Born2BeRoot Project Notes

📘 Born2BeRoot Project Notes

🛠️ System Setup and Configuration

🔹 User Management

- **Create a User**:

  ```
  sudo adduser <username>
  ```

- **Add User to Sudo Group**:

  ```
  sudo usermod -aG sudo <username>
  ```

- **Change Username**:

  ```
  sudo usermod -l <new_name> <old_name>
  ```

- **Change User Home Directory**:

  ```
  sudo usermod -d /home/<new_folder_name> -m <username>
  ```

- **Delete User**:

  ```
  sudo deluser <username>
  ```

- **Switch Users**:

  ```
  su - <username>
  ```

- **Kill User Processes**:

```
sudo pkill -KILL -u <username>
```

- **Check if User Exists**:

```
id <username>
```

- **Check User Processes**:

```
ps -u <username>
```

- **Check User Groups**:

```
getent group <group_name>
# or
cat /etc/group
```

🔹 Hostname Configuration

- **Check Current Hostname**:

```
hostnamectl
```

- **Set New Hostname**:

```
sudo hostnamectl set-hostname <new_hostname>
```

- **Update Hostname in Configuration Files**:

```
sudo nano /etc/hosts
sudo nano /etc/hostname
```

- **Restart Hostname Service**:

```
sudo reboot
# or
sudo systemctl restart systemd-hostnamed
```

🔹 SSH Configuration

- **Update System**:

```
sudo apt update
```

- **Install SSH Server**:

```
sudo apt install openssh-server
```

- **Check SSH Status**:

```
sudo service ssh status
```

- **Edit SSH Configuration**:

```
sudo nano /etc/ssh/sshd_config
sudo nano /etc/ssh/ssh_config
```

- **Restart SSH Service**:

```
sudo service ssh restart
```

- **Connect via SSH**:

```
ssh <username>@localhost -p 4242
```

🔒 Security Configuration

🔹 Firewall (UFW) Setup

- **Install UFW**:

```
sudo apt install ufw
```

- **Enable Firewall**:

```
sudo ufw enable
```

- **Allow Port 4242**:

```
sudo ufw allow 4242
```

- **Check Firewall Status**:

```
sudo ufw status
```

🔹 Sudo Password Policy

- **Create Custom Sudo Configuration File**:

```
sudo touch /etc/sudoers.d/<file_name>
```

- **Set Password Policy in File**:

```
Defaults passwd_tries=3
Defaults badpass_message="Custom error message"
Defaults logfile="/var/log/sudo/sudo_config"
Defaults log_input, log_output
Defaults iolog_dir="/var/log/sudo"
Defaults requiretty
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
```

🔹 Password Policy for Users

1. **Password must meet these criteria**:
   - Minimum of 10 characters.
   - Must contain at least one uppercase letter and one number.
   - Cannot contain the username.
   - Cannot have more than 3 consecutive identical characters.
2. **Password Expiration**:

   - Password expires every 30 days.
   - Minimum of 2 days before the password can be changed again.
   - Warning message 7 days before expiration.
3. **Additional Rules for Root Password**:
   - Must have at least 7 characters that are not part of the old password.
   - The root password should follow the same policies as above.

🔹 Additional Sudo Policies

1. **Limited Authentication Attempts**:

   ```
   Defaults passwd_tries=3
   ```

2. **Custom Error Message**:

   ```
   Defaults badpass_message="Incorrect password, try again."
   ```

3. **Log Sudo Commands**:

   ```
   Defaults logfile="/var/log/sudo/sudo_config"
   Defaults log_input, log_output
   Defaults iolog_dir="/var/log/sudo"
   ```

4. **Restrict Sudo Usable Directories**:

   ```
   Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
   ```

5. **Enable TTY Mode for Security**:

   ```
   Defaults requiretty
   ```

📊 System Monitoring and Information

🔹 System Information Commands

- **Check System Architecture and Kernel Version**:

```
uname -a
```

- **Check Number of Physical Processors**:

```
grep "physical id" /proc/cpuinfo | wc -l
```

- **Check Number of Virtual Processors**:

```
grep "processor" /proc/cpuinfo | wc -l
```

- **Check RAM Usage**:

```
free --mega
```

- **Check Last Boot Time**:

```
who -b
```

🔹 Disk and CPU Usage Monitoring

- **Monitor Disk Usage with `df` and `awk`**:

```
df -m | grep "/dev/" | grep -v "/boot/" | awk '{total += $3} END {print total}'
df -m --output=source,used | awk '/^\/dev\// && !/boot/ {total += $2} END {print total}'
df -m | awk '$1 ~ /^\/dev\// && $6 !~ /^\/boot\// {total += $2 ; use_m += $3} END {printf ("%.2f%%\n", use_m/total*100)}'
```

- **Monitor CPU Usage**:

```
vmstat 1 2 | tail -1 | awk '{print $15}'
vmstat 1 2 | awk 'NR == 4 {print $15}'
vmstat 1 2 | awk 'NR == 4 {printf ("%.2f%%\n", 100-$15)}'
```

- **Check Active Connections**:

```
ss -ta | awk '$1 ~ /ESTAB/ {total += 1} END {print total}'
```

🔹 LVM and User Monitoring

- **Check LVM Status**:

```
lsblk | awk '$6 ~/lvm/ {found = 1} END {if(found) {print "Yes"} else
{print "No"}}'
```

- **Count Unique Logged-in Users**:

```
who | awk '{print $1}' | sort | uniq | wc -l
```

📋 Project Requirements and To-Do

1. **Create `signature.txt`**: Add this file to the root of your repository.
2. **Encrypted Partitions**: Create at least 2 encrypted partitions using LVM.
3. **SSH Configuration**: Ensure SSH is running on port 4242 and root login is disabled.
4. **Firewall Configuration**: UFW must be active, and only necessary ports should be open.
5. **Hostname**: Set hostname to your login followed by "42" (e.g., `wil42`).
6. **User Creation**: Besides root, a user with your login name should exist and belong to `user42` and `sudo` groups.
7. **Password Policy**: Implement a strong password policy as outlined above.
8. **Monitoring Script**: Create a `monitoring.sh` script that displays key system information every 10 minutes using `wall`.

🎯 Bonus Objectives

1. **Advanced Partitioning**: Configure partitions to achieve the required structure.
2. **Web Server Setup**: Configure a functional WordPress site using `lighttpd`, `MariaDB`, and `PHP`.
3. **Additional Service**: Configure another useful service and justify your choice during the defense.

4. **Custom Services**: Add more services if necessary, and adapt UFW/Rocky rules as needed.