

BoB 13th

Track training assignments

glue_privesc Interim Report



CLASS	Cloud DFIR class I
Mentor	NIKO
Submission Date	2024년 08월 13일
track/name /phone(last 4 digits)	digitalforenisc/YeomSeungvin /6827

Table of Contents

1.Setting Up Analysis Environment	3
2. Future Action Items	5

1. Setting Up Analysis Environment

First, I install every tools about this class.

```
sudo snap install curl
curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o
"awscliv2.zip"
unzip awscliv2.zip
sudo ./aws/install
Download CloudGoat
sudo apt install git
git clone https://github.com/RhinoSecurityLabs/cloudgoat.git
Install terraform
sudo apt-get update && sudo apt-get install -y gnupg
software-properties-common
wget -O- https://apt.releases.hashicorp.com/gpg | \
gpg --dearmor | \
sudo tee /usr/share/keyrings/hashicorp-archive-keyring.gpg > /dev/null
gpg --no-default-keyring \
--keyring /usr/share/keyrings/hashicorp-archive-keyring.gpg \
--fingerprint
echo "deb [signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg] \
https://apt.releases.hashicorp.com $(lsb_release -cs) main" | \
sudo tee /etc/apt/sources.list.d/hashicorp.list
sudo apt update
sudo apt-get install terraform
Check on progress https://forms.gle/vTdwgNNU36KawECG6
Break until 4.30pm KST
Fill the form and finish the above setup.
Prepare python environment
sudo apt install python3.12-venv
```

I installed the tools by referring to this photo.

```
n0rellfe@B00K-09A7VOM8LQ:/mnt/c/Users/n0rel/OneDrive/aws_cli/cloudgoat-master$ ./cloudgoat.py create glue_privesc
Using default profile "BOB_Class" from config.yml...
Loading whitelist.txt...
A whitelist.txt file was found that contains at least one valid IP address or range.

*****
Updating previously deployed glue_privesc scenario.

To recreate this scenario from scratch instead, run `./cloudgoat destroy glue_privesc` first.
*****

Now running glue_privesc's start.sh...
./cloudgoat already exists.
Overwrite (y/n)? y
Initializing the backend...
Initializing provider plugins...
```

So, I create aws instance about glue_privesc

Many errors occurred, including permission errors, database connection errors, configuration errors, and database version errors, among others.

First, permission error, there were many errors related to the AWS user, so I added the following permission

권한 정책 (10)			
사용자에게 직접 연결된 정책을 통해 또는 그룹을 통해 권한을 정의합니다.			
검색		필터링 기준 유형	
		모든 유형	
<input type="checkbox"/>	정책 이름	유형	연결 방식
<input type="checkbox"/>	AmazonEC2FullAccess	AWS 관리형	직접
<input type="checkbox"/>	AmazonRDSDataFullAccess	AWS 관리형	직접
<input type="checkbox"/>	AmazonRDSFullAccess	AWS 관리형	직접
<input type="checkbox"/>	AmazonS3FullAccess	AWS 관리형	직접
<input type="checkbox"/>	AmazonSSMFullAccess	AWS 관리형	직접
<input type="checkbox"/>	AWSGlueConsoleFullAccess	AWS 관리형	직접
<input type="checkbox"/>	AWSGlueServiceRole	AWS 관리형	직접
<input type="checkbox"/>	AWSLambda_FullAccess	AWS 관리형	직접
<input type="checkbox"/>	IAMFullAccess	AWS 관리형	직접
<input type="checkbox"/>	IAMUserChangePassword	AWS 관리형	직접

Second, DB version error, Additionally, the default database version was Postgres 13, but since it was not supported, I changed it to Postgres 16.

Config file's path is 'cloudgoat/scenarios/glue_privesc/terraform/rds.tf'

```
n0rellife@B00K-09A7VOM8LQ:/mnt/c/Users/n0rel/OneDrive/cloudgoat$ cat scenarios/glue_privesc/terraform/rds.tf
resource "aws_db_instance" "cg-rds" {
  allocated_storage = 20
  storage_type      = "gp2"
  engine            = "postgres"
  engine_version    = "16.3"
  instance_class    = "db.t3.micro"
  db_subnet_group_name = aws_db_subnet_group.cg-rds-subnet-group.id
  db_name           = var.rds-database-name
  username          = var.rds-username
  password          = var.rds-password
  parameter_group_name = "default.postgres16"
  publicly_accessible = false
  skip_final_snapshot = true

  port = "5432"
}
```

So, I get ip and port

```
Apply complete! Resources: 59 added, 0 changed, 0 destroyed.

Outputs:
cg_web_site_ip = "190.158"
cg_web_site_port = 5000

[cloudgoat] terraform apply completed with no error code.

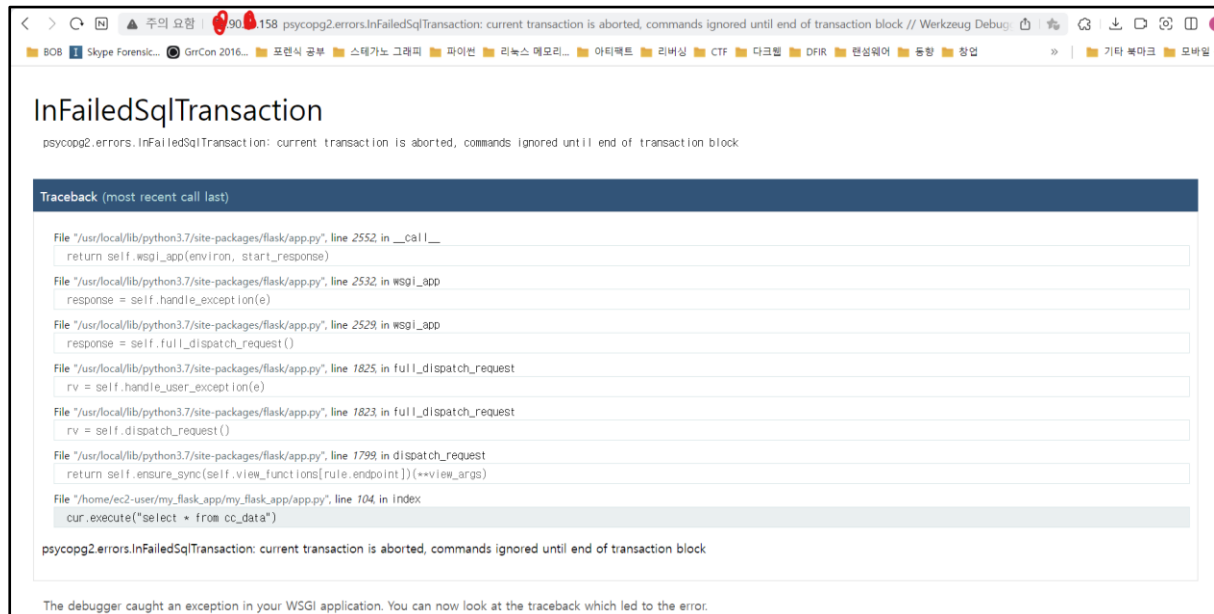
[cloudgoat] terraform output completed with no error code.
cg_web_site_ip = 190.158
cg_web_site_port = 5000

[cloudgoat] Output file written to:

/mnt/c/Users/n0rel/OneDrive/cloudgoat/glue_privesc_cg1d3tw70p71kr/start.txt
```

The server address is different from the one I asked you about earlier, and I did not create a new database either.

But..... The same error occurred again...



The screenshot shows a web browser window with a URL bar containing "90.158 psycopg2.errors.InFailedSqlTransaction: current transaction is aborted, commands ignored until end of transaction block // Werkzeug Debug". The browser's address bar also shows "BOB", "Skype Forensic...", "GnCon 2016...", "포렌식 공부", "스태가노 그래픽", "파이썬", "리눅스 메모리...", "아티팩트", "리버싱", "CTF", "다크웹", "DFIR", "현상위어", "동향", "참고", "기타 북마크", and "모바일".

InFailedSqlTransaction

psycopg2.errors.InFailedSqlTransaction: current transaction is aborted, commands ignored until end of transaction block

Traceback (most recent call last)

```
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 2552, in __call__
    return self.wsgi_app(environ, start_response)
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 2532, in wsgi_app
    response = self.handle_exception(e)
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 2529, in wsgi_app
    response = self.full_dispatch_request()
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 1825, in full_dispatch_request
    rv = self.handle_user_exception(e)
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 1823, in full_dispatch_request
    rv = self.dispatch_request()
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 1799, in dispatch_request
    return self.ensure_sync(self.view_functions[rule.endpoint])(**view_args)
File "/home/ec2-user/my_flask_app/my_flask_app/app.py", line 104, in index
    cur.execute("select * from co_data")

psycopg2.errors.InFailedSqlTransaction: current transaction is aborted, commands ignored until end of transaction block
```

The debugger caught an exception in your WSGI application. You can now look at the traceback which led to the error.

2. Future Action Items

After resolving the error, I plan to proceed with solving the problem according to the provided scenario.