

Hack the Box Operation Blackout 2025: Phantom Check by Melisa Nyamukondiwa

Scenario

Sherlock Scenario



Tallon suspects that the threat actor carried out anti-virtualization checks to avoid detection in sandboxed environments. Your task is to analyze the event logs and identify the specific techniques used for virtualization detection. Byte Doctor requires evidence of the registry checks or processes the attacker executed to perform these checks.

Scenario analysis

- It can be determined that a threat actor carried out an attack but attempted to avoid detection through anti-virtualization checks
- An article on picussecurity.com explains that Virtualization/Sandbox Evasion is a technique utilized by adversaries as a part of their defense evasion strategy to detect and avoid virtualization and analysis environments, such as malware analysis sandboxes. If the malware detects a virtual machine or sandbox environment, it disengages from the victim or does not perform malicious functions, such as downloading the additional payload.
- The task is to analyze the event logs to determine the techniques used for virtualization evasion.

Files/Artifacts Included

The following files were included as part of the investigation and will be centered within this writeup.

Name	Date modified	Type	Size
 Microsoft-Windows-Powershell	2025/04/09 11:24	Event Log	1 092 KB
 Windows-Powershell-Operational	2025/04/09 11:24	Event Log	15 428 KB

These were two event logs; a Powershell Log and a Powershell Operational Log. These logs show “internal operations from the engine, providers, and cmdlets to the Windows event log.” ([Microsoft Learn](https://learn.microsoft.com/en-us/windows/eventlog/)).

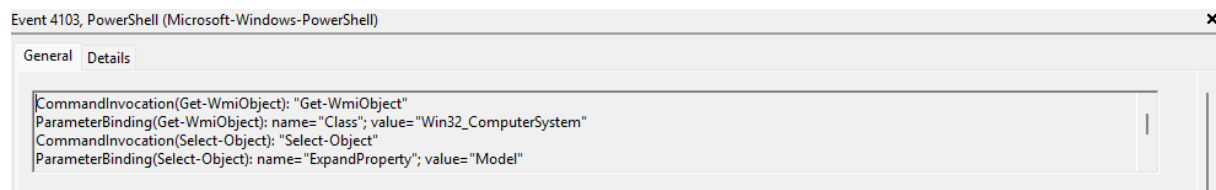
Question 1

Which WMI class did the attacker use to retrieve model and manufacturer information for virtualization detection?

WMI (Windows Management Instrumentation) was used to retrieve the model and manufacturer detection.

The find tool was utilized to find events where the WMI query was used.

Search query used: wmi



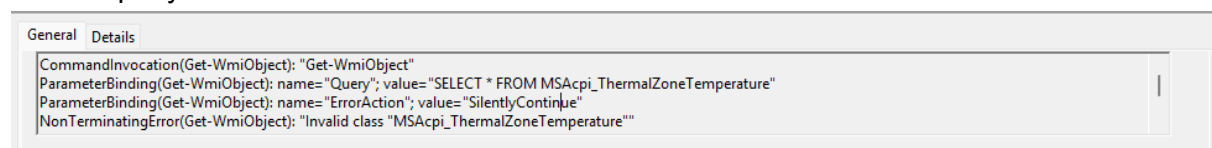
The answer was in value= ""

Task 2

Which WMI query did the attacker execute to retrieve the current temperature value of the machine?

In order to determine the WMI class for temperature, the keyword for temperature thermal was utilized in the find tool

Search query= Thermal

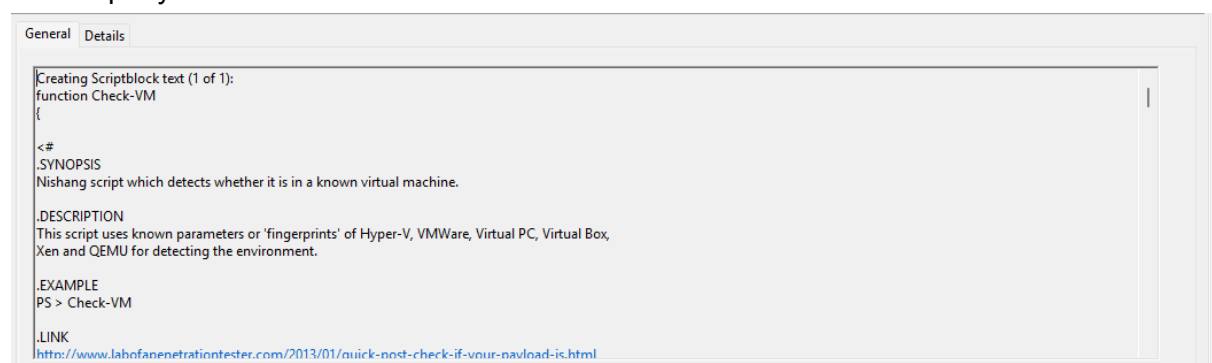


The answer was thus located in value= ""

Task 3

The attacker loaded a PowerShell script to detect virtualization. What is the function name of the script?

Search query= function



The answer is the name of the function.

Task 4

Which registry key did the above script query to retrieve service details for virtualization detection?

The answer was in the abovementioned script

```
if (!$hyperv)
{
    $hyperv = Get-Childitem HKLM:\SYSTEM\ControlSet001\Services
    if (($hyperv -match "vmicheartbeat") -or ($hyperv -match "vmicvss") -or ($hyperv -match "vmicshutdown") -or ($hyperv -match "vmixchange"))
    {
        $hyperv = $true
    }
}
```

Task 5

The VM detection script can also identify VirtualBox. Which processes is it comparing to determine if the system is running VirtualBox?

In order to find out what processes were being compared to find out if the virtualization software being run was Virtualbox, the comment **#Virtualbox** had the script showing the processes. It was thus determined which two scripts were being compared as they were under **Get-Process**

```
#Virtual Box

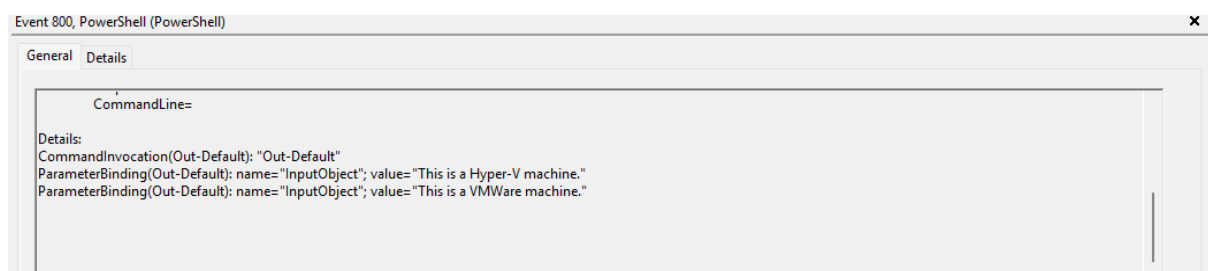
$vb = Get-Process
if (($vb -eq "vboxservice.exe") -or ($vb -match "vboxtray.exe"))
{
    $vbvm = $true
}
if (!$vbvm)
{
    $vb = Get-Childitem HKLM:\HARDWARE\ACPI\FADT
```

Task 6

The VM detection script prints any detection with the prefix 'This is a'. Which two virtualization platforms did the script detect?

In order to find this; the Powershell log was queried using the find tool.

Search query used: "This is a"



Observations

- Attackers sometimes use ant-vm checks often by running scripts which detect the presence of a virtual machine or sandbox
- Powershell and Powershell operations logs are useful for finding traces of evasion utilising queries and keywords associated with this technique.
- Attackers will try to find out system information using get queries and powershell scripts

Lessons Learned

- How to query event logs to more efficiently find traces of an attack or evasion
- How to read powershell scripts to determine their activities

Conclusion

This lab required the analysis of Windows event logs, namely the Powershell and Powershell Operational logs. Through analysis and search queries it was possible to find the scripts and queries the attacker used to determine the model and manufacturer information for virtualization detection. In addition, a script which found the exact virtualization platform was found within the event logs. This lab helped to understand how attackers often evade detection when their malware is executed in sandboxed or virtualized environments. This prevents the investigation and eradication of the attacker's malware.