University of Utah
School of Computing
CS 6967: Security Operations

Lab 10 Response Outline

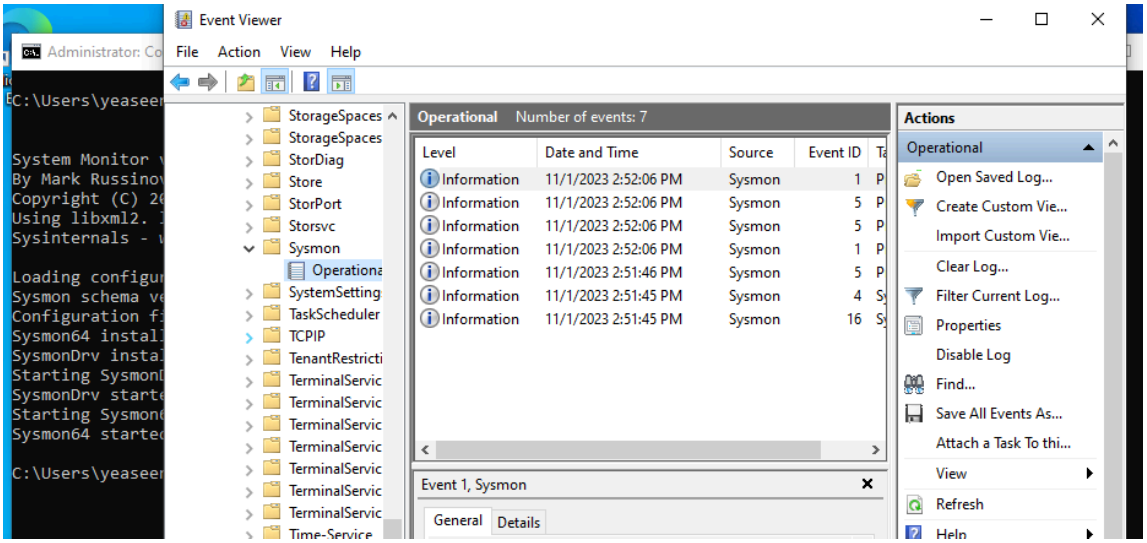
Lab 10: Threat Hunting With Sysmon

Test 1: Check That Sysmon Is Working Properly

Summary of test experience:

In Test 1, we are required to install and configure Sysmon on Windows to perform Threat Hunting.

Screenshot of test results:



```
C:\Users\yeaseer

System Monitor v
By Mark Russinov
Copyright (C) 20
Using libxml2. I
Sysinternals - w

Loading configur
Sysmon schema ve
Configuration fi
Sysmon64 install
SysmonDrv instal
Starting SysmonD
SysmonDrv starte
Starting Sysmon6
Sysmon64 started

C:\Users\yeaseer
```

Operational Number of events: 7

Level	Date and Time	Source	Event ID	Ta
Information	11/1/2023 2:52:06 PM	Sysmon	1	P
Information	11/1/2023 2:52:06 PM	Sysmon	5	P
Information	11/1/2023 2:52:06 PM	Sysmon	5	P
Information	11/1/2023 2:52:06 PM	Sysmon	1	P
Information	11/1/2023 2:51:46 PM	Sysmon	5	P
Information	11/1/2023 2:51:45 PM	Sysmon	4	Sy
Information	11/1/2023 2:51:45 PM	Sysmon	16	Sy

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

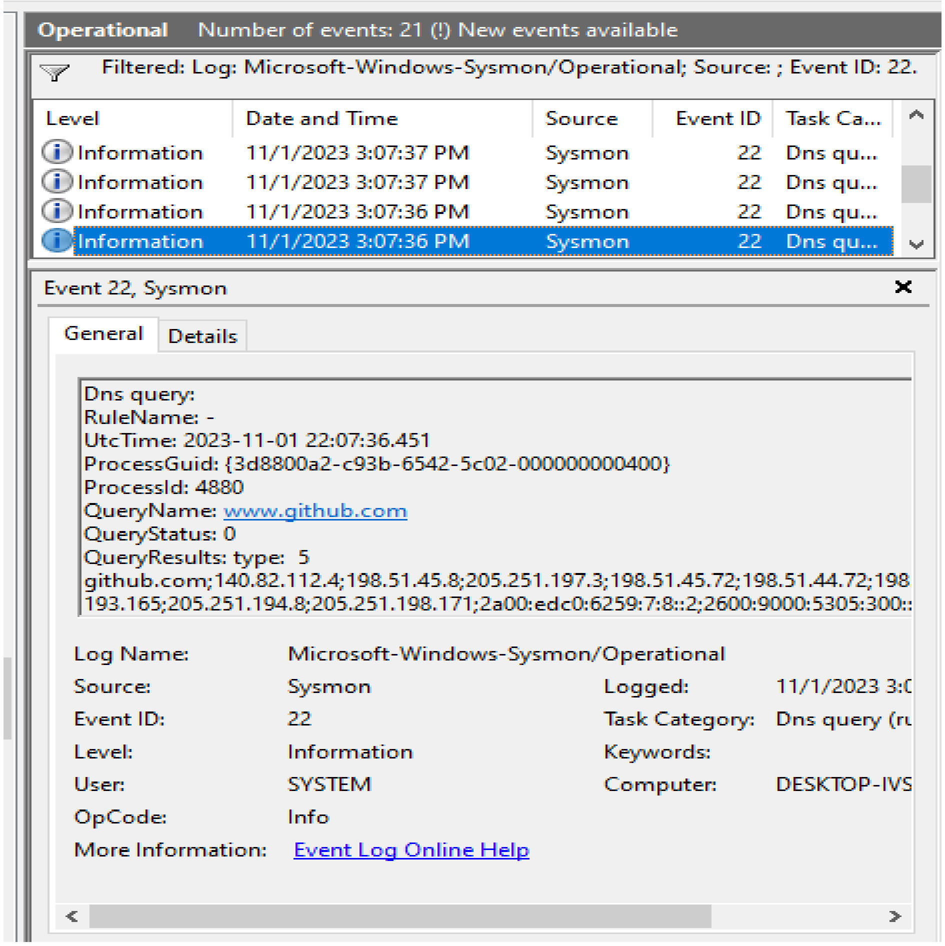
From the above image, the Operational folder exists under the Sysmon folder, indicating the completeness of this Test.

Test 2: Test Whether Sysmon Works

Summary of test experience:

This test aims to update the configuration file and run the Sysmon tool based on a new configuration file.

Screenshot of test results:



Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 22.

Level	Date and Time	Source	Event ID	Task Ca...
Information	11/1/2023 3:07:37 PM	Sysmon	22	Dns qu...
Information	11/1/2023 3:07:37 PM	Sysmon	22	Dns qu...
Information	11/1/2023 3:07:36 PM	Sysmon	22	Dns qu...
Information	11/1/2023 3:07:36 PM	Sysmon	22	Dns qu...

```
Dns query:
RuleName: -
UtcTime: 2023-11-01 22:07:36.451
ProcessGuid: {3d8800a2-c93b-6542-5c02-000000000400}
ProcessId: 4880
QueryName: www.github.com
QueryStatus: 0
QueryResults: type:  5
github.com;140.82.112.4;198.51.45.8;205.251.197.3;198.51.45.72;198.51.44.72;198
193.165;205.251.194.8;205.251.198.171;2a00:edc0:6259:7:8::2;2600:9000:5305:300::
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	11/1/2023 3:0
Event ID:	22	Task Category:	Dns query (ru
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-IVS
OpCode:	Info		
More Information:	Event Log Online Help		

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

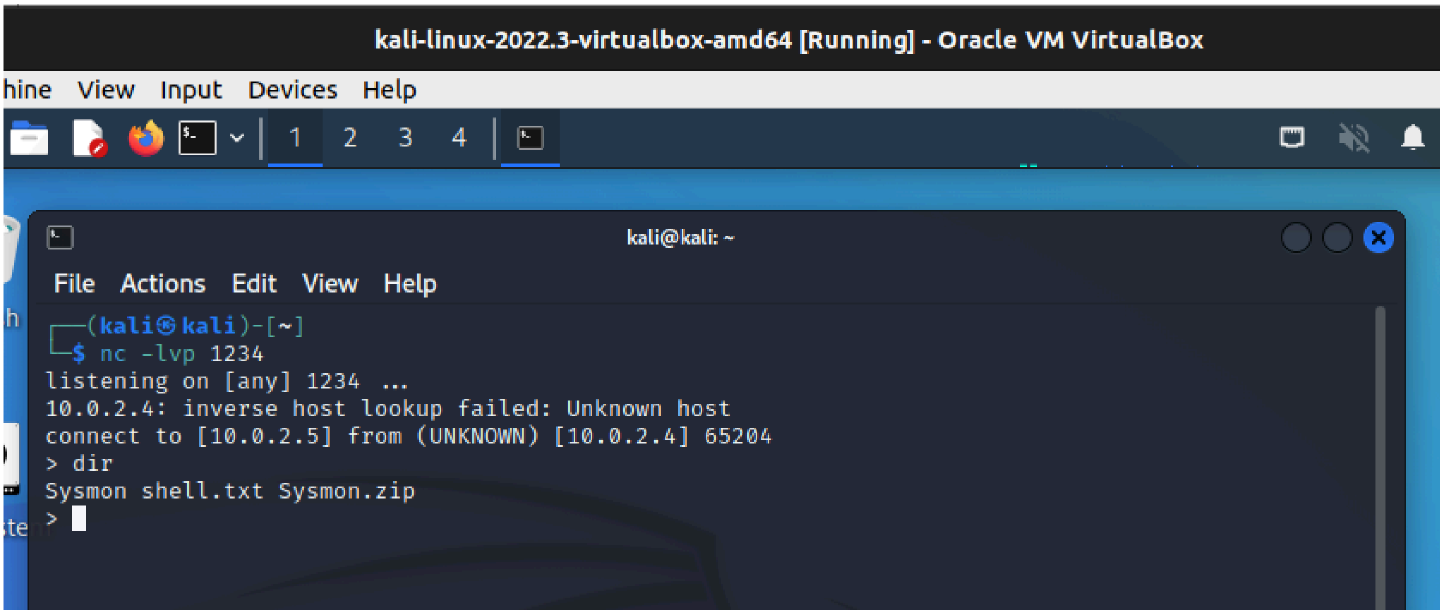
The above screenshot shows that Sysmon captured the query “www.github.com” under its event on 22.

Test 3: Test the Reverse Shell Attack

Summary of test experience:

In this test, a reverse shell script is run on the Windows machine to create a reverse shell on the Kali machine, which is the attacker here. Here, I faced a problem. The given command to invoke the reverse shell script wasn’t working. So, I used this: **powersehll -command “& { Invoke-Expression (Get-Content -Raw .\shell.txt) }”**

Screenshot of test results:



kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
hine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
10.0.2.4: inverse host lookup failed: Unknown host
connect to [10.0.2.5] from (UNKNOWN) [10.0.2.4] 65204
> dir
Sysmon shell.txt Sysmon.zip
> 
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

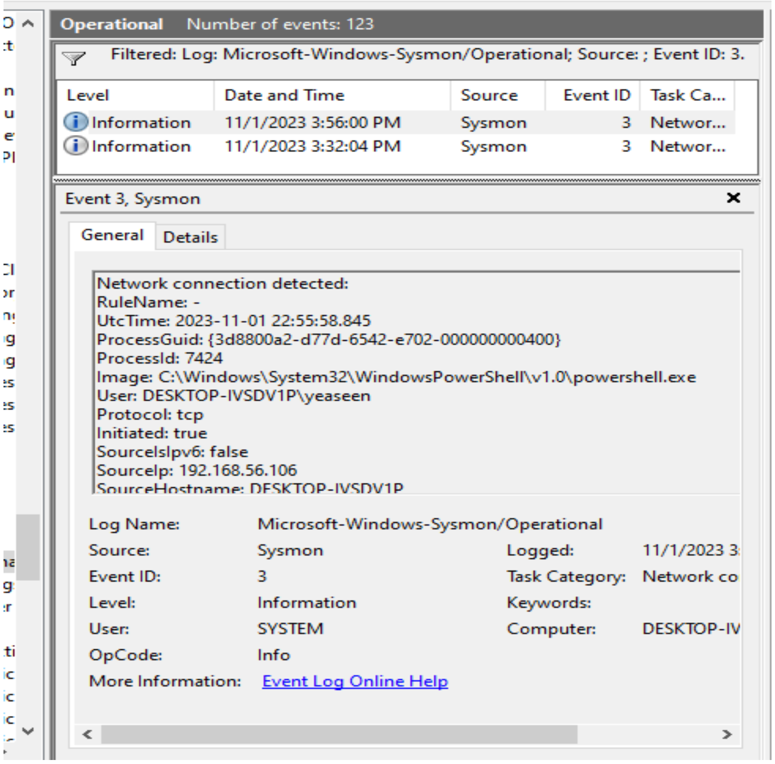
From the above screenshot, it can be seen that the Kali machine got access to the shell of the Windows machine.

Test 4: Check Sysmon Logs

Summary of test experience:

In this test, we must go through the Sysmon logs to unveil the reverse shell attack. The scenario here is a powershell execution through the network connection, which is an unusual scene. Event Id 3 from the Sysmon configuration file should capture and write this in the log.

Screenshot of test results:



Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 3.

Level	Date and Time	Source	Event ID	Task Ca...
Information	11/1/2023 3:56:00 PM	Sysmon	3	Networ...
Information	11/1/2023 3:32:04 PM	Sysmon	3	Networ...

```
Network connection detected:
RuleName: -
UtcTime: 2023-11-01 22:55:58.845
ProcessGuid: {3d8800a2-d77d-6542-e702-000000000400}
ProcessId: 7424
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
User: DESKTOP-IVSDV1P\yeaseen
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.56.106
SourceHostname: DESKTOP-IVSDV1P
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	11/1/2023 3:
Event ID:	3	Task Category:	Network co
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-IV
OpCode:	Info		
More Information:	Event Log Online Help		

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

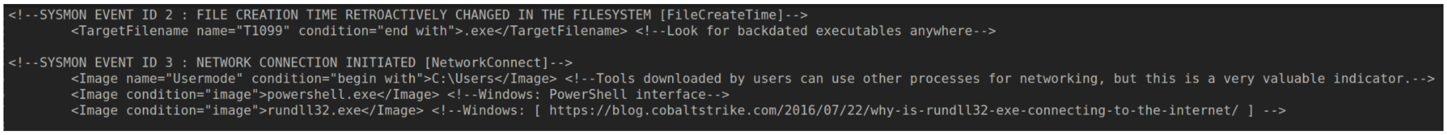
The above screenshot shows that the “powershell.exe” image is executed under the Network connection, which is captured by Event ID 3 from the configuration file of Sysmon.

Test 5: Identify the Minimal Set of Commands

Summary of test experience:

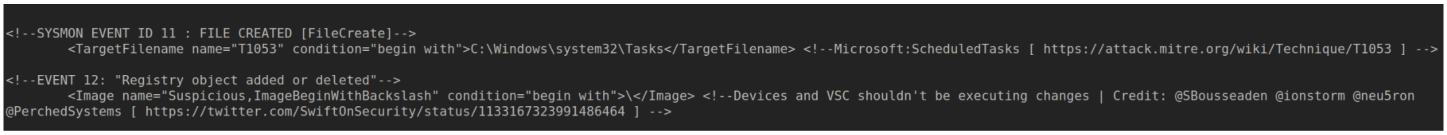
This test requires us to identify the minimal set of commands/rules in the Sysmon configuration that enabled logging of the above reverse shell attack. I went through the Sysmon logs to find which events from the configuration file captured which rules.

Screenshot of test results:



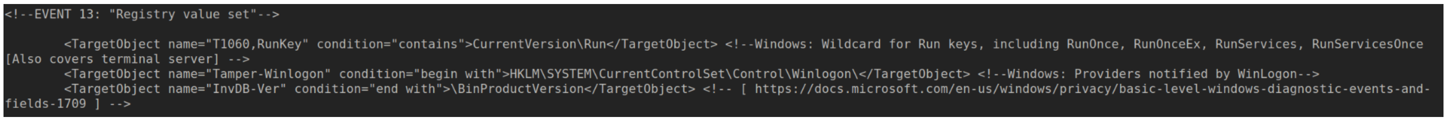
```
<!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM [FileCreateTime]-->
        <TargetFilename name="T1099" condition="end with">.exe</TargetFilename> <!--Look for backdated executables anywhere-->

<!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
        <Image name="Usermode" condition="begin with">C:\Users</Image> <!--Tools downloaded by users can use other processes for networking, but this is a very valuable indicator.-->
        <Image condition="image">powershell.exe</Image> <!--Windows: PowerShell interface-->
        <Image condition="image">rundll32.exe</Image> <!--Windows: [ https://blog.cobaltstrike.com/2016/07/22/why-is-rundll32-exe-connecting-to-the-internet/ ] -->
```



```
<!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
        <TargetFilename name="T1053" condition="begin with">C:\Windows\system32\Tasks</TargetFilename> <!--Microsoft:ScheduledTasks [ https://attack.mitre.org/wiki/Technique/T1053 ] -->

<!--EVENT 12: "Registry object added or deleted"-->
        <Image name="Suspicious,ImageBeginWithBackslash" condition="begin with">\</Image> <!--Devices and VSC shouldn't be executing changes | Credit: @SBousseaden @ionstorm @neu5ron
@PerchedSystems [ https://twitter.com/SwiftOnSecurity/status/1133167323991486464 ] -->
```



```
<!--EVENT 13: "Registry value set"-->

        <TargetObject name="T1060,RunKey" condition="contains">CurrentVersion\Run</TargetObject> <!--Windows: Wildcard for Run keys, including RunOnce, RunOnceEx, RunServices, RunServicesOnce
[Also covers terminal server] -->
        <TargetObject name="Tamper-Winlogon" condition="begin with">HKLM\SYSTEM\CurrentControlSet\Control\Winlogon\</TargetObject> <!--Windows: Providers notified by WinLogon-->
        <TargetObject name="InvDB-Ver" condition="end with">\BinProductVersion</TargetObject> <!-- [ https://docs.microsoft.com/en-us/windows/privacy/basic-level-windows-diagnostic-events-and-
fields-1709 ] -->
```

Provide a brief (1–2 sentences) explanation of the results answering the question: How does the image demonstrate that you completed the test?

Among the above rules captured by Sysmon, the most important is the execution powershell and rundll executables in the network connection. Also, event ID 12, whose task is to screen registry objects added or deleted, captured a suspicious image that began with a backslash.