Name: Ankita Vartak

IST 615

Lab1 – Virtual Machines in Azure

PART -1

In this Lab we are creating a Linux Virtual Machine using Azure Portal and then we will be connecting to running Virtual Machine using SSH.

Here are some screenshots of my Lab work:

1. Created a SSH key from public key file:

Graphical user interface, text, application, email

Description automatically generated

1. Created VM:

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

1. Adding a value to private key path:

Graphical user interface, text, application, email

Description automatically generated

1. Commands executed:

Graphical user interface, text

Description automatically generated

1. Command “systemctl” executed to see if HTTP server is up and active:

A screenshot of a computer

Description automatically generated with medium confidence

1. In Network security added a new port for inbound rule to the VM:

Graphical user interface, text, application, email

Description automatically generated

1. Finally, the Apache server web page loads:

Graphical user interface, text, application, Word, email

Description automatically generated

PART -2

1. What is a key pair and what is it used for?

Using passwords with SSH connections makes the VM susceptible to password brute-force assaults even if SSH offers an encrypted connection. A public-private key pair, sometimes referred to as SSH keys, is a more reliable and preferred method of connecting to a Linux virtual machine with SSH.

1. Who stores the public portion of the key pair? Who stores the private portion of the

key pair?

* The public key is placed on your Linux VM or any other service that you

wish to use with public-key cryptography. This can be shared with anyone.

* The private key is what you present to verify your identity to your Linux VM

when you make an SSH connection. Consider this confidential information

and protect this like you would a password or any other private data.

1. What is SSH? What is it used for?

Secure Shell (SSH) is an encrypted connection protocol that allows secure sign-ins over

unsecured connections. SSH allows you to connect to a terminal shell from a remote

location using a network connection.

4. When you make a change to a network security group rule, does the change affect

only the instance you’re currently working on or other instances, too? Explain.

Yes, it does affect the other instances too. If no security group is applied, then all traffic is allowed by Azure. If the VM has a public IP, this could be a serious risk, particularly if the OS doesn't provide a built-in firewall. The rules are evaluated in priority order, starting with the lowest priority rule. Deny rules always stop the evaluation. For example, if a network interface rule blocks an outbound request, any rules applied to the subnet will not be checked. For traffic to be allowed through the security group, it must pass through all applied groups.

1. What is the effect of the default network security settings for a new virtual machine?

Last rule is a default rule added to every security group for both inbound and outbound traffic with a priority of 65500. That means to have traffic pass through the security group, you must have an allow rule, or the final default rule will block it.

a) Neither outbound nor inbound requests are allowed – Deny All rule

b) Outbound requests are allowed. Inbound traffic is only allowed from within the

virtual network. – By default

c) There are no restrictions: all outbound and inbound requests are allowed. – Allow rule

6. Suppose you have several Linux virtual machines hosted in Azure. You will administer these

VMs remotely over SSH from three dedicated machines in your corporate headquarters.

Which of the following authentication methods would typically be considered best-practice

for this situation?

a) Username and password – SSH Connection

b) Private key – SSH keys

c) Private key with passphrase – to access the VM

I think Private key with passphrase will be the best practice.