Task-14

QRadar Logs

**Process Audit An attempt was made to duplicate a handle to an object.**

When a program opens an object like a file, it gets a "handle" to that file which it references in subsequent operations on the object. Windows checks permissions at the time of the open (aka handle request) but not afterwards. Windows allows you to duplicate a handle and hand it off to another thread or process which then inherits whatever level of access the first program obtained to the object when the program opened. Therefore, a thread impersonating a different user or a process running as a different user could exploit the potentially higher level of access of the first program for that object. And that apparently is why this event is logged. Unfortunately, this event doesn't seem to provide enough information to determine if the Handle was given to a lower security thread or process. Consequently, I classify this event as noise.

Windows security log event id 4690

Examples of 4690

An attempt was made to duplicate a handle to an object.

Subject:

Security ID: ACME\Administrator

Account Name: Administrator

Account Domain: ACME

Logon ID: 0x1f41e

Source Handle Information:

Source Handle ID: 0x858

Source Process ID: 0x1ac

New Handle Information:

Target Handle ID: 0x4c

Target Process ID: 0x1ac

**Process audit: A handle to an object was requested**

When you enable auditing on an object (e.g., file or folder), this is the first event recorded when an application attempts to access the object in such a way that matches the audit policy defined for that object in terms of who is requesting the access and what type of access is being requested. (it appears that two subcategories must be enabled, Handle Manipulation and one other such as File System or Registry depending on what type of object you are auditing.)

This event will be Audit Success or Audit Failure depending on whether the user account under which the account is running has the requested permissions or not.

Windows security log event id 4656

**Process audit: The handle to an object was closed**

After successfully opening an object, a program eventually closes it which is documented by this event.  4658 helps you determine how long the object was open. For this event to be useful you must link it back to the earlier event ID 4656 with the same handle ID.

Windows Security log event ID 4656

**A privileged service was called**

Event 4673 indicates that the specified user exercised the user right specified in the Privileges field.  
  
Note: "User rights" and "privileges" are synonymous terms used interchangeably in Windows.  
  
Some user rights are logged by this event - others by 4674. Still other, ""high-volume"" rights are not logged when they are exercised unless you enable the security option "Audit: Audit the use of Backup and Restore privilege".   
  
Unfortunately, Microsoft has overloaded these privileges so that each privilege may govern your authority to perform many different operations and which privilege is required for which operations is not well documented. Therefore, seeing that a privilege was exercised doesn't really tell you much.  In Win2008 this has been improved with better information in the Server: and Service Name: fields.  In general, though, I still classify these events as noise.  Microsoft admits: "These are high volume events, which typically do not contain sufficient information to act upon since they do not describe what operation occurred."  
  
Note: 4673 and 4674 do not log any activity associated with Logon Rights such as the SeNetworkLogonRight. Do not confuse events 4673 and 4674 with events 4717 and 4718 which document rights assignment changes as opposed to the exercise of rights which is the purpose of events 4673 and 4674.

Windows security log event ID 4673