CWL
CyberWarFare Labs

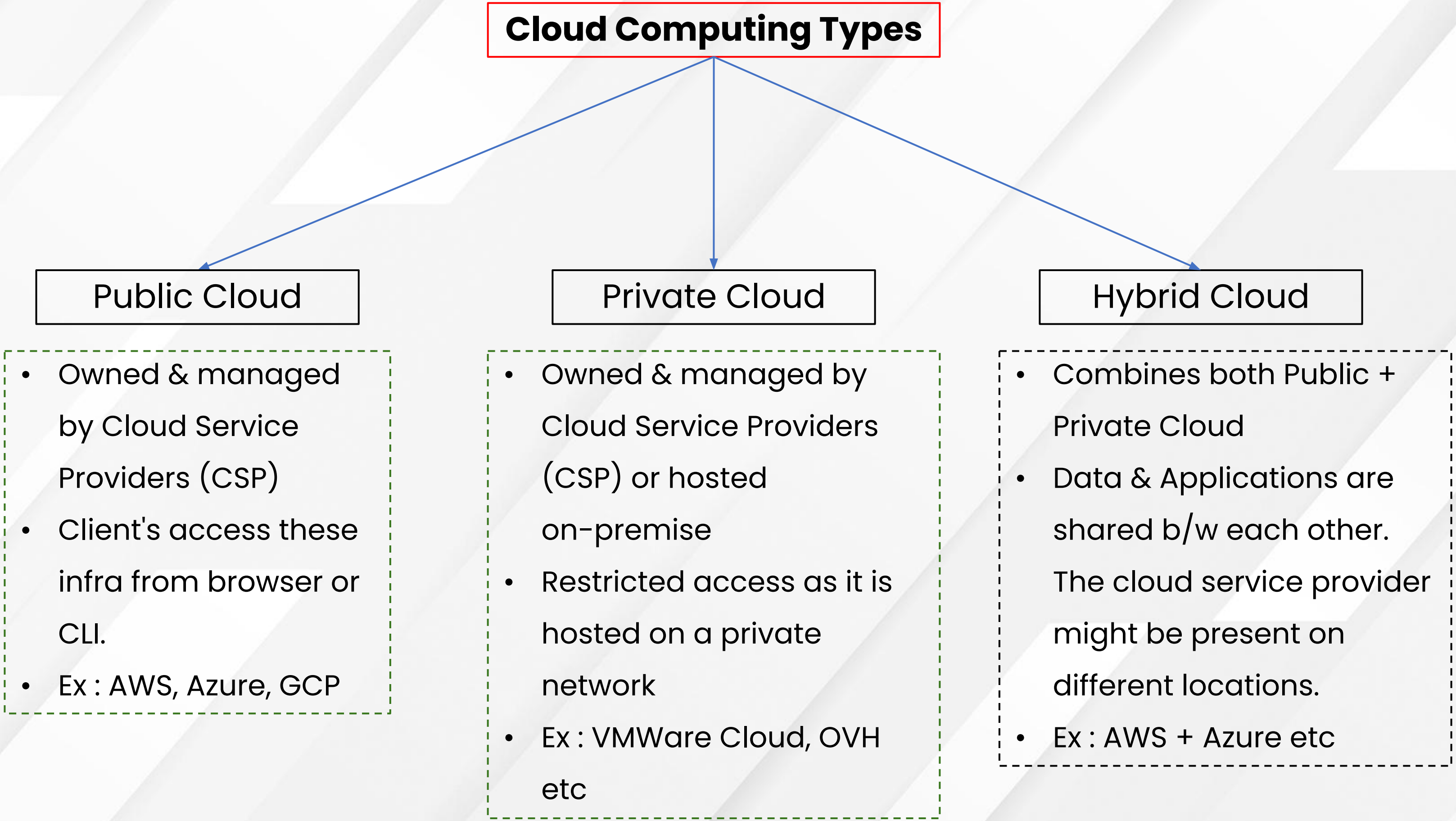
CLOUD PENETRATION TESTING
MODULE - 6

6. Cloud Basics & Penetration Testing

Cloud Basics

- Cloud computing refers to on-demand delivery and utilization of computing resources like servers, software, networking, databases etc.
- Companies have big data centers located at various regions of country which is offered as solutions to the clients
- It follows pay as you go model, which means running your infrastructure on their premise on rental basis

- Currently, cloud services are offered by leading vendors like:



Cloud Computing Types

Public Cloud

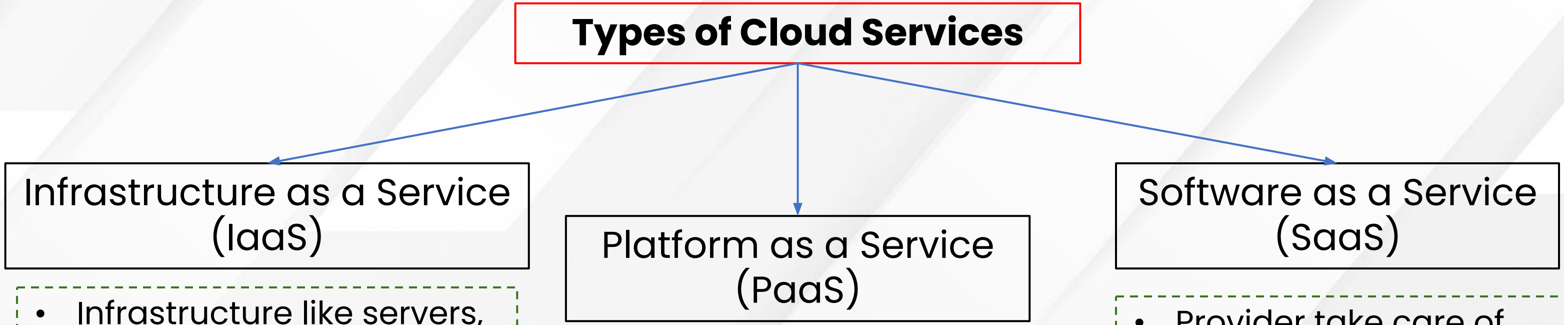
- Owned & managed by Cloud Service Providers (CSP)
- Client's access these infra from browser or CLI.
- Ex : AWS, Azure, GCP

Private Cloud

- Owned & managed by Cloud Service Providers (CSP) or hosted on-premise
- Restricted access as it is hosted on a private network
- Ex : VMWare Cloud, OVH etc

Hybrid Cloud

- Combines both Public + Private Cloud
- Data & Applications are shared b/w each other. The cloud service provider might be present on different locations.
- Ex : AWS + Azure etc



Types of Cloud Services

Infrastructure as a Service (IaaS)

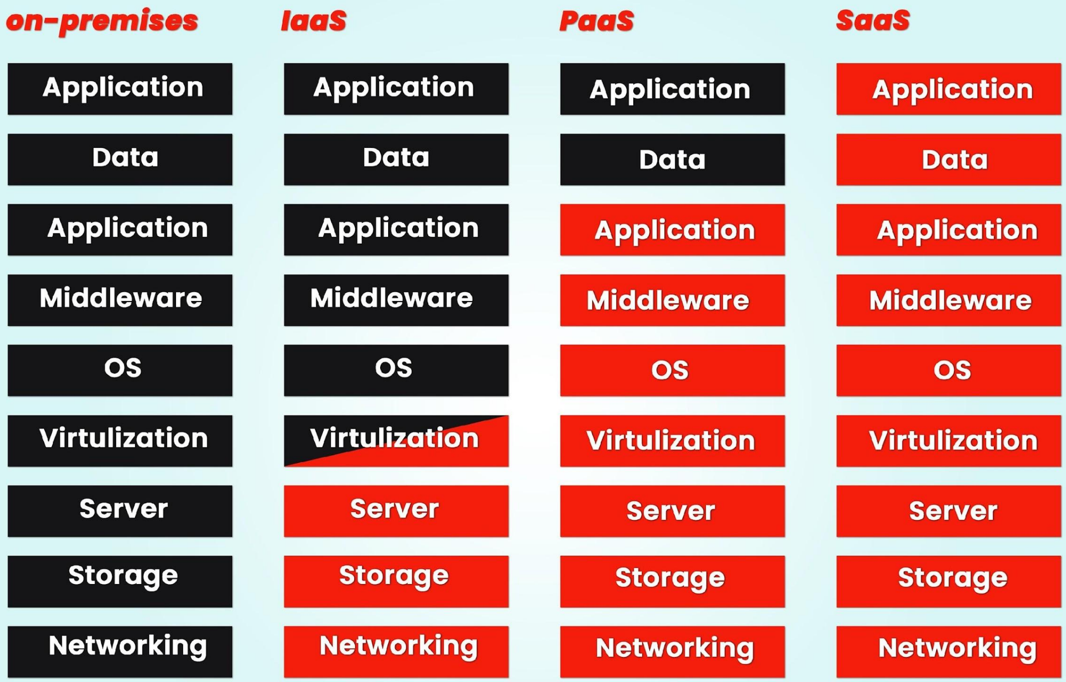
- Infrastructure like servers, VM etc are managed by the providers & can be used on-demand
- Compute, storage, networking & virtualization etc are provided.
- As it is managed, there is no requirement of maintaining our infra.
- Ex : AWS

Platform as a Service (PaaS)

- Platform are provided by the providers to build, run & manage applications etc
- Storage, networking, tools, OS all are managed by the providers
- Ex : Azure

Software as a Service (SaaS)

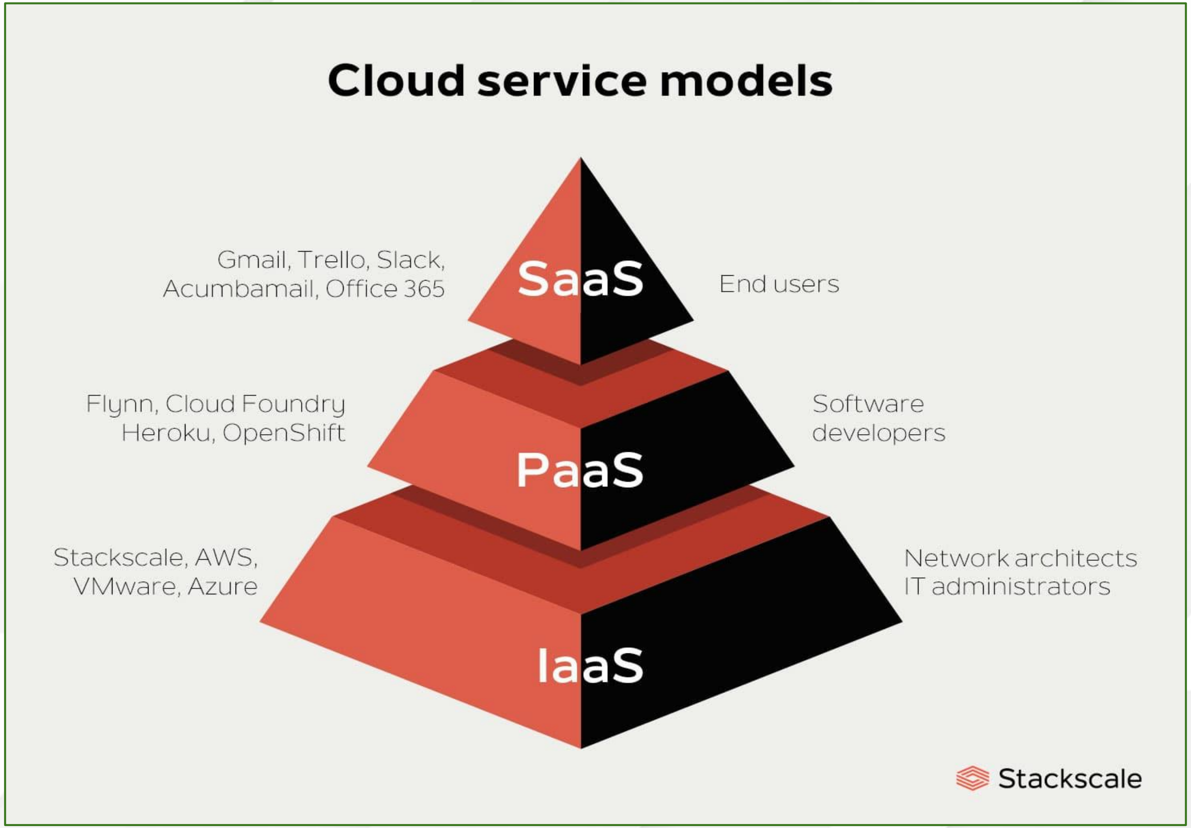
- Provider take care of entire IT application stack
- From H/W to Application itself.
- Ex : Gmail



on-premises	IaaS	PaaS	SaaS
⬛ Application	⬛ Application	⬛ Application	🟥 Application
⬛ Data	⬛ Data	⬛ Data	🟥 Data
⬛ Application	⬛ Application	🟥 Application	🟥 Application
⬛ Middleware	⬛ Middleware	🟥 Middleware	🟥 Middleware
⬛ OS	⬛ OS	🟥 OS	🟥 OS
⬛ Virtulization	⬛🟥 Virtulization	🟥 Virtulization	🟥 Virtulization
⬛ Server	🟥 Server	🟥 Server	🟥 Server
⬛ Storage	🟥 Storage	🟥 Storage	🟥 Storage
⬛ Networking	🟥 Networking	🟥 Networking	🟥 Networking

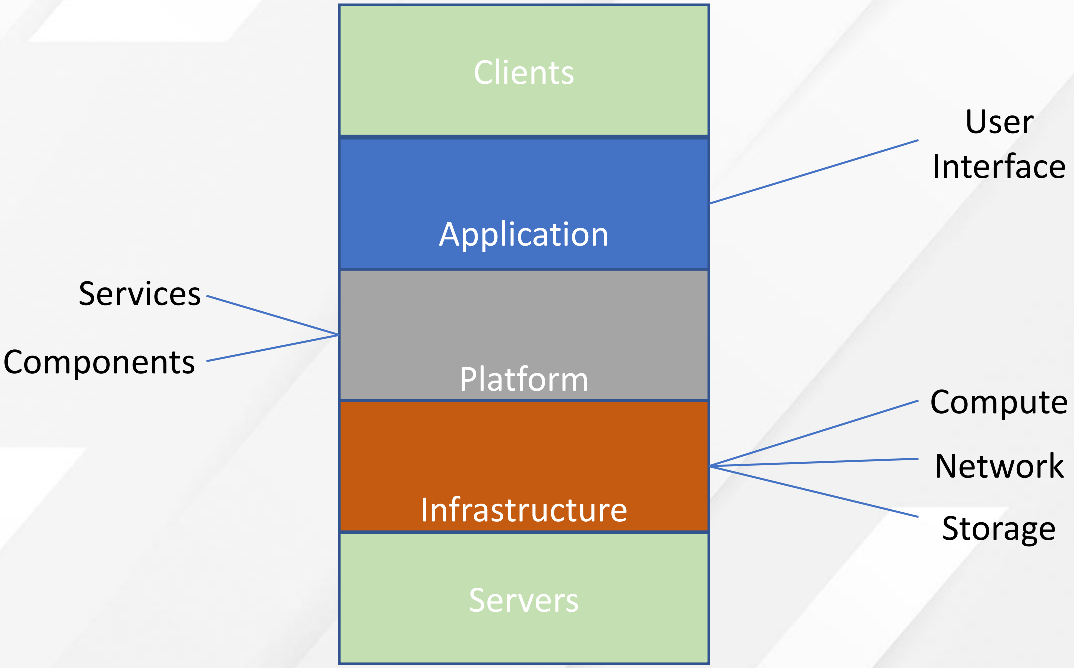
⬛ Managed by your team

🟥 Managed by a provider

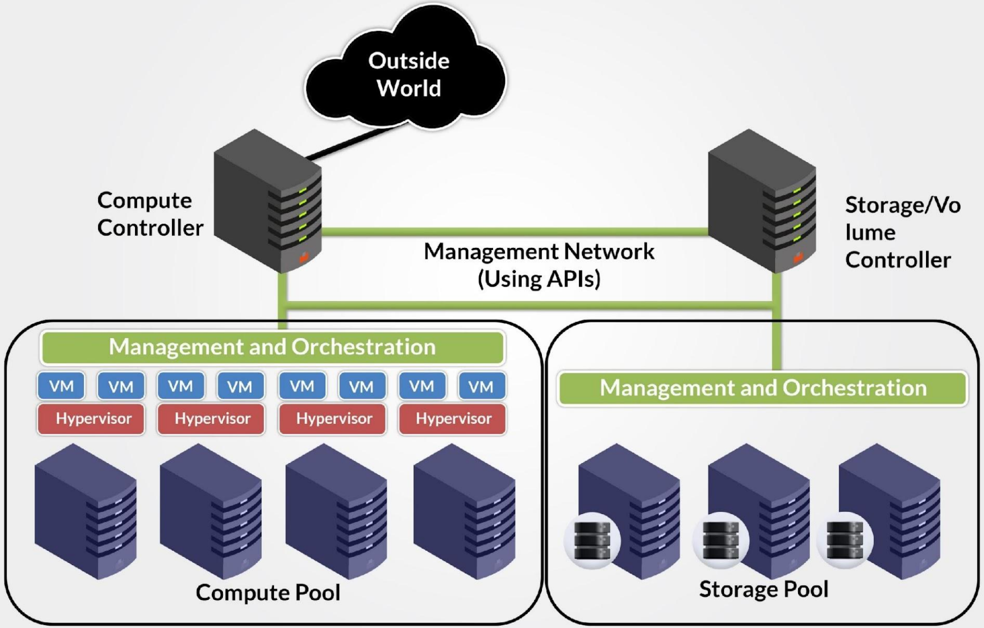

Cloud service models
Gmail, Trello, Slack, Acumbamail, Office 365
SaaS
End users
Flynn, Cloud Foundry Heroku, OpenShift
PaaS
Software developers
Stackscale, AWS, VMware, Azure
IaaS
Network architects IT administrators
Stackscale

Ref : https://www.stackscale.com/blog/cloud-service-models/

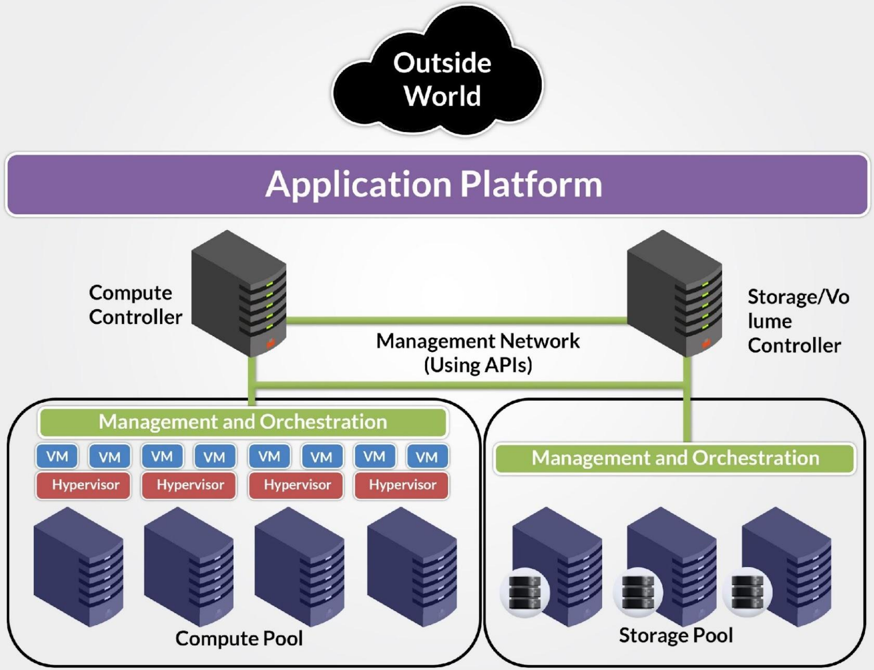
➤ Cloud Computing Stacks



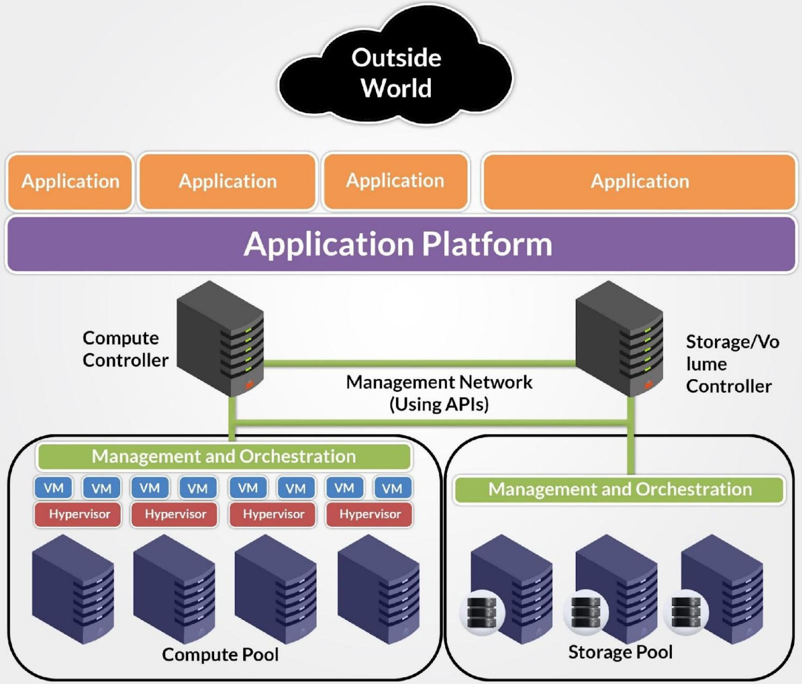
What is IaaS ?


Outside World
Compute Controller
Storage/Volume Controller
Management Network (Using APIs)
Management and Orchestration
VM
VM
VM
VM
VM
VM
VM
VM
Hypervisor
Hypervisor
Hypervisor
Hypervisor
Compute Pool
Management and Orchestration
Storage Pool

What is PaaS ?


Outside World
Application Platform
Compute Controller
Storage/Volume Controller
Management Network (Using APIs)
Management and Orchestration
VM
VM
VM
VM
VM
VM
VM
VM
Hypervisor
Hypervisor
Hypervisor
Hypervisor
Compute Pool
Management and Orchestration
Storage Pool

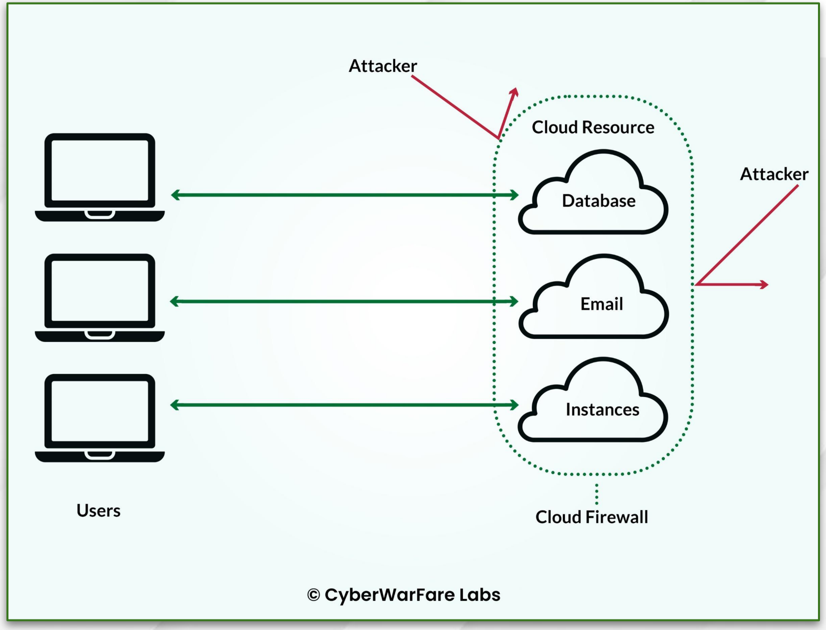
What is SaaS ?



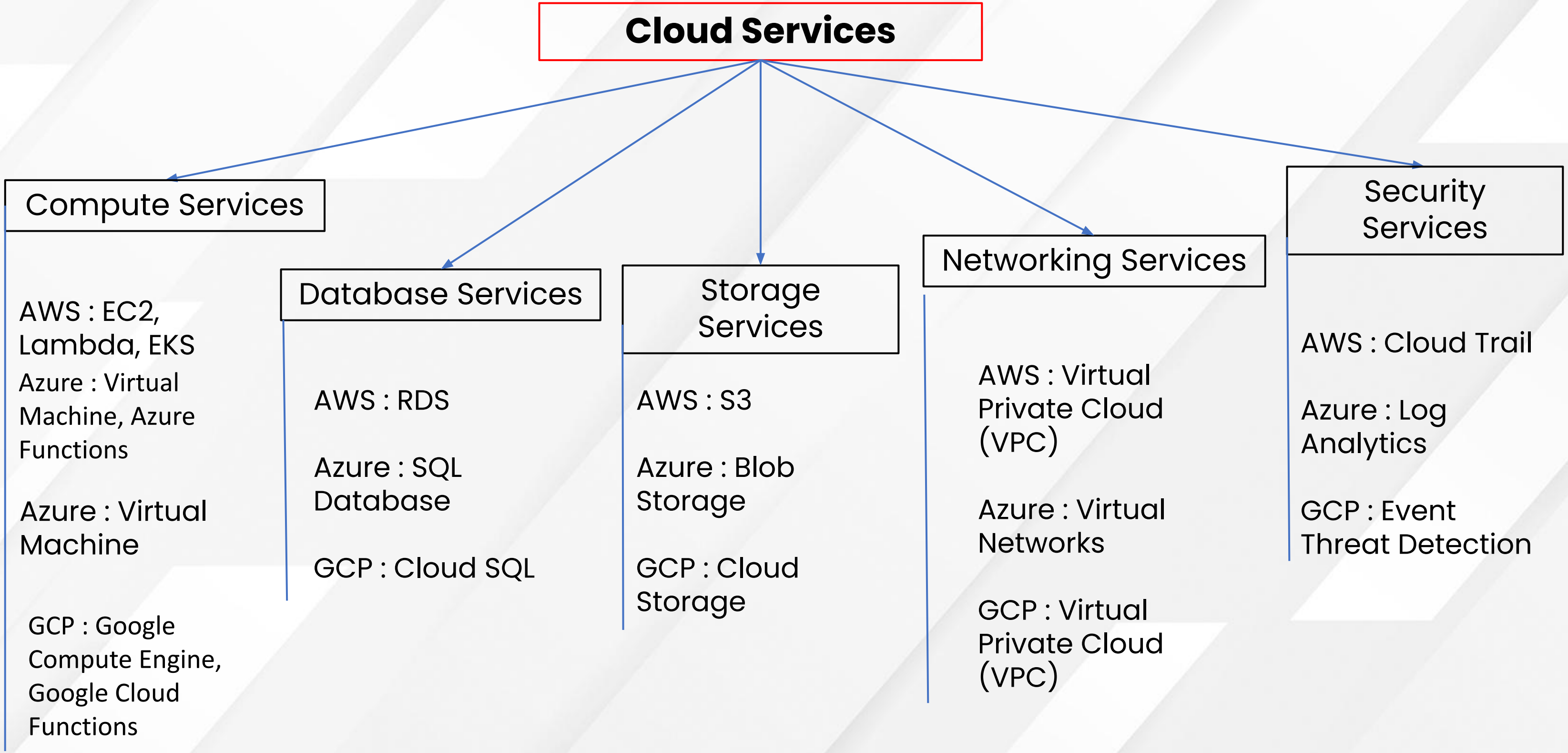
© CyberWarFare Labs

Cloud Firewall (security groups)

- ➢ They are hosted in cloud environment. They can protect on-premise as well as cloud resources
- ➢ Authorized users can connect to the cloud from anywhere and on any network
- ➢ The main use case is that it can be scaled to handle more traffic



© CyberWarFare Labs



Cloud Services

Compute Services

AWS : EC2, Lambda, EKS

Azure : Virtual Machine, Azure Functions

Azure : Virtual Machine

GCP : Google Compute Engine, Google Cloud Functions

Database Services

AWS : RDS

Azure : SQL Database

GCP : Cloud SQL

Storage Services

AWS : S3

Azure : Blob Storage

GCP : Cloud Storage

Networking Services

AWS : Virtual Private Cloud (VPC)

Azure : Virtual Networks

GCP : Virtual Private Cloud (VPC)

Security Services

AWS : Cloud Trail

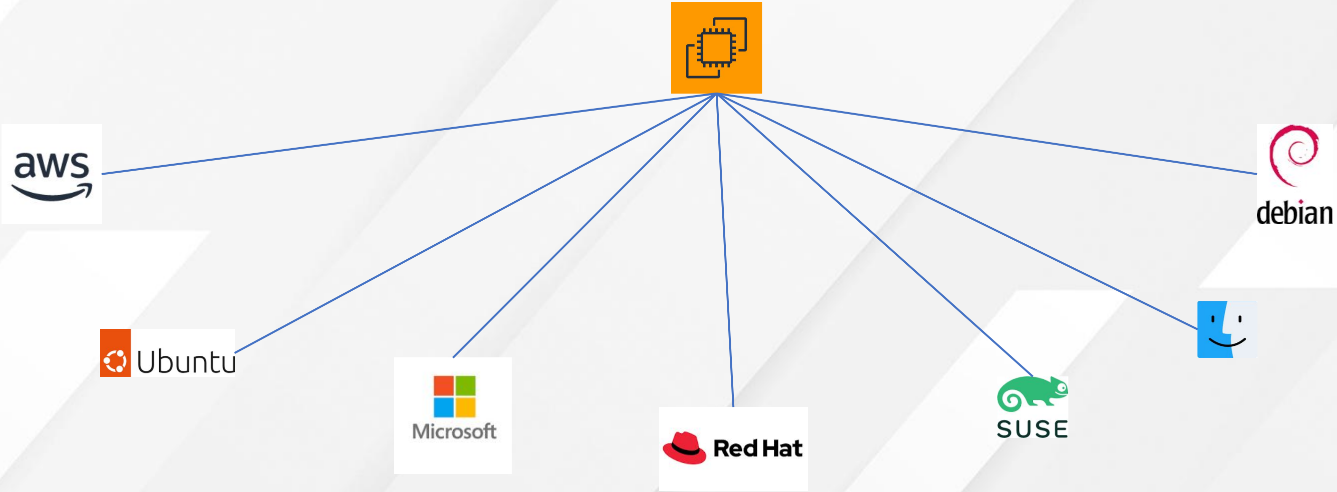
Azure : Log Analytics

GCP : Event Threat Detection

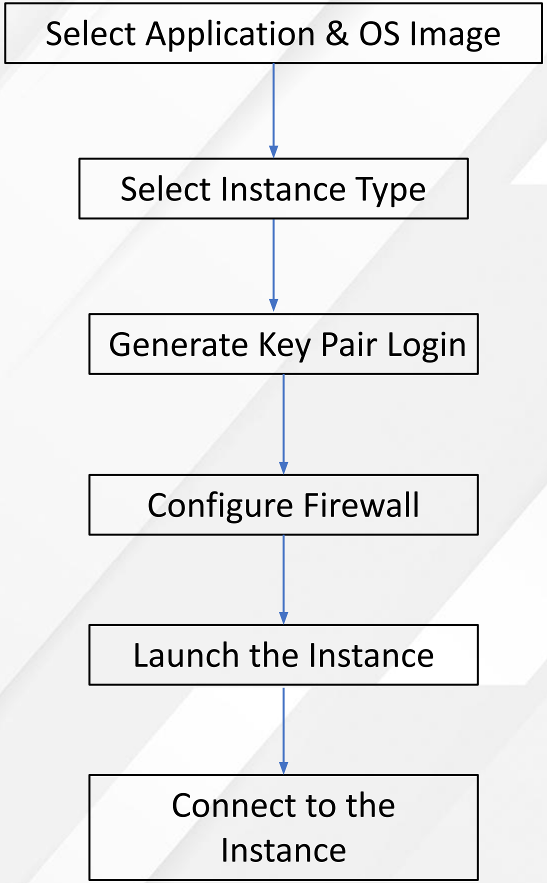
COMPUTE

➢ Amazon Elastic Compute Cloud (EC2)

- Web based computing
- Resources can be scaled as per requirement
- Resources are shared among customers but are isolated from each other



- ➢ **Spawn a compute resource in AWS**



Select Application & OS Image

Select Instance Type

Generate Key Pair Login

Configure Firewall

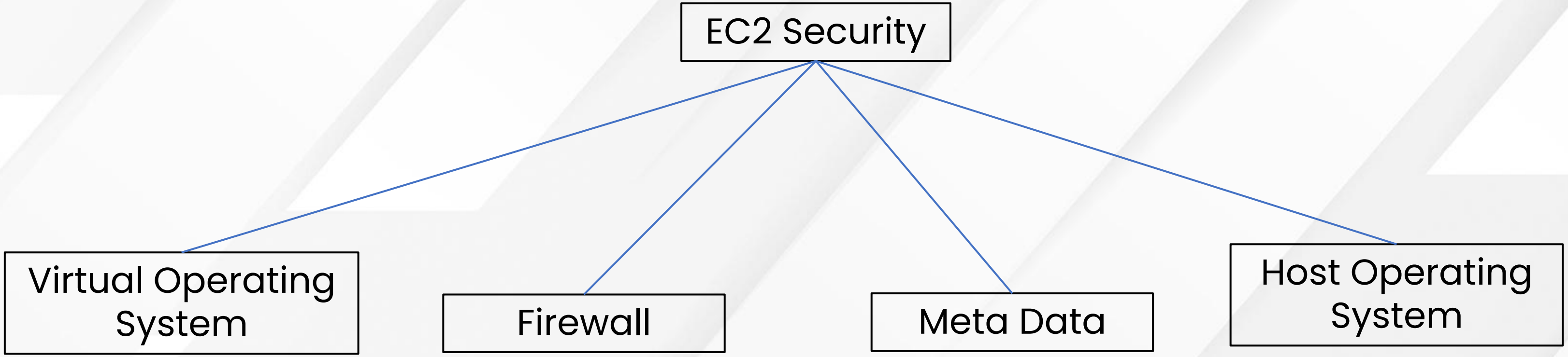
Launch the Instance

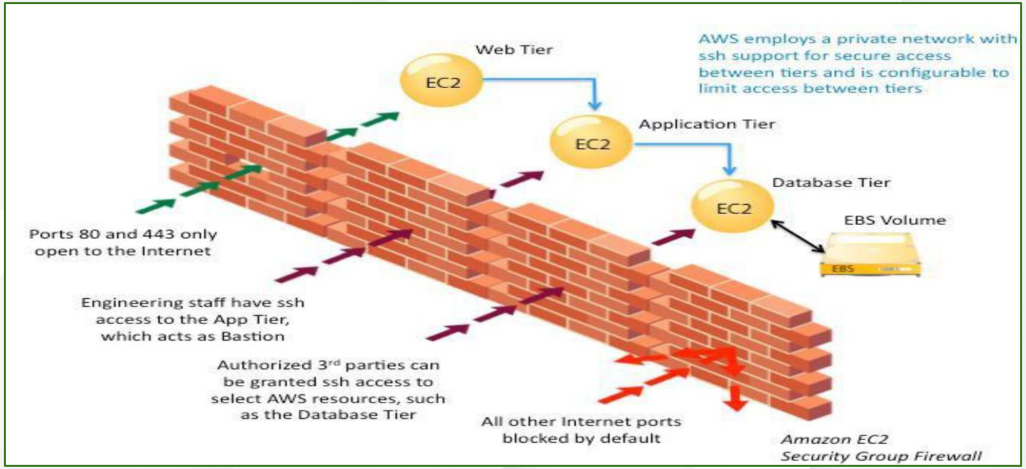
Connect to the Instance

DEMO 1 : Spawning AWS EC2

DEMO 2 : Accessing EC2 from :

1. Linux / Mac Machine
2. Windows Machine


EC2 Security
Virtual Operating System
Firewall
Meta Data
Host Operating System


Web Tier
EC2
Application Tier
EC2
Database Tier
EC2
EBS Volume
EBS
AWS employs a private network with ssh support for secure access between tiers and is configurable to limit access between tiers
Ports 80 and 443 only open to the Internet
Engineering staff have ssh access to the App Tier, which acts as Bastion
Authorized 3rd parties can be granted ssh access to select AWS resources, such as the Database Tier
All other Internet ports blocked by default
Amazon EC2 Security Group Firewall

➢ Virtual Operating Systems

- Vulnerability in amazon machine image (AMI) template
- Example : OS specific vulnerability, Application focused vulns etc
- Installed unknown middleware agents in the Virtual Machines
- The installed middleware agents open a new attack surface unknown to the end customers / organizations

Middleware	Operating system	Open source
Open Management Infrastructure (OMI)	Linux	https://github.com/microsoft/omi
Microsoft Azure Guest Agent (WALinuxAgent)	Linux	https://github.com/Azure/WALinuxAgent
Operations Management Suite (OMS)	Linux	https://github.com/microsoft/OMS-Agent-for-Linux
Dependency agent	Linux	No
Azure pipelines agent	Linux, Windows	https://github.com/microsoft/azure-pipelines-agent
Azure RD Agent Service	Windows	No

Middleware	Operating system	Open source
Google Accounts Daemon	Linux	https://github.com/GoogleCloudPlatform/compute-image-packages/blob/master/packages/python-google-compute-engine/google_compute_engine/accounts/accounts_daemon.py
Google OSConfig agent	Windows, Linux	https://github.com/GoogleCloudPlatform/osconfig
Google guest agent	Windows, Linux	https://github.com/GoogleCloudPlatform/guest-agent

Middleware	Operating system	Open source
AWS Systems Manager Agent (SSM Agent)	Windows, Linux, macOS	https://github.com/aws/amazon-ssm-agent
AWS PV Drivers	Windows	No
AWS ECS container agent	Windows, Linux	https://github.com/aws/amazon-ecs-agent
AWS EC2 Hibernation Initialization Agent	Linux	https://github.com/aws/amazon-ec2-hibinit-agent

Metadata Service

- Data that provides information about other data
- It provides data that we can use to manage the running instance
- The Metadata can be retrieved locally from the following URL :

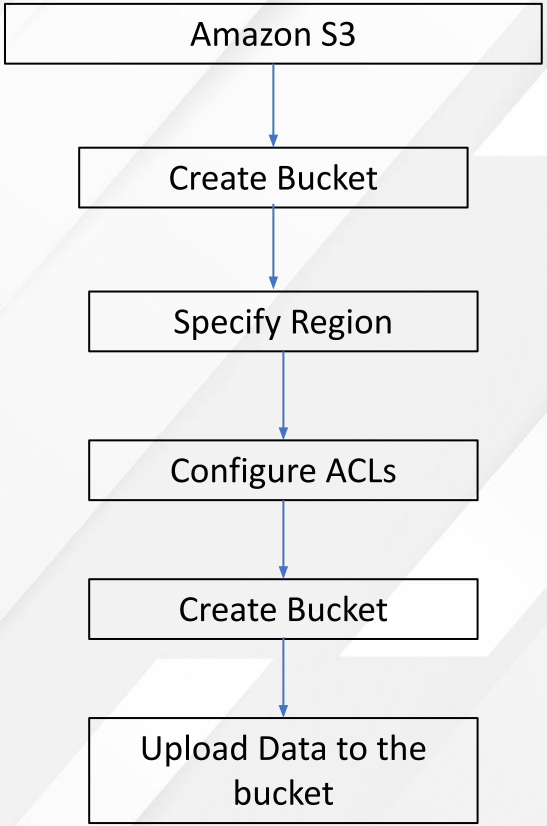
http://169.254.169.254/latest/meta-data

- The attacker with enough rights can retrieve the metadata & steal the instance identity

- Enumeration about the instance, role attached to it etc can be done

STORAGE

- **Spawn a Storage resource in AWS**



Amazon S3

Create Bucket

Specify Region

Configure ACLs

Create Bucket

Upload Data to the bucket

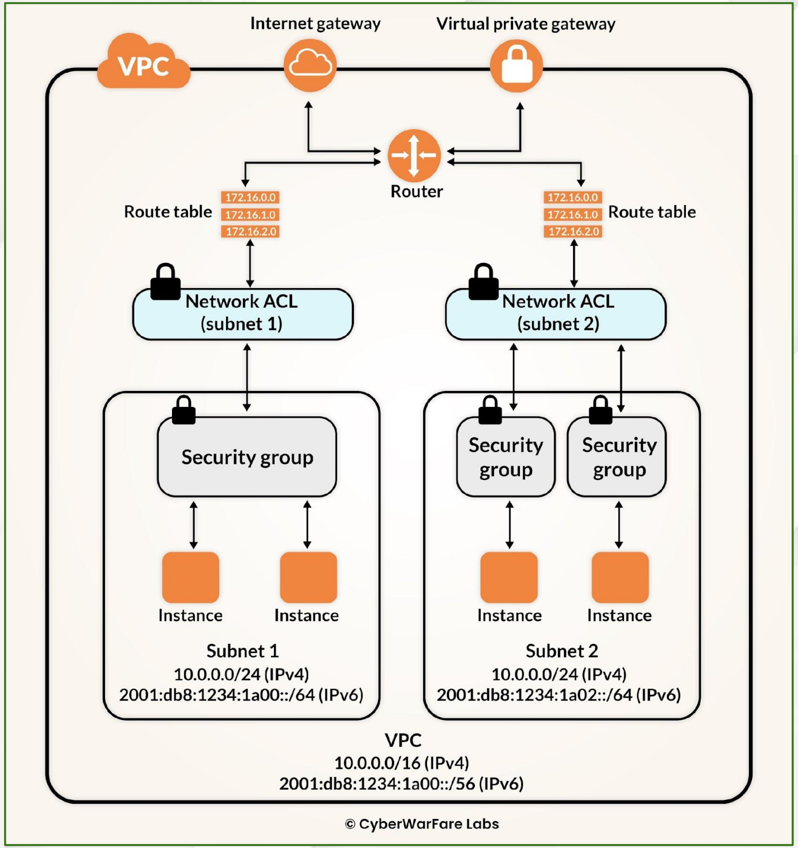
DEMO 2 : Creating AWS S3 Bucket

CWL
CyberWarFare Labs

NETWORKING

Virtual Private Cloud

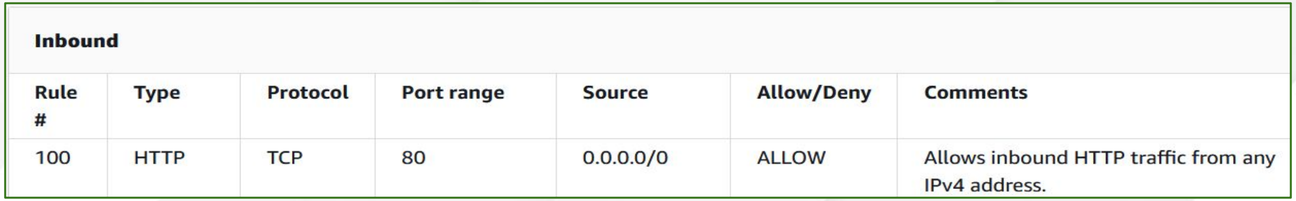
- It is a secure, isolated private cloud hosted within a public cloud
- VPC uses the following networking technologies for isolating computing resources from public cloud:
  - Subnets
  - VLAN
  - VPN



© CyberWarFare Labs

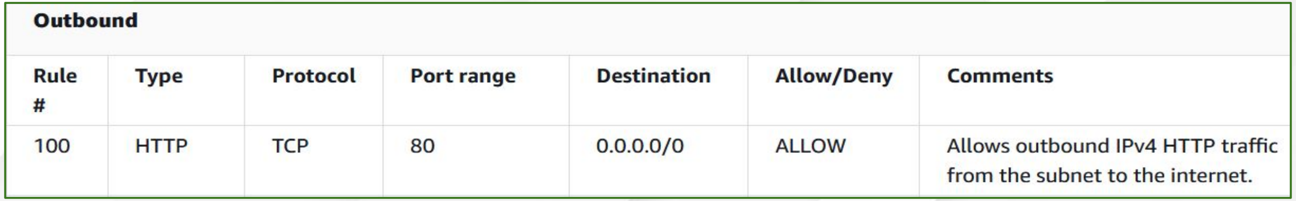
Network Access Control Lists (NACLs)

- They are firewall of the **VPC Subnets** and are applicable at the VPC subnet level.
- NACL’s are stateless, which means any rule applied to the incoming rule will not be applicable to the outgoing rule.
- It supports both allow as well as deny rule.



Inbound

Rule #	Type	Protocol	Port range	Source	Allow/Deny	Comments
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows inbound HTTP traffic from any IPv4 address.

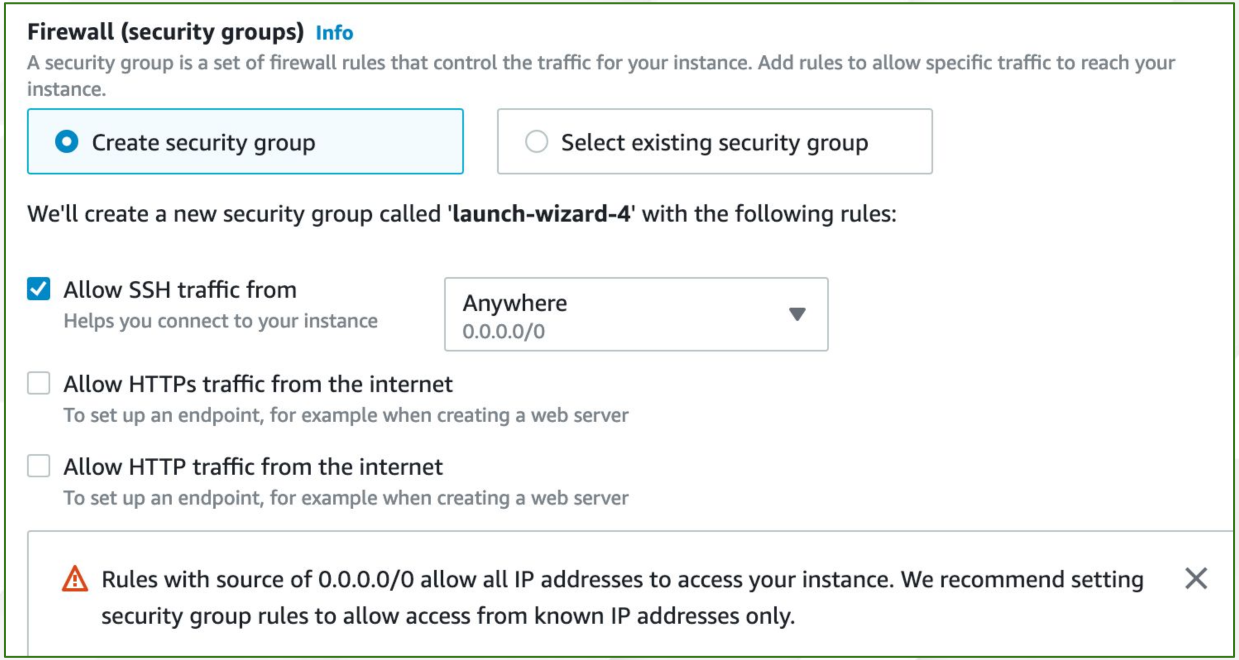


Outbound

Rule #	Type	Protocol	Port range	Destination	Allow/Deny	Comments
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows outbound IPv4 HTTP traffic from the subnet to the internet.

➢ Security Groups

- Set of Firewall rules that control the traffic for the instance.



Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-4**' with the following rules:

☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

□ Allow HTTPs traffic from the internet
To set up an endpoint, for example when creating a web server

□ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

EXERCISES

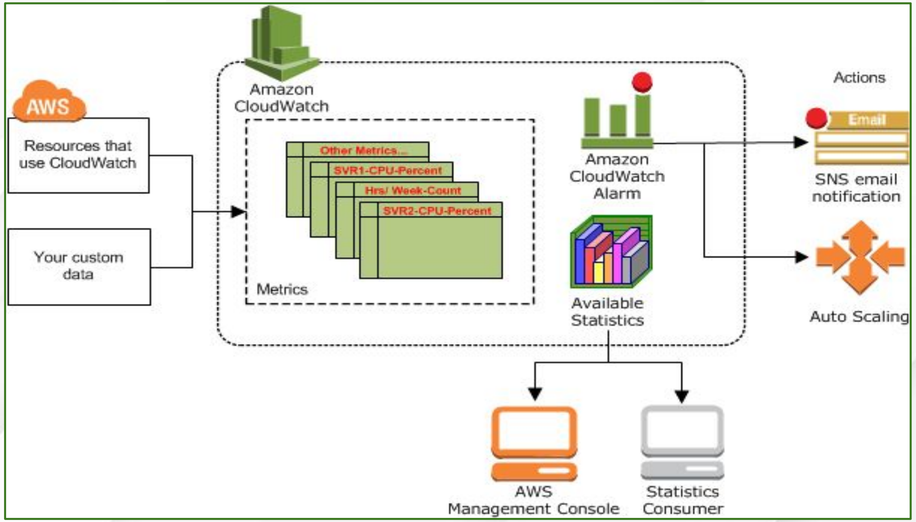
Exercise 1 : Setup a Web Server Rule in EC2 Security Group

Exercise 2 : Setup a Database Server Rule in EC2 Security Group

AWS SECURITY SERVICE

CloudWatch

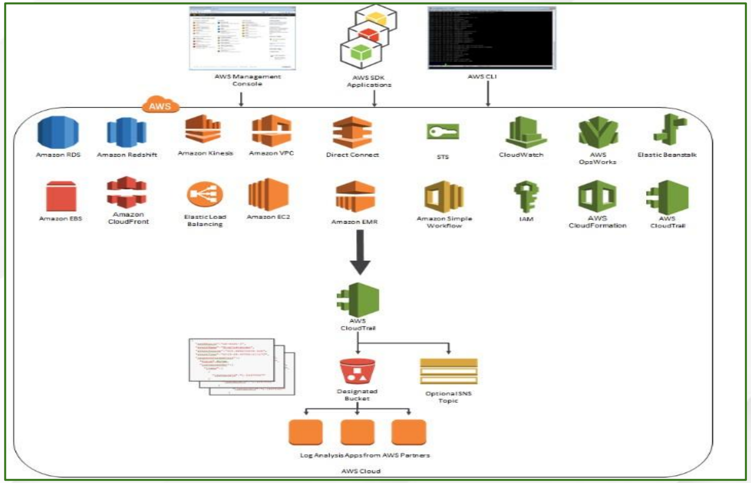
- It monitors AWS resources and applications in real time
- Alarms can be created during the analysis of the resource
- An AWS service like EC2 provides metrics into a repository and CloudWatch retrieve and create statistics based on those metrics
- There are AWS services that publish CloudWatch metrics. Listed [here]



Ref : https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_architecture.html

➤ CloudTrail

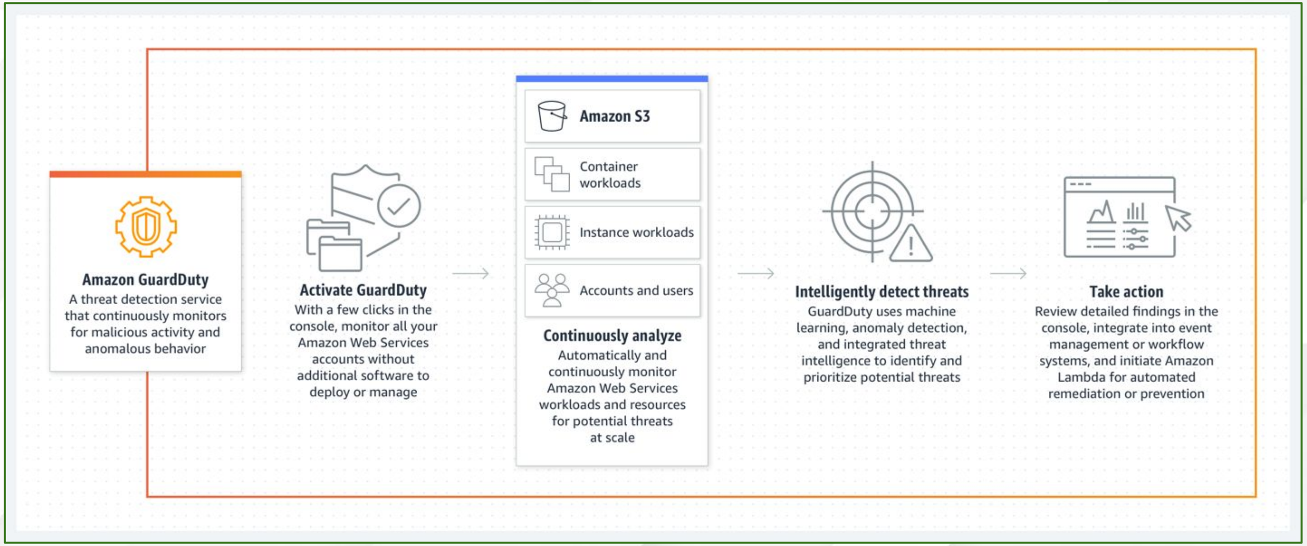
- Actions taken by a user, role or an AWS services are recorded as events
- It enables auditing, security monitoring by tracking user activity and API usage
- **CloudWatch** monitors performance, whereas **CloudTrail** monitors actions in the AWS environment



Ref : https://www.whizlabs.com/wp-content/uploads/2016/12/AWS-Article2-1.jpg

➢ AWS Guard Duty

- Threat Detection service that continuously monitors for malicious activity and unauthorized behaviour in AWS services
- Targets Amazon S3, Workloads, AWS accounts and logs / events from Cloudtrail, VPC & DNS



Amazon GuardDuty
A threat detection service that continuously monitors for malicious activity and anomalous behavior

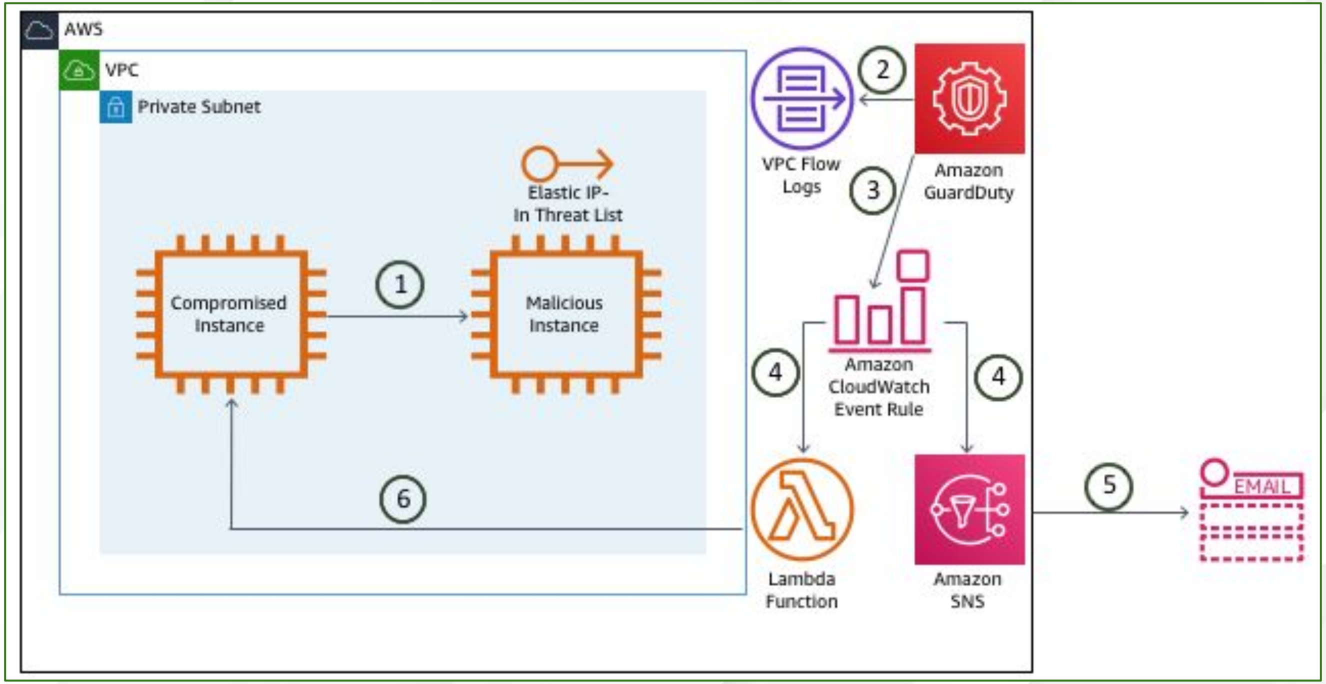
Activate GuardDuty
With a few clicks in the console, monitor all your Amazon Web Services accounts without additional software to deploy or manage

Continuously analyze
Automatically and continuously monitor Amazon Web Services workloads and resources for potential threats at scale

Intelligently detect threats
GuardDuty uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats

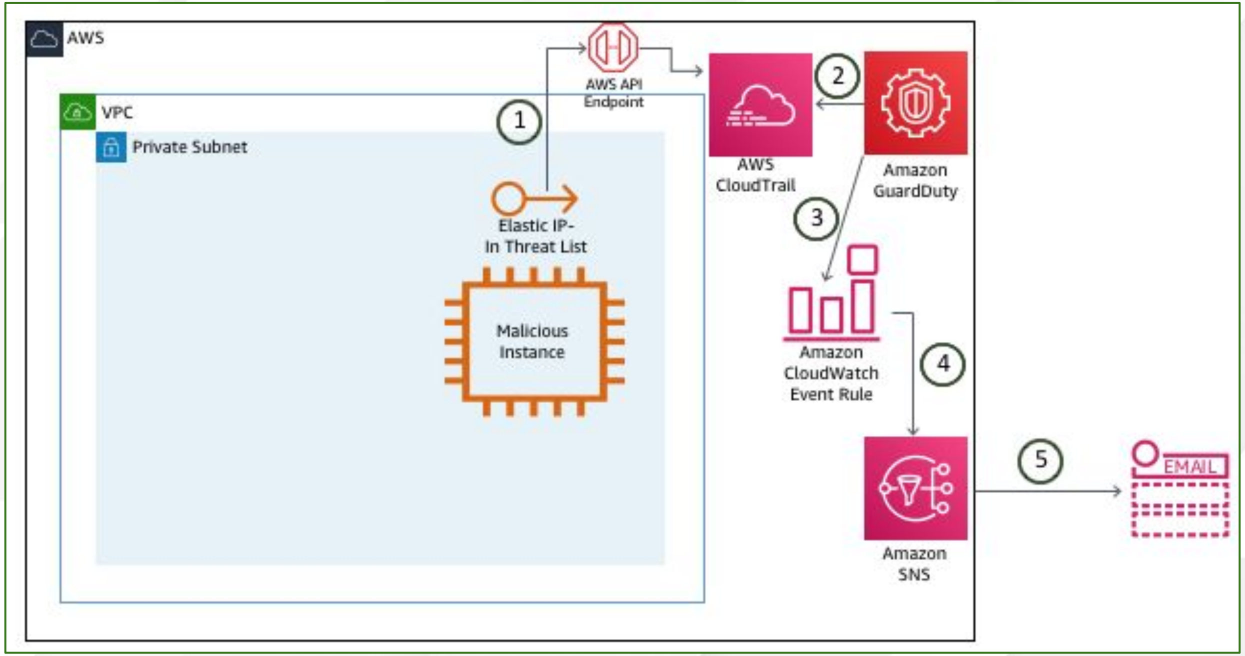
Take action
Review detailed findings in the console, integrate into event management or workflow systems, and initiate Amazon Lambda for automated remediation or prevention

Case Study 1 : Threat Detection – Compromised EC2 Instance



https://scalesec.com/blog/threat-detection-with-aws-guardduty/

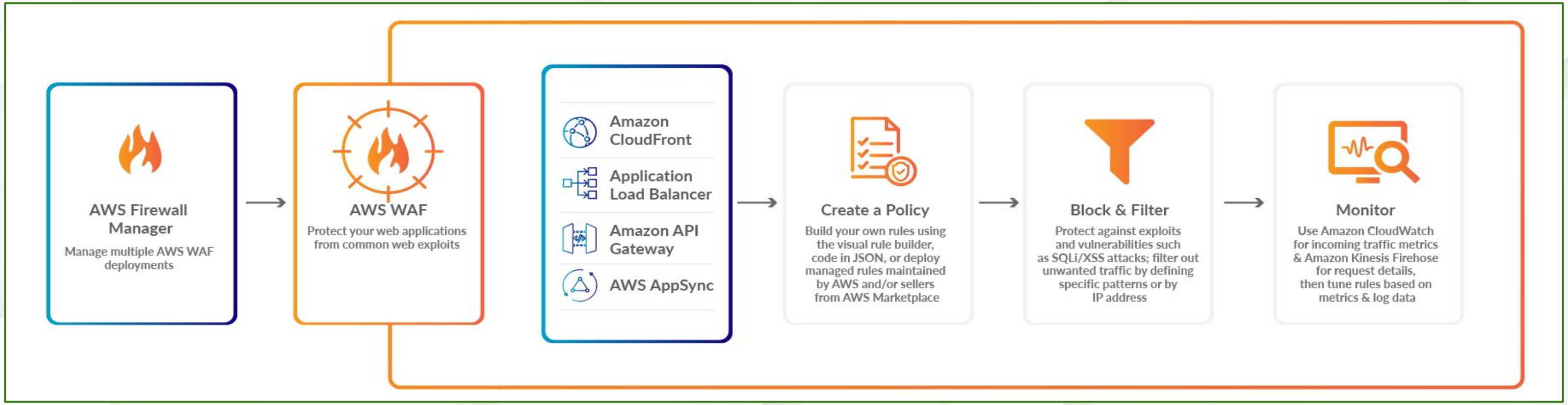
Case Study 2 : Threat Detection – Compromised IAM Credentials



https://scalesec.com/blog/threat-detection-with-aws-guardduty/

➢ AWS WAF & Shield

- Web application firewall which monitors web requests forwarded to API Gateway, CloudFront & Load Balancer
- It limits the web traffic and stop various typical crime patterns
- AWS WAF works with : **Access Control Lists (ACL), Rules & Rule Group**
- One of the feature “**AWS Managed Rules**” provides protection against common vulnerabilities (apart from custom rule writing functionality)

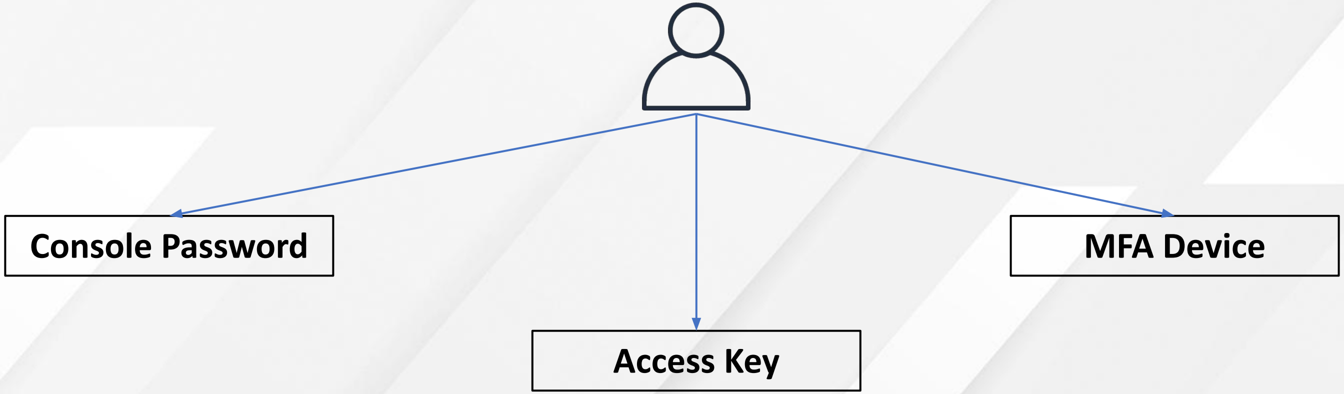

AWS Firewall Manager
Manage multiple AWS WAF deployments
AWS WAF
Protect your web applications from common web exploits
Amazon CloudFront
Application Load Balancer
Amazon API Gateway
AWS AppSync
Create a Policy
Build your own rules using the visual rule builder, code in JSON, or deploy managed rules maintained by AWS and/or sellers from AWS Marketplace
Block & Filter
Protect against exploits and vulnerabilities such as SQLi/XSS attacks; filter out unwanted traffic by defining specific patterns or by IP address
Monitor
Use Amazon CloudWatch for incoming traffic metrics & Amazon Kinesis Firehose for request details, then tune rules based on metrics & log data

CyberWarFare Labs

IDENTITY AND ACCESS MANAGEMENT (IAM):

➢ IAM

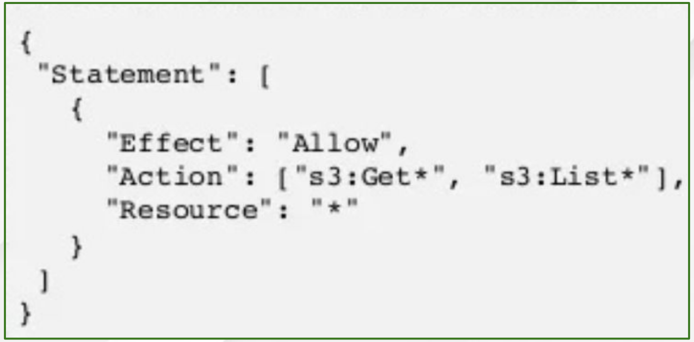
- IAM enables the administrators to control “**who”** can **perform “what” actions** in **AWS account**
- Users / services are denied by-default to access the resources until they are provided with explicit permissions
- Permissions are generally assigned to each IAM entity. For Example :
  - Backend Developer -> Access to Amazon S3



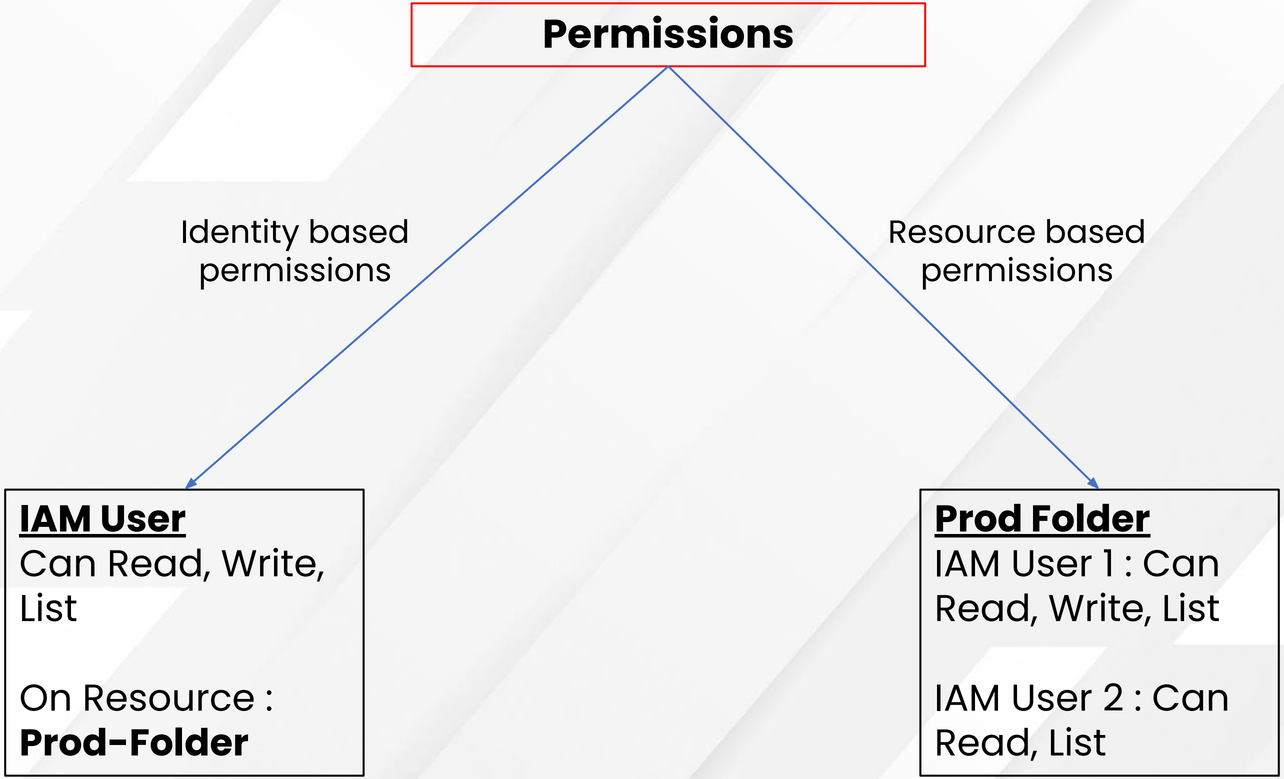
➤ IAM Policies

- Permissions are assigned using Policies
- Policies can belong to **identity based** as well as **resource based** permissions
- It contains a statement (permissions in JSON) which details the following:

Who	**Yash (IAM User)**
What Actions	**Can GET/PUT objects in S3**
Which AWS resources	*****
When	**Till 31st March 2024**
Where	**From XYZ IP Range**
How	**After MFA**



```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:Get*", "s3:List*"],
      "Resource": "*"
    }
  ]
}
```



Permissions

Identity based permissions

Resource based permissions

<u>IAM User</u>
Can Read, Write, List

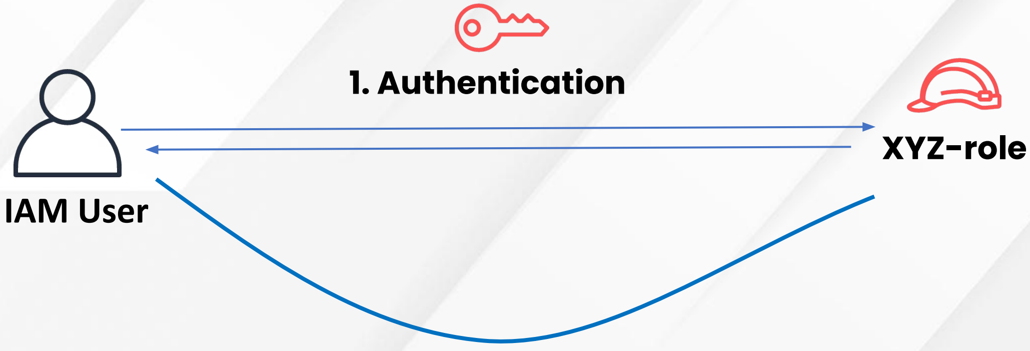
On Resource :
Prod-Folder

<u>Prod Folder</u>
IAM User 1 : Can Read, Write, List

IAM User 2 : Can Read, List

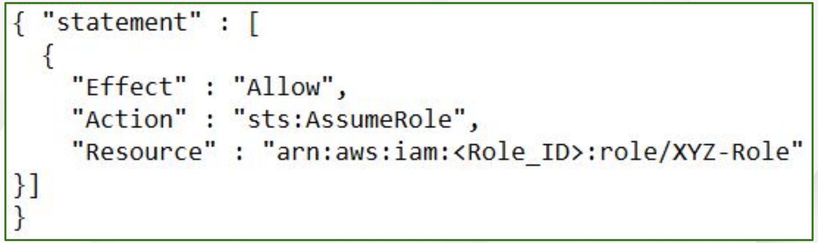
➤ IAM Roles

- When the root user do not need to share the security credentials, roles are used.
- Roles are permission policies that determine what an identity can or cannot perform
- It can be assumed by anyone who has permission to do as granted by administrator
- Permission are assigned to :
  - **The Principal** (Who will assuming the role)
  - **The Role** (Who can assume the role)
- Generally roles are preferred instead of long term credentials as credentials will not be shared
- Least privilege concept are applicable in scenarios



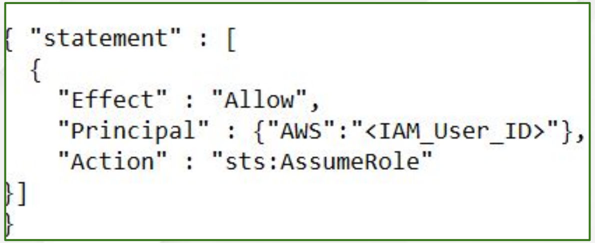
2. XYZ-role is assumed

IAM User – Identity Based Permission



```
{ "statement" : [
  {
    "Effect" : "Allow",
    "Action" : "sts:AssumeRole",
    "Resource" : "arn:aws:iam:<Role_ID>:role/XYZ-Role"
}]
}
```

XYZ Role – Resource Based Permission



```
{ "statement" : [
  {
    "Effect" : "Allow",
    "Principal" : {"AWS":"<IAM_User_ID>"},
    "Action" : "sts:AssumeRole"
}]
}
```

DEMO 3 : Creating IAM User with S3 Full Access

CWL
CyberWarFare Labs

DEMO : Creating IAM User & Authenticate using CLI

Google Cloud Platform (GCP)

Google Compute Engine (GCE)

- It is a part of **Google's IaaS (Infrastructure as a Service)** service that provides virtual machines (VMs)
- Users can select machine type customize it and spawn it within seconds

CWL
CyberWarFare Labs

DEMO : Google Compute Engine (GCE)

GCE Firewall Rules

- Firewall rules are defined at the network level & only apply to network
- Explicit ingress / egress rules with Deny / Allow rules can be defined
- Firewall Network Tags can then be applied to the compute engine to apply the firewall

DEMO : GCE Firewall Rules

Google Storage

- Cloud Storage is a service for storing your objects in **Google Cloud**
- Storage contains buckets where we can place objects like file etc.
- Permissions are generally assigned to each IAM entity. For Example :

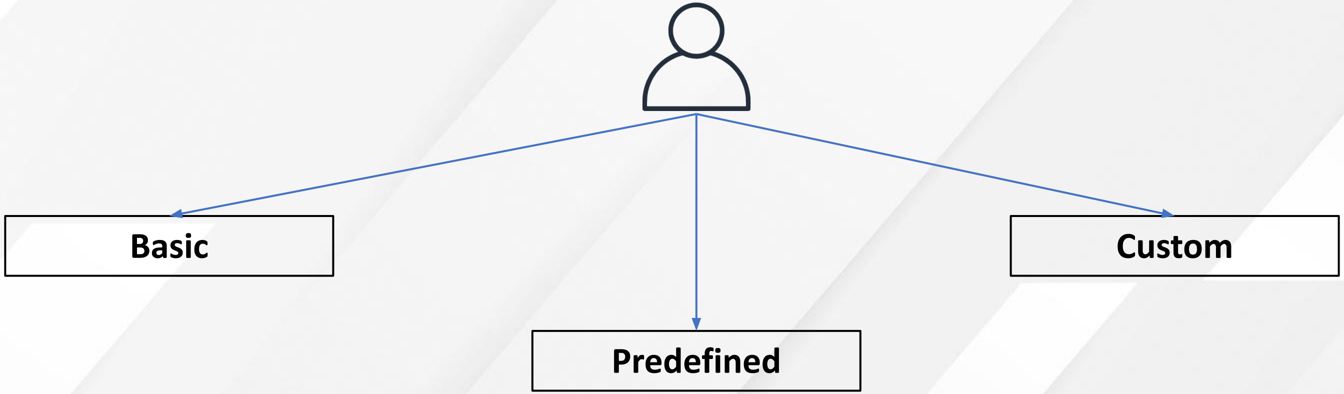
DEMO : GCP Storage

IAM

- IAM enables the administrators to control “**who”** can **perform “what” actions** in **GCP account**
- Users / services are denied by-default to access the resources until they are provided with explicit permissions

- GCP IAM **Roles** contains set of **permissions** that determine **which operations can be used on a specific resource**

- GCP IAM **Policies** define **which identities** have **what kind of access to an attached specified resource**



DEMO : GCP IAM User

CyberWarFare Labs

Microsoft Azure

Azure Virtual Machine

- ➢ They are image service instances that provide **on-demand** and **scalable** computing resources with usage-based pricing
- ➢ Access the spawned machine using SSH, RDP or Browser based

DEMO : Azure Virtual Machine

Network Security Group (NSG)

- NSG filters traffic in network level, implementing this will prevent traffic to & from the azure resources
- It is a Network Security Firewall

CWL
CyberWarFare Labs

DEMO : Azure VM Network Security Groups

Azure Blob Storage

➢ Azure Blob Storage is Microsoft's object storage solution for the cloud

➢ Storage have containers, which store blobs

DEMO : Azure Blobs

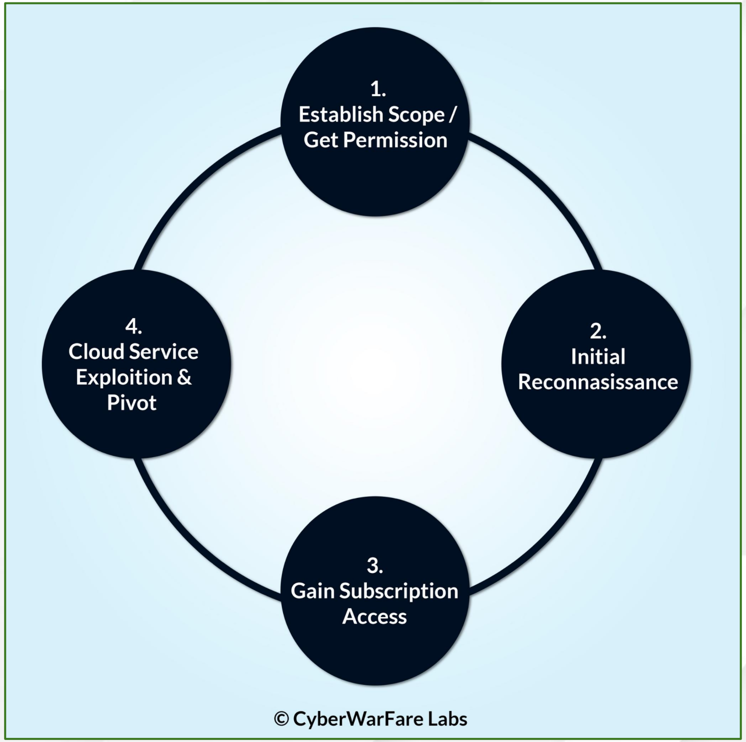
Azure Active Directory

- Azure Active Directory (Azure AD) is a cloud-based identity and access management service
- This service helps employees access **external resources,** such as **Microsoft 365**, the Azure portal, and thousands of other SaaS applications

CWL
CyberWarFare Labs

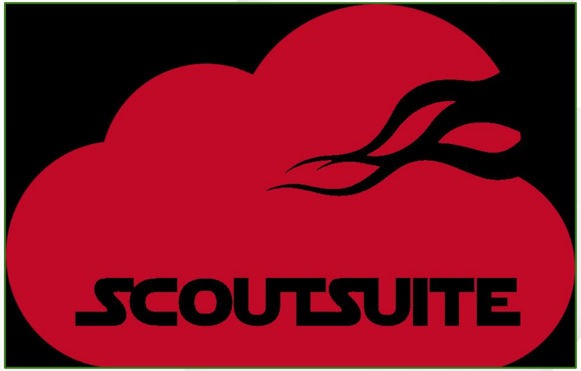
DEMO : Azure Active Directory

Penetration Testing in Cloud Environment



- Scout Suite

https://github.com/nccgroup/ScoutSuite



EXERCISE

Exercise : Configure, Run & Create a report of Assessment using ScoutSuite

Module 6 : Capstone Project

- ➢ Thoroughly understand the case studies present in **Page 39 & 40**
- ➢ Create a VPC having 2 subnets which contains 2 EC2 instances. The condition is that one will be public & other private. Public instance must be accessible using IP (implement **NACL & SGs**) & public can communicate with public & vice-versa
- ➢ Explore, Understand & Configure ScoutSuite in VM environment

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live