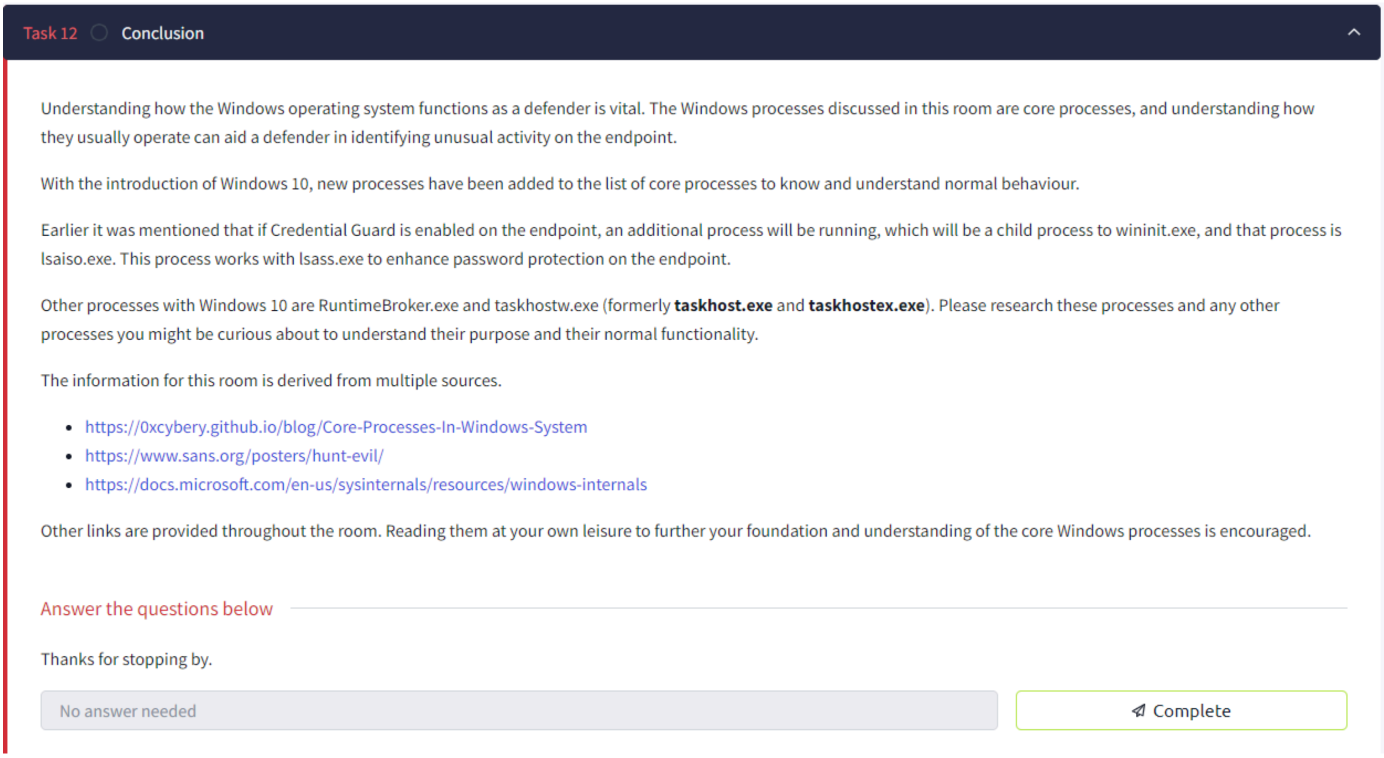
90 - conclusion



Understanding how the Windows operating system functions as a defender is vital. The Windows processes discussed in this room are core processes, and understanding how they usually operate can aid a defender in identifying unusual activity on the endpoint.

With the introduction of Windows 10, new processes have been added to the list of core processes to know and understand normal behaviour.

Earlier it was mentioned that if Credential Guard is enabled on the endpoint, an additional process will be running, which will be a child process to wininit.exe, and that process is lsaiso.exe. This process works with lsass.exe to enhance password protection on the endpoint.

Other processes with Windows 10 are RuntimeBroker.exe and taskhostw.exe (formerly **taskhost.exe** and **taskhostex.exe**). Please research these processes and any other processes you might be curious about to understand their purpose and their normal functionality.

The information for this room is derived from multiple sources.

- https://0xcybery.github.io/blog/Core-Processes-In-Windows-System
- https://www.sans.org/posters/hunt-evil/
- https://docs.microsoft.com/en-us/sysinternals/resources/windows-internals

Other links are provided throughout the room. Reading them at your own leisure to further your foundation and understanding of the core Windows processes is encouraged.

Answer the questions below

Thanks for stopping by.

No answer needed