ICS 35.110

CCS L 79

T/CSAC

团　　体　　标　　准

T/CSAC XXX—XXXX

网络空间安全仿真 基于技战术体系的安全测评方法

Cyber range- Security test and evaluation method based on attack technology and tactics model

（征求意见稿）

2023-03-12

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国网络空间安全协会　　发布

目　　次

前　　言 III
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
3.1 评价对象　target of evaluation 1
3.2 测试 test 1
3.3 测试用例 test case 1
3.4 战术阶段 tactical stage 2
3.5 安全测评人员 Cybersecurity Evaluation Workforce 2
3.6 知识 knowledge 2
3.7 技能 skill 2
3.8 资产 asset 2
3.9 识别 identify 2
3.10 赋值 assignment 2
4 符号和缩略语 2
5 概述 2
5.1 攻击技战术模型概述 2
5.2 基于攻击技战术模型的安全测评流程 3
6 确定实施方案 4
6.1 制定计划 4
6.2 组建团队 4
6.3 搭建测评环境 5
6.4 构建攻击技战术 6
6.5 体系化模拟 7
6.6 制定应急处置方案 8
7 测评执行 9
7.1 实施攻击测试 9
7.2 测评处置 9
8 风险量化计算 10
8.1 资产赋值 10
8.2 威胁识别 10
8.3 弱点识别 11
8.4 风险值计算原理 13
8.5 风险结果判定 13
9 防护能力量化计算 14
9.1 攻击检测能力识别 14
9.2 攻击阻断能力识别 14
10 结果判定 15

10.1 确定技术指标 15
10.2 信息系统类判定准则 15
10.3 安全产品类判定准则 15
11 测评总结 16
11.1 测试反馈 16
11.2 测评后处置 17
11.3 差距报告 17
附 录 A （资料性） ATT&CK 框架的战术阶段 18
附 录 B （资料性） 测评人员知识和技能要求 19
附 录 C （资料性） 目标场景搭建基本步骤 22
C.1 目标网络拓扑准备 22
C.2 路由脚本配置及下发 22
附 录 D （资料性） 攻击场景特殊性要求 23
D.1 概述 23
D.2 企业场景 23
D.3 工业控制系统场景 23
D.4 移动终端场景 23
D.5 金融行业场景 23
附 录 E 检测评估统计表 25
参 考 文 献 26

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国网络空间安全协会提出并归口。

本文件起草单位：鹏城实验室、广州大学网络空间先进技术研究院、中汽研软件测评（天津）有限公司、中国电信股份有限公司广东研究院、哈尔滨工业大学(深圳)、北京升鑫网络科技有限公司、北京永信至诚科技股份有限公司、中汽创智科技有限公司、中国第一汽车集团公司、广东为辰信息科技有限公司、零束科技有限公司、重庆长安汽车股份有限公司、南方电网科学研究院有限责任公司、兴唐通信科技有限公司、深圳供电局有限公司、中国联合网络通信有限公司、中国移动通信集团有限公司、中国信息通信研究院、北京天融信网络安全技术有限公司、安天科技集团股份有限公司、北京神州绿盟科技有限公司、奇安信科技集团股份有限公司、北京奇虎科技有限公司、湖南星汉数智科技有限公司、四川亿览态势科技有限公司、软极网络技术（北京）有限公司、新华三技术有限公司、中国电子信息产业集团有限公司第六研究所、浙江国利网安科技有限公司、博智安全科技股份有限公司、电子科技大学、北京理工大学、北京邮电大学、上海交通大学、上海电力大学、电子科技大学广东电子信息工程研究院

本文件主要起草人：贾焰，鲁辉，韩伟红，贾世准，田志宏，李树栋，张曼，向文丽，孙丽群，陶莎，蔡晶晶，陈俊，周密，林文辉，罗富财，苏申，周可，程度，卞建超，马兰，胡宁，顾钊铨，王晔，廖清，李润恒，安伦，王帅，金华敏，贺可勋，杨彦召，薛信钊，郭超，李影，孙琦，禹晶晶，赵焕宇、罗蕾，周鑫强，汪向阳，匡晓云，杨祎巍，孟琦，胡伟，孙强强，连耿雄，陈璐，刘伟，徐雷，陶冶，邱勤，徐天妮，谢玮，孟楠，石悦，李雪莹，王龑，吴潇，肖新光,李晨，肖岩军，宫智，孙翔，武鑫，张屹，王新宇，燕玮，王绍杰，薛金良，包贤晨，傅涛，郑轶，张凯,李炜。

网络靶场　基于技战术体系的安全测评方法

1　范围

本文件描述了基于技战术体系在网络靶场环境中对信息系统、安全产品等对象进行安全测评的方法，包括：基本概念、分析原理和流程要求。

本文件适用于指导组织基于技战术体系开展安全测评工作。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022 信息安全技术 术语

《信息安全技术 网络安全从业人员能力基本要求》（征求意见稿）

ISO/IEC TS 17027:2014 Conformity assessment — Vocabulary related to competence of persons used for certification of persons

ISO/IEC 13335-1:2004 Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management

3　术语和定义

GB/T 25069-2022 和 ISO/IEC TS 17027:2014 界定的以及下列术语和定义适用于本文件。

3.1

评价对象　target of evaluation

被评价的信息技术产品或系统及其相关的指南文档。

3.2

测试 test

使评价对象按预定方法/工具产生特定行为，以获取证据来证明其安全确保措施是否有效的过程。

[来源：GB/T 25069-2022，3.65，有修改：“评估对象”改为“评价对象”]

3.3

测试用例 test case

为测试某个特殊功能或性能而编制的一组测试输入、执行条件以及预期结果，其内容包括测试目标、测试环境、输入数据、测试步骤、预期结果、测试脚本等，用于核实某个测试对象是否满足某个特定要求。

3.4

战术阶段 tactical stage

攻击技战术模型所抽象出来的攻击者进行攻击的不同阶段，每个战术阶段包含只多项攻击技术。

3.5

安全测评人员 Cybersecurity Evaluation Workforce

从事网络安全测评工作，承担相应的工作职责，并具有相应的知识和技能的人员。

3.6

知识 knowledge

通过经验或教育获取的事实、信息、真理、原理或者领悟。

[来源：ISO/IEC TS 17027:2014，2.56]

3.7

技能 skill

通过教育、培训、经验或其他方式完成任务或活动并获得预期结果的一种才能。

［来源：ISO/IEC TS 17027:2014，2.74］

3.8

资产 asset

对组织有价值的信息或资源,是安全策略保护的对象。

［来源：ISO/IEC 13335-1:2004，2.2］

3.9

识别 identify

对某一评估要素进行标识域辨别的过程。

3.10

赋值 assignment

对识别楚的评估要素根据已定的量化模型给予定量数值的过程。

4 符号和缩略语

下列缩略语适用于本文件。

ATT&CK：对抗性战术、技术和常识（Adversarial Tactics, Techniques, and Common Knowledge）

KVM：基于内核的虚拟机（Kernel-based Virtual Machine）

SSH：安全外壳协议（Secure Shell）

RDP：远程桌面协议（Remote Desktop Protocol）

VNC：虚拟网络控制台（Virtual Network Console）

APT：高级持续性威胁攻击（Advanced Persistent Threat）

5 概述

5.1 攻击技战术模型概述

攻击技战术模型，即 ATT&CK 模型。ATT&CK 是由 MITRE 公司创建并持续维护的一个对抗战术和技术的知识库，全称 Adversarial Tactics, Techniques, and Common Knowledge, 简称 ATT&CK。

ATT&CK 是在洛克希德·马丁公司提出的 Kill Chain 模型的基础上，构建的一套更细粒度、更易共享的知识模型和框架。ATT&CK 是一个基于黑客攻击实战结果建立的网络攻击战术和技术的知识体系，描述了网络攻击的行为模型，反映出整个攻击周期的各个阶段。ATT&CK 包含三个核心部分，即战术、技术和过程（TTPs），战术表示攻击者的目标，技术表示攻击者达成战术目标的方法与手段，过程显示攻击者如何执行某项技术。

ATT&CK 模型是不断演化的，约 6 个月左右会更新 1 次。除非特别声明，在依照本文件进行安全测评时，均应以 ATT&CK 矩阵的当前版本为依据。

5.2 基于攻击技战术模型的安全测评流程

基于攻击技战术的安全测评受到组织实际业务、安全需求、系统规模等方面的影响，需明确评估目标、范围、工具、团队、技术方案、环境和相关应急措施等，制定安全测评计划，组建测评实施团队，搭建测评环境，构建面向评价对象的攻击技战术并进行体系化模拟，同时制定面向安全测评全流程的应急处置措施，确定实施方案，为组织具体开展测评工作提供指导。在测评启动之后，主要包括如下工作：

a） 制定计划：根据前期调研和收集的情况、测评组织和被测方确定的目标范围等，明确双方职责，制定测评各个环节的工作计划和进度安排；

b） 组建团队：根据测试需求组建测评团队，明确团队分组即职责；

c） 搭建测评环境：在网络靶场环境中设计部署目标网络，作为开展安全测评的环境；

d） 构建攻击技战术：根据评价对象情况、信息收集分析情况等，制定攻击方案，利用 ATT&CK 框架作为评估“标尺”，覆盖 ATT&CK 框架的攻击技战术。同时，攻击技战术构建应根据场景区域、场景访问策略、场景节点、场景漏洞，构建攻击技战术线路。

e） 体系化模拟：对构建的攻击战术和技术进行体系化模拟实现；

f） 测评执行：按照事前拟定的攻击方案，采用选定的攻击技战术对评价对象进行攻击测试；

g） 量化评估：对评价对象（信息系统、安全产品）的安全风险、安全防护能力等进行量化计算；

h） 结果判定：对测试结果通过与否进行判定。

基于攻击技战术模型的安全测评流程如下图所示。

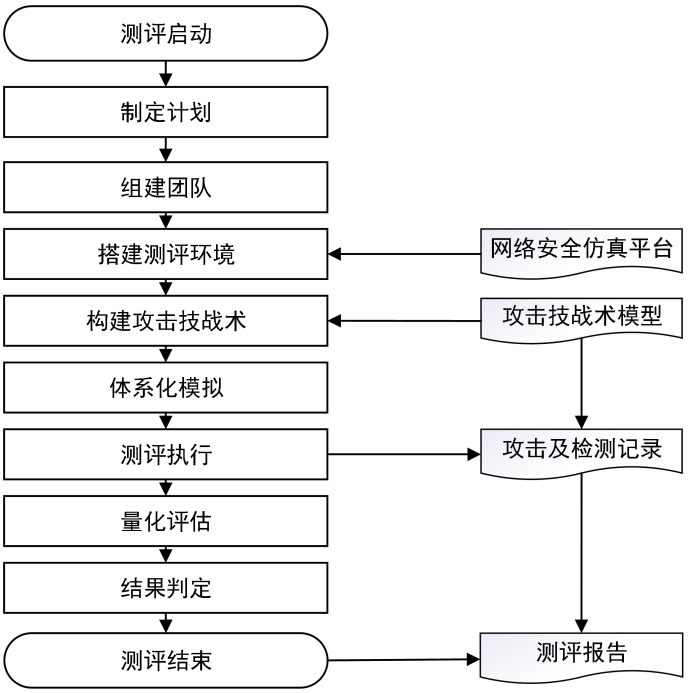

图1 基于攻击技战术模型的安全测评流程图

6 确定实施方案

6.1 制定计划

6.1.1 主要工作

在制定测评计划时，测评机构与测评人员应做充分的调研与准备，应开展以下工作：

a) 测评方对评价对象进行情况收集，被测方应予以配合。情况收集包括但不限于以下内容：
   1) 评价对象的拓扑结构或功能模块信息；
   2) 评价对象的软硬件配置信息；
   3) 安全域划分信息、应用概况等环境搭建要素；
   4) 其他用于安全测评的必要信息。
b) 由测评方和被测方召开会议，签订委托测评协议，明确评估目标、评估范围等；
c) 安全风险评估范围应为：组织全部的信息及与信息处理相关的各类资产、管理机构，或者组织某个独立的信息系统、关键业务流程和部门；
d) 根据被测方实际需求和评估范围，应制定评估实施活动的总体计划，用于指导评估工作，具体包括组建团队、搭建测评环境、构建攻击技战术、体系化模拟、测评实施、量化评估、编制报告等环节的工作计划和时间进度安排等；
e) 应与被测方协商沟通测评计划表，提高测评效率；

6.1.2 双方职责

在制定测评计划时，测评方与被测方应遵守各自的职责，为顺利开展安全测评创造良好条件。

a) 测评方职责：
   1) 组建测评项目组；
   2) 指出被测方应提供的基本资料；
   3) 向被测方介绍安全测评工作流程和方法；
   4) 向被测方说明测评工作可能带来的风险和规避方法；
   5) 了解被测方的信息化建设以及评价对象的基本情况；
   6) 初步分析系统的安全状况，准备测评工具和文档。
b) 被测方职责：
   1) 向测评方介绍本单位的信息化建设及发展情况；
   2) 提供测评方需要的相关资料；
   3) 为测评人员的信息收集工作提供支持和协调，参与制定应急预案。

6.2 组建团队

6.2.1 总体要求

根据测评项目要求组建测评团队，明确测评实施各团队的工作职责，此外还应注重测评团队人员的知识和技能建设。

6.2.2 测评实施团队

测评实施团队包含环境搭建组、攻击测试组、检测评估组、报告输出组和测评仲裁组，各团队人员的角色及其相应的工作职责描述如下：

表 1 测评实施团队角色和职责

序号	团队人员角色	工作职责描述
1	环境搭建人员	对评价对象的信息收集，评价对象的仿真环境搭建，模拟攻击环境搭建，以及环境的管理和维护
2	攻击测试人员	攻击方案制定，模拟攻击实施，模拟攻击工具库管理和维护
3	检测评估人员	攻击结果记录分析，对攻击结果做量化评估
4	报告输出人员	负责测评全周期情况记录和分析，测评报告撰写
5	测评仲裁人员	对攻击测试和检测评估结果进行监督或者判定

各测评实施团队基于以上工作职责做好组内人员的工作分工。

6.2.3 测评人员要求

测评人员应该具备安全测评职责相关的知识和技能，必要时需要开展相关知识和技能业务培训，并制定培训机制和团队建设计划。

6.3 搭建测评环境

6.3.1 基本要求

目标场景构建与管理应采用灵活便捷的方式快速设计部署大型目标网络，对目标网络的节点内部程序提供多种方式进行灵活配置，能够提供网络设备虚拟化、虚拟交换机流量镜像等多种方式提高目标网络的逼真程度，提供丰富的互联接入方式使目标网络与异域的设备和网络或互联网互联互通，并提供统一的资源管理支撑目标网络的构建。具备包括：实验场景配置能力、虚拟网络能力、互联接入能力、节点管理能力、资源管理能力。

6.3.2 测试场景配置

a) 应支持根据评估范围完成网络拓扑、应用软件和带内程序的配置；
b) 应支持测试场景配置的统一描述，支持通过导入拓扑脚本的方式完成目标网络的配置和部署；
c) 应支持在目标网络部署生成后对目标网络内的带内程序进行批量配置。

6.3.3 互联接入管理

a) 应支持远程实物设备或网络等接入到虚拟网络中；
b) 应支持通过便捷配置实现目标网络和互联网的访问与控制；
c) 应支持在目标网络中接入透明设备，并且不改变设备的透明属性。

6.3.4 测试网络生成

a) 应支持KVM、容器、裸金属服务器、物理设备等多种节点生成方式，各种生成方式均能通过已有的镜像快速部署；
b) 应支持对不同厂商、不同型号的网络安防设备进行虚拟化；
c) 应支持对跨宿主机器的流量进行隧道封装；
d) 应支持虚拟交换机配置流量镜像复现流量分析场景。

6.3.5 节点控制管理

a) 应支持构建通道使非目标网络内的节点和网络同目标网络内节点之间进行可控访问；
b) 应支持虚拟节点全生命周期管理和控制，支持虚拟化节点、容器节点和实物节点的无差异管理；

c) 应支持对虚拟节点的状态和日志进行监控。

6.3.6 测试资源管理

a) 应支持对测试过程中需要的工具、脚本、试验设备等资源进行统一管理；
b) 应支持对各类试验资源的查看和使用权限进行管理。

6.3.7 场景搭建流程

组织应根据明确测评需求，设计整体环境搭建方案，包括目标网络拓扑设计和资源规划，为搭建目标场景环境提供指导。

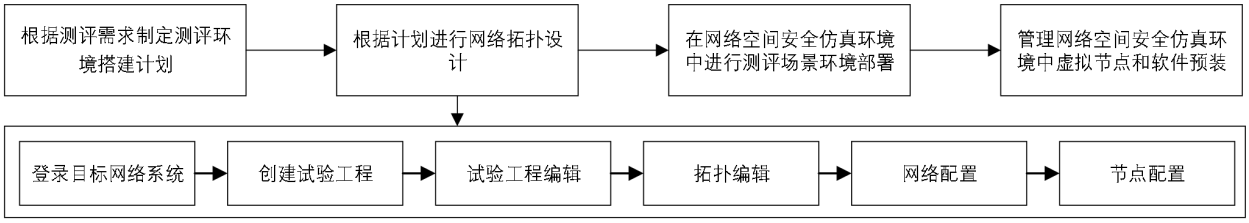

图2 场景搭建流程

a) 根据测评需求制定测评环境搭建计划

根据需求方提出的需求，应根据场景需求完成制定测评环境搭建计划。计划内容包括但不限于：使用人员对象、网络拓扑、资源分配、靶标设计、预装软件、任务制定、采集及检测范围、分析及评估对象等。

b) 根据计划进行网络拓扑设计

根据提供的系统入口登录目标网络系统，依次进行创建试验过程、试验过程编辑、拓扑编辑、网络配置、节点配置等。系统应支持创建空白工程、根据模板创建工程、根据文件导入工程以及根据设备分布创建工程等多种方式，应结合不同需求与系统实际，选择不同方式创建试验工程。试验工程应支持删除、修改权限等编辑操作。拓扑结构和网络配置应根据需要，支持拖拽式/脚本配置等方式进行编辑。网络节点应支持基本属性配置、批量创建、配置检查等功能。

c) 在网络靶场平台中进行测评场景环境部署

测评场景环境部署应在网络拓扑设计完成且确认无误后进行操作，在部署过程中应实时监控部署状态，并支持取消部署、清空部署等操作。

d) 虚拟节点管理和软件预装

虚拟节点应支持相关信息和状态的查看，支持根据节点名称、类型、IP和自定义属性进行搜索，并可通过SSH、RDP、VNC等多种方式接入虚拟节点。系统应支持通过选取指定的虚拟机进行软件预装，以及查看已安装和可安装的软件。

6.4 构建攻击技战术

6.4.1 攻击方案选取原则

a) 攻击组织形式应主要从以下方式选取：
   1) 开放式招募白帽子攻击手参与测试；
   2) 安全测评团队人员按照攻击方案组织实施测试；
b) 在选择攻击技战术时，应遵循如下原则：
   1) 应选择一系列代表性技术进行测评，而非对整个 ATT&CK 框架；
   2) 应结合被测信息系统的类型、子系统/子网类型、已发生的攻击事件等信息，分析系统/子系统易遭受的攻击类型，选择恰当的攻击方法（如 APT29、FIN7 等）；

3) 应选取针对被测方所处行业或目前活跃度较高的 APT 攻击组织，应选取该 APT 组织体系化的攻击技术手法；
4) 应排除技术复杂，无法在实验室环境中实现的攻击操作；
5) 应选定攻击模拟软件、计划、测试用例；
6) 在工具选择上，应尽量大的程度上自动化还原整体攻击测试流程。
7) 选择攻击方法时，应参照以发生过的攻击事件的数据，攻击事件的数据可来自权威安全机构的网站等。

6.4.2 评价对象情况调研

安全测评团队应收集客户需求，确定测试范围、目标等。

在评价对象情况调研阶段，安全测评团队与客户组织应进行交互讨论，重点确定安全测评的范围目标限制条件以及测试细节。

该阶段应收集客户需求、准备测试计划、定义测试范围与边界、定义业务目标、项目管理与规划等活动。

安全测评团队应要求客户出具委托书，并同意实施方案。安全测评首先必须将实施方法、实施时间、实施人员，实施工具等具体的实施方案提交给客户，并得到客户的相应书面委托和授权。应做到客户对安全测评所有细节和风险的知晓、所有过程都在客户的控制下进行。

6.4.3 信息收集分析

安全测评团队应获取目标系统网络拓扑、系统配置与安全防御措施的信息；应按照主动和被动的策略进行信息收集。

通过信息收集有针对性的进行威胁建模和漏洞分析，提高模拟攻击的成功率，同时降低攻击测试对系统正常运行造成的不利影响。这一步应包括白盒收集、人力资源情报、踩点、寻找外网入口以及识别防御机制。

6.4.4 威胁建模

安全测评团队应根据评价对象调研和信息收集分析情况，执行威胁建模。

威胁建模应根据情报搜集阶段所获得的信息，对被测系统上潜在的安全漏洞与弱点进行标识，以攻击者的视角和思维来尝试利用目标系统的弱点。

威胁建模的工作应主要包括业务流程分析、威胁对手/社区分析。

6.4.5 漏洞分析

安全测评团队应分析前阶段的情报信息，找出实施攻击的攻击点。

漏洞分析阶段主要是从前面几个环节获取的信息分析和理解哪些攻击途径是可行的。

特别需要重点分析端口和漏洞扫描结果，提取到的服务 “旗帜”信息，以及在情报收集环节中得到的其他关键信息。

6.4.6 制定攻击方案

测评实施团队应根据评价对象情况、信息收集分析情况等，进行威胁建模和漏洞分析，并根据攻击方案选取原则，制定攻击方案，明确选取的攻击技战术。

6.5 体系化模拟

测评实施团队应建立体系化模拟方法，以保证攻击技战术的模拟能够达到有效的实施和体系化的合理应用，应明确以下内容：

a) 攻击技战术模型体系化模拟实现的流程；
b) 攻击技战术模型体系化模拟实现战术和技术；
c) 攻击技战术模型体系化模拟实现方法的案例；

6.6 制定应急处置方案

6.6.1 安全测评处置流程

安全测评的应急处置是以全局视角对安全测评流程、测评场景和测评目标进行监测，依靠网络靶场环境的数据采集和流量监测功能实现实时监测和应急处置，结合 ATT&CK 框架对安全测评流程进行评估，不断进行迭代以完善安全测评流程，提高安全测评的能力。

6.6.2 安全测评前的准备

安全测评前的准备，包含制定处置方案和处置制度，应急处置事件类型和等级，组建处置团队；

a) 测评处置方案应包含但不限于以下内容：
   1) 应能依靠网络靶场环境的网络资源探测功能对测评目标的联通性、状态和信息等进行实时监测；
   2) 应能依靠网络靶场环境的数据采集功能对测评环境进行实时监测，监测的指标包括：测评场景的拓扑合理性、网络连通性以及设备稳定性，以及监测测评流程各步骤的状态和结果等；
   3) 应针对可能的各种突发事件预备相应的突发事件处置预案，用于在测评过程中应对各种可能的突发事件；
   4) 应在处置预案中明确，一旦测评环境或测评目标发生故障或受到损害，需要维护的关键业务或关键事务，以及相应的恢复时间，按规定及时向测评管理层和事件相关的组织通报事件，并组织研判，形成事件报告；
   5) 应根据测评方案特点，选定处置评估方案；
   6) 应结合评估方案和 ATT&CK 框架，制定评估测评流程的指标和评估表。
b) 应急处置事件类型包含但不限于：

表 2 应急处置事件类型

序号	事件类型	描述
1	物理环境问题	对测评系统正常运行造成影响的物理环境问题和自然灾害，如断电、电磁感染、火灾、地震等。
2	硬件故障	对测评环境产生影响的设备硬件故障、网络通讯链路中断、系统本身或软件缺陷等问题。
3	软件故障	系统本身或软件缺陷等原因引起的问题。
4	操作违规	应该执行而没有执行相应的操作，或无意地执行了禁止的测评行为，如： 在约定时间范围之外进行测评； 违规攻击测评目标系统范围之外的其它系统； 禁止使用约定之外的其他环境进行测评操作； 未经审核就使用高危测评操作； 关闭测试测评环境中已经开启的监控服务、计划任务、应用类进程等。

5	数据泄密	泄露需要保密的测评目标相关信息，如：对外泄露测评数据资源或信息，泄露测评目标系统核心专利，安全配置，源码等。

c) 应急处置事件等级定义如下所示：

表 3 应急处置事件等级定义

等级	标识	描述
3	高	一旦发生将产生非常严重的经济损失或社会影响，如测评组织信誉严重破坏、经济损失重大
2	中	一旦发生会造成一定的经济损失，但影响面或影响程度不大
1	低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定的手段和处置预案能很快解决

d) 处置实施团队主要由测评仲裁人员组成。处置人员的主要任务是对测评流程的监测、应急处置和评估。

7 测评执行

7.1 实施攻击测试

由攻击测试组按照事前拟定的攻击方案，对选定的攻击技战术进行实现，将攻击技战术分解为若干攻击测试用例，执行后输出相关的攻击测试报告。检测评估组观察和验证测试用例是否及时反馈了结果，对攻击结果记录分析，对攻击结果做量化评估。

测评仲裁人员在测试执行过程中，应对攻击测试组的行为进行监督，并监测测评实施的有效性：

a) 数据采集：对测试执行过程中产生的相关数据，包括但不限于日志类，流量信息，武器使用信息等，进行采集。

b) 攻击检测：对测试执行过程中发生的攻击事件，包括但不限于包括但不限于蠕虫病毒攻击，跳板攻击，后门攻击，漏洞攻击等，进行收集汇总。

c) 行为监督及有效性监测：根据采集到的数据流量以及汇总的攻击事件对攻击测试组的行为进行评估反馈，保证攻击验证组没有偏离事先选定的攻击线路，以免超出测试范围，或造成不必要的资源浪费，确保攻击的有效性。

7.2 测评处置

测评处置是在安全测评过程中发现突发事件时，进行事件处置，包含但不限于如下步骤：

a) 监测预警

测评处置小组应利用网络靶场环境在测评执行中的数据采集、事件监测功能，建立监测预警，明确监测策略、监测内容、预警分级和预警后的应急处置预案。

b) 测评应急处置

应急处置小组应按照先应急处置、后调查评估的原则，在事件发生后依靠网络靶场环境的实时监测和可视化展示功能，全方位收集事件信息，快速定位事件位置，执行应急处置预案，控制事件事态，包括：停止当前测评工作、实施网络隔离、备份网络靶场环境数据、保护安全测评现场等，确保所有的响应活动被适当记录，便于事后分析。

同时，应根据应急处置规定，通报测评管理层和相关组织。

c) 处置和恢复

应急处置小组和测评管理层根据应急事件发展事态和应急处置事件等级（如事件等级 2 级以上），协调相关人员和资源，制定详细的处置方案，对事件进行更进一步的处置。

对造成测评停止或环境破坏的事件，需进行恢复处置。

对于造成损失的测评事件，应明确事后恢复的责任人，开展损害评估、赔偿、事件调查处理等工作。

当应急事件得以控制或消除时，应执行应急处置解除流程。

d) 处置总结报告

处置总结报告应包含但不限于：

1) 安全测评事件的发生、发展和处置过程；

2) 安全测评事件的原因和处置结果；

3) 安全测评事件的关键数据和特征，分析事件的性质、影响范围、危害程度和损失情况；

4) 安全测评事件对应的改进措施和预防措施。

8 风险量化计算

8.1 资产赋值

根据评估范围涉及的资产，形成资产清单并赋值。

a) 资产价值的数值为人工输入，由评估参与双方协商赋值；

b) 资产价值的赋值分为 1-5，共 5 个级别；

c) 资产价值的判定可以参考等级保护定级标准如下：

表 4 资产价值赋值

赋值	定义
1	对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序和公共利益
2	对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全
3	对象受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害
4	对象受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害
5	对象受到破坏后，会对国家安全造成特别严重损害

8.2 威胁识别

威胁值最终体现了风险发生的可能性，威胁值按照 ATT&CK 框架的战术阶段来赋值。

威胁值为手动输入，根据 ATT&CK 战术阶段不同，取值也不同，取值区间为 1-5，威胁值赋值标准参见下表：

表 5 威胁值赋值

威胁值	等级	可能性描述（威胁发生的频率）
5	很高	出现的频率很高（不少于1次/周），或在大多数情况下几乎不可避免，或可以证实经常发生过
4	高	出现的频率较高（介于1次/月和1次/周之间），或在大多数情况下很有可能会发生，或可以证实多次发生过
3	中等	出现的频率中等（介于1次/年和1次/月之间），或在某种情况下可能会发生，

		或被证实曾经发生过
2	低	出现的频率较小，或一般不太可能发生，或没有被证实发生过
1	很低	威胁几乎不可能发生，或仅可能在非常罕见或例外的情况下发生

8.3 弱点识别

弱点值的评定需要考虑两个因素，一个是弱点的严重程度，即一旦发生，对资产本身的破坏程度。另一个是弱点的暴露程度，这和当前的控制有关，如果控制得力，弱点暴露程度则会比较低。

弱点识别内容如下表所示：

表 6 弱点列表

弱点类别	弱点名称	弱点描述
资产管理	信息资产责任不清	对资产属主和保管者的责任不明确，难以保证信息资产分级及保护措施的落实
	缺乏信息分类机制	对信息资产/数据没有明确的分类和分级标准，缺乏相应的资产处理办法
通信与操作管理	缺乏对过程文件的集中控制	对业务活动中产生的记录、日志等文件没有进行集中管理
	缺乏变更管理程序	对信息系统进行变更时缺乏有效的控制流程
	缺乏职责分离机制	存在单个人员承担多项存在冲突或矛盾职责的情况，或者存在单个系统承担多种存在冲突或矛盾职能的情况
	对第三方服务缺乏评审监督和检查	对第三方提供的服务缺乏评审监督和检查，难以保证服务质量和安全性
	缺乏容量规划	对信息系统的性能及容量需求缺乏前瞻性规划，易导致资源不足或设施故障
	缺乏恶意代码/病毒防范机制	缺乏对病毒等恶意代码的防范和控制
	缺乏有效的备份	没有制定有效的备份策略，缺乏备份机制，或者备份操作不当
	缺乏网络接入和使用的安全管理	对各种网络服务的访问（包括即时通信服务），网络共享的设置，包括无线和拨号在内的网络接入方式缺乏管控措施
	缺乏移动计算机的使用管理	对笔记本电脑的使用、携带缺乏有效管控
	缺乏对移动介质的安全管控	对U盘、移动硬盘等移动介质的使用、携带缺乏有效管控
	缺乏终端的安全管理和准入机制	对用户终端的准入条件没有明确的规定
	缺乏电子邮件使用管理	没有对内部电子邮件进行安全管理
	缺乏对文件打印/复印及分发的控制	没有对文件打印过程进行有效管理
	缺乏对信息交换的安全管理	对组织内部各单位之间以及组织对外的各种信息交换途径、方式缺乏有效管控，包括Email、传真、电话、快递等

	缺乏软件分发管理机制	对各类软件的获取、License管理、分发、安装及使用缺乏有效管控
	缺乏对第三方人员的安全管理	
	对信息系统的监控不力	对网络信息系统的监控不足，缺乏日志记录和检查
访问控制	缺乏有效的访问控制	并没有制定针对各类IT设施（网络、服务器、操作系统、应用系统等）的访问控制策略和规范，或者访问控制执行不力
	缺乏有效的用户权限管理机制	对用户权限的申请、开设、复查等缺乏有效管控
	用户账号缺乏安全管理	用户账号可随意共享、传递，缺乏足够的账号安全管理意识和策略
	口令设置脆弱	用户口令设置过于简单
	缺乏有效的加密保护	没有通过必要的保密措施对数据或文件进行管控
	缺乏会话超时机制	没有对设置电脑自动锁屏策略，没有系统访问的会话时间限制
信息系统获取、开发与维护	缺乏软件开发/采购安全保障机制	对软件系统的开发/采购缺乏安全保障，包括安全需求分析、安全过程控制、安全测试和验收等
	程序设计漏洞	软件存在设计漏洞
	缺乏漏洞管理机制	缺乏应对软件漏洞的管理机制
	配置不当	对网络系统、应用系统或软件的配置不当
	缺乏认证授权机制	系统缺乏身份识别、身份认证及授权机制
	缺乏密码控制及使用策略	系统缺乏密码使用、密钥管理等控制机制
	缺乏充分的维护响应机制	在系统故障时无法实现及时响应
	服务水平协议不当	没有对服务水平进行明确定义
信息安全事件管理	缺乏有效的安全事件管理机制	没有应对信息安全事件的应急和处理机制
	缺乏对信息安全事件的记录	一旦发生信息安全事件，没有对处理过程进行明确记录
业务持续性管理	缺乏完整的BCP框架和落实机制	没有经过有效的BIA分析建立整个框架，也没有具体落实到各部门，或者BCP机制不够健全
	缺乏风险评估和BIA	没有采取有效的方法进行风险评估和业务影响分析
	缺乏重要系统的应急预案	缺乏重要系统的应急预案
	未定期开展业务连续性演练和测试	未定期开展业务连续性演练和测试
符合性	缺乏对相关法律法规的遵循	没有识别适用的信息安全相关法律
	缺乏有效的审计机制	对信息安全工作缺乏检查和审计
	缺乏ISMS文件控制程序	没有对信息安全管理体系文件进行必要的管控
	缺乏ISMS记录控制程序	缺少对信息安全管理体系评审和改进的记录

弱点值最终体现了风险发生的后果，弱点值为手动输入，取值区间为 1-5。弱点值赋值标准参见下表：

表 7 弱点值赋值

弱点值	等级	严重性描述（弱点一旦被利用可能对资产造成的冲击）

5	很高	以下情况中的任意一种： 弱点没有丝毫控制和掩饰，资产可能完全失控； 一旦弱点被威胁利用，将造成立即停工，且半天内无法恢复； 弱点被利用后将造成灾难性的后果，对资产造成完全损害；
4	高	以下情况中的任意一种： 弱点比较明显，易造成资产部分失控； 一旦弱点被威胁利用，将导致相关工作中断，但半天内可以恢复； 弱点被利用后将造成重大后果，对资产造成重大损害；
3	中等	以下情况中的任意一种： 弱点可以被发现，可能造成资产部分不可信； 一旦弱点被威胁利用，将造成工作延迟，无法以正常标准提供服务； 弱点被利用后将造成中等的后果，对资产造成一般性损害；
2	低	以下情况中的任意一种： 弱点可以被发现，但资产仍基本可信； 一旦弱点被威胁利用，将造成作效率降低，但所提供的服务不受影响； 弱点被利用后将造成次要的后果，对资产造成较小损害；
1	很低	以下情况中的任意一种： 弱点难以被发现，资产也可信可控； 一旦弱点被威胁利用，对工作的影响可以被正常的业务操作所吸收； 弱点被利用后将造成轻微的后果，对资产造成的损害可以忽略；

8.4 风险值计算原理

a) 针对模拟攻击下，资产在各阶段面临的弱点情况，分别计算风险值。

b) 风险值的计算公式建议如下：

风险值 ＝ 资产价值 × 弱点值 × 威胁值。

示例：A 资产（本次项目中资产为某个 IP 的主机）的风险计算公式为：

（A 资产风险值=Round（A 资产价值*A 资产弱点值*A 资产威胁值）,0）；

注：Round 函数为四舍五入的取整函数，结果是返回一个整数值，该数值是按照指定的小数位数进行四舍五入运算的结果。

表 8 风险值计算表

威胁可能性		1					2					3					4					5				
弱点严重性		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
资产价值区间	1	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15	4	8	12	16	20	5	10	15	20	25
	2	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30	8	16	24	32	40	10	20	30	40	50
	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45	12	24	36	48	60	15	30	45	60	75
	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60	16	32	48	64	80	20	40	60	80	100
	5	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75	20	40	60	80	100	25	50	75	100	125

8.5 风险结果判定

a) 经过计算的某个资产的风险值，分为低、中、高、极高共 4 级；

b) 风险级别的定义参见下表所示：

表 9 风险等级评定表

风险级别		风险值
极高风险	VBI	大于80
高风险	HBI	大于48小于等于80
中风险	MBI	大于32小于等于48
低风险	LBI	小于等于32

9 防护能力量化计算

9.1 攻击检测能力识别

攻击检测能力体现了评价对象针对各攻击技术（包括 ATT&CK 框架中技术与子技术）的检出能力。

a) 统计本次测评中模拟实现的技战术，明确对整个 ATT&CK 框架的覆盖率，根据各攻击技术的重要程度，按照 1-10 的数值赋予权重；

b) 通过观测模拟攻击过程中，记录评价对象对各战术阶段攻击技战术的检出情况、所采用的检测手段，形成检测结果记录表（示例见附录 E）；

c) 统计评价对象对各战术阶段攻击技术的检出数；

d) 计算得出攻击技术检出率，攻击技术检出率的计算公式建议如下：

攻击检出率 ＝ （检出的攻击技术权重之和÷ 攻击技术权重总和）X100%

e) 根据表 11 为各战术阶段的攻击检测能力进行赋值。

表 10 攻击检测能力赋值

能力值	等级	攻击检测能力描述
5	很高	攻击技术检出率≥95%
4	高	80%≤攻击技术检出率＜95%
3	中等	60%≤攻击技术检出率＜80%
2	低	40%≤攻击技术检出率＜60%
1	很低	攻击技术检出率＜40%

9.2 攻击阻断能力识别

攻击阻断能力体现了评价对象针对各攻击技术（包括 ATT&CK 框架中技术与子技术）的阻断能力。

a) 统计本次测评中模拟实现的技战术，明确对整个 ATT&CK 框架的覆盖率，根据各攻击技术的重要程度，按照 1-10 的数值赋予权重；

b) 通过观测各战术阶段模拟攻击，分析研判可阻断技术数量；

c) 计算得出攻击技术阻断率，攻击技术阻断率的计算公式建议如下：

攻击阻断率 ＝ (阻断的攻击技术权重之和 ÷ 攻击技术权重总和) X100%

d) 根据表 12 为各战术阶段的攻击阻断能力进行赋值。

表 11 攻击阻断能力赋值

能力值	等级	攻击阻断能力描述
5	很高	攻击技术阻断率≥95%
4	高	80%≤攻击技术阻断率＜95%

3	中等	60%≤攻击技术阻断率＜80%
2	低	40%≤攻击技术阻断率＜60%
1	很低	攻击技术阻断率＜40%

10 结果判定

10.1 确定技术指标

基于 ATT&CK 矩阵，攻击测试完成后应对攻击测试中所涉及的 ATT&CK 战术/技术/子技术进行汇总，计算战术/技术/子技术数量及其在 ATT&CK 矩阵中的覆盖率。在计算战术/技术/子技术数量及在 ATT&CK 矩阵中的覆盖率时，应参照 MITRE ATT&CK 矩阵的最新版本，且应明确是否以未去重的技术和子技术原始数量作为计算依据。战术/技术/子技术数量或 ATT&CK 矩阵覆盖率的通过指标值应由测试方与被测方共同协商约定，并在测评协议或测试报告中予以明确该约定值。

10.2 信息系统类判定准则

针对信息系统类测评对象，应根据测试执行结果，并依据本文件第 8 章对其安全风险结果做出判定，安全风险判定结果作为安全测评通过与否的重要依据。

a) 若安全风险判定结果存在“极高风险”或“高风险”，则不论战术/技术/子技术数量或 ATT&CK 矩阵覆盖率是否达到约定值，本次安全测评直接判定为：不通过；
b) 若安全风险判定结果为“中风险”或“低风险”，且战术/技术/子技术数量或 ATT&CK 矩阵覆盖率达到或者超过测试方与被测方的约定值，则本次安全测评判定为：通过。测试报告的正式结论应以战术/技术/子技术数量或 ATT&CK 矩阵覆盖率为前置条件。
c) 若安全风险判定结果为“中风险”或“低风险”，但战术/技术/子技术数量或 ATT&CK 矩阵覆盖率未达到测试方与被测方的约定值，则应增加攻击方案，直至战术/技术/子技术数量或 ATT&CK 矩阵覆盖率达到约定值，并重新根据安全风险判定结果，对本次安全测评判通过与否做出判定。
d) 若已知攻击方案或现有测试手段所涉及的战术/技术/子技术数量或 ATT&CK 矩阵覆盖率无法达到测试方与被测方的约定值，则测试方与被测方应重新协商约定值，并重新进行测试结果判定。

10.3 安全产品类判定准则

针对安全产品类测评对象，应根据测试执行结果，并依据本文件第 9 章对其攻击检测能力、攻击阻断能力及其防护能力值做出判定，判定结果作为安全测评通过与否的重要依据。

a) 仅具备攻击检测能力的安全类产品

根据本文件 9.1 节，对仅具备攻击检测能力的安全类产品的攻击技术检出率进行计算，对攻击检测能力等级做出判定。

1) 若攻击检测能力等级为“低”或“很低”（即攻击技术检出率＜60%），则不论战术/技术/子技术数量或 ATT&CK 矩阵覆盖率是否达到约定值，本次安全测评直接判定为：不通过。

2) 若攻击检测能力等级为“中等”及以上（即攻击技术检出率≥60%），且战术/技术/子技术数量或 ATT&CK 矩阵覆盖率达到或者超过测试方与被测方的约定值，则本次安全测评判定为：通过。测试报告的正式结论应以战术/技术/子技术数量或 ATT&CK 矩阵覆盖率为前置条件。

3) 若攻击检测能力等级为“中等”及以上（即攻击技术检出率≥60%），但战术/技术/子技术数量或 ATT&CK 矩阵覆盖率未达到测试方与被测方的约定值，则应增加攻击方案，直至战术/

技术/子技术数量或 ATT&CK 矩阵覆盖率达到约定值，并重新根据攻击技术检出率或攻击检测能力等级判定结果，对本次安全测评判通过与否做出判定。

4) 若已知攻击方案或现有测试手段所涉及的战术/技术/子技术数量或 ATT&CK 矩阵覆盖率无法达到测试方与被测方的约定值，则测试方与被测方应重新协商约定值，并重新进行测试结果判定。

b) 仅具备攻击阻断能力的安全类产品

根据本文件 9.2 节，对仅具备攻击阻断能力的安全类产品的攻击技术阻断率进行计算，对攻击阻断能力等级做出判定。

1) 若攻击阻断能力等级为“低”或“很低”（即攻击技术阻断率＜60%），则不论战术/技术/子技术数量或 ATT&CK 矩阵覆盖率是否达到约定值，本次安全测评直接判定为：不通过。

2) 若攻击阻断能力等级为“中等”及以上（即攻击技术阻断率≥60%），且战术/技术/子技术数量或 ATT&CK 矩阵覆盖率达到或者超过测试方与被测方的约定值，则本次安全测评判定为：通过。测试报告的正式结论应以战术/技术/子技术数量或 ATT&CK 矩阵覆盖率为前置条件。

3) 若攻击阻断能力等级为“中等”及以上（即攻击技术阻断率≥60%），但战术/技术/子技术数量或 ATT&CK 矩阵覆盖率未达到测试方与被测方的约定值，则应增加攻击方案，直至战术/技术/子技术数量或 ATT&CK 矩阵覆盖率达到约定值，并重新根据攻击技术阻断率或攻击阻断能力等级判定结果，对本次安全测评判通过与否做出判定。

4) 若已知攻击方案或现有测试手段所涉及的战术/技术/子技术数量或 ATT&CK 矩阵覆盖率无法达到测试方与被测方的约定值，则测试方与被测方应重新协商约定值，并重新进行测试结果判定。

c) 兼具攻击检测能力和攻击阻断能力的安全类产品

根据本文件 7.7 节，对兼具攻击检测能力和攻击阻断能力的安全类产品的攻击技术检出率和攻击技术阻断率进行计算，对攻击检测能力等级和攻击阻断能力等级做出判定。

1) 若攻击检测能力等级为“低”或“很低”（即攻击技术检出率＜60%）或者攻击阻断能力等级为“低”或“很低”（即攻击技术阻断率＜60%），则不论战术/技术/子技术数量或 ATT&CK 矩阵覆盖率是否达到约定值，本次安全测评直接判定为：不通过。

2) 若攻击检测能力等级为“中等”及以上（即攻击技术检出率≥60%）且攻击阻断能力等级为“中等”及以上（即攻击技术阻断率≥60%），且战术/技术/子技术数量或 ATT&CK 矩阵覆盖率达到或者超过测试方与被测方的约定值，则本次安全测评判定为：通过。测试报告的正式结论应以战术/技术/子技术数量或 ATT&CK 矩阵覆盖率为前置条件。

3) 若攻击检测能力等级为“中等”及以上（即攻击技术检出率≥60%）且攻击阻断能力等级为“中等”及以上（即攻击技术阻断率≥60%），但战术/技术/子技术数量或 ATT&CK 矩阵覆盖率未达到测试方与被测方的约定值，则应增加攻击方案，直至战术/技术/子技术数量或 ATT&CK 矩阵覆盖率达到约定值，并重新根据攻击技术检测能力等级或攻击技术阻断能力等级判定结果，对本次安全测评判通过与否做出判定。

4) 若已知攻击方案或现有测试手段所涉及的战术/技术/子技术数量或 ATT&CK 矩阵覆盖率无法达到测试方与被测方的约定值，则测试方与被测方应重新协商约定值，并重新进行测试结果判定。

11 测评总结

11.1 测试反馈

为保证评估的透明性和公开性，测试反馈应满足以下要求：

a) 测试反馈环节应贯穿整个 ATT&CK 评估服务的流程；
b) 各环节中的流程和工作成果都会输出相关报告；
c) 应反馈当次测评攻击向量选取问题，计算本次测评的攻击成功率等，优化攻击组织和工具选择。

11.2 测评后处置

安全测评后，应进行测评流程评估，并产出测评处置报告。

a) 测评流程评估应采用但不限于以下步骤：
   1) 制定评估方案
   测评流程评估主要针对测评流程的质量、价值、风险进行综合评估。
   2) 制定测评处置评估表
   根据评估方案，定义评估指标，制定测评处置评估表。
   3) 获取和分析监测数据
   根据网络靶场环境的实时监控，获取和分析测评环境和测评目标的各种数据，并依赖网络靶场环境的知识库，基于网络安全漏洞、攻击等知识和 ATT&CK 框架，结合场景知识图谱、融合安全事件、复合安全事件和技战术匹配等在线分析检测，进行处置评估分析。
   4) 输出评估结果
   根据评估分析，完成处置评估表。
b) 测评处置报告主要包含但不限于以下要素：
   1) 应包含测评处置方案、人员组织等概述；
   2) 应包含测评处置的测评项目、时间等介绍；
   3) 应包含对安全测评流程评估列表、评估明细和结果；
   4) 应包含安全测评流程完善建议，根据测评流程规范的评估存在的问题，组织测评实施团队对测评流程进行修订和完善；
   5) 应包含安全测评突发处置预案完善建议，根据安全测评事件应急处置工作经验和教训，进一步完善测评处置的相关措施和处置预案。

11.3 差距报告

由报告输出组汇总输出信息，进行差距评估报告总结，应满足以下要求：

a) 针对此次使用的攻击技术进行全面剖析，从收集数据源的广度、深度，检测平台测试用例的检测效果进行综合评估；
b) 根据攻击技术的威胁程度和攻击技术综合检测评分；
c) 应给出短期和长期工作改进计划。

附 录 A
（资料性）
ATT&CK 框架的战术阶段

表 A.1 ATT&CK 框架（V12 版本）的战术阶段

对应编号	阶段名称	描述
TA0043	侦察	侦察是攻击者主动或被动收集可用于支持目标定位的信息的技术阶段。
TA0042	资源开发	资源开发是攻击者试图掌握可以用来支持下一步行动的资源。
TA0001	初始访问	初始访问是攻击者将在企业环境中的落脚点。想要尽早终止攻击，那么“初始访问”将是一个很合适的起点。
TA0002	执行	执行战术是应用最过于广泛，当利用现有恶意代码时，都属于“执行”。
TA0003	持久化	攻击者尽量缩小控制控制对象成本的战术。即便运维人员采取重启、更改凭据等措施后，持久化仍然可以让计算机再次感染病毒或维护其现有连接。
TA0004	权限提升	攻击者用来在系统或网络上获取更高级别权限的技术。常见方法是利用系统漏洞，配置错误和漏洞。
TA0005	防御绕过	攻击者在整个进攻过程中避免被发现的技术。用于防御规避的技术包括卸载/禁用安全软件或混淆/加密数据和脚本。攻击者也会利用和滥用受信任的进程来隐藏和伪装他们的恶意软件。
TA0006	凭据访问	用于窃取凭据（例如帐户名和口令）的技术。包括密钥记录或凭据转储。使用合法的凭证可以访问被攻击系统，使其更难被发现，并提供创建更多帐户以帮助实现目标的机会。
TA0007	发现	用来获取有关系统和内部网络知识的技术。
TA0008	横向移动	攻击者用来进入和控制网络上的远程系统的技术组成。
TA0009	收集	用来收集信息的技术，并且从中收集与贯彻攻击者目标有关的信息来源。 通常，收集数据后的下一个目标是窃取（泄露）数据。
TA0011	命令与控制	输出渗出包含攻击者可能用来从网络中窃取数据的技术。
TA0010	数据渗出	被黑客入侵造成系统失常或信息泄露
TA00040	影响	影响包括攻击者用来通过操纵业务和运营流程来破坏可用性或损害完整性的技术。 用于影响的技术可以包括破坏或篡改数据。

附 录 B
（资料性）
测评人员知识和技能要求

以下是基于攻击技战术模型执行安全测评的测评人员的知识和技能要求，可适用于对安全测评人员的培养参考。

a) 通用知识和技能要求

1) 基于攻击技战术模型的安全测评人员应至少具备以下的通用知识：

- 网络安全基础知识（知识领域代码：K01）；

[来源：《信息安全技术 网络安全从业人员能力基本要求》（征求意见稿）]

- ATT&CK 攻击知识库基本知识，包括企业网络、移动网络和工业控制系统的 ATT&CK 战术、技术和子技术等基本知识；

2) 如果安全测评涉及具体行业或者领域，还需具备相应的专业领域知识：

- 新技术新应用安全（知识代码：K10-001）相关知识；
- 特定行业网络安全知识（知识代码：K10-002）相关知识；

[来源：《信息安全技术 网络安全从业人员能力基本要求》（征求意见稿）]

3) 基于攻击技战术模型的安全测评人员应至少具备以下的通用技能：

- 能够与组织内部和/或外部沟通与协调（技能代码：S01-01）；
- 能够理解组织业务（技能代码：S01-02）；
- 能够建立和/或执行网络安全相关制度、策略或机制（技能代码：S01-03）；

[来源：《信息安全技术 网络安全从业人员能力基本要求》（征求意见稿）]

- 能够理解和应用基于攻击技战术模型的安全测评标准体系；

b) 专业知识和技能要求

1) 环境搭建人员

基于攻击技战术模型进行安全测评的环境搭建人员应至少具备以下的专业知识：

- 密码技术、密码产品及服务功能及原理（知识代码 K09-001）；
- 数据安全管理和技术（知识代码 K03-001），包括数据安全基本概念、数据安全技术等；
- 个人信息保护管理和技术（知识代码 K03-002），包括个人信息保护技术、工具等；

网络产品原理与应用知识（知识代码：K06）领域中的：

- 网络设备功能及原理（知识代码 K06-002），包括交换机、路由器等网络设备工作原理、配置及网络架构设计相关知识；
- 网络安全产品功能及原理（知识代码 K06-003），包括网络安全产品原理及应用（防火墙、入侵检测、网闸、VPN 等）；

[来源：《信息安全技术 网络安全从业人员能力基本要求》（征求意见稿）]

- 网络仿真方法和技术，包括 vyos、openvpn 等常见网络仿真软件原理和功能、及其配置和使用方法，常见的企业、校园、数据中心等领域的网络架构；
- 软件系统仿真方法和技术，包括虚拟机、容器等虚拟机技术原理和功能，vmware、openstack、kubernetes 等常用虚拟化、容器软件的配置和使用方法；
- 安全防护仿真方法和技术，包括 vyos、snort、pfsense 等常见安全产品仿真软件原理和功能，以及配置和使用方法，防火墙、入侵检测、防病毒软件、WAF 和 VPN 等常见的业界主流安全产品的配置和使用方法；

基于攻击技战术模型进行安全测评的环境搭建人员应至少具备以下的专业技能：

- 能够对被测评方的目标系统进行信息收集和分析；
- 能够基于攻击技战术模型的安全测评标准，以及收集的目标系统信息，制定目标系统仿真方案，或者与目标相同互联方案，以及攻击测试环境搭建方案；
- 能够基于攻击技战术模型的安全测评标准，完成对目标系统仿真环境的搭建；
- 能够基于攻击技战术模型的安全测评标准，完成对攻击测试环境的搭建；
- 能够维护仿真环境和攻击测试环境的正常运行；

2) 攻击测试人员

基于攻击技战术模型进行安全测评的攻击测试人员应至少具备以下的专业知识：

- 密码技术、密码产品及服务功能及原理（知识代码 K09-001）；
- 数据安全管理和技术（知识代码 K03-001），包括数据安全基本概念、数据安全技术等；
- 个人信息保护管理和技术（知识代码 K03-002），包括个人信息保护技术、工具等；

网络产品原理与应用知识（知识领域代码：K06）领域中的：

- 网络安全产品功能及原理（知识代码 K06-003），包括网络安全产品原理及应用（防火墙、入侵检测、网闸、VPN 等）；
- 操作系统安全原理及使用（知识代码 K06-004）；
- 中间件安全原理及使用（知识代码 K06-005）；
- 数据库安全技术及使用（知识代码 K06-006）；

网络安全开发及测试技术知识（知识领域代码：K05）领域中的：

- 网络安全威胁和漏洞管理（知识代码 K05-003），包括威胁和漏洞概念、漏洞的发现、利用等技术和方法；
- 安全测试、评估方法（知识代码 K05-004），包括常用测试和评估方法，如黑盒测试、灰盒测试、白盒测试及压力测试等；
- 渗透测试方法和技术（知识代码 K05-005），包括 Web 安全、中间件、数据库等常见安全漏洞及利用方法，内网安全渗透测试知识，常用渗透测试工具等；
- 网络攻防技术（知识代码 K05-006），包括网络攻击原理、常见攻击方法、攻击技术和攻击后果，以及防御措施；

[来源：《信息安全技术 网络安全从业人员能力基本要求》（征求意见稿）]

- 复杂攻击技术，ATT&CK 攻击知识库中常见威胁组织的复杂攻击方法，以及常见攻击模拟工具的原理、功能和使用方法；

基于攻击技战术模型进行安全测评的攻击测试人员应至少具备以下的专业技能：

- 能够对被测评方的目标系统进行攻击测试相关的信息收集和分析；
- 能够基于攻击技战术模型的安全测评标准，对目标系统制定测评攻击方案；
- 能够基于测评攻击方案，选择模拟攻击工具；
- 能够基于测评攻击方案，完成攻击实施；
- 能够基于攻击技战术模型的安全测评标准，以及组织的规章制度要求，完成对攻击结果的记录；

3) 检测评估人员

基于攻击技战术模型进行安全测评的检测评估人员应至少具备以下的专业知识：

- 密码技术、密码产品及服务功能及原理（知识代码 K09-001）；
- 数据安全管理和技术（知识代码 K03-001），包括数据安全基本概念、数据安全技术等；
- 个人信息保护管理和技术（知识代码 K03-002），包括个人信息保护技术、工具等；

网络产品原理与应用知识（知识领域代码：K06）领域中的：

- 操作系统安全原理及使用（知识代码 K06-004）；

- 中间件安全原理及使用（知识代码 K06-005）；
- 数据库安全技术及使用（知识代码 K06-006）；

网络安全开发及测试技术知识（知识领域代码：K05）领域中的：

- 网络安全威胁和漏洞管理（知识代码 K05-003），包括威胁和漏洞概念等；
- 安全测试、评估方法（知识代码 K05-004），包括常用测试和评估方法，如黑盒测试、灰盒测试、白盒测试及压力测试等；
- 网络攻防技术（知识代码 K05-006），包括网络攻击原理、常见攻击方法、攻击技术和攻击后果，以及防御措施；

[来源：《信息安全技术 网络安全从业人员能力基本要求》（征求意见稿）]

- 基于攻击技战术模型的安全测评标准体系中的风险评估原理和方法；
- 基于攻击技战术模型进行安全测评的检测评估人员应至少具备以下的专业技能：
- 能够基于攻击技战术模型的安全测评标准，识别测评目标的资产、威胁、脆弱性和已有安全控制措施；
- 能够基于攻击技战术模型的安全测评标准，对攻击测试记录结果进行量化评估；
- 能够根据评估结果，以及组织的相关规章制度，编制评估报告；

4) 报告输出人员

基于攻击技战术模型进行安全测评的报告输出人员应至少具备以下的知识：

- 网络安全认证认可（知识代码：K02-005）；

[来源：《信息安全技术 网络安全从业人员能力基本要求》（征求意见稿）]

基于攻击技战术模型进行安全测评的报告输出人员应至少具备以下的专业技能：

- 能够基于攻击技战术模型的安全测评标准，以及组织规章制度要求，对测评全生命周期记录结果进行分析，并编制测评报告；

5) 测评仲裁人员

基于攻击技战术模型进行安全测评的测评仲裁人员应至少具备以下的专业知识：

- 质量管理知识，包括关于 ISO9000 质量管理相关知识，安全测评项目质量监督、审核的概念和方法；

基于攻击技战术模型进行安全测评的测评仲裁人员应至少具备以下的专业技能：

- 能够基于攻击技战术模型的安全测评标准和组织规范，对测评结果进行监督或者判决。

附 录 C
（资料性）
目标场景搭建基本步骤

C.1 目标网络拓扑准备

目标网络拓扑准备包括创建工程、编辑拓扑、目标网络部署三大任务。

a） 创建工程

创建工程需要输入工程名称、描述、规模、参考模板。

b） 编辑拓扑

拓扑编辑主要包括节点的编辑、边的编辑、节点信息的编辑。

c） 目标网络部署

执行部署并查看部署状态。

d） 关联工程

1) 点击关联工程；
2) 选择关联场景；
3) 绑定；
4) 点击就绪。

C.2 路由脚本配置及下发

1) 编写路由脚本；
2) 将配置好的脚本下发到路由器。

附 录 D
（资料性）
攻击场景特殊性要求

D.1 概述

基于测评场景的攻击技战术构建，安全测评团队应根据不同场景的特殊性构建差异化的攻击技战术。以下从企业场景、工业控制系统场景、移动终端场景、以及金融行业场景的特殊性进行阐述。

D.2 企业场景

企业场景主要涉及网络安全、系统安全。ATT&CK 框架中针对企业场景，总共有 14 项战术、222 项技术。其中攻击过企业场景的 Wizard Spider + Sandworm APT 覆盖了 11 项战术、105 项技术；Carbanak + FIN7 APT 覆盖了 11 项战术、71 项技术。

D.3 工业控制系统场景

相比于传统安全，工业控制系统安全具备以下三个差异特点：

a) 一是防护对象扩大，安全厂家更丰富。传统互联网更多关注网络设施、信息系统软硬件以及应用数据安全，工业控制系统安全扩展延伸至工厂内部，包含设备安全（工业智能装备及产品）、控制安全（SCADA、DCS 等）、网络安全（工厂内、外网络）、应用安全（平台应用、软件及工业 APP 等）以及数据安全（工业生产、平台承载业务及用户个人信息等数据）。
b) 二是连接范围更广，威胁延伸至物理世界。传统互联网按权重，攻击对象为用户终端、信息服务系统、网站等。工业互联网联通了工业现场与互联网，使网络攻击可直达生产一线。
c) 三是网络安全和生产安全交织，安全事件危害更严重。传统互联网安全事件大多表现为利用病毒、木马、拒绝服务等攻击手段造成信息泄露或篡改、服务中断等，影响工作生活和社会活动。而工业控制系统一旦遭受攻击，不仅影响工业生产运行，甚至会引发安全生成事故，给人民生命财产造成严重损失，若供给发生在能源、航天航空等重要领域，还将危害国家总体安全。

ATT&CK 框架中的针对工业控制系统的技战术，总共有 12 项战术、88 项技术。其中攻击过工业控制系统的 Triton APT 覆盖了 10 项战术、17 项技术。

D.4 移动终端场景

相比于网络安全，移动终端安全的特殊性在于通信加密、重打包、脱壳、apk 解包、OS 本身的特性等。

ATT&CK 框架中的针对移动终端的技战术，总共有 12 项战术、78 项技术。

D.5 金融行业场景

通过统计 ATT&CK 框架中攻击过金融行业的 APT 组织所使用的技术，可得出有 14 项战术、94 项技术被这些 APT 组织使用过，其中使用频率最高的 10 项技术为命令和脚本解释器、网络钓鱼、用户执

行、混淆文件或信息、签名的二进制代理执行、有效账户、应用层协议、主机指示符删除、入口工具转移、远程服务。

APT 组织对金融行业进行攻击时，较为常见的方式有：利用钓鱼及有效账户进行初始访问，使用命令和脚本解释器以及用户执行进行执行，使用有效账户进行持久化、特权提升，使用混淆文件或信息、签名的二进制代理执行、主机指引删除及有效账户进行防御绕过，使用远程服务进行横向移动，使用应用层协议及入口工具转移进行命令控制。

金融行业较为典型的攻击方案为：

a) 利用钓鱼发现有效账户-使用有效账户登录-使用混淆文件或信息等进行防御绕过-使用远程服务进行横向移动-进一步实现目的。

b) 通过信息收集发现有效账户-使用有效账户登录-使用签名的二进制代理执行等进行防御绕过-使用应用层协议等进行命令控制-进一步实现目的。

附 录 E

检测评估统计表

表 E.1 检测评估统计表

战术阶段	攻击技术实施数	攻击技术检出数	攻击技术阻断数	攻击技术检出率	攻击技术阻断率
侦察					
资源开发					
初始访问					
执行					
持久化					
权限提升					
防御绕过					
凭据访问					
发现					
横向移动					
收集					
命令与控制					
数据窃取					
危害					

参 考 文 献

[1] GB/T 25069-2022 信息安全技术 术语

[2] GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

[3] GB/T 24363-2009 信息安全技术 信息安全应急响应计划规范

[4] GB/T 37696-2019 信息技术服务 从业人员能力评价要求

[5] GB/T 20984-2007 信息安全技术 信息安全风险评估规范

[6] GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南

[7] GB/T 19001-2016 质量管理体系 要求

[8] GB/T 27400-2020 合格评定 服务认证技术通则

[9] 国家职业技能标准 职业编码：4-04-04-04 信息安全测试员

[10] X2-02-34-08 企业培训师国家职业标准

[11] 国家标准《信息安全技术 网络安全从业人员能力基本要求》（征求意见稿）

[12] RB/T 203-2018 中华人民共和国认证认可行业标准 — 信息安全领域检验检测机构安全管理要求

[13] ISO/IEC 19896-1：2018 IT security techniques — Competence requirements for information security testers and evaluators — Part 1：Introduction, concepts and general requirements

[14] ISO/IEC TS 17027:2014 Conformity assessment — Vocabulary related to competence of persons used for certification of persons

[15] https://attackevals.mitre-engenuity.org/

[16] http://www.pentest-standard.org/index.php/