Linux Server Administration Playbook

Services Included:

- **BIND** (DNS)
- **NTP** (Network Time Protocol)
- **MySQL** (Database)
- **Nginx/Apache HTTP** (Web Server)
- **Splunk** (Monitoring and Logging)

1. Changing Passwords

Passwords for user accounts and services should be updated regularly.

Change User Passwords:

1. Log in as the root user or use sudo privileges.
2. Execute:

   passwd <username>
3. Follow prompts to set a new password.

Change MySQL/MariaDB Root Password:

1. Log into MySQL:

   sudo mysql -u root
2. Update the password:

   ALTER USER 'root'@'localhost' IDENTIFIED BY 'new_password';

   FLUSH PRIVILEGES;

   EXIT;
3. The commands for changing the MariaDB root password is different:

   SET PASSWORD FOR 'root'@'localhost' = PASSWORD('new_password');

Update Splunk Admin Password:

1. Navigate to the Splunk etc/passwd directory.
2. Edit the password file and restart the Splunk service:

   splunk edit user admin -password new_password -auth admin:old_password

   splunk restart

2. Finding Open Ports and Associated Services Using Netstat

Use netstat to list active connections and services:

1. Install net-tools (if not already installed):

   sudo apt install net-tools # For Debian-based systems

   sudo yum install net-tools # For Red Hat-based systems

2. Execute the command:

   sudo netstat -tulnp

3. Interpret the output:
   - **Proto**: Protocol (e.g., TCP/UDP)
   - **Local Address**: Server IP and port
   - **State**: Connection status
   - **PID/Program name:** Service that is listening behind that port

3. Downloading our GitHub Repo

Our GitHub repository contains all our useful scripts and playbooks. Download them using WGET command:

1. Execute the following commands (you might have to type it manually to your terminal):

   wget https://github.com/csamnsu/CCDC_public/archive/refs/heads/main.zip

   unzip main.zip

2. All the scripts should be under "CCDC_public-main/scripts" folder. Always make sure that you are executing these scripts as the "root" user.

cd CCDC_public-main/scripts

chmod 700 *

./<script_name> #Execute script

3. At the very least, execute the "clamav_fail2ban_install.sh" in order to install ClamAV and Fail2ban.
4. Execute the "generic_bkup.sh" script in order to look at the system info and backup the config files of MySQL, Apache HTTP and the entire "/etc" directory.

4. Disabling SSH

1. Run the SYSTEMCTL commands to stop and disable SSH server (normally OpenSSH):

   sudo systemctl stop ssh (or sshd)

sudo systemctl disable ssh (or sshd)

2. Once disabled, run netstat to ensure that nothing is listening behind port 22.

5. Checking running active services:

Run the following SYSTEMCTL command to see running services which are active (persistent over reboot):

sudo systemctl list-units --type=service --state=running

These are system or third-party software that may or may not be listening behind network ports. Crosscheck this list with the netstate output; this will provide a better understanding of the server's nature and purpose.

6. Disabling Unnecessary Logins (Without Deleting Accounts)

1. Lock user accounts:

   sudo usermod -L <username>

2. To unlock:

   sudo usermod -U <username>

3. Change user shell to a non-login shell (e.g., /usr/sbin/nologin):

   sudo usermod -s /usr/sbin/nologin <username>

7. Creating a Basic IPTABLES Scheme

Allow Specific Services:

- **DNS** (BIND): UDP 53, TCP 53
- **NTP**: UDP 123
- **MySQL**: TCP 3306
- **Nginx/Apache HTTP**: TCP 80 (HTTP), TCP 443 (HTTPS)
- **Splunk**: TCP 8089 (default management port)

Rules:

1. Flush existing rules:

   sudo iptables -F

2. Set default policies:

   sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

sudo iptables -P OUTPUT ACCEPT

3. Allow loopback interface:

   sudo iptables -A INPUT -i lo -j ACCEPT

4. Allow established connections:

   sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

5. Allow services:

   sudo iptables -A INPUT -p udp --dport 53 -j ACCEPT # DNS UDP

   sudo iptables -A INPUT -p tcp --dport 53 -j ACCEPT # DNS TCP

   sudo iptables -A INPUT -p udp --dport 123 -j ACCEPT # NTP

   sudo iptables -A INPUT -p tcp --dport 3306 -j ACCEPT # MySQL

   sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT # HTTP

   sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT # HTTPS

   sudo iptables -A INPUT -p tcp --dport 8089 -j ACCEPT # Splunk

6. Save rules (persistent across reboots):

   sudo iptables-save | sudo tee /etc/iptables/rules.v4

7. Verify rules:

   sudo iptables -L -n –v

8. Monitor logs:

Always monitor logs for suspicious activities (failed login attempts, services crashing/stopping etc.):

tail -f /var/log/syslog OR tail -f /var/log/messages