تقرير مشروع – TryHackMe غرفةSysmon

اسم المشروع:

تحليل الأنشطة الخبيثة باستخدام Sysmon

الهدف من المشروع:

تعلم كيفية إعداد وتشغيل Sysmon على أنظمة Windows لمراقبة الأحداث الأمنية، وتحليل أنماط الهجوم المختلفة مثل Metasploit، Mimikatz، والبرمجيات الخبيثة، واكتشاف التقنيات المستخدمة في التهرب والتحكم المستمر (Persistence).

الأدوات والتقنيات المستخدمة:

- Sysmon System Monitorمن Microsoft Sysinternals
- Windows Event Viewer
- PowerShell
- Sigma Rules
- مهاجمات وهميةMetasploit ، Mimikatzتم تنفيذها داخل بيئةTryHackMe

---

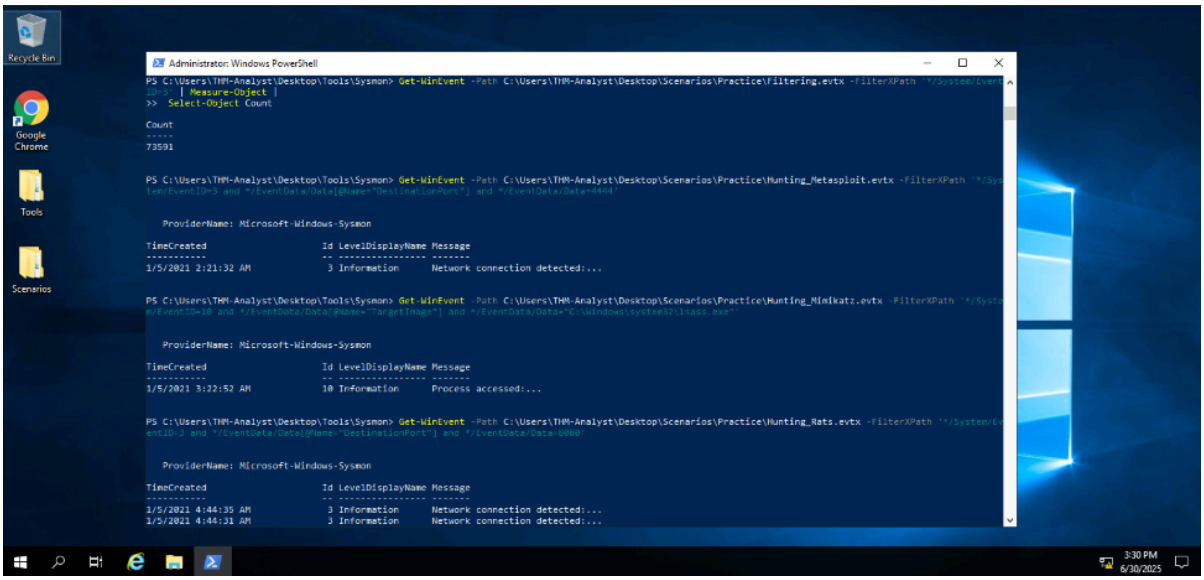
المهام المنجزة:

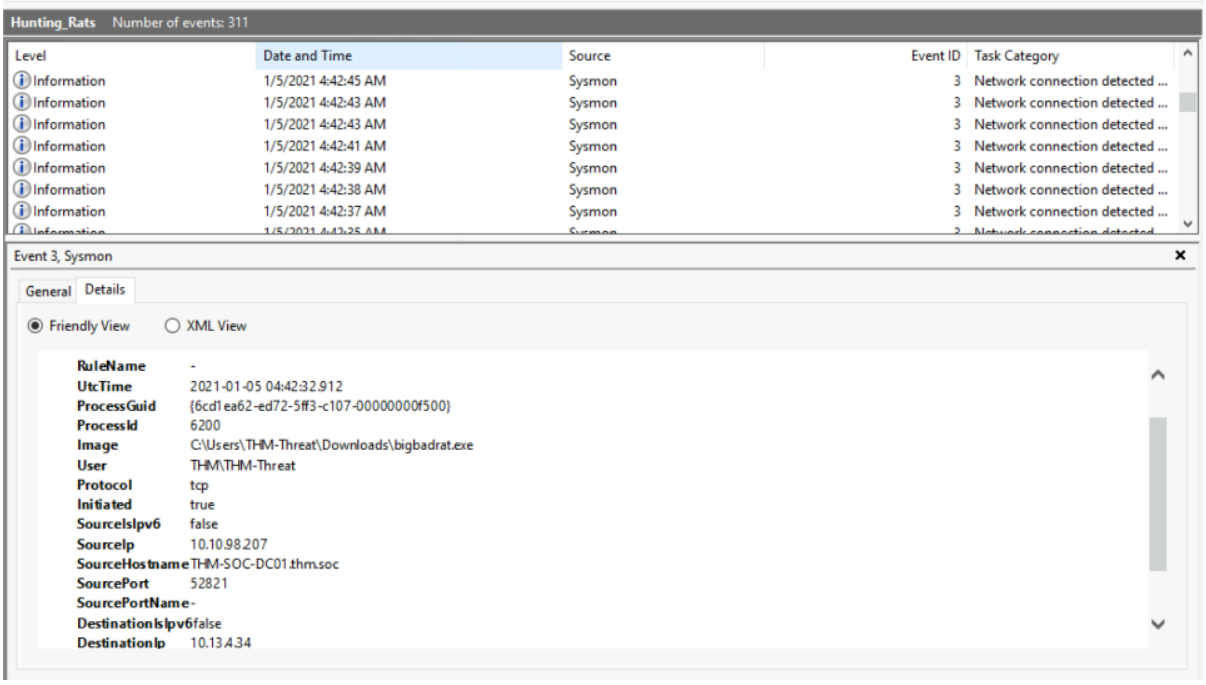
المهمة	الوصف
Task 1: Introduction	مقدمة حول أهمية Sysmon في البيئات الأمنية.
Task 2: Sysmon Overview	فهم كيفية عمل Sysmon وأهم الأحداث التي يمكن مراقبتها.
Task 3: Installing and Preparing Sysmon	تثبيت Sysmon وتكوينه باستخدام ملفات إعداد مخصصة (Configuration XML).
Task 4: Cutting out the Noise	تصفية الأحداث لتقليل الضجيج واكتشاف الأحداث المهمة فقط.
Task 5: Hunting Metasploit	تحليل هجوم باستخدام Metasploit وتحديد نشاط shellcode من خلال logs.
Task 6: Detecting Mimikatz	اكتشاف استخدام Mimikatz وسرقة كلمات المرور من الذاكرة.
Task 7: Hunting Malware	تتبع تشغيل برمجيات خبيثة وتحليل سلوكها داخل النظام.
Task 8: Hunting Persistence	الكشف عن تقنيات الـ Persistence مثل Run keys و Scheduled Tasks.
Task 9: Detecting Evasion Techniques	مراقبة محاولات المهاجم تجاوز أنظمة المراقبة أو تعطيل Sysmon.
Task 10: Practical Investigations	تحليل حادث أمني متكامل باستخدام جميع المهارات السابقة.

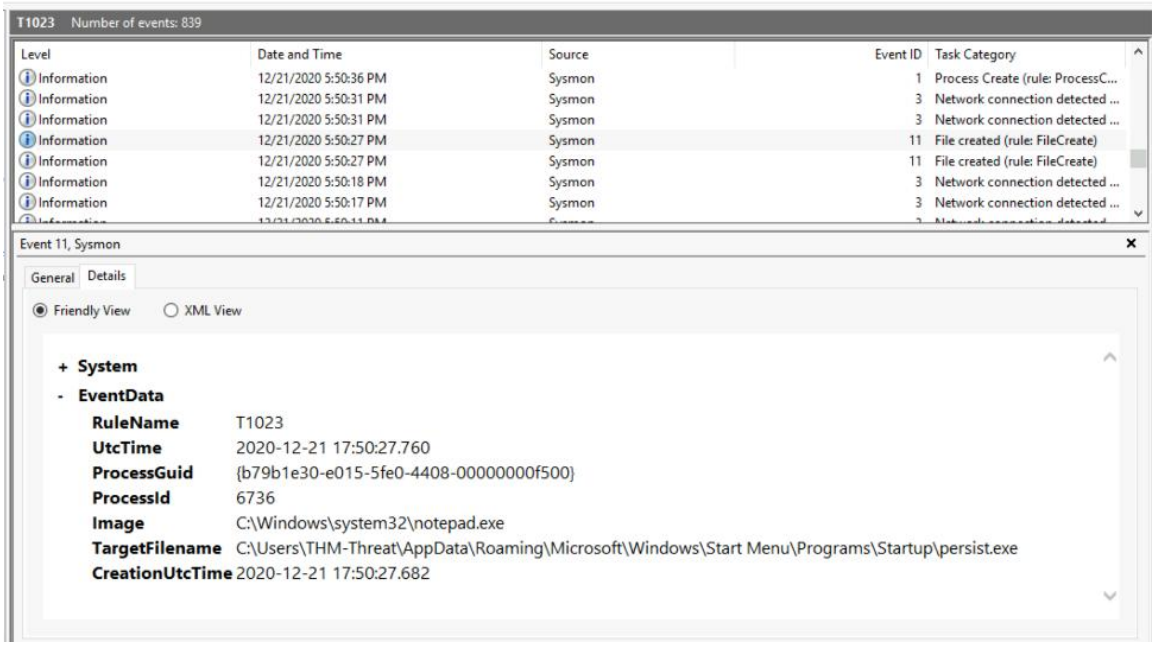
ملخص النتائج:

- تم بنجاح إعداد نظام مراقبة فعال باستخدام Sysmon.
- تم اكتشاف وتحليل عدة هجمات معروفة مثل Mimikatz و Metasploit.
- تم تطبيق مهارات Threat Hunting على سيناريوهات متنوعة مثل البرمجيات الخبيثة، السيطرة المستمرة، والتهرب.

لقطات من المشروع:






T1023 Number of events: 839
Level
Date and Time
Source
Event ID
Task Category
Information 12/21/2020 5:50:36 PM Sysmon 1 Process Create (rule: ProcessC...
Information 12/21/2020 5:50:31 PM Sysmon 3 Network connection detected ...
Information 12/21/2020 5:50:31 PM Sysmon 3 Network connection detected ...
Information 12/21/2020 5:50:27 PM Sysmon 11 File created (rule: FileCreate)
Information 12/21/2020 5:50:27 PM Sysmon 11 File created (rule: FileCreate)
Information 12/21/2020 5:50:18 PM Sysmon 3 Network connection detected ...
Information 12/21/2020 5:50:17 PM Sysmon 3 Network connection detected ...
Event 11, Sysmon
General
Details
Friendly View
XML View
+ System
- EventData
RuleName T1023
UtcTime 2020-12-21 17:50:27.760
ProcessGuid {b79b1e30-e015-5fe0-4408-00000000f500}
ProcessId 6736
Image C:\Windows\system32\notepad.exe
TargetFilename C:\Users\THM-Threat\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\persist.exe
CreationUtcTime 2020-12-21 17:50:27.682

Task 10 Practical Investigations

Event files used within this task have been sourced from the EVTX-ATTACK-SAMPLES and SysmonResources Github repositories.

Download Task Files

You can download the event logs used in this room from this task or you can open them in the Investigations folder on the provided machine.

Investigation 1 - ugh, BILL THAT'S THE WRONG USB!

In this investigation, your team has received reports that a malicious file was dropped onto a host by a malicious USB. They have pulled the logs suspected and have tasked you with running the investigation for it.

Logs are located in `C:\Users\THM-Analyst\Desktop\Scenarios\Investigations\Investigation-1.evtx`.

Investigation 2 - This isn't an HTML file?

Another suspicious file has appeared in your logs and has managed to execute code masking itself as an HTML file, evading your anti-virus detections. Open the logs and investigate the suspicious file.

Logs are located in `C:\Users\THM-Analyst\Desktop\Scenarios\Investigations\Investigation-2.evtx`.

Investigation 3.1 - 3.2 - Where's the bouncer when you need him

Your team has informed you that the adversary has managed to set up persistence on your endpoints as they continue to move throughout your network. Find how the adversary managed to gain persistence using logs provided.

Logs are located in `C:\Users\THM-Analyst\Desktop\Scenarios\Investigations\Investigation-3.1.evtx`

and `C:\Users\THM-Analyst\Desktop\Scenarios\Investigations\Investigation-3.2.evtx`.

Investigation 4 - Mom look! I built a botnet!

As the adversary has gained a solid foothold onto your network it has been brought to your attention that they may have been able to set up C2 communications on some of the endpoints. Collect the logs and continue your investigation.

Logs are located in `C:\Users\THM-Analyst\Desktop\Scenarios\Investigations\Investigation-4.evtx`.

Answer the questions below

What is the full registry key of the USB device calling svchost.exe in Investigation 1?

HKLM\System\CurrentControlSet\Enum\WpdBusEnumRoot\UMB\2&37c186b&0&STORAGE#VOLUME#_??_USBSTOR#DISK&V — ✓ Correct Answer

What is the device name when being called by RawAccessRead in Investigation 1?

\Device\HarddiskVolume3 — ✓ Correct Answer

What is the first exe the process executes in Investigation 1?

rundll32.exe — ✓ Correct Answer

What is the full path of the payload in Investigation 2?

C:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\S97WTYG7\update.hta — ✓ Correct Answer

What is the full path of the file the payload masked itself as in Investigation 2?

C:\Users\IEUser\Downloads\update.html — ✓ Correct Answer

What signed binary executed the payload in Investigation 2?

C:\Windows\System32\mshta.exe — ✓ Correct Answer

What is the IP of the adversary in Investigation 2?

10.0.2.18 — ✓ Correct Answer

What back connect port is used in Investigation 2?

4443 — ✓ Correct Answer

What is the IP of the suspected adversary in Investigation 3.1?

172.30.1.253 — ✓ Correct Answer

What is the hostname of the affected endpoint in Investigation 3.1?

DESKTOP-O153T4R — ✓ Correct Answer

What is the hostname of the C2 server connecting to the endpoint in Investigation 3.1?

empirec2 — ✓ Correct Answer

Where in the registry was the payload stored in Investigation 3.1?

HKLM\SOFTWARE\Microsoft\Network\debug — ✓ Correct Answer

What PowerShell launch code was used to launch the payload in Investigation 3.1?

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "$x=$((gp HKLM:Software\Microsoft\Network debug)) — ✓ Correct Answer

What is the IP of the adversary in Investigation 3.2?

172.168.103.188 — ✓ Correct Answer

What is the full path of the payload location in Investigation 3.2?

c:\users\q\AppData:blah.txt — ✓ Correct Answer

What was the full command used to create the scheduled task in Investigation 3.2?

"C:\WINDOWS\system32\schtasks.exe" /Create /F /SC DAILY /ST 09:00 /TN Updater /TR "C:\Windows\System32\WindowsPo — ✓ Correct Answer

What process was accessed by schtasks.exe that would be considered suspicious behavior in Investigation 3.2?

lsass.exe — ✓ Correct Answer

What is the IP of the adversary in Investigation 4?

172.30.1.253 — ✓ Correct Answer

What port is the adversary operating on in Investigation 4?

80 — ✓ Correct Answer

What C2 is the adversary utilizing in Investigation 4?

Empire — ✓ Correct Answer

التوصيات:

- الاعتماد على Sysmon في بيئات الإنتاج لأهميته في تسجيل الأنشطة الدقيقة.
- تخصيص ملفات التهيئة (Configuration) لتقليل الضجيج.
- دمج Sysmon مع أدوات) SIEM مثل Splunk أو (Wazuh لمراقبة الأحداث بشكل مركزي.