攻击图技术综述

胡天翔

November 29, 2016

1 研究背景和内容

目前，计算机网络已然构成了诸多信息技术基础设施的核心组成部分，这些设施包括电网、金融数据系统和应急通信系统领域等。保护这些网络免受恶意入侵对国家的经济和安全至关重要。我们常常能够在被利用来攻击这些系统的软件/应用中发现脆弱性，攻击者就是利用这些被公布或者没有被公布的脆弱性方才得以实施攻击。

但是就目前而言，组织网络的安全风险管理与其说是科学，不如说是一门艺术。系统管理员通过直觉和丰富的经验来操作，而不是依靠客观指标来指导和证明决策的制订。

攻击图技术旨在用于解决此类场景的问题，其包括可用于客观的模型和指标，评估企业网络中的安全风险的分析技术，以及指导管理员使用模型和指标帮助进行网络防御决策的理论和方法。

为了提高组织网络的安全性，有必要测量由不同网络配置提供的安全性。攻击图研究的目的是开发一个标准模型，用于测量计算机网络的安全性。标准模型将使我们能够回答诸如“我们比昨天更安全吗？”或“一个网络配置的安全性如何与另一个进行比较？”这样的问题。另外，有一个标准模型来衡量网络安全可以使用户，软件供应商和研究人员能够一起评估网络安全的方法和产品。

对于组织网络的安全风险分析主要有如下挑战：

安全漏洞非常泛滥 CERT [2]每周会报告约100个新的安全漏洞，这使得对于企业网络的安全管理（包括数百主机、每个主机上不同操作系统和应用程序以及它们上存在的可被利用的漏洞）非常困难。

攻击者发起的多步骤攻击 相比以前攻击者仅能发起简单的原子攻击而言，现在的攻击者为了能够突破各类防火墙/网关的防御，往往会采用多步骤、多宿主的攻击，逐渐渗透进整个网络，最终危及到关键系统。但是其每一步骤却又不足以引起防护系统的警报，这使得对于关键系统的保护具有挑战性。

现有防御手段不能处理攻击的复杂性 计算机系统遭受的攻击逐渐增多，当一个新的漏洞被报告出来

2 攻击图生成技术研究

3 攻击图分析技术研究

4 总结

参考文献

[1] Anoop Singhal, Ximming Ou, Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs, NISTSR 7788, 2011

[2] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison Wesley, 2007.