



# K8哥哥

(/)



## 【教程】Ladon以指定用户权限运行程序或命令

<% Visit %>

### 前言

Ladon内置Runas允许用户用其他权限运行指定的工具和程序。系统自带Runas命令需要交互式登陆，在webshell或不支持交互式的shell下使用麻烦。而Ladon的Runas则完美解决了以上问题，支持非交互式模拟登陆指定用户运行程序或命令。

### 应用场景

- 1.本机用户密码验证（权限不够读不到帐密或HASH的情况下，验证用户是否使用某个已知密码）
  - 2.SYSTEM权限降权，SYS权限下以用户身份执行命令，实现会话穿透，或访问特定用户的DBAPI加密数据
  - 3.低权限用户提权，网络服务帐户或用户权限下使用管理员权限来执行一些必须管理员才能执行的命令
  - 4.浏览器密码读取，本机存在多个用户，需要读取对应用户保存帐密（DBAPI），如Chrome、Firefox
- 提示：Runas条件是有帐密，提权降权也可使用GetSystem，无需帐密只需指定对应用户权限进程即可

### 用法

- ```
1  Ladon Runas user pass cmd
2  Ladon Runas user pass cmd domain
```

## 测试环境

当前机器默认开启UAC，登陆用户为null，管理员用户为k8gege，默认管理员用户为Administrator  
Runas在不同权限下模拟其它用户权限有一定区别，如UAC下模拟非内置管理员用户则受到UAC限制。

## 测试目的

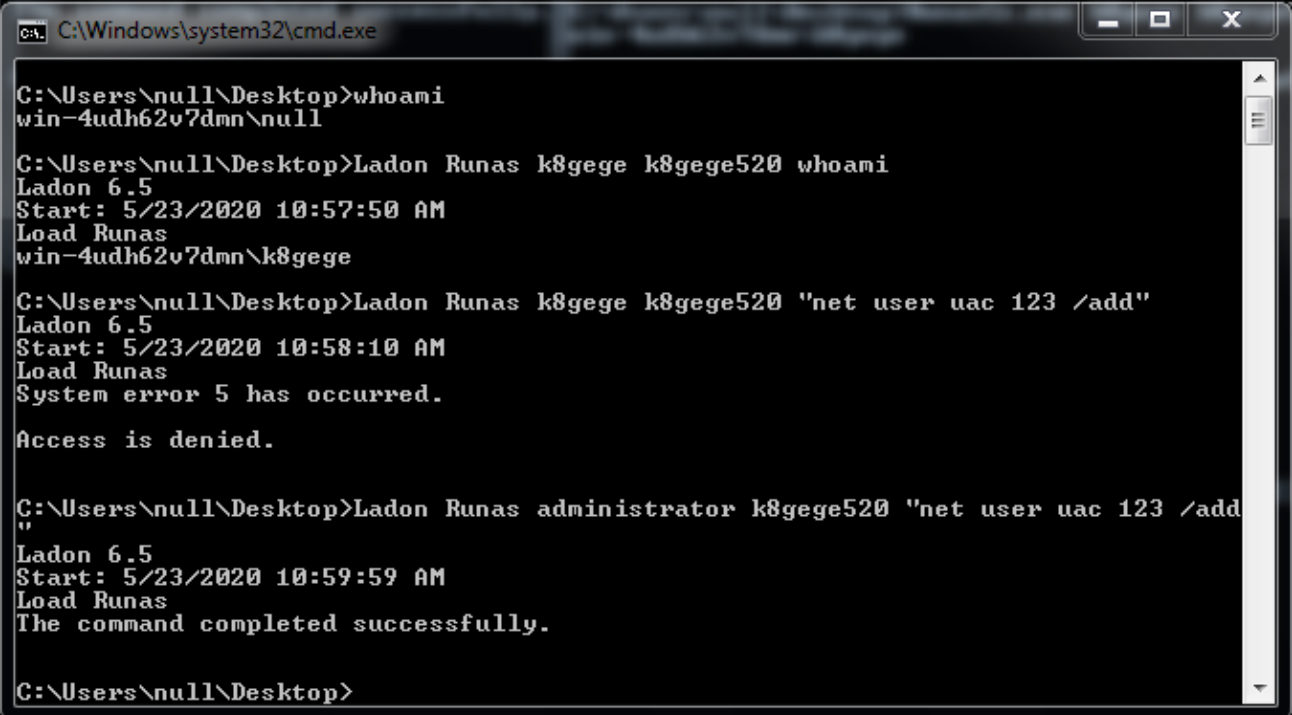
以不同权限模拟登陆同一用户执行添加用户命令，对比Runas的执行权限  
为什么用添加用户权限来对比，因为用户或管理员UAC是无法添加用户的  
通过是否可添加用户，可轻易区分模拟后的权限到底是具备什么权限

## Uac权限

非内置管理员用户在UAC权限下执行命令继承UAC权限，无法通过该用户权限添加用户  
但是模拟内置管理员Administrator权限则不受UAC影响，可以通过该权限添加用户。

Ladon Runas k8gege k8gege520 whoami

Ladon Runas Administrator k8gege520 whoami



```
C:\Windows\system32\cmd.exe

C:\Users\null\Desktop>whoami
win-4udh62v7dmn\null

C:\Users\null\Desktop>Ladon Runas k8gege k8gege520 whoami
Ladon 6.5
Start: 5/23/2020 10:57:50 AM
Load Runas
win-4udh62v7dmn\k8gege

C:\Users\null\Desktop>Ladon Runas k8gege k8gege520 "net user uac 123 /add"
Ladon 6.5
Start: 5/23/2020 10:58:10 AM
Load Runas
System error 5 has occurred.

Access is denied.

C:\Users\null\Desktop>Ladon Runas administrator k8gege520 "net user uac 123 /add"
Ladon 6.5
Start: 5/23/2020 10:59:59 AM
Load Runas
The command completed successfully.

C:\Users\null\Desktop>
```

## Administrator权限

管理员权限下模拟非内置管理员用户权限，是可以添加用户的

Ladon Runas k8gege k8gege520 whoami

```
Administrator: C:\Windows\System32\cmd.exe

C:\Users\null\Desktop>whoami
win-4udh62v7dmn\null

C:\Users\null\Desktop>Ladon Runas k8gege k8gege520 whoami
Ladon 6.5
Start: 5/23/2020 11:03:44 AM
Load Runas
win-4udh62v7dmn\k8gege

C:\Users\null\Desktop>Ladon Runas k8gege k8gege520 "net user adm 123 /add"
Ladon 6.5
Start: 5/23/2020 11:04:25 AM
Load Runas
The command completed successfully.

C:\Users\null\Desktop>
```

## System权限

SYSTEM权限下模拟非内置管理员用户权限，是可以添加用户的  
Ladon Runas k8gege k8gege520 whoami

```
Administrator: C:\Windows\System32\cmd.exe

C:\Users\null\Desktop>whoami
win-4udh62v7dmn\null

C:\Users\null\Desktop>Ladon Runas k8gege k8gege520 whoami
Ladon 6.5
Start: 5/23/2020 11:03:44 AM
Load Runas
win-4udh62v7dmn\k8gege

C:\Users\null\Desktop>Ladon Runas k8gege k8gege520 "net user adm 123 /add"
Ladon 6.5
Start: 5/23/2020 11:04:25 AM
Load Runas
The command completed successfully.

C:\Users\null\Desktop>
```

## 结论

在UAC下需要模拟管理员权限执行命令，先过UAC或使用内置管理员  
管理员或SYSTEM权限模拟的用户具备什么权限，它就有对应的权限

## 工具下载

最新版本: <https://k8gege.org/Download/Ladon.rar> (<https://k8gege.org/Download/Ladon.rar>)

历史版本: <https://github.com/k8gege/Ladon/releases> (<https://github.com/k8gege/Ladon/releases>)