4%	31.9%	3
		免杀	38.4%	44.8%	3
		常见隧道工具	-	49.2%	3
		云安全防护绕过	-	24.6%	3
		终端安全防护绕过	-	25.7%	3
攻击辅助	身份隐藏	匿名链路（如 Tor）	45.6%	47.4%	3
		盗取他人 ID/账号	29.0%	27.2%	3
		使用跳板机	50.0%	58.0%	3
		冒用他人身份	31.1%	30.3%	3
		利用代理服务器	68.0%	73.1%	3
	大模型辅助	大模型深度伪造	-	19.7%	3
		利用大模型辅助爆破	-	33.4%	3
		大模型辅助漏洞挖掘	-	18.4%	3
		大模型辅助开发	-	13.7%	3
		大模型辅助 EXP 开发	-	15.5%	3

	情报收集与分析	公开情报收集	-	-	1
		开源安全情报	-	63.5%	2
		黑灰产情报	-	-	3
		目标系统信息	-	-	3
		关键人锁定	-	-	3
其他能力	大模型攻击	大模型越狱	-	25.7%	3
		大模型组建安全	-	21.0%	3
	掌握 cpu 指令集	x86	47.3%	44.3%	3
		MIPS	17.4%	11.4%	3
		ARM	24.5%	24.1%	3
		PowerPC	13.5%	11.1%	3
	团队协作	行动总指挥（策略制定、任务分发、进度把控等）	22.8%	20.0%	3
		情报收集人员	45.2%	46.4%	3
		武器装备制造（漏洞挖掘、工具编写）	21.0%	27.2%	3
		打点实施（获取接入点、Web 渗透等）	52.3%	65.8%	3
		社工钓鱼人员	23.2%	25.4%	3
		内网渗透	25.5%	30.3%	3
		攻击成果报告	-	-	2

下表给出了实战化白帽人才能力图谱中，防守侧白帽人才对于各项能力的平均掌握率情况，供各界研究者参考。在“学习难度”一栏中，1 表示基础能力、2 表示进阶能力、3 表示高阶能力。

大类	小类	能力项	平均掌握率（2024）	学习难度
检查与整改	安全检查	资产梳理	74.1%	1
		基线检查	48.3%	1
		渗透测试/漏洞发现	76.1%	3
		有效性验证	57.0%	3
	整改加固	应用漏洞修复与升级	61.7%	1
		安全设备加固	53.5%	1
		安全策略优化	50.0%	2
		防护措施补全	56.2%	2
	规则优化	规则优化	49.5%	3
		降噪	30.1%	3
		威胁建模	31.1%	3
监测与分析	告警监测	终端告警	61.7%	1
		服务器告警	63.4%	1
		流量告警	70.9%	1
		业务系统告警	50.5%	1
		蜜罐/密点告警	56.0%	1
		其他安全设备告警	32.1%	1
	事件分析	安全事件识别	75.1%	2
		攻击手法识别	72.4%	2
		被攻击目标识别	59.7%	2
响应与处置	应急响应	失陷设备隔离	63.7%	1
		无补丁漏洞修复	31.3%	2
		数据恢复	27.4%	3
		应急工具包	28.6%	3
	常见应急场景	常见木马/病毒处置	67.7%	2
		网页篡改	51.7%	2
		DDOS 防御	33.3%	2
		流量劫持恢复	25.6%	2
		数据泄露	38.6%	2
		APT	17.9%	3
溯源与反制	追踪溯源	日志分析	78.4%	2
		操作系统排查	61.2%	2
		流量数据分析	61.0%	2

		内存与进程分析	37.3%	2
		威胁情报检索	48.8%	2
		社交网络溯源	42.3%	2
		代码同源性分析	21.9%	3
	攻击反制	反向 web 漏洞利用	51.5%	3
		黑客工具漏洞利用	48.8%	3
		反向社工	46.8%	3
		蜜罐/密点部署	49.3%	3
		常见黑客工具使用	44.5%	3
其他能力	协同指挥与决策	安全规划	39.8%	3
		响应流程制定	33.3%	2
		防守角色分配	42.8%	2
		指挥与决策	24.1%	3
	情报收集	公开信息情报收集	78.1%	1
		威胁情报平台使用	73.9%	2
		自制情报收集工具	26.6%	3
	报告攥写	应急处置报告	55.2%	2
		防守成果报告	56.0%	2
		总结整改报告	48.5%	3

附录 2 实战化白帽人才能力图谱攻击侧能力详解

一、 Web 漏洞利用与挖掘

Web 漏洞利用与挖掘是指针对 Web 系统或应用中存在的安全漏洞进利用和挖掘的攻击手段。具体又包括 Web 漏洞利用和 Web 漏洞挖掘两个方面。前者是指利用已知的各类 Web 漏洞进行攻击的技术能力，后者是指发现系统中存在的新的 Web 漏洞的能力。

从技术原理来看，最常见的 Web 漏洞主要包括以下 12 种类型：命令执行、SQL 注入、代码执行、逻辑漏洞、解析漏洞、信息泄露、XSS、配置错误、弱口令、反序列化、文件上传、权限绕过。针对这 12 种不同技术原理的漏洞进行利用和挖掘，就分别对应了 Web 漏洞利用与挖掘各自包含的 12 项不同能力。

（一） Web 漏洞利用

Web 漏洞利用能力是指利用 Web 系统或应用的安全漏洞实施网络攻击的能力。

由于 Web 系统是绝大多数机构业务系统或对外服务系统的构建形式，所以 Web 漏洞利用也是最常见，最基础的网络攻击形式之一。在实战攻防演习中，白帽子最为经常利用的 Web 漏洞形式包括：命令执行、SQL 注入、代码执行、逻辑漏洞、解析漏洞、信息泄露、XSS、配置错误、弱口令、反序列化、文件上传、权限绕过等。

1） 命令执行

命令执行漏洞，是指黑客可以直接在 Web 应用中执行系统命令，从而获取敏感信息或者拿下 Shell 权限的安全漏洞。造成命令执行漏洞最常见的原因是 Web 服务器对用户输入命令的安全检测不足，导致恶意代码被执行。命令执行漏洞常常发生在各种 Web 组件上，包括 Web 容器、Web 框架、CMS 软件、安全组件等。

2） SQL 注入

SQL，是 Structured Query Language 的缩写，意为结构化查询语言。SQL 注入漏洞，是最常见的安全漏洞形式之一，是指通过构造特定的 SQL 语句，可以实现对数据库服务器的非授权查询，进而造成数据库数据泄露的安全漏洞。SQL 注入漏洞产生的主要原因是软件系统对输入数据的合法性缺少校验或过滤不严。

3） 代码执行

代码执行漏洞，是指通过构造特殊的语句或数据，使软件可以在设计流程之外，执行特定函数或命令的安全漏洞。造成代码执行漏洞的主要原因是，开发人员在编写代码时，没有充分校验输入数据的合法性。

4） 逻辑漏洞

逻辑漏洞，是指由于程序设计逻辑不够严谨，导致一些逻辑分支处理错误，或部分流程被绕过，进而引发安全风险的安全漏洞。

5） 解析漏洞

解析漏洞，是指服务器应用程序在解析某些精心构造的后缀文件时，会将其解析成网页脚本，从而导致网站沦陷的漏洞。大部分解析漏洞的产生都是由应用程序本身的漏洞导致的。此类漏洞中具有代表性的便是 IIS6.0 解析漏洞，此漏洞又有目录解析和文件解析两种利用方式，但也有少部分是由于配置的疏忽所产生的。

6） 信息泄露

信息泄露漏洞，是指造成系统或服务器中，本应被保护或不可见的敏感信息被意外泄露的安全漏洞。这些信息包括账号密码、系统配置、运行状态、关键参数、敏感文件内容等。造成信息泄露漏洞的主要原因包括运维操作不当、系统代码不严谨等。

7） XSS

XSS，全称为 Cross Site Scripting，意为跨站脚本攻击，为了和更加常用的 CSS（Cascading Style Sheets，层叠样式表）有所区分，特别简写为 XSS。

XSS 攻击，通常是指通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是 JavaScript，但实际上也可以包括 Java、VBScript、ActiveX、Flash 或某些普通的 HTML 等。攻击成功后，攻击者可能得到更高的权限（如执行一些操作）、私密的网页内容、会话信息和 Cookie 等各种用户敏感信息。

最早期的 XSS 攻击示例大多使用了跨站方法，即：用户在浏览 A 网站时，攻击者却可以通过页面上的恶意代码，访问用户浏览器中的 B 网站资源（如 Cookie 等），从而达到攻击目的。但随着浏览器安全技术的进步，早期的跨站方法已经很难奏效，XSS 攻击也逐渐和“跨站”的概念没有了必然的联系。只不过由于历史习惯，XSS 这个名字一直被延用了下来，现如今用来泛指通过篡改页面，使浏览器加载恶意代码的一种攻击方法。

在本文中，白帽子的 XSS 能力，是指白帽子能够发现软件或系统的设计缺陷或安全漏洞，构造 XSS 攻击代码，实现网络攻击的技术能力。

8） 配置错误

配置错误，是指由软件或系统的配置不当导致安全风险的安全漏洞。例如，文件的或服务的访问权限、可见范围配置不当，网络安全规则的设置错误等，都有可能使系统处于暴露或风险之中。配置错误的本质是系统的使用或运维不当，而不是系统的设计或开发问题。造成配置错误的主要原因是运维人员的疏忽或专业技能不足。

9） 弱口令

弱口令也是安全漏洞的一种，是指系统登录口令的设置强度不高，容易被攻击者猜到或破解。造成弱口令的主要原因是系统的运维人员、管理人员安全意识不足。常见的弱口令形式包括：系统出厂默认口令没有修改；密码设置过于简单，如口令长度不足，单一使用字母或数字；使用了生日、姓名、电话号码、身份证号码等比较容易被攻击者猜到的信息设置口令；设置的口令属于流行口令库中的流行口令。

10） 反序列化

反序列化漏洞，是指反序列化过程可以被操控或篡改，进而引发恶意代码执行风险的安全漏洞。

序列化和反序列化都是基础的计算机技术。序列化就是把计算机中的“对象”转换成字节流，以便于存储的一种方法。反序列化是序列化的逆过程，即将字节流还原成“对象”。

在反序列化过程中，如果输入的字节流可以被控制或篡改，就有可能产生非预期的“对象”。这就是反序列化漏洞。此时，攻击者通过构造恶意字节流输入，就可以在反序列化过程中，在对象被还原的过程中，使系统执行恶意代码。

11） 文件上传

文件上传漏洞，是指可以越权或非法上传文件的安全漏洞。攻击者可以利用文件上传漏洞将恶意代码秘密植入到服务器中，之后再通过远程访问去执行恶意代码，达到攻击的目的。

12） 权限绕过

权限绕过漏洞，是指可以绕过系统的权限设置或权限管理规则执行非法操作的安全漏洞。造成权限绕过漏洞的主要原因是，软件或系统的开发人员对数据处理权限的设计或判定不严谨、不全面。

（二） Web 漏洞挖掘

Web 漏洞挖掘能力是指在 Web 系统或应用中，发现新的安全漏洞的能力。

在白帽子挖掘的 Web 应用漏洞中，比较常见的漏洞形式包括：命令执行、SQL 注入、代码执行、逻辑漏洞、解析漏洞、信息泄露、XSS、配置错误、弱口令、反序列化、文件上传、权限绕过等。关于这些漏洞类型的具体含义，参见上述 “（一）Web 漏洞利用”，这里不再累述。

二、 系统层漏洞利用与挖掘

为应对各种各样的网络攻击，操作系统内部有很多底层的安全机制。系统层漏洞利用与挖掘指针对操作系统、服务器或网络设备等系统层面的安全漏洞进行攻防利用与漏洞挖掘的能力。其中，系统层漏洞挖掘，要求具备能够深入分析系统架构、配置及源代码，发现系统层面的潜在安全漏洞，为增强系统防御提供关键信息和修复建议的能力。

系统层漏洞利用与防护能力，主要包括 7 种最为常用的、典型的系统层安全机制，即 SafeSEH、DEP、PIE、NX、ASLR、SEHOP、GS。

而最常用的系统层漏洞挖掘能力（方法）主要包括 6 种，即代码跟踪、动态调试、Fuzzing 技术、补丁对比、软件逆向静态分析、系统安全机制分析。

（一） 系统层漏洞利用与防护

为应对各种各样的网络攻击，操作系统内部有很多底层的安全机制。而每一种安全机制，都对应了一定形式的网络攻击方法。对于白帽子来说，学习和掌握底层的系统安全机制，发现程序或系统中安全机制设计的缺陷或漏洞，是实现高水平网络攻击的重要基础技能。在实战攻防演习中，最为实用、也是最为常用的 7 种典型的系统层安全机制包括：SafeSEH、DEP、PIE、NX、ASLR、SEHOP、GS。

1） SafeSEH

当系统遭到攻击时，程序运行就会出现异常，并触发异常处理函数。而要使攻击能够继续进行，攻击者就常常需要伪造或篡改系统异常处理函数，使系统无法感知到异常的发生。

SafeSEH，（Safe Structured exception handling）是 Windows 操作系统的一种安全机制，专门用于防止异常处理函数被篡改，即在程序调用异常处理函数之前，对要调用的异常处理函数进行一系列的有效性校验，如果发现异常处理函数不可靠或存在安全风险，则应立即终止异常处理函数的调用。反之，如果 SafeSEH 机制设计不完善或存在缺欠，就有可能被攻击者利用，欺骗或绕过。

在本文中，白帽子的 SafeSEH 能力，是指白帽子掌握 SafeSEH 的技术原理，并能够发现程序或系统中 SafeSEH 机制的设计缺陷，并加以利用实施攻击的能力。

2） DEP

DEP，是 Data Execution Protection 的缩写，意为数据执行保护，作用是防止数据页内的数据被当作执行代码来执行，从而引发安全风险。

从计算机内存的角度看，数据和代码的处理并没有特别明确区分，只不过是在系统的调度下，CPU 会对于不同内存区域中的不同数据，进行不一样的计算而已。这就使得系统在处理某些经过攻击者精心构造的数据时，会误将其中的一部分“特殊数据”当作可执行代码来执行，从而触发恶意命令的执行。而 DEP 机制设计的重要目的就是仿制这种问题的发生；反之，如果 DEP 机制设计不完善或存在缺欠，就有可能被攻击者所利用，欺骗或绕过。

在本文中，白帽子的 DEP 能力，是指白帽子掌握 DEP 的技术原理，并能够发现程序或系统中 DEP 机制的设计缺陷，并加以利用实施攻击的能力。

3） PIE

PIE 是 Position-Independent Executable 的缩写，意为地址无关可执行文件，与 PIC（Position-Independent Code，地址无关代码）含义基本相同，是 Linux 或 Android 系统中动态链接库的一种实现技术。

在本文中，白帽子的 PIE 能力，是指白帽子掌握 PIE 的技术原理，并能够发现程序或系统中 PIE 机制的设计缺陷，并加以利用实施攻击的能力。

4） NX

NX，是 No-eXecute 的缩写，意为不可执行，是 DEP（数据执行保护）技术中的一种，作用是防止溢出攻击中，溢出的数据被当作可执行代码来执行。NX 的基本原理是将数据所在内存页标识为不可执行，当操作系统读到这段溢出数据时，就会抛出异常，而非执行恶意指令。反之，如果 NX 机制设计不完善或存在缺欠，就可以被攻击者利用并发动溢出攻击。

在本文中，白帽子的 NX 能力，是指白帽子掌握 NX 的技术原理，并能够发现程序或系统中 NX 机制的设计缺陷，并加以利用实施攻击的能力。

5） ASLR

ASLR，Address Space Layout Randomization 的缩写，意为地址空间随机化，是一种操作系统用来抵御缓冲区溢出攻击的内存保护机制。这种技术使得系统上运行的进程的内存地址无法被预测，使得与这些进程有关的漏洞变得更加难以利用。

在本文中，白帽子的 ASLR 能力，是指白帽子掌握 ASLR 的技术原理，并能够发现程序或系统中 ASLR 机制的设计缺陷，并加以利用实施攻击的能力。

6） SEHOP

SEHOP，是 Structured Exception Handler Overwrite Protection 的缩写，意为结构化异常处理覆盖保护。其中，结构化异常处理是指按照一定的控制结构或逻辑结构对程序进行异常处理的一种方法。如果结构化异常处理链表上面的某个节点或者多个节点，被攻击者精心构造的数据所覆盖，就可能导致程序的执行流程被控制，这就是 SEH 攻击。而 SEHOP 就是 Windows 操作系统中，针对这种攻击给出的一种安全防护方案。

在本文中，白帽子的 SEHOP 能力，是指白帽子掌握 SEHOP 的技术原理，并能够发现程序或系统中 SEHOP 机制的设计缺陷，并加以利用实施攻击的能力。

7） GS

GS，意为缓冲区安全性检查，是 Windows 缓冲区的安全监测机制，用于防止缓冲区溢出攻击。

缓冲区溢出是指当计算机向缓冲区内填充数据位数时，填充的数据超过了缓冲区本身的容量，于是溢出的数据就会覆盖在合法数据上。理想的情况是：程序会检查数据长度，而且并不允许输入超过缓冲区长度的字符。但是很多程序都会假设数据长度总是与所分配的储存空间相匹配，这就为缓冲区溢出埋下隐患，即缓冲区溢出漏洞。GS 就是通过对缓冲区数据的各种校验机制，防止缓冲区溢出攻击的发生。

在本文中，白帽子的 GS 能力，是指白帽子掌握 GS 的技术原理，并能够发现程序或系统中 GS 机制的设计缺陷，并加以利用实施攻击的能力。

（二） 系统层漏洞挖掘

系统层漏洞的挖掘需要很多相对高级的漏洞挖掘技术与方法。从实战角度看，以下 6 种挖掘方法最为实用：代码跟踪、动态调试、Fuzzing 技术、补丁对比、软件逆向静态分析、系统安全机制分析。

1） 代码跟踪

代码跟踪，是指通过自动化分析工具和人工审查的组合方式，对程序源代码逐条进行检查分析，发现其中的错误信息、安全隐患和规范性缺陷问题，以及由这些问题引发的安全漏洞，提供代码修订措施和建议。

2） 动态调试

动态调试，原指软件作者利用集成环境自带的调试器跟踪自己软件的运行，来协助解决自己软件的错误。

不过，对于白帽子来说，动态调试通常是指使用动态调试器（如 OllyDbg x64Dbg 等），为可执行程序设置断点，通过监测目标程序在断点处的输入输出及运行状态等信息，来反向推测程序的代码结构、运行机制及处理流程等，进而发现目标程序中的设计缺陷或安全漏洞的一种分析方法。

3） Fuzzing 技术

Fuzzing 技术，是一种基于黑盒（或灰盒）的测试技术，通过自动化生成并执行大量的随机测试用例来触发软件或系统异常，进而发现产品或协议的未知缺陷或漏洞。

4） 补丁对比

每一个安全补丁，都会对应一个或多个安全漏洞。通过对补丁文件的分析，往往可以还原出相应漏洞的原理或机制。而利用还原出来的漏洞，就可以对尚未打上相关补丁的软件或系统实施有效攻击。而补丁对比，是实战环境下，补丁分析的一种常用的、有效的方式。

补丁对比，是指对原始文件和补丁文件分别进行反汇编，然后对反汇编后的文件做比较找出其中的差异，从而发现潜在的漏洞的一种安全分析方法。

5） 软件逆向静态分析

在本文中，软件逆向静态分析，是指将对软件程序实施逆向工程，之后对反编译的源码或二进制代码文件进行分析，进而发现设计缺陷或安全漏洞的一种安全分析方法。

对开放源代码的程序，通过检测程序中不符合安全规则的文件结构、命名规则、函数、堆栈指针等，就可以发现程序中存在的安全缺陷。被分析目标没有附带源程序时，就需要对程序进行逆向工程，获取类似于源代码的逆向工程代码，然后再进行检索和分析，也可以发现程序中的安全漏洞。这就是软件逆向静态分析。

软件逆向静态分析，也叫反汇编扫描，由于采用了底层的汇编语言进行漏洞分析，在理论上可以发现所有计算机可运行的漏洞。对于不公开源代码的程序来说，这种方法往往是最有效的发现安全漏洞的办法。

6） 系统安全机制分析

操作系统的安全机制，就是指在操作系统中，利用某种技术、某些软件来实施一个或多个安全服务的过程。主要包括标识与鉴别机制，访问控制机制，最小特权管理机制，可信通路机制、安全审计机制，以及存储保护、运行保护机制等。

在本文中，系统安全机制分析能力，是指对操作系统的各种安全机制的进行分析，进而发现系统设计缺陷或安全漏洞的方法。

三、 安全工具使用

在攻击侧，安全工具的使用是指在安全分析或攻防实战过程中，通过使用一系列成熟的、专用的安全工具，对网络系统进行监测、分析，乃至实现特定的攻击活动的攻击方法。

其中比较常见的基础安全工具包括：Burp Suite、Sqlmap、Nmap、Wireshark、AppScan、AWVS、MSF、Cobalt Strike 等。

经常被用到的高级工具包括：IDA、Ghidra、Binwalk、OllyDbg、Peach fuzzer 等。

（一） 基础安全工具

基础安全工具是指安全分析或攻防实战过程中，经常使用到的一些初级的、基础的软件工具。比较常见的基础安全工具包括：Burp Suite、Sqlmap、AppScan、AWVS、Nmap、Wireshark、MSF、Cobalt Strike 等。

1） Burp Suite

Burp Suite 是一个常用的 Web 攻击工具的集合平台，经常被安全工作者用来测试 Web 系统安全性，也是实战攻防演习中攻击队的常用平台。

使用者通过平台集成的工具，既可以对目标发起手动攻击，也可以自定义规则发起自动攻击；既可以探测和分析目标漏洞，也可以使用爬虫抓取和搜索页面内容。

2） Sqlmap

Sqlmap 是一个开源的渗透测试工具，可以用来进行自动化检测。Sqlmap 可以利用常见的 SQL 注入漏洞，获取数据库服务器的权限。Sqlmap 还具有功能比较强大的检测引擎,可提供针对各种不同类型数据库的渗透测试的功能选项，包括获取数据库中存储的数据，访问操作系统文件，甚至可以通过外带数据连接的方式执行操作系统命令。

3） AppScan

AppScan 是 IBM 公司推出的一款 Web 应用安全测试工具，采用黑盒测试的方式，可以扫描常见的 Web 用安全漏洞。AppScan 功能比较齐全，支持登录、报表等功能。在扫描结果中，不仅能够看到 Web 应用被扫出的安全漏洞，还提供了详尽的漏洞原理、修改建议、手动验证等功能。

在实战攻防演习中，AppScan 是一个很方便的漏洞扫描器。

4） AWVS

AWVS 是 Acunetix Web Vulnerability Scanner 的缩写。它是一个自动化的 Web 应用程序安全测试工具，可以审计和检查 Web 漏洞。AWVS 可以扫描任何可通过 Web 浏览器访问的和遵循 HTTP/HTTPS 规则的 Web 站点和 Web 应用程序。可以通过检查 SQL 注入攻击漏洞、XSS 漏洞等来审核 Web 应用程序的安全性。

5） Nmap

Nmap 是 Network Mapper 的缩写，意为网络映射器，是一款开放源代码的网络探测和安全审核的工具。它的设计目标是快速地扫描大型网络，但也可以用于扫描单个主机。

Nmap 使用原始 IP 报文来发现网络上有哪些主机，每台主机提供什么样的服务，哪些服务运行在什么操作系统上，这些主机使用了什么类型的报文过滤器或防火墙等。虽然 Nmap 通常用于安全审核，但许多系统管理员和网络管理员也用它来做一些日常的工作，比如查看整个网络的信息，管理服务升级计划，以及监视主机和服务的运行。

在实战攻防演习中，Nmap 常用来对目标系统进行资产分析。

6） Wireshark

Wireshark 是一个免费开源的网络数据包分析软件，它可以帮助网络管理员检测网络问题，帮助网络安全工程师检查信息安全相关问题。
在实战攻防演习中，数据包分析也是非常重要的基础工作。

7） MSF

MSF 是 Metasploit Framework 的缩写，这不仅仅是一个工具软件，它是为自动化地实

施经典的、常规的、复杂新颖的攻击，提供基础设施支持的一个完整框架平台。它可以使使用人员将精力集中在渗透测试过程中那些独特的方面上，以及如何识别信息安全计划的弱点上。

MSF 的能够让用户通过选择它的渗透攻击模块、攻击载荷和编码器来实施一次渗透攻击，也可以更进一步编写并执行更为复杂的攻击技术。

8） Cobalt Strike

Cobalt Strike 是一款 C/S 架构的商业渗透软件，适合多人团队协作。可模拟 APT 对抗，进行内网渗透。Cobalt Strike 集成了端口转发、端口扫描、Socks 代理、提权、凭据导出、钓鱼、远控木马等功能。该工具几乎覆盖了 APT 攻击链中所需要用到的各个技术环节

9） DNSLog

DNSLog 利用 DNS 协议的特性，将需要收集的信息编码成 DNS 查询请求，然后将请求发送到 DNS 服务器。通过 DNS 服务器的响应来获取信息，这些信息被记录在 DNS 日志中，类似于传统的日志文件。DNSLog 的实现方式多种多样，其中最常见的是使用第三方 DNS 服务。

10） HTTPLog

HTTPLog 是一个功能强大的日志库，专为 HTTP 请求设计，能够记录并展示 HTTP 请求和响应的详细信息，助力开发者在开发和调试过程中快速定位问题。通过 HTTPLog，开发者可以实时查看 HTTP 请求的发送和接收过程，包括请求头、请求体、响应状态码、响应体等内容，极大地提高了开发效率和调试便利性。同时，它还支持多种日志格式和灵活的配置选项，满足不同场景下的日志记录需求。

11） Goby

Goby 是一个功能强大的网络安全工具，它基于网络空间测绘技术，通过为目标网络建立完整的资产知识库，实现快速的安全应急。同时，Goby 也是一款深受 Ruby 启发的面向对象解释器语言，其核心实现完全采用纯 Go 语言编写，结合了 Ruby 的优雅语法和 Go 的高性能与并发处理能力，为后端开发提供了全新的选择。

12） Behinder

Behinder 是一款功能强大的开源后渗透测试工具，它提供了直观易用的界面来管理和操作被渗透的系统，支持文件上传下载、命令执行、进程管理等多种后渗透操作。此外，Behinder 还以其动态加密通信流量的特性而闻名，使得传统的安全设备难以检测其通信流量，增加了渗透测试的隐蔽性和安全性。

13） AntSword

AntSword（蚁剑）是一款功能强大的开源 Web 管理工具，专为网站渗透测试和安全研究设计。AntSword 提供远程文件操作、数据库管理、命令执行等丰富功能，通过图形化界面简化 Web 站点管理，支持跨平台使用，满足渗透测试和安全研究需求。

（二） 高级安全工具

高级安全工具同样是白帽子的必修课，只不过这些工具对于使用者有更高的基础技能要求，初学者不易掌握。在实战化环境中，最为经常被用到的工具包括：IDA、Ghidra、Binwalk、

OllyDbg、Peach fuzzer 等。

1） IDA

IDA，是一个专业的反汇编工具，是安全渗透人员进行逆向安全测试的必备工具，具有静态反汇编和逆向调试等功能，能够帮助安全测试人员发现代码级别的高危安全漏洞。

2） Ghidra

Ghidra,是一款开源的跨平台软件逆向工具,目前支持的平台有 Windows、macOS 及 Linux，并提供了反汇编、汇编、反编译等多种功能。Ghidra P-Code 是专为逆向工程设计的寄存器传输语言，能够对许多不同的处理器进行建模。

3） Binwalk

Binwalk，是一个文件扫描提取分析工具，可以用来识别文件内包含的内容和代码。Binwalk 不仅可以在标准格式本件中进行分析和提取，还能对非标准格式文件进行分析和提取，包括压缩文件、二进制文件、经过删节的文件、经过变形处理的文件、多种格式相融合的文件等。

4） OllyDbg

OllyDbg，是一款强大的反汇编工具。它结合了动态调试与静态分析等功能。是一个用户模式调试器，可识别系统重复使用的函数，并能将其参数注释。OllyDbg 还可以调试多线程应用程序，从一个线程切换到另一个线程、挂起、恢复和终止，或改变它们的优先级。

5） Peach fuzzer

Peach Fuzzer 是一款智能模糊测试工具，广泛用于发现软件中的缺陷和漏洞。Peach Fuzzer 有两种主要模式：基于生长的模糊测试和基于变异的模糊测试。

四、 编程与开发

编写和优化攻击代码与脚本，用于渗透测试、漏洞利用，甚至是设计并实现木马程序、黑客工具，以支持攻防需求，是白帽子在攻击侧需要具备的较高级能力。编程与开发能力主要包括 Web 开发与编程、编写 PoC 或 EXP 等利用两个方面。

在 Web 开发与编程方面，白帽子最为经常遇到和需要掌握的编程语言包括：Java、PHP、Python、C/C++、Golang 等。

而编写 PoC 或 EXP 等利用，又可以分为一般利用和高级利用。编写 PoC 或 EXP 等一般利用主要包括针对 Web 漏洞、智能硬件/IoT 漏洞、WAF 等防护设备绕过等利用。编写 PoC 或 EXP 高级利用，则主要包括编写针对 Windows、Android、iOS、Linux、macOS 等操作系统，以及针对网络安全设备等的漏洞利用。

（一） Web 开发与编程

掌握一门或几门的开发与编程语言，是白帽子深入挖掘 Web 应用漏洞,分析 Web 站点及业务系统运行机制的重要基础能力。在实战攻防演习中，白帽子最为经常遇到和需要掌握的编程语言包括：Java、PHP、Python、C/C++、Golang 等。

1） Java

Java 是一种面向对象的计算机编程语言，具有简单性、功能强大、分布式、健壮性、安全性、平台独立与可移植性、多线程及动态性的特点，经常用于编写桌面应用程序、Web 应用程序、分布式系统和嵌入式系统应用程序等。

2） PHP

PHP 原为 Personal Home Page 的缩写，后更名为 Hypertext Preprocessor，但保留了人们已经习惯的“PHP”的缩写形式。其含义为：超文本预处理器，是一种通用开源脚本语言。PHP 主要适用于 Web 开发领域，是在服务器端执行的，常用的脚本语言。PHP 独特的语法混合了 C、Java、Perl 以及 PHP 自创的语法，利于学习，使用广泛。

3） Python

Python 是一种跨平台的计算机程序设计语言， 是一个高层次的，结合了解释性、编译性、互动性和面向对象的脚本语言。最初被设计用于编写自动化脚本(Shell)，随着版本的不断更新和语言新功能的添加，逐渐被用于独立的、大型项目的开发。

4） C/C++

C/C++是一种通用的编程语言，广泛用于系统软件与应用软件的开发。语言具有高效、灵活、功能丰富、表达力强和较高的可移植性等特点，在程序设计中备受青睐，是当前使用最为广泛的编程语言。在 Web 开发中常用于嵌入式设备的开发。

5） Golang

Golang 语言，简称 Go 语言，是由三位 Google 工程师开发的一种静态强类型、编译型语言。Go 语言语法与 C 相近，但具有内存安全、垃圾回收、结构形态及 CSP-style 并发计算等功能。

（二） 编写 PoC 或 EXP 等一般利用

编写漏洞验证代码或漏洞利用代码，是比单纯的漏洞发现更加具有实战意义的白帽能力。其中主要包括 PoC 或 EXP 等两种方式。

PoC，是 Proof of Concept 的缩写，即概念验证，特指为了验证漏洞存在而编写的程序代码。有时也经常被用来作为 0day、Exploit（漏洞利用）的别名。

EXP，是 Exploit 的缩写，即漏洞利用代码。一般来说，有漏洞不一定就有 EXP，而有 EXP，就肯定有漏洞。

PoC 和 EXP 的概念仅有细微的差别，前者用于验证，后者则是直接的利用。能够自主编写 PoC 或 EXP，要比直接使用第三方编写的漏洞利用工具或成熟的漏洞利用代码困难的多。但对于很多没有已知利用代码的漏洞或 0day 漏洞，自主编写 PoC 或 EXP 就显得非常重要了。

此外，针对不同的目标或在不同的系统环境中，编写 PoC 或 EXP 的难度也不同。针对 Web 应用和智能硬件/IoT 设备等，编写 PoC 或 EXP 相对容易，属于进阶能力；而针对操作系统或安全设备编写 PoC 或 EXP 则更加困难，因此属于高阶能力了。

（三） 编写 PoC 或 EXP 等高级利用

在前述“进阶能力”中的“（三）编写 PoC 或 EXP 等利用”中，我们已经介绍了 PoC 和 EXP 的概念，这里不再累述。相比于针对 Web 应用和智能硬件/IoT 设备编写 PoC 或 EXP，针对各种类型的操作系统和安全设备编写 PoC 或 EXP 要更加困难，属于高阶能力。

高阶能力中，比较被关注的几个操作系统和设备包括：Windows、Android、iOS、Linux、macOS、网络安全设备。

1） Windows

由微软公司开发的个人电脑操作系统。

在本文此处，Windows 代指能够在 Windows 操作系统上找到漏洞并利用漏洞编写 PoC 或 EXP 的能力。

2） Android

由 Google 公司和开放手机联盟领导及开发的操作系统，主要使用于移动设备，如智能手机和平板电脑。

在本文中，Android 代指能够在 Android 操作系统上找到漏洞并利用漏洞编写 PoC 或 EXP 的能力。

3） iOS

由苹果公司开发的移动操作系统，主要使用于 iPhone、iPod touch、iPad 上。

在本文中，iOS 代指能够在 iOS 操作系统上找到漏洞并利用漏洞编写 PoC 或 EXP 的能力。

4） Linux

主要使用于服务器的操作系统， Ubnutu、CentOS 等均属基于 Linux 内核基础上开发的操作系统。

在本文中，Linux 代指能够在 Linux 操作系统上找到漏洞并利用漏洞编写 PoC 或 EXP 的能力。

5） macOS

由苹果公司开发的操作系统，主要运用于 Macintosh 系列计算机。macOS 的架构与 Windows 不同，很多针对 Windows 的计算机病毒在 macOS 上都无法攻击成功。

在本文中，macOS 代指能够在 macOS 操作系统上找到漏洞并利用漏洞编写 PoC 或 EXP 的能力。

6） 网络安全设备

在实战化环境中，经常会遇到的网络安全设备包括 IP 协议密码机、安全路由器、线路密码机、防火墙、安全服务器、公开密钥基础设施（PKI）系统、授权证书（CA）系统、安全操作系统、防病毒软件、网络/系统扫描系统、入侵检测系统、网络安全预警与审计系统等。

网络安全设备本身也会存在各种各样的安全漏洞，在近年来的实战攻防演习中，受到越来越多的重视和利用。

在本文中，网络安全设备代指能够在各类网络安全设备中找到漏洞并利用漏洞编写 PoC 或 EXP 的能力。

五、 社工与渗透

在对目标网络进行入侵活动时，社会工程学（也称为社工钓鱼）方法和网络渗透方法是最为主要、最为常用的攻击手段。在此将二者合并简称为社工与渗透能力。

（一） 社工钓鱼

社工钓鱼，是指利用社会工程学手法，利用伪装、欺诈、诱导等方式，利用人的安全意识不足或安全能力不足，对目标机构特定人群实施网络攻击的一种手段。社工钓鱼，既是实战攻防演习中经常使用的作战手法，也是黑产团伙或黑客组织最为经常使用的攻击方式。在很多情况下，“搞人”要比“搞系统”容易得多。

社工钓鱼的方法和手段多种多样。在实战攻防演习中，最为常用，也是最为实用的技能主要有三种：社工库收集、鱼叉邮件和社交钓鱼。其中，前面两个都属于情报收集能力，而后面两个则属于攻防互动能力。

1） 社工库收集

社工库收集能力，是指针对特定目标机构的社工库信息的收集能力。

所谓社工库，通常是指含有大量用户敏感信息的数据库或数据包。这些敏感信息包括但不限于，如账号、密码、姓名、身份证号、电话号码、人脸信息、指纹信息、行为信息等。由于这些信息非常有助于攻击方针对特定目标设计有针对性的社会工程学陷阱，因此将这些信息集合起来的数据包或数据库，就被称为社会工程学库，简称社工库。

社工库是地下黑产或暗网上交易的重要标的物。不过，在实战攻防演习过程中，白帽子所使用的社工库资源，必须兼顾合法性问题，这就比黑产团伙建立社工库的难度要大得多。

2） 鱼叉邮件

鱼叉邮件能力，是指通过制作和投递鱼叉邮件，实现对机构内部特定人员有效欺骗的一种社工能力。

鱼叉邮件是针对特定组织机构内部特定人员的定向邮件欺诈行为，目的是窃取机密数据或系统权限。鱼叉邮件有多种形式，可以将木马程序作为邮件的附件发送给特定的攻击目标，也可以构造特殊的、有针对性的邮件内容诱使目标人回复或点击钓鱼网站。鱼叉邮件主要针对的是安全意识或安全能力不足的机构内部员工。不过，某些设计精妙的鱼叉邮件，即便是经验的安全人员也难以识别。

3） 社交钓鱼

社交钓鱼能力，是指通过社交软件或社交网站与攻击目标内的成员进行沟通交流，骗取对方信任并借此收集相关情报信息的能力。社交钓鱼，一般建立在使人决断产生认知偏差的基础上，具体形式包括但不限于：微信、QQ 等社交软件/网站的在线聊天、电话钓鱼、短信钓鱼等。

社交钓鱼，其实也是网络诈骗活动的主要方法，但以往实战攻防演习中还很少被使用。

但随着防守方能力的不断提升，直接进行技术突破的难度越来越大，针对鱼叉邮件也有了很多比较有效的监测方法，于是近两年，社交钓鱼方法的使用就开始越来越多了。

（二） 内网渗透

内网渗透，是指当攻击方已经完成边界突破，成功入侵到政企机构内部网络之后，在机构内部网络中实施进一步渗透攻击，逐层突破内部安全防护机制，扩大战果或最终拿下目标系统的攻击过程。

在实战攻防环境下，白帽子比较实用的内网渗透能力包括：工作组或域环境渗透、内网权限维持/提权、数据窃取、常见隧道工具使用、横向移动、免杀、云安全防护绕过与终端安全防护绕过等。

1） 工作组、域环境渗透

工作组和域环境都是机构内部网络结构的基本概念。工作组通常是指一组相互联结，具有共同业务或行为属性的终端（计算机）集合。组内终端权限平等，没有统一的管理员或管理设备。通常来说，工作组的安全能力上线就是每台终端自身的安全能力。

域环境，则是由域控服务器创建的，具有统一管理和安全策略的联网终端的集合，域控服务器和域管理员账号具有域内最高权限。通常来说，域环境的安全性要比工作组高很多，但如果域管理员账号设置了弱口令，或域控服务器存在安全漏洞，也有可能导致域控服务器被攻击者劫持，进而导致域内所有设备全部失陷。

出于安全管理的需要，大型机构的内部网络一般都会被划分为若干个域环境，不同的域对应不同的业务和终端，执行不同的网络和安全管理策略。而在一些网络管理相对比较松散的机构中，内网中也可能只有若干的工作组，而没有域环境。

在本文中，白帽子的工作组、域环境渗透能力，是指白帽子能够掌握内网环境中，工作组或域环境的运行管理机制，能够发现其中的设计缺陷或安全漏洞，并加以利用实施攻击的能力。

2） 横向移动

横向移动，通常是指攻击者攻破某台内网终端/主机设备后，以此为基础，对相同网络环境中的其他设备发起的攻击活动，但也常常被用来泛指攻击者进入内网后的各种攻击活动。

在本文中，白帽子的横向移动能力，是泛指以内网突破点为基础，逐步扩大攻击范围，逐步攻破更多内网设备或办公、业务系统的技术能力。

3） 内网权限维持/提权

攻击者通常是以普通用户的身份接入网络系统或内网环境，要实现攻击，往往还需要提升自身的系统权限，并且使自身获得的高级系统权限能够维持一定的时间，避免被系统或管理员降权。提升系统权限的操作简称提权，维持系统权限的操作简称权限维持。

在实战环境下，系统提权的主要方式包括：利用系统漏洞提权、利用应用漏洞提权、获取密码/认证提权等。

在本文中，白帽子的内网权限维持/提权能力，是指白帽子在内网环境中，能够利用各种安全设计缺陷或安全漏洞，提升自己的系统权限，以及维持提权有效性的技术能力。

4） 数据窃取

对机密或敏感数据的窃取，是实战攻防演习工作中最常见的预设目标之一，也是黑客针对政企机构网络攻击活动的主要目的之一。一般来说，机构内部的很多办公系统、业务系统、生产系统中，都会有专门的服务器或服务器集群用于存储核心数据，数据服务器的防护一般也会比其他网络设备更加严密一些。

在本文中，白帽子的数据窃取能力，是指白帽子能够熟练掌握服务器的数据库操作，能够在内网中找到机构的核心系统数据服务器，能够获取服务器访问或管理权限，能够在防守方不知情的情况下将数据窃取出来并秘密外传的技术能力。

5） 免杀

免杀，英文为 Anti Anti-Virus，是高级的网络安全对抗方式，是各种能使木马病毒程序免于被杀毒软件查杀的技术的总称，可以使攻击者编写的木马病毒程序在目标主机上秘密运行，不被发现。

免杀技术，不仅要求开发人员具备木马病毒的编写能力，同时还需要对各种主流安全软件的运行框架、杀毒引擎的工作原理、操作系统的底层机制、应用程序的白利用方式等，有非常深入的了解，并能据此编写对抗代码。使用免杀技术，对于白帽的基础能力要求非常之高。

在本文中，白帽子的免杀技术能力，是指白帽子能够编写木马病毒程序实现免杀的技术能力。通过使用第三方工具（如加密壳）在某些安全防护薄弱的环境下也能达到免杀目的，但这种基础能力不属于本文描述的免杀技术能力。

6） 常见隧道工具

隧道工具是指利用一种网络协议封装另一种网络协议的技术手段，用于数据伪装、穿越防火墙或绕过网络安全设备的检测。这些工具通常具备高度隐蔽性和灵活性，能够帮助攻击者建立安全的通信通道，以实现远程控制和数据传输等目的。

常见的隧道工具包括 HTTP 隧道、DNS 隧道、ICMP 隧道、SSH 隧道等。其中，HTTP 隧道利用 HTTP 协议的广泛性和复杂性，将任意类型的网络流量通过 HTTP 数据包进行传输，实现高效稳定的隐蔽通信；DNS 隧道则通过 DNS 查询和响应机制传输数据，适用于特定网络环境；ICMP 隧道利用 ICMP 协议（如 ping 命令）封装数据，实现简单的隐蔽通信；而 SSH 隧道则通过 SSH 协议建立加密通道，提供更高安全性的数据传输服务。例如，CobaltStrike、Empire 等渗透测试工具均支持多种隧道功能，可根据具体需求进行选择和配置。

7） 云安全防护绕过

云安全防护指利用云计算技术和安全策略，为云环境中的数据和系统提供全面保护，以抵御外部攻击和内部威胁，确保云服务的连续性和数据的完整性、保密性。

云安全防护在攻防演练中通常包括防火墙、入侵检测与防御系统（IDS/IPS）、数据加密、访问控制、安全审计等关键要素。这些要素协同工作，通过实时监控、智能分析和快速响应，有效识别和阻止潜在的安全威胁，为攻防演练提供坚实的安全保障。同时，云安全防护还具备灵活性和可扩展性，能够根据演练需求进行动态调整和优化。

而所谓的云安全防护绕过，就是指了解云安全防护的基本原理和技术手段，进而能够采

取有效措施，绕过相关安全防护措施对云服务系统实施攻击，且不被发现的能力。

8） 终端安全防护绕过

终端安全防护绕过是指攻击者采用一系列技术手段和策略，规避或突破终端系统上的安全防护措施，以实现对目标系统的非法访问、数据窃取或恶意操作等目的的攻击能力。这些技术手段可能包括利用系统漏洞、绕过安全策略、伪装合法行为等。

实现终端安全防护绕过的具体方式多种多样，包括但不限于利用脚本攻击、模拟合法行为、进程篡改、内存解密等。攻击者可能通过精心设计的攻击链，逐步渗透目标系统，最终绕过终端安全防护机制，达成其攻击目标。同时，一些高级的攻击手段还可能利用加密技术、多态变形等技术来增加攻击的隐蔽性和复杂性。

六、 攻击辅助

攻击辅助是指能够提升攻击活动成功率，或避免自身非发现的各类辅助性技术手段。这些技术手段通常都不是直接的攻击技术，但与各种攻击技术、社工手法配合使用，就能大大提升攻击活动的效率和成功率。目前，攻击辅助能力主要体现在身份隐藏、大模型辅助及情报收集与分析三方面。

（一） 身份隐藏

为避免自己的真实 IP、物理位置、设备特征等信息在远程入侵的过程中被网络安全设备记录，甚至被溯源追踪，攻击者一般都会利用各种方式来进行身份隐藏。在实战攻防演习中，攻击方所采用的身份隐藏技术主要有以下几类：匿名网络、盗取他人 ID/账号、使用跳板机、他人身份冒用和利用代理服务器等。

1） 匿名网络

匿名网络泛指信息接受者无法对信息发送者进行身份定位与物理位置溯源，或溯源过程极其困难的通信网络。这种网络通常是在现有的互联网环境下，通过使用特定的通信软件组成的特殊虚拟网络，从而实现发起者的身份隐藏。其中以 Tor 网络（洋葱网络）为代表的各类“暗网”是比较常用的匿名网络。

在本文中，白帽子的匿名网络能力，是指白帽子能够使用匿名网络对目标机构发起攻击，并有效隐藏自己身份或位置信息的能力。

2） 盗取他人 ID/账号

盗取他人 ID/账号，一方面可以使攻击者获取与 ID/账号相关的系统权限，进而实施非法操作；另一方面也可以使攻击者冒充 ID/账号所有人的身份进行各种网络操作，从而实现攻击者自身身份隐藏的目的。

不过，在实战攻防演习中，通常不允许随意盗取与目标机构完全无关人员的 ID/账号，因此，在本文中，白帽子的盗取他人 ID/账号能力，是指白帽子能够盗取目标机构及其相关机构内部人员 ID/账号，以实现有效攻击和身份隐藏的能力。

3） 使用跳板机

使用跳板机，是指攻击发起者并不直接对目标进行攻击，而是利用中间主机作为跳板机，

经过预先设定的一系列路径对目标进行攻击的一种攻击方法。使用跳板机的原因主要有两个方面：一是受到内网安全规则的限制，目标机器可能直接不可达，必须经过跳板机才能间接访问；二是使用跳板机，攻击者可以在一定程度上隐藏自己的身份，使系统中留下的操作记录多为跳板机所为，从而增加防守方溯源分析的难度。

在本文中，白帽子使用跳板机的能力，是指白帽子能够入侵机构内部网络，获得某些主机控制权限，并以此为跳板，实现内网横向移动的技术能力。

4） 他人身份冒用

他人身份冒用，是指通过技术手段对身份识别系统或安全分析人员进行欺骗，从而达到冒用他人身份实现登录系统、执行非法操作及投放恶意程序等攻击行为。这里所说的他人身份冒用技术不包括前述的盗取他人 ID/账号。

在本文中，白帽子的他人身份冒用能力，是指白帽子能够使用各种技术手段冒用他人身份，入侵特定系统的技术能力。

5） 利用代理服务器

代理服务器，是指专门为其他联网设备提供互联网访问代理的服务器设备。在不使用代理服务器的情况下，联网设备会直接与互联网相连，并从运营商那里分配获得全网唯一的 IP 地址。而在使用代理服务器的情况下，联网设备则是首先访问代理服务器，再通过代理服务器访问互联网。

代理服务器的设计，最初是为了解决局域网内用户联结互联网的需求而提出的，局域网内所有的计算机都通过代理服务器与互联网上的其他主机进行通信。对于被通信的主机或服务器来说，只能识别出代理服务器的地址，而无法识别事出局域网内哪一台计算机与自己通信。

在实战攻防环境下，攻击方使用代理服务器联网，就可以在一定程度上隐藏自己的 IP 地址和联网身份，增加防守方的溯源难度和 IP 封禁难度。在某些情况下，攻击者甚至还会设置多级代理服务器，以此实现更加深度的身份隐藏。

在本文中，白帽子的利用代理服务器能力，是指白帽子在攻击过程中，能够使用一级或多级代理服务器，从而实现身份隐藏的能力。

（二） 大模型辅助

大模型辅助是指在网络攻防实战过程中，通过使用各种大模型工具，实现加速攻击效率、智能分析预测目标系统潜在弱点，并自动优化攻击手段等目的的攻击辅助方法。目前在白帽子中比较流行的大模型辅助方法包括：大模型深度伪造、大模型辅助爆破、大模型漏洞挖掘、大模型开发及大模型辅助 EXP 开发。

1） 大模型深度伪造

大模型深度伪造是指利用生成式人工智能大模型工具，辅助生成能够以假乱真的图像、视频、语音、文字等深度伪造内容，从而提升社工钓鱼活动的成功率。目前，在网络安全实战攻防演习中，利用大模型生成深度伪造的电子邮件、钓鱼网站等内容最为常见。

2） 大模型辅助爆破

大模型辅助爆破是指利用大模型工具，针对特定应用系统，快速制定爆破策略、自动生成爆破程序、自动实施爆破攻击的一种辅助攻击方法。在大模型工具的辅助下，网络爆破攻击甚至可以实现完全的自动化，甚至还能自动制定策略以躲避应用系统自身的防爆破策略。

3） 大模型辅助漏洞挖掘

大模型辅助漏洞挖掘是指利用大模型工具，实现针对特定应用系统的自动化的漏洞挖掘工作。需要说明的是，仅就目前的大模型发展现状而言，漏洞挖掘的具体技术方法仍然需要由攻击者自己来实现，但攻击者可以通过使用大模型工具，辅助探测网络结构、分析网络特点、并制定和优化漏洞挖掘策略。

4） 大模型辅助开发

大模型辅助开发是指利用大模型平台，帮助开发者实现自动编程的能力。开发者只需要用自然语言向大模型平台描述自己的开发需求，大模型平台就会帮助开发者自动生成相关代码程序。如果开发者需要开发具有黑客性质的攻击程序，一般还需要掌握黑产大模型的使用或民用大模型平台的“越狱”方法。

5） 大模型辅助 EXP 开发

大模型辅助 EXP 开发是指利用大模型平台来加速和优化 EXP 开发过程的能力。利用大模型，可以自动化地分析漏洞信息、生成潜在的攻击代码片段，甚至辅助开发人员完成 EXP 的编写和测试，从而提高 EXP 开发的效率和准确性。

（三） 情报收集与分析

情报收集与分析是网络安全实战攻防演习过程中，攻击队必不可少的前期准备工作。只有充分的掌握目标系统的精准情报，才能实现对目标系统的高效攻击。具体来说，主要包括公开情报收集、开源安全情报、黑灰产情报、目标系统信息及关键人锁定等几个方面。

1） 公开情报收集

公开情报收集是指通过新闻咨询、搜索引擎、社交媒体等渠道，广泛搜集目标单位在互联网上被公开披露的信息，包括但不限于主要业务、近期活动、供应商与合作伙伴等。收集这些信息，可以为网络探测、社工钓鱼和供应链攻击提供重要的参考。

2） 开源安全情报

开源安全情报收集是指通过全球各大威胁情报平台、开源检测平台等，检索和收集与目标单位相关的技术情报和威胁情报，内容包括但不限于：数据泄露情况、重要资产暴露、漏洞历史报告、攻击信息历史报告等。收集此类情报，可以帮助攻击者更加高效的获得目标单位已知的安全弱点。

3） 黑灰产情报

黑灰产情报收集是指在黑客论坛、暗网平台等黑灰产交易渠道中，寻找与目标单位、系统相关的黑灰产交易信息，如数据泄露、安全漏洞、系统权限等。在网络安全实战攻防演习活动中，此类情报的利用价值很高。

4） 目标系统信息

目标系统信息包括目标单位信息（如：IP 地址、域名、APP、小程序、公众号等）、网络拓扑架构、系统组件等。了解目标系统的网络架构、网络设备、连接方式、重要节点位置、操作系统、数据库、中间件、Web 服务器及版本信息等。

收集目标系统信息，是渗透攻击的重要技术基础。

5） 关键人锁定

关键人锁定指通过各类情报信息的综合分析，找到与目标系统相关的关键岗人员的个人信息，包括但不限于邮箱、电话、社交账号，个人身份信息等内容。所谓的关键岗位，包括系统管理员、运维人员、客服人员、领导、财务等，需要根据具体的攻击目标而定。关键人一旦锁定，也就为后续的社工钓鱼、技术渗透锁定了攻击方向。

七、 其他攻击能力

除了前述各项安全能力外，实战化白帽攻击人才还需要具备以下一些通用或特殊能力，包括大模型安全、掌握 CPU 指令集与团队协作等。

（一） 大模型安全

大模型安全是指能够对针对应用系统所使用的 AI 大模型本身进行攻击的一种安全能力。具体来说，又可以分为大模型越狱和大模型组件安全两个方向。

由于大模型技术已经在众多行业中得到了普及应用，因此，大模型本身的安全问题也倍受关注。在 2024 年的网络安全实战攻防演习中，已经有攻击队能够通过对应用系统大模型的攻击，实现既定的攻击目标任务。

1） 大模型越狱

大模型越狱是指攻击者通过精心设计的提示词、角色扮演或其他狡猾指令，诱导或绕过大模型的内置安全机制和防护措施，使其输出潜在的危险、违法或有害内容，进而达成攻击目标。

这种攻击手法充分利用了大模型对复杂上下文的强大处理能力，通过巧妙构造输入内容，使得大模型在不知不觉中被“洗脑”，进而违反原有的安全设定。其关键在于发现并利用大模型在理解和响应特定类型输入时的漏洞或缺陷，从而达到越狱攻击的目的。同时，随着大模型技术的不断发展，这种攻击手法也在不断演进和复杂化，这页对大模型的安全提出了更高的挑战。

2） 大模型组件安全

大模型组件安全一般是指确保大规模预训练模型（大模型）的组成部分，包括数据输入、处理逻辑、输出结果等，在面临各种潜在攻击时能够保持稳定性、保密性和完整性，从而保护整个系统免受未授权访问、数据泄露或功能破坏的风险。

而在本白皮书中，大模型组件安全是指针对大模型组件的攻击能力，即攻击者能够对大模型组件发起攻击，并使琦产生错误决策的攻击能力。从当前实践来看，针对大模型组件的攻击的方法主要包括模式欺骗、样本投毒、漏洞利用等。

（二） 掌握 CPU 指令集

CPU 指令集，即 CPU 中用来计算和控制计算机系统的一套指令的集合。每一种不同的 CPU 在设计时都会有一系列与其他硬件电路相配合的指令系统。指令系统包括指令格式、寻址方式和数据形式。一台计算机的指令系统反应了该计算机的全部功能。机器类型不同，其指令集也不同。而白帽子对 CPU 指令集的掌握程度，将直接决定白帽子进行系统层漏洞挖掘与利用的能力水平。本文指掌握不同架构下的底层程序分析。

目前，最为常见的 CPU 指令集包括 x86、MIPS、ARM 和 PowerPC。

1） x86

x86 一般指 Intel x86。x86 指令集是 Intel 为其 CPU 专门开发的指令集合。

通过分析 x86 指令集可以找到 intel 下相关软件或系统的运行机制，从而通过指令实现底层攻击。

2） MIPS

MIPS（Microcomputer without Interlocked Pipeline Stages）的含义是无互锁流水级微处理器，该技术是 MIPS 公司（著名芯片设计公司，）设计开发的一系列精简的指令系统计算结构，最早是在 80 年代初期由斯坦福(Stanford)大学 Hennessy 教授领导的研究小组研制出来的。由于其授权费用低，因此被 Intel 外的大多数厂商使用。

通过分析 MIPS 指令集可以找到除 Intel 外大多厂商（多见于工作站领域）的软件或系统运行机制，从而通过指令实现底层攻击。

3） ARM

ARM（Advanced RISC Machines），即 ARM 处理器，是英国 Acorn 公司设计的，低功耗的第一款 RISC（Reduced Instruction Set Computer，精简指令集计算机）微处理器。

在本文中，ARM 指 ARM 指令集。ARM 指令集是指计算机 ARM 操作指令系统。ARM 指令集可以分为跳转指令、数据处理指令、程序状态寄存器处理指令、加载/存储指令、协处理器指令和异常产生指令六大类。

4） PowerPC

PowerPC（Performance Optimization With Enhanced RISC-Performance Computing）是一种精简指令集架构的中央处理器，其基本的设计源自 IBM 的 POWER 架构。POWER 是 1991 年，Apple、IBM、Motorola 组成的 AIM 联盟所发展出的微处理器架构。PowerPC 处理器有广泛的实现范围，包括从高端服务器 CPU（如 Power4） 到嵌入式 CPU 市场（如任天堂游戏机）。但苹果公司自 2005 年起，旗下计算机产品转用 Intel CPU。

（三） 团队协作

随着网络安全实战攻防演习实践的不断深入和防守方的整体能力持续提升，白帽子单凭强大的个人能力单打独斗取得胜利的希望越来越小。而由 3~5 人组成的攻击小队，通过分工协作的方式高效完成攻击行动的模式已经越来越成熟。而对于白帽子来说，是否拥有团队协作的作战经验，在团队中扮演什么样的角色，也是白帽子实战化能力的重要指标。

团队作战，成功的关键的是协作与配合。通常来说，每只攻击队的成员都会有非常明确的分工和角色。在实战攻防演习实践中，攻击队比较常见的角色分工主要有 7 种，分别是：

行动总指挥、情报收集人员、武器装备制造人员、打点实施人员、社工钓鱼人员、内网渗透人员、攻击成果报告撰写人员。需要说明的是，在实际演习过程中，一人分饰多个角色也是非常普遍的。

1） 行动总指挥

通常是攻击队中综合能力最强的人，需要有较强的组织意识、应变能力和丰富的实战经验，负责策略制定、任务分发、进度把控等。

2） 情报收集人员

负责情报侦察和信息收集，收集内容包括但不限于：目标系统的组织架构、IT 资产、敏感信息泄露、供应商信息等。

3） 武器装备制造人员

负责漏洞挖掘及工具编写，是攻击队的核心战斗力量，不仅要能找到漏洞并利用漏洞，还要力求在不同环境下达到稳定、深入的漏洞利用。

4） 打点实施人员

负责获取接入点，进行 Web 渗透等。找到薄弱环节后，利用漏洞或社工等方法，获取外网系统控制权限，之后寻找和内网连通的通道，建立据点（跳板）。

5） 社工钓鱼人员

负责社工攻击。利用人的安全意识不足或安全能力不足等弱点，实施社会工程学攻击，通过钓鱼邮件或社交平台等进行诱骗，进而成功打入内网。

6） 内网渗透人员

负责进入内网后的横向移动。利用情报收集人员的情报结合其他弱点来进行横向移动，扩大战果。尝试突破核心系统权限，控制核心任务，获取核心数据，最终完成目标突破工作。

7） 攻击成果报告

在网络安全实战攻防演习活动中，攻击队每取得一项攻击成果，都需要撰写一份攻击成果报告上报给演习指挥部，用于评审专家给攻防双方评分。撰写攻击成果报告，也需要一定的格式规范，特别是需要能够清楚的描述攻击成果及“等分原因”（积分规则一般由演习活动主办方制定）。

附录 3 实战化白帽人才能力图谱防守侧能力详解

一、 检查与整改

检查与整改，主要是指在网络安全运营过程中，或在网络安全实战攻防演习之前，对机构网络安全建设与运营的摸底排查和整改加固工作，目的是通过事前有针对性的自查工作，提前发现问题、提前消除隐患。

（一） 安全检查

安全检查，是指按照特定的流程、框架和规范，对机构的网络安全建设与运营状况进行逐一排查并确定问题的过程。安全检查一般需要检查人员具备资产梳理、渗透测试/漏洞发现、安全评估、有效性验证等技术能力。

1） 资产梳理

资产梳理，是指通过对各类网络资产、数据资产、安全资产等在线资产的梳理，使系统的运营者或演习中的防守一方，能够全面了解自有阵地、清晰把握防守重点、提前明确关键责任人等信息的一种安全管理方法，，目的是为防守策略的制定提供基础决策依据。

资产梳理包括但不限于：敏感信息梳理、网络架构梳理、互联网资产发现、内网资产梳理、云资产梳理、安全资产梳理、供应链梳理、业务连接性梳理、相关人员信息、API 接口、集权系统/集权设备等。

2） 基线检查

基线检查，是指按照机构设定的网络安全基线标准，对业务系统、网络设备、办公终端等进行安全检查，以确定检查对象是否达到基线要求的标准。一旦发现没有达标的项目，应立即进行整改，直至达标。

3） 渗透测试/漏洞发现

渗透测试/漏洞发现，是指测试人员在获得合法授权之后，通过对目标系统进行攻击渗透，测试系统是否存在防守弱点、技术缺陷或安全漏洞等风险的一种安全检测方法。渗透测试/漏洞发现与其他各类网络安全评估方法的主要不同，在于其采用的是攻击者视角，测试过程中通常也会允许使用一些无害的，或者是破坏性轻微的攻击手法和黑客工具。

通常情况下，渗透测试/漏洞发现主要针对的系统包括：互联网系统、集权系统、业务系统、安全设备等。而要完成渗透测试工作，通常也要求测试者掌握各类网路攻防技术和漏洞挖掘技术。

4） 有效性验证

有效性验证，是指为验证相关机构或防守单位已经部署的各类网络安全措施和安全策略是否实际有效、验证安全设备或安全系统是否能正常有效运行，而进行的一系列测试工作的总称。有效性验证的常用方法包括但不限于：现场检查、上机排查、流程演练、漏洞验证、模拟攻击测试等。

（二） 整改加固

整改加固，是指对已经发现的安全漏洞、敏感信息泄露、资产暴露、策略不足、弱口令等问题进行及时定位和修补，提前排除各类技术隐患的安全工作。整改加固过程一般需要具备漏洞修复与升级、防护措施补全、安全设备加固和安全策略初始化等技术能力。

1） 应用漏洞修复与升级

应用漏洞修复与升级，是指对于已经检出安全漏洞的各类系统，包括但不限于操作系统、应用平台、业务系统等进行安全升级或加固的过程。对于已经有官方补丁的系统，应在确认不会引发业务中断或兼容性问题的情况下，对系统进行升级和打补丁。而对于没有官方补丁的系统，如果自研或定制开发的系统，则需手动修复安全漏洞或采取必要的加固防范措施，以确保系统漏洞不会被攻击者利用。

2） 安全设备加固

安全设备加固，是特指针对各类网络安全设备、网络安全系统的升级和加固。

需要说明的是，安全设备的升级与加固方式，与操作系统或应用平台不太一样，一般只能使用特定供应商的官方补丁工具包，按照特定的专业规范进行升级和加固操作，操作不当还有可能把设备刷成“砖头”。由于安全厂商数量众多，安全设备品类繁多，安全人员想要全面掌握各类网络安全设备的升级和加固方法，还是有一定挑战性的。

3） 安全策略优化

安全规则初始化，是指对于已经完成科学部署的一系列网络安全设备和安全系统，进行具体防护规则初始化配置。

安全规则初始化，不仅需要全面了解各类网络安全设备和系统的配置方法，还要充分了解内外部安全环境以及需要重点防御的安全威胁类型，能够将威胁与规则进行匹配。此外，安全规则的初始化，还必须认真考虑、详细验证安全规则可能给整个业务系统正常运行造成的影响。一条看似平常的安全规则，完全有可能与正常业务相冲突，从而导致业务中断或业务系统异常。

安全设备配置能力，是指对常见的网络安全设备，如防火墙、EDR、NDR、SOC、堡垒机、上网行为管理等，进行熟练的系统设置和安全规则配置的能力。特别的，当系统内部存在大量安全设备时，安全人员还需要掌握能够给大量安全设备进行批量规则下发的策略与方法。

4） 防护措施补全

防护措施补全，是指如果在安全检查过程中，发现网络系统中存在诸如安全设备部署不全、流量监测数据补全、重要岗位无人值守、关键流程存在缺失等防护措施不到位的问题时，进行整改和措施补全的过程。此外，科学合理的部署蜜罐、蜜点等诱捕措施，也属于防护措施补全的相关工作。

需要说明的是，防护措施并非是一成不变的，而是需要根据机构业务特征、IT 架构进行有针对性的设计和部署，对于安全人员的综合能力要求较高。

（三） 规则优化

规则优化，是指根据攻防态势的动态变化、根据事件分析及追踪溯源的结果，对各类网络安全设备、网络安全系统的识别与拦截规则进行动态优化配置。

1） 规则优化

规则优化能力，是指能够根据攻防态势及安全事件分析结果，设计各类安全设备规则的优化策略的能力，包括但不限于对错误规则或无效规则的清理、对不完善规则的调整、对新增必要规则的补全等。同时，动态规则优化，还必须考虑规则与正常业务的兼容性问题，能够完成试验环境搭建与测试。

2） 降噪

降噪主要是指通过部署安全设备、优化告警策略等手段，减少误报和无效告警的数量，从而提高对真实网络攻击的识别能力和响应效率。这一工作对于防守方在演习中保持清醒的头脑、快速定位并应对真实威胁至关重要。

3） 威胁建模

威胁建模是一种通过系统化、结构化的方法，对可能面临的网络攻击威胁进行识别、评估和分析的过程。它旨在帮助防守方深入了解潜在的安全风险，预测攻击者的可能行为，并制定相应的防御策略。

一般包括识别威胁、评估风险、指定策略、动态调整等多个主要步骤。正确的威胁建模有助于防守方更好的了解自身安全情况，提高应对网络攻击的能力。

二、 监测与分析

监测与分析，是指通过各类网络安全设备或系统，对机构内部网络中发生的各类网络安全威胁事件进行实时监测和分析研判的安全工作。监测与分析，不仅是日常网络安全运营过程中最主要的工作，也是网络安全实战攻防演习过程中最为主要的基础性工作。监测与分析工作，具体来说有可以分为告警监测与事件分析两大类。

（一） 告警监测

告警监测，一般是指通过各类网络安全软件、设备及监测平台，对监测范围内的所有系统中发生的各类网络安全告警信息进行实时监测、汇总的安全工作。告警监测能力，在网络安全实战攻防演习的实战阶段，防守方最为基础性的实战化技能，也是日常网络安全运营工作中最为重要的基础技能。

告警监测的主要范围一般包括：终端告警监测、服务器告警监测、流量告警监测、业务系统告警监测、蜜罐/蜜点告警监测及其他安全设备告警监测。

1） 终端告警监测

资产梳理，是指通过对各类网络资产、数据资产、安全资产等在线资产的梳理，使系统的运营者或演习中的防守一方，能够全面了解自有阵地、清晰把握防守重点、提前明确关键责任人等信息的一种安全管理方法，，目的是为防守策略的制定提供基础决策依据。

终端告警监测，是指针对终端安全软件或相关设备与系统（如 EDR）产生的告警信息进行的监测、分析与处置，监测内容包括但不限于：异常访问、异常操作、病毒木马、漏洞利

用、非法外联等。

2） 服务器告警监测

服务器告警监测，是指针对服务器安全软件或相关设备与系统产生的告警信息进行的监测、分析与处置。相比于普通的办公终端，服务器上运行的业务和系统都要更为复杂，入侵途径和攻击手法也更为广泛，一旦发生安全事件影响面一般也要更大。相应的，服务器上的网络安全监测方法、安全系统部署方式、以及对应的各种处置手段也都与办公终端有很大的不同。

3） 流量告警监测

流量告警监测，是指针对流量威胁检测设备发出的各类告警信息的监测、分析与处置，广泛用于网络安全运营和实战功放演习中的威胁发现。

基于网络流量数据的威胁检测，是现代网络安全技术的重要方法之一。无论攻击者的攻击目的和目标是什么，其攻击活动都一定会通过网络进行传输，并引起网络数据的异常，因此通过网络流量检测各类安全威胁，往往十分高效。此外，部署流量威胁检测设备，一般也不会影响网络中各类设备和系统的运营。

4） 业务系统告警监测

业务系统告警监测，是指针对由机构内部的业务系统、生产系统在运行过程中产生的各类安全告警信息的监测、分析与处置。

与网络安全相关的告警信息，并不一定都来自于网络安全软件、设备或系统。很多业务系统本身也能发出各类安全告警信息。比如，邮件管理系统会自动发出各类异常登录、垃圾邮件或爆破攻击的告警信息；数据库系统也会对各类高风险操作进行记录和告警；服务器系统监测到 CPU 使用率过高并发出告警，很可能是因为系统感染了挖矿木马；工业生产系统突然停止运行并告警，也有可能是因为感染了木马病毒。所以，各类生产系统、业务系统自身发出的安全告警，也应当列入网络安全监测的视野之内。

需要特别说明的是，想要看懂业务系统告警信息，不仅要求安全人员具有基本的网络安全技术能力，还要求安全人员必须对相关机构的业务系统，甚至是相关业务本身都有一定了了解。唯有如此，安全人员才能真正准确把握网络安全与业务安全之间的关系。

5） 蜜罐/蜜点告警监测

蜜罐/蜜点告警监测，是指针对事先部署在机构系统内部的蜜罐或蜜点系统产生的各类告警信息的监测、分析与处置。相关告警信息一般是由攻击者进入蜜罐或踩中蜜点，并进行各类风险操作而触发的。通过监测相关告警信息，可以帮助安全人员在真实的网络攻击发生之前，捕获攻击者的各类关键信息和行为特征。

蜜罐（Honeypot Technology）是一种用来欺骗、扰乱和诱捕攻击者的诱饵系统，促使攻击者把时间花费在虚假的目标系统上，同时也使安全人员得以观察攻击者的行为并采取主动防御措施，进而对攻击者进行溯源或反制。蜜罐应对的不是攻击或漏洞，而是关注攻击者本身。一些设计非常简易但有效蜜罐，也被称蜜点。

6） 其他安全设备告警监测

网络安全设备和系统多种多样，不同的安全设备和系统也会发出各种不同的告警信息。除了前述比较主要的由终端、服务器、流量和蜜罐产生的告警信息外，安全人员在实际的安全运营或攻防演习中，还应尽可能的熟练掌握诸如：防火墙、堡垒机、上网行为管理、VPN等其他各类安全设备产生的各类安全告警信息的监测、分析与处置。

（二） 事件分析

事件分析，是指当疑似网络安全事件发生时，安全人员对于安全事件的性质、原因、攻击面、攻击手段、临时响应措施等进行基本的分析、识别和研判的过程。

也就是说，在事件分析中，一线安全人员需要有能力通过直接线索做出以下基本判定，如：一起事件是否确实为安全事件？是什么样的技术原因触发这个事件？哪些网络资产已经失陷或正在被攻击？快速处置此类问题的常用方法是什么？

完成事件分析，通常需要安全人员具备以下能力：安全事件识别、网络故障识别、攻击手法识别、攻击目标识别。

1）安全事件识别

安全事件识别，是指对疑似安全事件进行基础分析，明确识别事件是否为安全事件，并初步判断触发事件的主要原因的能力。

安全事件识别的难点在于对非安全事件的识别。从实践来看，安全设备发出的告警越多，其中含有非安全事件的可能性就越大。大量的告警信息，实际上是由于安全规则与业务系统存在冲突，导致大量业务流量被识别为了安全威胁。而安全人员就需要有能力对各类告警信息进行综合分析，从中找到真正有威胁的安全事件，并采取相应的安全措施进行应对。而对于识别出的非安全事件，则应进行规则优化，在不会漏报的前提下，努力减少非安全事件触发的告警信息。这就是后面将要说的“降噪”。

2）攻击手法识别

攻击手法识别，是指通过网络安全系统告警、各类业务系统告警、威胁情报信息等，对攻击者当前正在使用的主要攻击手法，如漏洞利用、漏洞扫描、病毒投放、口令爆破、DDoS攻击等进行分析和识别的能力。只有明确了攻击手手法，才能采取有效措施进行应对。

3）被攻击目标识别

被攻击目标识别，是指通过网络安全系统告警、各类业务系统告警、威胁情报信息等，对当前可能已经失陷或正在遭受攻击的网络资产进行识别、定位和确认的能力。

注意，这里所说的攻击目标识别，和追踪溯源或应急响应过程中所说的“确定失陷范围”还有所不同。完全确定失陷范围，一般需要综合日志和告警信息进行逐个排查。而这里所说的攻击目标识别，仅仅限于以告警信息和威胁情报信息等直接线索进行攻击目标判定，目的是为了能够在第一时间做出快速、准确的响应动作。

三、 响应与处置

在完成安全事件的分析或通过追踪溯源完成对攻击者的研判之后，安全人员需要在第一时间对网络安全防护系统进行优化配置，阻断网络攻击活动，阻止事件影响扩散，这就是响

应与处置工作。要做好响应与处置工作，不仅需要具备基本的应急响应能力，还需要具备常见应急场景处置的经验。

（一） 应急响应

应急响应，是指当安全事件发生之后，对系统进行的紧急抢救和处置措施，目的是阻断攻击活动，阻止安全事件的影响扩散。在应急响应过程中，应急人员一般需要具备多种主要能力，具体包括：失陷设备隔离、无补丁漏洞修复、数据恢复与应急工具包使用四大类。

1） 失陷设备隔离

失陷设备隔离，是指对疑似或已经确定被攻击者攻陷的网络设备，如办公终端、服务器等采取的隔离措施，目的是阻断失陷设备与内网其他网络设备的通信，防止木马病毒扩散，或是防止攻击者以失陷设备为跳板攻击其他内网设备。

隔离失陷设备最为简单有效的方法就是物理隔离，包括拔网线、断 WiFi、断电、采用物理手段封堵端口等。不过，定位设备的物理位置往往需要一定的时间，当有大量设备被同时感染时，手动拔线效率也太低；而且对某些重要的业务系统，强行做物理隔离也可能存在其他风险或引起不必要的麻烦。因此，在实际操作环境中，逻辑隔离的方式往往更为普遍，也更为迅速。

逻辑隔离的方法也有很多种，比较常见是网段隔离和访问控制等。

网段隔离，就是把整个内网 IP，根据不同业务、不同工区或应急需要，人为的划分成一个个较小的区域。当有某些高传染性的病毒爆发时，一旦发现一台设备被感染，往往需要立即对整个网段进行隔离。

而访问控制，主要是指对访问网络资源的权限进行严格的认证和控制。常用操作方法包括加策略、改口令、设置黑白名单等。

2） 无补丁漏洞修复

无补丁漏洞修复能力，是指对于那些没有现成的官方安全补丁的系统漏洞，进行手动修复或临时加固的能力。

当我们已知攻击者正在利用某些漏洞对系统进行攻击时，我们需要对漏洞进行修复或加固。这些漏洞如果有官方补丁，当然应该及时打上官方补丁。但在网络安全实战攻防演习中，攻击队利用的很可能是 0day 漏洞，或没有官方补丁的漏洞，这时，就需要安全人员能够手动修复这些安全漏洞，或采取某些临时加固措施，防止漏洞被利用。

需要说明的事，修漏洞和挖漏洞的能力并不等价。会挖洞的人不一定会修洞。因为修复漏洞不仅需要知道漏洞存在的原理，还必须了解平台代码的开发逻辑、开源工程的版本管理、以及触发漏洞的代码在业务体系中的作用。唯有如此，才能正确的修复漏洞，避免因修复漏洞而产生次生灾害。

3） 数据恢复

数据恢复能力，是指通过专业工具部分或全部恢复被删除或破坏的系统数据，以及使用备份数据（包括冷备份、热备份和云备份等）辅助业务系统恢复的技术能力。

对于某些重要系统，如等保三级以上的系统，相关法律法规对于系统遭破坏时的修复时

间，都有非常明确的要求。因此，安全人员不仅需要掌握必要的数据恢复能力，在某些情况下，还要依法具备快速的数据恢复技术能力。

4） 应急工具包

专业安全公司一般会为专业的应急响应人员配备应急工具包，其中包括应急笔记本、各类应急软件、特制安全工具等。应急人员需要能够熟练掌握应急工具包中的软硬件使用。

（二） 常见应急场景处置

常见应急场景处置，主要包括：常见木马/病毒、网页篡改、DDoS 防御、流量劫持恢复、数据泄露及 APT 等场景的处置。每一类特定的应急响应场景，都对应一系列特定的处置流程和专用方法。熟练掌握常见应急响应场景的处置方法，可以大大提升网络安全事件的响应与处置效率。

1） 常见木马/病毒处置

常见木马/病毒的处置能力，是指能够熟练使用各类安全工具或安全方法，对诸如蠕虫病毒、勒索软件、挖矿木马、流氓软件等各类常见的木马病毒程序，进行隔离、清除和系统修复的的能力。

2） 网页篡改

当发现网页被篡改时，需要迅速隔离受影响的系统或文件，防止篡改内容进一步扩散。同时，尽快从最近的安全备份中恢复网站数据，确保网站恢复正常运行。在恢复网站后，深入分析篡改事件的原因，查找并修复网站中存在的安全漏洞。这包括更新系统和应用程序的安全补丁、强化账户密码管理、加强网站访问控制和监控等。同时，建立持续的安全监测机制，定期审查网站的安全性，并采取必要的更新和改进措施，以防止类似事件再次发生。

3） DDoS 防御

防御 DDoS 攻击，通常需要使用流量清洗设备或云抗 D 服务。安全人员不仅需要掌握流量清洗设备的使用方法，还需要了解主流云抗 D 服务商，知道如何快速采购云抗 D 服务，以及如何进行系统、DNS 等配置，以便隐藏自己，适应 DDoS 防御需要。

4） 流量劫持恢复

流量劫持恢复能力，是指当系统遭到流量劫持攻击时，能够修复系统配置，使系统的网络访问恢复正常的安全技术能力。

流量劫持是一种通过在应用系统中植入恶意代码、在网络中部署恶意设备、使用恶意软件等手段，控制客户端与服务端之间的流量通信、篡改流量数据或改变流量走向，造成非预期行为的网络攻击技术。

流量劫持的主要目的是引流推广、钓鱼攻击、访问限制、侦听窃密等。常见的流量劫持表现为：流氓软件、广告弹窗、网址跳转等。常见的流量劫持手段分为：DNS 劫持、HTTP 劫持、链路层劫持等。

解决劫持攻击的主要方法是修复被攻击者篡改的各类网络配置。劫持方法不同，修复方式也不尽相同。

5） 数据泄露

当发现数据泄露事件时，需要立即启动应急响应计划，迅速评估泄露的范围、影响及潜在风险，采取措施控制泄露的进一步扩散，如关闭受影响的系统或服务，限制访问权限等。

在控制泄露后，应急人员需要进行全面的损失评估，包括数据丢失的详细情况、受影响的用户数量及潜在的法律和财务影响。同时，制定并实施恢复计划，包括从备份中恢复数据、通知受影响的用户及合作伙伴、加强安全防御措施等，以尽快恢复业务运营并降低长期影响。

6） APT

APT，全称为高级持续性威胁（Advanced Persistent Threat），通常是指有政府背景的网军组织发动的网络战攻击活动。对于 APT 活动的发现和处置，需要较高的专业安全能力。特别是由于 APT 活动具有“高级”和“持续性”的特点 简单的清除病毒程序和封堵特定 IP 往往都是无效的。处置 APT 活动，一般需要更加全面的系统排查和专业的威胁情报分析。

四、 溯源与反制

溯源与反制，是网络攻防活动中，防守方抑制攻击活动的重要举措。在网络安全实战攻防演习活动中，如果能够对攻击队进行有效的溯源和反制，可以为防守队获得额外积分。

（一） 追踪溯源

追踪溯源，是指对网络攻击活动的源头进行追溯的一种安全方法，内容一般包括但不限于：失陷资产判定、入侵路径还原、攻击者网络资产分析、攻击者行为特征分析、攻击者在网络空间及物理空间中定位、攻击者身份识别等多个方面。

追踪溯源工作，往往需要多方位的安全技能支撑。要完成溯源工作，一般需要分析人员掌握以下主要技能：日志分析、操作系统排查、流量数据分析、文件系统分析、内存与进程分析、数字取证技术、代码同源性分析、威胁情报检索、社交网络溯源、攻击者画像等。

1） 日志分析

日志分析，是指通过深入挖掘操作系统、网络设备及安全设备的日志数据，提取出诸如 IP 地址、登录时间、执行的命令、异常报告等与网络安全事件相关的关键攻击信息，并加以汇总分析的一种安全分析方法。通过日志数据提取关键攻击信息，是溯源分析中最为基础分析技术。

2） 操作系统排查

操作系统排查，是指通过操作系统的系统命令或系统工具，对设备及操作系统的运行状态、网络状态、通信信息、配置信息、账户信息、运行程序、历史操作等关键信息进行排查，进而发现恶意应用、非法用户、爆破记录等攻击信息的一种安全分析方法。

3） 流量数据分析

流量数据分析，是指通过对网络流量数据的全面深入分析，发现诸如漏洞利用（也称为：攻击利用）、病毒传播、DDoS、非法外联及各类安全风险事件的一种安全分析方法。流量数据分析，通常需要有专业的流量威胁监测设备来提供告警数据支撑。

4） 内存与进程分析

内存与进程分析，是指通过深入分析内存中的数据和进程信息，实时了解攻击活动相关手法与详细情况的一种安全分析方法，分析内容包括但不限于恶意代码运行情况、攻击者操作痕迹等重要信息。

5） 威胁情报检索

威胁情报检索，是指通过国内外主流的威胁情报平台，进行威胁情报线索查询、收集与整理的一种技术方法。由于主流的威胁情报平台通常具有海量的数据基础和高效的分析引擎，因此，分析人员通过使用威胁情报平台进行威胁情报检索，效率会远远高于分析人员自己从 0 开始整理情报。

6） 社交网络溯源

社交网络溯源，是指在国内外社交网络平台上，对攻击者进行溯源的一种安全分析方法，具体包括两个方面：一是在不同语言的社交网络上收集威胁信息；二是将已有线索与社交网络信息关联起来，从而更加高效的定位出攻击者的身份信息。

特别是由于很多个人黑客都会在社交网络或黑产交易平台上开设个人账号，因此，社交网络溯源，在溯源分析过程中往往非常有效。这也使其成为高级溯源分析人员的一种必备技能。

7） 代码同源性分析

代码同源性分析，是指对不同的恶意程序、不同的攻击脚本之间是否存在相互关联，是否为相同或相近的攻击源头（包括组织或个人）制作与转播等问题，进行判断的一种安全分析方法。其主要判别依据包括但不限于：代码书写与注释习惯、代码遗与传继承关系、代码的传播途径与方式等。代码同源性分析可以帮助分析人员为不同维度的溯源线索快速的建立起关联关系。

（二） 攻击反制

反制，也称为攻击反制，是指通过各种技术及社工手段，对攻击者进行渗透、控制、数据获取等反向攻击活动，以实现压制攻击活动、抓捕攻击者等目的。

反制，也称为攻击反制，是指在溯源的基础上，通过各种技术及社工手段，对攻击者进行渗透、控制、数据获取等反向攻击活动，以实现压制攻击活动、抓捕攻击者等目的。

在多数情况下，普通政企机构想要对攻击者实施攻击反制，需要得到有关部门的法律授权。不过，在网络安全实战攻防演习过程中，防守方对攻击队采取攻击反制措施，通常是被允许的，还有可能因此而获得更高的比赛分数。

攻击反制的基础是溯源，没有明确的攻击源头，就无法进行有效的、精确的反制。然而，反制并不仅仅需要溯源，还需要具备其他很多攻防能力，如：反向 Web 漏洞利用、黑客工具漏洞利用、反向社工、蜜罐部署、常见黑客工具使用等。

需要特别说明的是，尽管攻击反制中，也需要使用到很多攻击者或攻击队使用的黑客技术和黑客工具，但由于攻击反制是对攻击者的攻击，其具体技战术方法与一般的攻击队攻击还是有一些明显区别的。

1） 反向 Web 漏洞利用

反向 Web 漏洞利用，主要是指防守一方利用攻击者终端、服务器或在线系统等网络资产中存在的 Web 漏洞，实施反向渗透攻击，进而达到夺取攻击者的终端、系统和服务器控制权，获取攻击者资料与数据等目的的攻击手段。

与人们的一般想象不同，尽管攻击者通常都很擅长漏洞利用，但这并不意味着攻击者所使用的系统就是安全的或没有漏洞的。甚至很多时候，由于攻击者专注于攻击，反而会忽视了自身的防御。客观的说，会挖洞不等于会修洞，会修洞也不一定有时间、有精力修复各种安全漏洞。

2） 黑客工具漏洞利用

黑客工具漏洞利用，是指利用各种黑客工具或渗透工具自身存在的漏洞或后门对攻击者进行攻击反制的方法。

事实上，由于严重缺乏系统性的更新升级与安全维护；各种黑客工具或渗透工具中的安全漏洞，往往比一般网站的 Web 漏洞更普遍、存在时间也更持久。此外，黑客工具在设计之初就是为了实施攻击的，而不是自我防护，因此并没有充分考虑自身的安全问题。因此，一旦防守队发现或掌握了攻击者所使用的黑客工具存在的安全漏洞，往往就可以结合诱捕系统（蜜网、蜜罐、蜜点），在“神不知鬼不觉”之间，实现对攻击者的反制。

例如，以下各类黑客工具，均以有比较成熟的漏洞利用反制措施了。如：NPS 未授权漏洞反制、Cobalt Strike（简称 CS）反制、DNSLog 反制、HTTPLog 反制、Goby 反制、AntSword（蚁剑）反制、AWVS 反制、Burp 反制、SQLMap 反制等。

3） 反向社工

反向社工，是指防守一方针对攻击者发起的社会工程学攻击活动。例如，通过邮件、聊天工具等，诱骗攻击者进入蜜罐或下载木马程序，套取攻击者敏感信息等。

由于攻击者通常都善于欺骗和钓鱼，因此，对攻击者实施反向社工，往往需要具备比攻击者更加高级的社工能力和社工手段。

4） 蜜罐/蜜点部署

反制过程中可以使用蜜网、蜜罐、蜜标、蜜点等诱捕技术，对攻击者进行诱捕，使其认为攻击得手，但实际上却留下了攻击痕迹和关键信息，甚至是将防守方埋藏的木马程序“盗走”安装。

一般来说，安全监测只要求值守人员能够看懂蜜罐或蜜点发出的监测告警信息，并能据此做出有效防御即可。而要想真正实现对攻击者的诱捕乃至反制，就必须具备蜜罐或蜜点的精密部署能力，具备对诱饵文件进行伪装和埋藏的能力。

5） 常见黑客工具使用

攻击反制，本质上也是一种攻击活动。因此，对于各类常见黑客工具，也应有一定的掌握。下面列出了目前比较常见黑客工具。

基础安全工具：BurpSuite、SQLMap、AppScan、AWVS、Nmap、Wireshark、MSF、Cobalt Stirke

高级安全工具：IDA、Ghider、binwalk、OllyDbg、peach fuzzer、

其他工具：DNSLog、HTTPLog、Goby、AntSword（蚁剑）

五、 其他能力

除了前述各种安全能力外，实战化白帽防守人才还需要具备以下一些通用或特殊技能。

（一） 协同指挥与决策

协同指挥与决策能力，是指在网络安全实战攻防演习过程中，对防守一方的整体指挥、组织和协调能力。这是一种比较高级的能力，不仅需要有扎实的技术基础，还需要有大量的防守实战经验和指挥作战经验。需要此项能力的，一般是网络安全实战攻防演习防守队的总指挥。

从执行层面来看，协同指挥与决策能力还可以分解为安全规划、响应流程制定、防守角色分配和指挥与决策这四项具体能力。

1） 安全规划

安全规划，指在攻防演习前，对目标系统进行全面的风险评估，识别潜在的安全威胁和漏洞，并基于评估结果制定详细的安全防护策略和应急预案，以确保演习过程中的系统安全和数据保护。

根据安全规划，合理调配人力、物力和技术资源，确保在演习过程中能够及时响应和处置各类安全事件。同时，建立应急响应团队，进行必要的培训和演练，提高团队应对突发事件的能力和效率。

2） 响应流程制定

响应流程制定，是指结合防守单位的组织架构、IT 架构、业务系统特点及行业规范要求等，为安全事件的响应制定流程，以确保任何安全事件，都能得到有计划、有步骤的科学处置。

需要特别强调的是，响应流程的制定，不能只考虑单纯的安全工作，还必须统筹考虑防守机构的业务流程，凡是可能受到安全事件影响的组织或部门，都应被纳入到响应流程之中。

SOAR，是安全编排自动化与响应系统的缩写。SOAR 能够帮助企业和组织将繁杂的安全运营（尤其是安全响应）过程梳理为任务和剧本，将分散的安全工具与功能转化为可编程的应用和动作，然后借助编排和自动化技术，将团队、工具和流程高度协同起来。

在安全事件的响应过程中，参与处置的安全人员并不需要掌握 SOAR 中任务和剧本的编写能力，但需要能够熟练使用 SOAR 系统上的工单功能，包括根据自己的角色触发工单，以及根据系统派发的工单和自己的角色，完成对工单的响应。这就是 SOAR 工单响应能力。

需要说明的是，在实际应用环境中，SOAR 不一定都是独立存在的，相关功能常常会被嵌入到 SOC、态势感知、指挥平台之中。

3） 防守角色分配

防守分配角色，是指根据整体安全策略、设备部署情况、响应流程设计等，对参与网络

安全实战攻防演习的所有人员进行角色分配。

需要特别强调的是，防守角色分配不能只考虑专业安全团队，还必须将 IT 技术人员、网络运维人员、主要业务关联方等的工作人员，全部纳入角色分配。唯有如此，事件响应流程才能得以执行。

4） 指挥与决策

指挥与决策，是网络安全实战攻防演习活动中，最为核心的、也是最为高难度的工作，需要依据响应流程设计、防守角色分配，完成整个防守团队协同指挥工作，并能够对重大安全问题的研判、对关键安全策略的实施做出最终决策。

（二） 情报收集

情报收集，是一项贯穿网络安全实战演习始终的重要工作。不论是在检查与整改阶段、监测与分析阶段、响应与处置阶段、还是溯源与反制阶段，都需要用到情报收集能力。因此，我们将情报收集能力单独提取出来，作为一项关键能力进行单独说明。特别的，这里所说的情报，并不一定都是“威胁情报”。企业日常建设、运营与宣传等工作的情报，也都有收集的意义和价值。

作为防守一方，一般需要掌握以下几类情报收集能力：公开信息情报收集、威胁情报平台使用、自制情报收集工具。

1） 公开信息情报收集

公开信息情报收集，是指通过互联网公开渠道，对防守单位、攻击队各类情报信息的收集。收集这些公开信息情报，可以帮助防守队发现潜在风险点、预判攻击队行动方向，以便更好的完成防守工作。

例如，了解防守单位近期将参与哪些重大活动，就可以预防有针对性的社工钓鱼；了解防守单位都有哪些关键的 IT 供应商，就可以更好的防范供应链攻击；了解各个攻击队的历史战绩和行动特点，就能提前进行有针对性的防守；了解公开的系统或产品漏洞信息，可以进行提前补救和预防。

需要特别说明的是，如果安全人员能够收集到一些防守单位愿意向安全人员公开的内部 IT 资料，也将非常有助于防守工作的实施。

2） 威胁情报平台使用

威胁情报平台使用，是指能够熟练使用国内外主流威胁情报平台，对威胁情报信息进行查询、收集与整理的能力。

威胁情报在防守策略制定、追踪溯源等工作中，都有很多重要的、甚至是关键的应用。

3） 自制情报收集工具

在某些情况下，需要安全人员自制一些情报收集工具，来解决特定目的的情报收集需求，这些情报往往很难在公开渠道或主流威胁情报平台上直接获得。

例如，我们想从某个机构网站上摘录有特定关键词的页面；我们想对某个小语种的境外社区进行分析等。

自制情报收集工具并非是必要能力，但在某些特殊环境下非常有用。

（三） 报告撰写

报告撰写，是一项非常基础的文字能力，一般需要按照特定的规范进行书写。针对网络安全实战攻防演习防守一方的特定情况，撰写以下几类典型报告，是安全人员需要具备的基本能力，具体包括：应急处置报告、防守成果报告、总结整改报告三类。

1） 应急处置报告

应急处置报告，也可以称为安全事件响应报告，是指针对特定的单一网络安全事件撰写的分析与处置报告。应急处置报告，一般需要完整的描述一个事件的发现、分析、处置与结果的全部过程，准确的分析攻击源、攻击范围、事件影响和处置措施等关键问题。

2） 防守成果报告

防守成果报告，一般是指网络安全实战攻防演习中的防守单位，就单次攻防事件，或单一攻击队的活动，向演习裁判组提交的，说明防守一方取得主要成果的报告，目的是按照攻防演习规则，争取获得防守队得分。

不同于应急处置报告，防守成果报告一般关注的不是事件的发生与处置过程，而是关注于防守侧取得的防守“成果”。如：对攻击活动的有效识别与拦截情况，对攻击队的溯源分析结果等。

3） 总结整改报告

总结整改报告，一般是指在网络安全实战攻防演习结束之后，由承担防守任务的主防单位，向防守单位和裁判组提交的，关于此次演习的综合性总结与整改报告。内容通常包括演习时间、演习投入、告警统计、事件响应情况、防守队成果、发现主要问题、关键整改建议等内容。

撰写总结整改报告，一版要求逻辑清晰、内容全面、通俗易懂。

附录 4 补天漏洞响应平台

补天漏洞响应平台（https://www.butian.net），成立于 2013 年 3 月，是国内专注于漏洞响应的第三方平台。补天平台通过充分引导民间白帽力量，实现实时的、高效的漏洞报告与响应。

成立 10 年来，补天平台已经成为全中国影响力最大的漏洞响应平台之一，同时也是最活跃的网络安全从业者交流平台之一。通过奇安信攻防社区、补天白帽大会、“补天杯”破解大赛、补天城市沙龙、补天校园行，搭建安全从业者开放、分享、成长的平台，把国内外网络安全专家、业界大咖、安全厂商、研究机构聚集到一起，将多种形式结合建立网络安全从业者技术生态。同时在实战化的趋势下，人是支撑安全业务的最重要因素，补天平台也成为汇聚海量实战型网络安全人才的资源池。通过提供真实的训练环境，开放实战工具箱和资源，定制专属课程、顶级黑客进行技术教学，依托长期积累，利用独有的技术人才优势，培养出具有顶级技术的网络安全实战型人才，为行业提供强有力的人才保障，提升支撑安全业务的各项能力，应对新形势下的网络安全挑战。

2021 年 12 月 16 日，由北京冬奥组委技术部组织，补天漏洞响应平台提供技术平台和运营支持的“冬奥网络安全卫士”招募启动，这是奥运史上首次以公开招募白帽子协助网络安全信息系统排查短板、挖掘相关漏洞以及收集网络安全情报信息等工作，经过层层选拔的冬奥网络安全卫士 24 小时在线，发起超过 2000 万次测试请求，测试总时长超过 1 万小时，成功发现了大量有效系统漏洞和冬奥相关威胁情报，为保障冬奥会网络安全发挥了巨大作用。对此，中央网信办冬奥会网络安全专家研判组组长、中国工程院院士方滨兴给予了高度肯定——“白帽子作为冬奥网络安全卫士的突出表现，也证明了白帽子群体是可信任的、可管理的，同时更是有能力的、有水平的。”

面对复杂多变的网络安全态势和层出不穷的攻击手段，补天平台采用 SRC、众测等方式服务广大企业，以安全众包的形式让白帽子从模拟攻击者的角度发现问题，解决问题，帮助企业树立动态、综合的防护理念，守护企业网络安全。补天平台将多种安全服务有机的整合起来，进一步提升企业的漏洞响应能力、积极防御能力和常态化安全运营能力。

截止 2024 年 8 月，平台注册白帽子已达 13.5 万余名，累计为 46.4 万家企业报告的漏洞超过 187 万个。补天漏洞响应平台先后被公安部、工信部、国家信息安全漏洞共享平台（CNVD）、国家信息安全漏洞库（CNNVD）分别评定为技术支持先进单位、漏洞信息报送突出贡献单位和一级技术支撑单位。

网聚安全力量，为社会提供准确、详实的漏洞情报，实现漏洞的及时发现与快速响应是补天平台始终坚持并不断履行的社会使命。通过营造实战化的学习环境、建设协同育人的导师制度、构建技能衔接的知识体系培养的实战化人才为企业网络安全贡献力量，为国家安全保驾护航。