Intro to Cloud Security | Tryhackme Writeup/Walkthrough | By Md Amiruddin

Md Amiruddin · Follow
Published in InfoSec Write-ups
21 min read · Mar 1, 2023

Learn fundamental concepts regarding securing a cloud environment.

Room Link : https://tryhackme.com/room/introductiontocloudsecurityc6

Task 1 : Introduction

Cloud computing is one of the IT industry's most common and evolving terms. In simple terms, it means delivering computing services over the internet. The customer does not need to buy and maintain physical data centres and servers in cloud computing. Instead, all services can be used with **pay-as-you-go pricing** (pay as per the usage of the services) and on an as-needed basis (we can access services when needed).

Learning Objectives

- Understanding cloud security models.
- Security through policies & procedures.
- Security through identity & access management.

- Security through networking management.
- Security through storage management.

Course Pre-requisites
Understanding of following topics is recommended before starting the course:

- HTTP Protocols & Servers.
- Principles of Security.

Task 2 : Architectural Concepts of Cloud

Characteristics of Cloud

A few years back, no one could even imagine that organisations would place their data and operations on a geographically miles away platform that unknown people would manage. However, cloud computing is becoming so popular that organisations of every type and size use it for different purposes, such as storing data, taking backups, disaster recovery and Business Continuity Operations (BCO). It is becoming popular due to the following characteristics:

- **Scalability**: In cloud computing, organisations only buy resources at a time. Instead, they buy upon the need. Also, resources can be scaled up or down as per business needs and requirements.
- **Simplicity**: Renowned cloud service providers believe in simple design & interface. Usually, the customer only needs to buy and use the cloud services

with little configuration.

- **Cost Effective**: Cloud computing allows us to pay for our services. The cost is reduced as a third party provides infrastructure and does not need to be purchased at once.
- **Enhance Automation**: Cloud computing services require limited human administration, so companies can focus more on their goals without worrying about managing and maintaining systems.

Models of Cloud Computing

The following three cloud computing models are based on what the cloud provider offers and the needs of customers/organisations.

Infrastructure as a Service (IaaS)

In IaaS, infrastructure is provided by cloud providers. The customer has complete control of operating systems, services and applications.

- Cloud Provider's Responsibility: Maintaining and providing data centres with racks, machines, cables, and utilities.
- Customer's Responsibility: In this case, the customer manages logical resources like software and operating system.

Platform as a Service (PaaS)

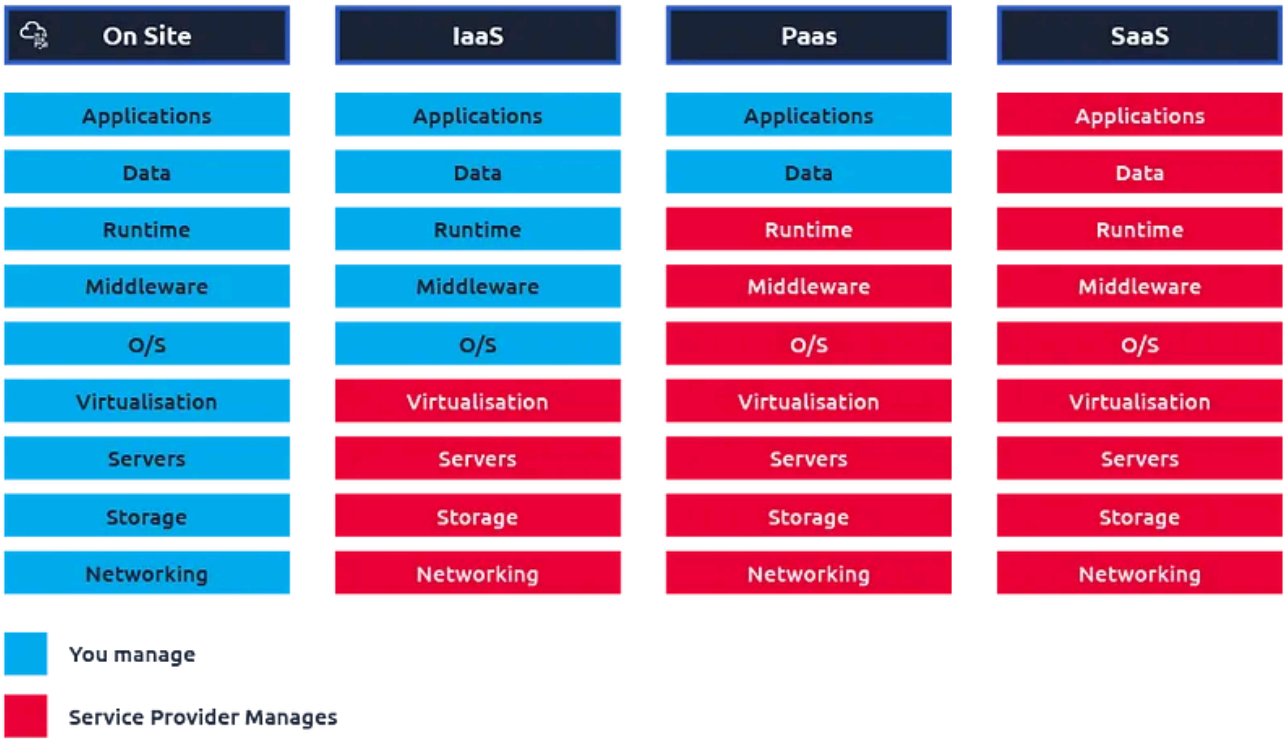
It contains all services offered in IaaS with the addition of an operating system (the user manages that in IaaS).

- Cloud Providers' Responsibility: In Platform as a Service, a cloud provider offers infrastructure and platform. Customers can choose any platform as per their needs. The service provider is responsible for managing the infrastructure and platform.
- Customer's Responsibility: Customers can install software as per their requirements.

Software as a Service (SaaS)

It includes every service that is being provided in IaaS and PaaS.

- Cloud Providers' Responsibility: In SaaS, everything is managed by the cloud provider, including infrastructure, OS and software.
- Customer Responsibility: This model is used by customers who need more technical skills in managing things. They only pay and use the services without worrying about the underlying architecture.



Cloud Deployment Models

Public Cloud

In the public cloud, as the name suggests, resources provided by cloud providers are shared among multiple customers. **Organisation A** will use resources from the same hardware that offers services to any other organisation. For example, Microsoft Azure and Amazon Web Services (AWS) are examples of public clouds. However, they also offer Virtual Private Cloud (VPC) services.

Private Cloud

In the private cloud, customers will not share the underlying resources (hardware and software) as in the public cloud, and resources are dedicated to a single customer. **Organisation A** will get a Virtual machine hosted on a system specifically dedicated to a particular customer.

Hybrid Cloud

It is a combination of a public and private cloud. For example, **Organisation A** might want to use some private cloud resources (to host confidential data of the production system) but also want some public cloud (for testing of the applications/software) so that the production system does not crash during testing.

Important Terminologies

There are some essential terminologies of cloud computing that one needs to understand. Some of the concepts are defined below:

- **Virtualisation:** Virtualisation is the primary technology used in cloud computing that allows sharing of instances of an application or resources among multiple customers or users simultaneously.
- **Compute:** Defined as the processing power customers require to run their applications and systems for data processing and carry out different tasks. In cloud computing, customers can get computing power from a combination of virtual machines hosted in the cloud environment.
- **Storage:** In cloud computing, we do not need to buy and maintain physical hard drives; instead, our data is stored in logical pools of physical storage on cloud provider premises, and we can scale up and scale down the resources as per needs.
- **Networking:** As cloud computing is a system of computers/processes that are interconnected, maintaining a high-speed network connection is very important. The cloud provider is responsible for providing network connectivity to meet customer needs without disruption.

Answer the questions below :

```
1. In Infrastructure as a Service, what will be deployed by the vendor (Hardwar
A. Hardware

2. What is the type of cloud dedicated to a single customer called?
A. Private
```

Task 3 : Cloud Security Concepts

To understand cloud security concepts, first, we need to know what we need to protect in the cloud. The simple answer is "**Data**". Data is an asset and can be anything and any piece of information that any customer or organisation has. Data must be categorised into different levels (as defined below) before sharing in cloud platforms so that appropriate controls can be applied to protect it from a security point of view. There are three main classes of data depending on their sensitivity:

- **Confidential data:** Confidential data can be considered the most critical data any organisation can have. Confidential information/data, if exposed, can damage an organisation's reputation and even includes personally identifiable information.
- **Internal data:** Internal data is information that, if exposed, causes moderate risk or harm to the company.
- **Public data:** Public data is any information included on (or intended for) the public. There is no consequence if public data is leaked because it's already meant for use by everyone.

Cloud Data Lifecycle

In today's world, organisations store and use large amounts of data, including critical and sensitive data of the customers. Data on the cloud should be managed through its lifecycle to ensure its secure usage in every phase.

Major Steps

Data life cycle means the sequence of steps a particular data goes through from its creation to its deletion phase.

Security Aspects in Cloud Data Lifecycle

Each phase of the cloud data lifecycle requires protection. Below are the cloud data lifecycle stages, security considerations and requirements.

Create/Update

The create phase is the initial phase of the data lifecycle. It includes the newly created data and data that is being freshly imported from other data sources. In this phase, the data owner should be defined, and categorisation or classification of data should be done. Security aspects and challenges in this phase are as below:

- **Implementing SSL/TLS:** Secure communication through SSL/TLS should be implemented so that it will be difficult for the attacker to listen to data transferred between the customer and the cloud provider.
- **Encryption:** Data should be encrypted so that if data is exposed, the attacker cannot read it without decrypting it.
- **Secure connections:** Secure connections and paths should be established for the data transfer so that change of data breach is minimised (ensures data security in transit).

Store

Data is processed based on its form (structured or unstructured) and stored in a container generally known as a database. Security aspects at this stage are as below:

- **Encryption:** Data should be encrypted to protect data at rest.
- **Backup:** Backup should be taken to prevent data loss; if data is lost, it can be restored from the available backups.

Use

As we know, if data is encrypted, it must be decrypted to be used by the application. Security aspects include the following means:

- **Secure connections:** Encrypted paths should be established before data transfer to ensure the confidentiality and integrity of data in transit.
- **Secure platform:** A secure authentication mechanism should be used, protected from attacks and vulnerabilities.
- **Restrict Permissions:** Data owners should set strict permissions to modify and process data from unauthorised persons.
- **Secure Virtualisation:** There is the concept of virtualisation in cloud computing in which resources among users are shared. So cloud providers need to ensure that one customer's data should not visible to other customers.

Share

Share data within or outside the cloud infra; challenges include:

- **Jurisdiction:** Regulatory mandates/restrictions of sharing data across specific locations/regions.
- **Data Loss Prevention (DLP):** Data Loss Prevention (DLP) helps to detect and prevent data breaches or unwanted destruction of sensitive data. It contains sensitive data from being shared with unauthorised persons.

Archive

Long-term storage of data and applications; security aspects include:

- **Encryption:** Data should be encrypted before storing in cloud premises

- **Physical Security:** It demands that the storage servers are physically secured and prevented from unauthorised access through biometrics, CCTV, etc.
- **Location:** Reflects a physical location where data will be stored. Environmental factors such as natural disasters, climate, etc., can pose risks and consider Jurisdictional aspects (local and national laws) are key factors at this stage.
- **Backup Procedure:** How will data be recovered when required and How often full/incremental backups will be carried out?

Destroy

Data should be destroyed once of no use so that it cannot be misused by any user (intentional or unintentional). Crypto shredding is a process in which encrypted data is useless by destroying cryptographic keys (without keys, data cannot be decrypted).

Security Issues in the Cloud & its Solution

Despite the benefits of cloud computing, several security challenges must be addressed effectively. These challenges raise concerns about fundamental security properties such as confidentiality, integrity and availability. Significant issues are as defined below:

- **Data confidentiality:** When the data is hosted in the cloud, its privacy is at risk. As users have no physical access to their data once it has been outsourced, they don't know how the confidentiality of their data is being maintained. Cloud service providers can examine the data of the users without detection.
- **Virtualisation issues:** It allows the resources to be shared among the users. We need a mechanism to ensure isolation and secure communication between VMs. Users are not isolated in a multitenant environment, so one user can examine the data of another user.
- **Insecure interfaces and API:** Cloud services are managed by the customers with the help of software or APIs. So vulnerable software or API can be risky, and data or customer confidentiality and integrity are at risk.
- **Malicious insiders:** Some malicious insiders can cause the data breach of other clients. Taking advantage of shared technology vulnerabilities, these insiders

can leak the data of other users or exploit security weaknesses, thus causing security threats to the other customers on the cloud.

- **Account or service hijacking:** Several methods can cause account or service hijacking. These include phishing frauds, vulnerability exploitation and password reuse among users.
- **Access Control Mechanism (ACM):** In a cloud computing environment, users and cloud servers are not in the same domain. Enforcing efficient and reliable access to information is critical when data is outsourced to the cloud. An unauthorised person can gain access to the data due to a lack of access control rights.

Answer the questions below :

```
1. What is the first phase in the cloud data lifecycle?
A. Create

2. Click the View Site button at the top of the task to launch the static site
A. THM{CLOUD_11101}
```

Task 4 : Cloud Security Risks Concerning Deployment Models

This task will briefly discuss various cloud deployment models and their associated risks. Read along the following topics to get an understanding of various cloud models.

Private Cloud

As studied, a private cloud is an environment in which resources are dedicated to a single customer. These are suitable for customers that are more concerned about the security of their data. Associated risks are as under:

- **Personnel threats:** This includes both unintentional and intentional threats. Customers have no control over the provider's data centre and administrators. Any insider can cause damage to customers' data (either intentionally or unintentionally).
- **Natural disasters:** Private cloud is vulnerable to natural disasters.
- **External attacks:** Multiple attacks, such as unauthorised access, Man-in-the-middle attacks, and Distributed Denial of Service, can compromise the user's data.

Public Cloud

In the public cloud, resources among users are shared with the help of virtualisation technology. Some risks include:

- **Vendor Lock-In:** The customer becomes a dependent service provider in the public Cloud. It becomes nearly impossible for the customer to move the data out of the cloud infra before the end of the contract term; thereby, the customer becomes the hostage of the provider.
- **Threat of new entrants:** Your cloud provider may provide services to your competitor in the public cloud.

- **Escalation of Privilege Authorised**: In the public cloud, users may try to acquire unauthorized permissions. A user who gains illicit administrative access may be able to gain control of devices that process other customers' data.

Community Cloud

Computing & storage infrastructure is shared between a specific community or organisation members. Some risks include:

- **Vulnerability**: In a community cloud, any node may have vulnerabilities, which can also cause intrusions on the other nodes. Also, in a community, cloud configuration management and baselines are almost impossible (and very difficult to enforce).
- **Policy and administration**: It is challenging to enforce decisions and procedures in the community cloud, posing a severe challenge and threat.

Answer the questions below :

```
1. In which cloud model does the customer become the hostage of cloud providers
A. Public

2. Is it challenging to enforce specific business decisions and procedures in t
A. yea
```

Task 5 : Security Through Access Management

Access management is an important feature that ensures that the "right people" should do the "right job" within the "right set of permissions". Access management has a critical role in cloud security as data is stored over the internet, and due to a plethora of cyber-attacks, it is inherently insecure. In cloud computing, Access Management is implemented through the following measures:

- **Create Identities**: Cloud infrastructure creates "digital identities" that can relate to a person, user, API or service. An entity is a set of properties that can be recorded.

- **Authentication Factors**: Each identity is allocated with a specific set of characteristics unique to that particular identity and helps to distinguish it from other identities. If they are matched, then the essence of that user is confirmed. These characteristics are called “Authentication Factors”, which include: username, password, PIN, biometric, certificate, FaceID, etc.
- **Roles**: Each identity has a specific role which defines the domain under which that particular identity functions.

In Amazon, Access Management is implemented through Identity & Access Management (IAM). IAM is considered the “heart of access management” services to configure & perform fine-grained control and access policies to AWS resources. It is a web service that enables Amazon users to grant access to various services & resources to different users.

Features of IAM

- Give rights & permissions of resources in your amazon account to other people without sharing passwords, etc.
- Grant role-based access to users based on their access rights.
- Enable multi-factor authentication.
- Enable and manage permissions and access policies across amazon accounts & resources.

IAM Important Terminologies

To understand IAM, we must be very clear about its important terminologies:

- Resources: These are objects within a particular service; these include users, roles, groups & policies.
- Identities: Represent certain users permitted and authorised to perform specific roles and actions.
- Entities: A subset of resources which are used for authentication purposes. It includes users & roles.
- Principals: A person or some application requesting to use Amazon resources after signing in.

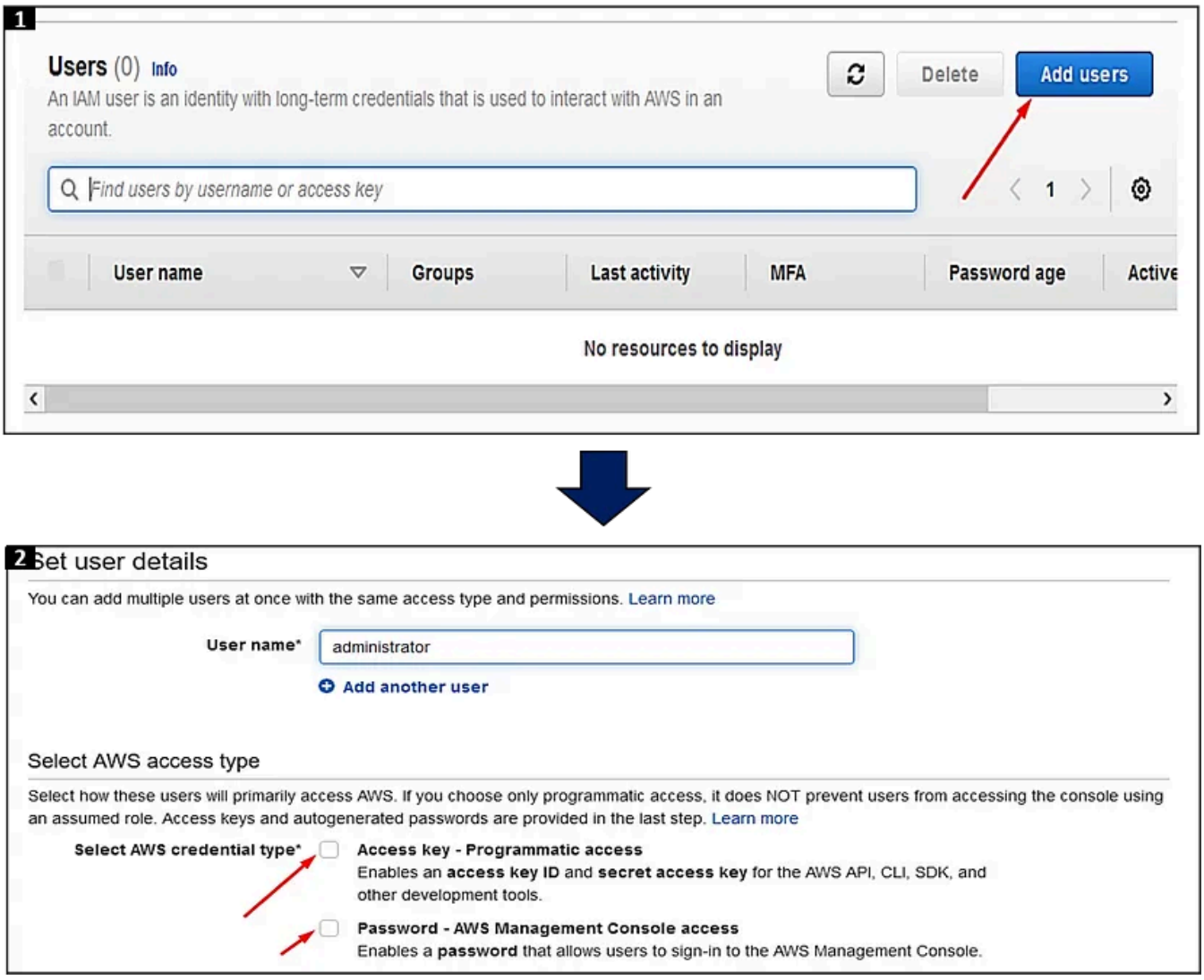
Using Cloud Environment

We will use examples from Amazon Web Services (AWS) throughout the room. Although the room can be completed with the provided text and image content, the practical exercises require an AWS account. Having an AWS account is optional for this room, but if you are interested, you can visit this URL to understand how to create and activate a new AWS account.

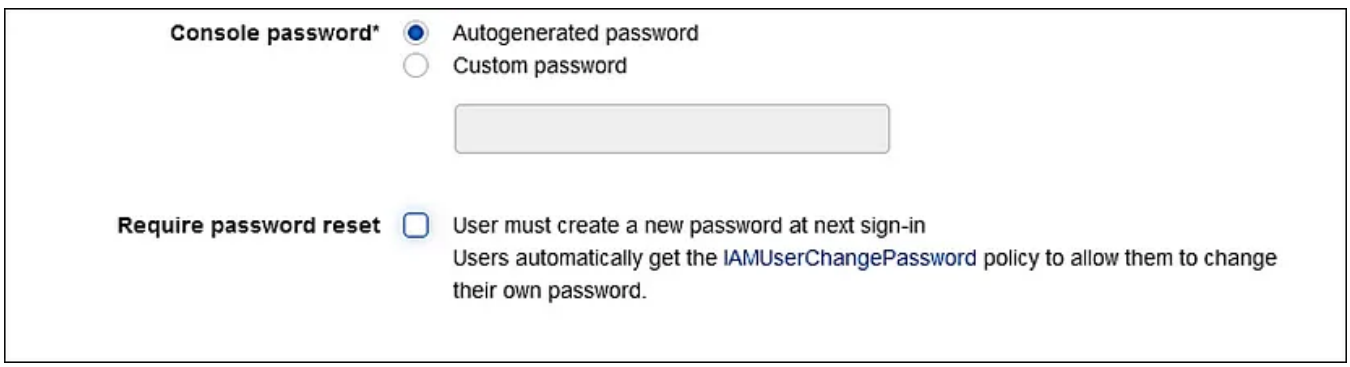
Practical Exercise

Create an IAM user account with administrative privileges in your AWS account. IAM users with administrative privileges will have complete access to AWS resources. Moreover, it can grant permissions to other users as well.

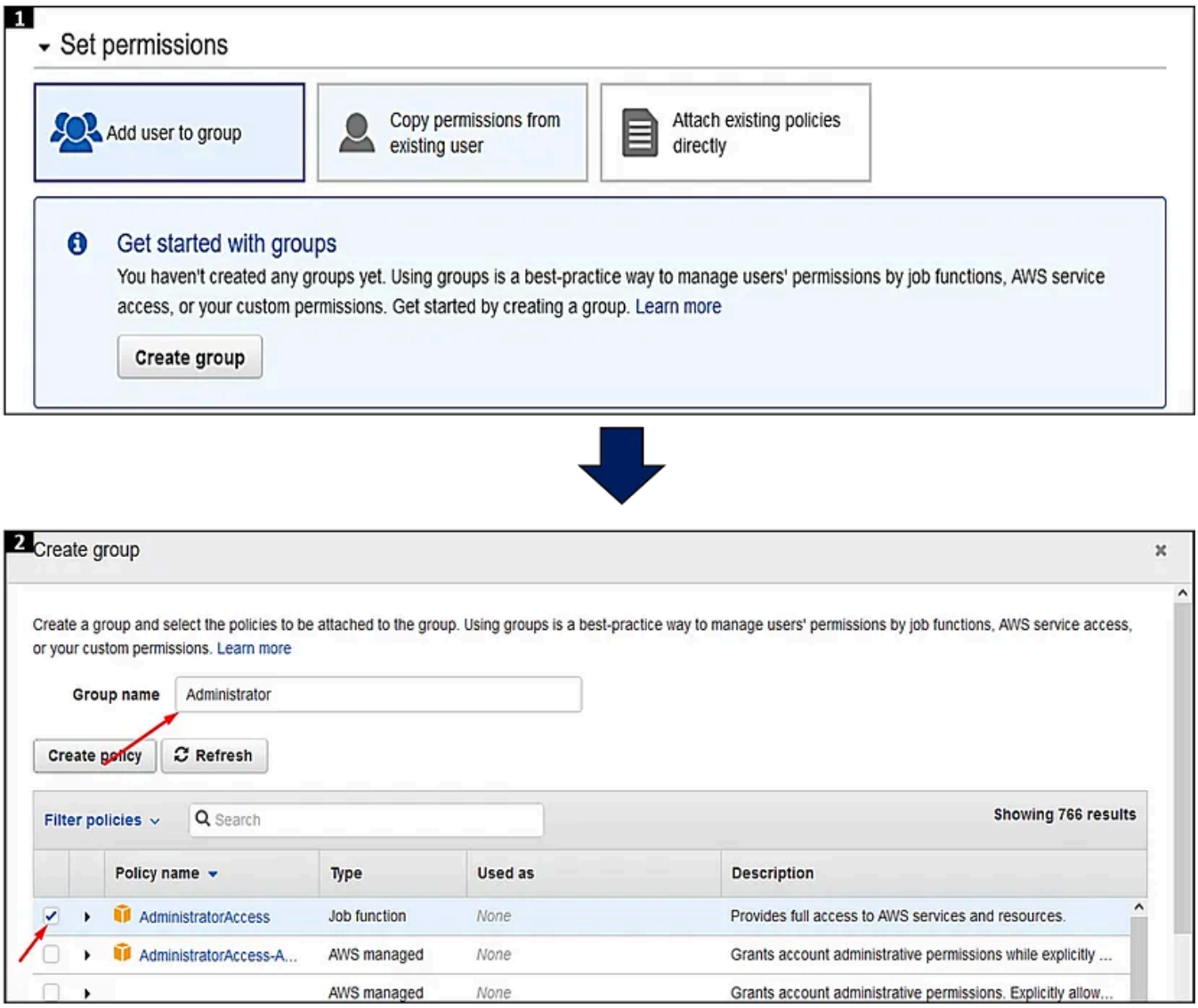
- Login to your AWS account by visiting `console.aws.amazon.com` and navigating "IAM" in the services menu.
- Go to "Users" in the navigation pane and click `Add users`.



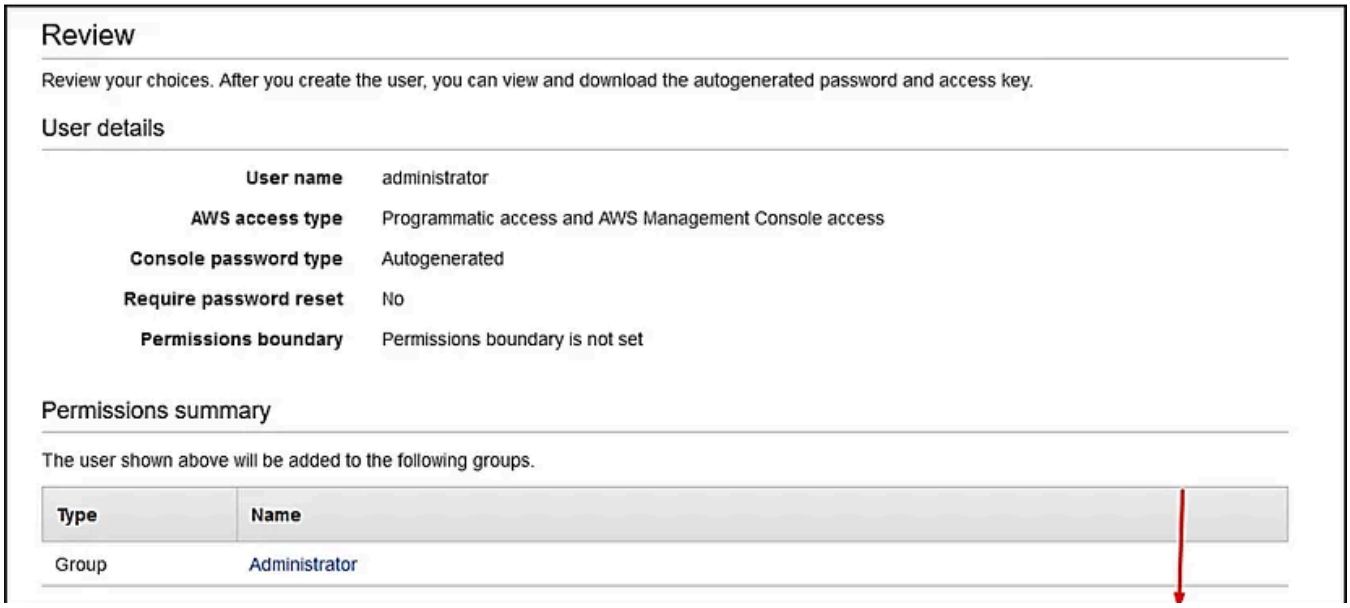
- Enter the new username and the user's sign-in name, and Select the type of access you want to assign to the new user. There are two types of access settings; Programmatic Access, If the user wants AWS CLI, SDK, API or tools for PowerShell and Management Console Access, for providing access to the management console.
- Add **console password.** You can provide custom-generated passwords as well as auto-generated passwords.



- Choose “Next” to go to permissions. Since no group is created, so click on “Create Group”.
- Enter the group name & check `AdministratorAccess` Policy.



- Click `Create Group` and then `Review` to go through the settings. If everything is up to the mark, then click **Create User**.



Key ID, Secret Access Key & Password etc.

Answer the questions below :

```
1. Are FaceID and biometric types of Authentication factors (yea/nay)?
A. yea

2. I have completed the practical exercise.
A. No answer needed
```

Task 6 : Security Through Policies

Another method of ensuring cloud security is through enforcing policies & permissions. Policies are a set of guidelines and controls which attach to identities and make permissions. The cloud infrastructure evaluates the permissions defined

in the policy to determine whether the request should be allowed or denied whenever an identity requests any service. In a typical cloud environment, there are the following types of policies:

- **Identity-based Policies:** Attached to identities and grant permissions.
- **Resource-based Policies:** These are implemented on resources (data & services) and define who is authorised to access that resource.
- **Session-based Policies:** These temporary policies allow access to specific resources for a particular time.

Security through Policies in AWS

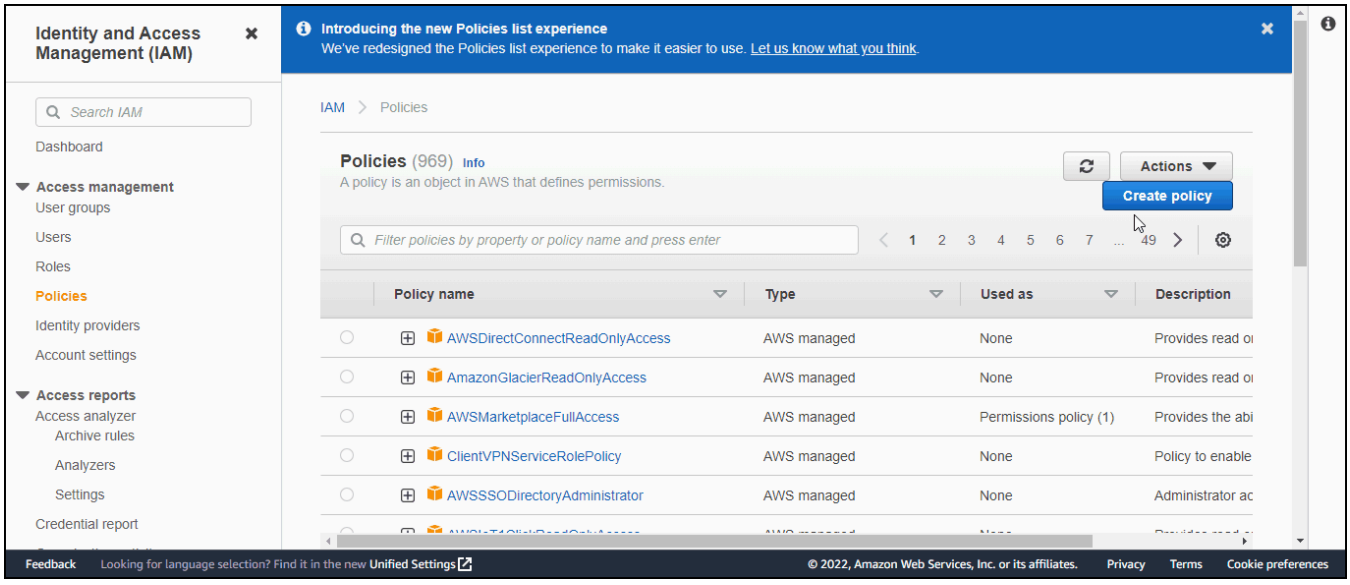
In AWS, policies are implemented by AWS IAM. As we have already covered the features of IAM in the previous task, we will directly see how policies are implemented.

Practical Exercise

Consider a scenario where a user wants to access resources during a particular date & time.

- Login to your AWS account, Open `IAM` in the services menu and click on `Open Policies`.
- Click on Create Policy — AWS IAM provides two approaches to create a policy, i.e. via **JSON & Visual Editor**.

- To define a policy, we first select a service and determine a certain action on a particular resource under a specific condition.



- In the above example, we have selected the service RDS and denied all permissions. We can attach the policy with an identity so the user cannot access the RDS service. The primary idea is to have a granular level of access control through policies to restrict or enable access to a specific resource.

Answer the questions below :

```
1. In a cloud environment, can we create a policy to enable Database access for
A. yea
```

Task 7 Security Through Network Management

Network security is an essential component of cloud security to protect the infrastructure from intruders. Cloud computing is inherently different from the on-premises model, wherein various approaches, including physical firewalls, protect on-premises deployments. Generally, network security of cloud infrastructure is maintained by following a layered approach:

- **Layer 1 — Network Security through Security Groups:** Security groups are the most fundamental aspect of maintaining network security in cloud infrastructure. In simple terms, security groups are a set of “allow rules” that allows specific traffic. Contrary to traditional firewalls, security groups do not have “deny rules”. The absence of any “allow rule” against particular traffic means it is denied. So we can say that security groups operate on the principle of “**deny all unless allowed explicitly**”.
- **Layer 2 — Network Security through Network Access Control Lists (NACLs):** The concept of NACL is related to protecting the Virtual Private Cloud (VPC). NACLs are used to create rules to protect specific instances of VPC. NACLs are different from Security Groups in that NACLs contain “deny rules” as well; e.g. we may make a rule to block a particular IP address from accessing the VPC.
- **Layer 3 — Vendor Specific Security Solutions:** Cloud computing service providers are also well aware of the inherent weaknesses & cyber-attacks that can target their infrastructure. So they have deployed their specific security solutions. These solutions vary from vendor to vendor, e.g. AWS has DNS Firewall & Network Firewall both.

Network Security in AWS

The following components manage network security in AWS:

- Security Groups.
- Network Access Control List.
- DNS Firewall.
- Network Firewall

Practical Exercise

In this exercise, we will Deny All Traffic on Port 22 via NACL through the following steps:

- Login to your AWS account & Navigate to VPC in the services menu
- Open NACL in the left pane & Click on `Create Network ACL`

- Enter basic settings such as name, VPC and tags (optional) and click create network ACL

- Select the newly created ACL and Click on `Edit Inbound Rules` under the **Inbound Rules** tab. Now create a “New rule” and configure settings as shown in the figure below:

The above rule will deny all the traffic at port 22. We can also allowlist/blocklist specific IPs for connecting to any port to limit the attack surface for the intruder.

Answer the questions below:

```
1. Is it a good practice to operate security groups on the principle of “deny a
A. yea
```

Task 8 : Security Through Storage Management

As we have studied in Task 2, storage is crucial in cloud computing. Storage security in a cloud environment aims to ensure that data must remain safe while at rest and in transit during the various phases of the data lifecycle. The following approaches provide cloud storage protection:

- **Create Geographical Boundaries**: Define geographical regions and set policies permitting data access.
- **Set Role-based Authorisation**: Create identities and assign roles to access a particular data set per the rights and privileges.
- **Data Encryption**: Almost all cloud service providers allow data encryption at rest. With this approach, server-side encryption is applied to data.

Important Aspects

For any storage (file, database, etc.), the following aspects are of utmost importance:

- Connection String with database containing hostname, username and password must be used using secure means.
- Access security policy.
- Data encryption standards.
- Physical security measures by the cloud service provider.

Storage Security in AWS

The cloud environment provides different types of data repositories to store data. In terms of AWS, we have Relational Database Service (RDS), Simple Storage Service (S3), Redis, etc., to keep and retrieve data. Data security is ensured by applying various policies to database instances per the data sensitivity.

Practical Exercise

In this example, we will Create S3 Bucket and enable data encryption at rest.

- Login to your AWS account & Navigate to S3 in the services menu.
- Click on create bucket & Enter basic information such as bucket name, AWS region, etc. The bucket name must be globally unique; there can’t be two buckets with the same name.

- Enable Server Side Encryption and select `Encryption Key Type`. For the demo, we have selected “Amazon S3 managed keys".
- Now click, `Create bucket`. Congrats, you have created your first S3 bucket with server-side encryption.

Answer the questions below :

```
1. Encryption of data at rest is unnecessary if we carry out encryption at trar
A. nay
```

Task 9 : Cloud Security — Some Additional Concepts

Disaster Recovery (DR) & Backup

Cloud is considered an excellent source for establishing Disaster Recovery and Backup sites. In cloud computing environments, there is a famous terminology known as **Cloud Disaster Recovery (CDR)**, a combination of approaches, tools & techniques that ensures backup data, resources and other applications on cloud infrastructure. In case of any disaster, cloud service providers provide backups of on-premises environments to ensure the regular continuity of business operations. Following are the essential concepts in terms of Disaster & Recovery in cloud computing through the following three approaches:

- **Cold DR:** This is the most straightforward approach and inexpensive but has the largest RTO (Recovery Time Objective). It entails storing data and saving images

& snapshots of machines. All snapshots must be recovered to resume business operations in a disaster situation.

- **Warm DR**: It works on the principle of near real-time synchronisation of actual data and applications with disaster sites. A copy of all data and services is being maintained at the DR setup, hosted on a cloud environment. This data is just being kept as a backup to resume business operations in a disaster scenario. When a disaster occurs, the DR site is configured to resume operations. RTO, in this case, is the time required for configuring the DR site to become operational.
- **Hot DR**: It has practically zero RTO but is the most expensive. In this approach, the actual and DR sites work in parallel and share the workload through load balancers. In case of disaster, all workload is shifted to the DR site.

Security through Monitoring & Logging

It is accurate to say that monitoring and logging are the hallmarks of maintaining security, and cloud computing is no exception. Nowadays, cloud service providers provide excellent approaches to logging and monitoring. Customers can take advantage of this option to keep an oversight on all the operations of their cloud environment. Following are some generic logging and monitoring approaches in a cloud computing environment:

- **Real-time Logging**: Almost all cloud service providers monitor and log all identities and resources.
- **Monitoring & Logging of API Calls**: All cloud instances have the provision for recording API calls made to cloud infrastructure. Typical logs include the source IP address of the user or service, time, etc.
- **Credential Reports**: Another essential thing that cloud service provider monitors are user accounts logs. Common logged factors include user account, account last used date, password last change data and password last used date, etc.

Monitoring & Logging into AWS

The following components manage monitoring and logging in AWS:

- Identity & Access Management: Basic logging features related to access management, e.g. logs credential reports of user accounts.

- CloudTrail: Logs all API calls made to AWS resources.
- CloudWatch: Monitors the entire cloud infra and informs about applications status performance changes, ensuring better resource utilisation.
- GuardDuty: Ensures continuous monitoring of malicious activity and unauthorised behaviour.

Practical Exercise

In this exercise, we will generate Credential Report for the AWS account. IAM provides an excellent feature of generating a credential report that lists all users and the status of their credentials, including passwords, Multi-Factor Authentication Status, usage & change history.

- Login to your AWS account by visiting `console.aws.amazon.com` & Navigate to `IAM` in the services menu.
- In the navigation pane, choose `Credential Report` & click “Download Report” on the next page.

- The report will be downloaded in CSV format and contain various vital fields, such as `password_last_used, password_last_changed, user_creation_time, etc.`

Updates & Patching

Updating & patching is an essential parts of the calculus of the entire security paradigm. In cloud computing environments, “Automated & Scheduled Patch Management” ensures that security and other related updates are routinely applied.

Patch Management in AWS

Patch management in AWS is managed by a component called “Systems Manager”. Patch Management in AWS has the following concepts:

- Patch manager ensures automatic & scheduled updating of cloud resources and can be used to update operating systems and applications.
- Provides scanning option to scan complete infrastructure regarding missing patches.

Practical Exercise

In this exercise, we will gain an understanding of AWS Patch Manager.

- Log in to your AWS account & Open `Systems Manager` from the services menu.
- Open `Patch Manager` in the left window under Node Management.

- There are two types of patching mechanisms, i.e., Patches without a Schedule and Scheduled Patching.

- We will click on Patch Now for patching without scheduling this task. In the next section, we must enter all the necessary details for patching.

Answer the questions below :

```
1. Is it a good practice to keep Disaster Recovery Backups of a server in the s
A. nay
```

Task 10 : Conclusion

In this room, we have briefly touched on significant security aspects of the cloud. The complete ecosystem of cloud security can be summarized into the following categories:

- **Security through access management:** Ensure that the right people should perform the right job within the right set of permissions.
- **Security through policies:** Set conditions and guidelines under which users & resources can perform specific actions.

- **Security through networking:** Ensure that cloud instances remain safe from network-oriented attacks.
- **Security through storage management:** Ensure the security of sensitive data stored in cloud storage through various means, including encryption and geographical settings, etc.
- Essential concepts like security through logging, Disaster Recovery & Backup, the importance of updates, etc.

Cloud computing is an emerging field that has gained popularity due to its two distinctive features: pay-as-you-use and on-demand scalability. With these features, usability and acceptance of cloud computing have increased manifold, giving rise to security threats. Fortunately, cloud computing service providers offer robust security features “ready to be deployed” by the customers. These features are not only easy to be deployed but also provide resilient security protection.

A complete pathway will be designed explicitly to protect cloud infrastructure in upcoming rooms.

Thankyou For Reading.

Tryhackme | Tryhackme Walkthrough | Cloud | Cloud Security | Cloud Computing

Follow

Published in InfoSec Write-ups

49K Followers · Last published 10 hours ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Follow

Written by Md Amiruddin

155 Followers · 6 Following

This is a profile of a cybersecurity enthusiast and CTF writer. He is an experienced information security professional and highly motivated individual.

No responses yet

What are your thoughts?

Respond

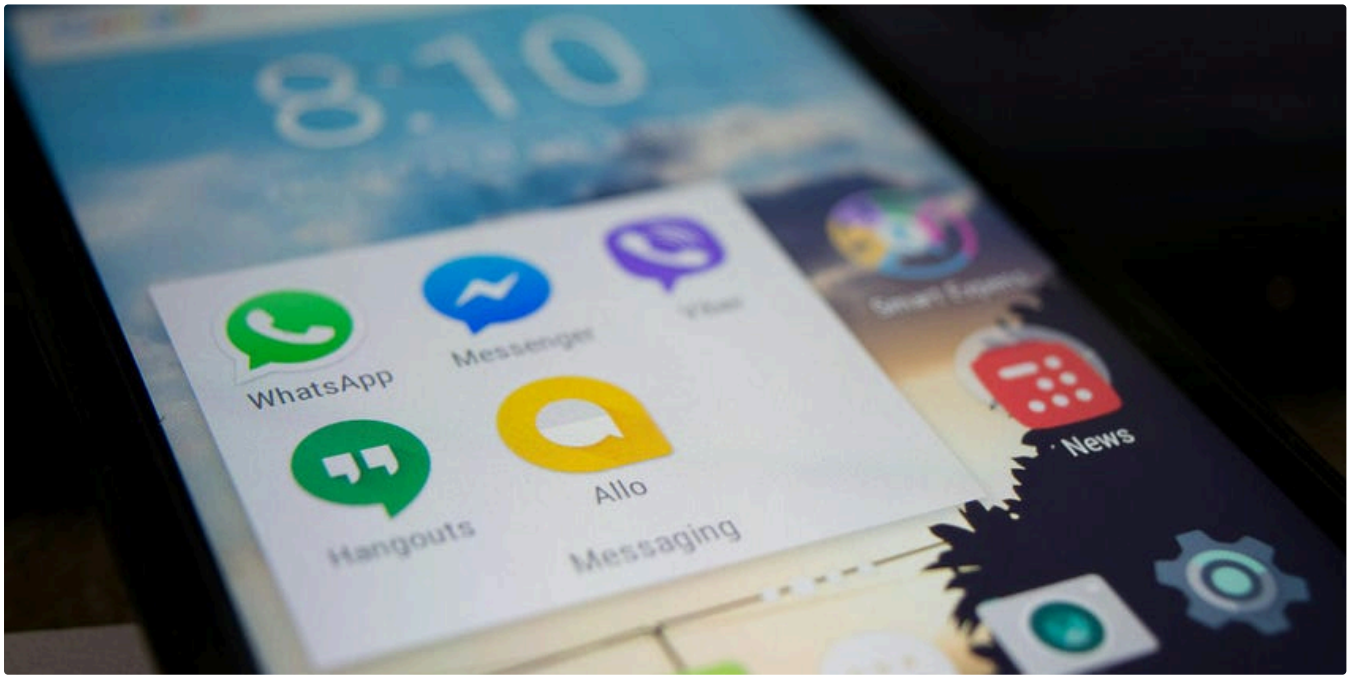
More from Md Amiruddin and InfoSec Write-ups

In InfoSec Write-ups by Md Amiruddin

Vulnhub Writeup/Walkthrough SickOS 1.1 | By Md Amiruddin

This CTF walkthrough is similar to the labs found in the OSCP exam course.

Dec 21, 2022

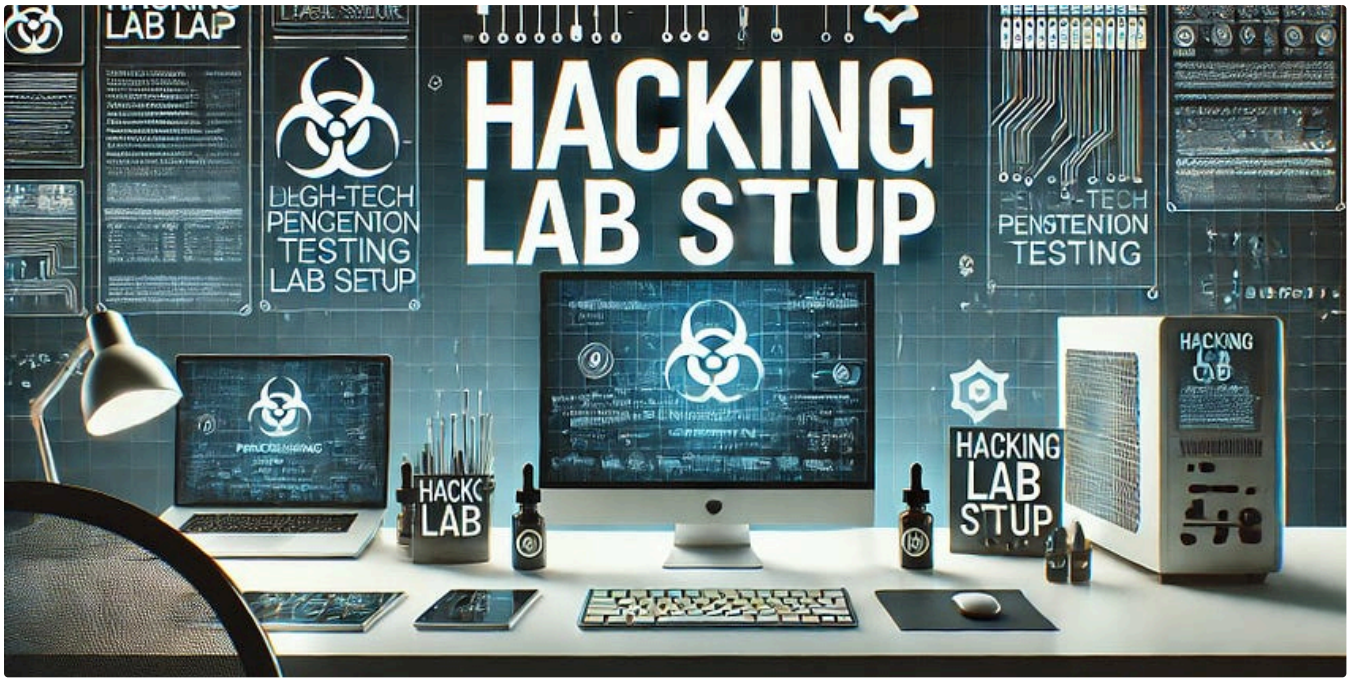


In InfoSec Write-ups by Visir

Could You Be the Next Victim? How to Protect Your Google Account Now

Today, nearly everyone is connected to the internet, and this dependency grew exponentially during the COVID-19 pandemic. With more people...

6d ago 15



In InfoSec Write-ups by Shanzah Shahid

Hack Like a Pro: Mastering Penetration Testing with Virtual vs Physical Lab Setups

Learn how to build a powerful, cost-effective testing environment to sharpen your ethical hacking skills.

2d ago 44 2

In InfoSec Write-ups by Md Amiruddin

Intro to Docker | Tryhackme Writeup/Walkthrough | By Md Amiruddin

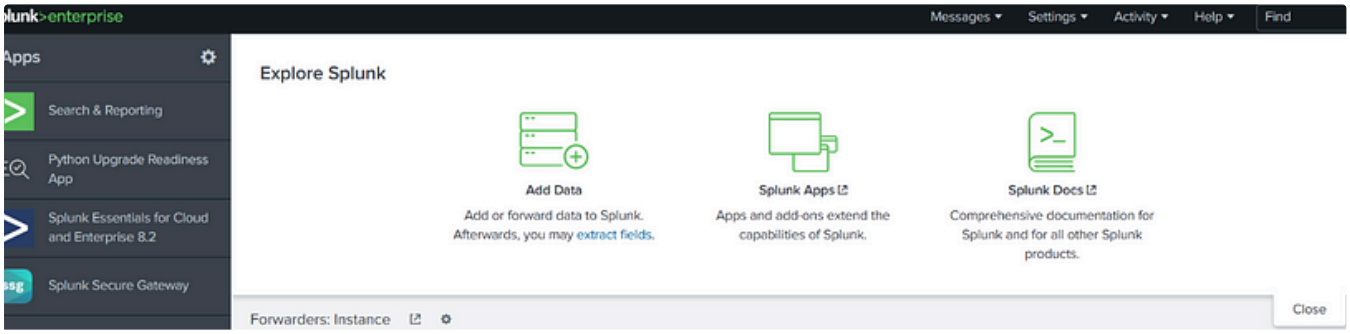
Learn to create, build and deploy Docker containers!

May 5, 2023 5

See all from Md Amiruddin

See all from InfoSec Write-ups

Recommended from Medium



Sudarshan Patel

📊 📈 Tryhackme | Splunk: Dashboards and Reports 🔒 📌

Creating Dashboards and Reports in Splunk.

Jul 27, 2024

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

Sep 7, 2024 10

Lists

Staff picks

793 stories · 1548 saves

Stories to Help You Level-Up at Work

19 stories · 909 saves

Self-Improvement 101

20 stories · 3184 saves

Productivity 101

20 stories · 2697 saves

IritT

SOC Lab: Building a Cybersecurity Environment for Threat Detection and Defense

Creating a home cybersecurity lab is one of the most effective ways to gain a deep understanding of network security, traffic management...

Dec 5, 2024 2

In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50

Sunny Singh Verma [SuNnY]

Multi-Factor Authentication TryHackMe Writeup | Detailed | → SuNnY

Room PreRequisites

Sep 4, 2024 50

CyferNest Sec

JWT Security | TryHackMe Walkthrough

TASK 2: Token-Based Authentication

Nov 26, 2024

See more recommendations