Microsoft Sentinel Tutorial with Heatmap Showing Live RDP Brute Force Attacks

Based on Video Created By: Josh Madakor
Blog Created By: Jose Romero

Lab Overview:

The objective of this lab is to set up Microsoft Sentinel, a cloud-based Security Information and Event Management (SIEM) system. Additionally, a virtual machine will be created in the cloud and configured as a honeypot, intentionally made highly vulnerable to the internet. This setup will allow monitoring and logging of various attacks originating from diverse IP addresses worldwide. The ultimate goal is to create a geographical map displaying the origins of these attacks.

Technologies and Protocols Used:

- Microsoft Azure - Microsoft's public cloud computing platform. It provides a broad range of cloud services, including computing, analytics, storage, and networking. Users can choose from these services to develop and scale new applications or run existing applications in the public cloud.
- Services within Azure:
  - Log Analytics Workspace - a logical storage unit in Azure where all log data generated by Azure Monitors are stored.
  - Sentinel (Microsoft's SIEM) - is a cloud-native security information and event management (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise
- PowerShell – is a task automation and configuration management program from Microsoft, consisting of a command-line shell and the associated scripting language.
- Remote desktop protocol - is a secure, interoperable protocol that creates secure connections between clients, servers, and virtual machines.

Overview of technical steps:

The process begins by setting up an Azure subscription, which offers $200 worth of free credits. Next, the objective is to create a virtual machine within Azure, intending to temporarily disable the external firewall and the Windows firewall. This step, though unconventional for ensuring security, is aimed at deliberately exposing the virtual machine to the internet, making it an attractive target for potential attackers. This approach will aid in swiftly gathering data on intrusion attempts from various sources.

Following this, a log repository will be created in Azure, known as a Log Analytics Workspace. This workspace will serve as a centralized hub for ingesting and storing logs generated by the vulnerable virtual machine. To enhance cybersecurity efforts, Microsoft Sentinel will be set up. With Microsoft Sentinel, a visual map will be created to illustrate the origin and characteristics of these intrusion attempts, aiding in identifying the geographic locations and other relevant details about the attackers.

As part of the strategy, PowerShell will be utilized in this lab. The primary motivation behind this choice is that typically, when a login attempt fails on a Windows machine, limited information about the source of the attack is received. However, the intention is to go a step further by using PowerShell to extract the IP address from the Windows logs and transmit this information to a third-party API. This API will enrich the data by providing latitude, longitude, and additional geographical information, such as the country and state or province. The processed data will be sent back to the virtual machine to create custom logs that include this valuable geographic information.

Step by step overview of lab:
1. Create an Azure subscription, which includes free $200 credits for use.
2. Set up a virtual machine in Azure named "honeypot-vm" and disable external and Windows firewalls, making it a target for potential RDP brute force attacks.
3. Utilize a PowerShell script to extract the IP addresses of attackers attempting to compromise the "honeypot-vm." Send these IP addresses to a third-party API to retrieve specific location information.
4. Establish a log repository in Azure known as a Log Analytics Workspace, which will serve as a centralized hub for ingesting and storing logs generated by "honeypot-vm."
5. Configure Microsoft Sentinel to gain insights into intrusion attempts. Create visual maps that display the origin and characteristics of these attacks, allowing the identification of the geographic locations and other relevant details of the attackers.

Lab Topology:
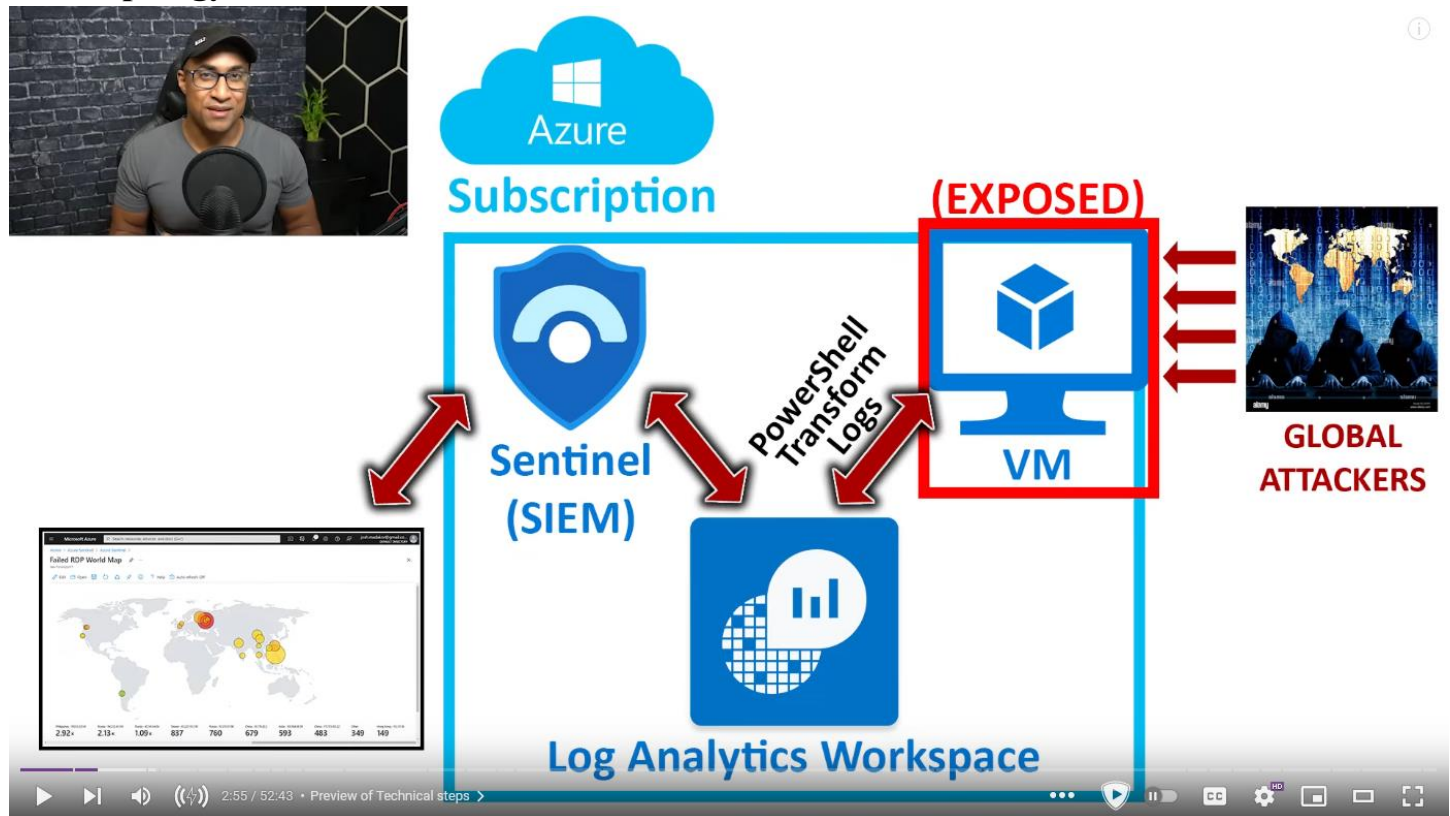
Step 1: Create free Azure account
1. Create an account with link.
2. Click "Start Free" and complete account creation.
3. Click on "Go to the Azure Portal" or go to portal.azure.com once finished with creation of account.

Build in the cloud with an Azure free account

Create, deploy, and manage applications across multiple clouds, on-premises, and at the edge

Start free   Pay as you go
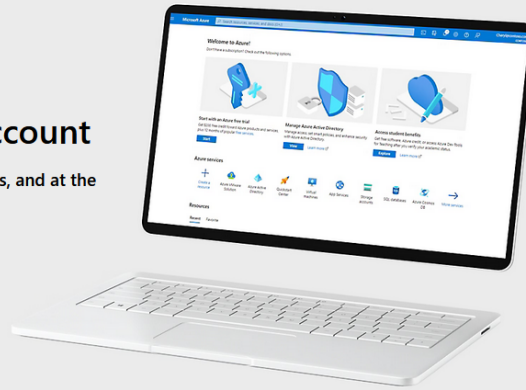
Popular services free for 12 months

↓ View all services

55+ other services free always

↓ View all services

Start with $200 Azure credit

↓ You'll have 30 days to use it—in addition to free services

Step 2: Once on virtual machine page click "create" then "azure virtual machine"

1. In the search bar search and click virtual machine
2. Once in "Create a virtual machine" page it will show "project details" and "instance details"
3. For "Project details" enter information below
   a. Click create new under resource group and name it Honeypotlab
4. For "Instance details" enter information below
   a. Name the virtual machine: honeypot-vm
   b. Under region: (US) East US or your current region
   c. Under Availability options: No infrastructure redundancy required
   d. Under security type: Standard
   e. Under Image: Windows 10 pro, version 22H2 – x64 Gen2
   f. Under size: Standard_B1s - 1 vcpu, 1 GiB memory
   g. Create a username and password for admin account
5. Finally, check confirm box which will leave the rest in their default options

Saturday, October 28, 2023

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ | Azure subscription 1 ⌄

Resource group * ⓘ | (New) Honeypotlab ⌄
Create new

Instance details

Virtual machine name * ⓘ | honeypot-vm ✓

Region * ⓘ | (US) East US ⌄

Availability options ⓘ | No infrastructure redundancy required ⌄

Security type ⓘ | Standard ⌄

Image * ⓘ | ⊞ Windows 10 Pro, version 22H2 - x64 Gen2 (free services eligible) ⌄
See all images | Configure VM generation

> 🔷 This image is compatible with additional security features. <u>Click here to swap to the Trusted launch security type.</u>

VM architecture ⓘ
  ○ Arm64
  ● x64

ⓘ Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ | ☐

> ⓘ You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription. Learn more ⧉

Size * ⓘ | Standard_B1s - 1 vcpu, 1 GiB memory ($7.59/month) (free services eligible) ⌄
See all sizes

Step 3: NIC network security group configuration

1. Click "Next: Disks >" and leave disk page as is
2. Click "Next: Networking >"
3. Once in Networking page under NIC network security group click advanced then create new
   a. A default inbound rule (1000: default-allow-rdp) will show, click trash can icon to the right of it and **remove** it.
   b. Select *Add an inbound rule*
      i. Match the settings of the new rule as follows:
      ii. Set *Destination port ranges*: *
      iii. Priority: 100
      iv. Name: DANGER_ANY_IN
4. Leave the rest of the settings as default Click Add > OK > Review + create - wait a bit to load and click Create

Create network security group ...

DANGER_ANY_IN
honeypot-vm-nsg   ✕

Name *
honeypot-vm-nsg

Inbound rules ⓘ

| 100: DANGER_ANY_IN |
| Any |
| Custom (Any/Any) |

+ Add an inbound rule

Outbound rules ⓘ

No results.

+ Add an outbound rule

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Destination port ranges * ⓘ
*

Protocol
● Any
○ TCP
○ UDP
○ ICMP

Action
● Allow
○ Deny

Priority * ⓘ
100

Name
DANGER_ANY_IN

Step 4: Create Log Analytics Workspace

1. While waiting for the virtual machine to deploy, go back to the search bar, search and click Log Analytics workspaces
2. Click the blue "Create Log Analytics Workspaces" button
3. Under the basics tab select the following
   a. Resource source group: Honeypotlab
   b. Name: law-honeypot1
   c. Region: East US 2
4. Click Review + Create and click Create

Create Log Analytics workspace ...

Basics   Tags   Review + Create

ⓘ A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more ✕

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ   Azure subscription 1

  └ Resource group * ⓘ   Honeypotlab
                           Create new

Instance details

Name * ⓘ   law-honeypot1 ✓

Region * ⓘ   East US

Saturday, October 28, 2023

5

Step 5A: Enable log collection from virtual machine to log analytics workspace

1. Back in the search bar search and click Microsoft Defender for Cloud
2. Once on the dashboard click "Environment Settings" then "law-honeypot1"

Step 5B: Configure Defender Plans & Data Collection Settings

1. Under Defender Plans do the following
   a. Enable Servers ON
   b. Disable SQL servers on machines OFF
   c. Enable Clous Security Posture Management ON
   d. Hit Save
2. Under Data Collection tab select All Events
3. Hit Save

Settings | Data collection

law-honeypot1

✕

Search «

Settings

🛡 Defender plans

🔍 Data collection

💾 Save

Store additional raw data - Windows security events

To help audit, investigate, and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace.

Select the level of data to store for this workspace. Charges will apply for all settings other than "None".
Learn more

All Events

All Windows security and AppLocker events.

Common

A standard set of events for auditing purposes.

Minimal

A small set of events that might indicate potential threats. By enabling this option, you won't be able to have a full audit trail.

None

No security or AppLocker events.

Step 6: Connect log analytics workspace to honeypot-vm

1. Back in the search bar search and click Log Analytics Workspaces
2. Select law-honeypot1 then virtual machines then honeypot-vm
3. Click connect
4. Wait for message confirmation

honeypot-vm ⋯

Virtual machine

🔌 Connect   🔌 Disconnect   🔄 Refresh

Status

This workspace

Workspace Name

law-honeypot1

Message

Step 7: Setup Microsoft Sentinel to workspace

1. Back in the Azure search bar, search and click Microsoft Sentinel
2. Click the blue "Create Microsoft Sentinel" button then select law-honeypot1 then click add

Saturday, October 28, 2023

Add Microsoft Sentinel to a workspace ···

+ Create a new workspace   ↻ Refresh

🔵 Microsoft Sentinel offers a 31-day free trial. See Microsoft Sentinel pricing for more details.

Filter by name...

Workspace ↑↓	Location ↑↓	ResourceGroup ↑↓	Subscription ↑↓	Directory ↑↓
🔵 law-honeypot1	eastus	honeypotlab	Azure subscription 1	Default Directory

Step 8A: Log into virtual machine through host machine

1. Back in the Azure search bar, find honeypot-vm
2. Copy the public IP address

Home >

honeypot-vm 📌 ☆ ···
Virtual machine

🔍 Search «   🖉 Connect ▷ Start ↻ Restart ☐ Stop 📷 Capture 🗑 Delete ↻ Refresh 📱 Open in mobile 🗨 Feedback 🖥 CLI / PS

🔲 Overview
📄 Activity log
👥 Access control (IAM)
🏷 Tags
✕ Diagnose and solve problems

Settings
🔧 Networking
🖉 Connect

∧ Essentials   JSON View

Resource group (move) : Honeypotlab   Operating system : Windows (Windows 10 Pro)
Status   : Running   Size   : Standard B1s (1 vcpu, 1 GiB memory)
Location   : East US   Public IP address : 20.127.84.161
Subscription (move) : Azure subscription 1   Virtual network/subnet : honeypot-vm-vnet/default
Subscription ID   : 7eefedcf-a155-44cc-9188-7efef4bdb47d   DNS name : Not configured
                                              Health state   : -
Tags (edit)   : Add tags

Step 8B: RDP from host window machine

1. Press host machine start button
2. Search and open Remote Desktop Connection
3. Paste the Azure virtual machine IP into computer section
4. Before connecting, click "show options" then display and scale down display configuration for easier viewing
5. Click connect
6. In the enter credentials window click "more choices" then "Use a different account"
7. Enter invalid credentials in order to generate a log for later viewing.
8. Then, enter the credentials created for the Azure virtual machine in Step 3, click OK.
9. Accept the certificate warning
10. Logging in should be completed when "Remote Desktop Connection" shows at the top left of the screen.

Saturday, October 28, 2023
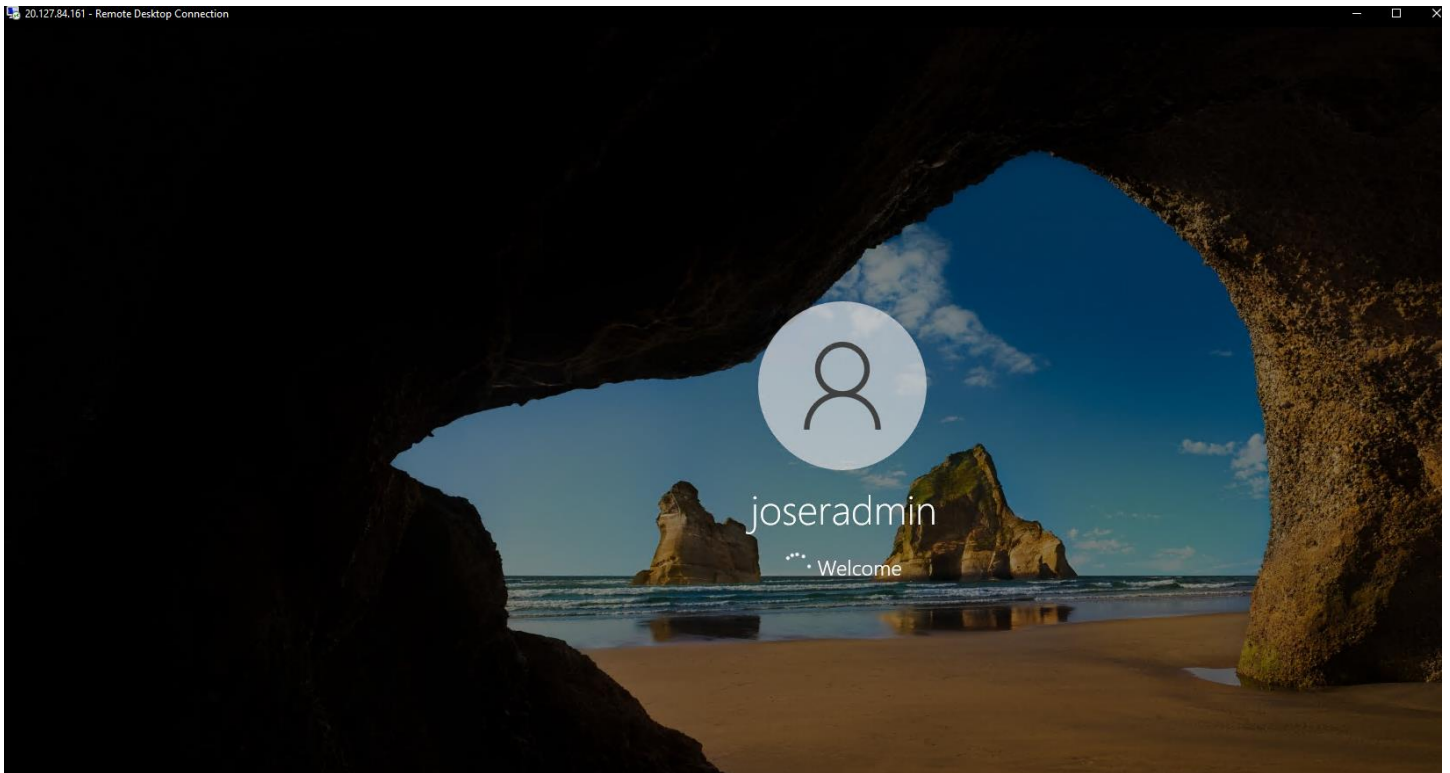
Step 10: Setting up virtual machine

1. Click NO to all privacy settings and Accept
2. Open and set up edge
3. Press start button, search, and click Event Viewer
4. Click windows logs then security then filter current log by "Audit Failure" (failed login attempt)
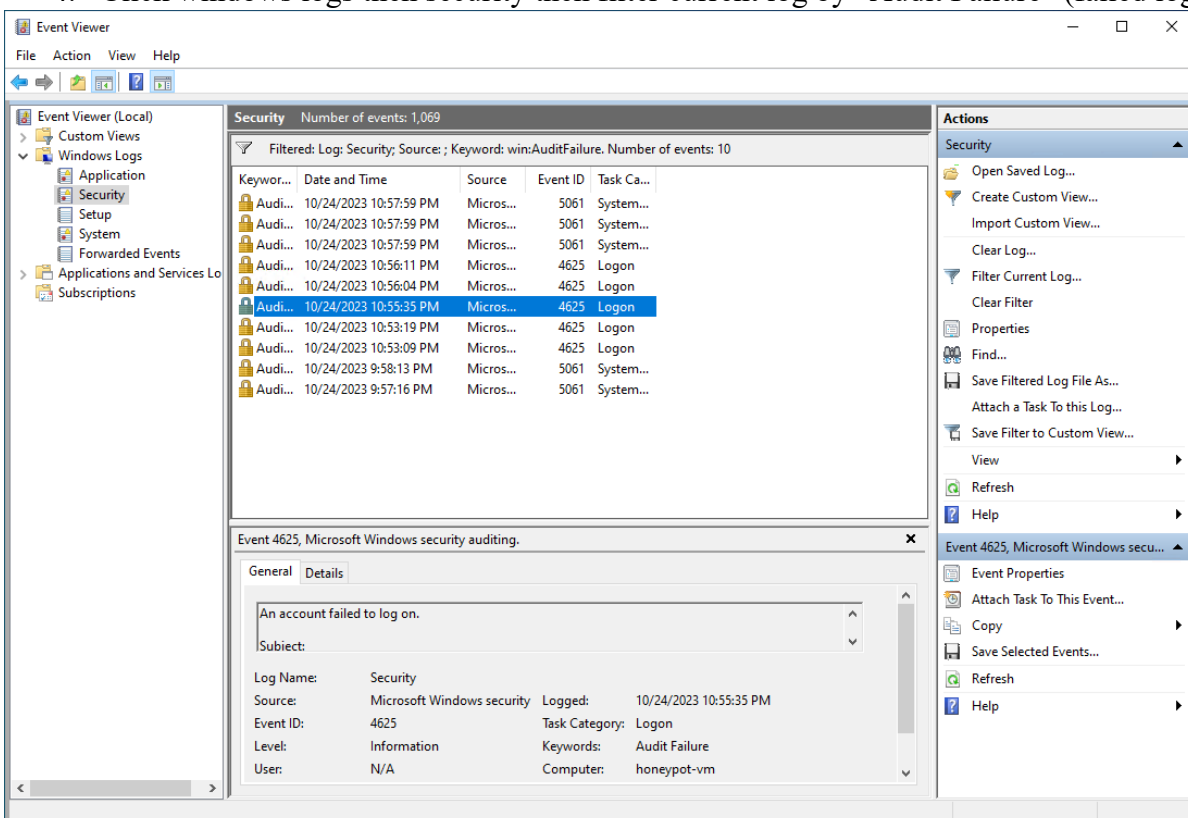
Step 11: Turn off firewall

1. Press the start button on host machine and search CMD to open command prompt and ping (EX. ping 192.222.129.200) the virtual machine, it should not work yet
2. Search and open wf.msc on virtual machine
3. Click Windows Defender Firewall Properties near the middle of the page
4. Under the Domain Profile
    a. Firewall state: OFF
5. Under Private Profile
    a. Firewall state: OFF
6. Under Public Profile
    a. Firewall state: OFF
7. Click Apply then OK
8. Try to ping the virtual machine again from your host machine, it should now work
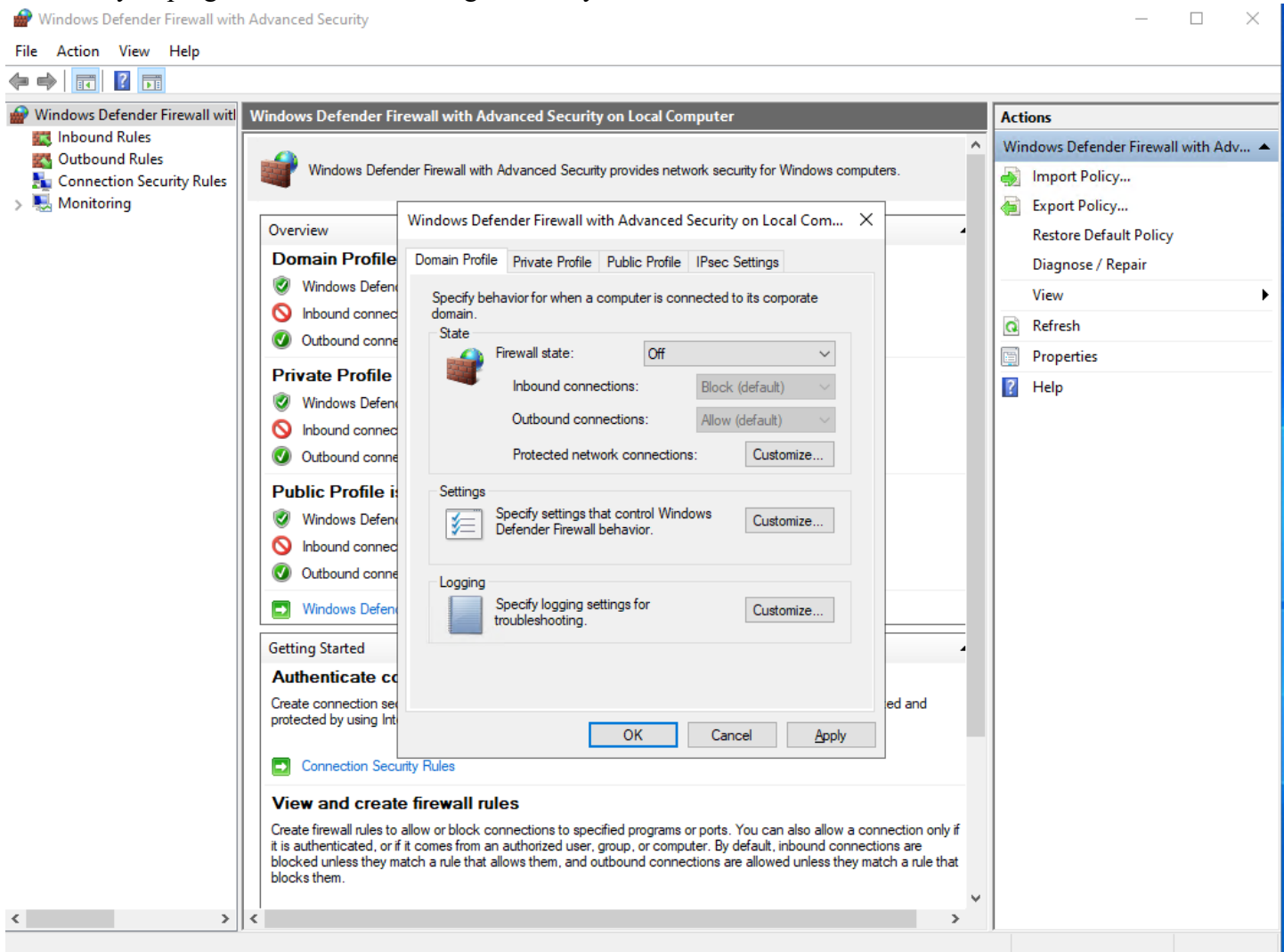
Step 12A: Download PowerShell Script

1. Open PowerShell ISE
2. Copy/paste the code into a new ps1 file and name it Log_Exporter then save it to the desktop of the virtual machine
3. Get API key - IPGeolocation

4. Create an account and log in
5. Copy and paste API key in your PowerShell script $API_KEY = "your API key"
6. Save file.
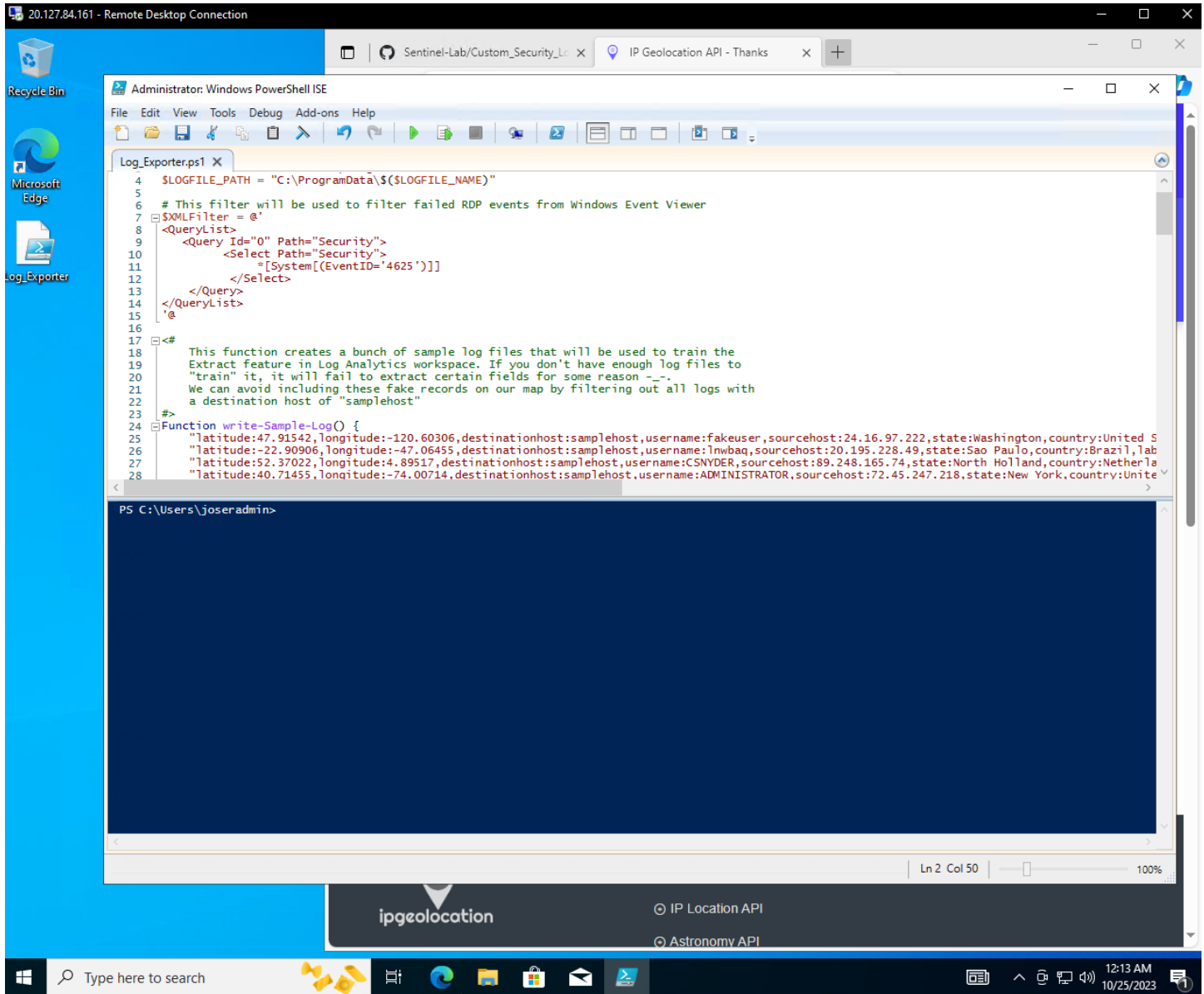
Step 12B: Run and Test PowerShell Script
1. Test and run the script pass pressing green play button at top of window
2. Purple logs should appear indicating latitude/longitude of failed logins (some sample logs & some audit failures)

Saturday, October 28, 2023

```
10          <Select Path="Security">
11              *[System[(EventID='4625')]]
12          </Select>
13      </Query>
14  </QueryList>
15  '@
16
17  <#
18      This function creates a bunch of sample log files that will be used to train the
19      Extract feature in Log Analytics workspace. If you don't have enough log files to
20      "train" it, it will fail to extract certain fields for some reason -_-.
21      We can avoid including these fake records on our map by filtering out all logs with
22      a destination host of "samplehost"
23  #>
24  Function write-Sample-Log() {
25      "latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United S
26      "latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,lab
27      "latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherla
28      "latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:Unite
29      "latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,country
30      "latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,country:Malaysia,label:Mala
31      "latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turkey,l
32      "latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,country:Russia,label:Russia
33      "latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Nether
34      "latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Belize,label:Belize
```

```
    Directory: C:\ProgramData

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/25/2023  12:32 AM              0 failed_rdp.log
latitude:10.79154,longitude:106.73084,destinationhost:honeypot-vm,username:AZUREUSER,sourcehost:45.118.146.131,state:Ho Chi Minh City,label:Vietnam -
45.118.146.131,timestamp:2023-10-25 00:12:56
latitude:10.79154,longitude:106.73084,destinationhost:honeypot-vm,username:STUDENT,sourcehost:45.118.146.131,state:Ho Chi Minh City,label:Vietnam - 45
.118.146.131,timestamp:2023-10-25 00:12:50
latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joseradmin1$,sourcehost:192.145.116.249,state:Virginia,label:United States
- 192.145.116.249,timestamp:2023-10-24 22:56:11
latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joseradmin1$,sourcehost:192.145.116.249,state:Virginia,label:United States
- 192.145.116.249,timestamp:2023-10-24 22:56:04
latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joserradmin1$,sourcehost:192.145.116.249,state:Virginia,label:United States
- 192.145.116.249,timestamp:2023-10-24 22:55:35
latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joseradmin1$,sourcehost:192.145.116.249,state:Virginia,label:United States
- 192.145.116.249,timestamp:2023-10-24 22:53:19
latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joseradmin1$,sourcehost:192.145.116.249,state:Virginia,label:United States
- 192.145.116.249,timestamp:2023-10-24 22:53:09
```

Step 13A: Create custom IPGeolocation in Log Analytics Workspace

1. Back on host machine got to azure portal then search and click Log Analytics Workspace then law-honeypot1 then tables then create then new custom log (MMA-Based)
2. Back on virtual machine search RUN then search C:\ProgramData\ and open the failed_rdp.txt file.
3. Open and copy all the sample logs.
4. Back on the host machine, open notes and paste our sample logs.
5. Save the file in a txt format and upload it in the Create a custom log page. Click next and you should see the sample logs
6. Click next and under the collection paths tab select windows under type and C:\ProgramData\failed_rdp.log under path
7. Click next and under details tab type in for custom log name "FAILED_RDP_WITH_GEO"
8. Click next then Create then Review + Create

Saturday, October 28, 2023

Create a custom log · · ·

✓ **Sample**   ② **Record delimiter**   ③ Collection paths   ④ Details   ⑤ Review + Create

Select a record delimiter. Select **New line** for files with a single entry per line, or specify a **Timestamp** delimiter for entries spanning more than one line. Learn more

Record delimiter

Select record delimiter   ● New line   ○ Timestamp

Preview

Records

latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,s...

latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,st...

latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,st...

latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.2...

latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.2...

latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Pen...

latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196....

latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:nu...

latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,...

latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:n...

latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:...

latitude:10.79154,longitude:106.73084,destinationhost:honeypot-vm,username:AZUREUSER,sourcehost:45.118.14...

latitude:10.79154,longitude:106.73084,destinationhost:honeypot-vm,username:STUDENT,sourcehost:45.118.146.1...

latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joseradmin1$,sourcehost:192.145....

latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joseradmin1$,sourcehost:192.145....

latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joserradmin1$,sourcehost:192.145...

latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joseradmin1$,sourcehost:192.145....

latitude:39.05232,longitude:-77.48270,destinationhost:honeypot-vm,username:joseradmin1$,sourcehost:192.145....

Step 13B: Create custom IPGeolocation in Log Analytics Workspace

1. Go back to log analytics workspace then click law-honeypot1 then General then Logs then type in SecurityEvent and click blue run button. It should show the same security logs from our virtual machines Event Viewer.
2. Give it time and search: FAILED_RDP_WITH_GEO_CL it will return sample logs.
3. Take a look at the sample logs and find the geo-data

Step 14: Extract and categorize geo-data from the raw data of the sample logs

1. Type in the query log the following:
   FAILED_RDP_WITH_GEO_CL

```
|extend username = extract(@"username:([^,]+)", 1, RawData),
     timestamp = extract(@"timestamp:([^,]+)", 1, RawData),
     latitude = extract(@"latitude:([^,]+)", 1, RawData),
     longitude = extract(@"longitude:([^,]+)", 1, RawData),
     sourcehost = extract(@"sourcehost:([^,]+)", 1, RawData),
     state = extract(@"state:([^,]+)", 1, RawData),
     label = extract(@"label:([^,]+)", 1, RawData),
     destination = extract(@"destinationhost:([^,]+)", 1, RawData),
     country = extract(@"country:([^,]+)", 1, RawData)
|where destination != "samplehost"
|where sourcehost != ""
|summarize event_count=count() by timestamp, label, country, state, sourcehost, username, destination,
longitude, latitude
```

2. Take a look at the logs and check if the RawData was successfully parsed out as label, country, state, source host, username, destination, longitude, latitude, event count

Step 15A: Setup Map within Microsoft Sentinel

1. Search and click Microsoft Sentinel then choose law-honeypot1 and under Threat management choose Workbooks then click Add workbook
2. Click edit then click the " … "on the right side on the screen and remove the two widgets.
3. Click Add then Add query and paste the following into the query:
   FAILED_RDP_WITH_GEO_CL

```
|extend username = extract(@"username:([^,]+)", 1, RawData),
     timestamp = extract(@"timestamp:([^,]+)", 1, RawData),
     latitude = extract(@"latitude:([^,]+)", 1, RawData),
     longitude = extract(@"longitude:([^,]+)", 1, RawData),
     sourcehost = extract(@"sourcehost:([^,]+)", 1, RawData),
     state = extract(@"state:([^,]+)", 1, RawData),
     label = extract(@"label:([^,]+)", 1, RawData),
     destination = extract(@"destinationhost:([^,]+)", 1, RawData),
     country = extract(@"country:([^,]+)", 1, RawData)
```

Saturday, October 28, 2023

|where destination != "samplehost"
|where sourcehost != ""
|summarize event_count=count() by timestamp, label, country, state, sourcehost, username, destination, longitude, latitude

Step 15B: Attack Visualization on Map within Microsoft Sentinel

1. Click Run Query
2. Under Size select Full
3. Click map settings
4. Under Metric Label select country
5. Hit Apply then Save and Close
6. The map should show where the virtual machine is being attacked from
7. The failed logins might be the only things on the map made, but after some time refresh and look again.

Step 15C: Save Attack Visualization

1. Hit save and close
2. Hit the floppy disk at the top to save the map.
3. Title: Failed RDP World Map
4. Location: East US
5. Resource group: honeypot-lab
6. Click apply
7. And done!
8. Click Auto refresh ON to refresh every so often (make sure PowerShell script is running) to load more logs into the map

Failed RDP World Map 📌 ⋯

law-honeypot1

✏️ Edit 🗁 Open 💾 ↻ ☁️ 📌 ☺ ? Help 🕐 Auto refresh: 15 minutes

China	United States	Vietnam	Russia
524	5	2	2

Step 16: Delete Lab when completed

1. Once you are finished with the lab delete the resources
2. Search and click Resource group then honeypot-lab then delete resource group
3. Type the name honeypot-lab to confirm deletion

Saturday, October 28, 2023