**组员： 刘云峰 王浩正 霍崧岳 杨峥勇 高倩**

1. **项目概况**

网络扫描，是基于Internet的、探测远端网络或主机信息的一种技术，也是保证系统和网络安全必不可少的一种手段。主机扫描，是指对计算机主机或者其它网络设备进行安全性检测，以找出安全隐患和系统漏洞，网络扫描和主机扫描都可归入漏洞扫描一类。

通过漏洞扫描，扫描者能够发现远端网络或主机的配置信息、 TCP/UDP端口的分配、提供的网络服务、服务器的具体信息等。这也就意味着：黑客利用它来寻找对网络或系统发起攻击的途径，而系统管理员则利用它来有效防范黑客入侵。

1. **运行环境**

Linux

1. **扫描原理**

漏洞扫描可以划分为ping扫描、端口扫描、OS探测、脆弱点探测、防火墙扫描五种主要技术，每种技术实现的目标和运用的原理各不相同。

按照 TCP/IP协议簇的结构，ping扫描工作在互联网络层；端口扫描、防火墙探测工作在传输层； ping扫描确定目标主机的IP地址，端口扫描探测目标主机所开放的端口。

1. **功能**

扫描器并不是一个直接的攻击[网络漏洞](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%BC%8F%E6%B4%9E" \t "https://baike.baidu.com/item/_blank)的程序，它仅仅能帮助我们发现目标机的某些内在的弱点。一个好的扫描器能对它得到的数据进行分析，帮助我们查找目标[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "https://baike.baidu.com/item/_blank)的漏洞。但它不会提供进入一个系统的详细步骤。

扫描器应该有三项功能：发现一个主机或网络的能力；一旦发现一台主机，有发现什么服务正运行在这台主机上的能力；通过测试这些服务，发现漏洞的能力。

编写扫描器程序必须要很多TCP/IP程序编写和C,Perl和或SHELL语言的知识。需要一些Socket编程的背景，一种在开发客户/服务应用程序的方法。开发一个扫描器是一个雄心勃勃的项目，通常能使程序员感到很满意。

　　此外，网络扫描时发送的数据或多或少都会含有扫描 者自身相关信息，从而也可以抓取扫描时的数据包，对扫描者进行反向追踪，这也是一个值得研究的方向。