TITLE: Windows Incident Response Quick Checklist
Version: 1.1.2025
Author: Abrar Hussain

DISCLAIMER: FOR EDUCATIONAL AND PROFESSIONAL USE. ALWAYS TEST IN A LAB ENVIRONMENT FIRST.

BRIEF INTRODUCTION: This checklist is intended for rapid triage of a potentially compromised Windows system using only built-in utilities.

PHASE 2: IDENTIFICATION & ANALYSIS

1. USER ACTIVITY & LOGON SESSIONS

```
query user
```

```
qwinsta
```

```
net sessions
```

2. IDENTIFY UNUSUAL ACCOUNTS:

a. *dir /a "C:\Users\"*
b. *net user*
c. Look for unusual user accounts created specially in RDP or administrator group (C:\> lusrmgr.msc or C:\> *net localgroup administrators*).
    i. Filter out the usernames which resembles the naming convention of your organization
    ii. Search the account creation events, Event ID#4720

3. IDENTIFY PERSISTENCE IN COMMON REGISTRY KEYS:

d. Look for registry keys in Run and Run once location.
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon

4. UNUSUAL SCHEDULE TASKS:

i. Look for unusual schedule tasks O. Schtasks /query
ii. Schedule Tasks Folder: C:\Windows\System32\Tasks

```
Get-ChildItem -Path "C:\Windows\System32\Tasks" -Force | Select-Object FullName, Length, LastWriteTime |
Format-Table -AutoSize
```

5. WMI PERSISTENCE MECHANISM:

```
Get-WMIObject -Namespace root\Subscription -Class __FilterToConsumerBinding

# Check for CommandLineEventConsumers (most common for malware - runs a command)

Get-WMIObject -Namespace root\Subscription -Class CommandLineEventConsumer

# Check for ActiveScriptEventConsumers (runs VBScript/JScript)

Get-WMIObject -Namespace root\Subscription -Class ActiveScriptEventConsumer

# Check for other types (less common for attacks)

Get-WMIObject -Namespace root\Subscription -Class __EventConsumer
```

6. IDENTIFY UNUSUAL PROCESSES:

```
Get-WmiObject Win32_Process | % { "$($_.ProcessId) $($_.Name) $($_.GetOwner().User) $($_.CommandLine)" }
```

e. Check for unknown process specially starting with ‘SYSTEM’ or ‘Administrator’ privileges.
f. Use taskmgr.exe or *tasklist /v /fo csv*
g. Use procmon tool to monitor the process hierarchy, search the anomaly across processes.
   i. Have reference from SANS Evil Hunt Poster: https://sansorg.egnyte.com/dl/WFdH1hHnQI

7. CHECK PERSISTENCE IN AUTO START PROGRAM FOLDER:

h. Check AutoStart program of windows
i. *C:\Users\user_name\AppData\Roaming\Microsoft\Windows\Start Menu\Programs*
j. *"%ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup"*
k. *"%AppData%\Microsoft\Windows\Start Menu\Programs\Startup"*

8. UNUSUAL SERVICES:

l. Check for unusual services by services.msc or net start.
   i. *wmic service get Name,DisplayName,PathName,StartMode,State*

```
Get-WmiObject Win32_Service | Select-Object Name,DisplayName,StartMode,State,StartName,PathName | Export-Csv -Path Services.csv -NoTypeInformation
```

9. UNUSUAL NETWORK CONNECTIVITY:

m. Check for file share and network connectivity

```
Netstat -naob
Netstat -naob | findstr “ESTABLISHED”
Netstat -naob | findstr “LISTENING”
```

n. Netbios sessions

```
nbtstat -S
nbtstat -N
```

o. Arp Record

```
arp -a
```

10. UNSUAL BINARY PATHS AND CREATION

- C:\ProgramData\
- C:\Windows\Temp\
- C:\Windows\
- C:\Users\Public\
- %UserProfile%\Download

11. RECENT FILES

```
%UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\
```

```
dir /a /t:c "C:\Users\*.exe" /s | findstr /i "2025"
```

12. LAST DELETED

```
dir -Force "C:\` $Recycle.Bin"
```

```
Get-ChildItem -Force "C:\`$Recycle.Bin" -Recurse |  Where-Object { -not $_.PSIsContainer } |  Select-Object @{Name="SID";Expression={$_.Directory.Parent.Name}}, Name, FullName
```

13. COLLECT KEY EVIDENCE FILES:

EVTX logs (C:\Windows\System32\winevt\Logs\).

- **Prefetch Files:** Great for seeing execution history (even if the file was deleted).
  - Location: C:\Windows\Prefetch. Analyze with PECmd.exe or WindowsPrefetchView.
- **Jump Lists:** Reveals files accessed by the user via applications.
  - Location: C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
- **Shim Cache:** Tracks application compatibility; can show evidence of execution even if prefetch is disabled.
  - Parse the registry hive: SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache
- **UserAssist:** Tracks GUI program execution (e.g., double-clicked items).
  - Registry: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

14. BROWSER EXTENSION:

%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Extensions