附件1

“护网 2022”网络安全攻防实战演习评分规则

一、攻击方评分规则

序号	类型	赋值规则	备注
（一）获取权限：得分上限的对象是单个防守单位及其所有下属机构			
1	获取参演单位的域名控制权限	一级域名 100 分，二级域名 50 分	根据域名类型给分，单个防守方单位（含所有下属机构）得分上限为 500 分。影响特别重大成果的由指挥部研判后给分
2	获取 PC 终端、移动终端权限（手机、Pad）	PC 终端:20 分/台 移动终端:50 分/台	得分上限为 500 分。其中 PC 终端，应为 system 或 root 权限。
3	获取邮箱权限	邮箱账号口令：20 分/个	得分上限为 200 分。使用默认密码猜解账户成功的只给一次分（公共自主注册邮箱不给分）。
		系统管理员权限：500 分-1000 分	获取自建、在用的邮件系统管理员权限，可以查看、获取全量邮件内容。得分上限为 1000 分。特别重大战果由指挥部研判后给分。
4	获取办公化自动化系统权限	200 分-500 分	获取全局性自建、在用的 OA、即时通讯、项目管理、财务等系统管理员权限，可以查看、获取大量信息。得分上限为 1000 分。特别重大战果由指挥部研判后给分。

5	获取身份、账户管理平台权限（SSO,4A）	系统管理员权限 300 分，能登入的系统 100 分/个	同一系统的同等权限（包括管理员）只得一次分。得分上限为 1000 分。
6	获取域控系统权限	系统管理员权限 200 分，域内可控服务器 10 分/台	得分上限为 4000 分，特别重大成果的由指挥部研判后给分
7	获取堡垒机、运维机权限	系统管理员权限 200 分，托管的服务器 10 分/台	
8	获取云管理平台控制权	系统管理员权限 200 分，云上主机 10 分/台	单个云平台得分不超过 2000 分，得分上限为 4000 分。特别重大成果的由指挥部研判后给分
9	获取大数据系统权限	/	按数据量和重要程度给分，得分上限 3000 分。特别重大成果的由指挥部研判后给分
10	获取数据库连接账号密码（含 SQL 注入）	普通用户权限 50 分，管理员权限 100 分。	同一系统的同等权限（包括管理员）只得一次分。得分上限为 1000 分，特别重大战果由指挥部研判后给分。
11	获取网络设备权限	依据最终成果倒溯给分，如和核心目标同网段，300 分。以路由器为例，小型 50 分，中型 150 分，大型 300 分。	包括防火墙、路由器、交换机、网闸、光闸、摆渡机、VPN 等。需提供路由表等证据或连接数量截图。得分上限为 2000 分，特别重大战果由指挥部研判后给分。
12	获取工业互联网系统权限	/	包括车联网、智能制造、远程诊断、智能交通等，根据系统重要程度由指挥部研判后给分。
13	获取物联网设备管控平台权限	带控制功能的物联网平台 200 分，按照平台上连接的点数计算 5 分/台	得分上限为 1000 分，特别重大战果由指挥部研判后给分。

14	获取安全设备权限	普通用户权限 50 分，管理员权限 200 分	包括 IDS、审计设备、WAF 等安全设备控制权限（含分布式部署系统的管理后台）。得分上限为 1000 分，特别重大战果由指挥部研判后给分。
15	获取一般 Web 应用系统、FTP 等应用权限	普通用户权限 20 分，系统管理员权限 100 分。	同一系统的同等权限（包括管理员）只得一次分，使用默认密码猜解账户成功的只给一次分（公共自主注册 web 系统不给分）。与服务器主机权限不可兼得。得分上限为 2000 分，特别重大战果由指挥部研判后给分。
16	获取服务器主机权限（含 webshell 权限）	普通用户权限 50 分，管理员权限 100 分。	虚拟主机、Docker 容器等视同主机。通过多网卡进入新网络区域的，按照进入的网络类型给分。与其他应用系统权限不可兼得。
17	获取其他系统、服务器、设备等权限	/	由指挥部参照演习目标系统给分
（二）突破网络边界：突破同一类网络边界只给一次分，一个单位上限是 8000 分			
18	进入逻辑隔离业务内网	1000 分	提供详实确凿的证明材料（如防火墙、vpn、多网卡主机、网络设备的控制截图，能访问内网的截图证明等） DMZ 区、办公内网视为互联网区。
19	进入逻辑强隔离业务内网	2000 分	提供详实确凿的证明材料（如网闸类隔离设备的控制截图，能访问的截图证明等）

20	进入核心生产网（如铁路调度专网、银行核心账务网、电力生产控制大区、运营商信令网、能源生产物联网等）	5000 分	提供详实确凿的证明材料（如防火墙、vpn、多网卡主机、网络设备的控制截图，能访问内网的截图证明等）
21	其他情况	/	根据各单位内部网络实际情况，由指挥部核定给分
（三）获取目标系统权限			
22	互联网区	5000 分/个	如果获取互联网区目标系统外的其他重要业务系统权限，能够影响全行业或某一地区重大业务开展，且报告逻辑清晰，条理清楚，视同目标系统给分，最高 4000 分。
23	业务内网	7000 分/个	如果获取业务内网区目标系统外的其他重要业务系统权限，能够影响全行业或某一地区重大业务开展，且报告逻辑清晰，条理清楚，视同目标系统给分，最高 6000 分。
24	核心生产网（如铁路调度专网、银行核心账务网、电力生产控制大区、运营商信令网、能源生产物联网等）	10000 分/个	如果获取核心生产网区目标系统外的其他重要业务系统权限，能够影响全行业或某一地区重大业务开展，且报告逻辑清晰，条理清楚，视同目标系统给分，最高 9000 分。
25	其他情况	/	由指挥部核定给分
（四）发现演习前已有攻击事件（需提交独立分析报告）			
26	发现已植入的 webshell 木马、主机木马	100-500 分/个主机，根据木马发现的网络重要性给分。	提供包含确凿证据的详细分析报告（创建时间、功能分析、访问日志、上传的

			工具武器、攻击行为记录等），由指挥部研判后给分。
27	发现黑客利用破解的密码登录主机系统	100-500 分/个主机，根据登录主机的网络重要性给分。	提供包含确凿证据的详细分析报告（创建时间、访问日志、上传的工具武器、攻击行为记录等），由指挥部研判后给分。
28	发现主机异常新增账号	100-500 分/个主机，根据主机的网络重要性给分。	提供包含确凿证据的详细分析报告（创建时间、访问日志、上传的工具武器、攻击行为记录等），由指挥部研判后给分。
29	发现隐蔽控制通道（发现了跳板类软件：端口转发、代理程序等）	100-500 分/个主机，根据隐蔽控制通道的重要性给分。	提供包含确凿证据的详细分析报告（创建时间、功能分析、访问日志、上传的工具武器、攻击行为记录等）由指挥部研判后给分。
30	发现其他系统被控制的线索情况	/	由指挥部核定给分
（五）漏洞发现			
31	提交 0-Day 或未被正式公开 N-Day 漏洞	0-10000 分	（1）根据漏洞对重要行业和关键信息基础设施的重要程度给分，如影响范围、网络位置、可获取的权限等。分为高中低三挡，高 5000-10000，中 2000-6000，低 0-3000，指挥部根据具体情况研判给分，详见漏洞加分表。 （2）必须在演习期间使用该漏洞进行攻击操作
（六）沙盘推演支撑			

32	攻击方案被采纳作为主方案	7000 分	按照沙盘推演行业和场次累计计算。指挥部统一评判。
33	参与沙盘推演，但未被采纳为主方案	5000 分	
二、减分规则			
（一）提交成果不完整			
1	未完整上报攻击成果，没有提交漏洞截图或详情，普通成果缺乏完整链条，重大成果缺乏关键环节。	指挥部有权驳回、减分或不给分，直至补充完整	
（二）被防守方溯源			
2	被防守方溯源到攻击队员、攻击资源	减 3000 分	1.攻击队员或公司被溯源，减 3000 分 2.以攻击队员或公司被溯源为前提，攻击溯源（如攻击主机、web 系统等）被控，减 500 分/个
（三）违反演习规则制度：违规行为记入个人和队伍档案，并根据违规行为的严重程度，进行分级处理，包括扣分、公开通报、终止个人或队伍本次资格、个人或单位加入黑名单，行业禁入。			

二、防守方评分规则

一、加分规则
1.防守方的扣分是多支攻击队从该防守方获取的成果总分。
2.防守方加分包括：基础得分与附加分。
3.基础得分是根据防守方提交的成果报告逐一打分后累加的总得分，每个报告对应一起攻击事件的处置，分别从监测发现、分析研判、应急处置、通报预警、协同联动、追踪溯源 6 方面打分，具体公式为：该起攻击事件被扣分数×各评分点实际得分（百分比）×80%。注：基础得分的上限是攻击方战果得分的 80%。
4.防守方提交的每一份报告围绕一起攻击事件编写，只有属于演习范畴的安全事件（属于已认定的攻击方战果）方可得分，同一起事件不允许出现在多份报告中。
5.附加分上限为 3000 分，所有防守方单位都可以提交。
6.防守方提交的报告数量上限为 50 个。
7.报告要有逻辑性，要提供确凿证据的文字描述和日志、设备界面截图等。
8.本次演习设计了“防护值”公式：（1）防守方被扣分情况下：防护值=（基础得分÷扣分+附加分÷3000×0.2）×10000；（2）防守方未扣分情况下：防护值=（0.8+附加分÷3000×0.2）×10000。

序号	评分点	具体评分点	评价具体指标
1	监测发现（25%）	及时性（防守方自证，5%）	提交攻击时间、发现时间等
2		采用工具或手段（3%）	提交监测发现使用的工具或手段包括但不限于：安全设备、态势感知平台、流量分析等
3		覆盖率（结束的时候算总的覆盖率，9%）	防守方发现的被控 IP（填写被控 IP 地址、URL、被攻击单位名称等），占各攻击队控制其 IP 的总数
4		有效性（是否能够发现攻击方有效攻击手段，8%）	18 种攻击方有效攻击手段： ①互联网侧信息收集

			②涉“重点人”敏感信息收集 ③供应链信息收集 ④应用层漏洞利用 ⑤系统层漏洞利用 ⑥钓鱼邮件攻击 ⑦社工欺骗利用攻击 ⑧弱口令攻击 ⑨网站木马攻击 ⑩内核/内存木马攻击 ⑪无线网络攻击 ⑫物理接触攻击 ⑬权限提升 ⑭授权、认证机制绕过 ⑮搭建隐蔽通道 ⑯内网敏感信息搜集利用 ⑰供应链打击 ⑱内存口令提取
5	分析研判（15%）	锁定涉事单位及关联单位（3%）	确定该起事件涉及的资产范围、资产所属单位、运营单位等
6		锁定主要责任人及相关责任人（3%）	确定该起事件的主要责任人、直接责任人、其他具体负责人员等人员及其相关责任
7		明确事件性质以及应采取的措施（3%）	按照涉事单位网络安全分级分类管理办法和应急处置预案确定事件性质及应有的处置方案

8		研判攻击的影响范围（3%）	确定攻击事件对业务连续性、稳定性、数据安全性等带来的影响，并明确影响范围
9		分析研判采用的攻击或手段（3%）	在分析研判过程中采用的攻击或手段，例如日志提取工具、关联分析工具及方法、情报提取工具及方法等及发挥的具体作用
10	应急处置（25%）	抑制攻击的能力（9%）	阻断有效攻击源（如 IP、物理接口、服务等）（6%）
11			处置社会工程学攻击的方式与效果（如何处置）（3%）
12		根除攻击的能力（8%）	漏洞定位与修复能力（定位漏洞位置，快速修复漏洞）（小时级）（4%）
13			清除或处理攻击工具、异常账号等攻击载体（4%）

14		恢复能力（8%）	业务整改恢复能力（按时间评分）
15	通报预警（15%）	准确性（5%）	是否能将涉及该事件的时间、影响范围、危害以及对策措施等情况，详实准确的通过文字、图表等形式表达出来
16		穿透性（5%）	能否将通报预警信息及时传递到一线实战部门和具体责任人
17		有效性（5%）	针对该起事件，相关方在接到通报后已在开展隐患消除工作
18	协同联动（10%）	单位内各部门之间的联动（2%）	针对该起事件单位内部安全部门、业务部门、管理部门等相关部门在处置事件过程中的联动机制、责任分工及产生的实际效果
19		行业内部的各单位的联动（3%）	针对该起事件单位行业内部相关在处置事件过程中的联动机制、责任分工及产生的实际效果

20		与公安机关、主管部门联动（3%）	针对该起事件与属地公安机关、主管部门的联动机制、联动防御体系、联动效率及产生的实际效果
21		与下属单位的联动（2%）	针对该起事件单位与下属单位在处置事件过程中的联动机制、责任分工及产生的实际效果
22	追踪溯源（10%）	溯源到场内攻击队设备信息（4%）	根据路径长度、路径还原完整度和复杂度酌情给分
23		溯源到场外攻击队设备信息（2%）	根据路径长度、路径还原完整度和复杂度酌情给分
24		溯源到攻击队员虚拟身份（2%）	根据路径长度、路径还原完整度和复杂度酌情给分
25		追踪溯源攻击主机或攻击控制主机（2%）	根据攻击主机或控制主机的可信度、路径长度、路径还原完整度和复杂度酌情给分
26	附加分项	零日漏洞的发现和处置（上限 1500 分）	在演习期间发现零日漏洞攻击事件（提交漏洞特征、原理、利用方法等说明文档，以及 POC 程序），处置和采取应对措施及时有效

27	附加分项	上报涉及本单位非法攻击线索（在演习期间发生，在演习范畴之外），并对攻击者画像（上限 1500 分）	例如木马、后门、逻辑炸弹等，并尝试对攻击者画像，提交攻击者组织属性或个人属性、所使用的攻击工具、所拥有的攻击设施、网络活动规律、攻击手法及特点等
二、减分规则			
序号	**类型**	**扣分规则**	**备注**
（一）非正常防守			
1	发现防守方非正常防守，包括封 C 段、网站不可用、网站首页被改为图片，被发现并提交确切证据	每 30 分钟减 10 分，5 个小时仍未整改的，每 30 分钟减 20 分	指挥部研发专门的系统，由攻击队提交防守方非正常防守的线索证据，系统核验并通知防守方，并给予 2 个小时处置时间，2 小时后开始扣分，采用滴血式扣分方法，指导防守方改正行为
（二）系统或网络被控：攻击方获取系统权限或突破网络边界，防守方相应扣分			
1、权限被控			
2	被获取参演单位的域名控制权限	一级域名 100 分，二级域名 50 分	影响特别重大成果的由指挥部研判后评分
3	被获取 PC 终端、移动终端权限（手机、Pad）	PC 终端 20 分，移动终端 50 分	PC 终端为 system 权限或 root 权限
4	被获取邮箱账号权限	邮箱账号口令：20 分	被攻击方使用默认密码猜解账户成功的只扣一次分
		系统管理员权限：500 分-1000 分	特别重大成果的由指挥部研判后评分
5	被获取办公自动化系统权限	200 分-500 分	获取全局性自建、在用的 OA、即时通讯、项目管理、财务等系统管理员权限

6	被获取身份、账户管理平台权限（SSO,4A）	系统管理员权限 300 分，能登入的系统 100 分/个。	特别重大成果的由指挥部研判后评分
7	被获取域控系统权限	管理员权限 200 分，域内可控服务器 10 分/台。	特别重大成果的由指挥部研判后评分
8	被获取堡垒机、运维机权限	管理员权限 200 分，托管的服务器 10 分/台。	特别重大成果的由指挥部研判后评分
9	被获取云管理平台控制权	管理员权限 200 分，云上主机 10 分/台。	特别重大成果的由指挥部研判后评分
10	被获取大数据系统权限	/	按数据量和重要程度评分，特别重大情况由指挥部研判后评分
11	被获取数据库连接账号密码（含 SQL 注入）	普通用户权限 50 分，管理员权限 100 分。	同一系统的同等权限（包括管理员）只扣一次分
12	被获取网络设备权限	依据最终成果倒溯减分，如和核心目标同一网段，300 分。以路由器为例，小型 50 分，中型 150 分，大型 300 分。	包括防火墙、路由器、交换机、网闸、光闸、摆渡机、VPN 等，特别重大情况由指挥部研判后评分
13	被获取工业互联网系统权限	/	包括车联网、智能制造、远程诊断、智能交通等，根据系统重要程度由指挥部研判后评分。

14	被获取物联网设备管控平台	带控制功能的物联网平台 200 分，按照平台上连接点数计算 5 分/台	特别重大成果的由指挥部研判后减分
15	被获取安全设备权限	普通用户权限 50 分，管理员权限 200 分	包括 IDS、审计设备、WAF 等安全设备控制权限（含分布式部署系统的管理后台），特别重大情况由指挥部研判后评分
16	被获取一般 Web 应用系统、FTP 等应用权限	普通用户权限 20 分，管理员权限 100 分	同一系统的同等权限（包括管理员）只得一次分。如果服务器主机权限同时被控，只扣一次分
17	被获取服务器主机权限（含 webshell 权限）	普通用户权限 50 分，管理员权限 100 分	与其他扣分项不叠加扣分。特别重大成果的由指挥部研判后评分
18	被获取其他重要业务系统、生产系统、数据系统等权限	/	由指挥部参照演习目标系统评分
19	被获取其他系统、服务器、设备等权限	/	由指挥部核定评分
2、网络边界被突破			
20	被攻击者进入逻辑隔离业务内网	-1000 分	/
21	被攻击者进入逻辑强隔离业务内网	-2000 分	/
22	被攻击者进入核心生产网（如铁路调度专网、银行核心账务网、电力生产控制大区、	-5000 分	/

	运营商信令网、能源生产物联网等）		
23	其他情况	/	/
3、目标系统被控			
24	互联网区	-5000 分	如果互联网区目标系统外的其他重要业务系统权限被控，能够影响全行业或某一地区重大业务开展，视同目标系统失分，最高减 4000 分。
25	业务内网	-7000 分	如果业务内网区目标系统外的其他重要业务系统权限被控，能够影响全行业或某一地区重大业务开展，视同目标系统失分，最高减 6000 分。
26	核心生产网	-10000 分	如果核心生产网区目标系统外的其他重要业务系统权限被控，能够影响全行业或某一地区重大业务开展，视同目标系统失分，最高减 9000 分。

三、零日漏洞评分标准

分值范围	设备类	软件类	系统/服务类
8000~10000 分	骨干网路由器/防火墙代码执行+权限提升	OpenSSL 远程代码执行 OpenSSL 登录绕过 Chrome 浏览器代码执行+沙箱逃逸	Windows 升级服务代码执行/文件替换 VMware/KVM 虚拟机逃逸 SSH 连接认证绕过

5000~8000 分	骨干网路由器/防火墙代码执行+网闸代码执行+权限提升	Office 代码执行 Acrobat 代码执行 QQ/微信代码执行 Coremail 代码执行	Apache/Nginx 远程代码执行 SOC 系统代码执行 WindowsSMB 服务代码执行 VNC 连接认证绕过 SqlServer 数据库代码执行 Oracle 数据库代码执行
3000~5000 分	万兆级防火墙越权访问 万兆路由器越权访问 IPS 设备/VPN 设备代码执行+权限提升 堡垒机代码执行+权限提升 网闸越权访问	360 安全卫士代码执行 腾讯安全管家代码执行 WPS 代码执行 蓝信/钉钉代码执行 Exchange 邮件客户端代码执行 Coremail 越权访问（管理权）	Linux、Windows 提升至最高权限 SOC 系统越权访问（管理权） WindowsRDP 连接认证绕过 PHP/Perl 代码执行 Sqlserver 数据库越权访问 MySQL 代码执行
1500~3000 分	千兆级防火墙越权访问 企业级千兆路由器越权访问 VPN 设备越权访问 IPS 设备代码执行 堡垒机代码执行 设备代码执行	WinZip、WinRAR、7Zip 代码执行 瑞星代码执行 Coremail 越权访问（访问权） Foxmail 邮件客户端代码执行 行业 OA 系统代码执行	腾讯 OAuth 认证服务绕过 京东 OAuth 认证服务绕过 支付宝 OAuth 认证服务绕过 MySQL 越权访问 Sqlite 代码执行 Struct2 代码执行 Weblogic 代码执行 IIS 代码执行 Redis 代码执行

			Shiro 代码执行
500~1500 分	百兆级防火墙越权访问 企业级百兆路由器越权访问 IPS 设备越权访问 堡垒机越权访问 家用路由器远程代码执行+权限提升	主流行业 OA 系统越权访问	百度 OAuth 认证服务绕过 Sqlite 越权访问
100~500 分	摄像头代码执行+权限提升 家用路由器代码执行	小型行业 OA 系统文件上传、路径穿越	JBoss 代码执行 Shiro 认证绕过
100 分~200 分	摄像头越权访问 家用路由器越权访问	小众行业 OA 系统文件下载、敏感信息泄露	Redis 越权访问
评分考虑： 1、由于演习的关注点是漏洞对关键信息基础设施的影响，主要考虑漏洞对演习的得分贡献； 2、同一个系统的同类漏洞，还需要考虑漏洞的触发条件苛刻、漏洞复现的稳定程度和漏洞的利用难度等因素，因此得分存在一定的浮动范围； 3、由于这里的评分更多的是从结果导向来判断，可以采用多个漏洞组合达成某一结果，也就是说这里的一项评分可能是针对几个漏洞的组合，而不一定是针对单个漏洞。			

附件 2

“护网 2022”网络安全攻防实战演习数据上报模板

1、演习基本情况表

（1）实网攻防

省份	省（市）	演习级别	演习开始时间	演习结束时间	攻击队伍数量	攻击人员总数	行业数量	防守单位数量	目标系统数量	演习发现的问题隐患数量	重大战果数量（1000分以上）	下发督促整改法律文书数量	已整改的问题隐患数量

（2）沙盘推演

省份	省（市）名称	演习级别	演习开始时间	演习结束时间	沙盘推演行业	攻击方单位名称	防守方单位名称	攻击方案

2、领导批示表

领导姓名	领导职务	批示指示内容

3、防守单位信息表

防守单位	行业	总得分	防护值	排名	参演人数	单位地址	网络安全联络人	联系人电话

4、攻击方信息表

队伍名称	队伍的分	排名	姓名	联系电话	身份证号	擅长技术方向	所属单位名称（必须写全称）	职务	演习中是否有违法行为	演习中是否有违规行为	违规类型

5、其他参演人员信息表

参演角色	姓名	单位	手机号	身份证号

6、问题隐患表

得分	攻击单位名称	防守单位名称	被控系统名称	外网 IP	内网 IP	URL	系统层级	信息系统类型		问题隐患类型		成果报告文件（1000分以上提供）
								大类	小类	大类	小类	

7、发现演习前攻击事件线索

（1）攻击线索基本信息

攻击事件类别	发现时间	发生时间	被攻击单位名称	被攻击系统名称	被攻击系统域名	被攻击系统 IP（内网）	被攻击系统 IP（外网）	攻 击 源 IP	利用的漏洞	处置措施	指纹、日志、样本等线索内容描述

（2）侦察调查信息

社交网络账号	邮箱	手机号	所属组织	其他信息	真实姓名	是否立案