Security Compliance

S. No	Action Items	Complied to?
Server Operating System (OS) Hardening Activities		
1.	Ensure that the OS is updated with the latest version of security patches.	❑ Yes ❑ No
2.	Ensure that Created a separate volumes for /var, /var/log, and /home.	❑ Yes ❑ No
3.	Ensure that Created a separate volumes for /tmp, /var/tmp, /dev/shm and nodev, nosuid, and noexec option set on above volumes.	❑ Yes ❑ No
4.	Ensure that automouting is disabled for CD/DVDs and USB.	❑ Yes ❑ No
5.	Ensure that password is set for single user mode.	❑ Yes ❑ No
6.	Ensure that the stateful firewall rules are configured on the system. ❑ Default all firewall policy is set to Deny. ❑ Firewall rules exist for all open ports. ❑ Firewall rules for new outbound and established connections are configured.	❑ Yes ❑ No
7.	Ensure that SELinux is configured.	❑ Yes ❑ No
8.	Kernel tuning parameters should be set in sysctl.conf ❑ IP forwarding is disabled ❑ ICMP redirects are not accepted ❑ Packet redirect sending is disabled ❑ Source routed packets are not accepted ❑ TCP SYN Cookies is enabled ❑ Broadcast Requests are Ignored ❑ Bad Error Message Protection enabled	❑ Yes ❑ No
9.	Ensure that Auditd and Syslogs (like rsyslog, syslog, syslog-ng, etc) service are enabled, running and rotated.	❑ Yes ❑ No
10.	Ensure that the OpenSSH is configured securely ❑ SSH Protocol is set to 2. ❑ SSH LogLevel is set to INFO. ❑ SSH PermitEmptyPasswords is disabled. ❑ SSH root login is disabled. ❑ SSH banner is disabled.	❑ Yes ❑ No

11.	Ensure that unused services are disabled (Ex. Cups, xinetd, telnet,etc.)	❑ Yes ❑ No
12.	Ensure that unused network protocols are disabled.	❑ Yes ❑ No
13.	Ensure that Network Time Protocol (NTP) is configured and synced with ntp.iitb.ac.in.	❑ Yes ❑ No
14.	Ensure that crond is restricted to authorized users.	❑ Yes ❑ No
15.	Ensure that each user has a distinct/individual user account for accessing the system.	❑ Yes ❑ No
16.	Enforce usage of strong and periodical change of user passwords.	❑ Yes ❑ No
17.	Ensure that users' dot files are not group or world writable.	❑ Yes ❑ No
18.	Ensure usage of sudo access policy to delegate admin-level tasks.	❑ Yes ❑ No
19.	Ensure that no world-writable files exist on the system .	❑ Yes ❑ No
20.	Ensure that no unowned files and directories exist on the system.	❑ Yes ❑ No
21.	Ensure that sticky bit permission is set on all world-writable directories.	❑ Yes ❑ No
22.	Ensure that the Intrusion Prevention System (IPS) like Fail2Ban is configured.	❑ Yes ❑ No
23.	Ensure that the File System Integrity Checking like AIDE is configured.	❑ Yes ❑ No
	Web Server Application Hardening Activities	
24.	Ensure that a Web Server is updated with the latest version of security patches	❑ Yes ❑ No
25.	Ensure that the web server runs as a non-root user.	❑ Yes ❑ No
26.	Ensure that unnecessary modules are disabled on the Web server.	❑ Yes ❑ No
27.	Ensure that the webserver directory listing is disabled.	❑ Yes ❑ No
28.	Ensure that the Document Root directory is set on proper permissions.	

	❑ Owner should be a root user. ❑ Permission parameter should not be set to full access i.e., 777 (drwxrwxrwx) ❑ Sticky bit permission is set on all world-writable directories	❑ Yes ❑ No
29.	Ensure that HTTP Trace method is disabled.	❑ Yes ❑ No
30.	Ensure that HTTP Proxy Server is not enabled.	❑ Yes ❑ No
31.	Ensure that a web server does not advertise the software/OS versions.	❑ Yes ❑ No
32.	Ensure that the mod_security is installed and enabled.	❑ Yes ❑ No
33.	Ensure that all default web server content is removed	❑ Yes ❑ No
34.	Ensure that web server syslog facility is configured.	❑ Yes ❑ No
35.	Ensure SSL/TLS is configured. ❑ Disabled TLSv1.0 and TLSv1.1 Protocols. ❑ Disabled Weak SSL/TLS Ciphers. ❑ Disabled Weak SSL Protocols.	❑ Yes ❑ No
	Database Server Hardening Activities	
36.	Ensure that a Database Server is updated with the latest version of security patches.	❑ Yes ❑ No
37.	Ensure that the database server unnecessary modules are disabled or removed	❑ Yes ❑ No
38.	Ensure that the database server daemon uses a dedicated least privileged account	❑ Yes ❑ No
39.	Ensure that the database server daemon has not started with safe mode	❑ Yes ❑ No
40.	Ensure that the database server default database and users are removed.	❑ Yes ❑ No
41.	Ensure that the database server no users have Wildcard hostnames.	❑ Yes ❑ No
42.	Ensure that the database server command history is disabled.	❑ Yes ❑ No
	Web Application Hardening Activities	

43.	Ensure that the applications and their respective 3rd party plugins, codes., etc., are updated with the latest version of security patches.	❑ Yes ❑ No
44.	Ensure that the application has implemented proper validation on all input parameters in client and server side.	❑ Yes ❑ No
45.	Ensure that the application has implemented with proper HTTP Security Headers.	❑ Yes ❑ No
46.	Ensure that the application has implemented with proper error-handling.	❑ Yes ❑ No
47.	Ensure that the application does not store any plain passwords in config files or source code or in database.	❑ Yes ❑ No
48.	Ensure that the application Directory traversal is disabled.	❑ Yes ❑ No
49.	Ensure that all communications are done through encrypted channel, If application is integrated with any 3rd party Applications or using any APIs for external communication.	❑ Yes ❑ No
50.	Ensure that the login functionality is configured securely ❑ The CAPTCHA feature is implemented on the login and registration form. ❑ Proper Session Timeout is implemented. ❑ Admin URLs are accessible from specific IP addresses only or disabled. ❑ The password is stored in a database with hash format.	❑ Yes ❑ No
51.	Ensure that the application version information files are disabled or removed	❑ Yes ❑ No
52.	Ensure that proper permission is set on the application directories and files.	❑ Yes ❑ No
53.	Ensure that the application doesn’t have File upload in public modules.	❑ Yes ❑ No
54.	Ensure that Trace/PUT/DELETE and other non-required methods in application or web-server are disabled.	❑ Yes ❑ No
55.	Ensure that the application directory listing is disabled	❑ Yes ❑ No
56.	Ensure that restrict each application for minimum access like Websites, those are to be used in local-network, should not be accessible from any other network.	❑ Yes ❑ No
57.	Ensure that the application process runs as a non-root user.	❑ Yes ❑ No

58.	Ensure that the CAPTCHA is implemented on all entry-forms in PUBLIC pages.	❑ Yes ❑ No
59.	Ensure that Email addresses, where ever used, are in form of an image and replace “@” with [at] and “.” with [dot]	❑ Yes ❑ No