|  |
| --- |
| Cyber Defenders |
| Elastic-Case |
| Threat Hunting |

|  |
| --- |
| Abdallah Chbaro  10/04/2023 |

Table des matières

# Scenario

An attacker was able to trick an employee into downloading a suspicious file and running it. The attacker compromised the system, along with that, The Security Team did not update most systems. The attacker was able to pivot to another system and compromise the company. As a SOC analyst, you are assigned to investigate the incident using Elastic as a SIEM tool and help the team to kick out the attacker.

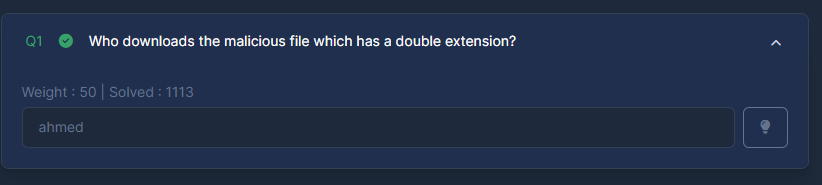
# WriteUp

As a SOC analyst, the first step I would do is to understand the context. We can start first by looking into the following, instead of starting answering the questions:

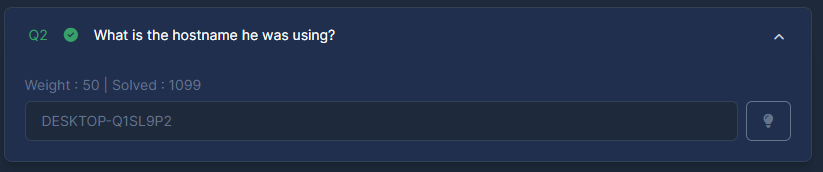
1. HostNames
2. UserNames
3. IP addresses

## Question 1

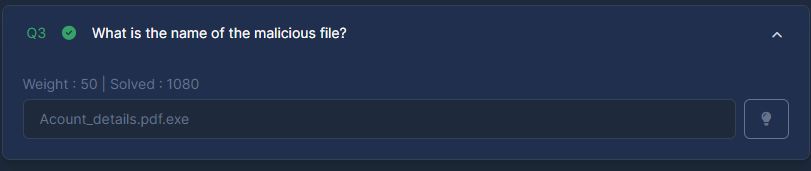
In the first question, they are specifying that the attacker tricked the user into downloading a malicious file. Hence, it is remote execution. We can search for Event ID 4104, which refers to the execution of a remote PowerShell command.



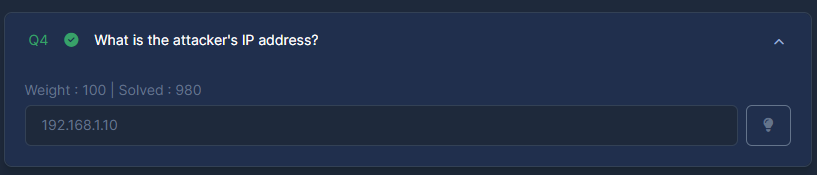
## Question 2



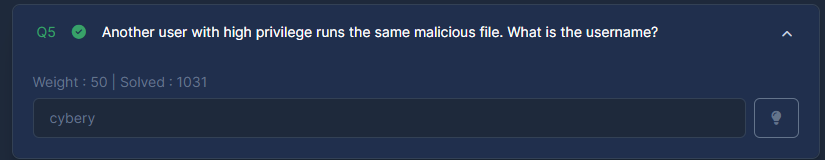
## Question 3



## Question 4

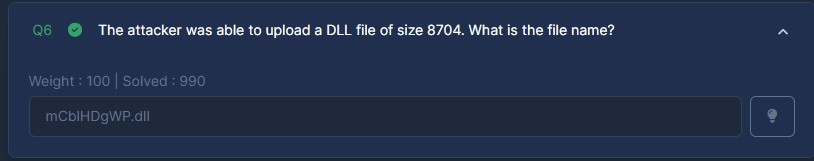


## Question 5



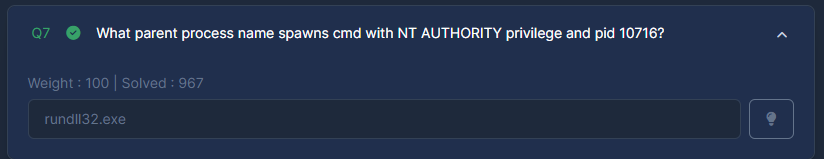
## Question 6

We can search for file size equals 8704:

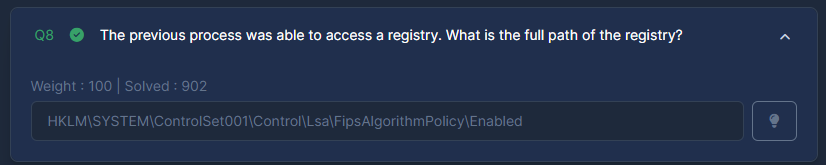


## Question 7

We can search for PID equals 10716:

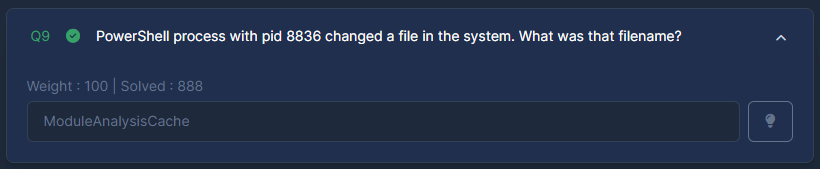


## Question 8



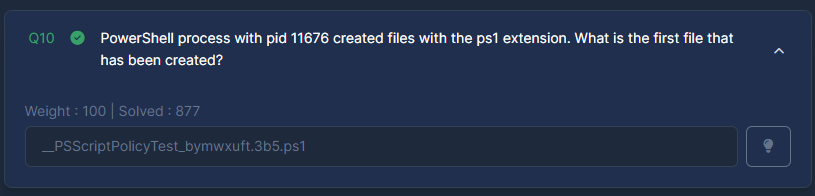
## Question 9

We can search for process.name equals powershell.exe and PID equals 8836:



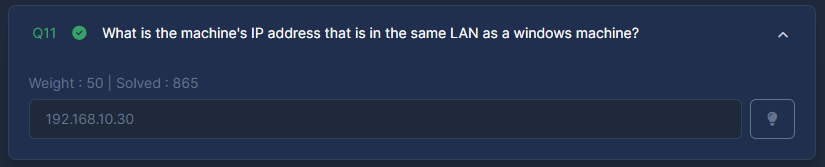
## Question 10

We can search for process.name equals powershell.exe and PID equals 11676 and ps1:



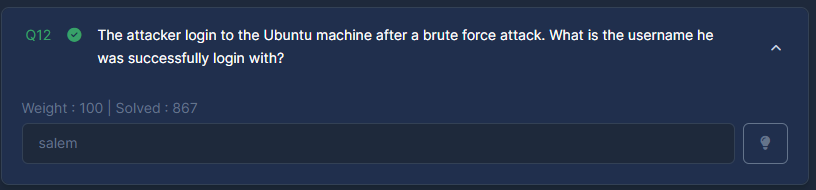
## Question 11

We can search for host.ip: 192.168.10.0/24 and NOT host.ip: 192.168.10.10:



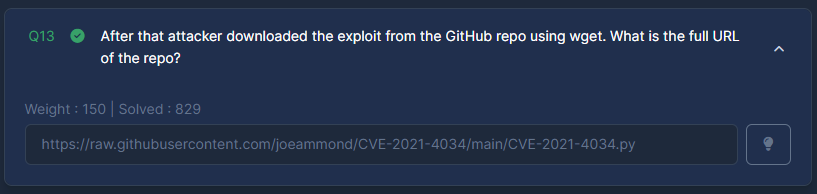
## Question 12

We can search for: system.auth.ssh.event: “Accepted”:



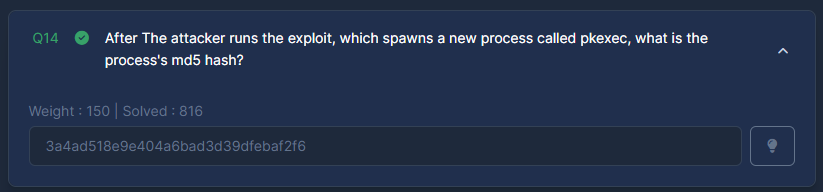
## Question 13

We can search for Wget:



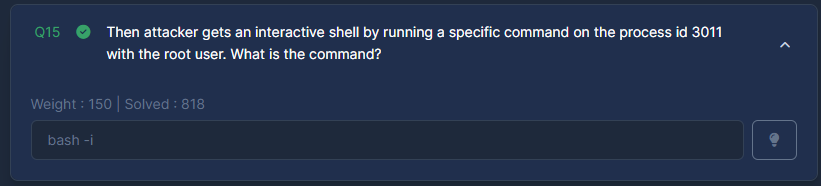
## Question 14

We can search for process.name equals pkexec:



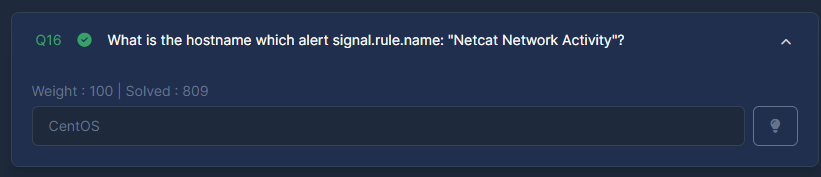
## Question 15

From the previous question, we find bash -i:



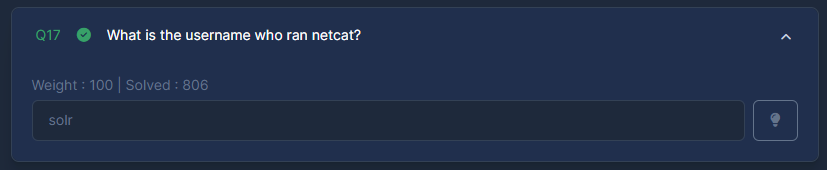
## Question 16

We can search for Netcat Network Activity:



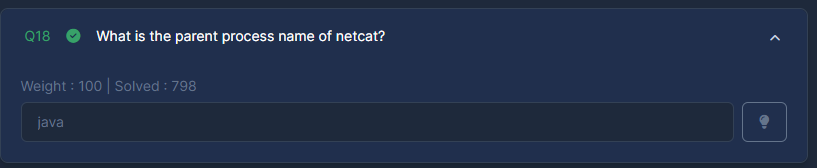
## Question 17

We can search for nc:



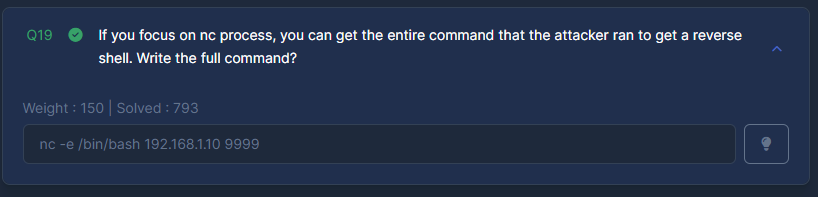
## Question 18

We can see the parent process name in the same log:



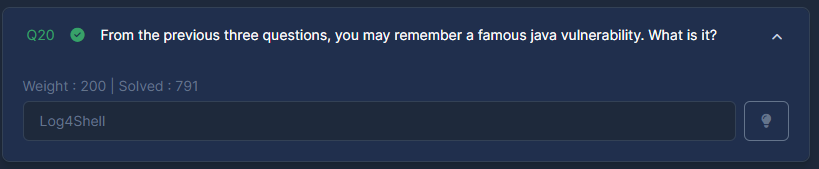
## Question 19

We can find the command in the same log:



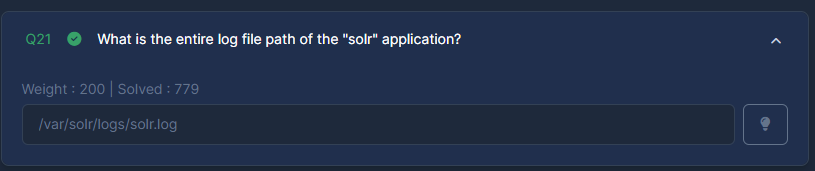
## Question 20

Some research will reveal it is Log4Shell:

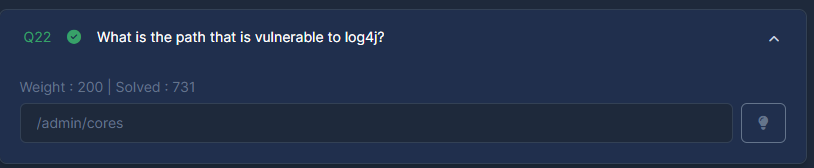


## Question 21

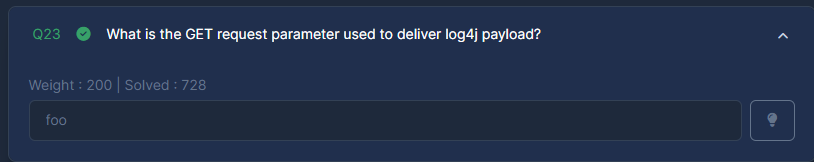
We can search for solr and log:



## Question 22



## Question 23



## Question 24

