
PwnAdventure3



Welcome to Pwnie Island!

Pwn Adventure 3: Pwnie Island is a limited-release, first-person, true open-world MMORPG set on a beautiful island where anything could happen. That's because this game is intentionally vulnerable to all kinds of silly hacks! Flying, endless cash, and more are all one client change or network proxy away. Are you ready for the mayhem?!

- Official Site: <http://www.pwnadventure.com/>

YouTube Series

This setup is part of a video series covering the different hacks and challenges in this game.

- Let's Play/Hack - Pwn Adventure 3: Pwnie Island - part 1 [39:20]
- Setup Private Server with Docker - Pwn Adventure 3: part 2 [8:42]
- Information Gathering / Recon - Pwn Adventure 3: part 3 [14:09]
- Recover Game Classes with gdb - Pwn Adventure 3: part 4 [11:28]
- Hooking on Linux with LD_PRELOAD - Pwn Adventure 3: part 5 [12:07]
- Flying and our first Flag! (Cow King) - Pwn Adventure 3: part 6 [6:34]
- Teleporting and Hovering (Unbearable Revenge) - Pwn Adventure 3: part 7 [9:31]

-
- Find the hidden Golden Eggs - Pwn Adventure 3: part 8 [10:26]
 - Developing a TCP Network Proxy - Pwn Adventure 3: part 9 [12:26]
 - Analyzing the Game Network Protocol - Pwn Adventure 3: part 10 [14:48]
 - Implementing Autoloot with the Proxy - Pwn Adventure 3: part 11 [12:33]
 - Exploiting an Integer Overflow (Fire and Ice) - Pwn Adventure 3: part 12 [19:59]
 - †: Signed and Unsigned Integers - Integer Overflows - Pwn Adventure 3: part 12.5 [3:12]
 - Analyzing the Blocky Logic Puzzle - Pwn Adventure 3: part 13 [10:51]
 - Failing at Machine Learning (Blocky part 2) - Pwn Adventure 3: part 14 [14:34]
 - Reversing Input Validation (Keygen part 1) - Pwn Adventure 3: part 15 [12:27]
 - Reversing Custom Encoding (Keygen part 2) - Pwn Adventure 3: part 16 [16:01]
 - Understanding the Key Verification Algorithm (Keygen part 3) - Pwn Adventure 3: part 17 [13:10]
 - RSA Implemented in Assembler (Keygen part 4) - Pwn Adventure 3: part 18 [16:23]
 - RSA Implemented in JavaScript (Keygen part 5) - Pwn Adventure 3: part 19 [4:32]
 - The Last Flag (Overachiever) - Pwn Adventure 3: part 20 [5:31]

Excluding the casual Let's Play at the start, the whole series is covering all challenges of Pwn Adventure 3 in less than 4 hours.

Install Server

Requirements

From the official README:

- At least 2GB of RAM, more RAM will allow more instances to be run on a single machine
- The Game Server does not need any graphics hardware and runs purely on console. It is known to run well on Amazon AWS and Digital Ocean VPS instances.
- The Game Server requires a lot of RAM to run, but uses fork and copy-on-write memory to allow many instances to run on a single host.
- For a server with 2GB of RAM, it is not recommended to run more than 5 instances, but a server with 8GB of RAM can typically run as many as the CPU can handle.
- It is recommended to use 2-3 instances per CPU core if you have sufficient RAM. You may be able to run 4-5 instances per core, but doing so may introduce slight lag.
- The files for the client and server are over 2GB as well, so several GB of free disk space are required.

There are several ways to build and deploy your own server.

Option 1 - Original

One option is to download and follow the instructions included in the README of the official files. The download can be found on the official website here <http://www.pwnadventure.com/#server>.

Option 2 - Guide

@Beaujeant created an excellent, and easy to follow step-by-step guide. It was also the basis for building the docker image from Option 3. The guide can be found here: <https://github.com/beaujeant/PwnAdventure3/blob/master/INSTALL-server.md>.

Option 3 - Docker

This option is super easy, as long as `docker` and `docker-compose` are installed on a host. It makes it easy to run and tear down a server, without making changes to the actual host system.

First, gather all necessary files:

```
1 git clone https://github.com/LiveOverflow/PwnAdventure3.git
2 cd PwnAdventure3
3 wget http://pwnadventure.com/pwn3.tar.gz
4 tar -xvf pwn3.tar.gz
```

In order to run the server, `docker` and `docker-compose` have to be installed. Docker is moving fast, so it's a good idea to follow the current official steps for installation (which could also include to remove an older system version of docker):

- Docker CE Ubuntu: <https://docs.docker.com/install/linux/docker-ce/ubuntu/>.
- `docker-compose`: <https://docs.docker.com/compose/install/>
- make sure the current user is part of the `docker` group with: `sudo usermod -a -G docker $USER`. restart or re-login and verify with `id` that the user is part of the docker group.

Then simply build the image and launch the master and game server:

```
1 docker-compose build
2 docker-compose up
```

`docker-compose up` can also run in detached/background mode with `-d`.

Install Client

First download the client from the official website here: <http://www.pwnadventure.com/#downloads>

To get a client connected to the new server, the `server.ini` for the client has to be modified. The server launched with docker expects that hostnames `master.pwn3` and `game.pwn3` are being used (These could theoretically be changed in the docker/setup files).

The `server.ini` for the client has to look something like this:

```
1 [MasterServer]
2 Hostname=master.pwn3
3 Port=3333
4
5 [GameServer]
6 Hostname=game.pwn3
7 Port=3000
8 Username=
9 Password=
10 Instances=
```

Make sure that the client can reach these hosts, for example by adding them to the `/etc/hosts` file. In this example the server is running on `192.168.178.57` and the entry for them would be:

```
1 192.168.178.57 master.pwn3
2 192.168.178.57 game.pwn3
```

Warning: Using an IP as `Hostname` in the `server.ini` does not work! I spent 2 hours trying to figure out what was wrong.

To stop the server, simply type `docker-compose down`.

Warning: The database file is not persistent - taking down the container resets everything. So backup first.

Troubleshooting

Error: docker-compose build

```
1 $ docker-compose build
2 Building init
3 ERROR: Error processing tar file(exit status 1): write /client/
   PwnAdventure3_Data/PwnAdventure3/PwnAdventure3/Content/Paks/
   Characters.pak: no space left on device
```

A: Get more disk space.

```
1 $ docker-compose build
2 Building init
3 ERROR: Couldn't connect to Docker daemon at http+docker://
  localunixsocket - is it running?
```

A: Your user is probably not part of the `docker` group or docker service not running. `sudo usermod -a -G docker pwn3`, verify with `id`. Or `service docker restart`.

File Integrity

Check if the archive is corrupted

```
1 $ md5sum pwn3.tar.gz
2 d3f296461fa57996018ce0e4e5a653ee  pwn3.tar.gz
3 $ sha1sum pwn3.tar.gz
4 022bd5174286fd78cd113bc6da6d37ae9af1ae8e  pwn3.tar.gz
```

PwnAdventure3 Client Errors

Connection Error: Unable to connect to master server

This probably means that the MasterServer is not reachable.

- Client issues:
 - Check the `[MasterServer]` entry in the client's `server.ini`
 - Can you ping `master.pwn3` from the host from your system?
 - Is the IP correct in the `/etc/hosts` file?
- Server issues:
 - Is the server not running and listening on port 3333?
 - Check with `sudo netstat -tulpn`
 - * Is the master server listening: `tcp6 0 0 :::3333 :::* LISTEN 31913/docker-proxy`
 - Check `docker ps` if the two containers are up
 - * master server running? `880f93374070 pwn3server "/opt/pwn3/setup/mas..."0.0.0.0:3333->3333/tcp, 5432/tcp pwnadventure3_master_1`

Waiting in connection queue...

This means the MasterServer *is* reachable and is waiting now for a free GameServer that can be given to the client. This probably means that no GameServer is running, or was not able to connect to the MasterServer.

- Server issues:

- Is a game server running and listening on port 3000–3005?
- Check listening processes with `sudo netstat -tulpn`
- `tcp6 0 0 :::3000 :::* LISTEN 32160/docker-proxy`
- Is `pwnadventure3_game_1` container running? Check with `docker ps -a`
 - * `84343f81034f pwn3server "/opt/pwn3/setup/gam..."0.0.0.0:3000-3010->3000 tcp, 5432/tcp pwnadventure3_game_1`
- do you see the following line in the log from `docker-compose up`: `line 1: 7 Killed ./PwnAdventure3Server; pwnadventure3_game_1 exited with code 137`
 - * GET MORE RAM!

Docker versions

These versions were used during testing as a host:

```
1 $ uname -a
2 Linux ubuntu 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13
   01:07:32 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
3 $ docker-compose version
4 docker-compose version 1.19.0, build 9e633ef
5 docker-py version: 2.7.0
6 CPython version: 2.7.13
7 OpenSSL version: OpenSSL 1.0.1t  3 May 2016
8 $ docker --version
9 Docker version 17.12.1-ce, build 7390fc6
```

Credits

The true heroes, are the people who built the game <3

Pwn Adventure 3 is the brainchild of one Rusty Wagner. He's responsible for the idea, the planning, and nearly all of the execution (programming, level design, quests, and so forth). Without him, there would be no game! Special thanks also goes to the Ghost in the Shellcode organizers for their support during development and testing.

By Vector35 - <https://vector35.com/> (the company behind the popular disassembler Binary Ninja)