



# Sprint 2 Presentation

AWS



# Table of Contents

Timeline

About AWS

Prowler

Scout Suite

DJ Hammer

Prowler Auditing

Scout Suite  
Challenges

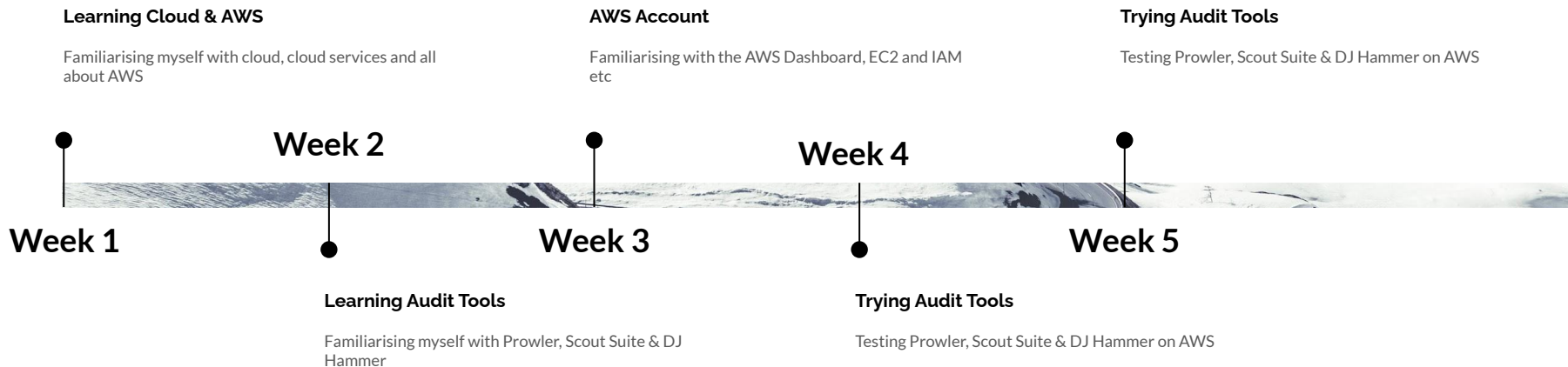
Resolution

DJ Hammer  
Challenges &  
Plans

Conclusion



# Timeline





# What is AWS?

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster.



# AWS



# AWS Cloud Services

1

Amazon Elastic Compute Cloud (EC2)

3

AWS Identity and Access Management  
(IAM)

2

Amazon S3 Bucket

4

Amazon RDS



# Amazon EC2

- Provides scalable computing capacity in the AWS cloud.
- Leveraging it enables organizations to develop & deploy applications faster
- Users can:
  - a. launch virtual servers
  - b. configure security & networking
  - c. manage cookies from an intuitive dashboard.





# Amazon IAM

- Can specify who or what can access services & resources in AWS
- Centrally manage fine-grained permissions
- Analyze access to refine permissions across AWS.







# Audit Tools





# Prowler

## O1

- Open Source Security Tool
- Works with AWS, Azure & Google Cloud security
- Used for best practices assessments, audits, incident response, continuous monitoring, hardening & forensics readiness
- Perform quick inventory check





# Scout Suite

## 02

- Enables security posture assessment of cloud environments
- Presents a clear view of the attack surface automatically
- Provides a point-in-time security-oriented view of the cloud account it was run in
- Written in Python





# DJ Hammer

## 03

- Designed to keep your Amazon Web Services landscape safe
- Detects typical AWS services vulnerabilities on a regular basis
- Writes information about discovered vulnerabilities to DynamoDB tables.



Dow Jones  
Hammer




Week 3


Create Instance


## Console Home [Info](#)


[Reset to default layout](#)[+ Add widgets](#)


⋮ Recently visited [Info](#) ⋮


Billing


EC2


CloudShell


S3


Directory Service

IAM

Key Management Service

WAF & Shield

AWS Firewall Manager

AWS Cost Explorer



## Week 3

### Instances (2) [Info](#)

[Connect](#)[Instance state ▼](#)[Actions ▼](#)[Launch instances](#)[1](#)[Name ▼](#)[Instance ID](#)[Instance state ▼](#)[Instance type ▼](#)[Status check](#)[Alarm status](#)[Availability](#)[myEC2instance](#)[i-004f837890d0ee76d](#)[⊖ Stopped ⓘ](#)[t2.micro](#)[-](#)[No alarms](#)[ap-s](#)[Linux](#)[i-074ab44a3c9de0fdf](#)[⊖ Stopped ⓘ](#)[t2.micro](#)[-](#)[No alarms](#)[ap-s](#)

Dropdown to start/stop instance



# Prowler







# Installation

Link: <https://docs.prowler.cloud/en/latest/>

## Step 1: aws configure

```
[cloudshell-user@ip-10-6-39-121 ~]$ aws configure
AWS Access Key ID [None]: AKIA37BTDS6T5T5A77SV
AWS Secret Access Key [None]: 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
Default region name [None]: ap-southeast-1
Default output format [None]:
[cloudshell-user@ip-10-6-39-121 ~]$
```

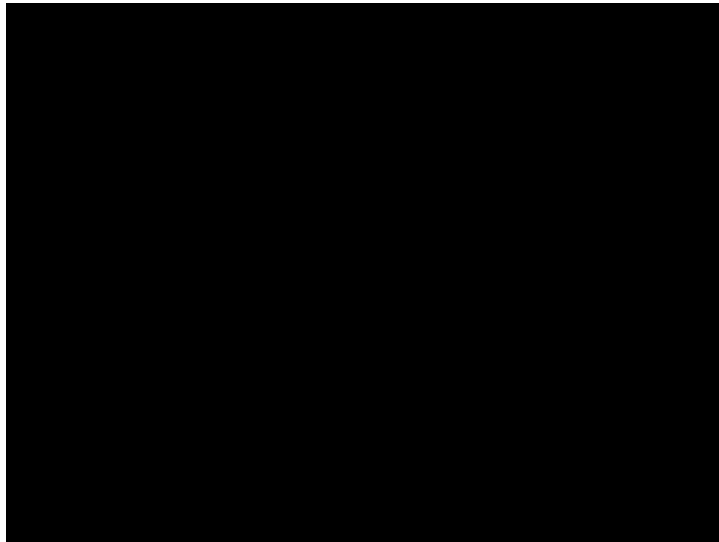
## Step 2: Install dependencies & Python

```
sudo yum -y install gcc openssl-devel bzip2-devel libffi-devel
wget https://www.python.org/ftp/python/3.9.16/Python-3.9.16.tgz
tar xzf Python-3.9.16.tgz
cd Python-3.9.16/
./configure --enable-optimizations
sudo make altinstall
python3.9 --version
cd
```





# Installing Dependences





# Installation

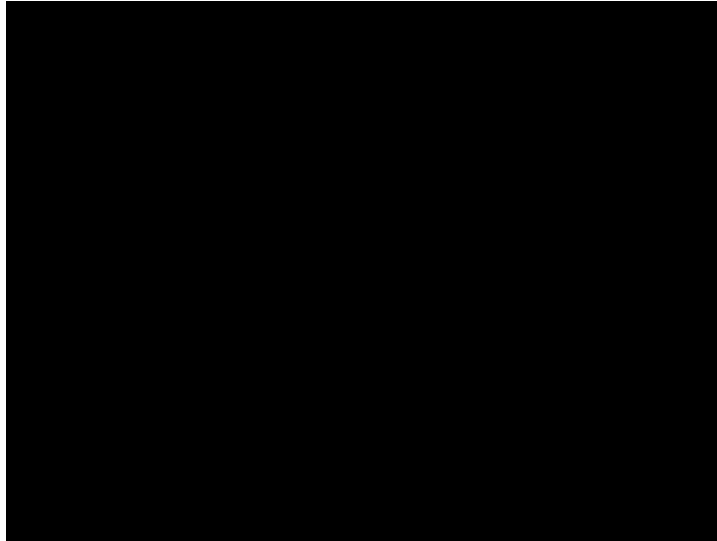
Link: <https://docs.prowler.cloud/en/latest/>

Step 3: Install prowler from pip

```
pip3.9 install prowler  
prowler -v
```

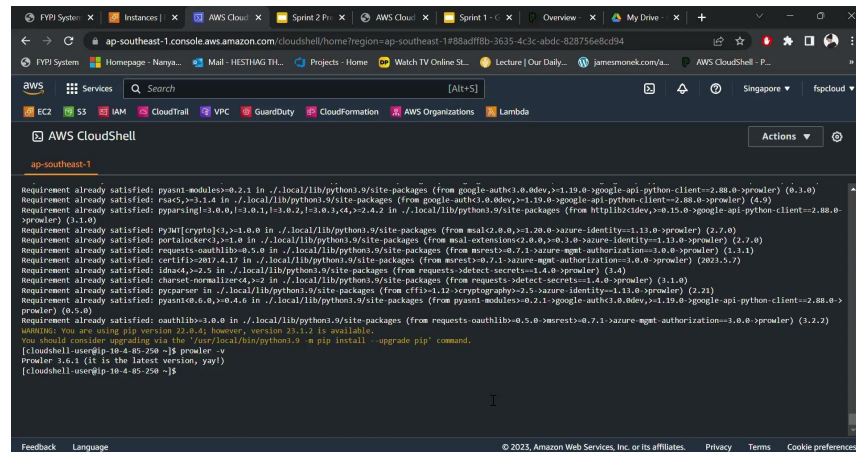


# Installing Prowler





# Launch Prowler



```
Requirement already satisfied: pyasn1-modules<0.2.1 in ./local/lib/python3.9/site-packages (from google-auth<3.0.0dev>=>1.19.0>google-api-python-client<2.88.0>prowler) (0.3.0)
Requirement already satisfied: rsa<5.0>=>3.1.4 in ./local/lib/python3.9/site-packages (from google-auth<3.0.0dev>=>1.19.0>google-api-python-client<2.88.0>prowler) (4.9)
Requirement already satisfied: pyyaml<3.0.0>=>1.0.0,1.3.0.2,1.3.0.3,4,>2.4.2 in ./local/lib/python3.9/site-packages (from httplib2<dev>=>0.15.0>google-api-python-client<2.88.0>prowler) (3.1.0)
Requirement already satisfied: pyjwt[crypto]<3.0>=>1.0.0 in ./local/lib/python3.9/site-packages (from msal<2.0.0>=>1.20.0>azure-identity<1.13.0>prowler) (2.7.0)
Requirement already satisfied: portalocker<3>=>1.0 in ./local/lib/python3.9/site-packages (from msal-extensions<2.0.0>=>0.3.0>azure-identity<1.13.0>prowler) (2.7.0)
Requirement already satisfied: requests-oidc<0.5.0> in ./local/lib/python3.9/site-packages (from msrest<0.7.1>azure-mgmt-authorization<3.0.0>prowler) (1.1.1)
Requirement already satisfied: certifi<2017.4.17 in ./local/lib/python3.9/site-packages (from msrest<0.7.1>azure-mgmt-authorization<3.0.0>prowler) (2023.7.2)
Requirement already satisfied: idna<4,>2.5 in ./local/lib/python3.9/site-packages (from requests<detect-secrets<3.4.0>prowler) (3.4)
Requirement already satisfied: charset-normalizer<2.2 in ./local/lib/python3.9/site-packages (from requests<detect-secrets<3.4.0>prowler) (3.1.0)
Requirement already satisfied: pyperclip in ./local/lib/python3.9/site-packages (from ftfpy<1.12.0>cryptograpy=>2.5>azure-identity<1.13.0>prowler) (2.21)
Requirement already satisfied: pyasn1<0.6.0>=>0.4.6 in ./local/lib/python3.9/site-packages (from pyasn1-modules<0.2.1>google-auth<3.0.0dev>=>1.19.0>google-api-python-client<2.88.0>prowler) (0.5.0)
Requirement already satisfied: oauthlib<3.0.0> in ./local/lib/python3.9/site-packages (from requests-oidc<0.5.0>msrest<0.7.1>azure-mgmt-authorization<3.0.0>prowler) (3.2.2)
WARNING: You are using pip version 22.0.4; however, version 23.1.2 is available.
You should consider upgrading via the '/usr/local/bin/python3.9 -m pip install --upgrade pip' command.
[cloudshell-user@ip-10-4-85-250 ~]$ prowler -v
prowler 3.0.1 (it is the latest version, yay!)
[cloudshell-user@ip-10-4-85-250 ~]$
```



### Overview Results:

Account 822593427367 Scan Results (severity columns are for fails only):

\* You only see here those services that contains resources.

```
- HTML: /home/cloudshell-user/output/prowler-output-822593427367-20230628074822.html
- JSON-OCFS: /home/cloudshell-user/output/prowler-output-822593427367-20230628074822.ocsf.json
- CSV: /home/cloudshell-user/output/prowler-output-822593427367-20230628074822.csv
- JSON: /home/cloudshell-user/output/prowler-output-822593427367-20230628074822.json
```



# Save Scans

## Tabs layout

New tab

Split into rows

Split into columns

## Files

**Download file**

Upload file

Restart AWS CloudShell

Delete AWS CloudShell home directory

## Download file



Download files from your AWS CloudShell to your local desktop. Folders are not supported.

### Individual file path

You can copy the file path from the command-line and paste it below.

`/home/cloudshell-user/output/prowler-output-822593427367-20230706042922.htr`

myfile.txt or /folder/myfile.txt.

Cancel

**Download**



# Scan Result

4  
7  
5

Filters Show 100 entries Search:

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags	Status Extended
PASS	medium	ec2	ap-southeast-1	ec2_instance_older_than_specific_days	Check EC2 Instances older than specific days.	i-004f837890d0ee76d	•Name=myEC2instance	EC2 Instance i-004f837890d0ee76d
PASS	medium	ec2	ap-southeast-1	ec2_instance_public_ip	Check for EC2 Instances with Public IP.	i-004f837890d0ee76d	•Name=myEC2instance	EC2 Instance i-004f837890d0ee76d
PASS	medium	ec2	ap-southeast-1	ec2_instance_internet_facing	Check for internet facing EC2 instances	i-004f837890d0ee76d	•Name=myEC2instance	EC2 Instance i-004f837890d0ee76d profile.



# Other commands

The screenshot shows the AWS CloudShell interface with a terminal window displaying a table of AWS services and their resource counts. The table has columns for service name, resource count, and several numerical columns. Below the table, there is a note about detailed results and a list of files in the current directory.

Service	Resource Count	Column 3	Column 4	Column 5	Column 6
aws:iam	1	0	0	0	0
aws:iam	1	0	0	0	0
aws:network-firewall	1	0	0	17	0
aws:resourceexplorer2	1	0	0	0	1
aws:s3	1	0	1	126	37
aws:sqs	2	0	0	0	0
aws:sns	1	0	0	1	0
aws:vpc	1	0	0	64	0

\* You only see here those services that contains resources.

Detailed results are in:

- HTML: /home/cloudshell-user/output/prowler-output-822593427367-20230707012525.html
- JSON: /home/cloudshell-user/output/prowler-output-822593427367-20230707012525.ocsf.json
- CSV: /home/cloudshell-user/output/prowler-output-822593427367-20230707012525.csv
- JSON: /home/cloudshell-user/output/prowler-output-822593427367-20230707012525.json

[cloudshell user@ip-10-4-02-237 ~]\$



# **prowler aws -M csv json json-asff html**

Detailed results are in:

- HTML: /home/cloudshell-user/output/prowler-output-822593427367-20230707013407.html
  - JSON-ASFF: /home/cloudshell-user/output/prowler-output-822593427367-20230707013407.asff.json
  - CSV: /home/cloudshell-user/output/prowler-output-822593427367-20230707013407.csv
  - JSON: /home/cloudshell-user/output/prowler-output-822593427367-20230707013407.json
- [cloudshell-user@ip-10-4-82-237 ~]\$



# prowler aws -M csv json json-asff html

6  
7  
5  
2  
0  
8

Filters Show 100 entries

Search:

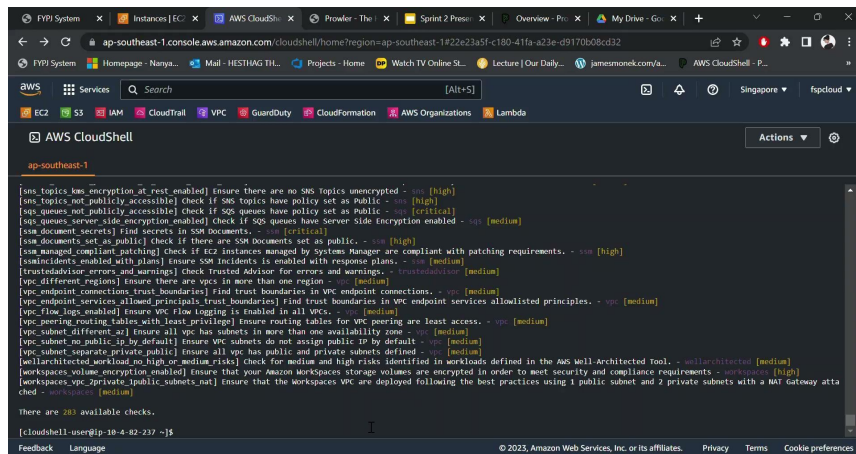
Filters Active - 0

Clear Filters Collapse All Show All

Status	Severity	Service Name	Region
FAIL 677	critical 83	account 3	ap-northeast-1 40
INFO 3	high 596	backup 2	ap-northeast-2 41
PASS 1188	low 60	cloudformation 8	ap-northeast-3 30
	medium 1129	cloudtrail 2	ap-south-1 30
		cloudwatch 622	ap-southeast-1 294
		ec2 733	ap-southeast-2 108

Check ID	Check Title	Resource ID	Resource Tags
----------	-------------	-------------	---------------

# prowler <provider> --list-checks



```
ap-south-east-1.console.aws.amazon.com/cloudshell/home?region=ap-south-east-1&22e23a5f-c180-41fa-a23e-d9170b08cd22

AWS CloudShell
ap-south-east-1

[aws_topics.kms_encryption_at_rest_enabled] Ensure there are no SMO topics unencrypted - aws [high]
[aws_topics_not_publicly_accessible] Check if SMO topics have policy set as Public - aws [high]
[smq_queues_not_publicly_accessible] Check if SQS queues have policy set as Public - aws [critical]
[smq_queues_server_side_encryption_enabled] Check if SQS queues have Server Side Encryption enabled - aws [medium]
[ssm_document_secrets] Find secrets in SSM Documents - aws [critical]
[ssm_documents_set_as_public] Check if there are SSM Documents set as public - aws [high]
[ssm_managed_compliant_patching] Check if EC2 instances managed by Systems Manager are compliant with patching requirements - aws [high]
[ssm_incidents_enabled_with_plans] Ensure SSM Incidents is enabled with response plans - aws [medium]
[trustedadvisor_errors_and_warnings] Check Trusted Advisor for errors and warnings - trustedadvisor [medium]
[vpc_different_regions] Ensure there are vpcs in more than one region - aws [medium]
[vpc_endpoint_connections_trust_boundaries] Find trust boundaries in VPC endpoint connections - aws [medium]
[vpc_endpoint_services_all_aws_principals_trust_boundaries] Find trust boundaries in VPC endpoint services allowedlist principles - aws [medium]
[vpc_flow_logs_enabled] Ensure VPC Flow logging is enabled in all VPCs - aws [medium]
[vpc_peering_routing_tables_with_least_privilege] Ensure routing tables for VPC peering are least access - aws [medium]
[vpc_subnet_different_availability_zones] Ensure all VPC has subnets in more than one availability zone - aws [medium]
[vpc_subnet_no_public_ip_by_default] Ensure VPC subnets do not assign public IP by default - aws [medium]
[vpc_subnet_separate_public_private_subnets] Ensure all vpc has public and private subnets defined - aws [medium]
[wellarchitected_workload_no_high_or_medium_risks] Check for medium and high risks identified in workloads defined in the AWS Well-Architected Tool - wellarchitected [medium]
[workspaces_volume_encryption_enabled] Ensure that your Amazon WorkSpaces storage volumes are encrypted in order to meet security and compliance requirements - workspaces [high]
[workspaces_vpc_private_public_subnets_nat] Ensure that the workspaces VPC are deployed following the best practices using 1 public subnet and 2 private subnets with a NAT Gateway attached - workspaces [medium]

There are 283 available checks.

[cloudshell-user@ip-10-4-82-217 ~]$
```





# Challenges



# Scout Suite

Link: <https://www.virtuesecurity.com/kb/scoutsuite-quickstart/>

- Faced some issues when installing Scout Suite such as “error: could not install packages due to an oserror: [errno 28] no space left on device”
- Have since resolved it & am working on proceeding further to test Scout Suite



# How I Resolved It


**Instances (1/2)** [Info](#)

 **Connect**

 Find instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	
<input type="checkbox"/>	myEC2instance	i-004f837890d0ee76d	 Running	
<input checked="" type="checkbox"/>	Linux	i-074ab44a3c9de0fdf	 Running	


**EC2 Instance Connect** | Session Manager | SSH client | EC2 serial console

**Instance ID**  
 i-074ab44a3c9de0fdf (Linux)

**Connection Type**

☒ **Connect using EC2 Instance Connect**  
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

☐ **Connect using EC2 Instance Connect Endpoint**  
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

**Public IP address**  
 13.229.150.27

**User name**  
Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ubuntu.

ubuntu





# How I Resolved It

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Fri Jul  7 03:32:47 UTC 2023

System load:  0.26318359375   Processes:            113
Usage of /:   84.3% of 7.57GB   Users logged in:      0
Memory usage: 24%             IPv4 address for eth0: 172.31.70.59
Swap usage:   0%

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

  https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Thu Jul  6 07:55:35 2023 from 3.0.5.35
ubuntu@ip-172-31-70-59:~$
```



# DJ Hammer

Link:

[https://dowjones.github.io/hammer/configureddeploy\\_overview.html#25-create-ec2-key-pair-for-dow-jones-hammer](https://dowjones.github.io/hammer/configureddeploy_overview.html#25-create-ec2-key-pair-for-dow-jones-hammer)

- Reading through the document & additional research
- Will be working on testing DJ Hammer next week



# Thank you.

