Peer-graded Assignment: A new hire - you!

A new hire - you!

**PROMPT**

How would you solve business requirement 1, both technically and securely?

1. I will create all the servers with an up-to-date version of a CentOS-based Linux.

2. I will create DMZ for the servers that should not be accessed/viewed from outside of the network.

3. I will turn on the Firewall (Iptables/UFW) on all servers and accordingly, configure the servers.

4. I will turn off unnecessary services on servers, e.g., Log server, which has fewer interactions with normal users. In general, I will take the following preventive measures in order to increase the overall security of the servers. Use Strong and Unique Passwords. Generate an SSH Key Pair. Enable Automatic Updates for regular Software updates. Avoid Unnecessary Software. Disable Booting from External Devices and WAKE-ON-LAN service. Close Hidden Open Ports. Scan Log Files with Fail2ban.

5. I will use Ansible to automate system updates and software installation with secure SSH.

**PROMPT**

How would you solve business requirement 2, both technically and securely?

I will create different groups and assign proper permission to the group and each user. Users will be authenticated using LDAP.

**PROMPT**

How would you solve business requirement 3, both technically and securely?

I will try to expand my answer from several points of view: A user can be a member of several groups. For auditing purposes: During the audit, the auditor should check whether Linux systems allow remote login using SSH for everyone with root user status During the audit, the auditor should test the SSH passwordless login. Systems must be updated with the latest releases' patches, security fixes and kernels when those become available Auditing the Cron Jobs Status Auditing the Status of USB Devices Auditing the Status of SELinux Auditing Existing User Lists Auditing User Activities in the System as a result, auditor requires access to many resources in each department I will grant him super access to conduct his auditing without any troubles.

**PROMPT**

How would you solve business requirement 4, both technically and securely?

It is recommended to create a new user and assign root privilege to the user so that the user can run the admin task using sudo. Take a backup of files /etc/sudoers: edit file with visuo commanad and add the user names.

**PROMPT**

How would you solve business requirement 5, both technically and securely?

I block access to outbound traffic and allows only inbound traffic to the network in the firewall. I can also block the public IP.

**PROMPT**

How would you solve business requirement 6, both technically and securely?

They can have SSH access to the server. Provider RealVNC secure mode if the need GU option to access user the graphical and friendly.

**PROMPT**

Please upload any diagrams that support your positions in the prompts above here.