Security Audit Report

SentinelX Framework v2.0

Target System:	10.10.10.55
Date Generated:	2026-01-08 21:52:25
Report ID:	SX-20260108_215225
Authorization:	VERIFIED

CONFIDENTIAL DOCUMENT

This report contains sensitive information regarding the security posture of the target system. It is intended solely for authorized personnel and system administrators.

Executive Summary

This report summarizes the findings from a security assessment conducted using the SentinelX Framework. The assessment aimed to identify vulnerabilities, misconfigurations, and security gaps in the target infrastructure.

0	1	0	1
CRITICAL	HIGH	MEDIUM	LOW

Assessment Scope

- **Target:** 10.10.10.55
- **Modules Executed:** Nmap Scan, Nikto Web Scan, Log Analysis
- **Methodology:** Automated scanning and manual verification (where applicable).

Detailed Findings: Red Team

This section details offensive operations and potential vulnerabilities discovered during the reconnaissance and exploitation phases.

Nmap Scan

Status:	Completed
MITRE ID:	T1046

Raw Output

```
PORT 80/tcp OPEN
PORT 22/tcp OPEN
```

Nikto Web Scan

Status:	Completed
MITRE ID:	T1190

Raw Output

```
+ Target IP: 10.10.10.55
+ Apache/2.4.41 appears to be outdated.
```

Defensive Analysis: Blue Team

This section analyzes system logs, detection rules, and indicators of compromise (IOCs).

Log Analysis

MITRE ID: T1110

Findings

Finding	Severity	Details
Brute Force Detected	High	50+ failed logins from 192.168.1.5
Strange User Agent	Low	User-Agent: sqlmap/1.4

MITRE ATT&CK Mapping

The following table maps executed modules and findings to the MITRE ATT&CK knowledge base.

Module	Technique ID	Tactic / Description
Nmap Scan	T1046	Network Service Discovery - Enumerating remote services.
Nikto Web Scan	T1190	Exploit Public-Facing Application - Targeting web vulnerabilities.
Log Analysis	T1110	Brute Force - Guessing credentials via trial and error.