

## Wargame 6 (Week 7) | COMP6447 20T2

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

1. hack stuff

**This weeks challenges are ROP! Included in the zip file, is the exact version of libc used on the server.**

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

These challenges are a zip file with the password: Sp1d3rsAreScary:(

There are **4 exploitation challenges** this week and **1 reverse engineering challenge** !

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
swrop	6001	pwn
static	6002	pwn
roproprop	6003	pwn
ropme	6004	pwn
re	none	re

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.

## Reversing challenges

There is **one** reversing challenge this week. You need to submit the **most simplified version** of C that would compile into the supplied assembly

**simply putting each instruction into it's C counterpart is not correct. You must notice patterns and simplify the C code to understand what it is doing!!!**

```
int modulo_14(int a) {  
    int c = a + 0x10;  
    int d = c & 0x813910412;  
    int e = c + a - b;  
    int f = d * 0xde000 + e;  
}
```

```

        printf("%d\n", f);
    }

    vs

    struct s {
        int var_1;
        char var_2;
    };

    int module_14(struct s a) {
        printf("%d\n", a.var_1);
    }

```

**The first won't get any marks**

## 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.

```

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

re challenge
=====
General overview of problems faced
-----
needed to use man page to find arguments for atoi
```C
int main(int argc, char** argv) {
    int a = atoi(argv[1][0]);
    if (a > 20) {
        printf("%d\n", a + b);
    }
}
```

```

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 war6 war6.md

## Marking scheme

This week's wargames are worth 4 marks in total.

## Due date

The wargames are due **17:59 Tuesday 21th July (Sydney time)**. This is in Week 8.

## 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 2 months ago, last modified 4 days ago.