Vulnerability Management Lab Using Nessus

Overview

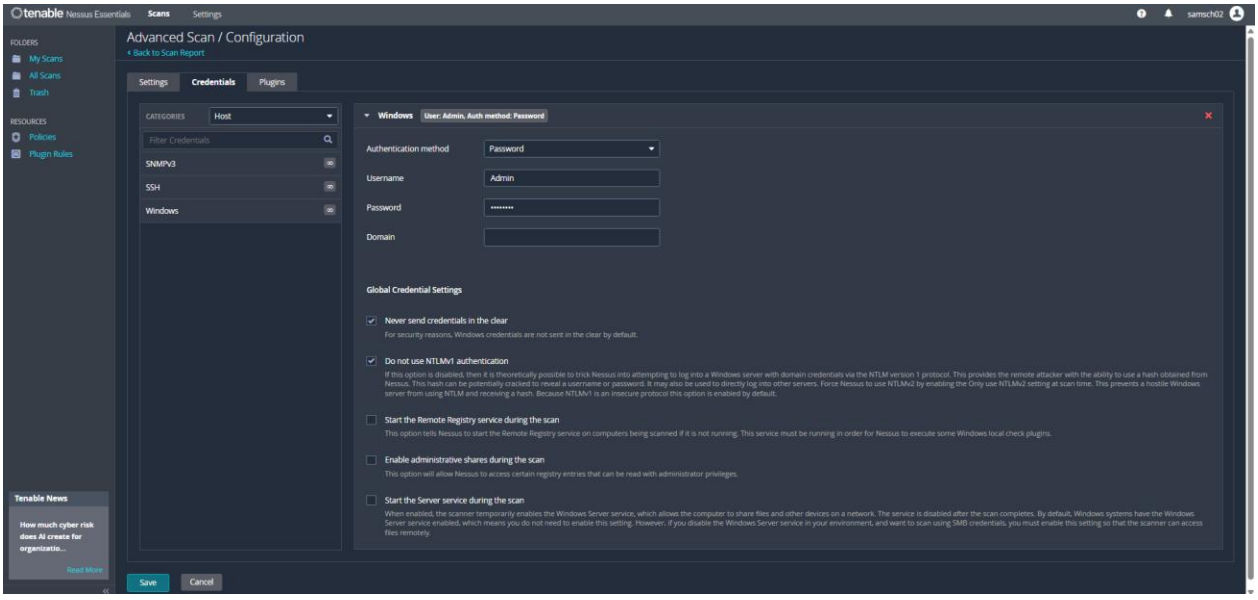
Performed a vulnerability assessment of two Windows 11 endpoints using Tenable Nessus to practice vulnerability scanning, risk identification, and remediation planning.

Step 1: Endpoint Preparation

Configured two Windows 11 endpoints for credentialed vulnerability scanning.

Prepared the systems by:

- Enabling authenticated scanning access
- Configuring administrative credentials
- Verifying network connectivity between the scanner and target devices

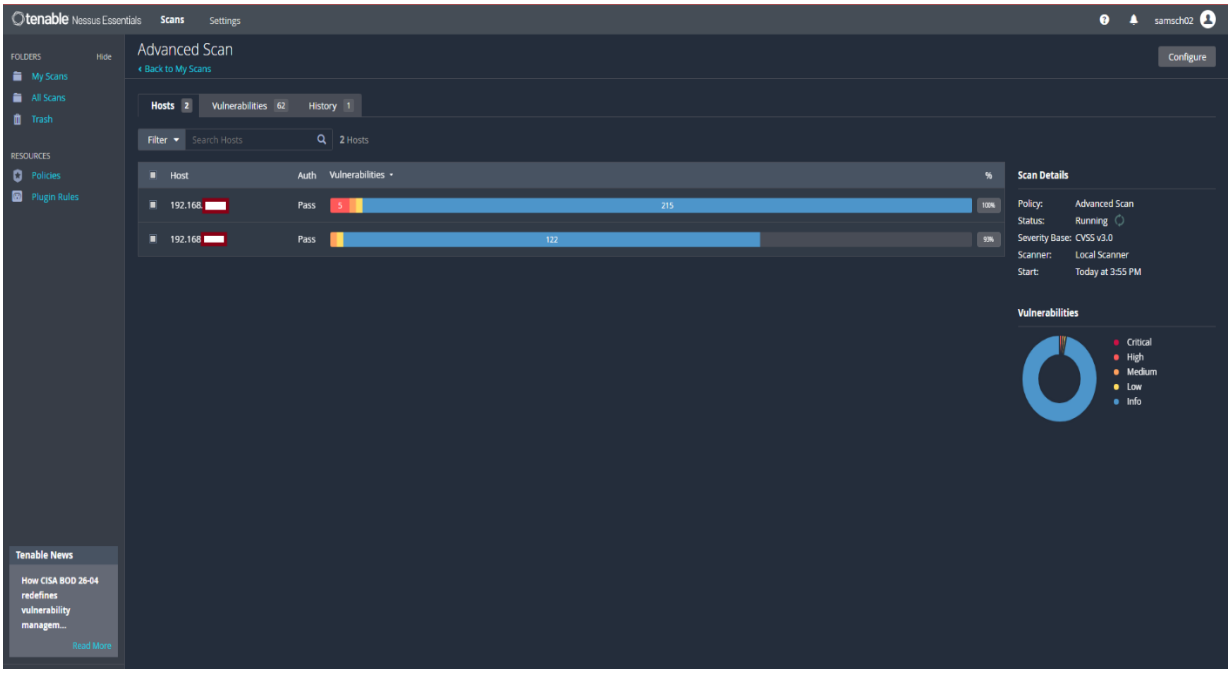


Step 2: Credentialed Nessus Scan

Created and executed an advanced credentialed scan using Nessus.

The scan evaluated:

- Operating system configuration
- Installed software
- Missing security updates
- Vulnerability exposure
- System settings

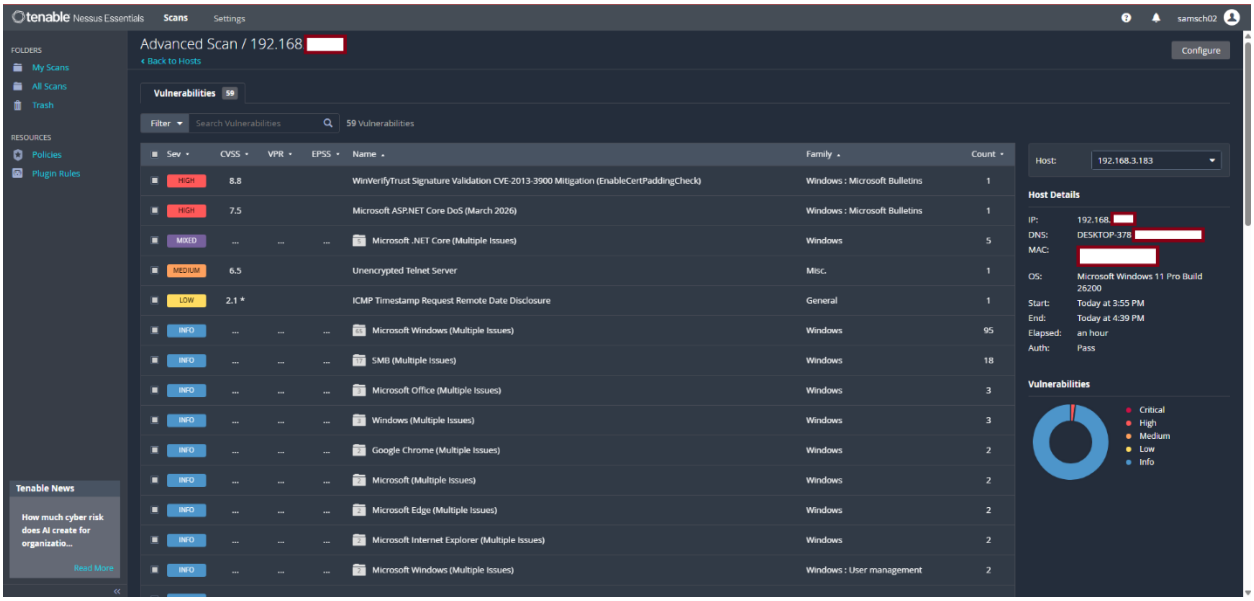


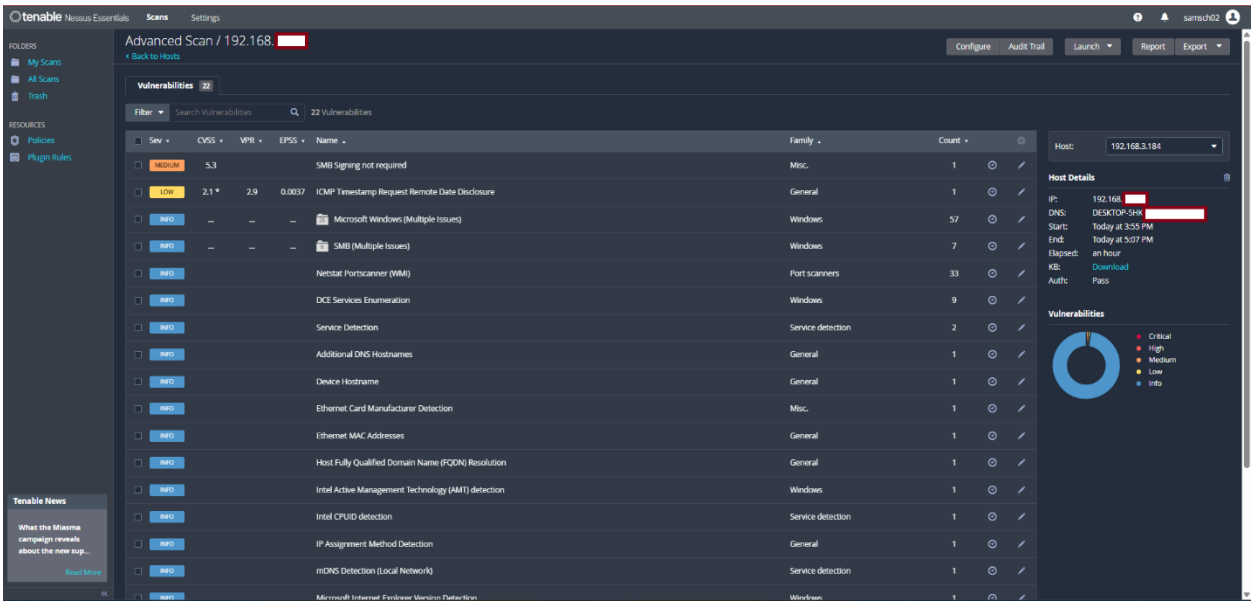
Step 3: Vulnerability Review & Analysis

Reviewed scan results to identify security findings and prioritize potential risks.

Analyzed:

- Severity ratings
- Affected systems
- Vulnerability details
- Recommended remediation steps





Step 4: Remediation & Security Improvements

Reviewed recommended actions to improve endpoint security.

Focused on:

- Reducing vulnerabilities
- Improving system configurations
- Understanding patch and security management processes

Project Outcome

Successfully completed a credentialed vulnerability assessment against Windows 11 endpoints using Nessus. This project provided hands-on experience with vulnerability management processes, security scanning, risk assessment, and interpreting security findings.