提权综述

1、提权定义

提高自己在服务器中的权限，主要针对网站入侵过程中，当入侵某一网站时，通过各种漏洞提升 WEBSHELL 权限以夺得改服务器权限。

2、基本概念

提权攻击原理是主要针对网站入侵过程中,当入侵某一网站时，通过各种漏洞提升 WEBSHELL 权限，从而进一步获得服务器权限。

3、掌握相关的提权工具进行提权

操作系统本身的提权

利用数控进行提权

系统配置不当提权

第三方软件提权

4、提权后的操作

清理痕迹--隐藏攻击

安装后门--长久控制

渗透内网-扩大战果

5、用户组权限

Administrators 属于该 administators 本地组内的用户，都具备系统管理员的权限，它们拥有对这台计算机最大的控制权限，可以执行整台计算机的管理任务。内置的系统管理员帐房 Administrator 就是本地组的成员，而且无法将它从该组删除。

Guests 该组是提供没有用户帐户，但是需要访问本地计算机内资源的用户使用，该组的成员无法永久地改变其桌面的工作环境。该组最常见的默认成员为用户帐号 Guest。

Users 该组员只拥有一些基本的权利，例如运行应用程序，但是他们不能修改操作系统的设置、不能更改其它用户的数据、不能关闭服务器级的计算机。 所有添加的本地用户帐户者自动属于该组。

6、文件权限

读取：该权限允许用户查看该文件夹中的文件以及子文件夹，也允许查看该文件夹的属性、所有者和拥有的权限等。

写入：该权限允许用户在该文件夹中创建新的文件和子文件夹，也可以改变文件夹的属性、查看文件夹的所有者和权限等。

执行：该权限允许用户在该文件夹中执行任何脚本文件或者.exe 可执行文件，此权限如果设置不当，会对计算机的安全带来严重危害。