ATTACK PATH ANALYSIS

Penetration Test Deliverable

Client:	**[SAMPLE COMPANY]**
Assessment Date:	**December 2024**
Assessor:	**Careful Security**
Classification:	**Confidential**

4.2 hrs	5	0	7
Time to Compromise	Attack Steps	Detection Events	Controls Bypassed

ATTACK PATH OVERVIEW

This document details the attack path identified during penetration testing, showing how an attacker progressed from initial phishing access to full domain administrator compromise in 4.2 hours. No security alerts were triggered during the attack simulation.

ATTACK CHAIN DETAIL

Step	Action	Target	Result	Time
1	Credential Phishing	Marketing User	VPN credentials obtained	+0:00
2	VPN Access (No MFA)	Corporate Network	Internal network access	+0:15
3	Workstation Compromise	WKS-042	Local admin hash extracted	+0:45
4	Lateral Movement	File Server FS-01	SMB access via pass-the-hash	+1:30
5	Credential Harvest	Service Account	svc_backup password in scripts	+2:45
6	Domain Admin	Domain Controller	Full domain compromise	+4:12

CRITICAL FINDINGS

ID	Finding	Severity	CVSS
AP-001	No MFA on VPN - Single factor authentication allowed network access	CRITICAL	9.8
AP-002	Local Admin Password Reuse - Same password across 847 workstations	CRITICAL	9.5
AP-003	Privileged Service Account - svc_backup in Domain Admins group	CRITICAL	9.2
AP-004	Credentials in Scripts - Plaintext password in file share scripts	HIGH	8.5
AP-005	No Network Segmentation - Flat network allowed lateral movement	HIGH	7.8

IMMEDIATE RECOMMENDATIONS

1. Enable MFA on all VPN and remote access systems within 7 days
2. Implement LAPS (Local Administrator Password Solution) for unique local admin passwords
3. Remove svc_backup from Domain Admins; implement least-privilege service accounts
4. Deploy secrets management solution; remove credentials from scripts
5. Implement network segmentation to limit lateral movement

QUESTIONS?

Contact Careful Security:

Email: icare@carefulsecurity.com

Phone: +1-818-533-1402

Web: carefulsec.com