**CrackMapExec扫描:**

通过 Responder、错误配置的 Web 应用程序、暴力破解或通过打印机获得了登录凭证，那么我们可以尝试扫描网络，看看这个帐户可以登录到哪里。使用像CrackMapExec（CME）这样的工具进行简单的扫描可以帮助找到内部网络上的初始入口点。

我们将使用其 REST API 启动 Empire，在 CME 中配置密码，让 CME 连接到 Empire，使用我们拥有的单一凭证扫描网络，最后，如果成功完成身份验证，则自动将 Empire 的 payload 推送到远程受害者的系统

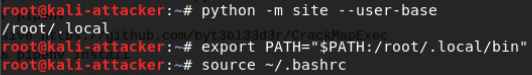
./empire --rest --password ‘password’

cme安装:

#~ apt-get install -y libssl-dev libffi-dev python-dev build-essential

#~ pip install --upgrade pip

#~ pip install --user pipenv



#~ git clone --recursive https://github.com/byt3bl33d3r/CrackMapExec

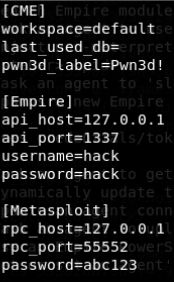
#~ cd CrackMapExec && pipenv install

#~ pipenv shell

#~ python setup.py install



cme.conf



普通本地用户、普通域用户无法弹回shell 本地管理员、域管理员可弹回shell

