CST8246 – SBA Practice Exam

Scenario-Based Lab: Blue Lab Infrastructure

Background

ICT Corp. is launching a secure development environment called Blue Lab, utilizing the RED and BLUE networks. You are assigned to configure and validate core services such as SSH, DNS, Web, Mail, LDAP, Samba, and NFS on your assigned server (172.16.30.MN) and validate them using a dedicated client located in the 172.16.31.0/24 network.

To ensure network isolation and service integrity, firewall rules must restrict access from all networks except the client subnet (unless multiple networks access are required). All configurations and tests must be performed using custom Bash scripts as part of an automated deployment. Use your MAGIC# (MN) wherever applicable (e.g., IPs, alias IPs, filenames, hostnames, content etc).

Initial Setup

- Configure the server with a static IP for the RED network (172.16.30.MN).
- Add an alias interface using the IP 172.16.32.MN.
- Create a local user account named **admin** with password **sba**.
- Enable and configure SSH access, including necessary firewall permissions.
- Configure **default-deny firewall rules** to allow access **only from the client network** (172.16.31.0/24). Block all access from other networks.
- Open only the **necessary ports** required by your selected services (refer to the *Firewall Configuration Requirement* section).
- Services that require access from multiple networks (e.g., NFS) must explicitly define **firewall exceptions** in their configuration to allow access as specified.

- **MINOR SERVICES (Choose TWO – 2 Marks Each)**

#	Service	Description
1	SSH Access	Enable SSH key-based login for both **admin** and **root**. The client user **cst8246** must be able to connect admin and root only.
2	Basic DNS Setup	Configure the DNS zone for blue.lab with the following records: • An **A record** for your server and any relevant subdomains (e.g., www1.blue.lab, mail.blue.lab (172.16.30.MN)) • An **MX record** pointing to the mail server for the domain (mail.blue.lab) • A corresponding **reverse zone** (PTR records) for the server and any configured alias IPs Additionally, **enable recursive DNS queries** from **31.0** network, allowing external systems to resolve names through your DNS server.
3	Basic Mail Service	Configure a mail service (e.g., Postfix) on your server to **accept and deliver messages addressed to** admin@mail.blue.lab. Ensure that the mail server: • **Listens on the appropriate interface** • Recognizes mail.blue.lab as a valid destination domain • Delivers mail locally to the user **admin** From the client (172.16.31.MN), **send an email to admin@mail.blue.lab** using mail or nc. On the server, **confirm message reception** by checking the local mailbox of the **admin** user.
4	Basic Web Hosting	Create and configure two separate web pages on your web server: 1. When accessed via **server IP address**, the page should display: **"MN + DEFAULT"** 2. When accessed via **www.blue.lab**, the page should display: **"MN + BLUE"** Ensure proper **virtual host** setup, DNS or /etc/hosts resolution for www.blue.lab, and confirm both pages load correctly from a web browser from the client machine.
5	Basic LDAP Directory	Create a new directory structure under the domain blue.lab, including a container named **people**. Add an entry for **Tom Arthur** with the attributes: • cn: Tom • sn: Arthur • mail: tom.arthur@blue.lab

		Ensure the entry is **searchable from the client** using an LDAP query.
6	Samba Public Share	Configure a Samba share named **samba-public** that is: • **Browsable** on the network. • **Read/write accessible** to all users without authentication. • **mounted** by the client. From the **client**, create a file named **readme.smb** inside the share containing: Your Full Name & Your Magic# Confirm: • The client can access and create the file. • The server can see and read the file contents.
7	Basic NFS Share	Configure a **shared** directory over NFS that: • Provides **read/write access** to any client on the network. • Is mounted by the client. From the **client**, create a file named readme.nfs in the shared directory containing: Your Name & Magic# Confirm that: • The file is created and visible from the server. • The contents are correct.

- **MAJOR SERVICES (Choose TWO – 4 Marks Each)**

#	Service	Description
8	Master/Slave DNS	Configure your server as the **DNS master** for the domain blue.lab, including both **forward and reverse zones**. Configure the client system as a **DNS slave**, capable of receiving full zone transfers. • dns1 (primary nameserver) for blue.lab should point to your server's **main IP address** (172.16.30.MN), and • dns2 (secondary nameserver) should point to your server's **alias IP address** (172.16.32.MN). On the client, verify: 1. **Successful full zone transfers** from the master. 2. **Proper name resolution** for both forward (name → IP) and reverse (IP → name) lookups using dig.
9	Advanced Web Hosting	Host three **virtual websites** on your server: • www1.blue.lab • www2.blue.lab • secure.blue.lab (**served over HTTPS** and bound to your **alias IP**, 172.16.32.MN) Each site must: • Be configured using **Apache Name-Based Virtual Hosting** (for HTTP) • Use **a separate virtual host block** for HTTPS (for secure.blue.lab) • Display your **MAGIC#** and the **site's domain name** in the page content for identification On the client, verify: 1. HTTP access to www1.blue.lab and www2.blue.lab 2. HTTPS access to secure.blue.lab 3. Each page correctly displays your MAGIC# and domain name
10	Advanced Mail with Alias	Configure your server to **accept incoming mail addressed to** labfinal@blue.lab and **redirect it to a local user account** named foo. Additionally, **masquerade the server hostname** in outgoing mail so that messages appear to come from blue.lab instead of the actual system hostname. From the client (172.16.31.MN): • Send an email to labfinal@blue.lab • Confirm the mail is received and **delivered to the local user foo** on the server Validate: • Successful message delivery • Proper hostname masquerading in headers • Presence of the mail in foo's mailbox

11	LDAP with Host Entry	Configure your LDAP server to include a container (organizational unit) named hosts under the domain blue.lab. Inside this container, create an **LDAP entry for the device** www.blue.lab, including appropriate attributes such as ipHostNumber and cn. From the **client**, verify that the entry for www.blue.lab can be successfully **queried and resolved** via LDAP directory lookups.
12	Samba Private Share	Create a samba-private share: • Grant read/write access to **user1**, who must create a file ReadMe.smb containing their name • Grant read-only access to **user2** Verify both access levels from the client and confirm visibility from the server.
13	Advanced NFS	Create a **restricted** share under /srv/nfs via NFS with: • Read/write access for clients in the 172.16.31.0/24 subnetwork • Read-only access for clients in the 172.16.30.0/24 subnetwork Validate correct permission enforcement by creating and reading a file from both networks. (filename: ReadMe.nfs)

Firewall Configuration Requirement

For all services configured and tested in this exam:

- You must allow access **only from the client network 172.16.31.0/24**.
- Block all access from:
    - 172.16.30.0/24
    - 172.16.32.0/24

Note:
Services requiring **multi-network access** (e.g., NFS with read-only from 172.16.30.0/24 and read/write from 172.16.31.0/24) must explicitly define **firewall exceptions** for those networks and ports.
The **default-deny policy** still applies to **all other services and ports** from 172.16.30.0/24.

- Ensure that only the **necessary ports** are opened per service:
    - **SSH:** TCP 22
    - **DNS:** TCP/UDP 53
    - **Web:** TCP 80 and 443
    - **Mail:** TCP 25
    - **LDAP:** TCP 389
    - **Samba:** TCP 139, 445 and UDP 137, 138
    - **NFS:** TCP/UDP 2049 + required rpcbind, mountd, etc.

Your firewall rules must be part of your **Bash configuration scripts** and should be **validated** as part of your testing process.

Submission Guidelines

- You must configure and test **all selected services** using **custom Bash scripts**.
- For each selected service:
    - Write a dedicated Bash script that performs the configuration **automatically**.
    - Include validation steps inside the script or as a separate script.
- Organize your submission as follows:
    - A folder containing:
        - setup_<service>.sh for each service (e.g., setup_dns.sh, setup_samba.sh)
        - test_<service>.sh or inline testing logic
        - A main script (optional) to call all your scripts
    - A .doc or .pdf file with:
        - Screenshot evidence of script execution and successful output
- Submit the entire folder (zipped if needed) along with the documentation to the **corresponding Brightspace folder**.

Manual configuration without scripting will result in a grade penalty.