第八章、破解windows系统密码

author：杨哥团队-史密斯

一、利用5次shift漏洞破解win7密码

1.1 漏洞

```
1、在未登录系统时，连续按5次shift键，弹出程序c:\windows\system32\sethc.exe
2、部分win7及win10系统在未进入系统时，可以通过系统修复漏洞篡改系统文件名！
注：如win7或win10系统已修补漏洞2，则无法利用
```

1.2 破解过程相关知识

```
1、cmd工具路径
    c:\windows\system32\cmd
2、用户/账户密码存储位置
    c:\windows\system32\config\SAM          # 非逆转型加密、使用hash值类似的方法、MD5 SHA
3、修改账户密码：
    net  user  用户名  新密码
```

1.3 漏洞利用过程

```
案例：破解win7系统密码
实验步骤：
1、开启win7虚拟机，开机，并设置一个复杂密码；
2、关机，并开机，在出现windows启动界面时强制关机；
3、再开机，出现“启动修复（推荐）”及选择该项；    # 如为出现，多尝试几次第2步，如还不行，请换其他方法
4、出现系统还原提示，点击取消，等待几分钟后，会出现问题原因，点击查看详细信息；
5、打开最后一个链接即一个记事本；
6、记事本中点打开，并选择显示所有文件；
7、找到sethc并改名sethc-bak，再找到cmd，复制一份cmd改名为sethc
8、全部关闭，重启。
9、系统启动完毕后，连续按5次shift键，将弹出cmd工具，使用命令net  user  用户名  新密码，将当前用户密码修改掉即可，或者另外建立1个用户，并提升为管理员，注销后，可再删除新建的用户，这样的好处为不修改当前用户的密码即可登录系统。
```

二、利用PE系统破解XP密码

2.1 漏洞

```
PE系统，独立于硬盘系统的微型系统，通过PE系统启动可以对系统的SAM文件做修改
```

2.2 破解过程相关知识

账户密码存储文件：c:\windows\system32\config\SAM
U盘引导系统：开机修改启动顺序，并将U盘设置为第一启动顺序！（一般电脑是开机马上按F2键，进入BIOS，修改启动顺序，不同品牌电脑设置方法不一样，可咨询售后）

2.3 漏洞利用过程

1.下载PE制作工具（如老毛桃，大白菜，深度等），插入空U盘或光盘，一键制作PE系统到U盘
2.为XP系统设置一个复杂密码，并关机。
3.插入带有PE系统的U盘或光盘，开机，马上按F2，进入BIOS，设置启动顺序为U盘或光盘为第一位，保存
4.重启，进入PE菜单或PE系统，使用破解密码程序进行破解。（不同的PE系统菜单不一样，但一般都有破解密码选项）