Primary Access Token Manipulation

Exercise 4: Detection of Token Manipulation

Objective:

Learn to search and understand Event logs for detecting Token Manipulation.

Software:

Event Viewer, Sysmon

Steps:

1. Open Exercise 4 Folder

- This Folder is located on the Desktop. Open Event Viewer

2. Navigate to Sysmon Directory

- Sysmon is a Windows system driver which, once installed within the system will remain installed and monitor any activity within the system. When activities are detected it will collect the events and log them within Windows event log.

  1. This command was run prior to the exercises to document what has happened, you don't need to run it.

  2. ```
     sysmon -c detection.xml
     ```

  iii. This is the config file contents. This looks for tools that are able to run and modify tokens. This would be an example config file (can differ). This has been modified to reflect the lab contents.
     ```

```
<Sysmon schemaversion="4.40">
  <!-- Capture process creation events -->
  <EventFiltering>
    <RuleGroup name="Process Create" groupRelation="or">
      <ProcessCreate onmatch="include">
        <CommandLine condition="contains">mimikatz</Comma
        <CommandLine condition="contains">psexec</Command
        <CommandLine condition="contains">incognito</Comma
      </ProcessCreate>
    </RuleGroup>

    <!-- Capture image load events -->
    <RuleGroup name="Image Load" groupRelation="or">
      <ImageLoad onmatch="include">
        <Image condition="contains">mimikatz</Image>
        <Image condition="contains">psexec</Image>
        <Image condition="contains">incognito</Image>
      </ImageLoad>
    </RuleGroup>

    <!-- Capture access to sensitive processes -->
    <RuleGroup name="Process Access" groupRelation="or">
      <ProcessAccess onmatch="include">
        <TargetImage condition="contains">lsass.exe</Targe
        <TargetImage condition="contains">winlogon.exe</Ta
        <TargetImage condition="contains">services.exe</Ta
        <SourceImage condition="contains">mimikatz.exe</So
        <SourceImage condition="contains">psexec.exe</Sou
      </ProcessAccess>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```

- In Event Viewer, Click the drop down menu, Applications and Services Logs > Microsoft > Sysmon > Operational.

- Scroll through the content, Look specfically for Event ID: 10 This is where attemps to access memory of sensitive processes are identified. (lsass.exe and winlogon.exe)
- You will come across your “whoami.exe” which was run in Exercise 2 in Incognito.exe, where you will see the user as: NT AUTHORITY\SYSTEM