**第一部分 国内外现状及趋势分析**

一、国外研究现状及趋势

（包括该方面国外的总体研究水平、最新进展和发展预期，国外从事该方面研究的主要机构及其研究方法、成果；相关研究的学术影响、知识产权申请和授予、技术标准制定及产业应用状况，并列出主要的文献，专利、标准名称。限2000字以内。）

网络扫描是指探测局域或者互联网范围服务，搜索漏洞或渗透IT设备方法的行为。国外在该领域研究较早研究水平较高，新的研究成果层出不穷。在网络扫描技术方面从简单的全连接扫描，到半连接扫描再到秘密扫描，从单源扫描到分布式扫描[1]。文献[4]介绍了利用IP报头的时间戳选项进行主动探测的技术可行性评估研究，在扫描工具方面有业内常用的功能强大的nmap[2],也有最近出现的以快著称45分钟扫描整个IPv4空间的zmap[3]，该工具通过对传统扫描技术的发包速度和状态保存等多个优化使其速度达到nmap的1300多倍。

二、国内研究现状及趋势

（包括国内从事该方面研究的主要机构及其研究方法、研究水平；国内外研究方法、研究进展的对比分析；该方面研究可能取得的突破及预期成果。限2000字以内。）

国内在网络扫描方面起步较晚，和国外先进水平存在较大的差距，但是近些年发展速度较快，众多研究机构都在进行相关研究，所以在大规模高速扫描系统方面可能有所突破。

**第二部分 研究内容及目标**

1. 项目研究内容、研究方法及技术路线
2. 申报项目及所属指南方向的关联关系

（二）**项目目标及考核指标、评测方式/方法**

（限800字以内）

该项目的研究目标是在分析现有的网络扫描技术的基础上，针对大规模网络扫描，提出一种新的大规模网络快速扫描系统，并加以实现。做到功能与速度的结合，在扫描覆盖率与准确率相差不大的情况下，大幅提高扫描的速度。

评估方法为：使用相同指定配置的主机或服务器，在相同的网络环境下，对相同数目的目标集使用nmap等现有扫描工具和该项目成果进行多种扫描方式的扫描，记录实验结果中的覆盖率，正确率和完成所耗时间，并进行比较。

考核指标为：在上述实验评估中，在覆盖率和正确率相差不超过5%的情况下，扫描速度与其它工具相比提高3倍以上。

（三）项目成果的呈现形式及描述

（限500字以内）

项目成果以Linux C程序编写的软件形式呈现，在Linux环境下运行，使用精简高效的命令行形式进行操作，软件模块划分清晰，功能完备，提供丰富的功能命令集。针对不同的扫描方式设计多种扫描模块。提供多种输出格式，满足不同的结果形式要求。

二、项目研究内容提、研究方法及技术路线

（一）项目的主要研究内容

（限1500字以内）

该项目主要研究内容是在分析现有的网络扫描技术的基础上，针对大规模网络扫描，提出一种新的大规模网络快速扫描系统，并加以实现。现有的扫描技术有：全连接扫描（Open Scan），半连接扫描（Half-Open Scan），隐秘扫描（Stealth Scans），存活性扫描（Sweep Scans）等。现有的网络扫描工具基本都使用了上述的扫描方法，而且也存在一些不足。Namp的扫描功能比较强大，可以实现端口探测，版本检测和系统检测等，但是在大规模网络应用上存在速度较慢的问题；而近年出现的zmap扫描速度有了很大提升，但是其主要针对的是单端口扫描，功能相对较少。将二者优势结合将具有巨大意义。

（二）项目拟采取的研究方法

1、项目研究拟解决的问题，及拟采用的方法、原理、机理、算法、模型等

（研究方法、技术路线可用图表描述。限800字以内）

该项目旨在解决网络扫描速度和扫描功能的矛盾，在保持多样的扫描功能的同时，相对目前的扫描工具，对扫描速度进行优化和提高。

拟采用namp和zmap等成熟工具的主要技术，并进行结合和优化，进行良好的模块划分和整体架构设计，更好的整合二者的优势。

2、项目研究方法（技术路线）的可行性、先进性分析

（限500字以内）

在对nmap和zmap的深入研究后，对二者的核心技术有了深入理解，对zmap的优化技术的核心及实现有了较深的认识，通过系统设计和模块设计可以将二者的优势分别体现，进一步通过良好的整体架构，就可能将二者优势结合，实现大规模网络扫描速度功能及速度的整体优化。

[1] Bou-Harb, E. et al. 2014. Cyber scanning: A comprehensive survey. IEEE Communications Surveys and Tutorials. 16, 3 (2014), 1496–1519.

[2] Lyon G F. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning[M]. Insecure, 2009.

[3]Durumeric Z, Wustrow E, Halderman J A. ZMap: fast internet-wide scanning and its security applications[C]// Usenix Conference on Security. USENIX Association, 2013:605-620.

[4] W. de Donato, P. Marchetta, and A. Pescap´e, “A hands-on look at active probing using the IP prespecified timestamp option,” in Passive and Active Measurement. Springer, 2012, pp. 189–199.