Sysmon Challenge

Here we can find the whole challenge that I did. We need to search for the correct directory and open the corrected files to start the challenge.

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.

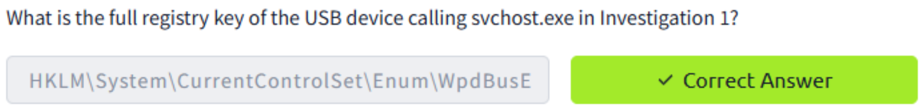
Logs are located in C:\Users\THM-Analyst\Desktop\Scenarios\Investigations\Investigation-3.1.evtx

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

Investigation 4 - Mom look! I built a botnet!

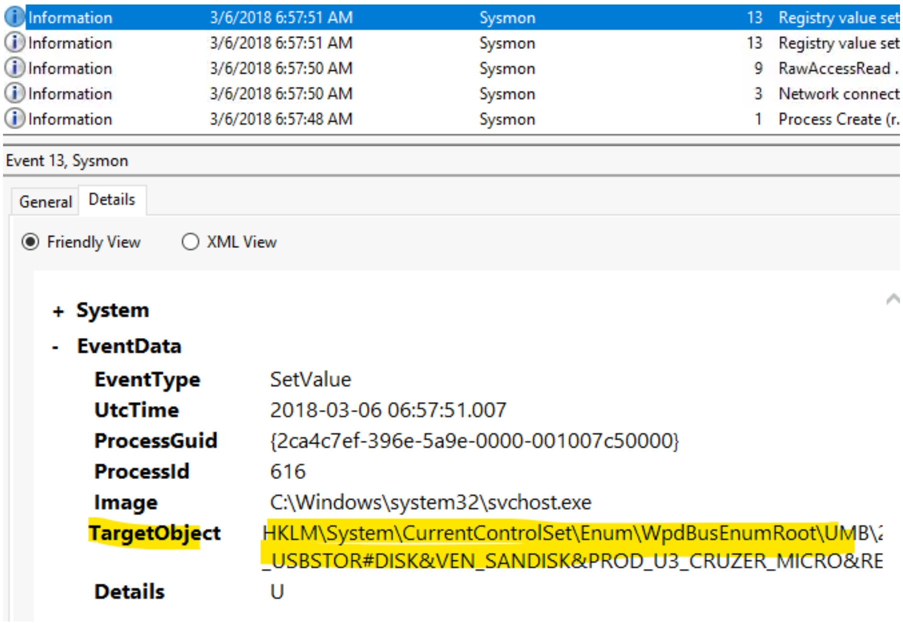
As the adversary has gained a solid foothold onto your network it has been brought to your attention that they may have been able to set up C2 communications on some of the endpoints. Collect the logs and continue your investigation.

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



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

HKLM\System\CurrentControlSet\Enum\WpdBusE



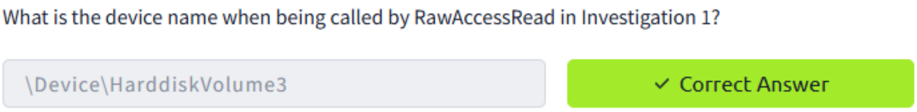
Information	3/6/2018 6:57:51 AM	Sysmon	13	Registry value set
Information	3/6/2018 6:57:51 AM	Sysmon	13	Registry value set
Information	3/6/2018 6:57:50 AM	Sysmon	9	RawAccessRead .
Information	3/6/2018 6:57:50 AM	Sysmon	3	Network connect
Information	3/6/2018 6:57:48 AM	Sysmon	1	Process Create (r.

Event 13, Sysmon

+ System

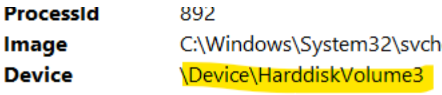
- EventData

EventType	SetValue
UtcTime	2018-03-06 06:57:51.007
ProcessGuid	{2ca4c7ef-396e-5a9e-0000-001007c50000}
ProcessId	616
Image	C:\Windows\system32\svchost.exe
TargetObject	HKLM\System\CurrentControlSet\Enum\WpdBusEnumRoot\UMB\ _USBSTOR#DISK&VEN_SANDISK&PROD_U3_CRUZER_MICRO&RE
Details	U

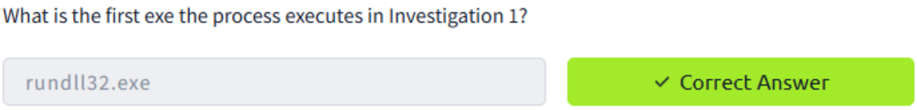


What is the device name when being called by RawAccessRead in Investigation 1?

\Device\HarddiskVolume3

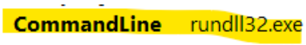


ProcessId	892
Image	C:\Windows\System32\svchost.exe
Device	\Device\HarddiskVolume3



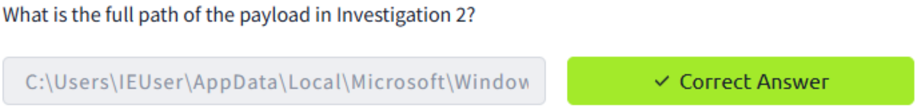
What is the first exe the process executes in Investigation 1?

rundll32.exe



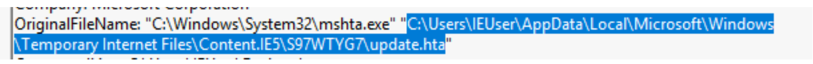
CommandLine rundll32.exe

I opened the correct file for this question.

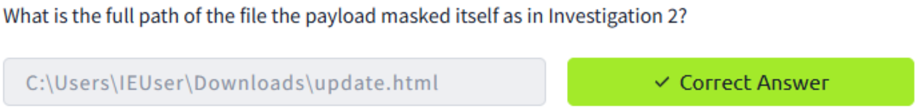


What is the full path of the payload in Investigation 2?

C:\Users\IEUser\AppData\Local\Microsoft\Window

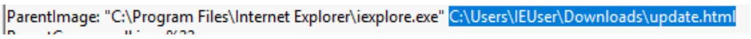


OriginalFileName: "C:\Windows\System32\mshta.exe" "C:\Users\IEUser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\S97WTYG7\update.hta"

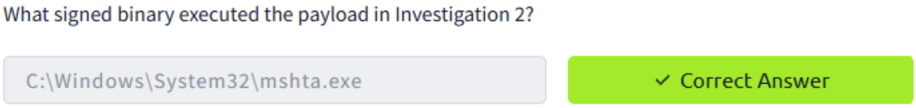


What is the full path of the file the payload masked itself as in Investigation 2?

C:\Users\IEUser\Downloads\update.html



ParentImage: "C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\IEUser\Downloads\update.html



What signed binary executed the payload in Investigation 2?

C:\Windows\System32\mshta.exe

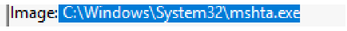
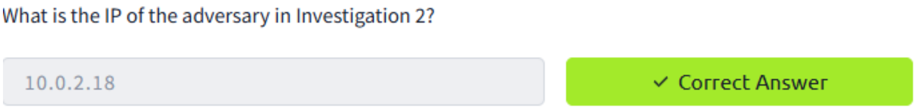
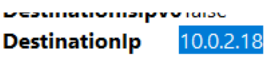
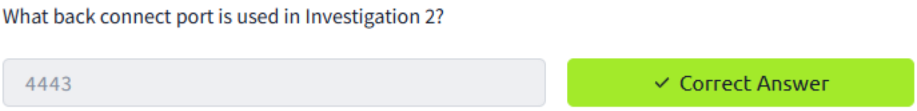


Image: C:\Windows\System32\mshta.exe

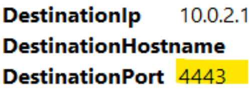

What is the IP of the adversary in Investigation 2?

10.0.2.18 ✓ Correct Answer

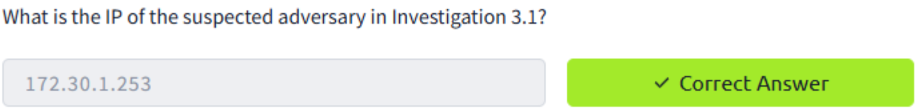

DestinationIsIpv6 false
DestinationIp 10.0.2.18


What back connect port is used in Investigation 2?

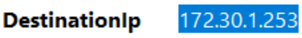
4443 ✓ Correct Answer

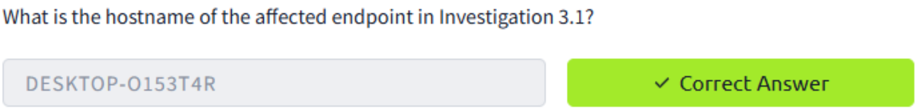

DestinationIp 10.0.2.18
DestinationHostname
DestinationPort 4443

I opened the new file for investigation 3.

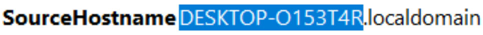

What is the IP of the suspected adversary in Investigation 3.1?

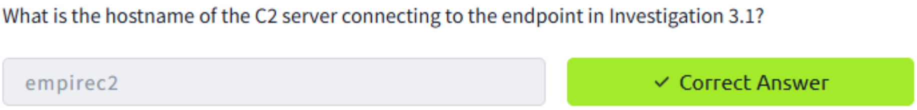
172.30.1.253 ✓ Correct Answer


DestinationIp 172.30.1.253

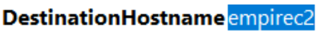

What is the hostname of the affected endpoint in Investigation 3.1?

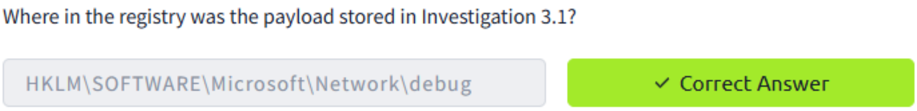
DESKTOP-O153T4R ✓ Correct Answer


SourceHostname DESKTOP-O153T4R.localdomain

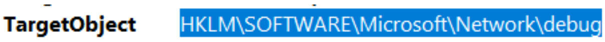

What is the hostname of the C2 server connecting to the endpoint in Investigation 3.1?

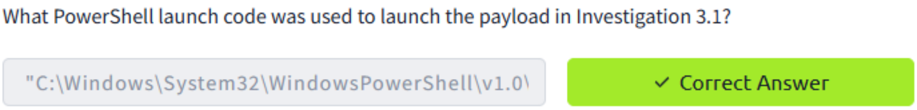
empirec2 ✓ Correct Answer


DestinationHostname empirec2

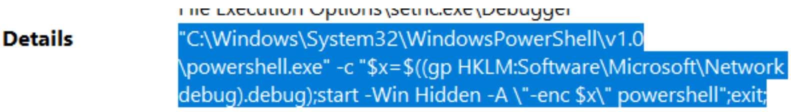

Where in the registry was the payload stored in Investigation 3.1?

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

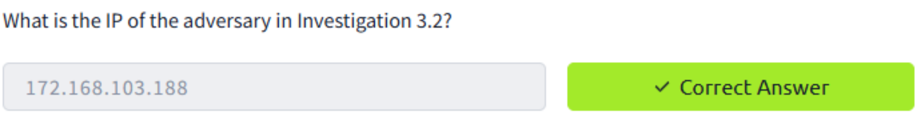

TargetObject HKLM\SOFTWARE\Microsoft\Network\debug


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

"C:\Windows\System32\WindowsPowerShell\v1.0\ ✓ Correct Answer

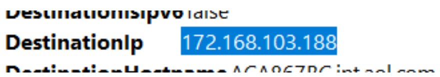

File Execution Options\sethc.exe\Debugger

Details "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "$x=$((gp HKLM:Software\Microsoft\Network debug).debug);start -Win Hidden -A \"-enc $x\" powershell";exit;

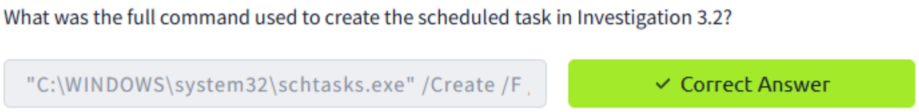


What is the IP of the adversary in Investigation 3.2?

172.168.103.188

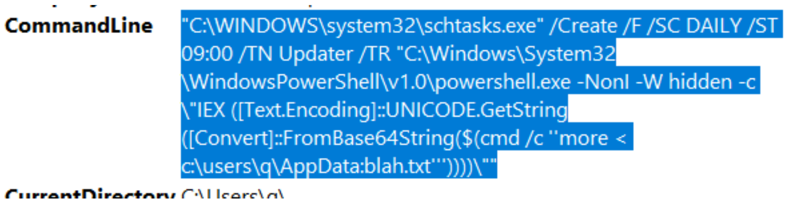


```
DestinationIsIpv6 false
DestinationIp     172.168.103.188
DestinationHostname ACA867BC.int.aol.com
```

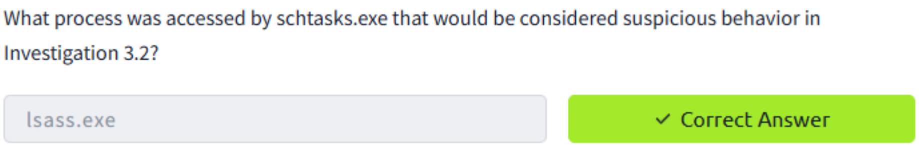


What was the full command used to create the scheduled task in Investigation 3.2?

"C:\WINDOWS\system32\schtasks.exe" /Create /F

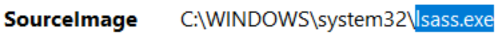


```
CommandLine     "C:\WINDOWS\system32\schtasks.exe" /Create /F /SC DAILY /ST
                09:00 /TN Updater /TR "C:\Windows\System32
                \WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c
                \"IEX ([Text.Encoding]::UNICODE.GetString
                ([Convert]::FromBase64String($(cmd /c ''more <
                c:\users\q\AppData:blah.txt'''))))\""
CurrentDirectory C:\Users\q\
```



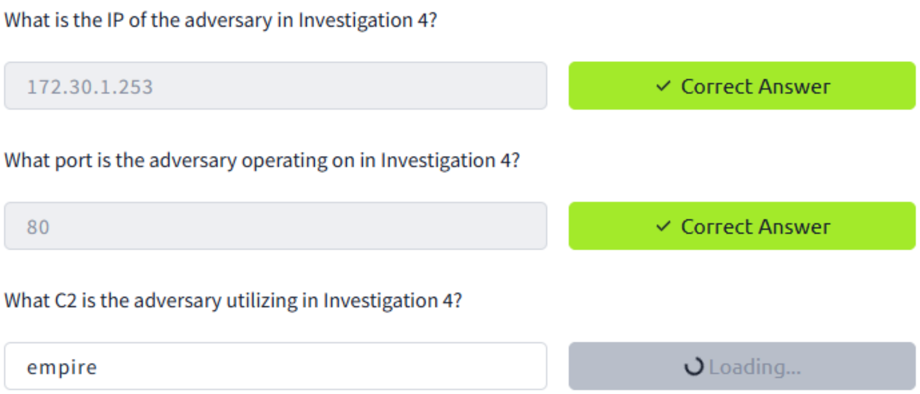
What process was accessed by schtasks.exe that would be considered suspicious behavior in Investigation 3.2?

lsass.exe



```
SourceImage     C:\WINDOWS\system32\lsass.exe
```

The last investigation:



What is the IP of the adversary in Investigation 4?

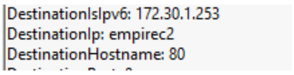
172.30.1.253

What port is the adversary operating on in Investigation 4?

80

What C2 is the adversary utilizing in Investigation 4?

empire



```
DestinationIsIpv6: 172.30.1.253
DestinationIp: empirec2
DestinationHostname: 80
```