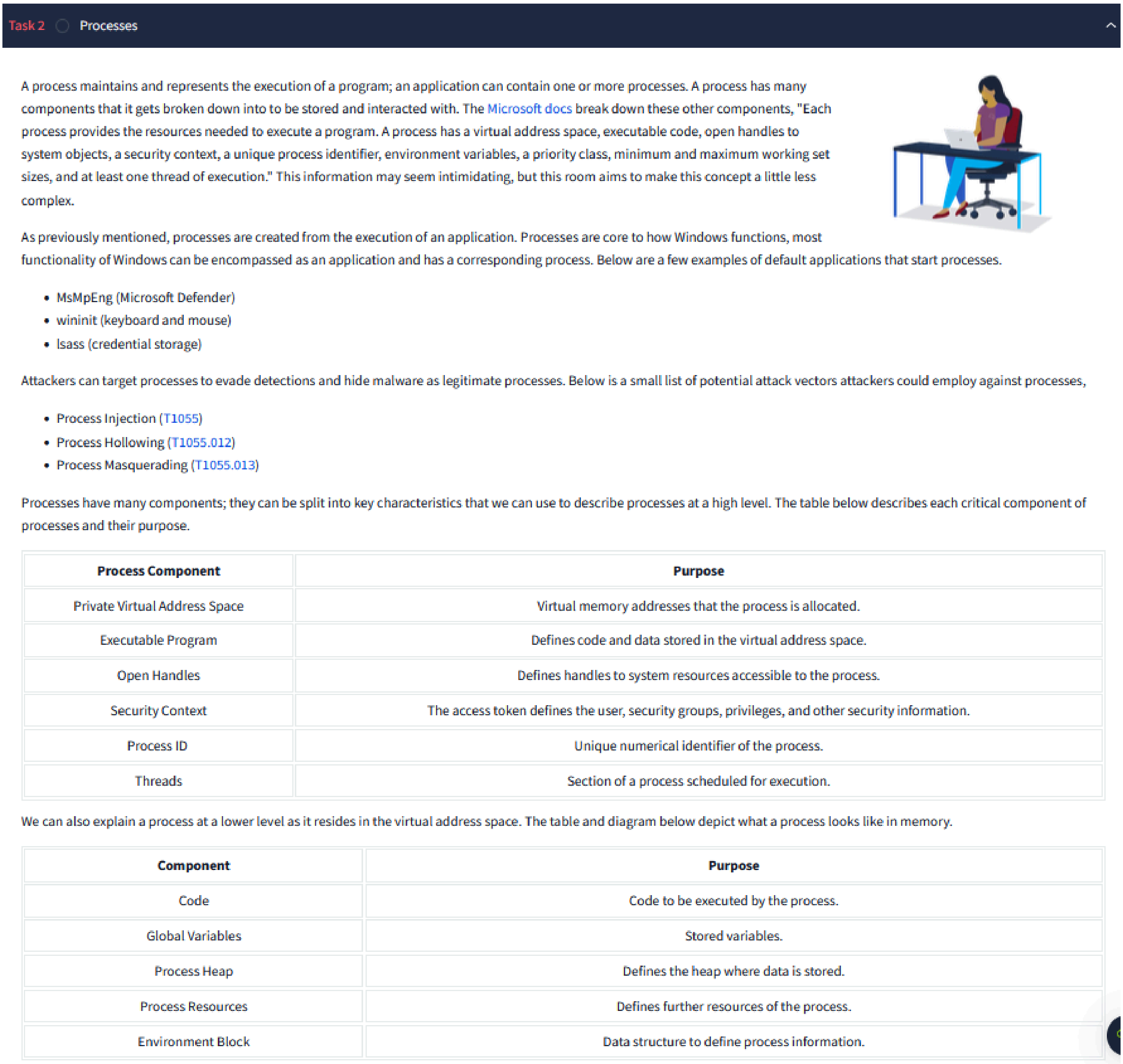
0 - Processes

Process Injection - https://attack.mitre.org/techniques/T1055/

Process Hollowing - https://attack.mitre.org/techniques/T1055/012/

Process Masquerading - https://attack.mitre.org/techniques/T1055/013/



A process maintains and represents the execution of a program; an application can contain one or more processes. A process has many components that it gets broken down into to be stored and interacted with. The Microsoft docs break down these other components, "Each process provides the resources needed to execute a program. A process has a virtual address space, executable code, open handles to system objects, a security context, a unique process identifier, environment variables, a priority class, minimum and maximum working set sizes, and at least one thread of execution." This information may seem intimidating, but this room aims to make this concept a little less complex.

As previously mentioned, processes are created from the execution of an application. Processes are core to how Windows functions, most functionality of Windows can be encompassed as an application and has a corresponding process. Below are a few examples of default applications that start processes.

- MsMpEng (Microsoft Defender)
- wininit (keyboard and mouse)
- lsass (credential storage)

Attackers can target processes to evade detections and hide malware as legitimate processes. Below is a small list of potential attack vectors attackers could employ against processes,

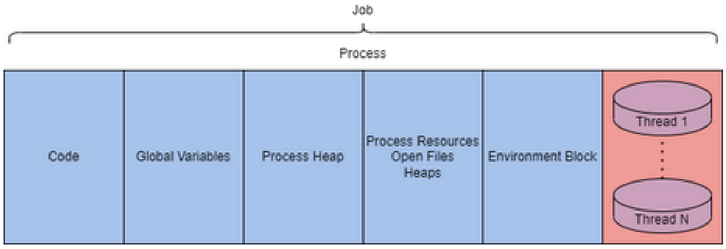
- Process Injection (T1055)
- Process Hollowing (T1055.012)
- Process Masquerading (T1055.013)

Processes have many components; they can be split into key characteristics that we can use to describe processes at a high level. The table below describes each critical component of processes and their purpose.

Process Component	Purpose
Private Virtual Address Space	Virtual memory addresses that the process is allocated.
Executable Program	Defines code and data stored in the virtual address space.
Open Handles	Defines handles to system resources accessible to the process.
Security Context	The access token defines the user, security groups, privileges, and other security information.
Process ID	Unique numerical identifier of the process.
Threads	Section of a process scheduled for execution.

We can also explain a process at a lower level as it resides in the virtual address space. The table and diagram below depict what a process looks like in memory.

Component	Purpose
Code	Code to be executed by the process.
Global Variables	Stored variables.
Process Heap	Defines the heap where data is stored.
Process Resources	Defines further resources of the process.
Environment Block	Data structure to define process information.



This information is excellent to have when we get deeper into exploiting and abusing the underlying technologies, but they are still very abstract. We can make the process tangible by observing them in the *Windows Task Manager*. The task manager can report on many components and information about a process. Below is a table with a brief list of essential process details.

Value/Component	Purpose	Example
Name	Define the name of the process, typically inherited from the application	conhost.exe
PID	Unique numerical value to identify the process	7408
Status	Determines how the process is running (running, suspended, etc.)	Running
User name	User that initiated the process. Can denote privilege of the process	SYSTEM

These are what you would interact with the most as an end-user or manipulate as an attacker.

There are multiple utilities available that make observing processes easier; including Process Hacker 2, Process Explorer, and Procmon.

Processes are at the core of most internal Windows components. The following tasks will extend the information about processes and how they're used in Windows.

Answer the questions below

Open the provided file: "Logfile.PML" in Procmon and answer the questions below.

No answer needed

✓ Correct Answer

What is the process ID of "notepad.exe"?

5984

✓ Correct Answer Hint

What is the parent process ID of the previous process?

3412

✓ Correct Answer Hint

What is the integrity level of the process?

High

✓ Correct Answer Hint