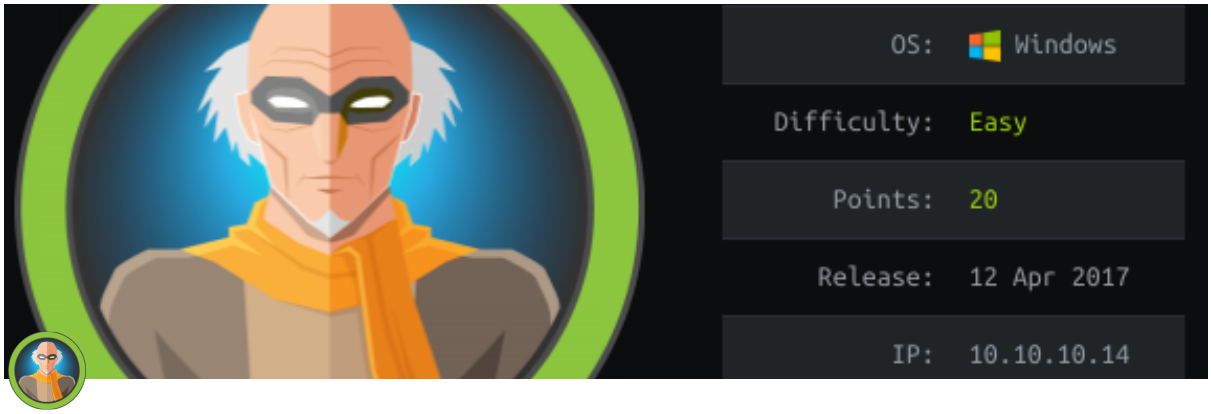


Grandpa

Running nmap we'll get this output

```
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-title: Under Construction
| http-webdav-scan:
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|   WebDAV type: Unknown
|   Server Date: Sat, 05 Dec 2020 16:15:08 GMT
|   Server Type: Microsoft-IIS/6.0
|_  Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
```

Now we know that Microsoft IIS 6.0 is running on this machine and as always google is our friend

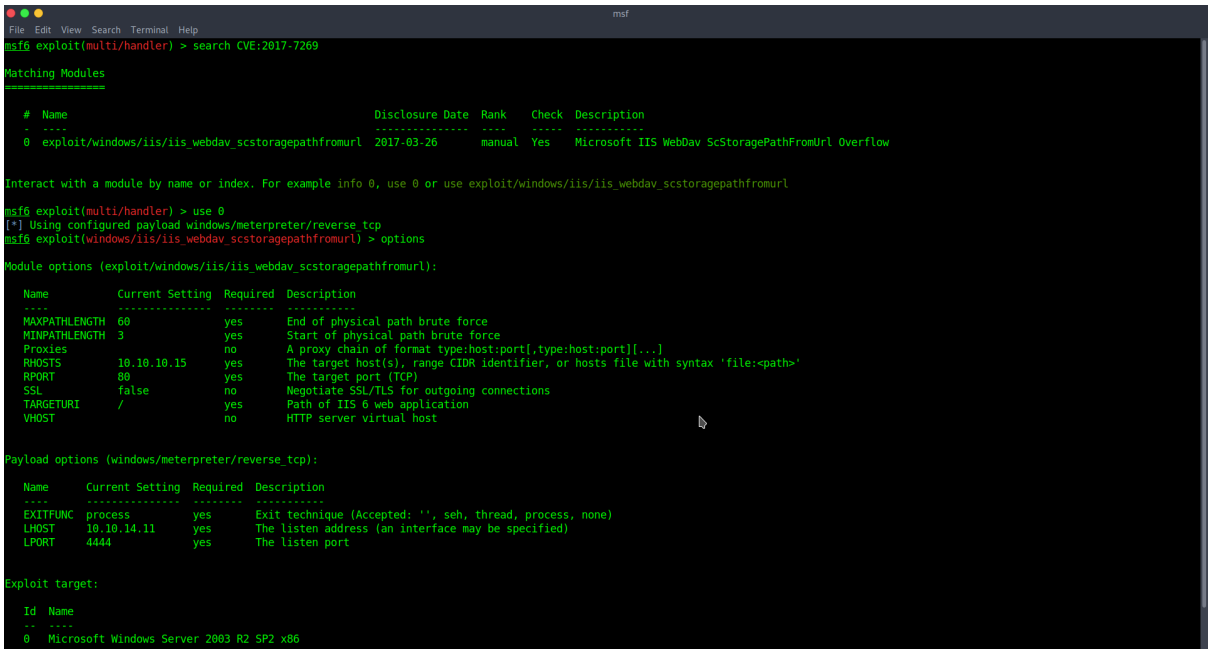
Remote code execution in Microsoft IIS 6.0

Published: 2017-03-28

Risk	Critical
Patch available	YES
Number of vulnerabilities	1
CVE ID	CVE-2017-7269
CWE ID	CWE-119
Exploitation vector	Network
Public exploit	This vulnerability is being exploited in the wild.
Vulnerable software Subscribe	Microsoft IIS Server applications / Web servers Windows Server Operating systems & Components / Operating system Windows Operating systems & Components / Operating system

https://www.cybersecurity-help.cz/vdb/SB2017032801

Ad fortunately metasploit have what we need: search cve:2017-7269



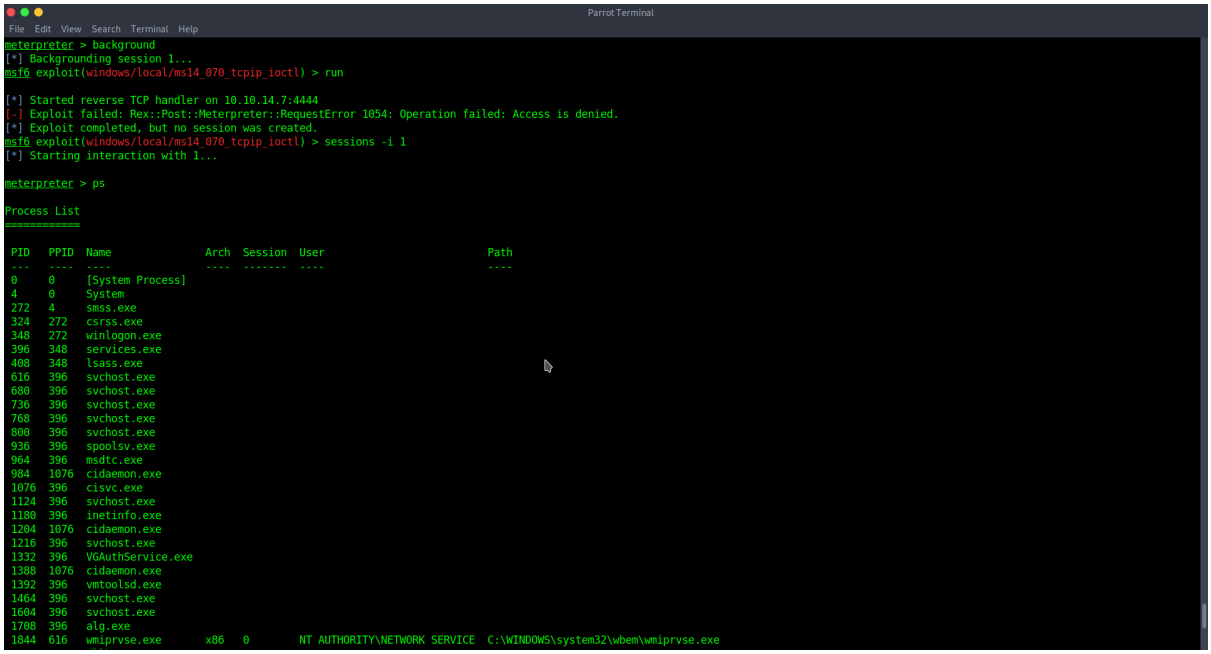
Once we're in we can start looking for the privilege escalation.

Using the exploit suggestor of metasploit "post/multi/recon/local_exploit_suggestor" with the current session we get some possible exploit but one is more interesting than the other

```
exploit/windows/local/ms14_070_tcpip_ioctl
```

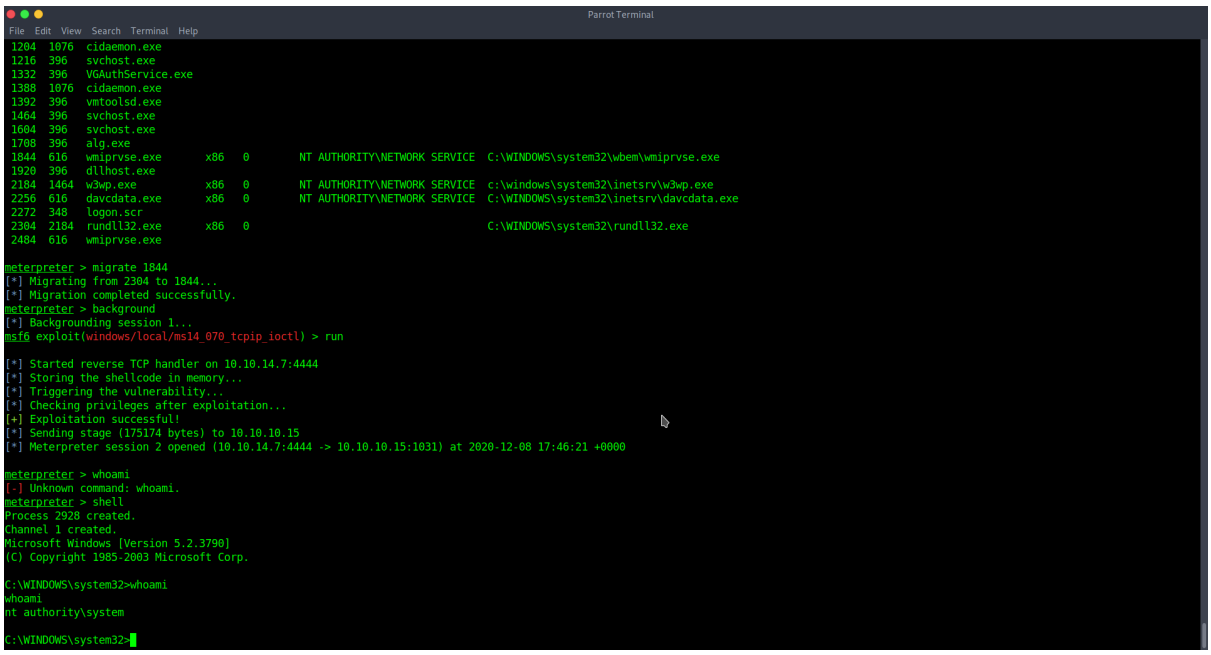
But running it we get an error, we haven't the privilege for completing this exploit.

Looking at the active process we can see this:



There's a process by <NT AUTHORITY> we can try to migrate on that one

Let's try to migrate on that process running "migrate <process id>" in the meterpreter console and retry the priv escalation exploit



Now we're "nt authority" and we have the complete access to this machine!