Course: CYB301

Security Defense and Response

(Canadian Context)

Lab 7: Cloud Security

Coordinator and Instructor:

Muhammad Siddiqui

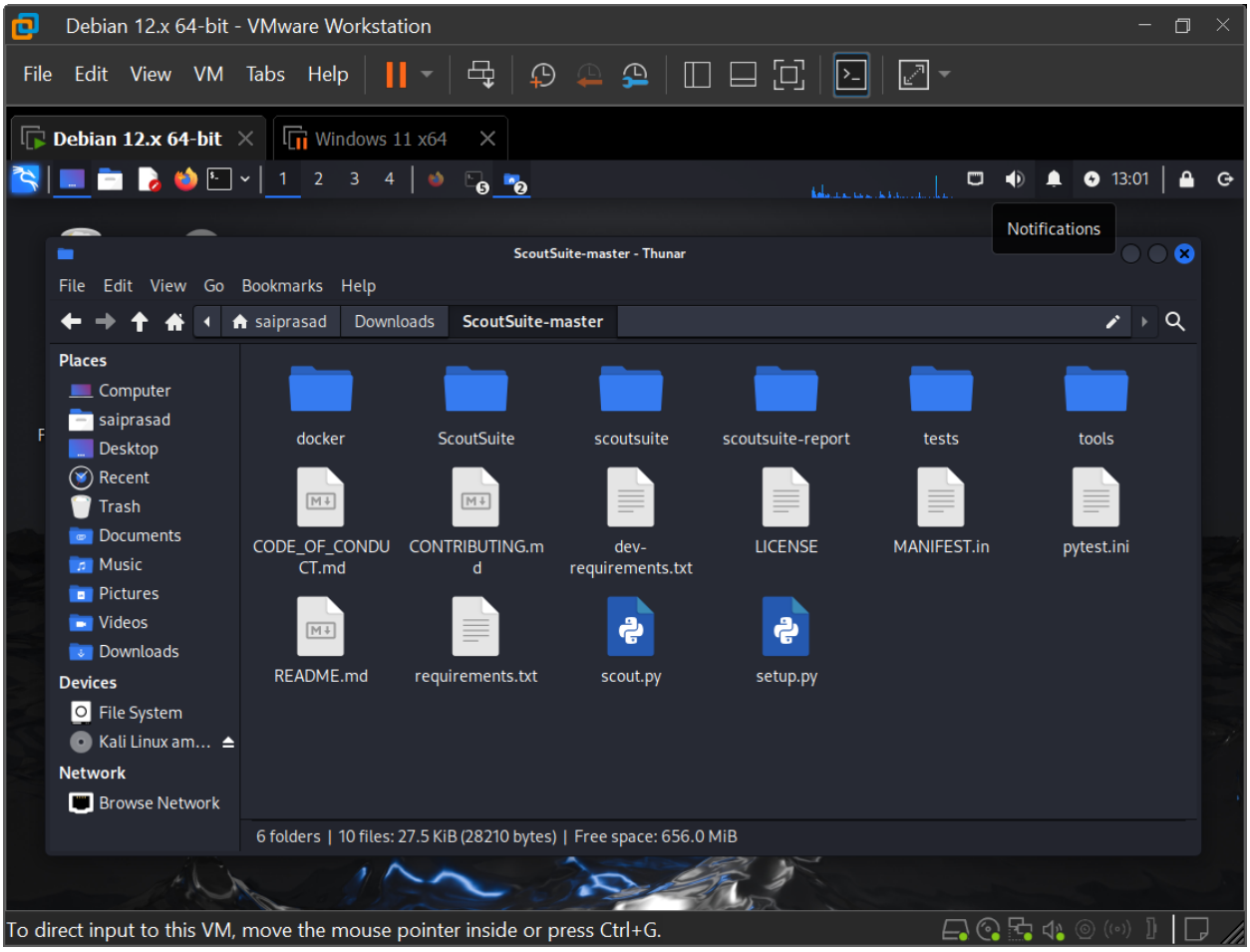
Saiprasad Raman - 23074624

Cloud Security

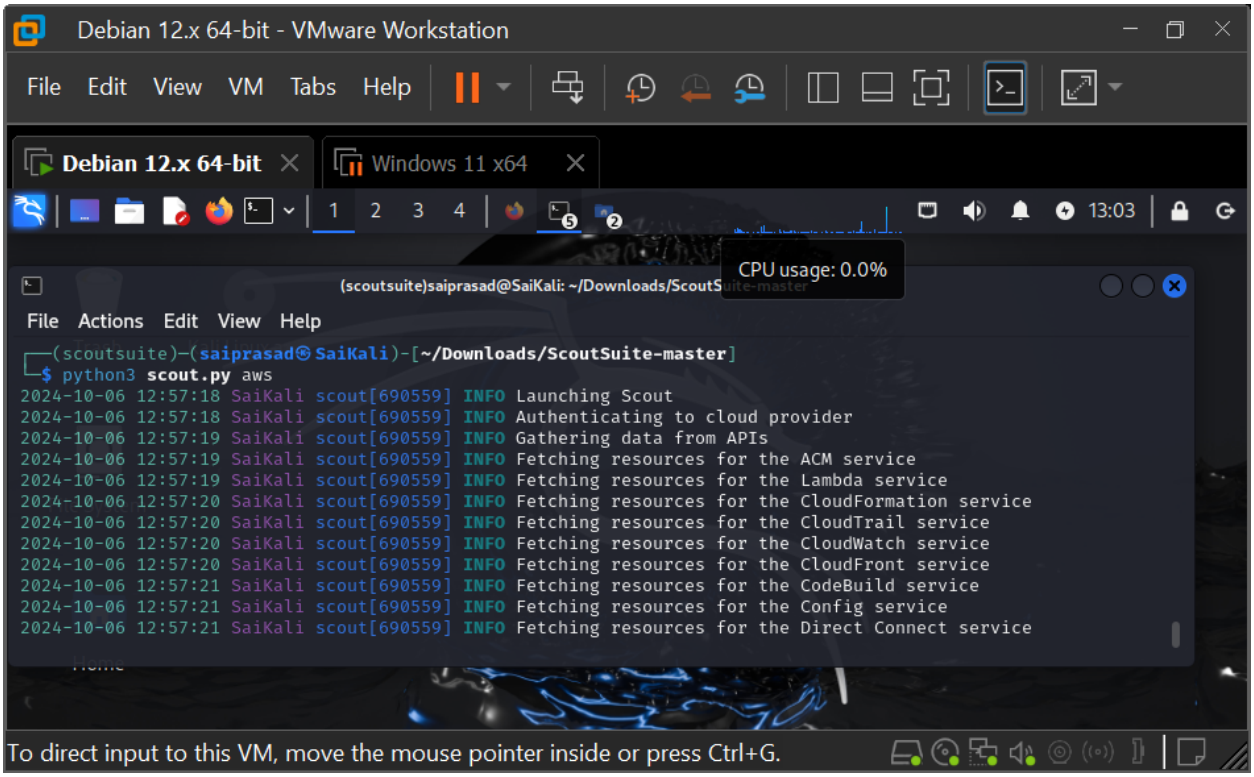
Activity 1: Run a ScoutSuite Assessment.

ScoutSuite is a Python script available for free download. In this activity, you will download and run the tool. Note that running ScoutSuite requires read-only access to a cloud account. You should only run this scan against an account that you have permission to scan. Use Kali Linux VM to perform all the activities of this lab.

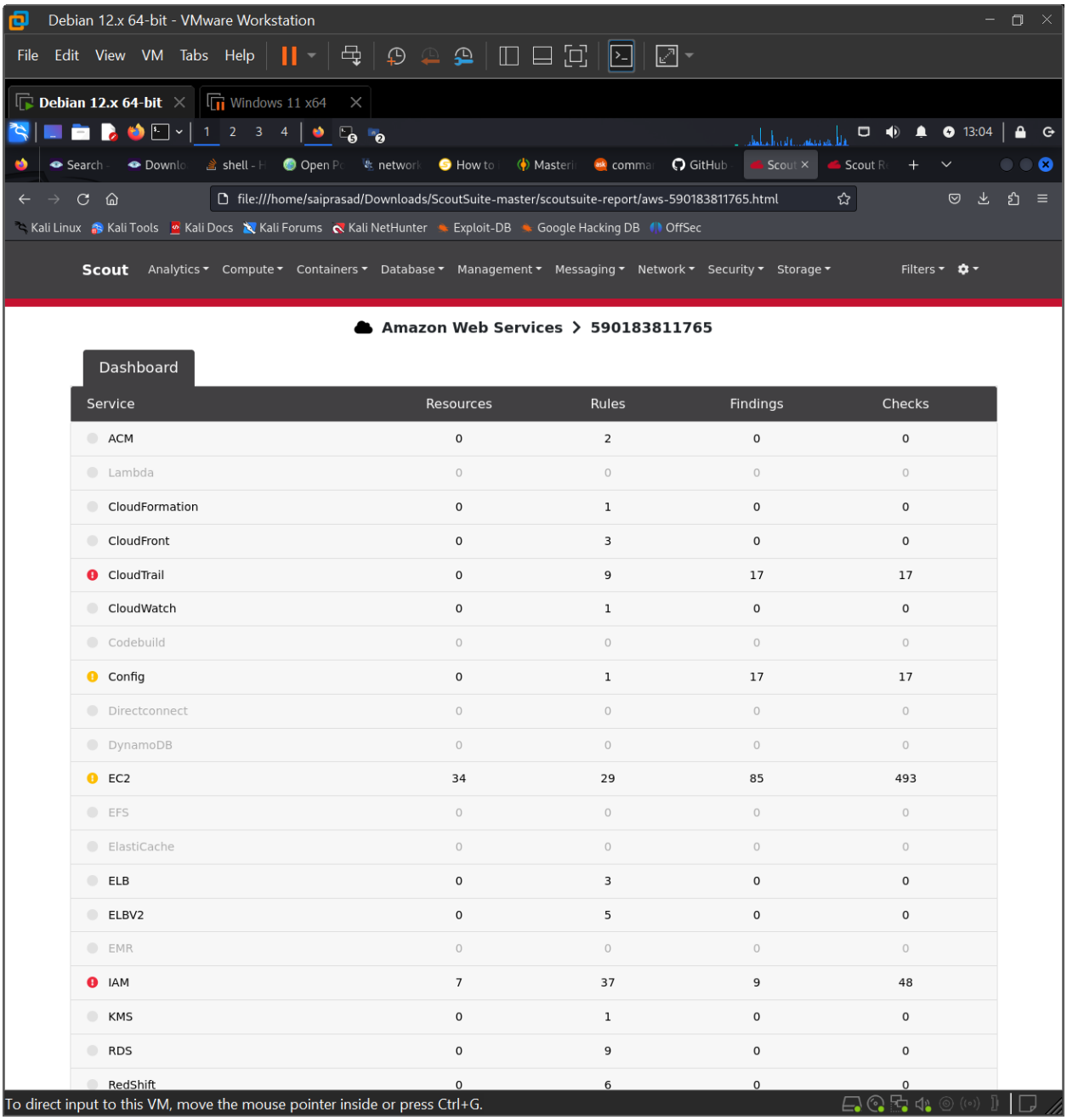
1. Download ScoutSuite from the GitHub repository at [github.com/nccgroup/ScoutSuite.](github.com/nccgroup/ScoutSuite)



2. Run it on a system that has Python installed using the command **python3 scout.py**. Review the instructions presented to you to configure and run ScoutSuite against the cloud provider of your choice.



3. Analyze the findings from your ScoutSuite report.



Service	Resources	Rules	Findings	Checks
ACM	0	2	0	0
Lambda	0	0	0	0
CloudFormation	0	1	0	0
CloudFront	0	3	0	0
CloudTrail	0	9	17	17
CloudWatch	0	1	0	0
Codebuild	0	0	0	0
Config	0	1	17	17
Directconnect	0	0	0	0
DynamoDB	0	0	0	0
EC2	34	29	85	493
EFS	0	0	0	0
ElastiCache	0	0	0	0
ELB	0	3	0	0
ELBV2	0	5	0	0
EMR	0	0	0	0
IAM	7	37	9	48
KMS	0	1	0	0
RDS	0	9	0	0
RedShift	0	6	0	0

4. What are the most pressing vulnerabilities that you found? How would you address them?

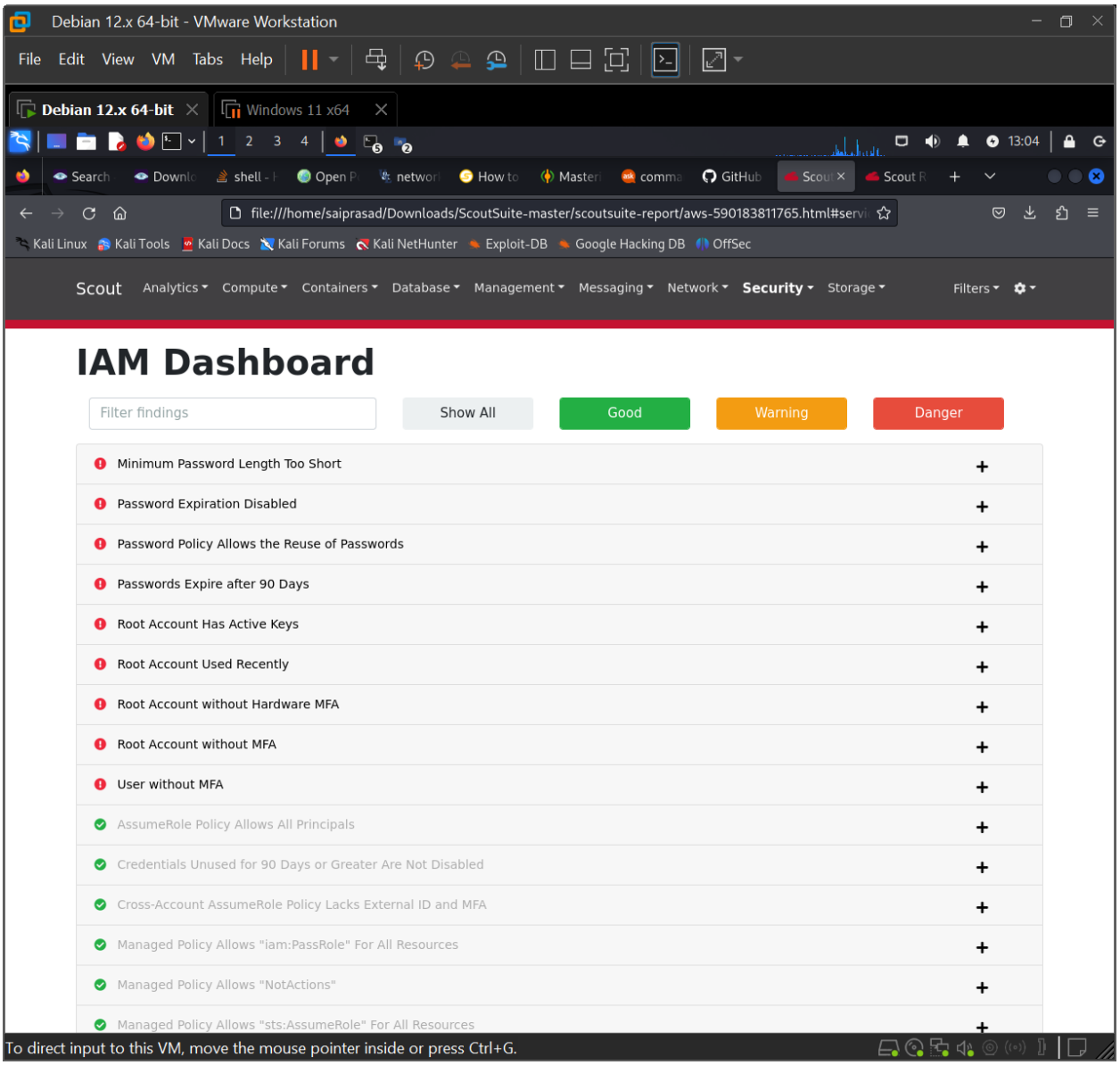
Ans.

Vulnerabilities:

1. Multifactor Authentication wasn't setup for this account.
2. Root account has active keys

Solution:

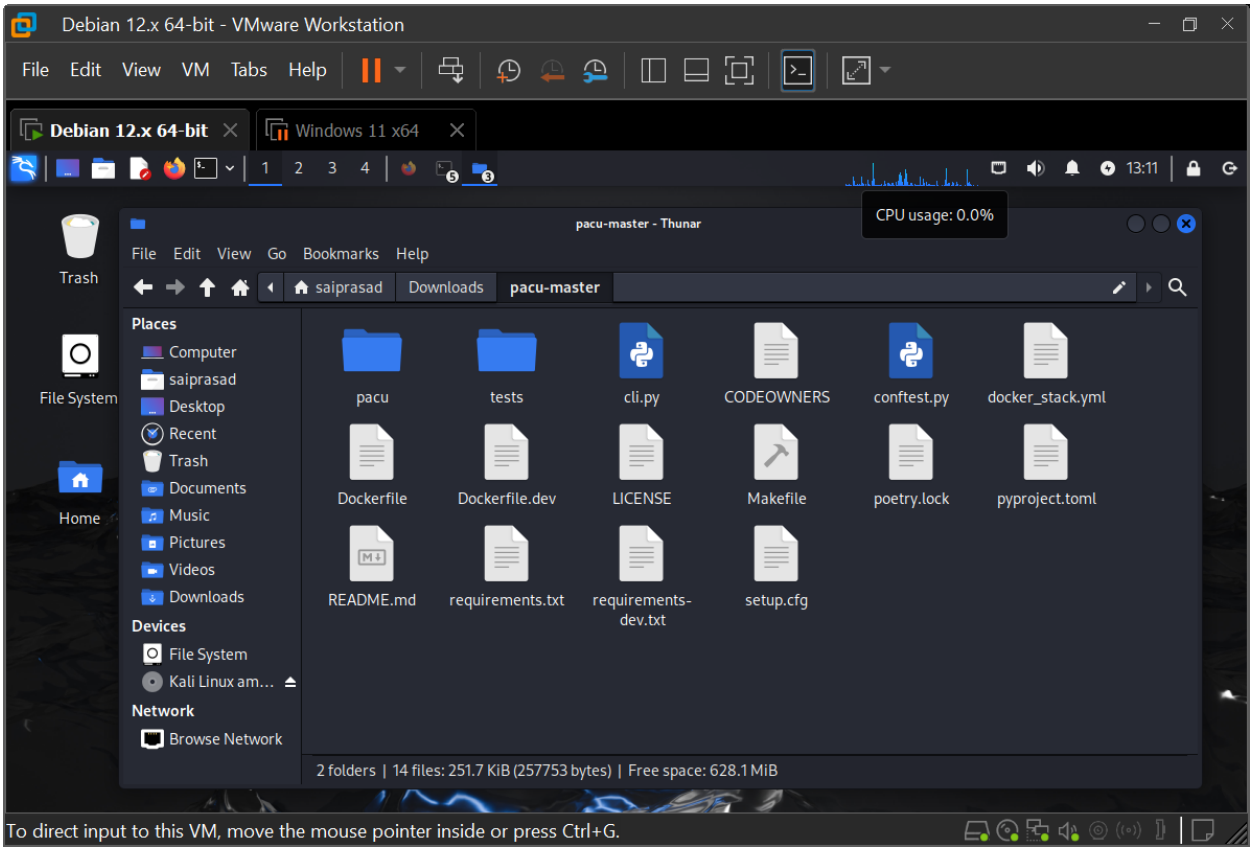
1. Enable MFA using the Authenticator app
2. Create a new user and provide it with an access key and id.



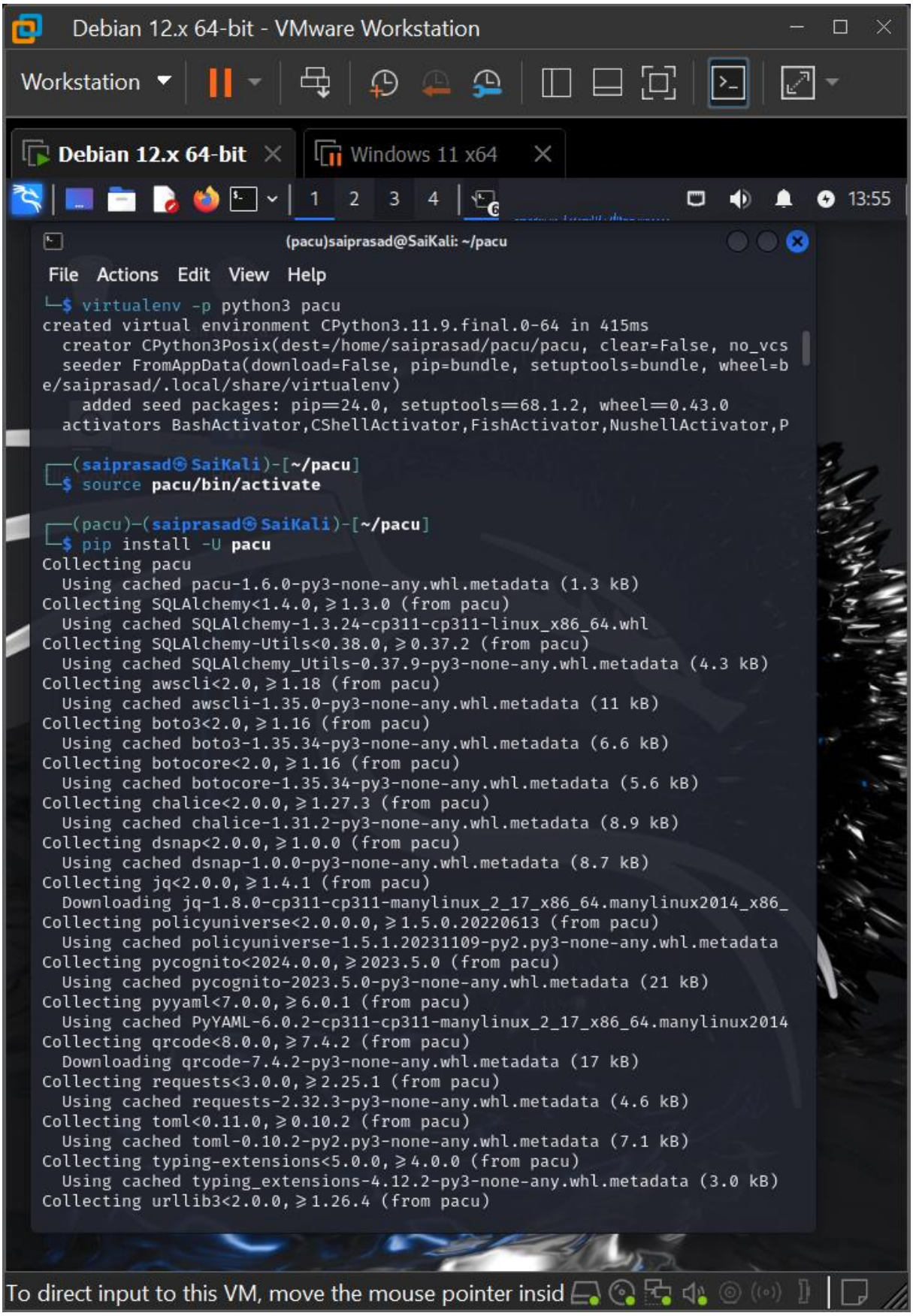
Activity 2: Explore the Exploits Available with Pacu.

Pacu is also a Python script available for free download. In this activity, you will download and run the tool. Running Pacu requires access to an AWS account. You should only run Pacu against an account that you have permission to scan.

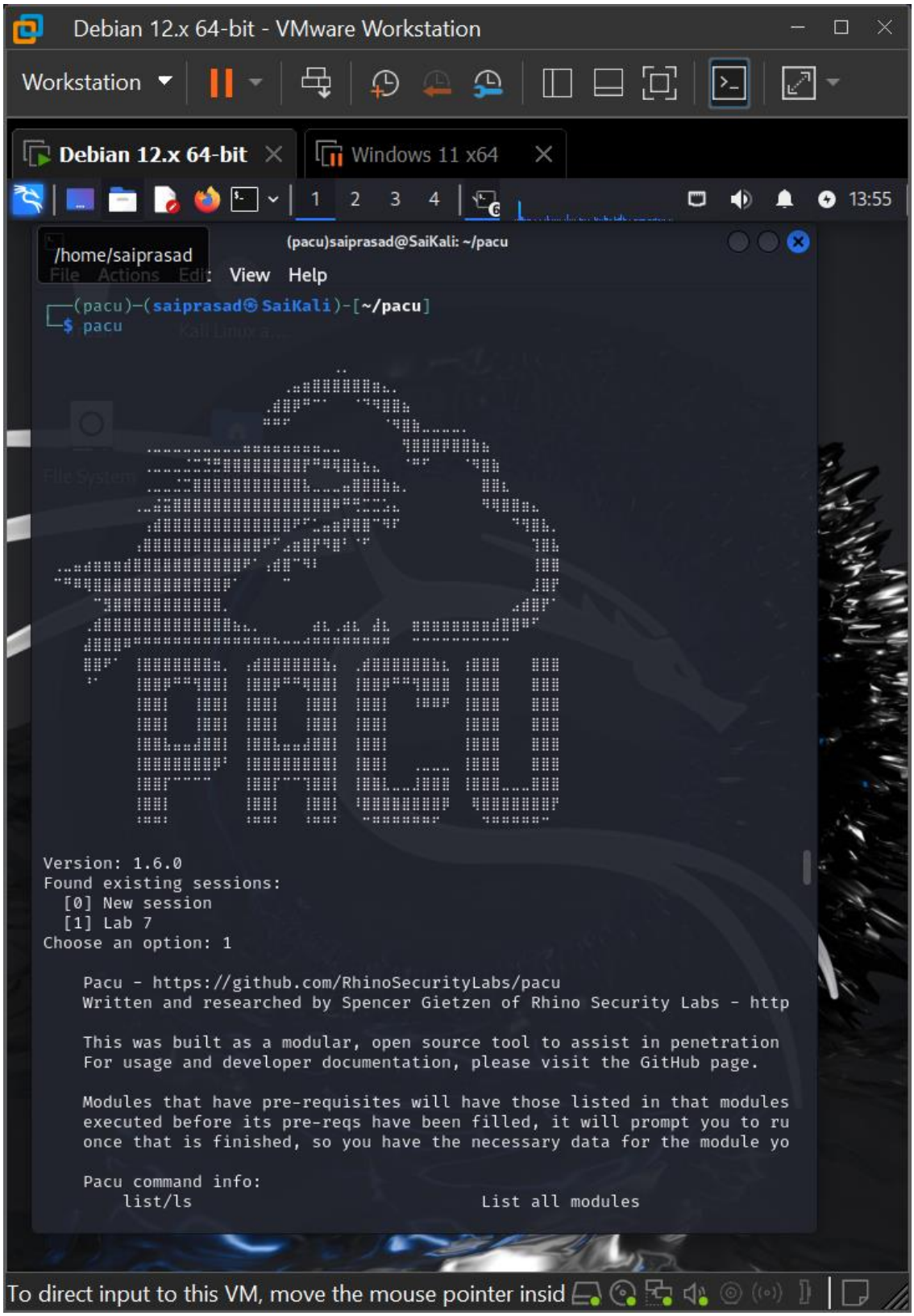
1. Download Pacu from the GitHub repository at **github.com/RhinoSecurityLabs/pacu.**



2. Install and configure Pacu on your system using the command **bash install.sh**.



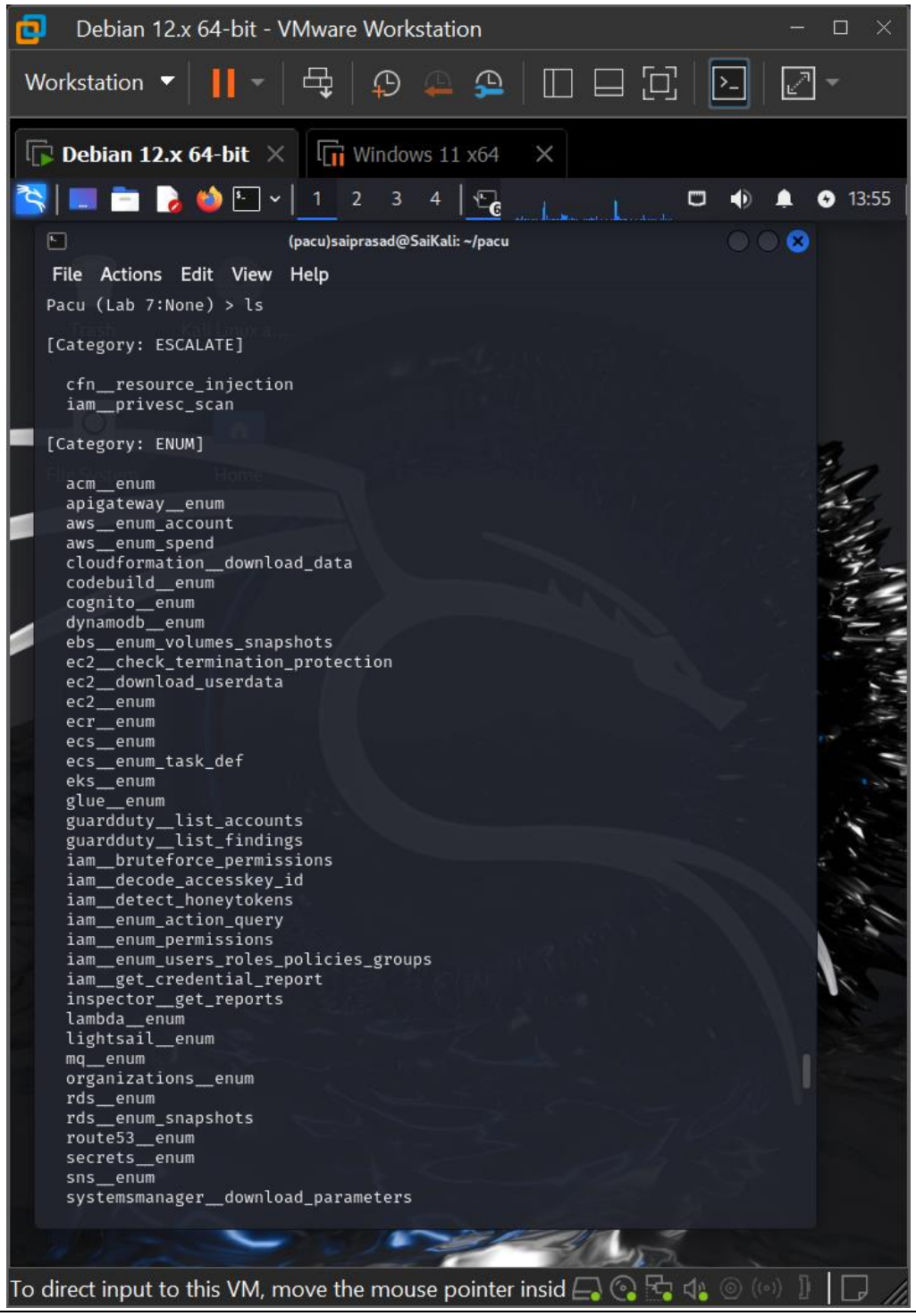
3. Run it on a system that has Python installed using the command **python3 pacu.py**. Review the instructions presented to you to configure and run Pacu against the cloud provider of your choice.



4. Run the list command to determine the modules currently available in Pacu. Which of these seem most valuable to you? How might you use them in a penetration test?

Ans.

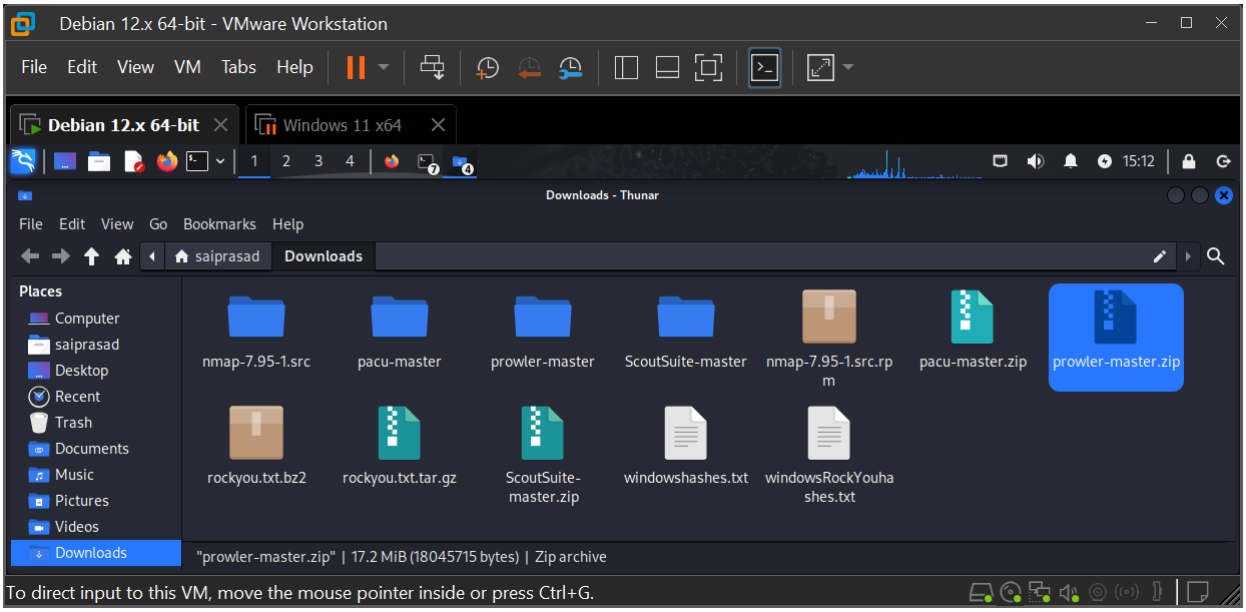
1. Iam__privesc_scan: This module would be used to inject group policies into the AWS account. This can be used to deny or add certain rights to the users, setting password policy.
2. S3__download_bucket: This can be used to download the data of the users.
3. Iam__backdoor_users_keys: Allowing users to stay connected to the AWS services by updating their Access Key and Access IDs to Administrator's.



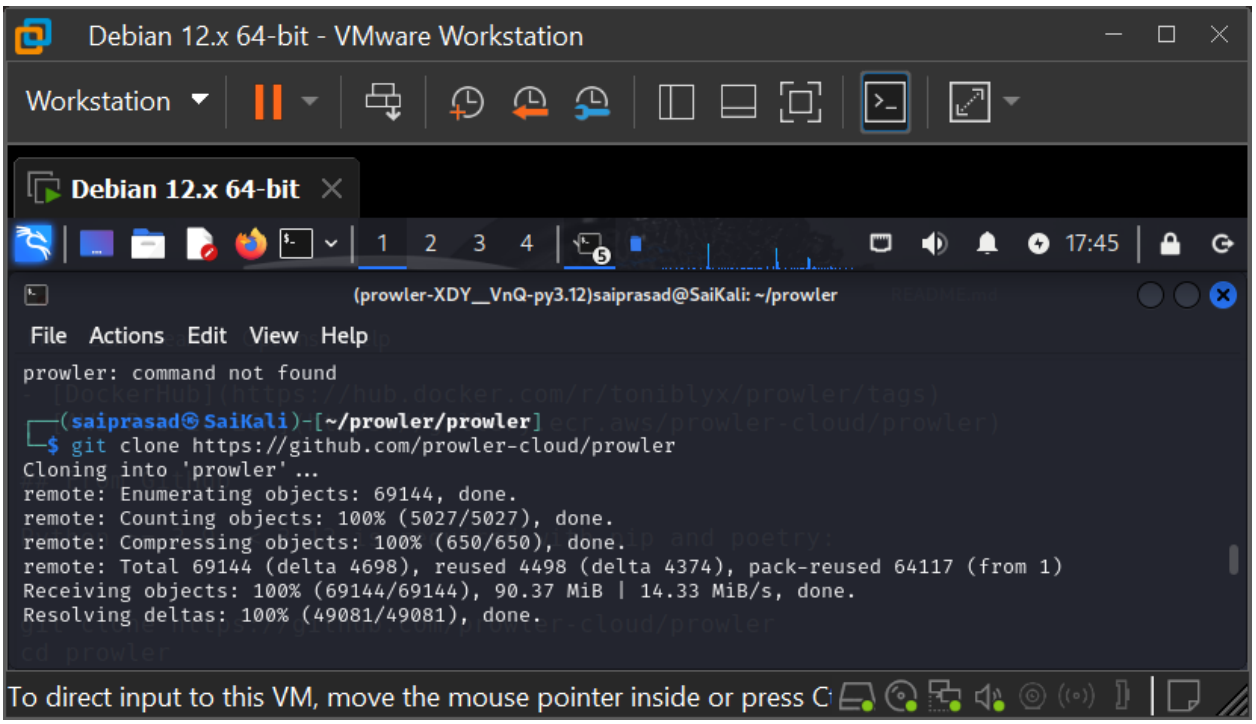
Activity 3: Scan an AWS account with Prowler (Optional).

Prowler is a command-line tool available for free download. In this activity, you will download and run the tool. Note that running Prowler requires read-only access to an AWS account. You should only run this scan against an account that you have permissionS to scan.

1. Download Prowler from the GitHub repository at: **github.com/toniblyx/prowler**.



2. Install it on your system, configure it, and run a scan. <u>This is a fairly complex process</u>, but you will find a document walking you through the current steps to do so in the README.md file in the Prowler GitHub repository.



Debian 12.x 64-bit - VMware Workstation

File Edit View VM Tabs Help

Debian 12.x 64-bit

1 2 3 4 17:46

(prowler-XDY__VnQ-py3.12)saiprasad@SaiKali: ~/prowler

CPU usage: 3.9%

File Actions Edit View Help

```
┌──(saiprasad㉿SaiKali)-[~/prowler/prowler]
└─$ poetry shell
Creating virtualenv prowler-XDY__VnQ-py3.12 in /home/saiprasad/.cache/pypoetry/virtualenvs
Spawning shell within /home/saiprasad/.cache/pypoetry/virtualenvs/prowler-XDY__VnQ-py3.12
┌──(saiprasad㉿SaiKali)-[~/prowler/prowler]
└─$ emulate bash -c '. /home/saiprasad/.cache/pypoetry/virtualenvs/prowler-XDY__VnQ-py3.12/bin/activate'

┌──(prowler-XDY__VnQ-py3.12)─(saiprasad㉿SaiKali)-[~/prowler/prowler]
└─$ poetry install
Installing dependencies from lock file

Package operations: 211 installs, 0 updates, 0 removals

  - Installing wrapt (1.16.0)
  - Installing zipp (3.20.2)
  - Installing deprecated (1.2.14)
  - Installing importlib-metadata (8.4.0)
  - Installing pycparser (2.22)
  - Installing six (1.16.0)
  - Installing attrs (24.2.0)
  - Installing cffi (1.17.1)
  - Installing jmespath (1.0.1)
  - Installing opentelemetry-api (1.27.0)
  - Installing python-dateutil (2.9.0.post0)
  - Installing rpds-py (0.20.0)
  - Installing urllib3 (2.2.3)
  - Installing botocore (1.35.29): Installing ...
  - Installing botocore (1.35.29)
  - Installing certifi (2024.8.30)
  - Installing charset-normalizer (3.3.2)
  - Installing cryptography (43.0.1)
  - Installing frozenlist (1.4.1)
  - Installing h11 (0.14.0)
  - Installing hpack (4.0.0)
  - Installing hyperframe (6.0.1)
  - Installing idna (3.10)
  - Installing multidict (6.1.0)
  - Installing opentelemetry-semantic-conventions (0.48b0)
  - Installing referencing (0.35.1)
  - Installing sniffio (1.3.1)
  - Installing typing-extensions (4.12.2)
  - Installing aiohappyeyeballs (2.4.2)
  - Installing aiosignal (1.3.1)
  - Installing anyio (4.6.0)
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

3. Analyze the findings from your Prowler report.

Debian 12.x 64-bit - VMware Workstation

File Edit View VM Tabs Help

Debian 12.x 64-bit

1 2 3 4 17:48

(prowler-XDY__VnQ-py3.12)saiprasad@SaiKali: ~/prowler

File Actions Edit View Help

```
┌──(prowler-XDY__VnQ-py3.12)─(saiprasad㉿SaiKali)-[~/prowler/prowler]
└─$ cd ..
┌──(prowler-XDY__VnQ-py3.12)─(saiprasad㉿SaiKali)-[~/prowler]
└─$ python prowler.py -v
Prowler 4.5.0 (You are running the latest version, yay!)

┌──(prowler-XDY__VnQ-py3.12)─(saiprasad㉿SaiKali)-[~/prowler]
└─$ prowler aws
                                 _
 _ __ _ __ _____      _| | __ _ _ __
| '_ \| '__/ _ \ \ /\ / / |/ _ \ '__|
| |_) | | | (_) \ V  V /| |  __/ |
| .__/|_|  \___/ \_/\_/ |_|\___|_|v4.5.0
|_| the handy multi-cloud security tool

Date: 2024-10-06 17:39:43

→ Using the AWS credentials below:
  · AWS-CLI Profile: default
  · AWS Regions: all
  · AWS Account: 590183811765
  · User Id: 590183811765
  · Caller Identity ARN: arn:aws:iam::590183811765:root

→ Using the following configuration:
  · Config File: /home/saiprasad/prowler/prowler/config/config.yaml
  · Mutelist File: /home/saiprasad/prowler/prowler/config/aws_mutelist.yaml
  · Scanning unused services and resources: False

Executing 472 checks, please wait...
→ Scan completed! |▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉▉| 472/472 [100%] in 3:31.7

Overview Results:
```

58.67% (176) Failed	40.0% (120) Passed	0.0% (0) Muted

Account 590183811765 Scan Results (severity columns are for fails only):

Provider	Service	Status	Critical	High	Medium	Low	Muted
aws	accessanalyzer	FAIL (17)	0	0	0	17	0
aws	account	FAIL (1)	0	0	1	0	0
aws	backup	FAIL (1)	0	0	0	1	0
aws	cloudtrail	FAIL (34)	0	17	0	17	0
aws	cloudwatch	FAIL (15)	0	0	15	0	0
aws	config	FAIL (17)	0	0	17	0	0
aws	drs	FAIL (17)	0	0	17	0	0
aws	ec2	PASS (34)	0	0	0	0	0
aws	emr	PASS (17)	0	0	0	0	0
aws	eventbridge	PASS (51)	0	0	0	0	0
aws	guardduty	FAIL (17)	0	0	17	0	0
aws	iam	FAIL (15)	3	2	8	2	0
aws	inspector2	FAIL (17)	0	0	17	0	0

To direct input to this VM, move the mouse pointer inside or press Ctrl+G

4. What are the most pressing vulnerabilities that you found? How would you address them?

Ans. The most affected is the compliance requirements are not being met. It is important to follow NIST, MITRE, CIS, CISA frameworks to mitigate these vulnerabilities. For example, making sure least privilege access is configured to non-Admin accounts.