中国实战化白帽人才能力白皮书

2021.1

补天漏洞响应平台 • 奇安信安服团队 • 奇安信行业安全研究中心

专家点评

红蓝对抗和实战化渗透，近年来受到越来越多企业的重视，也成为企业安全体系建设不可或缺的重要环节。尤其是每年的大型网络安全实战攻防演习更催生了行业对白帽子群体的关注和需求，也对白帽子能力提出了更高的要求。补天的实战化白帽能力白皮书是一个很好的行业尝试，可以作为白帽子群体能力发展的一个很好的参考，也可以为初学者答疑解惑，指明方向。

Tencent Blade Team 技术负责人 张博(cradmin)

补天平台作为国内最大的漏洞平台，拥有超过 7.4 万名白帽子，每年发放超过数千万漏洞奖金，收获数十万漏洞信息，基于这些数据和实践，补天平台对白帽子的等级、能力模型进行整理并发布本报告，报告中包含了不同等级白帽子所需要具备的能力、以及成长路径规划，对于即将成为白帽子或者希望可以成为更有实战化能力的白帽子来说非常具有参考价值。

字节跳动安全中心负责人 林伟

随着高级持续性威胁的增长，实战攻防技术的发展，传统的基于 OWASP TOP 10 以及 PTES 的渗透测试已经不再能满足各企事业单位对于网络防护能力、检测能力和响应能力的评估需求。因此网络安全检测应该与时俱进，将实战化的网络安全评估能力纳入到范畴当中，很欣喜能够看到补天作为国内影响力极高的漏洞响应平台能够在此做深入的思考和尝试，也将白帽子带到一个更高的实战能力水平上来。

京东安全攻防对抗组负责人 叶猛

这几年安全行业越来越成熟化，法律体系也在不断的完善，过了行业发展的野蛮期实战的机会变少了，实战性的人才也就跟着少了，大部分的白帽子都是通过“授权测试”和“打靶场”的方式获得有限的技术成长，再加上自动化工具越来越精细，白帽子变得“越来越懒”的同时也越来越迷茫，补天这一次从行业里开了一个好头，给更多想成为真正实战性人才的白帽子们，构建了一个更系统化的学习成长轨迹。

网络尖刀团队创始人 曲子龙

补天作为国内当下聚集白帽子最多的平台，对如此庞大的用户人群进行数据分析并制定相关标准是极具说服力的。该白皮书涵盖了白帽子年龄、学历、工作与否和年限，以及实战化能力的分级，因此对白帽级别的划分以及企业所需人才的分析便显得更具分量。真正是该行业下的企业、学习者以及感兴趣人群值得一看的内容。

ChaMd5 安全团队创始人 M

主要观点

- 白皮书结合补天漏洞响应平台白帽培养实践经验及奇安信集团安服团队蓝队攻防实战经验，首次提出了实战化白帽人才能力的基本概念，并系统性地给出了实战化白帽人才能力图谱。图谱为实战化白帽人才的系统性培养，以及白帽人才的自主学习，提供了重要的科学参考依据。
- 实战化白帽人才能力，是指在政企机构实际运行的业务系统、生产系统上进行的实战攻防演习过程中，作为攻击方的白帽子所需要具备各种攻防能力的集合。与传统的挖洞型白帽人才能力要求不同，实战化能力要求白帽子具备在真实的业务系统上，综合利用各种技术和非技术手段，进行动态实战攻防的能力。
- 白皮书将实战化白帽人才能力分为 3 个级别、14 大类、85 项具体技能。其中，基础能力 2 类 20 项、进阶能力 4 类 23 项、高阶能力 8 类 42 项。
- 补天漏洞响应平台针对具有实战攻防演习经验的 645 位高级白帽子的调研显示：目前国内白帽子人群所掌握的实战化攻防能力，仍主要集中在基础能力方面；而具备高阶能力的白帽人才则十分稀缺，特别是不同平台程序的分析能力、在系统层漏洞的挖掘与利用，以及相应的 PoC 或 EXP 的编写等方面，相关人才更是凤毛麟角。

摘　要

- 从行业分布来看，36.3%的白帽子来自于安全企业，34.9%的白帽子仍是学生，7.1%的白帽子来自政府机构事业单位。
- 从年龄分布来看，近半数的白帽子年龄在 22 岁及以下；35.7%的白帽子年龄在 23-27 岁。从学历来看，本科及以下学历超过 9 成。其中，本科学历占比 36.3%，本科在读占比 21.9%，还有 24.5%的白帽子为大专学历。
- 从从业时间来看，进入安全行业 1-3 年的白帽子最多，占比 51.2%；其次为拥有 4-6 年安全从业经验的白帽子，占比 21.2%。
- 本次调研显示，55.8%的白帽子目前仍然处于“无证上岗”的状态。
- 2020 年实战化白帽人才基础能力中，平均每个白帽子掌握 4 个 Web 漏洞利用方式；会使用 6 个安全工具。
- 2020 年实战化白帽人才进阶能力中，平均每个白帽子掌握 3 个 Web 漏洞的挖掘能力，能够使用 2 种编程语言对 Web 开发和编程，更擅长使用社工库与鱼叉邮件进行社工钓鱼。
- 2020 年实战化白帽人才高阶能力较弱，系统层漏洞利用与防护、系统层漏洞挖掘以及对不同系统编写 PoC 或 EXP 等高级利用能力掌握不够，相比之下，多数白帽子身份隐藏与内网渗透能力掌握较好。约 74.0%的白帽子具有组队参加有关部门组织的实战攻防演习活动的经验，19.4%的白帽子表示自己能够胜任团队协作中的任意角色。

关键字：实战化、白帽子、攻防演习、能力图谱、漏洞挖掘、社工钓鱼、内网渗透

目　　录

研究背景

白帽子，在很多人心中的印象就是挖洞高手。但随着网络安全实践工作的持续深入发展，白帽子已经成为了各项网络安全工作中不可或缺的关键要素。特别是近年来持续深入开展的网络安全实战攻防演习工作，对作为蓝队核心的白帽子，提出了越来越高的实战化能力要求。要求白帽子具备在实战对抗环境和实际业务环境中，实现有效的攻击的能力，并能够由此发现目标机构存在的安全问题或安全隐患。

实战化，对白帽子能力的要求更高，也更全面。一方面，对于具备实战化运行能力的大型政企机构来说，很多低级的安全漏洞早已修复，想要实现有效攻击，就必须具备发现某些高级安全漏洞的能力；另一方面，单纯知道某个漏洞的存在也不等于能够实现有效的攻击，白帽子还必须具备在实战化的业务环境下，实现漏洞有效利用的能力，这就要求白帽子具有社工能力、协作能力、业务分析能力等多种安全能力。

从实际工作需要出发，我们发现，目前国内白帽子的实战化能力还很不全面，存在诸多短板。绝大多数白帽子的能力集中于 Web 漏洞的挖掘与利用这样的初级或中级能力，而对于系统层漏洞挖掘、CPU 指令集、编写 POC 或 EXP 等中高级能力，则存在明显的人才缺失。

为提升国内白帽子群体的整体能力水平，适应日益重要的攻防演习实战需求，补天漏洞响应平台联合奇安信安服团队和奇安信行业安全研究中心，结合 1900 余个目标系统的攻防实战经验，首次系统性地总结了“实战化白帽子能力需求图谱”，并据此针对补天平台选取了 645 名白帽子进行了能力调研，形成了《中国实战化白帽人才能力白皮书》。在接受本次调研的白帽子中，约 74.0%的白帽子参加过有关部门组织的实战攻防演习活动。

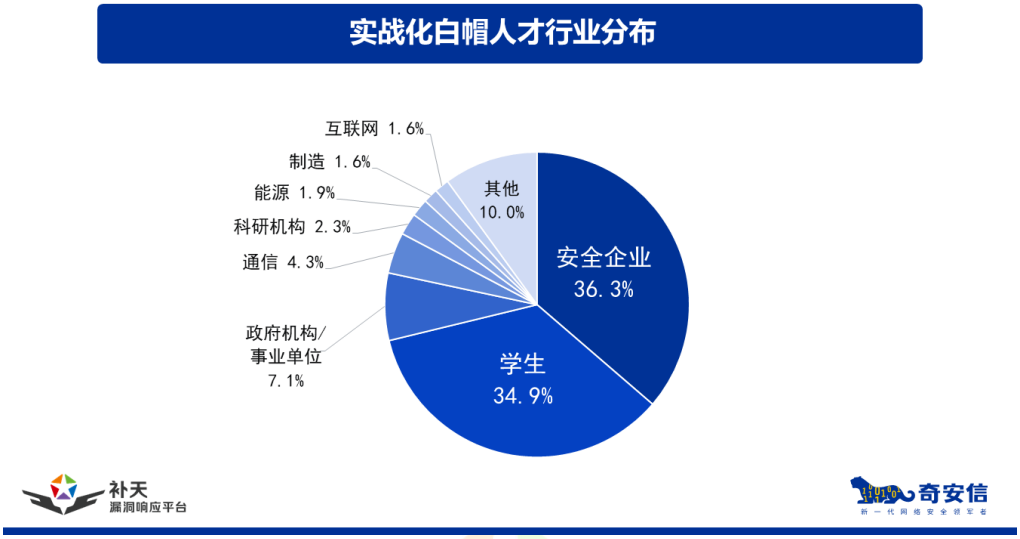
希望此项研究成果能够对安全行业的实战化白帽子人才发展及能力培养有所帮助。

第一章　中国白帽人才基本情况

在实战化白帽子能力调研过程中，课题组同时也对白帽子的一些基本状况进行了调研，包括行业分布、年龄与学历、从业时间、以及技能证书等几个方面。

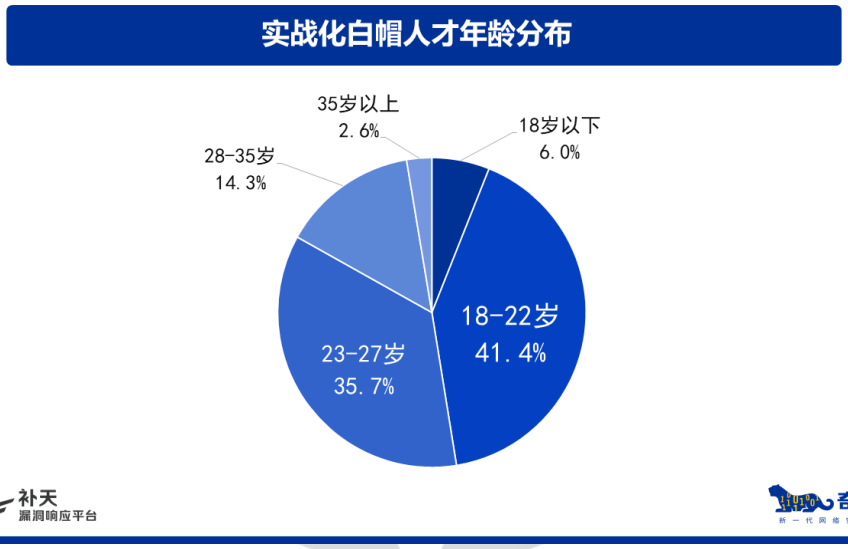
一、　行业分布

从行业分布来看，36.3%的白帽子来自于安全企业，34.9%的白帽子仍是学生，7.1%的白帽子来自政府机构事业单位。可见，白帽子由于其所需技能及时间耗费，更多集中在专业对口的安全企业从业者或精力充沛的学生党。

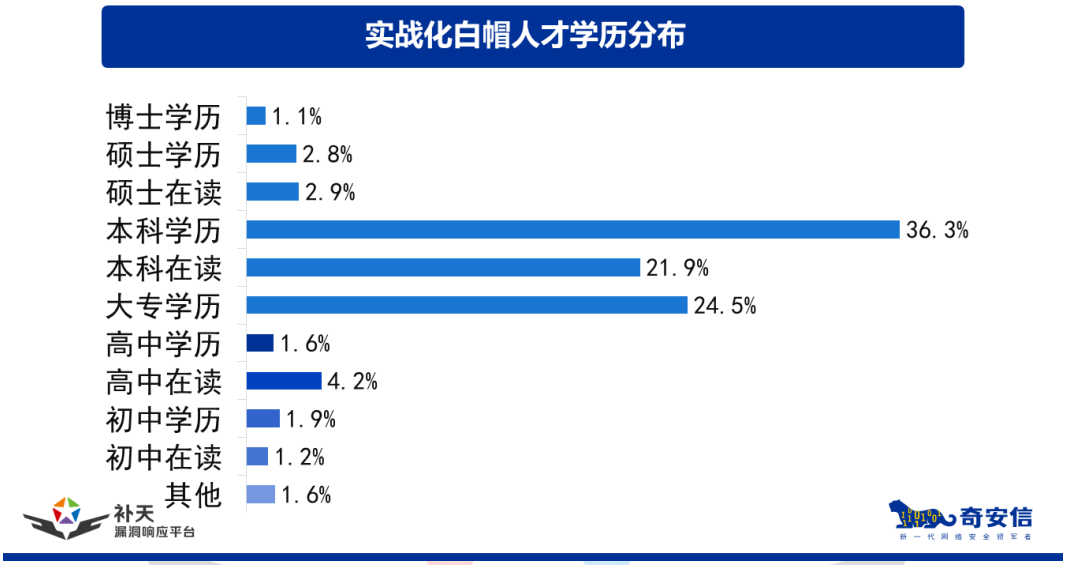


二、　年龄与学历

从年龄分布来看，近半数的白帽子年龄在22岁及以下；35.7%的白帽子年龄在23-27岁。



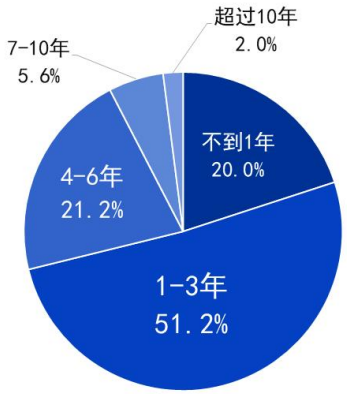
从学历来看，本科及以下学历超过 9 成。其中，本科学历占比 36.3%，本科在读占比 21.9%，还有 24.5%的白帽子为大专学历。



三、 从业时长

由于白帽子需要有一定安全基础，需要花费时间学习和锻炼才能成为真正的白帽子。从从业时间来看，进入安全行业 1-3 年的白帽子最多，占比 51.2%；其次为拥有 4-6 年安全从业经验的白帽子，占 21.2%，具体分布如下图所示。

实战化白帽人才从业时长

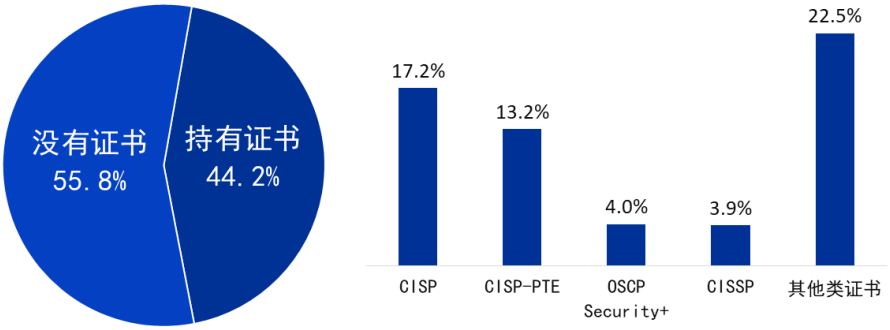


补天 漏洞响应平台
奇安信 新一代网络安全领军者

四、 技能证书

技能证书可以在一定程度上体现网络安全工作者的技能水平，对求职和就业有很大的帮助。因此，很多网络安全从业者都会考取 CISP、CISP-PTE、CISSP、OSCP Security+等专业技能证书。不过，本次调研显示，55.8%的白帽子目前仍然处于“无证上岗”的状态。

实战化白帽人才技能证书持有情况



补天 漏洞响应平台

注：一位白帽子会持有多种证书

奇安信 新一代网络安全领军者

第二章　实战化白帽人才能力需求

本章主要介绍实战化白帽人才能力的基本概念及其与传统白帽能力的区别，给出能力分级和分类的依据，并最终给出本白皮书整理的完整能力图谱。

一、　实战化能力与传统能力的区别

实战化白帽人才能力，是指在政企机构实际运行的业务系统、生产系统上进行的实战攻防演习过程中，作为攻击方的白帽子所需要具备各种攻防能力的集合。由于实战攻防演习是对真实黑客攻防过程进行模拟和再现，因此也要求白帽子在攻击过程中所使用的战术手法能够达到、甚至超过黑产组织或 APT 组织的攻击水平。与传统的挖洞型白帽人才能力要求不同，实战化能力要求白帽子具备在真实的业务系统上，综合利用各种技术和非技术手段，进行动态实战攻防的能力。

具体来说，主要有以下几个方面特点：

1）针对业务系统，而非 IT 系统

传统的或一般的白帽子挖洞工作，主要都是针对各类 IT 信息系统本身或系统中的设备、协议等，如各类 Web 系统、操作系统、PC 终端、IoT 设备、工控设备协议、区块链协议等等。而实战攻防演习工作的核心目标，是发现和解决由网络安全问题引发的业务安全及生产安全问题，攻击过程也是针对实际运行中的业务系统或生产设备。

此外，传统的挖洞工作主要关注的是对单一系统的单点突破，实战攻防演习更多关注的则是多个系统并存的复杂体系，关注的是复杂体系在运行、管理过程中存在的安全隐患。对于多数大中型政企机构来说，内部存在几十个，甚至上百个不同的信息化系统的情况是非常普遍的。

2）挖洞只是辅助，攻击必须有效

单纯的挖洞工作，一般只需证明漏洞的存在，提交漏洞报告即可。但在实战化的业务环境中，存在漏洞不等于能够实现有效的攻击。一方面，这是因为漏洞的实际触发可能依赖于诸多条件，这些条件在实际的业务环境中未必存在；另一方面，即便漏洞是有效的，但如果攻击者只能实现单点突破，而无法达到预设的最终目标，同样不能完成有效的攻击。

3）攻击是个过程，允许社工方法

对单一漏洞进行挖掘和利用，往往只能实现某个局部的技术目标。但事实上，在绝大多数的实战攻防演习过程中，攻击方需要连续突破多个外围系统或关联系统，才能最终达到计划中的攻击目标。也就是说，攻击者需要掌握一系列的漏洞，并能够对机构内部的 IT 架构、运行管理机制进行有效分析，才有可能找到有效的攻击路径，实现实战攻防演习环境下的有效攻击。事实上，在实战攻防演习过程中，攻击方可能需要连续数日，多人协作才能完成一整套攻击。

此外，一般的漏洞挖掘或渗透测试，是不允许使用社会工程学方法的。但在实战化环境下，社会工程学是必不可少的攻击手法，因为真实的攻击者一定会使用这项技能。事实上，以人为突破口，往往是实战攻防演习中攻击队的优先选择。

4） 动态攻防环境，有人运行值守

单纯的漏洞挖掘工作一般不需要考虑攻防过程，也就是不需要考虑防守方的参与。但在实战攻防演习过程，防守方实际上是有专业团队在进行安全运行维护和 24 小时值守工作的。攻击方一旦开始行动，就有可能被防守方发觉。而防守方一旦发现入侵行为，也会采取各种反制措施、诱捕行动，以及攻击溯源。所以，实战化能力就要求白帽子必须掌握一定的身份隐藏技能，诸如匿名网络、免杀技术、权限维持等各种安全对抗技术。

二、 实战化能力的分级与分类依据

实战化白帽人才能力可以依据不同的能力级别和技能类型进行划分。在本白皮书中，我们主要是综合考虑了掌握技能的难易程度、市场人才的稀缺程度，以及实战化能力的有效性这三个方面的因素，将白帽子的实战化能力从低到高依次划分为基础能力、进阶能力和高阶能力。

1） 掌握技能的难易程度

不同的能力，学习和掌握的难易程度也不同。而技能的难易程度是能力定级的首要因素。例如，Web 漏洞利用就相对容易，而 Web 漏洞挖掘就要困难一些，系统层漏洞的挖掘则更为困难。所以，这三种能力也就分别依次被列入了基础能力、进阶能力和高阶能力。

2） 市场人才的稀缺程度

人才的稀缺程度，也是能力定级的重要参考因素。例如，在所有白帽子中，掌握系统层漏洞利用的人平均来说只有 1 成左右；在 iOS 系统中，会编写 POC 或 EXP 的白帽子，也相对少见。因此，这些能力就被归入了高阶能力。

3） 实战化能力的有效性

总体而言，越是相对高阶的能力，防守方越难以防御和发现，其在实战攻防演习过程中发挥实效的几率也就越大。

接下来说分类问题。从不同的视角出发，我们可以对实战化能力进行不同的分类。而本白皮书所采用分类方法，主要考虑了以下几个方面的因素：

1） 只针对实战化过程中，最主要、最实用的能力进行分类，边缘技能暂未列入分类；
2） 不同的能力分类之间，尽量相互不交叉；
3） 分类与分级兼顾，同一领域的不同能力，如果分级不同，则作为不同的分类；
4） 将挖掘、利用、开发、分析等能力作为不同的技能来分类。比如，同样是 Web 系统，漏洞利用、漏洞挖掘、开发与编程，都是不同的能力分类。

三、 实战化白帽人才能力需求图谱

以前述分级与分类原则为基础，本白皮书将实战化白帽人才能力分为 3 个级别、14 大类、85 项具体技能。其中，基础能力 2 类 20 项，进阶能力 4 类 23 项，高阶能力 8 类 42 项。下图是汇集了上述所有信息的 2020 年实战化白帽人才能力图谱。

关于图中各项基本技能的具体含义，详见本白皮书附录 1：实战化白帽人才能力各项技能详解。

（一）基础能力

基础能力主要包括 Web 漏洞利用与基础安全工具使用两类。

1） Web 漏洞利用

主要包括命令执行、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、文件上传与权限绕过等漏洞。

2） 基础安全工具使用

主要包括 Burp Suite、Sqlmap、AppScan、AWVS、Nmap、Wireshark、MSF、Cobalt Strike 等安全工具。

（二）进阶能力

进阶能力主要包括 Web 漏洞挖掘、Web 开发与编程、编写 PoC 或 EXP 等利用、社工钓鱼四类。

1） Web 漏洞挖掘

主要包括命令执行、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、文件上传与权限绕过等漏洞。

2） Web 开发与编程

主要包括 Java、PHP、Python、C/C++、Golang 等编程语言的使用。

3） 编写 PoC 或 EXP 等利用

主要包括针对 Web 漏洞、智能硬件/IoT 漏洞等系统环境的漏洞编写 PoC 或者 EXP。

4） 社工钓鱼

主要包括开源情报收集、社工库收集、社交钓鱼和鱼叉邮件等几类社工钓鱼技能。

（三）高阶能力

高阶能力主要包括系统层漏洞利用与防护、系统层漏洞挖掘、身份隐藏、内网渗透、掌握 CPU 指令集、高级安全工具、编写 PoC 或 EXP 等高级利用、团队协作八大类。

1） 系统层漏洞利用与防护

主要包括 SafeSEH、DEP、PIE、NX、ASLR、SEHOP、GS 等。

2） 系统层漏洞挖掘

主要包括代码跟踪、动态调试、Fuzzing 技术、补丁对比、软件逆向静态分析、系统安全机制分析等。

3） 身份隐藏

主要包括匿名网络（如 Tor）、盗取他人 ID/账号、使用跳板机、他人身份冒用几类身份隐藏技能。

4） 内网渗透

主要包括工作组与域环境渗透方法、横向移动、内网权限维持/提权、数据窃取、免杀等方法。

5） 掌握 CPU 指令集

主要包括 x86、MIPS、ARM、PowerPC 等指令集。

6） 高级安全工具

主要包括 IDA、Ghidra、binwalk、OllyDbg、Peach fuzzer 等高级安全工具；编写 PoC 或 EXP 等高级利用包括：Android、iOS、Linux、macOS、网络安全设备等系统的编写。

7） 编写 PoC 或 EXP 等高级利用

主要包括在 Android、iOS、Linux、macOS、网络安全设备等操作系统上找到漏洞并编写 PoC 或 EXP 的能力。

8） 团队协作

主要包括行动总指挥、情报收集、武器装备制造、打点实施、社工钓鱼、内网渗透等。

第三章　中国白帽人才能力现状

2020 年 11-12 月，我们邀请了补天漏洞响应平台上 645 名白帽子进行了一次“中国白帽人才能力现状”调研。但受到当时条件限制，部分类型数据没能调研完整，文中标记为“暂无数据”。我们会在后续的持续调研过程中逐步补全所有数据。

一、　基础技能

（一） Web 漏洞利用

实战化白帽人才对不同类型 Web 漏洞利用的掌握情况如表 1 所示。

表1　　2020 年实战化白帽子 Web 漏洞利用能力的掌握情况

漏洞类型	掌握该技能的白帽子占比
命令执行	48.4%
代码执行	41.7%
解析漏洞	暂无数据
XSS	62.2%
弱口令	暂无数据
文件上传	暂无数据
SQL 注入	73.0%
逻辑漏洞	暂无数据
信息泄露	60.3%
配置错误	暂无数据
反序列化	暂无数据
权限绕过	56.1%

（二） 基础安全工具

实战化白帽人才对基础安全工具的掌握情况如表 2 所示。

表2　　2020 年实战化白帽子基础安全工具的掌握情况

基础安全工具	掌握该技能的白帽子占比
Burp Suite	95.2%
AppScan	58.8%
Nmap	88.5%
Wireshark	66.8%
Sqlmap	91.3%
AWVS	73.3%

MSF	68.4%
Cobalt Strike	53.5%

二、 进阶能力

（一） Web 漏洞挖掘

针对不同漏洞的 Web 漏洞挖掘能力掌握情况如表 3 所示。

表3 2020 年实战化白帽子 Web 漏洞挖掘能力的掌握情况

漏洞类型	掌握该技能的白帽子占比
命令执行	33.9%
代码执行	29.2%
解析漏洞	暂无数据
XSS	43.5%
弱口令	暂无数据
文件上传	暂无数据
SQL 注入	51.1%
逻辑漏洞	暂无数据
信息泄露	42.2%
配置错误	暂无数据
反序列化	暂无数据
权限绕过	39.3%

（二） Web 开发与编程

针对不同开发语言环境下的 Web 开发与编程，实战化白帽人才掌握情况如表 4 所示。

表4 2020 年实战化白帽子 Web 开发与编程能力的掌握情况

Web 开发与编程	掌握该技能的白帽子占比
Java	27.1%
PHP	44.2%
Python	66.5%
C/C++	21.7%
Golang	11.2%
熟悉语言但不会开发	32.3%
其他	7.0%

（三） 编写 PoC 或 EXP 等利用

在进阶能力中，PoC 或 EXP 等利用主要针对的是 Web 漏洞、智能硬件/IoT 漏洞等系统环境等。但受到调研条件限制，针对上述相关项目，暂无数据。

（四） 社工钓鱼

社工钓鱼主要为以下四大类，实战化白帽人才对社工钓鱼方法的掌握情况如表 4 所示。

表5 2020 年实战化白帽子社工钓鱼能力的掌握情况

社工钓鱼	掌握该技能的白帽子占比
开源情报收集	39.2%
社工库收集	69.9%
鱼叉邮件	60.9%
社交钓鱼	25.0%
其他	3.0%
都没用过	18.1%

三、 高阶能力

（一） 系统层漏洞利用与防护

针对系统层漏洞的利用与防护，实战化白帽人才对不同系统层安全机制的掌握情况如表 6 所示。

表6 2020 年实战化白帽子系统层漏洞利用与防护能力的掌握情况

基础安全工具	掌握该技能的白帽子占比
SafeSEH	16.6%
DEP	15.4%
PIE	13.8%
NX	13.2%
ASLR	13.8%
SEHOP	8.5%
GS	11.2%
都没用过	64.0%
其他	5.3%

（二） 系统层漏洞挖掘

针对系统层漏洞挖掘，实战化白帽人才对不同漏洞挖掘技能的掌握情况如下表 7 所示。

表7 2020 年实战化白帽子系统层漏洞挖掘能力的掌握情况

漏洞挖掘技能	掌握该技能的白帽子占比
代码跟踪	29.5%
动态调试	27.1%
Fuzzing 技术	37.8%

补丁对比	14.7%
软件逆向静态分析	24.2%
系统安全机制分析	暂无数据
都不擅长	35.0%
其他	3.9%

（三） 身份隐藏

实战化白帽人才对身份隐藏方法的掌握情况如表 8 所示。

表8　2020 年实战化白帽子身份隐藏能力的掌握

身份隐藏方法	掌握该技能的白帽子占比
匿名链路（如 Tor）	66.8%
盗取他人 ID/账号	26.2%
使用跳板机	51.4%
他人身份冒用	33.3%
都没用过	17.4%
其他	2.5%

（四） 内网渗透

实战化白帽人才对内网渗透的方法掌握情况如表 9 所示。

表9　2020 年实战化白帽子内网渗透能力的掌握

内网渗透方法	掌握该技能的白帽子占比
工作组、域环境渗透	72.6%
内网权限维持/提权	74.0%
横向移动	55.0%
数据窃取	44.2%
免杀	52.9%
都没用过	10.7%
其他	2.3%

（五） 掌握 CPU 指令集

实战化白帽人才对不同 CPU 指令集的掌握情况如表 10 所示。

表10　2020 年实战化白帽子 CPU 指令集的掌握

CPU 指令集	掌握该技能的白帽子占比
x86	39.4%
MIPS	5.4%
ARM	14.1%
Alpha	7.0%
其他	4.7%

都不会	50.9%

（六） 高级安全工具

白帽人才对高级安全工具的掌握情况如表 11 所示。

表11　2020 年实战化白帽子高级安全工具的掌握

高级安全工具	掌握该技能的白帽子占比
IDA	36.7%
Ghidra	9.8%
Binwalk	31.0%
OllyDbg	27.9%
Peach fuzzer	14.0%

（七） 编写 PoC 或 EXP 等高级利用

实战化白帽人才在不同系统下的编写 PoC 或 EXP 等高级利用掌握情况如表 12 所示。

表12　2020 年实战化白帽子编写 PoC 或 EXP 等高级利用的掌握

操作系统	掌握该技能的白帽子占比
Android	14.7%
iOS	5.0%
Linux	12.9%
macOS	3.1%
网络安全设备	19.0%
都不会	11.3%

（八） 团队协作与角色

在接受本次调研的 645 名白帽子中，约 74.0%的白帽子具有组队参加有关部门组织的实战攻防演习活动的经验，19.4%的白帽子表示自己能够胜任团队协作中的任意角色。在团队协作中，有过各种角色实战经验的白帽子占比如表 13 所示。

表13　2020 年实战化白帽子在团队协作中担任过的角色分布情况

团队协作中的角色	有相关角色实战经验的白帽子占比
行动总指挥	24.3%
情报收集	43.0%
武器装备制造（漏洞挖掘、工具开发）	23.1%
打点实施（获取接入点、Web 渗透等）	55.2%
社工钓鱼	25.0%
内网渗透	26.7%
其他	4.7%

四、 总结

下图是汇集了上述所有信息的，2020 年实战化白帽人才能力现状。

附录 1 实战化白帽人才能力各项技能详解

一、 基础能力

（一） Web 漏洞利用

利用 Web 系统或软件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、代码执行、解析漏洞、XSS、弱口令、文件上传、SQL 注入、逻辑漏洞、信息泄露、配置错误、反序列化、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） 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。

3） 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。

4） 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。

5） 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。

6） 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。

7） 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。

8） 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。

9） 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。

10）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。

11）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。

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） 基础安全工具

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） 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。

3） 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。

4） 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。

5） 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。

6） 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。

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

二、 进阶能力

（一） Web 漏洞挖掘

针对 Web 系统或软件的进行漏洞挖掘的能力。

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、代码执行、解析漏洞、XSS、弱口令、文件上传、SQL 注入、逻辑漏洞、信息泄露、配置错误、反序列化、权限绕过等。关于这些漏洞类型的具体含义，参见前述“基础能力”中的“（一）Web 漏洞利用”，这里不再累述。

（二） 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。

（三） 编写 PoC 或 EXP 等利用

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。

（四） 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四种：开源情报收集、社工库收集、鱼叉邮件和社工钓鱼。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） 开源情报收集

开源情报收集能力，是指在公开的互联网信息平台上，合法收集针对目标机构的关键情报信息的能力。例如，新闻媒体、技术社区、企业官网、客户资源平台等公开信息分享平台都是开源情报收集的重要渠道。白帽子可以通过开源情报收集，获取诸如企业员工内部邮箱、联系方式、企业架构、供应链名录、产品代码等关键情报信息。这些信息都可以为进一步的攻击提供支撑。

开源情报收集是白帽子首要的情报收集方式，其关键在于要从海量网络信息中，找到并筛选出有价值的情报信息组合。通常情况下，单一渠道公开的机构信息，大多没有什么敏感性和保密性。但如果将不同渠道的多源信息组合起来，就能够形成非常有价值的情报信息。当然，也不排除某些机构会不慎将内部敏感信息泄露在了互联网平台上。白帽子在互联网平台上直接找到机构内部开发代码，找到账号密码本的情况也并不少见。

2） 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。

3） 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。

4） 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。

社工钓鱼，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。

三、 高阶能力

（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。本小节总结了实战攻防演习中，最为实用、也是最为常用的 7 种典型的系统层安全机制。

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） 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。

（四） 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、横向移动、数据窃取和免杀等。

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） 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。

3） 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。

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。

（五） 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。

（六） 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。

（七） 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包括：Android、iOS、Linux、macOS。

1） 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。

2） 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。

3） 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。

4） 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。

5） 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。

（八） 团队协作

随着实战攻防演习实践的不断深入，防守方的整体能力持续提升。这就使得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 6 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、社工钓鱼人员和内网渗透人员。

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。

附录 2 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。

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。

2019 年 5 月，基于补天众测的漏洞治理与风险管理平台入选工业和信息化部公布网络安全技术应用试点示范项目名单，在网络安全漏洞领域唯一以安全厂商身份入选。作为奇安信集团独立开发运营的 SaaS 平台，通过标准化的工作流程驱动企业高效处置精英可信白帽发现的漏洞。持续生产和运营的安全风险线索能保障用户及时、精准的获知和处置。本平台聚焦为企业解决漏洞发现不全面、漏洞修复不彻底的难题以及威胁无法提前预知和防范的风险管理问题，帮助企业完善漏洞治理架构和风险管理机制，助力企业构建管理闭环、关口前移、源头治理的积极防御体系。

成立 7 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。

截至 2021 年 1 月，平台注册白帽子已达 74 000 余名，累计为 16 万多家企业报告的漏洞超过 57 万个。补天漏洞响应平台先后被公安部、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。

附录 3 奇安信蓝队能力及攻防实践

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

仅 2020 年全年，奇安信就参与了全国范围内 244 场实战攻防演习的蓝队活动，攻破了 1900 余个目标系统。累计派出蓝队 306 支次、投入蓝队专家 918 人次、投入工作量 6685 人天。项目涵盖党政机关、公安机关等机构，以及民生、医疗、教育、金融、交通、电力、银行、保险、能源、传媒、生态、水利、旅游等各个行业。在实战演习过程中，奇安信集团派遣最优秀的蓝队高手全力参与工作，并在所有行业化的实战攻防演习排名中名列前茅，其中排名第一的次数高达 66.7%。

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

如今，奇安信集团已组建起 10 余支技术高强、能力突出的网络蓝队，聘请具备 APT 高级渗透实战经验的专职攻防专家 100 余人，是目前国内规模最大、人数最多的蓝队队伍之一。

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

合作伙伴

感谢以上合作伙伴对本报告的支持，合作伙伴排序均按首字母排序，排名不分先后