Enabling Authenticated Scanning for Enhancing Vulnerability Management

To improve vulnerability assessment accuracy and compliance, I led an initiative to configure authenticated network scans in Tenable by identifying and resolving credential misconfigurations. Authenticated scans allow Tenable to perform in-depth vulnerability analysis and compliance checks, providing more detailed security insights.

Since Tenable was newly implemented in our organization, many assets lacked proper authentication, limiting the effectiveness of vulnerability scans. Due to competing priorities and ongoing infrastructure integration, configuring credentials had not been a main focus. My project aimed to resolve these gaps and enhance Tenable's scanning capabilities.

Key Steps in This Project:

- Identified assets failing vulnerability scans due to missing or misconfigured credentials.
- Performed root cause analysis to troubleshoot authentication failures and system access issues.
- Coordinated with asset owners and Identity & Access Management (IAM) teams to establish secure authentication credentials.
- Configured credentials into Tenable and performed authenticated scans to gain deeper insights into system vulnerabilities and security posture.

Key Accomplishments & Impact

- Successfully configured credentials for over 60 systems, significantly improving Tenable's vulnerability scanning coverage.
- Strengthened compliance enforcement by enabling Tenable to perform authenticated CIS benchmark scans.
- Improved security visibility and accuracy, allowing for more comprehensive risk assessments.
- Streamlined collaboration between security, IAM, and infrastructure teams to ensure long-term credential management.
- This project is ongoing, and further integrations will continue to enhance our security posture across the enterprise.