

kali linux渗透测试



第21课 绕过Windows用户账户控制，进行提取

用户帐户控制（简称 UAC）是微软公司在其 Windows Vista，及更高版本操作系统中采用的一种控制机制。

本期将带你了解它是如何保护你免受恶意软件侵害的，以及忽略 UAC 提示将可能给你系统带来的麻烦。

什么是UAC

一旦程序执行涉及系统更改/特定任务就会触发UAC。除非尝试执行它们的进程以管理员权限运行，否则这些操作都将被阻止。没有管理员权限将无法执行以下操作：

- a. 注册表修改
- b. 加载设备驱动程序
- c. DLL注入
- d. 修改系统时间（clock）
- e. 修改用户帐户控制设置
- f. 修改受保护的目录（例如Windows文件夹，Program Files）
- g. 计划任务（例如，以管理员权限自启动）



提权命令

```
1 getsystem getuid
```

如果失败，那就要想办法绕过目标系统的UAC保护

```
1 exploit/windows/local/bypassuac
```

```
2 exploit/windows/local/bypassuac_inject 直接运行在内存中，被查杀的概率低
```



The image features a central figure of a person wearing a black hoodie, with their right hand resting on the hood. The background is a vibrant blue digital landscape. On the right side, a glowing globe is visible, surrounded by intricate network patterns of lines and nodes. The overall aesthetic is high-tech and futuristic, with various icons like padlocks and data points scattered throughout the scene.

谢谢观赏