# Cloud goat, glue_privesc

Glue_privesc

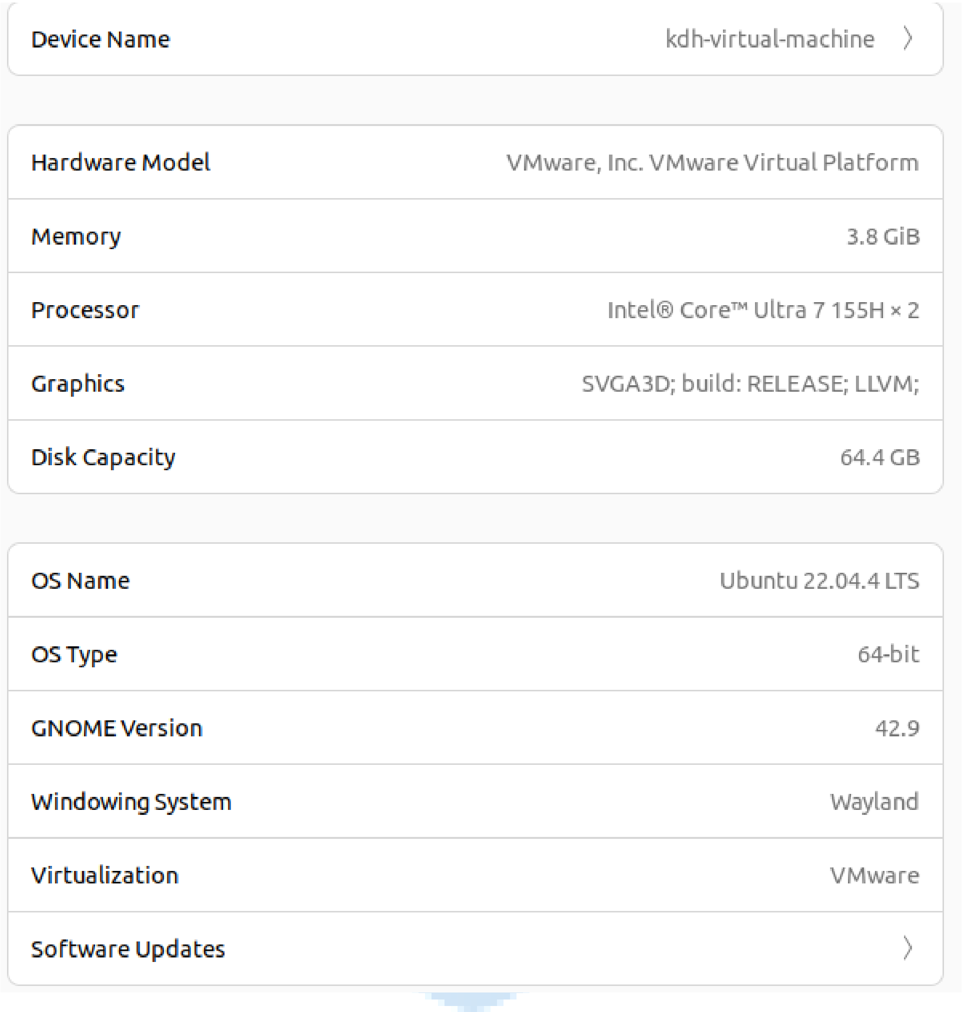
| | |
|---|---|
| 담당 멘토님 | 니코 멘토님 |
| 제출일 | 2024.xx.xx (월) |
| 트랙 | 디지털 포렌식(df)트랙 |
| 성명 | 김동한(kimdonghan) |

# 목차

# 1. Setting the environment

## 1.1. Setting

I set up the Ubuntu 22.04 version and finished reviewing the progress again until cloudgoat, aws setting IAM access key profile setting that I did in class.
The results completed are as follows.



| | |
|---|---|
| Device Name | kdh-virtual-machine 〉 |
| Hardware Model | VMware, Inc. VMware Virtual Platform |
| Memory | 3.8 GiB |
| Processor | Intel® Core™ Ultra 7 155H × 2 |
| Graphics | SVGA3D; build: RELEASE; LLVM; |
| Disk Capacity | 64.4 GB |
| OS Name | Ubuntu 22.04.4 LTS |
| OS Type | 64-bit |
| GNOME Version | 42.9 |
| Windowing System | Wayland |
| Virtualization | VMware |
| Software Updates | 〉 |

## 1.2. Understanding Scenario

## 1.3. Glue_privesc

The goal of this scenario is to find a secret string stored in the ssm parameter repository. As a result, we find that flag needs to be found.
The implemented environmental schematic diagram is provided and kindly informs you how the key was stored in the location.
In addition, it also tells you how to navigate the route.
1. An attacker may steal the Glue administrator's access key and secret key via SQL injection attack

on a web page.

2. Identifies vulnerable privileges. These privileges allow an attacker to discover the ability to create and execute tasks that can perform reverse shell attacks, simultaneously obtaining the desired role.

3. List the roles you want to use IAM:passrole, write a reverse-scented shell code, and insert .py into S3 through the web page.

4. To gain SSM access, you must create a Glue service job through the AWS CLI, which also runs the reverse shell code.

5. Runs the created job.

6. Extracting flag values from the ssm parameter repository ends.

I was also able to see more detailed path sheets, i.e., I could see what I could do just by following the command.

Since it's generated on AWS, I thought the money would continue to go out, so I tried to understand the scenario first. Next time, we're going to start the practice right away.