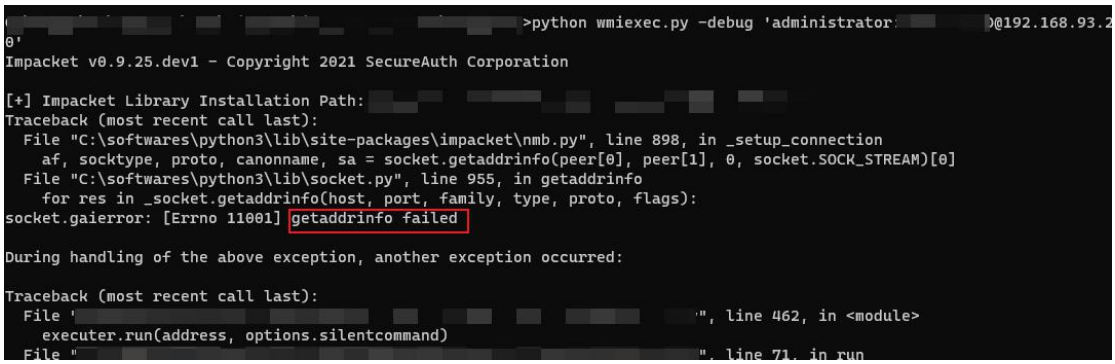
场景：
-打内网，需要用本机上的工具，但是使用 cmd 运行工具，流量一直代理不进去，工具一直报错。
-打内网的时候尝试 ping 目标，此时本机已经挂上了代理，但是没法正常连进内网

先说解决方案，解决第一个问题，得把 cmd 换成 powershell。
解决第二个问题，需要把 ping 换成 curl。

稍后再说原因，先实操。
//前置条件，proxifier 已经配置好了，如图：

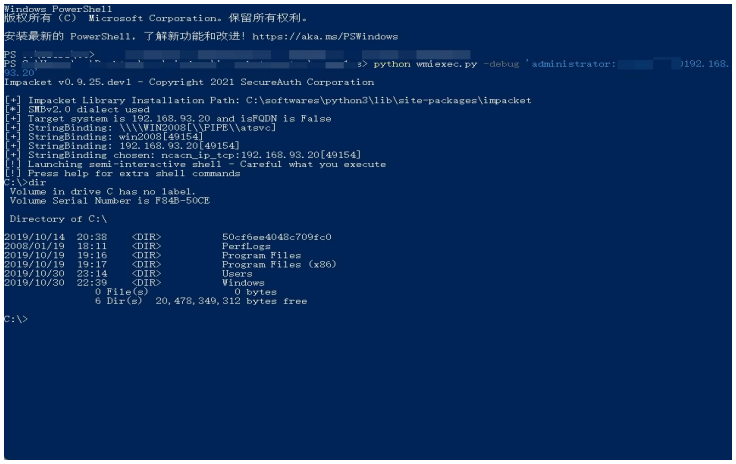
我这里用的是 socks5 代理

然后打开 cmd，尝试使用 impacket 中的 python 工具包的 wmiexec 去连接内网的机器



很显著的一条报错，获取地址信息失败，这里可以理解为流量没代理进去。
那么为什么会出现这种问题呢？
因为用的是 cmd

这里换 powershell 再进行同样的操作

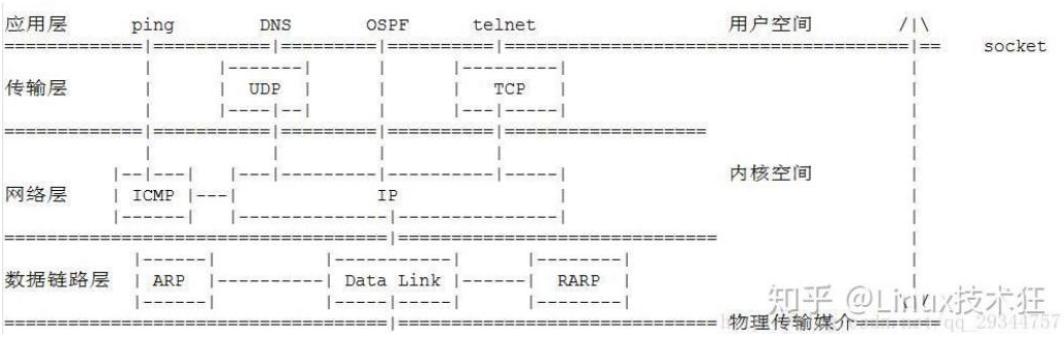


成功代理了进去，并且还能正常执行命令

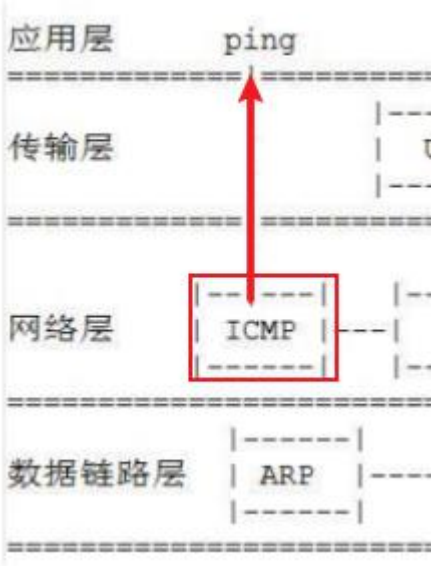
具体和 cmd 和 powershell 的特性有关，这里不去深究，只要知道执行命令，如果想走代理，

需要用 powershell 即可。

第二个问题，即便走了代理，也无法 ping 通内网。



看图比较好理解
ping 是 icmp 协议，上图可以很明显的看到，一根直线直接通上去了。



而我这里用的 socks5 代理，socks5 代理可以代理 tcp/udp 协议，因此也可以代理基于 tcp/udp 的 http/https 协议，但是代理不了 icmp 协议，因此 ping 命令无法走代理。
所以探测内网机器存活，如果想把流量代理进去，可以使用 curl 命令。

done