ICS 35.110
CCS M 11

YD

中 华 人 民 共 和 国 通 信 行 业 标 准

YD/T XXXX—202×

网络空间安全仿真 网络安全检测指南

Cybersecurity emulation — Technical guide for network range safety detection

2020-××-××发布　　2020-××-××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。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：华为技术有限公司、北京启明星辰信息安全技术有限公司、鹏城实验室、广州大学网络空间先进技术研究院、中国电信集团有限公司、湖南大学、桂林电子科技大学、中国电子信息产业集团有限公司第六研究所、四川亿览态势科技有限公司、北京天融信网络安全技术有限公司、博智安全科技股份有限公司、华信咨询设计研究院有限公司。

本文件主要起草人：余晓光、徐家林、杨洪起、行骁程、张赛楠、余滢鑫、毛春雄、李文兴、胡桥、王帅、陶莎、李千目、旷文钟、李振宇、燕玮、刘子健、王龑、毕程、赵谦、傅涛、孙小平、董平、喻朝新、雷琳琳、李丹。

网络空间安全仿真 网络安全检测指南

1 范围

本文件提供了网络空间安全仿真平台运行过程中涉及到的主要安全威胁的检测指南，包括流量检测、文件安全检测、系统行为检测和邮件安全检测。

本文件适用于作为网络空间安全仿真平台环境中安全威胁检测技术的设计、建设的参考指导。

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 XXXX-XXXX 网络空间安全仿真 术语

3 术语和定义

YD/T XXXX-XXXX 界定的术语和定义适用于本文件。

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)
CPU:中央处理器(central processing unit)
DDoS: 分布式拒绝服务攻击(Distributed denial of service attack)
FTP: 文件传输协议(File Transfer Protocol)
HTTP: 超文本传输协议(Hypertext Transfer Protocol)
ICMP: 网际报文控制协议(Internet Control Message Protocol)
IP:互联网协议(Internet Protocol)
IMAP: 因特网消息接入协议(Internet Message Access Protocol)
MAC: 介质访问控制层(Media Access Control)
POP3: 第三版电子邮局协议(Post Office Protocol Version 3)
RIP: 路由信息协议(Routing Information Protocol)
SMTP: 简单邮件传输协议(Simple Mail Transfer Protocol)
SNMP: 简单网络管理协议(Simple Network Management Protocol)
SQL: 结构化查询语言(Structured Query Language)
TCP: 传输控制协议(Transmission Control Protocol)
UDP: 用户数据报协议(User Datagram Protocol)
URL：统一资源定位系统（Uniform Resource Locator）

5 检测技术框架

本文件主要从流量检测技术、文件安全检测技术、系统行为检测技术、邮件安全检测技术介绍网络空间安全仿真平台运行环境的安全检测的技术方法和指南，其中数据采集和数据分析属于前述安全检测内容中各自参考采取的检测技术方法。

网络空间安全仿真平台运行环境总体安全检测技术参考框架如图1所示。

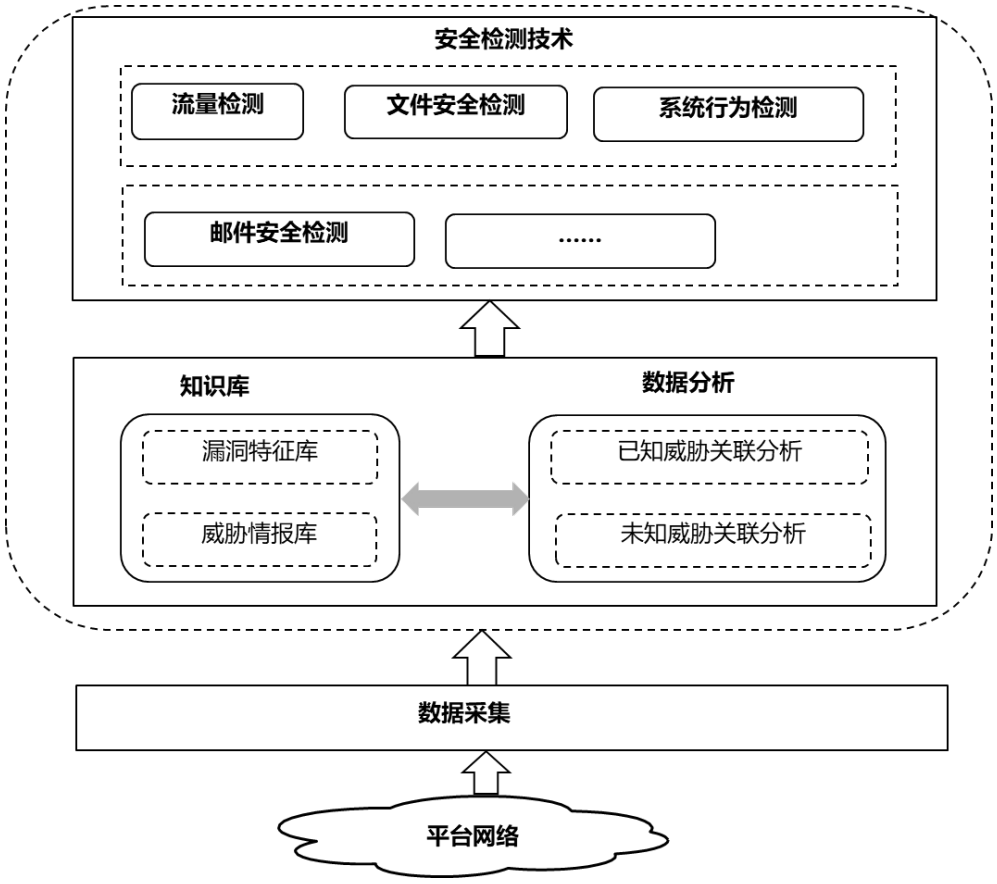

图1 安全检测技术框架

框架中流量检测、文件安全检测以及系统行为检测是目前对网络空间安全仿真平台运行环境所采用的通用检测技术，邮件安全检测属特殊检测场景。

6 流量检测

6.1 流量检测流程

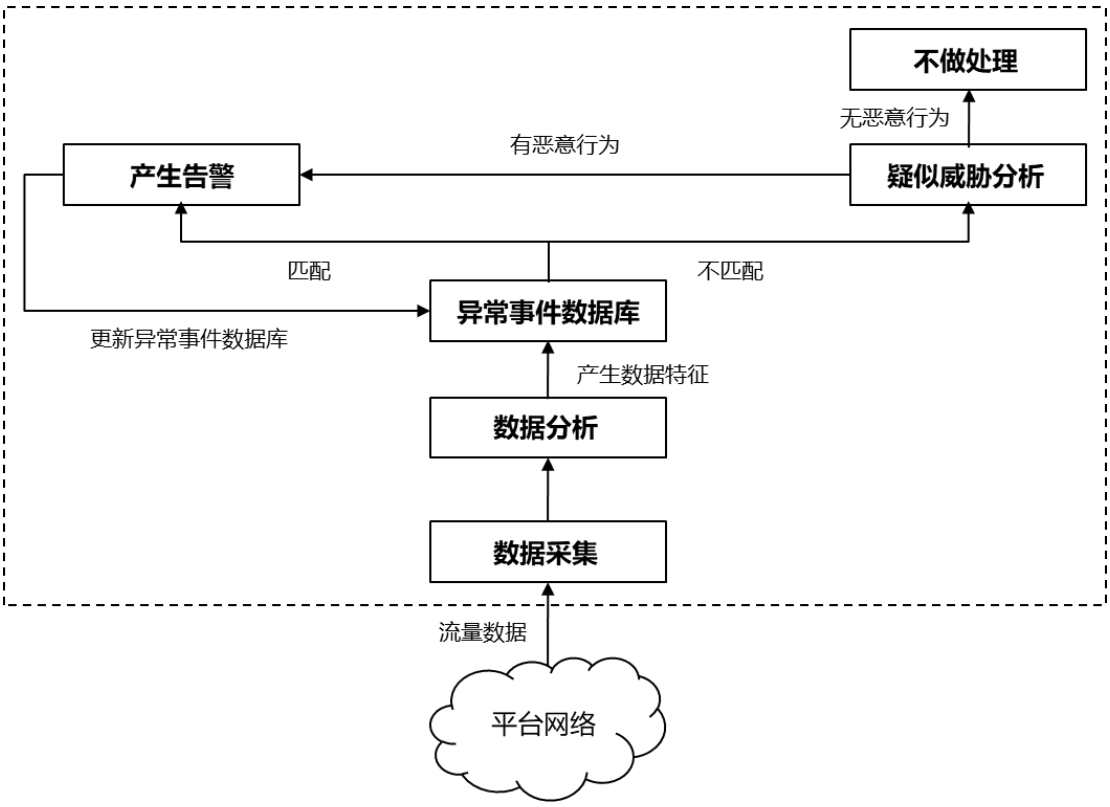

图 2 流量检测流程

如图 2 所示，流量异常检测技术主要由数据采集、数据分析、异常事件数据库、疑似威胁分析模块组成。其中，异常事件数据库中存储了大量攻击行为的数据特征，包括：端口扫描、拒绝服务攻击、缓冲区溢出攻击、通过移动热插拔设备对系统进行的攻击、木马后门攻击、恶意代码攻击、反序列化攻击、文件脆弱性攻击、浏览器脆弱性攻击、应用层安全漏洞攻击等。同时存储了各类欺骗行为的数据特征，如 IP 碎片化、协议端口重定向等。而疑似威胁分析模块中主要用于在异常事件数据库判断无异常后，再分辨数据流量是否有恶意行为，以便发现恶意攻击行为的早期铺垫动作。

流量检测技术基本流程包括：

a) 由数据采集模块采集指定网段、指定时间内的外部网络与网络空间安全仿真平台之间的流量，并送往数据分析模块；

b) 数据分析模块分析流量协议及内容信息，根据流量数据特征，与异常事件数据库进行比对，检查是否存在不合规或攻击行为；

c) 对于异常事件数据库匹配的流量生成告警事件，对于异常事件数据库中不匹配的流量存在以下两种情况：

   1) 若判定为正常业务流量则放行

   2) 若判定为非正常流量则送入疑似威胁分析模块进行分析，对于不存在恶意行为的流量放行，对于存在恶意行为的流量则生成告警并更新异常事件数据库

d) 如果同一时间段内出现的同一事件，可将异常事件合并，减少告警次数，避免出现告警风暴。

6.2 流量检测技术

6.2.1 流量协议识别

能识别以下常见网络协议：IP、TCP、UDP、ICMP、ARP、RIP、HTTP、FTP、IMAP、SNMP、SMTP、POP3。

对以上各类协议进行分析、解码，并提取特征信息，异常检测技术可以识别和分析流量协议的客户端和服务端对象、类型、内容。

6.2.2 流量分析

对网络内不同主机、不同类型的检测目标进行分析，发现入侵事件。

通过时间、系统状态等对一系列事件对流量进行关联分析，发现低危害事件中隐含的高威胁性攻击行为。

6.2.3 检测能力

6.2.3.1 异常检测

异常检测包括以下异常动作：端口扫描、拒绝服务攻击、缓冲区溢出攻击、通过移动热插拔设备对系统进行的攻击、木马后门攻击、恶意代码攻击、反序列化攻击、文件脆弱性攻击、浏览器脆弱性攻击、应用层安全漏洞攻击等。

6.2.3.2 疑似异常流量检测

安全流量检测技术不仅区分异常流量与正常流量，同时通过各类技术对疑似异常流量做出检测、告警。

6.2.3.3 特定流量监测

特定流量异常检测技术对整个网络环境或上述某一特定协议、特定异常的场景进行流量监测，监测内容包括：协议、流量源目地址、流量大小。

6.2.3.4 异常事件合并

异常事件合并技术具有对高频度发生的相同事件进行合并告警，避免出现告警风暴的能力。高频度阈值由授权管理员设置。

6.2.3.5 防躲避能力

防躲避能力指能够发现躲避或欺骗检测的行为，如 IP 碎片分片、TCP 流分段、URL 字符串变形、shell 代码变形、协议端口重定向等。

7 文件安全检测

7.1 文件安全检测流程

文件安全威胁检测主要是基于内容的检测技术，包括对文件的预处理、文件内容哈希特征匹配和基于模型监测三个步骤，文件安全检测流程如图 3 所示。

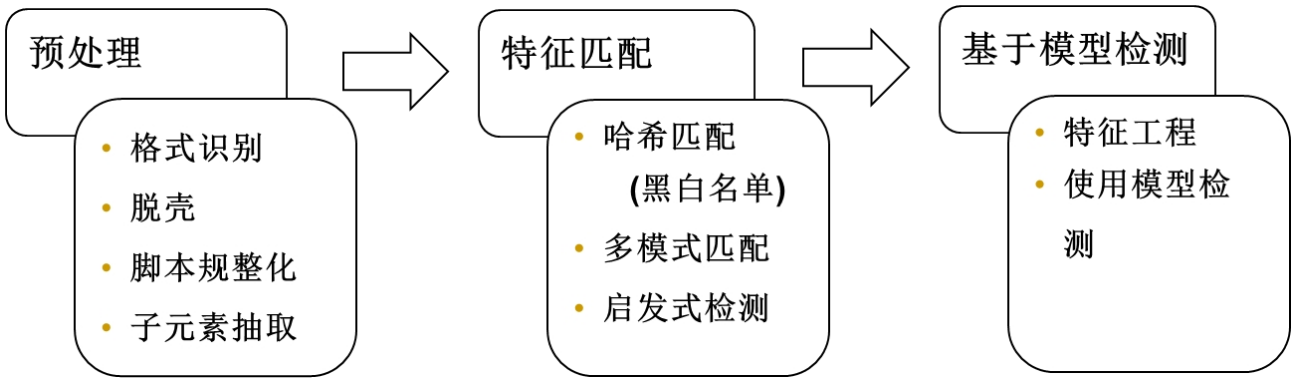

图 3 文件安全检测流程

对于需要检测的文件对象预处理，可参照如下步骤：

a) 基于文件头部、关键字、字符频率以及特殊位置内容等特征进行格式识别；

b) 通过静态或动态脱壳技术解压缩或解保护进行脱壳；

c) 通过脚本规整化增加特征覆盖度；

d) 通过抽取可能包含威胁的 URL、子文件、脚本等元素进行文件预处理。

文件预处理后，通过计算文件内容的哈希值，并通过多种模式匹配威胁情报库中，以实现具备威胁的文件检测。

除此之外，对恶意文件的检测，还可以通过特征工程、模型检测等基于模型检测方法实现文件安全威胁库的快速更新。

7.2 文件安全检测技术

7.2.1 文件内容检测

文件内容检测针对文件内容进行解析，匹配特征语句从而检测系统文件中是否包含僵尸病毒、木马、蠕虫、特定 shell、文件后门、流氓软件、恶意广告或者恶意程序。

7.2.2 非授权访问检测

非授权访问检测依据业务系统提供的日志和访问权限控制名单，设定判断规则进行分析处理。同时，对系统中的文件进行权限设置检测，从而判断文件权限设置是否符合安全设计需求。

7.2.3 人为失误/硬件故障检测

人为失误依据上报机制进行被动检测。

硬件故障检测依据上报被动检测加上特征主动检测。例如处理器崩溃导致的进程终止，既可依据处理人上报，也可依据 CPU 占用率变化特征进行判断。

7.2.4 文件运维巡检

文件运维巡检包括：

a) 针对文件丢失、篡改及损坏威胁，对文件完整性进行检测，对系统中的文件/目录建立校验码库，方便对文件完整性进行常态化检测；

b) 进行文件备份检测，可以与文件完整性检测同时进行，确保重要文件备份同步；

c) 进行文件销毁检测，可从销毁接口日志中同步销毁信息和定位销毁目标，并对销毁结果进行检测。

8 系统行为检测

8.1 检测方法及流程

基于用户和实体行为的异常和威胁检测方法如图 4 所示。

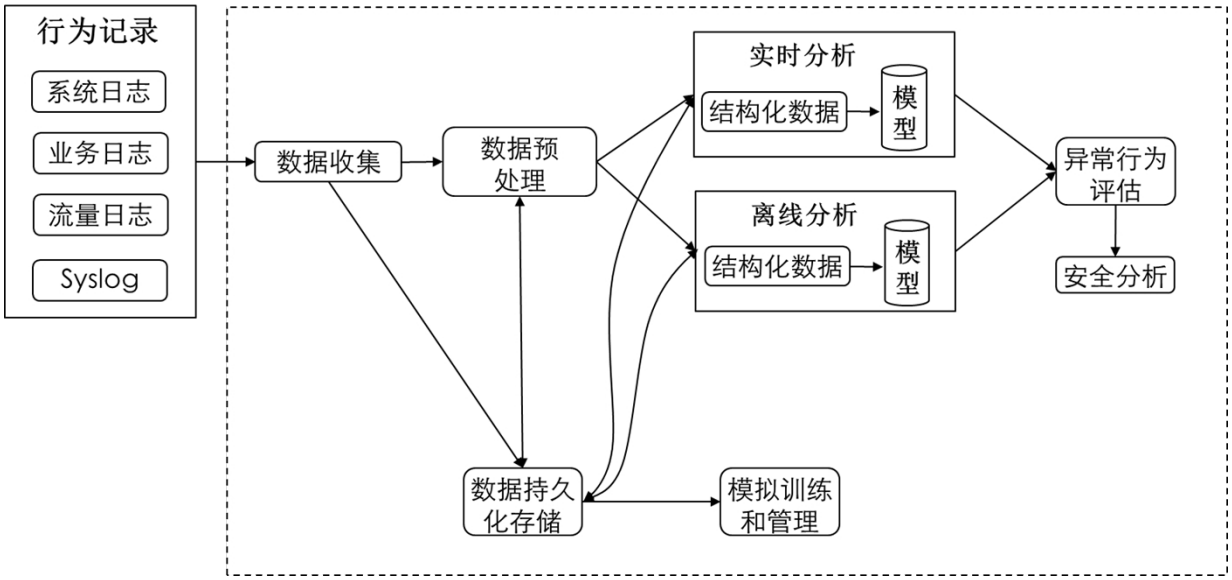

图 4 异常行为检测流程

基于系统异常行为的分析首先可以借助信息和日志管理类工具收集各种行为记录，例如系统日志、业务日志、流量日志、网络设备 syslog 等。然后通过数据预处理对收集的各类数据进行结构化处理抽取有价值信息。再通过实时分析或离线分析等检测与分析部件，对照提前学习得到的正常行为基线和通过威胁建模得到的威胁行为模型，对预处理过的数据进行实时和离线的异常行为检测与分析，对于检测到的异常行为再通过异常行为评估部件根据统计模型（如数量和概率等）进行威胁行为评估，最终基于检测与分析的威胁结果进行安全分析和处理。

8.2 行为检测技术

8.2.1 行为属性识别

系统行为检测技术主要检测系统能够识别主机行为、应用系统行为、数据库行为及其他针对网络安全仿真应用场景攻防或作弊行为。

a) 主机行为属性是指对主机产生的注册表、文件、进程等行为信息，包括创建、设置、删除注册表的键、值，创建、删除、重命名文件及读写特定目录，对主机内存进行相关操作，创建、关闭主机进程、线程；

b) 应用系统行为属性是指对应用系统攻击行为信息，包括暴力破解、缓冲区溢出、认证/会话预测、跨站脚本；拒绝服务、操作系统命令执行、路径遍历、远程文件包含、SQL 注入、WebShell 检测、网络爬虫、可疑文件上传、敏感路径猜测、异常 HTTP 方法、异常客户端请求、异常对象访问、第三方组件访问等；

c) 数据库行为属性是指对数据库操作的行为描述。包括数据库实例、数据库类型，数据库用户、操作系统用户、主机，数据库 IP、客户端 IP，数据库 MAC、客户端 MAC 数据外发，客户端程序、客户端端口，请求发生时间、执行时长，SQL 内容关键字、执行结果等常规审计；多关键字、正则表达式、语句级规则等高级审计；构建行为特征模型，通过检查数据库访问行为与基线的偏差来识别风险。

8.2.2 系统行为检测

8.2.2.1 基于规则的检测分析

提供关联分析功能，具体检测分析内容：

a) 根据行为属性判断攻防行为的级别，根据行为级别、累计发生次数等指标进行综合分析，并对攻防行为进行评估；
b) 根据多个行为属性关联分析出安全事件发生的因果关系，获得与攻防行为相关的攻击源、攻击类型、攻击目的地址、攻击时间，并根据行为属性序列获取攻防路径。

8.2.2.2 基于异常的行为检测

维护网络安全仿真的应用场景下合法用户的正常行为集合，以此区分攻防行为，具体检测分析内容：

a) 访问流量超限（DDoS攻击防护）；
b) 权限异常修改、提升（含应用场景下对账户的增加、删除、修改等；网络安全仿真应用场景下获得远程管理员权限、获得本地管理员权限、获得普通用户访问权限）；
c) 非授权访问、外联；
d) 文件非授权外发、下载；
e) 文件异常修改（含读取受限文件）；
f) 安全策略修改（含应用场景下防护设备/系统/组件的激活、停用）；
g) 日志异常变化（含应用场景下对日志记录的备份、删除）。

8.2.2.3 行为趋势分析

根据时间序列，由历史与当前数据推测攻击者下一步动作数据，以更高效地进行系统行为检测，提供复盘依据和评分辅助依据。

8.2.3 攻防行为评估

对网络安全仿真环境下攻防行为进行评估，对主机操作系统、网络设备、数据库、中间件等 IT 基础设施的行为分析；包括发生攻防行为的资产、资产类型分布，实体账号、特权账号变化，文件、数据流转等，评估攻击类型、攻击方式、攻击路线；防守类型、防守方式等。

9 邮件安全检测

9.1 垃圾邮件识别技术

9.1.1 垃圾邮件识别方法

垃圾邮件识别技术包括基于邮件内容特征和基于邮件连接特征两类，具体识别方法可参考 GB/T 30282-2013 中的 5.1.1.2 和 5.1.1.3。

9.1.2 基于邮件内容特征的垃圾邮件识别

可依据以下邮件内容特征来识别邮件是否为垃圾邮件：

a) 关键字过滤识别:可针对邮件的信头、信体、附件、主题、发件人、收件人、抄送人、正文中包含的文字而设定关键字，从而匹配识别垃圾邮件；
b) 数字特征匹配识别：可设定邮件或附件的大小、附件的数量、收件人总数等数量值，进行匹配识别垃圾邮件；
c) 附件特征匹配识别：根据附件文件名和附件文件类型等特征进行垃圾邮件识别；

d) 能识别出带病毒特征的邮件附件；
e) 其它特征识别。

9.1.3 基于邮件连接特征的垃圾邮件识别

可依据以下邮件连接特征来识别邮件是否为垃圾邮件：
a) 一段时间内同一主题的邮件接收次数；
b) 同一邮件来源 IP 地址对邮件服务端口的最大连接并发数；
c) 一段时间内同一邮件来源 IP 地址对邮件服务端口的最大连接数；
d) 其它连接特征。

9.2 邮件攻击检测技术

9.2.1 协议会话信息检测

在邮件协议层监测暴力破解邮箱账号口令、弱口令、异常登录这三种异常行为：
a) 通过对报文分析，分析账号登录时间地点频率等检测暴力破解账号口令行为；
b) 使用弱口令对邮箱账号进行匹配时及时提示用户；
c) 监测异常行为，在异常时间、地点，短时间登录多个邮箱的 IP 或者多个 IP 登录同一个邮箱。

9.2.2 邮件头信息检测

邮件消息头存在大量的用户的敏感信息，即使攻击者能够伪造正文信息，或者其他邮件头，但是仍然可以通过 received 字段回溯到邮件的历史信息，发现有误异常情况。

9.2.3 URL 链接过滤

攻击者往往发送包含钓鱼链接的 URL 诱导受害者点击，对于邮件中的 URL 链接过滤可通过如下几种方式：
a) 基于域名的特征过滤；
b) 基于页面的特征过滤；
c) 基于内容的特征识别；
d) 在以上信息之外，还需要结合公共反钓鱼平台提供的资源信息。

9.2.4 邮件内容过滤

内容过滤是过滤垃圾邮件的关键步骤，检测垃圾文本与图片，运用到图像分析识别对比等技术。

9.2.5 邮件附件过滤

大量恶意邮件通过附件的形式对受害者造成攻击，附件检测过滤主要对以下文件进行过滤：
a) 可执行脚本检测；
b) Office 文档等常见文件格式；
c) 可移植的可执行的文件检测。

参考文献

[1] GB/T 30282-2013 信息安全技术 反垃圾邮件产品技术要求和测试评价方法

[2] GB/T 29246-2017 信息技术 安全技术 信息安全管理体系 概述和词汇