

信息安全引论

实验四



实验环境

- <https://www.cloudrange.cn/>
- 账号名：a24XXX（XXX对应各组编号001~051）
- 初始密码：P@ssW0rd，在首次登录后需要修改，各人需要记住自己的密码，选择密码的原则：易记难猜
- 每个账号同时只能有一个位置登录，如果在第二个位置登录，会把第一个位置登录的同学踢出
- 2位同学一组，可以共同讨论一起完成实验
- 也可以独立完成，2个人协商好不同时间就可以

实验分组

帐号	组长	帐号	组长	帐号	组长
a24001	张子苏	a24010	温非凡	a24019	智旭生
a24002	袁傲慕飞	a24011	丁宏骏	a24020	朱俊霖
a24003	李玖熹	a24012	谢佳璇	a24021	任科同
a24004	毛嘉楷	a24013	张弛	a24022	石尚
a24005	许仕熠	a24014	马啸宇	a24023	兰晰程
a24006	黄学郅	a24015	连烨	a24024	胡建波
a24007	黄高翔	a24016	曹原	a24025	冯子康
a24008	张浩卓	a24017	陈冠霖	a24026	李兆彬
a24009	李致城	a24018	蒋轩林	a24027	孟德松

实验分组

帐号	组长	帐号	组长	帐号	组长
a24028	桑钰超	a24037	尹秋衡	a24046	李秀燕
a24029	潘馨仪	a24038	袁晓坤	a24047	邢政
a24030	徐培尧	a24039	张龄心	a24048	孙沐岩
a24031	庞湫凡	a24040	黄净栩	a24049	戴傅聪
a24032	刘鲁阳	a24041	淦林川	a24050	王子琪
a24033	尹骄洋	a24042	屈振华	a24051	王振宇
a24034	吕宗蔚	a24043	徐天艺		
a24035	罗珑赞	a24044	张金涛		
a24036	王昱博	a24045	杨嘉文		

实验四 内容

- 实验内容:

- ① 认知-Windows权限提升技术
- ② 探索-Windows权限提升
- ③ 认知-Windows凭据和凭据转储介绍
- ④ 认知-使用Mimikatz转储Windows凭据
- ⑤ 探索-Windows凭据转储
- ⑥ 探索-OWASP认证失效

Windows系统本地账户

本地账户存储在本地服务器上，与提权相关的本地账户包括管理员账户，默认本地系统账户，以及服务账户。

1. 管理员账户(Administrators)

管理员帐户可以完全控制本地计算机上的文件、目录、服务和其他资源。管理员帐户可以创建其他本地用户、分配用户权限和分配权限。默认管理员帐户无法删除或锁定，但可以重命名或禁用。

2. 默认本地系统账户

SYSTEM 账户由操作系统和在 Windows 下运行的服务使用。默认情况下，SYSTEM 账户被授予对 NTFS 卷上所有文件的完全控制权限。因此 SYSTEM 账户包含管理员账户所具有的功能。

3. 网络服务账户

NETWORK SERVICE 是服务控制管理器(SCM)使用的预定义本地账户，以这个账户运行的服务，允许把访问凭据提交给远程的计算机。

4. 本地服务账户

LOCAL SERVICE 账户是服务控制管理器使用的预定义本地账户，它在本地计算机上具有最低权限，并在网络上提供匿名凭据。

Windows收集系统和用户信息的方法

Windows 上收集系统和用户信息的方法:

1. Windows Management Instrumentation 命令行 (WMIC)
 - 它是Windows最有用的命令行工具，WMIC对于信息收集和后期开发非常实用
 - 用于各种系统维护和信息收集任务
2. Net 程序
 - 用于管理和配置操作系统
3. iccls
 - 用于管理目录访问控制列表 (DACL) 的 Microsoft 实用程序

提权常用命令-1

- **hostname:** 列出主机名
- **whoami:** 列出当前用户
- **net users:** 列出所有用户

```
命令提示符
Microsoft Windows [版本 10.0.19044.1826]
(c) Microsoft Corporation。保留所有权利。

C:\Users\mhlabs>hostname
MHLABS-WS1
```

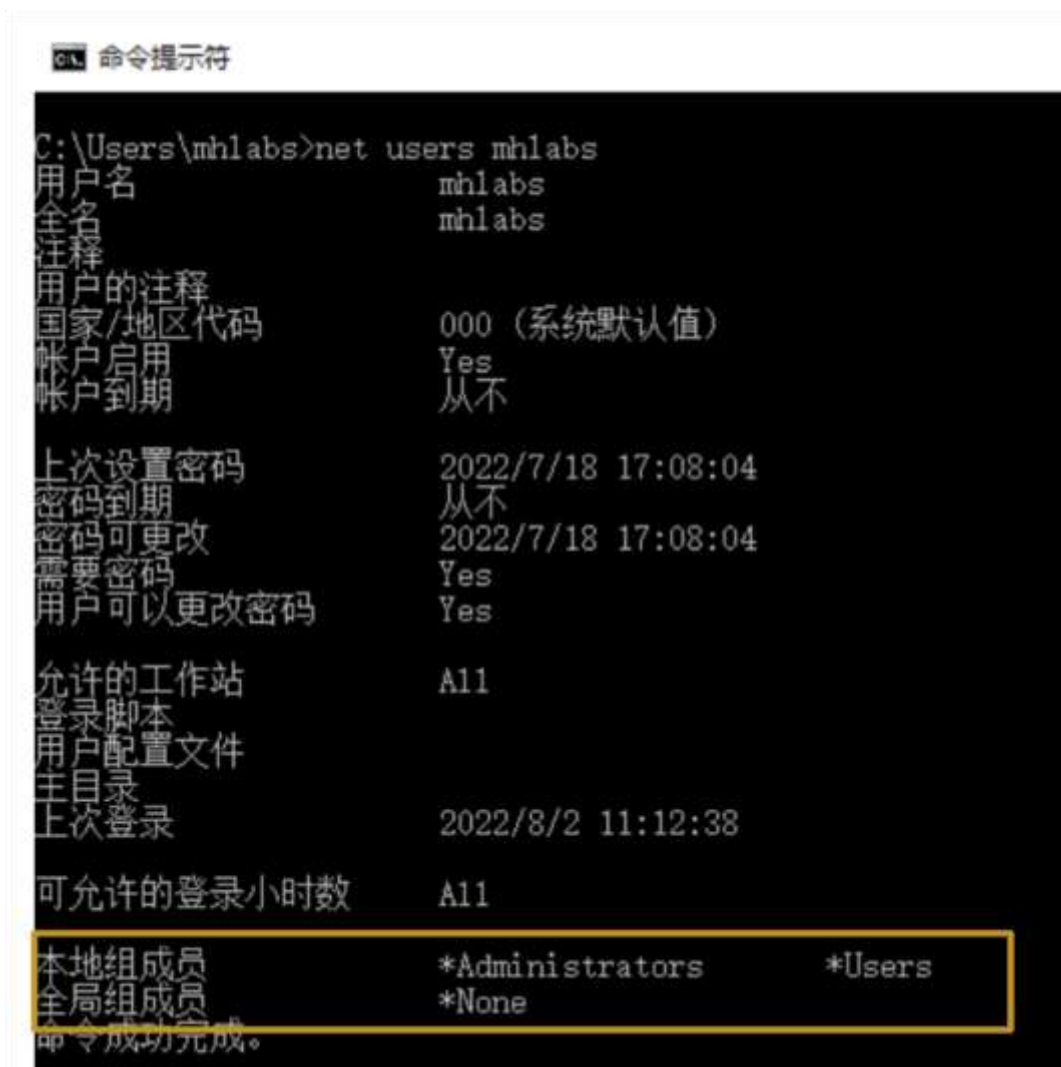
```
C:\Users\mhlabs>whoami
mhlabs-ws1\mhlabs
```

```
命令提示符
C:\Users\mhlabs>
C:\Users\mhlabs>net users
\\MHLABS-WS1 的用户帐户

-----
Administrator                DefaultAccount                Guest
mhlabs                        WDAGUtilityAccount
命令成功完成。
```


提权常用命令-2

- `net users mhlabs:` 进一步了解 mhlabs 账户



```
命令提示符
C:\Users\mhlabs>net users mhlabs
用户名                mhlabs
全名                  mhlabs
注释
用户的注释
国家/地区代码        000 (系统默认值)
帐户启用              Yes
帐户到期              从不
上次设置密码          2022/7/18 17:08:04
密码到期              从不
密码可更改            2022/7/18 17:08:04
需要密码              Yes
用户可以更改密码      Yes
允许的工作站          All
登录脚本
用户配置文件
主目录
上次登录              2022/8/2 11:12:38
可允许的登录小时数    All
本地组成员            *Administrators *Users
全局组成员            *None
命令成功完成。
```

提权常用命令-3

- **systeminfo:** 显示计算机详细配置信息

命令提示符

```
主机名: MHLABS-WS1
OS 名称: Microsoft Windows 10 企业版
OS 版本: 10.0.19044 暂缺 Build 19044
OS 制造商: Microsoft Corporation
OS 配置: 独立工作站
OS 构建类型: Multiprocessor Free
注册的所有人: Windows 用户
注册的组织:
产品 ID: 00328-90000-00000-AAOEM
初始安装日期: 2022/7/18, 23:27:18
系统启动时间: 2022/8/2, 9:05:03
系统制造商: VMware, Inc.
系统型号: VMware7,1
系统类型: x64-based PC
处理器: 安装了 2 个处理器。
[01]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1992 Mhz
[02]: Intel64 Family 6 Model 142 Stepping 10 GenuineIntel ~1992 Mhz
BIOS 版本: VMware, Inc. VMW71.00V.18452719.B64.2108091906, 2021/8/9
Windows 目录: C:\WINDOWS
系统目录: C:\WINDOWS\system32
启动设备: \Device\HarddiskVolume1
系统区域设置: zh-cn; 中文(中国)
输入法区域设置: zh-cn; 中文(中国)
时区: (UTC+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量: 5,791 MB
可用的物理内存: 3,537 MB
虚拟内存: 最大值: 6,751 MB
虚拟内存: 可用: 4,749 MB
虚拟内存: 使用中: 2,002 MB
```

命令提示符

```
虚拟内存: 最大值: 6,751 MB
虚拟内存: 可用: 4,749 MB
虚拟内存: 使用中: 2,002 MB
页面文件位置: C:\pagefile.sys
域: WORKGROUP
登录服务器: \\MHLABS-WS1
修补程序: 安装了 6 个修补程序。
[01]: KB5013887
[02]: KB5003791
[03]: KB5007401
[04]: KB5015807
[05]: KB5014671
[06]: KB5005699
网卡: 安装了 2 个 NIC。
[01]: Intel(R) 82574L Gigabit Network Connection
连接名: Ethernet0
启用 DHCP: 是
DHCP 服务器: 192.168.199.1
IP 地址:
[01]: 192.168.199.171
[02]: fe80::64bb:4187:9413:5bb9
[02]: Bluetooth Device (Personal Area Network)
连接名: 蓝牙网络连接
状态: 媒体连接已中断
Hyper-V 要求: 已检测到虚拟机监控程序。将不显示 Hyper-V 所需的功能。
C:\Users\mhllabs>z
```

提权常用命令-4

- 识别文件或文件夹的权限
- `icacls "C:\program Files"`，显示或修改指定的文件的访问控制列表

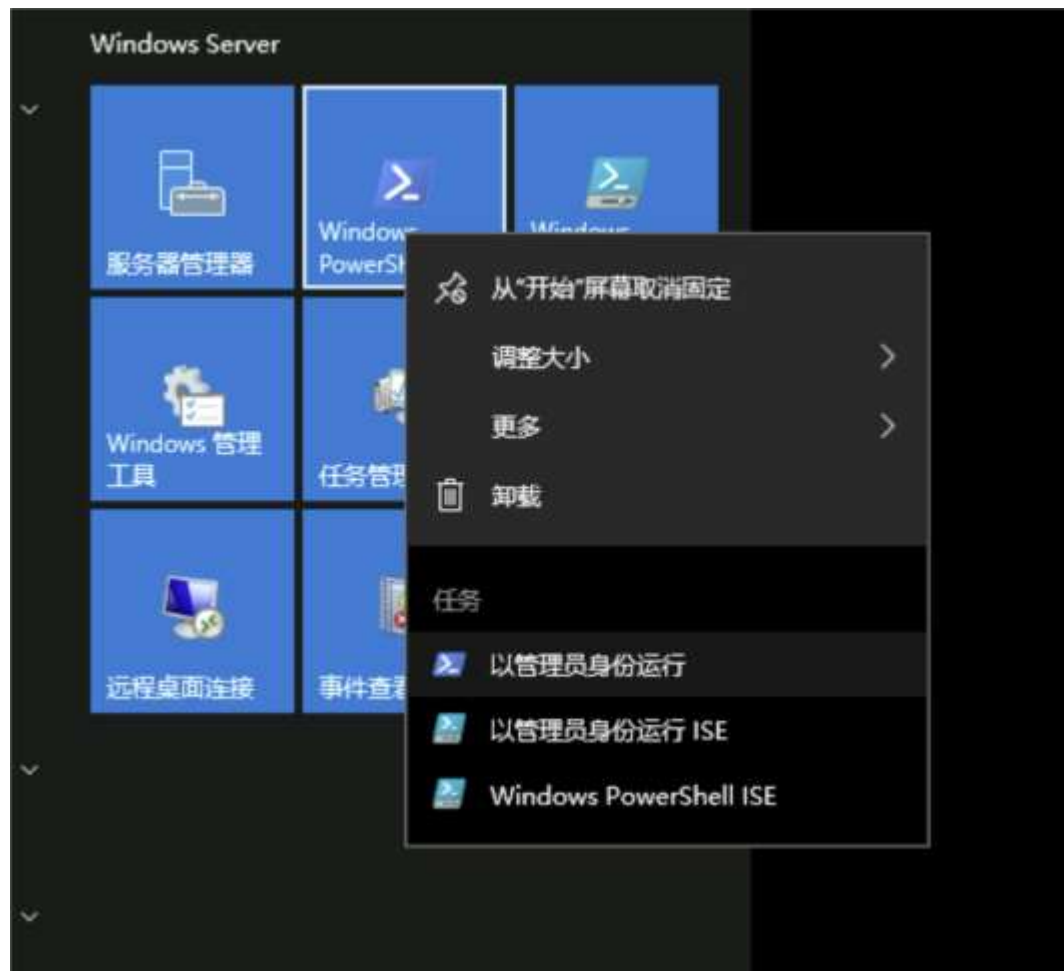
命令提示符

```
C:\Users\mhlabs>
C:\Users\mhlabs>
C:\Users\mhlabs>icacls "C:\Program Files"
C:\Program Files NT SERVICE\TrustedInstaller:(F)
                  NT SERVICE\TrustedInstaller:(CI)(IO)(F)
                  NT AUTHORITY\SYSTEM:(M)
                  NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
                  BUILTIN\Administrators:(M)
                  BUILTIN\Administrators:(OI)(CI)(IO)(F)
                  BUILTIN\Users:(RX)
                  BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
                  CREATOR OWNER:(OI)(CI)(IO)(F)
                  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(RX)
                  APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(OI)(CI)(IO)(GR,GE)
                  APPLICATION PACKAGE AUTHORITY\所有受限制的应用程序包:(RX)
                  APPLICATION PACKAGE AUTHORITY\所有受限制的应用程序包:(OI)(CI)(IO)(GR,GE)
```

已成功处理 1 个文件；处理 0 个文件时失败

系统重启

- shutdown -r
- MHI@bs-1!



Unquoted Service Path vulnerability

- 未引用的服务路径漏洞
- 如果可执行文件的路径中包含空格并且路径未用引号括起来，则服务易受攻击；利用漏洞需要具有写入权限。

实验说明

- ① 认知实验为视频讲解，熟悉相关知识的可以不用看。
- ② 探索实验是多个选择题，每个实验指定最长多少时间（比如45分钟）结束。
- 实验成绩只记录探索实验的完成得分



Q&A?