**Examining Live Threats in GuardDuty**

### Introduction

The EC2 instances in the Cloud Academy Lab environment have been communicating with each other since you enabled GuardDuty. Usually, some or all of the findings related to the instances communicating appear within 10 minutes. If not all of the findings are present, you can continue through the lab step to understand all of the findings that would eventually appear. The way the two instances communicate with each other is as follows:

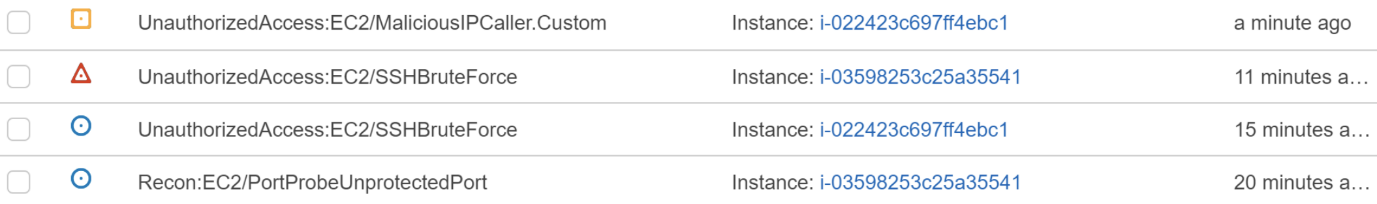
* The App Server instance simply makes HTTP requests to the Malicious Instance every 15 seconds.
* The Malicious Instance sends SSH connection attempts to the App Server instance every 4 seconds. The connection request does not include an SSH key causing the request to always be refused.

The signatures of each of these communication types are recognized by GuardDuty as threats. You will investigate the findings in this lab step.

### Instructions

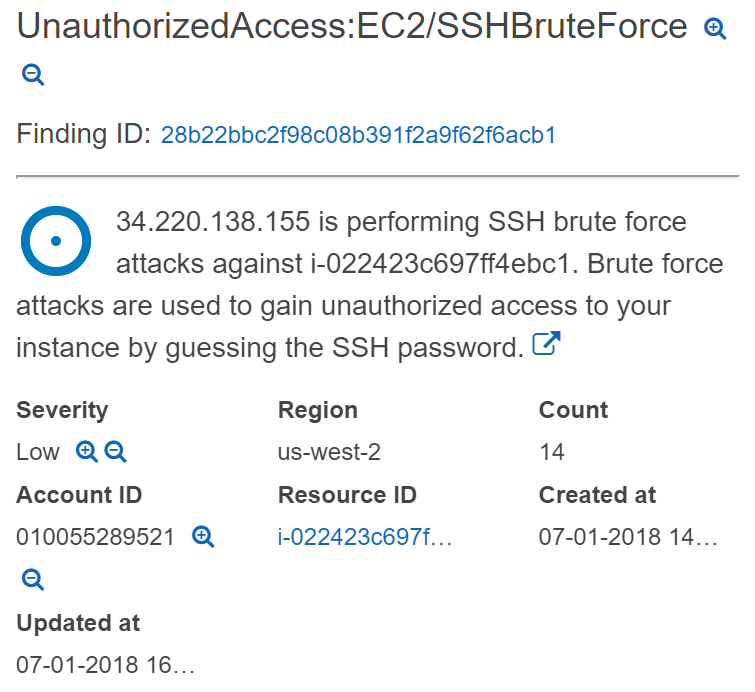
1. Click on **Findings** in the GuardDuty Console's sidebar.

Depending on how quickly you arrived at this lab step, you may see some or all of the following **Finding type** rows:



You can identify the real threats because they do not begin with **[SAMPLE]**. The first three findings in the table above are controlled by the Lab, and will eventually appear if you do not see them. The **Recon** finding is not controlled by the Lab, although, ports are intentionally left open to allow them to happen. An actual (low severity) threat from an external actor must take place for the finding to appear. This finding may not appear but commonly appeared during Lab development. To save time, you do not have to wait for all of them to continue.

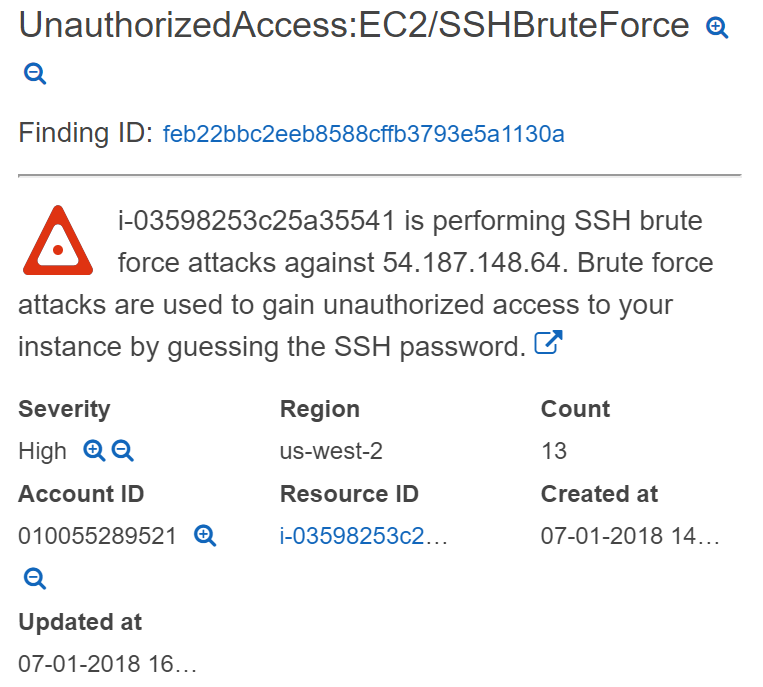
2. Click on the **UnauthorizedAccess:EC2/SSHBruteForce** finding with a blue circle (low severity):



The **EC2/SSHBruteForce** finding indicates an instance was involved in a brute force attack aimed at retrieving passwords or access keys. In the above image, you can see the description states that one of your instances (App Server) is the target of an attack from an IP address (the Public IP of the Malicious Instance). The finding is classified as **Low** severity meaning that it does not require immediate attention, but is something to address in the future, perhaps by blocking traffic from that IP in your VPC and only allowing SSH access through keys. You can see **Location** of the attacker's IP address in the **Actor**section of the finding details. Recall that the Malicious Instance is merely attempting to connect to the instance, but does not include a key so the attempt fails. The instance is not trying different passwords/keys, but the activity has the same signature as a brute force attack, namely, repeated attempts to make SSH connections in a short period of time.

Note: SSH findings are only reported if SSH is configured on the default port of 22.

3. Click on the **UnauthorizedAccess:EC2/SSHBruteForce** finding with a red triangle (high severity):



This finding is prompted by the same activity as the previous finding. However, this finding is identifying one of your instances (Malicious Instance) as an attacker, whereas the low severity finding was identifying one of your instances as a victim. This finding receives a high severity rating because it is likely that the instance has been compromised and is performing unauthorized activities. Immediate action is recommended. For example, terminating the instance or isolating it from external access to perform forensic analysis on the instance to discover the root cause.

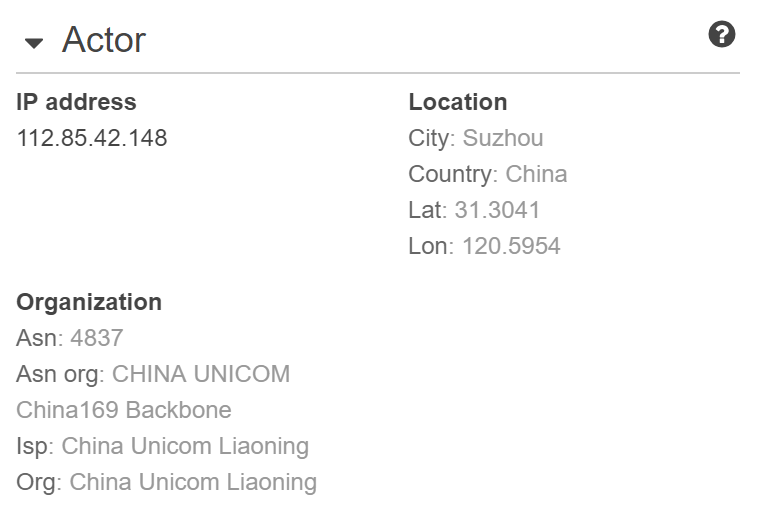
4. Click on the **UnauthorizedAccess:EC2/MaliciousIPCaller.Custom** finding with a yellow square (medium severity):



This finding indicates outbound TCP communication with an IP address in one of your GuardDuty threat lists. The **Threat list name** field tells you which list. The medium severity rating is used because it is recommended that you investigate the affected instance at your earliest convenience.

5. Click on the **Recon:EC2/PortProbeUnprotectedPort** with a blue circle (low severity).

This finding notifies you that an open port on one of your instances has been probed by known scanners on the internet. The finding is low risk, but you are advised to restrict access to known instances by configuring security groups, access control lists, or host firewalls. The **Actor**section tells you where the probe originated:



### Summary

In this lab step, you examined real EC2 threat findings for the Lab environment. You understood the signatures for each finding and actions that can be taken to remedy each.

It is worth noting that GuardDuty findings are event sources in CloudWatch Events. By using CloudWatch Events, it is possible to automatically react to GuardDuty findings.