# CIS-CAT REPORT RESPONSE

The test is mainly focused on 6 aspects of the system namely,

- Initial setup
- Services
- Network Configuration
- Logging and Auditing
- Access, Authentication and Authorization
- System Maintenance

Each of these categories have many subcategories and tests related to each of them.

Now if we look at the overall performance of our system assessment, the scores are as follows,

| | | |
|---|---|---|
| Initial setup | 14/29 | 48% |
| Services | 26/33 | 79% |
| Network Configuration | 12/7 | 63% |
| Logging and Auditing | 5/7 | 71% |
| Access, Authentication and Authorization | 9/34 | 26% |
| System Maintenance | 24/31 | 77% |

Overall performance: 90 tests passed, 59 failed tests and 4 unknown - 90.0 score with 59%

There is different level of assessments that can be done on a system, or a server and we have sed level 1 server profile test for this assessment meaning that this profile intends to be practical and prudent and provides a clear security benefit along with not inhibit the utility of the technology beyond acceptable means. This assessment profile is basically intended for servers, as was suggested in the name.

OBSERVATIONS:

From the above table, its safe to assume that the Access, Authentication and Authorization part of our server has the least score. Out of 34 tests it only passed 9 tests. So, we can assume that our server has the still a lot of room to improve in this area to be more secure. Access, Authorization and Authentication to the system is one of the most important pieces that must be secure and this piece being at 26% is not good for the enterprise or the entity that is using the server in question.

The report also provides an in-death view of what the test is, and you can Improve upon that. For example: Our server has failed most of the test based around *cron,* which is responsible for the system maintenance including system monitoring.

Similarly, In system maintenance our server failed tests like *ensuring password fields are not empty* or *ensuring root path integrity* etc.

We can say that comparatively, our Services, Logging and Auditing and System Maintenance are all slightly above average. Although there is room for making the server more secure in these aspects, they are still secure compared to other aspects of the machine.

ADDITIONAL HARDENING STEPS:

I would start with the least secure part of our system and work my way up (some choices are subject to priority). In this case that would be Access, Authentication and Authorization piece.

1. I would ensure the permissions to *cron* (*cron.daily*, *cron.hourly* etc) are all configured
2. I would make sure *SSH server* is properly configured, which includes authentication of users and root servers, protocols, MAC algorithms etc.
3. I would configure PAM, which is a service that implements modular authentication modules on UNIX systems. Most of the assessment configuration doesn't even exist on our given server. So, I would make its up and running properly.
4. I would carefully examine the *User Accounts and Environment,* which help to monitor the passwords of user accounts and user related items.

Next, I would move on to the Network Configuration piece. Although the initial setup is score is much lower than network configuration, I feel like this network part is much more exposed and vulnerable to external attacks than initial setup just because of the sheer volume of traffic.

1. I would make sure that the network parameters (host only) are properly configured. For example: our server failed to redirect ICMP packets because its disabled. This can be used against us if the attacker to send an invalid ICMP from a compromised host in attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system
2. I would ensure that the suspicious packets are logged
3. I would make sure that TCP SYN cookies is enabled which prevents attackers from using SYN flood to perform DoS attack.
4. I would focus on configuring firewall like configuring loopback traffic, firewall rules for all open ports etc.

Next, I would move on to the initial setup part and try to make sure that I can configure as much as I can to make up for the failed tests.

1. I would make sure that all the filesystems are enabled like cramfs, freevxfs, jffs2, hfs, hfsplus, squashfs, udf and FAT systems.
2. I would ensure the filesystem's integrity id regularly being monitored.
3. I would ensure the additional process hardening is in place like ensuring core dumps are restricted, ensuring XD/NX support is enabled.

Finally, after all this is done, I would try to improve upon the remaining three aspects of the server and see what test the server failed and try to come up with solutions to overcome those problems.