Wargame 4 | COMP6447 20T2

WARNING: this weeks challenges are tough, don't leave them to the end of the week. start early!!!

ASLR IS ENABLED THIS WEEK!!!

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

1. hack stuff

2. Defeat ASLR in a buffer overflow

3. Use format string vulns to pop shells

You can download the challenges here: https://cloudstor.aarnet.edu.au/plus/s/KKZm6ul8HHOhEzP

These challenges are a zip file with the password: GoogleCTFWasL1terallyUnsolvable!

There are **4 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	IP:PORT	type
door	plsdonthaq.me:4001	fmt string
snake	plsdonthaq.me:4002	buffer-overflow
formatrix	plsdonthaq.me:4003	fmt string
sploitwarz	plsdonthaq.me:4004	fmt string

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 war4 war4.md
```

Marking scheme

Each week's wargames are worth 3 marks in total.

Due date

The wargames are due **17:59 Tuesday 30th June (Sydney time).** This is in Week 5.

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 about a month ago, last modified 4 days ago.

You can also submit using `give cs6447 war4 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 war4`

Fetching...

You can also collect your submission using `6447 classrun -collect war4`

Fetching...