BAG-MulVAL 需求分析

项目背景：内网安全态势分析

随着计算机网络的迅速发展和日益普及，网络对于国家、企业、个人的重要性越来越大，网络的规模逐步扩大。然而伴随产生的网络安全问题也越来越严重， 成为影响国家和企业发展的战略要素之一。因此，网络安全技术已经成为信息安全领域的一个研究热点[1]。

人们花费很多的精力、物力和财力来解决这网络系统安全的问题，如提出了“网络与信息系统软件安全检测”、“网络与信息系统软件安全防御”、“网络与信息系统软件安全威胁风险分析”等技术和方法，解决网络与信息系统的安全问题。但这些技术和方法都只是从单一方面解决网络与信息系统软件的安全问题，如何能主动、及时地发现网络与信息系统软件的漏洞，展示漏洞给网络与信息系统带来的危害，防范并消除这些危害，需要有一集**漏洞检测分析、漏洞危害展示与安全量化评估**于一体的综合性的技术和方

法[2]。

如何提升内网安全性

对于个人电脑，人们的安全策略通常是对安全软件扫描到的漏洞进行及时修复，对系统提示的软件与系统升级进行及时升级。

但对于企业网络、工控网络等实时性要求较强的网络系统，漏洞修复、系统升级、软件升级等操作都会干扰网络的工作，影响业务，甚至造成不可挽回的损失。所以对于企业网络等不能采取个人电脑这样简单粗暴的方式提升网络系统安全性，而需要**综合考虑整个网络的安全态势**，折衷地、有选择地进行安全性的提升。

所以需要一种技术和方法来对整个网络进行综合的安全态势分析。

如何进行内网安全态势分析

一般人们通过使用扫描器来得到漏洞信息，对网络安全态势进行评估。

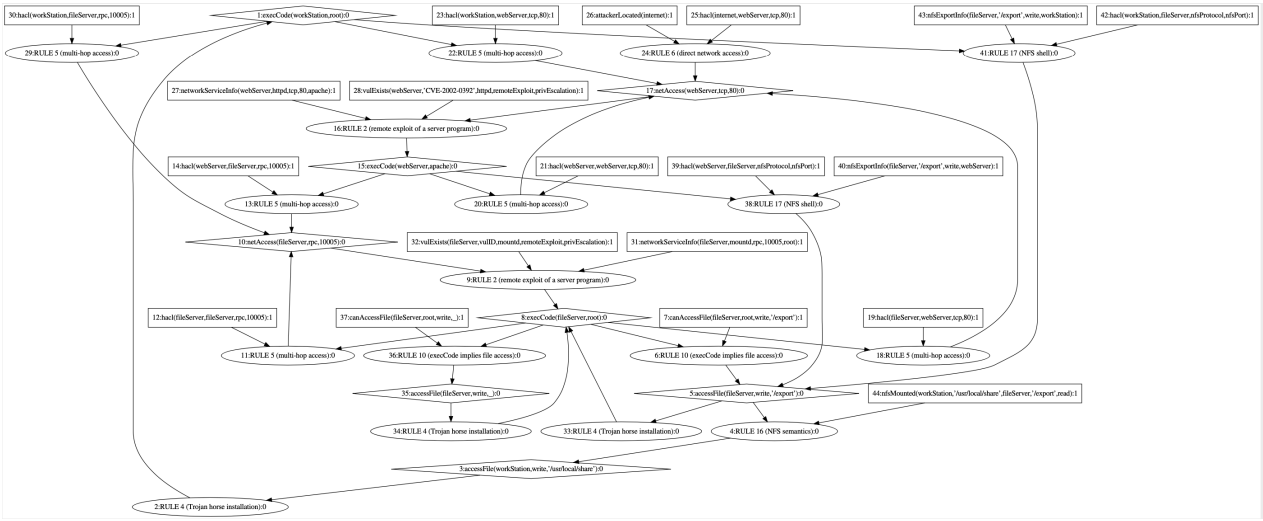
对于个人电脑，一般的扫描器能扫描到本机的漏洞的类型，危害性。对个人电脑来说，这样足矣。但对于大型网络来说，这远远不够。扫描器得出的个体漏洞对本机的危害性并不能体现该漏洞对整个网络的危害性。我们还需要知道漏洞与整个网络的关系，不同主机的漏洞间的关系。因为网络中主机是互联的，一台主机的漏洞会对其他主机产生影响，不同主机之间的漏洞也会相互作用。所以为了分析网络系统的安全性，需要把整个网络的所有主机配置信息、互联信息、漏洞信息结合起来分析。渗透测试就是一种这样的综合分析方法，但渗透测试任务繁重，耗时耗力。所以需要一集**漏洞检测分析、漏洞危害展示与安全量化评估**于一体的快速的综合性的技术和方法。

利用MulVAL[3]：一种企业网络安全分析开源工具

MulVAL的作用

攻击图是一种用图形的方式来描述攻击者从攻击起始点到达到攻击目标的所有攻方法击路径的方法，通过攻击图可以很好的进行网络威胁分析评估。而MulVAL是其中一个较为流行的开源工具。它能基于Datalog和逻辑规则对整个网络的信息进行综合分析，最后生成所有可能的攻击路径，即攻击图，从而辅助进行企业网络安全态势感知。

MulVAL的不足



MulVAL生成内网的整个攻击图，包含所有可能的攻击路径。但由于攻击图时常非常复杂，且包含环路，即无效路径，所以对攻击图进行分析非常困难，甚至难以还原所有攻击路径。如上图就是一张非常复杂攻击图，而实际上这张攻击图对应的网络只有三台主机。所以需要一种方法对MulVAL生成的攻击图进行快速分析。

项目目标

- MulVAL目前只能在Linux上运行，系统的限制阻碍了其使用，且安装较为复杂。所以我通过将MulVAL整合到Linux服务器上的web应用中来解决这个问题。
- 通过图算法与基于CVSS的贝叶斯概率计算，从MulVAL攻击图中**拆分出所有有效的攻击路径**，并计算其**相对攻击成功概率**，即贝叶斯攻击图[4]，解决分析大型网络攻击图的问题。

---

1. 攻击图的网络威胁自动建模方法研究. 程叶霞, 姜文, 薛质, 程叶燕. 通信技术. 1002-0802(2012)09-0086-04 ↩

2. 拓扑漏洞分析及其应用研究. 李腾飞, 李强, 余祥, 黄海军. 第五届中国指挥控制大会论文集 ↩

3. http://people.cs.ksu.edu/~xou/argus/software/mulval/readme.html ↩

4. Computer Network Vulnerability Assessment Based on Bayesian Attribute Network. WANG Xiu-juan, SUN Bo, LIAO Yan-wen, XIANG Cong-bin. 1007-5321(2015)04-0106-07 ↩