Backdoor de 250 reais

Whoami

- Thiago Cunha – A.K.A Blu3B3@rd
- 29 anos
- Pai de 2 princesas
- Hobbies:
  - CTF (HTB - Cyb3rM0nstr0)
  - Vídeo Game
  - Bug Bounty
  - Ler Livros

Projeto

- Black Box
- Pentest Físico - Ter acesso a documentos que estavam na sala do presidente da empresa
- Pentest Lógico – Virar domain admin

Raspberry pi zero w

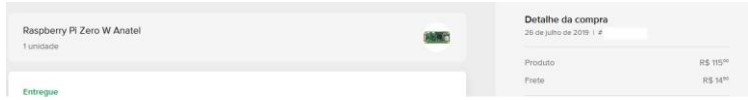
- Raspberry pi zero w
- Cron job para cliente do C2
- 64 Gb de memória – SD card
- Single-core 1 GHz
- 512 MB de RAM

Módulo Ethernet

- Conectores 5V GND
- HUB USB (pogo pin)
- 3 USB
- 1 Conector RJ45

$$?

- Raspberry pi zero w – R$ 115,00
- Case + placa adaptadora – R$ 88,57
- Ambiente cloud – R$ 0,00



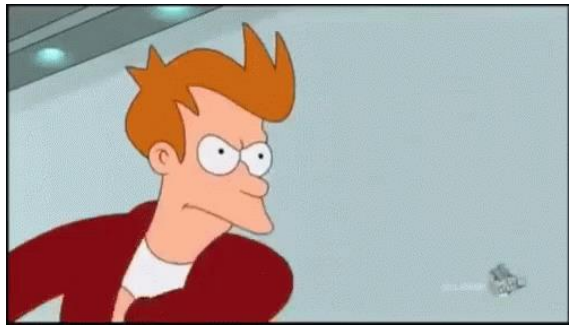
Oracle Cloud Infrastructure Free Tier

O Oracle Cloud Infrastructure Free Tier inclui uma avaliação promocional gratuita por tempo limitado que permite explorar uma ampla variedade de produtos Oracle Cloud Infrastructure e um conjunto de ofertas Always Free que nunca expiram.

Os recursos Free Tier e Always Free não estão disponíveis nas regiões do Cloud relativas ao setor governamental.

Avaliação Gratuita

A Avaliação Gratuita fornece $ 300 de créditos em nuvem válidos por até 30 dias. Você pode gastar esses créditos em qualquer serviço elegível do do Oracle Cloud Infrastructure.



Caldera – C2

- Baixo recurso computacional (Agent e Server)
- Skills já desenvolvidas
- Criação de novas Skills em Python

Link: https://caldera.readthedocs.io/en/latest/index.html

Teoria da escada

“Se você carregar uma escada entrará em qualquer lugar” – Steve Phillips

Link: https://www.reddit.com/r/videos/comments/cw4z7u/just_carry_a_ladder_and_enter_anywhere_for_free/

Vamos ao ataque

- 1º dia - Análise do ambiente físico
- 2º dia - invasão e by-pass da segurança física
- 3º dia – Coleta de credenciais e mapeamento das defesas da rede
- 4º dia – persistência e escalação de privilégio
- 5º dia – domain admin

1º dia

- Objetos analisados
  - Vestimenta das pessoas
  - Horários
  - Funcionários
  - Entradas e saídas do alvo
  - Controles de acesso

2º dia - Entrando no escritório

- Ponto de entrada – by pass
  - Manutenção – teoria da escada
- Entrada
  - Troca de roupa
  - Áreas menos movimentadas
  - Dispositivos conectados na rede
  - Implante colocado
  - Saída pelo estacionamento

Link: https://www.youtube.com/watch?v=NiEMcjSQOzg

3º dia

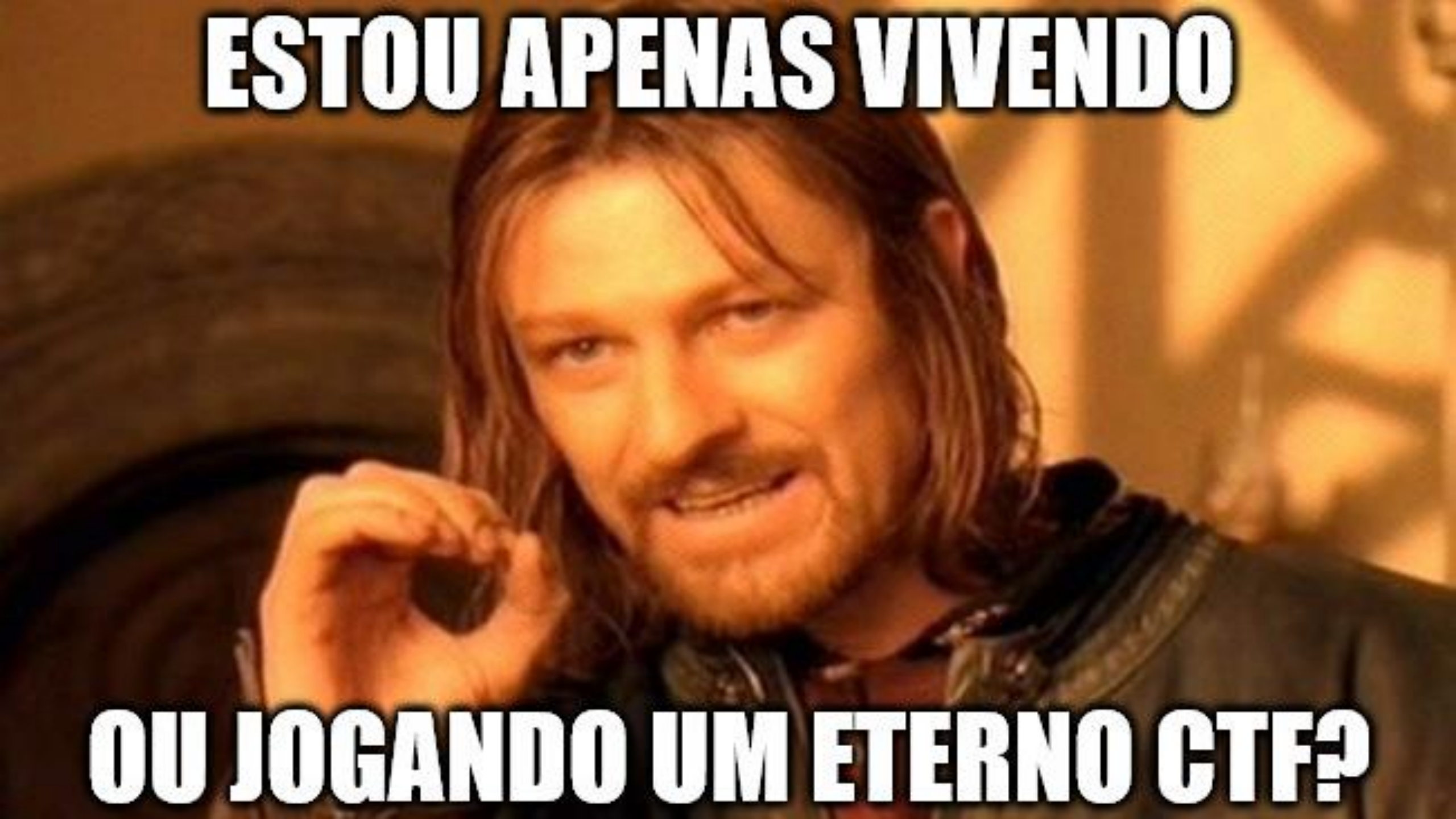
- Sniffing – WireShark
  - Credencial de sistema – HTTP
- Hping3
  - Windows 10
  - Linux - Apache
  - Windows Server 2012 R2 e 2016
- Responder
  - LLMNR e NBTNS
  - Hash NTLMv2
- Defesa
  - Firewall/Proxy

4º dia

- Acesso a máquinas
  - RDP
  - Instalação do cliente do C2
  - Persistência em processos do Windows
- Movimentação lateral
  - Reuso de credenciais coletadas
  - Descoberta do AD

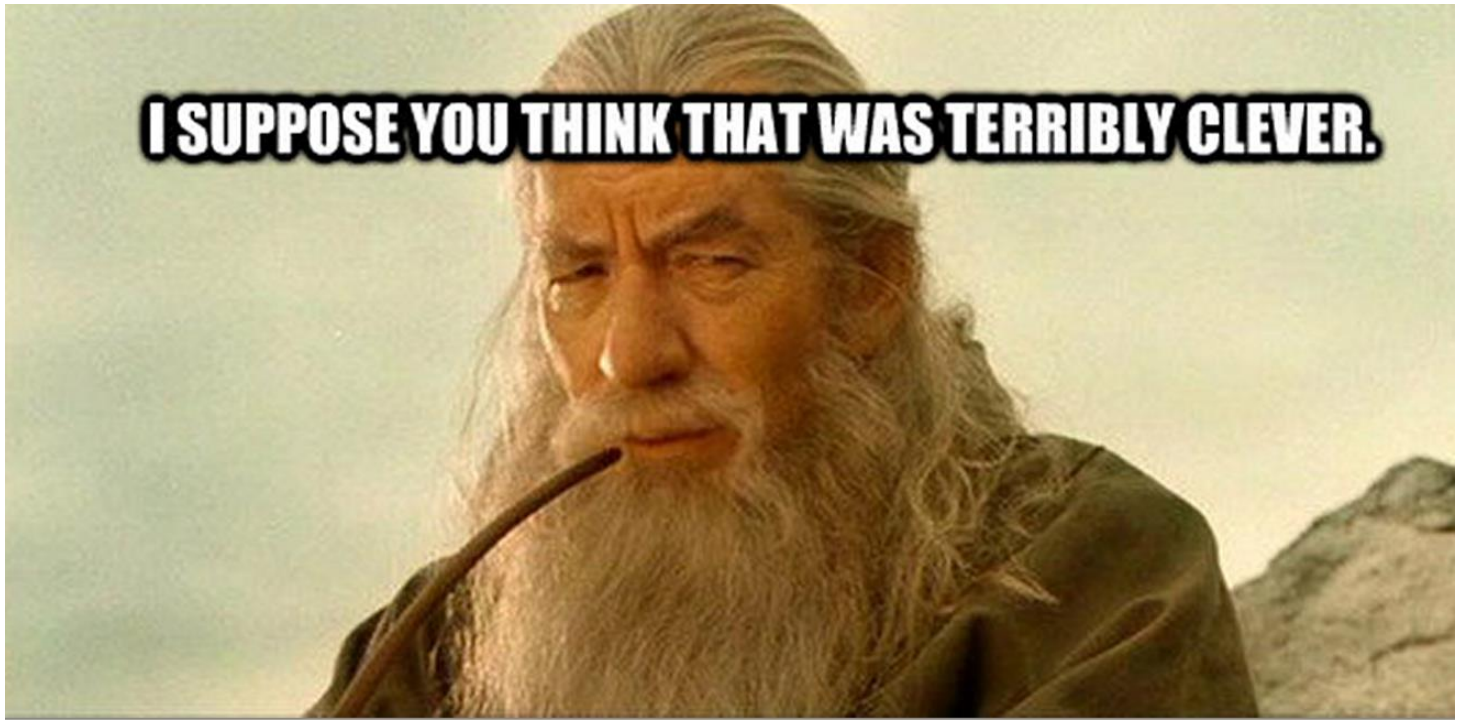
5º dia

- Tentativas de uso de ferramentas mais pesadas não funcionam
- Sem poder de fogo
- Nenhuma credencial válida coletada funciona
- Esperanças indo embora... Até que..
- Credencial HTTP funciona


ESTOU APENAS VIVENDO
OU JOGANDO UM ETERNO CTF?

5º dia

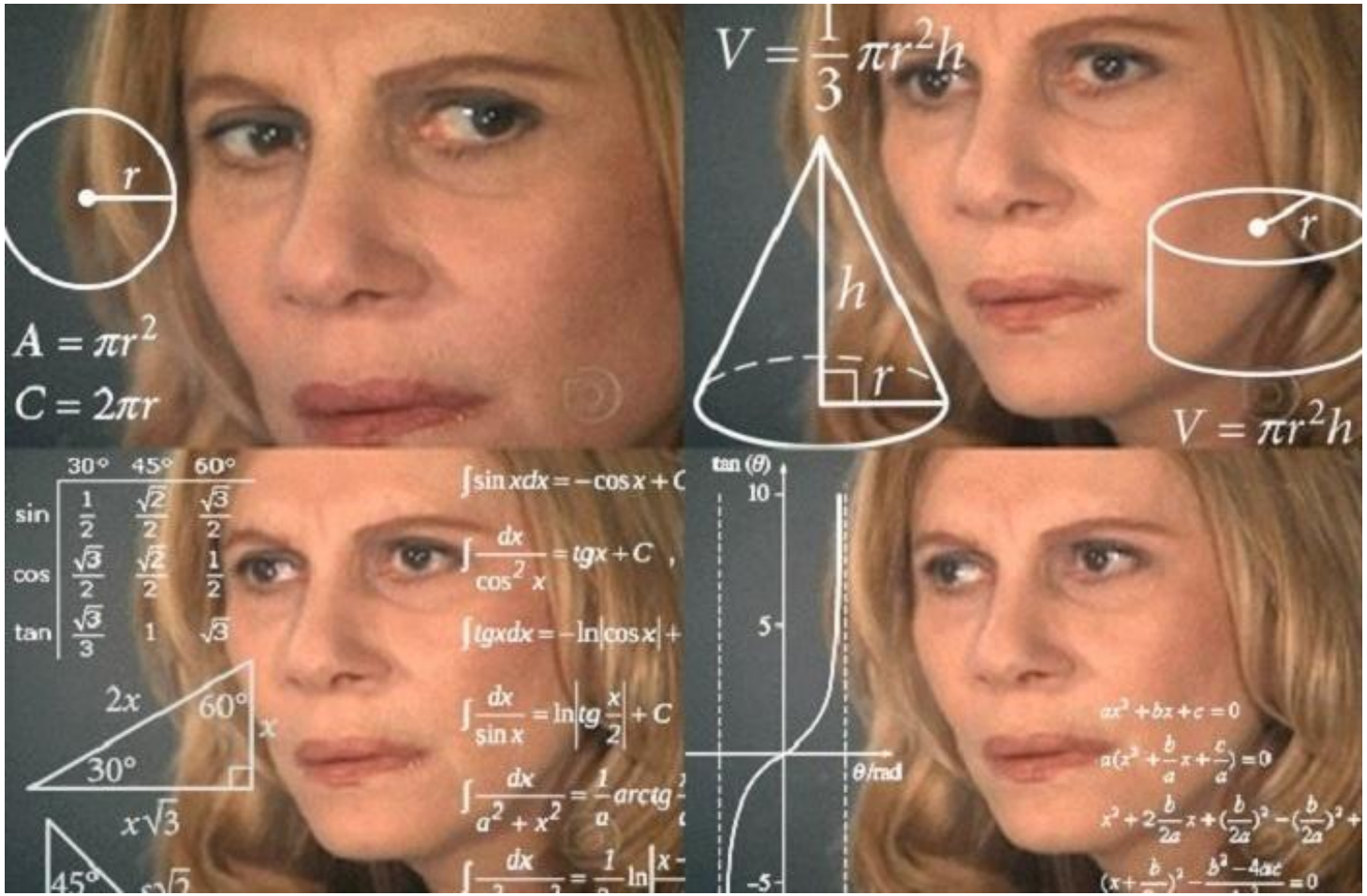
- Emergencia.txt
  - Usuário e senha de um domain admin
- Criado uma conta domain admin



Recomendações

- Desabilitar uso de LLMNR e NBTNS
- Configurar NAC
- Não salvar senhas em arquivos de texto
- Utilizar Soluções de inspeção de rede (IPS, AntiAPT, IDS, XDR)
- Antivírus de boa qualidade

Duvidas?


r
$A = \pi r^2$
$C = 2\pi r$
$V = \frac{1}{3}\pi r^2 h$
h
r
r
$V = \pi r^2 h$
30° 45° 60°
sin
cos
tan
2x
60°
30°
x
$x\sqrt{3}$
45°
$\int \sin x dx = -\cos x + C$
$\int \frac{dx}{\cos^2 x} = tgx + C$
$\int tgx dx = -\ln|\cos x| +$
$\int \frac{dx}{\sin x} = \ln\left|tg\frac{x}{2}\right| + C$
$\int \frac{dx}{a^2 + x^2} = \frac{1}{a} arctg$
tan (θ)
10
5
-5
θ/rad
$ax^2 + bx + c = 0$
$a(x^2 + \frac{b}{a}x + \frac{c}{a}) = 0$
$x^2 + 2\frac{b}{2a}x + (\frac{b}{2a})^2 - (\frac{b}{2a})^2 +$
$(x + \frac{b}{a})^2 - \frac{b^2 - 4ac}{} = 0$

Obrigado!

- LinkedIn: thiagocunhasilva
- Github: Blu3B3ard
- Instagram: blu.ebeard