文章编号：2096-1472(2020)-05-38-05
DOI:10.19644/j.cnki.issn2096-1472.2020.05.011

网络靶场攻防场景设计框架

张月红

(上海电子信息职业技术学院，上海 201411)
✉64688613@qq.com

摘　要：随着网络威胁的暴露范围越来越广，开发新的工具来改进网络防御是一个重大挑战。网络防御中最重要的问题是人员技能培训，网络靶场就是用于此目的。它提供用于训练和对抗比赛的虚拟环境。本文用VDSL语言定义了一个定制的网络环境，并实现了一个框架，允许将网络靶场场景转换为Prism模型。这样就可以进行训练和赛事结果的定量分析并可以对这个框架进行持续优化。

关键词：网络靶场；VDSL；攻防场景；框架
中图分类号：TP311.1　**文献标识码**：A

A Framework for Designing Attack and Defense Scenarios in Cyber Range

ZHANG Yuehong

(*Shanghai Technical Institute of Electronics & Information*, *Shanghai* 201411, *China*)
✉64688613@qq.com

Abstract: As exposure to cyber threats is getting wider and more prevalent, it becomes a major challenge to develop new tools to improve cyber defense. The most important issue in cyber defense is staff training, and cyber ranges are used for this purpose. A cyber range is a virtual environment used for training and competition. This paper defines a customized network environment with VDSL (Virtual Scenarios Descriptive Language) language and implements a framework allowing to convert the cyber range scenarios into Prism models. In this way, the quantitative analysis of training and competition results can be carried out and the framework can be continuously optimized.

Keywords: cyber range; VDSL; attack and defense scenarios; framework

1 引言(Introduction)

当前，IT安全在我们的生活中变得越来越重要，网络威胁的程度越来越广泛，给个人生活、企业生产乃至国家重点基础设施等带来的风险都是严重的。开发新的技术和新的工具来提高网络防御能力是一个重大挑战。北约合作网络防御中心将网络防御定义为：探测或获取有关网络入侵、网络攻击或即将进行的网络行动的主动措施活动。很明显，这些活动在很大程度上取决于安全专家的技能。因此，防御的基础是对人员进行技能培训，技能可通过实践和演习活动进行强化[1]。受训人员必须在模拟真实应用，并且安全可控的场景中训练和操作，网络靶场用于提供这样的仿真受训环境。

2 需求分析(Demand analysis)

(1)网络靶场可支撑的用户分析[2]。

①学生：在模拟的应用环境中运用理论知识，提高操作技能，也可作为团队一员共同参与比赛，合力解决安全问题。

②教师：可以把网络靶场作为评价学生的实践课堂。

③组织：可以使用网络靶场来评估组织的安全能力、培训团队和测试新技术。

(2)在网络靶场内的演习涉及几个不同角色的团队，角色功能如图1所示。

①红色团队扮演攻击者的角色，试图通过达到访问特定数据或破坏特定资源实现攻击。可以使用的攻击工具有：用于攻击的脚本、用于注入目标的恶意软件或后门、用于拦截数据流的工具或异常流量生成器等。

②蓝色团队的任务是防御，其目的是在有限的时间内验证和改进基础设施的安全性，可以使用用于执行安全分析和故障管理的工具及数字取证工具等。

③绿色团队负责维护物理和在线基础设施，相当于运维团队，可以使用用于基础设施监控的工具，如监控和网络管理软件等。

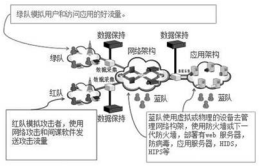

图1 网络靶场团队

Fig.1 Cyber range team

(3)网络靶场所需组件的逻辑表示，如图2所示。

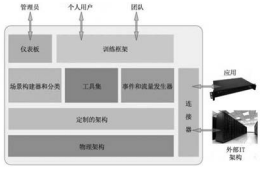

图2 网络靶组件

Fig.2 Cyber range components

①训练框架是各类用户的接入点，支持个人训练和团队培训相关的事务管理与组织。

②仪表板是一个交互式工具，由管理员使用，用于管理和监控网络靶场。

③工具集为网络靶场用户提供一套攻击和防御工具，用于设备和系统的训练和测试。

④事件和流量生成器模块可以在自动模式下模拟基础设施内的正常流量。

⑤连接器允许网络靶场的传统架构扩展到不同的架构，称为混合网络靶场架构，以便将硬件或物理设备插入到模拟场景中。

(4)场景

场景[3]是包括网络、硬件、软件，以及在实践过程中的操作环境。网络靶场的主要目的是准备满足训练要求的场景。在如图3所示的场景中，整个网络由服务器机房、实验室、会议室和控制室四个子网组成。在服务器机房网络中，有三个节点，一个具有特定的操作系统漏洞，其他的都包含易受攻击的服务和恶意软件。在实验室网络中，连接了两台笔记本电脑，其中一台可以通过远程登录访问，另一台移动终端可以进入会议室网络。会议室网络包含具有文件服务器功能(即SAMBA服务)的主机。控制室网络包含一台运行了防病毒软件的个人计算机和一台包含有要保护数据(也就是FLAG值)的个人计算机。

蓝队在靶场内先执行一定时间的防御任务，然后停止并切换到脱机状态。然后红对开始进入攻击状态，红队访问功能受限，仅能访问公共子网。红队的目标是通过实施多种技术最终到达目标节点并窃取目标FLAG数据。

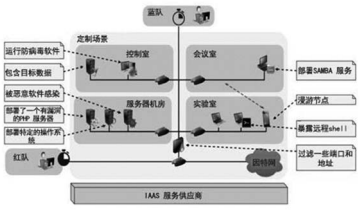

图3 场景示例

Fig.3 Example of scenario

3 相关技术(Relevant technologies)

涉及相关技术包括：领域特定语言(Domain-Specific Language，DSL)、虚拟场景描述语言(Video Scene Description Language，VSDL)、Prism模型(Prism Model)检查器和离散时间马尔可夫链(Discrete Time Markov Chain，DTMC)。

(1)领域特定语言DSL是解决特定问题的领域规范语言

①Xtext，它是一个基于Eclipse的框架，用于实现DSL。它使用户能够快速实现语言，并负责实现开发集成环境的所有方面，例如，链接器、编译器、类型检查器和解析器。

②Xtend，它是一种通用编程语言，与完全用Xtext开发的代码具有互操作性。Xtend源于Java编程语言，但它有比Java更简洁的语法和一些额外的功能。

(2)虚拟场景描述语言VSDL

虚拟场景描述语言VSDL是一种用于为网络靶场建模虚拟场景领域特定语言。

使用虚拟场景描述语言实现的场景。场景由名字和一系列场景元素标识，场景元素包括节点或网络。节点和网络都由唯一的标识符标识。对于节点，可以表示为：类型(如服务器、客户端、移动设备等)，硬件配置文件(CPU数量、RAM和磁盘大小等)，软件功能(特定操作系统或操作系统系列等)。对于网络，可以表示为接入公共网络、寻址方法和所连接的节点。

图4 VSDL示例

Fig.4 VSDL example

以如图3所示的场景为例，用VSDL语言描述后的示例如图4所示，可以看到其中对于实验室和会议室网络，规定了以下特别功能：当漫游节点从会议室移动到实验室时，要求最多t=15秒后节点必须连接于网络，并且在0和t时间值内，漫游节点应处于未连接状态。

(3)Prism模型检查器

Prism模型检查器是一个建模和分析概率行为的系统工具。这些系统包括安全协议、随机算法等。模型是用Prism语言定义的，而属性可以通过各种时态逻辑来指定。Prism模型检查器的输入形式是马尔可夫链。如图5所示为概率模型检查器实现的功能示例。概率模型检验允许对系统进行定量分析，用以确定在网络靶场范围内攻击发生的概率是多少？攻击成功的概率有多大？

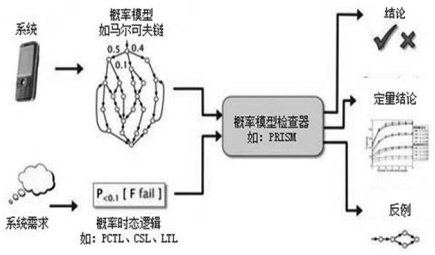

图5 概率模型检查

Fig.5 Probabilistic model checking

(4)马尔可夫链

马尔可夫链是一种马尔可夫过程。一个过程满足马尔可夫性质，就如同一个人能够仅仅基于当前状态就可以对未来进行预测，也就是说以系统的当前状态为条件判断和预测未来，未来和过去的状态是完全独立的。当马尔可夫过程的状态空间是离散值时，它被称为马尔可夫链。马尔可夫链可以被看作是一系列随机事件，其中系统的当前状态与所有过去状态无关。

离散时间马尔可夫链(DTMC)[4]指具有离散状态空间和离散时间$\{X_t, t>0\}$的随机过程。

$$P(X_{t+1}|X_t,\ldots\ldots,X_1) = P(X_{t+1}|X_t)$$

(5)Prism建模语言

先解释Prism语言的基本概念：模块的并行组合和同步，之后可以了解Prism模型检查器中的模型是如何定义的。

并行组合：在Prism模型的每个状态中，都有一些可用的命令，在这些命令之间选择哪个命令？选择取决于模型的类型。对于DTMC，选择是有概率，可以以相同的概率选择每个启用的命令。

同步：在Prism模型中，命令可以标记为动作。这些操作将用于使两个(或更多)模块同时执行转换。

用Prism语言编写的概率模型可以用rewards值或者与模型的状态或状态转换相关的值来量化[5]。rewards结构可用于计算预期得分等属性，也可以分配给模型状态和状态转换。

状态rewards：rewards结构为模型的每个状态分配20个reward。左边为布尔值，记为受保护状态，右边的值(20)记为rewards。简单地理解为，满足保护的状态被记作布尔值true，并分配相应的rewards。如图6所示。

```
rewards
    true : 20;
endrewards
```

图6 状态rewards

Fig.6 State rewards

转换rewards：定义与状态rewards相同，也可以在rewards和endrewards的结构体中定义。其中转换rewards用以下语法编写：[动作]布尔值：rewards，可以解释为满足防护要求的状态转换，得到rewards。

```
rewards
  [] true : 200;
  [connected_to_network_A] true : 500;
  [sql_injection] true : 10000;
endrewards
```

图7 转换rewards

Fig.7 Transition of rewards

如图7所示的示例可以解释为：在没有动作标签的情况下，模型中的所有转换分配200的rewards；标有“与网络连接的行动”的转换分配值为500；对所有标有SQL注入动作的转换给予分配10000。

可以通过两种方式指定基于rewards的财富值：

R bound [rewardprop](在这个条件表达式中，其中bound为比较运算符，可以是小于、小于等于、大于或大于等于)。

R query [rewardprop](在这个赋值表达式中，query为赋值运算符，可以是等于多少、最小是多少、最大是多少)。

如果从模型状态开始时与模型的rewardprop相关联的预期报酬满足bound这个条件表达式，那么，R bound [rewardprop]条件运算的结果为真，则R query [rewardprop]将返回实际预期rewards值。总财产R将返回在rewards结构中指定的预期总数。

4 设计(Design)

首先利用扩展VSDL语法定义场景，其中包含对存有漏洞节点的记录，实现了一个结合VSDL规范和漏洞描述符的Prism模型生成器，其结果是一个需要用Prism验证的模型。网络靶场攻击策略架构[6]的目标是实现如图8所示的逻辑流程。首先在VSDL中编写场景，然后根据场景生成Prism模型，用于验证漏洞利用情况，此时可以接受场景或对场景进一步优化。

图8 架构逻辑流程

Fig.8 Logical flow

(1)VSDL中的漏洞规范

VSDL规范根据其核心元素(即节点和网络)及其特性描述场景。在这种情况下，可将漏洞视为额外的节点特性。因此，使用新的节点属性扩展了VSDL的语法。格式为：Vulnerability:<identifier>。为了研究漏洞，必须对场景中的漏洞特性进行研究。例如在图9中，标明了Pc_1这台机器遭受SQL注入攻击。

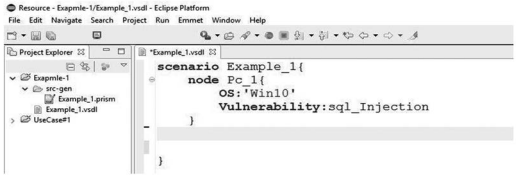

图9 SQL注入攻击

Fig.9 SQL injection attack

(2)代码生成

代码生成过程是这样的：框架获取从JSON文件生成Prism代码所需的信息。这意味着对于每种类型的漏洞，都需要一个适当的JSON文件。整个过程可以描述如下：靶场攻击策略框架从场景中读取所需漏洞的类型，然后从相应的JSON文件中获取必要的信息来创建Prism代码。

如果选择跨站点脚本(XSS)漏洞，需要一个名为XSS.json的文件，其中包含创建Prism模型所需要的有用信息。该模型显然将使用Prism语言编写，那么如何创建此JSON文件?

(3)漏洞规范脚本语言

创建了一个规范脚本，用于为任何类型的漏洞创建适当的JSON文件。每个场景都可以用Prism模型来表示，Prism模型可以包含全局变量、常量、模块，还有rewards结构。考虑到每个模型的组件和VSDL场景的特性，为JSON文件创建了一个标准结构，如图10所示。JSON对象分为三个部分：头部、主体和rewards。

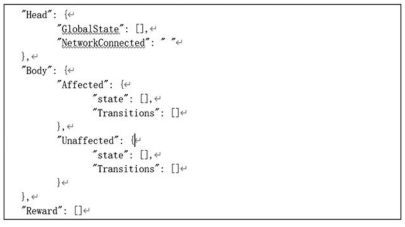

图10 JSON对象的组成部分

Fig.10 Components of JSON object

①头部

头部可以包括全局变量(所有模块都可以读写的变量)和常量。它由两部分组成：

全局状态GlobalState：是一个数组，可以包含全局变量和常量。

网络连接情况：将NetworkConnected定义为一个特定常数，用以表示节点X是否连接到网络Y。

定义样式如下：

const bool $Nodename_connected_to_network_$netwrokName

如果需要这些信息来表达某一种类型的漏洞，必须在适当的JSON文件中指定它，这种情况下，靶场攻击策略框架会用适当的信息去替换$nodeName和$networkName变量。如果场景指定Pc_2未连接到网络会议室，生成的代码为：const bool Pc_2_connected_to_MeetingRoom=false,如果不需要这些类型的信息，可以省略它并将其留空。

②主体

为每个节点创建一个模块。如果此节点包含一个漏洞，则将其标记为被影响，否则将其标记为未受影响。易受攻击节点的状态和转换在被影响对象中指定，而其他节点的状态和转换在未被影响对象中指定。例如，如果某个节点存在注入漏洞，则可以通过如图11所示方式指定被影响的对象。

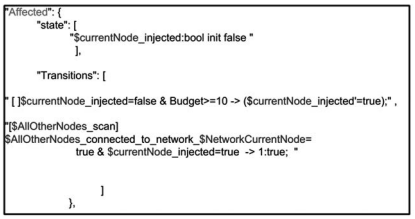

图11 标记被影响对象

Fig.11 Marking an affected object

如果Pc_1是受影响的节点，靶场攻击策略框架从受影响的节点对象获取信息，并将图11中的$currentNode替换为“Pc_1”，将$NetworkCurrentNode替换为Pc_1所连接的网络。如图12所示，这是为Pc_1生成的Prism模块代码。

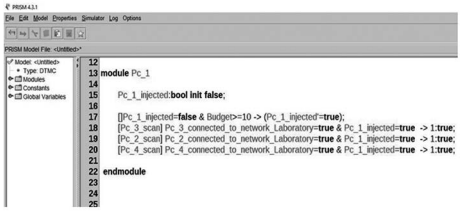

图12 模块示例

Fig.12 Module example

③rewards

在如图13所示的奖励示例中包含靶场框架用于reward结构信息的数组。例如：[$allothernodes]true:已知的pc_*+1；

框架将使用所有未受影响的节点名(场景中没有指定漏洞的节点)替换$ allothernodes，如图13所示。按照上面解释的结构，为其他类型的漏洞创建JSON文件很简单。

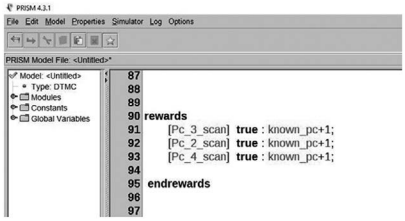

图13 奖励示例

Fig.13 Reward example

5 使用用例(Use case)

以注入攻击为例来描述一个测试用例，并产生由策略设计框架自动生成的Prism代码。

(1)注入攻击

注入是Web安全中的一个主要问题。它被列为2017年OWASP前10名中的头号Web应用程序安全风险[7]。这种类型的攻击允许攻击者将代码注入程序或查询，或将恶意软件注入计算机，以便执行读取、修改数据库或远程调用系统命令类操作。

对于测试用例，仅考虑一般的注入攻击，测试环境中有四台名为Pc_1、Pc_2、Pc_3、Pc_4的计算机。还有两个网络，称为实验室和会议室，其中Pc_1易受注入攻击，场景描述如图14所示。在图15中，可以看到由框架生成的Prism代码。

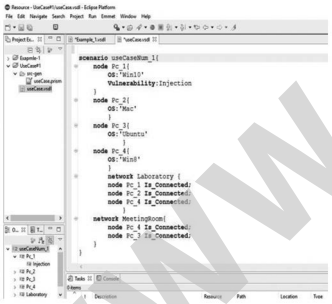

图14 场景

Fig.14 Scenario

图15 prism代码

Fig.15 Prism code

(2)Prism实验

一旦有了Prism代码，就可以应用这些属性来分析它。对于生成的Prism模型，reward是已知Pc的数量。在Prism模型中，指定要实现某类攻击，需要预置一个最小的预算，Pc_1_injected=false & Budget>=10，此时Pc_1_injected=true。现在，如果想验证Prism需要的预算最少，如预算设为50的情况下，可以得到期望reward为2的值，如图16所示。

图16 赋值的结果

Fig.16 Result of property

6 结论(Conclusion)

本文设计并实现一个框架，允许用高级语言编写场景。靶场攻击策略框架可以分析场景并获取必要的信息，然后加载适当的JSON文件，由JSON文件创建一个固定的结构，它允许向框架提供信息，以便从场景自动创建适当的Prism代码。框架使用这些Prism代码信息生成Prism模型。框架还可以将reward属性应用到创建的Prism模型中，并使用reward结果评估或进一步优化网络靶场，使其更接近真实环境。未来如果有一个著名攻击的数据库，可行的做法是将攻击树集成到框架中，这样可以详细研究攻击方法和防御方法，也可以研究攻击成功的概率。

参考文献(References)

[1] 方滨兴,贾焰,李爱平,等.网络空间靶场技术研究[J].信息安全学报,2016(03):1-9.

[2] 李建华.多元化多层次网络空间安全人才培养创新与实践[J].信息安全研究,2018(12):1073-1082.

[3] 李炜,余慧英,吴华颖.网络空间博弈中的场景研究[J].信息安全研究,2018(5):415-419.

[4] 孙美凤,黄飞,陈云菁.基于特征模式的马尔可夫链异常检测模型[J].计算机工程,2008,34(24):155-156;159.

[5] 王元卓,林闯,程学旗,等.基于随机博弈模型的网络攻防量化分析方法[J].计算机学报,2010,33(9):1748-1762.

[6] 刘智国,于增明,王建,等.面向未来的网络靶场体系架构研究[J].信息技术与网络安全,2018,47(6):41-46.

[7] Arun Prasath Sivanesan,Akshay Mathur,Ahmad Y Javaid. A Google Chromium Browser Extension for Detecting XSS Attack in HTML5 Based Websites[C].2018 IEEE International Conference on Electro/Information Technology(EIT). IEEE,2018.

作者简介：

张月红(1975-)，女，硕士，副教授.研究领域：渗透测试，漏洞挖掘，WEB安全.