**Blue Team X**

**POLICY & PROCEDURES**

### **Audit Vulnerability Scanning Policy**

### **Effective Date:** <Month Day, Year> **Rev.** 1

**Policy:** Vulnerability management is an essential component of Blue Team’s information security program and the process of vulnerability assessment is vittal to operational vulnerability management. This policy lays out the procedures for vulnerability assessment to determine the threats and potential vulnerabilities.

**Purpose:** To authorize personnel of Blue Team to perform information security vulnerability assessment for the purpose of determining areas of vulnerabilities.

**Details:**

* The development, implementation and execution of vulnerability assessment process is the responsibility of the Blue Team Captain (BTC).
* Periodic vulnerability assessments scans will be performed on all network equiptment deployed on Blue Team IP address space.
* Vulnerability tools that maybe used to assess are open source tools (OpenVas, Microsoft Baseline Security Analyzer, ect…) and must be approved by BTC. This approvel can come in the form of verble or written.
* Blue Team personnel are expected to fully cooperate with any vulnerability assessment being conducted on systems for which they are held accountable.
* Any vulnerability scans or penetration testing performed outside the network of Blue Team’s IP address space, must have the approval of the BTC in writing. A simple memorandum of approvel will meet the requirements of this action.
* All third party security companies, organizations, panels, boards or individuals that want to run external vulnerability scans must summit their request in writing to the BTC. The BTC is then required to approve the request. Approvel can be the BTC writing approved on the request, print, date, and sign at the bottom of the request.
* This policy provides the authority for Blue Team’s Information Security Team to conduct scans, audits, and risk assessments to ensure the integrity of information/resources, to investigate incidents, to ensure conformance to security policies, or to monitor user/system activity where appropriate.

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date of** | **Author** | **Description of Changes** |
|  |  |  |  |
|  |  |  |  |