链滴

drozer 安装与使用

作者：Mrq123
原文链接：https://ld246.com/article/1597316604400
来源网站：链滴

```
<pre><code class="highlight-chroma"><span class="highlight-line"><span class="highlight
cl">因工作需求要对某app进行测试，因为此前没有app测试经验，打算使用漏扫一把梭。挑选droza
此app进行测试。
</span></span></code></pre>


<h2 id="1-安装">1.安装</h2>
<pre><code class="highlight-chroma"><span class="highlight-line"><span class="highlight
cl">首先需要使用adb对手机进行连接，这里使用逍遥模拟器。
</span></span><span class="highlight-line"><span class="highlight-cl">对连接主机查看，
使用一下命令，下文会有解释。。
</span></span></code></pre>
<pre><code class="highlight-chroma"><span class="highlight-line"><span class="highlight
cl">adb devices
</span></span></code></pre>
<pre><code class="highlight-chroma"><span class="highlight-line"><span class="highlight
cl">adb forward tcp:31415 tcp:31415
</span></span></code></pre>
<p><img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2020/08/image-644ffd7e.png?imageView2/2/interlace/1/format/jpg"><b
>
也可以使用 adb shell，对主机进行操作。<br>
在模拟器上安装 drozer-agent，其开启 31415，上文 adb 已对其进行连接。<br>
<a href="https://ld246.com/forward?goto=https%3A%2F%2Fgithub.com%2Fmwrlabs%2Fdro
er%2Freleases%2Fdownload%2F2.3.4%2Fdrozer-agent-2.3.4.apk" target="_blank" rel="nofoll
w ugc">https://github.com/mwrlabs/drozer/releases/download/2.3.4/drozer-agent-2.3.4.apk
/a><br>
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https://b3
ogfile.com/file/2020/08/image-49b75696.png?imageView2/2/interlace/1/format/jpg"><br>
等待 drozer 连接。<br>
在安装 drozer 所需要的库时候，遇到了 pip install 总是超时的问题，所以在终端设置了 http 代理
不知道是不是我的 ssr 有问题，报错原因是代理处池的问题。所以选择了 V2rayN，设置 http 代理后
重启终端就可以了（按照道理来说，关闭终端临时的代理会取消，不知道为啥会这个，可能当时开了
多终端吧）。</p>
<pre><code class="highlight-chroma"><span class="highlight-line"><span class="highlight
cl">set http_proxy=http://127.0.0.1:1080
</span></span><span class="highlight-line"><span class="highlight-cl">set https_proxy=h
tp://127.0.0.1:1080
</span></span></code></pre>
<p><img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2020/08/image-3b80645f.png?imageView2/2/interlace/1/format/jpg"><b
>
下面开始安装 drozer。</p>
<pre><code class="highlight-chroma"><span class="highlight-line"><span class="highlight
cl">pip2 install wheel
</span></span><span class="highlight-line"><span class="highlight-cl">pip2 install pyyam

</span></span><span class="highlight-line"><span class="highlight-cl">pip2 install pyha
crest
</span></span><span class="highlight-line"><span class="highlight-cl">pip2 install proto
uf
</span></span><span class="highlight-line"><span class="highlight-cl">pip2 install pyope
ssl
</span></span><span class="highlight-line"><span class="highlight-cl">pip2 install twiste
```

pip2 install service identity
</code></pre>
<p>之后下载 drozer-2.4.4-py2-none-any.whl 文件。</p>
<pre><code class="highlight-chroma"><span class="highlight
cl">https://github.com/FSecureLABS/drozer/releases/download/2.4.4/drozer-2.4.4-py2-none
any.whl
</code></pre>
<p>使用 pip 命令安装：pip install drozer-2.4.4-py2-none-any.whl
去 python 的 script 文件中找到 drozer.bat 文件，运行该文件。</p>
<pre><code class="highlight-chroma"><span class="highlight
cl">drozer.bat console connect
</code></pre>
<p>如果没有找到 drozer.bat 去作者的 github 上找。
<a href="https://ld246.com/forward?goto=https%3A%2F%2Fgithub.com%2FFSecureLABS%2
drozer" target="_blank" rel="nofollow ugc">https://github.com/FSecureLABS/drozer<b
>
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https://b3
ogfile.com/file/2020/08/image-687db824.png?imageView2/2/interlace/1/format/jpg"></p>
<h2 id="2-使用">2.使用</h2>
<p>首先去找到测试的 app 包名。
adb shell pm list packages -3</p>
<p>展示攻击面：</p>
<pre><code class="highlight-chroma"><span class="highlight
cl">run app.package.attacksurface example
</code></pre>
<p>找到 sieve 中可以访问的 url：</p>
<pre><code class="highlight-chroma"><span class="highlight
cl">run app.provider.finduri com.jlnx.tianshu
</code></pre>
<p>具体命令可在以下网站查看
<a href="https://ld246.com/forward?goto=https%3A%2F%2Fmp.weixin.qq.com%2Fs%3F__bi
%3DMzI1NzI2Mzg1Ng%3D%3D%26mid%3D2247484016%26idx%3D1%26sn%3D97fecc0eb8
c46e9d95b72bfc1f7aa5d%26chksm%3Dea1b53efdd6cdaf93ec3e21da48a4925055356992e21
28990d3ee963ae7738869fc5a8994a7%26mpshare%3D1%26scene%3D1%26srcid%3D0813BA
Ux9zZ60D9EcellGqm%26sharer_sharetime%3D1597301534780%26sharer_shareid%3Df2cb3f
bc23f628093c6abe3f4b45754%23rd" target="_blank" rel="nofollow ugc">https://mp.weixin.
q.com/s?__biz=MzI1NzI2Mzg1Ng==&mid=2247484016&idx=1&sn=97fecc0e
88c46e9d95b72bfc1f7aa5d&chksm=ea1b53efdd6cdaf93ec3e21da48a4925055356992e2
b28990d3ee963ae7738869fc5a8994a7&mpshare=1&scene=1&srcid=0813BAI
x9zZ60D9EcellGqm&sharer_sharetime=1597301534780&sharer_shareid=f2cb3fbbc
3f628093c6abe3f4b45754#rd</p>
<p>参考文献：
<a href="https://ld246.com/forward?goto=https%3A%2F%2Fgithub.com%2FFSecureLABS%2
drozer%2Fissues%2F357" target="_blank" rel="nofollow ugc">Issue #357 · FSecureLABS/droz
r</p>