A command injection attack occurs when data received from the user is not properly sanitized and passed to the system shell.

In this example lab, I investigate a Command Injection Attack. As seen below, within the logs there are various commands that are showing the target's file structure like ls or dir. The attack occurred at 9:03 AM on March 1st 2022. The attacker’s IP is 192.168.31.156. The attack is likely successful from the request 200 OK response status code.

