**40、[安洵杯 2019]Attack**

foremost命令分离出压缩包，wk,加密了。用wireshark打开，文件->导出对象->http->save all，发现lsass.dmp，lsass.dmp放到mimikatz.exe目录下,在mimikatz\_trunk\x64目录下执行下列命令。

privilege::debug  
sekurlsa::minidump lsass.dmp  
sekurlsa::logonpasswords full

得到密码解压。