信息安全研究 第8卷 第7期 2022年7月
Journal of Information Security Research Vol.8 No.7 July 2022
DOI:10.12379/j.issn.2096-1057.2022.07.04

高安全等级系统抗攻击能力测评研究

蒋建春[1] 文伟平[2] 胡陈勇[3]
[1](中国科学院软件研究所 北京 100190)
[2](北京大学软件与微电子学院 北京 100871)
[3](北京中科卓信软件测评技术中心 北京 100193)
(jianchun@iscas.ac.cn)

Research on Evaluation Anti-attack Capability for High Security Level System

Jiang Jianchun[1], Wen Weiping[2], and Hu Chenyong[3]
[1](*Institute of Software, Chinese Academy of Sciences, Beijing* 100190)
[2](*School of Software & Microelectronics, Peking University, Beijing* 100871)
[3](*Beijing Zhongke Zhuoxin Software Test Center, Beijing* 100193)

Abstract High security level protection objects are generally three-level or above protection systems, which are extremely important protection objects. However, at present, the evaluation of high security level protection objects focuses on compliance security evaluation, and the evaluation work is limited to static security configuration inspection. It is difficult to confirm the actual utility of security mechanisms and security products, and there is a lack of anti-attack ability evaluation of such protection objects. Therefore, this paper analyzes the anti-attack capability evaluation requirements of the high security level system, and puts forward the anti-attack capability evaluation model based on the APT threat path. By constructing APT threat capability library in the high security level system, different types of APT organizations are simulated to analyze the protection capability of the level protection object. In this paper, the construction method and key technologies of threat capability model are presented, and the model is implemented. Finally, this paper constructs 520 threat path test cases to test and evaluate the anti-attack ability of the evaluation object.

Key words advanced persistent threat; evaluation model; threat capability model; APT; classified security protection

摘 要 高安全等级保护对象一般是三级以上的保护系统,是极其重要的保护对象,但是,当前高安全等级保护对象测评偏重于合规性安全评估,测评工作限于静态性安全配置检查,安全机制及安全产品的实际效用难以确认,缺乏等保对象的抗攻击能力评估.因此,分析了高安全等级系统的抗攻击能力测评需求,提出了基于APT威胁路径的抗攻击能力测评模型,通过构建高安全等级系统APT

收稿日期:2022-05-26
基金项目:国家重点研发计划项目(2020YFB1005802)
引用格式:蒋建春, 文伟平, 胡陈勇. 高安全等级系统抗攻击能力测评研究[J]. 信息安全研究, 2022, 8(7): 666-674

威胁能力库，模拟实现不同类型的 APT 组织来分析等级保护对象的保护能力.给出了威胁能力模型的构建方法以及关键技术的阐述，并对模型进行了实现.最后，通过构建 520 个威胁路径测试用例，以测试和评估测评对象的抗攻击能力.

关键词 高级持续威胁；测评模型；威胁能力模型；APT；等级保护

中图法分类号 TP309.1

高安全等级保护对象[1]一般是三级以上的保护系统，典型系统为国家关键信息基础设施，其安全受损将对国家安全、经济运行、社会秩序、公共利益等造成重大影响.目前，等级保护对象面临着不同动机的威胁者，承受不同类型的攻击.网络信息泄露、恶意代码、垃圾邮件、网络恐怖主义、网络间谍、网络战等都将影响到等级保护对象安全.根据 CNCERT[2]抽样监测数据显示，针对关键信息基础设施的高级持续威胁(advanced persistent threat，APT)日趋常态化.2018 年，全球专业网络安全机构发布了各类高级威胁研究报告 478 份，同比增长约 3.6 倍.已被确认的 APT 攻击组织包括 APT28、Lazarus、Group 123、海莲花、MuddyWater 等 53 个.网络安全相关研究工作表明[3-5]，国外 APT 组织已经针对我国的金融、政府、教育、科研等目标系统持续发动攻击.高安全等级的保护对象具有重要的价值，因此成为高级持续威胁组织的关注点.

针对高安全等级保护对象，国家相关部门已经颁布了网络安全法律法规和系列技术规范，从法律责任、系统建设、应用开发、运行维护、安全管理等各方面提出具体性要求[6].同时，国家等级保护测评机构按照测评标准，评估其是否符合网络安全等级保护要求.但是，当前高安全等级保护对象测评偏重于合规性安全评估，测评工作限于静态性安全配置检查，安全机制及安全产品的实际效用难以确认，缺乏等保对象的抗攻击能力评估.基于此，本文提出一种基于网络安全威胁路径想定抗攻击能力测评方法，通过构建高安全等级系统 APT 威胁能力库，模拟不同类型的 APT 组织来分析等级保护对象的保护能力，验证保护对象相关安全机制的效用.

1 相关工作

MITRE 机构研究人员根据已发生的攻击实例，提出了攻击敌手模型框架 MITRE ATT&CK[7]，并用此框架评估产品和系统安全.同时，构建一种网络敌手语言和检测引擎 CALDERA[8]，可以复制真实的网络入侵行为.NVISO 研究人员通过开展网络敌手仿真(adversary emulation)，以测试网络弹性及高级持续威胁.美国 CERT 研究人员提出一种全球网络敌手能力链模型(adversarial capability chain，ACC)[9]，ACC 基于漏洞生命期 5 阶段能力链，即漏洞首次发现(discovery)、漏洞破坏力验证(validation)、漏洞利用攻击可逃避防护(escalation)、漏洞利用攻击低成本(democratization)、漏洞利用攻击普适化(ubiquity).美国伊利诺伊大学提出了以敌手的视角评估安全方法 ADVISE(adversary view security evaluation)[10]，该方法使用 Möbius 模型工具形式化构建敌手模型，并以此分析信息系统的安全属性.国外公司提供 130 多种攻击者模板，其中，包括国家级别黑客机构、网络犯罪分子组织、激进的个人黑客等.文献[11-12]提出网络安全测量方法.

为验证网络安全的实际保护能力. 国内外相关人员都陆续开展了网络安全测评工作.文献[13]提出网络敌手模型.文献[14]对 Windows 7 操作系统的 5 种典型安全机制 GSStackProtection，SafeSEH，HcapProtection，DEP，ASLR 抵御攻击的整体效果进行了分析，通过实际的测试用例与获得的测试数据证明 Windows 7 系统安全性改进.文献[15]提出了网络安全等级保护 2.0 云计算安全合规能力模型，基于网络安全等级保护基本要求，对云计算平台及系统的保护对象、安全措施及安全能力进行识别，构建网络安全等级保护 2.0 云计算安全合规模型，分析得出云计算平台及系统的安全技术能力.开源网络敌手模拟工具相继出现，如 Metta[16]，HackTheBox[17]，Red Team Automation[18]，BT3(blue team training toolkit)[19].

2 抗攻击能力测评模型

2.1 抗攻击能力测评需求分析

《网络安全等级保护基本要求》GB/T 22239—2019[20]针对不同级别的等级保护对象，给出了5个能力保护级要求，具体分析如表1所示：

表1 网络安全等级保护能力要求分析表

能力级别	自然威胁来源	非自然威胁来源	恶意攻击资源数量	恶意攻击危害程度
一级	一般自然灾害	个体威胁者	拥有很少资源	关键资源损害
二级	一般自然灾害	小型组织	拥有少量资源的威胁源	重要资源损害
三级	较为严重的自然灾害	外部有组织的团体	拥有较为丰富资源	主要资源损害
四级	严重的自然灾害	来自国家级别的敌对组织	拥有丰富资源的威胁源	资源损害

2.2 抗APT攻击能力测评模型

抗APT攻击能力测评模型由系统威胁者能力模型库、等级评测对象威胁路径、系统威胁用例生成、系统威胁能力执行引擎、等级评测对象、抗攻击能力评估构成，如图1所示.

1）等级评测对象.

等级评测对象，即高安全等级保护对象一般是指三级以上的保护系统，通常为关键信息基础设施.这些系统的抗攻击能力要求能够抵御有组织的复杂攻击.本文定义为以 H 为高安全等级保护对象节点集，N 为节点集内保护对象的数量，则等级保护系统对象 S 可表示如下：

$$S=\{h_i \mid h_i \in H, i=1,2,\cdots,N\}.$$

以 O 表示构成任意节点组件集合，o_i 为 O 的第 i 元素，即 $o_i \in O$，则第 k 个等级保护节点的构成组件集表示为 $Oh_k=\{o_i \mid o_i \in O, i=1,2,\cdots,N\}$，$o_i$ 为构成 h_k 的组件元素.

2）系统威胁者能力模型库.

本文定义 C 为能力集合，B 为威胁行为集合，G 为系统威胁组织集合.

定义1. 系统威胁能力.

系统威胁能力为一个二元组，即 $c=\langle b,o\rangle$，其中，c 表示威胁者对某个对象可以实施的威胁操作，b 表示威胁者的行为，o 表示 b 操作的对象.

定义2. 系统威胁者组织能力模型.

定义 $\langle g_i,c_j\rangle$ 表示系统威胁者的组织 g_i 拥有的能力为 c_j，则系统威胁者的组织 g_i 能力模型可以表示为二元组 $\langle g_i,c_j\rangle$ 的集合，即

$$CG_i=\{\langle g_i,c_j\rangle \mid c_j \in C, g_i \in G, i,j=1,2,\cdots,N\}.$$

3）等保评测对象威胁路径想定生成.

给定等级保护对象 $h_i \in H$，有威胁组织 $g_k \in G$ 的能力 c_j，使得 $c_j=(b_j,o_j)$ 的 $o_j \in Oh_i$，则 g_k 威胁 h_i 路径描述如下：

$$g_k \xrightarrow{b_j} o_j \rightarrow h_i.$$

此威胁路径可记为三元组：$\langle g_k,c_j,h_i\rangle$.

4）系统威胁测试用例生成.

给定等级保护对象 $h_i \in H$，对应测试用例为威胁路径的集合，即

$$TS_i=\{\langle g_k,c_j,h_i\rangle \mid g_k \in G, c_j \in C, h_i \in H\},$$

其中 TS_i 表示等级保护对象 h_i 的测试用例集.

5）系统威胁能力执行引擎.

系统威胁能力执行引擎模拟 g_k，对 h_i 实施 c_j，即验证威胁路径 $\langle g_k,c_j,h_i\rangle$ 的可行性.

6）保护对象抗攻击能力分析与评估.

给定等级保护对象 h_i，含有 g_k 的测试集为 $TS_{ik} \subseteq TS_i$，威胁路径验证可行的集合为 P_{ki}，则等级保护对象 h_i 对抗威胁组织 g_k 的能力计算如下：

$$\Delta_k=1-\frac{|P_{ki}|}{|TS_{ik}|},$$

其中 $|TS_{ik}|$ 表示集合 TS_{ik} 的元素数量，$|P_{ki}|$ 表示集合 P_{ki} 的元素数量，Δ_k 的数值大小表示等级保护对象 h_i 对抗威胁组织 g_k 的能力.

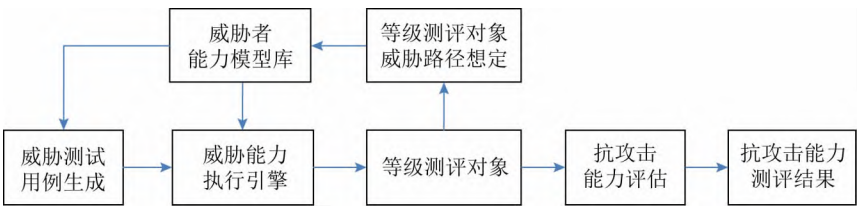

图1 抗攻击能力测评模型

3 模型实现与关键技术

3.1 系统组成结构

本文抗攻击能力测评系统由高安全等级测评对象库、等级测评对象威胁路径想定、威胁组织者模型、系统威胁能力执行引擎、抗攻击能力分析组成，如图 2 所示.

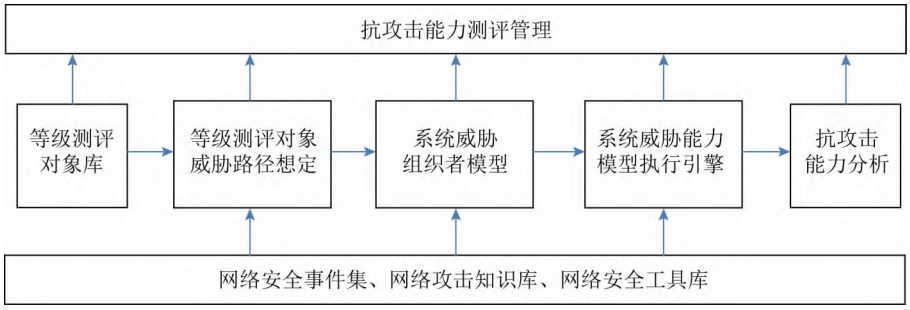

图 2 抗攻击能力测评系统框架

3.2 系统 APT 威胁组织者模型构建

本文系统威胁组织能力库构建方法主要有基于 APT 网络安全事件和网络攻击知识库集成，如图 3 所示.

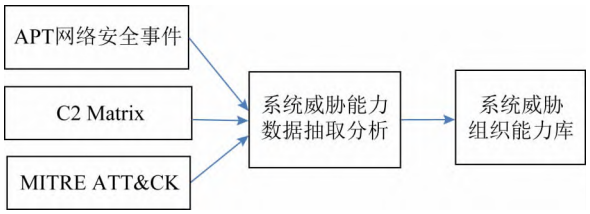

图 3 系统威胁组织能力库构建方法

1) APT 网络安全事件数据挖掘.

通过收集 APT 网络安全事件数据，抽取 APT 攻击案例的威胁操作行为和目标对象，构建高安全等级保护对象的组织威胁者的能力算子.

2) 网络攻击知识库集成.

目前，网络上已公开的网络攻击知识库有 MITRE ATT&CK，C2 Matrix. 其中：MITRE ATT&CK 是基于真实的观察形成的网络敌手知识库；C2 (command and control) 是 APT 组织攻击者常利用的战术，用于控制端和受控目标的之间联系. 开源 C2 Matrix 包含 35 个命令和控制框架[21].

APT 威胁组织能力库以 XY 标识，其数据格式表示为二元组 $\langle x, y\rangle$，其中，x 为操作行为描述，y 为操作对象.

3.3 等级评测对象威胁路径想定生成

等级评测对象威胁路径想定生成方法利用等级保护对象的组件、APT 威胁组织能力库，通过威胁数据分析自动生成等级保护节点 APT 威胁路径，如图 4 所示：

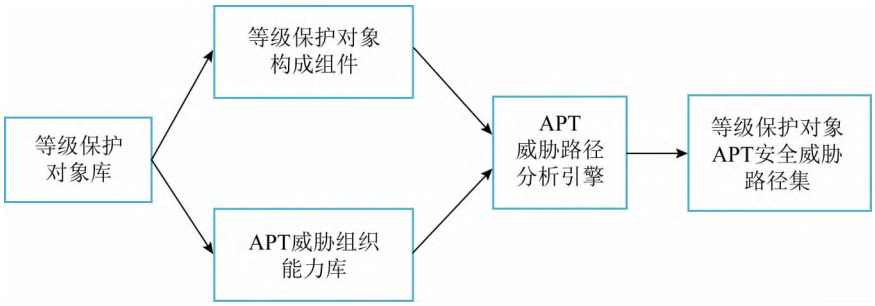

图 4 等级保护对象 APT 威胁路径分析

设 P_i 是等级保护节点 h_i 威胁路径集合，P 是等级保护节点所有的威胁路径集合.

算法 1. 等级保护对象高级威胁路径分析算法.

输入：H 为等级保护节点 h_i 集合、O 为等级保护节点 h_i 构成的组件集、XY 为 APT 威胁组织能力库；

输出：P.

步骤 1. 从 H 选取 1 个等级保护节点 h_i，直至集合 H 的元素遍历完；

步骤 2. 获取 h_i 的组件 $o_i \in O$；

步骤 3. 从 XY 中遍历取元素$\langle x_j, y_j \rangle$；

步骤 4. 若 $y_j = o_i$，则生成威胁路径 $x_j \rightarrow y_j$；

步骤 5. 将$\langle x_j, y_j \rangle$添加到 P_i；

步骤 6. 重复步骤 3，直至集合 XY 的元素取完；

步骤 7. 确定等级保护节点威胁路径集合 P_i.

APT 组织的攻击活动通常表现为水平移动，即通过等级保护节点的威胁关联，构成复杂的威胁路径，形成 APT 组织的水平移动攻击.

设 H 为等级保护节点集，即 H 的集合元素为等级保护对象独立节点；$\boldsymbol{M}$ 为威胁关联矩阵，$\boldsymbol{M}$ 的集合元素是节点之间威胁关联函数 $R(h_i, h_j)$ 值，该值为 1 或 0，1 表示等级保护节点 h_i 的威胁行为可以威胁到 h_j，0 表示等级保护节点之间不存在威胁相互影响.

算法 2. APT 水平移动威胁路径分析算法.

输入：H，$\boldsymbol{M}$；

输出：等级保护节点关联威胁集.

步骤 1. 选择待测评的等级保护节点 $h_i \in H$；

步骤 2. 选择等级保护节点 $h_i \in H$ 的安全威胁集合 P_i；

步骤 3. 确定 $h_i \in H$ 与 $h_j \in H$ 的 $R(h_i, h_j)$；

步骤 4. 如果 $R(h_i, h_j) = 1$，则生成等级保护节点 h_i 和 h_j 的威胁关联$\langle P_i, P_j \rangle$；

步骤 5. 重复步骤 3，直到与 h_i 有威胁关联的等级保护节点分析完毕；

步骤 6. 输出等级保护节点 h_i 的关联威胁集；

步骤 7. 重复步骤 1，直到等级保护节点的分析完毕.

3.4 系统 APT 威胁能力模型执行引擎

系统威胁能力模型执行引擎的功能是模拟实现 APT 组织对等级保护节点的威胁操作.该引擎支持插件模式，按照 APT 组织的攻击过程，集成各种工具或 APT 样本数据.具体实现方法如下：

1）攻击工具集成实现.

如图 5 所示，根据 APT 组织所利用的攻击方法和对应的操作，可以集成软件工具实现威胁者的操作.

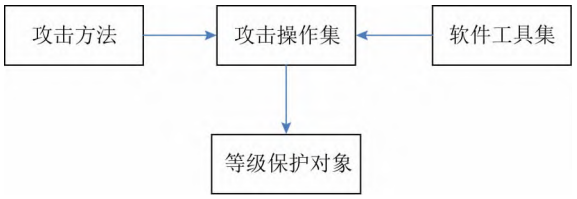

图 5　APT 威胁操作集成示意图

2）APT 攻击样本数据重放.

将 APT 组织的攻击样本数据通过网络流量重放、文件拷贝等工具，输入到等级保护测评对象中，以验证等级保护的安全机制防护能力，如图 6 所示：

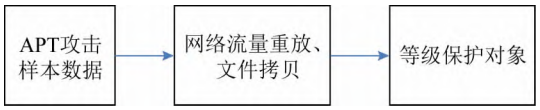

图 6　APT 攻击样本数据重放示意图

4　模型应用验证与分析

4.1　模型应用方法

4.1.1　模型应用

根据等级保护对象的能力保护要求，对于给定的高安全等级保护对象，抗攻击能力测评过程如下：

1）获取等级保护对象的组件配置信息；

2）选取 APT 威胁者的能力库，想定生成等级保护对象威胁路径集；

3）测试验证等级保护对象的威胁路径可行性；

4）给出实际可行的威胁路径数量与想定威胁路径数的比值，记为 α；

5）计算抗 APT 攻击能力的量化数值 $\Delta = 1 - \alpha$.

4.1.2　模型实现

本文从已公开的典型 APT 组织活动报告中提取 APT 威胁组织能力库，并生成威胁路径测试用例集（APT 攻击样本集），最后在待测信息系统中重放 APT 攻击样本，计算并输出待测信息系统抗攻击能力.具体实现过程如下：

1）构建 APT 威胁者组织能力库.本文从近年来已公开的网络攻击活动报告中提取 9 个典型

APT 威胁者组织，并基于待测信息系统列举出每个 APT 组织的典型威胁能力，如表 2 所示：

表 2　APT 典型威胁能力

APT 威胁者 ID	APT 威胁者组织名称	威胁能力枚举
G_1	Bitter	〈Arbi. Exec.，Binary〉〈Exploit，MS Word〉〈Exploit，MS Excel〉〈Avoid. Detect.，File〉
G_2	Equation	〈Arbi. Exec.，Binary〉〈Avoid. Detect.，File〉
G_3	Fancybear	〈Arbi. Exec.，Binary〉〈Exploit，MS Word〉〈Exploit，MS Excel〉〈Avoid. Detect.，File〉
G_4	Lazarus	〈Arbi. Exec.，Binary〉〈Arbi. Scr. Exec.，Script〉〈Exploit，MS Excel〉〈Avoid. Detect.，File〉
G_5	lvban	〈Arbi. Exec.，Binary〉〈Exploit，MS Word〉〈Avoid. Detect.，File〉
G_6	MuddyWater	〈Arbi. Exec.，Binary〉〈Arbi. Scr. Exec.，Script〉〈Exploit，MS Word〉〈Exploit，MS Excel〉〈Avoid. Detect.，File〉
G_7	OceanLotus	〈Arbi. Exec.，Binary〉〈Arbi. Scr. Exec.，Script〉〈Exploit，MS Word〉〈Exploit，Internet Explorer〉〈Avoid. Detect.，File〉
G_8	Oilrig	〈Arbi. Exec.，Binary〉〈Exploit，MS Excel〉〈Avoid. Detect.，File〉
G_9	WhiteElephant	〈Arbi. Exec.，Binary〉〈Exploit，MS Word〉〈Exploit，MS Power Point〉〈Avoid. Detect.，File〉

为便于后文描述，对表 2 中的威胁能力进行通用定义，如表 3 所示：

表 3　通用威胁定义

威胁能力 ID	威胁能力描述
C_1	任意代码执行(Arbi. Exec.)
C_2	漏洞利用(Exploit)
C_3	恶意脚本执行(Arbi. Scr. Exec.)
C_4	逃逸检测(Avoid. Detect.)

2) APT 威胁路径想定.本文想定 APT 组织者能把攻击载荷投送到目标对象，形成点对点威胁路径，即表示为二元组形式〈威胁行为，目标对象〉.

3) APT 威胁者能力实现.本文通过文件拷贝的方式将 APT 攻击样本投送到目标对象，然后观察攻击样本在目标对象的执行情况，以验证相应的 APT 威胁路径是否可行.

4.2　模型应用测评示例

4.2.1　测评环境构建

为验证本文提出的抗攻击能力测评模型，本文构建了一个典型的待测网络信息系统，如图 7 所示.受控环境中部署一个典型的企业邮件系统、办公终端作为测评对象.

在待测网络信息系统中，假定 APT 威胁者收集企业员工的邮箱信息，并将攻击样本(包括可执行恶意代码、恶意文档、恶意脚本 3 种类型)发送给企业员工，网络信息安全意识薄弱的员工在办公终端中打开并运行邮件附件，从而 APT 威胁者可以获得办公终端的控制权进而实施进一步的恶意活动.在本文的测评中，考虑上述待测信息系统的节点信息如表 4 所示.

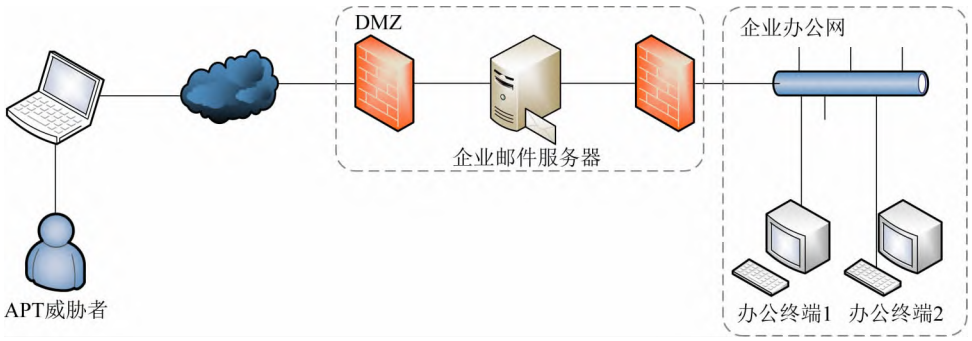

图 7　抗 APT 攻击能力测评网络信息系统拓扑结构图

表 4　抗 APT 攻击能力测评网络信息系统配置

节点 ID	节点名称	组件信息
E_1	办公终端 1	• Windows 7 x64，内部版本 7601：Service Pack 1 • MS Office 2007，版本 12.0.4518.1014 • Adobe Reader，版本 9.4.0 • 360 安全卫士，主程序版本：13.0.0.2002，木马库：2022-01-17
E_2	办公终端 2	• Windows 10 x64，版本 21H1，内部版本 19043.1466 • MS Office 2007，版本 12.0.4518.1014 • Adobe Reader，版本 9.4.0 • Windows Defender，反恶意软件客户端版本：4.18.2111.5，引擎版本：1.1.18900.2，防病毒软件版本：1.357.194.0，反间谍软件版本：1.357.194.0
M_1	企业邮件服务器	• Ubuntu Linux 5.13.0-28 • ClamAV，版本 0.104.2/26445/Sun Feb 6 17：26：12 2022

4.2.2　测评数据集

本文实验枚举了 9 个 APT 威胁者组织对测评对象的威胁路径，并构建 520 个威胁路径测试用例，以测试和评估测评对象的抗攻击能力.表 5 列举了本文测评中所使用的测试用例数.需要指出的是，并非所有 APT 威胁者组织均具备所有的威胁能力和威胁路径.

表 5　APT 威胁路径及测试用例

威胁路径	APT 威胁者								
	G_1	G_2	G_3	G_4	G_5	G_6	G_7	G_8	G_9
$\langle C_1,E_1\rangle$	41	57	24	6	93	2	49	6	53
$\langle C_1,E_2\rangle$	41	57	24	6	93	2	49	6	53
$\langle C_2,E_1\rangle$	14	—	33	15	7	53	19	6	25
$\langle C_2,E_2\rangle$	14	—	33	15	7	53	19	6	25
$\langle C_3,E_1\rangle$	—	—	—	9	—	6	2	—	—
$\langle C_3,E_2\rangle$	—	—	—	9	—	6	2	—	—
$\langle C_4,M_1\rangle$	55	57	57	30	100	61	70	12	78

注：对于不适用的威胁路径标记为“—”.

4.2.3　测评结果分析

根据 4.2.1 节所述的测评环境和 4.2.2 节所述的测评数据集，基于本文提出抗攻击能力测评模型，对测评对象的 3 个节点 E_1，E_2，M_1 按照威胁路径重放测试用例，并计算每个节点的抗攻击能力.

1）办公终端节点 E_1 的抗攻击能力测评结果分析.

从表 6 可以看出，节点 E_1 对于著名的 APT 组织 OceanLotus（海莲花组织）抗攻击能力最强，而对于 Oilrig 组织的抗攻击能力最弱，甚至无法防御该 APT 威胁者的任何测试用例.

表 6　办公终端节点 E_1 的抗 APT 攻击能力测评结果

APT 威胁者 ID	抗攻击能力			
	$\langle C_1,E_1\rangle$	$\langle C_2,E_1\rangle$	$\langle C_3,E_1\rangle$	E_1 合计
G_1	0.000 0	0.357 1	—	0.090 9
G_2	0.122 8	—	—	0.122 8
G_3	0.000 0	0.060 6	—	0.035 1
G_4	0.000 0	0.200 0	0.111 1	0.133 3
G_5	0.064 5	0.857 1	—	0.120 0
G_6	0.000 0	0.075 5	0.000 0	0.065 6
G_7	0.142 9	0.631 6	0.000 0	0.271 4
G_8	0.000 0	0.000 0	—	0.000 0
G_9	0.150 9	0.000 0	—	0.102 6

注：对于不适用的 APT 威胁者 ID 标记为“—”.

2）办公终端节点 E_2 的抗攻击能力测评结果分析.

从表 7 可以看出，由于 E_2 的环境为 Windows 10 操作系统，因此总体上比 E_1 的 Windows 7 操作系统的抗攻击能力显著提升.E_2 对于 Equation 组织（方程式）具有较好的抗攻击能力，而对于来自南亚大陆的 APT 组织 Bitter（蔓灵花）其抗攻击能力相对较弱.

表 7　办公终端节点 E_2 的抗 APT 攻击能力测评结果

APT 威胁者 ID	抗攻击能力			
	$\langle C_1,E_2\rangle$	$\langle C_2,E_2\rangle$	$\langle C_3,E_2\rangle$	E_2 合计
G_1	0.268 3	0.642 9	—	0.363 6
G_2	0.877 2	—	—	0.877 2
G_3	0.458 3	0.363 6	—	0.403 5
G_4	0.500 0	0.733 3	0.888 9	0.733 3
G_5	0.537 6	0.142 9	—	0.510 0
G_6	1.000 0	0.849 1	0.333 3	0.803 3
G_7	0.612 2	0.842 1	1.000 0	0.685 7
G_8	0.333 3	1.000 0	—	0.666 7
G_9	0.679 2	0.960 0	—	0.769 2

注：对于不适用的 APT 威胁者 ID 标记为“—”.

3）企业邮件服务器 M_1 的抗攻击能力测评结果分析.

如表 8 所示，由于该服务器为 Linux 系统，无法直接打开和运行邮件附件，因此威胁路径仅为测试用例样本的逃逸检测能力.M_1 对于 Oilrig 组

织具有很好的抗攻击能力，而对于 OceanLotus 组织的抗攻击能力最弱.

4）系统抗攻击能力整体测评结果分析.

由于 APT 攻击通常为多阶段活动，为此，对测评对象应整体分析抗攻击能力.图 8 示出了所有节点(E_1,E_2,M_1)抗攻击能力的综合评价.可以看出，尽管不同节点对于不同 APT 威胁者的抗攻击能力有较大差异，但是对于待测信息系统(测评对象)整体而言，其具有相近的抗攻击能力.图 8 中横坐标为 APT 威胁者，直方图中的不同颜色区块分别表示节点 E_1,E_2,M_1 的抗攻击能力.其中，黄色区块表示测评对象的整体抗攻击能力，计算方法如下：

$$\Delta_k=1-\frac{|P_{E_1k}|+|P_{E_2k}|+|P_{M_1k}|}{|TS_{E_1k}|+|TS_{E_2k}|+|TS_{M_1k}|},$$

其中 Δ_k 表示测评对象对于 APT 威胁者 G_k 的抗攻击能力.

表 8　邮件服务器抗 APT 攻击能力测评结果

APT 威胁者 ID	抗攻击能力
	$\langle C_4,M_1\rangle$
G_1	0.636 4
G_2	0.719 3
G_3	0.614 0
G_4	0.066 7
G_5	0.350 0
G_6	0.868 9
G_7	0.242 9
G_8	1.000 0
G_9	0.512 8

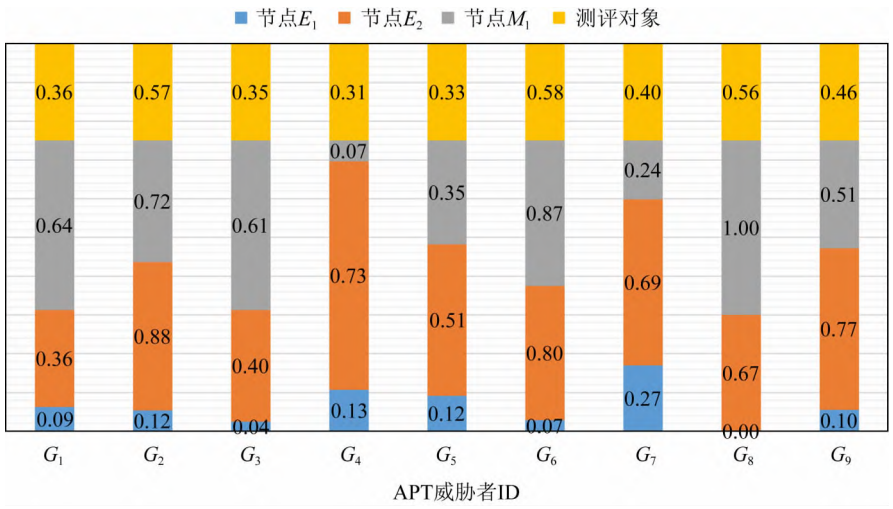

图 8　测评对象抗 APT 攻击能力结果

4.3　相关工作讨论

网络安全等级保护 2.0 增加了新的安全控制域：安全运营中心(SOC).当测评对象中的任一节点检测到威胁时，安全运营中心所部署的安全信息事件与管理系统(SIEM)或态势感知系统可以快速将威胁情报同步至测评对象的所有节点.为此，测评对象在 SOC 环境下的抗攻击能力测评方法有所变化，应将测评对象的所有威胁路径中的全部节点均验证通过的测试用例视为测评对象的整体威胁，其抗攻击能力计算如下：

$$\Delta'_k=1-\frac{|P_{E_1k}\cap P_{E_2k}\cap P_{M_1k}|}{|TS_{E_1k}\cup TS_{E_2k}\cup TS_{M_1k}|}.$$

测评结果如表 9 所示：

表 9　基于等保 2.0 的测评对象抗攻击能力测评结果

APT 威胁者 ID	抗攻击能力
G_1	0.654 5
G_2	0.929 8
G_3	0.701 8
G_4	0.800 0
G_5	0.680 0
G_6	0.934 4
G_7	0.800 0
G_8	1.000 0
G_9	0.846 2

5 结束语

本文研究分析高安全等级系统的抗攻击能力测评需求，提出一种基于攻击路径的高安全等级保护的抗APT攻击能力测评模型，给出了国家级别、敌对组织、拥有丰富资源等威胁者能力模型构建方法，并提供了相关实现参考.后续的研究工作将进一步完善威胁者能力模型和威胁知识库自动化构建，以用于实际的网络安全等级保护测评服务，探索构建基于APT攻击能力驱动网络靶场服务平台，开展关键信息基础设施的网络攻防演练.

参 考 文 献

[1] 盘善海，裴华. 高安全等级网络安全防护体系研究与设计[J]. 通信技术，2021，54(7)：1715-1720

[2] Khan M B. Advanced persistent threat：Detection and defence [J]. arXiv preprint，arXiv:2004.10690，2020

[3] 南亚地区APT组织. 南亚地区APT组织2019年度攻击活动总结 [EB/OL]. [2022-06-12]. https://cdn. modb. pro/doc/20703

[4] 恒安嘉新(北京)科技股份公司. 2020年网络安全态势报告[J]. 信息安全研究，2021，7(3)：198-206

[5] 张博，崔佳巍，屈肃，等. 高级持续性威胁及其重构研究进展与挑战[J]. 信息安全研究，2021，7(6)：512-519

[6] 方禹. 2021年国内网络安全相关立法回顾及思考[J/OL]. 中国信息安全，2021 [2022-06-12]. https://www. secrss. com/articles/37994

[7] Mitre. ATT&CK matrix for enterprise [EB/OL]. [2022-06-12]. https://attack.mitre.org/.

[8] Applebaum A，Miller D，Strom B，et al. Intelligent，automated red team emulation [C] //Proc of the 32nd Annual Conf on Computer Security Applications. New York：ACM，2016：363-373

[9] Spring J，Kern S，Summers A. Global adversarial capability modeling [C] //Proc of APWG Symp on Electronic Crime Research (eCrime). Piscataway，NJ：IEEE，2015：1-21

[10] LeMay E，Ford M D，Keefe K，et al. Model-based security metrics using adversary view security evaluation (ADVISE) [C] //Proc of the 8th Int Conf on Quantitative Evaluation of Systems. Piscataway，NJ：IEEE，2011：191-200

[11] Pham L H，Albanese M，Priest B W. A quantitative framework to model advanced persistent threats [C] //Proc of the 15th Int Conf on Security and Cryptography (SECRYPT 2018). 2018：282-293 [2022-06-12]. https://www.scitepress.org/papers/2018/68726/68726.pdf

[12] Sugrim S，Venkatesan S，Youzwak J，et al. Measuring the effectiveness of network deception [C] //Proc of the IEEE Int Conf on Intelligence and Security Informatics (IEEE ISI 2018). Piscataway，NJ：IEEE，2018：142-147

[13] 蒋建春，文伟平. 网络敌手模型研究[J]. 信息网络安全，2008，8(9)：15-18

[14] 周虎生，文伟平，尹亮，等. Windows 7操作系统关键内存防攻击研究[J]. 信息网络安全，2011，11(7)：38-41

[15] 张振峰，张志文，王睿超. 网络安全等级保护2.0云计算安全合规能力模型[J]. 信息网络安全，2019，19(11)：1-7

[16] Uber. Metta，an information security preparedness tool [EB/OL]. [2022-06-12]. https://github. com/uber-common/metta

[17] Ibrahim S H，Nassar M. Hack the box：Fooling deep Learning abstraction-based monitors [J]. arXiv preprint，arXiv:2107.04764，2021

[18] Qsecure-labs. overlord [EB/OL]. [2022-06-12]. https://github.com/qsecure-labs/overlord

[19] Encripto A S. Blue team training toolkit (BT3)[EB/OL]. [2022-06-12]. https://www.bt3.no/

[20] 马力，祝国邦，陆磊.《网络安全等级保护基本要求》(GB/T 22239—2019)标准解读[J]. 信息网络安全，2019，19(2)：77-84

[21] thec2matrix. C2 matrix [EB/OL]. [2022-06-12]. https://www.thec2matrix.com/matrix

蒋建春

博士，副研究员.主要研究方向为网络信息安全、信息物理系统安全.

jianchun@iscas.ac.cn

文伟平

博士，教授，博士生导师.主要研究方向为系统与网络安全、大数据与云安全、智能计算安全.

weipingwen@pku.edu.cn

胡陈勇

硕士.主要研究方向为网络安全与软件工程.

huchenyong@stchina.com.cn