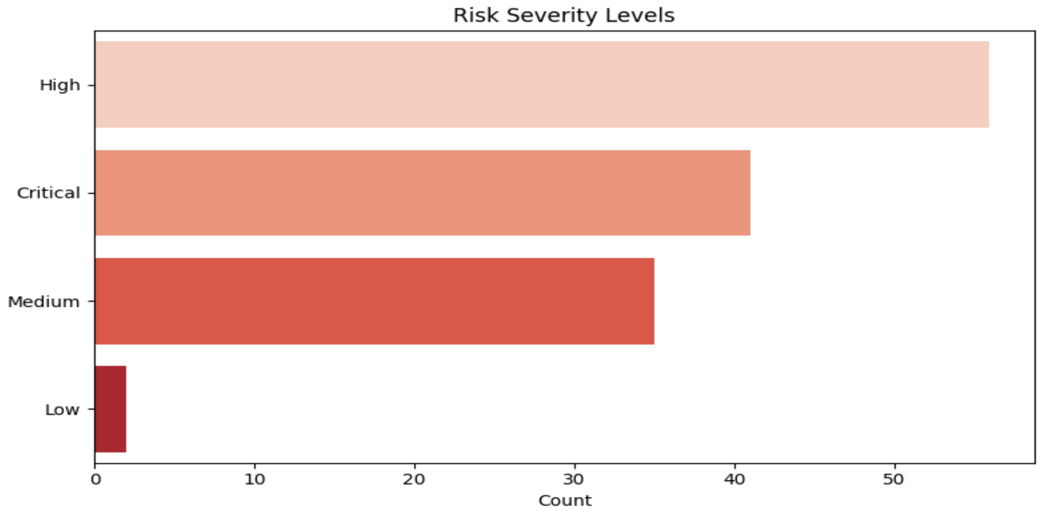
■ NIST-Aligned Cybersecurity Risk Assessment Report

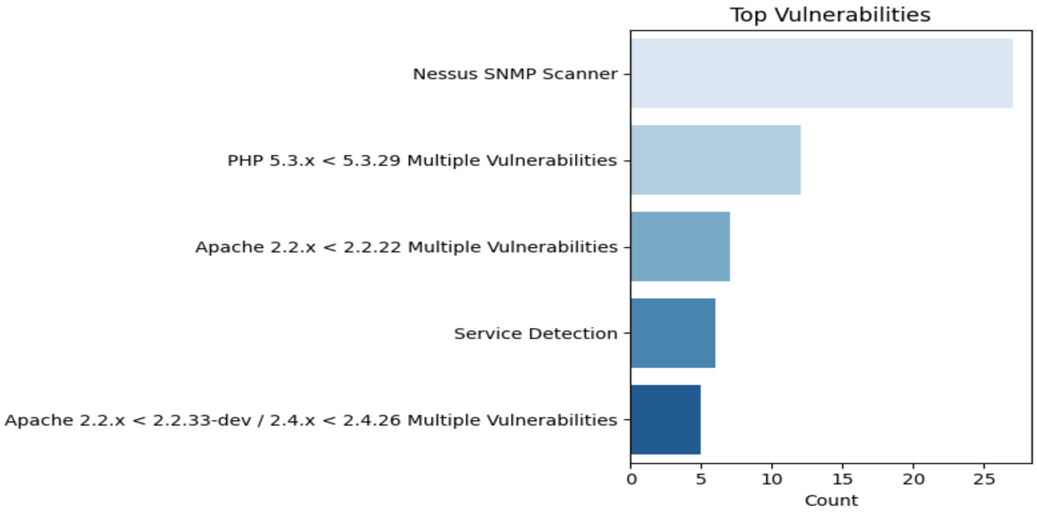
Executive Summary

Cybersecurity Risk Summary for Executive Audience Our recent vulnerability scan has revealed a concerning level of risk across our network. I'd like to highlight the key findings and recommend immediate action to mitigate these threats. **High-Level Threats:** * The scan detected **56 High-risk vulnerabilities**, which could allow unauthorized access, data theft, or disruption of critical systems. * These risks are concentrated on specific hosts (we'll discuss them below), but could potentially affect multiple systems if left unaddressed. **Common Vulnerabilities:** * Nessus SNMP Scanner vulnerabilities (27 instances): This indicates potential exposure to network reconnaissance and exploitation attacks. * PHP 5.3.x < 5.3.29 Multiple Vulnerabilities (12 instances): These are known issues in outdated PHP versions that could lead to remote code execution or information disclosure. * Apache 2.2.x < 2.2.22/33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities (14 instances): Outdated Apache versions expose our systems to cross-site scripting (XSS), denial-of-service (DoS) attacks, and remote code execution. **Key Affected Systems:** * The most vulnerable host is **192.168.11.131**, with a total of 210 vulnerabilities detected. * Other affected hosts are likely to have similar issues due to the widespread nature of these vulnerabilities. **Overall Cybersecurity Posture and Urgency:** Our scan results indicate a concerning level of risk, which requires immediate attention from our security team and IT staff. I strongly recommend that we prioritize remediation efforts for the top-vulnerable systems and address the common vulnerabilities identified in this report. Specifically: 1. Update all PHP versions to 5.3.29 or later. 2. Patch Apache to version 2.2.22/33-dev (2.4.x) or later. 3. Implement SNMP access controls and restrict access to trusted sources only. 4. Perform thorough vulnerability scanning on a regular basis to monitor our progress. I urge the executive team to prioritize cybersecurity and allocate necessary resources to address these critical issues. With swift action, we can minimize the risk of exploitation and protect our organization's sensitive data and systems.

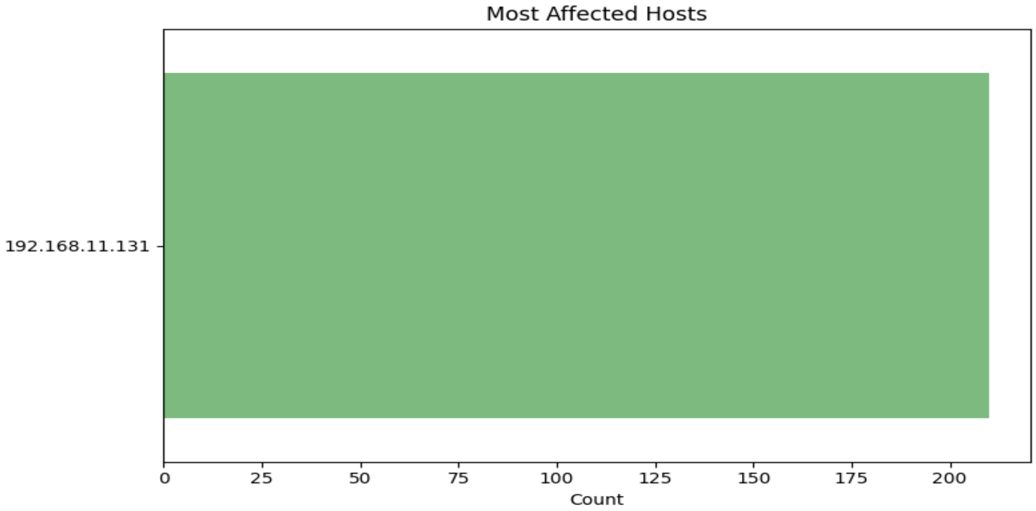
Risk Severity Levels



Top Vulnerabilities



Most Affected Hosts



Top Risks & NIST Mapping

Risk ID	Description	Severity	System	NIST Function	Mitigation	NIST Controls
R1	Here are the requested information: **Microsoft Windows LAN Manager SNMP LanMan Users Disclosure** A remote attacker can exploit this vulnerability to disclose sensitive information about users on a Microsoft Windows system, including user names and IDs.	Medium	192.168.11.131	Identify	Implement a patch management plan to ensure that all syst Implement the "Configuration Management" and " Vulnerab	Control IDs: AC-2, AC-12
R2	N/A	High	192.168.11.131	N/A	N/A	N/A
R3	N/A	Medium	192.168.11.131	N/A	N/A	N/A
R4	Here are the requested information for the "Apache Tomcat Default Files" vulnerability: **Apache Tomcat Default Files Vulnerability** Apache Tomcat is a popular web server and servlet container that contains default files that can be accessed by unauthorized users, potentially allowing rem	Medium	192.168.11.131	Identify	Remove or restrict access to unnecessary default files. Impl	AC-2 (IDENTIFY)
R5	N/A	Medium	192.168.11.131	N/A	N/A	N/A