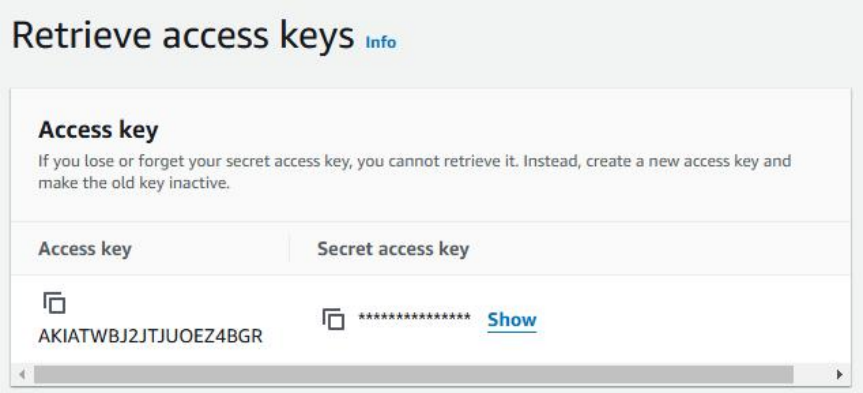
ISIN 335 –Penetration Testing Project 3
Instructor: Gerald Emerick

Penetration Testing Project 3

Use your AWS Free Tier account for this assignment. In this assignment you will install, configure, and use the AWS CLI. You will learn about the Pacu penetration testing framework for AWS. You will install, configure, and run basic use cases of the Pacu penetration testing framework in you AWS Free Tier account.

1. Create an IAM user, assign roles, and obtain secret access keys.
    a. Login to your Free Tier AWS Console.
    b. Go to IAM -> Users
    c. Add a new user named “auditor”
        i. Set access type to “Programmatic Access”
        ii. Assign the ReadOnlyAccess and SecurityAudit policies to the auditor user
        iii. Copy the Access Key ID and Secret Access Key values to a safe document. You will need these later.



2. Using Kali 4 EC2 Instance from the previous assignment.
    a. Start the instance
    b. Establish an SSH connection to the instance.
    c. Install the aws command line utility by executing the following commands:
        i. sudo apt-get update
        ii. sudo apt-get install python3-pip
        iii. sudo pip3 install --upgrade --user awscli
        iv. export PATH=~/.local/bin:$PATH

    d. Configure the aws CLI.
        i. Execute the command “aws configure”
            - Enter the AWS Access Key from the auditor user you created.
            - Enter the AWS Secret Access Key from the auditor user you created.
            - Enter the code for the region of the user. This can be found in the URL of your web browser when managing the EC2 instance or IAM in the AWS Console. The value and may resemble “us-east-1” or something similar.

- Enter “text” for the Default output format

```
┌──(kali㉿kali)-[~]
└─$ aws configure
AWS Access Key ID [None]: AKIATWBJ2JTJUOEZ4BGR
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]: text
```

e. Kali aws cli

i. Execute the command “aws ec2 describe-instances”. Your instance meta-data should display in the output.

ii. Create an S3 bucket and upload one file to the bucket.

iii. Execute the command “aws s3 ls s3://[your bucket name]” You should see your file listed.

iv. Peform the following commands. You should receive permissions errors as your auditor user does not have permission to perform the operations. **Adjust permissions, roles, and policies as necessary to successfully execute the commands.**

- Create a file – “touch index.html”
- Copy the file to S3 “aws s3 cp index.html s3://[your bucket name] “

- Start your Ubuntu instance aws ec2 start-instances --instance-ids [one of your instance ids]
- Get an attribute of the Ubuntu instance – “aws ec2 describe-instance-attribute --attribute instanceType --instance-id [your instance id] ”
- Get Security Group information for your Ubuntu instance “aws ec2 describe security-groups --group-ids [your security group ID] “

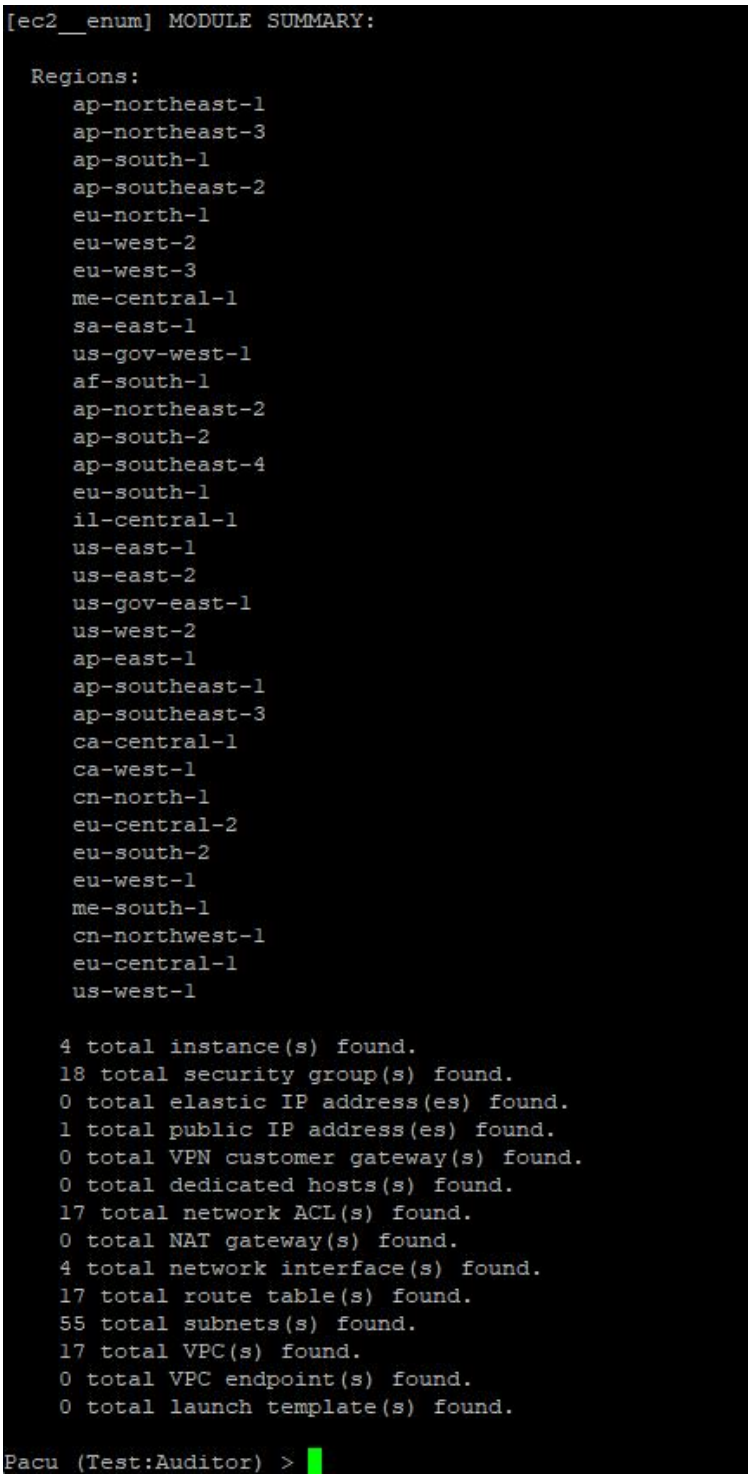
```
┌──(kali㉿kali)-[~]
└─$ touch index.html

┌──(kali㉿kali)-[~]
└─$ aws s3 cp index.html s3://supercoolpentestingbucketforzach
upload: ./index.html to s3://supercoolpentestingbucketforzach/index.html

┌──(kali㉿kali)-[~]
└─$ aws ec2 start-instances --instance-ids i-0e739c8fcffb3c30c
STARTINGINSTANCES       i-0e739c8fcffb3c30c
CURRENTSTATE    0       pending
PREVIOUSSTATE   80      stopped

┌──(kali㉿kali)-[~]
└─$ aws ec2 describe-instance-attribute --attribute instanceType --instance-id i-0e739c8fcffb3c30c
i-0e739c8fcffb3c30c
INSTANCETYPE    t2.micro

┌──(kali㉿kali)-[~]
└─$ aws ec2 describe-security-groups --group-ids sg-0b61lee664555353c
SECURITYGROUPS  Kali Linux Security Group       sg-0b61lee664555353c    SecurityGroupKali       253490777299    vpc-078a0eb8eb565dd2d
IPPERMISSIONS   0       tcp     65535
IPRANGES        0.0.0.0/0
IPPERMISSIONS   21      tcp     21
IPRANGES        0.0.0.0/0
IPPERMISSIONS   22      tcp     22
IPRANGES        0.0.0.0/0
IPPERMISSIONS   -1      icmp    -1
IPRANGES        0.0.0.0/0
IPPERMISSIONSEGRESS     -1
IPRANGES        0.0.0.0/0
```

3. Review the AWS Penetration Testing video and AWS penetration testing tool PACU including the following web page and demonstration video. Write a 150 to 200 word synopsis of your review that includes the key concerns within AWS penetration testing and the key features of PACU tool. a. https://rhinosecuritylabs.com/aws/pacu-open-source-aws-exploitation-framework/

b. https://youtu.be/5NbFcC3yPhM

PACU is a framework that is used for AWS security-testing. It is primary used as an "exploitation" program similar to Metasploit. It is meant to be a program utilized by red team within the AWS cloud. This can involve testing for security reasons, alongside finding vulnerabilities that would expose sensitive information if not properly configured. The key concerns that I look at involve how penetration testing in AWS could lead to potentially exposing sensitive data if not done correctly. Additionally, if IAM is not configured properly it could lead to unauthorized access and/or privilege escalation which could jeopardize an organization's AWS environment. Another main concern that I noticed is that PACU needs the access key and secret key which while necessary provides a major weakpoint for PACU which could lead to exploitation of the system.

4. Install the Pacu penetration testing framework by issuing the following commands
    a. Change from kali user to root user using "sudo –i"
    b. git clone https://github.com/RhinoSecurityLabs/pacu.git
    c. cd pacu
    d. bash install.sh **or** sudo ./install.sh
    e. python3 ./cli.py
    f. From the Pacu command prompt
        i. Enter "set_keys"
        ii. Enter the access and secret keys for the auditor user that you created in the previous steps. Do not enter a session token value.
        iii. Enter "ls" to list all of the pacu modules
        iv. Enter "search ec2" to list all of the ec2 related modules.
        v. Enter "help ec2__enum" and review command options.
        vi. Enter "run ec2__enum". Provide a screenshot of the results. Pacu will enumerate instances, security groups, and other AWS items.



vii. Execute the “data” command to view all data that Pacu has collected so far.

viii. Enter “run cloudtrail__download_event_history”. Describe the output.

The command has an error when running due to the security token being invalid as we did not include that within the set_keys step.

ix. Enter “whoami”. Describe the output.

The whoami command provides everything as null besides AccessKeyID, SecretAccessKey, and KeyAlias as those are all forms that were inputted on PACU login.

5. Stop all EC2 instances.

6. Write a brief synopsis of the assignment including key learning items, any challenges that you encountered, and questions that you may have.

   The main takeaways I learned from this penetration testing assignment is that PACU is a tool that is really cool but has a lot of areas that are concerning. Additionally, AWS is quite fun to mess around with its configuration. I did have quite a few challenges during this lab initially though. A major obstacle I encountered was a missing install.sh bug which led me down a rabbit hole. My way to fix this was to create a new Kali instance, repeat the steps that went well, and then to create an isolated environment to install PACU from the installation guide online on GitHub. I was also a bit confused by step 4 area vi. This task created a failure because of the session token being invalid, which I thought happened because we did not set a session token. Overall, I had a great experience with these assignments and this class as a whole. I do not have any questions at this time.

Deliverables / What to Submit

1. A single PDF with screenshots of all required steps clearly labeled.
2. PACU synopsis.
3. A synopsis of the assignment.

Extra credit – Download, configure and run Scout Suite from github within your AWS Kali machine. Successfully execute the tool against your AWS Free Tier account and provide a synopsis of the tool's features.