Monday Monitor

Swiftspend Finance, the coolest fintech company in town, is on a mission to level up its cyber security game to keep those digital adversaries at bay and ensure their customers stay safe and sound.

Led by the tech-savvy Senior Security Engineer John Sterling, Swiftspend's latest project is about beefing up their endpoint monitoring using Wazuh and Sysmon. They've been running some tests to see how well their cyber guardians can sniff out trouble. And guess what? You're the cyber sleuth they've called in to crack the code!

The tests were run on Apr 29, 2024, between 12:00:00 and 20:00:00. As you dive into the logs, you'll look for any suspicious process shenanigans or weird network connections, you name it! Your mission? Unravel the mysteries within the logs and dish out some epic insights to fine-tune Swiftspend's defences.

Machine Access

Click the **Start Machine** button attached to this task to start the VM. Give the machine about **5 minutes** to fully set up the environment. Access the Wazuh Dashboard using your browser at https://10-10-193-254.reverse-proxy-eu-west-1.tryhackme.com and use the credentials listed below:

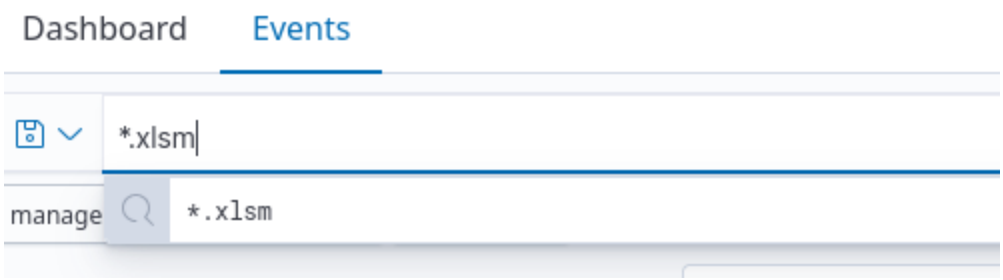
Username	admin
Password	Mond*yM0nit0r7

Once logged in, navigate to the **Security** events module and use the saved query to access the logs.

Note : First change the time accordingly Apr 29, 2024, between 12:00:00 and 20:00:00 and then use the saved query

Q-1 Initial access was established using a downloaded file. What is the file name saved on the host?

We are looking for the file that was downloaded , search for the common file types and analyze the filtered logs



Analyze the logs

_index	wazuh-alerts-4.x-2024.04.29
agent.id	003
agent.ip	10.10.205.57
agent.name	Windows_SwiftSpend2
data.win.eventdata.commandLine	\"powershell.exe\" & {$url = 'http://localhost/SwiftSpend_Financial_Expenses.xlsm' Invoke-WebRequest -Uri $ur sm}
data.win.eventdata.company	Microsoft Corporation
data.win.eventdata.currentDirectory	C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\
data.win.eventdata.description	Windows PowerShell
data.win.eventdata.fileVersion	10.0.17763.1 (WinBuild.160101.0800)

Flag-1 : *SwiftSpend_Financial_Expenses.xlsm*

Q2: What is the full command run to create a scheduled task?

Search for scheduler or similar words , go through the logs

data.win.eventdata.fileVersion	10.0.17763.1613 (WinBuild.160101.0800)
data.win.eventdata.hashes	MD5=2F6CE97FAF2D5EEA919E4393BDD416A7,SHA256=4B679CCC4E0E84A9EDDC24362EA4A86835597A90D94A1AE0EA905D7BCD9F771C,IMPHASH=0BF09EE8918142EE8D325D5955AA1CD9
data.win.eventdata.image	C:\\Windows\\System32\\schtasks.exe
data.win.eventdata.integrityLevel	High
data.win.eventdata.logonGuid	{c5d2b969-8a47-662f-8b54-0a0000000000}
data.win.eventdata.logonId	0xa548b
data.win.eventdata.originalFileName	schtasks.exe
data.win.eventdata.parentCommandLine	\"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f & schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34\"
data.win.eventdata.parentImage	C:\\Windows\\System32\\cmd.exe
data.win.eventdata.parentProcessGuid	{c5d2b969-aada-662f-6a02-000000002201}
data.win.eventdata.parentProcessId	6520
data.win.eventdata.parentUser	ATOMIC\\Administrator

Flag -2 : *\"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f & schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Ge*

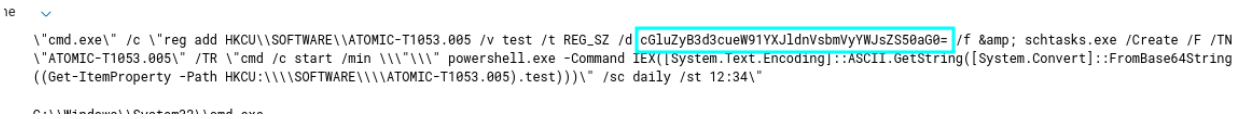
t-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34\"

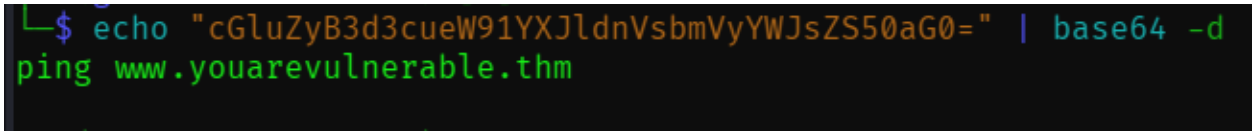
Q3 What time is the scheduled task meant to run?

Flag-3 : 12:34 (It is present in the last question answer)

Q4 What was encoded?

Decode the base64 encoded string in the command





Flag-4 : *ping www.youarevulnerable.thm*

Q5 What password was set for the new user account?

On the left side panel enable the data.win.eventdata.commandLine field which may useful to analyse the logs fastly

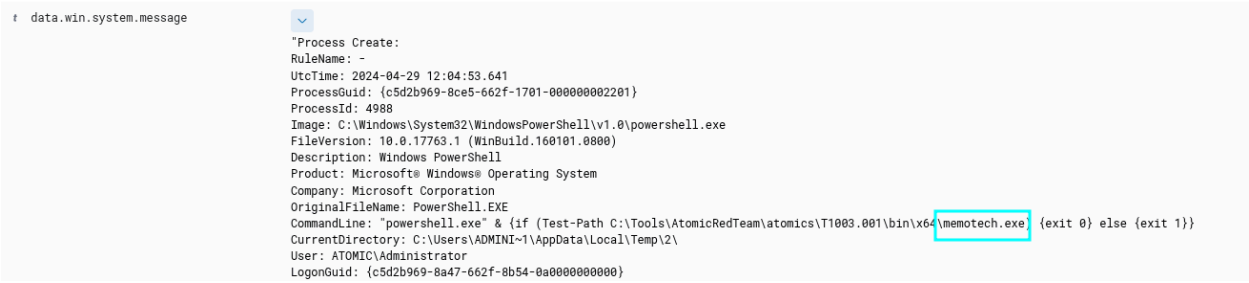
Go throught logs , find the answer

t	_index	wazuh-alerts-4.x-2024.04.29
t	agent.id	003
t	agent.ip	10.10.205.57
t	agent.name	Windows_SwiftSpend2
t	data.win.eventdata.commandLine	\"C:\\Windows\\system32\\net.exe\" user guest I_AM_M0NIT0R1NG
t	data.win.eventdata.company	Microsoft Corporation
t	data.win.eventdata.currentDirectory	C:\\Users\\Administrator\\
t	data.win.eventdata.description	Net Command

Flag-5 : *I_AM_M0NIT0R1NG*

Q6 What is the name of the .exe that was used to dump credentials?

I was just gone through the logs accidentally i got this



Flag-6 *: memotech.exe*

Q7：Data was exfiltrated from the host. What was the flag that was part of the data?

Go Through the logs one by one while searching for the Q5 I found this Flag

Flag-7 *THM{M0N1T0R_1$_1N_3FF3CT}*