**HackTheBox Optimum**

nmap -T4 -p- -A 10.10.10.8

Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-12 17:04 EST

Nmap scan report for 10.10.10.8

Host is up (0.10s latency).

Not shown: 65534 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http HttpFileServer httpd 2.3

|\_http-server-header: HFS 2.3

|\_http-title: HFS /

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 2012|Vista|2008|7 (90%)

OS CPE: cpe:/o:microsoft:windows\_server\_2012 cpe:/o:microsoft:windows\_vista::- cpe:/o:microsoft:windows\_vista::sp1 cpe:/o:microsoft:windows\_server\_2008::sp1 cpe:/o:microsoft:windows\_7

Aggressive OS guesses: Microsoft Windows Server 2012 (90%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (90%), Microsoft Windows Server 2012 R2 (90%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 7 Professional (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

1 104.69 ms 10.10.14.1

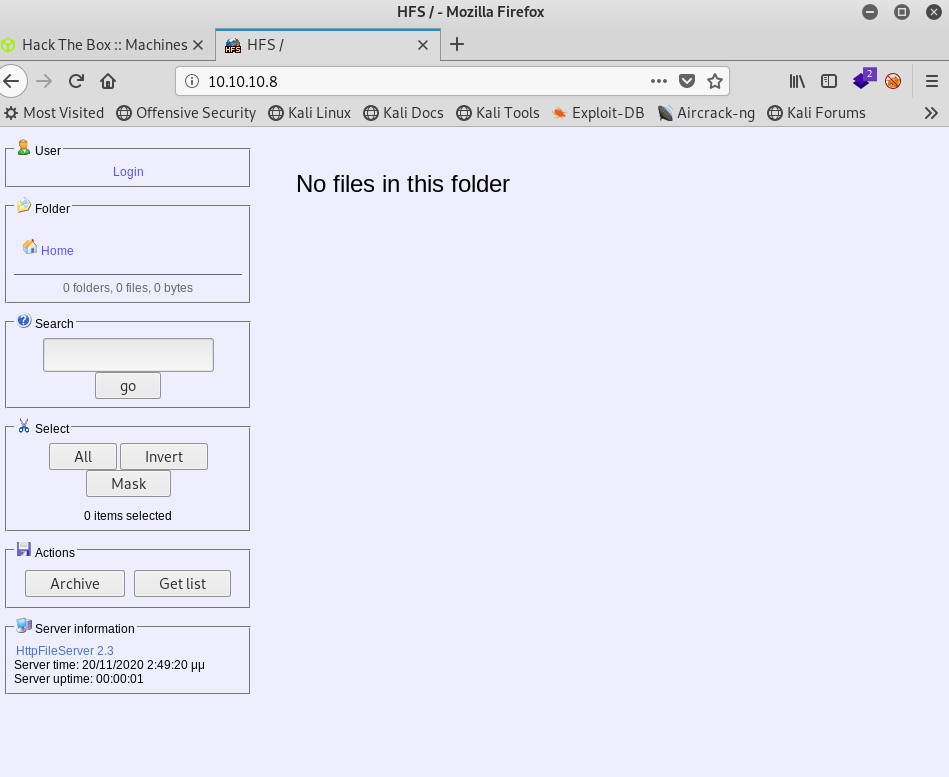
2 104.96 ms 10.10.10.8

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 197.71 seconds

I open firefox and go to 10.10.10.8

I see the webpage:



I see the httpFilerServer at the bottom version 2.3

It has a third party url:

[www.rejetto.com/hfs](http://www.rejetto.com/hfs)

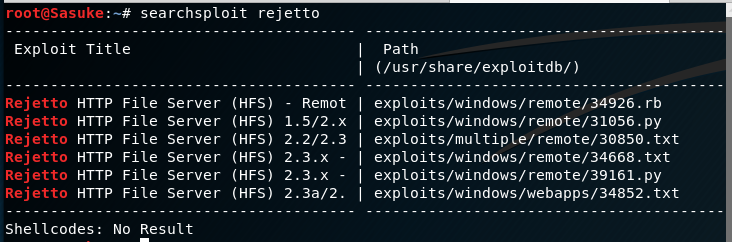
Given our nmap report:

80/tcp open http HttpFileServer httpd 2.3

This is our exploit

I open another terminal and type

Searchsploit rejetto

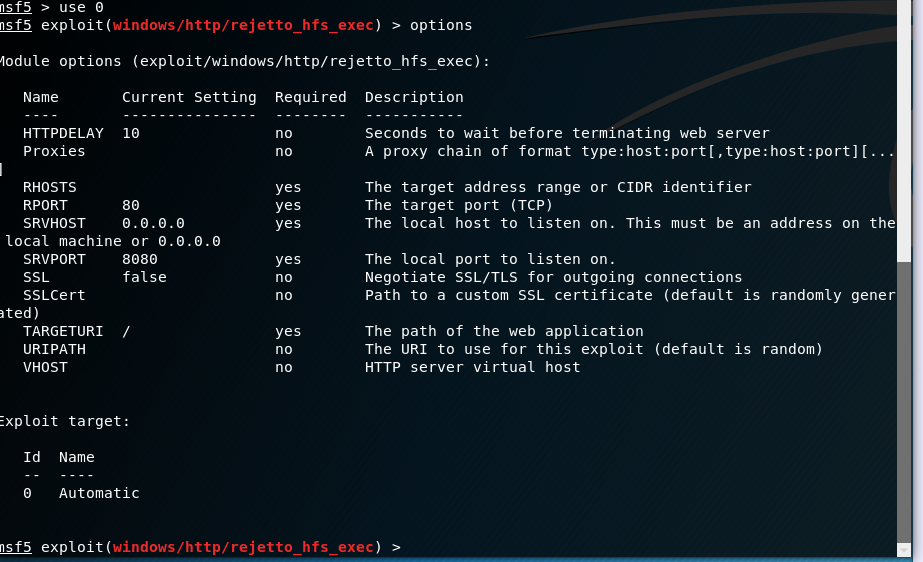


You can see above there are many exploits with version 2.3

Lets open msfconsole and see if an exploit is there for us to use:

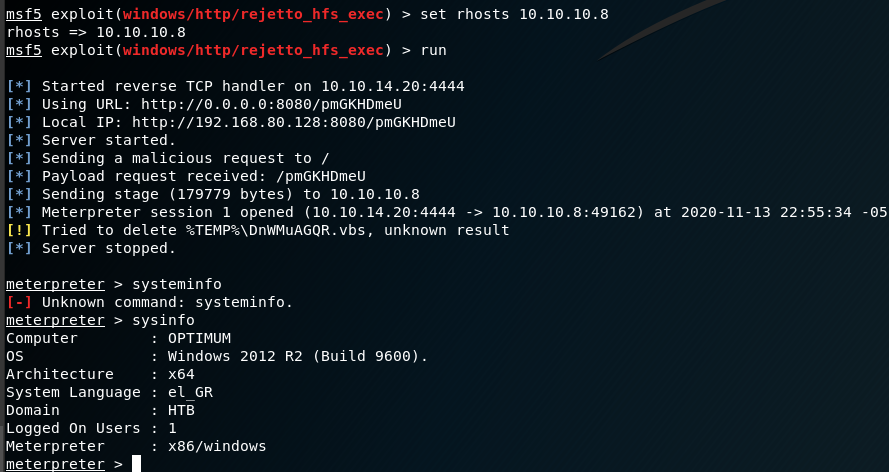


Perfect, one option to try out



It is time to try to set the rhosts and run the exploit

Success! We are in:



We can tell the OS is Windows 2012 R2 (build 9600)

And as a x64 OS as well

Time to set our payload for the correct version:



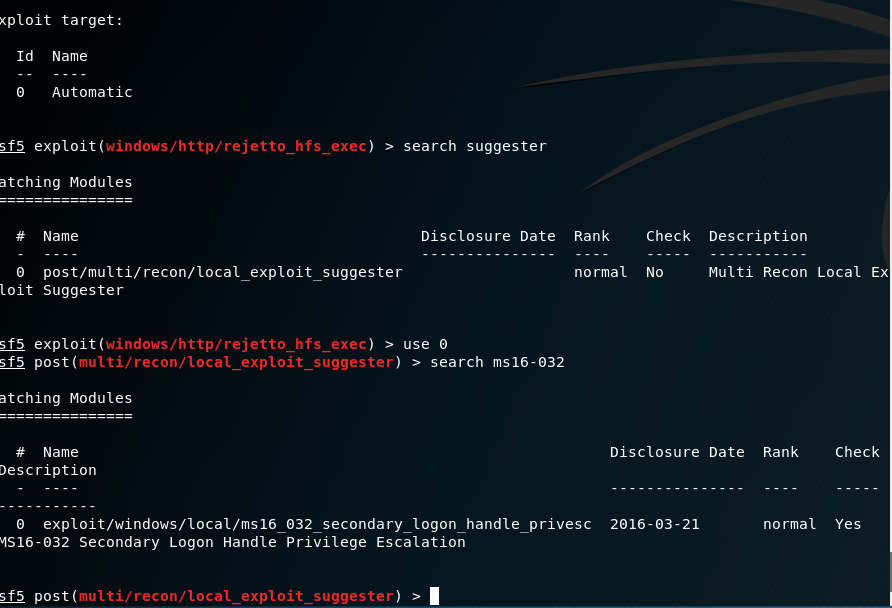
I then google windows 2012 r2 (Build 9600)

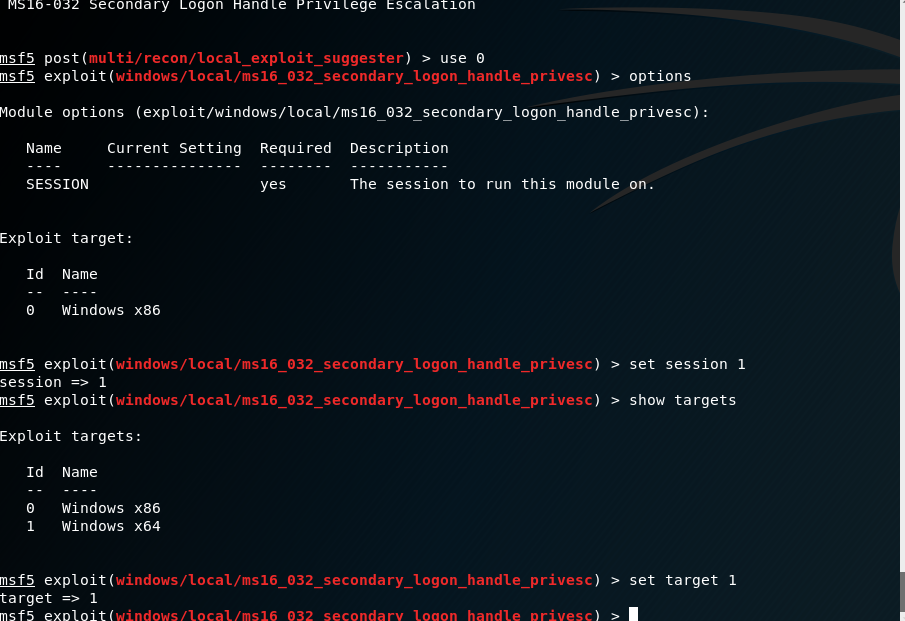
<https://www.exploit-db.com/exploits/39719>

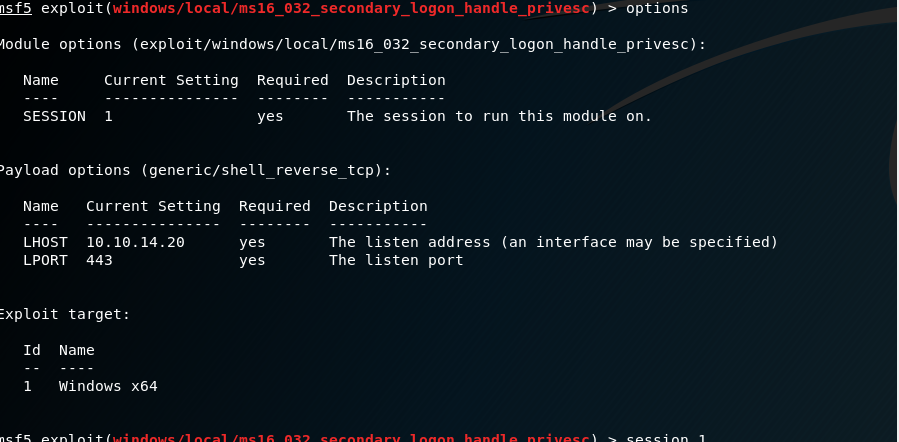
This exploit above can be uploaded on the user account

The URL gives me a MS16-032 exploit

I have to search for that in Metasploit







Now that everything is ready,

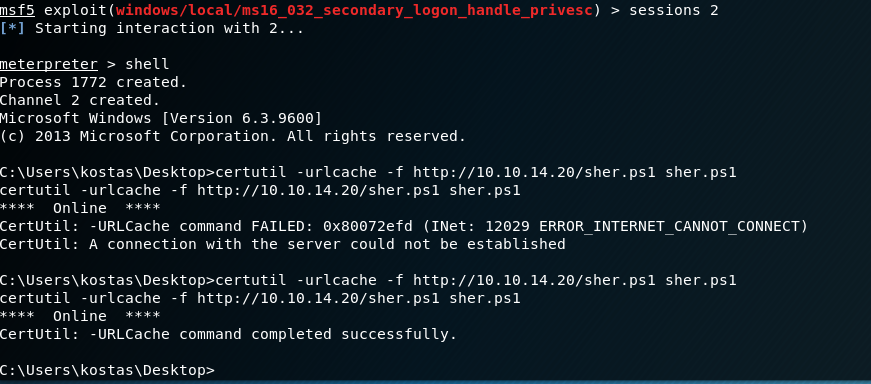
Using the exploit from the URL above.

I saved it as a sher.ps1 file in root

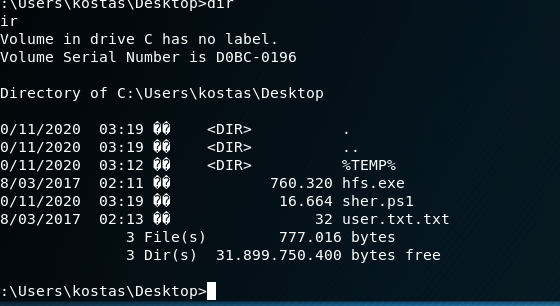
I then opened another terminal to run SessionHTTPServer to have it

Connect on port 80



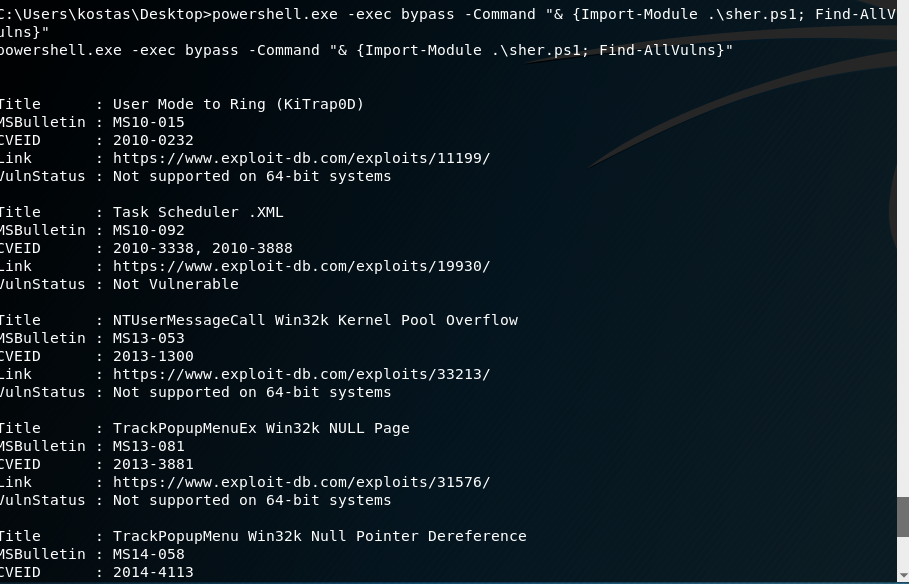


Success! Connected!



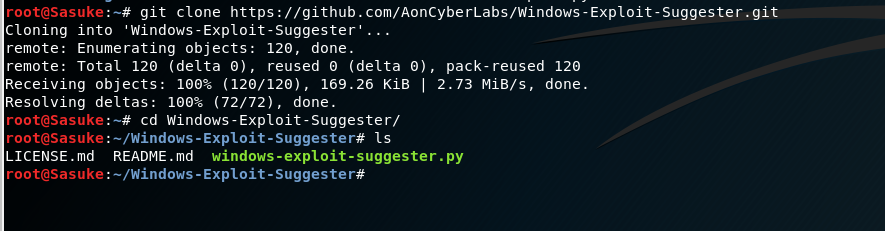
My Exploit is there!

Now I need to import sher.ps1

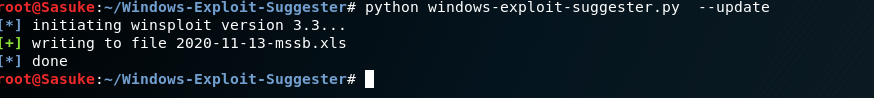


I see three vulnerabilities that the powershell ran

I google windows exploit suggester and clone a github <https://github.com/AonCyberLabs/Windows-Exploit-Suggester.git>



I need to update the exploit for an excel database following the git hub instructions



Now I need to go back to my shell and type systeminfo and copy all the data:

Host Name: OPTIMUM

OS Name: Microsoft Windows Server 2012 R2 Standard

OS Version: 6.3.9600 N/A Build 9600

OS Manufacturer: Microsoft Corporation

OS Configuration: Standalone Server

OS Build Type: Multiprocessor Free

Registered Owner: Windows User

Registered Organization:

Product ID: 00252-70000-00000-AA535

Original Install Date: 18/3/2017, 1:51:36 ��

System Boot Time: 20/11/2020, 2:48:50 ��

System Manufacturer: VMware, Inc.

System Model: VMware Virtual Platform

System Type: x64-based PC

Processor(s): 1 Processor(s) Installed.

[01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz

BIOS Version: Phoenix Technologies LTD 6.00, 12/12/2018

Windows Directory: C:\Windows

System Directory: C:\Windows\system32

Boot Device: \Device\HarddiskVolume1

System Locale: el;Greek

Input Locale: en-us;English (United States)

Time Zone: (UTC+02:00) Athens, Bucharest

Total Physical Memory: 4.095 MB

Available Physical Memory: 3.480 MB

Virtual Memory: Max Size: 5.503 MB

Virtual Memory: Available: 4.933 MB

Virtual Memory: In Use: 570 MB

Page File Location(s): C:\pagefile.sys

Domain: HTB

Logon Server: \\OPTIMUM

Hotfix(s): 31 Hotfix(s) Installed.

[01]: KB2959936

[02]: KB2896496

[03]: KB2919355

[04]: KB2920189

[05]: KB2928120

[06]: KB2931358

[07]: KB2931366

[08]: KB2933826

[09]: KB2938772

[10]: KB2949621

[11]: KB2954879

[12]: KB2958262

[13]: KB2958263

[14]: KB2961072

[15]: KB2965500

[16]: KB2966407

[17]: KB2967917

[18]: KB2971203

[19]: KB2971850

[20]: KB2973351

[21]: KB2973448

[22]: KB2975061

[23]: KB2976627

[24]: KB2977629

[25]: KB2981580

[26]: KB2987107

[27]: KB2989647

[28]: KB2998527

[29]: KB3000850

[30]: KB3003057

[31]: KB3014442

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) 82574L Gigabit Network Connection

Connection Name: Ethernet0

DHCP Enabled: No

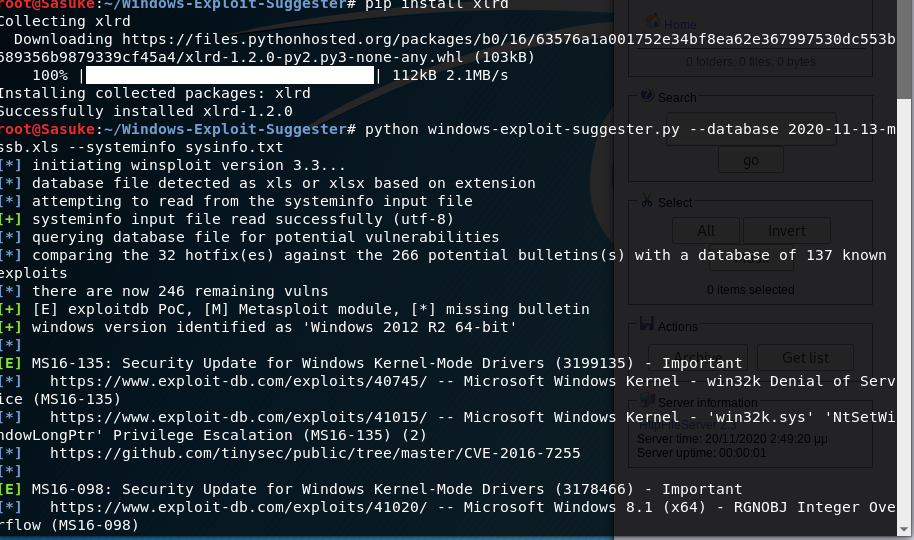
IP address(es)

[01]: 10.10.10.8

Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.

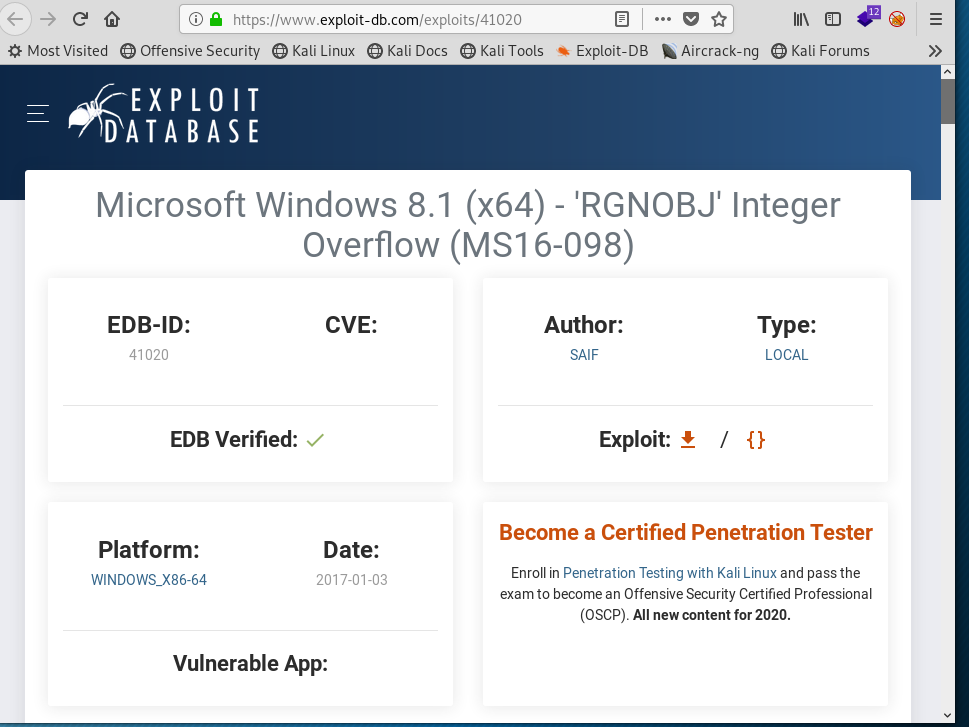
I created a txt file for the info above





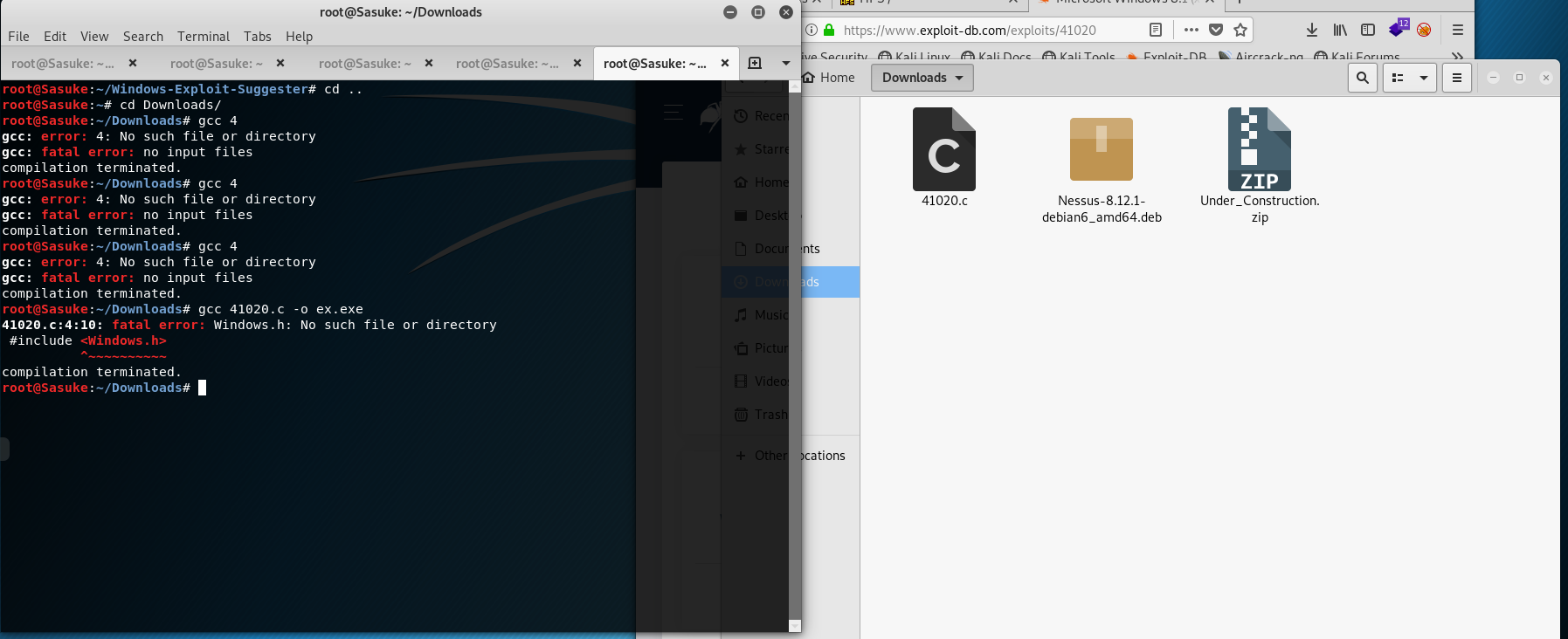
MS16-098 looks like our match!

It has a URL that takes us to:



Downloading the exploit

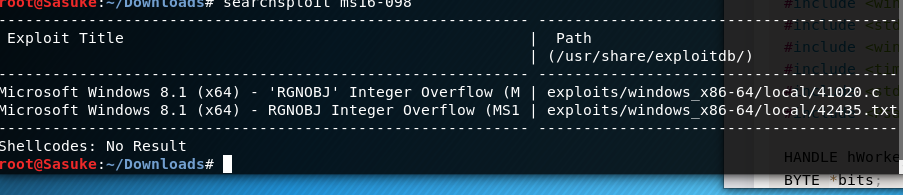
And it failed said it was missing windows.h



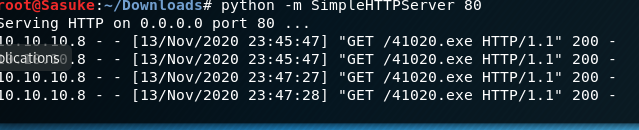
Going back to the website to download the binary link

<https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/41020.exe>

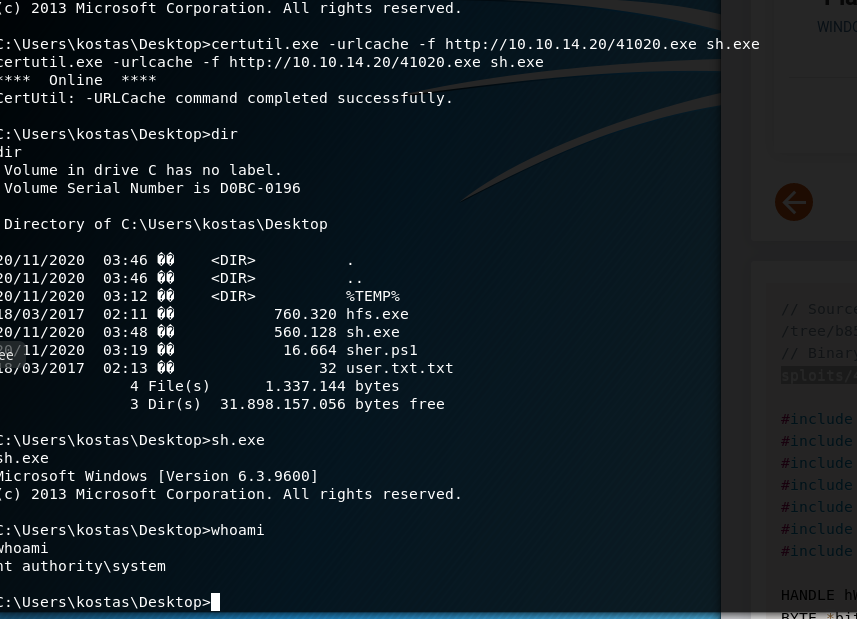
Double checking that ms16-098 is there for us to use



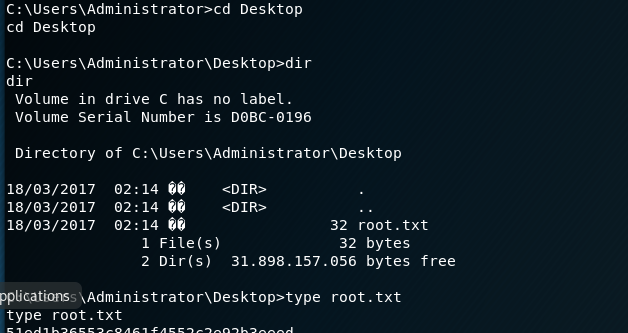
I now had to kill the python SimpleHTTPServer 80 and run it again in the downloads folder since the exploit is downloaded there



I run the exploit:



Success! Rooted this machine, grabbing the flag now:



Success! Rooted