**EQUIPMENT TEST PLAN**

**Snort - Linux 2 Web Server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Project Title: | **AWS CyberShift Initiative** |  | Date Prepared: | 27th 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 the cloud environment.  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:**   * Verify that Snort is correctly installed on the Linux 2 web server in the Hyper-V virtual environment. * Ensure that Snort is actively monitoring network traffic. * Validate that Snort can detect and log suspicious or malicious network activity.   **Test Network :**    **Success Criteria:**  **Snort installation:**   * Snort is successfully installed on the Linux 2 web server. * The Snort service starts without any errors. * Snort configuration files are correctly set up.   **Active monitoring:**  Snort is actively monitoring network traffic on the server's network interface.  Snort generates logs for incoming network traffic.  **Detection of suspicious or malicious activity:**  Snort can detect and log alerts for predefined network attack signatures.  When test network traffic containing known attack signatures is sent to the server, Snort generates corresponding alerts.  **Custom rule functionality:**  Custom Snort rules can be created and applied.  When test network traffic matching the custom rule criteria is sent to the server, Snort generates the expected alerts. |
| **Test resources required (people, hardware, software, test tools)** |
| Snort Versions that could be tested  |  |  | | --- | --- | | **Snort Version** | **Description** | | **Snort 2.9.17** | Latest stable version as of September 2021 | | Snort 2.9.16 | Previous stable version | | Snort 2.9.15 | Older stable version | | **Snort 3.0.1** | Latest major release with new architecture |  People, Roles, and Time Allocation  |  |  |  | | --- | --- | --- | | **Role** | **Name** | **Resource Allocation** | | Project Manager | Giuseppe Raciti | As Needed | | Cyber Security Specialist | Shaun Heywood | **100%** | | Cloud Architect / Engineer | Mark Byrne | **100%** | | Server Administrator | Mauricio Guerra | **100%** | |
| **Test schedule** |

|  |  |  |
| --- | --- | --- |
| **Date** | **Milestones** | **Resource Allocation** |
| June 27th | Test Planning | Project Manager - 25% |
| June 28th | Environment Setup | Cloud Architect/Engineer - 100% |
| June 29th | Snort Installation | Server Administrator - 100% |
| June 30th | Test Execution | Cyber Security Specialist - 100% |
| July 1st | Test Execution | Cyber Security Specialist - 100% |
| July 2nd | Test Completion | All team members for final review |

|  |
| --- |
| **Test Case** |
| |  |  | | --- | --- | | **Test ID:** | TC-0002 | | **Node List:** | Linux 2 Web Server | | **Test Description:** | Verify successful installation and functionality of Snort IDS on the Linux 2 web server | | **Test Phase:** | Feature | | **Test Suite:** | Intrusion Detection System (IDS) - Snort Functionality Verification | |  | | | **Test Setup:** | | | 1. Hardware: Linux 2 web server running on a Hyper-V virtual environment. 2. Software: Linux 2 operating system, Snort IDS. 3. Configuration: Snort rules and configuration files set up correctly. 4. Create a custom rule in DDoS.rules file of Snort:   alert tcp any any -> any any (msg:"Custom Rule - Traffic generated by hping3"; dsize:0; content:"hping3"; sid:100001; rev:1;)   1. Test Tools: Nmap for network scanning, Hping3 for network traffic generation. | | | **Test Steps:** | | | 1. Start the Linux 2 web server and ensure it is operational. 2. Launch the Snort IDS service on the server. 3. Execute a network scan using Nmap to generate test traffic: 4. Run the following command: nmap -p 80 192.168.2.100 **-p 80**: Specifies the port to target (e.g., port 80 for HTTP). **192.168.2.100**: The target IP address of the Linux web server VM. 5. Observe the Snort logs for any generated alerts and logged network activity. 6. Generate specific network traffic using hping3 to test custom Snort rules: 7. Run the following command to generate TCP traffic with the content "hping3":  hping3 -c 10 -p 80 –-flood --rand-source 192.168.2.100 **-c 10:** Specifies the number of packets to send. In this case, it is set to 10, indicating that hping3 will send 10 packets. **-p 80:** Specifies the destination port number. Port 80 is commonly used for HTTP traffic. **- -flood:** Specifies flood the target system with a high volume of packets **--rand-source:** Spoof the source IP address field in the packets, using randomly generated IP addresses **192.168.2.100**: The target IP address of the Linux web server VM. 8. Observe the Snort logs for the triggered alert based on the custom rule. 9. Send legitimate network traffic to the server and observe Snort's behavior: 10. Access the web server from a different machine or browser. 11. Perform typical web browsing activities, such as accessing web pages, submitting forms, etc. 12. Verify that Snort logs the legitimate network traffic without generating false positives. | | | **Expected Results:** | | | * The Linux 2 web server starts successfully. * Snort IDS service starts without any errors. * The Nmap scan generates network traffic, and Snort logs the activity with any detected alerts. * The **hping3** command generates TCP traffic with the content "**hping3**," triggering the custom rule and generating an alert in Snort. * Legitimate network traffic is monitored by Snort without generating false positives. | | | **Observed Results:** | | | In a successful test, the observed results indicate that Snort is functioning correctly and generating the expected alerts.    As a result of the match, Snort successfully generated an alert as specified in the custom rule. The alert message would be displayed, providing information about the detected traffic generated by hping3.  The successful observation of the generated alert confirms that Snort is correctly configured, capable of detecting the specific traffic pattern, and generating alerts accordingly. This indicates that Snort is functioning as expected and capable of identifying potential security threats or suspicious activities in the network | | | **Pass/Fail:** | Based on the provided information, we can assess the test result as follows:  **Pass/Fail**: **Pass**  Based on the observed result and the nature of the firewall log entry, it indicates that pfSense successfully blocked the DDoS network traffic from the WAN interface to the private network range of 192.168/16. This aligns with the expected behavior and the configured firewall rule in pfSense.  Since the observed result matches the expected behavior, we can consider the test result as **Pass**. | |