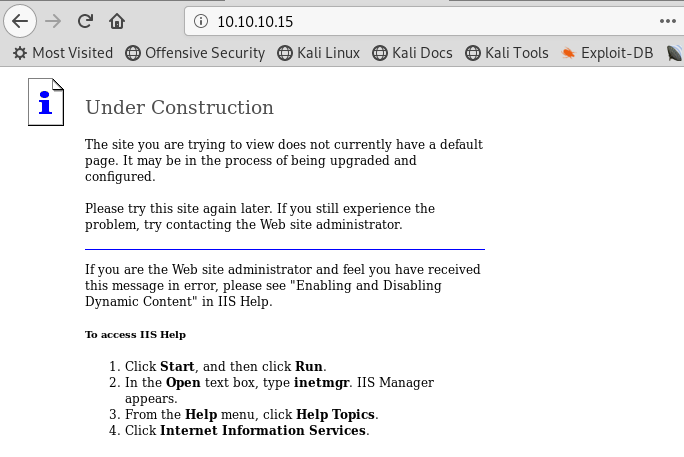
**Hackthebox Granny**

Tried to go to 10.10.10.15 on the web, got this:



Starting with my nmap scan for 10.10.10.15

nmap -T4 -p- -A 10.10.10.15

Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-15 18:41 EST

Nmap scan report for 10.10.10.15

Host is up (0.10s latency).

Not shown: 65534 filtered ports

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-title: Under Construction

| http-webdav-scan:

| Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK

| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

| Server Type: Microsoft-IIS/6.0

| Server Date: Sun, 15 Nov 2020 23:47:36 GMT

|\_ WebDAV type: Unkown

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING): Microsoft Windows 2003|2008|XP|2000 (92%)

OS CPE: cpe:/o:microsoft:windows\_server\_2003::sp1 cpe:/o:microsoft:windows\_server\_2003::sp2 cpe:/o:microsoft:windows\_server\_2008::sp2 cpe:/o:microsoft:windows\_xp::sp3 cpe:/o:microsoft:windows\_2000::sp4

Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft Windows Server 2008 Enterprise SP2 (92%), Microsoft Windows Server 2003 SP2 (91%), Microsoft Windows XP SP3 (90%), Microsoft Windows 2003 SP2 (89%), Microsoft Windows XP (87%), Microsoft Windows Server 2003 SP1 - SP2 (86%), Microsoft Windows XP SP2 or Windows Server 2003 (86%), Microsoft Windows 2000 SP4 (85%), Microsoft Windows XP SP2 or Windows Server 2003 SP2 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 105.87 ms 10.10.14.1

2 105.92 ms 10.10.10.15

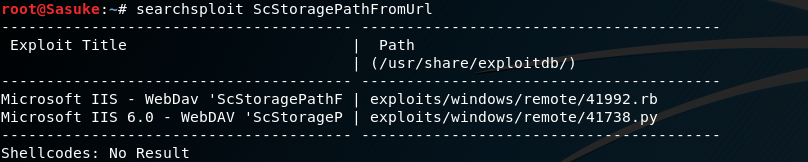
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 205.82 seconds

I googled microsoft iis httpd 6.0 exploit

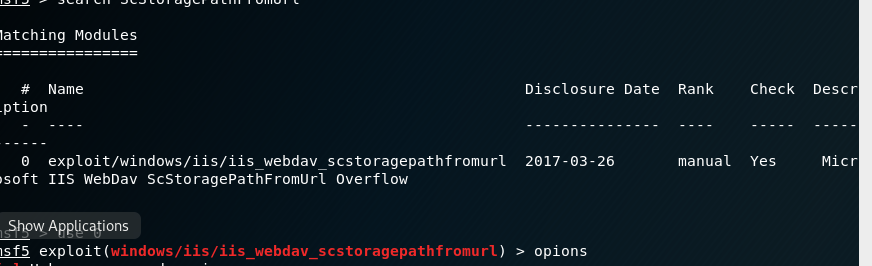
And found a software called ScStoragePathFromUrl

I opened another terminal and searchsploit ScStoragePathFromUrl

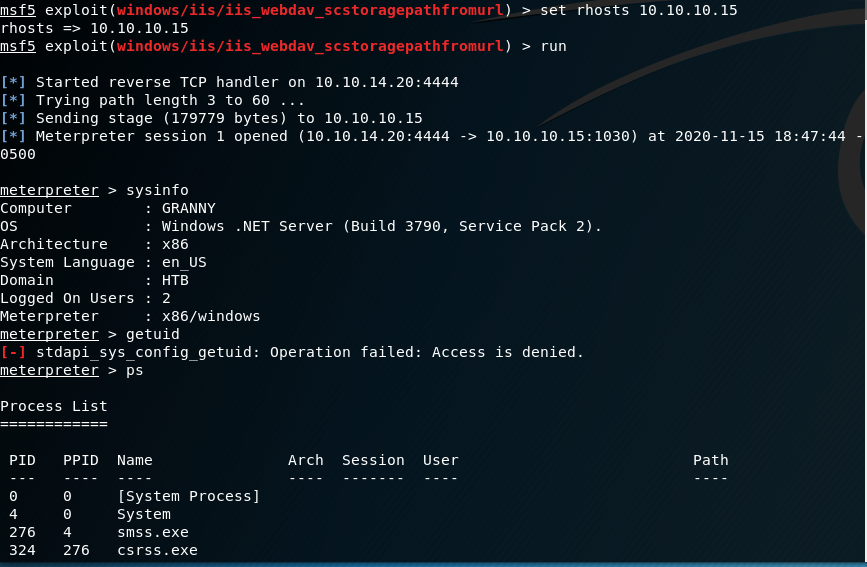


I launched Metasploit

And searched for ScStoragePathFromUrl

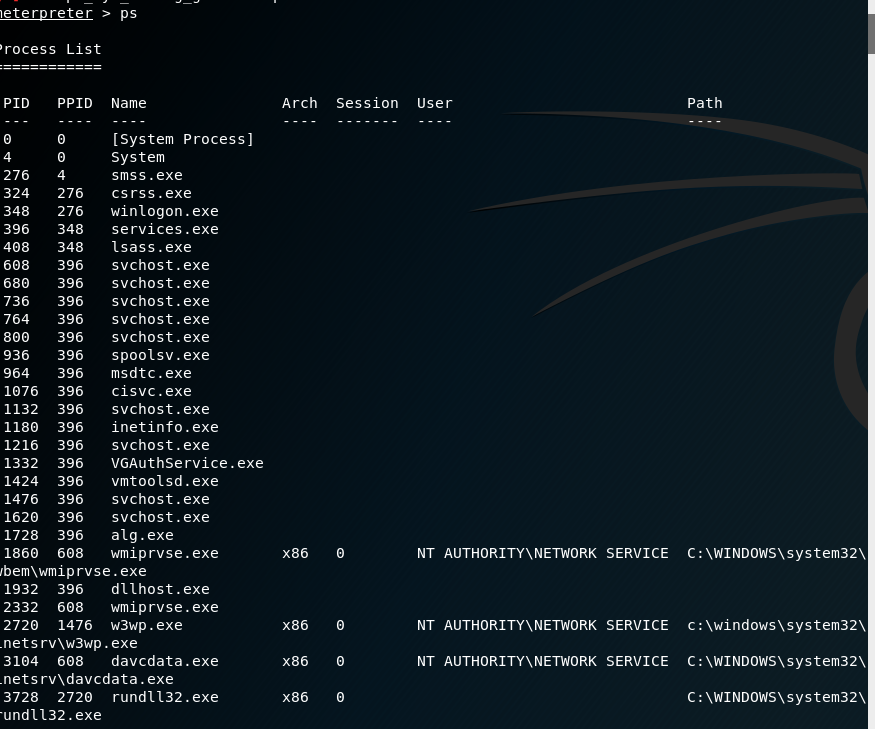


Made sure the rhost and everything is all correct



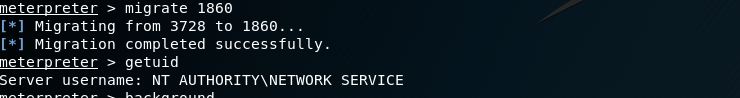
Success! I am in but as you can tell, only user access.

I ran PS to see what services are running



I then saw 1860 has an admin authority access

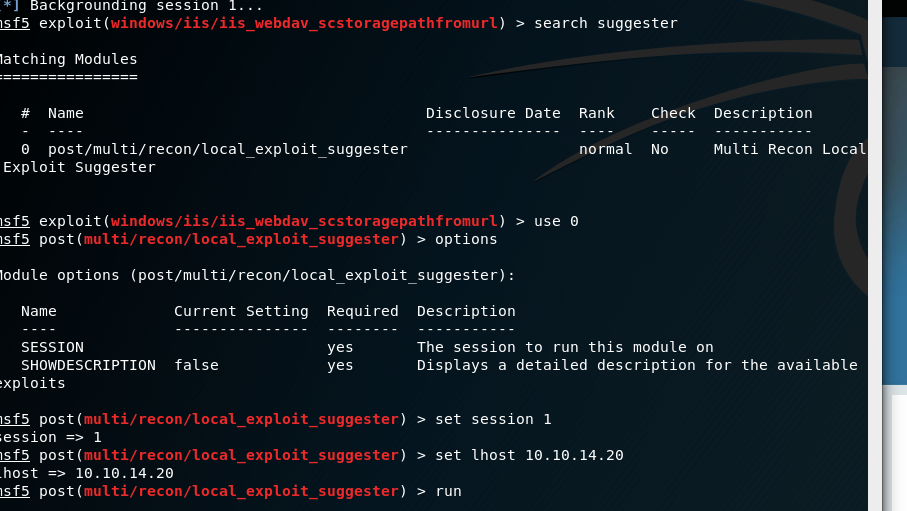
I tried migrating to that port



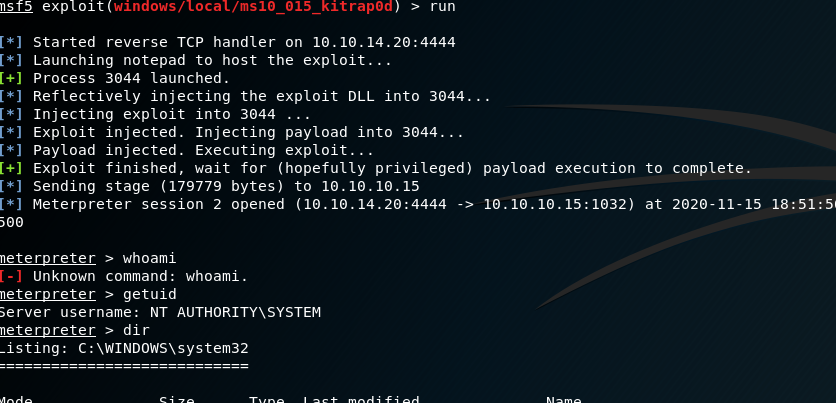
Success!

Now time to get admin access:

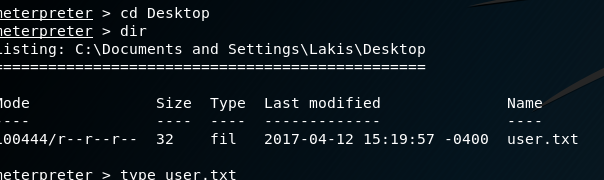
Searched for a suggester in metapsloit



Made sure the lhost and everything is correct, and ran the exploit:



Success!! Time to find user and root flags:



And root: