**EQUIPMENT TEST PLAN**

**Splunk - Linux 2 Web Server**

| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | | 23rd of June, 2023 |
| --- | --- | --- | --- | --- | --- |

| **Overall project scope and objectives** | | | | | |
| --- | --- | --- | --- | --- | --- |
| The AWS CyberShift Initiative project will secure OzCazual's cloud infrastructure and enable a safe and secure migration from their existing local server to Amazon AWS.  The primary goal is to address the sudden 200% increase in online sales and staff, create a scalable infrastructure that can meet future business demands, and ensure the confidentiality, integrity, and availability of the systems and customer data.  The project will Implementing various security controls, and upgrade the systems and tools currently used at OzCazual | | | | | |
| **Test objectives and success criteria** | | | | | |
| **Test Objectives:**  The objective of the test is to intentionally generate failed login attempts on the Sophos firewall virtual switch protecting a Linux 2 web server in an Azure Hyper-V environment. The goal is to ensure that these failed login attempts are logged by the Sophos firewall and subsequently recorded in Splunk, which is installed on the Linux server as a log management solution.  **Success Criteria:**  **Verify Sophos Firewall Configuration:**   * Ensure that the Sophos firewall virtual switch is properly configured to log failed login attempts. * Confirm that the firewall is set up to forward these logs to the Linux server running Splunk.   **Generate Failed Login Attempts:**   * Initiate multiple login attempts to the Linux web server from a test machine or simulated attack tool. * The login attempts should deliberately use incorrect credentials to ensure failure.   **Confirm Sophos Firewall Logging:**   * Access the Sophos firewall management console and check the logs to confirm the presence of failed login attempts. * Verify that the logs contain the relevant details, such as the source IP address, timestamp, and reason for the login failure.   **Validate Splunk Integration:**   * Access the Splunk management console on the Linux server and navigate to the Splunk data inputs configuration. * Ensure that the data input for the Sophos firewall logs is correctly configured and active.   **Check Splunk Log Ingestion:**   * Monitor the Splunk index for the incoming logs from the Sophos firewall. * Verify that the failed login attempts from the firewall are being ingested by Splunk.   **Search and Analyze Splunk Logs:**   * Use Splunk's search capabilities to query and filter the logs related to the failed login attempts. * Ensure that the relevant logs are searchable and accessible within Splunk. * Validate that the failed login attempts are properly indexed and categorized.   **Review Log Content:**   * Inspect the log entries in Splunk to ensure they contain the necessary information, such as the source IP, timestamp, event type, and any additional relevant details. * Confirm that the failed login attempts are accurately recorded and indexed within Splunk.   By successfully completing these objectives and meeting the defined success criteria, it can be confirmed that the Sophos firewall is properly logging failed login attempts and that Splunk is effectively ingesting and recording these logs for further analysis and monitoring.  **Test Network :** | | | | | |
| **Test resources required (people, hardware, software, test tools)** | | | | | |
| To ensure resource estimation, test build guidance, and historical recording, it is essential to document the people, hardware, software, and test tools required to complete the test. Accurate documentation of hardware and software versions is crucial for consistent and reliable test results. Here is a summary of the necessary components: Software Versions to Be Tested  | **Software Version** |  | | --- | --- | | Splunk | Latest | | Splunk Universal Forwarder | Latest | | Azure Management Portal | N/A | | SSH client software | Latest |  People, Roles, and Time Allocation  | **Role** | **Name** | **Resource Allocation** | | --- | --- | --- | | Project Manager | Giuseppe Raciti | 10% | | Cyber Security Specialist | Shaun Heywood | 20% | | Test LeCloud Architect/Engineer | Mark Byrne | 15% | | Server Administrator | Mauricio Guerra | 15% | | | | | | |
| **Test schedule** | | | | | |
| | **Date** | **Milestones** | **Resource Allocation** | | --- | --- | --- | | **01/07/2023** | Test Kick-off Meeting | Project Manager (Giuseppe Raciti), 5% | | Configure Azure Hyper-V Environment | Cloud Architect/Engineer (Mark Byrne), 30% Server Administrator (Mauricio Guerra), 30% | | Install and Configure Splunk Components | Cloud Architect/Engineer (Mark Byrne), 20% Server Administrator (Mauricio Guerra), 20% | | Define and Test Search Query | Cyber Security Specialist (Shaun Heywood), 40% Server Administrator (Mauricio Guerra), 30% | | Configure Real-Time Alerting | Cyber Security Specialist (Shaun Heywood), 40% | | **02/07/2023** | Scalability and Load Testing | Cyber Security Specialist (Shaun Heywood), 30%  Server Administrator (Mauricio Guerra), 30% | | Bug Identification and Reporting | Cyber Security Specialist (Shaun Heywood), 20%  Server Administrator (Mauricio Guerra), 10% | | Review Test Results with the Team | Project Manager (Giuseppe Raciti), 5% | | | | | | |

| **Test Case** | | | | | |
| --- | --- | --- | --- | --- | --- |
| | **Test ID:** | **TC010** | | --- | --- | | **Node List:** | Sophos Firewall  Linux 2 Web Server  Splunk | | **Test Description:** | This test aims to verify the successful logging and forwarding of failed login attempts from the Sophos firewall to Splunk. Additionally, it validates the functionality of a pre-existing alert that triggers upon failed logins on the firewall. The test will ensure that the alert generates the expected notification | | **Test Phase:** | System Integration Testing | | **Test Suite:** | Log Management and Monitoring | | **Test Setup:** | * Set up a test environment consisting of a Sophos firewall virtual switch, a Linux 2 web server running Splunk, and a test machine for login attempts. * Configure the Sophos firewall to log failed login attempts and forward them to Splunk. * Create an alert in Splunk to detect failed logins on the firewall | | **Test Steps:** | 1. Open the Splunk Web Interface. 2. Navigate to the Search & Reporting section. 3. Enter the search query to filter web server login attempts 4. **host="OZCAZUAL-WEBSERVER" EventCode=4625 FailureReason="Unknown user name or bad password." Message="An account failed to log on\*" ssh OR sshd"** 5. Click the "Search" button to execute the search query. 6. Ensure that the search results show the SSH login events that have failed, including the specified failure reason and message. 7. Verify that the search query has been saved as an alert. 8. Simulate a failed SSH login attempt by triggering a test event. 9. Confirm that the alert is triggered and a notification is sent. | | **Expected Results:** | 1. The search results precisely filter and display the failed SSH login events that meet the specified criteria. 2. Save the search query as an alert. 3. When a failed SSH login attempt takes place, trigger the alert and send a notification. 4. The search results must accurately filter and display the failed SSH login events that match the specified criteria. 5. Save the search query as an alert. 6. Whenever a failed SSH login attempt occurs, the alert should be triggered and a notification should be promptly sent. | | **Observed Results:** | The Sophos firewall logs successfully captured the failed login attempts.  Splunk received the forwarded logs and indexed them accordingly.  The Splunk management console displayed the received logs related to the failed logins.  The pre-configured alert for failed logins on the firewall triggered as expected.  The alert generated a notification in Splunk. | | **Pass/Fail:** | Pass/Fail: **Pass**  The test was successful (Pass) as the Sophos firewall accurately logged and forwarded the failed login attempts, Splunk effectively received and indexed the logs, the Splunk alert triggered as expected, and the notification was generated within the Splunk environment. | | | | | | |