

Resources / Wargames (/COMP6447/22T2/resources/75148) / Wargame 1

Wargame 1

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

1. Learn how to use pwntools

You will require some sort of scripting language to solve these challenges.

Before you start, we recommend looking through lab 0 and lab 1 for a tutorial on how to setup your machine to complete these challenges + tutorials on how to use pwntools.

You can download the challenges here: <https://cloudstor.aarnet.edu.au/plus/s/3p3BYhFPjqD70cW>
(<https://cloudstor.aarnet.edu.au/plus/s/3p3BYhFPjqD70cW>)
(<https://cloudstor.aarnet.edu.au/plus/s/3p3BYhFPjqD70cW>)

These challenges are a zip file with the password: B@nanasareh3althy

There are 2 challenges this week, they **are** weighted equally.

Try to solve these challenges locally, the challenges are also hosted on our servers, and **you need to connect to these** to get the flag.

Challenge	IP:PORT
intro	comp6447.wtf:20478
too-slow	comp6447.wtf:20677

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

These flags are **UNIQUE** per student. Sharing flags will result in a **0 mark**.

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.

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

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 war1 war1.md
```

Marking scheme

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

Due date


The wargames are due **17:59 Monday 6th June (Sydney time)**. This is in Week 2.

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 16 days ago (Wednesday 18 May 2022, 11:35:23 AM), last modified 6 days ago (Saturday 28 May 2022, 09:03:21 AM).

Comments

 [Q \(/COMP6447/22T2/forums/search?forum_choice=resource/75152\)](/COMP6447/22T2/forums/search?forum_choice=resource/75152)

 [\(/COMP6447/22T2/forums/resource/75152\)](/COMP6447/22T2/forums/resource/75152)

 Add a comment



Zelun Li (</users/z5260511>) about 2 hours ago (Fri Jun 03 2022 14:26:33 GMT+1000 (Australian Eastern Standard Time)), last modified about 2 hours ago (Fri Jun 03 2022 14:26:46 GMT+1000 (Australian Eastern Standard Time))

Well done! You have successfully completed the basics!

Hi,

After getting this from the server how do we view the flag? It didn't send back a flag.

Reply



Chi Zhang (/users/z5211214) [3 days ago \(Tue May 31 2022 23:33:34 GMT+1000 \(Australian Eastern Standard Time\)\)](#)

For task 1 is the hidden flag the final answer?

Reply



Christovian Tanuarta (/users/z5258947) [2 days ago \(Wed Jun 01 2022 09:52:46 GMT+1000 \(Australian Eastern Standard Time\)\)](#)

/flag after gaining access to get the flag is what I did.

Reply



Simon Blain (/users/z5200681) [4 days ago \(Mon May 30 2022 11:09:17 GMT+1000 \(Australian Eastern Standard Time\)\)](#)

Hi,

I am a bit confused about the address 'xV4\x12\n' we are sent. It seems to be in hex but there is the V in the second character. Is there a typo in this address or am I just misunderstanding something?

Thanks

Reply



Andrew Yu (/users/z5169772) [3 days ago \(Tue May 31 2022 15:34:13 GMT+1000 \(Australian Eastern Standard Time\)\)](#)

There is no backslash in front of the first x, think about what that means (and how python will read out byte strings to you).

Reply



Hashimi-Mahmood Chau (/users/z5242398) [3 days ago \(Tue May 31 2022 10:14:42 GMT+1000 \(Australian Eastern Standard Time\)\)](#)

Yep, I'm also stuck on this part. Did you manage to figure it out?

Reply



Simon Blain (/users/z5200681) [3 days ago \(Tue May 31 2022 10:44:48 GMT+1000 \(Australian Eastern Standard Time\)\)](#)

Not yet, I moved on to part 2 for now.

Reply

