PTES Penetration Testing Report

A controlled penetration testing simulation was conducted against a deliberately vulnerable lab environment (VulnHub VM) to evaluate the organization's exposure to common web application and system-level threats. The assessment followed the Penetration Testing Execution Standard (PTES) and used industry-standard tools including Kali Linux, Metasploit, and OpenVAS. The objective was to identify exploitable weaknesses, validate risk, and provide actionable remediation guidance.

Findings

Automated vulnerability scanning identified a critical remote code execution (RCE) weakness in a web application component, which was confirmed during the exploitation phase. The vulnerability allowed unauthorized command execution on the target system, indicating insufficient patch management and exposure to known exploits. The finding aligns with the PTES Exploitation phase and represents a high business risk due to the potential for full system compromise.

Timestamp	Target IP	Vulnerability	PTES Phase
2025-08-25 13:00:00	192.168.0.108	Drupal RCE	Exploitation

Recommendations

Apply vendor security patches immediately, restrict unnecessary services, and implement web application hardening. After remediation, a rescan should be performed to verify that the vulnerability has been successfully mitigated.

Non-Technical Stakeholder Brief

A security assessment was performed to evaluate how easily an attacker could compromise a system using publicly known weaknesses. The test revealed a critical vulnerability that could allow unauthorized access and control of the affected server. This issue increases the risk of data theft, service disruption, and reputational damage if exploited in a real-world scenario.

The good news is that the vulnerability can be fixed through timely software updates and improved security configuration. It is strongly recommended to apply patches immediately and conduct regular security scans to ensure continued protection.