Practice Labs - Ethical Hacker v10

Cloud Computing

Introduction

Ethical Hacking
Exploitation
Security
Cloud Computing
Vulnerabilities

Welcome to the **Cloud Computing** Practice Lab. In this module, you will be provided with the information needed to develop your knowledge.

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Cloud Vulnerabilities and Exploitation
- Exercise 2 - Protecting Cloud Resources

After completing this lab, you will have further knowledge of:

- Cloud Deployment Models
- Cloud Computing Services
- Benefits of Cloud Computing

- Threats to Cloud Computing
- Cloud Computing Attacks
- Cloud Security Considerations
- Cloud Security Deployments

Exam Objectives

The following exam objectives are covered in this lab:

- **4.2** Information Security Programs

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **45 minutes** to complete this lab.

Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

> Click **Next** to view the Lab topology used in this module.

Lab Topology

This lab contains supporting materials for Certified Ethical Hacker v10.

Click **Next** to proceed to the first exercise.

Exercise 1 - Cloud Vulnerabilities and Exploitation

Over the last few years, cloud computing has become increasingly popular. Many organizations have moved from on-premises infrastructure to cloud infrastructure.

Just like local infrastructure, cloud infrastructure has its own set of vulnerabilities and threats.

In this exercise, you will learn about cloud vulnerabilities.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Cloud Deployment Models
- Cloud Computing Services
- Benefits of Cloud Computing
- Threats to Cloud Computing
- Cloud Computing Attacks

Task 1 - Cloud Deployment Models

There are different cloud deployment models, which are as follows:

Private Cloud

A private cloud can either be set up by the organization itself or by a third-party service provider. In a community cloud, users share the same set of data.

Public Cloud

The public cloud works on shared infrastructure. The users usually have a subscription to pay-per-use fee models to access information in the public cloud. You can scale your infrastructure as and when you need to.

Hybrid Cloud

A hybrid cloud uses two different clouds - public and private. The database servers are in your private cloud, whereas the Web servers are hosted in the third-party cloud shared environment. The database servers will typically store the sensitive information and, therefore, need to be hosted on the private cloud. The front-end of the database servers, which is the Web site or Web application, is hosted on the public cloud for scalability purposes.

Community Cloud

In a community cloud, users share the same set of data and resources. It is accessed by multiple parties, such as universities and colleges that have the same goal.

Task 2 - Cloud Computing Services

There are different types of Cloud Computing Services available. When a user is accessing something in a cloud environment, they are accessing a type of cloud computing service.

The types of cloud computing services are:

Software as a Service (SaaS)

In Software as a Service, an application is licensed to users after they purchase a subscription. The license holder must then renew their subscription to continue to use the full features of the application. Typically, users will need a Web browser to access the application. For example, a GoToMeeting, which is hosted online.

Examples include:

- Dropbox
- Microsoft OneDrive
- Microsoft Office 365
- Cisco WebEx
- Citrix GoToMeeting
- Google Apps

Infrastructure as a Service (IaaS)

Infrastructure as a Service is an online service that provides the virtualization of underlying network infrastructures such as physical computing resources, location, data partitioning, scaling, security, and backups. Virtual machines, software-defined networking, and virtual network devices are all considered parts of the IaaS model.

IaaS provides flexibility in upscaling and downscaling the infrastructure as required. Moreover, it will allow the team to do the following:

- Create virtual machines (VMs)
- Install operating systems in each VM
- Deploy middleware
- Create storage buckets

Examples are:

- Amazon EC2
- Cisco Metapod
- Microsoft Azure
- Google Compute Engine (GCE)

Platform as a Service (PaaS)

In Platform as a Service, a platform for development is offered to users on a subscription basis. In this model, a set of development tools are provided by the service provider. It reduces the cost of purchasing these tools.

Examples are:

- Google App Engine
- Microsoft Azure
- Intel Mash Maker

Network as a Service (NaaS)

With Network as a Service, the clients have access to the additional network resources, such as switches and routers. The third-party provider owns the resources and provides it to an organization either through a fixed fee or component-wise fee.

Examples are:

- Amazon
- Rackspace
- AT&T
- Level 3 Communications

Security as a Service (SECaaS)

Security as a Service offers cloud-based security solutions. When you implement this solution, it removes the burden of having the on-premises hardware.

Examples are:

- Cloudbric
- CloudFlare
- Incapsula

Task 3 - Benefits of Cloud Computing

The reason behind the popularity of cloud computing is the benefits that it offers over on-premise computing. Below is a list of benefits that are offered by cloud computing:

IT Costs

Reduced IT costs are one of the key benefits of using cloud computing. For example, imagine you have to procure 10 or more servers to upgrade your infrastructure. It takes time to procure the server or any hardware. However, on the cloud, you can do this in a few minutes. You end up saving the huge cost of procuring the servers, reduce the delay drastically, and save on energy costs for the organization. You also save on the physical space needed for hosting the servers and the manpower that is required to manage them. When you need to decommission a server, it is also a quick process to release the server back to the service provider.

Scalability

Cloud computing allows you to scale your IT infrastructure up or down on an on-demand basis. You can provision new servers, add or remove memory, or any other component when required. All of this can happen within a few minutes. For example, if you know that your Web server is going to be overloaded over a certain time period, you can scale up your infrastructure during that time, then scale back down afterward.

Business Continuity

Cloud computing helps you protect your data in all kinds of situations, whether it is a natural disaster or simply a power outage. When you host your data in a cloud application, such as Microsoft OneDrive, your data is available instantly, as long as you have internet access.

In the backend, the data in the cloud is replicated to multiple servers, and depending on your location, you are directed to the servers that are near you. This allows fast access to your data.

For example, imagine that due to a malware attack, you have lost all your data on your laptop. If this data did not exist on the cloud, you would have to restore it from the backup, which could be a difficult or lengthy task. If the data existed on the cloud, such as in the Microsoft OneDrive application, the data could be restored must faster.

Loss Prevention

Assume that you have all your data stored on a file server within your office premises. The data from your laptop is regularly backed up to the file server. In a situation where there is a malware attack on the network, the file server and your laptop are affected. You are likely to lose your data.

If this data resided in the cloud environment, then even after losing data on your laptop, your data was safe in the cloud. The data is safe and can also be accessed from any other system or laptop that has an internet connection.

Collaboration Efficiency

Collaboration is another key advantage of cloud computing. Multiple users can work together on a single document or on a project. The access can be granted at different levels. For example, one user can be given Reader access, while the other users can have the Editor access. The access permissions can differ from application to application.

Automatic Updates

When you have applications in the cloud environment, you do not need to worry about the update process. The cloud service provider will update the applications or operating system as and when updates are available. You get the benefit of having the most updated and recent version of the application or operating system. This brings another advantage of freeing up your IT team from rolling out updates for applications and operating systems.

Security

The cloud service provider uses the latest security tools to monitor the data hosted by its clients. When you have inhouse data, you need to hire skilled security professionals and purchase security hardware and applications. When the data is hosted in the cloud, it is the cloud service provider's responsibility to protect your data.

Mobility

With the increased use of mobile phones, tablets, and laptops, users require 24/7 access to their data. A user can be on the move, in office, or at home when they want to access the data. This access becomes difficult when it is stored inhouse on the file servers. However, if the data is stored in the cloud, it is easy to access using a mobile phone, tablet, or laptop.

Task 4 - Threats to Cloud Computing

Just like an on-premise infrastructure, cloud computing is also prone to several threats. Some of the key threats to cloud computing are:

- Management interface failure
- Virtual Machine (VM) level attacks
- Compliance issues or risks
- Malicious insider
- Service failure
- Service termination
- Loss of encryption keys
- Weak authentication
- Network failure
- Licensing risks
- Hardware failure
- Privilege escalation
- Inadequate infrastructure design
- Unknown risk profile
- Cloud service provider shutting down

- Intentional or accidental data deletion
- Multitenancy
- Misconfigurations
- Access management issues

Task 5 - Cloud Computing Attacks

Just like the on-premise infrastructure, cloud computing is also prone to several types of attacks. These include:

- Social engineering attacks
- XSS attacks
- Domain Name System (DNS) attacks
- SQL injection attacks
- Wrapping attacks
- Network sniffing
- Session riding
- Side-Channel Attacks or Cross-guest VM breaches
- Cryptanalysis attacks
- DoS and DDoS attacks
- OpenStack component attacks
- Man-in-the-Middle (MITM) attacks
- VM level attacks

Most of these attacks are common to the on-premises IT infrastructure. For example, an XSS attack can be performed on an inhouse hosted Web application.

Exercise 2 - Protecting Cloud Resources

Along with the benefits, cloud computing also brings a wide spectrum of new security risks. You can use various methods to minimize and mitigate security risks. Even though the data resides in the cloud, it is your responsibility to protect it. Therefore, you must use various methods to ensure protection against data loss or theft and minimize the threats to data privacy.

In this exercise, you will learn about some common methods used to prevent the IoT device exploitation.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Cloud Security Considerations
- Cloud Security Deployments

Task 1 - Cloud Security Considerations

While working with cloud computing, you should keep the following security considerations in mind:

Geo-resilience

When opting for cloud services from a cloud service provider, you need to ensure that it offers enough security services to protect your data. You should also raise questions about the locations of the provider's data centers. You need to be assured that the cloud service provider can provide geo-resiliency in case of any incident, such as a fire or a flood. It is better to opt for a service provider that has a global presence and data replicated to multiple data centers.

Data Isolation

Malware, such as ransomware, is spreading fast. Just like any on-premises server or system, cloud-based systems can also be infected by it. Therefore, you need to ensure that the cloud service provider follows the practice of data isolation, which is to also keep an offline copy of the data.

Encryption

Without encryption, data at rest and in transit is vulnerable. If no encryption is used, there is a high risk of data loss or exposure of confidential data to an attacker. You need to ensure that when the data moved to or from the cloud or being moved between two clouds, it is encrypted.

Network Segmentation

Most cloud service providers use multitenant environments. When opting for a cloud service, you need to evaluate the type of segmentation that the cloud service provider is using and how your data will be segmented from the other customers who exist in the same multitenant environment.

It is best to use the zone approach that can help you isolate the following:

- Instances
- Containers
- Applications
- Full systems

Identity and Access Management

To protect your data, you must implement identity and access management policies. Strict access to the data must be implemented through policies that use access control lists. You also need to ensure that the privileges are role-based. When the data is in the cloud, you must enforce role-based access control. This can prevent unwanted access to the data. All access to the data must be monitored and tracked.

Monitoring

After you move the application and its data to the cloud, it will be the users who will be using them. You must ensure that the user actions are being monitored.

Password Usage

You must apply the password policies in the cloud environment. Most of the cloud service providers allow you to configure password policies. You must ensure that the users do not have simple passwords, and passwords must change after a certain duration. You should also implement account lockout policies.

Vulnerability Management

Most cloud service providers perform vulnerability management of their environment. If that is carried out, you should check the report. If you have deployed a custom Web application in the cloud environment, you must ensure that you perform a vulnerability assessment.

Patch Management

Each cloud service provider uses a method to perform patch management. While the cloud service provider will take care of the usual applications and operating system updates, you would need to focus on the custom applications that you have deployed. You need to ensure that all vulnerabilities are patched with the latest updates.

Alerts and Reporting

See what reporting is available through your cloud vendor(s) and use a tool such as SIEM (Security Information and Event Management) to integrate and centralize it with data from in-house and other vendor solutions as much as possible. This will allow you to have a complete picture of what is happening in your environment.

Incident Response Plan

You must ensure that the cloud service provider has an incident response plan to tackle any issue that may occur. The cloud service provider must have the ability to detect and respond to security incidents.

Task 2 - Cloud Security Deployments

The cloud security deployment refers to the security implementation and deployment of various tools and technologies, which can help to safeguard data in the cloud.

Application Layer

At the application layer, you need to deploy the Web Application Firewall (WAF). This will help you filter the traffic to the Web application.

Network Layer

There are various tools that can be deployed to protect the information at the network layer. Some of the key tools are:

- Next-Generation IDS/IPS devices
- Next-Generation Firewalls
- DNSSec tools
- Anti-DDoS tools
- OAuth configuration
- Deep Packet Inspection (DPI) tools

The Root of Trust (RoT)

RoT uses a trusted computing module that is trusted by the operating system. With the help of the trusted computing module, RoT is able to detect any unauthorized changes to the operating system or the programs that are installed. It is also capable of detecting the rootkits and can perform on the fly drive encryption.

Computer and Storage

Computer and storage can be secured using various methods, such as:

- Host-based Intrusion Detection (HIDS)
- Host-based Intrusion Prevention Systems (HIPS)
- Integrity checks
- File system monitoring

- Logfile analysis
- Kernel level detection
- Encryption

Physical Security

Physical security is a critical part of securing the information. No matter what you use to secure your information, if the device holding the information is not secure and an attacker gets access, other security methods would fail.

Review

Well done, you have completed the **Cloud Computing** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Cloud Vulnerabilities and Exploitation
- Exercise 2 - Protecting Cloud Resources

You should now have further knowledge of:

- Cloud Deployment Models
- Cloud Computing Services
- Benefits of Cloud Computing
- Threats to Cloud Computing
- Cloud Computing Attacks
- Cloud Security Considerations
- Cloud Security Deployments

Feedback