KPLABS Course

AWS Certified Cloud Practitioner 2021

Security Aspect

ISSUED BY

Zeal Vora

REPRESENTATIVE

instructors@kplabs.in

Section - Security Aspect

Module 1: Shared Responsibility Model

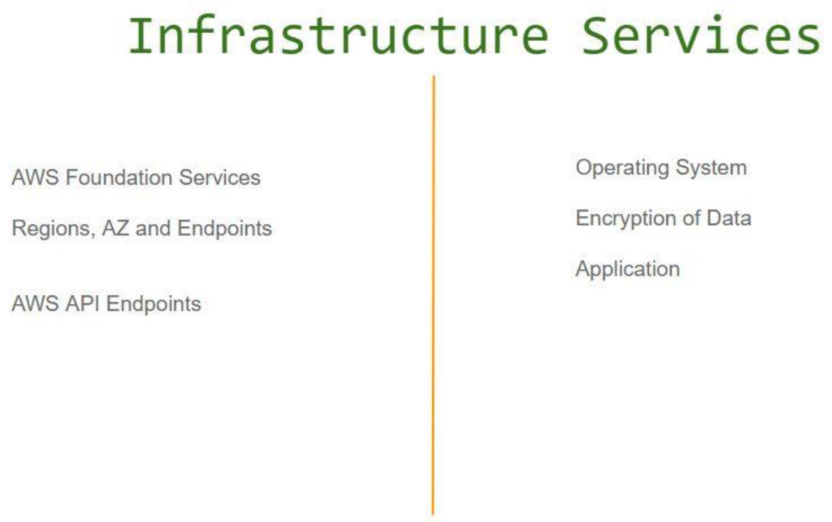
AWS has more than 140+ services available. Each of them is classified into:-

- Infrastructure Services
- Container Services
- Abstract Services

1.1 Infrastructure Services:

Infrastructure-as-Service are ones where organization outsources physical components of Data Center, such as storage, hardware, servers, and networking

Example: EC2, EBS, Autoscaling, VPC

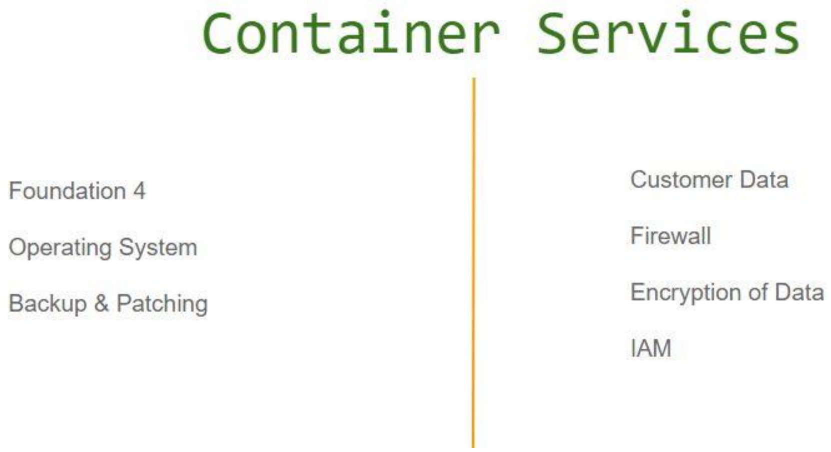


1.2 Container Services

Container Services are the one which runs on top AWS Managed EC2 instances.

Here the customers do not manage the OS or platform layer.

Example: RDS, Elastic MapReduce, Elastic BeanStalk.



Container Services

Foundation 4

Operating System

Backup & Patching

Customer Data

Firewall

Encryption of Data

IAM

1.3 Abstract Services

Abstract Services just provides the management layer to the users.

We can interact with these services via its Endpoints.

Here the customers do not manage the OS or platform layer.

Example: SES, SQS, SNS, S3

1.4 Security Responsibility is Shared

Security Responsibility will always be shared between you and your hosting provider.

The Hosting Provider has to ensure Security OF the Cloud
You have to ensure Security IN the Cloud.

With both the entities doing their job, we can then say that our systems are secured.

Module 2: Principle of Least Privilege

The principle of least privilege is the practice of limiting access to the minimal level that will allow normal functioning.

A user should only have access to the data, hardware that they need, to be able to perform their assigned duties.

The principle of Least privilege goes much deeper than expected. We can understand it with the following example and it’s associated pointers:

A software developer wants to access an application server to see the logs. You being a system administrator, you need to provide him access. How will you give access?

i) Create the user with the useradd command & share credentials.
ii) Create the user with useradd command & add him to sudoers list.

iii) Ask the developer on what log file he wants to access, verify if his access is justified and only allow him to have access to that specific log file and nothing else.

From the above three-pointers, the third pointer is very important.

Module 3: Identity and Access Management (IAM)

Enables you to control who can do what in your AWS account.

User, groups, roles, and permissions.

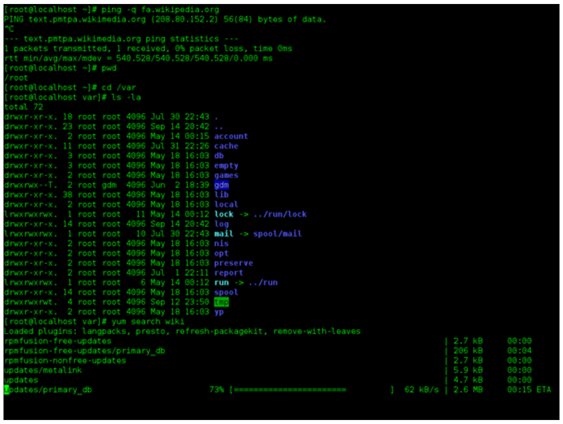
Security - Deny by default.

It is recommended to never use a ROOT user. Always create an IAM user for everyone and set MFA for an additional layer of security.

Module 4: AWS CLI

Command Line Interface (CLI) is a way of interacting with the system in the form of commands

It is considered as the fastest way of doing things in a repeated, automated fashion.



```
[root@localhost ~]# ping -q fa.wikipedia.org
PING text.pmtpa.wikimedia.org (208.80.152.2) 56(84) bytes of data.
^C
--- text.pmtpa.wikimedia.org ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 540.528/540.528/540.528/0.000 ms
[root@localhost ~]# pwd
/root
[root@localhost ~]# cd /var
[root@localhost var]# ls -la
total 72
drwxr-xr-x. 18 root root 4096 Jul 30 22:43 .
drwxr-xr-x. 23 root root 4096 Sep 14 20:42 ..
drwxr-xr-x.  2 root root 4096 May 14 00:15 account
drwxr-xr-x. 11 root root 4096 Jul 31 22:26 cache
drwxr-xr-x.  3 root root 4096 May 18 16:03 db
drwxr-xr-x.  3 root root 4096 May 18 16:03 empty
drwxr-xr-x.  2 root root 4096 May 18 16:03 games
drwxrwx--T.  2 root gdm  4096 Jun  2 18:39 gdm
drwxr-xr-x. 38 root root 4096 May 18 16:03 lib
drwxr-xr-x.  2 root root 4096 May 18 16:03 local
lrwxrwxrwx.  1 root root   11 May 14 00:12 lock -> ../run/lock
drwxr-xr-x. 14 root root 4096 Sep 14 20:42 log
lrwxrwxrwx.  1 root root   10 Jul 30 22:43 mail -> spool/mail
drwxr-xr-x.  2 root root 4096 May 18 16:03 nis
drwxr-xr-x.  2 root root 4096 May 18 16:03 opt
drwxr-xr-x.  2 root root 4096 May 18 16:03 preserve
drwxr-xr-x.  2 root root 4096 Jul  1 22:11 report
lrwxrwxrwx.  1 root root    6 May 14 00:12 run -> ../run
drwxr-xr-x. 14 root root 4096 May 18 16:03 spool
drwxrwxrwt.  4 root root 4096 Sep 12 23:50 tmp
drwxr-xr-x.  2 root root 4096 May 18 16:03 yp
[root@localhost var]# yum search wiki
Loaded plugins: langpacks, presto, refresh-packagekit, remove-with-leaves
rpmfusion-free-updates                                                          | 2.7 kB     00:00
rpmfusion-free-updates/primary_db                                               | 206 kB     00:04
rpmfusion-nonfree-updates                                                       | 2.7 kB     00:00
updates/metalink                                                                | 5.9 kB     00:00
updates                                                                         | 4.7 kB     00:00
updates/primary_db                     73% [=======================          ]  62 kB/s | 2.6 MB     00:15 ETA
```

<u>GUI vs CLI -</u>

- Create a directory called a TEST
- Inside it, create three text file named one.txt, second.txt and third.txt
- The contents in each one of them would be “this is kplabs demo”
- The permission of all these files should be 600

The above use-case can be automated via CLI and can be repeated hundreds of times with just a click of a button. Doing things GUI way will take more time.

AWS CLI is used for managing AWS resources from the terminal.

It makes room for automation & makes things much faster.

To start interacting with AWS resources using CLI, you will need the following things:

- Access / Secret Key of ROOT or an IAM user.
- AWS CLI Package installed.
- Configure AWS CLI package with “aws configure” command.

Module 5: IAM Role

IAM Role contains a set of policies and any entity assuming that role will be able to have permissions mentioned in the role.

A role can be used by :

- An IAM user

- A web service offered by the AWS such as EC2
- An external user authenticated by external IdP service compatible with SAML etc.

EC2 ReadOnly
S3 ReadOnly
EC2 ReadOnly
S3 ReadOnly

Module 6: Compliance

There is a Regulatory Compliance program formed either by Governments or an independent body that defines a set of policies and procedures that an organization must follow.

For example:-

PCI DSS	(PCI SSC - VISA, Master, JCB, AE)
HIPAA	(US Government)
RBI PSS	(Reserve Bank of India)

The organization needs to be compliant with one the compliance depending on their Business.

For example:-

PCI DSS	→	ORG that deals with storing, processing or transmitting CHD.
HIPAA	→	ORG that deals with health care data.
RBI PSS	→	ORG that deals with Digital Wallets in India

Failure to comply can lead to legal actions and major penalties.

All of this compliance is very much related to the “Security” of the information.

It means a lot to us as a “ Security Professional”.

A lot of organization now has “Compliance Officer” and they hire Security Professionals whose main aim is to help the organization conform to various regulatory compliance.

PCi Security Standards Council®

Module 7: AWS Artifact

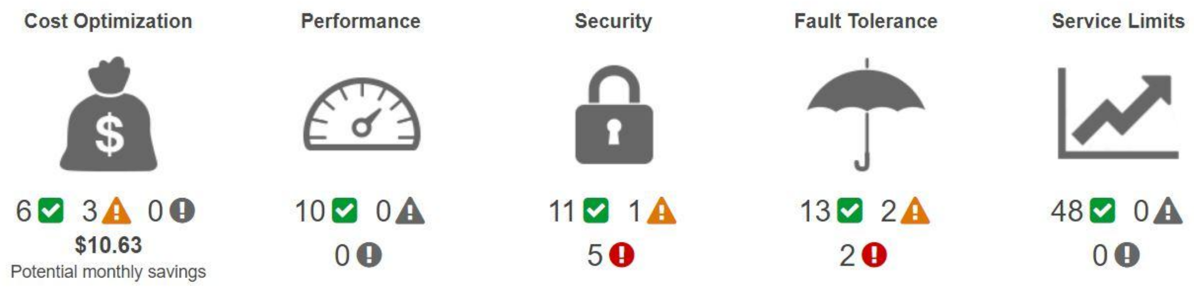
The AWS Artifact portal provides on-demand access to AWS' security and compliance documents, also known as audit artifacts.

Lots of AWS services are compliant against various compliance like PCI DSS, HIPAA and others.

If the organization is using certain AWS services, then the auditor will ask the organization to show a certificate that the service is compliant.

Module 8: AWS Trusted Advisor

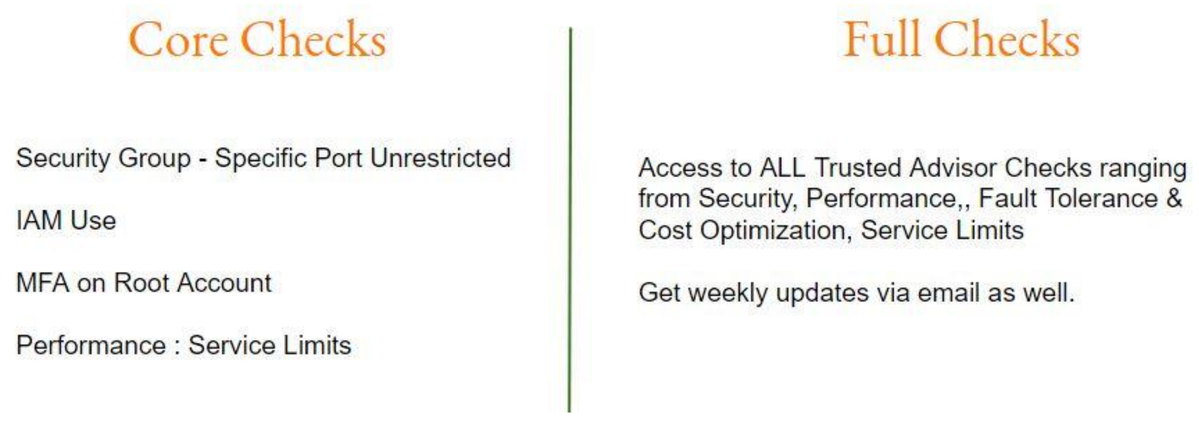
AWS Trusted Advisor analyzes your AWS environment and provides best practice recommendations in five major categories:



There are 2 types of checks available depending on your subscription:-

i) Core Checks & Recommendations

ii) Full Trusted Advisory Benefits



Core Checks

Security Group - Specific Port Unrestricted

IAM Use

MFA on Root Account

Performance : Service Limits

Full Checks

Access to ALL Trusted Advisor Checks ranging from Security, Performance,, Fault Tolerance & Cost Optimization, Service Limits

Get weekly updates via email as well.

Module 9: AWS CloudTrail

There is MUST need for organizations to record the activities that happen within your Infrastructure as well as in your Servers.

Example Auditor Question:-
  Show me what did Anne did on the 3rd of January 2017 between 10 AM to 2 PM.

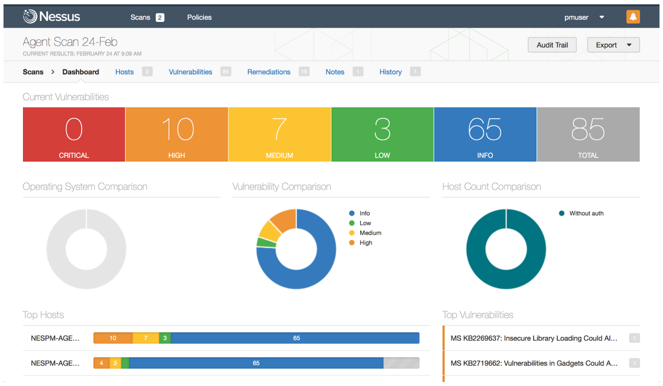
User	Action	Time
James	Logged In	3:50 PM
Anne	Modified SG	7:30 PM
Susan	New EC2	11:00 PM

AWS CloudTrail is an auditing service and actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.

Module 10: AWS Inspector

WS Inspector is similar to a vulnerability scanner that will scan the system for specific assessment rules and provide the results.

It relies on the agent installed on the server to scan the server.
It is very similar to industry-standard vulnerability scanners like Nessus.



MS KB2269637: Insecure Library Loading Could Al... 1

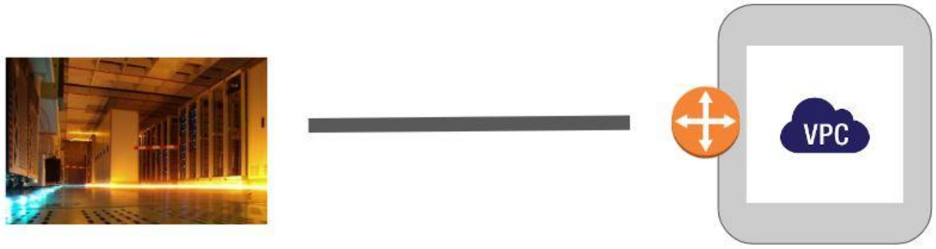
MS KB2719662: Vulnerabilities in Gadgets Could A... 1

AWS Inspector has certain pre-defined templates based on which we can scan.

- CVE (Common Vulnerabilities & Exposure)
- CIS Benchmarks on OS Security
- Security Best Practices
- Runtime Behaviour Analysis

Module 11: Direct Connect

AWS Direct connect let's customers establish a dedicated direct network connection between the client's network and one of the direct connect locations.



Benefits of Direct Connect:

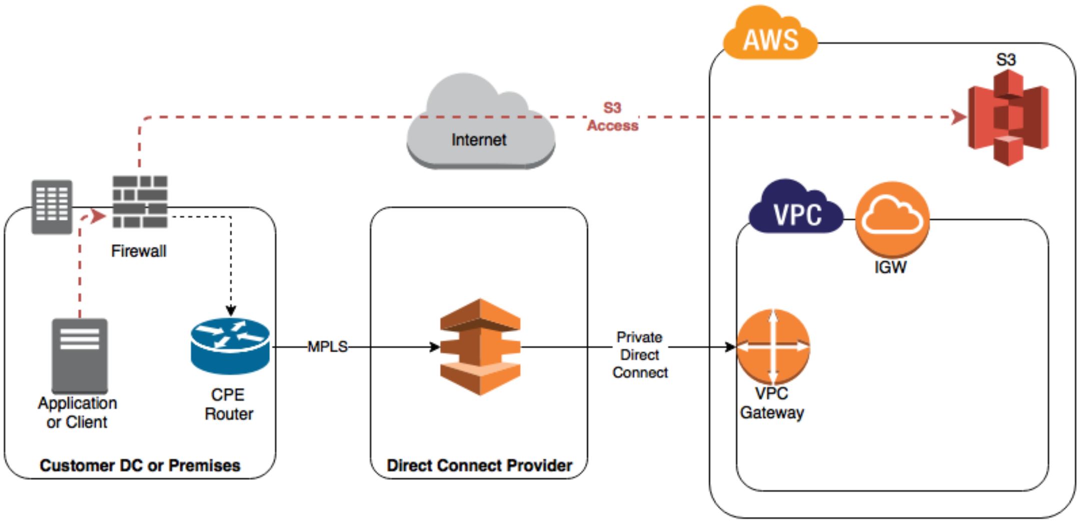
Having a direct connection between the customer's data center to AWS brings a tremendous amount of benefits, some of them includes:

i) Consistent Network Performance:

ii) Reduces our bandwidth costs

iii) Private connectivity to our AWS VPC

The architecture of Direct Connect connection can be described with the following diagram:

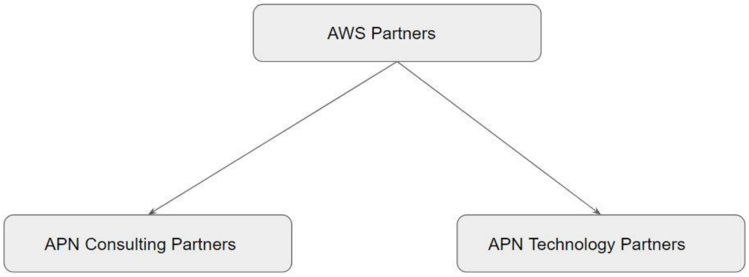


Module 12: AWS Partner Network (APN)

AWS Partner Network (APN) is a group of external vendors that have received an endorsement from AWS regarding their expertise in building and implementing solutions for AWS.

<u>Let's understand with an example:</u>

- Team of 5 people are very good into the security aspect of AWS.
- They have decided to create a company for consulting organizations to secure their resources.
- They registered to become APN



12.1 APN Consulting Partner

APN Consulting Partners are professional services firms that help customers of all types and sizes design, architect, build, migrate, and manage their workloads and applications on AWS, accelerating their journey to the cloud.

Let’s understand with an example:

- Small Corp has all their servers in the datacenter.
- They want to migrate to AWS.
- They don’t yet have an expert who can guide them in this process.
- Small Corp can opt for services from APN Consulting Partner.

12.2 APN Technology Partner

APN Technology Partner refers to organizations that are developing their own products/services that they will deploy on top of AWS to sell it to the customers.

Example:

Trend Micro is one of the APN Technology partners who have their own solution related to Anti-Virus, IPS and others.

aws partner network

Select
Technology
Partner

Module 13: Dealing with Security Breach AWS

Security Breach can happen at various levels.

Some of the examples can be found below:

- AWS Access/Secret Keys are leaked.
- EC2 instance is hacked.
- S3 buckets data is leaked (improper configurations)

Security Breaches are fairly common in organizations.

There are certain actions that customers can taken in-case of security breach:

- Change your AWS account root user password.

- Respond to any notifications you received from AWS Support.

- Rotate and delete all root and AWS Identity and Access Management (IAM) access keys.

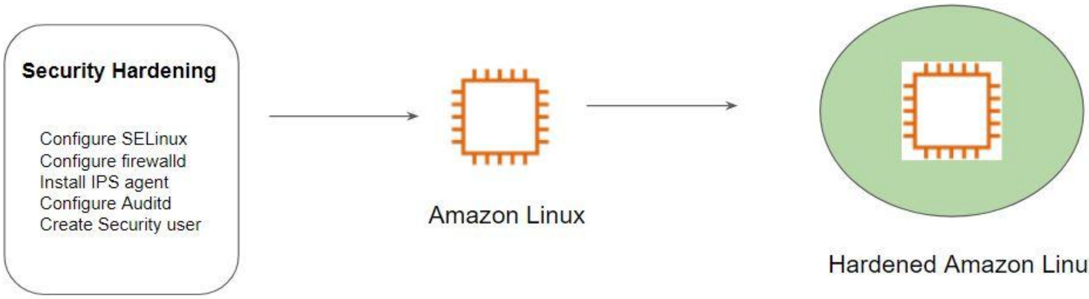
- Delete potentially compromised IAM users, and change the password for all other IAM users.

- Delete any resources on your account you didn't create, such as EC2 instances and AMIs, EBS volumes and snapshots, and IAM users.

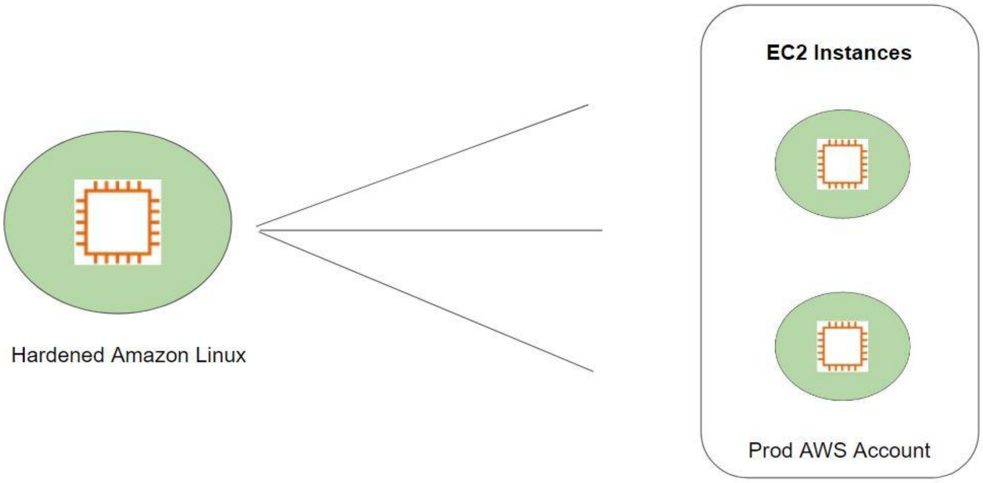
Module 14: Amazon Machine Image (AMI)

Amazon Machine Image (AMI) is the master image from which new EC2 instances can be launched.

Let’s understand with an example:



The architecture of Hardened AMI Deployment:

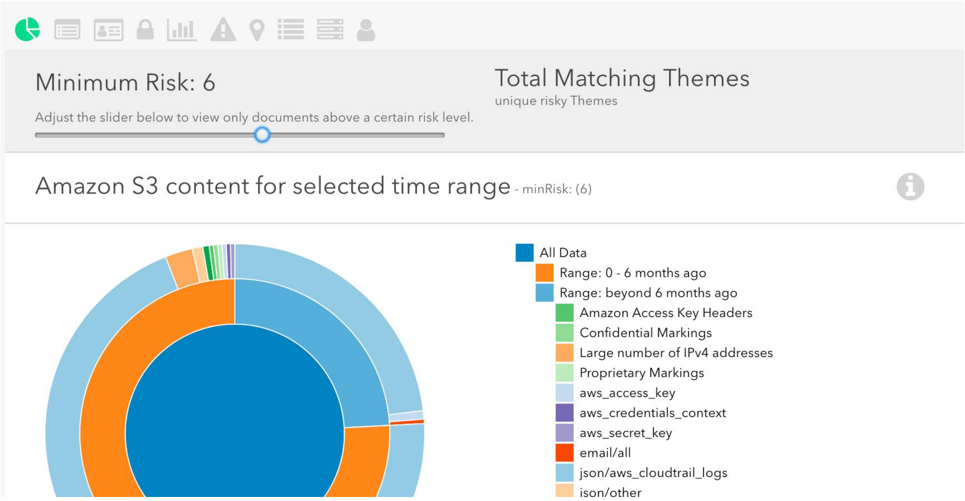


Module 15: AWS Macie

AWS Macie, a new security service that makes use of machine learning to identify and protect sensitive data stored in AWS from breaches, data leaks, and unauthorized access

Macie can automatically discover as well as classify the data post which assigns them a business value and monitors them to detect any suspicious activity based on access patterns.

S3 might contain sensitive information like PII data, database backups, SSL private keys, and various others.



Minimum Risk: 6

Adjust the slider below to view only documents above a certain risk level.

Total Matching Themes

unique risky Themes

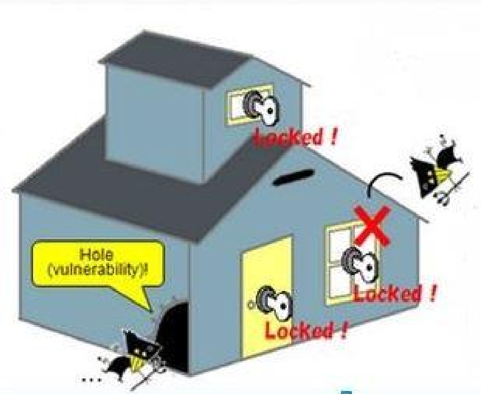
Amazon S3 content for selected time range - minRisk: (6)

Module 16: Vulnerability, Exploit, Payload

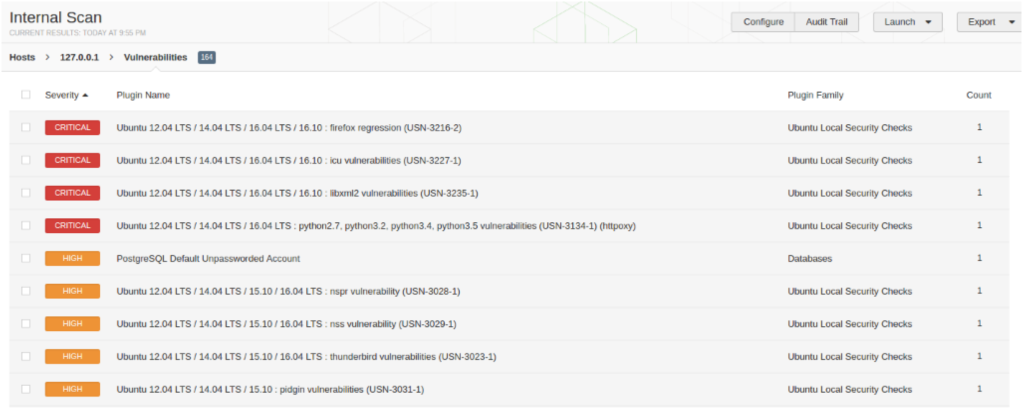
Vulnerability:- Bad Software Code

Exploit- Program that exploits code to get inside.

Payload:- Stealing Data, Ransomware, etc



Scan Results of Vulnerability Scanners:



Internal Scan

CURRENT RESULTS: TODAY AT 9:55 PM

Hosts › 127.0.0.1 › Vulnerabilities 164

□	Severity ▴	Plugin Name	Plugin Family	Count
□	CRITICAL	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : firefox regression (USN-3216-2)	Ubuntu Local Security Checks	1
□	CRITICAL	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : icu vulnerabilities (USN-3227-1)	Ubuntu Local Security Checks	1
□	CRITICAL	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS / 16.10 : libxml2 vulnerabilities (USN-3235-1)	Ubuntu Local Security Checks	1
□	CRITICAL	Ubuntu 12.04 LTS / 14.04 LTS / 16.04 LTS : python2.7, python3.2, python3.4, python3.5 vulnerabilities (USN-3134-1) (httpoxy)	Ubuntu Local Security Checks	1
□	HIGH	PostgreSQL Default Unpassworded Account	Databases	1
□	HIGH	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : nspr vulnerability (USN-3028-1)	Ubuntu Local Security Checks	1
□	HIGH	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : nss vulnerability (USN-3029-1)	Ubuntu Local Security Checks	1
□	HIGH	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 / 16.04 LTS : thunderbird vulnerabilities (USN-3023-1)	Ubuntu Local Security Checks	1
□	HIGH	Ubuntu 12.04 LTS / 14.04 LTS / 15.10 : pidgin vulnerabilities (USN-3031-1)	Ubuntu Local Security Checks	1

Module 17: AWS Inspector

AWS Inspector is similar to a vulnerability scanner that will scan the system for specific assessment rules and provide the results.

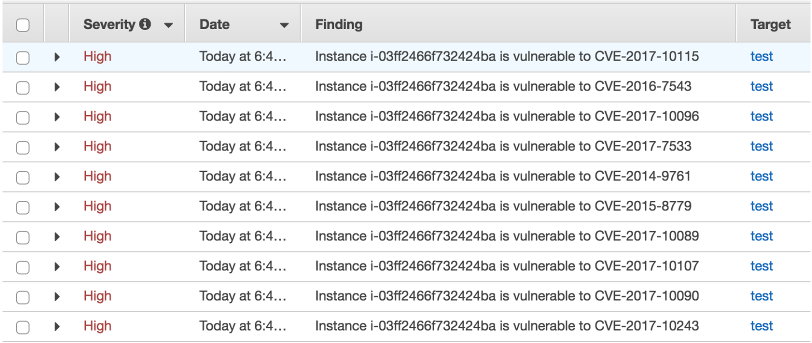
It relies on the agent installed on the server to scan the server.

AWS Inspector has certain pre-defined templates based on which we can scan.

- CVE (Common Vulnerabilities & Exposure)
- CIS Benchmarks
- Security Best Practices
- Network Reachability

i) CVE:

As the name suggests, this rule will scan for all the packages in the OS to see if there are any vulnerabilities associated with the version of packages installed.



□		Severity	Date	Finding	Target
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2017-10115	test
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2016-7543	test
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2017-10096	test
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2017-7533	test
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2014-9761	test
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2015-8779	test
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2017-10089	test
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2017-10107	test
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2017-10090	test
□	▸	High	Today at 6:4…	Instance i-03ff2466f732424ba is vulnerable to CVE-2017-10243	test

ii) CIS Benchmarks

This rule will check the OS against the CIS benchmarks to verify whether the server is following all the best practices mentioned in the CIS Benchmarks.

CIS® Center for Internet Security®

iii) Security Best Practices

This is a set of certain rules which the Inspector will check against and report.

- Disable Root Login via SSH
- Support SSH V2 only.
- Disable Password Authentication via SSH
- Configure maximum password age and minimum length.
- Configuring password complexity.
- Configure permissions for system directories.

iv) Network Reachability:

Shows findings of the ports that are reachable from the internet through an internet gateway

It can help if ports are misconfigured at the security group level.

AWS Inspector Agent is not required for these scans.

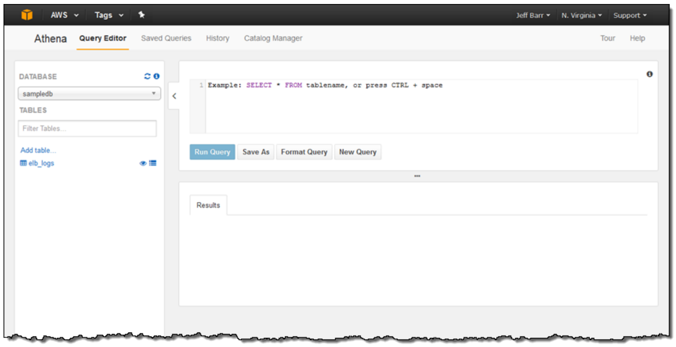
Module 18: AWS Athena

AWS Athena is a service that allows us to analyze various log files from S3 using standard SQL

Let's understand it with an example:

We have CloudTrail logs in AWS S3 and you want to see who has logged in, in the past 3 days.

- Create EC2 instances.
- Deploy monitoring stack like Splunk, ELK or others.
- Add the data source from S3 to import CloudTrail logs.
- Begin Analyzing.



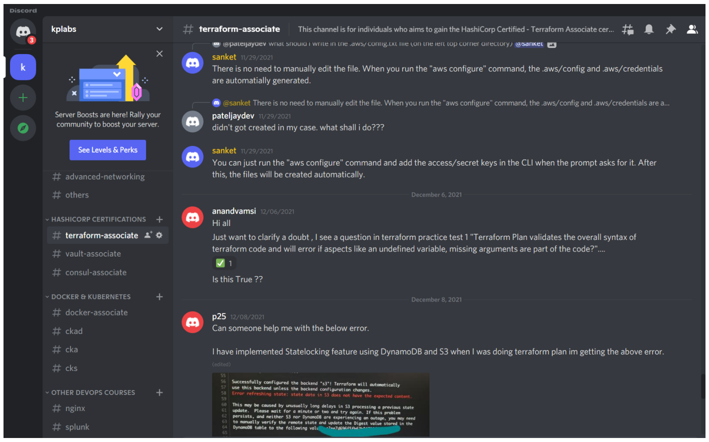
```
Example: SELECT * FROM tablename, or press CTRL + space
```

Join Our Discord Community

We invite you to join our Discord community, where you can interact with our support team for any course-based technical queries and connect with other students who are doing the same course.

Joining URL:

http://kplabs.in/chat



This channel is for individuals who aims to gain the HashiCorp Certified - Terraform Associate cer...

@pateljaydev what should i write in the .aws/config.txt file (on the left top corner directory) @sanket

sanket 11/29/2021
There is no need to manually edit the file. When you run the "aws configure" command, the .aws/config and .aws/credentials are automatially generated.

@sanket There is no need to manually edit the file. When you run the "aws configure" command, the .aws/config and .aws/credentials are a...

pateljaydev 11/29/2021
didn't got created in my case. what shall i do???

sanket 11/29/2021
You can just run the "aws configure" command and add the access/secret keys in the CLI when the prompt asks for it. After this, the files will be created automatically.

December 6, 2021

anandvamsi 12/06/2021
Hi all

Just want to clarify a doubt , I see a question in terraform practice test 1 "Terraform Plan validates the overall syntax of terraform code and will error if aspects like an undefined variable, missing arguments are part of the code?"....

✅ 1

Is this True ??

December 8, 2021

p25 12/08/2021
Can someone help me with the below error.

I have implemented Statelocking feature using DynamoDB and S3 when I was doing terraform plan im getting the above error.
(edited)

```
Successfully configured the backend "s3"! Terraform will automatically
use this backend unless the backend configuration changes.
Error refreshing state: state data in S3 does not have the expected content.

This may be caused by unusually long delays in S3 processing a previous state
update.  Please wait for a minute or two and try again. If this problem
persists, and neither S3 nor DynamoDB are experiencing an outage, you may need
to manually verify the remote state and update the Digest value stored in the
DynamoDB table to the following valu[redacted]
```