Replay Attack Exercise 1

Intro

You withdrew 1 ETH from a centralized exchange to your wallet.

When you looked at the withdrawal transaction, you realized that it was from a multi-signature wallet smart contract.

Looking at the transaction, you noticed that two signatures were sent to the function:

Signature 1:

```
{
  r: '0x02efb15972bac0ba578c0f95623bd95d10ca5f601d1d999308187e7dae738733',
  s: '0x213c76c501b9d9d5d4e81215ba15f1feb6e78be070dbca257f2b61d163e84255',
  v: 28,
}
```

Signature 2:

```
{
  r: '0x132e7ee1157ea4d2638187b2244202d8088a39cc7293a6895dfdf7fcfd3172ae',
  s: '0x18146aa45b156b100b280a91da1df53b533d7ec4e7d2c1740d0fe0e031ef8056',
  v: 28,
}
```

There's 100 ETH in this wallet right now. Can you get it all?

Accounts

- 0 - Deployer & Signer 1
- 1 - Signer 2
- 2 - Attacker (You)

Tasks

Task 1

Drain all the MultiSig wallet ETH!

Task 2

Make sure the MultiSig wallet is secured so that future attacks won't be possible.

Test the attack and make sure it failed, you may change the `before` section for this task.