PTES-Style Technical Report

Executive Summary:

A full-scope adversary simulation was executed in a controlled lab to validate detection and response capabilities across network and cloud environments. The engagement demonstrated successful initial access via credential-harvesting phishing, escalation through misconfigured IAM roles, persistent C2 via HTTPS beacons, lateral movement using native Windows tools, and data exfiltration from an S3 bucket. Several high-severity findings were identified: missing least-privilege controls on IAM roles, public S3 exposure, insufficient PowerShell logging, and weak anti-phishing defenses.

Findings:

- Phishing (T1566): Captured session tokens using a proxying phishing kit — CVSS 7.5. Mitigation: Adopt phishing-resistant MFA and continuous user awareness training.
- Cloud Privilege Escalation (T1588/T1078.004): Over-privileged IAM roles allowed role assumption and lateral cloud compromise — CVSS 9.0. Mitigation: Enforce least-privilege, role-review automation, enable CloudTrail + IAM access analyzer.
- Living-Off-The-Land (T1059/T1055): Fileless PowerShell and process injection reduced visibility — CVSS 8.0. Mitigation: Enable script block logging, AMSI, and EDR behavioral rules.
- C2 over HTTPS (T1071): Covert TLS-based C2 required advanced network telemetry for detection — CVSS 8.5. Mitigation: JA3 fingerprinting, egress filtering, proxy inspection.

Recommendations:

Immediate enforcement of IAM policies, enable detailed cloud logging, strengthen endpoint telemetry, and schedule recurring adversary-emulation tests to validate controls.