敏感数据定位

内网的核心敏感数据，不仅包括数据库、电子邮件，还包括个人数据及组织的业务数据、技术数据等。可以说，价值较高的数据基本都在内网中。

资料、数据、文件的定位流程：

```
定位内部人事组织结构
在内部人事组织结构中寻找需要监视的人员
定位相关人员的机器
视相关人员存放文档的位置
列出存放文档的服务器的目录
```

重点核心业务机器

```
高级管理人员 系统管理人员 财务/人事/业务人员的个人计算机
产品管理系统服务器
办公系统服务器
财务应用系统服务器
核心产品源码服务器（SVN/GIT服务器）
数据库服务器
文件服务器，
共享服务器
电子邮件服务器
网站监控系统服务器
信息安全监控服务器
生产工厂服务器
```

敏感信息和敏感文件

```
站点源码备份文件，
数据库备份文件等等
游览器保存的密码和游览器的cookie
其他用户会话，
3389和ipc$连接记录，
回收站中的信息等等
Windows的无线密码
网络内部的各种账号密码，
包含电子邮箱，V**，FTP等等
```

在内网中,我们一定要知道自己拿下的机器的人员的职位（职位高的人在内网中权限也高，计算机中的敏感信息也多，还有一种就是特殊职位的人员，例如上面说的，一般都有一些与职位相关的敏感信息。）还有就是拿下一台机器后要先维权，权限稳了再收集信息，信息收集一定要全面仔细，信息收集完了再搞内网。往目标主机中传工具用完就删。翻文件的话，可以使用一些搜索命令来快速寻找。

1.指定目录下搜集各类敏感文件

```
dir /a /s /b d:\"*.txt"
dir /a /s /b C:\"*.xlsx"
dir /a /s /b d:\"*.md"
dir /a /s /b d:\"*.sql"
dir /a /s /b d:\"*.pdf"
dir /a /s /b d:\"*.docx"
dir /a /s /b d:\"*.doc"
dir /a /s /b d:\"*conf*"
dir /a /s /b d:\"*bak*"
dir /a /s /b d:\"*pwd*"
dir /a /s /b d:\"*pass*"
dir /a /s /b d:\"*login*"
dir /a /s /b d:\"*user*"
```

2.指定目录下的文件中搜集各种账号密码

```
findstr /si pass *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si userpwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si pwd *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si login *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
findstr /si user *.inc *.config *.ini *.txt *.asp *.aspx *.php *.jsp *.xml *.cgi *.bak
```