界面左上角是菜单按钮和搜索栏。三个选项卡分别是数据库信息（Database Info）、节点信息（Node Info）和查询（Queries）。数据库信息选项卡中显示了所分析域的用户数量、计算机数量、组数量、会话数量、ACL 数量、关系等信息，用户可以在此处执行基本的数据库管理操作，包括注销和切换数据库，以及清除当前加载的数据库。节点信息选项卡中显示了用户在图表中单击的节点的信息。查询选项卡中显示了 BloodHound 预置的查询请求和用户自己构建的查询请求。

界面右上角是设置区。第一个是刷新功能，BloodHound 将重新计算并绘制当前显示的图形；第二个是导出图形功能，可以将当前绘制的图形导出为 JSON 或 PNG 文件；第三个是导入图形功能，可以导入 JSON 文件；第四个是上传数据功能，BloodHound 将对上传的文件进行自动检测，然后获取 CSV 格式的数据；第五个是更改布局类型功能，用于在分层和强制定向图布局之间切换；第六个是设置功能，可以更改节点的折叠行为，以及在不同的细节模式之间切换。

2.14.2 采集数据

在使用 BloodHound 进行分析时，需要调用来自活动目录的三条信息，具体如下。

- 哪些用户登录了哪些机器？
- 哪些用户拥有管理员权限？
- 哪些用户和组属于哪些组？

BloodHound 需要的这三条信息依赖于 PowerView.ps1 脚本的 BloodHound。BloodHound 分为两部分，一是 PowerShell 采集器脚本（有两个版本，旧版本叫作 BloodHound_Old.ps1，新版本叫作 SharpHound.ps1），二是可执行文件 SharpHound.exe。在大多数情况下，收集此信息不需要系统管理员权限，如图 2-93 所示。

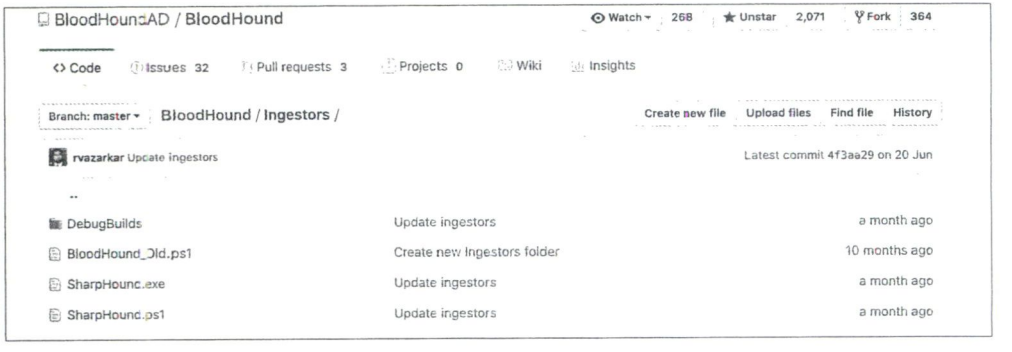

图 2-93 下载数据并采集脚本