功能概述

在日常运维过程中，经常会遇到需要确认终端端口开放状态的场景，例如确认某终端上共享打印机是否正常开放对应端口供连接。

功能介绍

nmap工具属于早期的Linux下的网络扫描和嗅探工具包，属于网络连接端扫描软件，可用来扫描网上电脑开放的网络连接端信息，确定服务运行情况及端口连接情况，并且可以推断目标终端的操作系统版本信息。

安装使用

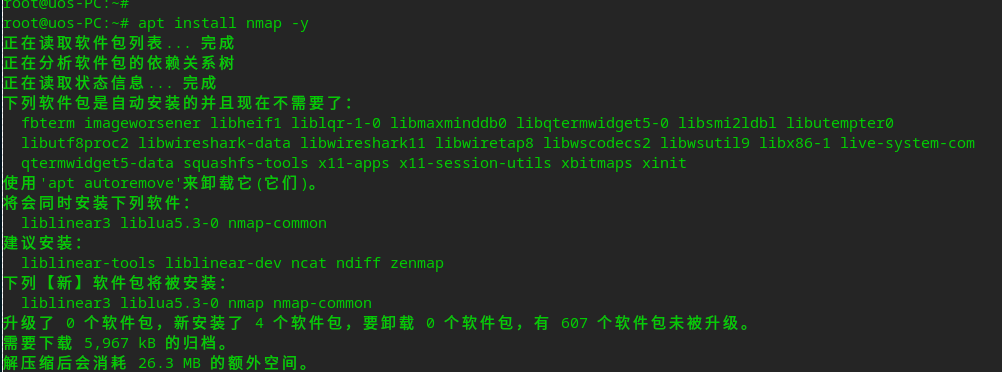
nmap工具相关的用途说明：

* 检测网络上的主机
* 检测主机上开放的端口
* 检测操作系统，硬件地址，以及软件版本
* 检测脆弱性的漏洞（nmap的脚本）

下面以用户需求统计同一个网段的局域网内设备MAC地址作为举例说明如下：

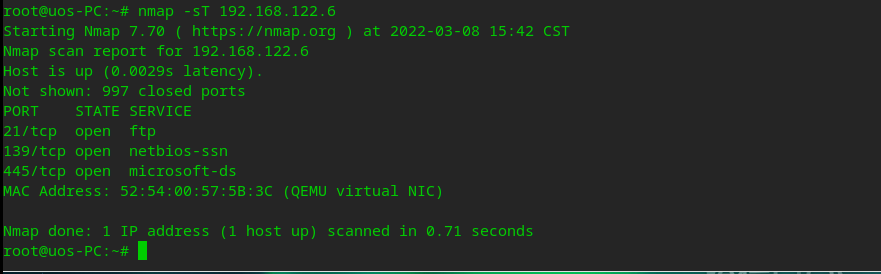
一：安装工具

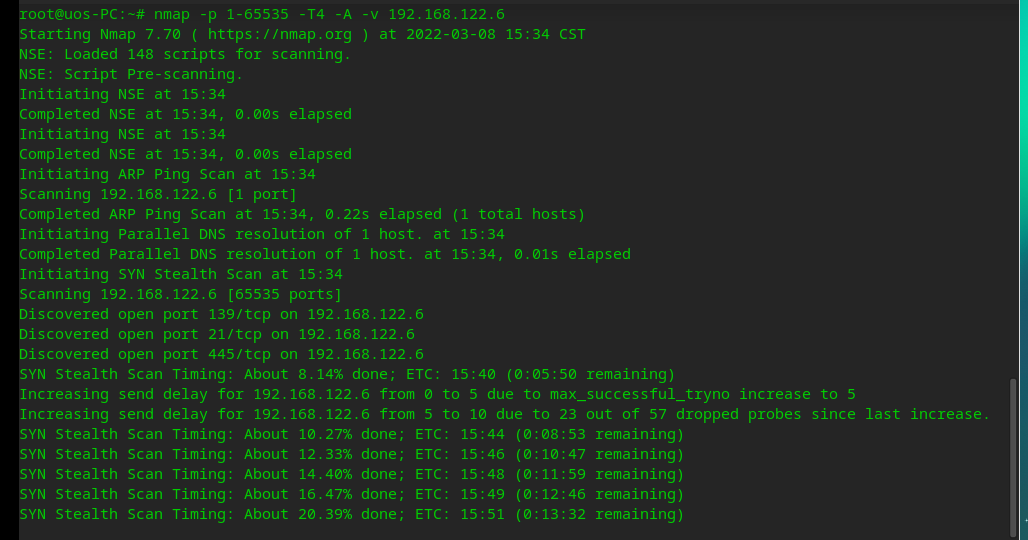
uos@uos-PC:~$ sudo apt install nmap



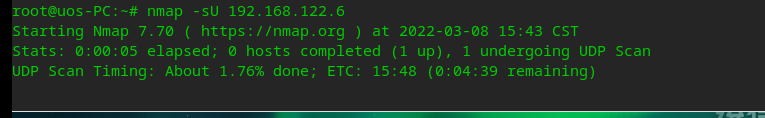
二：扫描某主机（以192.168.122.6举例）TCP及UDP端口并生成报告

a、 扫描TCP端口





b、 扫描UDP端口

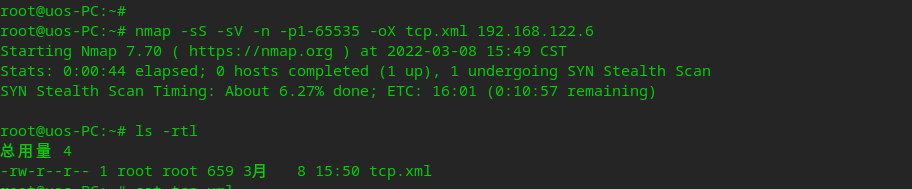


c、生成报告：

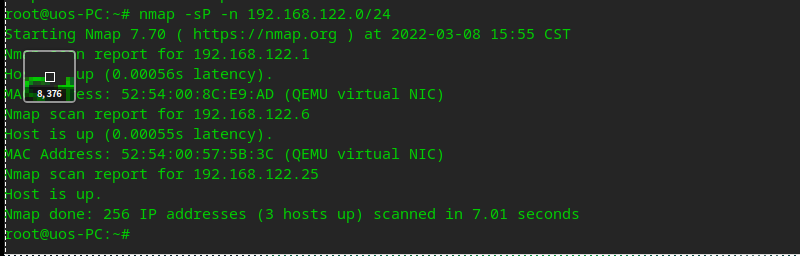
输出指令相关的参数介绍如下：

-oN  文件名 #输出普通文件

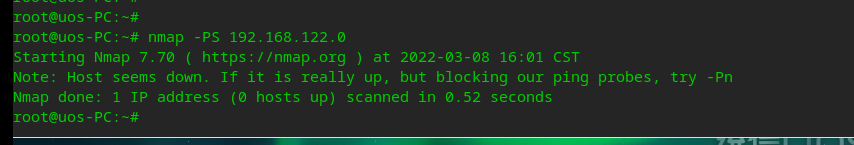
-oX  文件名.xml #输出xml文件



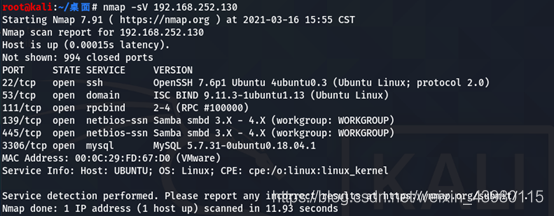
三：扫描网段内（以192.168.122.0/24举例）活跃设备的MAC地址



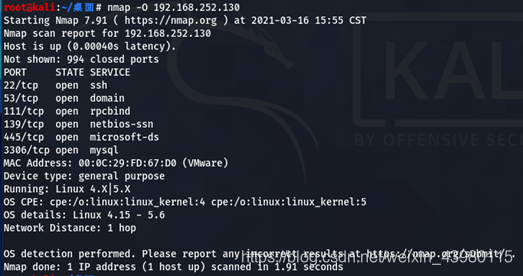
四：扫描网段内（以192.168.122.0/24举例）活跃的终端



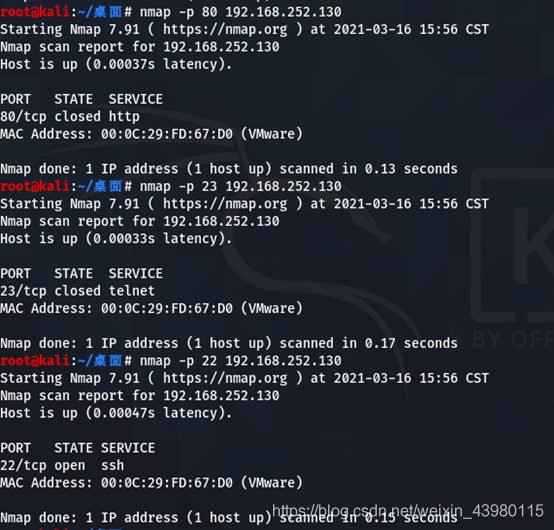
五：查看开放端口提供服务的对应版本信息



六：查看某终端的操作系统版本信息



七：扫描特定主机的特定端口



©统信软件技术有限公司。访问者可将本网站提供的内容或服务用于个人学习、研究或欣赏，以及其他非商业性或非盈利性用途，但同时应遵守著作权法及其他相关法律的规定，不得侵犯本网站及相关权利人的合法权利。除此以外，将本网站任何内容或服务进行转载，须备注：**该文档出自【faq.uniontech.com】统信软件知识分享平台**。否则统信软件将追究相关版权责任。