我们组主要实现了对教育网中清华IP段的多方面的分析，并实现了多功能的P检索系统。

我们将分为四个部分展示：数据测量，数据分析，并将展示我们的网站DEMO，最后是Qand A环节。

首先是数据测量，数据测量花费时间很多：我们采用多来源的数据

一个是通过nmap工具测量，将timeout设置为了60s

另外我们还综合了censys的开放API

接着我们将展示我们的数据分析部分：

基于端口状态，网络资源位置，网络设备的端口空闲程度，网络设备的服务名称，

1. 基于端口状态，我们将获取的端口状态根据返回信息分为open,closed,filtered三类，覆盖全部端口的状态情况
2. 端口服务：过滤掉出现次数不超过50次的服务

--------------------------------------------------------------------------------------------------------

在校内活跃着很多主机，他们为不同范围的用户提供者各种各样的服务。比如为实验室提供Gitlab，wiki等http服务，提供数据库服务，提供远程ssh连接服务，或者提供网络打印服务；或者比如为系内甚至全校提供报名，审批等http服务。通过这些服务我们可以推测出主机的运营者是如何通过网络服务用户的工作和生活的。所以，我们希望通过扫描全校的在线主机，得到在不同端口开放的网络服务，最终对全校的网络服务使用情况得到一个总体的认识。

---------------------------------------

（3）HTTP类：图中明显可以看出，http服务占比超过了一半，再加上其他的http类的服务，总数远高于安全性比较高、现在普遍比较提倡使用的https。

（4）FTP类：ftp和ftp-data加起来超过了90%，而采用加密传输的ftps、rsftp则只有零星的一点。

由此可见，尽管服务种类非常丰富，但存在比较多的问题，比如http、ftp的服务种类大多比较陈旧，可能带来潜在的安全问题。

1. SSH服务：（openssh占据了完全的统治地位。但是我们可以看到大部分openssh版本都比较旧，几乎没有使用最新的openssh 7.6的。这可能带来一些安全隐患。）

我们可以看出校内活跃着五花八门的网络服务。但是其中存在很多问题，比如说Https的数量远远不如Http，比如大多数SSH服务的版本都很陈旧，这都会带来潜在的安全问题。

59.66.109.9、59.66.200.76均有1000个端口（端口数超过30的只有这两个i）

（6）网络设备空闲程度：图中是去掉了两个有1000多个端口的异常ip之后，ip的端口数的柱状图。

（7）网络设备空闲程度：由此可见，清华校内的资源比较富足，从端口的角度看，空闲比例相当高。

这一段对应分布在号数大于等于14的紫荆公寓。那一片是W楼博士生宿舍。我们推测，可能是博士生时常需要在实验室远程登录放在宿舍的台式机，所以telnet和snmp格外地多。

DEMO演示：如何高效的获得类似的信息？解决方案！