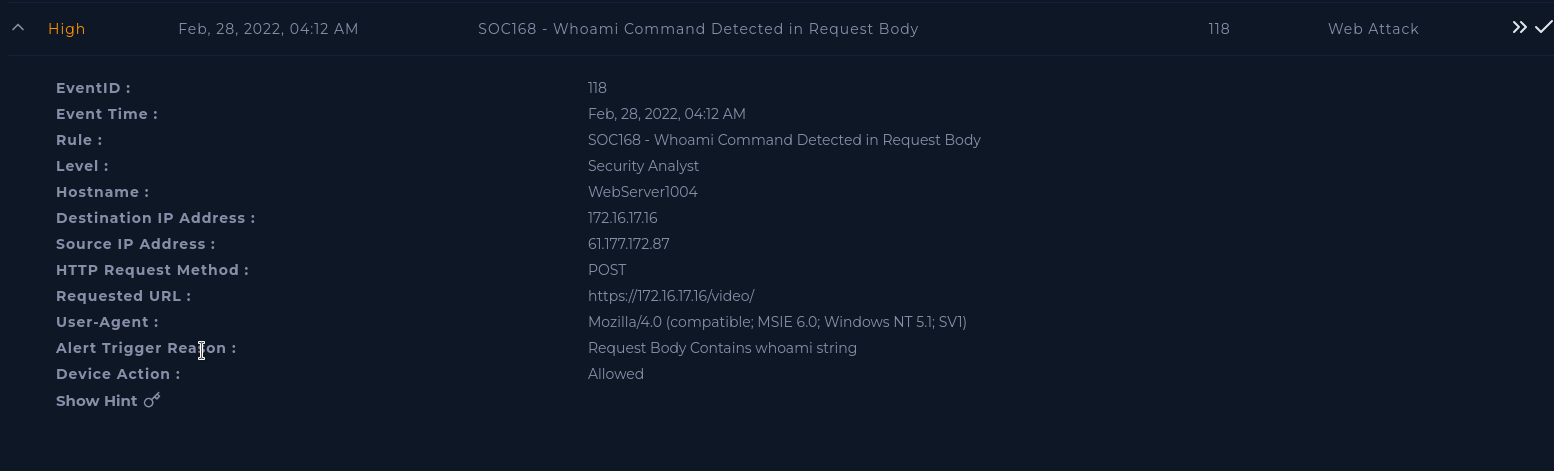
I’m going to be creating a case for LetsDefend’s “SOC168 - Whoami Command Detected in Request Body” alert.



First it is a good practice to summarize information received from the alert.

When did the event occur?

The event occurred at 4:12 AM on February 28, 2022.

What is the source ip?

61.172.172.87

Checking the IP in virus total showed no malicious results, and that it was an IP from a Data Communication Division in China.

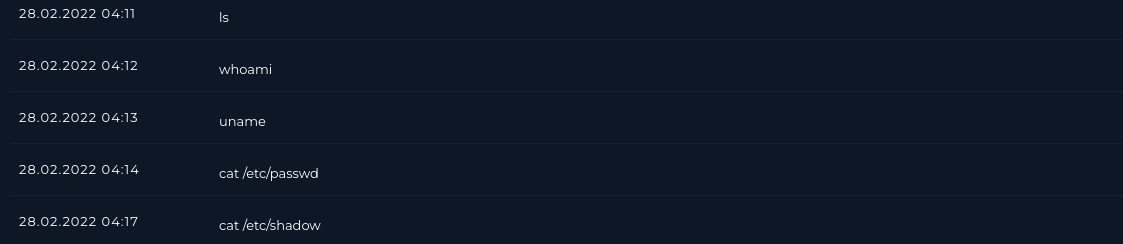
Who was the target?

WebServer1004 IP 172.16.17.16

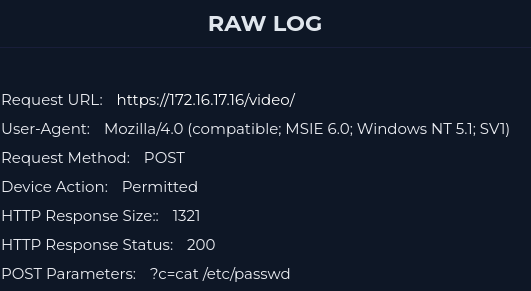
Why did the alert occur?

The request body contains a whoami string.

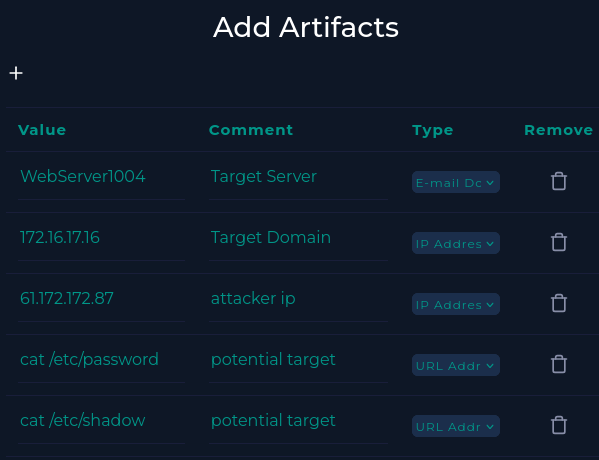
First, going to the Endpoint Security of WebServer1004 I can find the recorded logs during the event. Looking into this terminal is concerning. We can see multiple terminal commands that could be used in copying or editing a password list.



To see more information, I am going to look into Log Management to find the Raw Data of each log. Unfortunately, these raw data logs seem like they are pointing towards a successful attack. Each log has a successful 200 response status and a large response size. Next I look through the email log to see if this was a planned or practice attack, but find no emails employing this was planned.



Artifacts:



Analysis Notes:  
After investigation it is safe to conclude that this alert is a true positive, and should be escalated for further investigation. It is possible that the password file or shadow file were compromised. I have contained the affected WebServer1004 for further investigation.