**Hackthebox Grandpa**

Running nmap in terminal for 10.10.10.14

nmap -T4 -p- -A 10.10.10.14

Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-15 14:46 EST

Nmap scan report for 10.10.10.14

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 COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH

|\_http-server-header: Microsoft-IIS/6.0

|\_http-title: Under Construction

| http-webdav-scan:

| Server Type: Microsoft-IIS/6.0

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

| Server Date: Sun, 15 Nov 2020 19:51:26 GMT

| WebDAV type: Unkown

|\_ Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK

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 2003 SP2 (91%), Microsoft Windows XP SP3 (90%), 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

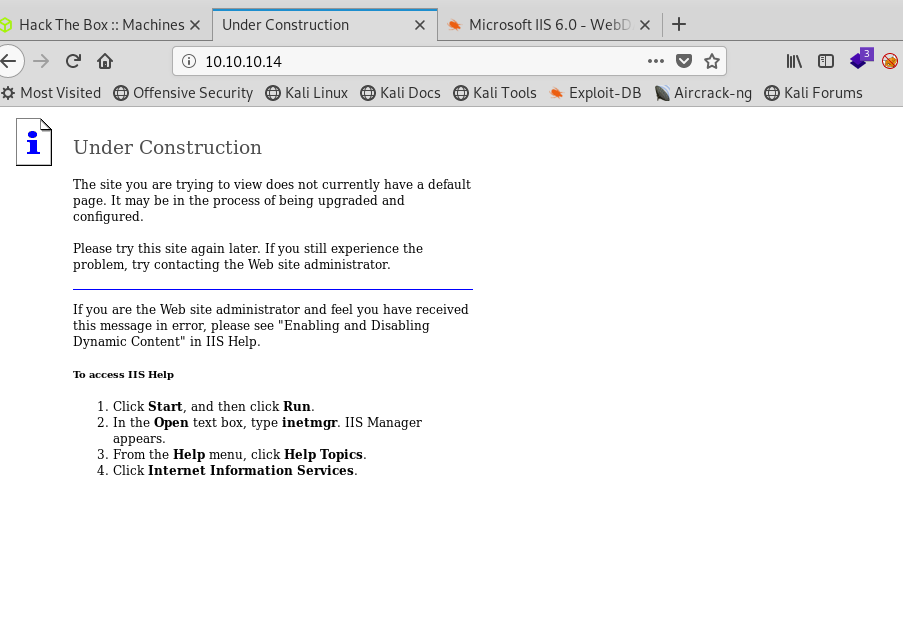
1 101.97 ms 10.10.14.1

2 102.17 ms 10.10.10.14

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 119.01 seconds

I went out to the website

****

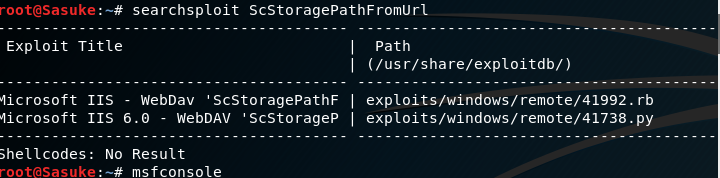
**Nothing to exciting**

**I googled Microsoft IIS httpd 6.0 exploits**

[**https://www.exploit-db.com/exploits/41738**](https://www.exploit-db.com/exploits/41738)

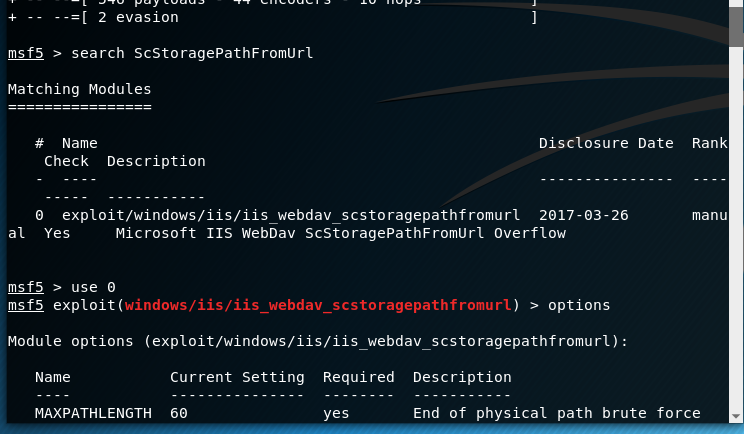
**Found a ScStoragePathFromUrl**

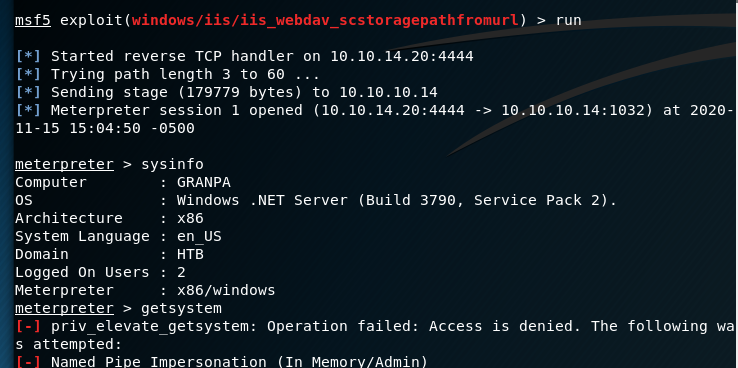
**I opened another terminal tab and went to searchsploit ScStoragePathFromUrl**

****

**Found a couple of options**

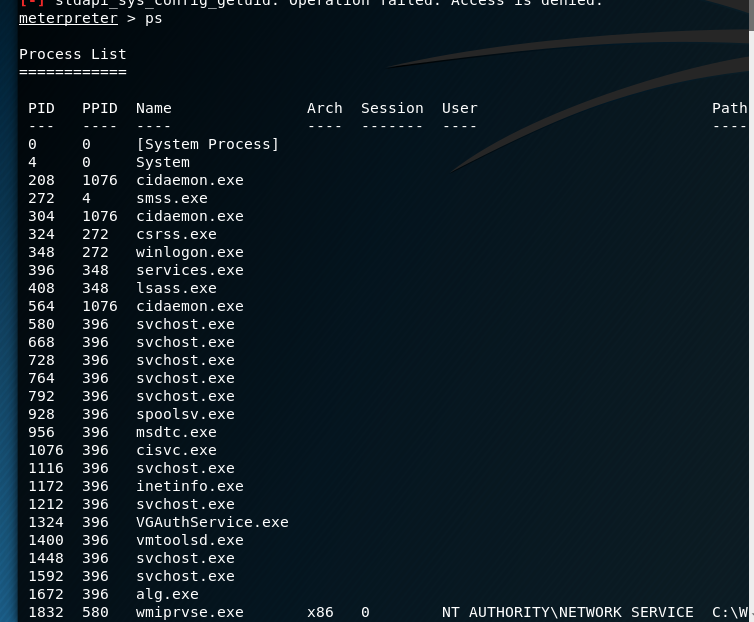
**Opened Metasploit**

****

****

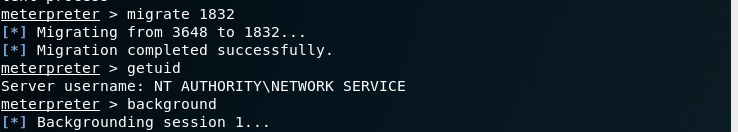
**Success we are in but not admin**

**I open ps and see what services we are running**

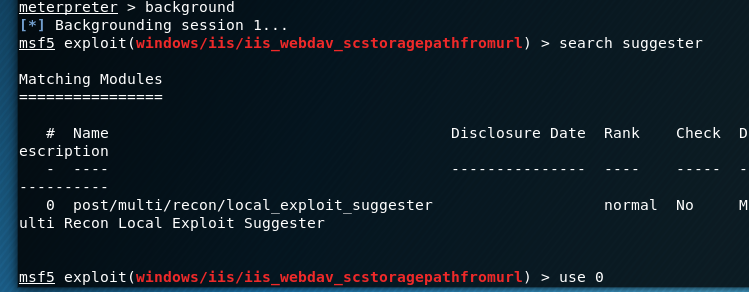
****

**I see at the bottom, a NT auth service running**

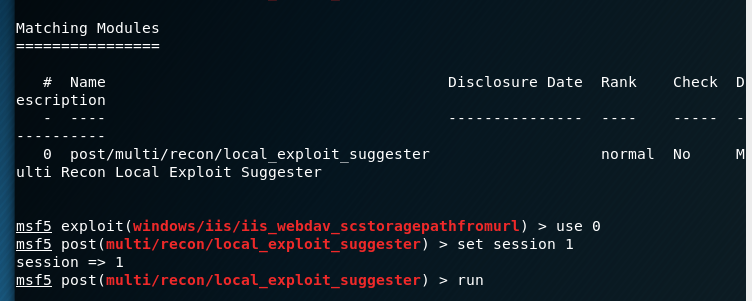
**I then migrate to 1832**

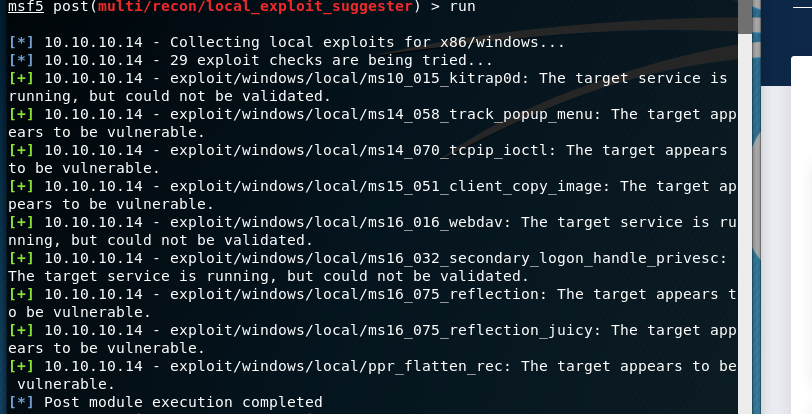
****

**I then open background and search suggester**

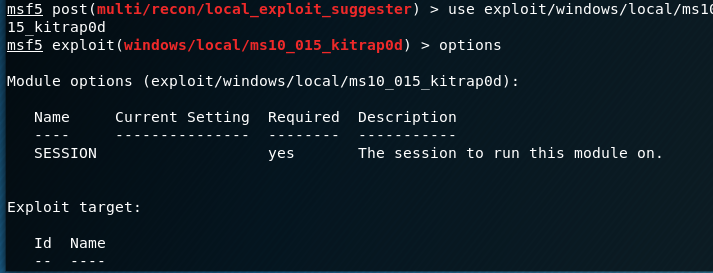
****

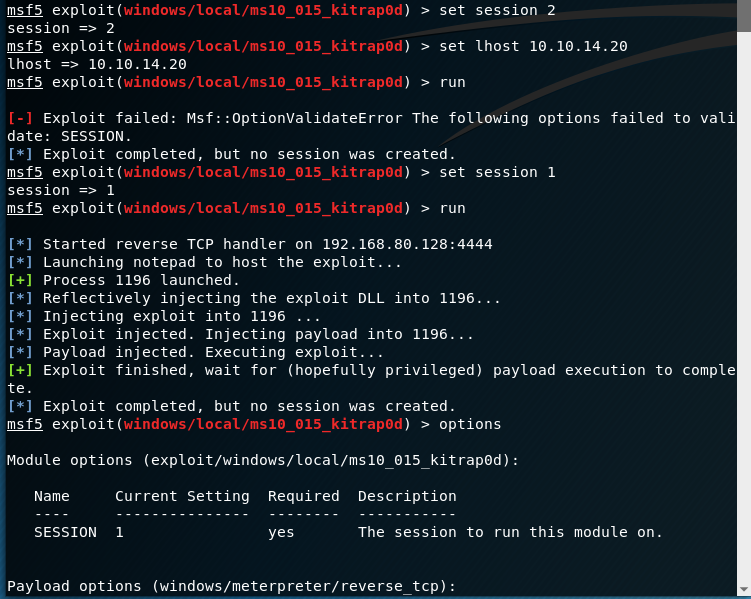
**Lucky enough, only one exploit**

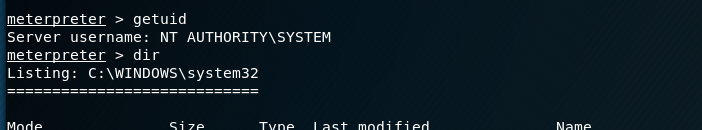
****

****

**Found 9 vulnerabilities to use , I tried the top one**

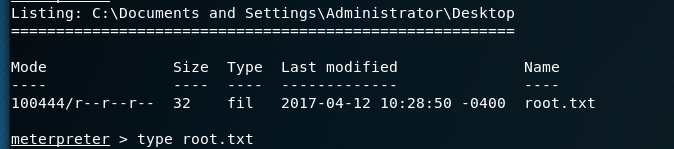
****

****

****

**Success! We are admin access**

****

****

**Success Both flags captured!**