HACKPROVE

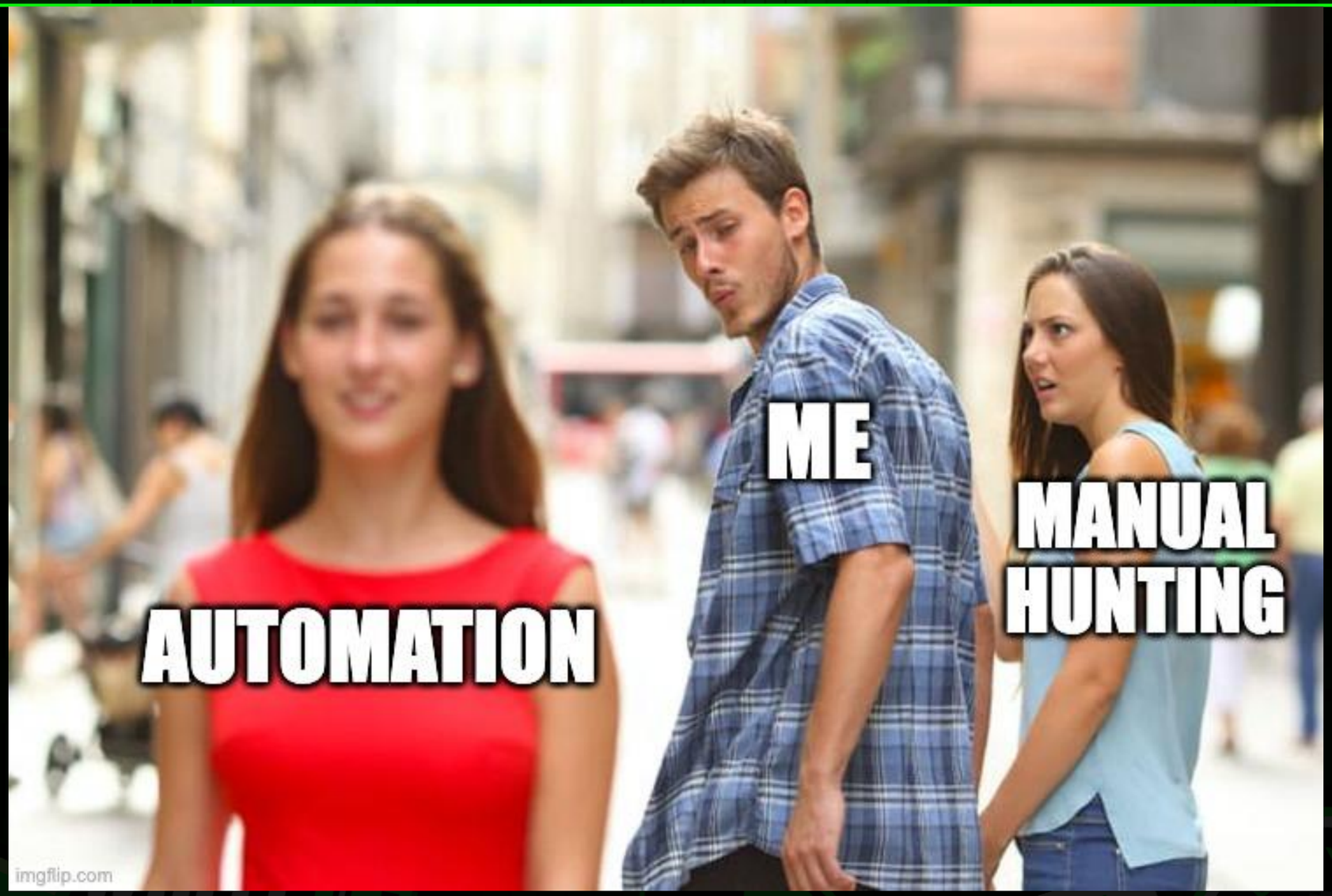
2025 HACKPROVE WORLD

Bug Bounty at Scale Through Automation

2025/01/11 Abiral Shrestha

$ whoami

- Abiral Shrestha (@proabiral)
- Kathmandu, Nepal
- Cofounder ThreatNix / Threat CON
- 7 years of Bug bounty experience
- Top 25 Hackerone - all time.


ME
AUTOMATION
MANUAL HUNTING
imgflip.com

Importance of automation workflow for Bug bounty

Importance of subdomain enumeration

Passive Subdomain Enumeration

- Amass
- Subfinder

Example : CVE-2019-9670

```
+-----------------------+----------------------+-----------+
| subdomain             | insertedDate         | source    |
+-----------------------+----------------------+-----------+
| zimbra-[redacted]     | 2024-11-08 16:58:59 | subfinder |
+-----------------------+----------------------+-----------+
```

Synacor Zimbra Collaboration <8.7.11p10 - XML External Entity Injection,critical:CVE-2019-9670:https://zimbra-[redacted]/Autodiscover/Autodiscover.xml

5:31 PM

```
<html>
    <head>
        <title>
            JSP Command Execution
        </title>
    </head>
    <body>
        <pre>
            <cmd_output>
                uid=999(zimbra) gid=999(zimbra)
                groups=999(zimbra),0(root)
                zimbra
                /opt/zimbra/log
            </cmd_output>
        </pre>
    </body>
</html>
```

```
<cmd_output>
    {
    "Code" : "Success",
    "LastUpdated" : "2024-11-11T05:58:12Z",
    "Type" : "AWS-HMAC",
    "AccessKeyId" : "A
    "SecretAccessKey"
    "Token" :
```

Notes

[redacted] awarded a bounty of $[redacted],000 for zimbra-[redacted] - Remote Code Execution via XXE CVE-2019-9670 (#2[redacted]).

Example : Exposed Heap Dump

subdomain	insertedDate	source
pricing-api-[redacted]	2024-10-30 01:43:20	amass

Spring Boot Actuator - Heap Dump Detection,critical:springboot-heapdump:https://pricing-api-[redacted]/actuator/heapdump

2:04 AM

HACKPROVE

2025 HACKPROVE WORLD

```
                                                                                                                  `#  200!  x    0     l P!         A   8  8
?@
  !     !  Q     "     bX  8!  8  h ,  `  x  ~ 3!  `  x) !     !     !     ">0 j?h  QX!             !       @A       ?@
                                                                                                                  "     bX  #
  p[8b3899de-19128] Mapped to Actuator web endpoint 'heapdump'.health.SystemHealth@7cd09fe]nported [application/vnd.spring-boot.ac
tuator.v3+json, application/vnd.spring-boot.actuator.v2+json, application/json]ibe.[redacted], X-Amzn-Trace-Id:"Root=1-6722584
[redacted] accept:"application/json", authorization:"Bearer eyJraWQiO[redacted], Sec-WebSocket-Proto
col:"graphql-ws"]"] for HTTP GET /subscriptionsthIndicator matched:
      - @ConditionalOnMissingBean (names: readinessStateHealthIndicator; SearchStrategy: all) did not find any beans (OnBeanCondit
ion)
--
```

[redacted] rewarded proabiral with a [redacted] bounty and [redacted] bonus.

Thank you!

Looking forward for more submissions,

Active Enumeration

- Subdomain Bruteforcing
  - https://github.com/d3mondev/puredns

```
~# cat /tmp/wordlist.txt
admin
github
test
dev
stage
kibana
www
```

```
admin.example.com
github.example.com
test.example.com
dev.example.com
stage.example.com
kibana.example.com
www.example.com
```

```
% puredns bruteforce /tmp/wordlist.txt example.com -r /tmp/resolvers.txt
```

Resolvers

Need Good resolvers that :

- Responds with correct DNS answers
- Responds NXDOMAIN for non existing domain

https://github.com/vortexau/dnsvalidator

https://github.com/proabiral/Fresh-Resolvers

Wordlists

- https://wordlists.assetnote.io/
- https://github.com/danielmiessler/SecLists/tree/master/Discovery/DNS
- https://github.com/trickest/wordlists/tree/main/inventory

Custom wordlist

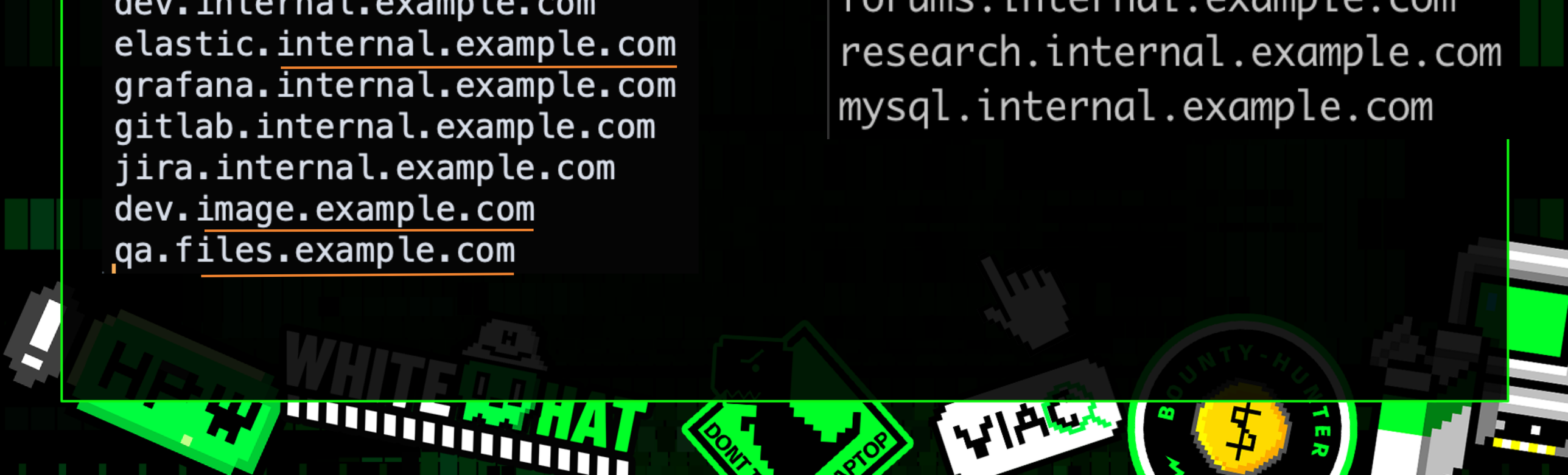
- From your existing subdomain
- https://www.merklemap.com/dns-records-database

  https://github.com/proabiral/wordlist

Subdomain Brute Force

```
aws.staging.example.com
s3.staging.example.com
elb.staging.example.com
upload.staging.example.com
github.internal.example.com
dev.internal.example.com
elastic.internal.example.com
grafana.internal.example.com
gitlab.internal.example.com
jira.internal.example.com
dev.image.example.com
qa.files.example.com
```

```
azure.staging.example.com
images.staging.example.com
stats.staging.example.com
forums.internal.example.com
research.internal.example.com
mysql.internal.example.com
```



https://github.com/trickest/dsieve

```
foobar@foobars-MacBook-Pro ~ % sort -u /tmp/domain.txt | dsieve -f 3 -top 2
internal.example.com
staging.example.com
```

Bruting

```
foobar@foobars-MacBook-Pro pattern_matching % cat domain.txt
internal-grafana-stg-1.example.com
internal-gitlab-stg-1.example.com
internal-node-stg-1.example.com
dev.bitbucket.example.com
dev.jira.example.com
dev.elastic.example.com
dev.jira-1-internal.example.com
dev.devops-1-internal.example.com
```

https://github.com/proabiral/patternalyzer

```
foobar@foobars-MacBook-Pro ~ % patternalyzer domain.txt
dev.{replace_this}-1-internal.example.com
internal-{replace_this}-stg-1.example.com
dev.{replace_this}.example.com
```

```
internal-docker-stg-1.example.com
internal-github-stg-1.example.com
internal-splunk-stg-1.example.com
dev.zabbix-1-internal.example.com
dev.kibana-1-internal.example.com
```

Results


DVWA
Vulnerability: Command Injection
Ping a device
Enter an IP address:
Submit
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data

Subdomain takeover at [redacted]com

[redacted] In progress · Submitted 18[redacted]st activity 4 days ago

[redacted]

10 points

P3 Unresolved

Comment 1

Stats :
6000+ number of new subdomains founds with this

Permute

```
admin.example.com          -> dev.admin.example.com, admin.dev.example.com, devadmin.example.com,
                              dev-admin.example.com, admindev.example.com, admin-dev.example.com
storage01.example.com       -> storage02.example.com, storage03.example.com
dev.admin.example.com   -> otherword.admin.example.com, anotherword.admin.example.com
```

- Ripgen / gotator / goaltdns
- Regulator

subdomain	insertedDate	source
grafana.	2023-04-14 06:09:36	ripgen_nowordlist

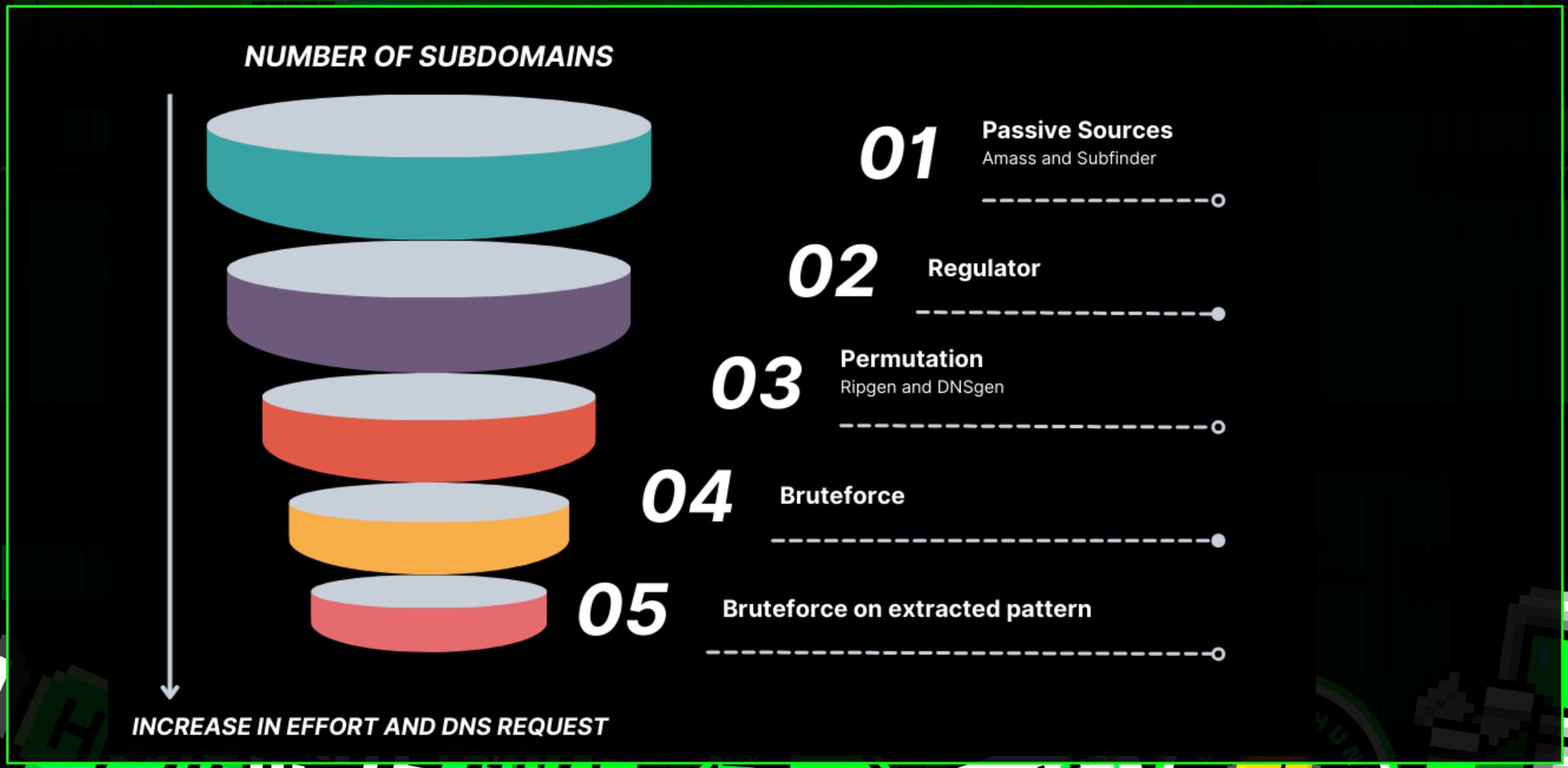
high:grafana-default-login:https://grafana.

6:52 AM

rewarded you with a bounty of $,000 for SSRF (AWS Creds leakage) via Default Grafana login - grafana you're as excited as we are, go ahead and tweet about it!

HACKPROVE

2025 HACKPROVE WORLD




WILDCARDS
WILDCARD EVERYWHERE
imgflip.com

Wildcards

```
foobar@foobars-MacBook-Pro ~ % host doesnotexists.messenger.com
doesnotexists.messenger.com is an alias for star.facebook.com.
star.facebook.com is an alias for star.c10r.facebook.com.
star.c10r.facebook.com has address 163.70.146.23
```

Wildcards on domain with resolvers in China:

https://www.assetnote.io/resources/research/insecurity-through-censorship-vulnerabilities-caused-by-the-great-firewall

https://www.usenix.org/system/files/sec21-hoang.pdf

https://recon-royale.com/

@pxmme1337

RECON ROYALE 👑

"HEAVY IS THE HEAD THAT WEARS THE CROWN."

⚔ Go To War! ⚔

Submit your subdomains

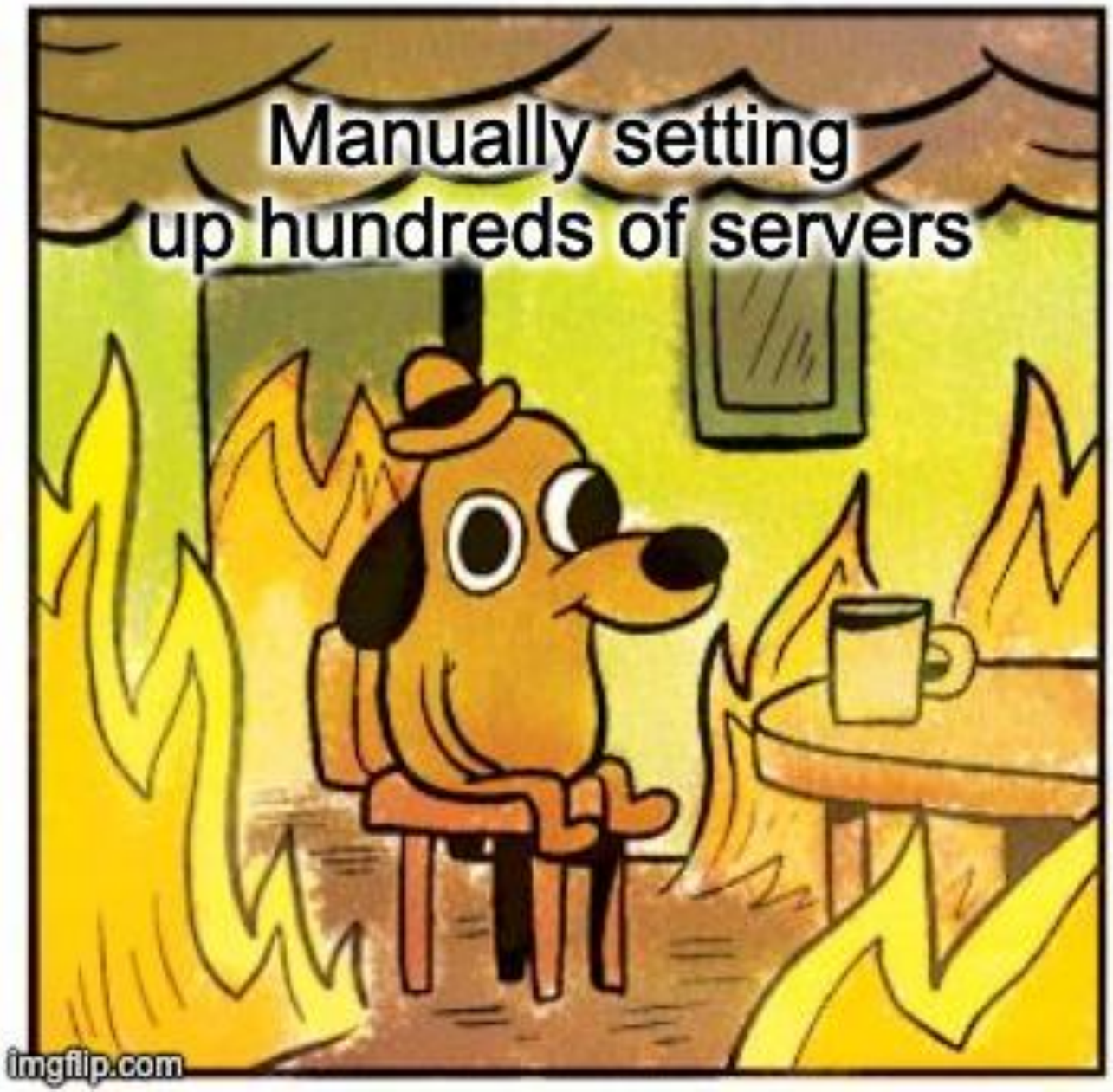
🎯 *Current Target* 🎯

handmade.com

Time until next round: 11:49:28

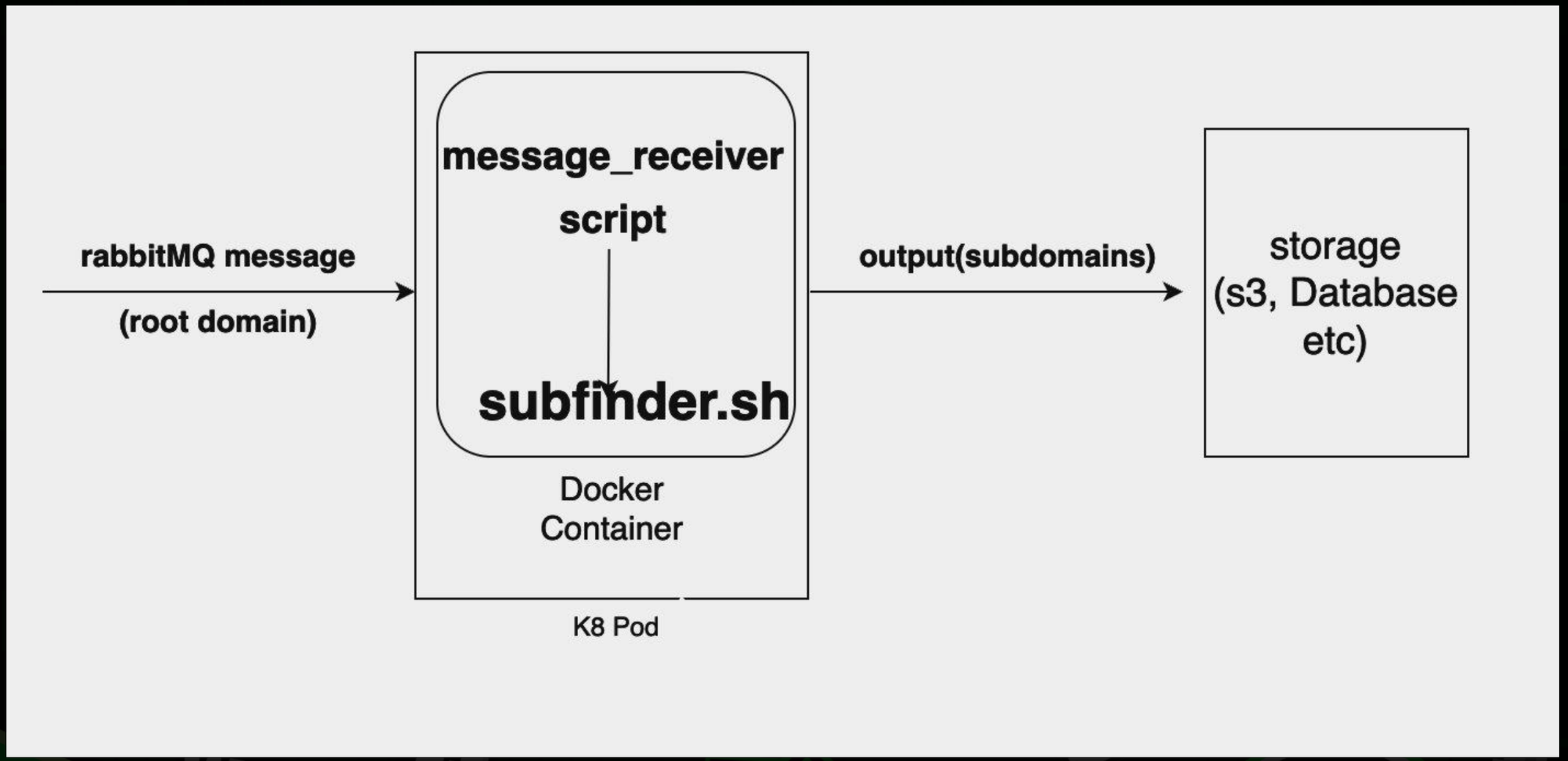
Scaling

- Setting up and maintaining multiple servers is time-consuming and inefficient.
- Becomes unmanageable at scale (e.g., beyond 5 servers).
- Difficulties in:
  - Coordinating outputs from multiple servers.
  - Distributing domains to scan across the servers.



Scaling

- Existing solutions (Axiom / Fleex / ShadowClone)
- Problems I faced with them –
  - Not suitable for long running task
  - No retry on failure
  - Charges are higher if you run them continuously


rabbitMQ message
(root domain)
message_receiver
script
subfinder.sh
Docker
Container
K8 Pod
output(subdomains)
storage
(s3, Database
etc)

```
### Building golang scripts on golang image
FROM golang AS builder
WORKDIR /project

### subfinder building
RUN go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest

## building my scripts
RUN GO111MODULE=off go get github.com/rabbitmq/amqp091-go
RUN GO111MODULE=off go get github.com/go-sql-driver/mysql
COPY ../images_helper_files/*.go /project/
RUN for i in *.go; do GO111MODULE=off go build $i; done

## copying to smaller debian image
FROM debian:stable-slim

WORKDIR /project

COPY --from=builder /go/bin/subfinder /usr/local/bin/
COPY --from=builder /project/insert2DB .
COPY --from=builder /project/rabbitmq_receive .
COPY subfinder/main.sh .


CMD ["./rabbitmq_receive","-queue","subfinder"]
```

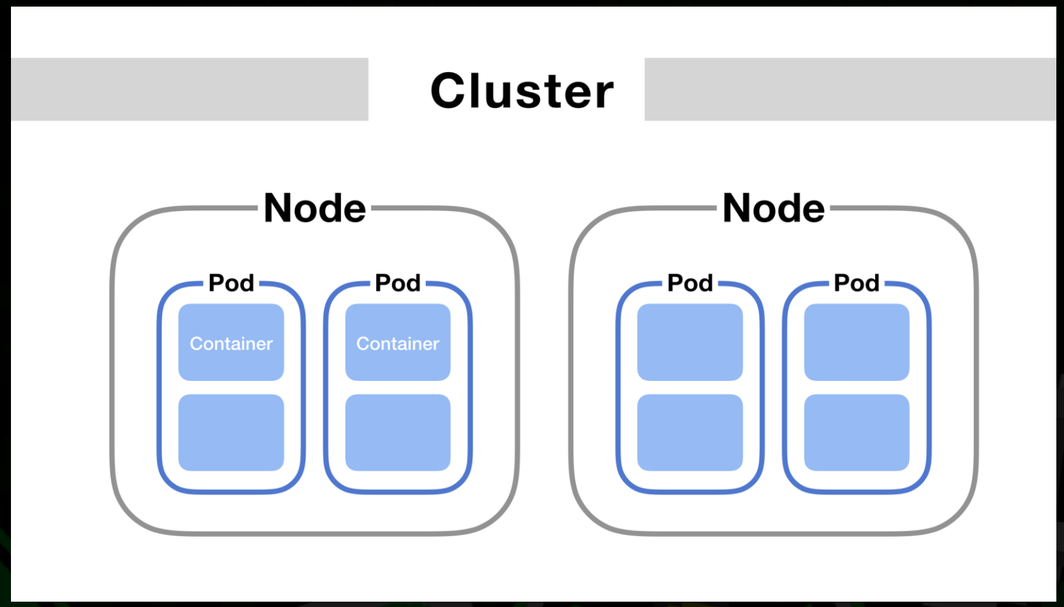
Kubernetes

- Container orchestration tools
- Easy Scaling / Replication
- Auto heal

Kubernetes – key concepts

Pod: The smallest deployable unit; a group of containers.

Node: A machine (VM or physical) that runs Pods.



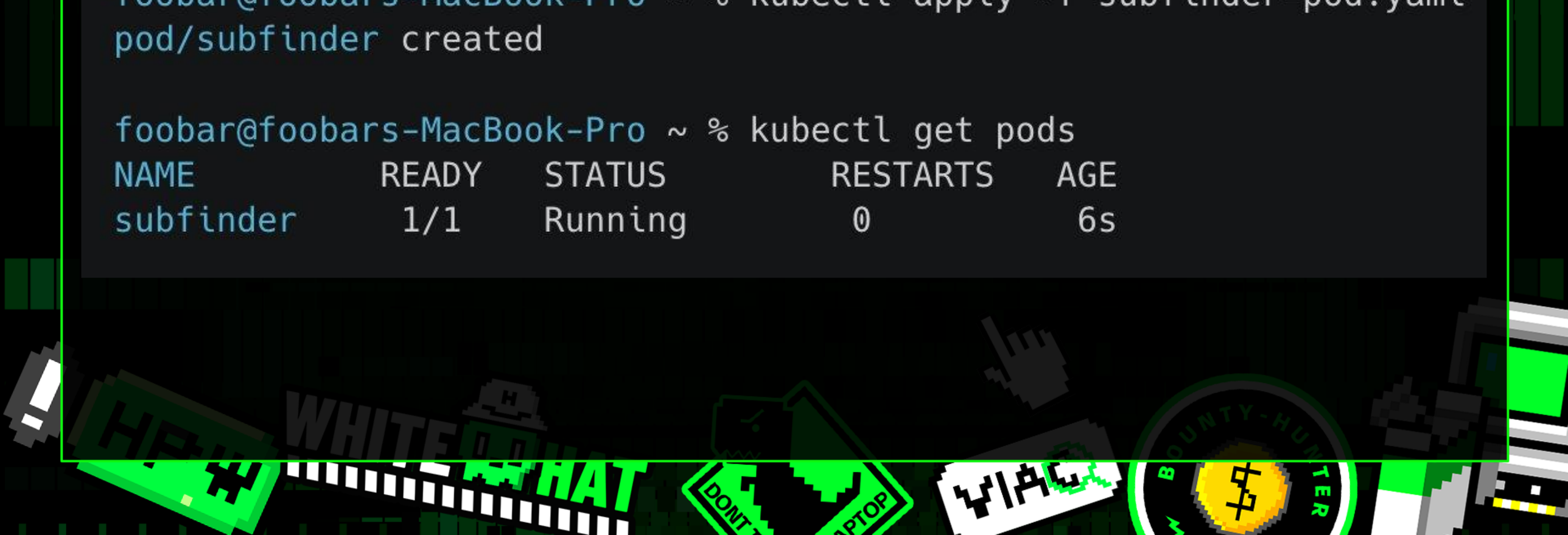
Kubernetes

YAML Files for pods definition :

```
foobar@foobars-MacBook-Pro /tmp % cat subfinder_pod.yaml
apiVersion: v1
kind: Pod
metadata:
  name: subfinder-pod
  labels:
    name: subfinder
spec:
  containers:
  - name: subfinder-container
    image: rg.fr-par.scw.cloud/[redacted]/subfinder:latest
```

```
foobar@foobars-MacBook-Pro ~ % kubectl apply -f subfinder-pod.yaml
pod/subfinder created

foobar@foobars-MacBook-Pro ~ % kubectl get pods
NAME          READY   STATUS    RESTARTS   AGE
subfinder     1/1     Running   0          6s
```



Deployment

```
foobar@foobars-MacBook-Pro tmp % cat subfinder-deployments.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: subfinder-deployment
  labels:
    type: subfinder
spec:
  replicas: 5
  selector:
    matchLabels:
      type: subfinder
  template:
    metadata:
      name: subfinder-pod
      labels:
        type: subfinder
    spec:
      containers:
      - name: subfinder-container
        image: rg.fr-par.scw.cloud/[redacted]/subfinder:latest
```

```
foobar@foobars-MacBook-Pro ~ % kubectl apply -f subfinder_deployment.yaml
deployment.apps/subfinder-deployment configured

foobar@foobars-MacBook-Pro ~ % kubectl get nodes | grep -i subfinder
NAME                             READY       UP-TO-DATE   AVAILABLE       AGE
subfinder-deployment             50/50         50             50            10m
```

Anti - Affinity

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: subfinder-deployment
  labels:
    type: subfinder
spec:
  replicas: 5
  selector:
    matchLabels:
      type: subfinder
  template:
    metadata:
      name: subfinder-pod
      labels:
        type: subfinder
    spec:
      podAntiAffinity:
        requiredDuringSchedulingIgnoredDuringExecution:
          - labelSelector:
              matchExpressions:
                - key: type
                  operator: In
                  values:
                    - "subfinder"
            topologyKey: kubernetes.io/hostname
      containers:
      - name: subfinder-container
        image: rg.fr-par.scw.cloud/[redacted]subfinder:latest
```

Anti - Affinity

```
spec:
    podAntiAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        - labelSelector:
            matchExpressions:
              - key: type
                operator: In
                values:
                  - "subfinder"
          topologyKey: kubernetes.io/hostname
```

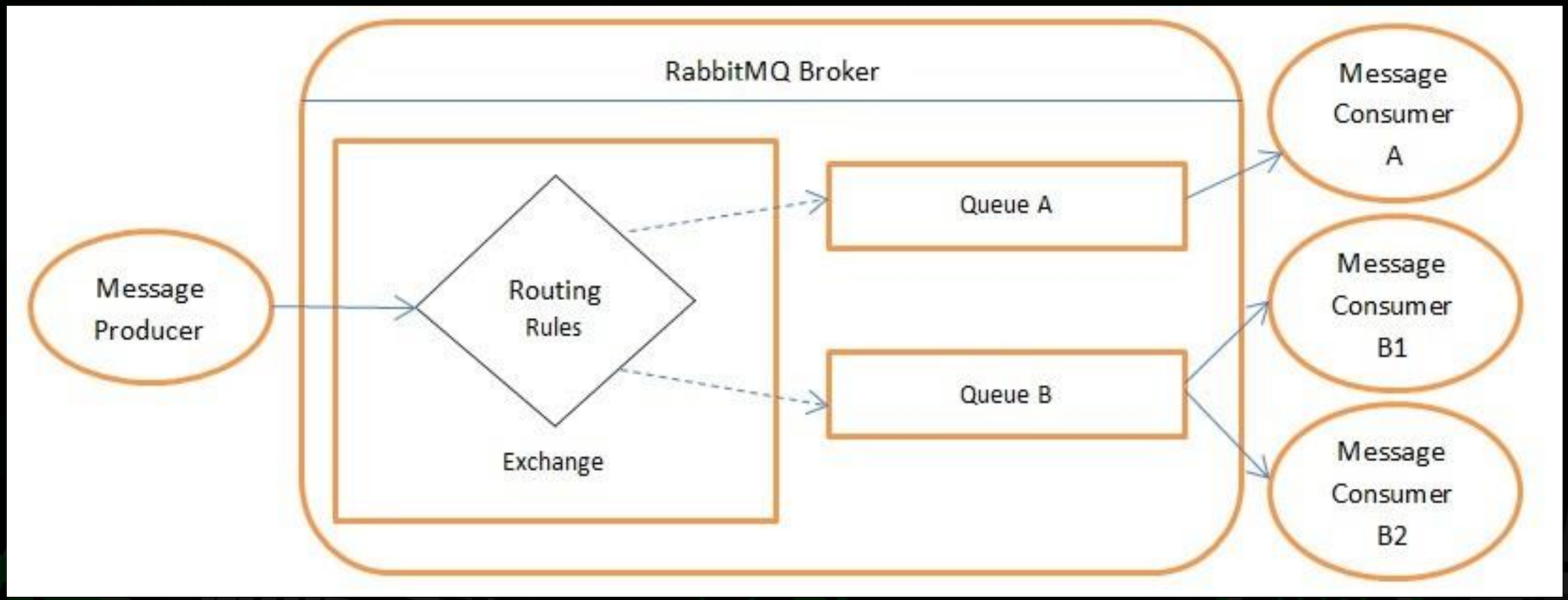
Problem

Race Conditions: Multiple pods pulling the same task simultaneously.

Error Handling: No easy way to retry or reassign failed tasks.

Task Queue Management: Difficulty in tracking which tasks are processed.

RabbitMQ


RabbitMQ Broker
Message Producer
Routing Rules
Exchange
Queue A
Queue B
Message Consumer A
Message Consumer B1
Message Consumer B2

RabbitMQ

- Avoids Race Conditions:
- Handles Failures Gracefully
- Distributes Tasks
- Prioritizes Messages

Shoutout

@infosec_au

@trick3st

@assetnote

@nbk_2000

@Jhaddix

@G0LDEN_infosec

@seanyeoh

@pdiscoveryio

@pdnuclei

And more

HACKPROVE

2025 HACKPROVE WORLD

THANK YOU

@proabiral