Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

mondaymonitor – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | mondaymonitor – Enrico Santarelli |
| **N° Revisão** | 1 |
| **Data de publicação** | 21/10/2024 |
| **Link** | <https://tryhackme.com/r/room/mondaymonitor> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Enrico Santarelli | Membro |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 21/10/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

Contextualização 3

Desenvolvimento 3

Initial access was established using a downloaded file. What is the file name saved on the host. 3

What is the full command run to create a scheduled task? 4

What is the scheduled task meant to run 4

What was encoded? 5

What password was set for the new user account? 5

What is the name of the .exe that was used to dump credentials? 6

Data was exfiltrated from the host. What was the flag that was part

of the data? 6

Conclusão 7

Referências 7

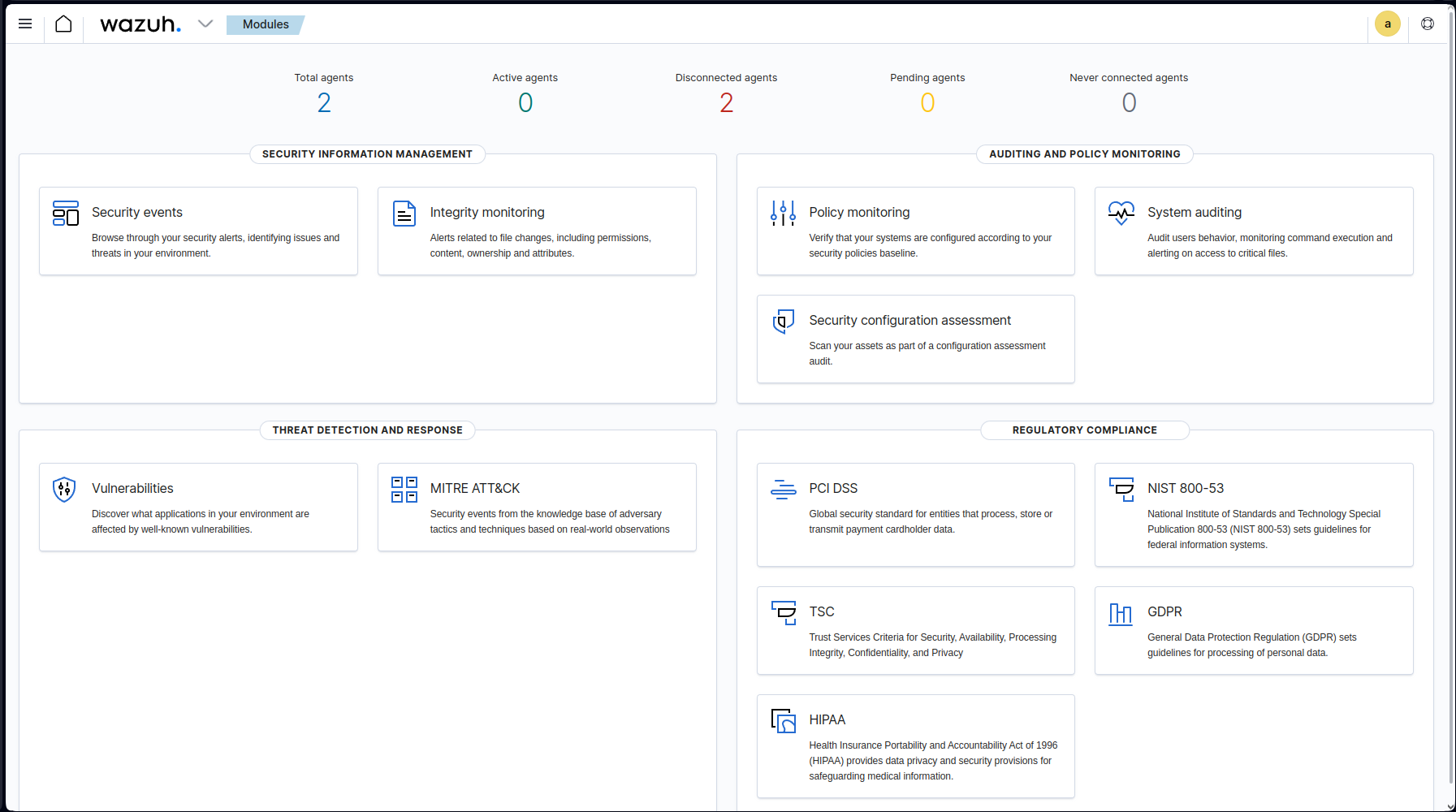
**Contextualização**

O CTF compões a trilha de SOC Level 1. A ideia da sala é treinar as habilidades de análise de eventos utilizando a ferramenta Wazuh.

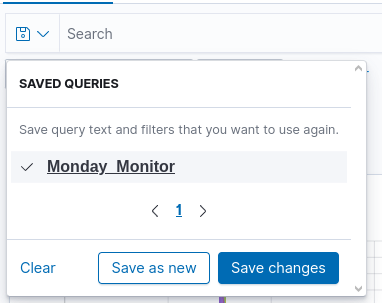
**Desenvolvimento**

**Initial access was established using downloaded file. What is the file name saved on the host?**

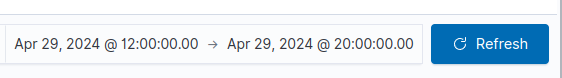
Primeiramente, vamos iniciar a ferramenta Wazuh para análisar os eventos.

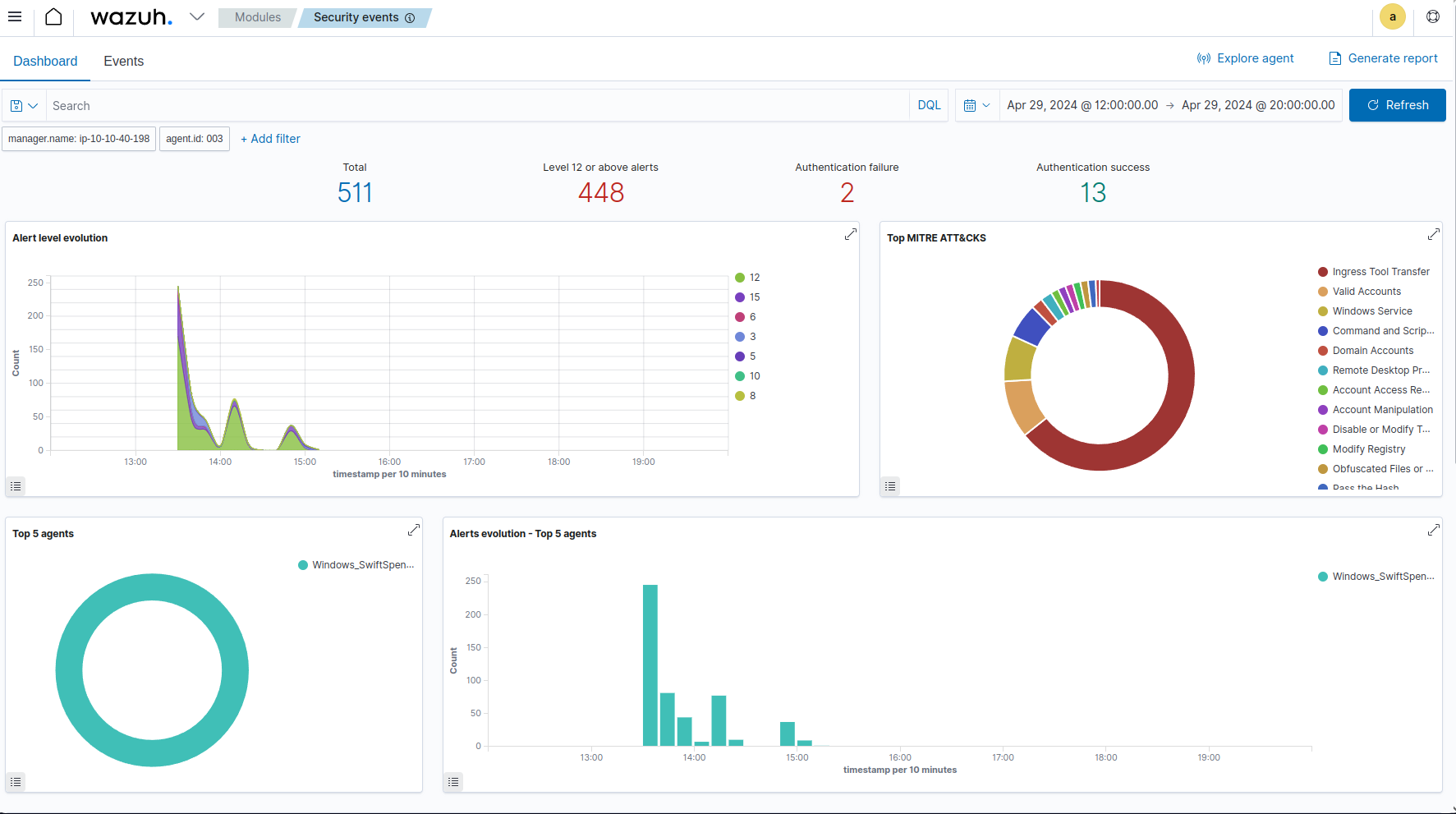


Em seguida, devemos entrar na aba de Security Events e usar a query disponibilizada pela sala: "Monday Monitor".

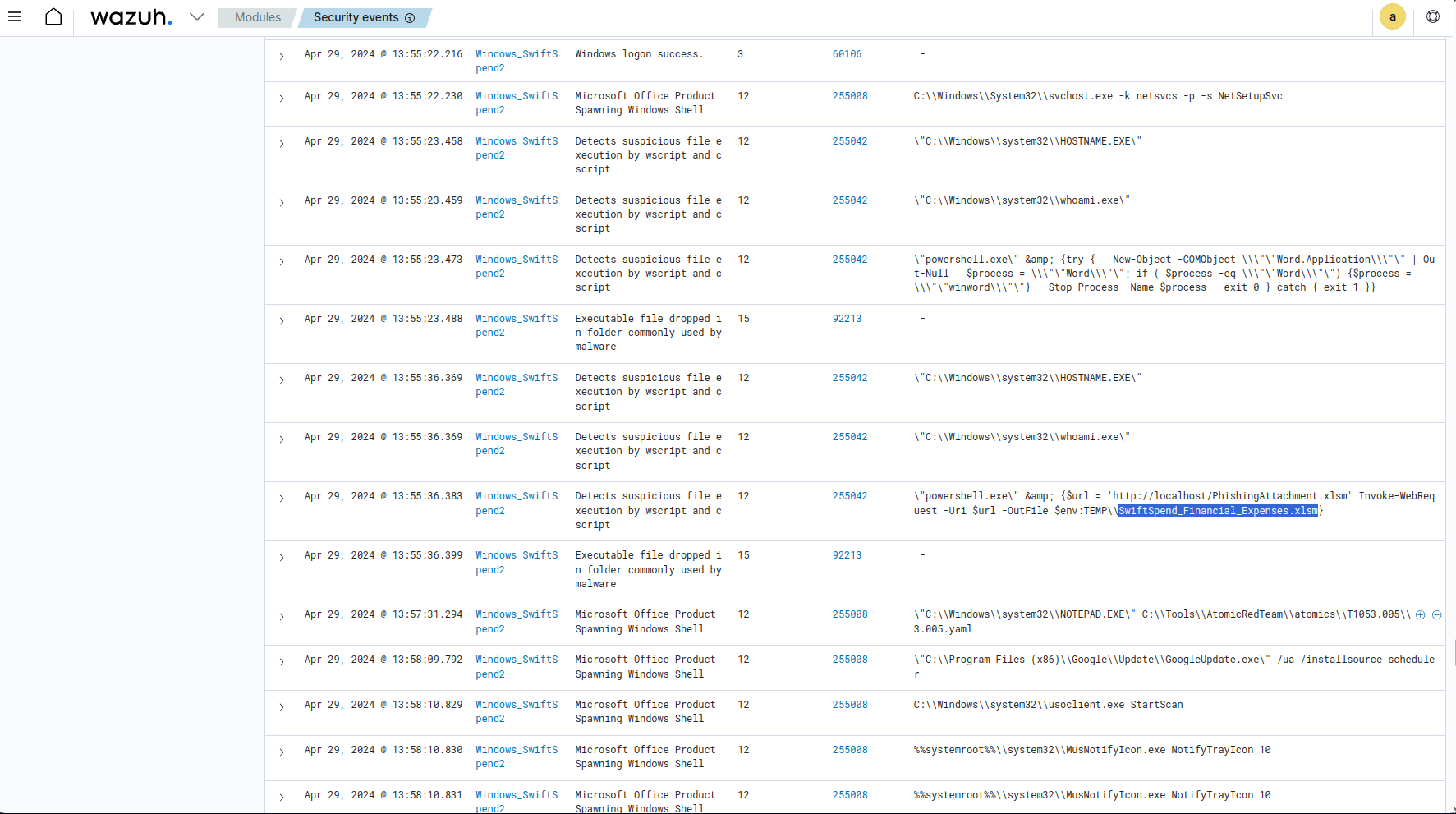


Para completar a configuração da análise, devemos adotar o intervalo de tempos dos testes.



  
Agora, vamos acessar a aba "Events" para ver os eventos um por um, colocar os comandos CLI como coluna da tabela de eventos e ordenar em ordem cronológica.

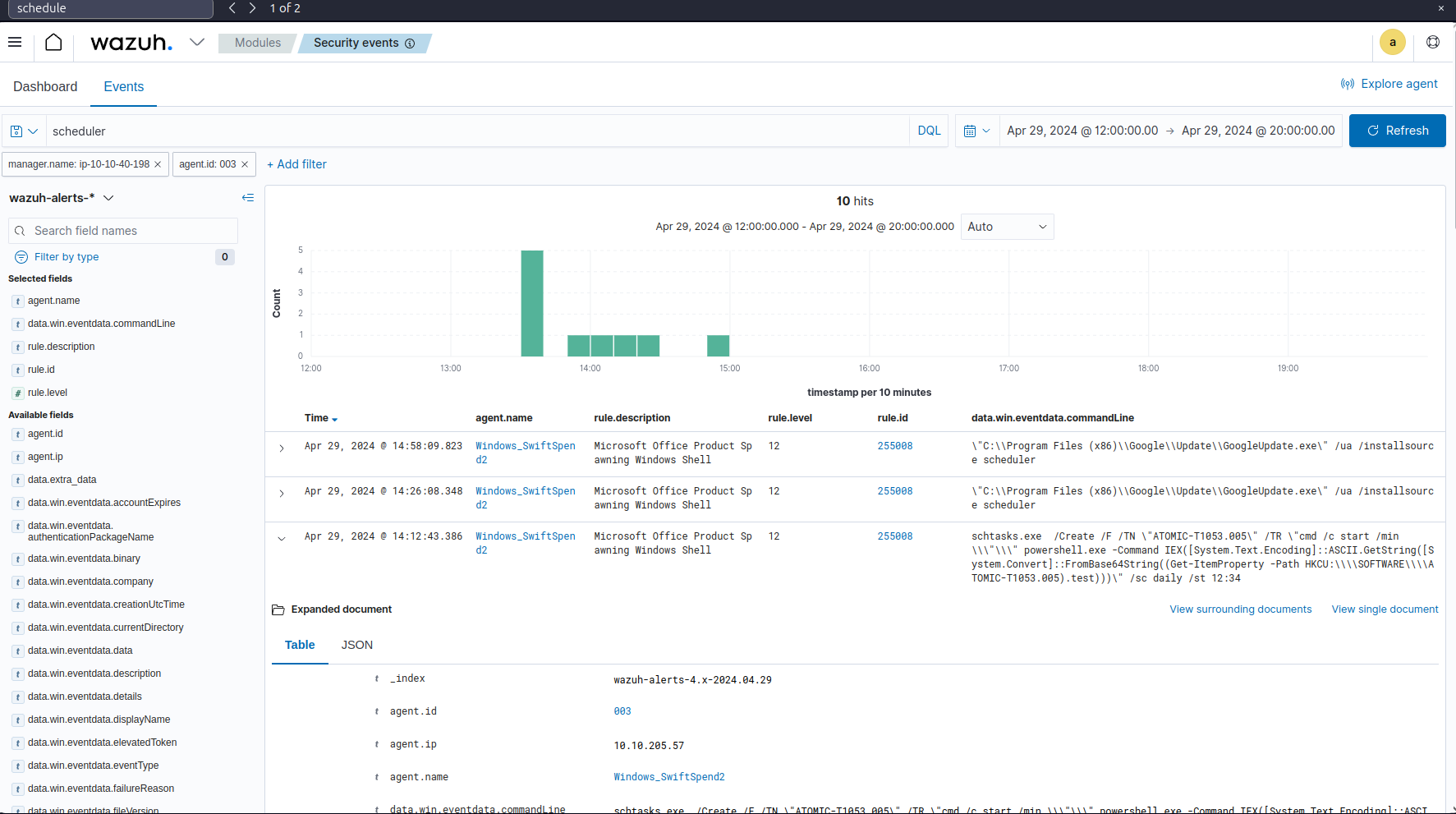
Dessa forma, encontramos um download de um arquivo suspeito.



R: SwiftSpend\_Financial\_Expenses.xlsm.

**What is the full command run to create a schedule task?**

Dentro do Windows as tarefas agendadas são agendadas por um scheduler. Portanto, vamos filtrar os eventos pela string "scheduler".

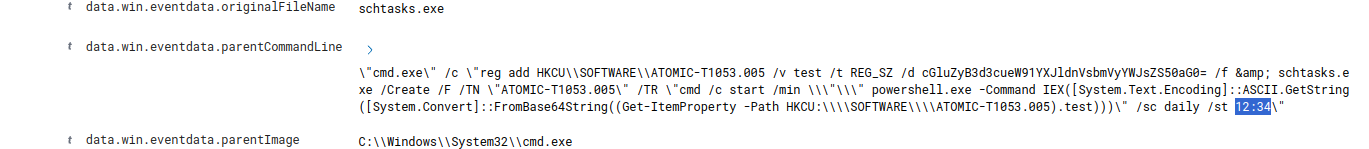


Um dos eventos filtrados foi criado pelo executável de agendamento: schtasks.exe. O comando utilizado está na propriedade data.win.eventdata.commandLine.

R: \"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\".

**What time is the scheduled task meant to run?**

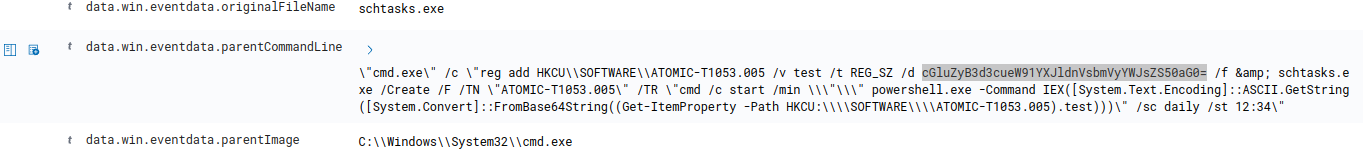
O tempo de execução da tarefa agendada está marcado no próprio comando de agendamento encontrado.

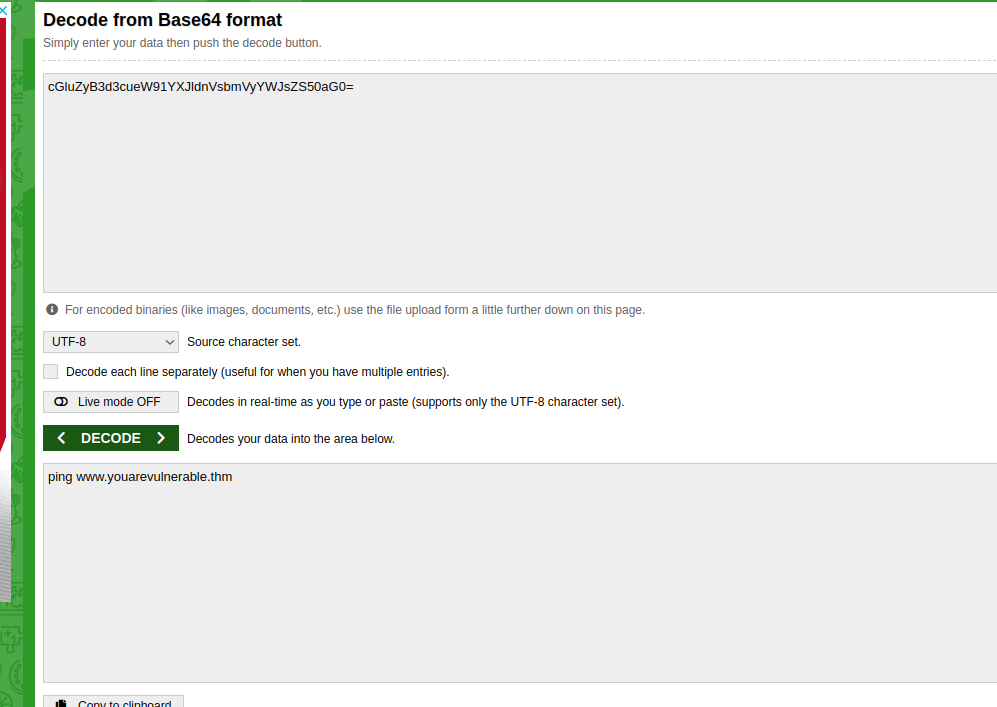


R: 12:34.

**What was encoded?**

Dentro do comando há uma string em base64.

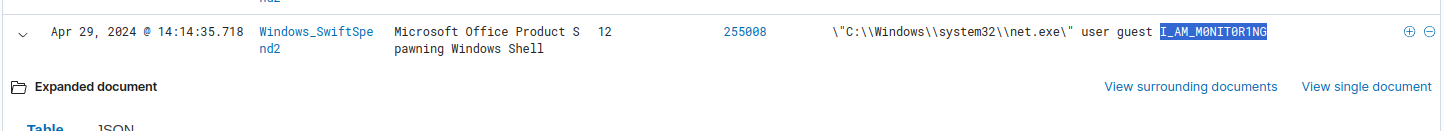
  
Utilizando o website base64decode, podemos encontrar o que foi codificado. Ref: [https://www.base64decode.org.](https://www.base64decode.org/)



R: ping [www.youarevulnerable.thm](http://www.youarevulnerable.thm).

**What password was set for the new user account?**

Procurando pelos eventos, se encontra um comando utilizado sobre o usuário "guest" com uma possível senha atribuída.



R: I\_AM\_M0NIT0R1NG.

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

Mais acima, nós encontramos um executável fazendo um dump sobre o usuário john.sterling, que é aquele que buscamos.



R: memotech.exe.

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

Buscando nos eventos, podemos encontrar um deles com a flag procurada no meio do comando utilizado.



R: THM{M0N1T0R\_1$\_1N\_3FF3CT}.

**Conclusão**

Este CTF oferece uma experiência prática de nível fácil, ideal para iniciantes na área de Blue Team que desejam colocar em prática os aprendizados das salas teóricas de Wazuh.

**Referências**

* [https://www.base64decode.org](https://www.base64decode.org/)