Wargame 8 (Week 9) | COMP6447 20T2

The following wargames will provide you with exercises where you will be required to:

1. hack stuff

This weeks challenges are Harder ROP!

You will need to use a libc-database to figure out the version of remote libc for these chals

You can download the challenges here: https://cloudstor.aarnet.edu.au/plus/s/Wfp3KQEQYxnX1xU

These challenges are a zip file with the password: Wh3reIsJazz'sJumper?

There are **2 exploitation challenges** this week!

Try to solve the **exploitation** challenges locally first, then connect to our servers to obtain the flags. To get full marks you must get the flag from our servers.

Challenge	PORT	type
bsl	8001	pwn
piv_it	8002	pwn

Each **exploitation** challenge has a flag to submit. The flag is in the format FLAG{XXX}. To get full marks in this wargame, you need to submit all flags.

Submission Instructions

A markdown document (.md) containing the following for each challenge:

We are interested in proof that you understood the challenge, the vulnerabilities and how to exploit them. This is not intended as a formal bug report.

```
chal1
==========================
Flag: FLAG{hi}
General overview of problems faced
------------------------------------
Had to hack the program
Script/Command used
------------------
```
print "hello_world"
```
```

Please submit the document as a markdown file on give. You may submit as many times as you like. Only your most recent submission will be marked.

Submission

```
give cs6447 war8 war8.md
```

Marking scheme

This week's wargames are worth 5 marks in total.

Due date

The wargames are due **17:59 Tuesday 4th August (Sydney time).** This is in Week 10.

Late Penalty

Late submissions will have marks deducted from the maximum achievable mark at the rate of 1 mark *per day* that they are late.

Resource created 3 months ago, last modified 3 days ago.

You can also submit using `give cs6447 war8 file1 file2 file3 ...`

Hold CTRL when clicking files to upload multiple files at the same time.

You can also check your submission using `6447 classrun -check war8`

Fetching...

You can also collect your submission using `6447 classrun -collect war8`

Fetching...