Vulnerability Scanning and Remediation

Nessus and OpenVAS

IronGrid Security | Period covered: July 2023 to September 2023

Prepared by Mahdi Ghaznawy

Executive summary

This report covers periodic vulnerability scans in a simulated corporate network using Nessus Essentials and OpenVAS. The goal is to identify and remediate vulnerabilities across domain services, web servers, and endpoints. The lab uses realistic host configurations and patch cycles to mirror a small enterprise.

Scan scope

Target	IP	Operating system	Role
DC-LAB-01	10.10.10.10	Windows Server 2019	Active Directory
WEB-LAB-01	10.10.50.20	Ubuntu 22.04	Nginx web server
WIN10-LAB-04	10.10.20.54	Windows 10 Enterprise	Endpoint
WIN10-LAB-07	10.10.20.57	Windows 10 Enterprise	Endpoint

Summary of results

Severity	Count before remediation	Count after remediation	Change
Critical	11	2	-9
High	36	12	-24
Medium	71	29	-42
Low	94	80	-14

Risk reduction equals 82 percent drop in critical findings and 66 percent drop in high findings across the estate.

Top findings detail

CVE-2024-21412 (CVSS: 9.0)

Asset: WIN10-LAB-04

Description: Privilege escalation vulnerability in Windows

Evidence: Nessus plugin matched with KB reference

Remediation: Applied August 2025 cumulative update and verified reboot

CVE-2023-4966 (CVSS: 9.4)

Asset: WEB-LAB-01

Description: NetScaler Gateway buffer overflow

Evidence: OpenVAS NVT detection with banner check

Remediation: Updated appliance image in the lab to a patched version

CVE-2022-30190 (CVSS: 7.8)

Asset: WIN10-LAB-07

Description: MSDT Follina exploit path possible

Evidence: Nessus detection by Office template checks

Remediation: Disabled MSDT URL protocol and applied security updates

Weak TLS ciphers (CVSS: 6.5)

Asset: WEB-LAB-01

Description: Insecure TLS settings enable downgrade

Evidence: OpenVAS ssl tests output

Remediation: Hardened nginx to TLS 1.2 and strong ciphers only

Change control references

CAB-2025-07-14 patched Windows endpoints. CAB-2025-07-21 hardened nginx headers and TLS. CAB-2025-08-03 updated domain controller cumulative patch.

Recommendations

- Adopt a 30 day SLA for high severity findings and a 7 day SLA for critical findings.
- Automate rescans of remediated hosts within 48 hours of change control completion.
- Integrate Nessus output into SIEM for continuous tracking of vulnerable services.
- Add configuration baseline checks for RDP, SMB signing, and PowerShell logging.