LOMBA KETERAMPILAN SISWA

SEKOLAH MENENGAH KEJURUAN
TINGKAT PROVINSI DKI JAKARTA XXX 2022

IT NETWORK SYSTEMS ADMINISTRATION

LKS2022_ITNSA_MODUL_A

MODUL A
CLIENT SERVER

Introduction

In this test project, you will be asked to install, configure, and integrate different services using GNU/Linux Debian and Windows virtual machines. If there is any required value for configuration that is not specified in the test project, you can use the default value.

General Configuration

Configure the hostname and IP addresses of all nodes to match the given details in this test project.

Edge Area

This area serves as the perimeter between **skill39.org** and **internal.net** to the external network.

Firewall

Configure firewall on **FW** using **iptables**. Drop all incoming traffic by default, and permit only necessary traffic required for all services in this test project to work.

NAT

To make the mail service and DNS service on the **skill39.org** network accessible from the external network, configure NAT on **FW.**

DHCP

Set **FW** as DHCP server for the **skills39.org** network. **SRV-1** & **SRV-2** should lease IP addresses from this DHCP server with static leases.

HAProxy

Configure HAProxy to serve **https://www.internal.net, https://private.skills39.org, and https://www.skills39.org**. HTTP access should be redirected to HTTPS, and enable the built-in HAProxy statistics page on port 2022.

DMZ Area

This area consists of servers that serve public services.

Mail

Configure a mail server on **SRV-1** for the **internal.net** domain. Mail Server can be accessed from **mail.internal.net**. SMTP Submission with TLS, IMAPS, and POP3S should be configured so users can send and receive emails securely. Active Directory users should be able to authenticate to the mail server.

Web

Install **Nginx** on **SRV-1** and **SRV-2**. Configure two websites on both servers:

- www.skills39.org
    - Document root: /opt/web/www.skills39.org
    - Web content: Welcome to www.skills39.org
- private.skills39.org
    - Document root: /opt/web/private.skills39.org
    - Web content: Welcome to private.skills39.org
    - Use basic authentication: should be accessible by Active Directory users.

The web server should only listen on port 8080 and add a specific HTTP Header **X-Served-By: skills39.org**.

DNS

Set up BIND9 as an authoritative DNS server for **skills39.org** on both **SRV-1** & **SRV-2**. **SRV-1** should be configured as the master DNS server, while **SRV-2** acts as the slave DNS server. When a new DNS record is created on **SRV-1**, it should be replicated automatically on **SRV-2**.

VRRP

Configure VRRP on both **SRV-1** & **SRV-2** with virtual IP **10.10.10.100**, with **SRV-2** acting as the standby one. When the network interface of **SRV-1** is down, the **SRV-2** should be promoted to become active. The virtual IP should be used as the published address for the DNS and Web service.

Internal Area

This area contains services that are mostly used for internal purposes and dependencies that are required for services in the DMZ area. Services in this area should not be accessible publicly, except for VPN.

Active Directory

Configure a new Active Directory forest **internal.net** with **DC** as the primary controller, and use the highest available forest version. Populate this forest with 1000 Active Directory users, **user0001@internal.net** - **user1000@internal.net**, with password **P@ssw0rd**. Configure the following policies for all entities in the AD forest:

- Hide Recycle Bin
- Logon Banner with any content
- Automatic share mount on drive Z: to SMB share on **FILES**.

Certificate Authority

Set up Active Directory Certificate Service on **DC** to configure it as a root Certificate Authority. All TLS certificates needed in this test project should be signed by this root CA and trusted on all nodes.

File Share

Create an SMB share on **FILES** from physical path **C:\Shares**, and make this SMB share invisible. The **C:\Shares** directory should contain the following directories:

- Public: Readable by all Active Directory Users
- Private: Full access only for **user0991@internal.net - user1000@internal.net.**

When accessing the share, users should only see the directory to which they have access and should not be allowed to put files with the **txt** extension.

iSCSI

Add two additional virtual disks on **FILES** of any size. Use the virtual disk to create an iSCSI target that will be mounted on **SRV-1** & **SRV-2** to be used as the document root for their websites.

Web

Configure IIS Web Server on **FILES** to serve **https://www.internal.net**. This site should be accessible from the external network. Use **C:\www\www.internal.net** as the document root.

VPN

Set up a remote access VPN on **FILES** with client certificate authentication. When connected to the VPN, the client should be able to fully access the **skill39.org** & **internal.net** networks. Configure the VPN connection on **CLIENT**.

Logical Topology

