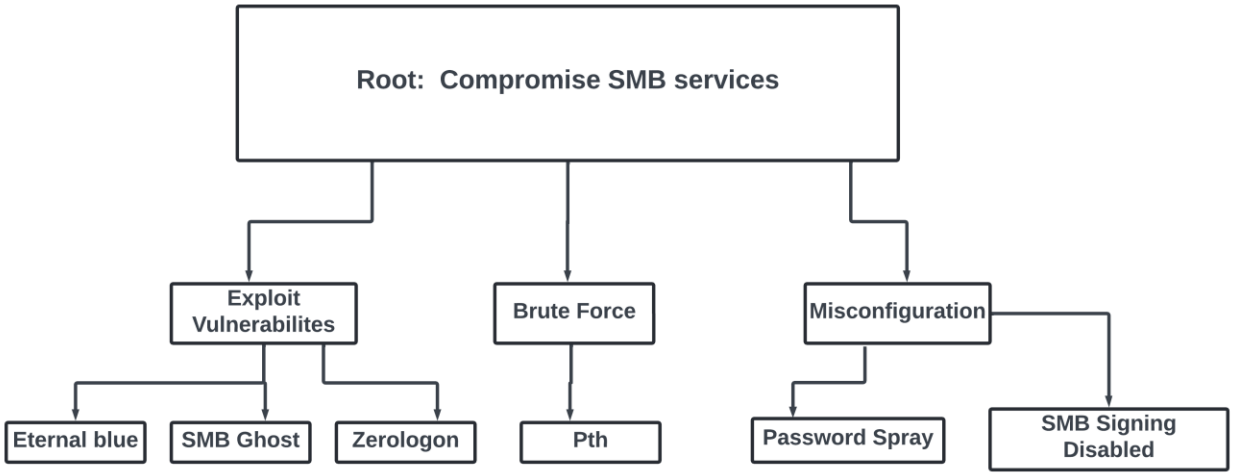
LAB 4
RED teaming tool part



Mitigation Strategies

Patch Management:

Disable SMBv1 and patch vulnerabilities like EternalBlue, SMBGhost, and ZeroLogon.

Hardening:

Enable SMB signing and encryption.

Restrict anonymous access to shares (set RestrictAnonymous=2 in registry).

Credential Security:

Enforce strong passwords and multi-factor authentication (MFA).

Use LAPS (Local Administrator Password Solution) to randomize local admin passwords.

Network Segmentation:

Block SMB (port 445) at external firewalls.

Segment internal networks to limit lateral movement.

Monitoring:

Alert on unusual SMB traffic (e.g., PsExec usage, failed login spikes).

Hunt for Mimikatz or Pass-the-Hash activity in logs.