ICS 35.24
CCS L70

YD

中华人民共和国通信行业标准

YD/T [××××××]—[××××]
[代替 YD/T]

网络安全众测平台第三方安全审计技术要求

Technical specifications for third-party security audit of network security crowdsourced testing platforms

[点击此处添加与国际标准一致性程度的标识]

（报批稿）

[点击此处添加本稿完成日期]

[××××]-[××]-[××]发布　　[××××]-[××]-[××]实施

中华人民共和国工业和信息化部　发布

目　　次

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。

本文件属于网络安全众测系列标准之一，该系列标准包括：

YD/T 3744 网络安全众测平台技术要求

YD/T 3745 网络安全众测服务管理要求

YD/T XXXX 网络安全众测平台第三方安全审计技术要求

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这些专利的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：国家计算机网络应急技术处理协调中心、上海斗象信息科技有限公司、阿里云计算有限公司、北京奇虎科技有限公司、北京东方通网信科技有限公司、中国信息通信研究院、杭州安恒信息技术股份有限公司。

本文件主要起草人：王晖、张奇、肖佃艳、吕梦凡、邹潇湘、张屹、吴昊、姚一楠、景慧昀、崔婷婷、范乐君、王文磊、邹昕、王博、舒敏、李政、张大江、俞斌、李其蓉。

网络安全众测平台第三方安全审计技术要求

1 范围

本文件规定了网络安全众测平台的第三方审计业务场景、工作流程、主要任务和技术要求。

本文件适用于参与网络安全众测服务的个人、组织和机构，也可以作为网络安全主管部门进行监督、检查的依据。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

YD/T 3744-2020 网络安全众测平台技术要求

YD/T 3745-2020 网络安全众测服务管理要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全众测平台 cybersecurity crowdsource testing platform

组织或机构依托其安全经验，通过互联网建立一个安全测试协作平台，组织授权测试实体，规范并监督安全测试过程，对签约众测需求方提供安全渗透测试与漏洞发现等服务。

3.2

授权测试实体 authorized test entity

不恶意利用漏洞进行破坏或通过漏洞获得非法利益的白帽子黑客或安全公司，包括通过利用自身的技术在客户授权的前提下对测试目标进行安全测试，帮助客户查找计算机系统或网络系统的漏洞、向众测需求方报告并配合修复，确保众测需求方系统安全。

3.3

众测需求方 crowdsource testing demand-side

安全测试需求企业与网络安全众测平台签订授权测试协议，并同意平台授权给授权测试实体进行安全测试的实体统称。

3.4

第三方审计 third-party audit

对授权测试实体测试过程产生的日志信息，进行外部独立审计的组织机构。审计目的是确定测试过程是否存在恶意破坏等高风险行为。

3.5

安全审计 security audit

对信息系统的各种事件及行为实行监测、信息采集、分析，并针对特定事件及行为采取相应的动作。

4 缩略语

下列缩略语适用于本文件。

ARP：地址解析协议（Address Resolution Protocol）

DNS：域名系统（Domain Name System）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket Layer）

ICMP：控制报文协议（Internet Control Message Protocol）

IGMP：网际组管理协议（Internet Group Management Protocol）

POP3：邮局协议版本3（Post Office Protocol - Version 3）

TCP：传输控制协议（Transmission Control Protocol）

UDP：用户数据报协议（User Datagram Protocol）

DDoS：分布式拒绝服务攻击（Distributed Denial of Service）

APT：高级可持续威胁攻击（Advanced Persistent Threat）

5 安全审计描述

5.1 需求描述

针对众测需求方要求引入第三方审计机构的网络安全众测服务项目，网络安全众测平台应协助众测需求方和第三方审计机构，对授权测试实体的测试行为进行审计，主要包括：连接审计系统后再进行测试；记录测试人员的测试行为及测试流量，以备后期取证；审计授权测试实体是否有未授权的入侵网络、干扰网络正常功能、窃取网络数据等危害网络安全的行为或活动，对整个测试过程进行控制。

5.2 业务场景

5.2.1 应用识别

基于对授权测试实体的测试流量进行采集、过滤、整形，并对测试流量进行关联分析，有效的识别授权测试实体对众测需求方测试的过程中所使用的应用情况。

5.2.2 网络协议解析

第三方审计基于对众测过程流量捕获、协议解析、协议转存实现无丢失抓包、存包。通过安全策略设置有效发现异常流量，并通过预先设置好的应对策略，对网络协议流量进行处理。

5.2.3 异常行为发现

授权测试实体在众测过程中，可能会对众测需求方进行高风险操作，如服务器提权、拖库等行为。授权测试实体在进行高风险操作时，其行为会和正常的众测行为基线存在差异。因此，可以通过对授权测试实体的监测以及众测行为的管理，及时发现异常行为，从而及时进行告警。

5.2.4 安全溯源

安全溯源是指当攻击、仿冒等网络事件发生以后，能根据与此相关的例如日志记录、时间等信息，找到引发事件的实体。而在网络安全众测流量审计中，可以针对授权测试实体进行身份识别，同时对其网络痕迹进行还原。

5.3 工作流程

第三方安全审计工作流程分为：

a) 审计准备阶段：审计立项，明确审计依据，制定审计方案，编制工作计划。
b) 审计实施阶段：第三方审计接入网络安全众测平台、众测需求方进行审计，收集审计内容，开展审计工作，审计结果沟通。
c) 审计终结阶段：撰写审计报告，提交报告。

5.4 主要任务

5.4.1 众测第三方审计任务

在众测第三方审计任务中，审计方根据测试过程中记录的测试流量等内容，对授权测试实体的测试行为和流量进行审计。

本项要求包括：

a) 审计方根据测试过程中记录的测试流量等内容，对授权测试实体的测试行为和流量进行审计。
b) 审计结果应以审计报告的形式交付给众测需求方说明该次安全测试审计情况，帮助网络安全众测平台提升对众测授权测试实体的管控能力。

5.4.2 编写审计报告

第三方审计结束后，审计组应对取得的审计证据进行综合分析，并撰写审计报告，模板参见附录A。主要包括下列内容：

a) 安全审计报告的内容包括但不限于测试范围、测试时间、测试人员、审计内容及审计结果等。
b) 安全审计报告内容应客观、完整、清晰、及时。

6 技术要求

6.1 流量审计

网络安全众测平台的业务流量是指授权测试实体与众测需求方之间的流量。

流量审计是第三方审计需要对网络安全众测平台的业务流量进行实时审计分析。流量审计过程如图1所示。

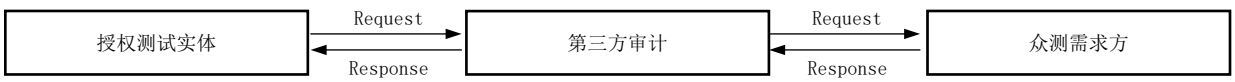

图1　网络安全众测流量审计过程示意图

流量审计主要包括流量接口、流量日志、流量异常、流量数据管控等内容。流量审计协议种类包括但不限于HTTP、HTTPS、TCP、UDP、ICMP、IGMP、POP3、ARP、DNS等。

流量审计要求包括：

a) 流量接口：第三方审计机构应对网络安全众测平台进行众测中的流量数据接口的规范性及流量走向等进行审计。

b) 流量日志：第三方审计机构对安全测试目标过程中的所有流量日志进行留存，应保存 6 个月以上，用于后续流量分析、审计、备查等。

c) 流量异常：建立网络安全众测平台或用户的正常流量基线，发现异常流量（包括但不限于上传恶意文件、拖库、篡改信息等）。

d) 流量数据管控: 对安全测试流量进行格式整理和切片处理，并按照项目、时序、测试人员等维度将流量进行切片，整理、筛选后，形成行为分析模型能够读取的格式。

6.2　行为审计

行为审计是指对网络行为进行实时监督、响应和记录，从而发现异常行为并给予快速处理。

行为审计包括授权测试实体行为审计、网络安全众测平台行为审计。

授权测试实体行为审计要求包括：

a) 对授权测试实体拖库、服务器提权等未授权行为进行监督。

b) 通过对授权测试实体在线时长、次数、流量、时段、访问目标、访问频次、访问时长等的统计，分析授权测试实体的行为特征、可信程度等。

c) 对授权测试实体的高风险行为如撞库攻击、批量账号登录、扫描器攻击，未授权下载和上传后门等进行回溯分析。

网络安全众测平台行为审计要求包括：

a) 网络安全众测平台的网络行为、管理行为应遵循 YD/T 3744-2020 及 YD/T 3745-2020 的相关要求。

b) 网络安全众测平台应遵循 YD/T 3744-2020 第 6 章 6.1 节及 YD/T 3745=2020 第 8 章的相关规定进行用户数据隔离、数据库加固、身份鉴别、访问控制、资源监控等。

6.3　内容审计

内容审计是指在审计行为经用户和系统授权的前提下，对平台流量报文的净荷进行深度分析、信息还原，防止隐私泄露等。

内容审计包括测试内容审计、测试报告内容审计、网络安全众测平台内容审计。

内容审计要求包括：

a) 测试内容审计：对测试内容进行审计分析，以防止用户隐私、敏感数据等泄露。

b) 测试报告内容审计：对授权测试实体提交的测试报告内容进行分析过滤，保障测试报告的专业性、漏洞等敏感数据的保密性等。

c) 网络安全众测平台内容审计：对网络安全众测平台传输的报文内容进行审计分析，对数据进行保密性、完整性检验等。

6.4　威胁审计

威胁审计是对网络流量进行解析，以发现并处置相关威胁，并且对威胁进行实时监测和审计分析。

威胁审计要求抓取授权测试实体对目标测试的行为流量进行威胁情报审计分析，主要包括DDoS攻击、APT攻击、僵尸网络、黑客工具、勒索病毒、挖矿木马、恶意下载、流氓推广、窃密木马、网络蠕虫等。

6.5 人员审计

人员审计是对授权测试实体在文件、履行职责等方面进行审计核实。

授权测试实体相关文件包括但不限于授权测试实体与网络安全众测平台签署的用户及保密协议，基于网络安全众测平台的身份、技能认证等。

人员审计要求包括：

a) 授权测试实体应与网络安全众测平台签署用户及保密协议。

b) 授权测试实体应配合网络安全众测平台完成身份、技能认证。

c) 在测试过程中，应按协议要求，进行安全测试。

附 录 A
（资料性）
网络安全众测第三方审计机构审计报告模板

A.1 审计概述

A.1.1 项目简介

简述审计项目背景及意义、委托方等项目基本情况。

A.1.2 审计依据

分类列出开展审计活动所依据的标准、文件和合同等。
YD/T 3744 信息安全技术 网络安全众测服务管理要求
YD/T 3745 信息安全技术 网络安全众测服务技术要求
YD/T XXXX 网络安全众测平台第三方安全审计技术要求

A.1.3 审计过程

描述审计工作流程、各阶段完成的关键任务和工作时间节点等内容。

A.1.4 报告分发范围

说明网络安全众测审计报告正本份数与分发范围。

A.2 单项审计结果分析

A.2.1 流量审计

A.2.1.1 流量统计

对授权测试实体vpn账户接入的使用情况进行数据统计，形成授权测试实体投入时间，有效测试时长，测试流量分布等描述 。

A.2.1.2 流量接口

针对众测活动中流量数据接口的规范性及流量走向等进行分析。形成被审计对象流量数据接口类型和流量走向描述，给出符合性评价。

A.2.1.3 异常流量

将众测活动中流量与正常流量基线比对，形成众测活动中流量特征描述，给出有无异常流量的评价及对应截图、数据包佐证（包括但不限于上传恶意文件、拖库、篡改信息等）。

A.2.2 行为审计

A.2.2.1 授权测试实体行为审计

针对众测活动中授权测试实体在线时长、次数、流量、时段、访问频次、访问时长、异常操作等进行统计分析。形成授权测试实体特征、行为描述，给出符合性评价。

A.2.2.2 网络安全众测平台行为审计

针对网络安全众测平台在数据传输、数据隔离、数据库加固、身份鉴别、访问控制、资源监控等方面的措施进行评估，形成被审计对象在数据传输、数据隔离、数据库加固、身份鉴别、访问控制、资源监控等方面的保护措施及存在的安全问题描述。

A.2.3 威胁审计

针对授权测试实体对目标测试的行为流量进行威胁情报审计分析，形成包括APT，僵尸网络、黑客工具、勒索病毒、挖矿木马、恶意下载、流氓推广、窃密木马、网络蠕虫等威胁的描述。

A.2.4 人员审计

对授权测试实体与网络安全众测平台签署的用户及保密协议，身份、技能认证，有无违规测试等内容进行统计确认，形成符合性评价表。

A.3 总体评价

根据被审计对象审计结果和审计过程中了解的相关信息，对本次众测活动的安全及规范性进行说明和评价，包括授权测试实体的测试行为的规范性，审计数据的完整性，安全测试流量数据的可信度等。基于综合评价结果对本次众测活动是否符合审计技术要求给出总体结论。

附件 众测流量日志

编制报告必要时或按照众测需求方要求，附上相关流量日志内容。