

# 1 - Threads

## Task 3 Threads

A thread is an executable unit employed by a process and scheduled based on device factors.

Device factors can vary based on CPU and memory specifications, priority and logical factors, and others.

We can simplify the definition of a thread: "controlling the execution of a process."

Since threads control execution, this is a commonly targeted component. Thread abuse can be used on its own to aid in code execution, or it is more widely used to chain with other API calls as part of other techniques.



Threads share the same details and resources as their parent process, such as code, global variables, etc. Threads also have their unique values and data, outlined in the table below.

Component	Purpose
Stack	All data relevant and specific to the thread (exceptions, procedure calls, etc.)
Thread Local Storage	Pointers for allocating storage to a unique data environment
Stack Argument	Unique value assigned to each thread
Context Structure	Holds machine register values maintained by the kernel

Threads may seem like bare-bones and simple components, but their function is critical to processes.

### 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 thread ID of the first thread created by notepad.exe?

5908

✓ Correct Answer

🔍 Hint

What is the stack argument of the previous thread?

6584

✓ Correct Answer

🔍 Hint

First thing to answer the questions is to filter the package by process name and search for the name of the .exe file.

So, the stack argument is the "Unique value" assigned to the thread, or also referred to as Thread ID. In this instance, the last questions was asking for the Unique value assigned to the thread previous to the one mentioned in question 2.

We can see the first Thread Created, and the Threat ID assigned.


Process Monitor - C:\Users\THM-Attacker\Desktop\ProcessMonitor\Logfile.PML						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
7:21:0...	notepad.exe	5984	Process Start		SUCCESS	Parent PID: 3412, ...
7:21:0...	notepad.exe	5984	Thread Create		SUCCESS	Thread ID: 5908
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\notepad.exe	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:21:0...	notepad.exe	5984	ReadFile	C:\Windows\System32\notepad.exe	SUCCESS	Offset: 141,824, Le...
7:21:0...	notepad.exe	5984	CreateFile	C:\Users\Administrator	SUCCESS	Desired Access: E...
7:21:0...	notepad.exe	5984	ReadFile	C:\Windows\System32\notepad.exe	SUCCESS	Offset: 126,976, Le...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 528
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 528
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	SUCCESS	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
7:21:0...	notepad.exe	5984	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Thread Create		SUCCESS	Thread ID: 3828
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\popt4.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ffd...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\gdi32full.dll	SUCCESS	Image Base: 0x7ffd...
Showing 1,441 of 1,176,740 events (0.12%)				Backed by C:\Users\THM-Attacker\Desktop\ProcessMonitor\Logfile.PML		





Now, the stack argument of the previous thread would be the Thread value assigned to the previous thread.


Process Monitor - C:\Users\THM-Attacker\Desktop\ProcessMonitor\Logfile.PML						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
7:21:0...	notepad.exe	5984	Process Start		SUCCESS	Parent PID: 3412 ...
7:21:0...	notepad.exe	5984	Thread Create		SUCCESS	Thread ID: 5908
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\notepad.exe	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:21:0...	notepad.exe	5984	ReadFile	C:\Windows\System32\notepad.exe	SUCCESS	Offset: 141,824, Le...
7:21:0...	notepad.exe	5984	CreateFile	C:\Users\Administrator	SUCCESS	Desired Access: E...
7:21:0...	notepad.exe	5984	ReadFile	C:\Windows\System32\notepad.exe	SUCCESS	Offset: 126,976, Le...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 528
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 528
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: R...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	SUCCESS	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
7:21:0...	notepad.exe	5984	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
7:21:0...	notepad.exe	5984	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
7:21:0...	notepad.exe	5984	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
7:21:0...	notepad.exe	5984	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	Thread Create		SUCCESS	Thread ID: 3828
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\vpct4.dll	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7ff6...
7:21:0...	notepad.exe	5984	Load Image	C:\Windows\System32\odbc32full.dll	SUCCESS	Image Base: 0x7ff6...
Showing 1,441 of 1,176,740 events (0.12%)				Backed by C:\Users\THM-Attacker\Desktop\ProcessMonitor\Logfile.PML		

Go to properties, and we can see the Thread value:

 Event Properties

 Event

 Process

 Stack

Date:1/15/2022 7:21:03.0715369 PM

Thread:6584

Class:Process

Operation:Process Start

Result:SUCCESS

Path:



Duration:0.0000000

Parent PID:3412

Command line:"C:\Windows\system32\notepad.exe"

Current directory:C:\Users\Administrator\

Environment:  
=::=:\  
ALLUSERSPROFILE=C:\ProgramData  
APPDATA=C:\Users\Administrator\AppData\Roaming  
CLIENTNAME=PIMENTO-BOX  
CommonProgramFiles=C:\Program Files\Common Files  
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files  
CommonProgramW6432=C:\Program Files\Common Files  
COMPUTERNAME=CHANGE-MY-HOSTN  
ComSpec=C:\Windows\system32\cmd.exe  
DriverData=C:\Windows\System32\Drivers\DriverData  
FPS\_BROWSER\_APP\_PROFILE\_STRING=Internet Explorer  
FPS\_BROWSER\_USER\_PROFILE\_STRING=Default  
HOMEDRIVE=C:  
HOMEPATH=\Users\Administrator  
LOCALAPPDATA=C:\Users\Administrator\AppData\Local  
LOGONSERVER=\\CHANGE-MY-HOSTN  
NUMBER\_OF\_PROCESSORS=2  
OS=Windows\_NT  
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\Syste  
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC



☐ Next Highlighted

Copy All

Close