Executive Summary

The red team simulation began with open-source reconnaissance to map the target environment. Initial access was achieved through a phishing campaign, leading to exploitation of vulnerabilities and credential harvesting. Attackers moved laterally across the network and successfully exfiltrated sensitive data. Despite detection of the initial phishing attempt, subsequent attack phases went largely unnoticed by existing security controls.

Findings

- Reconnaissance: External assets and services were identified, revealing several unmonitored entry points.
- Initial Access: A phishing payload was delivered and executed, granting internal access. The phishing attempt was detected, but user susceptibility remains a concern.
- Exploitation: Weak system configurations and credential storage allowed for local privilege escalation.
- Lateral Movement: Using harvested credentials, attackers accessed additional systems without triggering internal alerts.
- Exfiltration: Data was compressed and removed from the environment without detection.
- Detection: Security monitoring identified the phishing attempt but missed exploitation, lateral movement, and exfiltration activities.

Recommendations

- Conduct regular, practical phishing awareness training for all users.
- Deploy advanced endpoint detection that can identify unusual process activity and behavioral anomalies.
- Implement strict network segmentation to limit the impact of lateral movement.
- Expand logging and monitoring to cover internal authentication, process creation, and data movement.
- Perform regular vulnerability and configuration reviews.
- Update incident response procedures and test them with realistic scenarios.
- Schedule regular joint red team/blue team exercises to iteratively improve detection and response.

Action	Description	Suggested Owner
1. Enhance User Security Awareness	Conduct regular, interactive phishing simulations and security awareness training for all employees.	Security Awareness team
2. Deploy Advanced Endpoint Protection	Implement endpoint detection and response (EDR) tools capable of identifying advanced malicious activity, including behavioral analysis and process anomaly detection.	IT Security / SOC
3. Strengthen Network Segmentation	Segment critical assets and enforce strict access controls to contain potential attacker lateral movement within the network.	Network Engineering / IT Security
4. Expand Logging & Alerting	Expand SIEM coverage to include detailed internal authentication, process creation, and data movement logs. Fine-tune alerting for suspicious internal activity.	Security Operations / SOC
5. Regular Patch & Configuration Management	Maintain a rigorous patch management cycle and regularly review system configurations to close vulnerabilities and reduce misconfigurations.	System Administration / IT

6. Update & Test Incident Response Procedures	Revise incident response protocols to ensure rapid containment, eradication, and recovery. Conduct regular incident response drills.	Incident Response Team
7. Schedule Regular Purple Team Exercises	Run collaborative red team/blue team exercises to continuously improve detection, response, and recovery capabilities.	CISO / Security Leadership
8. Improve Privileged Access Management	Implement stricter controls on privileged accounts, including just-in-time access and credential rotation.	IT Security / Identity Management