Incident Summary

An internal Windows workstation was compromised through weak authentication controls and exposed SMB services, resulting in unauthorized interactive access via Remote Desktop Protocol.

Attack Timeline

Initial Access

- Attacker discovered exposed SMB (445) and RDP (3389) services
- SMB signing was not enforced

Credential Access

- Password spray attack against SMB succeeded
- Weak password (Password123) reused by local user account

Privilege / Access Escalation

- Valid credentials enabled RDP interactive logon
- Attacker obtained full desktop access as legitimate user

Impact

- User session disruption
- Full workstation compromise
- Potential lateral movement risk

Detection Opportunities

- SMB authentication failures followed by success

- RDP logon (Event ID 4624, Logon Type 10)
- New RDP source IP
- User-reported forced logoff

Root Causes

- Weak password policy
- No account lockout enforcement
- SMB signing disabled
- RDP exposed without network restrictions

Remediation Recommendations

- Enforce strong password policy
- Enable account lockout thresholds
- Disable SMBv1
- Require SMB signing
- Restrict RDP via firewall / VPN
- Monitor RDP logon events