**域渗透——Local Administrator Password Solution**

<http://static.hx99.net/static/drops/tips-10496.html>

在实际的域环境中，域内主机的本地管理员账户往往被忽视，再加上统一的配置，域内主机的本地管理员密码往往相同，这就带来了一个问题，如果获得一台域内主机的本地管理员密码，其他域内主机的本地管理员密码自然就知道了，解决这个问题最好的办法就是确保每台域内主机有不同的密码，并且定期更换。

所以微软在2015年3月1号发布了LAPS（Local Administrator Password Solution）协议。

配合powershell