|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Test Case ID** | **Test Scenario** | **Test Steps** | **Test Data** | **Expected Results** | **Actual Results** | **Pass/Fail** |
| AC-1 | Access Control Policy and Procedures | Open documentation policy (AC-1) | Documentation for Test Cases.docx | Text file is opened with access policy listed | File is opened | PASS |
| AC-14 | Permitted Actions Without Identification or Authentication | Open documentation policy (AC-14) | Documentation for Test Cases.docx | Text file is opened with policy listed with description of organization policy | File is opened | PASS |
| AC-19 | Access Control for Mobile Devices | Check response when logging in to the database with a username and password on a mobile device | user: admin  pass: admin | Login should be successful | Login is successful | PASS |
| **AC-2** | Account Management | Log in to an admin account, and then log out and log in to a guest or temporary account |  | Each account should have different privileges | Accounts have different privileges | PASS |
| AC-5 | Separation of Duties | [1](https://nvd.nist.gov/800-53/Rev4/control/AC-5)) Assign roles to table for anyone accessing database  2) Create a username and password specific to each user | user: admin  pass: admin | Admin should be able to log in with administrator privileges | Admin is able to login | PASS |
| **AC-7** | Unsuccessful Login Attempts | Attempt to log on to the admin account with a false password three times | user: admin  pass: badpass1 | Login should fail and a message to retry a different password should appear | Access denied for the user and message Message appears after one try saying "You have reached the maximum attempts. You are now locked out. " | semi - PASS |
| **AC-8** | System Use Notification | Log on to a user account and attempt to access a database | user: user  user: user | A banner should appear that warns the user that they are about to access important information | "You are about to access crucial information and your actions may be monitored. IF you wish to continue clicking ok." | PASS |
| **AU-8** | Time Stamps | 1) Login as a user or admin  2) Query the database | user: user  user: user  SELECT \* FROM event\_scrite | Login should be successful with a time stamp indicating time stamp. Query should also result in a time stamp after | Timestamps appear for after you log in and after you query the database | Pass for 1/2 requirements |
| **AT-4** | Security Training Records | Open documentation for policy AT-4 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| **CA-5** | Plan of Action and Milestones | Open documentation policy(ca-5) | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| CA-7 | Continuous Monitoring | The organization will specify which threats in the database will be monitored and status messages will be set up when a new threat is added.  Step 1: Open document policy (CA-7) | Documentation for Test Cases.docx | Organization will follow guidelines and attempt to implement continuous monitoring | File is opened and guidelines followed | PASS |
| PE-12 | Emergency Lighting | Open documentation policy PE-12 | Documentation for Test Cases.docx | File is able to be opened | File is opened and guidelines followed | PASS |
| CM-10 | Software Usage Restrictions | 1) Administrator will create a spreadsheet and document any software licenses that are currently in use, date of license, and expiration date  2) Software on that list can be manually or automatically blocked from being used on the system |  | When a user tries to download a foreign piece of software an error message will pop up and block them from installing the software |  |  |
| CM-7 | Least Functionality | 1) Go to firewall settings  2) Change firewall settings to block specific ports | Port 80 | Choose a port and blocked part will not allow connections | Port is blocked from outbound and inbound traffic | PASS |
| CM-11 | User Installed Software | Open documentation policy on CM-11 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| CP-1 | Contingency Planning Policy and Procedures | Open documentation on CP-1 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| CP-2 | Contingency Plan | Open documentation on CP-2  Step 1: Develop a contingency plan that identifies essential business functions, provides recovery objectives, restoration priorities, and addresses maintaining these essential business functions | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| CP-3 | Contingency Training | Open documentation on CP-3 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| CP-4 | Contingency Plan Testing | 1) The organization will run a simulation of a cyber incident  2) Roles within the organization will be measured using organization metrics  3) Results are calculated from if roles successfully did the necessary actions | Roles in gtd | Simulation is organized and ran by organization | Simulation was unable to be made by organization | FAIL |
| CP-9 | Information System Backup | 1) Go to database files  2) Back up the database manually or automatically (cloud, zip, etc) | Global Terrorism database | A backup is made in zip format | A backup is available in a zip file | PASS |
| IA-1 | Identification And Authentication Policy and Procedures | Open documentation policy on IA-1 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| IA-4 | Identifier Management | 1) Login as administrator | \* Screenshot of roles in database \* | Admin should be able to see all the roles and permissions of other users | Admin is able to see roles and permissions | Pass |
| IR-4 | Incident Handling | Open documentation policy on IR-4 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| IR-5 | Incident Monitoring | Open documentation on IR-5 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| IR-6 | Incident Reporting | Open documentation on IR-6 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| MA-1 | System Maintenance Policy and Procedures | Open documentation on MA-1 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| PL-2 | System Security Plan | 1) Administrator opens up documentation policy (PL-2) | PL-2.txt | Admin opens file and is able to read file | Admin opens file and is able to read | PASS |
| PL-4 | Rules of Behavior | 1) User opens up app/site to access database  2) User must accept conditions | N/A | User clicks ok and logs in | User clicks ok and is then able to log in | PASS |
| RA-5 | Vulnerability Scanning | 1) Download wireshark or other tool  2) Run wireshark over the network | Wireshark | Packets are scanned while wireshark is running | Packets are scanned while wireshark is running | PASS |
| SA-2 | Allocation of Resources | Open documentation on SA-2 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| SC-5 | Denial of Service Protection | Open documentation on SC-5 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| SI-12 | Information Handling and Retention | Open documentation on SI-12 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| PE-13 | Fire Protection | Open documentation on PE-13 | Documentation for Test Cases.docx | File is able to be opened | File opened | PASS |
| SI-3 | Malicious Code Protection | 1) User attempts a sql injection (ex: 105 OR 2=2) | user: 1 OR 2=2 | A warning saying "Malicious code detected appears" | A message saying incorrect username and password appears | FAIL |
| SI-4 | Information System Monitoring | 1) Open wireshark or other software  2) Sort by tcp/udp and mysql and monitor all traffic in network for unauthorized network | wireshark packets | Wireshark is opened and network traffic is recorded | Network traffic is successfully recorded in Wireshark | PASS |