Sherlock Challenge – Phantom Check

Martina Giacobbe

July 23, 2025

Overview

Phantom Check is a Sherlock challenge designed to showcase common virtualization detection techniques used by attackers. The challenge emphasizes detection engineering skills by exploring how malicious scripts attempt to determine whether they are executing in a Windows virtual machine (VM) environment.

1 Skills Acquired

Players are expected to learn and apply:

- Identification of specific WMI (Windows Management Instrumentation) queries used for virtualization detection.
- Analysis of PowerShell scripts aimed at uncovering virtualization environments.
- Creation of detection rules based on file paths, registry keys, or processes linked to virtual platforms.

2 What is WMI?

Windows Management Instrumentation (WMI) is a Microsoft framework that facilitates system management and monitoring on Windows operating systems. It allows applications and users to access and manipulate data regarding the status of local and remote systems.

WMI works through a set of interfaces that expose system resources, enabling tasks such as:

- Querying hardware and software configurations.
- Managing processes and services.
- Performing remote operations.

More information and query examples can be found at: `https://learn.microsoft.com/en-us/windows/win32/wmisdk/querying-wmi`

3 Challenge Questions and Solutions

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

Query: `Get-WmiObject`
Answer: `Win32_ComputerSystem`

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

Query and Answer: `SELECT * FROM MSAcpi_ThermalZoneTemperature`

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

By reviewing PowerShell Event ID 4104 in the event logs, the script can be found.
Answer: `Check-VM`

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

Inside the identified PowerShell script, a registry path is referenced for querying service-related data:
Answer: `HKLM:001`

5. How did the VM detection script identify VirtualBox?

The script uses the `Get-Process` cmdlet and checks for:

- `vboxservice.exe`
- `vboxtray.exe`

Answer: `vboxservice.exe, vboxtray.exe`

6. The VM detection script prints any detection with the prefix "This is a". Which two virtualization platforms did it identify?

Answer: `Hyper-V, VMware`

Conclusion

Phantom Check is a valuable exercise for understanding how adversaries can detect VM environments to evade detection or analysis. By learning to recognize WMI queries, registry inspection, and process-based indicators, defenders can create robust detection rules that identify these tactics early during post-exploitation or malware analysis.