

Office Lab

Created: 04-01-2021 19:09:30

Updated: 10-01-2021 00:15:45

Author: xShadowx

#Scanning And Enumeration.

So we have three(3) ports open

- 1. An ssh port on 22
 - 2. A web server running on 80.
 - 3. A web server(secure) on 443.

#Web without secure strip

A screenshot of a web browser showing a WordPress site. The title bar says "Dunder Mifflin - Just another WordPress site". The page content includes a heading "It is a WordPress Site.", a category "UNCATEGORIZED", a main title "New DM Forum Page", and a post by "dwight" on "May 8, 2020" with "No Comments". The post text reads: "Hey guys, it's your future manager, Dwight. Yes, you heard that right! I made an accountability booster to set off once you guys make 5 mistakes in a single day, which I bet will happen! I started a forum page on a subdomain, y'all can vent there before I send out an email to corporate. PS: Can't wait to fire you Jim! 😊".

Web With Secure Strip

A screenshot of a web browser showing the "Apache2 Ubuntu Default Page". The page features the Ubuntu logo and the text "Default Apache2 Server Page.". It includes a "Configuration Overview" section with a tree diagram of configuration files and a bulleted list of file descriptions.

```
/etc/apache2/
|-- apache2.conf
   |-- ports.conf
   |-- mods-enabled
      |-- *.load
      |-- *.conf
   |-- conf-enabled
      |-- *.conf
   |-- sites-enabled
      |-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

#Directories Found By dir-search

```
[15:46:11] 403 - 275B - ./htaccess_sc
[15:46:11] 403 - 275B - ./htm
[15:46:11] 403 - 275B - ./html
[15:46:11] 403 - 275B - ./htpasswd_test
[15:46:11] 403 - 275B - ./htpasswd
[15:46:14] 403 - 275B - ./httr-oauth
[15:46:14] 403 - 275B - ./php
[15:47:24] 301 - 0B - /index.php → http://office.csl/
[15:47:24] 301 - 0B - /index.php/login/ → http://office.csl/login/
[15:47:28] 200 - 19KB - /license.txt
[15:47:47] 200 - 7KB - /readme.html
[15:47:51] 403 - 275B - /server-status
[15:47:51] 403 - 275B - /server-status/
[15:48:07] 301 - 311B - /wp-admin → http://office.csl/wp-admin/
[15:48:07] 302 - 0B - /wp-admin/ → http://office.csl/wp-login.php?redirect_to=h
ttp%3A%2F%2Foffice.csl%2Fwp-admin%2F&reauth=1
[15:48:07] 400 - the user 1B - /wp-admin/admin-ajax.php
[15:48:07] 200 - 0B - /wp-config.php
[15:48:07] 500 - 3KB - /wp-admin/setup-config.php
[15:48:07] 200 - 1KB - /wp-admin/install.php
[15:48:07] 301 - 313B - /wp-content → http://office.csl/wp-content/
[15:48:07] 200 - 0B - /wp-content/
[15:48:07] 200 - 69B - /wp-content/plugins/akismet/akismet.php
[15:48:07] 500 - 0B - /wp-content/plugins/hello.php
[15:48:07] 403 - 275B - /wp-content/upgrade/
[15:48:07] 403 - 275B - /wp-content/uploads/
[15:48:08] 301 - 314B - /wp-includes → http://office.csl/wp-includes/
[15:48:08] 403 - 275B - /wp-includes/
[15:48:08] 200 - 0B - /wp-cron.php
[15:48:08] 500 - 0B - /wp-includes/rss-functions.php
[15:48:08] 302 - 0B - /wp-signup.php → http://office.csl/wp-login.php?action=re
gister
[15:48:08] 200 - 5KB - /wp-login.php
[15:48:09] 405 - 42B - /xmlrpc.php
```

So Before going and checking every single directory in here i decided to hunt directories for the other server too(the secure one with the default page)

```

Target: https://172.31.3.1/
Output File: /root/ctf/csl/office/dirsearch/reports/172.31.3.1/_21-01-09_15-51-05.txt

[15:51:05] Starting:
[15:51:18] 403 - 276B - ./ht_wsr.txt
[15:51:18] 403 - 276B - ./htaccess.bak1
[15:51:18] 403 - 276B - ./htaccess.sample
[15:51:18] 403 - 276B - ./htaccess.orig
[15:51:18] 403 - 276B - ./htaccess.save
[15:51:18] 403 - 276B - ./htaccessBAK
[15:51:18] 403 - 276B - ./htaccessOLD
[15:51:18] 403 - 276B - ./htaccessOLD2
[15:51:18] 403 - 276B - ./htaccess_extra
[15:51:18] 403 - 276B - ./htaccess_orig
[15:51:18] 403 - 276B - ./htaccess_sc
[15:51:18] 403 - 276B - ./htm
[15:51:18] 403 - 276B - ./html
[15:51:18] 403 - 276B - ./httpd.conf
[15:51:18] 403 - 276B - ./htpasswd
[15:51:18] 403 - 276B - ./httrc
[15:51:22] 403 - 276B - ./php
[15:52:27] 301 - 310B - /forum → https://172.31.3.1/forum/
[15:52:27] 200 - 29KB - /forum/
[15:52:32] 200 - 11KB - /index.html
[15:53:00] 403 - 276B - /server-status/
[15:53:00] 403 - 276B - /server-status
[15:53:15] 200 - 5KB - /wordpress/wp-login.php
[15:53:16] 200 - 32KB - /wordpress/

Task Completed

[root💀 kali]-(~/ctf/csl/office/dirsearch]
# 

```

The /forum page seemed a bit interesting so i decided to look at that, and...

A Conversation between people

Dwight
5 mistakes and an email will be sent to corporate automatically at 5PM today. Should you have any questions, ask them here.
I finally got Meredith to get off hold for 30 minutes and go back to work.

Meredith
This just turned into a real job.

William Charles Schnider
Don't do any work folks, then we won't have any mistakes!
Anyway, www.creedthoughts.gov - check it out

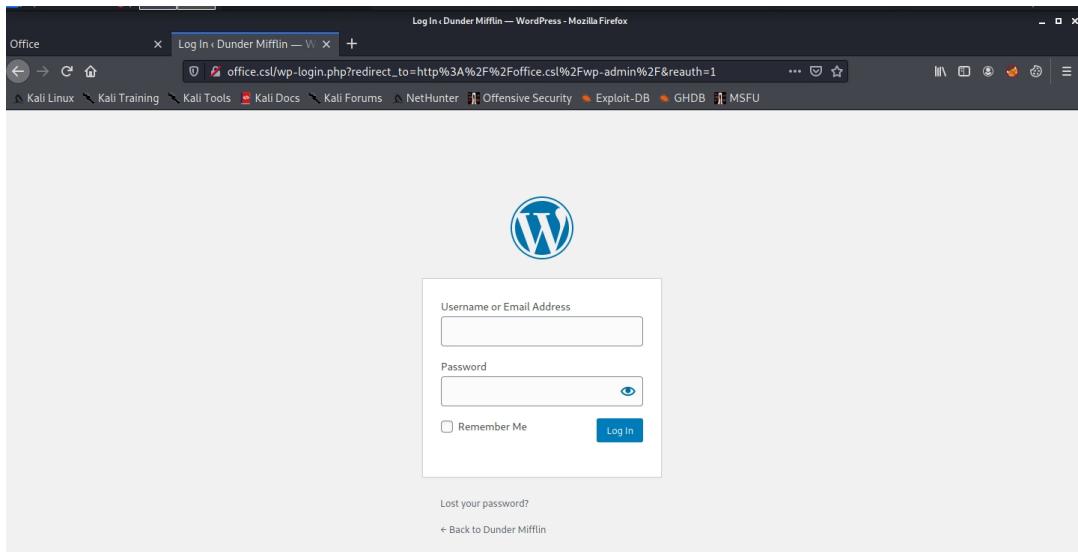
Andy
Creed, why is your name set to "William Charles Schnider"?
This reflects in the chat logs, corporate is going to be very confused over this.

Phyllis
I'm going to go ahead and start guessing passwords to trip the device.

Oscar
I need someone to manage a shipment over in the accounting department.

Kevin
On it!

This page got my eye as previously i found a word-press login page



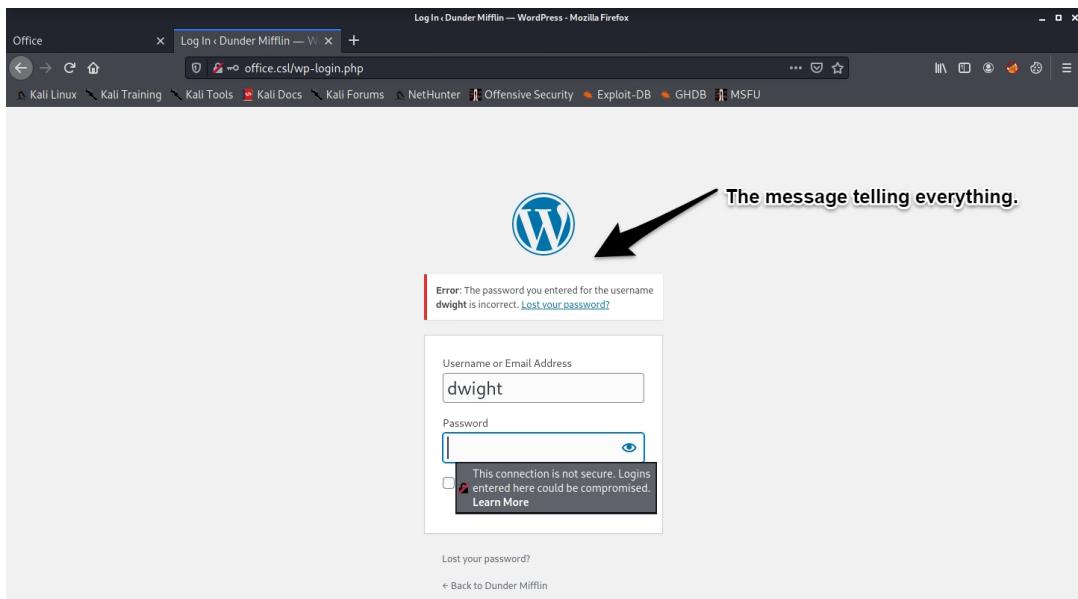
But there was still one problem that was i needed a username so while reading the conversation i found this

This guy is telling some usefull info that he managed to forward the portal to localhost on his account.

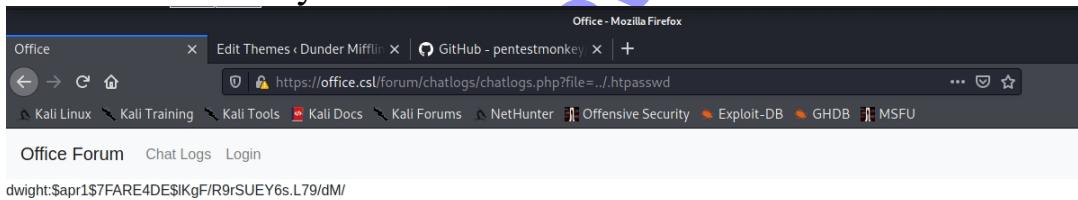
It appears that these people are guessing passwords of someone and in the end two people tell a person dwight to shutdown the machine.

These two.

So from here i thought checking any available username for person d-w-i-g-h-t and i got lucky.



So this message by the server has confirmed everything - there is a user named d-w-i-g-h-t on word-press but we don't have the password yet so in the scan results the word-press version was 5.4.1 so lets search for any exploit against that before spending hours on dictionary attacks.



So i found out that the web service is vulnerable to a L.F.I{ Local File Inclusion } so i decided to take a word list full of these random payload and w fuzz that out

i will always look out for the ht password file as this contains
passwords
so i found the password and cracked it using john.

```

└─[root@kali]─[~/ctf/csl/office/hash]
# john --wordlist=/home/kali/rockyou.txt hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)

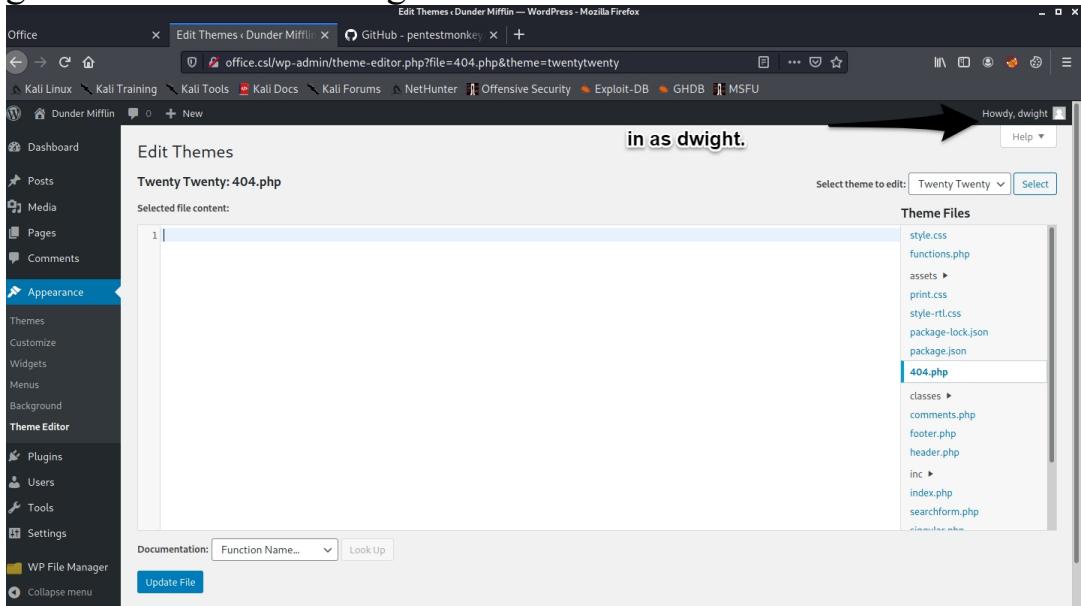
└─[root@kali]─[~/ctf/csl/office/hash]
# john --show hash.txt
?:cowboys1                                Password.

1 password hash cracked, 0 left

└─[root@kali]─[~/ctf/csl/office/hash]
# 

```

Then i decided to login to word-press using these credentials and i got in as the user d-w-i-g-h-t.



Now i will edit the 404 page the error page and access the page from other u-r-l to get a reverse shell.
unfortunately this did not worked for some reason and after some time searching here and there i found this

I Uploaded my file here and then access from other url.

Got shell but as web and got user access and the access flag.
now we needed root so i ran lin-peas and discovered a port open
on 10000 and decided to forward it to my localhost using ssh (with
-L localhost:10000:localhost name@office.cs1)
and i found this then

The web-min framework was very vulnerable so i found a matching exploit for it(credits to m-e-t-a-s-p-l-o-i-t)
and after exploiting i got a shell as root.

```
Swap usage: 0%  
root@office:~# ls  
ls  
system.txt  
root@office:~# cat system.txt  
cat system.txt  
39bd97013feb7508923ed8ace6fe6130 f  
root@office:~#
```

And also the system flag and pwned the machine.
Awesome.