

Hacking DevOps Ecosystems: Container Registries

Dr. Victor Pasknel
Morphus Labs



Victor Pasknel

- Doutor em Informática Aplicada @ Unifor
- Pentester / Red Team @ Morphus (~12 anos)
- Pesquisador @ MorphusLabs
- Professor Universitário
- Baterista @ Omminous
- Medium: @pasknel
- Palestrante:
 - H2HC / BSides SP / NullByte
 - BWCON / JampaSec / CAJUsec
 - Python Brasil / Python Nordeste
 - Roadsec / MindTheSec (SP & RJ)



Agenda

1. Motivação
2. Container Registries
3. Registry API
4. In the Wild



Motivação

- Pentest (**<=2018**)
 - Foco em infraestrutura tradicional
 - Active Directory (AD)
 - Bancos de dados
 - SAP
 - Mainframes
 - Etc...

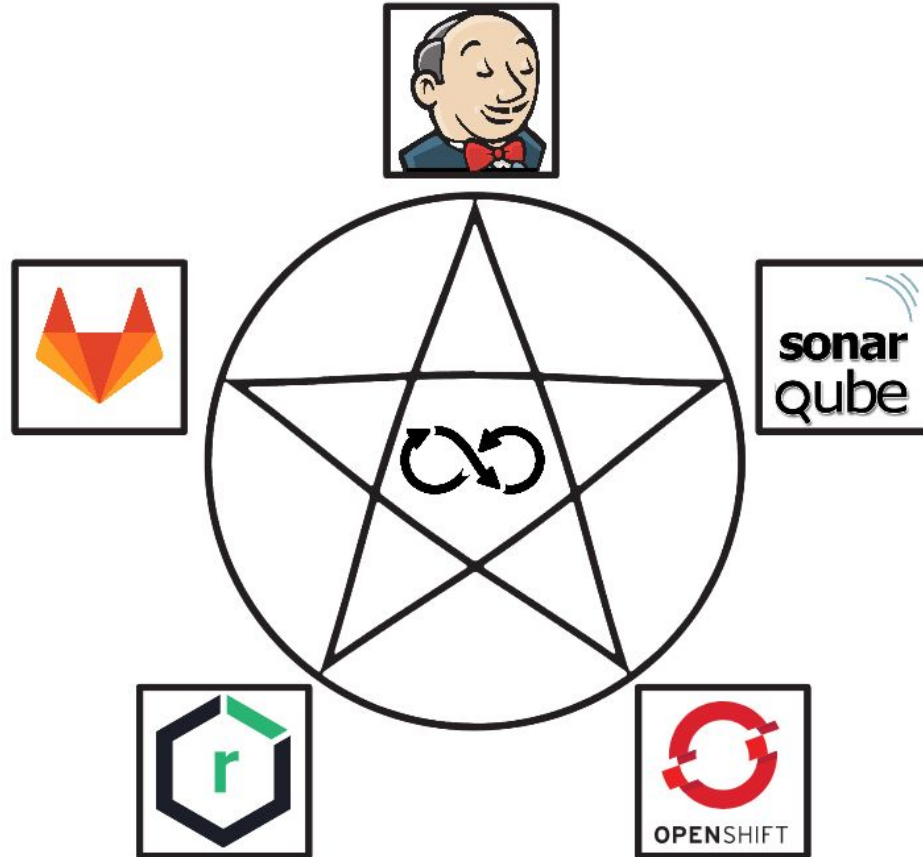


Motivação

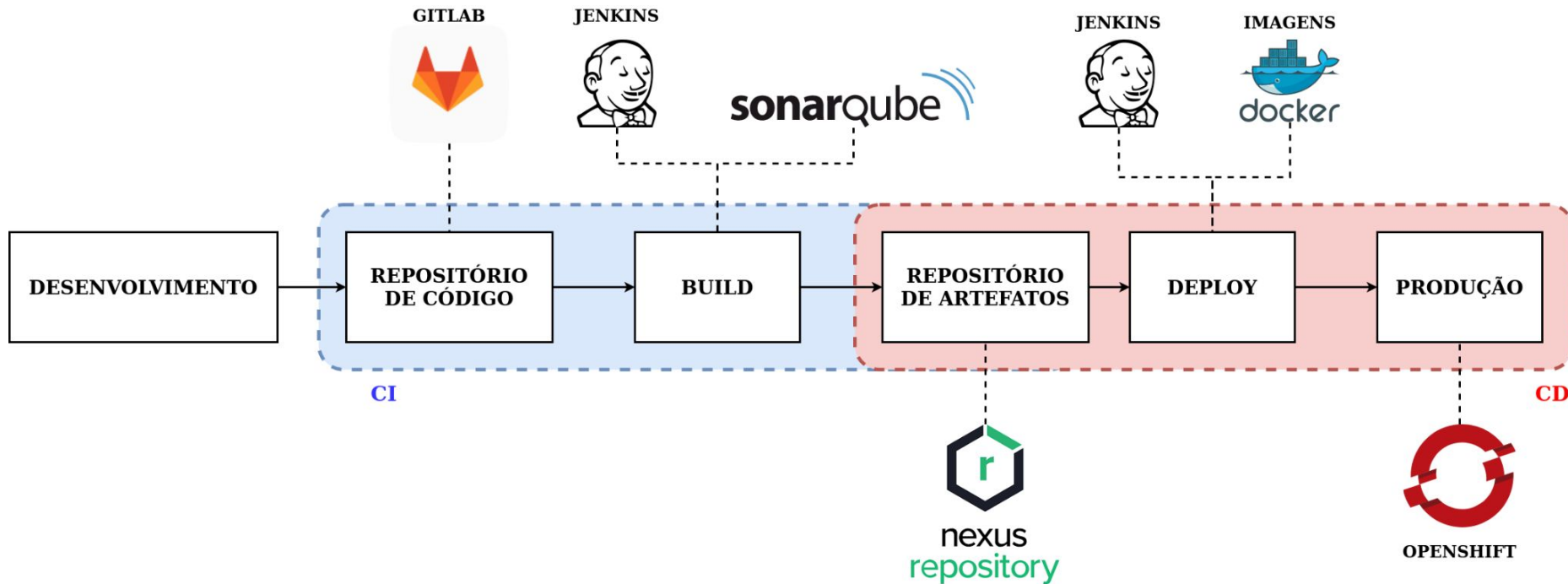
- Pentest Atual (**>= 2019**)
 - Novos pontos de ouro
 - Cloud
 - AWS
 - GCP
 - Azure



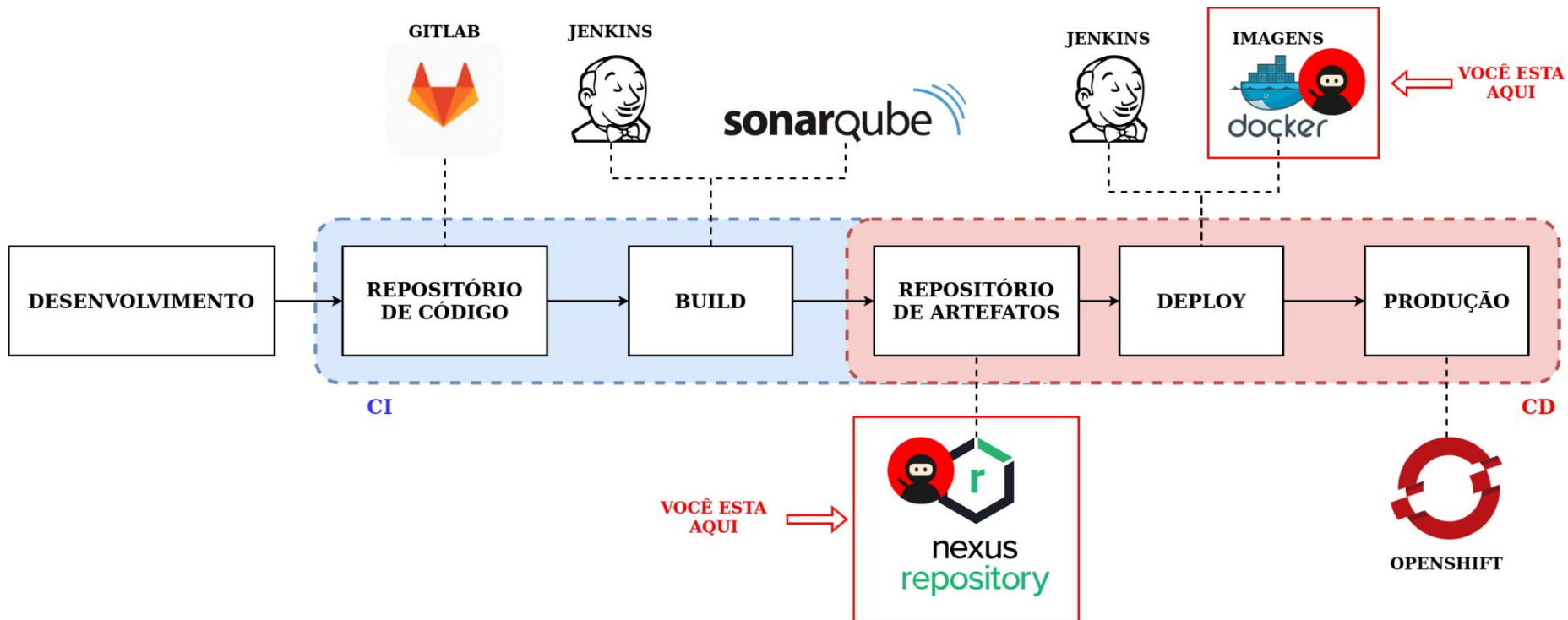
DevOps Pentagram



Ecosistema DevOps



Ecosistema DevOps



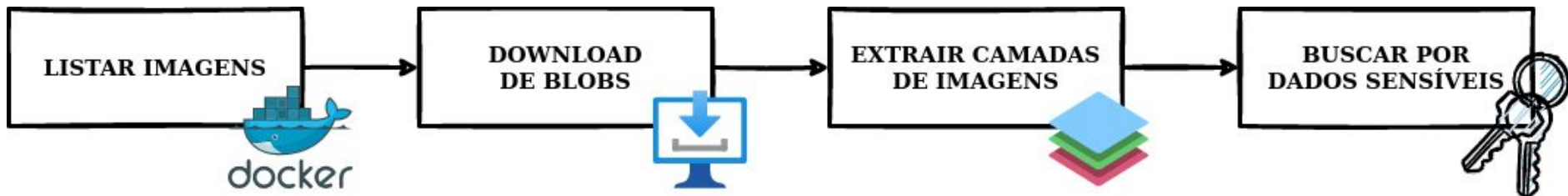
Container Registries

- Armazenamento de imagens de containers
- Alternativa para registros em cloud (Docker Hub)
- Acessível através de API Rest
- Porta padrão: 5000/TCP
- Exemplos:
 - Docker Registry
 - Sonatype Nexus
 - JFrog



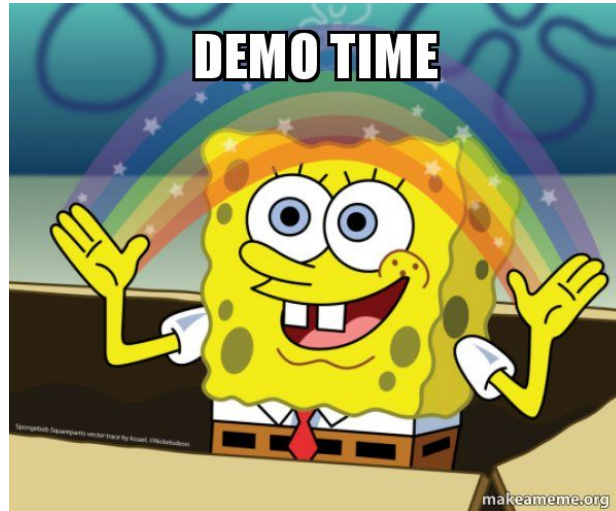
Container Registries

- Metodologia de ataque



Container Registries

- Metodologia de ataque:



Container Registries

- Experiências vividas:
 - Ambientes On-premise:
 - Nexus (~70%)
 - A maioria das vezes sem autenticação para **leitura**!
 - Podemos listar e baixar conteúdo de imagens!
 - Utilizado como repositório de artefatos e registro de imagens de containers.
 - Credencial de acesso geralmente é encontrada em Gitlab / Jenkins.
 - Outros (~30%)
 - JFrog & Docker Registry
 - Ambientes Cloud:
 - ECR
 - GCR




In The Wild

- Shodan:
 - Encontrando registries expostos na internet
 - Pesquisa:
 - *port:5000 docker registry*



In The Wild


 SHODAN

Explore

Downloads

Pricing [↗](#)


port:5000 docker registry



TOTAL RESULTS


5,096


TOP COUNTRIES



United States	1,360
China	967
Germany	707
France	233
Ireland	157

[More...](#)


 View Report

 View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

64.227.106.179 [↗](#)

[DigitalOcean, LLC](#)

 United States, Santa Clara


cloud

HTTP/1.1 200 OK
Cache-Control: no-cache
Date: Thu, 01 Sep 2022 10:41:57 GMT
Content-Length: 0

Docker Registry HTTP API:
Error: UNAUTHORIZED

159.223.29.105 [↗](#)

[DigitalOcean, LLC](#)

 United States, New York City

cloud

HTTP/1.1 200 OK
Cache-Control: no-cache
Date: Thu, 01 Sep 2022 10:39:18 GMT
Content-Length: 0

Conclusões

- Novas oportunidades de ataques em ecossistemas DevOps
 - O caminho mais rápido de comprometer a Cloud é através do DevOps!
 - As joias da coroa estão atualmente no DevOps
 - Uso de APIs oficiais para realizar ataques
- Muitos profissionais de segurança ainda não “acordaram” para DevOps
- Total falta de monitoramento em ambientes de DevOps

