Computação Distribuída

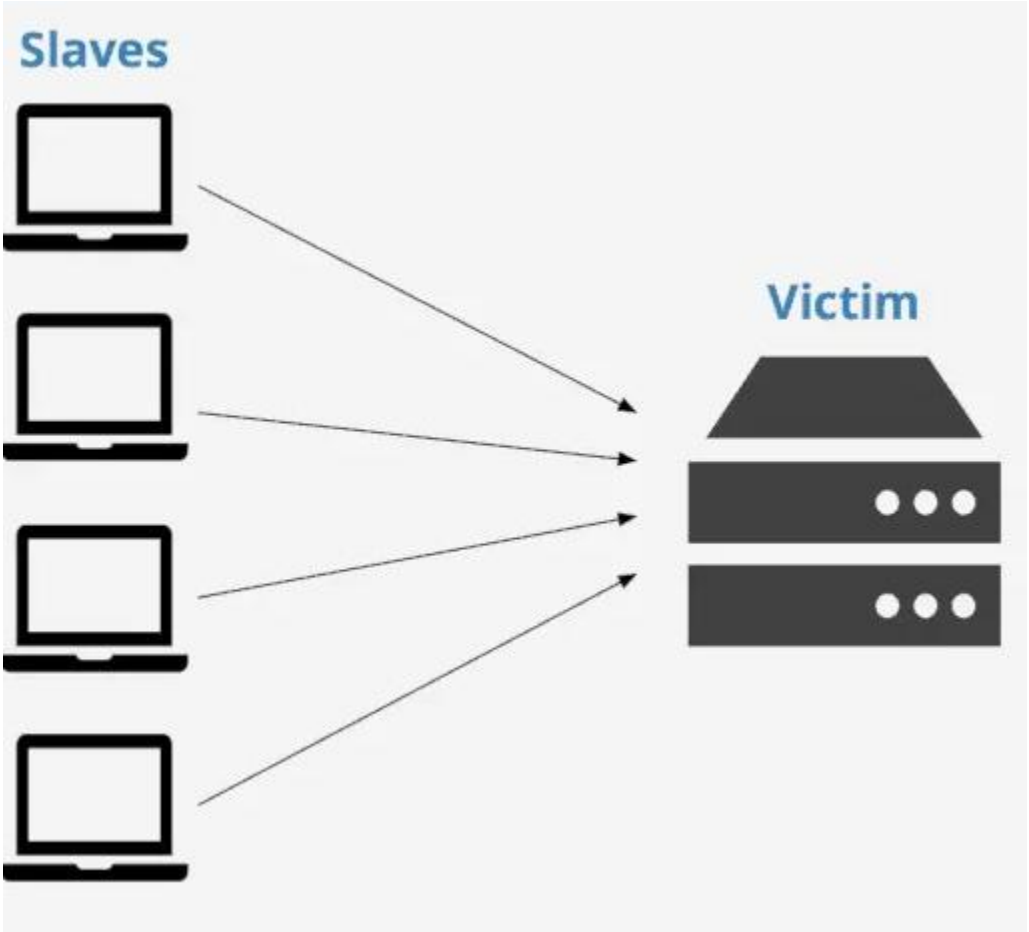
Projeto Final

Distributed Password Cracker

LEI / Universidade de Aveiro
Diogo Gomes & Nuno Lau
Junho 2021

Introdução

O objetivo deste projeto é desenvolver um sistema distribuído de descoberta de passwords. Existe um servidor que tem a capacidade de testar se as passwords que lhe são submetidas (usando HTTP Basic Authorization) estão corretas ou não. Durante este trabalho deve ser desenvolvida uma aplicação distribuída peer-to-peer de clientes desse servidor que vai tentar descobrir a password correta no menor tempo possível.



O servidor considera que um cliente que não acerta na password um certo número de vezes seguidas (este valor é aleatório) é mal comportado e passa-o ao estado BANNED. Para os clientes no estado BANNED no servidor, durante um certo tempo fixo (BANNED_TIME), todas as passwords submetidas serão reportadas como incorretas (mesmo que a password correta tenha sido tentada). Para evitar ficar BANNED ou para voltar ao estado inicial, os clientes podem limitar as interações com o servidor durante um certo tempo (COOLDOWN_TIME), ao fim do qual, podem novamente submeter passwords para teste sem risco de estar BANNED no servidor.

Os clientes devem ser executados em containers docker e no máximo podem existir 3 containers. O servidor não irá permitir mais de 3 ligações com IPs distintos, limitando assim a sua interação com os 3 containers docker.

Por sua vez, o servidor deve ser executado diretamente pelo host docker (que tem o endereço DNS host.docker.internal). O serviço está disponível no porto 8000/TCP do host e implementa o protocolo HTTP 1.1.

Requisitos

- Não devem recorrer a bibliotecas externas, apenas as bibliotecas standard do python são autorizadas
- Não podem utilizar mais do que 3 containers Docker

Objetivos

- Implementar o sistema distribuído peer-to-peer de clientes que comunicam entre si e com o servidor de forma a descobrir a password no menor tempo possível.
- Encontrar a password no menor tempo possível (implementações mais rápida/eficientes corresponderão a melhores notas)
- Para notas finais mais elevadas (>16), a solução deverá ser tolerante a falhas (do servidor e dos clientes)

Prazo

25 de junho de 2021
Entrega através do Github Classroom (automática)

GitHub Classroom

- Este projeto é realizado em **grupos de 2** alunos.
- Para resolver este projeto deverá começar por aceitar o mesmo em https://classroom.github.com/g/vpRRYOWy
- Ao aceitar o projeto será criado um repositório online a partir do qual deve fazer um clone local (no seu computador).

- Deverá enviar as suas alterações periodicamente para o repositório e manter-se atento ao canal *#cd* em https://detiuaveiro.slack.com

Referências

1. Basic access authentication, Wikipedia, https://en.wikipedia.org/wiki/Basic_access_authentication
2. https://docs.docker.com/get-started/overview/
3. https://www.ua.pt/pt/stic/dockers