القرصنة الأخلاقية في الحوسبة السحابية

د. ماجد سعيد أفندي
باحث ومختص في الأمن السيبراني

Website: **https://drmajedafandi.com/**
Twitter: **@dr_MajedAfandi**

عن هذه الدورة

المواضيع التعليمية

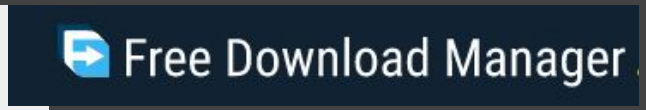
- التعرف على مفاهيم وخصائص ومكونات الحوسبة السحابية
- الإختراق الأخلاقي ومراحله في الحوسبة السحابية
- التعرف على أدوات وأساليب إختراق خدمات الحوسبة السحابية - تطبيق عملي

متطلبات المعمل

1. Download and install VirtualBox
2. Download the Kali VirtualBox image

Supportive Tools:

- Download Manager
- official 7z app



مراجع الحلقات

- جميع المصادر المذكورة يمكن الحصول عليها من خلال صفحتي في:

GitHub

رسالة إخلاء المسؤولية

المعلومات المقدمة في هذا التدريب هي من أجل أغراض تعليمية فقط, والمدرب غير مسؤول عن أي سوء استخدام للمعلومات.

قد تكون بعض الأدوات والتقنيات المستخدمة في هذه الدورات التدريبية غير قانونية حسب أنظمة بعض الدول, يرجى مراجعة القوانين المحلية الخاصة بك.

يرجى ممارسة وإستخدام جميع الأدوات المقدمة في هذا التدريب في معمل غير متصل بـ إنترنت ليس لك أو أي لأي شبكة أخرى

Disclaimer Message

The information provided on this training is for educational purposes only. The instructor is not responsible for any misuse of the information.

Some of the tools and technologies used in these training sessions may be illegal depending on where you reside. Please check with your local laws.

Please practice and use all the tools that are shown in this training in a lab that is not connected to the Internet or any other network.

محاور الفصل الأول-

- مفاهيم وخصائص الحوسبة السحابية
- الإختراق الأخلاقي ومراحله في الحوسبة السحابية

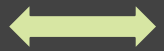
تعريف وخصائص الحوسبة السحابية

National Institute of Standards and Technology (NIST)

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources

Cloud Services Essential Characteristics:

- On-demand self-service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured services



المعهد الأمريكي الوطني للمعايير والتقنية (NIST)

الحوسبة السحابية هي إطار يسمح بالوصول المناسب والسريع عبر الشبكة إلى مجموعة مشتركة من موارد الحوسبة عند الطلب لإستخدامها على أن تتوفر فيها الخصائص التالية:

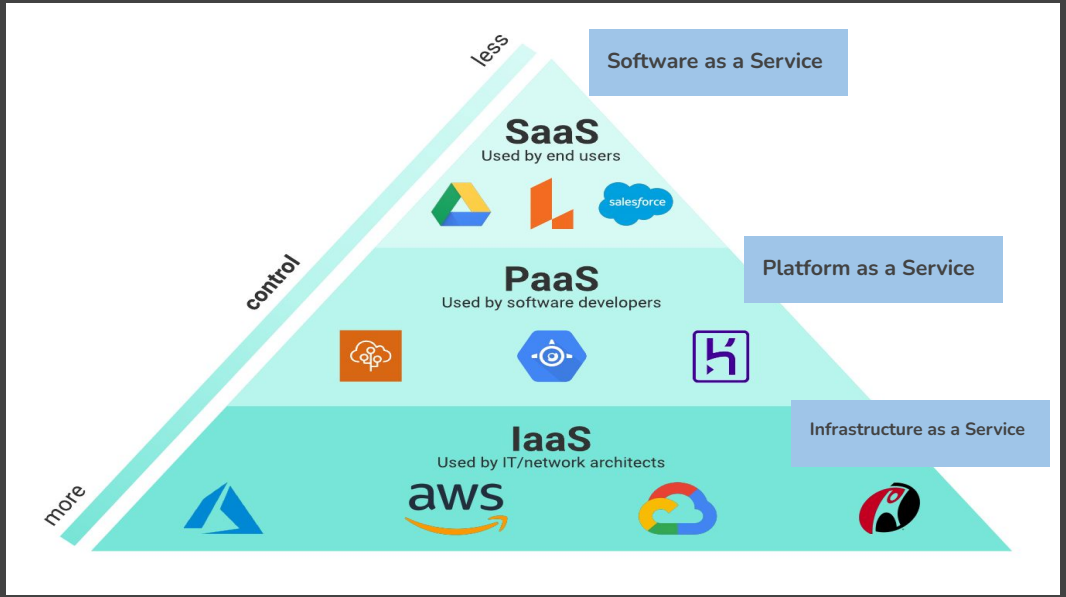
- طلب الموارد بناء على الخدمة الذاتية
- وصول واسع للشبكة (من أي مكان)
- تقديم موارد الحوسبة بكافة أنواعها وبشكل مرن ومتسارع

Cloud Service Models

SaaS: Software services through applications that are hosted, packaged, and delivered by third party cloud providers.

PaaS: Provides the facilities & platforms required to support the complete lifecycle of building, deploying and delivering web applications without worrying about storage and infrastructure capabilities

IaaS: Provides technology infrastructure (storage, networking, servers, and other computing resources via the cloud)



Cloud Deployment Models

Public Cloud: Provides computing services via shared IT infrastructure built in a multi-tenant architecture

Private Cloud: Provides computing services via a proprietary architecture dedicated to a single subscriber or business entity

Hybrid Cloud: Orchestrate the integration of various IT infrastructures that are hosted in different environments (on-premises, private/cloud) into a single, unified, and agile computing infrastructure

Community Cloud: Provides computing services via a proprietary architecture dedicated to a single subscriber or business entity

Multi-Cloud Model: Provides the facilities & platforms required to support the complete lifecycle of building, deploying and delivering web applications without worrying about storage and infrastructure capabilities

Example- AWS Cloud Services

Compute
- Amazon EC2
- AWS Lambda
- Amazon Elastic Container Service (ECS)

Storage
- Amazon Elastic Block Store (EBS)
- Amazon Simple Storage Service (S3)
- Amazon Glacier

Application Services
- Amazon Simple Notification Service (SNS)
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)

Networking
- Amazon Virtual Private Cloud (VPC)
- Subnets
- Routing
- Network Access Control Lists
- Security Groups

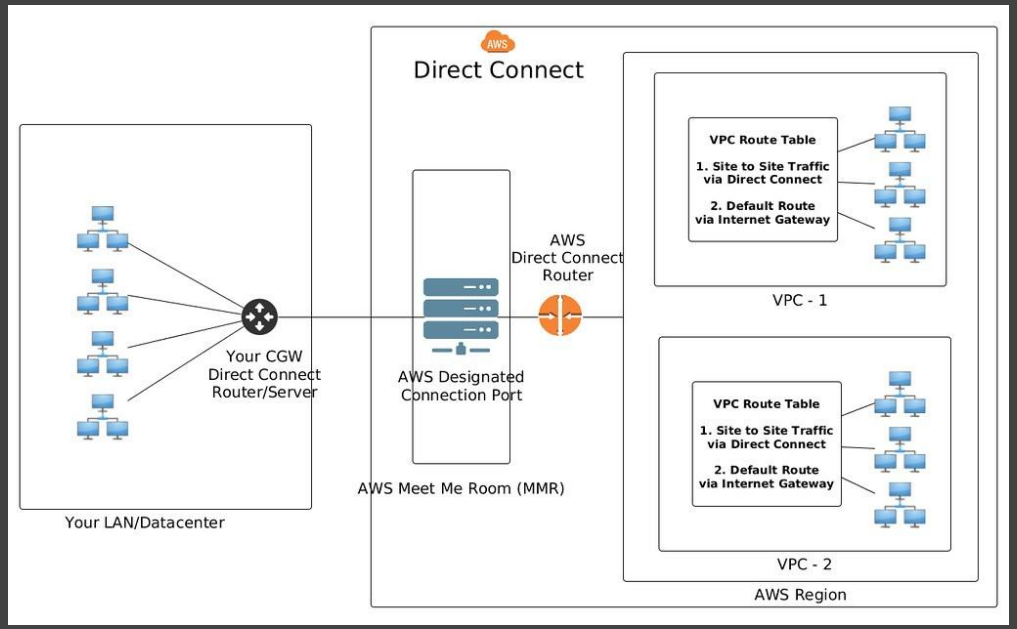
Development/Deployment
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodeBuild
- AWS CodePipeline
- AWS Elastic Beanstalk
- AWS OpsWorks

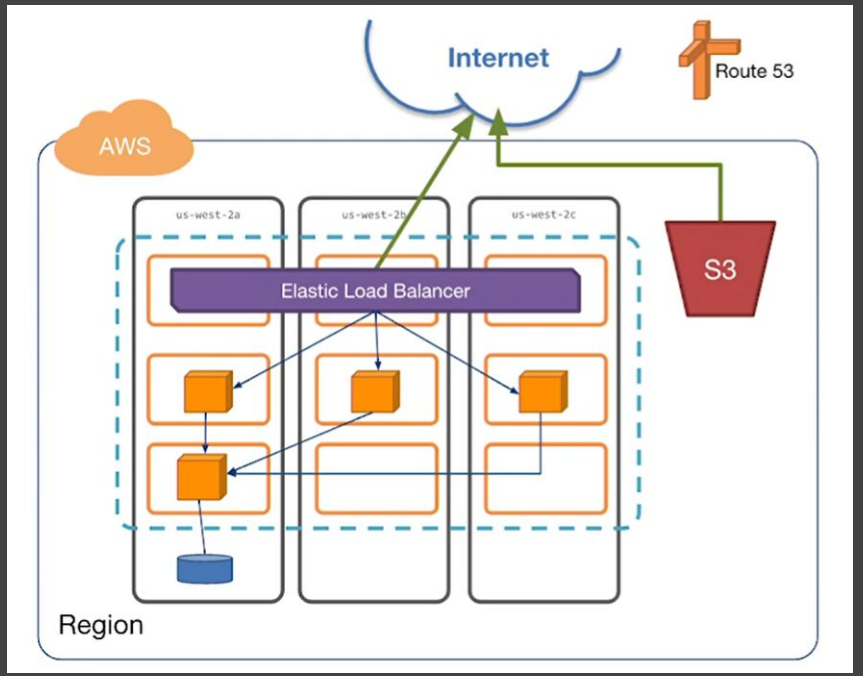
Datastores
- Amazon Relational Database Service
- Amazon DynamoDB
- Amazon ElastiCache
- Cassandra/Mongo (on EC2)

Analytics
- Amazon Kinesis
- Amazon Elasticsearch Service
- Amazon Redshift
- Amazon EMR
- Amazon Athena

amazon web services

Example- AWS Cloud Architecture





amazon web services

الجزء الثاني

الإختراق الأخلاقي ومراحله في الحوسبة السحابية

Pen-Testing Definition

"Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network." (NIST 800-115)

- It Involves launching real attacks to look for or identify more than one vulnerability on one or more systems to assess the effectiveness of existing controls

Common Methodologies

- **Penetration Testing Execution Standard**
  - http://www.pentest-standard.org
- **OWASP Testing Guide**
  - https://www.owasp.org/index.php/OWASP_Testing_Project
- **NIST 800-115: Technical Guide to Information Security Testing and Assessment**
  - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
- **Open-Source Security Testing Methodology Manual (OSSTMM)**
  - http://www.isecom.org/research/

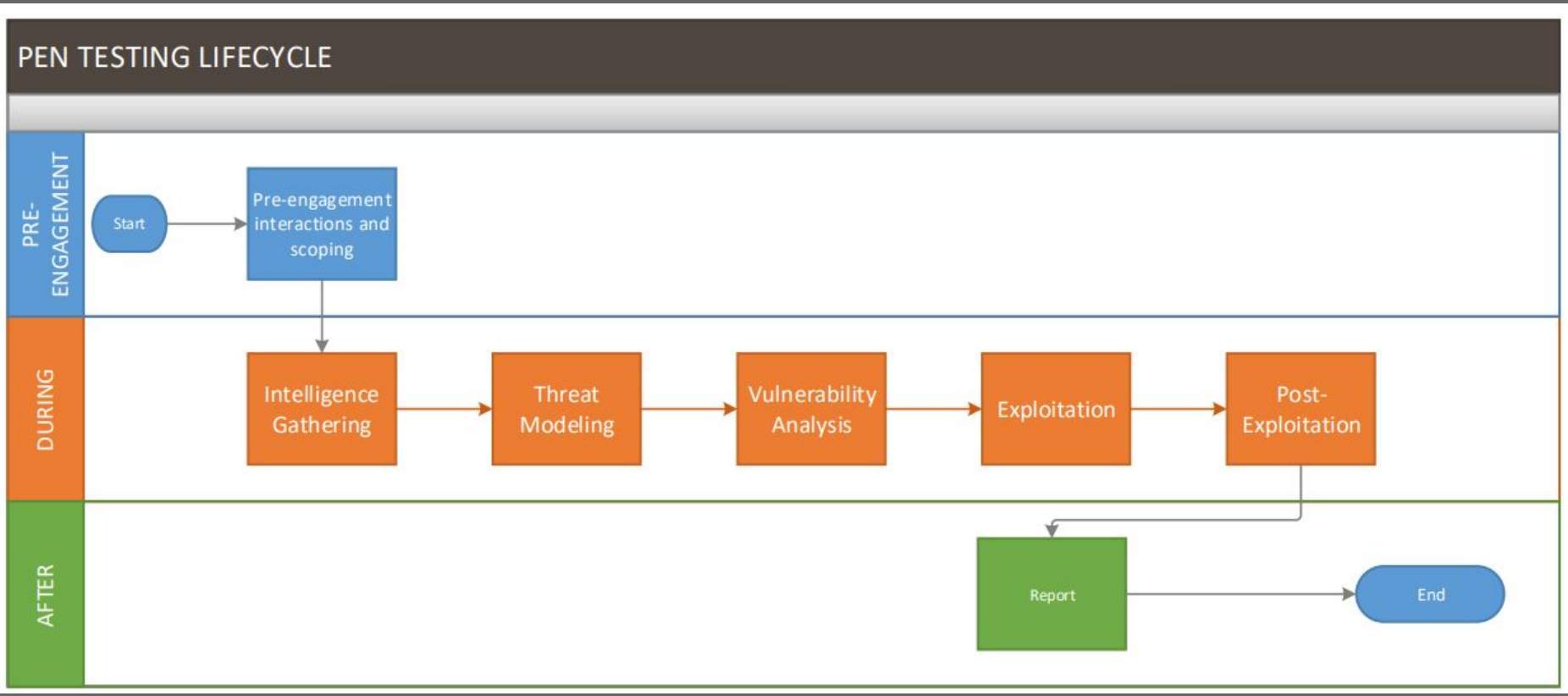
Types

White-Box: All info is provided to the individual conducting the pen-testing. This test type is normally used to test new applications before they are put into production and are routinely conducted as part of the SDLC to identify vulnerabilities before rolling out to production.

Black-Box: Only public info is provided mimicking hackers activities in real world. This test could miss some weaknesses that were not identified by the tester. Also, it can have an impact on production services as things might break down!

Gray-Box: This types sits in the middle of the two types above.

PEN TESTING LIFECYCLE



Aligned with: http://www.pentest-standard.org/

Pen Testing in the Cloud

SaaS

- Attempt to gain unauthorized access for a user or admin to obtain data
- Attempt to add/modify user accounts or create additional tokens on the system

Examples- gain email access to office 365 | gather customer info from Salesforce

In this scenario, you test the software itself through the appropriate channels, but generally SaaS is out of scope for applications pen testing

PaaS

- Attack the application at the container level
- Needs to be careful during the attack attempts and avoid exploiting the host or other non-client containers

In PaaS, there will be restrictions on escaping the VM/segments environments when conducting apps pen testings due to cloud nature of shared resources

IaaS

- Testing policies vary between service providers
- AWS provides a specific method for testing infrastructure including a list of permitted services
- Azure provides a specific testing lab for findings bug

This cloud architecture provides the least amount of restrictions since providers are limited in forcing security controls and let their clients decide how they construct their infrastructures

Attackers View of SaaS | PaaS | IaaS