网安实践（二）暨virtualbox使用踩坑

硬件部分

遇到的问题：

* 在不开启硬件3D加速的情况下，虚拟机的图形运算是由主机的cpu完成的，因此对轻薄本使用的性能较弱的低压U负载较大
* 在virtualbox内安装win10虚拟机且开启增强功能以调整分辨率后，假如同时开启了硬件3D加速，则会发生界面加载错误的情况（似乎类似显卡驱动错误）
* 还有一点很坑：不能利用睿频，所以（好像）会一直运行基频下；这对Intel 10代酷睿这种基频奇低的CPU简直是巨大的打击……

临时的解决方案：

* 为虚拟机分配2个核，4线程（不确定是否能够使用超线程）
  + 从任务管理器来看，不能使用超线程
* 调小窗口，减缓运算压力
* 允许风扇在噪音可接受的范围内提高转速

软件部分

遇到的问题

* 微软提供的vs开发包都大的出奇……尤其是最近的vs19/20，竟然要10GB以上空间
* 文件传输问题，没有在主机和虚拟机之间快速通讯的工具
* DVWA的下载安装问题；
  + 问题1：校园网无法访问GitHub
  + 问题2：在chrome中下载后显示权限失败；（似乎是一个自解压zip文件）
* win10防火墙：
  + 设置入站和出站规则在控制面板而非设置
  + 非常强大，在win10下运行的ie也会利用windows defender
* 事实证明，win10最烦人的地方在于更新，后台运行且极占资源
  + 被感染了竟然还在更新……

解决方案

* 向老师询问后得知需要使用windows SDK，所以还要再考虑
  + 使用了vc6
* 在主机搭建了一个python ftp服务器，设置虚拟机网络连接方式为NAT，双方都能ping通后在虚拟机中成功访问
  + 换成了http服务器，py自带的，临时用一下还是可以的
* 依然没有成功下载，让同学给我发了一个，再用上面的服务器发过去
* 暂时还没看懂

Wannacry相关

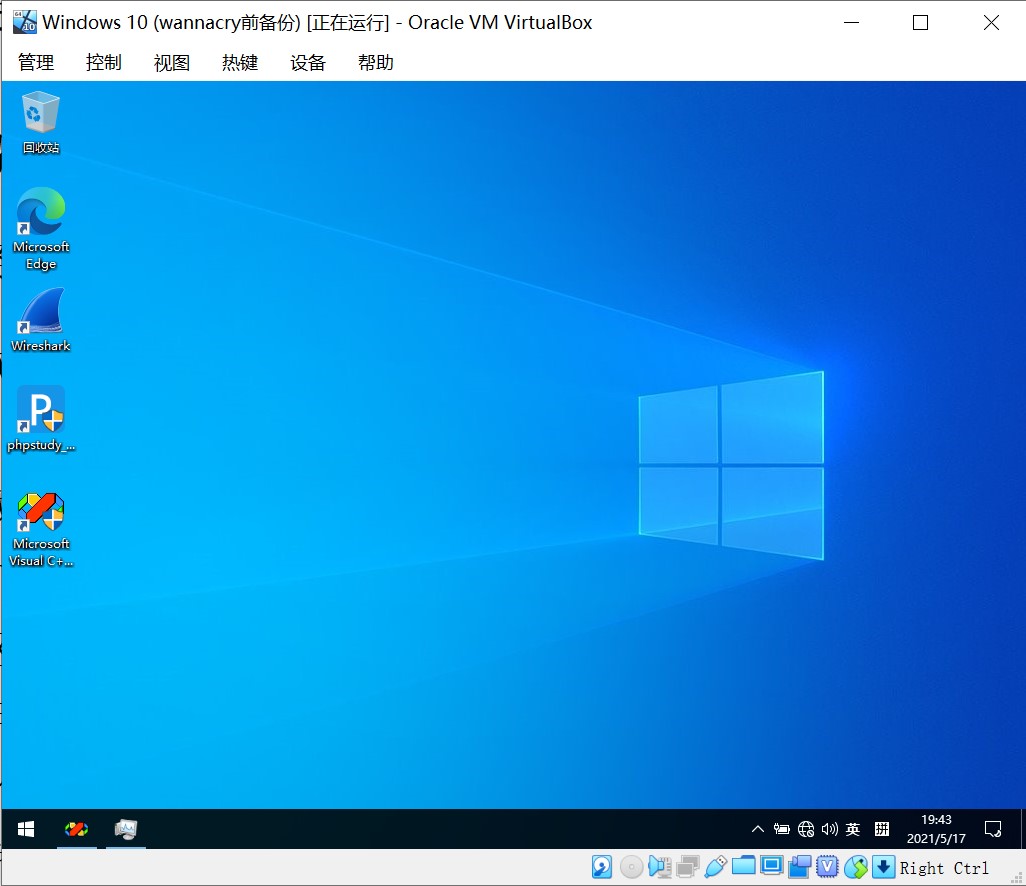
现象观察

* 创建了部分文件于桌面（也可能是病毒同级文件夹）
* 跳出一个是否执行cmd命令的提示框，查询得应该是在利用cmd直接添加注册表
* 查看任务管理器，发现diskpart在运行且消耗cpu资源，猜测正在进行大规模硬盘读写（但是diskpart不是用来分区的吗）
* 桌面更改，文件变化，记事本打开后出现以WANNACRY开头的乱码
* 硬盘空间被几乎占满，出现一个名为hibsys.WNCRYT的文件，在appdata的temp文件下

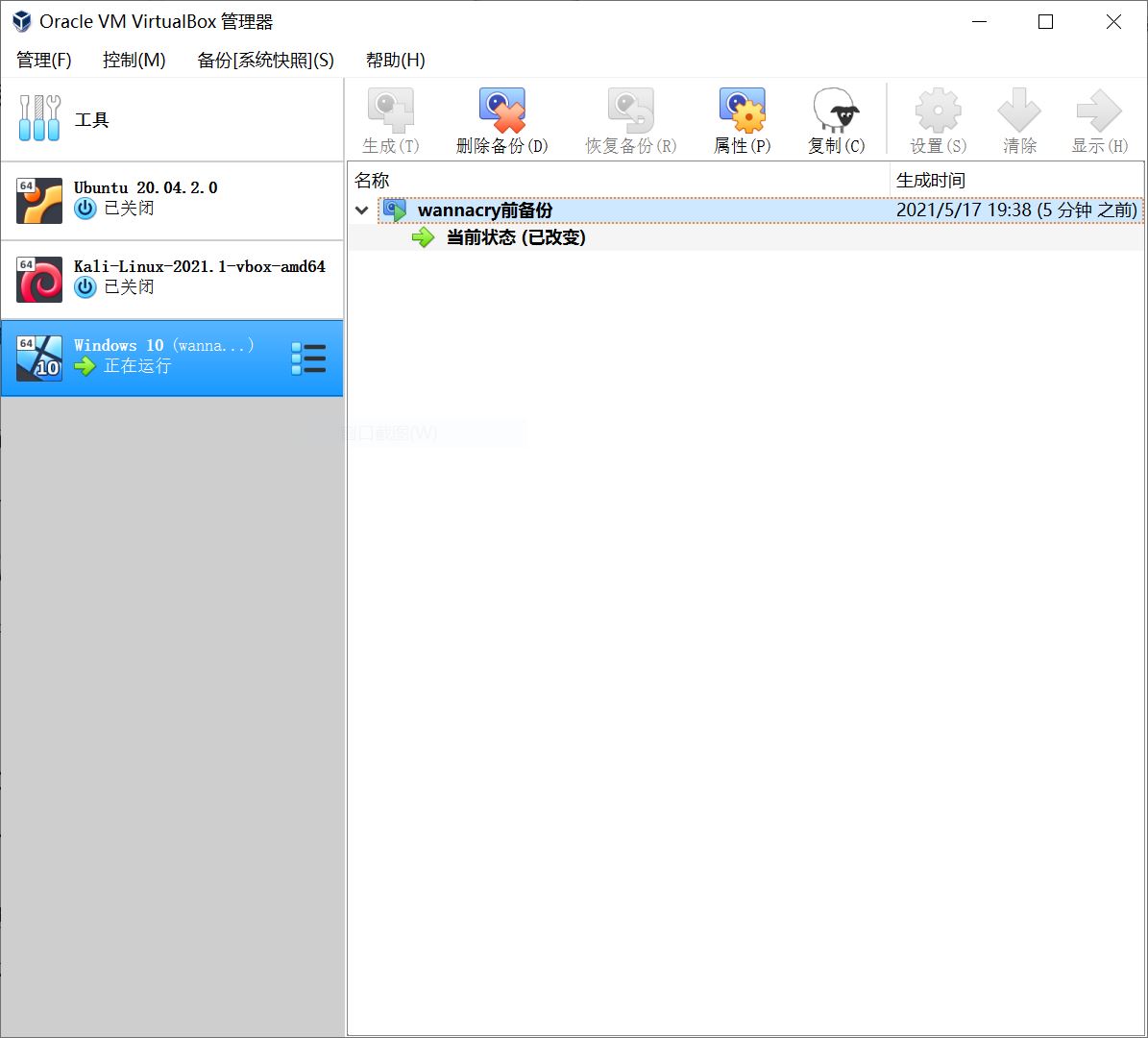
应对措施

* win10几乎不可能被感染，除非所有的病毒防护和防火墙全部关闭
* 查询得知，wannacry会先创建加密文件，再删除源文件
  + 因此，在短时间内，可以恢复部分被删除的文件（机械硬盘似乎很有优势）
  + 但是由于文件读写操作过多，能恢复的文件非常有限
  + 多硬盘，多设备备份，异地备份，云备份将会非常有效
* 及时关闭网络（甚至拔网线），断电，阻止继续加密，在其他设备上插入硬盘进行备份

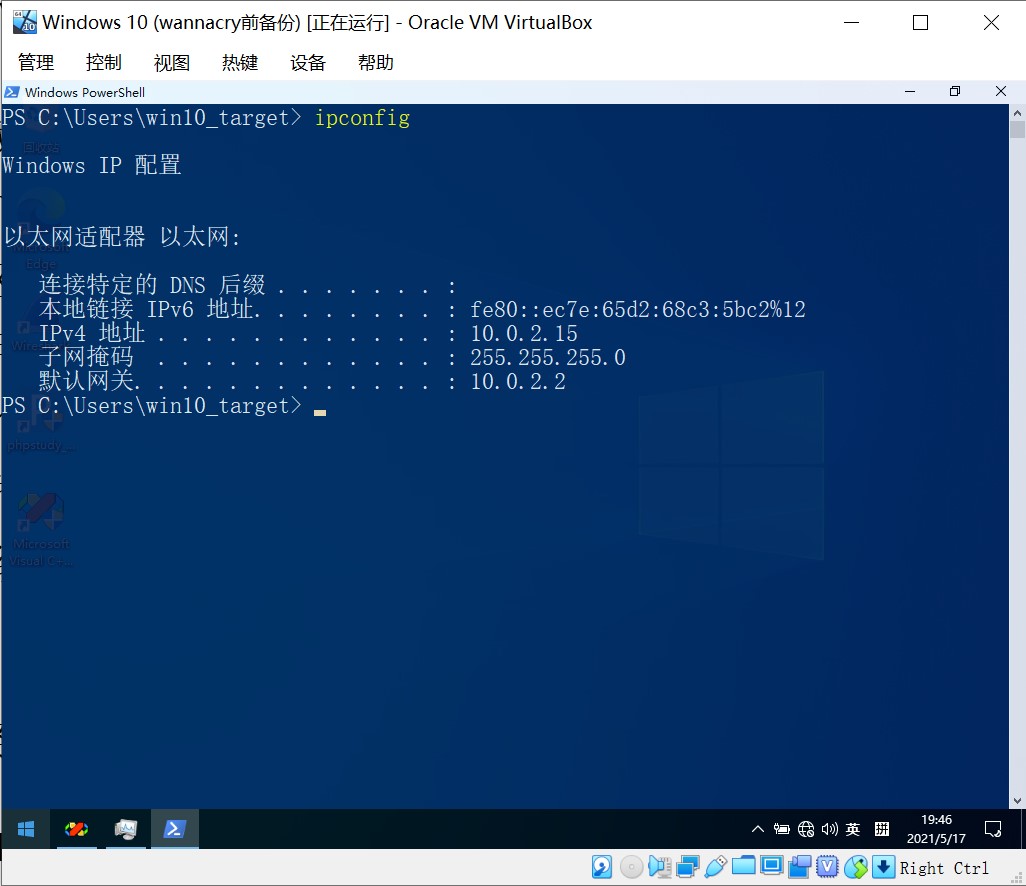
截图如下：



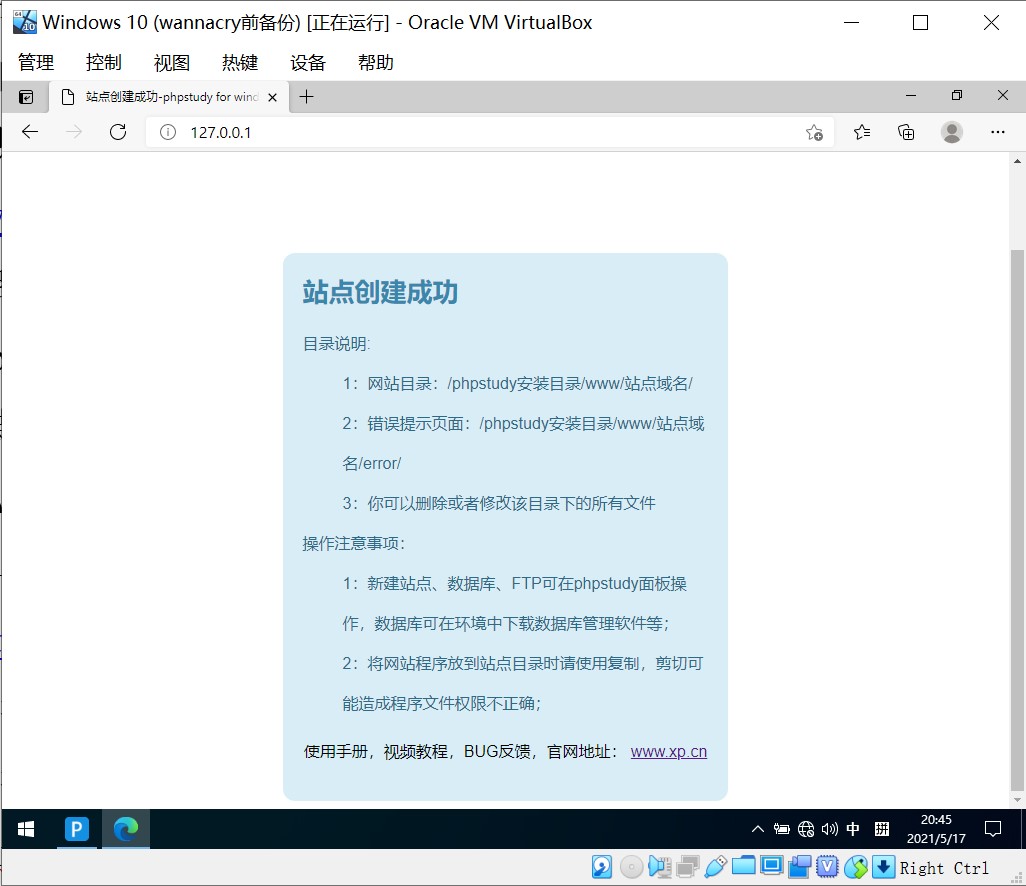
安装win10靶机



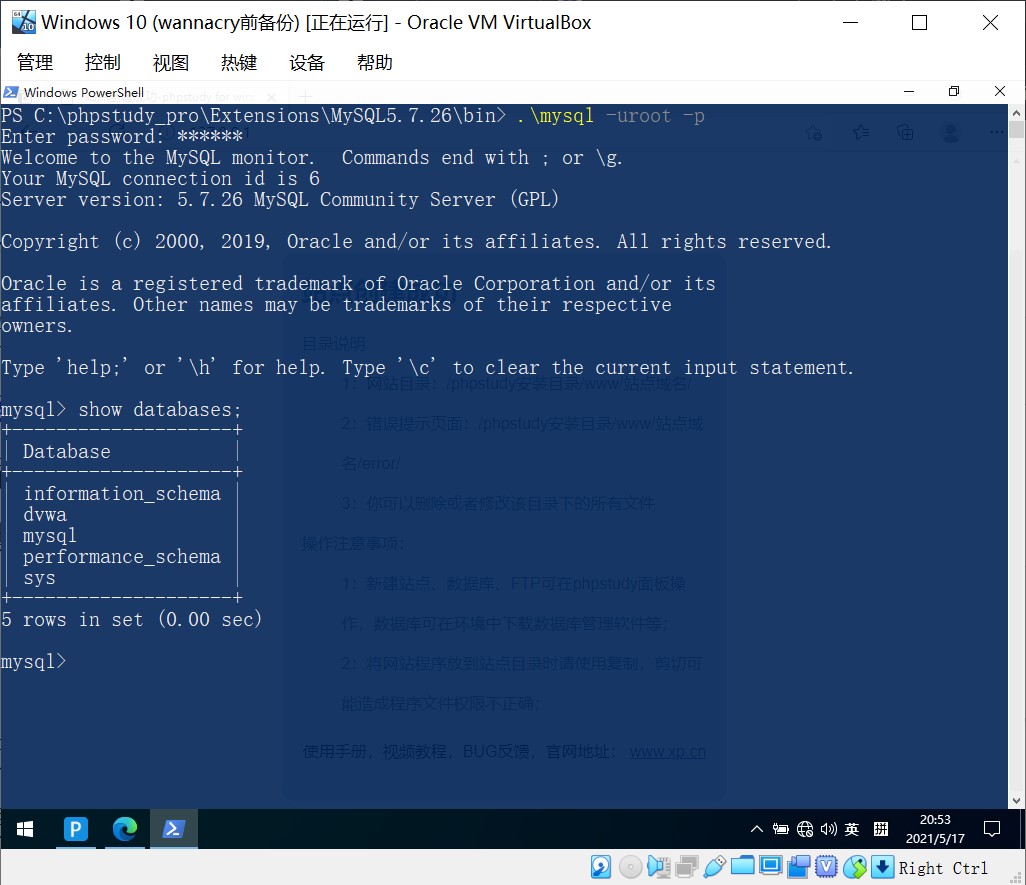
快照备份



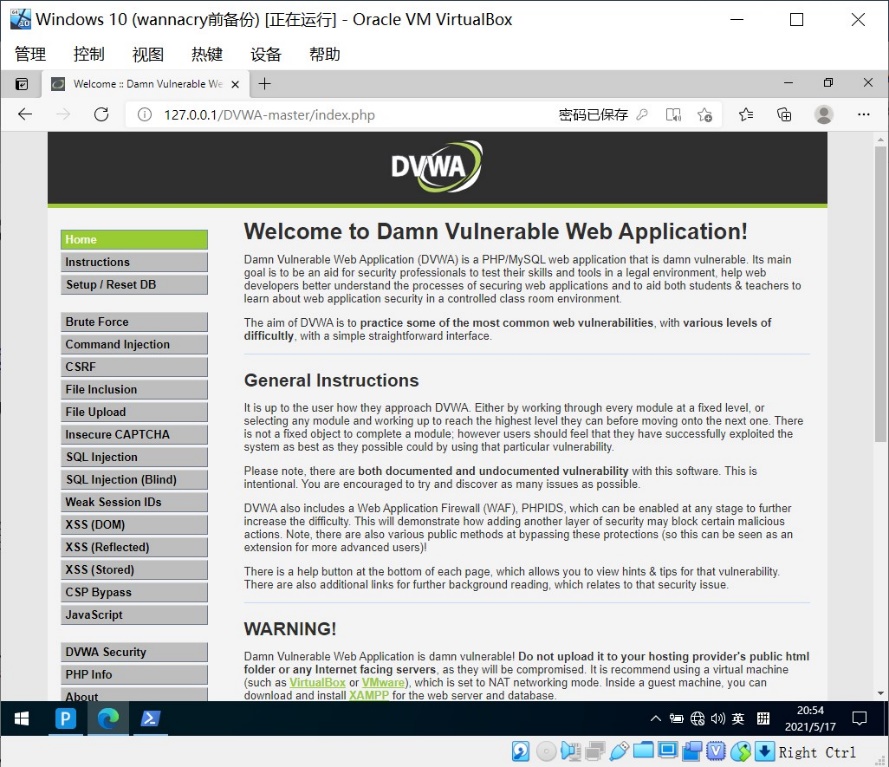
Ipconfig查看网络情况



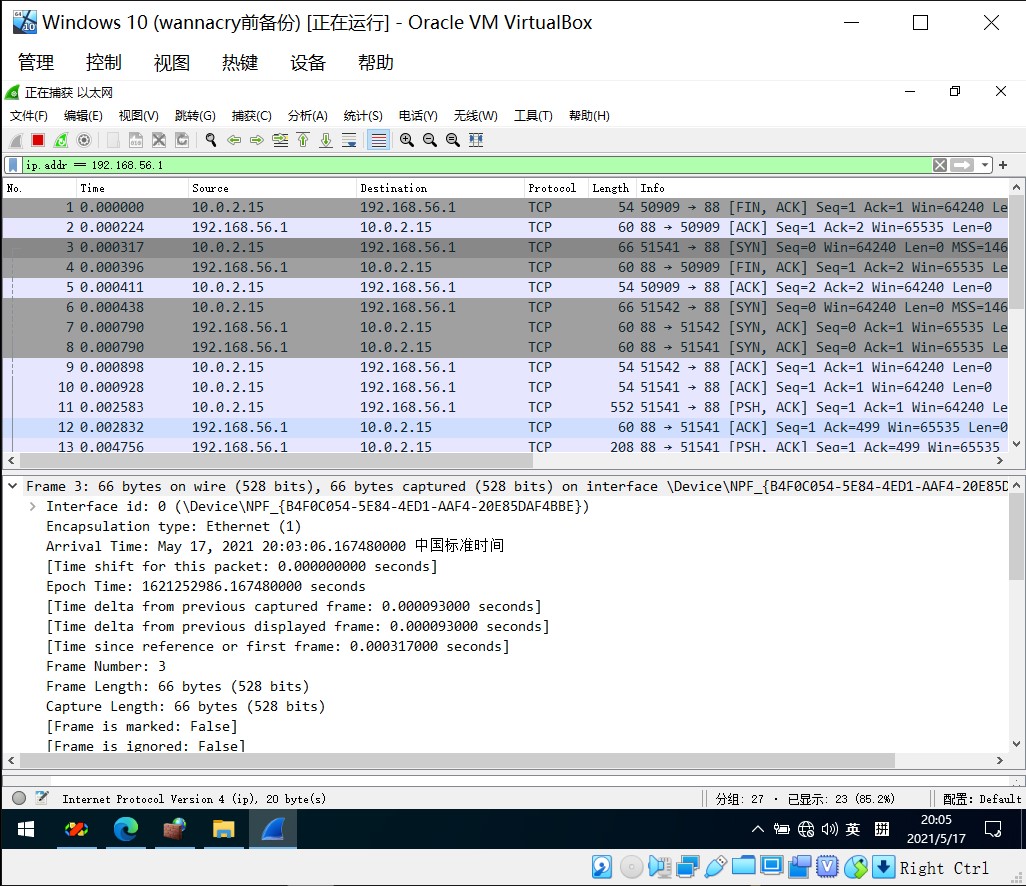
安装phpstudy



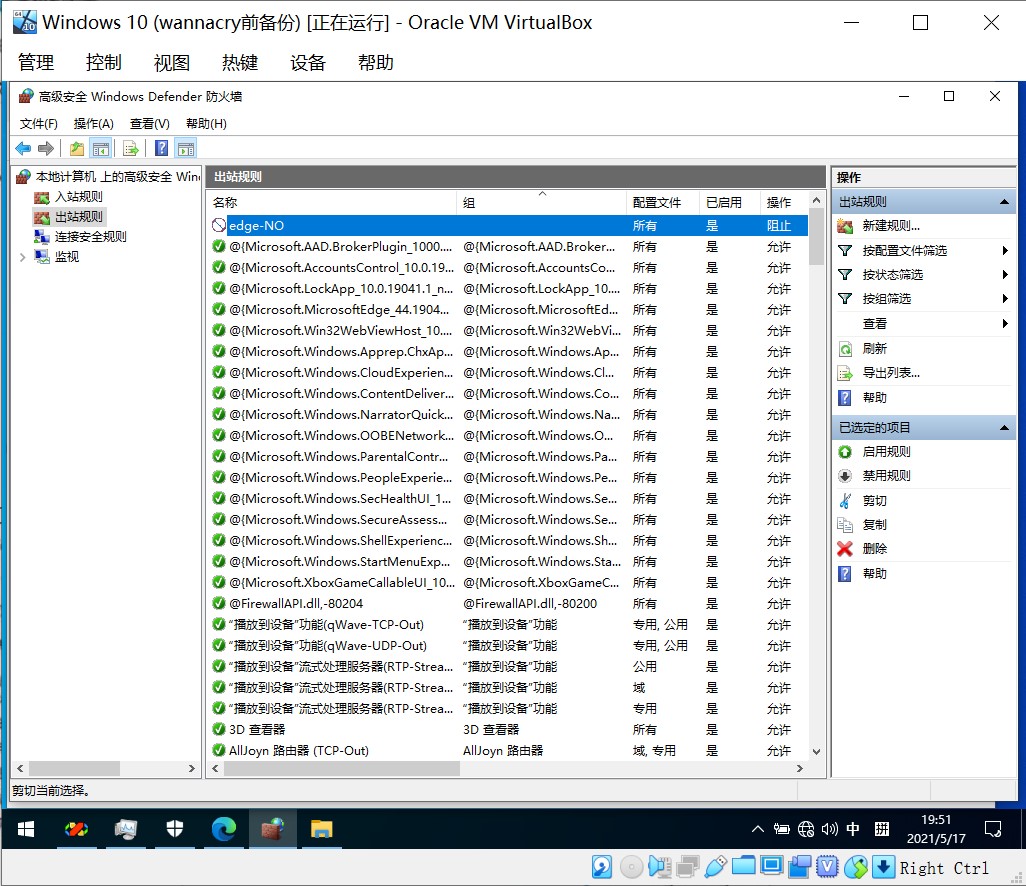
命令行中的mysql服务



DVWA安装



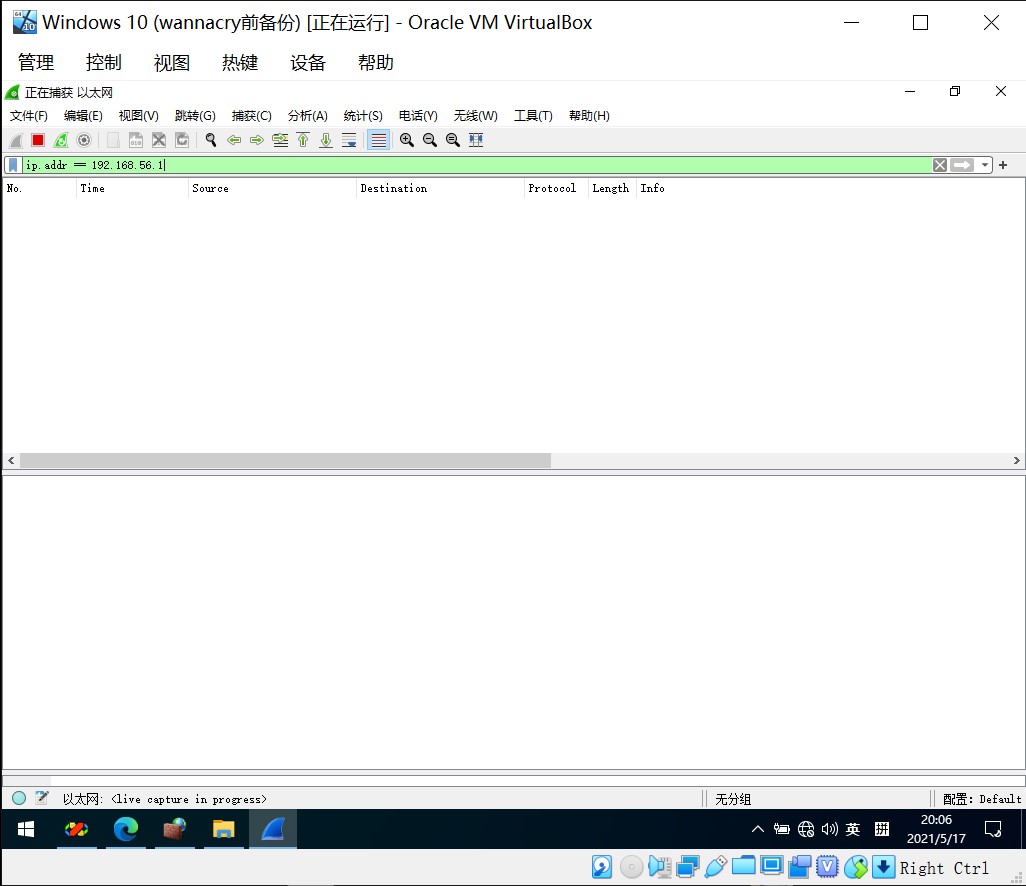
以查看主机http服务器为例



添加针对edge浏览器的出站规则



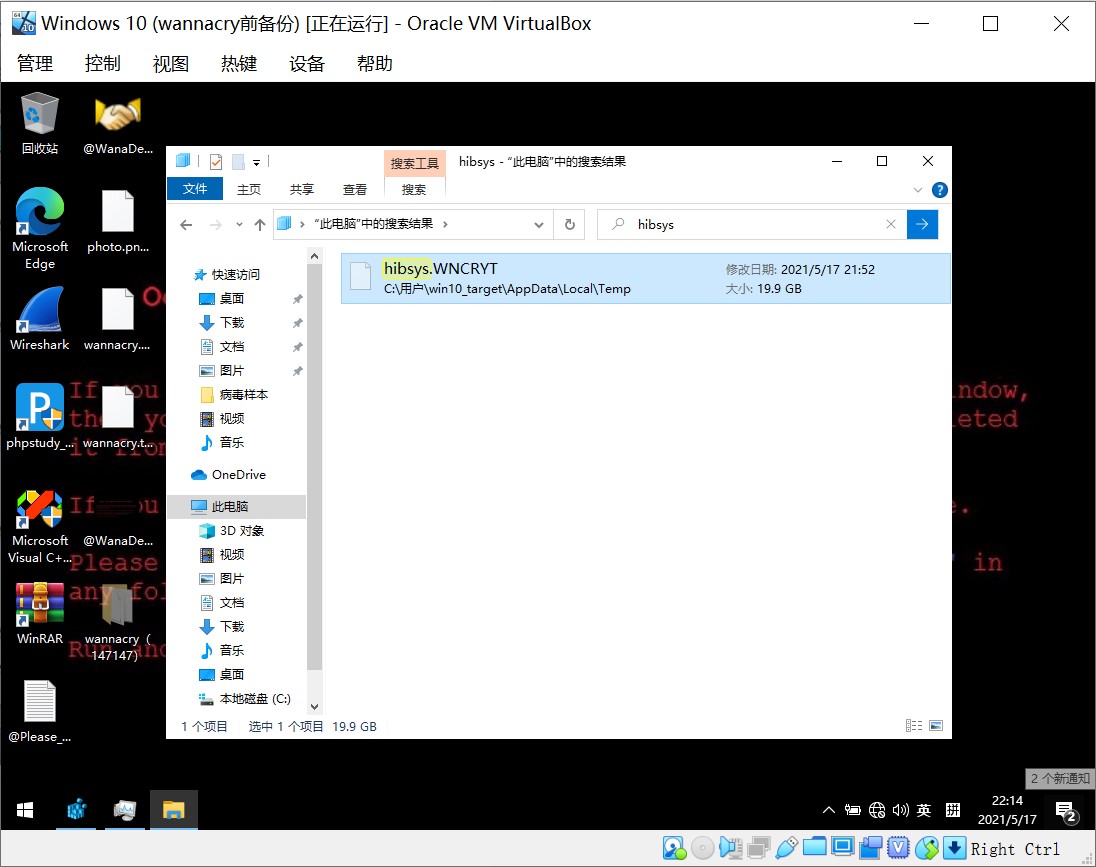
启用出站规则后



Wireshark抓包情况



启动wannacry



Wannacry自动创建的文件