Financial Institution Red Team Exercise

Simulated attack scenario with detailed findings and remediation recommendations.

Executive Summary

This red team engagement was conducted to assess the security posture of a financial institution by simulating a realistic cyber attack. The objective was to identify vulnerabilities in people, processes, and technology, and evaluate the organization's ability to detect and respond to such attacks.

Attack Scenario

The red team executed a multi-phase attack that began with phishing emails to key employees. Once access was gained, privilege escalation and lateral movement techniques were used to access critical systems, extract sensitive data, and simulate exfiltration of financial records.

Key Findings

- Lack of Multi-Factor Authentication (MFA) on VPN access.
- Inadequate monitoring of privileged account activity.
- End-users susceptible to social engineering.
- Poor segmentation between corporate and critical infrastructure.

Recommendations

- Enforce MFA across all remote access points.
- Implement behavior-based anomaly detection tools.
- Conduct recurring phishing simulations and awareness training.
- Strengthen network segmentation and firewall rules.