### vpn漏洞挖掘方法

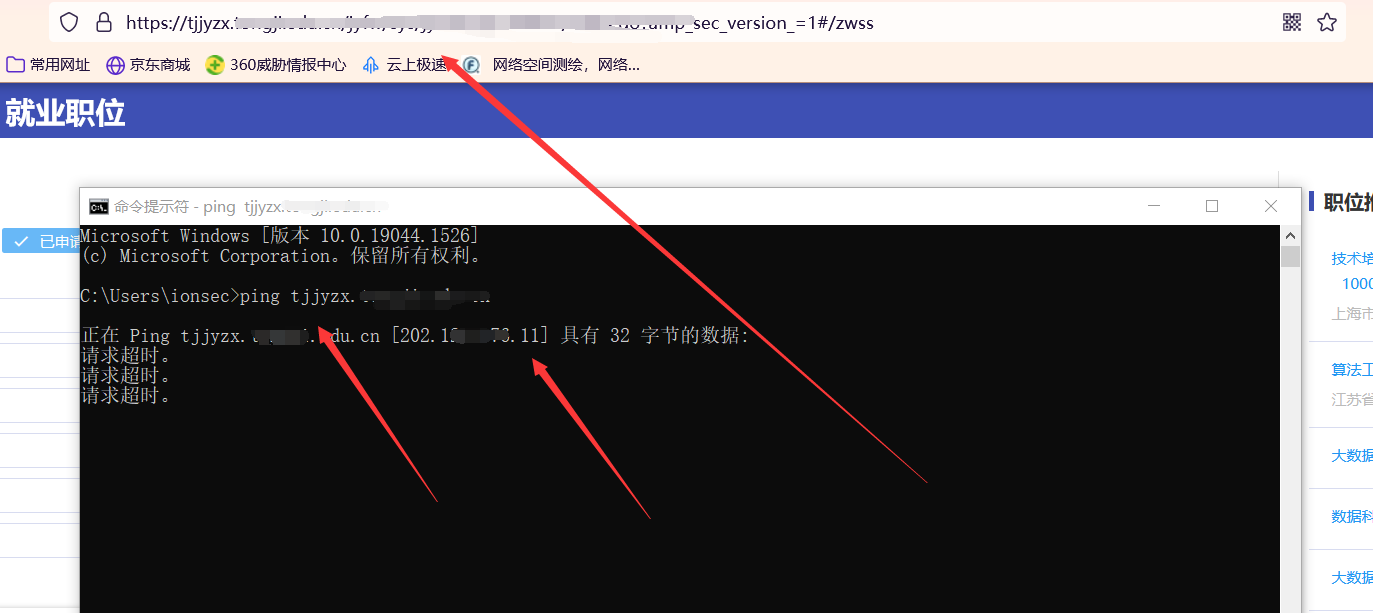
1. 当你获取到sslvpn的时候，你可以进入内网，对其网段进行扫描挖掘漏洞，在内网中的漏洞是非常多的，比如数据库弱口令、ssh弱口令、设备弱口令、nday等等漏洞，当然这些都可以使**用fscan进行**即可

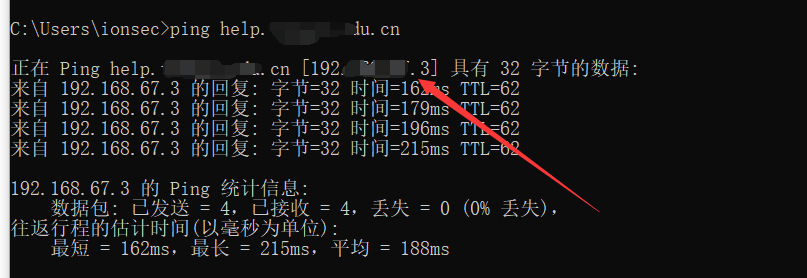
网段的获取：

登录一站式服务大厅：



来到这里将能打开的应用都打开，然后获取url进行ping



可以获取到一个ip，此时可以猜想这个网段肯定不止这一个服务然后进行二分法对b段ping存活即可

同理如上图可以看出存在192这个网段，那么就可以继续对这个网段利用python来探测b段或者使用Namp等工具。