#901640 - Implement CIS Benchmark for SSH on SUSE Linux Enterprise 15

Objective:

This task involves studying the CIS Benchmark recommendations for SSH on SUSE Linux Enterprise 15 and applying the suggested policies to enhance SSH security. You will:

- Research and analyze CIS Benchmark guidelines for SSH.
- Create a case study documenting the current SSH configuration on your system.
- Implement recommended security measures for root login, password-based access, and SSH port.

Scenario:

Your company aims to improve security by adhering to industry best practices. This task focuses on implementing the CIS Benchmark recommendations for SSH on your SUSE Linux Enterprise 15 system.

CIS (Center for Internet Security)

The Center for Internet Security (CIS) is a nonprofit organization that provides guidelines and best practices for securing information systems. It focuses on improving cybersecurity by developing and promoting standards and practices to help organizations protect their data and systems from cyber threats.

CIS Benchmark

A CIS Benchmark is a set of best practice guidelines and security configurations developed by CIS for various operating systems, applications, and network devices. These benchmarks provide detailed recommendations for hardening systems against potential security vulnerabilities. They are widely used by organizations to improve their security posture and ensure compliance with industry standards. Each benchmark includes specific configurations and settings designed to enhance the security of the respective system or application.

Research and Analyze CIS Benchmark Guidelines for SSH

The CIS Benchmarks provide comprehensive security guidelines designed to safeguard various systems, including SSH on SUSE Linux Enterprise 15. The key areas of focus for SSH security include:

1. Disable Root Login: Prevent direct root access to reduce the risk of unauthorized privilege escalation.
2. Disable Password-Based Authentication: Enforce the use of SSH keys for authentication to minimize the risk of brute-force attacks.
3. Change the Default SSH Port: Change the default port (22) to a nonstandard port to reduce the risk of automated attacks.

These recommendations are part of a broader strategy to minimize attack vectors and secure the SSH service from potential threats.

Current SSH Configuration File: /etc/ssh/sshd_config

Below is the current configuration before implementing CIS recommendations.

```
PermitRootLogin yes

PasswordAuthentication yes

#Port 22
```

- PermitRootLogin yes: Allows direct root login, which poses a security risk as root access gives full control over the system.
- PasswordAuthentication yes: Password authentication is enabled, increasing the risk of brute-force attacks.
- Port 22: The default SSH port is set to 22, making it a common target for automated attacks.

Implement Recommended Security Measures

Based on the recommended CIS Benchmark , the following changes will be implemented to enhance SSH security

Disable Root Login:

- Disabling root login improves security by preventing attackers from directly accessing the root account. Instead, users must log in with their personal accounts and use sudo or su to gain root privileges, which adds an extra layer of security and accountability.
- Set PermitRootLogin no in /etc/ssh/sshd_config.

```
PermitRootLogin no
```

Disable Password-Based Authentication:

- Disabling password-based authentication enhances security by forcing users to authenticate using more secure methods, such as SSH key-based authentication. SSH keys are more difficult to compromise compared to passwords and provide a higher level of security.
- Set PasswordAuthentication no in /etc/ssh/sshd_config.

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
PermitEmptyPasswords no
```

Change the SSH Port

- Changing the SSH port from the default (22) to a non-standard port reduces the risk of automated attacks, such as port scanning and brute force attacks, which commonly target the default port. Using a nonstandard port adds a layer of obscurity to your SSH service.
- Set Port to a non-default value in /etc/ssh/sshd_config.
-

```
Port 2200
```

```
opensuse:~ # systemctl status sshd
● sshd.service - OpenSSH Daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2024-08-31 12:41:07 IST; 4s ago
  Process: 25068 ExecStartPre=/usr/sbin/sshd -t $SSHD_OPTS (code=exited, status=0/SUCCESS)
  Process: 25065 ExecStartPre=/usr/sbin/sshd-gen-keys-start (code=exited, status=0/SUCCESS)
 Main PID: 25069 (sshd)
    Tasks: 1
   CGroup: /system.slice/sshd.service
           └─25069 /usr/sbin/sshd -D

Aug 31 12:41:06 opensuse.example.com systemd[1]: Starting OpenSSH Daemon...
Aug 31 12:41:06 opensuse.example.com sshd-gen-keys-start[25065]: Checking for missing server keys in /etc/ssh
Aug 31 12:41:07 opensuse.example.com sshd[25069]: Server listening on 0.0.0.0 port 2200.
Aug 31 12:41:07 opensuse.example.com sshd[25069]: Server listening on :: port 2200.
Aug 31 12:41:07 opensuse.example.com systemd[1]: Started OpenSSH Daemon.
```

Verify Configuration

To ensure the changes are effective, perform the following checks:

- Attempt to SSH as the root user. The connection should be denied.

```
root@ubuntu:~# ssh -p 2200 root@192.168.7.189
************************************************************************
WARNING: Unauthorized access to this system is prohibited.
All activities are monitored and recorded.
************************************************************************

Password:
Password:
Password:
Received disconnect from 192.168.7.189 port 2200:2: Too many authentication failures
Disconnected from 192.168.7.189 port 2200
root@ubuntu:~#
```

- Try to SSH using a password. The connection should be denied.

```
user@192.168.7.189: Permission denied (publickey).
root@ubuntu:~/.ssh# ssh user@192.168.7.189
```

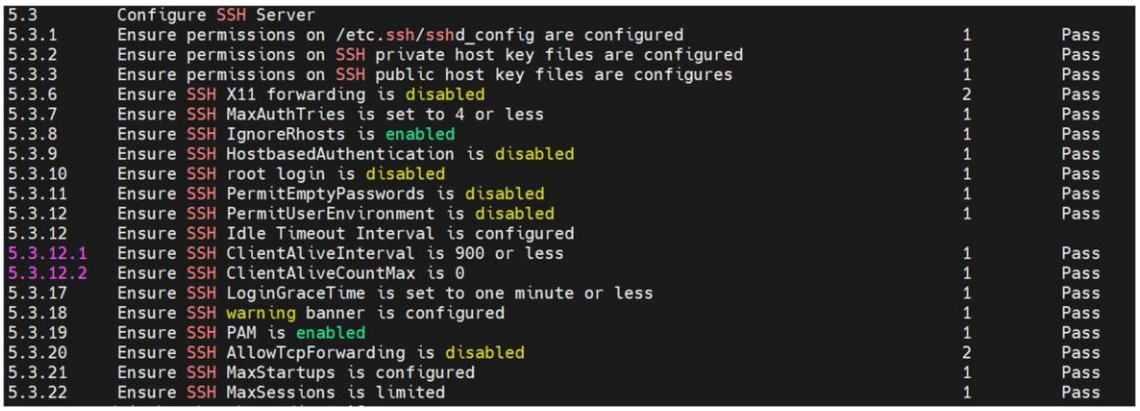
- Connect using SSH keys on the new port. The connection should succeed.

```
root@ubuntu:~# ssh -p 2200 user@192.168.7.189
************************************************************************
WARNING: Unauthorized access to this system is prohibited.
All activities are monitored and recorded.
************************************************************************

Last login: Sat Aug 31 10:54:27 2024 from 192.168.7.133
Have a lot of fun...
user@opensuse:~>
```

By implementing these measures, you can significantly improve the security of your SSH configuration, making it more resilient against unauthorized access and attacks.

- All recommended CIS Benchmark settings have been successfully applied, including the disabling of root login (5.3.10), password authentication, and port forwarding, ensuring full compliance and enhanced SSH security on SUSE Linux Enterprise 15



```
5.3         Configure SSH Server
5.3.1       Ensure permissions on /etc.ssh/sshd_config are configured                    1         Pass
5.3.2       Ensure permissions on SSH private host key files are configured              1         Pass
5.3.3       Ensure permissions on SSH public host key files are configures               1         Pass
5.3.6       Ensure SSH X11 forwarding is disabled                                        2         Pass
5.3.7       Ensure SSH MaxAuthTries is set to 4 or less                                  1         Pass
5.3.8       Ensure SSH IgnoreRhosts is enabled                                           1         Pass
5.3.9       Ensure SSH HostbasedAuthentication is disabled                               1         Pass
5.3.10      Ensure SSH root login is disabled                                            1         Pass
5.3.11      Ensure SSH PermitEmptyPasswords is disabled                                  1         Pass
5.3.12      Ensure SSH PermitUserEnvironment is disabled                                 1         Pass
5.3.12      Ensure SSH Idle Timeout Interval is configured
5.3.12.1    Ensure SSH ClientAliveInterval is 900 or less                                1         Pass
5.3.12.2    Ensure SSH ClientAliveCountMax is 0                                          1         Pass
5.3.17      Ensure SSH LoginGraceTime is set to one minute or less                       1         Pass
5.3.18      Ensure SSH warning banner is configured                                      1         Pass
5.3.19      Ensure SSH PAM is enabled                                                    1         Pass
5.3.20      Ensure SSH AllowTcpForwarding is disabled                                    2         Pass
5.3.21      Ensure SSH MaxStartups is configured                                         1         Pass
5.3.22      Ensure SSH MaxSessions is limited                                            1         Pass
```

Thank You

dasaremahir333@gmail.com