1. Creating a virtual machine on Azure, the vm created is going to be an exposed machine that is being attacked.
   1. Re-define the firewall rule in advanced network option, set destination port ranges to be all(\*), and allow any protocols.
2. Create new log analytics workspace
   1. Creating custom log that contains geographic information, discover where the hackers located at.
   2. Storing the logs and SIEM azure sentinel will connect to the workspace to display the geodata on the map.
3. Microsoft defender for cloud
   1. Management-> environment setting->log-anaglyhtics-workspace-honey-pot1
   2. Defender plan-> Turn on servers, turn off SQL servers, no need of that
   3. Data collection-> All events/ all raw events, logs and any security data are saved to previously created log analytics workspace
4. LAW, connect to vm
5. Sentinel setting up, add the law to sentinel
6. Using xfreerdp to remotely log into the windows virtual machine.
   1. xfreerdp /dynamic-resolution +clipboard /cert:ignore /v:20.84.53.115 /u:\_your\_user\_name\_here /p:'\_your\_password\_here'
7. VM-Windows->Event Viewer
8. Free IP location geolocation API: <https://ipgeolocation.io/>
9. Turn off firewall on vm in wf.msc properties on right pane->turn off firewall in domain/private/public profiles
   1. Check by ping is working

Before :

Text

Description automatically generated

After:

Text

Description automatically generated

1. Creating exporter log using .ps1 file

Text

Description automatically generated

1. Log back to azure law to create customized log->Set path to be the output path on vm (C:\ProgramData\failed\_rdp.log)
   1. Make sure the sample log is saved as .log extension, otherwise the Query page in Logs options does not work properly.
   2. Double check the both in-bound and out-bound of the vm should be opened for all ports, fail to do so also result in Query not working properly.
2. Run Query “Failed\_Rdp\_with\_geo\_cl” in logs options to generate results captured in json form predefined in IPGeolocation API.
3. Select the RawData in the Query Results, right clicked it to extract a new filed

Graphical user interface, text, application, email

Description automatically generated

1. Run the powershell script on vm to record the new event logs
2. Go to Azure Sentinel and create a new workbook,
   1. Remove default workbooks
   2. Adding query criteria 
   3. Visualize by map

Graphical user interface, application

Description automatically generated

Chart, scatter chart, bubble chart

Description automatically generated

Graphical user interface

Description automatically generated