



Course: CYB301
Security Defense and Response
(Canadian Context)

Lab 7: Cloud Security

Coordinator and Instructor:
Muhammad Siddiqui

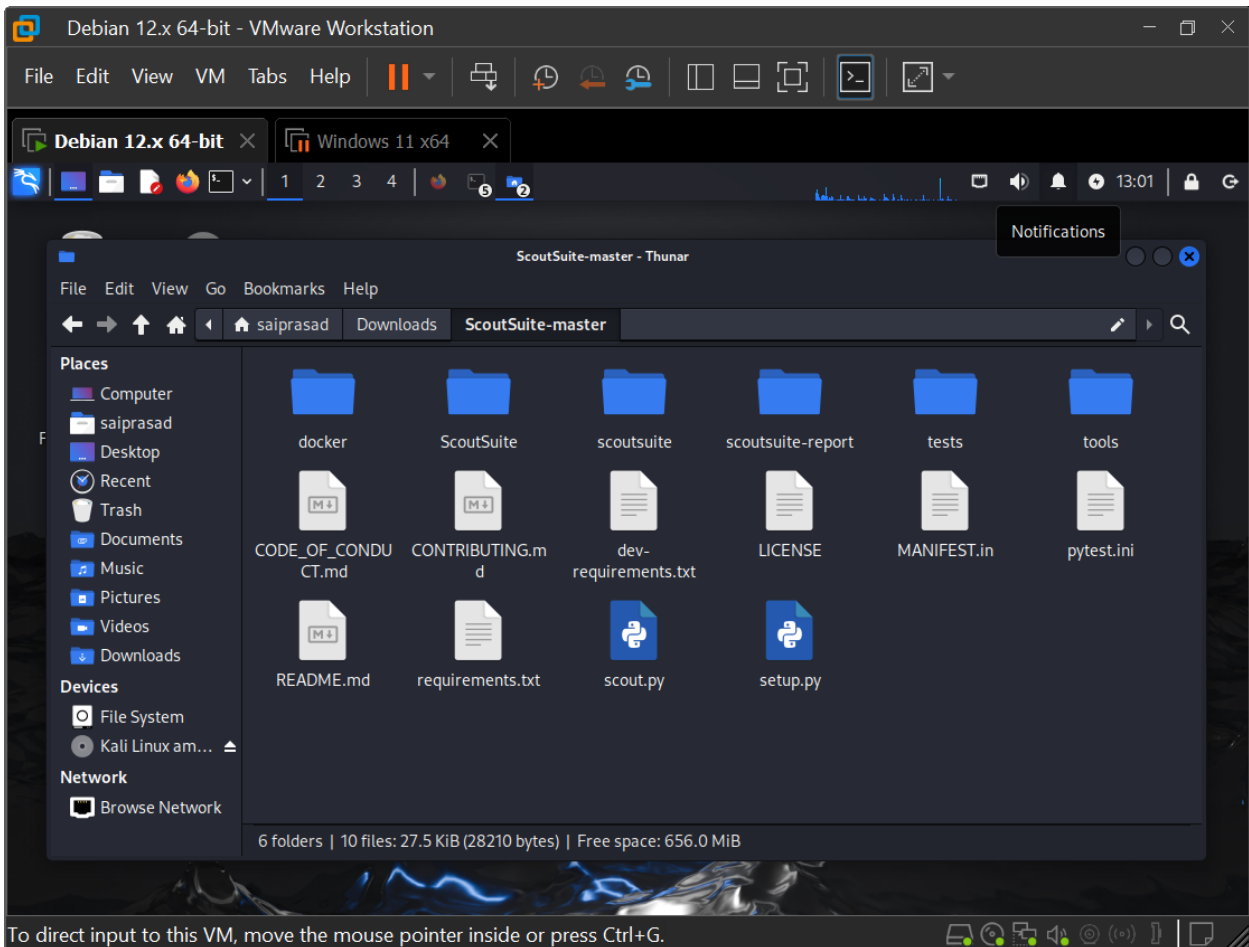
Saiprasad Raman - 23074624

Cloud Security

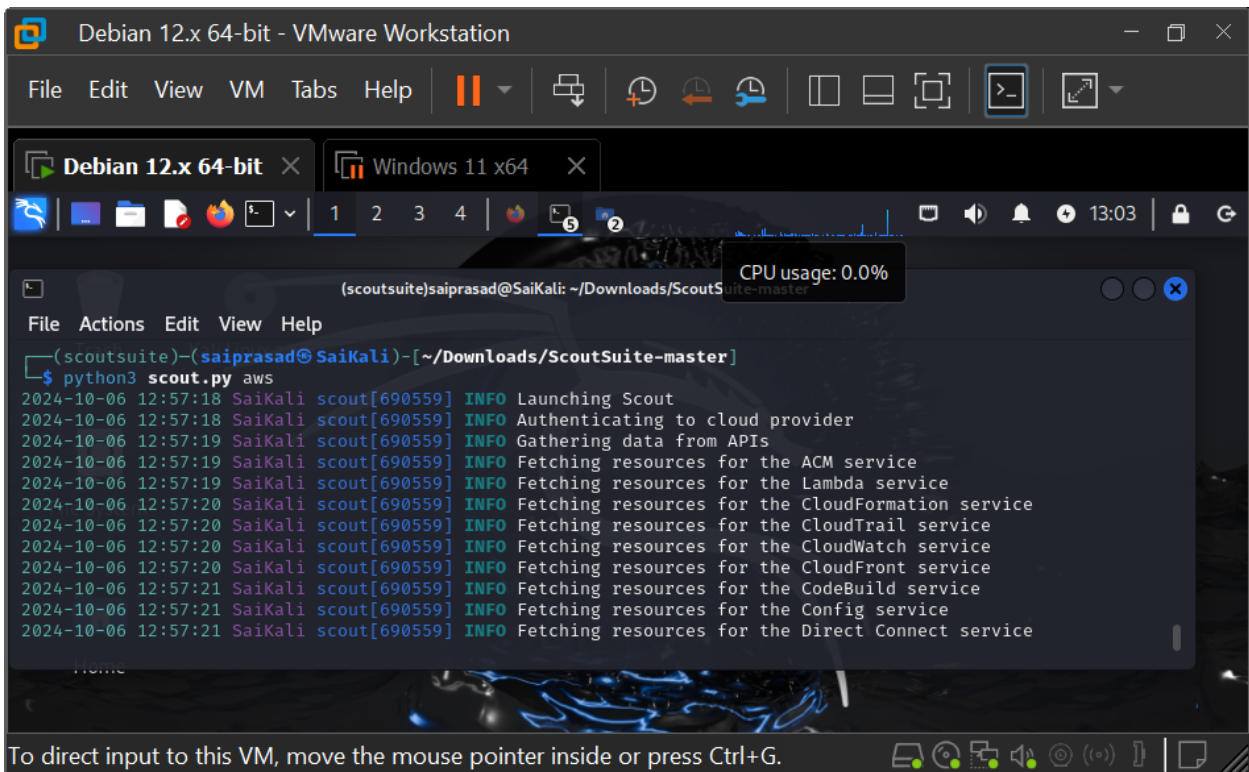
Activity 1: Run a ScoutSuite Assessment.

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.



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.



The screenshot shows a VMware Workstation interface with a Debian 12.x 64-bit VM running. The terminal window displays the following output:

```
(scoutsuite)saiprasad@SaiKali: ~/Downloads/ScoutSuite-master
File Actions Edit View Help
(scoutsuite)-(saiprasad@ SaiKali)-[~/Downloads/ScoutSuite-master]
$ python3 scout.py aws
2024-10-06 12:57:18 SaiKali scout[690559] INFO Launching Scout
2024-10-06 12:57:18 SaiKali scout[690559] INFO Authenticating to cloud provider
2024-10-06 12:57:19 SaiKali scout[690559] INFO Gathering data from APIs
2024-10-06 12:57:19 SaiKali scout[690559] INFO Fetching resources for the ACM service
2024-10-06 12:57:19 SaiKali scout[690559] INFO Fetching resources for the Lambda service
2024-10-06 12:57:20 SaiKali scout[690559] INFO Fetching resources for the CloudFormation service
2024-10-06 12:57:20 SaiKali scout[690559] INFO Fetching resources for the CloudTrail service
2024-10-06 12:57:20 SaiKali scout[690559] INFO Fetching resources for the CloudWatch service
2024-10-06 12:57:20 SaiKali scout[690559] INFO Fetching resources for the CloudFront service
2024-10-06 12:57:21 SaiKali scout[690559] INFO Fetching resources for the CodeBuild service
2024-10-06 12:57:21 SaiKali scout[690559] INFO Fetching resources for the Config service
2024-10-06 12:57:21 SaiKali scout[690559] INFO Fetching resources for the Direct Connect service
```

Below the terminal window, a message states: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

3. Analyze the findings from your ScoutSuite report.

The screenshot shows a VMware Workstation window with a Debian 12.x 64-bit VM. The browser displays the ScoutSuite report for AWS account 590183811765. The report shows a table of services with their respective resources, rules, findings, and checks. The 'EC2' service has the highest number of findings (85) and checks (493).

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?

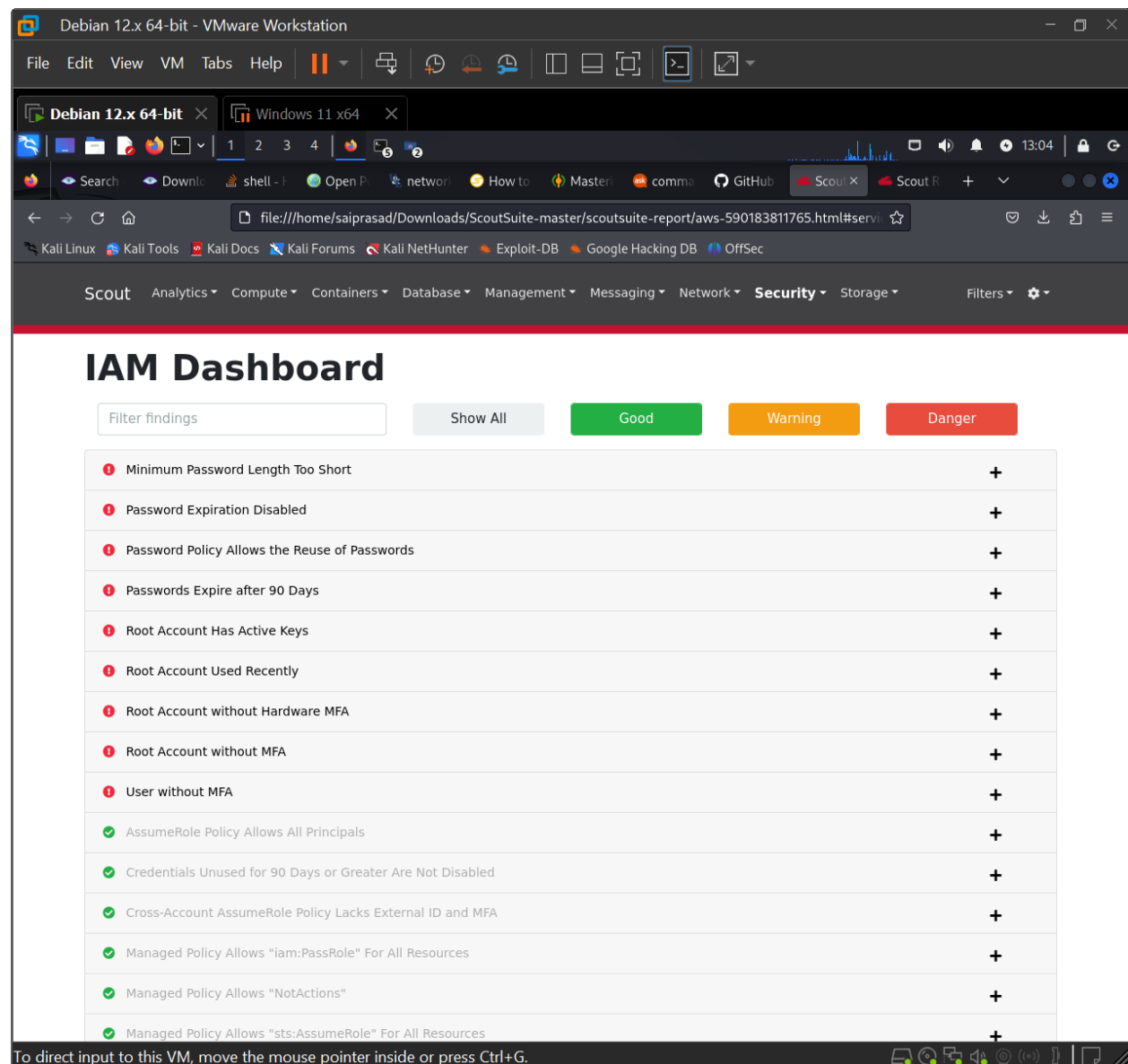
Ans.

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.



Debian 12.x 64-bit - VMware Workstation

File Edit View VM Tabs Help

Debian 12.x 64-bit Windows 11 x64

Search Download shell - Open P network How to Master comma GitHub Scout x Scout R

file:///home/saiprasad/Downloads/ScoutSuite-master/scoutsuite-report/aws-590183811765.html#servi

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Scout Analytics Compute Containers Database Management Messaging Network **Security** Storage Filters

IAM Dashboard

Filter findings Show All Good Warning Danger

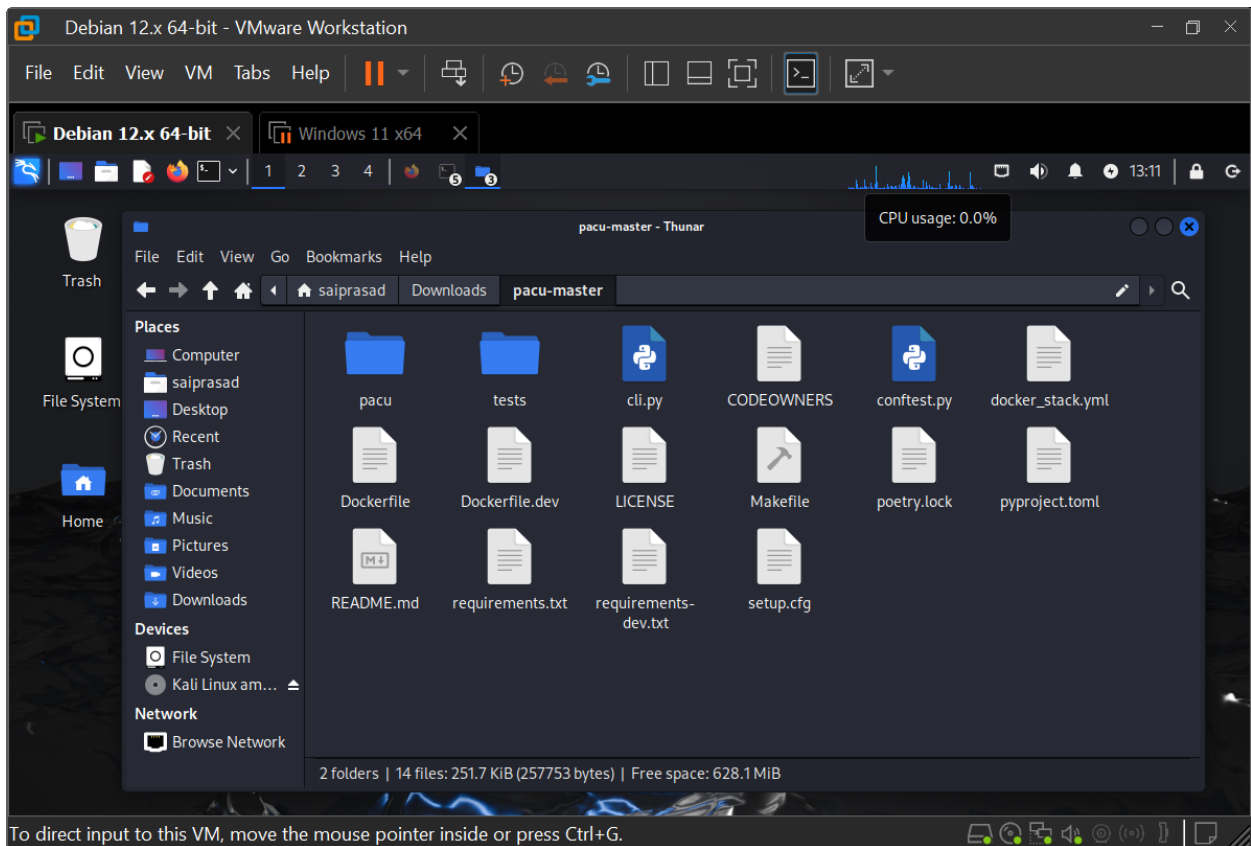
Minimum Password Length Too Short	+
Password Expiration Disabled	+
Password Policy Allows the Reuse of Passwords	+
Passwords Expire after 90 Days	+
Root Account Has Active Keys	+
Root Account Used Recently	+
Root Account without Hardware MFA	+
Root Account without MFA	+
User without MFA	+
AssumeRole Policy Allows All Principals	+
Credentials Unused for 90 Days or Greater Are Not Disabled	+
Cross-Account AssumeRole Policy Lacks External ID and MFA	+
Managed Policy Allows "iam:PassRole" For All Resources	+
Managed Policy Allows "NotActions"	+
Managed Policy Allows "sts:AssumeRole" For All Resources	+

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

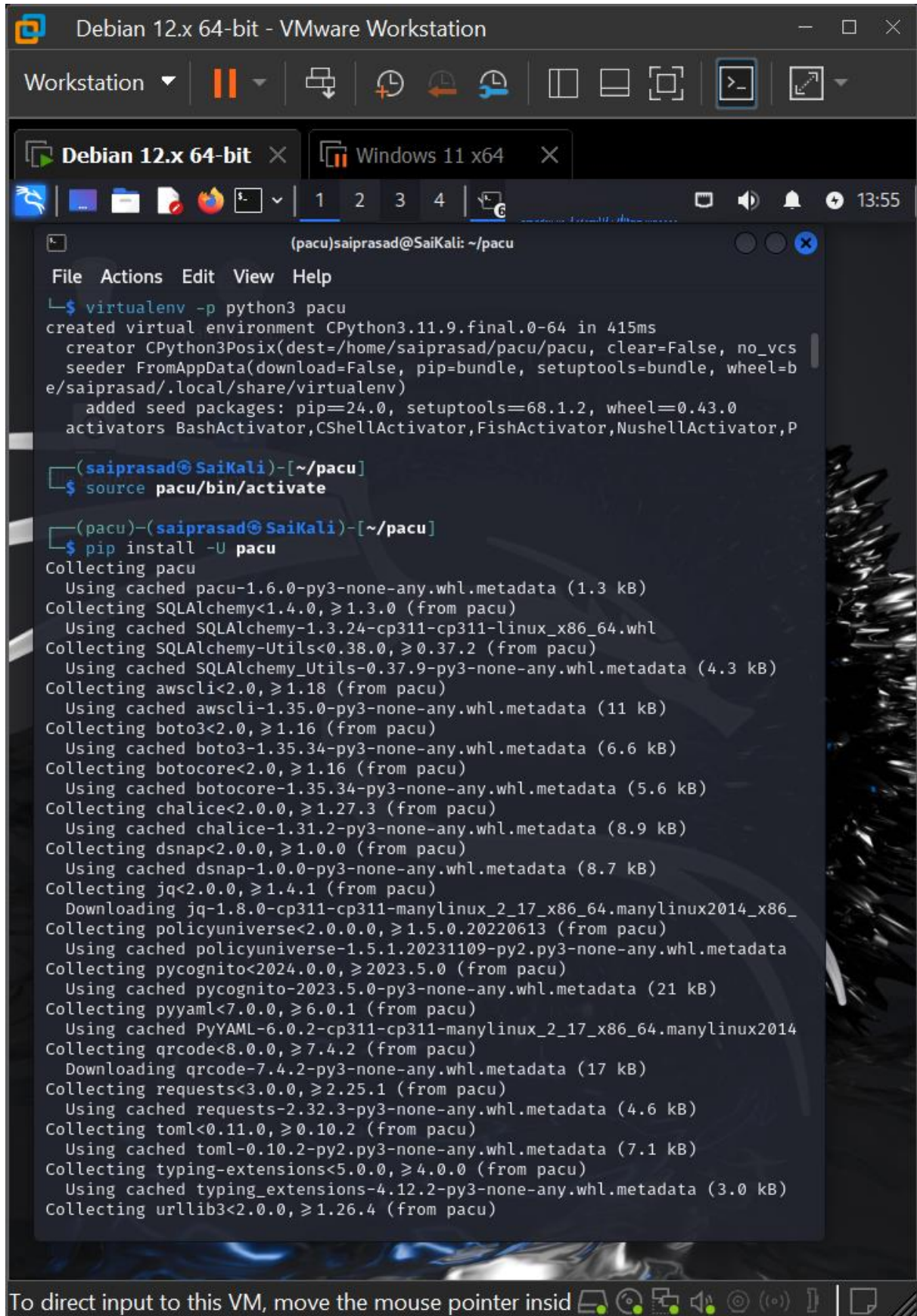
Activity 2: Explore the Exploits Available with Pacu.

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.



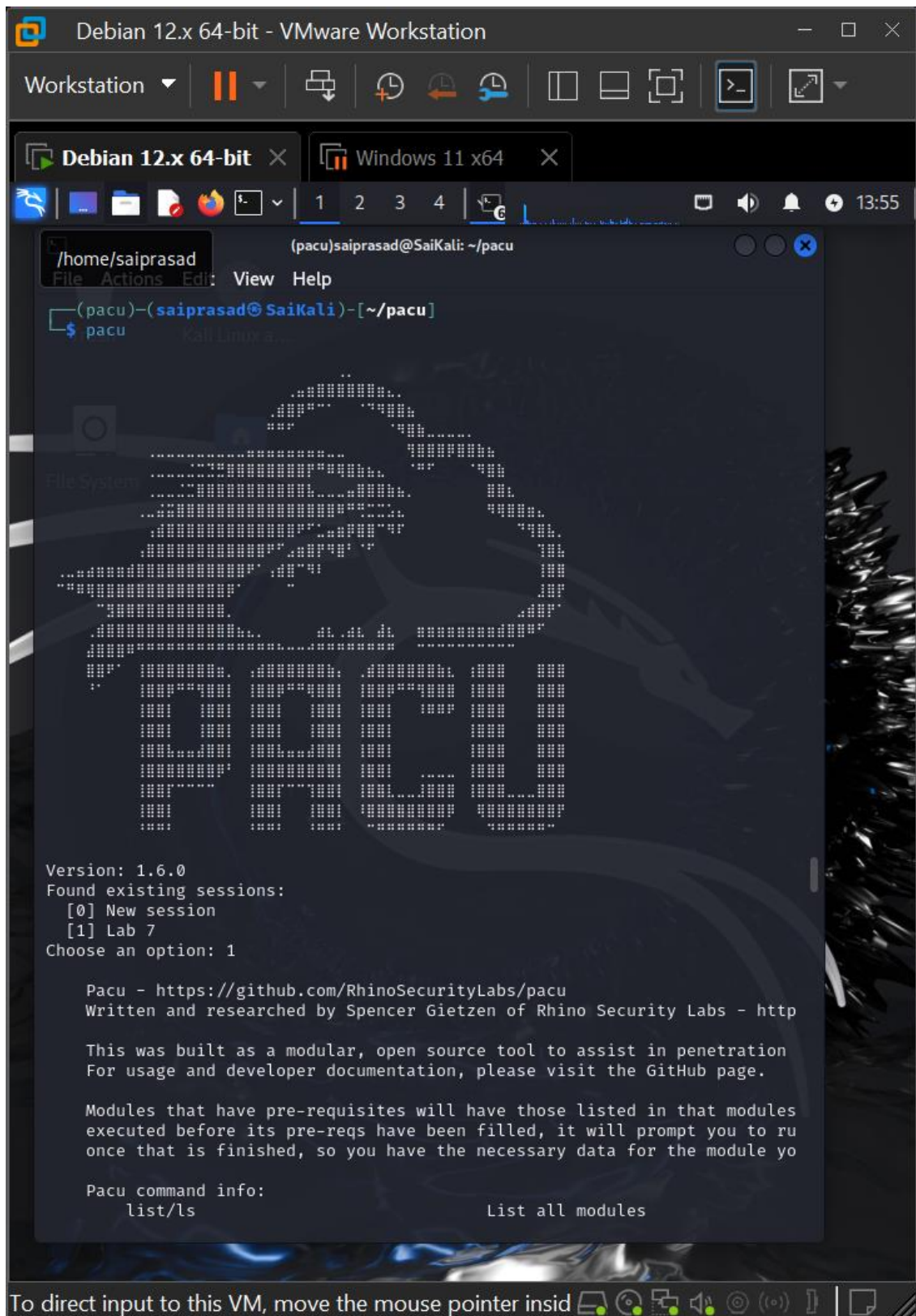
2. Install and configure Pacu on your system using the command **bash install.sh**.



```
Debian 12.x 64-bit - VMware Workstation
Workstation
Debian 12.x 64-bit x Windows 11 x64
(pacu)saiprasad@SaiKali: ~/pacu
File Actions Edit View Help
└─$ virtualenv -p python3 pacu
created virtual environment CPython3.11.9.final.0-64 in 415ms
creator CPython3Posix(dest=/home/saiprasad/pacu/pacu, clear=False, no_vcs
seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=b
e/saiprasad/.local/share/virtualenv)
added seed packages: pip=24.0, setuptools=68.1.2, wheel=0.43.0
activators BashActivator,CShellActivator,FishActivator,NushellActivator,P
(saiprasad@ SaiKali)~[~/pacu]
└─$ source pacu/bin/activate
(pacu)~(saiprasad@ SaiKali)~[~/pacu]
└─$ pip install -U pacu
Collecting pacu
  Using cached pacu-1.6.0-py3-none-any.whl.metadata (1.3 kB)
Collecting SQLAlchemy<1.4.0, ≥1.3.0 (from pacu)
  Using cached SQLAlchemy-1.3.24-cp311-cp311-linux_x86_64.whl
Collecting SQLAlchemy-Utils<0.38.0, ≥0.37.2 (from pacu)
  Using cached SQLAlchemy_Utils-0.37.9-py3-none-any.whl.metadata (4.3 kB)
Collecting awscli<2.0, ≥1.18 (from pacu)
  Using cached awscli-1.35.0-py3-none-any.whl.metadata (11 kB)
Collecting boto3<2.0, ≥1.16 (from pacu)
  Using cached boto3-1.35.34-py3-none-any.whl.metadata (6.6 kB)
Collecting botocore<2.0, ≥1.16 (from pacu)
  Using cached botocore-1.35.34-py3-none-any.whl.metadata (5.6 kB)
Collecting chalice<2.0.0, ≥1.27.3 (from pacu)
  Using cached chalice-1.31.2-py3-none-any.whl.metadata (8.9 kB)
Collecting dsnap<2.0.0, ≥1.0.0 (from pacu)
  Using cached dsnap-1.0.0-py3-none-any.whl.metadata (8.7 kB)
Collecting jq<2.0.0, ≥1.4.1 (from pacu)
  Downloading jq-1.8.0-cp311-cp311-manylinux_2_17_x86_64.manylinux2014_x86_
Collecting policyuniverse<2.0.0.0, ≥1.5.0.20220613 (from pacu)
  Using cached policyuniverse-1.5.1.20231109-py2.py3-none-any.whl.metadata
Collecting pycognito<2024.0.0, ≥2023.5.0 (from pacu)
  Using cached pycognito-2023.5.0-py3-none-any.whl.metadata (21 kB)
Collecting pyyaml<7.0.0, ≥6.0.1 (from pacu)
  Using cached PyYAML-6.0.2-cp311-cp311-manylinux_2_17_x86_64.manylinux2014
Collecting qrcode<8.0.0, ≥7.4.2 (from pacu)
  Downloading qrcode-7.4.2-py3-none-any.whl.metadata (17 kB)
Collecting requests<3.0.0, ≥2.25.1 (from pacu)
  Using cached requests-2.32.3-py3-none-any.whl.metadata (4.6 kB)
Collecting toml<0.11.0, ≥0.10.2 (from pacu)
  Using cached toml-0.10.2-py2.py3-none-any.whl.metadata (7.1 kB)
Collecting typing-extensions<5.0.0, ≥4.0.0 (from pacu)
  Using cached typing_extensions-4.12.2-py3-none-any.whl.metadata (3.0 kB)
Collecting urllib3<2.0.0, ≥1.26.4 (from pacu)
```

To direct input to this VM, move the mouse pointer inside

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.

```
Debian 12.x 64-bit - VMware Workstation
Workstation
Debian 12.x 64-bit x Windows 11 x64 x
(pacu)saiprasad@SaiKali: ~/pacu
File Actions Edit View Help
Pacu (Lab 7:None) > ls

[Category: ESCALATE]

  cfn__resource_injection
  iam__privesc_scan

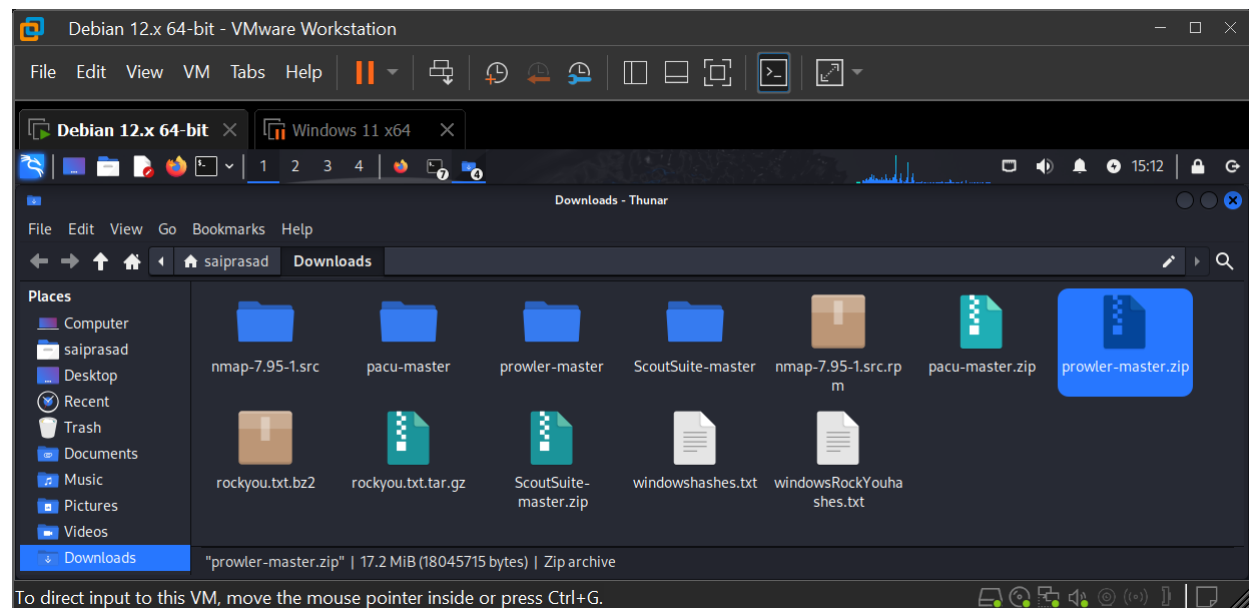
[Category: ENUM]

  acm__enum
  apigateway__enum
  aws__enum_account
  aws__enum_spend
  cloudformation__download_data
  codebuild__enum
  cognito__enum
  dynamodb__enum
  ebs__enum_volumes_snapshots
  ec2__check_termination_protection
  ec2__download_userdata
  ec2__enum
  ecr__enum
  ecs__enum
  ecs__enum_task_def
  eks__enum
  glue__enum
  guardduty__list_accounts
  guardduty__list_findings
  iam__bruteforce_permissions
  iam__decode_accesskey_id
  iam__detect_honeytokens
  iam__enum_action_query
  iam__enum_permissions
  iam__enum_users_roles_policies_groups
  iam__get_credential_report
  inspector__get_reports
  lambda__enum
  lightsail__enum
  mq__enum
  organizations__enum
  rds__enum
  rds__enum_snapshots
  route53__enum
  secrets__enum
  sns__enum
  systemsmanager__download_parameters
```

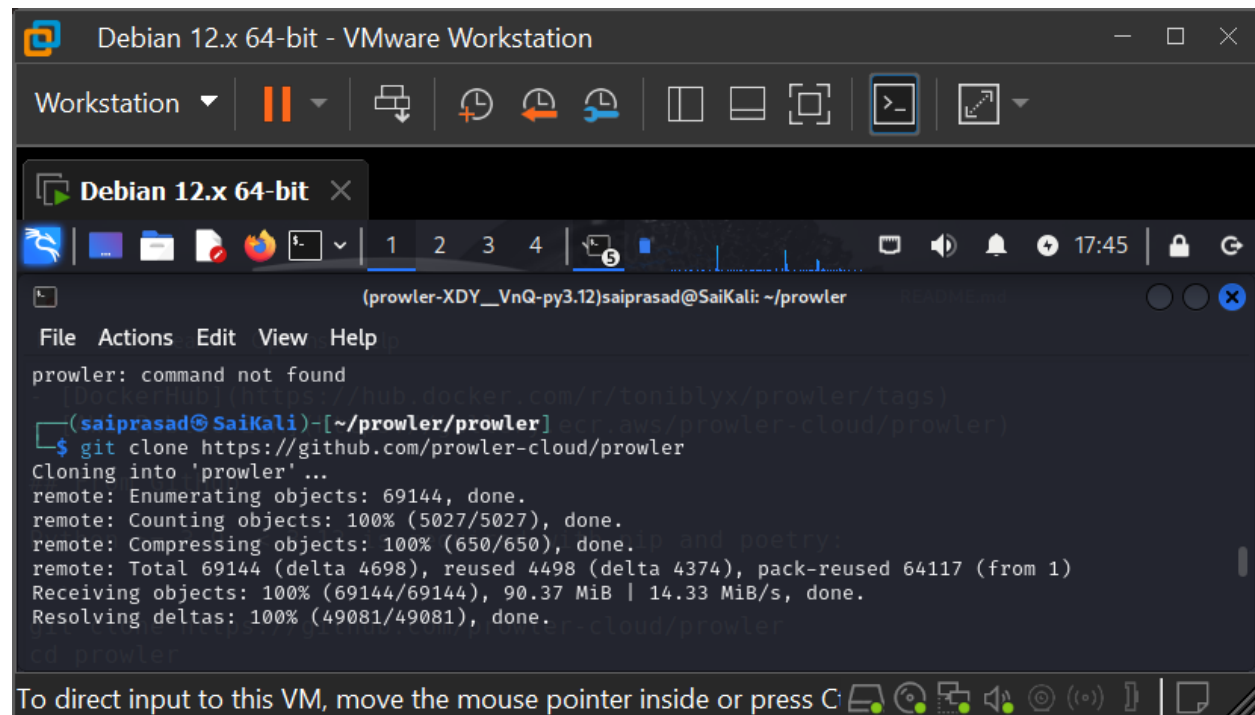
Activity 3: Scan an AWS account with Prowler (Optional).

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 permission 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. This is a fairly complex process, 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

(prowler-XDY__VnQ-py3.12)saiprasad@SaiKali 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 boto3 (1.35.29): Installing...
- Installing boto3 (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.



```
(prowler-XDY_VnQ-py3.12)~(saiprasad@SaiKali)~/prowler
File Actions Edit View Help
(prowler-XDY_VnQ-py3.12)~(saiprasad@SaiKali)~/prowler
$ cd ..
$ python prowler.py -v
Prowler 4.5.0 (You are running the latest version, yay!)
$ prowler aws

Prowler 4.5.0
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: MANUAL
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.

Debian 12.x 64-bit - VMware Workstation

File Edit View VM Tabs Help

Debian 12.x 64-bit

(prowler-XDY_VnQ-py3.12)saip

File Actions Edit View Help

- HTML: /home/saiprasad/prowler/output/prowler-output-590183811765-20241006173943.html

Compliance Status of AWS_ACCOUNT_SECURITY_ONBOARDING_AWS Framework:

36.67% (110) FAIL	0.67% (2) PASS	0.0% (0) MUTED
-------------------	----------------	----------------

Compliance Status of AWS_AUDIT_MANAGER_CONTROL_TOWER_GUARDRAILS_AWS Framework:

0.67% (2) FAIL	0.0% (0) PASS	0.0% (0) MUTED
----------------	---------------	----------------

Compliance Status of AWS_FOUNDATIONAL_SECURITY_BEST_PRACTICES_AWS Framework:

18.33% (55) FAIL	2.33% (7) PASS	0.0% (0) MUTED
------------------	----------------	----------------

Compliance Status of AWS_FOUNDATIONAL_TECHNICAL_REVIEW_AWS Framework:

15.67% (47) FAIL	8.33% (25) PASS	0.0% (0) MUTED
------------------	-----------------	----------------

Compliance Status of AWS_WELL_ARCHITECTED_FRAMEWORK_SECURITY_PILLAR_AWS Framework:

32.33% (97) FAIL	21.33% (64) PASS	0.0% (0) MUTED
------------------	------------------	----------------

Compliance Status of CIS_1.4_AWS Framework:

24.67% (74) FAIL	4.33% (13) PASS	0.0% (0) MUTED
------------------	-----------------	----------------

Compliance Status of CIS_1.5_AWS Framework:

30.33% (91) FAIL	4.33% (13) PASS	0.0% (0) MUTED
------------------	-----------------	----------------

Compliance Status of CIS_2.0_AWS Framework:

30.33% (91) FAIL	4.33% (13) PASS	0.0% (0) MUTED
------------------	-----------------	----------------

Compliance Status of CIS_3.0_AWS Framework:

30.33% (91) FAIL	4.33% (13) PASS	0.0% (0) MUTED
------------------	-----------------	----------------

Compliance Status of CISA_AWS Framework:

20.67% (62) FAIL	2.33% (7) PASS	0.0% (0) MUTED
------------------	----------------	----------------

Estado de Cumplimiento de ENS_RD2022_AWS:

35.33% (106) NO CUMPLE	10.33% (31) CUMPLE	0.0% (0) MUTED
------------------------	--------------------	----------------

Compliance Status of FEDRAMP_LOW_REVISION_4_AWS Framework:

20.33% (61) FAIL	2.67% (8) PASS	0.0% (0) MUTED
------------------	----------------	----------------

Compliance Status of FEDRAMP_MODERATE_REVISION_4_AWS Framework:

20.0% (60) FAIL	2.67% (8) PASS	0.0% (0) MUTED
-----------------	----------------	----------------

Compliance Status of FFIEC_AWS Framework:

--	--	--

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