

**Project Name :**

**O**bserving Live RDP Brute Force Attacks from Around the World with Azure Sentinel and a Custom PowerShell Script.

**Team Members :**

* **N**ishant Choutele
* **S**hrikant Meher

**INDEX**

|  |  |
| --- | --- |
| 1 | Introduction­­­­ |
| 2 | Create Virtual Machine |
| 3 | Allow all in Firewall |
| 4 | Create Log Analytics Workspace |
| 5 | Enable gathering VM logs in Security Center |
| 6 | Connect Log Analytics to VM |
| 7 | Setup Azure Sentinel |
| 8 | Turn of Windows Firewall on VM |
| 9 | Download PowerShell Script |
| 10 | Get Geolocation.io API Key |
| 11 | Run Script To get Geo Data from attackers |
| 12 | Create custom log in LAW to bring in our custom log |

Azure Sentinel is a cloud-native security information and event management (SIEM) solution that helps organizations detect, investigate, and respond to security threats. It provides a unified view of security data from across your organization, including your on-premises and cloud environments.

In this topic, we will set up Azure Sentinel and connect it to a live virtual machine acting as a honey pot. We will then use a custom PowerShell script to look up the attackers' geolocation information. This will allow us to observe live RDP brute force attacks from all around the world and track the location of the attackers.

This topic is relevant to security professionals who want to learn how to use Azure Sentinel to detect and investigate RDP brute force attacks. It is also relevant to anyone who is interested in learning more about how to use PowerShell to gather geolocation information.

Benefits of using Azure Sentinel to detect and investigate RDP brute force attacks:

Azure Sentinel provides a unified view of security data from across your organization, including your on-premises and cloud environments. This makes it easier to detect and investigate security threats.

Azure Sentinel uses machine learning to identify patterns and anomalies in your security data. This can help you to detect threats that you would not be able to detect manually.

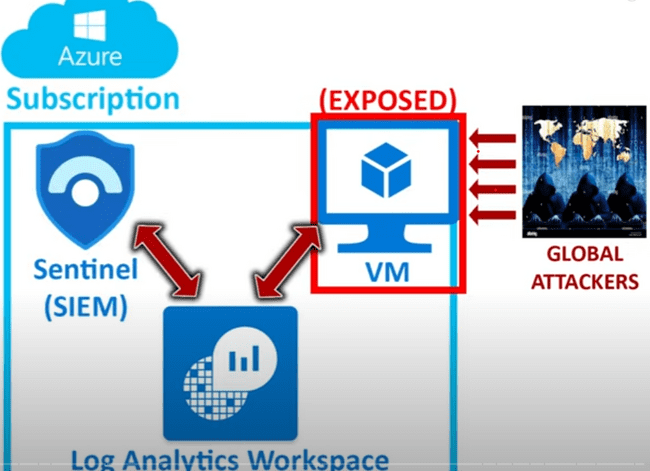
Azure Sentinel provides a variety of tools to help you investigate security threats. These tools include incident response tools, threat hunting tools, and forensics tools.

Benefits of using a custom PowerShell script to look up attackers' geolocation information:

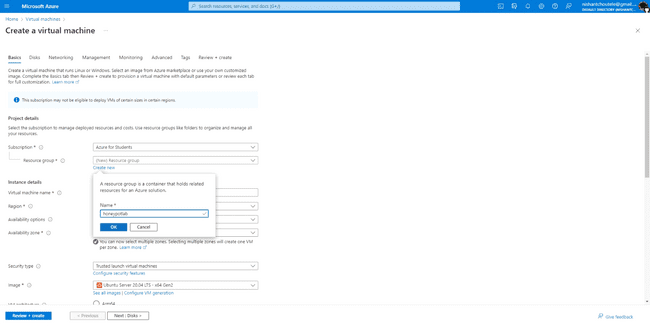
PowerShell is a powerful scripting language that can be used to automate a variety of tasks.

The custom PowerShell script that we will be using in this topic is very efficient and can quickly look up the geolocation information of a large number of IP addresses.

The custom PowerShell script is also very flexible and can be modified to meet your specific needs.



1. Creating a virtual machine

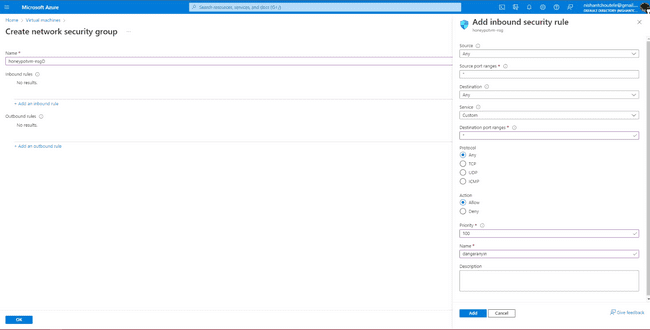


Resource group honeypot lab and vm name honey pot

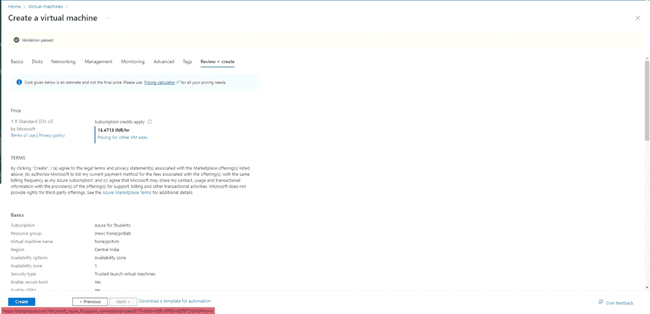


2. Allow all in firewall

create a new network security group by giving destination port a \* and setting priority to 100 so that security goes to its minimal stage



Review and create



3.Create a log analytics workspace

A Log Analytics workspace is a unique environment in Azure Monitor for storing and analyzing log data from Azure Monitor and other Azure services, such as Microsoft Sentinel and Microsoft Defender for Cloud. Each workspace has its own data repository and configuration, but it might combine data from multiple services.

Log Analytics workspaces are used to collect, store, and analyze log data to identify trends, patterns, and insights. Log Analytics workspaces can also be used to create alerts and notifications to help you quickly identify and respond to security threats.

Log Analytics workspaces are a powerful tool for monitoring and managing your Azure resources. They can help you to identify and troubleshoot problems, improve performance, and secure your environment.

Benefits of using a Log Analytics workspace:

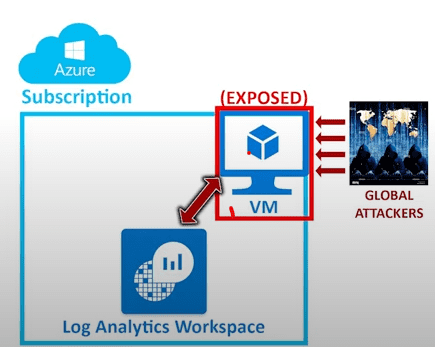
Centralized logging: Log Analytics workspaces provide a centralized location to store and analyze log data from all of your Azure resources. This makes it easier to identify trends and patterns in your data.

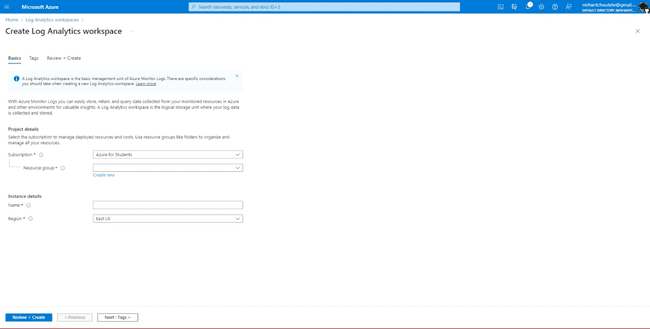
Advanced analytics: Log Analytics workspaces support advanced analytics capabilities, such as machine learning and artificial intelligence. This can help you to identify threats and problems that you would not be able to detect manually.

Alerting and notifications: Log Analytics workspaces can be used to create alerts and notifications to help you quickly identify and respond to security threats.

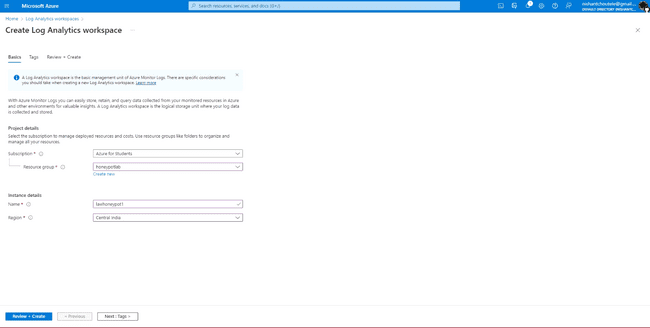
Compliance: Log Analytics workspaces can help you to comply with industry and regulatory requirements, such as PCI DSS and HIPAA.

If you are using Azure resources, I recommend that you create a Log Analytics workspace to collect and analyze your log data. Log Analytics workspaces are a powerful tool for monitoring and managing your Azure environment.



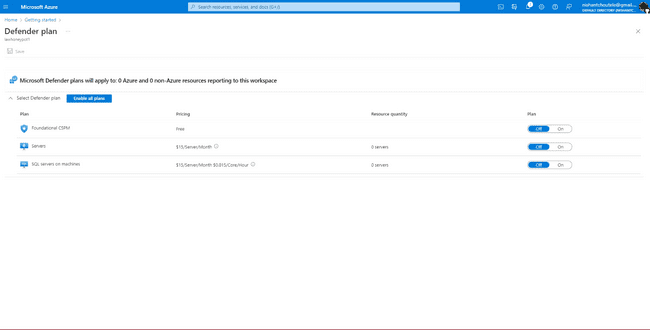


Use the same resource group and create

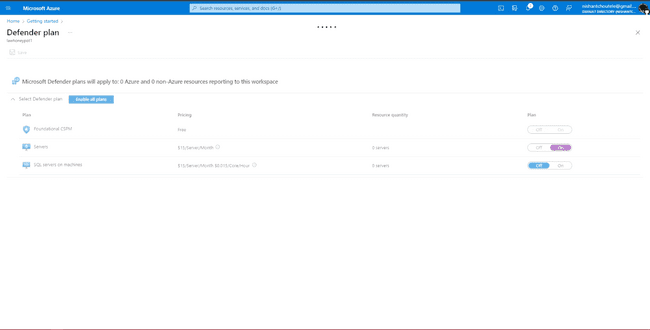


4.Enable gathering VM logs in Security Center

After creating go to Azure security center > pricing and settings> choose the created log analytics

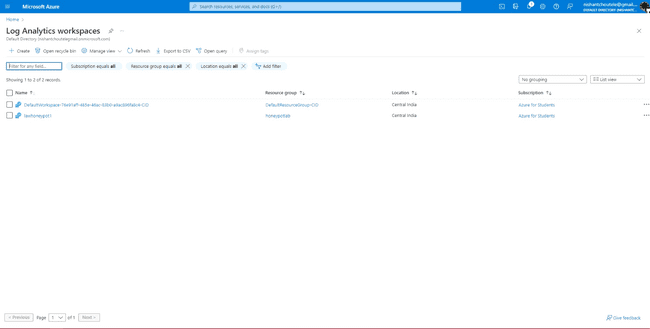


Set servers on and SQL servers off

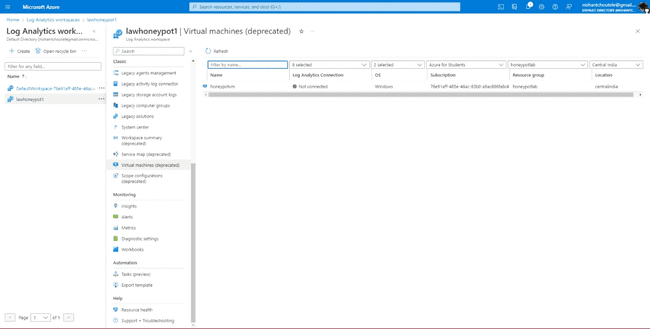


5.Connect Log Analytics to VM

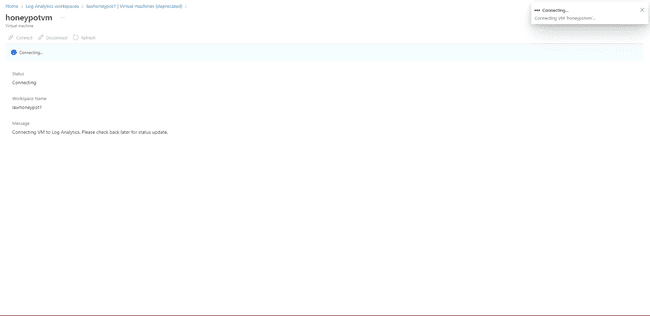
Now go to log analytics workspace and connect the VM



click on the virtual machine



Connect



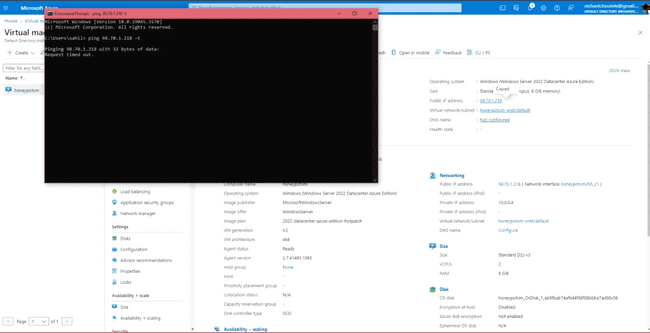
6.Setup Azure Sentinel

create> select the workspace connected to virtual > select ADD

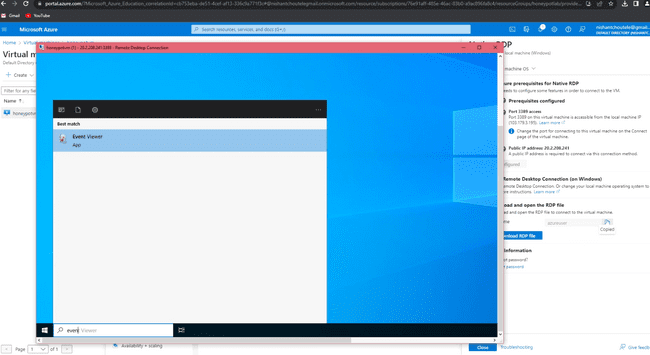


Before loggin in to virtual machine. Go to cmd and ping the public ip of the virtual machine

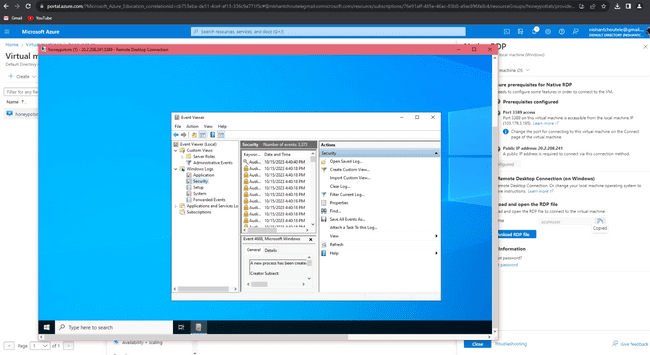
with the command ping 192.168.0.0 -t



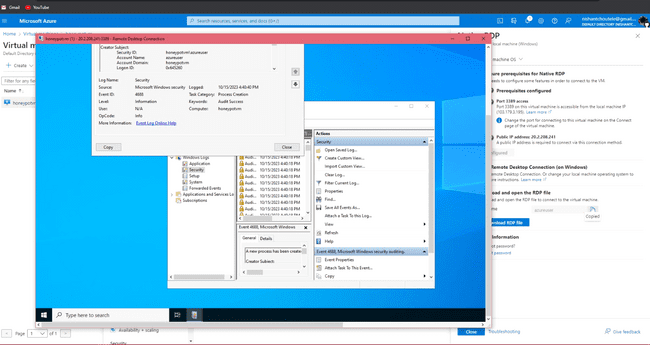
It will show request timeout. connect to the VM and go to Event Viewer



Go to Windows Logs> Security

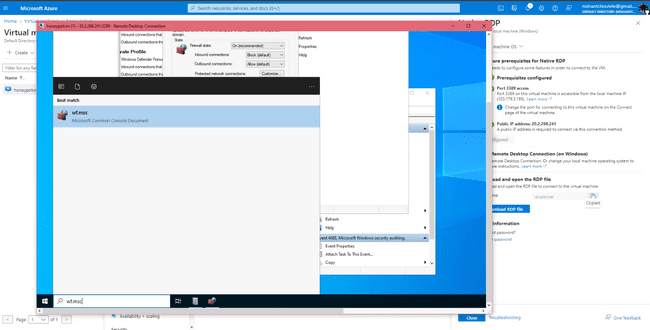


Click on the folders and check the login info of the user who logged in

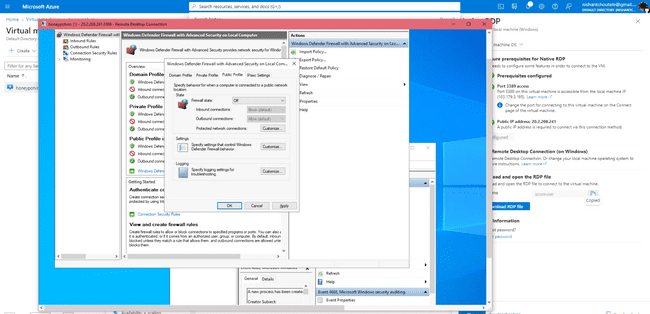


7. Turn of Windows Firewall on VM

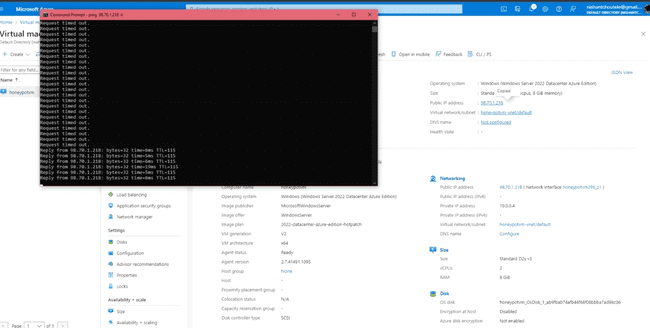
NOW go to wf.msc



Put Domain profile, private profile and private profile firewall status off so the attackers can see it

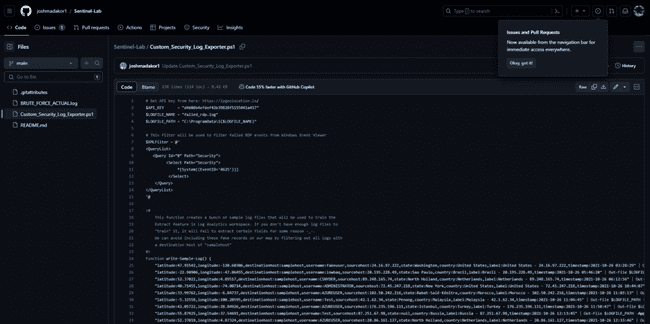


Now check the ping status in cmd

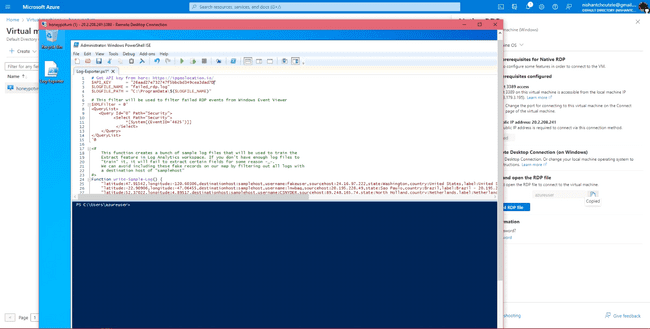


8.Download PowerShell Script

Now copy the script of custom security log

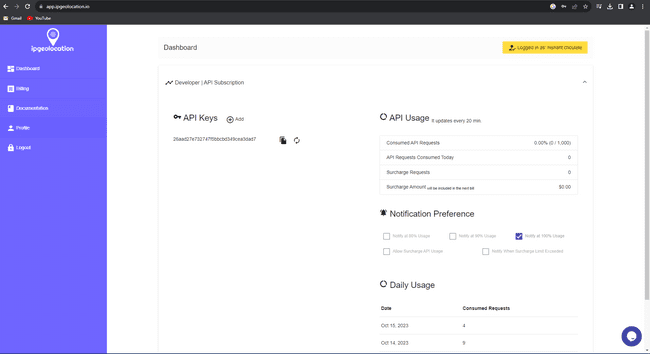


Paste it inside the Powershell.ISE and save it naming log exporter



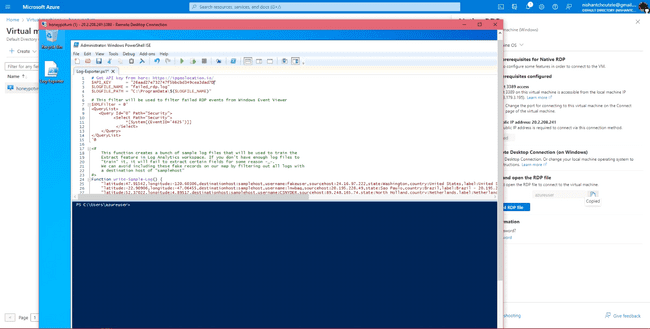
9.Get Geolocation.io API Key

now go to ipgeolocation for the API key without it we wont be getting the geodata and we wont be getting latitute, longitude etc.



copy the api key and paste it in the script and Run!

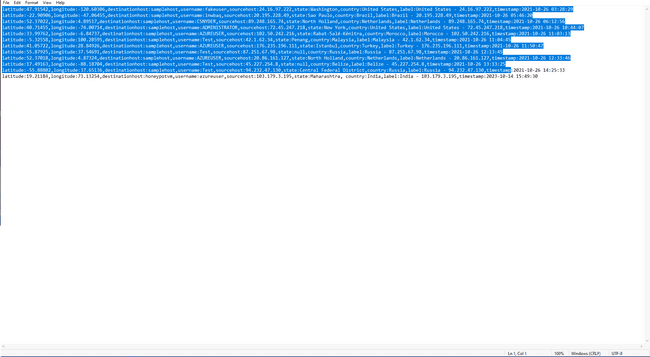
This script runs in a loop. It looks through the event log and all th security log grabs all the events of people who failed to login into the honeypot virtual machine grabs the ip address and gets the geo data through the api key.



After running a log file get created inside the given path which trains the log analytics workspace to provide the data in a format which get showed in powershell



This the sample data to train the logt analytics works space

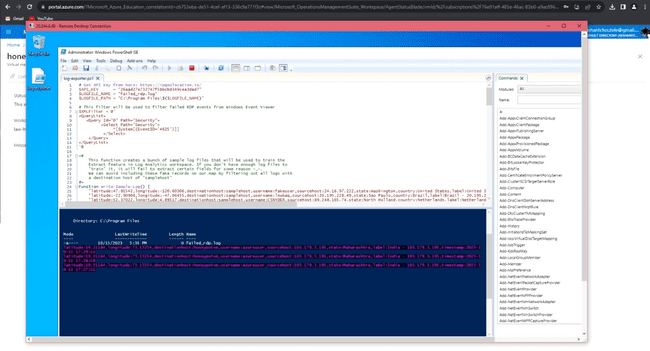


This is the data that is actual failed logon dummy attack we did

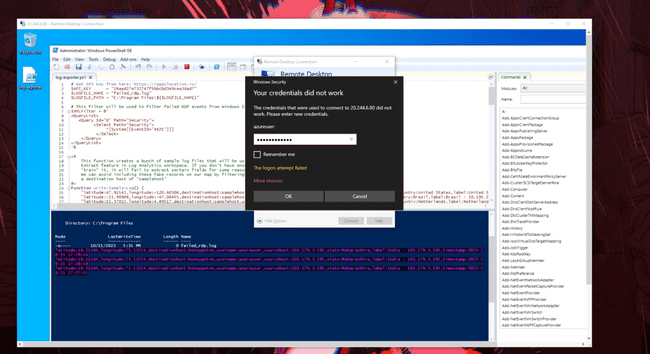


10.Run Script To get Geo Data from attackers

This is how the data looks in powershell after multiple dummy attacks.



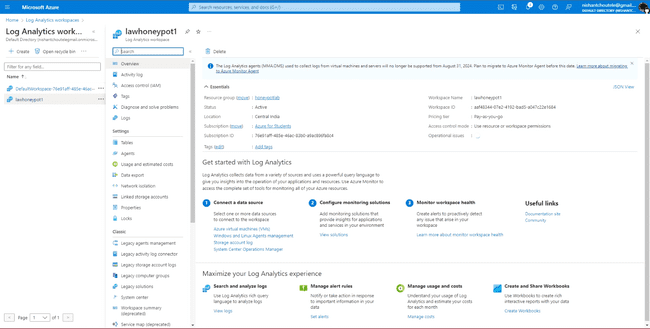
Logging into the virtual machine entering a wrong password aka dummy brutforce attack.



LOGIN gets failed and it shows the data with an exact time and location from when it was done.

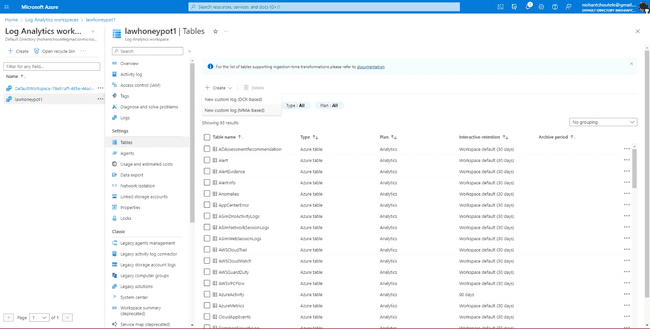


Now go to log analytics workspace> overview> tables

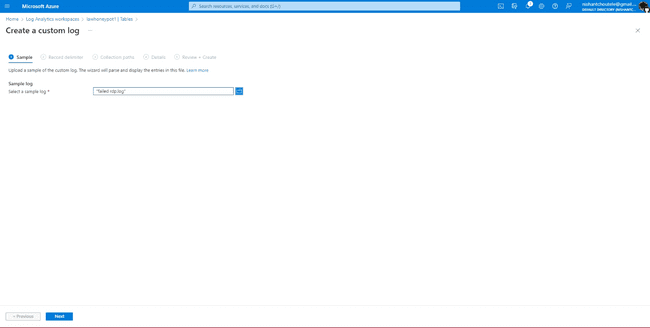


11.Create custom log in LAW to bring in our custom log

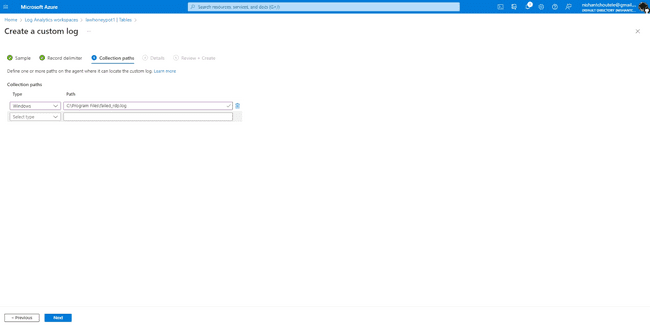
Create> new custom log MMA based.



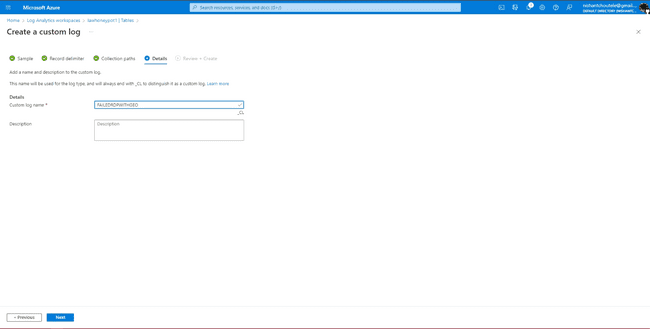
Give the path of the file which collects the geo data>next



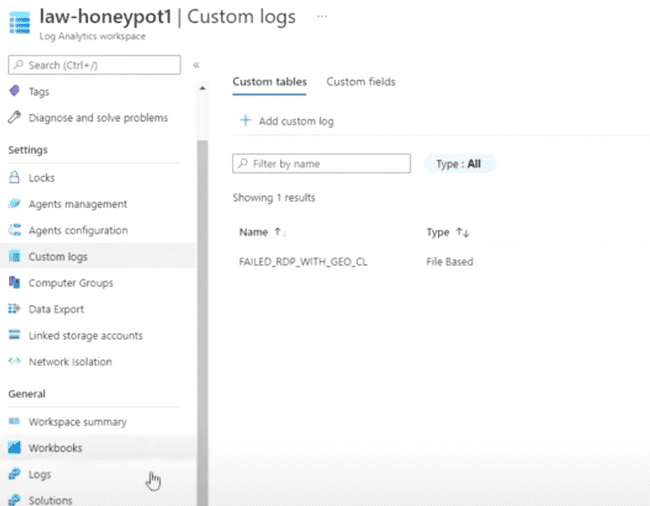
Copy the path of the failed RDP file and paste it



Give the custom log a name and create.



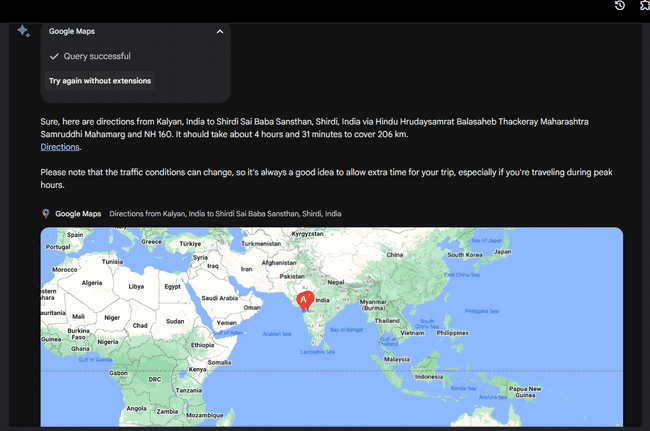
Go to the workbook it will show the log file named FAILED RDP WITH GEO CL (CL stands for custom logs)



Copy the file name and paste it in bard



Bard will take the file name as a query and show the live location of the attackers.



**Thank you!!!**