# Windows Lab - MITRE ATT&CK; Mapping Summary

This document summarizes the MITRE ATT&CK; techniques observed during a controlled Windows authentication lab. The exercise simulated weak password policies and exposed services to understand risk, detection opportunities, and defensive mitigation strategies.

| Lab Phase | MITRE Tactic | Technique | Technique ID |
|---|---|---|---|
| Port & Service Discovery | Discovery | Network Service Discovery | T1046 |
| SMB Enumeration | Discovery | Remote System Discovery | T1018 |
| SMB Enumeration | Discovery | Account Discovery | T1087 |
| Password Spray | Credential Access | Brute Force (Password Spraying) | T1110.003 |
| RDP Login | Initial Access | Valid Accounts | T1078 |
| RDP Access | Lateral Movement | Remote Services (RDP) | T1021.001 |
| Credential Reuse Validation | Persistence / Access | Valid Accounts | T1078 |

## Detection Opportunities (Blue-Team Mapping)

- T1110.003 – Monitor multiple failed logons (Event ID 4625) followed by success (Event ID 4624).
- T1021.001 – Monitor RDP logons (Event ID 4624, Logon Type 10).
- T1078 – Alert on unusual successful authentication from new source IP addresses.
- T1046 – Detect excessive internal port scanning behavior.